

Web Interface
for
All OmniConverter[®] and RuggedNet[®]
Switch Products

USER MANUAL

Table of Contents

1.0	Overview.....	4
1.1	New Features.....	4
2.0	Web Interface	5
2.1	Overview	5
2.1.1	Module Real Time LED Indicators Section	6
2.1.2	Module Menu Option Section	6
2.1.3	Module Identification Section.....	7
2.1.4	Module Configuration Section.....	7
2.2	Login	9
2.3	Module Menu Option Section	10
2.3.1	Status.....	10
2.3.1.1	Module Overview	10
2.3.1.2	Module Information	13
2.3.1.3	Port Statistic Overview.....	14
2.3.1.4	Port Statistics Detailed.....	15
2.3.1.5	SFP Port Info	17
2.3.2	Hardware Configuration Screens.....	20
2.3.2.1	DIP Switch	20
2.3.2.2	Port / Interface Overview	23
2.3.2.3	Port / Interface Detailed	25
2.3.3	Service Management.....	30
2.3.3.1	Module	30
2.3.3.2	IPv4 Configuration	32
2.3.3.3	SNMP.....	34
2.3.3.4	Time and Date.....	39
2.3.3.5	NTP / SNTP	40
2.3.3.6	LLDP	41
2.3.3.7	IGMP	45
2.3.4	Service Activation	49
2.3.4.1	VLAN Configuration	49
2.3.4.2	VLAN Interface.....	51
2.3.4.3	Rate Limiting & Shaping	53
2.3.4.4	Cos / QoS	59
2.3.5	Protection.....	61
2.3.5.1	Link Redundancy	61
2.3.5.2	RSTP	62
2.3.5.3	MRP	65
2.3.5.4	LAG/LLDP.....	70
2.3.6	Security.....	75
2.3.6.1	Authenticate, Authorize, Account (AAA).....	75
2.3.6.2	Access Control List (ACL).....	80
2.3.6.3	Secure Shell (SSH).....	81
2.3.6.4	User	83
2.3.6.5	Storm Control.....	88
2.3.7	Maintenance	90
2.3.7.1	Firmware Upgrade	90
2.3.7.2	Module Maintenance.....	92
2.3.7.3	Browser Settings.....	93
2.3.7.4	Syslog	94
2.3.7.5	SNMP Traps.....	97
2.3.7.6	SMTP.....	99
2.3.7.7	Splash Screen.....	100

3.0	Appendix A: Firmware Update	101
3.1	Overview	101
3.2	Save Current Settings	101
3.3	Copy the Files to Your Hard Drive.....	101
3.4	Updating the Firmware Using the Web Interface	101
4.0	Warranty and Copyright.....	104
5.0	Customer Support Information	105

1.0 OVERVIEW

The Web Interface provides configuration and monitoring of the following products:

OmniConverter G/M	4 and 8 Port Switches
OmniConverter GPoE+/M	4 and 8 Port PoE Switches
OmniConverter GHPoE/M	4 Port High Power PoE Switch
OmniConverter GHPoEBT/M	4 Port 802.3bt PoE Switch
RuggedNet G/Mi	4 and 8 Port Industrial Switches
RuggedNet GPoE+/Mi	4 and 8 Port PoE Industrial Switches
RuggedNet GHPoE/Mi	4 Port High Power PoE Industrial Switch
RuggedNet GHPoEBT/Mi	4 Port 802.3bt PoE Industrial Switch



The module functions can be configured using the IP-based Web management interface. The IP-based web management can be accessed through any of the Ethernet RJ-45 or fiber ports and facilitates the configuration and real-time operation monitoring of each port.

The factory default IP address is 192.168.1.220.

The web management software provides intuitive and easy-to navigate menu options.

NOTE: The Web Interface is compatible with Microsoft Internet Explorer 11 and later, Microsoft Edge version 39 and later, Firefox version 53 and later, Google Chrome version 46 and later, and Safari version 10 and later.

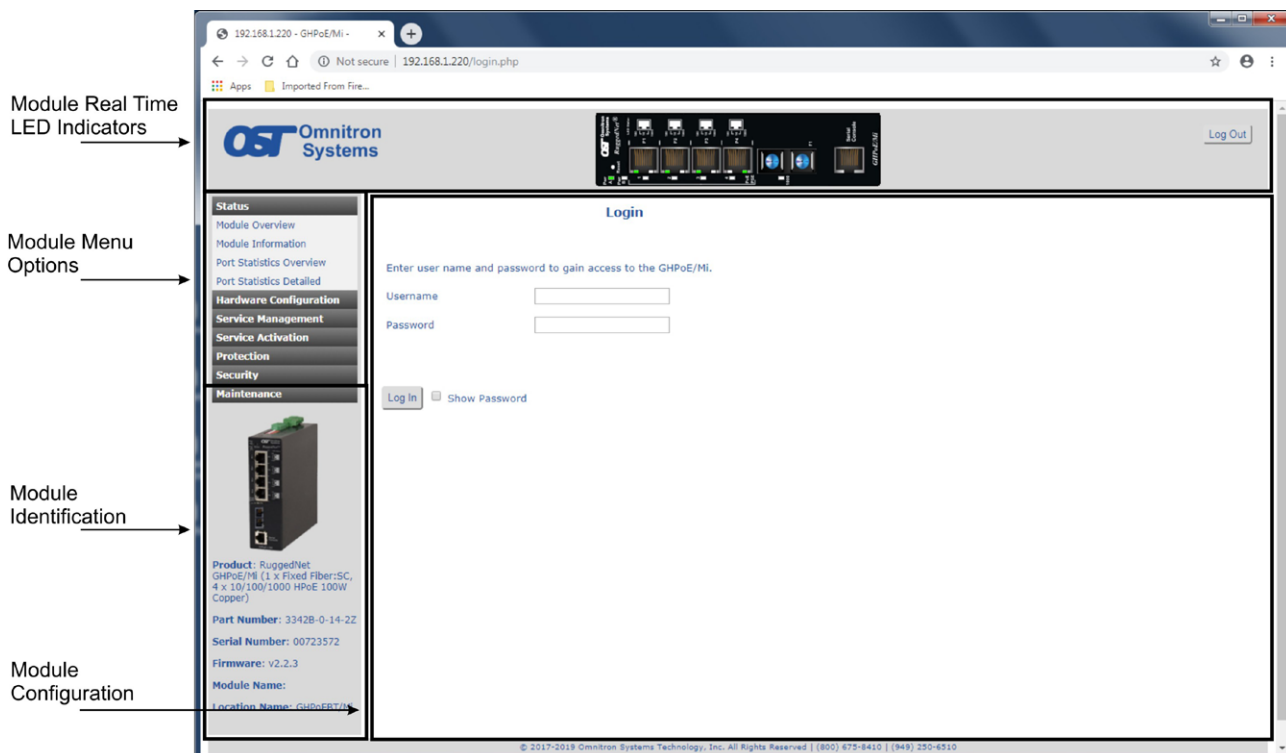
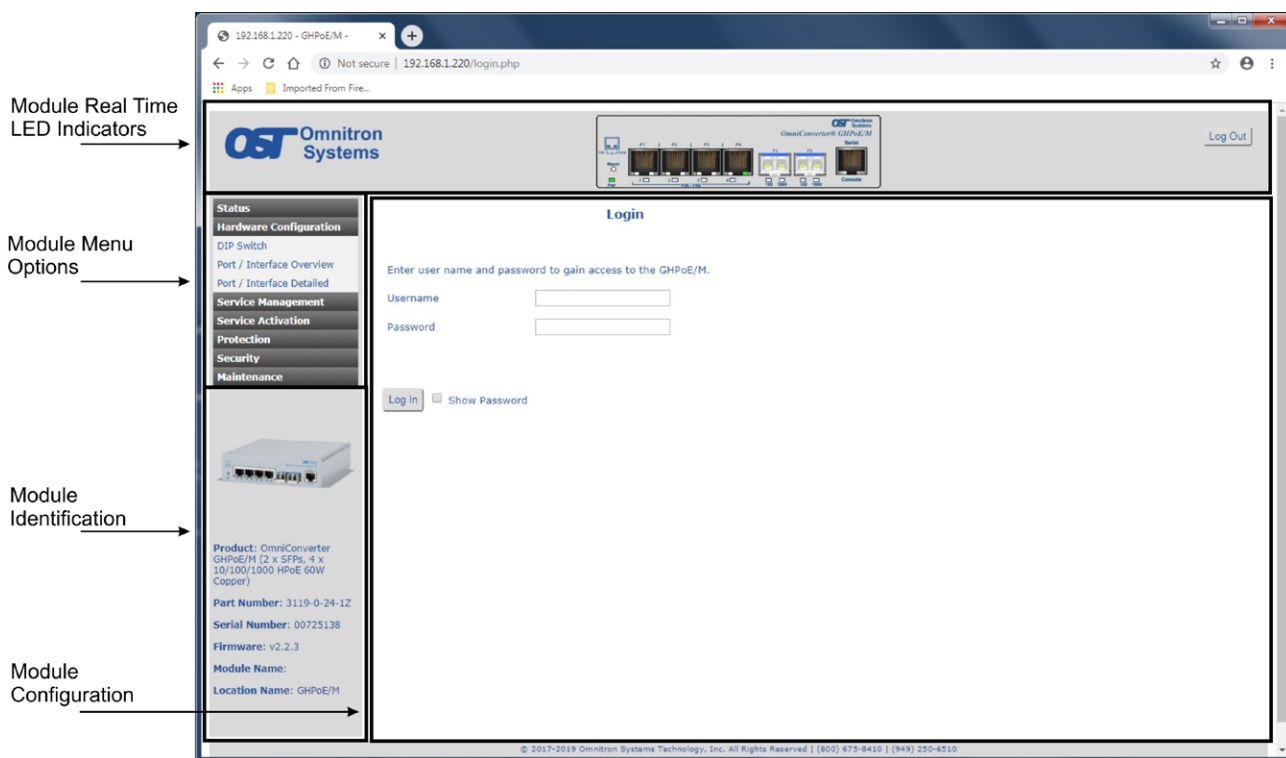
1.1 NEW FEATURES

Firmware release 2.2 adds Internet Group Management Protocol (IGMP), Link Aggregation Groups (LAG), Media Redundancy Protocol (MRP), Simple Mail Transfer Protocol (SMTP), Storm Prevention and multiple user support.

2.0 WEB INTERFACE

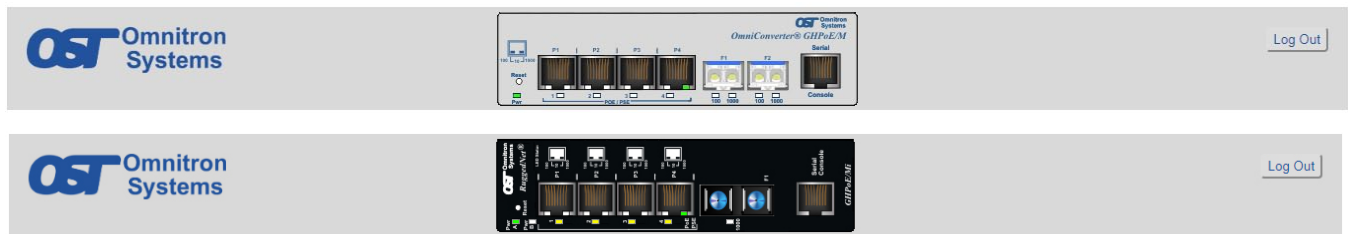
2.1 OVERVIEW

The web management interface is divided into four sections; Module Real Time LED Indicators, Module Menu Options, Module Identification and Module Configuration.



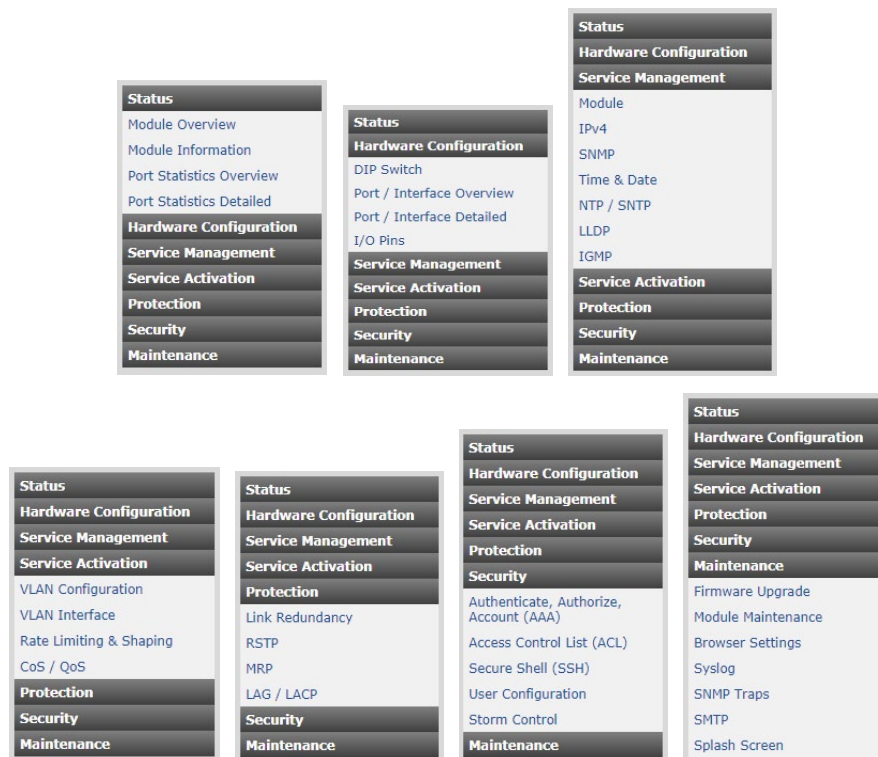
2.1.1 Module Real Time LED Indicators Section

This section of the web interface provides real time information on the status of the LEDs on the module. Status is updated based on the refresh rate of the page (see Browser Settings) The exact model of the module is displayed with the corresponding LED indicators.



2.1.2 Module Menu Option Section

This section of the web interface provides access to the available menu options. Clicking on the menu option expands the selection showing the available sub menu options.



2.1.3 Module Identification Section

This section of the web interface provides information on the module. This includes model description, part number, serial number, firmware revision, module name and location.



Product: OmniConverter
GHPoE/M (2 x SFPs, 4 x 10/100/1000 HPoE 60W Copper)
Part Number: 3119-0-24-1Z
Serial Number: 00725138
Firmware: v2.2.3
Module Name:
Location Name: GHPoE/M



Product: RuggedNet
GHPoE/Mi (1 x Fixed Fiber:SC, 4 x 10/100/1000 HPoE 90W Copper)
Part Number: 3342B-0-14-2Z
Serial Number: 00723572
Firmware: v2.2.1
Module Name:
Location Name: GHPoE/Mi

2.1.4 Module Configuration Section








This section of the web interface displays the configuration options based on the menu option selected.

Module Configuration screen will vary depending on the model.

Module Overview

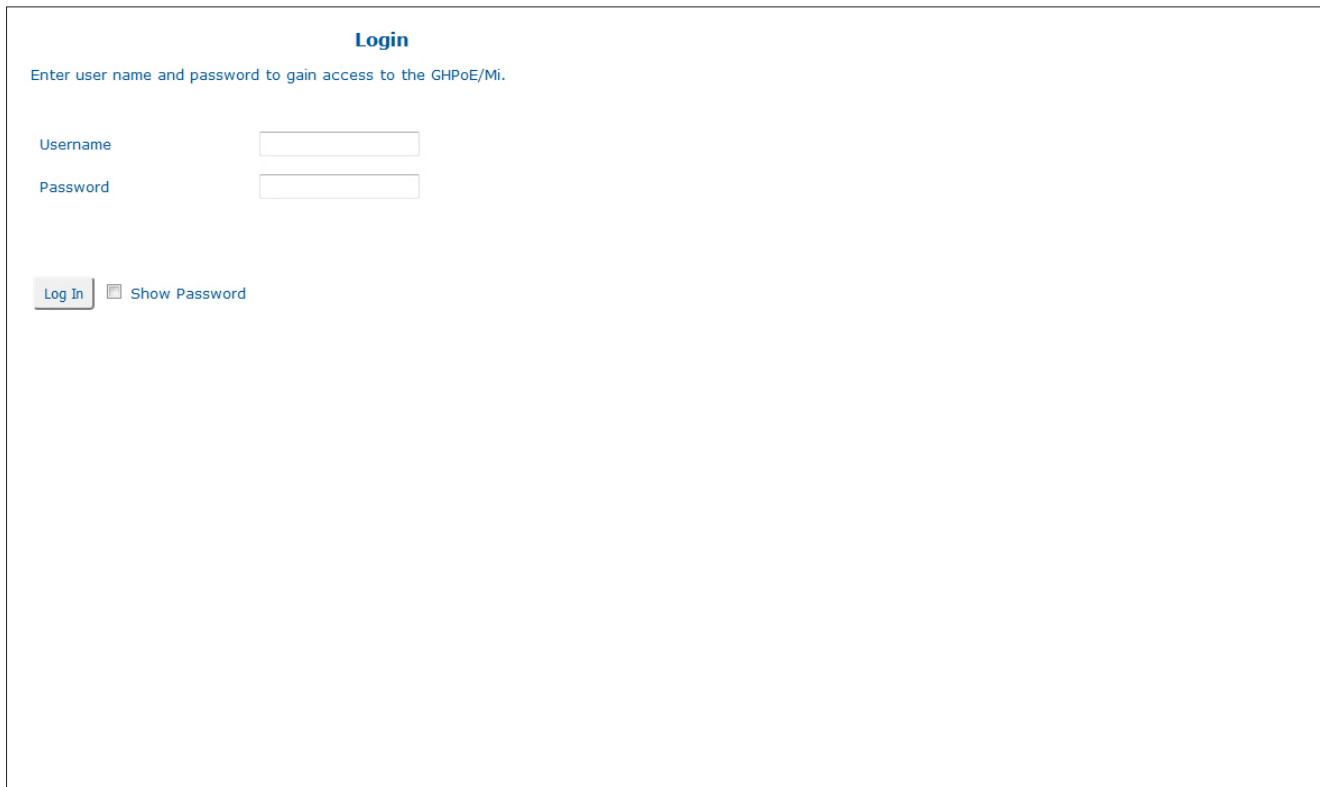
Module Mode										
Single Switch, Normal Mode, Not Protected										
Port Status					PoE Status					
Port	Port Type	Port Function	Link State	Port State	PSE State	PD State	PD Class	Voltage (V)	Current (ma)	Power (W)
F1	SFP-Empty	Port		No link	---	---	---	---	---	---
F2	SFP-Empty	Port		No link	---	---	---	---	---	---
P1	Copper PSE	Port		1000 FDX	(Active)	802.3af (15.4W)	3	56.65	98.63	5.59
P2	Copper PSE	Port		1000 FDX	(Active)	HPoE (60W)	4	47.5	243	11.54
P3	Copper PSE	Port		100 FDX	(Active)	802.3af (15.4W)	3	56.41	42.97	2.42
P4	Copper PSE	Port		1000 FDX	(Non-PD)	---	---	---	---	---
Power Status										
Pwr A	Power input		54.6VDC		Total current	416mA				
Pwr B	Power input		54.6VDC							
<div>Refresh<input checked="" type="checkbox"/> Auto Refresh</div>										

Module Overview

Module Mode				
Single Switch, Normal Mode, Not Protected				
Port Status				
Port	Port Type	Port Function	Link State	Port State
F1	SFP-Empty	Port		No link
F2	SFP-Empty	Port		No link
P1	Copper	Port		No link
P2	Copper	Port		No link
P3	Copper	Port		No link
P4	Copper	Port		No link
Power Status				
Pwr	Power input		52.9VDC	Total current 52mA
<div>Refresh<input checked="" type="checkbox"/> Auto Refresh</div>				

2.2 LOGIN

Enter the IP address of the module into the web browser. The module will respond with the Login screen. Enter the Username and Password to gain access to the module.



The screenshot shows a web browser window displaying a login interface. At the top, the word "Login" is centered in blue. Below it, a message in blue text reads: "Enter user name and password to gain access to the GHPoE/Mi." There are two input fields: "Username" and "Password", each with a corresponding text label to its left. Below the "Password" field, there is a "Log In" button and a checkbox labeled "Show Password".

A model with two (2) fiber ports and four (4) RJ-45 ports is used for all examples in this manual.

2.3 MODULE MENU OPTION SECTION

2.3.1 Status

The following options are available.



2.3.1.1 Module Overview

The Module Overview screen provides information on the Port Types (copper or fiber), Link State, Port State (speed, duplex), PSE State (active or standby) and PD related information.

Module Overview screen will vary depending on the model.

Module Overview

Module Mode








Single Switch, Normal Mode, Not Protected

Port Status					PoE Status					
Port	Port Type	Port Function	Link State	Port State	PSE State	PD State	PD Class	Voltage (V)	Current (ma)	Power (W)
F1	SFP-Empty	Port		No link	---	---	---	---	---	---
F2	SFP-Empty	Port		No link	---	---	---	---	---	---
P1	Copper PSE	Port		1000 FDX	(Active)	802.3af (15.4W)	3	56.65	98.63	5.59
P2	Copper PSE	Port		1000 FDX	(Active)	HPoE (60W)	4	47.5	243	11.54
P3	Copper PSE	Port		100 FDX	(Active)	802.3af (15.4W)	3	56.41	42.97	2.42
P4	Copper PSE	Port		1000 FDX	(Non-PD)	---	---	---	---	---
Power Status										
Pwr A	Power input		54.6VDC		Total current	416mA				
Pwr B	Power input		54.6VDC							

Refresh

☒ Auto Refresh

Module Overview

Module Mode				
Single Switch, Normal Mode, Not Protected				
Port Status				
Port	Port Type	Port Function	Link State	Port State
F1	SFP-Empty	Port		No link
F2	SFP-Empty	Port		No link
P1	Copper	Port		No link
P2	Copper	Port		No link
P3	Copper	Port		No link
P4	Copper	Port		No link
Power Status				
Pwr	Power input		52.9VDC	Total current 52mA

Refresh

☒ Auto Refresh

NOTE: The number of ports and power supplies will vary depending on the model.

Port Status

Port

Indicates the port designation.

Port Type

Indicates if the port is a fixed fiber, SFP or copper port.

Port Function

Indicates if the port is configured as a standard switch port or a primary or secondary port for Link Redundancy.

Link State

Displays the state of the link (green or amber). Green indicates a good active link. Amber indicates a possible problem. See Section 5.0 Verify Operation.

Port State

Indicates the link, speed and duplex of the port.

PoE Status (only displayed on models supporting PoE power)

PSE State

Indicates if the port is an active PoE connection or a non-PoE device. It also provides a graphical indication of the amount of power provided to the attached PD.

PD State

Displays the type of IEEE PoE device discovered (802.3af, 802.3at or HPoE) and the amount of power required by the class of PD. 802.3bt is displayed as HPoE.

PD Class

Displays the class of IEEE PoE device discovered (up to class 8).

Voltage (VDC)

Displays the amount of voltage provided.

Current (ma)

Displays the amount of current provided.

Power (W)

Displays the amount of power provided.

Power Supply Status

Pwr A

Displays a green indication if the power is applied and displays the detected voltage. Pwr is displayed on modules with one power input.

Pwr B

Displays a green indication if the power is applied and displays the detected voltage. Pwr B is only displayed on modules with two power inputs.

A **Logout** button is located in the upper right corner of the screen. Click the **Logout** button to exit the web interface.

A **Refresh** button and **Auto Refresh** check box is also located at the bottom left corner of the screen. Click the **Refresh** button to update the screen. Click on the **Auto Refresh** check box for automatic refreshing of the screen. The rate of refresh is configured from the Browser Settings screen, found under Maintenance.

2.3.1.2 Module Information

The Module Information screen provides information on the part number, serial number, firmware revision, manufacturing date, MAC address, temperature as well as information on uptime and system utilization.

Module Information screen will vary depending on the model.

Module Information	
Item Name	Item Value
Module Type	OmniConverter GHPoE/M
Port Types	2 x SFPs, 4 x 10/100/1000 HPoE 60W Copper
Part Number	3119-0-24-1Z
Serial Number	00725138
Firmware Revision	v2.2.3
Product Revision	10
Manufacturing Date	19-Mar-2019
MAC Address	00-06-87-02-fa-a0
System Time	01-Jan-2000 00:37:25 AM
System Up Time	0 days, 0 hours, 34 mins, 7 secs
CPU Utilization	8%
RAM Utilization	75.1MB out of 507.6MB (14.8%)
Flash Utilization	165.3MB out of 798.5MB (20.7%)
Module Temperature	48° C
<div>Refresh <input checked="" type="checkbox"/> Auto Refresh</div>	

A **Refresh** button and **Auto Refresh** check box is also located at the bottom left corner of the screen. Click the **Refresh** button to update the screen. Click on the **Auto Refresh** check box for automatic refreshing of the screen. The rate of refresh is configured from the Browser Settings screen, found under Maintenance.

2.3.1.3 Port Statistic Overview

The Port Statistic Overview screen provides information on transmit and receive data traffic for each port on the module.

Port Statistics Overview								
Port	Packets Rx	Packets Tx	Octets Rx	Octets Tx	Errors Rx	Errors Tx	Dropped Rx	Dropped Tx
F1	0	0	0	0	0	0	0	0
F2	0	0	0	0	0	0	0	0
P1	107	194	33177	65647	0	0	0	0
P2	101	191	31658	66296	0	0	0	0
P3	40	234	26352	69527	0	0	0	0
P4	387	526	56990	279896	0	0	0	0

Clear Counters Refresh ☒ Auto Refresh

NOTE: The number of ports will vary depending on the model.

A **Clear Counters** button is located at the bottom left corner of the screen to clear the statistic on the module. Click on the **Clear Counters** button to clear the statistics.

A **Refresh** button and **Auto Refresh** check box is also located at the bottom left corner of the screen. Click the **Refresh** button to update the screen. Click on the **Auto Refresh** check box for automatic refreshing of the screen. The rate of refresh is configured from the Browser Settings screen, found under Maintenance.

2.3.1.4 Port Statistics Detailed

The Port Statistic Detailed screen provides more detailed information on the transmit and receive data traffic. Use the Port Selection pull-down menu to select the port to be displayed.

The module has eight transmit queues for data traffic of different priorities. The Port Statistic Detailed screen displays the number of packets in each queue.

Port Statistics Detailed			
Port Selection: F1 ▼			
Receive (Rx) Counters		Transmit (Tx) Counters	
Type	Total	Type	Total
Octets	0	Octets	0
Packets	0	Packets	0
Unicast Packets	0	Unicast Packets	0
Multicast Packets	0	Multicast Packets	0
Broadcast Packets	0	Broadcast Packets	0
Pause Packets	0	Pause Packets	0
Errored Packets	0	Errored Packets	0
Dropped Packets	0	Dropped Packets	0
Receive Packet By Size		Packets per Queue	Total
64 bytes	0	Queue 0	0
65-127 bytes	0	Queue 1	0
128-255 bytes	0	Queue 2	0
256-511 bytes	0	Queue 3	0
512-1023 bytes	0	Queue 4	0
1024-10240 bytes	0	Queue 5	0
		Queue 6	0
		Queue 7	0

[Clear Counters](#) [Refresh](#) ☒ Auto Refresh

Receive (Rx) and Transmit (Tx) Counters

Octets

The total number of good bytes of data transmitted/received by a port.

Packets

The total number of good Unicast, Multicast and Broadcast packets transmitted/received by a port.

Unicast Packets

The total number of Unicast packets transmitted/received by a port.

Multicast Packets

The total number of Multicast packets transmitted/received by a port.

Broadcast Packets

The total number of Broadcast packets transmitted/received by a port.

Pause Packets

The total number of Pause packets transmitted/received by a port.

Error Packets

The total number of Excessive Collision and Late Collision packets transmitted/received by a port.

Dropped Packets

The total number of dropped packets transmitted/received by a port.

Receive Packet by Size

64 bytes

The total number of packets (including bad packets) received that were 64 octets in length.

65-127 bytes

The total number of packets (including bad packets) received that were between 65 and 127 octets in length.

128-255 bytes

The total number of packets (including bad packets) received that were between 128 and 255 octets in length.

256-511 bytes

The total number of packets (including bad packets) received that were between 256 and 511 octets in length.

512-1023 bytes

The total number of packets (including bad packets) received that were between 512 and 1023 octets in length.

1024-[max size] bytes

The total number of packets (including bad packets) received that were between 1024 and maximum allowed frame size in length.

Transmitted Packets per Queue

Indicates the number of packets in each priority queue (0 is the lowest, 7 is the highest).

A ***Clear Counters*** button is located at the bottom left corner of the screen to clear the statistic on the module. Click on the ***Clear Counters*** button to clear the statistics.

A ***Refresh*** button and ***Auto Refresh*** check box is also located at the bottom left corner of the screen. Click the ***Refresh*** button to update the screen. Click on the ***Auto Refresh*** check box for automatic refreshing of the screen. The rate of refresh is configured from the Browser Settings screen, found under Maintenance.

2.3.1.5 SFP Port Info

SFP Port Info screen is only available on models with SFP ports.

The SFP Port Info screen provides the A0/A2 Hexadecimal and A0/A2 Decoded values for the installed SFP transceiver.

Use the Port Selection pull-down menu to select the port to be displayed. Use the Page Selection pull-down to select the A0/A2 Hexadecimal or A0/A2 Decoded pages to be displayed.

SFP Port Information

Port Selection: F1 Page Selection: A0 Hexadecimal

	Hexadecimal																ASCII Equivalent
Row	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF	
00:	03	04	07	00	00	00	02	12	00	01	01	01	0d	00	0c	78x
10:	00	00	00	00	4f	6d	6e	69	74	72	6f	6e	20	53	79	73Omnitron Sys
20:	74	65	6d	73	00	00	06	87	37	32	30	37	2d	31	20	20	tems...7207-1
30:	20	20	20	20	20	20	20	20	30	31	30	30	05	1e	00	03	0100....
40:	00	1a	00	00	38	42	32	30	30	34	30	30	34	37	20	208B20040047
50:	20	20	20	20	30	38	31	31	32	37	20	20	58	b0	01	61	081127 X..a
60:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
70:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
80:	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
90:	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
a0:	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
b0:	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
c0:	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
d0:	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
e0:	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
f0:	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff

Refresh

☒ Auto Refresh

A **Refresh** button and **Auto Refresh** check box is also located at the bottom left corner of the screen. Click the **Refresh** button to update the screen. Click on the **Auto Refresh** check box for automatic refreshing of the screen. The rate of refresh is configured from the Browser Settings screen, found under Maintenance.

Use the Page Selection pull-down to select the A0 or A2 Decoded pages. Select A0.

SFP Port Information

Port Selection: F1 Page Selection: A0 Decoded

Variable Name	Value
Identifier	SFP/SFP+
Extended Identifier	SFP Module
Connector	LC
Transceiver	1000BASE-LX, Long distance (L), Single Mode (SM), 100 MBytes/sec
Encoding	8B/10B
Nominal Bit Rate (Mbps)	1300
Rate Identifier	Unspecified
9um Fiber Length (km)	12
Vendor Name	Omnitron Systems
Vendor OUI	00:06:87
Vendor Part Number	7207- 1
Vendor Revision Number	0100
Vendor Serial Number	8B20040047
Vendor Date Code	11/27/2008
Wavelength (nm)	1310
Options	RX_LOS, TX_FAULT, TX_DISABLE
Diagnostic Monitoring Type	Avg Pwr, Ext Cal, Diagnostic Monitoring
Enhanced Options	RX_LOSS, TX_FAULT, W/A Flags
SFF-8472 Compliance	SFF-8472 Rev. 9.3

Refresh ☒ Auto Refresh

The following general information is available:

- Identifier
- Connector
- Encoding
- Rate Identifier
- Vendor Name
- Vendor Part Number
- Vendor Serial Number
- Wavelength (nm)
- Diagnostic Monitoring Type
- SFF-8472 Compliance
- Extended Identifier
- Transceiver
- Normal Bit Rate (Mbps)
- 9um or OM1/OM2/OM3 Fiber Length
- Vendor OUI
- Vendor Revision Number
- Vendor Date Code
- Options
- Enhanced Options

A **Refresh** button and **Auto Refresh** check box is also located at the bottom left corner of the screen. Click the **Refresh** button to update the screen. Click on the **Auto Refresh** check box for automatic refreshing of the screen. The rate of refresh is configured from the Browser Settings screen, found under Maintenance.

Use the Page Selection pull-down to select the A0 or A2 Decoded pages. Select A2.

SFP Port Information	
Port Selection:	F1
Page Selection:	A2 Decoded
Variable Name	Value
Measured Temperature (°C)	50.3
Measured Vcc (V)	3.4
Measured Bias (mA)	8.4
Measured Tx Power (dBm)	-5.9
Measured Rx Power (dBm)	-40.4
Temperature High/Low Alarm (°C)	85.0/-15.0
Temperature High/Low Warning (°C)	80.0/-10.0
Vcc High/Low Alarm (V)	3.8/2.8
Vcc High/Low Warning (V)	3.6/3.0
Bias High/Low Alarm (mA)	80.0/0.1
Bias High/Low Warning (mA)	70.0/0.5
Tx Power High/Low Alarm (dBm)	-1.0/-11.5
Tx Power High/Low Warning (dBm)	-2.0/-10.5
Rx Power High/Low Alarm (dBm)	-5.9/-25.9
Rx Power High/Low Warning (dBm)	-6.9/-22.9
<input type="button" value="Refresh"/> <input checked="" type="checkbox"/> Auto Refresh	

The following diagnostic information is available:

- Measured Temperature
- Measured Bias
- Measured Rx Power
- Temperature High/Low Warning
- Vcc High/Low Warning
- Bias High/Low Warning
- Tx Power High/Low Warning
- Rx Power High/Low Warning
- Measured Vcc
- Measured Tx Power
- Temperature High/Low Alarm
- Vcc High/Low Alarm
- Bias High/Low Alarm
- Tx Power High/Low Alarm
- Rx Power High/Low Alarm

A **Refresh** button and **Auto Refresh** check box is also located at the bottom left corner of the screen. Click the **Refresh** button to update the screen. Click on the **Auto Refresh** check box for automatic refreshing of the screen. The rate of refresh is configured from the Browser Settings screen, found under Maintenance.

2.3.2 Hardware Configuration Screens

The following options are available.



2.3.2.1 DIP Switch

The DIP Switch screen provides information on the function and physical setting of each DIP-switch. DIP-Switch screen will vary depending on the model.

DIP Switch

DIP Switch	Function	Physical Setting	Soft Switch Configuration
1	Device mode	Single switch mode	Single switch mode ▾
2	Switch mode	Normal switch mode	Normal switch mode ▾
3,4	Protection mode	No redundant fiber	No redundant fiber ▾
5	MAC learning	MAC learning enabled	MAC learning enabled ▾
6	Force PoE Power	Auto PoE Power	Auto PoE Power ▾
7	L2CP	L2CP tunnel	L2CP tunnel ▾
8	PoE reset	No PoE reset on fiber link drop	No PoE reset on fiber link drop ▾

Global Settings

Physical DIP switches

Apply Save Cancel

Configuration

DIP switches active, software override disabled ▾

To change the DIP-switch settings, use the pull-down menu under the Global Settings and select the ***DIP-switches disabled, software override active*** option. Click on the ***Apply*** button to activate the changes.

Once the Global Setting has been changed to ***DIP-switches disabled, software override active***, the soft switch DIP-switch settings can be modified by using the pull-down menu next to next selection. When the Global Setting is configured for ***DIP-switches active, software override disabled***, no soft switch configuration changes are allowed. Changes can only be made to the physical hardware DIP-switches.

To change the individual DIP-switch settings, use the pull-down menu associated with the DIP-switch. The table below defines the DIP-switch settings. See individual Quick Start Guides for more information.

GHPoE and GHPoEBT models

Switch	Function	Soft Switch Configuration Options
1	Device Mode (models with 2 uplink ports only)	Single switch mode (factory default) Dual switch mode
2	Switch mode	Normal switch mode (factory default) Directed switch mode
3,4	Protection mode (models with 2 uplink ports only)	No redundant uplink (factory default) Redundant uplink no return to primary Redundant uplink return to primary
5	MAC Learning	MAC learning enabled (factory default) MAC learning disabled
6	Forced PoE	Auto PoE (factory default) Force PoE enabled
7	L2CP	L2CP tunnel (factory default) L2CP discard
8	PoE Reset	No PoE reset on uplink drop (factory default) PoE reset on uplink drop

GPoE+ models

Switch	Function	Soft Switch Configuration Options
1	Device Mode (models with 2 uplink ports only)	Single switch mode (factory default) Dual switch mode
2	Switch mode	Normal switch mode (factory default) Directed switch mode
3,4	Protection mode (models with 2 uplink ports only)	No redundant uplink (factory default) Redundant uplink no return to primary Redundant uplink return to primary
5	MAC Learning	MAC learning enabled (factory default) MAC learning disabled
6	Pause	Pause disabled (factory default) Pause enabled
7	L2CP	L2CP tunnel (factory default) L2CP discard
8	PoE Reset	No PoE reset on uplink drop (factory default) PoE reset on uplink drop

G/M models

Switch	Function	Soft Switch Configuration Options
1	Device Mode (models with 2 uplink ports only)	Single switch mode (factory default) Dual switch mode
2	Switch mode	Normal switch mode (factory default) Directed switch mode
3,4	Protection mode (models with 2 uplink ports only)	No redundant uplink (factory default) Redundant uplink no return to primary Redundant uplink return to primary
5	MAC Learning	MAC learning enabled (factory default) MAC learning disabled
6	Pause	Pause disabled (factory default) Pause enabled
7	L2CP	L2CP tunnel (factory default) L2CP discard
8	Reserved	

Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

2.3.2.2 Port / Interface Overview

The Port / Interface Overview screen allows the ports to be configured for speed, duplex, flow control, port access and PSE state. It also provides the ability to reset power to the Powered Devices attached to the copper PSE ports.

Port / Interface Overview screen will vary depending on the model.

Port / Interface Overview								
Port	Port Type	Link	PSE State	Port State	Flow Control	Port Access	PoE State	Reset Interface
F1	SFP-Empty		---	Auto negotiation ▼	Disabled ▼	Enabled ▼	---	---
F2	SFP-Empty		---	Auto negotiation ▼	Disabled ▼	Enabled ▼	---	---
P1	Copper PSE		(Active)	Auto negotiation ▼	Disabled ▼	Enabled ▼	HPoE Auto Detect 60W ▼	Power Cycle Port P1
P2	Copper PSE		(Active)	Auto negotiation ▼	Disabled ▼	Enabled ▼	HPoE Auto Detect 60W ▼	Power Cycle Port P2
P3	Copper PSE		(Active)	Auto negotiation ▼	Disabled ▼	Enabled ▼	HPoE Auto Detect 60W ▼	Power Cycle Port P3
P4	Copper PSE		(Non-PD)	Auto negotiation ▼	Disabled ▼	Enabled ▼	HPoE Auto Detect 60W ▼	Power Cycle Port P4

Apply Save Cancel

Port Configuration					
Port	Port Type	Link	Port State	Flow Control	Port Access
F1	SFP-1000X		Auto negotiation ▼	Disabled ▼	Enabled ▼
F2	SFP-1000X		Auto negotiation ▼	Disabled ▼	Enabled ▼
P1	Copper		Auto negotiation ▼	Disabled ▼	Enabled ▼
P2	Copper		Auto negotiation ▼	Disabled ▼	Enabled ▼
P3	Copper		Auto negotiation ▼	Disabled ▼	Enabled ▼
P4	Copper		Auto negotiation ▼	Disabled ▼	Enabled ▼
P5	Copper		Auto negotiation ▼	Disabled ▼	Enabled ▼
P6	Copper		Auto negotiation ▼	Disabled ▼	Enabled ▼
P7	Copper		Auto negotiation ▼	Disabled ▼	Enabled ▼
P8	Copper		Auto negotiation ▼	Disabled ▼	Enabled ▼

Apply Save Cancel

NOTE: The number of ports will vary depending on the model.

Port

Indicates the port designation.

Port Type

Indicates if the port is a fixed fiber, SFP or copper port.

Link

Displays the state of the link (green or amber). Green indicates a good active link. Amber indicates a possible problem. See Section 5.0 Verify Operation.

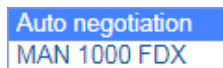
PSE State

Indicates if the port is an active PoE connection or a non-PoE device. It also provides a graphical indication of the amount of power provided to the attached PD.

Port State

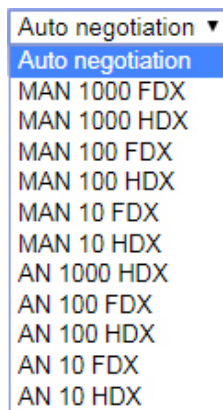
Use the Port State pull-down menu to change the negotiation state of the selected port.

The fiber ports can be configured for:



The default setting is Auto negotiation.

The copper ports can be configured for:



The default setting is Auto negotiation.

Flow Control

Use the Flow Control pull-down menu to enable or disable flow control on the selected port.

Port Access

Use the Port Access pull-down menu to enable or disable port access on the selected port. When disabled on a RJ-45 port, the connected PD will remain powered but data access is disabled.

PoE State (only displayed on models supporting PoE power)

Use the PoE State pull-down menu to configure the PoE/PSE for the selected port. The options are:

HPoE Auto Detect 100W ▼

PoE Disabled

PoE Auto Detect 802.3af

PoE Auto Detect 802.3af/at

PoE Force On

HPoE Auto Detect 100W

PoE power can be disabled, auto detect to 802.3af, auto detect to 802.3af/at, Forced On or HPoE Auto Detect 100W (60W or 100W depending on the model).

Reset Interface

Click on the **Power Cycle Port x** button to reset the power to the attached Powered Device. The power is removed for 5 seconds, then reapplied.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

2.3.2.3 Port / Interface Detailed

The Port / Interface Detailed screen allows the ports to be configured with specific attributes. These include flow control, MAC learning, port mirroring, port output, port security and advanced PoE port settings.

Port / Interface screen will vary depending on the model.

Use the Port Selection pull-down menu to selected the desired port. Use the pull-down menus associated with the attribute to change the parameter.

Port / Interface Detailed

Port Selection: F1 ▼

General		Power Over Ethernet	
Item Name	Configured	Item Name	Configured
Port State	Auto negotiation ▼	PoE State	---
Port Name	Port F1	Heartbeat	---
Flow Control	Disabled ▼	PD IPv4 Address	---
Port Access	Enabled ▼	Heartbeat Restart Time (s)	---
Mac Learning	Enabled ▼	Heartbeat Interval Time (s)	---
Unknown Multicast/Unicast	Accept ▼	Heartbeats Lost Before Error	---
Port Mirroring	Mirroring Disabled ▼	Heartbeats # Restarts	---
Cable Test	---	Heartbeat Error Action	---
Loop Protection	Disabled ▼	Heartbeat Status	---
Loop Protection Transmit (s)	1	PSE Schedule On/Off Time	---
		Schedule On Time	---
		Schedule Off Time	---
		PSE Power Off/On	---

Apply

Save

Cancel

Port / Interface Detailed
 Port Selection: F1 ▼

General	
Item Name	Configured
Port State	Auto negotiation ▼
Port Name	Port F1
Flow Control	Disabled ▼
Port Access	Enabled ▼
Mac Learning	Enabled ▼
Unknown Multicast/Unicast	Accept ▼
Port Mirroring	Mirroring Disabled ▼
Cable Test	---

Apply Save Cancel

General

Port State

Use the Port State pull-down menu to configure the port for negotiation, speed and duplex.

Port Name

Use the text box to enter a name for the port.

Flow Control

Use the Flow Control pull-down menu to enable or disable flow control on the port.

Port Access

Use the Port Access pull-down menu to enable or disable port access. When disabled, the connected PD will remain powered but data access is disabled.

MAC Learning

Use the MAC Learning pull-down menu to enable or disable MAC learning on the port.

Unknown Multicast/Unicast

Use the Unknown Multicast/Unicast pull-down menu to accept or reject unknown multicast and unicast traffic.

Port Mirroring

Use the Port Mirroring pull-down menu to enable or disable port mirroring. When enabled, select the port to be mirrored.

Cable Test

To run a cable test, use the Port Selection pull-down menu to select a RJ-45 port.

Click on the **Cable Test Port x** button to run the cable test on the selected port. Once completed, the results of the cable test is displayed.

Loop Protection

Loop protection is provided using Configuration Test Protocol (CTP). When loop protection is enabled on a port, the port will generate Configuration Test Protocol (CTP) frames. When the module receives its own CTP message either on the generating port or another port, loop prevention will automatically block the port from sending out normal user data until the loop is removed.

When a port is blocked, the port will continue to send out periodic CTP frames in order to determine if the block has been removed. When the module does not receive its own CTP message either on the generating or another port, the port will be unblocked.

Use the Loop Protection pull-down menu to enable or disable loop protection on the port.

Loop Protection Transmit (s)

Use the text box to enter the value for the time interval between the transmission of the CTP frames. A value of 1 sec to 60 sec can be entered.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

When a PoE port is selected, the Power over Ethernet column of parameters are available for configuration.

Port / Interface Detailed

Port Selection: P1

General		Power Over Ethernet	
Item Name	Configured	Item Name	Configured
Port State	Auto negotiation	PoE State	HPoE Auto Detect 100W
Port Name	Port 1	Heartbeat	Disabled
Flow Control	Disabled	PD IPv4 Address	0.0.0.0
Port Access	Enabled	Heartbeat Restart Time (s)	60
Mac Learning	Enabled	Heartbeat Interval Time (s)	1
Unknown Multicast/Unicast	Accept	Heartbeats Lost Before Error	3
Port Mirroring	Mirroring Disabled	Heartbeats # Restarts	0
Cable Test	Cable Test Port P1	Heartbeat Error Action	Ignore errors
Loop Protection	Disabled	Heartbeat Status	---
Loop Protection Transmit (s)	1	PSE Schedule On/Off Time	Disabled
		Schedule On Time	Hour: 00 Min: 00 Sec: 00
		Schedule Off Time	Hour: 00 Min: 00 Sec: 00
		PSE Power Off/On	Power Cycle Port P1

Apply

Save

Cancel

To make changes to the Power Over Ethernet settings, the DIP Switch Global Settings must be configured for **DIP-switches disabled, software override active** option. Once the Global Setting has been changed to **DIP-switches disabled, software override active**, the Power Over Ethernet settings can be modified.

Power Over Ethernet (only displayed on models supporting PoE power)

PoE State

Initially, the setting will match the hardware setting for DIP-switch #6. Use the PoE State pull-down menu to select PoE Disabled, PoE Auto Detect 802.3af, PoE Auto Detect 802.3af/at, PoE Forced On or HPoE Auto Detect 100W (60W or 100W depending on the model).

Heartbeat

Use the Heartbeat pull-down menu to enable or disable heartbeat. The heartbeat signal is used to verify connectivity to the PD. The IP address of the PD must be configured for the heartbeat signal to work.

PD IPv4 Address

Enter the IP address of the PD in the text box.

Heartbeat Timers (s)

Use the Heartbeat Restart Time text box to enter a new value for the Restart timer. A value of 1 to 300 seconds is a valid entry. The Heartbeat Restart Time delays the start of the heartbeat signal after a reset condition.

Use the Heartbeat Interval Time text box to enter a new value for the Interval timer. A value of 1 to 300 seconds is a valid entry. The Heartbeat Interval Time is the time between heartbeats.

Heartbeat Lost Before Error

Use the Heartbeat Lost Before Error text box to enter a new value for the number of lost heartbeats. A value of 1 to 100 is a valid entry. The Heartbeat Lost Before Error configures the number of consecutive lost heartbeats before an error condition is declared.

Heartbeat # Restarts

Use the Heartbeat # Restart text box to enter a new value for the number of times to restart the PD after an error has been declared. A value of 0 indicates no limit to the number of restarts. A value of 0 to 16384 is a valid entry.

Heartbeat Error/Action

Use the Heartbeat Error/Action pull-down menu to configure what action is taken when a heartbeat error condition is declared.

- | | |
|-------------------|---|
| Ignore errors | Indicates the error condition is ignored. |
| Restart on errors | Indicates the power to the selected port (PD) is cycled Off and On. |
| Shutdown | Indicates the power to the selected port (PD) is turned Off. |

Heartbeat Status

Displays the status of the heartbeat.

PSE Schedule On/Off Time

PoE power on each port can be enabled or disabled based upon the Time of Day. PoE power can be scheduled to be turned ON and OFF one time during the day.

Use the PSE Schedule On/Off Time pull-down menu to enable or disable the scheduling feature.

Schedule On Time

The Schedule On Time sets the time when PoE power is applied.

Use the Hour / Min / Sec pull-down menus to set the On time of day. during the day and when the power is turned off.

Schedule Off Time

The Schedule Off Time sets the time when PoE power is removed.

Use the Hour / Min / Sec pull-down menus to set the Off time of day.

PSE Power Off/On

Use the ***Power Cycle Port x*** button to cycle the power to the attached PD.

Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

2.3.3 Service Management

The following options are available.



2.3.3.1 Module

The Module screen provides the ability to enable/disable Global Flow Control, FTP, HTTP, HTTPS, Telnet, Serial Console baud rate, MAC Aging and location specific information.

Module			
General		Location	
Item Name	Configured	Item Name	Configured
Module Name	<input type="text"/>	Location Name	<input type="text" value="GHPoE/Mi"/>
FTP	<input type="button" value="Disabled"/>	Address	<input type="text"/>
Telnet	<input type="button" value="Enabled"/>	City	<input type="text"/>
Global Flow Control (Pause)	<input type="button" value="Disabled"/>	State/Province	<input type="text"/>
Serial Baud Rate	<input type="button" value="57600 baud"/>	Postal/Zip Code	<input type="text"/>
MAC Aging Time	<input type="text" value="300"/>	Latitude (degrees)	<input type="text"/>
MAC Table Flush on Link Down	<input type="button" value="Enabled"/>	Longitude (degrees)	<input type="text"/>
HTTP	<input type="button" value="Enabled"/>	Altitude (m)	<input type="text"/>
HTTPS	<input type="button" value="Enabled"/>		
Certificate Filename	<input type="text"/>		
<input type="button" value="Apply"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>			

General

Module Name

Use the Module Name text box to enter a unique name for the module.

FTP

Use the FTP pull-down menu to enable or disable FTP. FTP will need to be enabled for any firmware updates. FTP is disabled by default.

Telnet

Use the Telnet pull-down menu to enable or disable Telnet. Telnet is enabled by default.

Global Flow Control (Pause)

Use the Global Flow Control pull-down menu to enable or disable flow control on the module.

Serial Baud Rate

Use the Serial Baud Rate pull-down menu to select the speed of the serial console port. The default speed is 57,600.

MAC Aging Time

Use the MAC Aging Time text box to enter a new value for the timer. A value of 10 to 600 seconds is a valid entry.

MAC Table Flush on Link Down

The module can be configured to flush the MAC table on the detection of a link down condition.

Use the MAC Table Flush on Link Down pull-down menu to enable or disable MAC Table Flush.

HTTP

Use the HTTP pull-down menu to enable or disable HTTP support. HTTP is enabled by default.

HTTPS

Use the HTTPS pull-down menu to enable or disable HTTPS support. HTTPS is enabled by default.

Certificate Filename

Use the Certificate Filename text box to enter the file name of the SSL/TLS certificate.

Location

Location Name

Use the Location Name text box to enter a name of the location of the installation.

Address/City/State/Province/Postal/ZIP Code

The physical location can be configured. Enter the information in the text boxes.

Latitude/Longitude/Attitude

The latitude, longitude and attitude can be configured. Enter the information in the text boxes.

Click the *Cancel* button to revert back to the previous Apply state.

Click on the *Apply* button to activate the changes.

Click the *Save* button to permanently save the changes.

2.3.3.2 IPv4 Configuration

The IPv4 Configuration screen provides the ability to configure the IP address, subnet mask and gateway of the module. DHCP and DHCP relay (option 82) can also be enabled and/or disabled.

IPv4	
Item Name	Configured
IPv4 Client	Enabled ▾
IPv4 Address	192.168.1.220
IPv4 Subnet Mask	255.255.255.0
IPv4 Gateway	192.168.1.1
DHCPv4 Client	Disabled ▾
DHCPv4 Relay	Disabled ▾
DHCPv4 Circuit ID	Enabled ▾
DHCPv4 Remote ID	Enabled ▾
DHCPv4 Remote Server IP Address	0.0.0.0
DHCPv4 Relay Client Type	Replace ▾
<div>Apply Save Cancel</div>	

IPv4 Client

Use the IPv4 Client pull-down menu to enable or disable IP protocol on the module.

IPv4 Address

Enter the IP address in the text box in the x.x.x.x format (x represents a decimal number between 0 and 255).

IPv4 Subnet Mask

Enter the Subnet Mask in the text box in the x.x.x.x format (x represents a decimal number between 0 and 255). Class A subnet mask is 255.0.0.0, Class B subnet mask is 255.255.0.0 and Class C subnet mask is 255.255.255.0.

IPv4 Gateway

Enter the Gateway in the text box in the x.x.x.x format (x represents a decimal number between 0 and 255).

DHCPv4 Client

Use the DHCPv4 Client pull-down menu to enable or disable DHCP on the module.

DHCPv4 Relay

Use the DHCPv4 Relay pull-down menu to enable or disable the DHCP relay function.

DHCP Relay Option 82 provides additional security when DHCP is used to allocate network addresses. It enables the controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources.

DHCPv4 Circuit ID

Use the DHCPv4 Circuit ID Selection pull-down menu to enable or disable the DHCP relay circuit ID.

DHCPv4 Remote ID

Use the DHCPv4 Remote ID Selection pull-down menu to enable or disable the DHCP relay remote ID.

DHCP Remote Server IP Address

Enter the DHCP server IP address in the text box in the x.x.x.x format (x represents a decimal number between 0 and 255).

DHCP Relay Client Type

Use the DHCP Relay Client Type pull-down menu to select Drop, Keep or Replace.

- | | |
|---------|--|
| Drop | Drops the DHCP relay frame received on a client port. |
| Keep | Forwards the DHCP relay frame received on a client to the server port without changing to the DHCP relay options. |
| Replace | Updates the DHCP relay frame received on a client port with the configured DHCP relay options before forwarding it to the server port. |

WARNING: Changing the IP address of the module will result in loss of connectivity once the *Apply* button is clicked.

Click on the *Apply* button to activate the changes.

Click the *Save* button to permanently save the changes.

DHCP Relay Process

The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers. A DHCP relay agent receives any DHCP broadcasts and forwards them to the specified DHCP server IP address.

1. The DHCP client generates a DHCP request.
2. The DHCP relay agent receives the broadcast DHCP request packet and inserts the relay agent information option (option 82) into the packet. The relay agent information option contains related sub options (Circuit ID and Remote ID).
3. The DHCP relay agent sends the DHCP packet to the DHCP server.
4. The DHCP server receives the packet, uses the sub options to assign IP addresses and other configuration parameters to the packet, and forwards the packet back to the client.
5. The sub option fields are removed by the relay agent and the IP address information is forwarded to the client.

NOTES:

If DHCPv4 Circuit ID is enabled and the DHCP Relay Client Type is set to Replace, the Circuit ID will be set as “br0” instead of the associated port number.

If the module is configured as a 2nd DHCP Relay agent in a network, the unicast DHCP packets from the first DHCP Relay agent are forwarded to the DHCP Server.

Click the *Cancel* button to revert back to the previous Apply state.

Click on the *Apply* button to activate the changes.

Click the *Save* button to permanently save the changes.

2.3.3.3 SNMP

The SNMP screen provides the ability to configure the SNMP parameters on the module.

SNMP Configuration

Instance Selection: General Settings

Global Configuration

Item Name	Configured
SNMP Agent	SNMPv1/v2c/v3
SNMP Traps	SNMPv2c

Trap Host Configuration

Item Name	IP Address	UDP Port
Trap Host 1	<input type="text" value="255.255.255.255"/>	<input type="text" value="162"/>
Trap Host 2	<input type="text" value="255.255.255.255"/>	<input type="text" value="162"/>
Trap Host 3	<input type="text" value="255.255.255.255"/>	<input type="text" value="162"/>
Trap Host 4	<input type="text" value="255.255.255.255"/>	<input type="text" value="162"/>
Trap Host 5	<input type="text" value="255.255.255.255"/>	<input type="text" value="162"/>
Trap Host 6	<input type="text" value="255.255.255.255"/>	<input type="text" value="162"/>
Trap Host 7	<input type="text" value="255.255.255.255"/>	<input type="text" value="162"/>
Trap Host 8	<input type="text" value="255.255.255.255"/>	<input type="text" value="162"/>

Apply Save Cancel

Use the Instance Selection pull-down menu to select the General Setting, SNMPv1/v2 Settings, SNMPv3 User 1 Settings, User 2 Settings, User 3 Settings or User 4 Settings port settings. Select General Setting.

SNMP Agent

Use the SNMP Agent pull-down menu to configure the SNMP agent by selecting None, SNMPv1/v2c, SNMPv3 or SNMPv1/v2c/v3. When None is selected, the module will not respond to any requests via the SNMP protocol.

SNMP Traps

Use the SNMP Traps pull-down menu to configure the trap generation type by selecting SNMPv2c or SNMPv3.

Trap Host 1 - 8

Enter the IP Address of the Trap Host in the text box in the x.x.x.x format. SNMP traps are used to report events that occur during the operation of a network, and may require the attention of the network administrator. The module is capable of sending SNMP traps to eight different SNMP Traphosts (IP addresses). Enter a UDP Port number in the text box for the selected Trap Host, if it is different than the global setting.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Instance Selection pull-down menu to select the General Setting, SNMPv1/v2 Settings, SNMPv3 User 1 Settings, User 2 Settings, User 3 Settings or User 4 Settings port settings. Select SNMP v1/v2c Settings.

SNMP Configuration

Instance Selection:

SNMPv1/v2c Settings

Item Name	Configured
Read Community	00 00 00 00 00
Write Community	00 00 00 00 00

Modify

Save

Cancel

Click the *Modify* button to change the Read or Write Community Names.

SNMP Configuration

Instance Selection:

SNMPv1/v2c Settings

Item Name	Configured
Read Community	<div></div>
Read Community (Again)	<div></div>
Write Community	<div></div>
Write Community (Again)	<div></div>

Apply

Save

Cancel

Read Community

The SNMP Read Community Name is necessary for reading (SNMP get) data from the module. The name can be a combination of 1-32 alphanumeric character string. “public” is the default setting.

Enter the new Read Community Name in the text box.

Read Community (Again)

Confirm the new Read Community Name by entering it the text box (again).

Write Community

The SNMP Write Community Name is necessary for writing (SNMP set) data to the module. The name can be a combination of 1-32 alphanumeric character string. “private” is the default setting.

Enter the new Write Community Name in the text box.

Write Community (Again)

Confirm the new Write Community Name by entering it the text box (again).

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Instance Selection pull-down menu to select the General Setting, SNMPv1/v2 Settings, SNMPv3 User 1 Settings, User 2 Settings, User 3 Settings or User 4 Settings port settings. Select SNMP v3 User x Settings.

SNMP Configuration

Instance Selection: SNMPv3 User 1 Settings ▾

Item Name	Configured
User Type	admin
User Name	admin
Security Level	noAuthNoPriv
Privacy Password	*****
Privacy Encryption	AES
Authentication Password	*****
Authentication Hashing	MD5

Modify Save Cancel

Click the **Modify** button to change the user parameters.

SNMP Configuration
Instance Selection: SNMPv3 User 1 Settings ▼

Item Name	Configured
User Type	admin ▼
User Name	<input type="text" value="admin"/>
Security Level	noAuthNoPriv ▼
Privacy Password	<input type="text"/>
Privacy Password (again)	<input type="text"/>
Privacy Encryption	AES ▼
Authentication Password	<input type="text"/>
Authentication Password (again)	<input type="text"/>
Authentication Hashing	MD5 ▼

Apply Save Cancel

SNMPv3 implements a security model that provides for message integrity, authentication, and encryption. Authentication for SNMPv3 is provided through a unique User Name, Authentication Password and Privacy Password for each access level. Since SNMPv3 supports multiple users, each access level provides secret keys for authentication and privacy. Privacy supports confidentiality by encrypting the data that is transmitted. MD5 and SHA are the specified authentication protocols and AES and DES are the specified privacy protocol.

User Type

Use the User Type pull-down menu to select the type of user; admin, read-write, read-only or deny.

- | | |
|------------|--|
| Admin | Has full read/write privileges including user name and password changes. |
| Read-write | Has full read/write privileges with the exception of user name and password operations. |
| Read-only | Can only view the configuration of the module and will not be allowed to make any changes. |
| Deny | Does not have any access to the module. |

User Name

Enter a unique User name in the text box. User names can be a combination of 1-32 alphanumeric character string.

Security Level

Use the Security Level pull-down menu to select the Security Level for each user; noAuthNoPriv, authNoPriv and authPriv.

noAuthNoPriv	Allows access without authentication and without privacy.
authNoPriv	Allows access with authentication, but without privacy.
authPriv	Allows access with authentication and with privacy.

Authentication and privacy uses different algorithms for encrypting and decrypting SNMPv3 packets.

Privacy Password

Enter the privacy password in the text box.

Privacy Password (again)

Re-enter the privacy password.

Privacy Encryption

Use the Privacy Encryption pull-down menu to select the encryption method; AES or DES

Authentication Password

Enter the authentication password in the text box.

Authentication Password (again)

Re-enter the authentication password in the text box.

Authentication Hashing

Use the Authentication Hashing pull-down menu to select the hashing algorithm; MD5 or SHA

Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

2.3.3.4 Time and Date

The Time and Date Configuration screen provides the ability to change the Time of Day, Date and Time Zone. The System Up Time is displayed along with the local time associated with the workstation running the web interface.

Time & Date

Item Name	Configured
Time of Day	Hour: 18 Min: 43 Sec: 54
Date	Day: 31 Month: Dec Year: 2000
Time Zone	PST (Pacific Standard Time) UTC - 08 hours
System Up Time	0 days, 2 hours, 44 mins, 19 secs
Work Station Local Time	12/11/2018 15:13:06

Apply

Save

Cancel

Copy Local Time

Use the pull-down menus associated with each item to make changes to the Time of Day, Date and Time Zone.

Click the **Copy Local Time** button to use the time and date of the local workstation.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

NOTE: Time and date is lost if the module loses power.

2.3.3.5 NTP / SNTP

The NTP / SNTP screen provides the ability to configure Network Time Protocol (NTP) and Simple Network Time Protocol (SNTP) on the module.

NTP / SNTP	
Item Name	Configured
NTP / SNTP Type	Time protocol disabled ▾
Time Server Request Interval (minutes)	8
Time Server 1 IP Address	255.255.255.255
Time Server 1 Status	Server disabled
Time Server 2 IP Address	255.255.255.255
Time Server 2 Status	Server disabled
<input type="button" value="Apply"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>	

NTP / SNTP Type

Use the NTP / SNTP Type pull-down menu to select Time protocol disabled, NTP enabled or SNTP enabled.

Time Server Request Interval (minutes)

Use the Time Server Request Interval text box to enter a new value for the time between server requests. A value of 1 to 60 minutes is a valid entry. The default is 8 minutes.

Time Server 1 IP Address

Enter the IP Address of the time server in x.x.x.x format in the text box.

Time Server 1 Status

Displays the status of the server.

Time Server 2 IP Address

Enter the IP Address of the second time server in x.x.x.x format in the text box.

Time Server 1 Status

Displays the status of the server.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

2.3.3.6 LLDP

The LLDP screen provides the ability to configure the module to support Link Layer Discovery Protocol (LLDP).

LLDP (Link Layer Discovery Protocol)
Instance Selection: Global

Global Configuration		Global Status	
Item Name	Configured	Item Name	Configured
Normal Transmission Interval (s)	<input type="text" value="30"/>	Capabilities Supported	Bridge, CVLAN, SVLAN
TTL Value Multiplier	<input type="text" value="4"/>	Capabilities Enabled	Bridge, CVLAN, SVLAN
Fast LLDP Transmission Interval (s)	<input type="text" value="1"/>	Number of Times Table Data Inserted	0
Maximum Number of Fast LLDP Messages	<input type="text" value="4"/>	Number of Times Table Data Deleted	0
Maximum Number of LLDP Messages	<input type="text" value="5"/>	Number of Times Table Data Dropped	0
Port Reinitialization Time (s)	<input type="text" value="1"/>	Number of Times Table Aged Out	0

Apply Save Cancel

The IEEE 802.1ab Link Layer Discovery Protocol defines a standard way for Ethernet devices to advertise information about themselves to their neighbors and store information they discover from the neighboring devices. Each device configured with an active LLDP agent will send and receive messages on all physical interfaces enabled for LLDP transmission.

Use the Instance Selection pull-down menu to select the global or port settings. Select Global.

Global Configuration

Normal Transmission Interval (s)

Sets the transmission frequency of LLDP updates in seconds. The range is 5 to 32,768 seconds and the default is 30 seconds. Enter the new value in the text box.

TTL Value Multiplier

Specifies the variable used as a multiplier of the Normal Transmission Interval to determine the time remaining before information in the outgoing Link Layer Discovery Protocol Data Unit (LLDPDU) is no longer valid. The range is 2 to 10 and the default is 4. Enter the new value in the text box.

Fast LLDP Transmission Interval (s)

Specifies the time interval between transmissions during fast transmission periods. The range is 1 to 3,600 seconds and the default value is 1 second. Enter the new value in the text box.

Maximum Number of Fast LLDP Messages

Specifies the number of LLDPDUs that are transmitted during a fast transmission period. The range is 1 to 8 messages and the default value is 4.

Maximum Number of LLDP Messages

Specifies the maximum number of consecutive LLDPDUs that can be transmitted at any time. The range is 1 to 10 and the default value is 5.

Port Reinitialization Time (s)

Specifies the delay time in seconds for LLDP to initialize on any interface. The range is 2 to 5 seconds and the default is 2 seconds.

Global Status

Capabilities Supported

Displays the system capabilities supported on the module.

Capabilities Enabled

Displays the system capabilities enabled on the module.

Number of Times Table Data Inserted

Indicates the number of times the information advertised has been inserted into tables.

Number of Times Table Data Deleted

Indicates the number of times the information advertised has been deleted from tables.

Number of Times Table Data Dropped

Indicates the number of times the information advertised could not be entered into tables.

Number of Times Table Aged Out

Indicates the number of times the information has aged out.

NOTES:

LLDP parameters that are not supported are *reinitDelay*, *txFastInit* and *txCredit*.

The *reinitDelay* sets the time from port disable to reinitialization. This parameter is not set.

The *txFastInit* sets the number of LLDPDUs that are transmitted during a fast transmission period. This parameter is set to 4.

The *txCredit* sets the maximum number of consecutive LLDPDUs that can be transmitted at any time. This parameter is not set.

Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

Use the Instance Selection pull-down menu to select the global or port settings. Select P1.

LLDP (Link Layer Discovery Protocol)

Instance Selection: Port F2 ▼

Port Configuration		Port Status	
Item Name	Configured	Item Name	Configured
LLDP Setting	Peer ▼	LLDP Status	LLDP PDUs are being received
LLDP Mode	Receive & Transmit ▼	LLDP PDUs Transmitted	27
Management Address TLV	Included ▼	LLDP PDUs Received	15
Port Description TLV	Included ▼	LLDP PDUs Discarded	0
System Name TLV	Included ▼	Unrecognized Port TLVs Received	0
System Description TLV	Included ▼		
System Capabilities TLV	Included ▼		

Port Peer Information				
Chassis ID	System Name	System Description	Port Description	Management Address
00:06:87:02:13:f0	XM5	9600-40-B1 v5.3.5 s/n 00713365	Port #4	IPv4 - 192.168.1.220

Apply Save Cancel

Port Configuration

LLDP Setting

Use the LLDP Setting pull-down menu to select how LLDP is configured on the module (Peer, Discard, Tunnel).

- Peer The port will participate in the LLDP process.
- Discard LLDP frames are dropped and no reply is generated.
- Tunnel LLDP frames will egress ports unchanged.

LLDP Mode

The LLDP agent can transmit and/or receive information about the capabilities and current status of the system. LLDP does not have a mechanism for soliciting specific information from other LLDP agents.

Use the LLDP Mode pull-down menu to select the operating mode as Transmit Only, Receive Only, Transmit and Receive or None. Transmit and Receive is the default.

The information fields are contained in each Link Layer Discovery Protocol Data Unit (LLDPDU) as a sequence of variable length information elements, that include Type, Length, and Value fields (TLVs). These TLVs are used to transmit and receive specific information about the system.

Management Address TLV

Same as the IP address of the module. Use the Management Address TLV pull-down menu to select if this information is Included or Not Included in the LLDPDU.

Port Description TLV

The Port Description is the same as the Port Name of the module. Use the Port Description pull-down menu to select if this information is Included or Not Included in the LLDPDU.

System Name TLV

The LLDP System name is the same as System Name of the module. Use the System Name pull-down menu to select if this information is Included or Not Included in the LLDPDU.

System Description TLV

The LLDP System Description is the same as the System Description of the module. Use the System Description pull-down menu to select if this information is Included or Not Included in the LLDPDU.

System Capabilities TLV

Provides the system capabilities of the module (i.e., Bridge/Switch SVLAN CVLAN). Use the System Capabilities pull-down menu to select if this information is Included or Not Included in the LLDPDU.

Port Status

LLDP Status

Displays the status of the LLDP connection.

LLDP PDUs Transmitted

Displays the total number of transmitted PDUs.

LLDP PDUs Received

Displays the total number of received PDUs.

LLDP PDUs Discarded

Displays the number of discarded PDUs.

Unrecognized Port TLVs Received

Displays the number of unrecognized TLVs.

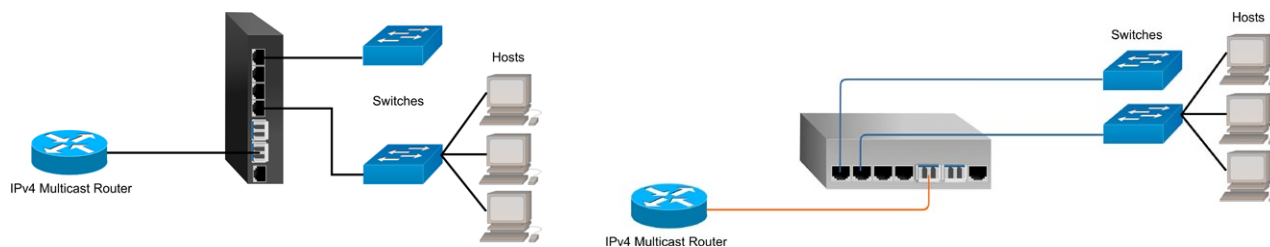
Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

2.3.3.7 IGMP

IGMP is used to modify the default route behavior for IPv4 Multicast Packets which are flooded to all ports. IGMP provides a method for forwarding IPv4 Multicast Packets to only the ports with hosts that want to receive the packets. IGMP communications occur between IPv4 Multicast Routers and Hosts.



IPv4 Multicast Packets have an address range of 224.0.0.0 to 239.255.255.255.

The IGMP screen provides the ability to configure the module to support Internet Group Management Protocol (IGMP).

Use the Instance Selection pull-down menu to select the Global, VID Interfaces or Routes settings. Select Global.

IGMP (Internet Group Management Protocol)
Selection: Global

Item Name	Configured
IGMP Snooping	Enabled
Flooding Unrecognized IGMP Groups	Disabled
IGMP Route Aging (s)	<input type="text" value="60"/>

Apply Save Cancel

IGMP Snooping

Use the IGMP Snooping pull-down menu to globally enable or disable IGMP snooping.

Flooding Unrecognized IGMP Groups

Use the Flooding Unrecognized IGMP Groups pull-down menu to enable or disable flooding of unrecognized groups.

IGMP Route Aging (s)

Enter a numeric value in the text box for the Route Aging (0 to 65535). The default value is 60 seconds.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Instance Selection pull-down menu to select the Global, VID Interfaces or Routes settings. Select VID Interfaces.

IGMP (Internet Group Managment Protocol)

Selection: VID Interfaces

Entry	VLAN ID	Ports Configured	Delete
1	1	F1,P1,P2,P3,P4,Mgmt	<input type="checkbox"/>
NEW			

Apply

Save

Cancel

Delete

Entry

System defined sequential number for each IGMP entry.

VLAN ID

Enter the VLAN ID associated with the IGMP group in the text box.

Port Configured

The name of the ports associated with the IGMP group will be displayed.

Delete

Check the box and click the **Delete** button to delete the IGMP entry.

Use the text boxes on the NEW entry row to add a new VID Interface. Click in the VLAN ID text box and enter a VLAN number.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Instance Selection pull-down menu to select the Global, VID Interfaces or Routes settings. Select Routes.

IGMP (Internet Group Managment Protocol)

Selection: Routes

Entry	IP Address	Type	Persistence	Router Port	Host Port	VLAN ID	Delete
1	225.100.100.1	Manual	Static	P1	P3	1	<input type="checkbox"/>
NEW		Manual	Static			1	

Apply

Save

Cancel

Delete

Entry

System defined sequential number for each IGMP entry.

IP Address

Enter the IP Address of the IGMP Group in the text box.

Type

Depending how the IGMP Interface is created, the Type will display Manual or Auto.

Persistence

Use the Persistence pull-down menu to select static or transient for the IGMP group. If transient is selected, the route will expire after the defined number of seconds configured by the IGMP Route Aging parameter.

Router Port

Enter the port number that is connected to the Multicast router in the text box. This can be a single or multiple ports.

Host Port

Enter the port number that is connected to the Host switch in the text box. This can be a single or multiple ports.

VLAN ID

Use the VLAN ID pull-down menu to select the VLAN associated with the IGMP group.

Delete

Check the box and click the **Delete** button to delete the IGMP entry.

Use the text boxes on the NEW entry row to add the new Route.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

2.3.4 Service Activation

The following options are available.



2.3.4.1 VLAN Configuration

The VLAN Configuration screen provides the ability to configure VLANs on the module.

VLAN Configuration

Entry	VLAN ID	VLAN Name	Delete
1	<input type="text" value="1"/>	<input type="text" value="VLAN1"/>	<input type="checkbox"/>
NEW	<input type="text"/>	<input type="text"/>	

Apply

Save

Cancel

Delete

Entry

System defined sequential number for each VLAN entry.

VLAN ID

Enter the VLAN ID in the text box.

VLAN Name

Enter the name for the VLAN ID in the text box.

Delete

Check the box and click the *Delete* button to delete the VLANs.

Use the text boxes on the NEW entry row to add a new VLAN ID. Click in the VLAN ID text box and enter a VLAN number. Click in the VLAN Name text box and enter a name for the VLAN.

Click on the *Apply* button to activate the changes. Once the information has been applied, a new entry is added to the VLAN Table. Continue to add VLAN IDs to the table.

Click the *Cancel* button to revert back to the previous Apply state.

VLAN Configuration

Entry	VLAN ID	VLAN Name	Delete
1	<input type="text" value="1"/>	<input type="text" value="VLAN1"/>	<input type="checkbox"/>
2	<input type="text" value="100"/>	<input type="text" value="Data"/>	<input type="checkbox"/>
NEW	<input type="text"/>	<input type="text"/>	

Apply

Save

Cancel

Delete

Click the *Save* button to permanently save the changes.

Click the *Cancel* button to revert back to the previous Apply state.

Click on the *Apply* button to activate the changes.

2.3.4.2 VLAN Interface

The VLAN Interface screen provides the ability to configure the ports for access, tunnel or trunk and assign VLAN IDs to the ports.

VLAN Interface
Trunk Ethertype Selection:

Port	Port Type	VID	Native VLAN	VID List
F1	Access port ▾	1 ▾	---	---
F2	Access port ▾	1 ▾	---	---
P1	Access port ▾	1 ▾	---	---
P2	Access port ▾	1 ▾	---	---
P3	Access port ▾	1 ▾	---	---
P4	Access port ▾	1 ▾	---	---
Mgmt	Access port ▾	1 ▾	---	---

Trunk Ethertype Selection

Use the Trunk Ethertype Selection text box to enter a new value for the Ethertype for a port configured as a trunk.

Port

Indicates the port designation.

Port Type

Use the Port Type pull-down menu to configure the port as a trunk, tunnel or access port.

- Trunk When configured as a trunk port:
 - Ingress: The tag is removed
 - Egress: A tag is added
- Tunnel When configured as a tunnel port,
 - Ingress: Untagged and tagged traffic is accepted
 - Egress: Traffic follows the assigned VID
- Access When configured as an access port
 - Ingress: Accepts only untagged traffic
 - Egress: Traffic follows the assigned VID

VID

Use the VID pull-down menu to select a VLAN ID. All VLAN IDs that were configured using the VLAN Configuration screen are available.

Native VLAN

When a native VLAN is configured, all untagged traffic on the trunk port is set to the VLAN ID associated with the native VLAN. Traffic assigned to a native VLAN when transmitted on a trunk port is untagged. Untagged traffic received on a trunk port is assigned to the VLAN associated with the native VLAN.

When the port is configured as a trunk port, use the Native VLAN text box to enter the native VLAN ID.

VID List

When the port is configured as a trunk port, use the VID List text box to enter the allowed VLAN ID ingressing the trunk port.

Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

2.3.4.3 Rate Limiting & Shaping

The Rate Limiting & Shaping screen provides the ability to add a bandwidth profile to a port on the module. Rate Limiting & Shaping screen will vary depending on the model.

Rate Limiting & Shaping

Selection: Ingress/Egress

	Ingress Rate					Egress Rate & Shaping			
Port	CIR	CBS	Policing	Class of Service	Performance Monitoring	CIR	Policing	Queue Type	Queue Mix
F1	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]	Disabled	<input type="text" value="1000000"/>	L2	Fairweight	<input type="text" value="fw,fw,fw,fw,fw,fw,fw,fw"/>
F2	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]	Disabled	<input type="text" value="1000000"/>	L2	Fairweight	<input type="text" value="fw,fw,fw,fw,fw,fw,fw,fw"/>
P1	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]	Disabled	<input type="text" value="1000000"/>	L2	Fairweight	<input type="text" value="fw,fw,fw,fw,fw,fw,fw,fw"/>
P2	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]	Disabled	<input type="text" value="1000000"/>	L2	Fairweight	<input type="text" value="fw,fw,fw,fw,fw,fw,fw,fw"/>
P3	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]	Disabled	<input type="text" value="1000000"/>	L2	Fairweight	<input type="text" value="fw,fw,fw,fw,fw,fw,fw,fw"/>
P4	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]	Disabled	<input type="text" value="1000000"/>	L2	Fairweight	<input type="text" value="fw,fw,fw,fw,fw,fw,fw,fw"/>

Apply Save Cancel

NOTE: The number of ports will vary depending on the model.

Use the Selection pull-down menu to select Ingress/Egress, Ingress, Egress or Egress Queues. Select Ingress/Egress.

Ingress Rate

Port

Indicates the port designation.

CIR (Committed Information Rate)

CIR specifies the maximum rate Ethernet frames are delivered per service performance objectives. These frames are referred to as being in-profile (green).

Use the CIR text box to enter a new value in kb/sec. A value of 64 to 1,000,000 is a valid entry. The default is 1,000,000.

CBS (Committed Burst Size)

CBS is the maximum number of bytes allowed for incoming Ethernet frames maintaining in-profile. The value of CBS will depend on the type of application or traffic being supported. Bursty data applications will require a larger CBS than more constant rate applications.

Use the CBS text box to enter a new value in kbytes. A value of 5 to 256 is a valid entry. The default is 15.

Policing

Use Policing pull-down menu to select whether bandwidth profiles are counted based upon L1 (frame + interframe gap + preamble), L2 only, or L3 only.

Class of Service

Use the Class of Service pull-down menu to select a class of service profile for the bandwidth profile. All class of service profiles that were configured using the CoS / QoS screen are available.

Performance Monitoring

Use the Performance Monitoring pull-down menu to enable or disable performance monitoring.

Egress Rate & Shaping

CIR (Committed Information Rate)

Egress CIR specifies the average rate Ethernet frames egress the port. When configuring Egress CIR, an egress queue type can be specified (starvation queuing - strict/low latency, weighted fair queuing - high latency or mixed). Starvation queuing processes all high priority traffic before any low priority traffic and uses a strict priority scheme. Weighted fair queuing will process high priority traffic more often than low priority traffic. The default weighted fair queuing mix is 33 (high priority), 25, 17, 12, 6, 3, 2, 1 (low priority).

Use the CIR text box to enter a new value in kb/sec. A value of 64 to 1,000,000 is a valid entry. The default is 1,000,000.

Policing

Use Policing pull-down menu to select whether bandwidth profiles are counted based upon L1 (frame + interframe gap + preamble), L2 only, or L3 only.

Queue Type

Use the Queue Type pull-down menu to select the type as starving, fairweight or mix.

Starving	All queues are set up to starving (strict) priority
Fairweight	All queues are setup for weighted fair queuing using the Queue Mix setting.
Mix	Each of the eight queues are set up individually: q7,q6,q5,q4, q3, q2, q1,q0 where qx can be one of two values (sp or fw).

Queue Mix

Use the Queue Mix text box to change the type of queuing for each egress priority queue.

sp The queue is set to strict priority. The listing of strict priority queues starts at highest priority queue (queue 7) and can only be selected from the highest queue sequentially without mixtures of weighted values between strict priority queues.

fw The queue is set to fairweight priority.

The following are some legal combinations:

fw, fw, fw, fw, fw, fw, fw, fw (default fairweight);

sp, sp, sp, sp, sp, sp, sp, sp (default starving);

sp, sp, fw, fw, fw, fw, fw, fw,

sp, sp, sp, sp, fw, fw, fw, fw

The following are not a legal combinations:

sp, fw, fw, sp, fw, fw, fw, fw;

fw,sp,sp,sp,sp,sp,sp,
sp,fw,fw,fw,fw,fw,fw,sp

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Selection pull-down menu to select Ingress/Egress, Ingress, Egress or Egress Queues. Select Ingress.

Rate Limiting & Shaping
Selection: Ingress

	Ingress Rate			
Port	CIR	CBS	Policing	Class of Service
F1	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]
F2	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]
P1	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]
P2	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]
P3	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]
P4	<input type="text" value="1000000"/>	<input type="text" value="15"/>	L2	[None]

Apply Save Cancel

NOTE: The number of ports will vary depending on the model.

Ingress Rate

Port

Indicates the port designation.

CIR (Committed Information Rate)

Use the CIR text box to enter a new value in kb/sec. A value of 64 to 1,000,000 is a valid entry. The default is 1,000,000.

CBS (Committed Burst Size)

Use the CBS text box to enter a new value in kbytes. A value of 5 to 256 is a valid entry. The default is 15.

Policing

Use Policing pull-down menu to select whether bandwidth profiles are counted based upon L1 (frame + interframe gap + preamble), L2 only, or L3 only.

Class of Service

Use the Class of Service pull-down menu to select a class of service profile for the bandwidth profile. All class of service profiles that were configured using the CoS / QoS screen are available.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Selection pull-down menu to select Ingress/Egress, Ingress, Egress or Egress Queues. Select Egress.

Rate Limiting & Shaping

Selection: Egress

	Egress Rate & Shaping			
Port	CIR	Policing	Queue Type	Queue Mix
F1	1000000	L2	Fairweight	fw, fw, fw, fw, fw, fw, fw, fw
F2	1000000	L2	Fairweight	fw, fw, fw, fw, fw, fw, fw, fw
P1	1000000	L2	Fairweight	fw, fw, fw, fw, fw, fw, fw, fw
P2	1000000	L2	Fairweight	fw, fw, fw, fw, fw, fw, fw, fw
P3	1000000	L2	Fairweight	fw, fw, fw, fw, fw, fw, fw, fw
P4	1000000	L2	Fairweight	fw, fw, fw, fw, fw, fw, fw, fw

Apply

Save

Cancel

NOTE: The number of ports will vary depending on the model.

Egress Rate & Shaping

Port

Indicates the port designation.

CIR (Committed Information Rate)

Use the CIR text box to enter a new value in kb/sec. A value of 64 to 1,000,000 is a valid entry. The default is 1,000,000.

Policing

Use Policing pull-down menu to select whether bandwidth profiles are counted based upon L1 (frame + interframe gap + preamble), L2 only, or L3 only.

Queue Type

Use the Queue Type pull-down menu to select the type as starving, fairweight or mix.

- Starving All queues are set up to starving (strict) priority
- Fairweight All queues are setup for weighted fair queuing using the Queue Mix setting.
- Mix Each of the eight queues are set up individually: q7,q6,q5,q4, q3, q2, q1,q0 where qx can be one of two values (sp or fw):

Queue Mix

Use the Queue Mix text box to change the type of queuing for each egress priority queue.

sp The queue is set to strict priority. The listing of strict priority queues starts at highest priority queue (queue 7) and can only be selected from the highest queue sequentially without mixtures of weighted values between strict priority queues.

fw The queue is set to fairweight priority.

The following are some legal combinations:

fw, fw, fw, fw, fw, fw, fw, fw (default fairweight);

sp, sp, sp, sp, sp, sp, sp, sp (default starving);

sp, sp, fw, fw, fw, fw, fw, fw,

sp, sp, sp, sp, fw, fw, fw, fw

The following are not a legal combinations:

sp, fw, fw, sp, fw, fw, fw, fw;

fw, sp, sp, sp, sp, sp, sp,

sp, fw, fw, fw, fw, fw, fw, sp

The actual weight for a queue type of fw is from the respective queue weight from the Queue Mix setting.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Selection pull-down menu to select Ingress/Egress, Ingress, Egress or Egress Queues. Select Egress Queues.

Rate Limiting & Shaping
 Selection: Egress Queues ▼

Egress Queue Rates								
Port	Q7	Q6	Q5	Q4	Q3	Q2	Q1	Q0
F1	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>
F2	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>
P1	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>
P2	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>
P3	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>
P4	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>	<input type="text" value="1000000"/>

Apply
Save
Cancel

NOTE: The number of ports will vary depending on the model.

Egress Queue Rates

Port

Indicates the port designation.

Q7...Q0

Enter the CIR rate for each egress priority queue in the text boxes.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

2.3.4.4 Cos / QoS

The CoS / QoS screen provides the ability to configure and display Class of Service profiles.

CoS / QoS

CoS / QoS Name	Default Class	Mode	Class	Type	Priority Selection	Delete Item
New CoS <input type="text"/>	1 <input type="text"/>	None <input type="text"/>	0 <input type="text"/>	<input type="text"/>	<input type="text"/>	

Apply

Save

Cancel

Delete

Class of Service (CoS) is supported by mapping customer frames into eight egress queues based on using the 3-bit Priority Code Point (PCP) field in the VLAN tag.

The priority of ingress frames correspond to eight possible values or priorities (0 through 7). Each frame is mapped to one of eight egress queues based on the PCP priority field. See the default mapping of PCP value to egress queue.

Quality of Service (QoS) Egress Queuing								
Priority Code Point (PCP)	0	1	2	3	4	5	6	7
Egress Queue (Class)	0	1	2	3	4	5	6	7

*Egress Queue vs Frame Priority
(Default Mapping)*

Class of Service profiles can use DSCP or PCP fields to reclassify and prioritize the ingress frames.

Differentiated Services Code Point (DSCP) profiles are associated with IP priority bits (ipPri). Values are 0 - 63. Priority Code Point (PCP) profiles are associated with the tagged priority bits (pbits). Values are 0 - 7.

Traffic priority can be re-classified by using several different settings. The Class setting can be used to re-classify which egress priority queue is to be used. The Priority Selection setting re-classifies the priority by changing the PCP value.

Traffic is mapped to eight egress queues based on the PCP values. The CoS / QoS screen provides the ability to change the egress queue (Class) or PCP value (Priority Selection) or both. Priority values are 0 - 7, 7 being the highest priority. Class values are 0 - 7, 0 being discard and 7 being the highest egress queue. Class values 0 - 7 correspond to egress queues 0 - 7.

Multiple CoS profile filters with the same name can be configured and applied to a single port by associating the CoS profile with a Bandwidth profile. If the ingress frame does not meet any of the configured CoS profiles, the ingress traffic will use the default class.

CoS / QoS Name

The pull-down menu selects New CoS or Modify Cos. To configure a new Cos profile, select New Cos. If a configured Cos profile needs to be modified, select Modify CoS.

Enter a new name for the CoS profile in the text box.

Default Class

Use the Default Class pull-down menu to change the priority of the PCP value.

Mode

Use the Mode pull-down menu to select the classification mode of none, Layer 2 (PCP) or Layer 3 (DSCP).

- | | |
|------------|---|
| Layer 2 | Selects the layer 2 classification only (PCP), IP classification is ignored. |
| Layer 3 | Selects the IP only classification (DSCP), layer 2 classification is ignored. |
| L2 over L3 | Selects layer 2 classification over IP classification when both are present. |
| L3 over L2 | Selects IP clarification over layer 2 when both are present. |

On an access port, only untagged frames are accepted with the following format: Data.

On a tunnel port, zero or one tag is allowed for DSCP selection with the following formats: Data Only or Ethertype (8100) and Data.

On a tunnel port, zero, one, or two layers of tags are allowed for DSCP selection with the following formats: Data Only or Ethertype (8100) and Data or Ethertype (88a8) and Data or Ethertype (88a8) and Ethertype (8100) and Data or Ethertype (8100) and Ethertype (8100) and Data.

If no CoS is assigned to a port, the egress frame will use the default Class value.

Class

Use the Class pull-down menu to select the egress priority queue to be used for the profile.

Type

The Class type is displayed depending on the Mode selected. Layer 2 will display PCP and Layer 3 will display DSCP.

Priority Selection

Enter the priority values in the Priority Selection text box.

Examples for PCP values are: 1 or 1,4 or 1..3 or 2..3,6..7 or none. A value of 0 - 7 are valid entries.

Examples for DSCP values are: 1 or 1,4 or 1..3 or 2..3,6..7 or none. A value of 0 - 63 are valid entries.

Delete Item

Check the box and click the **Delete** button to delete the selected CoS profiles.

Use the text boxes on the NEW entry row to add a new CoS profile. Click in the CoS/QoS Name text box and enter a name for the profile. Use the pull-down menus to configure the Default Class, Mode and Class. Enter a value in the Priority Selection text box.

Click on the **Apply** button to activate the changes. Once the information has been applied, a new entry is added to the CoS table. Click the **Save** button to permanently save the changes.

2.3.5 Protection

The following options are available.



2.3.5.1 Link Redundancy

Link Redundancy is only supported on models with 2 fiber or copper uplink ports.

The Link Redundancy screen provides the ability to configure the module for link redundancy. When configured for link redundancy, the module will transmit and receive traffic on the primary port (F1) and no traffic on the backup port (F2). When a fiber failure occurs on the primary port, the module will switch over to the backup port within 50msec.

Link Redundancy

Item Name	Configured
Link Redundancy Configuration	No Redundant fiber
Port F1 Status	Not available
Port F2 Status	Not available

Apply Save Cancel

In order to configure Link Redundancy, the hardware DIP-switch setting must be configured for *software override active*. To change the DIP-switch settings, go to section 2.3.2.1 and use the pull-down menu under the Global Settings and select the *DIP-switches disabled, software override active* option. Click on the *Apply* button to activate the changes.

Use the Link Redundancy Configuration pull-down menu to select the configuration for link redundancy as No Redundancy, Redundant fiber with no return to primary or Redundant fiber with return to primary. When configured for *Redundant fiber with no return to primary*, F1 and F2 operate as redundant links. A fault on the primary port F1, will cause a fail over to the secondary port F2 within 50msec. F1 will

become the secondary port once the port has been restored because **Redundant fiber with no return to primary** has been selected.

When configured for **Redundant fiber with return to primary**, a fault on the primary port F1, will cause a fail over to the secondary port F2 within 50msec. The module will return to the primary port F1 after the link has been restored for 6 seconds.

2.3.5.2 RSTP

The RSTP screen provides the ability to configure Rapid Spanning Tree Protocol (RSTP).

Rapid Spanning Tree (RSTP)
Instance Selection: Global ▼

Item Name	Configured
RSTP Bridge ID	
RSTP Designated Root	
RSTP Bridge Priority	32768
RSTP Bridge Aging Time (s)	20
RSTP Hello Time (s)	2
RSTP Forward Delay (s)	15

Apply Save Cancel

The Rapid Spanning Tree Protocol is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of RSTP is to prevent network loops and provide fast convergence after a topology change.

Use the Instance Selection pull-down menu to select Global, Port F1, Port F2, Port P1, Port P2, Port P3 or Port P4. Select Global.

RSTP Bridge ID

The RSTP Bridge ID is displayed.

RSTP Designated Root

The designated root is displayed.

RSTP Bridge Priority

The bridge with the lowest priority is elected as the Root Bridge for the domain. The Bridge Priority can be modified in increments of 4096 from 0 to 61,440. The default Bridge Priority is 32,768.

Enter a new value in the text box.

RSTP Bridge Age Time (s)

The amount of time a module saves configuration BPDUs. A value from 6 - 40 seconds is a valid entry. The default Bridge Max Age Time is 20 seconds.

Enter a new value in the text box.

RSTP Hello Time (s)

The Root Bridge sends configuration BPDUs every 2 seconds. A value from 1 - 5 seconds is a valid entry. The default Hello Time is 2 seconds.

Enter a new value in the text box.

RSTP Forward Delay (s)

The time interval for listening and learning states. A value from 4 - 30 seconds is a valid entry. The default Forward Delay is 15 seconds.

Enter a new value in the text box.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Instance Selection pull-down menu to select Global, Port F1, Port F2, Port P1, Port P2, Port P3 or Port P4. Select Port P1.

Rapid Spanning Tree (RSTP)

Instance Selection: Port P1 ▾

Item Name	Configured
RSTP Port Configuration	Tunnel ▾
RSTP Port State	Not available
RSTP Port Priority	<input type="text" value="128"/>
RSTP Port Path Cost	<input type="text" value="20000"/>

Apply Save Cancel

RSTP Port Configuration

Use the RSTP Port Configuration pull-down menu to select how BPDUs frames are handled (Discard, Peer or Tunnel).

Discard RSTP protocol is disabled on the module.

Peer RSTP protocol is enabled and RSTP BPDUs frames are processed.

Tunnel RSTP protocol is disabled on the module but RSTP BPDUs are tunneled through the module.

RSTP Port State

Displays the RSTP state of the port.

Spanning Tree protocol uses port cost and port priority to determine the best path to be used. The table below shows the recommended port cost based on link speed. The port with the lowest port cost has the highest priority.

Link Speed	Port Cost Values
10Mbps	2,000,000
100Mbps	200,000
1Gbps	20,000
10Gbps	2,000
100Gbps	200

Recommended Port Cost vs. Link Speed

RSTP Port Priority

If two paths have the same port cost, the bridges must select a preferred path. Port Priority is used to determine the preferred path. A value from 0 - 240, with 240 being the highest priority, is a valid entry. The default Port Priority is 128.

Enter a new value in the text box.

RSTP Port Path Cost

The cost of a port is typically based on port speed. The faster the port, the lower the port cost. See table below. A value from 1 - 200,000,000 is a valid entry. The default Port Cost is 20,000.

Enter a new value in the text box.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

2.3.5.3 MRP

The MRP screen provides the ability to configure Media Redundancy Protocol (MRP).

Media Redundancy Protocol (MRP)

Instance Selection: Global ▾

Item Name	Configured
MRP Configuration	Disabled ▾
Port F1 MRP	Disabled ▾
Port F2 MRP	Disabled ▾
Port P1 MRP	Disabled ▾
Port P2 MRP	Disabled ▾
Port P3 MRP	Disabled ▾
Port P4 MRP	Disabled ▾

Apply Add MRP Save Cancel

NOTE: The number of ports will vary depending on the model.

IEC 62439-2 defines Media Redundancy Protocol (MRP) as a ring protocol that is used in high availability industrial networks. MRP is implemented as a ring protocol similar to Ethernet Ring Protocol Switch (ERPS), which allows the ring to recovery from a single failure.

In an MRP ring, the ring manager is named Media Redundancy Manager (MRM) and the ring clients are named Media Redundancy Clients (MRCs).

MRM and MRC ring ports support three status: disabled, blocked, and forwarding. Disabled ring ports drop all the received frames. Blocked ring ports drop all the received frames except the MRP control frames. Forwarding ring ports forward all the received frames.

During normal operation, the network works in the Ring-Closed status (Figure 1). In this status, one of the MRM ring ports is blocked, while the other is forwarding. Conversely, both ring ports of all MRCs are forwarding. Loops are avoided because the physical ring topology is reduced to a logical stub topology.

In case of failure, the network works in the Ring-Open status (Figure 2). For instance, in case of failure of a link connecting two MRCs, both ring ports of the MRM are forwarding; the MRCs adjacent to the failure have a blocked and a forwarding ring port; the other MRCs have both ring ports forwarding. Also, in the Ring-Open status, the network logical topology is a stub.

The Global screen allows MRP to be enabled or disabled globally and on a per port bases.

MRP Configuration

Use the MRP Configuration pull-down menu to globally enable or disable MRP on the module.

Port F1 MRP

Use the Port F1 MRP pull-down menu to enable or disable MRP on the port.

Port F2 MRP

Use the Port F2 MRP pull-down menu to enable or disable MRP on the port.

Port P1 MRP

Use the Port P1 MRP pull-down menu to enable or disable MRP on the port.

Port P2 MRP

Use the Port P2 MRP pull-down menu to enable or disable MRP on the port.

Port P3 MRP

Use the Port P3 MRP pull-down menu to enable or disable MRP on the port.

Port P4 MRP

Use the Port P4 MRP pull-down menu to enable or disable MRP on the port.

Once MRP is enabled and the *Apply* button has been clicked, the *Add MRP* button will be active.

Click the *Add MRP* button to create a MRP instance.

Media Redundancy Protocol (MRP)
Instance Selection: New MRP ▾

Item Name	Configured
MRP Instance Name	<input type="text"/> *
MRP Role	Manager ▾
MRP Recovery Time	200 ms ▾
MRP Priority	<input type="text"/>
MRP Ring Domain ID	<input type="text"/>
Ring Port 1	Port F1 ▾ ***
Ring Port 1 State	MRP participant ▾
Ring Port 2	Port F1 ▾ ***
Ring Port 2 State	MRP participant ▾
VLAN ID	<input type="text"/>

* Not a valid MRP name or contains an illegal character. Please correct. Valid length is 1-32 characters and may contain a-z, A-Z, 0-9 and the special characters ! # \$ % & ' () * + , / : ;
< = > ? @ [\] ^ ` { | } ~ and space
*** The Ring Port selections must be different ports.

Create MRP Cancel

MRP Instance Name

Enter the name of the MRP instance in the text box.

MRP Role

Use the MRP Role pull-down menu to select Manager (MRM) or Client (MRC).

MRP Recovery Time

Enter the recovery time in the text box. Valid recovery times are 200 or 500 (ms).

MRP Priority

Enter the priority in the text box. Valid priority values are 0 to 65535. 40960 is the default value.

MRP Ring Domain ID

All devices in a ring configured with MRP must be part of the same domain. The domain is in a hexadecimal format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. The domain has a range of 0x00000000-0000-0000-0000-000000000001 – 0xFFFFFFFF-FFFF-FFFFFFFF-FFFFFFFFFFFFE. The default value is 0xFFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFF.

Enter the MRP Ring Domain ID in the text box.

Ring Port 1

Use the Ring Port 1 pull-down menu to select the port to be defined as Ring Port 1. Only the ports enabled with MRP will be available.

Ring Port 1 Status

Use the Ring Port 1 Status pull-down menu to configure the port status for MRP Participate or Block Traffic. It is recommended to initially leave the setting to MRP Participate. The MRP Protocol will block traffic automatically on one of the ports.

Ring Port 2

Use the Ring Port 2 pull-down menu to select the port to be defined as Ring Port 2. Only the ports enabled with MRP will be available.

Ring Port 2 Status

Use the Ring Port 2 Status pull-down menu to configure the port status for MRP Participate or Block Traffic. It is recommended to initially leave the setting to MRP Participate. The MRP Protocol will block traffic automatically on one of the ports.

VLAN ID

Configures the VLAN ID used for the MRP protocol.

Enter the VLAN ID in the text box. A VLAN ID must be configured using the VLAN Configuration and VLAN Interface menu options.

Click the *Create MRP* button to create the MRP instance.

Media Redundancy Protocol (MRP)

Instance Selection: Global ▼

Item Name	Configured
MRP Configuration	Enabled ▼
Port F1 MRP	Enabled ▼
Port F2 MRP	Enabled ▼
Port P1 MRP	Enabled ▼
Port P2 MRP	Disabled ▼
Port P3 MRP	Disabled ▼
Port P4 MRP	Disabled ▼

Apply

Add MRP

Save

Cancel

NOTE: The number of ports will vary depending on the model.

Use the Instance Selection pull-down menu to view the status of the MRP Instance. Select the MRP Instance name in the pull-down menu.

MRM Status

Media Redundancy Protocol (MRP)
Instance Selection: M1 ▾

Item Name	Configured
MRP Instance Name	<input type="text" value="M1"/>
MRP Role	Manager ▾
MRP Operational Role	Manager
MRP Recovery Time	200 ms ▾
MRP Priority	<input type="text" value="20000"/>
MRP Ring Domain ID	<input type="text" value="FFFFFFFF-FFFF-FFFF-000000000001"/>
Ring Port 1	Port F1 ▾
Ring Port 1 State	MRP participant ▾
Ring Port 2	Port F2 ▾
Ring Port 2 State	MRP participant ▾
VLAN ID	<input type="text" value="2"/>
Ring Status	Closed
Ring Port 1 Status	Blocking
Ring Port 2 Status	Forwarding

Apply Add MRP Save Cancel Delete

The last three entries show the status of the connection.

MRC Status

Media Redundancy Protocol (MRP)

Instance Selection: M1 ▼

Item Name	Configured
MRP Instance Name	M1
MRP Role	Client ▼
MRP Operational Role	Client
MRP Recovery Time	200 ms ▼
MRP Priority	20000
MRP Ring Domain ID	FFFFFFFF-FFFF-FFFF-000000000001
Ring Port 1	Port F1 ▼
Ring Port 1 State	MRP participant ▼
Ring Port 2	Port F2 ▼
Ring Port 2 State	MRP participant ▼
VLAN ID	2
Ring Status	N/A
Ring Port 1 Status	Forwarding
Ring Port 2 Status	Forwarding

Apply Add MRP Save Cancel Delete

2.3.5.4 LAG/LLDP

The LAG/LLDP screen provides the ability to configure the ports on the module to support Link Aggregation Group and Link Aggregation Control Protocol.

Link Aggregation Group (LAG)

Instance Selection: Global ▼

Item Name	Configured
LAG Configuration	Disabled ▼
System Identification	00-06-87-02-CB-A0
System Priority	0
Frame Forwarding	Standard ▼

Apply Save Cancel

Link Aggregation Groups (LAG) and Link Aggregation Control Protocol (LACP) are methods to provide more than one link between two devices and automate the configuration and maintenance of the links. LAG and LACP is defined in the IEEE 802.1ax standard.

Use the Instance Selection pull-down menu to select Global, Aggregation Group or Port Group. Select Global.

LAG Configuration

Use the LAG Configuration pull-down menu to Enable or Disable LAG.

System Identification

The System Identification is displayed.

System Priority

Enter a value for the System Priority in the text box. Enter a value from 0 to 65535.

Frame Forwarding

Use the Frame Forwarding pull-down menu to select the frame forwarding algorithm as Standard or MAC SA/DA XOR.

Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

Use the Instance Selection pull-down menu to select Global, Aggregation Group or Port Group. Select Aggregation Group.

Link Aggregation Group (LAG)

Instance Selection: Aggregation Group ▼

Aggr	LAG Mode	LACP Protocol	LACP Mode	Aggreg Type	Key Type	LACP Role	Tx Rate	Aggreg Key	Max Active
F1	Disabled ▼	Tunnel ▼	Static ▼	Individual ▼	Auto ▼	Passive ▼	Slow ▼	<input type="text" value="1"/>	4 ▼
F2	Disabled ▼	Tunnel ▼	Static ▼	Individual ▼	Auto ▼	Passive ▼	Slow ▼	<input type="text" value="2"/>	4 ▼
P1	Disabled ▼	Tunnel ▼	Static ▼	Individual ▼	Auto ▼	Passive ▼	Slow ▼	<input type="text" value="3"/>	4 ▼
P2	Disabled ▼	Tunnel ▼	Static ▼	Individual ▼	Auto ▼	Passive ▼	Slow ▼	<input type="text" value="4"/>	4 ▼
P3	Disabled ▼	Tunnel ▼	Static ▼	Individual ▼	Auto ▼	Passive ▼	Slow ▼	<input type="text" value="5"/>	4 ▼
P4	Disabled ▼	Tunnel ▼	Static ▼	Individual ▼	Auto ▼	Passive ▼	Slow ▼	<input type="text" value="6"/>	4 ▼

Apply Save Cancel

NOTE: The number of ports will vary depending on the model.

The following configuration options are available for each port.

LAG Mode

Use the LAG Mode pull-down menu to Enable or Disable LAG on the selected port.

LACP Protocol

Use the LACP Protocol pull-down menu to Enable or Disable LACP on the selected port.

LACP Mode

Use the LACP Mode pull-down menu to configure the link active mode to Static or Active on the selected port.

Aggreg Type

Use the Aggregation Type pull-down menu to select Aggregation or Individual on the selected port.

Key Type

Use the Key Type pull-down menu to select Fixed or Auto on the selected port.

LACP Role

Use the LACP Role pull-down menu to select Passive or Active for the selected port.

Tx Rate

Use the Tx Rate pull-down menu to select Slow or Fast for the selected port.

Aggreg Key

Enter the numeric value in the text box (0 to 65535) for the Aggregation Key on the selected port.

Max Active

Use the Max Active pull-down menu to select the number of ports.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Instance Selection pull-down menu to select Global, Aggregation Group or Port Group. Select Port Group.

Link Aggregation Group (LAG)
Instance Selection: Port Group ▼

			Aggregation			Partner		
Port	Port Priority	Port Key	Status	ID	LP	System ID	Port	Priority
F1	<input type="text" value="32768"/>	<input type="text" value="1"/>	Detached	0	None ▼	00-00-00-00-00-00	0	0
F2	<input type="text" value="32768"/>	<input type="text" value="2"/>	Detached	0	None ▼	00-00-00-00-00-00	0	0
P1	<input type="text" value="32768"/>	<input type="text" value="3"/>	Detached	0	None ▼	00-00-00-00-00-00	0	0
P2	<input type="text" value="32768"/>	<input type="text" value="4"/>	Detached	0	None ▼	00-00-00-00-00-00	0	0
P3	<input type="text" value="32768"/>	<input type="text" value="5"/>	Detached	0	None ▼	00-00-00-00-00-00	0	0
P4	<input type="text" value="32768"/>	<input type="text" value="6"/>	Detached	0	None ▼	00-00-00-00-00-00	0	0

Apply Save Cancel

NOTE: The number of ports will vary depending on the model.

Port Priority

Enter a value in the text box (0 to 65535). The default is 32768.

Port Key

Enter a value in the text box (0 to 65535).

Aggregation

Status

Displays the port status (Detached or Attached).

ID

Displays the Aggregation ID.

LP

Use the LP pull-down menu to configure the Logical Port number.

Partner

System ID

Displays the partner system ID.

Port

Displays the partner port number.

Priority

Displays the partner port priority.

Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

2.3.6 Security

The following options are available.



2.3.6.1 Authenticate, Authorize, Account (AAA)

The AAA screen provides the ability to configure Authentication, Authorization and Accounting (AAA), Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+) and Port Based Network Access Control (IEEE 802.1X).

Authenticate, Authorize, Account (AAA)

Selection: Authentication Method

Item Name	Configured
AAA Configuration	Disabled
Authentication Method	local

Apply Save Cancel

Authentication, Authorization and Accounting (AAA) is a framework for controlling access to computer resources, enforcing policies, auditing usage and providing the information necessary to bill for services. Remote Authentication Dial-In User Service (RADIUS) is a client/server system that secures networks against unauthorized access. When a user tries to access a specific module, the RADIUS server is contacted to authenticate and authorize.

Terminal Access Controller Access-Control System Plus (TACACS+) is a connection oriented Authentication, Authorization, and Accounting (AAA) protocol. TACACS+ is used to authenticate, authorize, and accounting for TCP connections.

Port Based Network Access Control is defined in IEEE 802.1X . It uses EAPoL (Ethernet Authentication Protocol over LAN) to communicate between the Supplicant (Client), Authenticator (Ethernet switch) and Authentication Server.

Use the Selection pull-down menu to select Authentication Method, TACACS+, RADIUS or Port Authentication (802.1x). Select Authentication Method.

AAA Configuration

Use the AAA Configuration pull-down menu to enable or disable AAA processing.

Authentication Method

In the Authentication Method text box, enter the authentication method (local, tacacs+ or radius). Multiple methods can be configured.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Selection pull-down menu to select Authentication Method, TACACS+, RADIUS or Port Authentication (802.1x). Select TACACS+.

Authenticate, Authorize, Account (AAA)
Selection: TACACS+

Item Name	Configured
TACACS+ Configuration	Disabled
Server Host 1	
Server Host 2	
Authentication Port	49
Accounting Port	49
Server Key	
Server Timeout (s)	60

ApplySaveCancel

TACACS+ Configuration

Use the TACACS+ Configuration pull-down menu to enable or disable TACACS+ processing.

Server Host 1

Enter the IP Addresses of the TACACS+ servers in the text box.

Server Host 2

Enter the IP Addresses of the TACACS+ servers in the text box.

Authentication Port

Enter the authentication port number in the text box. The default port number is 49.

Accounting Port

Enter the accounting port number in the text box. The default port number is 49.

Server Key

Enter the Server Key in the text box.

Server Timeout (s)

Enter the server timeout value in seconds in the text box. The default value is 60 seconds.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Selection pull-down menu to select Authentication Method, TACACS+, RADIUS or Port Authentication (802.1x). Select RADIUS.

Authenticate, Authorize, Account (AAA)
Selection: RADIUS

Item Name	Configured
RADIUS Configuration	Disabled
Server Host 1	
Server Host 2	
Authentication Port	1812
Accounting Port	1813
Server Key	
Server Timeout (s)	60
Number of Server Retries	2

Apply Save Cancel

RADIUS Configuration

Use the RADIUS Configuration pull-down menu to enable or disable RADIUS processing.

Server Host 1

Enter the IP Addresses of the RADIUS servers in the text box.

Server Host 2

Enter the IP Addresses of the RADIUS servers in the text box.

Authentication Port

Enter the authentication port number in the text box. The default port number is 1812.

Accounting Port

Enter the accounting port number in the text box. The default port number is 1813.

Server Key

Enter the Server Key in the text box.

Server Timeout (s)

Enter the server timeout value in seconds in the text box. The default value is 60 seconds.

Number of Server Retries

Enter a value in seconds between 0 and 10 in the text box. The default value is 2 seconds.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Use the Selection pull-down menu to select Authentication Method, TACACS+, RADIUS or Port Authentication (802.1x). Select Port Authentication (802.1x).

Authenticate, Authorize, Account (AAA)

Selection: Port Authentication (802.1X) ▼

802.1X Configuration: Disabled ▼ 802.1X Guest VLAN: Disabled ▼

Port	Port Mode	Port Type	Port Status	Retry Time (s)	Reauthorize Time (s)	Guest VLAN ID	Guest VLAN
F1	Tunnel ▼	On ▼	N/A	30	3600	1	Disable ▼
F2	Tunnel ▼	On ▼	N/A	30	3600	1	Disable ▼
P1	Tunnel ▼	On ▼	N/A	30	3600	1	Disable ▼
P2	Tunnel ▼	On ▼	N/A	30	3600	1	Disable ▼
P3	Tunnel ▼	On ▼	N/A	30	3600	1	Disable ▼
P4	Tunnel ▼	On ▼	N/A	30	3600	1	Disable ▼

Apply Save Cancel

NOTE: The number of ports will vary depending on the model.

802.1x Configuration

Use the 802.1x Configuration pull-down menu to enable or disable 802.1x processing.

802.1x Guest VLAN

Use the 802.1x Guest VLAN pull-down menu to enable or disable Guest VLAN.

Port

Indicates the port designation.

Port Mode

Use the Port Mode pull-down menu to select how 802.1x frames are handled (Discard, Peer or Tunnel).

- Discard 802.1X is disabled, 802.1X frames are discarded.
- Peer 802.1X is enabled and protocol is operating.
- Tunnel 802.1X is disabled, 802.1X frames are tunneled.

Port Type

Use the Port Type pull-down menu to select the authentication mode (Automatic, Mac Bypass, On or Off).

- Automatic Standard 802.1X authentication on a port.
- Mac Bypass 802.1X MAC bypass authentication on a port.
- On Port is always authorized, 802.1X disabled.
- Off Port is always unauthorized.

Port Status

The Port Status is displayed.

Retry Time (s)

Enter a value in seconds from 1 to 60 for the retry timer. The default value is 30 seconds.

Reauthorize Time (s)

Enter a value in seconds for the reauthorization time. The default value is 3600 seconds.

Guest VLAN ID

Enter the VLAN ID in the text box used for Guest access.

Guest VLAN

Use the Guest VLAN pull-down menu to enable or disable Guest VLAN on the specific port.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

2.3.6.2 Access Control List (ACL)

The ACL screen provides basic traffic filtering capabilities with Access Control Lists (ACL).

Access Control List (ACL)
ACL Status: Disabled Access Type Default : Permit

Entry	Protocol	Starting IP Address	Ending IP Address	Access Type	Destination Port	Delete
NEW	ARP			Deny	-1	

Apply Save Cancel Delete

Access Control Lists can prevent certain traffic from entering or exiting the management port. ACLs can be configured for ARP, ICMP, IP, TCP and UDP protocols. These protocols can be configured to be permitted or denied access.

ACL Status

Use the ACL Status pull-down menu to globally enable or disable ACL processing.

Access Type Default

Use the Access Type Default pull-down menu to configure the default ACL behavior as Permit or Deny.

Entry

When no ACL entries are configured, NEW is displayed. When ACL entries are defined, the system will number the entries sequentially.

Protocol

Use the Protocol pull-down menu to select the protocol as ARP, ICMP, IP, TCP or UDP.

Starting IP Address

Enter the starting source IP Address in the text box.

Ending IP Address

Enter the ending source IP Address in the text box.

Access Type

Use the Access Type pull-down menu to select the access type as Permit or Deny.

Destination Port

When TCP or UDP is selected under Protocol, enter the destination port number in the text box.

Click the **Delete** button to delete all ACL entries.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

2.3.6.3 Secure Shell (SSH)

The Secure Shell (SSH) screen provides the ability to configure and view SSH parameters on the module.

Secure Shell (SSH)

Item Name	Configured
SSH Protocol	Enabled ▾
SFTP Protocol	Enabled ▾
Plaintext Password	Enabled ▾
DSA/RSA Key Authentication	DSA/RSA ▾
TCP Port Number	22
RSA Fingerprint	a7:53:4d:86:69:fe:e6:f3:96:5b:ca:54:a1:be:47:e8
DSA Fingerprint	94:6c:52:12:17:e9:ad:a6:ec:34:50:7a:67:0c:08:d4

Apply Save Cancel Generate Keys

Secure Shell (SSH) protocol provides authentication, encryption, and the integrity of data transmitted over a network. SSH uses public-key cryptography to authenticate the remote devices and allows the remote device to authenticate the user. The module supports SSH Version 2.

SSH Protocol

Use the SSH Protocol pull-down menu to enable or disable SSH protocol.

SFTP Protocol

Use the SFTP Protocol pull-down menu to enable or disable SFTP protocol.

Plaintext Password

Use the Plaintext Password pull-down menu to enable or disable Plaintext Password.

DSA / RSA Key Authentication

Use the DSA / RSA Key Authentication pull-down menu to enable the specific encryption key. Select DSA Only, RSA Only or DSA/RSA. DSA/RSA is the default.

RSA Public key generated via the Rivest, Shamir and Adleman algorithm.

DSA Public key generated via the Digital Signature Algorithm.

The SSH function supports password (plain text) and public key authentication methods. Password is plain text entered in the client application.

TCP Port

A text box allows the configuration of the TCP Port used during a SSH session. A value of 1 to 65,535 is accepted.

RSA Fingerprint

The RSA fingerprint is displayed.

DSA Fingerprint

The DSA fingerprint is displayed.

Click the ***Generate Keys*** button to replace the current SSH keys and close all active SSH sessions.

Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

2.3.6.4 User

The User screen provides the ability to create and modify user accounts. Up to four user accounts can be configured.

User

User Selection: admin ▾

User		Global	
Item Name	Configured	Item Name	Configured
Username	admin	Authentication Retries	5
Password	*****	Authentication Timeout (s)	300
User Type	admin	Session Lockout (s)	300
Session Timeout (s)	300	FTP Session Timeout (s)	300
SSH filename		Strong Password	Not Required

Modify Add New User Save Cancel Delete

User

Username

Displays the user name.

Password

Displays ***** associated with the password.

User Type

Displays the type of user.

Session Timeout (s)

Displays the value in seconds for the User login session timeout.

SSH Filename

Displays the SSH filename.

Global

Authentication Retries

Displays the number of authentication retries.

Authentication Timeout (s)

Displays the value of the authentication timeout.

Session Lockout (s)

Displays the value in seconds for the session lockout.

FTP Session Timeout (s)

Displays the value in seconds of the FTP session timeout.

Strong Password

Displays the status of the Strong Password parameter.

Click the **Add New User** button to create another user account.

The Login screen is displayed.

To change the User parameters, enter the current username and password in the provided text boxes and click the **Log In** button.

User

User Selection: admin

Item Name	Configured
Username	<input type="text"/>
Password	<input type="password"/>

User
 User Selection: admin ▼

Item Name	Configured
Username	<input style="width: 100%;" type="text"/>
Password	<input style="width: 100%;" type="password"/>
New Password (again)	<input style="width: 100%;" type="password"/>
User Type	admin ▼
Session Timeout (s)	<input style="width: 100%;" type="text" value="300"/>
SSH filename	<input style="width: 100%;" type="text"/>

Create User
Save
Cancel

NOTES:

Username must contain 1-32 characters and may contain a-z, A-Z, 0-9 and the special characters dash (-), underscore (_) and period (.)

Passwords must contain 1-32 printable characters and may contain a-z, A-Z, 0-9 and the special characters ! # \$ % & ' () * + , / : ; < = > ? @ [\] ^ ` { | } ~ and space.

When changing the session timeout value using the Session Timeout (s) text box, the new value will not take effect until the user logs out and logs back in.

Username

Enter the username of the new user in the text box.

Password

Enter the password for the new user in the text box.

New Password (again)

Enter the password again in the text box.

User Type

Use the User Type pull-down menu to assign the user privileges.

- | | |
|------------|---|
| admin | An admin user has full read/write privileges including user name and password changes. |
| read-write | A read-write user has full read/write privileges with the exception of user name and password operations. |
| read-only | A read-only user can only view the configuration of the module and will not be allowed to make any changes. |
| deny | A deny user does not have any access to the module. |

Session Timeout (s)

Enter a new value for the session timeout in the text box. A value of 0 to 3600 seconds is a valid entry.

SSH Filename

Enter the new SSH filename in the text box.

Click the **Create User** button to create the user account.

Click the **Save** button to permanently save the changes.

To modify a user, use the User Selection pull-down menu and select the user.

Click the **Modify** button to change the parameters of the selected user.

The Login screen is displayed.

To change the User parameters, enter the current username and password in the provided text boxes and click the **Log In** button.

User

User Selection: admin

Item Name	Configured
Username	<input type="text"/>
Password	<input type="password"/>

User
 User Selection: admin ▼

User		Global	
Item Name	Configured	Item Name	Configured
Username	<input type="text" value="admin"/>	Authentication Retries	<input type="text" value="5"/>
Password	<input type="password"/>	Authentication Timeout	<input type="text" value="300"/>
New Password (again)	<input type="password"/>	Session Lockout (s)	<input type="text" value="300"/>
User Type	admin ▼	FTP Session Timeout (s)	<input type="text" value="300"/>
Session Timeout (s)	<input type="text" value="300"/>	Strong Password	Not Required ▼
SSH filename	<input type="text"/>		

Apply
Save
Cancel

NOTES:

Username must contain 1-32 characters and may contain a-z, A-Z, 0-9 and the special characters dash (-), underscore (_) and period (.)

Passwords must contain 1-32 printable characters and may contain a-z, A-Z, 0-9 and the special characters ! # \$ % & ' () * + , / : ; < = > ? @ [\] ^ ` { | } ~ and space.

When changing the session timeout value using the Session Timeout (s) text box, the new value will not take effect until the user logs out and logs back in.

Username

Enter the username of the new user in the text box.

Password

Enter the password for the new user in the text box.

New Password (again)

Enter the password again in the text box.

User Type

Use the User Type pull-down menu to assign the user privileges.

- | | |
|------------|---|
| admin | An admin user has full read/write privileges including user name and password changes. |
| read-write | A read-write user has full read/write privileges with the exception of user name and password operations. |
| read-only | A read-only user can only view the configuration of the module and will not be allowed to make any changes. |
| deny | A deny user does not have any access to the module. |

Session Timeout (s)

Enter a new value for the session timeout in the text box. A value of 0 to 3600 seconds is a valid entry.

SSH Filename

Enter the new SSH filename in the text box.

Authentication Retries

Enter a new value for the number of authentication retries.

Authentication Timeout (s)

Enter a new value for the authentication timeout.

Session Lockout (s)

Enter a new value in seconds for the session lockout.

FTP Session Timeout (s)

Enter a new value in seconds of the FTP session timeout.

Strong Password

Use the Strong Password pull-down menu to enable or disable strong passwords.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

2.3.6.5 Storm Control

The Storm Control screen provides the ability to configure storm prevention for broadcast, multicast and unicast traffic on each port.

Storm Control

Port Selection: F1 ▼

Item Name	Configured
Threshold Type	None ▼
Threshold High	<input type="text" value="0"/>
Threshold Low	<input type="text" value="0"/>
Broadcast Storm Control	Disabled ▼
Mutlicast Storm Control	Disabled ▼
Unicast Storm Control	Disabled ▼
Status	not blocking, recieving 0.00 Bits/Sec

Apply Save Cancel

Use the Port Selection pull-down menu to select the port.

Threshold Type

Use the Threshold Type pull-down menu to configure the Threshold for none, bit/sec or interface threshold %.

Threshold High

Enter a value for the High Threshold in bit/sec or threshold %. This will depend on the Threshold Type selection.

Threshold Low

Enter a value for the Low Threshold in bit/sec or threshold %. This will depend on the Threshold Type selection.

Broadcast Storm Control

Use the Broadcast Storm Control pull-down menu to enable or disable broadcast storm control.

Multicast Storm Control

Use the Multicast Storm Control pull-down menu to enable or disable multicast storm control.

Unicast Storm Control

Use the Unicast Storm Control pull-down menu to enable or disable unicast storm control.

Status

Displays the status of the configured storm control.

Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

2.3.7 Maintenance

The following options are available.



2.3.7.1 Firmware Upgrade

The Firmware Upgrade screen provides the ability to upgrade the firmware and bootloader. Also displayed is the current and swap images installed on the module and the current update status.

Firmware Upgrade

Current firmware revision	v2.2.4
Upgrade firmware	<div>Choose FileNo file chosenUpload</div>
Revert firmware	<div>Revert Firmware</div>
Current image version	v2.2.4, Nov 22 2019 09:53:01
Next swap image version	v2.1.10, Aug 09 2019 09:36:38
Current partition	1
Current update status	not busy, no error, complete (0)

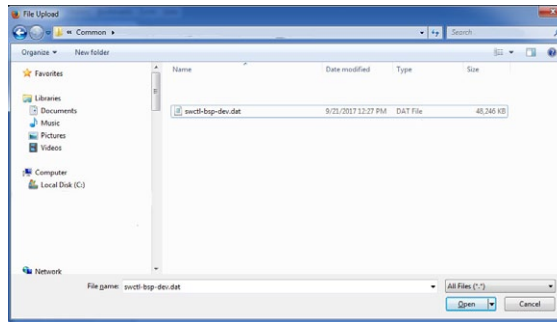
SaveCancel

Current firmware revision

Displays the current firmware.

Upgrade Firmware

To upgrade the firmware or bootloader, click the ***Browse*** button. A file selection screen will open.



Browse the workstation for the location of the firmware or bootloader file. Once selected, click the **Open** button. Click the **Upload** button to start the upgrade process.

Note: Filenames can not contain any spaces.

Revert firmware

The **Revert Firmware** button reverts the firmware to the revision listed in the Next swap image version. To change the reverted firmware revision (Next swap image version) to the latest version, repeat the upgrade procedure as indicated above.

Current image version

The details of the current firmware is displayed.

Next swap image version

The details of the backup firmware is displayed.

Current update status

The status of the upgrade is displayed.

Click the **Cancel** button to revert back to the previous Apply state.

Click the **Save** button to permanently save the changes.

2.3.7.2 Module Maintenance

The Module Maintenance screen provides the ability to restart, restore and save/restore the current/saved configuration. The current and swap image revisions are displayed.

The screenshot displays the 'Module Maintenance' interface. It features a title bar at the top. Below it, there are several rows of controls and status information. Each row consists of a label on the left and a button or text on the right. The rows are: 'Restart/Reboot' with a 'Restart' button; 'Restore factory defaults' with a 'Restore Factory Defaults' button; 'Restore factory defaults retaining IP address' with a 'Restore Factory Defaults Retaining IP' button; 'Save Current Configuration to Workstation' with a 'Save Current Configuration to Workstation' button; 'Restore Configuration from Workstation' with a 'Restore Configuration from Workstation' button; 'Current image version' with the text 'v2.2.4, Nov 22 2019 09:53:01'; 'Next swap image version' with the text 'v2.1.10, Aug 09 2019 09:36:38'; and 'Current partition' with the text '1'. At the bottom left, there are 'Save' and 'Cancel' buttons.

Module Maintenance	
Restart/Reboot	<button>Restart</button>
Restore factory defaults	<button>Restore Factory Defaults</button>
Restore factory defaults retaining IP address	<button>Restore Factory Defaults Retaining IP</button>
Save Current Configuration to Workstation	<button>Save Current Configuration to Workstation</button>
Restore Configuration from Workstation	<button>Restore Configuration from Workstation</button>
Current image version	v2.2.4, Nov 22 2019 09:53:01
Next swap image version	v2.1.10, Aug 09 2019 09:36:38
Current partition	1
<button>Save</button> <button>Cancel</button>	

Restart/Reboot

To restart the module, click the **Restart** button. A dialog box is displayed. Click **Yes** or **No** to continue with the restart process.

Restore factory defaults

To restore the module to factory defaults, click the **Restore Factory Default** button. A text box is displayed. Click **Yes** or **No** to continue with defaulting the module to factory settings.

Restore factory defaults retaining IP address

To restore the module to factory defaults but retain the current IP settings, click the **Restore Factory Default Retaining IP** button. A dialog box is displayed. Click **Yes** or **No** to continue with defaulting the module to factory settings.

Save Current Configuration to Workstation

To save the current configuration to a workstation, click the **Save Current Configuration to Workstation** button. A filename text box is displayed. Enter the name of the configuration in the text box. Click the **Save** button. A dialog box is displayed allowing the file to be Opened or Saved.

Restore Configuration from Workstation

To restore a configuration saved on a workstation, click the **Restore Configuration from Workstation** button. Click the **Browse** button. A file selection screen will open. Locate the file and click **Open**. Click the **Upload** button to complete the operation.

2.3.7.3 Browser Settings

The Browser Settings screen provides the ability to change the auto refresh, session timeouts and menu display options.

Browser Settings

Item Name	Configured
Auto Refresh Rate	30 seconds
Session Timeout	30 minutes
Auto Refresh	Enabled
Menu Type	Click to Expand

Apply

Cancel

Auto Refresh Rate

To change the Auto Refresh Rate, use the pull-down menu and select a new value.

3 seconds

5 seconds

10 seconds

15 seconds

20 seconds

30 seconds

60 seconds

Session Timeout

To change the Session Timeout, use the pull-down menu and select a new value.

1 minute

5 minutes

30 minutes

1 hour

4 hours

8 hours

No timeout

Auto Refresh

To enable or disable Auto Refresh, use the pull-down menu to select enable or disable.

Menu Type

Use the Menu Type pull-down menu to change the method of accessing the side menu (Always Expanded, Auto Expand or Click to Expand).

- | | |
|-----------------|--|
| Always Expanded | When selected, all side menu options are displayed. |
| Auto Expand | When selected, the menu option will expand when hovering the mouse over the selection. |
| Click to Expand | When selected, the menu option will expand once the option is clicked. |

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

2.3.7.4 Syslog

The Syslog screen provides the ability to view and configure Syslog functions.

Item Name	Configured
Syslog Protocol	Disabled
Syslog Server IP	192.168.1.221
Severity Logging Level	Info
Facility Code	23
Numbers of Entries to Display	15
Total Log Entries	0
Debug Entries	0
Info Entries	0
Notice Entries	0
Warning Entries	0
Error Entries	0
Critical Entries	0
Alert Entries	0
Emergency Entries	0

Apply Save Cancel

Syslog is a standard for message logging per RFC 5424. It is used to manage system messages and alerts. Each message is labeled with a facility code, indicating the software type generating the message, and the message is assigned a severity level.

Use the Selection pull-down menu to select Configuration or Log Entries. Select Configuration.

Syslog Protocol

Use the Syslog Protocol pull-down menu to select enable or disable syslog functionality.

Syslog Server IP

Enter the IP address of the syslog service in the text box.

Severity Logging Level

Use the Severity Logging Level pull-down menu to select the minimum entry level for the syslog record as Debug, Info, Notice, Warning, Error, Critical, Alert or Emergency.

Debug	Messages that contain information normally of use only when debugging a program.
Info	Informational messages.
Notice	Conditions that are not error conditions, but that may require special handling.
Warning	Warning conditions.
Error	Error conditions.
Critical	Hard device errors.
Alert	A condition that should be corrected immediately.
Emergency	A panic condition.

Facility Code

A facility code is used to specify the type of program that is logging the messages. Enter the Facility code in the text box.

Number of Entries to Display

Enter the number of entries to be displayed in the log.

Total Log Entries / Severity Entries

The number of the different entries are displayed.

Click the ***Cancel*** button to revert back to the previous Apply state.

Click on the ***Apply*** button to activate the changes.

Click the ***Save*** button to permanently save the changes.

Use the Selection pull-down menu to select Configuration or Log Entries. Select Log Entries.

Syslog

Selection: Log Entries

Display: ☒ Emergency ☒ Alert ☒ Critical ☒ Error ☒ Warning ☒ Notice ☒ Info ☒ Debug

ID	Severity Level	Date / Time	Message
1	Error	01/02/2000 04:05:49 PM	Link down port 2
2	Warning	01/02/2000 04:05:49 PM	PoE status port 2 error 0
3	Error	01/02/2000 04:05:52 PM	Link down port F2
4	Warning	01/02/2000 04:05:53 PM	Link up port 2
5	Warning	01/02/2000 04:05:55 PM	PoE status port 2 error 0
6	Warning	01/02/2000 04:05:56 PM	Link up port F2
7	Error	01/02/2000 04:06:02 PM	Link down port 2
8	Warning	01/02/2000 04:06:05 PM	Link up port 2
9	Error	01/02/2000 04:06:25 PM	Link down port 2
10	Warning	01/02/2000 04:06:28 PM	Link up port 2
11	Info	01/02/2000 04:11:40 PM	Serial console port session stopped user admin
12	Warning	01/02/2000 04:13:29 PM	Module configuration change

Save

Refresh

Next Page

Previous Page

Check the boxes of the severity level to be displayed in the log.

The Log Entries Table displays each message with ID, Level, Date / Time and Message.

The module retains the last 1000 entries.

Click the **Refresh** button to update the screen.

Click the **Next Page** button to display more trap entries.

Click the **Previous Page** button to to return to the previous page.

2.3.7.5 SNMP Traps

The SNMP Traps screen provides the ability to display the trap history on the module and also enable/disable specific traps.

SNMP Traps			
Selection: SNMP Log Entries			
Index	Date / Time	Trap #	Message
1737	01/02/2000 09:41:31 PM	25	PoE status port 4 error 1
1736	01/02/2000 09:41:19 PM	25	PoE status port 4 error 0
1735	01/02/2000 09:36:10 PM	25	PoE status port 4 error 1
1734	01/02/2000 09:35:52 PM	25	PoE status port 4 error 0
1733	01/02/2000 09:32:09 PM	25	PoE status port 4 error 1
1732	01/02/2000 09:32:02 PM	25	PoE status port 4 error 0
1731	01/02/2000 09:29:15 PM	25	PoE status port 4 error 1
1730	01/02/2000 09:28:56 PM	25	PoE status port 4 error 0
1729	01/02/2000 09:25:13 PM	25	PoE status port 4 error 1
1728	01/02/2000 09:25:07 PM	25	PoE status port 4 error 0
1727	01/02/2000 09:22:01 PM	25	PoE status port 4 error 1
1726	01/02/2000 09:21:58 PM	25	PoE status port 4 error 0
1725	01/02/2000 09:21:57 PM	25	PoE status port 4 error 1
1724	01/02/2000 09:21:55 PM	25	PoE status port 4 error 0
1723	01/02/2000 09:21:52 PM	25	PoE status port 4 error 1
Save Refresh Next Page Previous Page			

Use the Selection pull-down menu to select SNMP Log Entries or SNMP Trap Filtering. Select SNMP Log Entries.

Index

A index number is assigned to each trap entry

Date / Time

Displays the date and time of the trap entry.

Trap

Displays the identifying number for the trap.

Message

Displays a description of the trap.

Click the **Refresh** button to update the screen.

Click the **Next Page** button to display more trap entries.

Click the **Previous Page** button to to return to the previous page.

Use the Selection pull-down menu to select SNMP Log Entries or SNMP Trap Filtering. Select SNMP Trap Filtering.

SNMP Traps

Selection: SNMP Trap Filtering

Trap #	Description	Status	Severity Level
1	Module Cold Start	Allow	Notice
2	Module Reset	Allow	Warning
4	Module Power Removed	Allow	Warning
5	Module Power Applied	Allow	Warning
6	Link Down	Allow	Error
7	Link Up	Allow	Warning
8	Primary Link Up	Allow	Info
9	Primary Link Down	Allow	Error
10	Secondary Link Up	Allow	Info
11	Secondary Link Down	Allow	Info
12	Standby Link Up	Allow	Info
13	Standby Link Down	Allow	Info
14	Loop Prevention Block	Allow	Warning
15	Loop Prevention Clear	Allow	Info

ApplySaveCancelNext PagePrevious Page

The SNMP Trap Filtering screen provides a list of traps that can be generated by the module. Each individual trap can be enabled or disabled.

Trap

Identifies the trap by number.

Description

Provides a short description of the trap.

Status

Use the pull-down menu to enable (allow) or disable (filter) the individual traps.

Severity Level

The severity level for each individual trap is displayed.

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

Click the **Next Page** button to display more trap entries.

Click the **Previous Page** button to return to the previous page.

2.3.7.6 SMTP

The SMTP screen provides the ability to configure Simple Mail Transfer Protocol (SMTP) Relay Agent on the module.

SMTP Relay Agent	
Item Name	Configured
SMTP Forwarding	Disabled ▼
SMTP IP Address	<input type="text"/>
SMTP User Name	<input type="text"/>
SMTP From Address	<input type="text"/>
SMTP Password	<input type="text"/>
SMTP Port Number	25 <input type="text"/>
Email Recipients	<input type="text"/>
Event Severity Level	Info ▼

SMTP Forwarding

Use the SMTP Forwarding pull-down menu to enable or disable SMTP Event Forwarding.

SMTP IP Address

Enter the IPv4 address of the SMTP mail server in the text box.

SMTP User Name

Enter the name of the user that will be used to login to the email server in the text box.

SMTP Password

Enter the password for the selected email account in the text box.

SMTP Port Number

Enter the SMTP port number in the text box. The default port number is 25.

Email Recipients

Enter the 'from-address' to indicate who the email is from in the text box

Events Security Level

Use the Events Security Level pull-down menu to configure the minimum syslog severity error for forwarding events: emergency (highest), alert, critical, error, warning, notice, info (informational), debug (lowest).

Click the **Cancel** button to revert back to the previous Apply state.

Click on the **Apply** button to activate the changes.

Click the **Save** button to permanently save the changes.

2.3.7.7 Splash Screen

The Splash screen provides the ability to configure a message that is displayed after the module has been restarted or rebooted. The message is displayed after the Entry screen is displayed.

Splash Screen

Item Name	Configured
Input Data	<div></div>
Review Data	<div></div>

Enter a message to be displayed in the Input Data text box. The message is visible in the Review Data text box.

Splash Screen

Item Name	Configured
Input Data	<div>This product is for the use of authorized users only. Individuals using this product without authority are subject to monitoring of their activities.</div>
Review Data	<div>This product is for the use of authorized users only. Individuals using this product without authority are subject to monitoring of their activities.</div>

3.0 APPENDIX A: FIRMWARE UPDATE

3.1 OVERVIEW

Appendix A describes the procedure for updating the firmware using ftp and web interface.

3.2 SAVE CURRENT SETTINGS

Under normal circumstances the current configuration of the module will carry forward to the new version during the update, however, extreme events such as a power outage can lead to settings being lost. Prior to upgrading, it is recommended that the settings be recorded. The settings can be viewed using the Command Line Interface (CLI) over Telnet.

3.3 COPY THE FILES TO YOUR HARD DRIVE

The files should be copied to a convenient location on the hard drive of the workstation. The name of the firmware file is similar to vx_x_xx_PoE_Prod.dat. The 'x's represent the release revision of the firmware.

Depending on the operating system of the workstation and/or FTP installation, the name of the files may need to be renamed to the "DOS 8.3 Format". Rename the vx_x_xx_PoE_Prod.dat to PoE.dat and store the files in the root or c:\ directory.

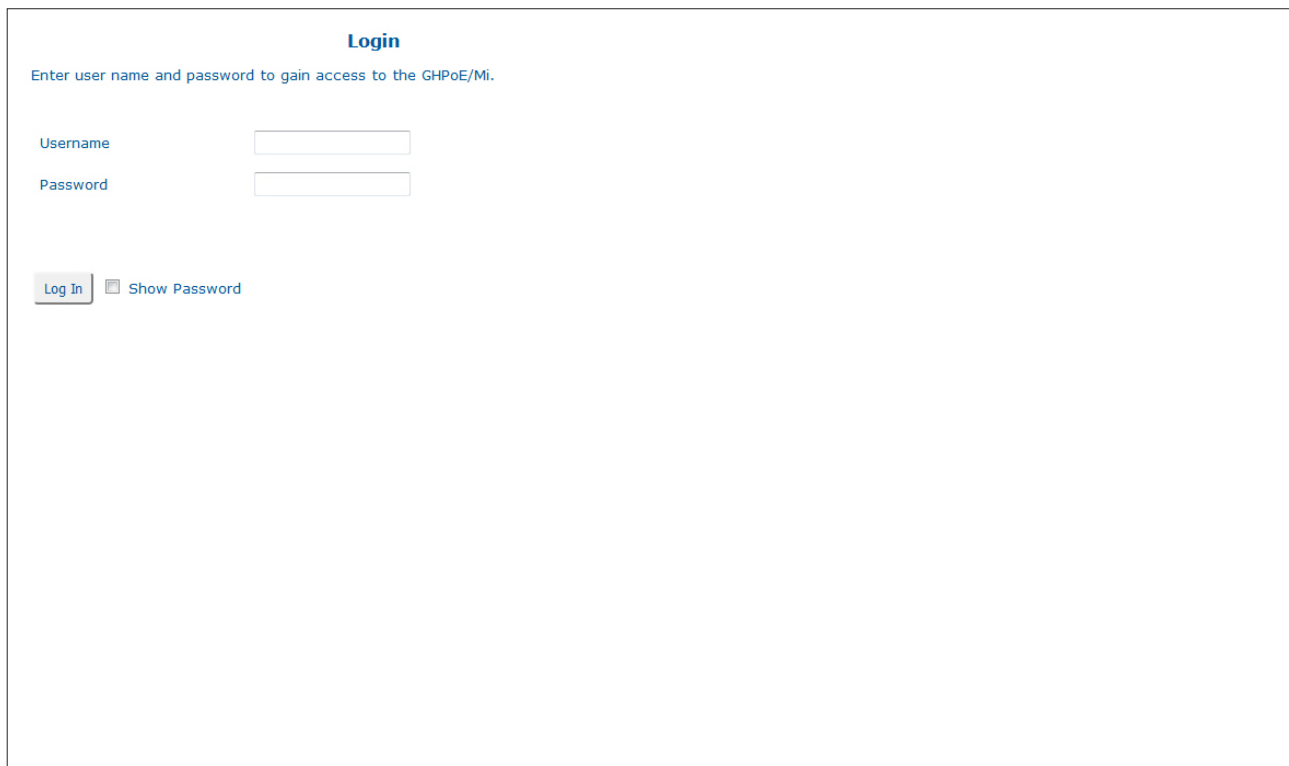
Renaming the file will allow the new file to overwrite the old file, saving memory allocation space on the switch.

3.4 UPDATING THE FIRMWARE USING THE WEB INTERFACE

The firmware on the module can be upgraded using the IP-based Web management interface. The IP-based web management can be accessed through any of the Ethernet RJ-45 or fiber ports and facilitates the configuration and real-time operation monitoring of each port.

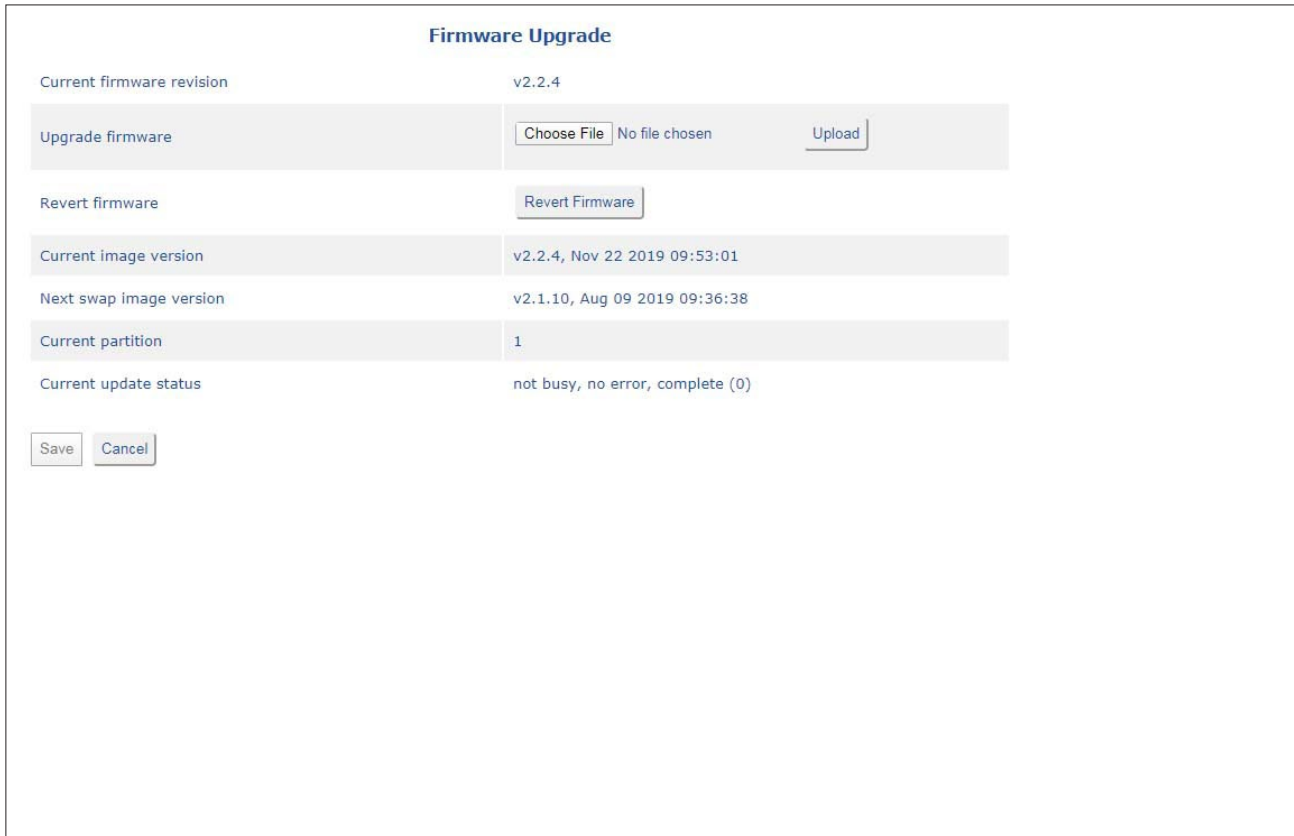
The factory default IP address is 192.168.1.220.

Enter the Username and Password to gain access to the module. The default user name and password is: admin, public

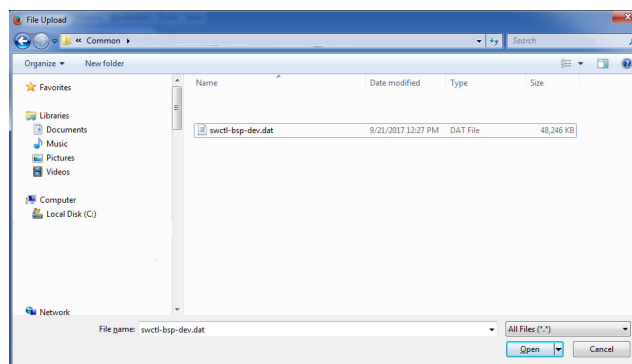


The screenshot shows a web-based login interface. At the top, the word "Login" is centered in blue. Below it, a blue instruction line reads: "Enter user name and password to gain access to the GHPoE/Mi." There are two input fields: "Username" and "Password", each with a corresponding text label to its left. Below the "Password" field is a checkbox labeled "Show Password". At the bottom left, there is a "Log In" button with a blue border.

Access the Firmware Upgrade screen to upgrade the firmware on the switch.

The image shows a web-based 'Firmware Upgrade' interface. At the top, the title 'Firmware Upgrade' is centered. Below it, the 'Current firmware revision' is displayed as 'v2.2.4'. There are two main sections: 'Upgrade firmware' and 'Revert firmware'. The 'Upgrade firmware' section contains a 'Choose File' button, the text 'No file chosen', and an 'Upload' button. The 'Revert firmware' section contains a 'Revert Firmware' button. Below these sections, several status fields are shown: 'Current image version' (v2.2.4, Nov 22 2019 09:53:01), 'Next swap image version' (v2.1.10, Aug 09 2019 09:36:38), 'Current partition' (1), and 'Current update status' (not busy, no error, complete (0)). At the bottom left, there are 'Save' and 'Cancel' buttons.

To upgrade the firmware, click the **Choose File** button. A file selection screen will open.



Browse the workstation for the location of the firmware file. Once selected, click the **Open** button.

Click the **Upload** button to start the upgrade process.

NOTE: Do not remove power during the upgrade procedure until the switch has rebooted with the new firmware.

After the firmware has been upgraded, it may be desirable to also upgrade the “Next swap image revision”. The switch can be reverted to the “Next swap image revision” by clicking on the **Revert Firmware** button. To change the reverted firmware revision (Next swap image version) to the latest version, repeat the upgrade procedure as indicated above.

Verify the firmware has been upgraded by accessing the Firmware Upgrade screen. The “Current firmware revision” will indicate the upgraded version. If the firmware was upgraded a second time, the “Next swap image revision” will also indicate the upgraded version.

Firmware Upgrade

Current firmware revision

v2.2.4

Upgrade firmware

Choose File

No file chosen

Upload

Revert firmware

Revert Firmware

Current image version

v2.2.4, Nov 22 2019 09:53:01

Next swap image version

v2.1.10, Aug 09 2019 09:36:38

Current partition

1

Current update status

not busy, no error, complete (0)

Save

Cancel

4.0 WARRANTY AND COPYRIGHT

General and Copyright Notice

This publication is protected by U.S. and international copyright laws. All rights reserved. The whole or any part of this publication may not be reproduced, stored in a retrieval system, translated, transcribed, or transmitted, in any form, or by any means, manual, electric, electronic, electromagnetic, mechanical, chemical, optical or otherwise, without prior explicit written permission of Omnitron Systems Technology, Inc.

The following trademarks are owned by Omnitron Systems Technology, Inc.: FlexPoint™, FlexSwitch™, iConverter®, miConverter™, NetOutlook®, OmniLight®, OmniConverter®, RuggedNet®, Omnitron Systems Technology, Inc.™, OST™ and the Omnitron logo.

All other company or product names may be trademarks of their respective owners.

The information contained in this publication is subject to change without notice. Omnitron Systems Technology, Inc. is not responsible for any inadvertent errors.

Warranty

This network product and the included AC/DC power adapter are warranted to the original purchaser (Buyer) against defects in material and workmanship for a period of two (2) years from the date of shipment. The warranty for the network product (excluding the AC/DC power adapter) can be extended to five (5) years by registering the product at www.omnitron-systems.com/support within ninety (90) days from the date of shipment. During the warranty period, Omnitron will, at its option, repair or replace a product which is proven to be defective with the same product or with a product with at least the same functionality.

For warranty service, the product must be sent to an Omnitron designated facility, at Buyer's expense. Omnitron will pay the shipping charge to return the product to Buyer's designated US address using Omnitron's standard shipping method.

Limitation of Warranty

The foregoing warranty shall not apply to product malfunctions resulting from improper or inadequate use and/or maintenance of the equipment by Buyer, Buyer-supplied equipment, Buyer-supplied interfacing, unauthorized modifications or tampering with equipment (including removal of equipment cover by personnel not specifically authorized and certified by Omnitron), or misuse, or operating outside the environmental specification of the product (including but not limited to voltage, ambient temperature, radiation, unusual dust, etc.), or improper site preparation or maintenance.

No other warranty is expressed or implied. Omnitron specifically disclaims the implied warranties of merchantability and fitness for any particular purpose.

The remedies provided herein are the Buyer's sole and exclusive remedies. Omnitron shall not be liable for any direct, indirect, special, incidental, or consequential damages, whether based on contract, tort, or any legal theory.

Environmental Notices

The equipment covered by this manual must be disposed of or recycled in accordance with the Waste Electrical and Electronic Equipment Directive (WEEE Directive) of the European Community directive 2012/19/EU on waste electrical and electronic equipment (WEEE) which, together with the RoHS Directive 2015/863/EU, for electrical and electronic equipment sold in the EU after July 2019. Such disposal must follow national legislation for IT and Telecommunication equipment in accordance with the WEEE directive: (a) Do not dispose waste equipment with unsorted municipal and household waste. (b) Collect equipment waste separately. (c) Return equipment using collection method agreed with Omnitron.

The equipment is marked with the WEEE symbol shown to indicate that it must be collected separately from other types of waste. In case of small items the symbol may be printed only on the packaging or in the user manual. If you have questions regarding the correct disposal of equipment go to www.omnitron-systems.com/support or e-mail to Omnitron at intlinfo@omnitron-systems.com.



5.0 CUSTOMER SUPPORT INFORMATION

If you encounter problems while installing this product, contact Omnitron Technical Support:

Phone: (949) 250-6510

Fax: (949) 250-6514

Address: Omnitron Systems Technology, Inc.

38 Tesla

Irvine, CA 92618, USA

Email: support@omnitron-systems.com

URL: www.omnitron-systems.com