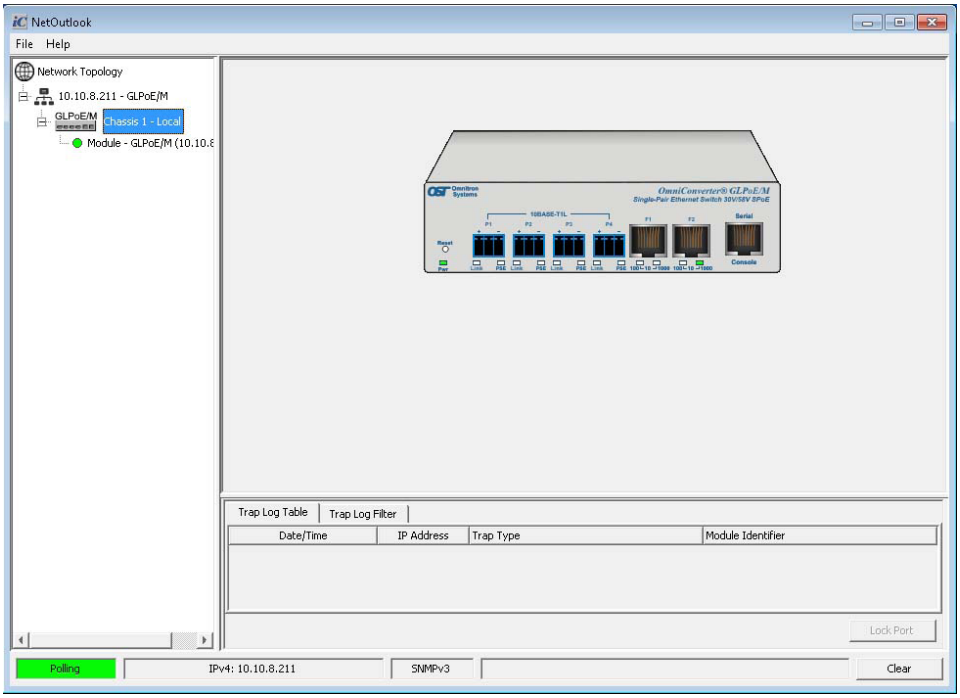
Omnitron Systems

OmniConverter and RuggedNet SPE Switches Network Management Software



User Manual

Release 5.3

www.omnitron-systems.com

General and Copyright Notice

Table of Contents

1.0 OVERVIEW

1.1 Using This Guide

This manual describes how to use NetOutlook to manage OmniConverter and RuggedNet switches. This guide is organized to help you install and configure the NetOutlook management software.

1.1.1 New Features

Revision 5.3.29 adds support for OmniConverter and RuggedNet SPE switches with firmware release 3.1.

1.2 Technical Support Contact Information

If you encounter problems while installing or operating this product, contact Omnitron Technical Support. Please make sure you have the following information when calling:

- NetOutlook software version number. Click on the ***Help*** button located in the top left corner of the screen. Click on the ***About*** button to display the version of the software.
- Version of firmware on the Management Module.

Phone: (949) 250-6510
Fax: (949) 250-6514
Address: Omnitron Systems Technology, Inc.
38 Telsa
Irvine, CA 92618, USA
E-mail: support@omnitron-systems.com
URL: http://www.omnitron-systems.com

1.3 General NetOutlook Description

NetOutlook is a general purpose SNMP-based graphical network management software that provides an efficient, user-friendly way to configure and manage devices installed on a single network or on a series of networks by providing an intuitive graphical display with real-time status and alarm (trap) information. It operates under Microsoft Windows, as well as other popular network management environments.

Module	Current Firmware	First Version Back	Second Version Back
OmniConverter SPE Switches	3.1	-	-
RuggedNet SPE Switches	3.1	-	-

NetOutlook 5.3 Compatibility

1.4 Management Overview

1.4.1 SNMP Management

The OmniConverter and RuggedNet Switches supports SNMPv1/v2c/v3 for basic configuration and real-time alarm reporting.

1.4.2 IP Management Capabilities

The OmniConverter and RuggedNet switches can be managed by accessing the IP address of the module through any Ethernet (fiber or copper) port.

2.0 INSTALLATION PROCEDURE

2.1 Recommended System Requirements

IBM or compatible PC with 1GHz CPU or better

Microsoft Windows Server 2003/2008/2012/2016, Windows Vista, Windows 7/8/10

CD-ROM, Ethernet Network Interface Card, 512MB RAM, 60MB of free hard drive space

SVGA monitor with 1024x768 resolution (1280x1024 recommended)

Windows compatible mouse

NOTE: In Windows, increasing the default font and/or changing the resolution may cause some screens to not display correctly. Decreasing the font size or screen resolution will correct the screen display output.

2.2 New Installation

1. Run the installer file **setup.exe** on the CD-ROM to install NetOutlook.
2. Click the ***Next*** button on the NetOutlook Setup screen to start the installation process.
3. Read and accept the Licensing Agreement by checking the 'I accept the terms of the Licence Agreement" box. Click the ***Next*** button to continue.
4. Select the destination directory to install the software. The default destination directory is "C:\Program Files\NetOutlook\." Click the ***Next*** button to continue.
5. A NetOutlook application icon is inserted in the Programs Section of the Start Menu located on the Windows Task Bar. The installation program also places a NetOutlook shortcut icon on the desktop.

2.3 Upgrade Installation

1. Run the installer file **setup.exe** on the CD-ROM to install the new version of NetOutlook.
2. Click the ***Next*** button on the NetOutlook Setup screen to start the installation process.
3. Read and accept the Licensing Agreement by checking the 'I accept the terms of the Licence Agreement" box. Click the ***Next*** button to continue.
4. Select the destination directory to install the software. The default destination directory is "C:\Program Files\NetOutlook\." Click the ***Next*** button to continue. NetOutlook automatically overwrites any previous version of NetOutlook.
5. A NetOutlook application icon is inserted in the Programs section of the Start menu located on the Windows task bar. The installation program can also place a shortcut icon on the desktop if that box is checked.

   NOTE: For Windows 2003 Server, NetOutlook explicitly uninstalls the previous version as part of the upgrade procedure.

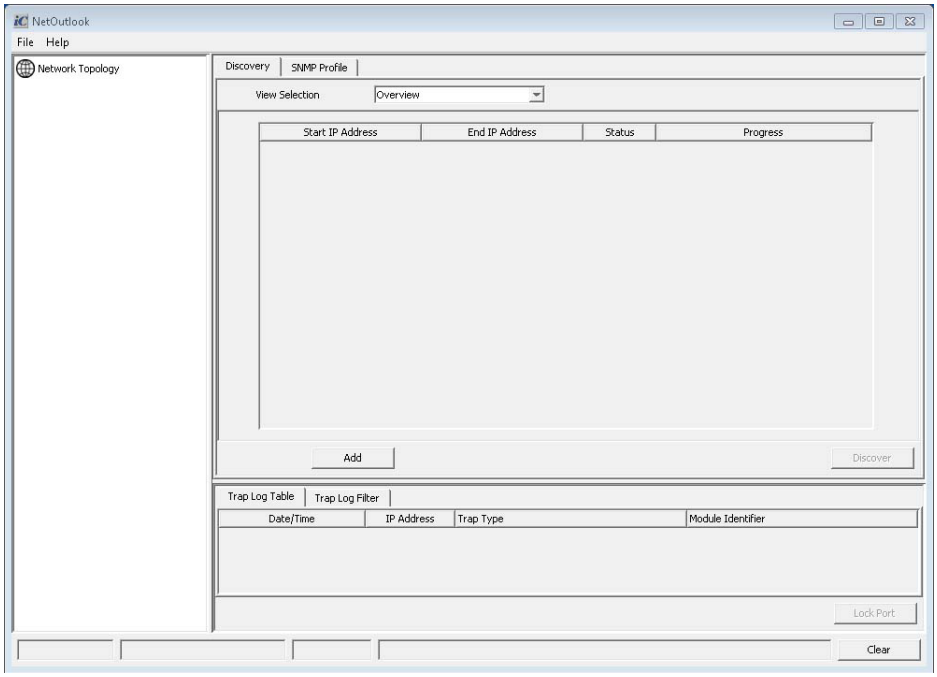
3.0 GETTING STARTED

3.1 Launch NetOutlook

When NetOutlook is launched, NetOutlook will check for a valid Software License Key. If the License Key is not stored in the User Folder or in the installation directory location from a previous version of NetOutlook, NetOutlook will prompt the user to Register the Software License Key.

Click on the NetOutlook Start Menu shortcut or double click the desktop icon created earlier in the installation to start the NetOutlook application (refer to section 2.0). The NetOutlook screen will appear. On the right side of the screen are two tabs: Discovery and SNMP Profile.

NOTE: It is recommended when running Windows 7 to launch NetOutlook in administrator mode. Right-clicking on the NetOutlook shortcut and selecting "run as Administrator".



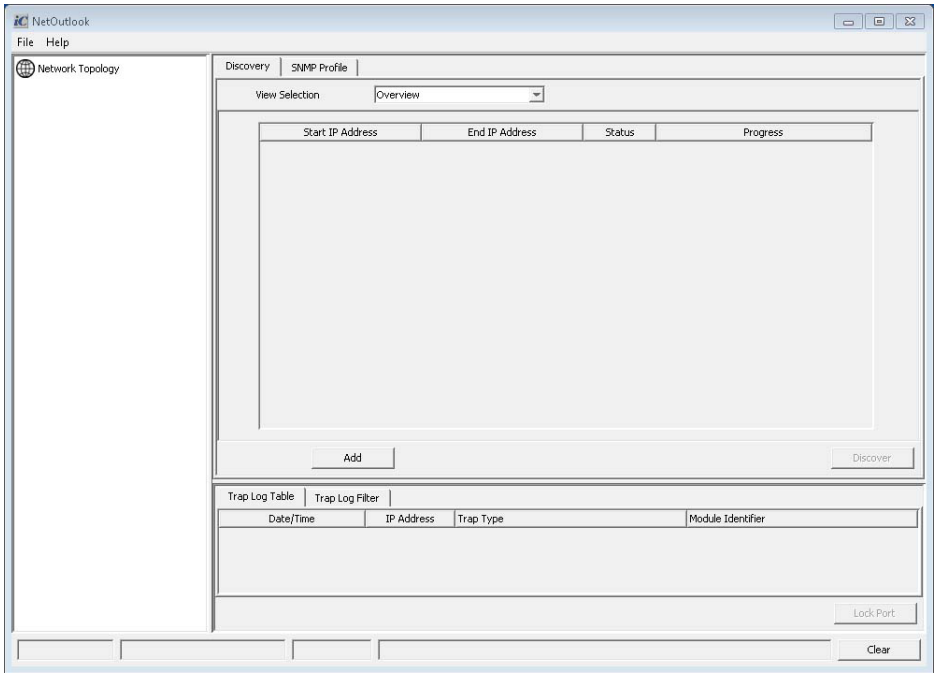
NetOutlook screen

NetOutlook will locate any previously saved IP addresses and display the results. If there are no IP addresses defined, use the Discovery tab to add a range of IP addresses to be auto-discovered.

NOTE: The Network Topology window is unique to each user that logs into the computer with NetOutlook installed.

3.2 Configuring IP Addresses and SNMP Profiles

The Discovery tab provides the ability to add, auto-discover, or delete IP addresses.

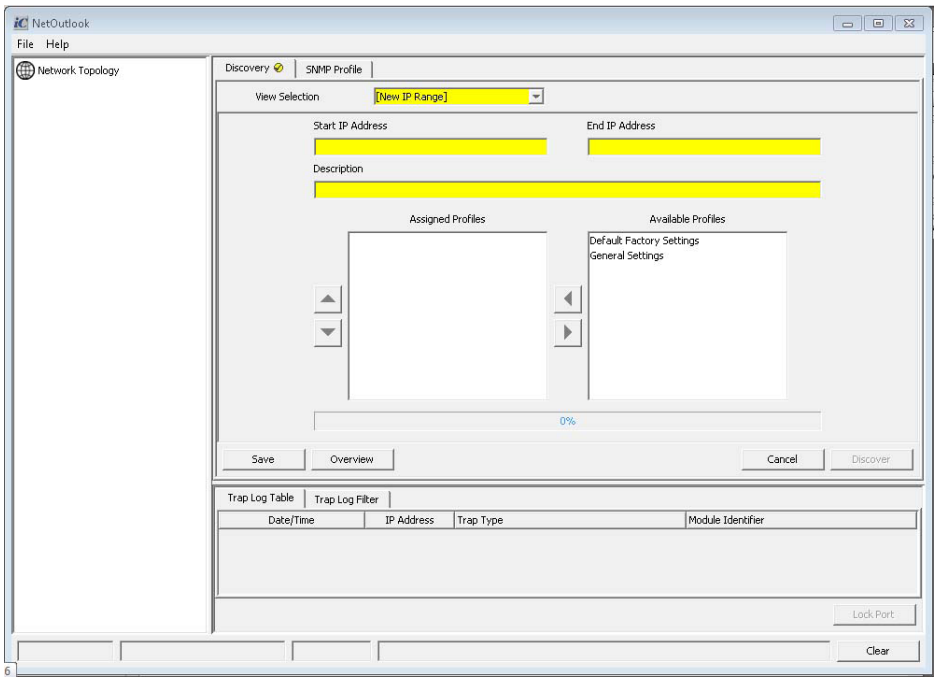


Network Topology - IP Address Range Tab

To add a new IP address, click on the ***Add*** button.

3.2.1 Configuring IP Addresses

Enter the new IP address in the Start IP Address text box. If a range of IP addresses is desired, enter the end IP address in the End IP Address test box. A description of the IP address range can be added using the Description text box.



IP Address Range Tab - Add IP Address

NOTE: The IP Addresses and/or IP Address Range Lists cannot overlap each other.

Select an SNMP Profile from the Available Profiles list to be used with the IP address. Click the left arrow to select the profile for the new IP Address.

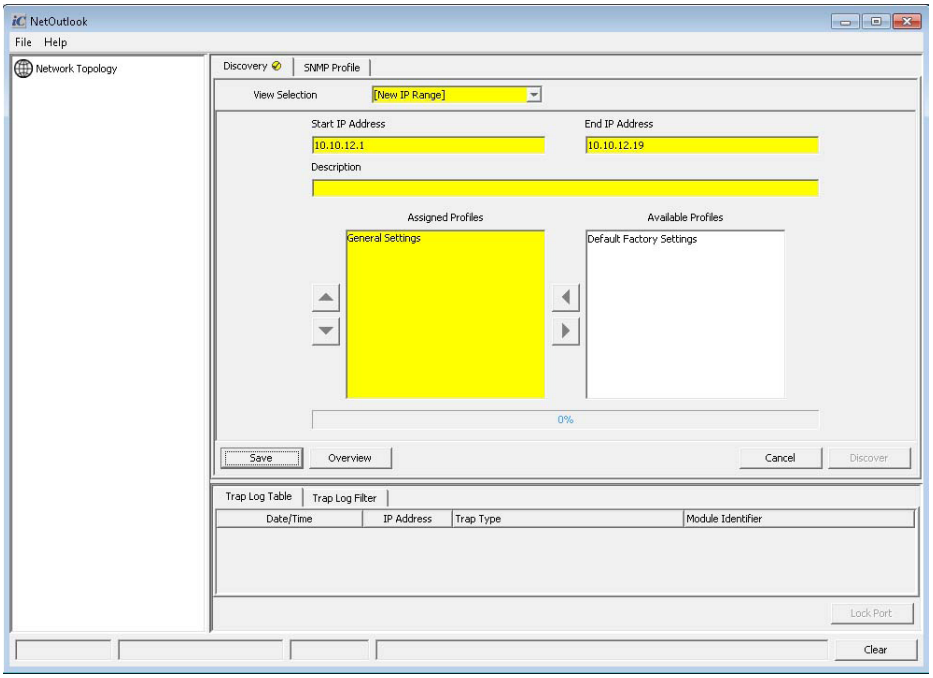
General Settings

The General Settings profile uses factory default settings for all SNMPv1 community names and SNMPv3 passwords and usernames. This profile can be changed (see Section 3.2.2).

Default Factory Settings

The Default Factory Settings profile uses factory default settings for all SNMPv1 community names and SNMPv3 passwords and usernames. This profile cannot be changed.

To change or create a new SNMP Profile, go to Section 3.2.2.

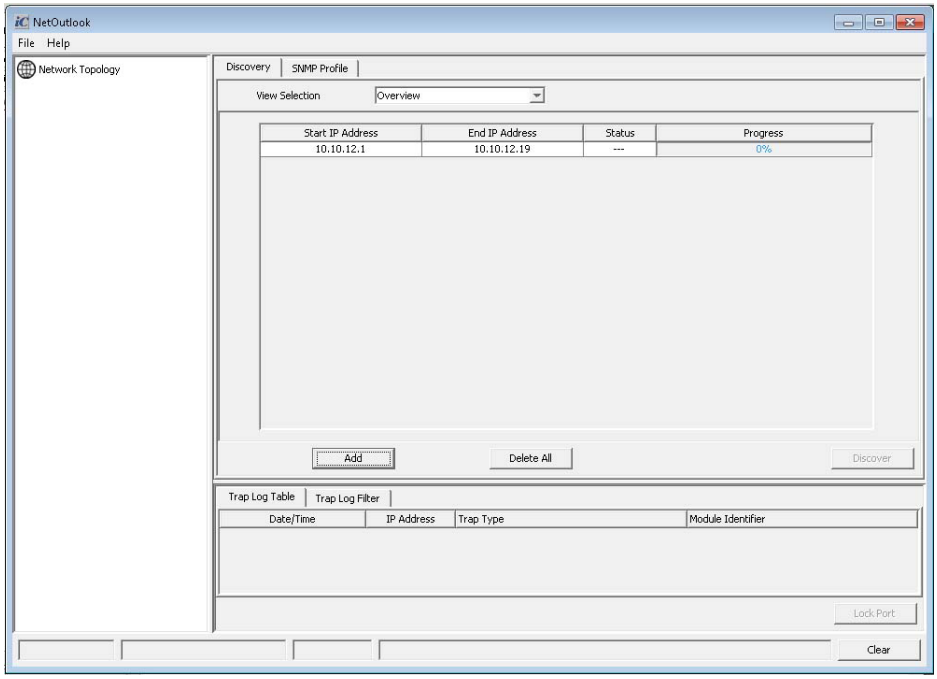


IP Address Range Tab - Add IP Address and SNMP Profile

Click the ***Save*** button to add the new IP address to the IP Address Range list. You may add as many IP addresses as needed.

IP Addresses can be deleted from the IP Address Range List by clicking on the IP Address and clicking the Delete button.

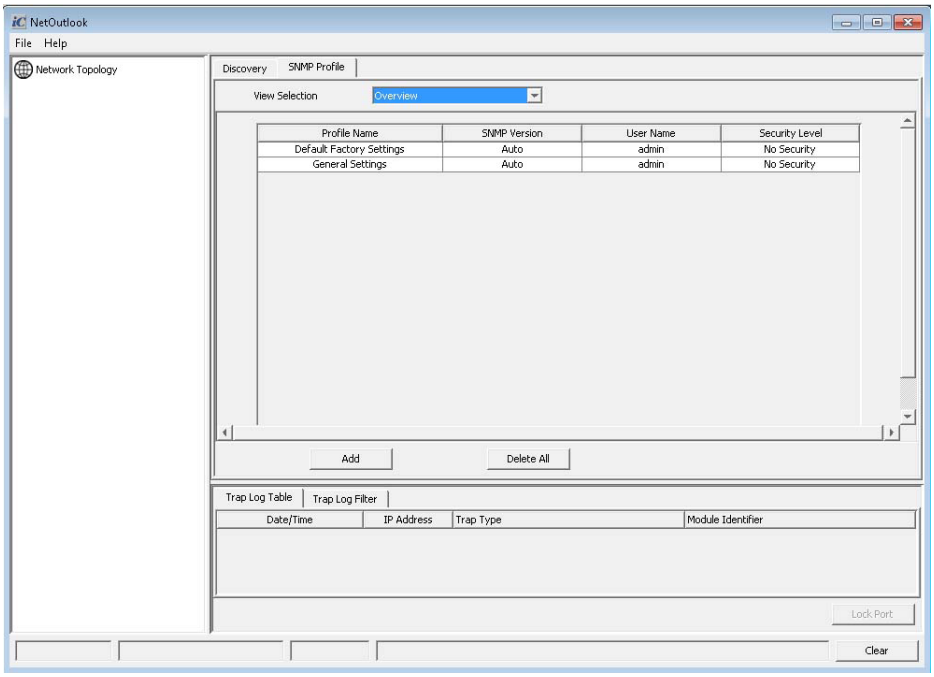
To delete all IP addresses in the IP Address Range List, click the ***Delete All*** button.



IP Address Range Tab - IP Address Range List

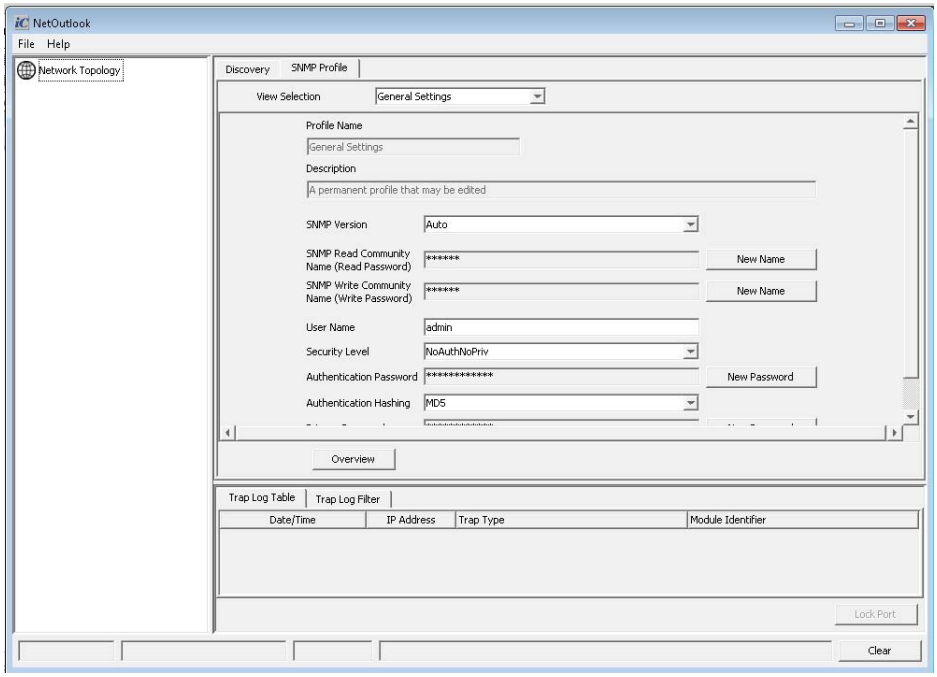
3.2.2 Configuring SNMP Profiles

An unique SNMP profile may be assigned for each IP address. The default profiles can be selected or new profiles can be created.



SNMP Profile Tab

To edit an existing profile, double-click on the entry located under the SNMP Profile List and use the pull-down menus and text boxes to change the desired parameters. The Default Factory Setting can not be changed.



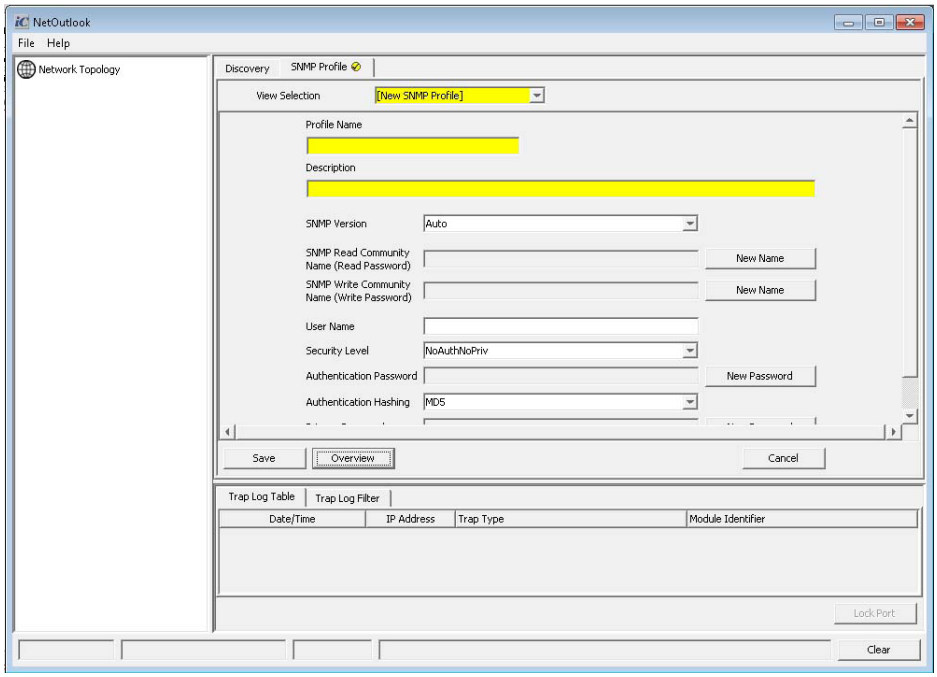
SNMP Profile Tab - Edit Existing Profiles

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

To create a new profile, click on the ***Add*** button.

NOTE: By creating a new SNMP profile, the module associated with the IP address must have the same SNMP parameters programmed or the module will not be accessible (see Section 5.6.3.4).

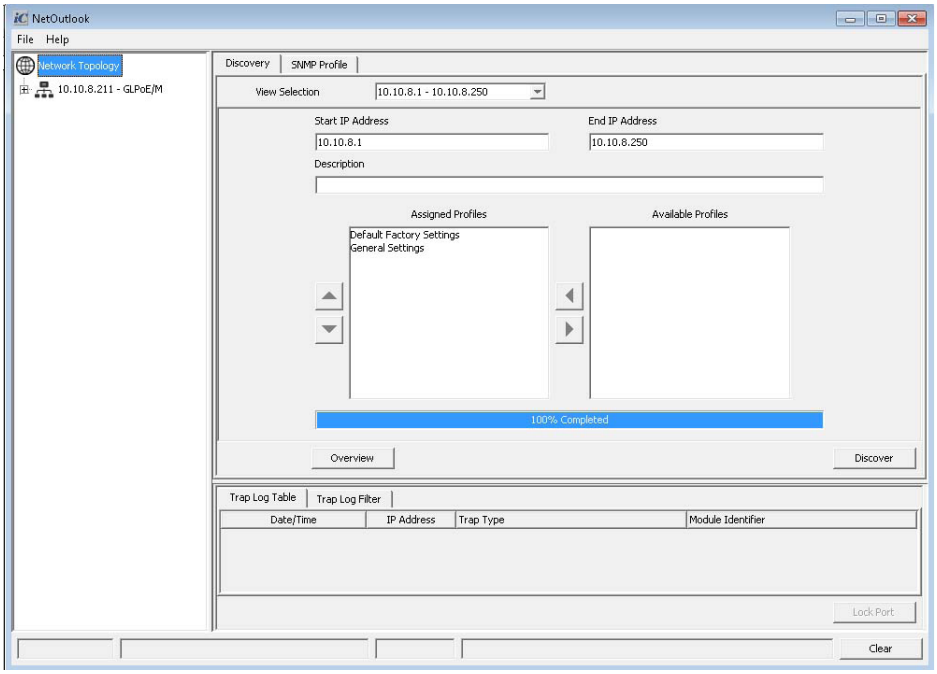
Use the pull-down menus and text boxes to change the SNMP version, SNMP Read/Write Community Names, SNMP v3 User Name, security level, authentication and privacy passwords.



SNMP Profile Tab - Adding a New Profile

Click the ***Save*** button to save the changes to the profile. The new profile will be displayed under the Discovery tab under the Available Profiles window..

To discover the modules associated with the IP addresses in the IP Address Range list, click the ***Discover*** button.

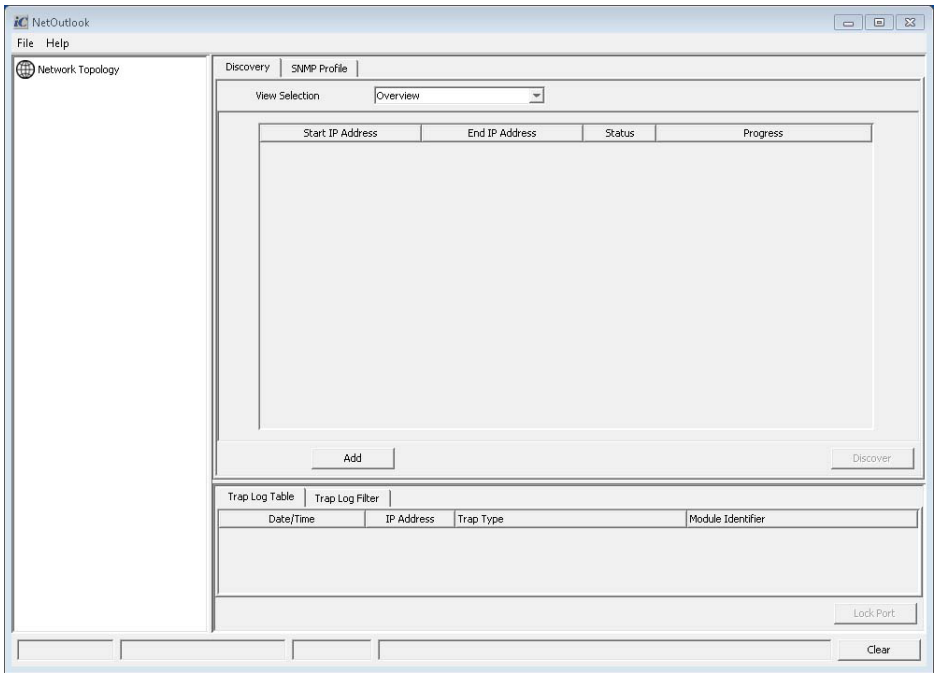


IP Address Range Tab - Discover IP Addresses

The discovered IP addresses are displayed under the Network Topology window.

3.3 Trap Log

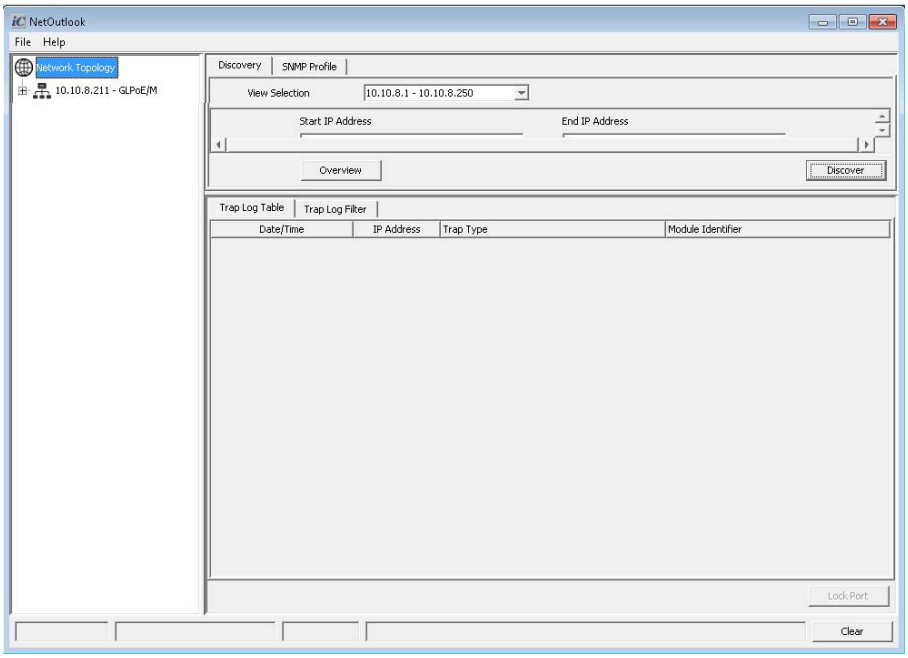
The trap log is located on the lower right of the NetOutlook window.



Trap Log Table Tab

Traps are status change events that occur during the operation of a network that may require special attention from the network administrator. NetOutlook can be configured to monitor and log the presence of various types of SNMP traps.

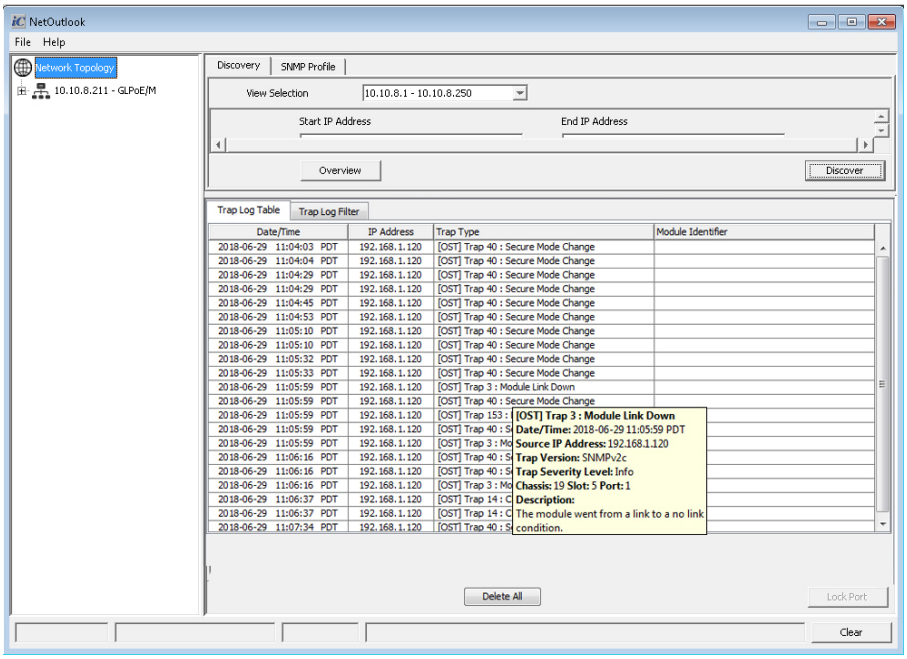
You can stretch the trap window by hovering the mouse pointer over the top of the window and pulling it up.



Trap Log Table - Expanded

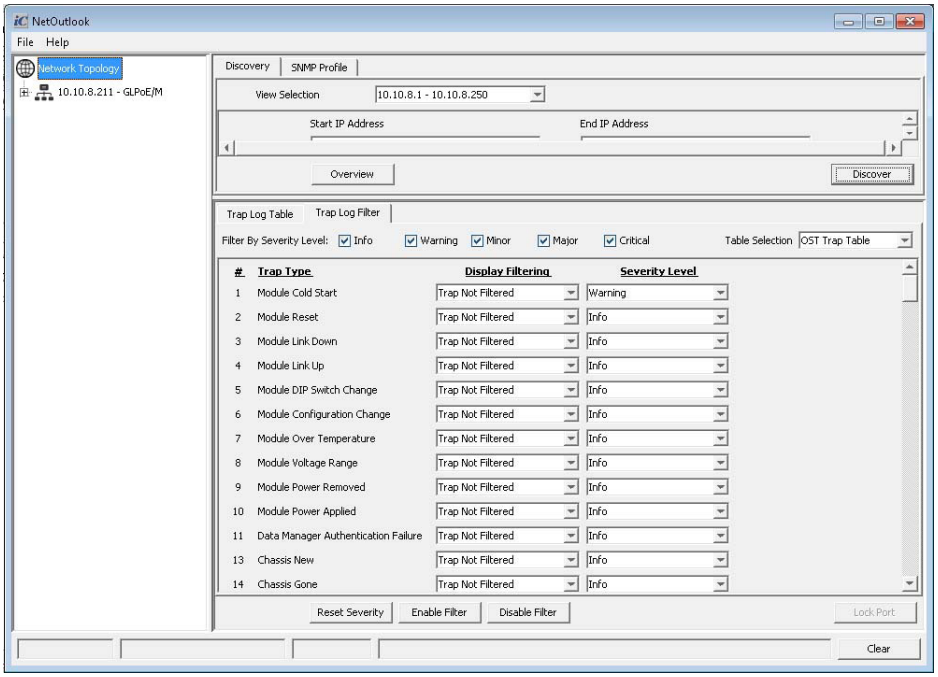
Traps are displayed under the Trap Log Table tab. The traps are displayed by date/time, IP address, trap type and module identifier.

Using the mouse, hovering over an entry in the Trap Type column. A dialog box will appear with additional information about the trap.



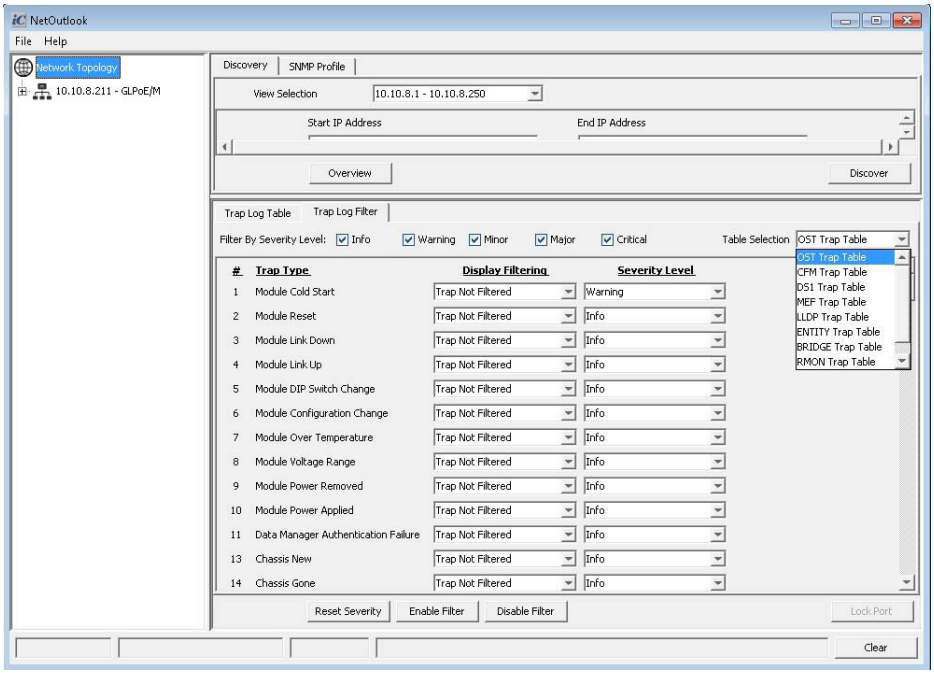
Trap Log Table - Details

Under the Trap Log Filter tab, individual SNMP traps can be enabled or disabled and the priority level of the trap can be modified. By default, all traps are enabled (traps not filtered) with a priority level of "Information".



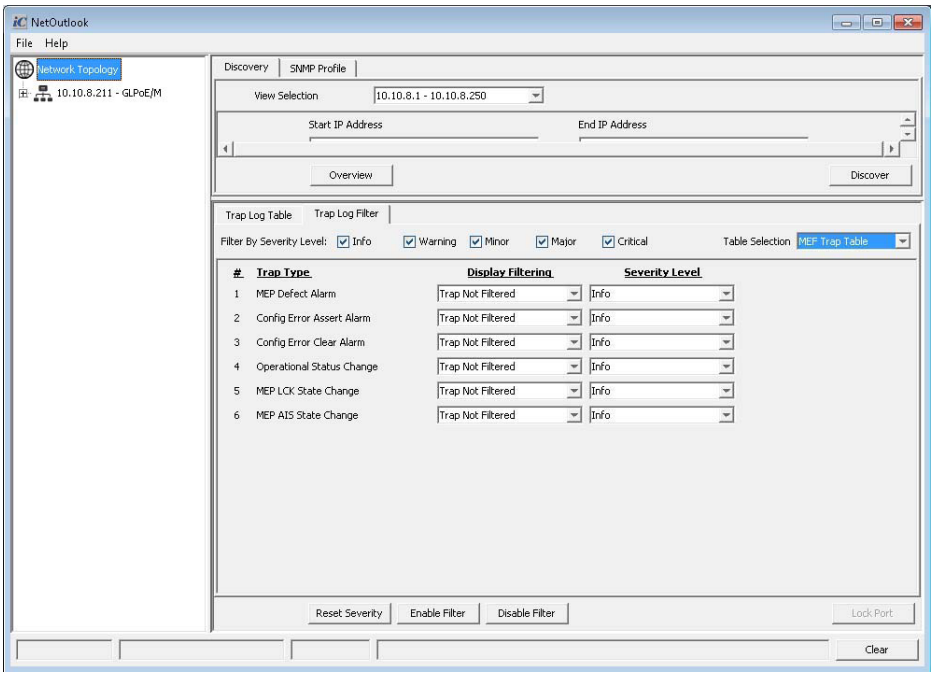
Trap Log Filter Tab

Approximately 160 trap types are displayed under the Trap Log Filter tab. To assist in locating a specific type of trap, use the Table Selection pull-down menu to display the available trap categories.



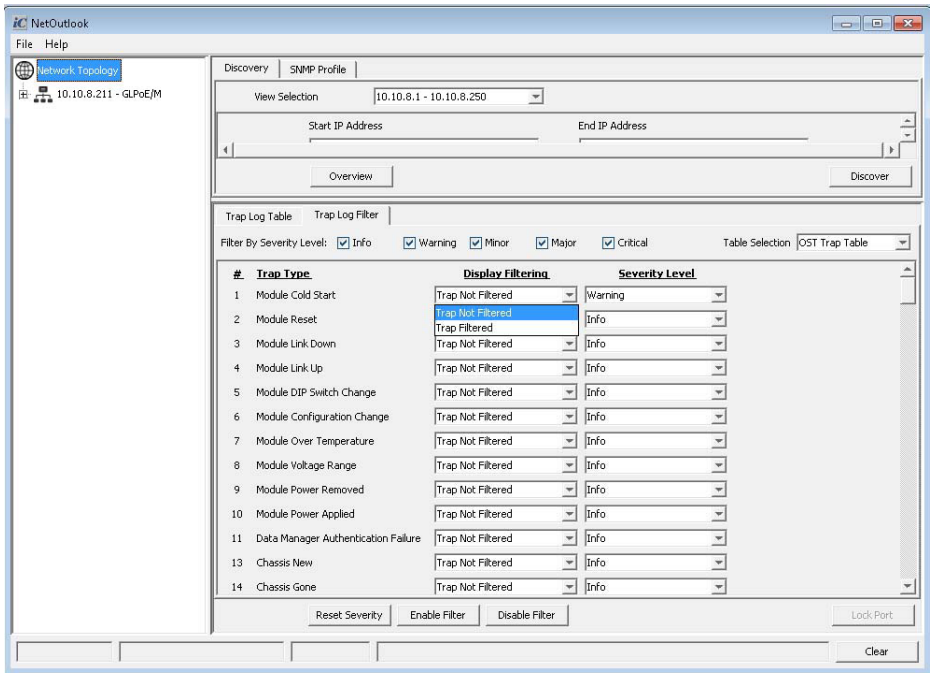
Trap Log Filtering - Table Selection

Once a category is selected, only the traps for that category will be displayed.



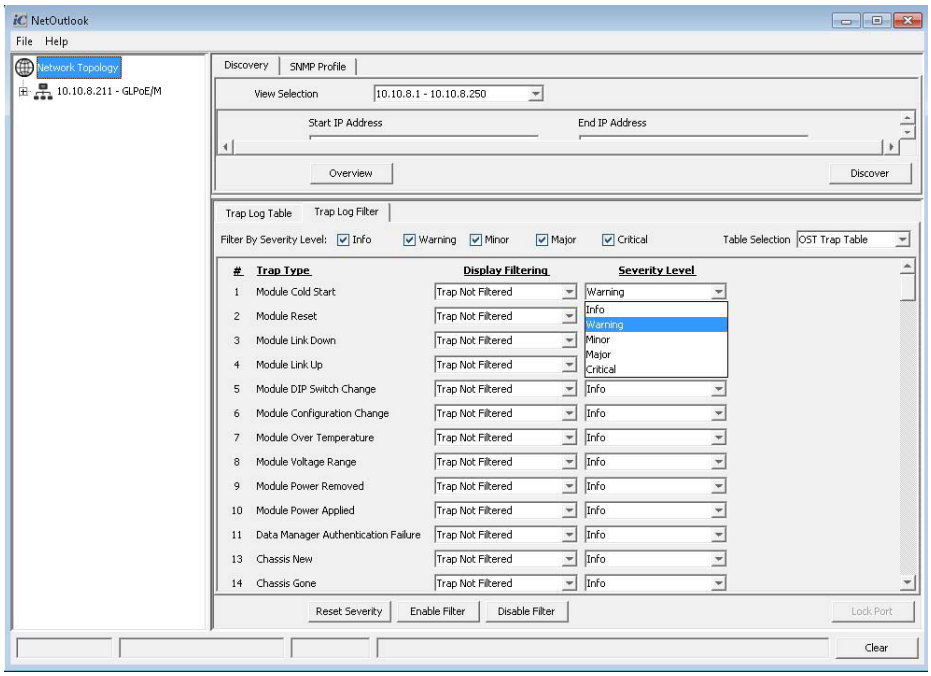
Trap Log Filtering - Traps by Catalogue

To disable a trap (Trap Filtered), use the Display Filtering pull-down menu associated with the desired trap and select the Traps Filtered selection.



Trap Log Filtering - Enable/Disable Traps

To change the severity level of a trap, use the Severity Level pull-down menu associated with the desired trap and select Info, Warning, Minor, Major or Critical. Click the ***Save*** button to save the changes.



Trap Log Filtering -Severity Level

Click the ***Enable Filter*** button to enable the filter on all traps. Click the ***Disable Filter*** button to disable the filter on all traps. Click the ***Reset Severity*** button to default all traps to the Info severity level.

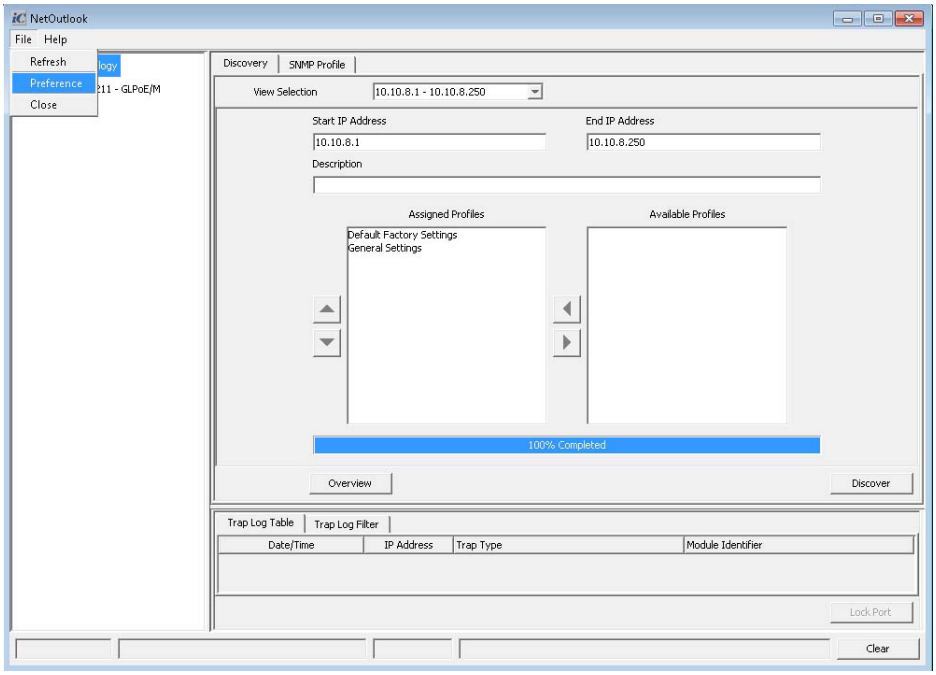
The SNMP port can be locked so other applications cannot use the port. Click on the ***Lock Port*** button in the button right corner to lock the port.

The traps can also be filtered by severity level. By default, all severity levels is displayed under the Trap Log tab. To change the displayed severity level, uncheck the desired severity level.

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

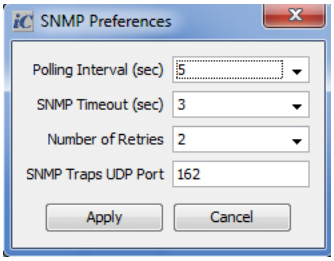
3.4 NetOutlook Preferences

The SNMP Preferences dialog box is used to set the parameters for communication between NetOutlook and the Ethernet devices. To access the SNMP Preference dialog box, click on the ***File*** button located in the top left corner of the screen.



NetOutlook screen - SNMP Preferences

To access the SNMP Preferences, click on ***Preferences***.



NetOutlook Preferences Dialog Box

Polling Interval (measured in seconds)

Configures the frequency at which NetOutlook retrieves SNMP data from the discovered Ethernet devices. The default value is 3 seconds. Use the Polling Interval pull-down menu to select a new value.

SNMP Timeout (sec)

Configures the maximum time allowed for a response from a chassis before initiating a retry. The default value is 3 seconds. Use the SNMP Timeout pull-down menu to select a new value.

Number of Retries

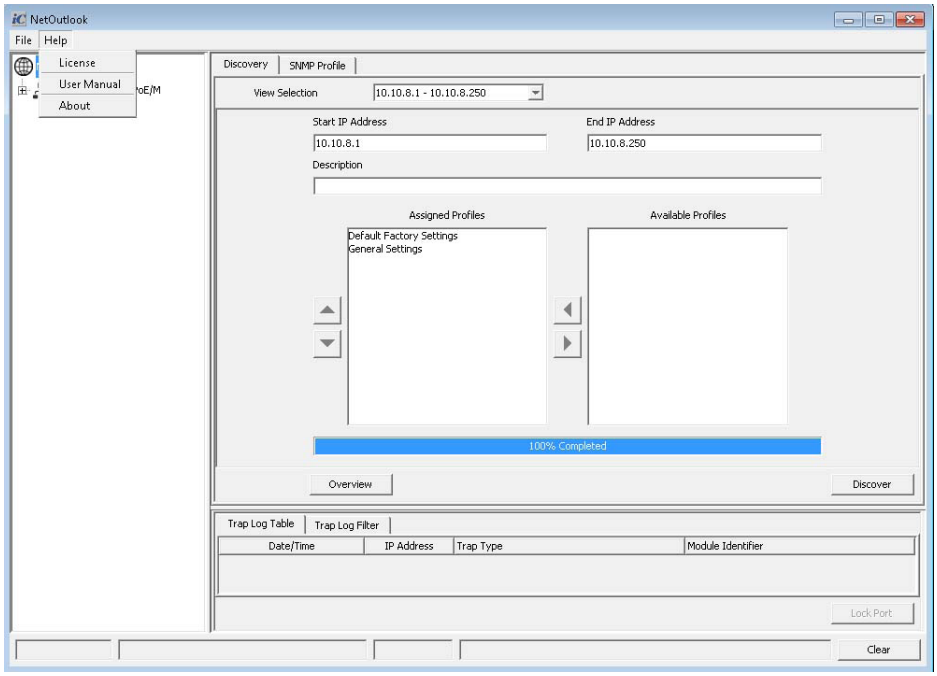
Configures the maximum number of polling retry attempts following an SNMP Time-out before generating an error. The default value is 2 retries. Use the Number of Retries pull-down menu to select a new value.

SNMP Traps UDP Port

Configures the port number used to send SNMP trap alarms. Enter a new value in the text box.

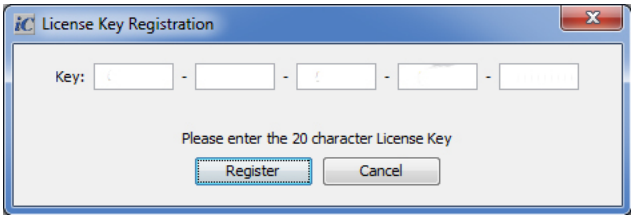
3.5 NetOutlook Help

The NetOutlook Help provides access to the License Key , a link to the User Manual and the version of the software. To access the NetOutlook Help dialog box, click on the ***Help*** button located in the top left corner of the screen.



NetOutlook screen - Help

Click on the ***Licence*** to view the key.



Licence Key

Click on the ***User Manual*** to view the online

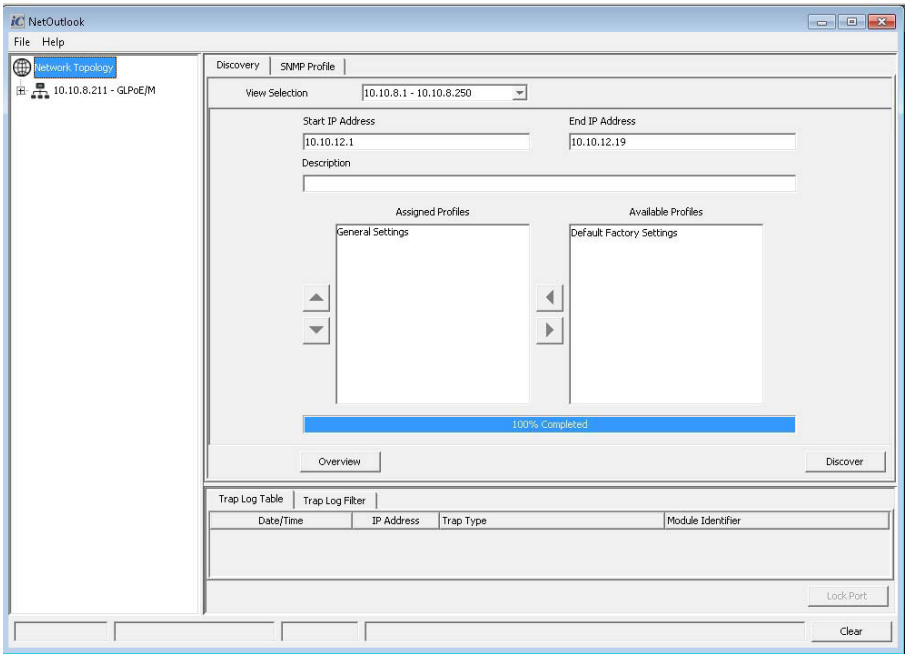
Click on ***About*** to view the version of NetOutlook.

About NetOutlook

4.0 NETWORK TOPOLOGY

4.1 Network Topology Tree

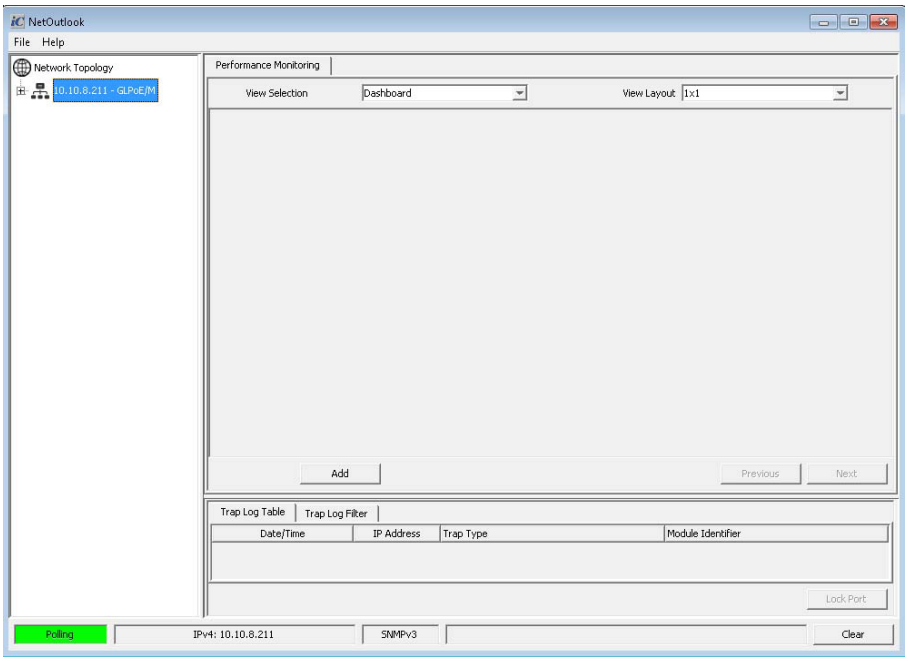
The Network Topology tree displays the list of IP addresses that have been discovered. The IP addresses are displayed under the Network Topology icon.



Network Topology

4.1.1 Performance Monitoring

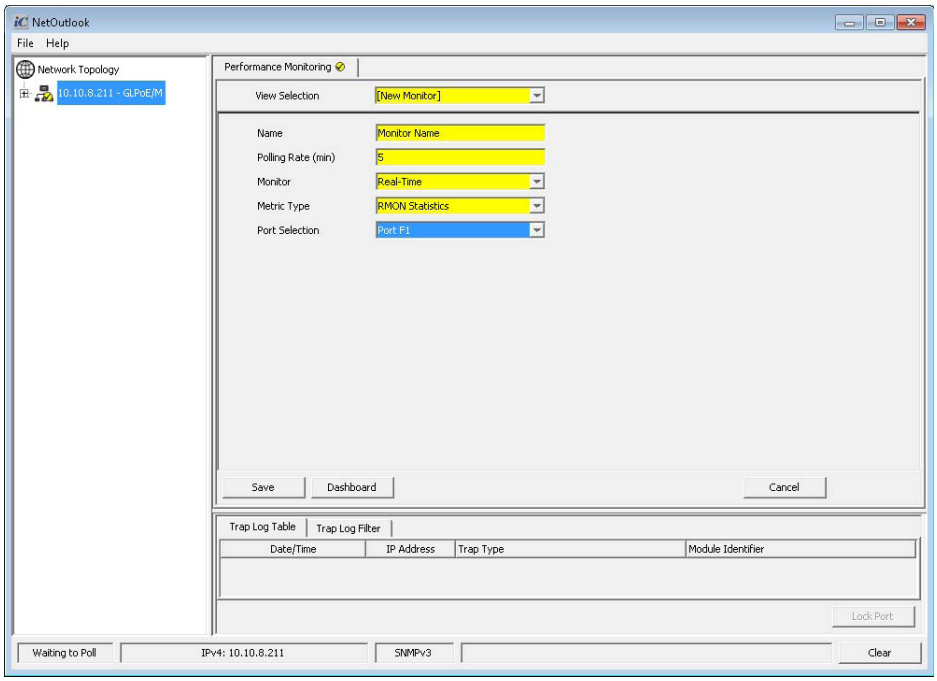
From the IP addressing list, access Performance Monitoring by clicking on the IP Address displayed in the Network Topology. The OmniConverter and RuggedNet SPE switches support Real-time monitoring of RMON statistics.



Performance Monitoring Screen

Across the top of the Performance Monitoring screen are two pull-down menus; View Selection and View Layout. The View Selection pull-down will allow the selection of the Performance Monitoring dashboard and any created profiles. The View Layout pull-down selects the size of the graphical display of the data (1x1, 2x2 or 3x3).

The Dashboard allows the user to create and delete Performance Monitoring profiles. To create a Performance Monitoring profile, click the ***Add*** button.



Performance Monitoring - Add Screen

Most of the text boxes have the factory default settings displayed. By hovering over the text box, a range of values that can be configured will be displayed.

Name

In the text box, create a new for the profile. The profile name will be able to be selected from the View Selection pull-down menu.

Polling Rate (min)

In the text box, enter the desired polling rate from 0 to 60 minutes. 0 minutes disables the polling.

Monitor

The Monitor Type available is Real-Time.

Real-Time supports RMON Statistics.

Metric Type

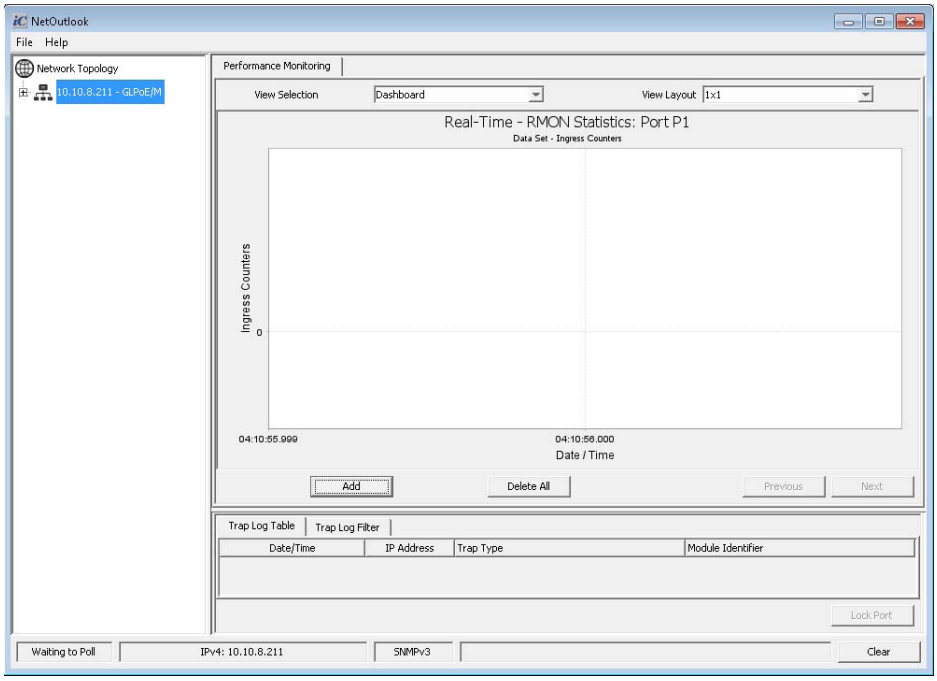
The Metric Type available is RMON Statistics.

Port Selection

Use the pull-down menu to select the port to be monitored.

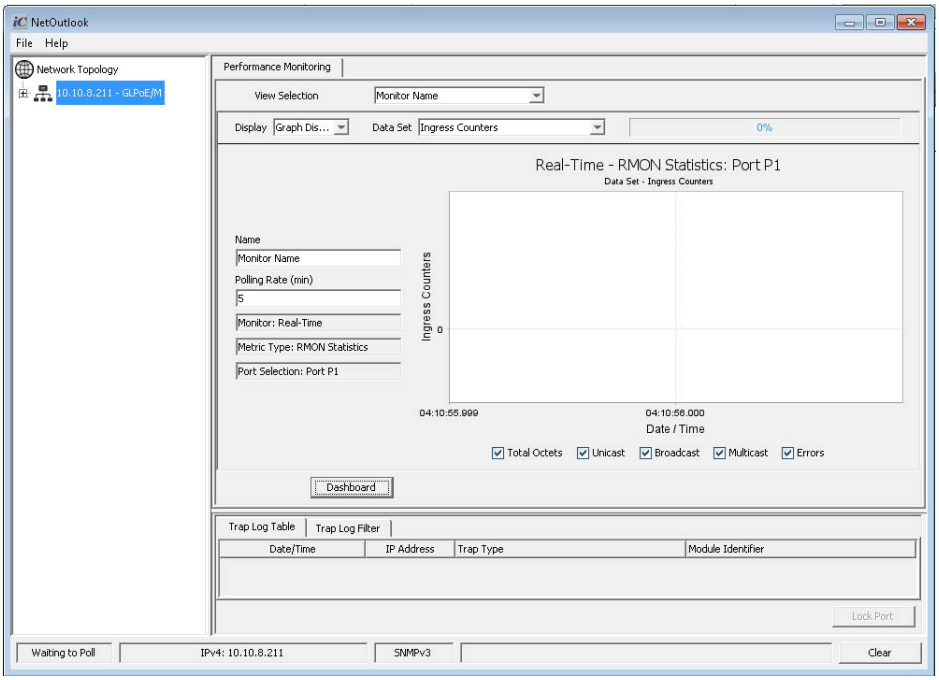
Click the ***Save*** button to save the profile.

4.1.1.1 Real-Time RMON Statistics



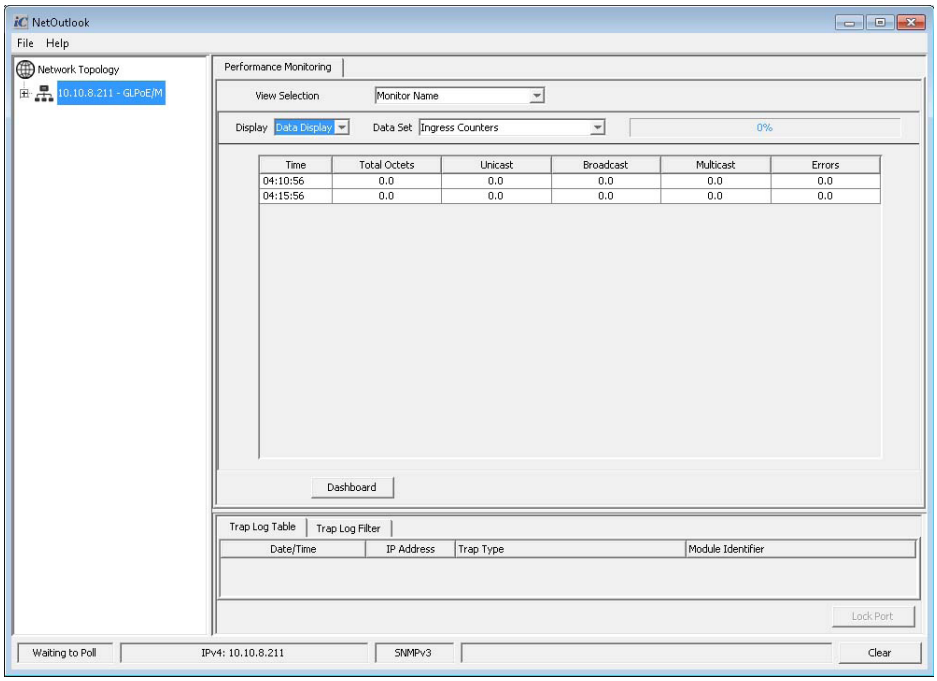
RMON Statistics

By double-clicking the graph and detailed screen will be displayed.



RMON Statistics - Detailed

The Display pull-down menu selects a graphical (Graph Display) or data (Data Display) display. Use the Display pull-down menu and select Data Display.



RMON Statistics - Detailed

The Data Set pull-down menu selects which counters are collected and displayed. The Data Set can be Ingress Counters, Ingress Frame Counters or Egress Counters.

Click the ***Dashboard*** button or select Dashboard for the View Selection pull-down to return to the Dashboard.

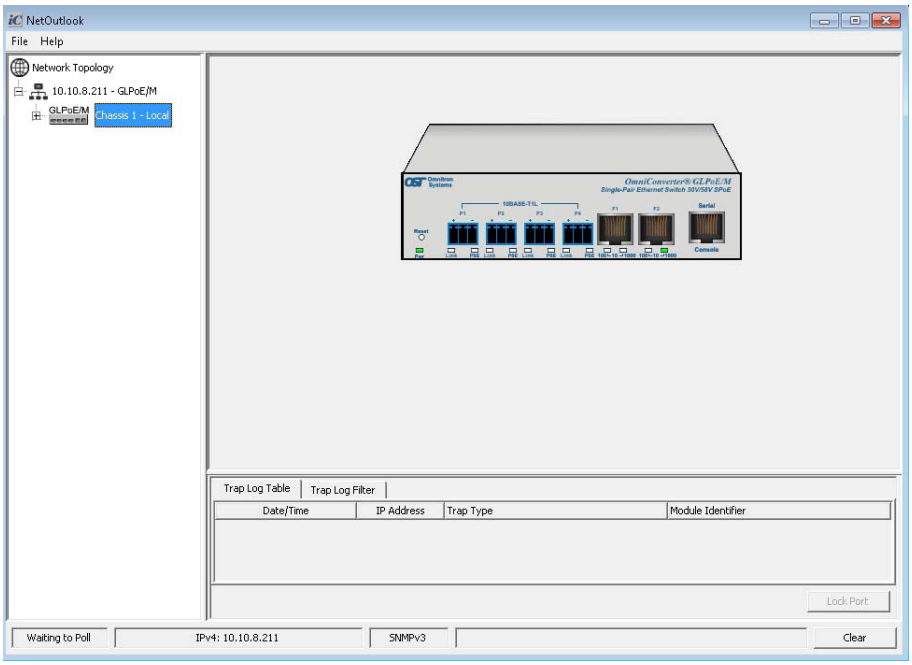
Use the Data Set pull-down to display Octets, Throughput or Utilization data.

Use the Display pull-down menu and select Data Display.

Click the ***Dashboard*** button or select Dashboard for the View Selection pull-down to return to the Dashboard.

4.1.2 Expanding the Network Tree

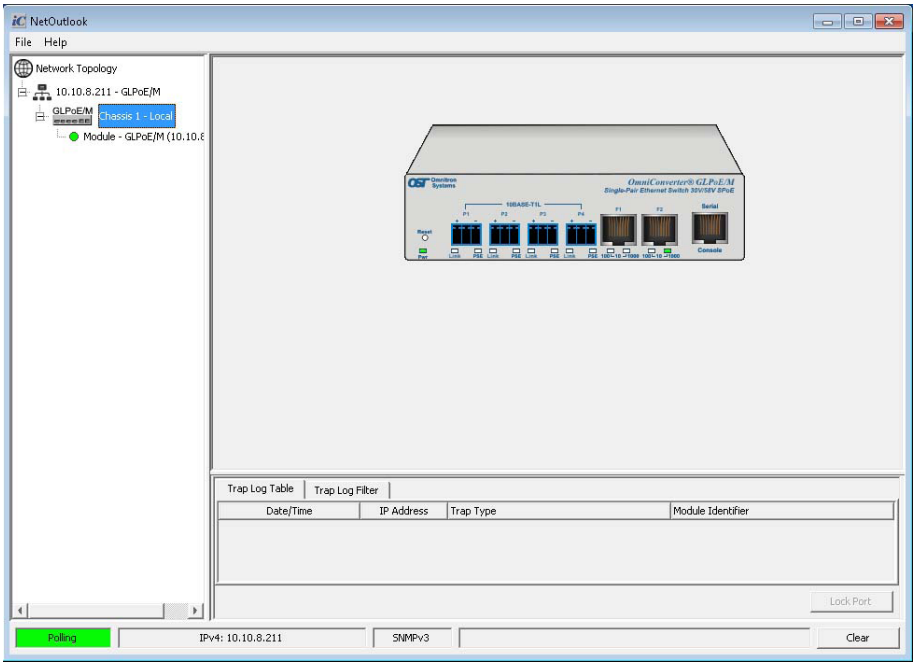
Clicking on the chassis icon under the IP address will display a graphical view of the chassis and all modules installed in the chassis.



Network Topology - Chassis View

NOTE: All chassis and standalone modules are referred to as Chassis.

Clicking on the + sign next to the chassis icon will display all modules installed in the chassis.



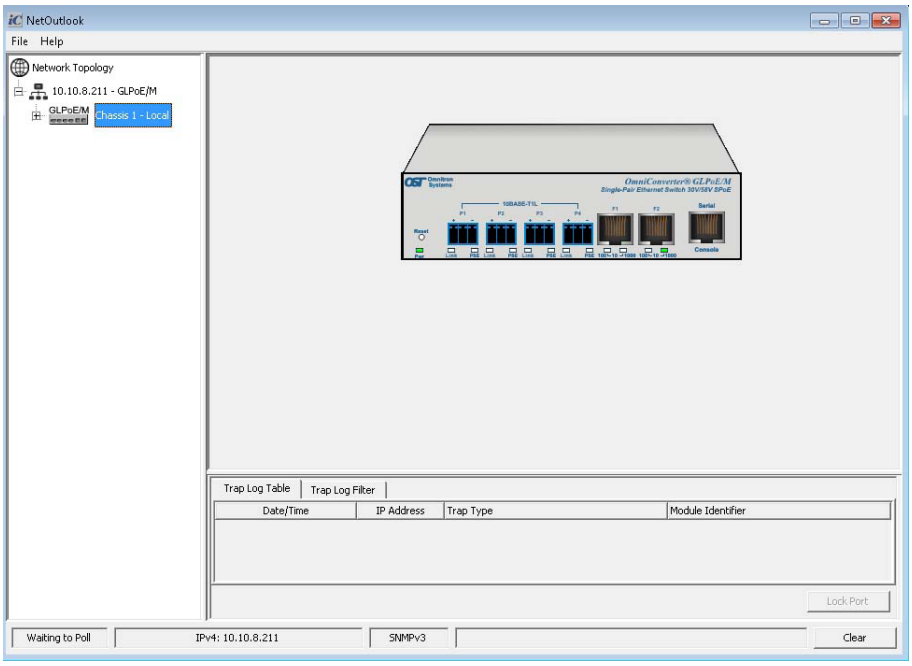
Network Topology - Chassis View Expanded

5.0 MODULE CONFIGURATION

NetOutlook uses a combination of graphical views and tabular screens to configure and monitor the modules and power supplies installed in the chassis. Each module, based on the complexity of the module, will support different tabular options. Each tabular screen is presented in the following sections to provide information on that screen. The tabular screens shown are not from any particular module but from different modules in order to show all the available options.

5.1 Chassis Views

The Chassis View provide a graphic representation of the OmniConverter and RuggedNet switches. From the Chassis View, module information can be viewed and monitored.



Network Topology

5.3 OmniConverter and RuggedNet SPE Ethernet Switches

Module options can be accessed by clicking on the image of the module displayed in the chassis view screen or expanding the chassis selection by clicking on the + sign next to the chassis and clicking on the entry under the expanded chassis.

A tabular screen representing the module will be displayed. The following tables indicate what tabs are available for each module type. Locate the module in the tables below to see the available options. Refer to the section listed in the table for more information on the available options.

Managed Modules											
Module	Model	Device Tab									
		System	Interface	Physical	DIP Switches	PoE	PoE Scheduler	I/O Pins	Port Statistics	SFP Info	Advanced
		Section 5.6.1.1	Section 5.6.1.2	Section 5.6.1.3	Section 5.6.1.4	Section 5.6.1.5	Section 5.6.1.6	Section 5.6.1.7	Section 5.6.1.8	Section 5.6.1.9	Section 5.6.1.10
GL/M	282x	X	X	X	X	-	-	-	X	X	X
GLPoE/M	952x	X	X	X	X	X	X	-	X	X	X
G/LMi	284x	X	X	X	X	-	-	X	X	X	X
GLPoE/Mi	954x	X	X	X	X	X	X	X	X	X	X
		Management Tab									
		IP Address	IPv6 Address	Protocol	SNMP	User Infor	SSH	Time & Date	Modbus TCP	Advanced	
		Section 5.6.2.1	Section 5.6.2.2	Section 5.6.2.3	Section 5.6.2.4	Section 5.6.2.5	Section 5.6.2.6	Section 5.6.2.7	Section 5.6.2.8	Section 5.6.2.9	
GL/M	282x	X	X	X	X	X	X	X	X	X	
GLPoE/M	952x	X	X	X	X	X	X	X	X	X	
GL/Mi	284x	X	X	X	X	X	X	X	X	X	
GLPoE/Mi	954x	X	X	X	X	X	X	X	X	X	
		Service Activation Tab						Service Protection Tab			
		VLAN	CoS/ QoS	Rate Limiting	LLDP	IGMP	MLD	Link Redundancy	Spanning Tree	MRP	LAG/ LACP
		Section 5.6.3.1	Section 5.6.3.2	Section 5.6.3.3	Section 5.6.3.4	Section 5.6.3.5	Section 5.6.3.6	Section 5.6.4.1	Section 5.6.4.2	Section 5.6.4.3	Section 5.6.4.4
GL/M	282x	X	X	X	X	X	X	X	X	X	X
GLPoE/M	952x	X	X	X	X	X	X	X	X	X	X
GL/Mi	284x	X	X	X	X	X	X	X	X	X	X
GLPoE/Mi	954x	X	X	X	X	X	X	X	X	X	X
		Security		Advanced Tab							
		ACL	AAA	SNMP Traps	Syslog	SMTP	Splash Screen				
		Section 5.6.6.1	Section 5.6.6.2	Section 5.6.7.1	Section 5.6.7.2	Section 5.6.7.3	Section 5.6.7.4				
GL/M	282x	X	X	X	X	X	X				
GLPoE/M	952x	X	X	X	X	X	X				
GL/Mi	284x	X	X	X	X	X	X				
GLPoE/Mi	954x	X	X	X	X	X	X				

5.6 Tabular Options

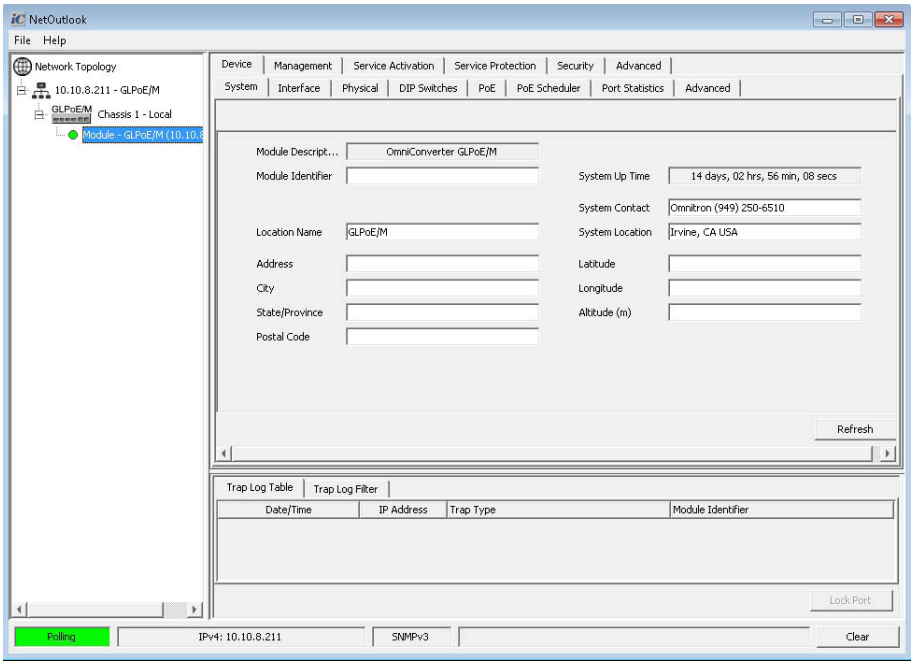
The tabular screens shown in the following sections are not from any particular module. Locate the module in the tables from Sections 5.2, 5.3, 5.4 and 5.5 to see the available options. Refer to the section listed in the tables for more information on the available options.

All module tabular screens will be displayed in this section to provide information on all options available for OmniConverter and RuggedNet SPE switches.

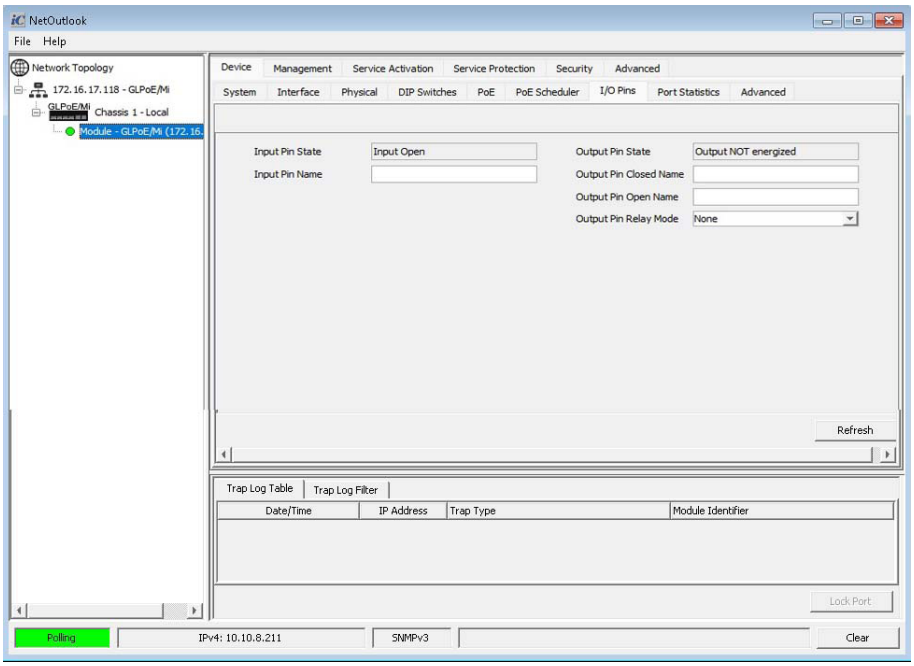
5.6.1 Device Tab

The Device tab provides a second row of tabular options to configure and display information on the specific module type.

The order of tabs described in this section are: System, Interface, Physical, DIP-switches, PoE, PoE Scheduler, Port Statistics, SFP Info, and Advanced.



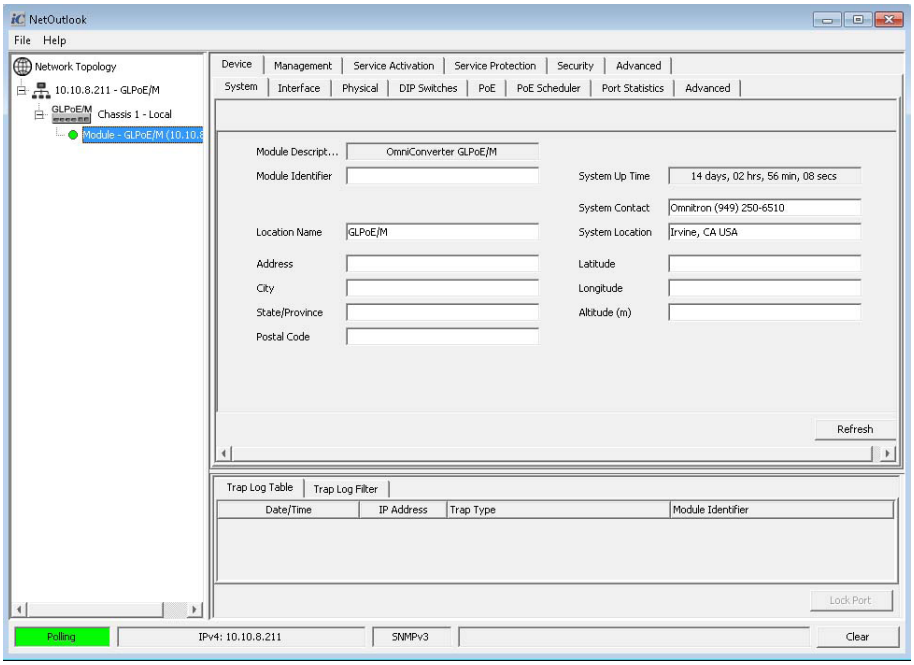
Device Tab - OmniConverter



Device Tab - RuggedNet

5.6.1.1 System Tab

The System tab displays the Module Description, Module Identifier, System Time, System Up Time, Chassis Number, Chassis Name, System Contact and System Location. Module physical location, Latitude, Longitude and Altitude is also displayed and can be modified. Tab options will vary depending on the module type.



System Tab

Module Description

The name of the module is displayed.

Module Identifier

A module identifier can be configured for the module. The Module Identifier is displays as one of the identifiers when a SNMP trap is generated. Enter a name in the text box.

Location Name

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

Address/City/State/Province/Postal Code

The address/city/state/province/postal code of the module can be configured. Enter the information in the text boxes.

System Up Time

The system up time is displayed

System Contact/System Location

A system contact and location can be configured. Enter the information in the text boxes.

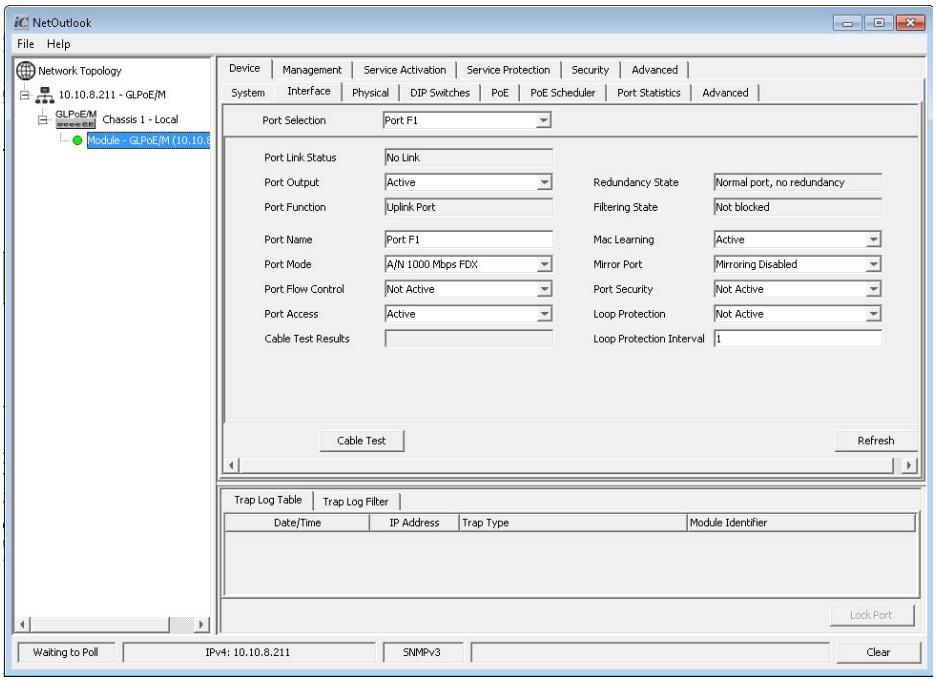
Latitude/Longitude/Altitude

The latitude, longitude and altitude for the chassis or module can be configured. Enter the information in the text boxes.

To save the changes, click on the ***Apply*** button.

5.6.1.2 Interface Tab

The Interface tab displays port link status, the administrative status, the operational status and port specific information of the port selected by the Port Selection pull-down menu. Tab options will vary depending on the module type.



Interface Tab

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

Port Link Status

Displays the link status of the selected port number. The link status will indicate the port speed and duplex mode.

Port Output

The output can be enabled (active) or disabled (not active) using the Port Output pull-down menu.

Port Function

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

Port Name

Port Name allows each port to be configured with a unique name. Enter the name of the port in the text box.

Port Mode

Use the Port Mode pull-down menu to change the speed and negotiation state of the selected port.

Port Flow Control

Use the Port Flow Control pull-down menu to enable (active) or disable (not active) flow control on the selected port.

Port Access

Use the Port Access pull-down menu to enable (active) or disable (not active) port access on the selected port. When disabled on a RJ-45 port, the connected PD will remain powered but data access is disabled.

Cable Test Results

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

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

Redundancy State

Displays the state of Link Redundancy.

Filtering State

Displays the state of the redundancy status of the port. The redundancy status is based on the redundancy protocol enabled on the port (Link Redundancy, RSTP, MRP, etc.).

MAC Learning

Use the MAC Learning pull-down menu to enable (active) or disable (not active) MAC learning on the port.

Mirror Port

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

Port Security

Use the Port Security pull-down menu to enable (active) or disable (not active) dropping of unknown multicast and unicast traffic.

Loop Protection

Use the Loop Protection pull-down menu to enable (active) or disable (not active) loop protection on the module.

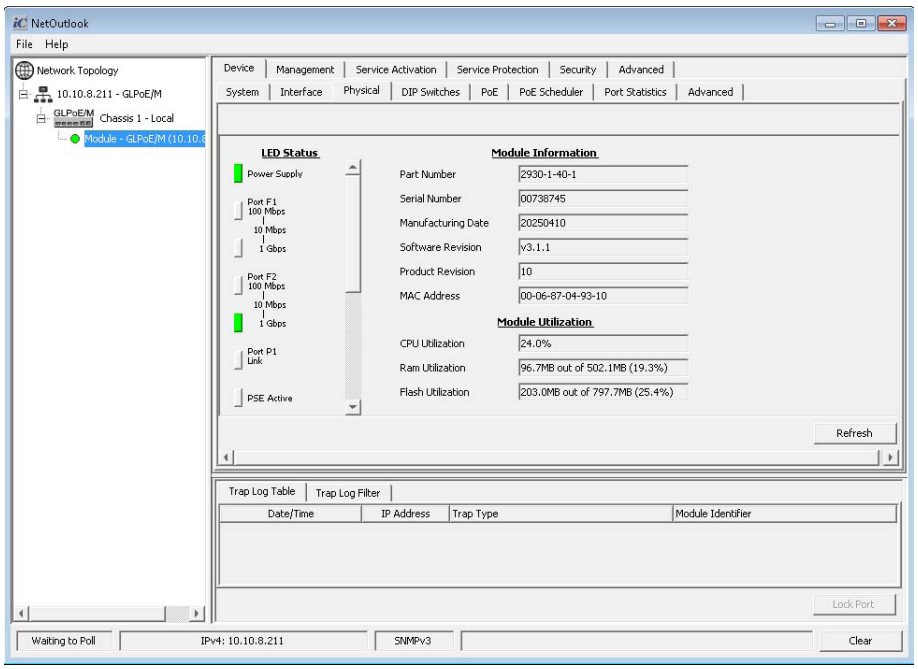
Loop Protection Interval

Enter the loop protection interval in the text box. The loop protection transmit interval can be set to 1-60 seconds.

To save the changes, click on the ***Apply*** button.

5.6.1.3 Physical Tab

The Physical tab displays the part and serial numbers, manufacturing date, software product revisions, CPU and memory utilization as well as the state of the LEDs. A green LED indicates the port is linked or the power has been applied.



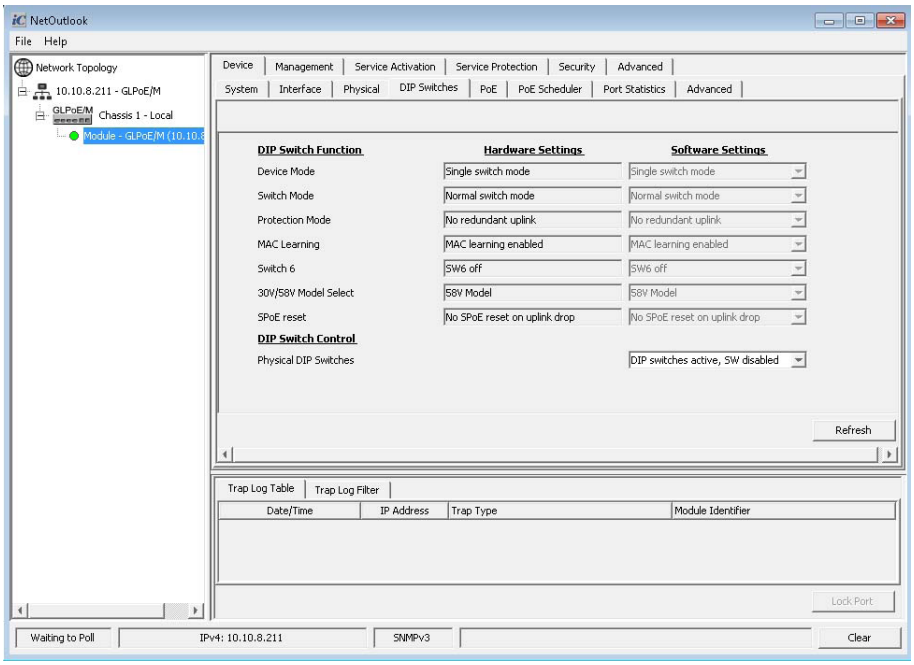
Physical Tab

5.6.1.4 DIP Switches Tab

The DIP Switches tab displays the DIP-switches that are available on the module. It displays the Hardware (physical DIP-switch setting) and Software (changed through NOL or command line) settings and provides a pull-down menu to change the setting. Tab options will vary depending on the module type.

See Appendix B for more information on the DIP-switches.

To save the changes, click on the ***Apply*** button.



DIP-Switches Tab

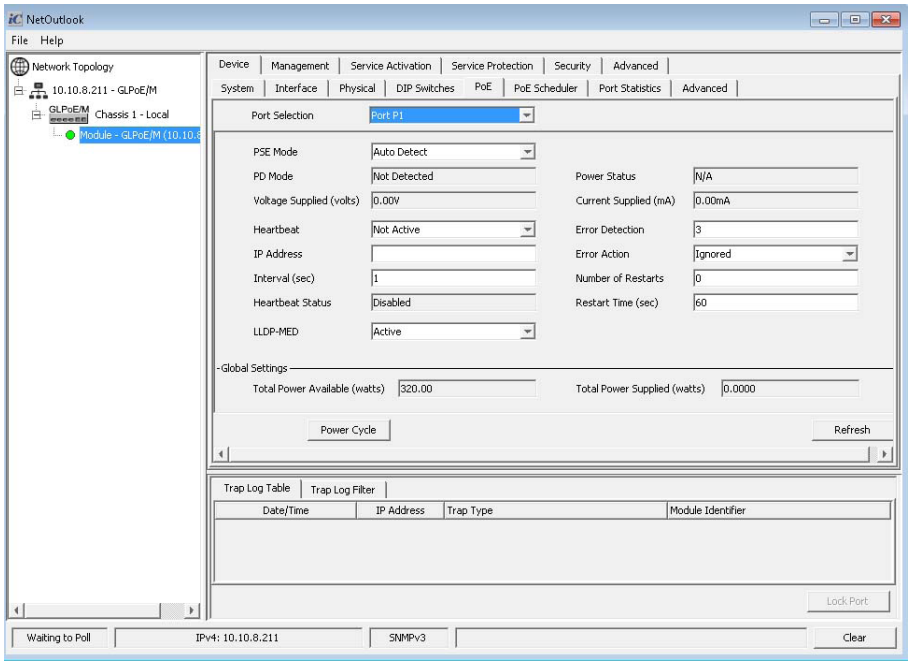
To change the DIP-switch settings on the OmniConverter and RuggedNet modules, use the Physical DIP Switches pull-down menu and select the DIP-switches disabled, software override active option.

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

Once the setting has been changed to DIP-switches disabled, software override active, the Software Settings switch DIP-switch can be modified by using the pull-down menu next to next selection.

5.6.1.5 PoE Tab

The PoE tab provides the ability to configure/display PoE related options on the module.



PoE Tab

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

PSE Mode

Use the PSE Port pull-down menu to enable auto detect or disable PoE on the selected port.

PD Mode

Displays the PD type detected by the module.

Voltage Supplied (volts)

Displays the amount of voltage supplied to the PD.

Heartbeat

Use the Heartbeat pull-down menu to enable (active) or disable (not active) the generation of a heartbeat. A heartbeat is generated to the configured IP address of the attached PD. When three consecutive heartbeats are not received, the PD will be restarted (power will be cycled Off and On).

IP Address

Configures the IP address of the PD. The IP address of the PD is used for the heartbeat signal. Enter the IP address in the text box.

Interval (sec)

Configures the transmission interval of the heartbeat signal. The default value is 1 second. Valid values are 1 to 300 seconds. Enter a new value in the text box.

Heartbeat Status

Displays the heartbeat status. Valid entries are Available, Error and Disabled.

LLDP-MED

Use the LLDP-MED pull-down menu to enable (active) or disable (not active) LLDP-MED support for PoE PDs.

Power Status

Displays the status of the PoE power. The status can indicate N/A, Normal, Over Current, Brownout or Insufficient Power.

N/A	Indicates the port is not connected to a PD.
Normal	Indicates the module is providing the proper power to the PD.
Over Current	Indicates the PD is consuming more power than the negotiated value.
Brownout	Indicates the available power is insufficient to fulfill the requested PD power load.
Insufficient Power	Indicates the requested power is less than the capability of the power supply.

Current Supplied (mA)

Displays the amount of current supplied to the PD.

Error Detection

Configures the number of consecutive lost heartbeats before an error condition is declared. The default value is 3 lost heartbeat signals.

Error Action

Configures what action will be taken when a heartbeat error condition is detected. Use the Error Action pull-down menu to select ignore, restart or shutdown.

Ignore	Indicates the error condition will be ignored. Ignore is the default setting.
Restart	Indicates the power to the selected port (PD) will be cycled Off and On.
Shutdown	Indicates the power to the selected port (PD) will be turned Off.

Number of Restarts

Configures the number of times a PD is restarted when the Error Action is set to restart. The default value is 0 indicating no limit to the number of restarts.

Restart Time (sec)

Use the 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 Restart Time delays the start of the heartbeat signal after a reset condition.

Global Settings

Total Power Available (watts)

Displays the total amount of power available to all PoE ports on the module.

Total Power Supplied (watts)

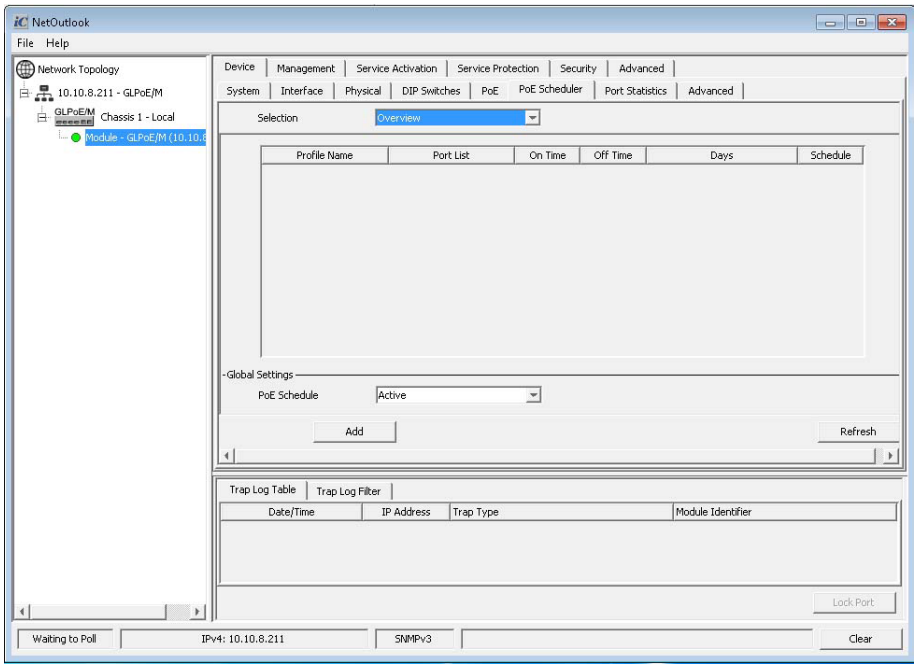
Displays the total amount of power suppled to all PoE ports on the module.

Click the ***Power Cycle*** button to cycle the power to the attached PD.

To save the changes, click on the ***Apply*** button.

5.6.1.6 PoE Scheduler Tab

The PoE Scheduler tab provides the ability to configure the time of day for PoE power to be turned On and Off. Multiple On/Off times can be configured for a single day.

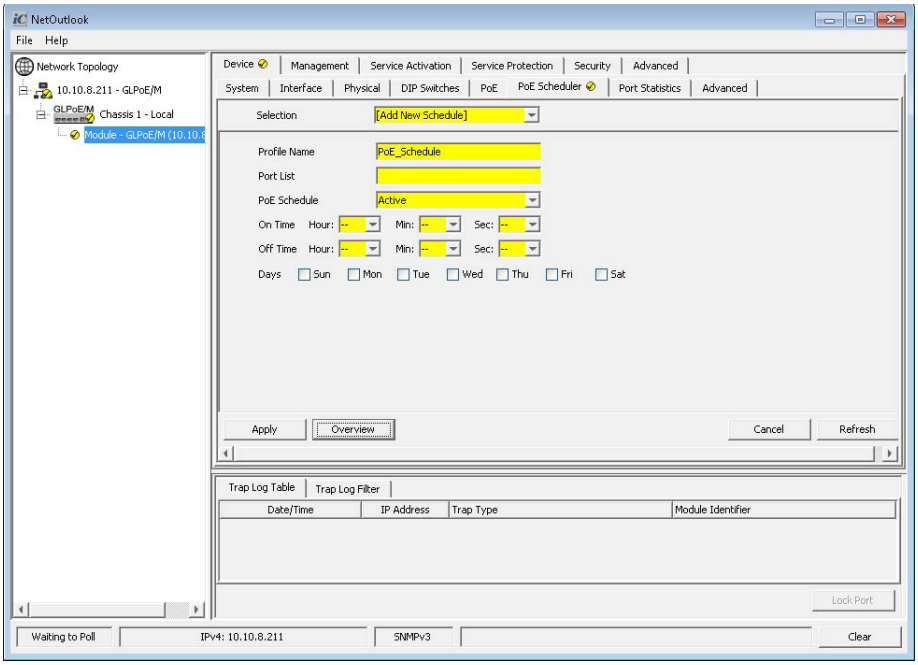


PoE Scheduler Tab

Global Settings

Use the PoE Schedule pull-down menu to globally enable (active) or disable (not active) PoE Scheduler on the module.

To configure a scheduling profile, click the ***Add*** button.



PoE Scheduler Tab - Add Scheduling Profile

Profile Name

Enter the name of the scheduling profile in the text box.

Port List

Enter the port number for the scheduling profile in the text box.

Port Schedule

PoE power on each scheduling profile can be enabled (active) or disabled (not active). Use the PSE Schedule pull-down menu to enabled (active) or disabled (not active) the scheduling profile.

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 time when the power is turned On.

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 time when the power is turned Off.

Days

Check the boxes for each day associated with the scheduling profile.

To save the changes, click on the ***Apply*** button.

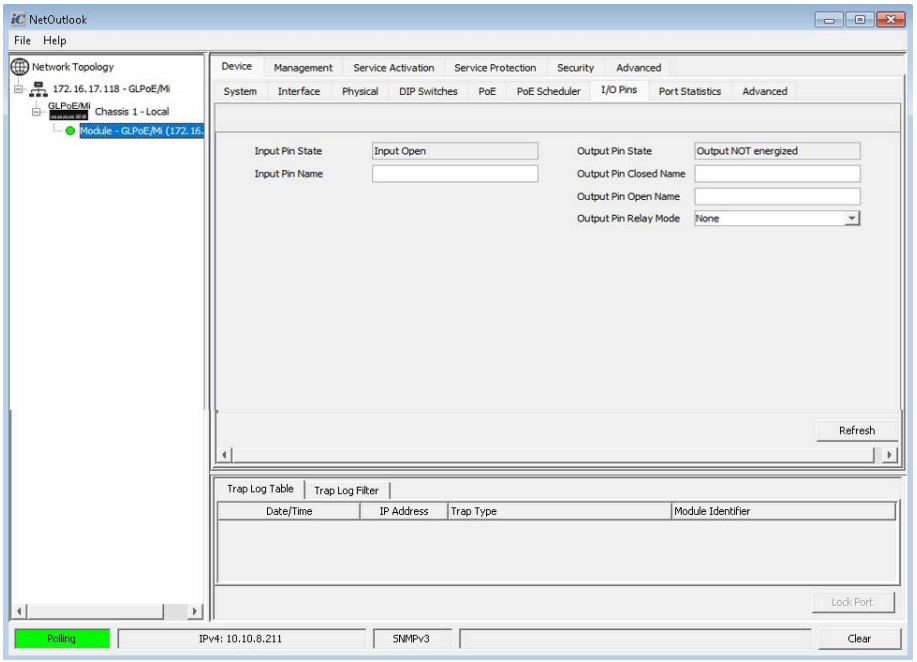
To view the profile, click the ***Overview*** button. From the Overview screen, click the ***Delete All*** button to delete all profiles.

To configure another profile, click the ***Add*** button.

5.6.1.7 I/O Pins Tab

I/O Pins tab is only available on RuggedNet models.

The I/O Pins tab provides status for the alarm relay and alarm input. It also provides the ability to assign a failure type and name to the alarm relay and alarm input.



I/O Pins Tab

Input Pin State

Displays the status of the alarm input (input open or input closed).

An alarm input is available for detecting external events such as door open or closed (pin 4 and 5). The alarm input provides 3.3VDC to detect an external open or shorted condition. Use the supplied connector to attach the wire to the external alarm. Use 16 - 24 AWG wire.

Input Name

Enter a name for the alarm input in the text box.

Output Pin State

Displays the status of the alarm relay (output not energized, output energized).

Energized	Indicates a normally open contact has closed or a normally closed contact has opened.
Not energized	Indicates a normally open contact is open or a normally closed contact is closed.

Output Pin Closed Name

Enter a name for the normally closed condition in the text box.

Output Pin Open Name

Enter a name for the normally opened condition in the text box.

Output Pin Relay Mode

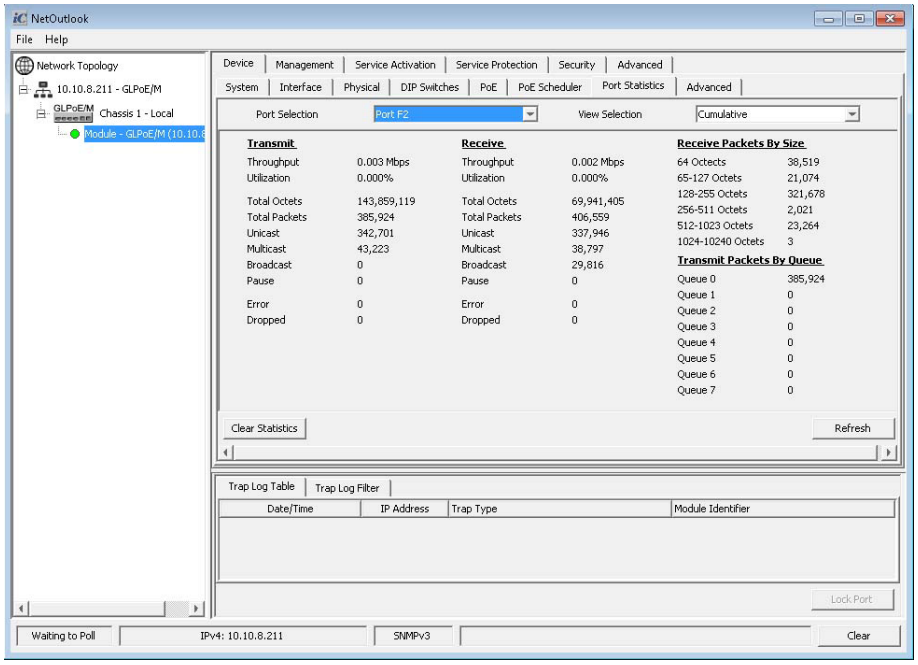
Use the Output Pin Relay Mode pull-down to select the type of error that will cause the output relay to close.

Force	The output relay is forced closed.
None	No error condition is enabled.
Input	An error condition is declared when the alarm input is detected as closed.
Power	An error condition is declared when an input power alarm is detected.
Input, Power	An error condition is declared when either an alarm input or input power alarm is detected.
Temperature	An error condition is declared when a temperature violation is detected.
Input, Temperature	An error condition is declared when either an alarm input or temperature violation is detected.
Power, Temperature	An error condition is declared when either an input power alarm or input power alarm is detected.
Input, Power, Temperature	An error condition is declared when either an input power alarm or input power alarm or temperature violation is detected.

An alarm relay is available to detect a user configured event. The three contacts closure pins can be configured for normally open (pin 1 and 2) or normally closed (pin 3 and 2) operation. The relay contacts support 110VDC/125VAC Maximum Voltage at a maximum current of up to 2 amps. Use the supplied connector to attach the wire to the external alarm. Use 16 - 24 AWG wire.

5.6.1.8 Port Statistic Tab

Port statistics tab displays the statistic for each port on the module. Use the Port Selection pull-down menu to select the desired port number. This tab is not available on all module types.



Port Statistics Tab

Use the ***Clear Statistic*** button to reset all of the statistic to zero for the selected port.

Use the View Selection pull-down menu to select the cumulative or since last baseline port statistic values.

Transmit

Throughput

Indicates the throughput of the selected port in Mbps

Utilization

Indicates the utilization of the selected port in %

Total Octets

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

Total Packets

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

Unicast

The total number of Unicast packets transmitted by a port.

Multicast

The total number of Multicast packets transmitted by a port.

Broadcast

The total number of Broadcast packets transmitted by a port.

Pause

The total number of Pause frames transmitted by a port.

Error

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

Dropped

The total number of packets dropped due to lack of resources during transmission by a port.

Receive

Throughput

Indicates the throughput of the selected port in Mbps

Utilization

Indicates the utilization of the selected port in %

Total Octets

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

Total Packets

The total number of good and error packets received by a port.

Unicast

The total number of Unicast packets received by a port.

Multicast

The total number of Multicast packets received by a port.

Broadcast

The total number of Broadcast packets received by a port.

Pause

The total number of Pause frames received by a port.

Error

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

Dropped

The total number of packets dropped due to lack of resources during reception by a port.

Receive by Size

64 Octets

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

65-127 Octets

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

128-255 Octets

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

256-511 Octets

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

512-1023 Octets

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

1024-[max size] Octets

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).

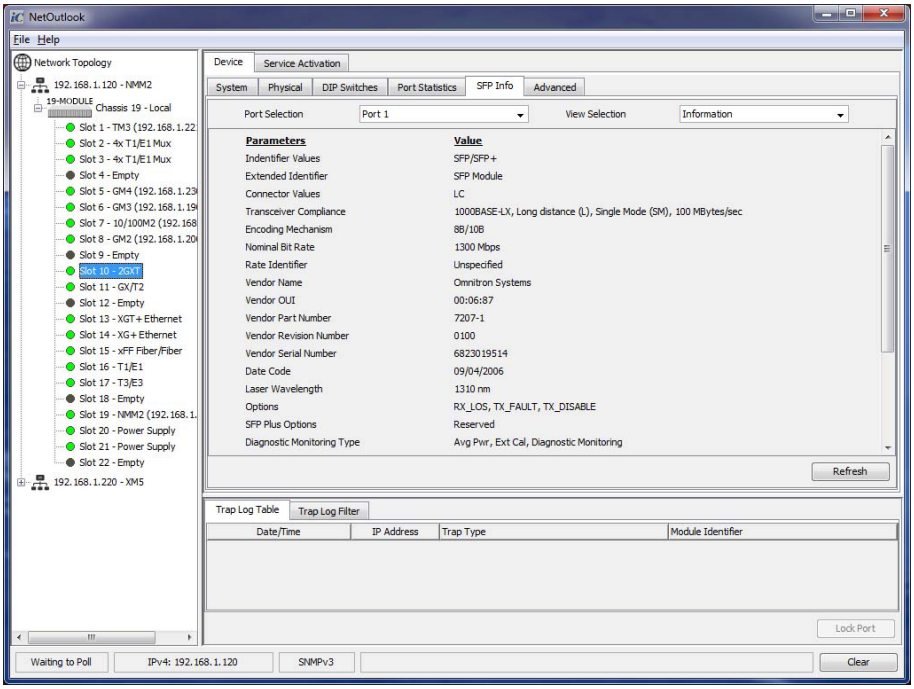
5.6.1.9 SFP Info Tab

The SFP Info tab is only available on modules supporting SFP transceivers.

The SFP Info tab provides general and specific status information on the installed SFP transceivers.

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

Use the View Selection to select the Information, Diagnostic, Page A0 Hex or Page A2 Hex screens. Select Information.

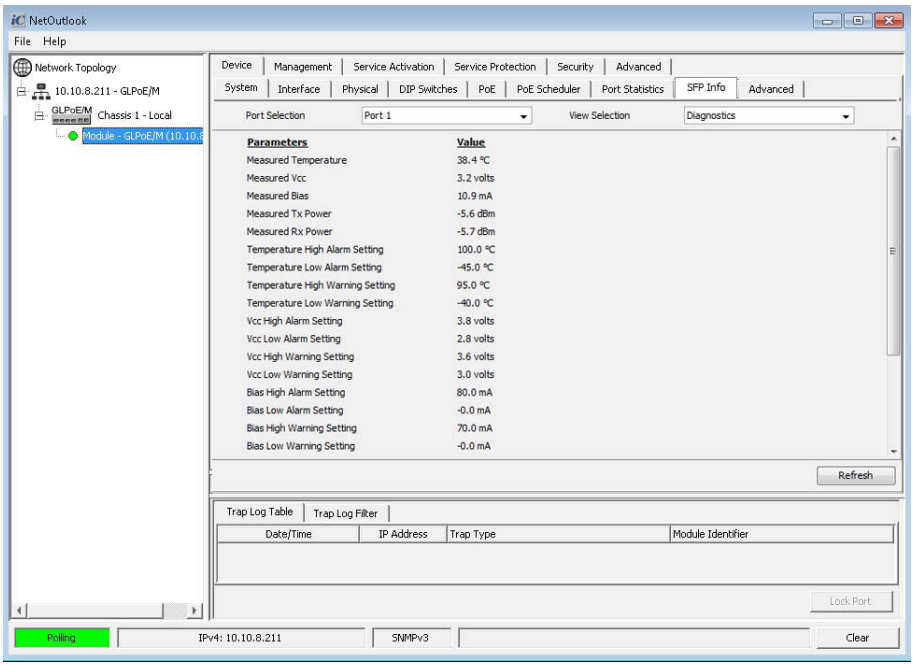


SFP Info Tab - Information

The following general information is available:

- Identifier Values
- Connector Values
- Encoding Mechanism
- Rate Identifier
- Vendor OUI
- Vendor Serial Number
- Laser Wavelength
- SFP Plus Options
- Enhanced Options
- Link Length for 9um fiber (km)
- Link Length for 62.5um fiber (OM1)
- Link Length for 50um fiber (OM3)
- Extended Identifier
- Transceiver Compliances
- Normal Bit Rate
- Vendor Name
- Vendor Revision Number
- Date Code
- Options
- Diagnostic Monitoring Type
- SFF-8472 Compliance
- Link Length for 9um fiber (m)
- Link Length for 50um fiber (OM2)
- Link Length for copper (m)

Use the View Selection to select the Information, Diagnostic, Page A0 Hex or Page A2 Hex screens. Select Diagnostic.

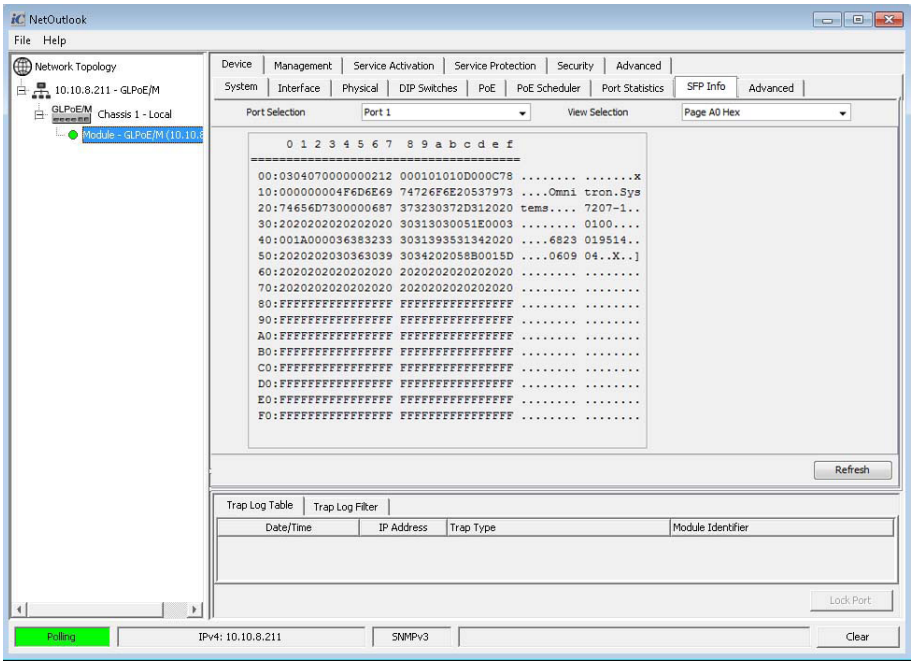


SFP Info Tab - Diagnostics

The following diagnostic information is available:

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

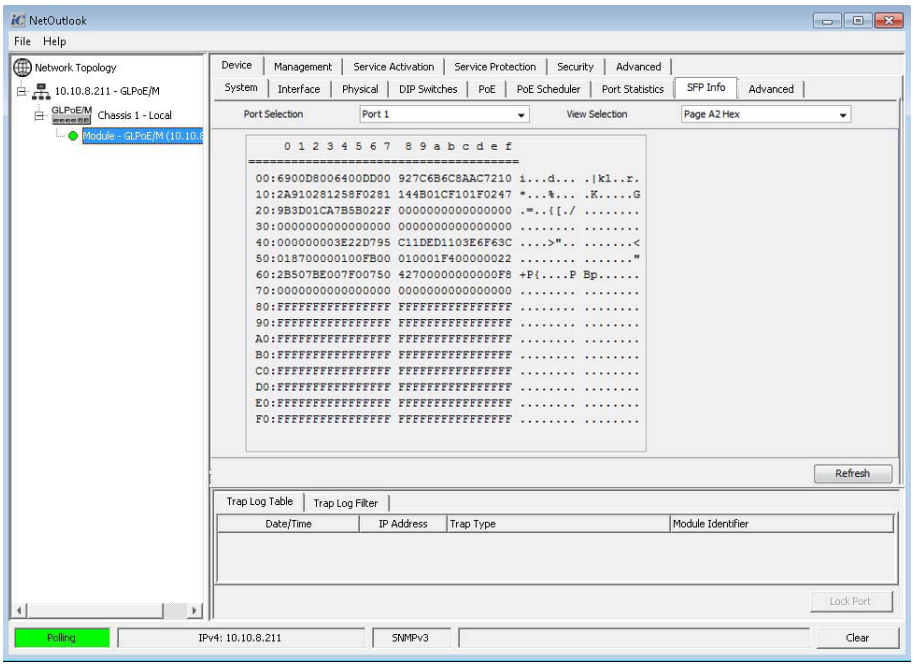
Use the View Selection to select the Information, Diagnostic, Page A0 Hex or Page A2 Hex screens. Select Page A0 Hex.



SFP Info Tab - A0 Hex

The A0 Hex page represents the Information page in hexadecimal.

Use the View Selection to select the Information, Diagnostic, Page A0 Hex or Page A2 Hex screens. Select Page A2 Hex.

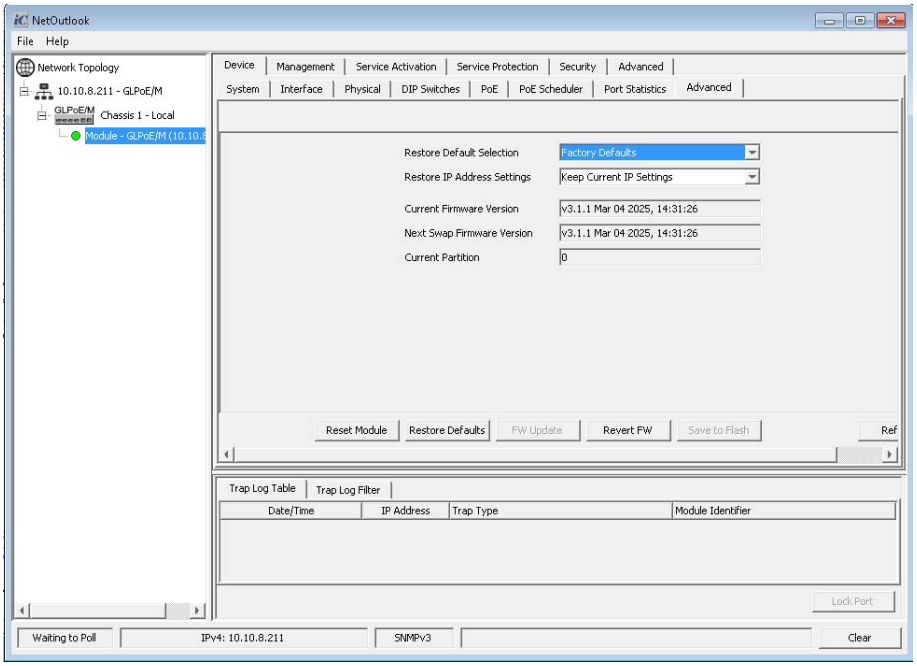


SFP Info Tab - A2 Hex

The A2 Hex page represents the Diagnostic page in hexadecimal

5.6.1.10 Advanced Tab

The Advanced tab provides the ability to reset or restore the firmware. The software revision on the module is also displayed. Tab options will vary depending on the module type.



Advanced Tab

To restore or default a module, use the Restore Default Selection and Restore IP Address Settings pull-down menus to select the desired options.

Restore Default Selection

Use the Restore Default Selection pull-down menu to select ***Factory Defaults***, ***Local Defaults*** or ***Previous Configuration***.

To restore a module to the factory default settings, select ***Factory Defaults*** from the Restore Default Selection pull-down menu. Click the ***Restore Defaults*** button. A warning prompt is displayed when the ***Restore Defaults*** button is clicked.

Click the ***Yes*** button to continue.

To restore a module to a local configuration stored on the module, select ***Local Defaults*** from the Restore Default Selection pull-down menu. Click the ***Restore Defaults*** button. A warning prompt is displayed when the ***Restore Defaults*** button is clicked.

Click the ***Yes*** button to continue.

To restore a module to a previous configuration stored on the module, select ***Previous Configuration*** from the Restore Default Selection pull-down menu. Click the ***Restore Defaults*** button. A warning prompt is displayed when the ***Restore Defaults*** button is clicked.

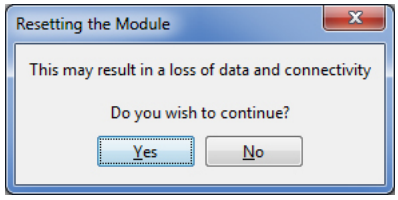
Click the ***Yes*** button to continue.

Restore IP Address Settings

Use the Restore IP Address Settings pull-down menu to select ***Keep IP Address Settings*** or ***Set to Restore IP Settings***.

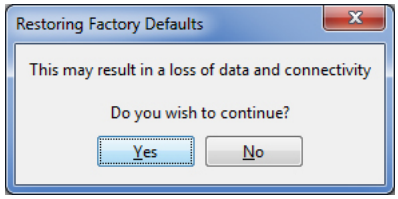
The Current and Next Swap Firmware Version are displayed in the text boxes.

To perform a reset of the module, click the ***Reset Module*** button. A warning prompt is displayed when the ***Reset Module*** button is clicked.



Click the ***Yes*** button to continue.

To restore a module to the factory default settings, click the ***Restore Defaults*** button. A warning prompt is displayed when the ***Restore Defaults*** button is clicked.



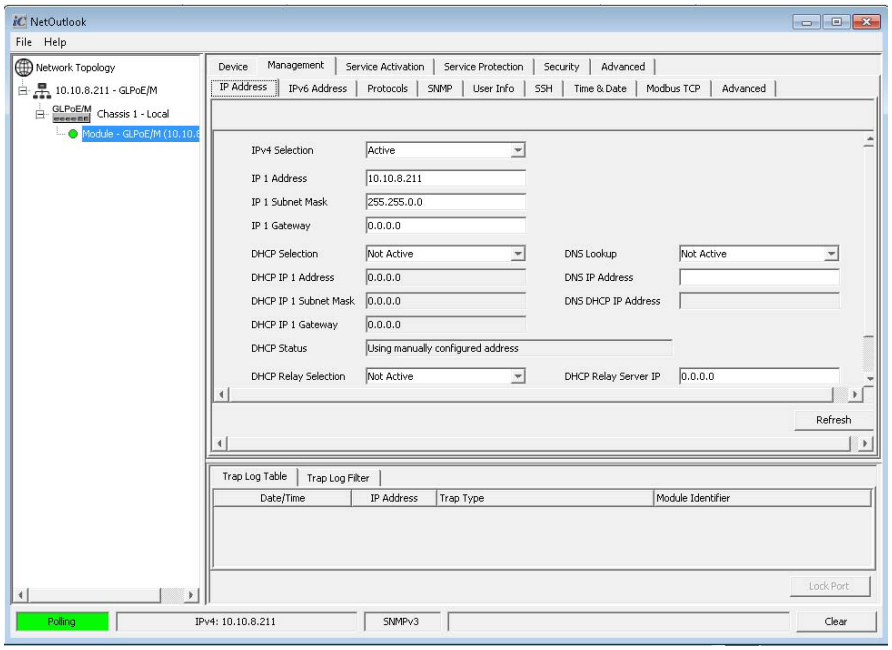
Click the ***Yes*** button to continue.

NOTE: Restore Defaults is not available on all managed module types.

5.6.2 Management Tab

The Management tab provides configuration and viewing of IP parameters, SNMP parameters, SSH, User Information and other network features.

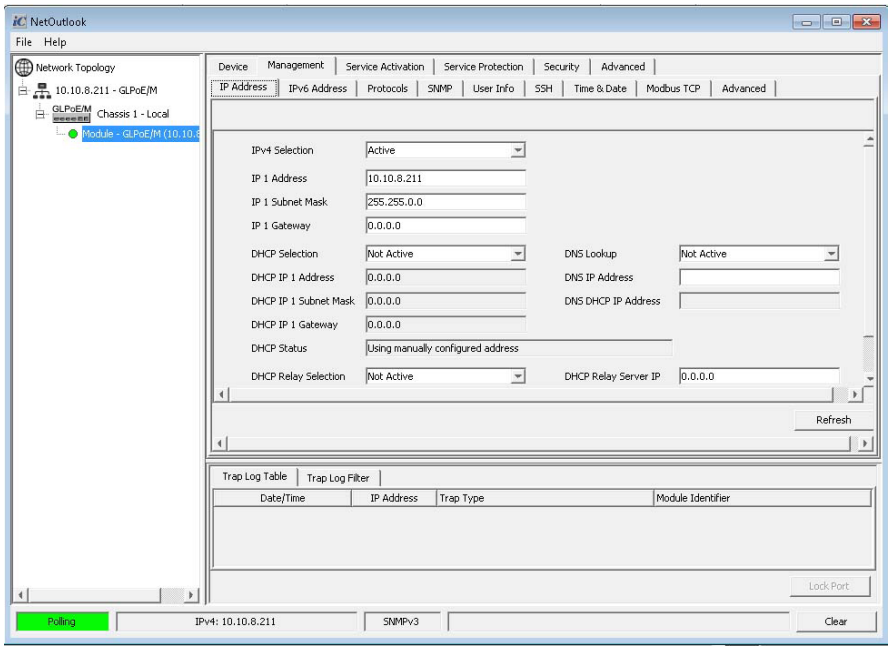
The order of tabs described in this section are: IP Address, IPv6 Address, Protocol, SNMP, User Info, SSH, Time & Date, Modbus TCP and Advanced.



Management Tab

5.6.2.1 IP Address Tab

The IP Address tab provides the ability to configure the IP address, subnet mask, gateway, DHCP and DHCP relay on the module.



IP Address Tab

IPv4 Selection

Use the IPv4 Selection pull-down menu to enable (active) or disable (not active) IP protocol on the module.

IP 1 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).

IP 1 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.

IP 1 Gateway

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

DHCP Selection

Use the DHCP Selection pull-down menu to enable (active) or disable (not active) on the module.

DHCP IP 1 Address

Displays the returned DHCP IP Address.

DHCP 1 Subnet Mask

Displays the returned DHCP Subnet Mask.

DHCP IP 1 Gateway

Displays the returned DHCP Gateway.

DHCP Status

Displays the status of the DHCP or manual process depending on the DHCP Selection setting.

DHCP Relay Selection

Use the DHCP Relay Selection pull-down menu to enable (active) or disable (not active) 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.

DHCP Relay Circuit ID

Use the DHCP Relay Circuit ID Selection pull-down menu to enable (active) or disable (not active) the DHCP Relay Circuit ID.

DHCP Relay Remote ID

Use the DHCP Relay Remote ID Selection pull-down menu to enable (active) or disable (not active) the DHCP Relay Remote ID.

DNS Lookup

Use the DNS Lookup pull-down menu to enable (active) or disable (not active) DNS Lookup.

DNS IP Address

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

DNS DHCP IP Address

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

The configured DNS address will be used by the module for DNS based operations if DHCP is disabled.

DHCP Relay Server IP

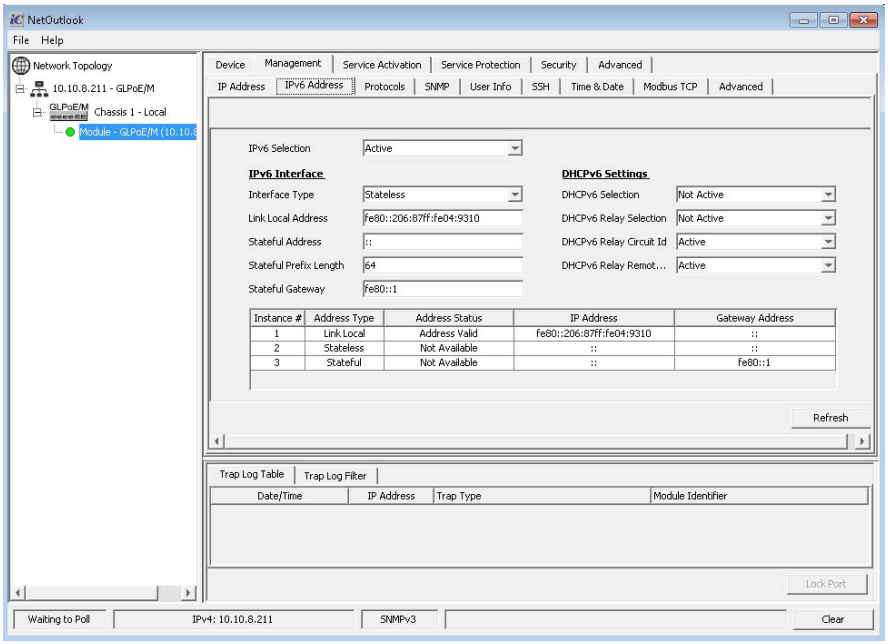
Enter the DHCP Relay Server IP address in the text box in the x.x.x.x format (x represents a decimal number between 0 and 255).

DHCP Relay Type

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

5.6.2.2 IPv6 Address Tab

The IPv6 Address tab provides the ability to configure IPv6 address parameters on the module. IPv6 address are eight 16-bit hexadecimal blocks separated by colons (ie. 2dfc:0:0:0:0217:cbff:fe8c:0).



IPv6 Address Tab

IPv6 Selection

Use the IPv6 Selection pull-down menu to enable (active) or disable (not active) IPv6.

IPv6 Interface

Interface Type

Use the Interface Type pull-down menu to configure the interface for stateful or stateless operation.

Stateful configuration requires a IPv6 service to provide the IPv6 address to the client (module) and requires both client and server to maintain the "state" of the address. Stateless auto configuration of IPv6 allows the client (module) to self configure the IPv6 address. The advantage is that the IPv6 service is not required to store any dynamic state information about any individual clients. A network can use both stateful and stateless auto configuration at the same time.

IPv6 stateful can be entered by the user and does not require an IPv6 service. However, if DHCPv6 is enabled the address will be acquired via DHCPv6 information provided by the server.

Link Local Address

Use the Link Local Address text box to manually enter an address.

When IPv6 is active, a link-local address is automatically configured on the interface.

Stateful Address

Use the Stateful Address text box to manually enter the IPv6 address.

Stateful Prefix Length

Use the Stateful Prefix Length text box to manually enter the prefix length up to 128.

Stateful Gateway

Use the Gateway Address text box to manually enter a new Gateway Address.

DHCPv6 Settings

DHCPv6 Selection

Use the DHCPv6 Selection pull-down menu to enable (active) or disable (not active) DHCPv6 on the module.

DHCPv6 Relay Selection

Use the DHCPv6 Relay Selection pull-down menu to enable (active) or disable (not active) DHCPv6 Relay agent on the module.

DHCPv6 Relay Circuit ID

Use the DHCPv6 Relay Circuit ID pull-down menu to enable (active) or disable (not active) DHCPv6 Relay Circuit ID on the module.

DHCPv6 Relay Remote ID

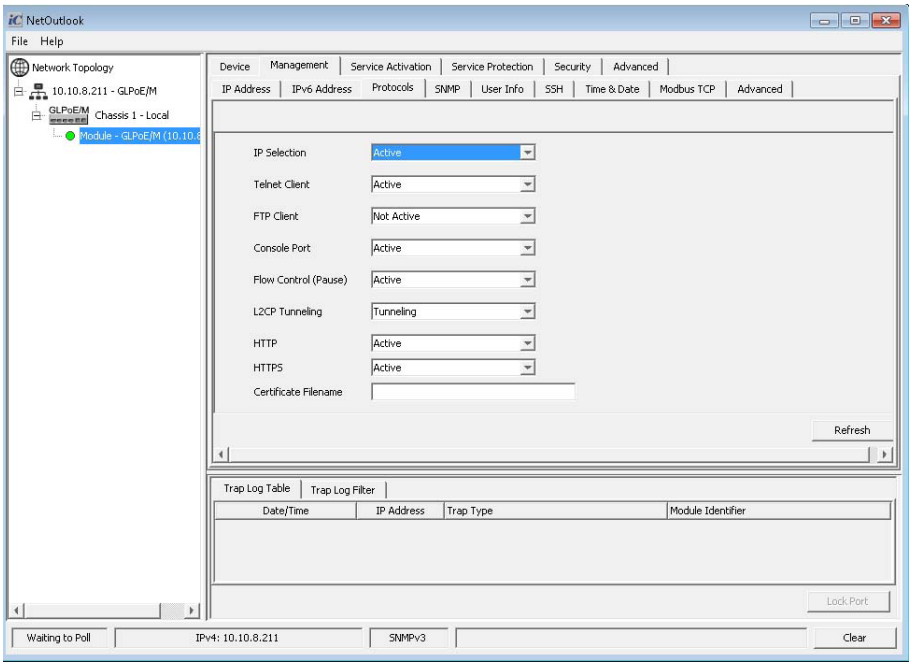
Use the DHCPv6 Relay Remote ID pull-down menu to enable (active) or disable (not active) DHCPv6 Relay Remote ID on the module.

The configured IPv6 addresses are displayed in the table. Interface #, Interface Type, Interface Status, IP Address and Gateway Address is displayed.

To save the changes, click on the ***Apply*** button.

5.6.2.3 Protocols Tab

The Protocols tab provides the ability to configure and display IP, Telnet, FTP, Console Port, Flow Control, L2CP Tunneling, HTTP and HTTPs protocols.



Protocols Tab

IP Selection

Use the IP Selection pull-down menu to enable (active) or disable (not active) IP on the module. When disabled, the module is considered IP less and will not respond to any IP requests.

Telnet Client

Use the Telnet Client pull-down menu to enable (active) or disable (not active) Telnet on the module.

FTP Client

Use the FTP Client pull-down menu to enable (active) or disable (not active) FTP on the module.

Console Port

Use the Console Port pull-down menu to enable (active) or disable (not active) access to the serial console interface.

Flow Control (Pause)

Use the Flow Control pull-down menu to enable (active) or disable (not active) flow control on the module.

L2CP Tunneling

Use the L2CP Tunneling pull-down menu to tunnel or discard L2CP packets on the module.

HTTP

Use the HTTP pull-down menu to enable (active) or disable (not active) HTTP support. HTTP is enabled (active) by default.

HTTPS

Use the HTTPS pull-down menu to enable (active) or disable (not active) HTTPS support. HTTPS is enabled (active) by default.

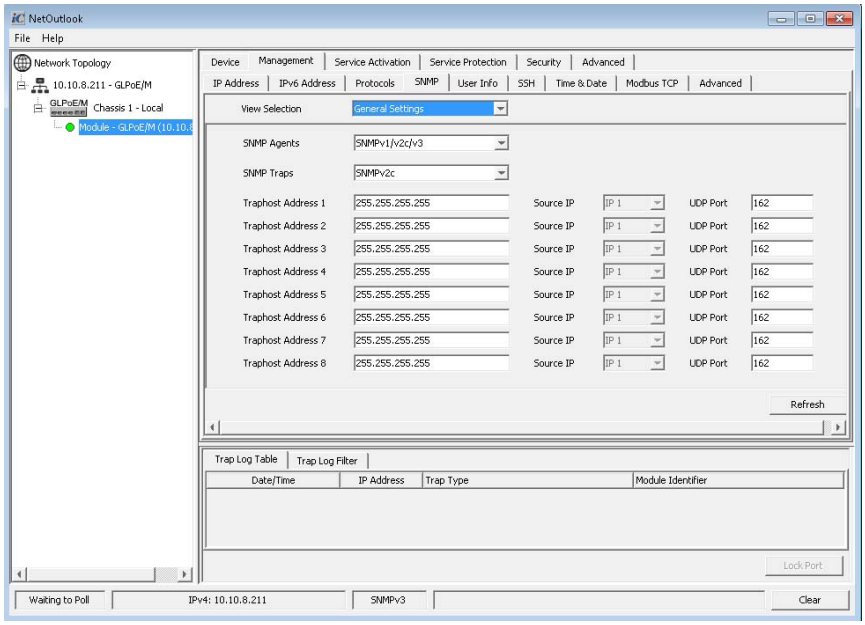
Certificate Filename

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

To save the changes, click on the ***Apply*** button.

5.6.2.4 SNMP Tab

The SNMP tab provides the ability to configure and display the SNMP parameters, Read/Write Community Names, Trap Host IP Addresses and SNMPv3 user rights. Tab options will vary depending on the module type.



SNMP Tab

Use the View Selection pull-down menu to select General Settings, SNMPv1/2vc Settings or SNMPv3 User Settings. Select General Settings.

SNMP Agents

Use the SNMP Agent pull-down menu to configure the SNMP agent by selecting SNMPv1/v2c, SNMPv3, SNMPv1/v2c/v3 or None. 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 select the way the module reports SNMP traps. Select SNMPv1, SNMPv2c or SNMPv3.

Traphost Address 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).

Source IP

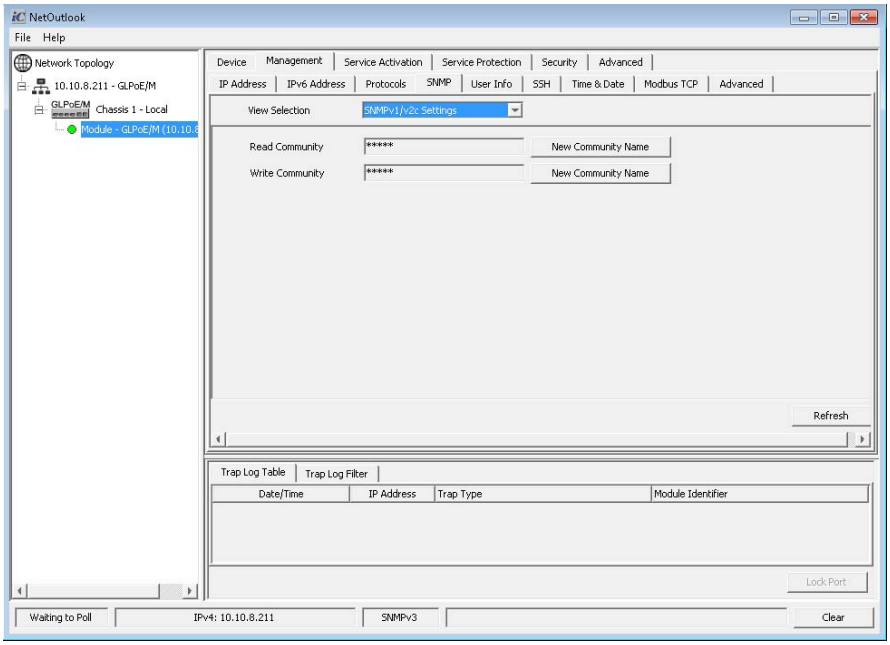
Depending on the management module type, the Source IP address can be selected. Use the Source IP pull-down menu to select IP 1 or IP 2.

UDP Port

Enter the UDP Port number for the SNMP UDP trap port number.

To save the changes, click on the ***Apply*** button.

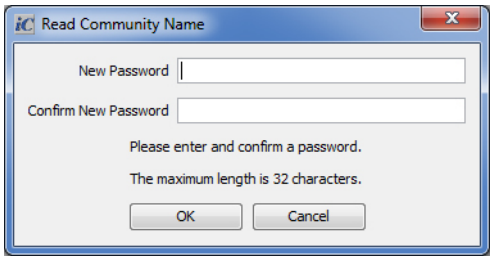
Use the View Selection pull-down menu to select General Settings, SNMPv1/v2c Settings or SNMPv3 User Settings. Select SNMPv1/v2c.



SNMP Tab - SNMPv1/v2c Settings

Read Community

Click the ***New Community Name*** button to change the SNMP Read Community name. A Read Community Name dialog box will be displayed.

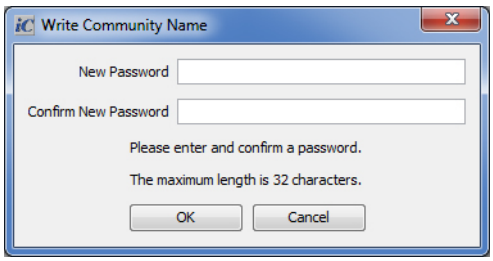


Enter the new password and confirm the new password. Click ***OK*** to change the password.

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.

Write Community

Click the ***New Community Name*** button to change the SNMP Write Community name. A Write Community Name dialog box will be displayed.

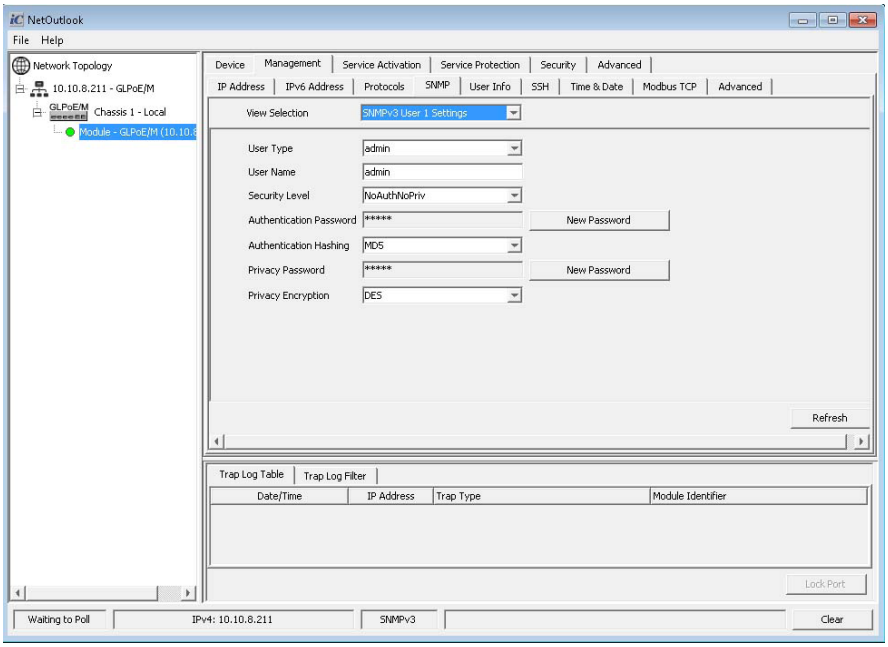


Enter the new password and confirm the new password. Click ***OK*** to change the password.

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. "public" is the default setting.

To save the changes, click on the ***Apply*** button.

Use the View Selection pull-down menu to select General Settings, SNMPv1/v2c Settings or SNMPv3 User Settings. Select SNMPv3.



SNMP Tab - SNMP v3 User

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. HMAC-MD5 and HMAC-SHA are the specified authentication protocols and CBC-DES is the specified privacy protocol. The module supports four simultaneous SNMPv3 users.

The User 1, User 2, User 3 and User 4 have the following information.

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.

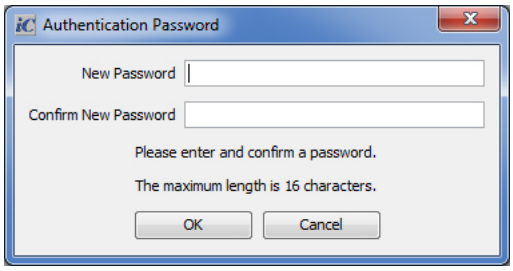
noAuthNoPriv	Allows access without authentication and without privacy.
authNoPriv	Allows access with authentication, but without privacy.
authPriv	Allows access with authentication and with privacy.

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

Authentication Password

Click the ***New Password*** button to change the Authentication Password.

An Authentication Password dialog box will be displayed.



"privateadmin" is the default password.

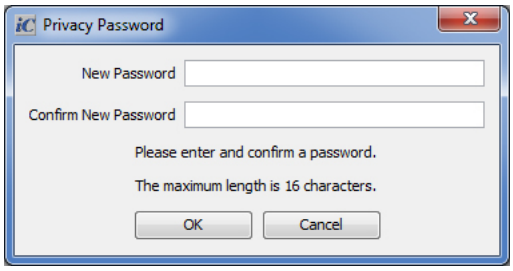
Enter the new password and confirm the new password. Click ***OK*** to change the password.

Authentication Hashing

Use the Authentication Hashing pull-down menu to select the hashing algorithm; MD5 or SHAPrivacy Password.

Click the ***New Password*** button to change the Privacy Password.

A Privacy Password dialog box will be displayed.



"publicguest" is the default password.

Enter the new password and confirm the new password. Click ***OK*** to change the password.

Privacy Encryption

Use the Privacy Encryption pull-down menu to select the encryption method; AES-128 or DES

To save the changes, click on the ***Apply*** button.

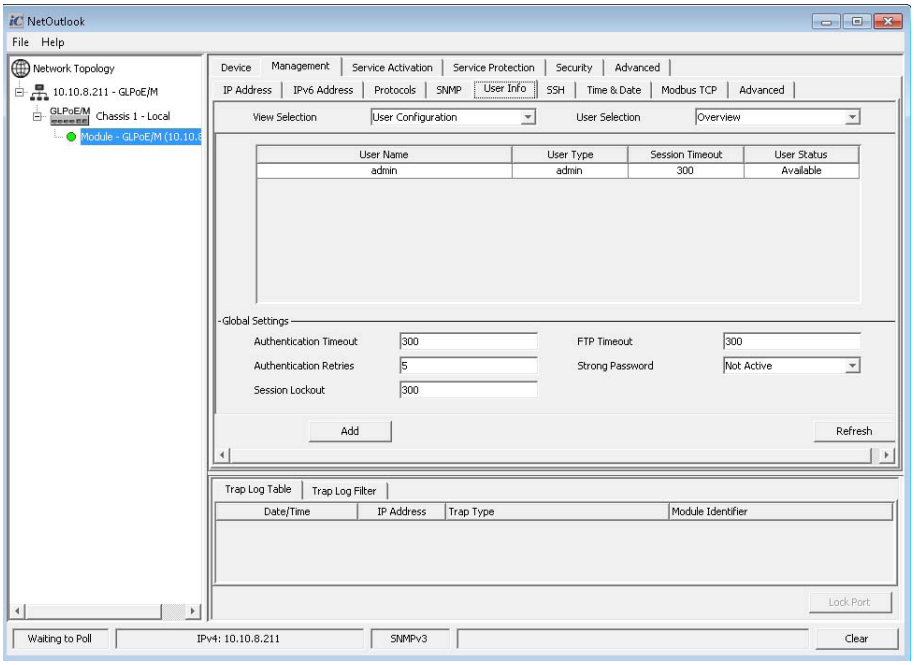
SNMPv3 Factory Default User Settings

User 1 Type	read-only
User 1 Name	guest
User 1 security level	noAuthNoPriv
User 1 privacy password	publicguest
User 1 authentication password	publicguest
User 2 Type	admin

User 2 Name	admin
User 2 security level	noAuthNoPriv
User 2 privacy password	privateadmin
User 2 authentication password	privateadmin
User 3 Type	deny
User 3 Name	guest1
User 3 security level	noAuthNoPriv
User 3 privacy password	publicguest
User 3 authentication password	publicguest
User 4 Type	deny
User 4 Name	guest2
User 4 security level	noAuthNoPriv
User 4 privacy password	publicguest
User 4 authentication password	publicguest

5.6.2.5 User Info Tab

The User Info tab provides the ability to modify, add or delete a user account.



User Info Tab

Use the View Selection pull-down menu to select User Configuration or User Session Status. Select User Configuration.

Global Settings

Authentication Timeout (s)

Enter the authentication timeout value in the text box. Valid entries are 0 to 300 seconds. 300 seconds is the default value.

Authentication Retries

Enter the number of authentication retries in the text box. Valid entries are 1 to 5. 5 retries is the default value.

Session Lockout (s)

Enter the Session Lockout value in the text box. Valid entries are 1 to 300 seconds. 300 seconds is the default value.

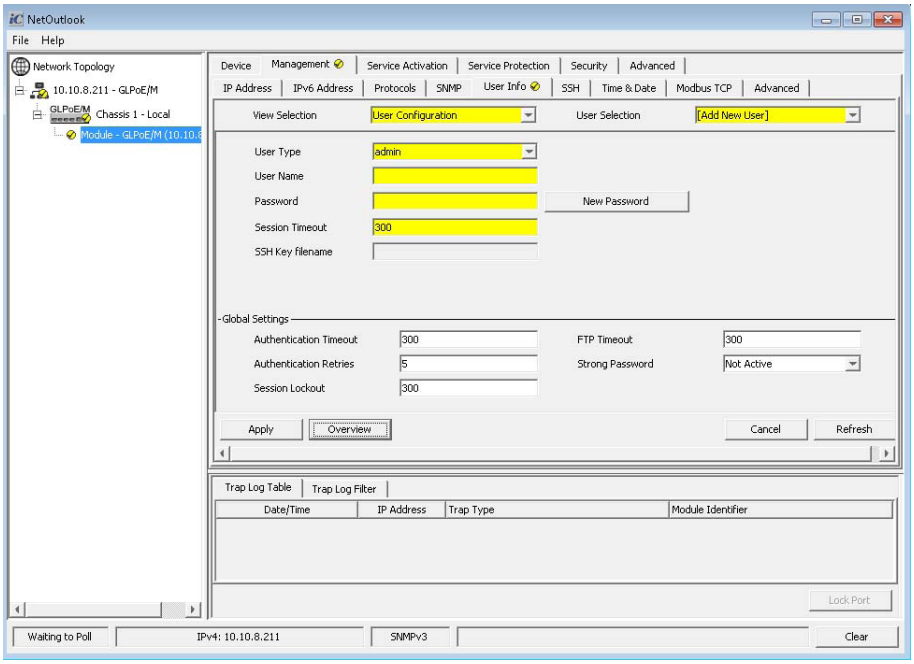
FTP Session Timeout (s)

Enter the FTP Timeout value in the text box. Valid entries are 1 to 3600 seconds. 300 seconds is the default value.

Strong Password

Use the Strong Password pull-down menu to enable (active) or disable (not active) the strong password option.

Click the ***Add*** button to configure a new user.



User Info Tab - New User

User Type

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

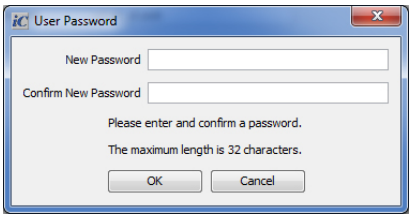
Admin	Has full read/write privileges including user name and password changes.
Read-write	Has full read/write privileges with the exception of user name and password operations.
Read-only	Can only view the configuration of the module and will not be allowed to make any changes.
Deny	Does not have any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

User Name

Use the text box to enter the name of the user.

Password

Click the ***New Password*** button to change the user password. A User Password dialog box will be displayed.



Enter the new password and confirm the new password. Click ***OK*** to change the password.

Session Timeout

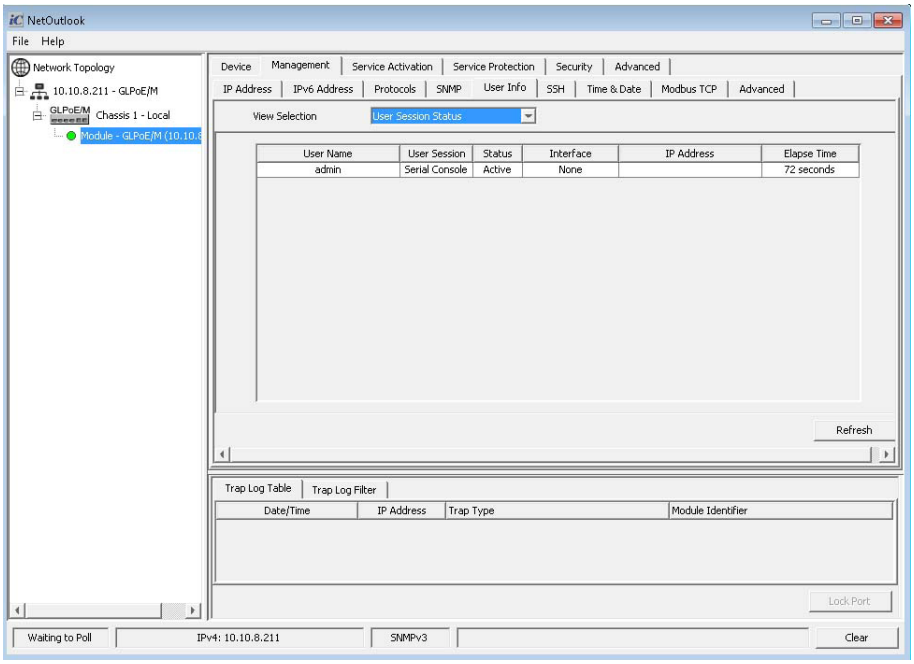
The session timeout can be changed from 0 to 3600 seconds. Use the text box to enter a new session timeout value.

SSH Key Filename

The SSH Key filename can be changed. Use the text box to enter a new filename.

To save the changes, click on the ***Apply*** button.

Use the View Selection pull-down menu to select User Configuration or User Session Status. Select User Session Status.



User Info Tab - User Session Status

The User Session Status lists the active sessions logged into the module. It provides information on the User Name, Session Type, Interface, IP Address (source) and Session Time.

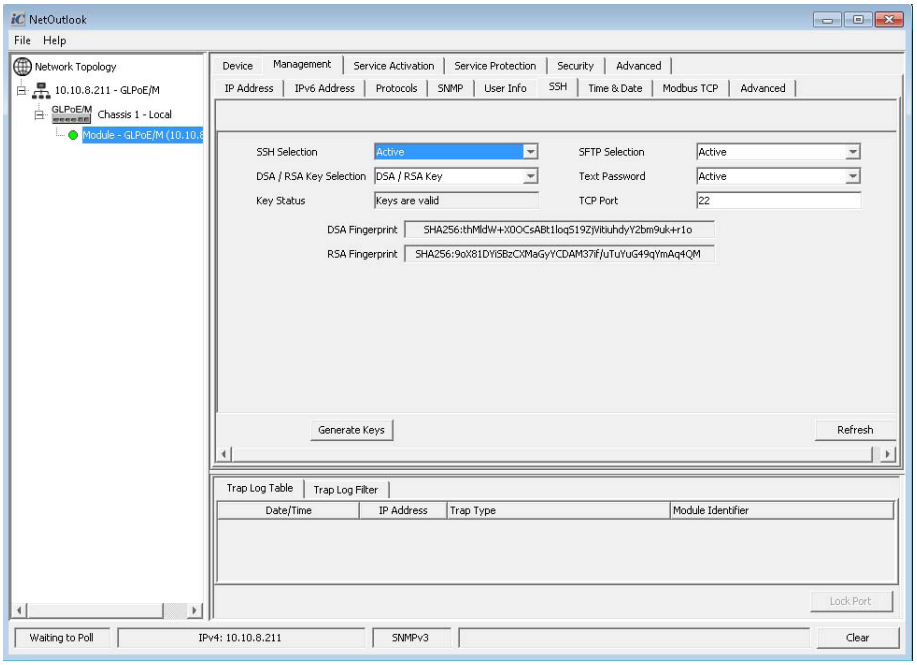
To save the changes, click on the ***Apply*** button.

To delete a user, use the User Selection pull-down menu and select the user name to be deleted.

Click on the ***Delete*** button to delete the user selection.

5.6.2.6 SSH Tab

The SSH tab provides the ability to configure and view SSH parameters on the module.



SSH Tab

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.

Use the View Selection pull-down menu to select Configuration or Status options. Select Configuration.

OmniConverter and RuggedNet switches do not support the Status pull-down option. The DSA and RSA fingerprints are displayed in the main screen.

SSH Selection

Use the SSH Selection pull-down menu to enable (active) or disable (not active) SSH protocol.

DSA / RSA Key Selection

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

Key Status

The status of the key is displayed.

SFTP Selection

Use the SFTP Selection pull-down menu to enable (active) or disable (not active) SFTP protocol.

Text Password

Use the Text Password pull-down menu to enable (active) or disable (not active) Test Password.

TCP Port

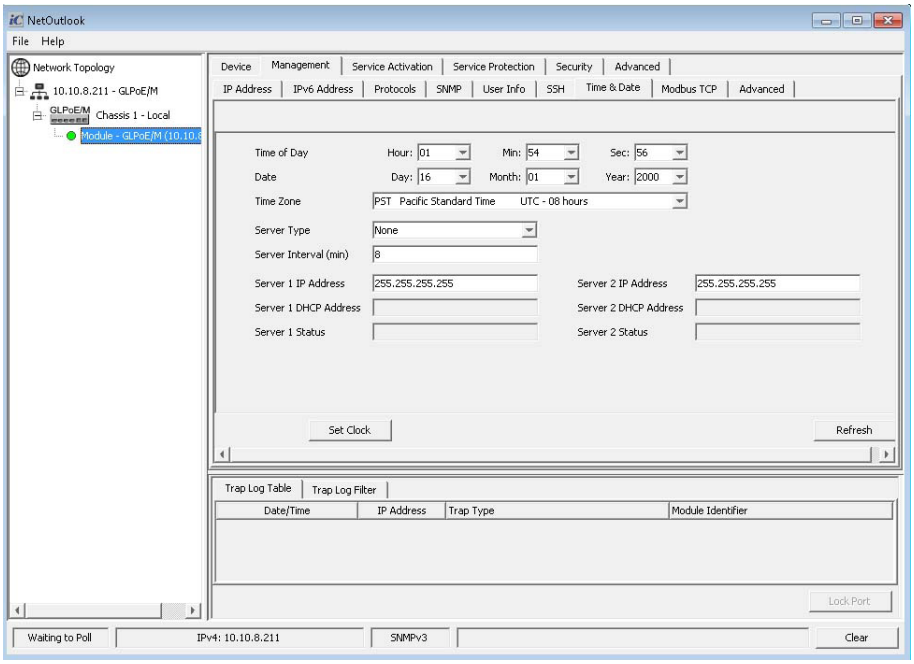
A text box allows the configuration of the TCP Port used during a SSH session. A value of 1 to 65,535 is accepted.

The RSA and DSA fingerprints are displayed.

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

5.6.2.7 Time and Date Tab

The Time and Date tab provides the ability to change the Time of Day, Date and Time Zone and SNTP parameters.



Time and Date Tab

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

Server Type

Use the server Type pull-down menu to select Time protocol None, SNTP or NTP.

Server Interval (minutes)

Use the Server 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.

Server 1 IP Address

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

Server 1 DHCP Address

The DHCP IP address will be displayed.

Server 1 Status

Displays the status of the server.

Server 2 IP Address

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

Server 2 DHCP Address

The DHCP IP address will be displayed.

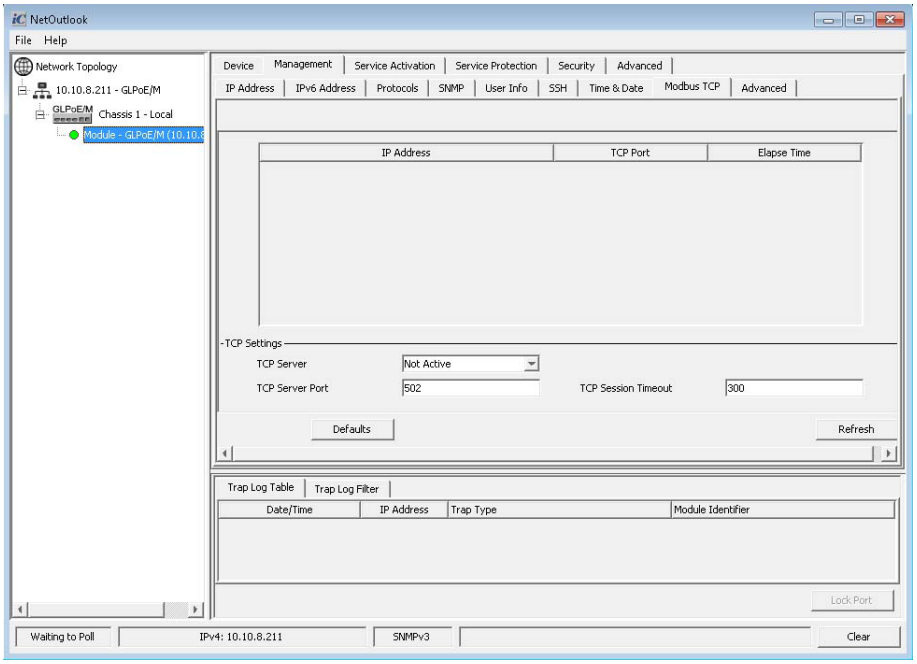
Server 2 Status

Displays the status of the server.

To save the changes, click on the ***Apply*** button.

5.6.2.8 Modbus TCP Tab

The Modbus TCP tab provides the ability configure Modbus TCP server port number and session timeout as well as view the connected TCP clients.



Modbus Tab

The window will display any connected TCP clients. The information provided is IP Address, TCP Port number and connection time.

TCP Settings

TCP Server

Use the TCP Server pull-down menu to enable (active) or disable (not active) Modbus TCP protocol.

TCP Server Port

Enter the TCP Server Port number in the text box. The default TCP Server Port number is 502.

TCP Session Timeout

Enter the TCP Session Timeout in seconds in the text box. The default value is 300 seconds.

To save the changes, click on the ***Apply*** button.

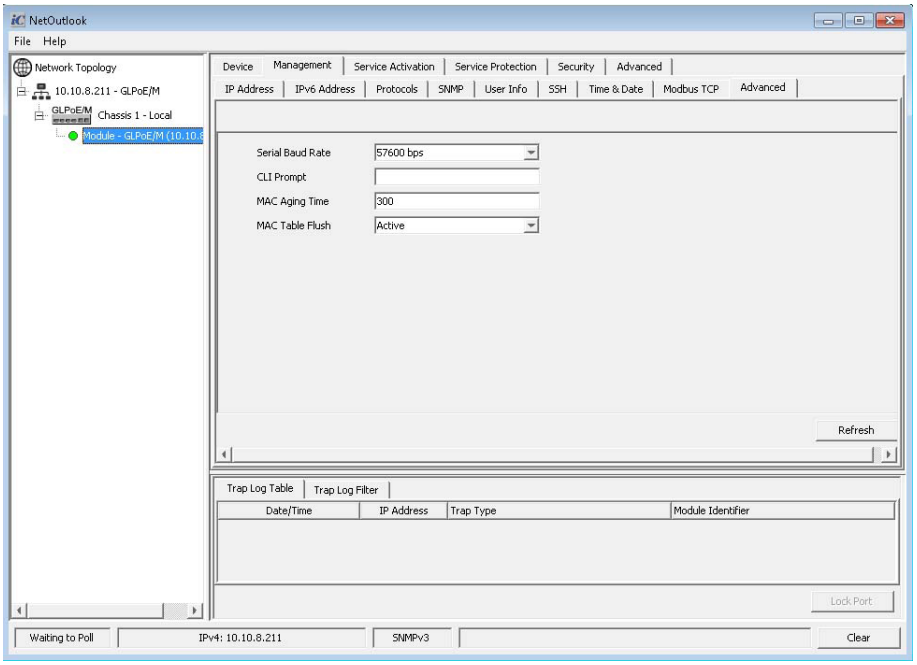
To cancel the changes, click the ***Cancel*** button.

To restore the factory defaults, click the ***Default*** button.

To refresh the screen, click the ***Refresh*** button.

5.6.2.9 Advanced Tab

The Advanced tab provides the ability to configure the Keep Alive trap generation and the Serial Console Port Baud rate. Tab options will vary depending on the module type.



Advanced Tab

Serial Baud Rate

Use the Serial Baud Rate pull-down menu to select the baud rate of the serial console port. The available rates are displayed. The default setting is 57,600bps.

CLI Prompt

Enter a custom prompt for the CLI interface in the text box.

MAC Aging Time

Enter a value in the text box for MAC aging (10 to 600 seconds).

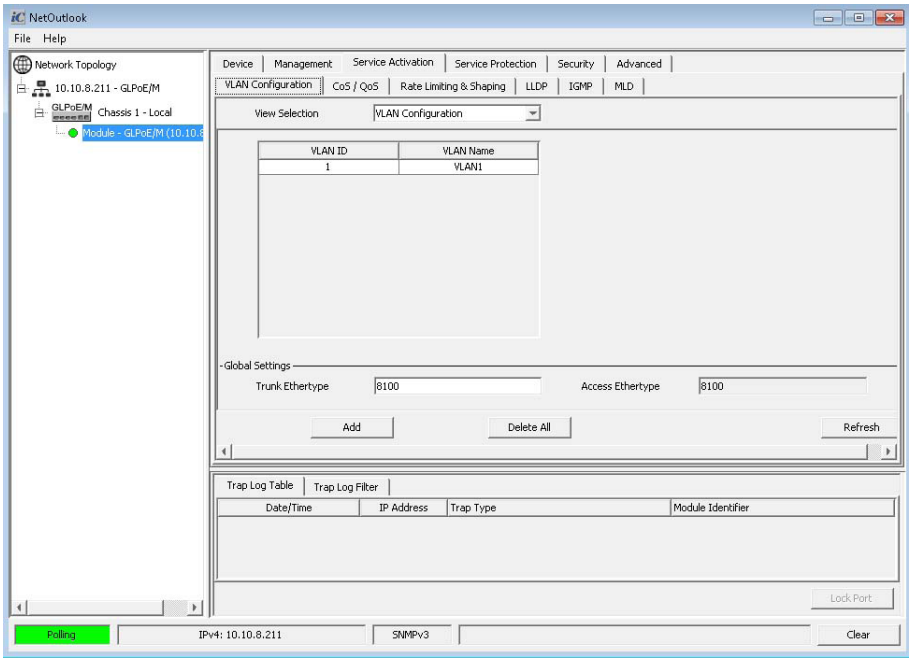
MAC Table Flush

Use the MAC Table Flush pull-down menu to enable (active) or disable (not active) the flushing of the MAC table.

To save the changes, click on the ***Apply*** button.

5.6.3 Service Activation

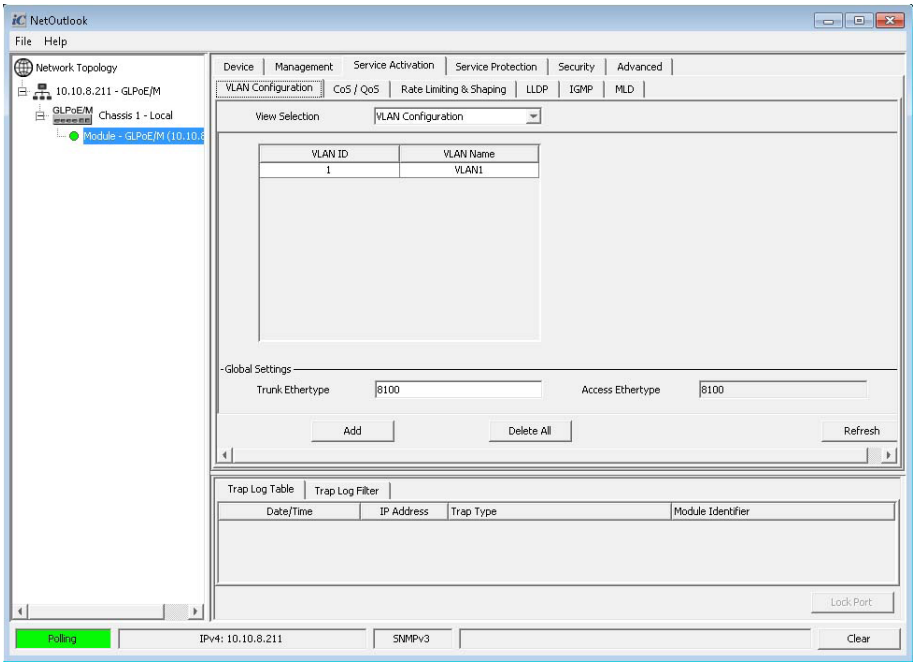
The Service Activation tab provides a second row of tabular options including VLAN Configuration, Class of Service/Quality of Service, Rate Limiting and Shaping, Layer, Link Layer Discovery Protocol (LLDP), Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) snooping.



Service Activation Tab

5.6.3.1 VLAN Configuration Tab

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



VLAN Configuration Tab

Use the View Selection pull-down to select VLAN Configuration or VLAN Interface. Select VLAN Configuration.

Global Settings

Trunk Ethertype

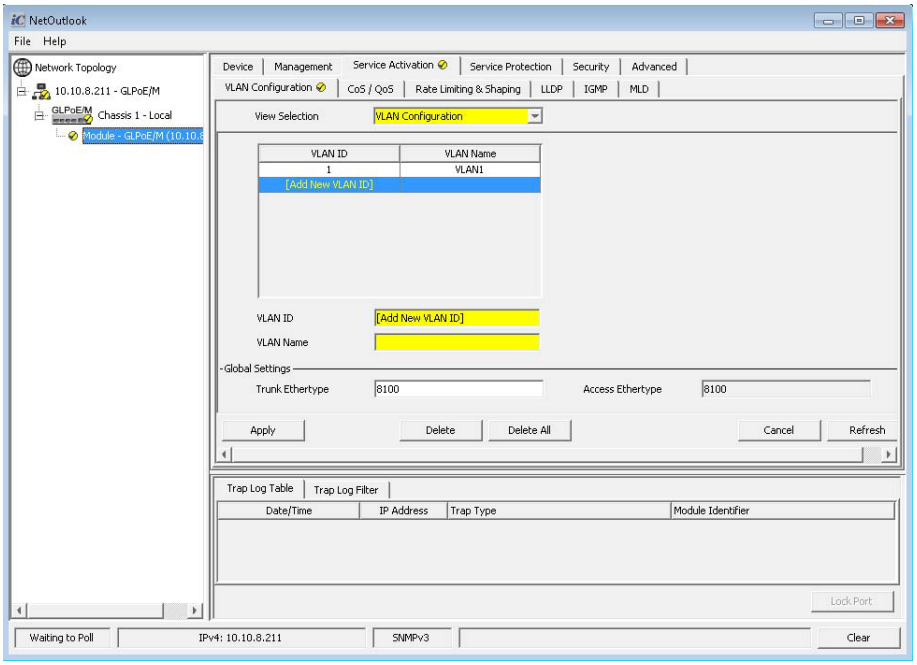
Enter the value for the Ethertype for the trunk interface in the text box. 8100 is the default value.

Access Ethertype

The access Ethertype is displayed in the text box. The value can not be changed.

All configuration VLANs will be displayed in the VLAN Configuration screen.

To configure a VLAN on the module, click the ***Add*** button.



VLAN Configuration Tab - Add Option

VLAN ID

Enter the VLAN ID in the text box.

VLAN Name

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

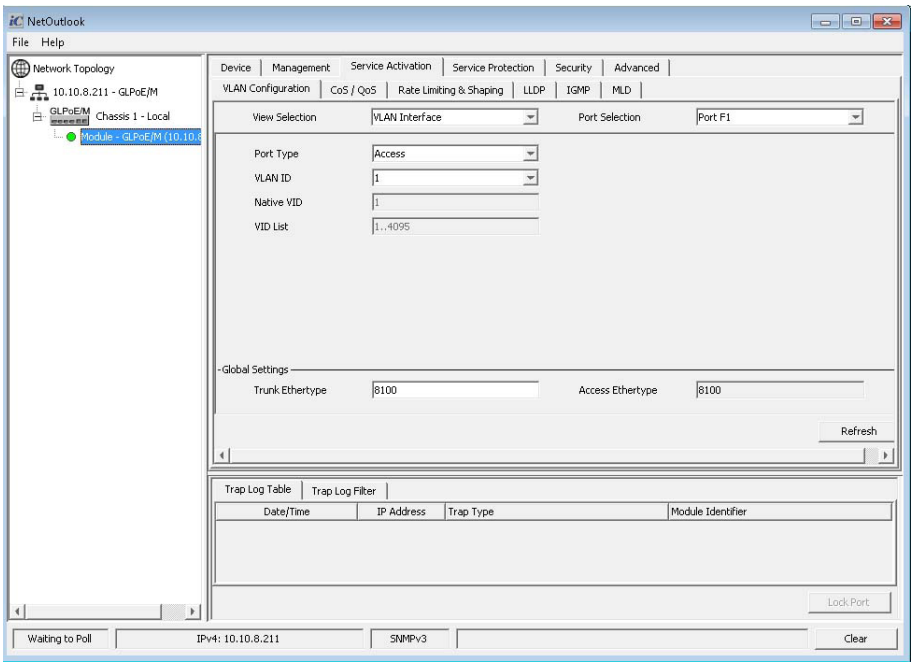
To save the changes, click on the ***Apply*** button.

Click the ***Delete*** button to delete a selected VLAN.

Click the ***Delete All*** button to delete all VLANs.

Once the ***Apply*** button has been clicked, the new VLAN will be displayed in the VLAN Configuration screen. To add another VLAN, click the ***Add*** button.

Use the View Selection pull-down and select VLAN Interface.



VLAN Configuration Tab - VLAN Interface

Port Selection

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

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

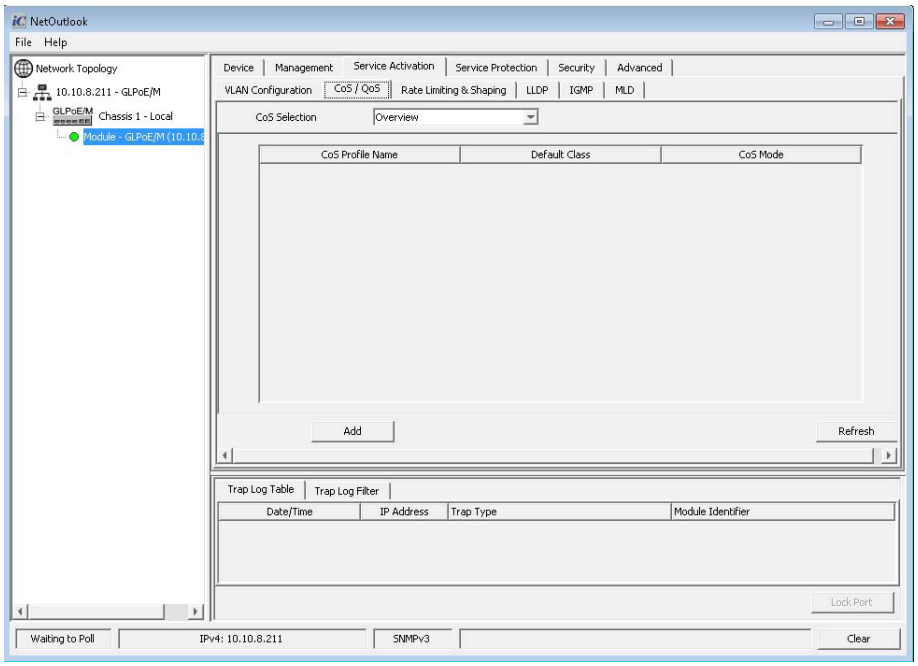
When the port is configured as a trunk port, use the VID List text box to enter the allowed VLAN ID ingressing the trunk port.

To save the changes, click on the ***Apply*** button.

Once the ***Apply*** button has been clicked, another port can be configured.

5.6.3.2 CoS/QoS Tab

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



Cos/Qos Tab

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.

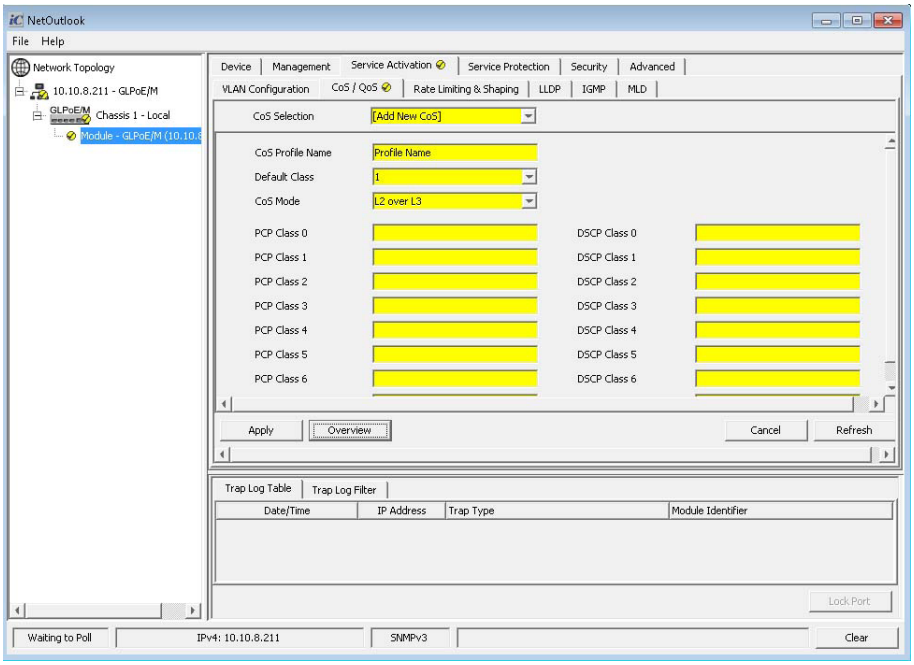
Differentiated Services Code Point (DSCP) profiles are associated with IP priority bits (ipPri). Values are 0 - 63. Priority Code Point (PCP) profiles are associated with the tagged priority bits (pbits). Values are 0 - 7.

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.

Click the ***Add*** button to configure a CoS/QoS profile.



Cos/Qos Tab - Add Option

CoS Selection

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

CoS Profile Name

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.

CoS Mode

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

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.

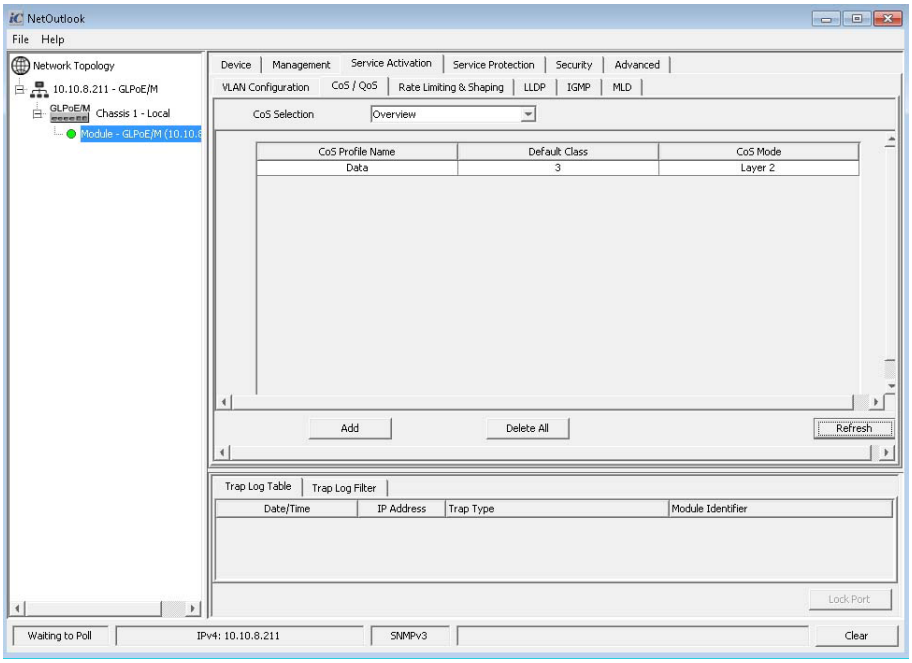
PCP Classes / DSCP Classes

Depending on the CoS Mode, a priority text box will be displayed. If Layer 2 is selected, the PCP class values can be configured. If Layer 3 is selected, DSCP class values can be configured.

Enter the priority values in the Class text box.

To save the changes, click on the ***Apply*** button. Once the ***Apply*** button has been clicked, another CoS profile can be configured. Click the ***Add*** button to configure another profile.

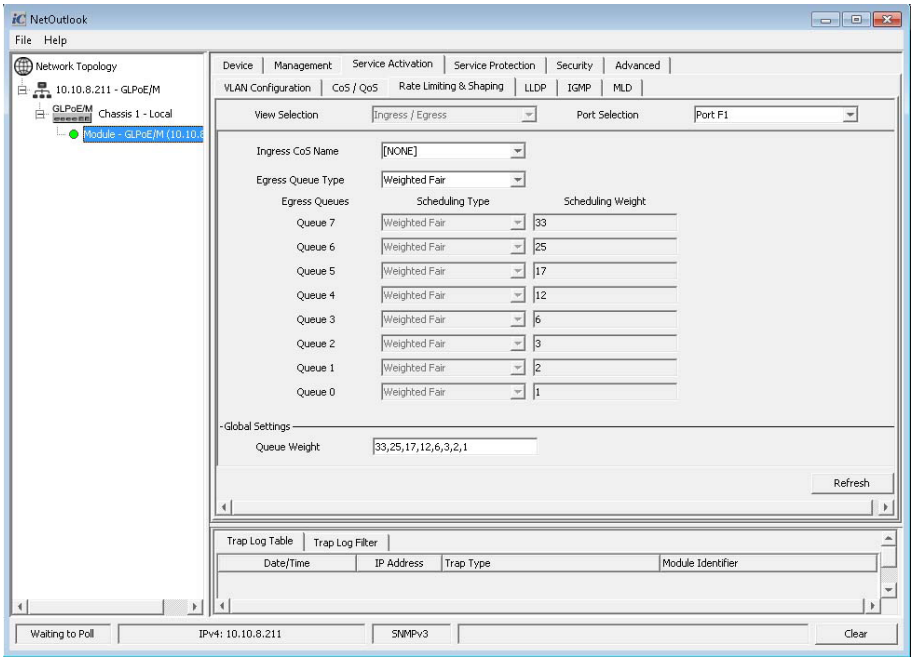
To view the configured CoS profile, use the CoS Selection pull-down menu and select Overview.



Cos/Qos Tab - Overview

5.6.3.3 Rate Limiting and Shaping Tab

The Rate Limiting & Shaping screen provides the ability to add a class of service profile and egress queue type to a port on the module.



Rate Limiting and Shaping Tab

Port Selection

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

Ingress CoS Name

Use the Ingress CoS Name pull-down menu to select a CoS

Egress Queue Type

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

Starving	All queues are set up to starving (strict) priority.
Weighted Fair	All queues are setup for weighted fair queuing using the Queue Mix setting.
Mix Mode	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).

Global Settings

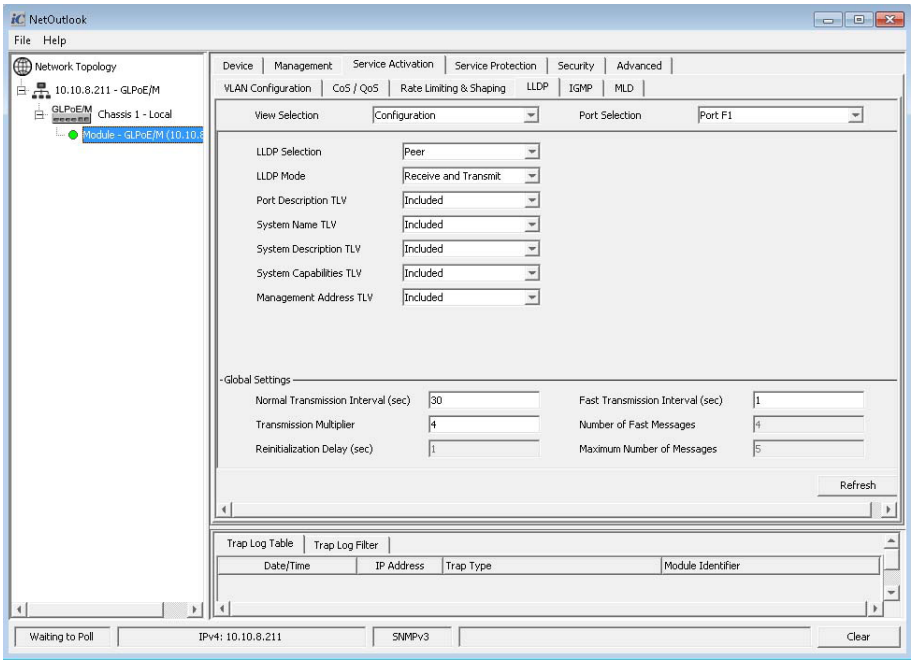
Queue Weight

The default queue weight is 33 (high priority), 25, 17, 12, 6, 3, 2, 1 (low priority). Use the text box to modify the queue weight.

To save the changes, click on the ***Apply*** button.

5.6.3.4 LLDP Tab

The LLDP tab provides the ability to configure the module to support Link Layer Discovery Protocol (LLDP). Tab options will vary depending on the module type.



LLDP Tab

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. LLDP allows an Optical Network Unit (ONU) in a DPoE network to perform DEMARC Auto-Configuration (DAC). Each device configured with an active LLDP agent will send and receive messages on all physical interfaces enabled for LLDP transmission.

Use the View Selection pull-down menu to select Configuration, System or Statistics. Select Configuration.

Use the Port Selection pull-down menu to select the port. The Configuration option for the selected port is displayed.

Configuration

LLDP Selection

Use the LLDP Selection 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 Disable. Transmit and Receive is the default.

The information fields are contained in each 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.

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 LLDPPD.

System Name TLV

The LLDP System name is the same as System Name of the module (i.e. GM4 2xSFP/UTP). Use the System Name pull-down menu to select if this information is Included or Not Included in the LLDPPD.

System Description TLV

The LLDP System Description is the same as the System Description of the module (i.e. Omnitron iConverter GM4 2xSFP/UTP 8975R-0E vx.x.xx s/n xxxxxx - GM4). Use the System Description pull-down menu to select if this information is Included or Not Included in the LLDPPD.

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 LLDPPD.

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 LLDPPD.

Global Settings

Normal Transmission Interval (sec)

Sets the transmission frequency of LLDP updates in seconds. The range is 5 to 65,534 seconds and the default is 30 seconds. Enter the new value in the text box.

Transmission 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 1 to 100 and the default is 4. Enter the new value in the text box.

Reinitialization Delay (sec)

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. Enter the new value in the text box.

Fast Transmission Interval (sec)

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.

Number of Fast Messages

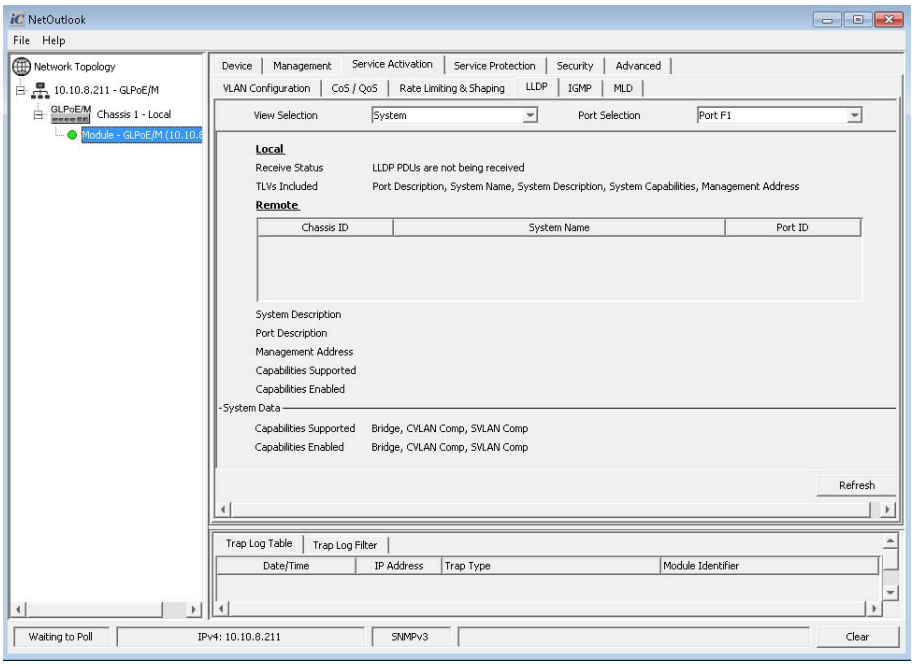
Specifies the number of LLDPDUs that are transmitted during a fast transmission period. The range is 1 to 8 messages and the default value is 4. Enter the new value in the text box.

Maximum Number of 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. Enter the new value in the text box.

To save the changes, click on the ***Apply*** button.

The View Selection pull-down menu to select Configuration, System or Statistics. Select System.



LLDP Tab - System

Local

Receive Status

Indicates if LLDP PDUs are being received from the remote device.

TLVs Included

Indicates what TLVs are included.

Select an entry in the remote window to display the specific values of the remote device.

Remote

System Description

Displays the received System Description.

Port Description

Displays the received Port Description.

Management Address

Displays the received Management Address.

Capabilities Supported

Displays the received Capabilities Supported.

Capabilities Enabled

Displays the received Capabilities Enabled.

System Data

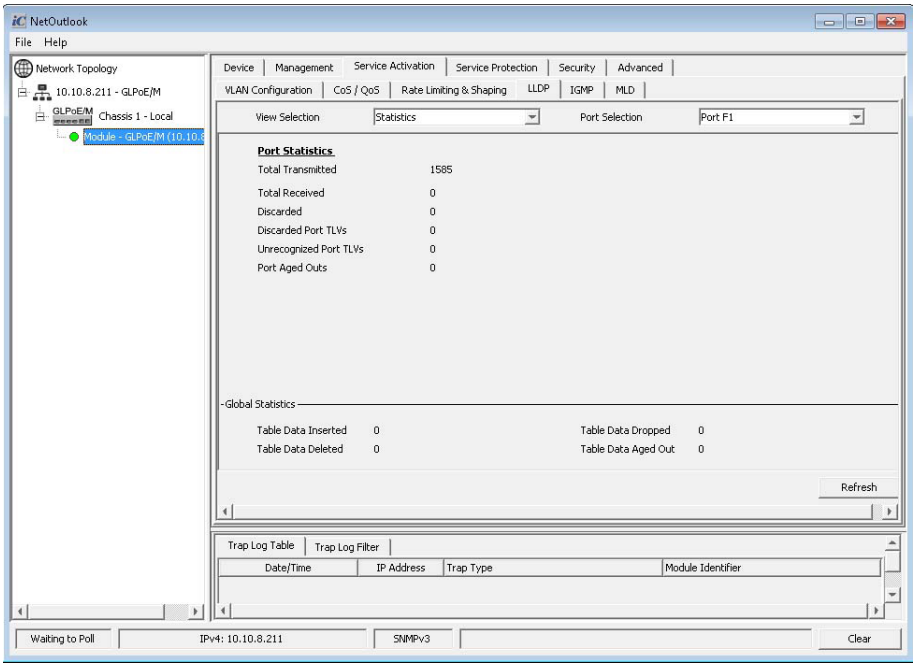
Capabilities Supported

Displays the system capabilities supported on the module.

Capabilities Enabled

Displays the system capabilities enabled on the module.

The View Selection pull-down menu to select Configuration, System or Statistics. Select Statistics.



LLDP Tab - Statistics

Global Settings

Table Data Inserted

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

Table Data Deleted

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

Table Data Dropped

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

Table Data Aged Out

Indicates the number of times the information has aged out

Port Statistics

Total Transmitted

Displays the total number of transmitted PDUs.

Total Received

Displays the total number of received PDUs.

Discarded

Displays the number of discarded PDUs.

Discarded Port TLVs

Displays the number of discarded TLV PDU.

Unrecognized Port TLVs

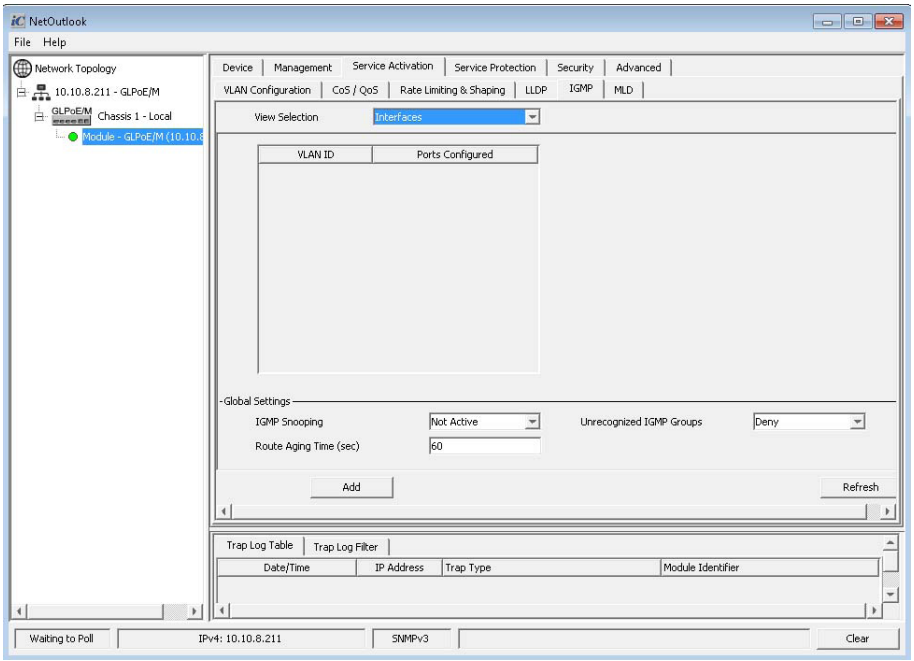
Displays the number of unrecognized TLVs.

Port Aged Outs

Displays the number of aged outs.

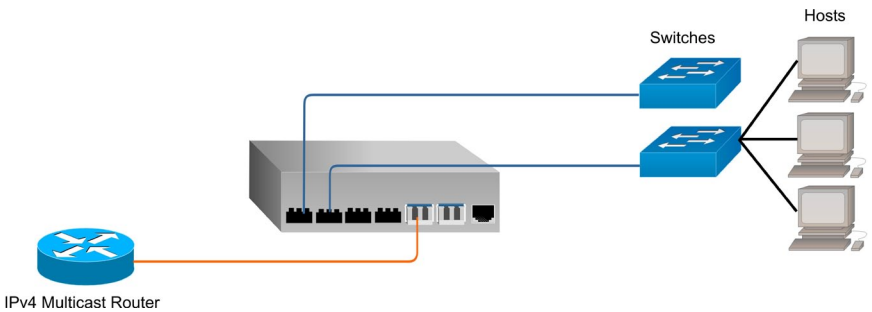
5.6.3.5 IGMP Tab

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



IGMP Tab

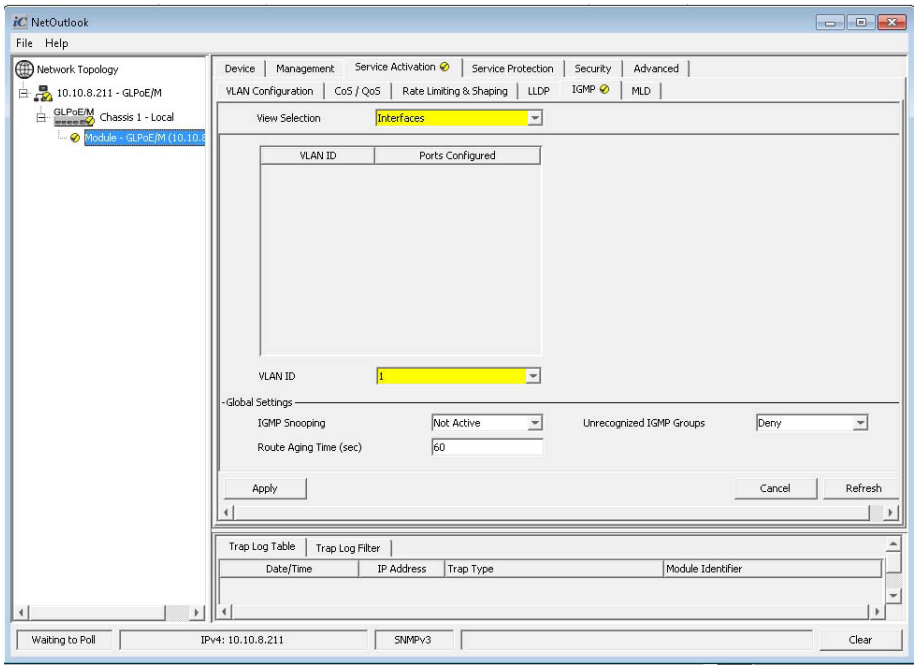
IGMPv1, v2, or v3 IPv4 snooping is based upon RFC 4541 which defines the basic operation of an IGMP snooping switch. IGMP is used to modify the default router behavior for IPv4 Multicast Packets which are flooded to all ports. IGMP provides a method for forwarding IPv4 Multicast Packets to only the ports 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 239.255.255.255 to 224.0.0.0.

Use the View Selection pull-down menu to select IGMP Interfaces or Routes. Select Interfaces.

Click the ***Add*** button to configure the IGMP Interfaces.



IGMP Tab - Add Interfaces

Global Selections

IGMP Snooping

Use the IGMP Snooping pull-down menu to globally enable (active) or disable (not Active) IGMP snooping.

Route Aging Time

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

Unrecognized IGMP Groups

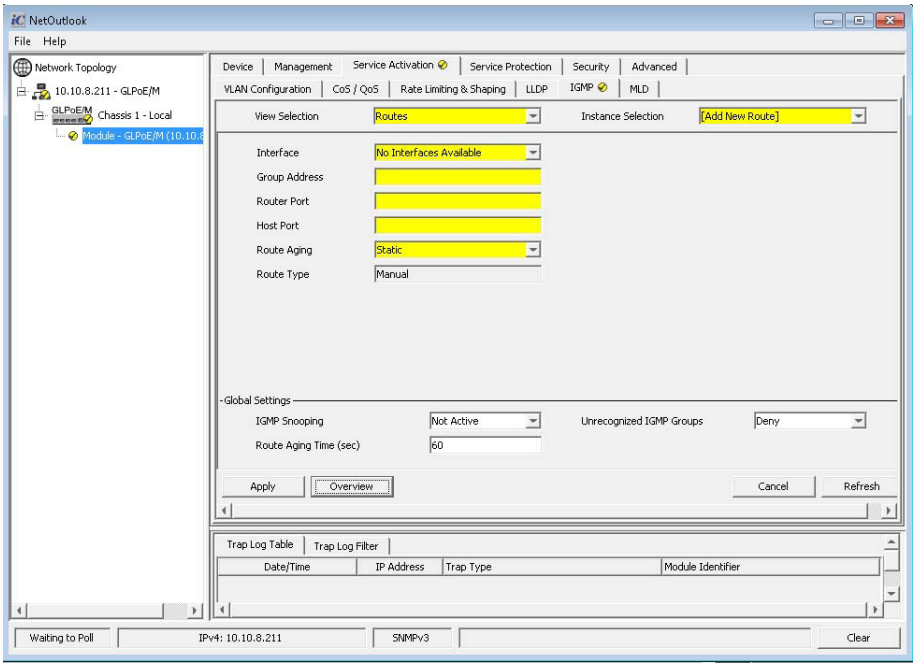
Use the Unrecognized IGMP Groups pull-down menu to configure how unrecognized IGMP groups are handled by the interface. Select Flood or Deny.

Use the VLAN ID pull-down menu to select the desired VLAN.

To save the changes, click on the ***Apply*** button.

Use the View Selection pull-down menu to select IGMP Interfaces or Routes. Select Routes.

Click the ***Add*** button to configure the IGMP Routes.



IGMP Tab - Add Routes

Interface

If multiple IGMP Interfaces were defined, use the Interface pull-down menu to select the IGMP Interface to be configured.

Group Address

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

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.

Route Aging

Use the Route Aging pull-down menu to enable (active) or disable (not Active) route aging.

Route Type

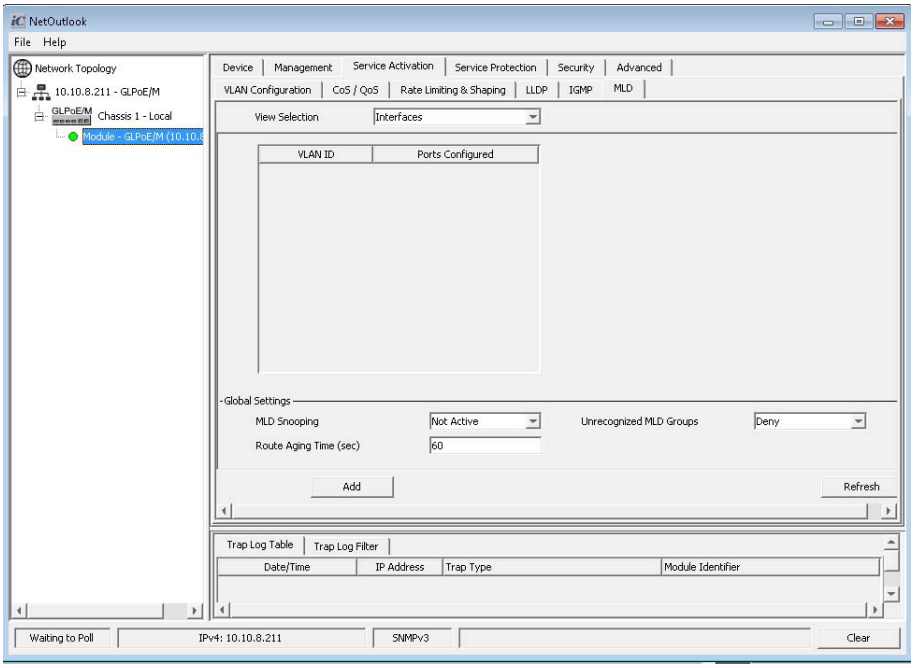
Depending how the IGMP Interface is created, the Route Type will display Manual or Auto.

To save the changes, click on the ***Apply*** button. Once the ***Apply*** button has been clicked, another IGMP instance can be configured. Click the ***Add*** button to configure another instance.

To view the configured IGMP instances, use the View Selection pull-down menu and select Overview.

5.6.3.6 MLD Tab

The MLD tab provides the ability to configure the module to support Multicast Listener Discovery (MLD) snooping



MLD Tab

Multicast Listener Discovery (MLD) snooping allows the switch to view MLD packets and make decisions based on their content. MLD uses source-based filtering, which enables hosts and routers to specify which multicast sources should be allowed or blocked for a specific multicast group.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports to forward IPv6 multicast traffic only to those ports that want to receive it.

Global Settings

MLD Snooping

Use the MLD Snooping pull-down menu to enable (active) or disable (not active) MLD Snooping.

Unrecognized MLD Groups

Use the Unrecognized MLD Groups pull-down menu to enable (active) or disable (not active) Flooding.

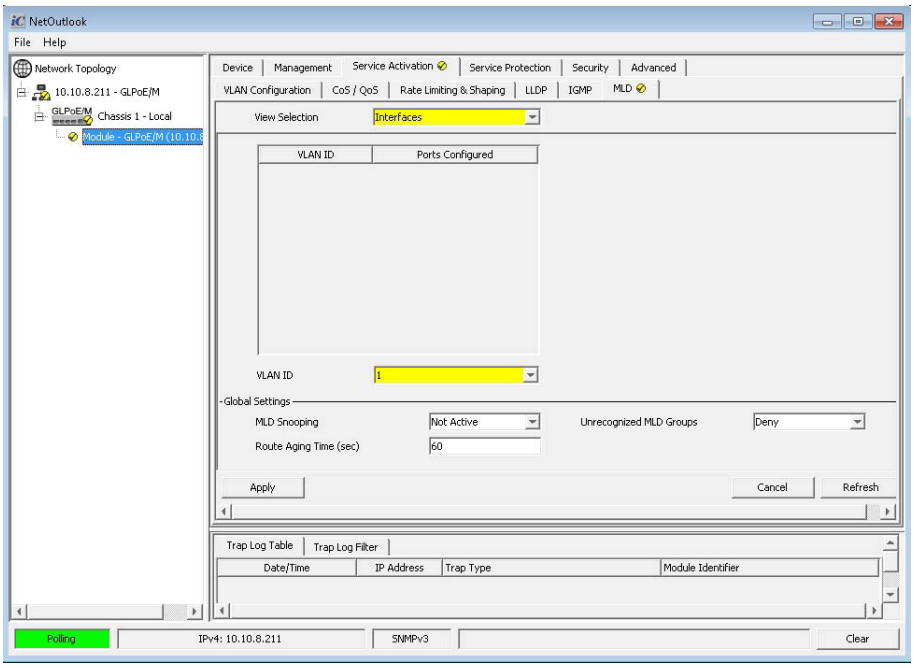
Route Aging Time (s)

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

NOTE: There are common variables that are shared between the IGMP and IPv6 MLD protocols. The variables are Snooping (enable / disable), Unrecognized Groups (enable / disabled) and Route Aging timer. If either protocol changes the shared variables, they will be changed under both protocols (IGMP and IPv6 MLD). Example: If Snooping is enabled under IPv6 MLD, Snooping will be enabled under IGMP.

Use the Selection pull-down menu to select Interfaces or Routes settings. Select Interfaces.

Click the ***Add*** button to configure the MLD Interfaces.



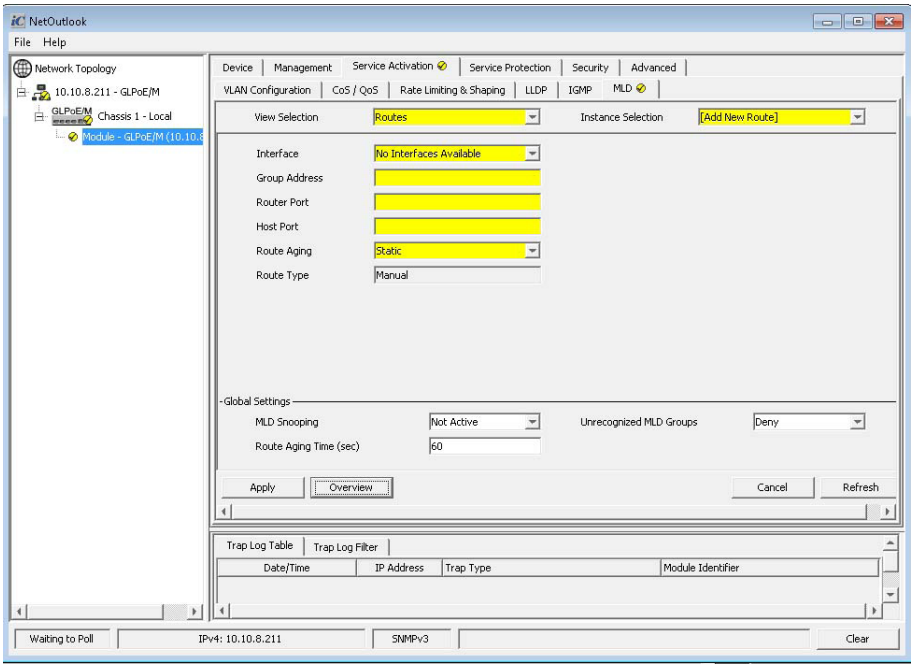
MLD Tab - Add Interface

Use the VLAN ID pull-down menu to select the desired VLAN.

To save the changes, click on the ***Apply*** button.

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

Click the ***Add*** button to configure the MLD Routes.



MLD Tab - Add Routes

Interface

Use the Interface pull-down menu to select a configured interface.

Group Address

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

Router Port

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

Host Port

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

Type

Depending how the MLD Group is created, the Type will display Manual or Auto.

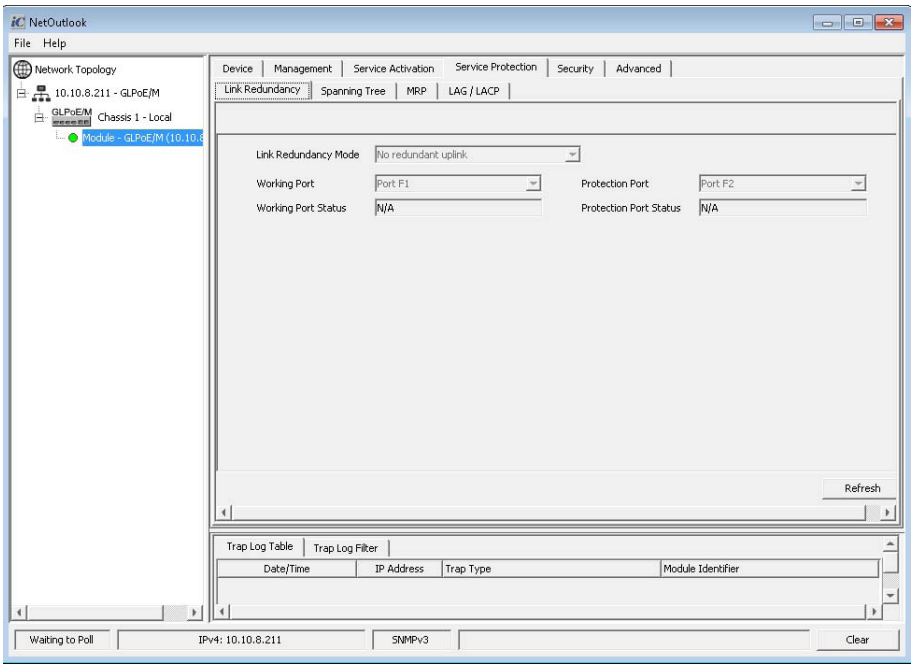
To save the changes, click on the ***Apply*** button. Once the ***Apply*** button has been clicked, another MLD group can be configured. Click the ***Add*** button to configure another group.

To view the configured MLD groups, use the View Selection pull-down menu and select Overview.

5.6.5 Service Protection Tab

The Service Protection tab provide options to configure and display different type of protection on the module. The tabs will vary depending on the module type.

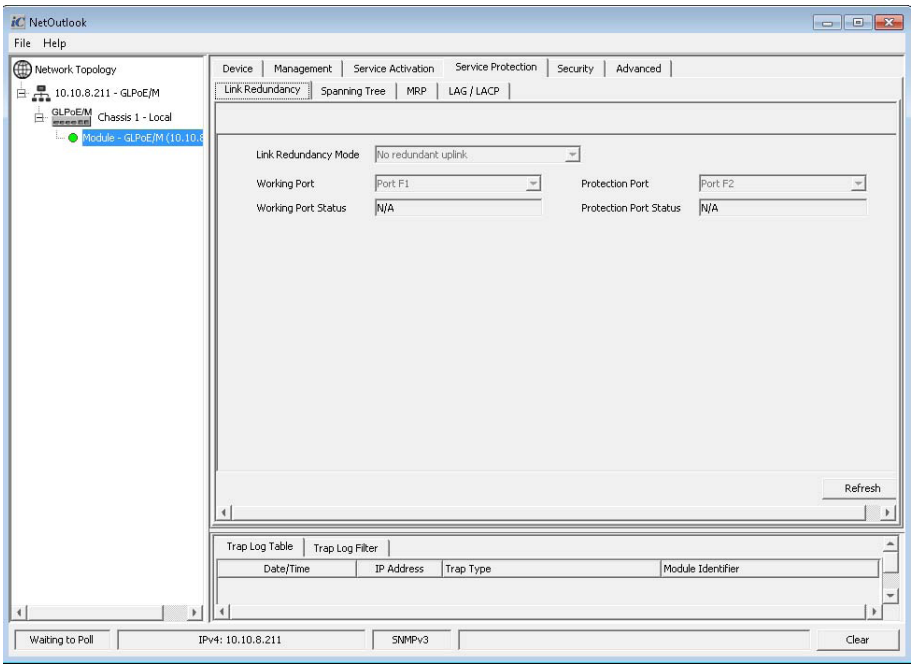
The order of tabs described in this section are: Link Redundancy, Spanning Tree, MRP and LAG/LACP.



Service Protection Tab

5.6.5.1 Link Redundancy Tab

The Link Redundancy tab provides the ability to configure the module for redundant links. When configured for link redundancy, the module will transmit and receive traffic on the working port and will not transmit and receive traffic on the protection port. When a fiber failure occurs on the working port, the module will switch over to the protection port within 50msec.



Link Redundancy Tab

Link Redundancy Mode

Use the Link Redundancy Mode pull-down menu to select No Redundancy, Redundancy with No Return to Primary or Redundancy with Return to Primary.

Working Port

Use the Working Port pull-down menu to select the working (primary) port.

Working Port Status

Displays the status of the port: Standby (Blocked) or Active (Forwarding)

Protection Port

Use the Protection Port pull-down menu to select the working (primary) port.

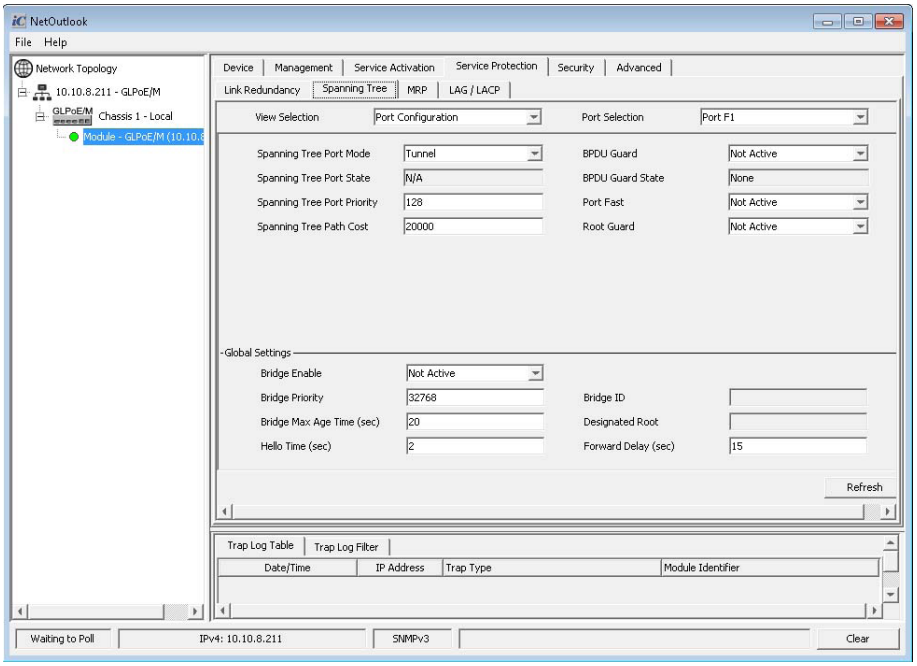
Protection Port Status

Displays the status of the port: Standby (Blocked) or Active (Forwarding)

To save the changes, click on the ***Apply*** button.

5.6.5.2 Spanning Tree Tab

The Spanning Tree tab provides the ability to configure Multiple Spanning Tree Protocol (MSTP).



Spanning Tree Tab

Multiple Spanning Tree Protocol (MSTP) is a protocol that creates multiple spanning trees (instances) for each VLAN. This allows each VLAN to be configured with a root bridge and forwarding topology.

Use the View Selection pull-down menu to select Port Configuration or MSTP Configuration. Select Port Configuration.

Use the Port Selection pull-down menu to select the port for the spanning tree configuration.

Port Configuration

Spanning Tree Port Mode

Use the Spanning Tree Port Mode pull-down menu to select the protocol for the port (Discard, MSTP, RSTP or Tunnel).

Discard	RSTP/MSTP protocols are disabled.
MSTP	MSTP is enabled and the protocol is operating.
RSTP	RSTP is enabled and the protocol is operating.
Tunnel	RSTP/MSTP protocols are disabled. BPDU frames are tunneled.

Spanning Tree Port State

Displays the Spanning Tree 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

Spanning Tree 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.

Spanning Tree 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.

BPDU Guard

BPDU Guard is used to protect the Spanning Tree Topology from BPDU related attacks. BPDU Guard must be enabled on a port that should never receive a BPDU from the connected device.

Use the BPDU Guard pull-down menu to enable (active) or disable (not active) BPDU Guard.

BPDU Guard State

Displays the BPDU guard state of the port.

Port Fast

Port Fast allows ports to enter a forwarding state in four seconds. Port Fast allows faster convergence on ports that are attached to end stations and do not present the potential to cause forwarding loops.

Use the Port Fast pull-down menu to enable (active) or disable (not active) Port Fast.

Root Guard

Root Guard ensures that the port on which root guard is enabled is the designated port.

Use the Root Guard pull-down menu to enable (active) or disable (not active) Root Guard.

Global Settings

Bridge Enable

Use the Bridge Enable pull-down menu to enable (active) or disable (not active) Spanning Tree.

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.

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.

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.

Bridge ID

The Bridge ID is displayed.

Designated Root

The designated root is displayed.

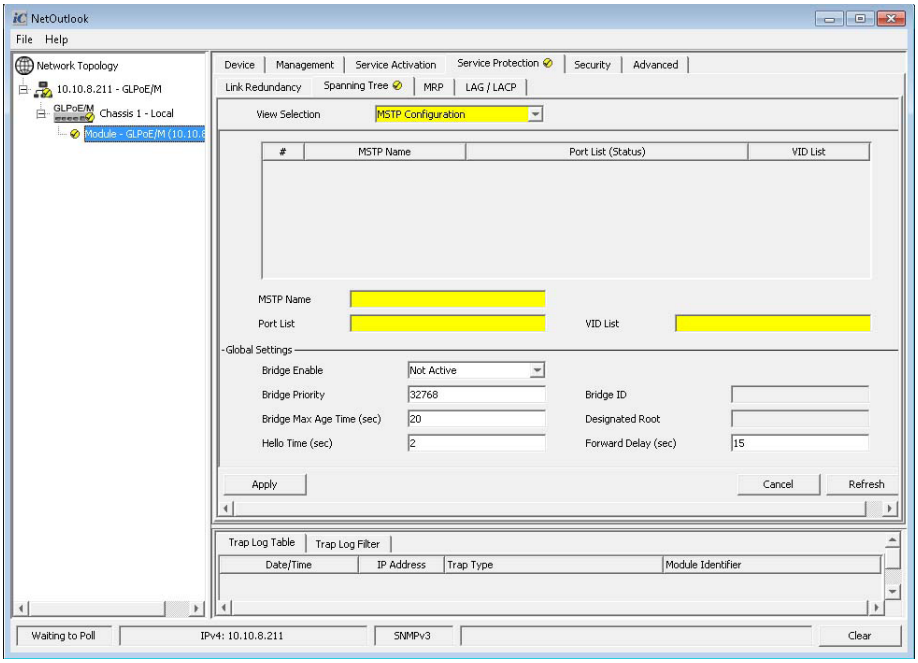
Forward Delay (s)

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.

To save the changes, click on the ***Apply*** button.

Use the View Selection pull-down menu to select Port Configuration or MSTP Configuration. Select MSTP Configuration.

Click the ***Add*** button to configure the MSTP instance.



Spanning Tree Tab - MSTP Configuration

MSTP Name

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

Port List

Enter the ports associated with the MSTP instance in the text box.

Port Status

The port status will be displayed.

VID List

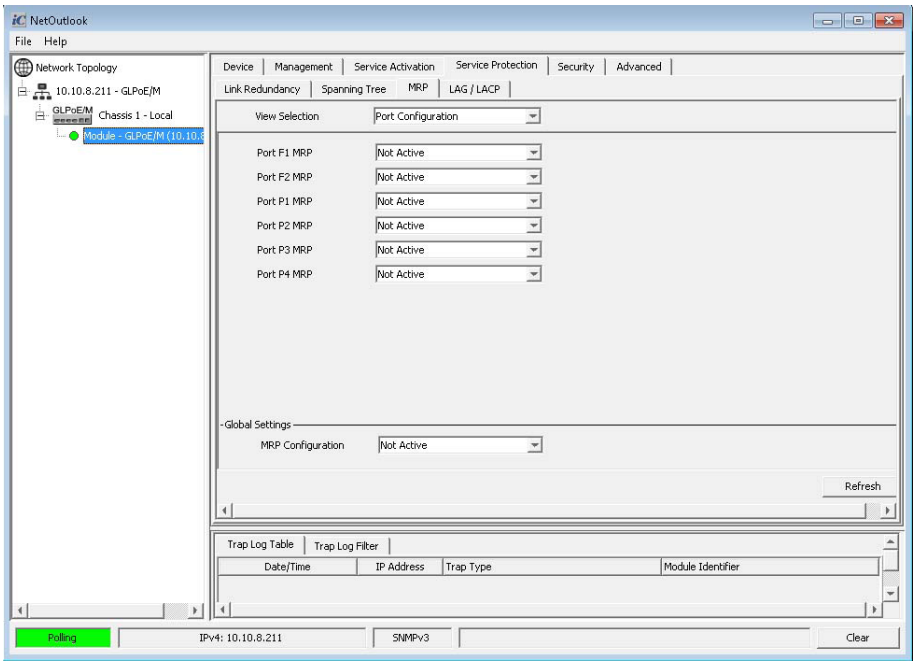
Enter the VIDs associated with the MSTP instance in the text box.

To save the changes, click on the ***Apply*** button.

5.6.5.3 MRP Tab

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

Use the View Selection pull-down menu to select Port Configuration or MRP Configuration. Select Port Configuration.



MRP Tab

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. 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. 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.

Use the Port MRP pull--down menu to enable (active) or disable (not active) MRP on the port.

Global Settings

MRP Configuration

Use the MRP Configuration pull-down menu to globally enable (active) or disable (not active) MRP on the module.

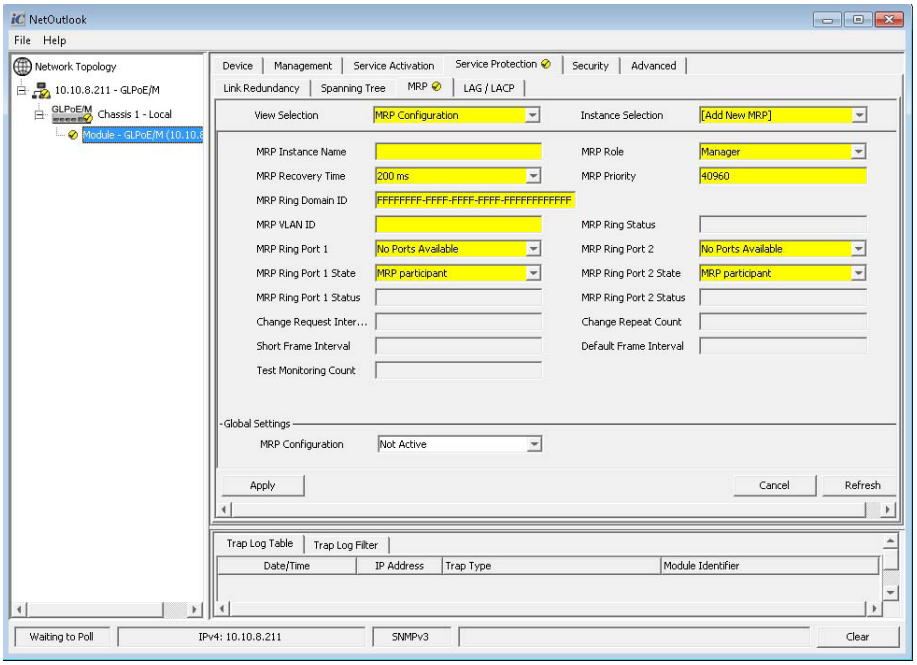
Port Configuration

The number of ports will vary depending on the model.

To save the changes, click on the ***Apply*** button.

Use the View Selection pull-down menu to select Port Configuration or MRP Configuration. Select MRP Configuration.

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



MRP Tab - MRP Configuration

MRP Instance Name

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

MRP Recovery Time

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

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-FFFFFFFFFFFE. The default value is 0xFFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF.

Enter the MRP Ring Domain ID in the text box.

MRP 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.

MRP Ring Port 1

Use the MRP 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.

MRP Ring Port 1 State

Use the MRP Ring Port 1 State pull-down menu to select MRP Participate or Block Traffic.

MRP Ring Port 1 Status

The MRP Ring Port 1 Status displays the status of the ring port; MRP Participate or Block Traffic. The MRP Protocol will block traffic automatically on one of the ports.

Change Request Interval

Displays the change request interval.

Short Frame Interval

Displays the short frame interval.

Test Monitoring Count

Displays the test monitoring count.

MRP Role

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

MRP Priority

MRP Priority option is only available when the MRP Role is configured as Manger (MRM).

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

MRP Ring Status

The status of the MRP Ring is displayed

MRP Ring Port 2

Use the MRP 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.

MRP Ring Port 2 State

Use the MRP Ring Port 2 State pull-down menu to select MRP Participate or Block Traffic.

MRP Ring Port 2 Status

The MRP Ring Port 2 Status displays the status of the ring port; MRP Participate or Block Traffic. The MRP Protocol will block traffic automatically on one of the ports.

Change Repeat Count

Displays the change repeat count.

Default Frame Interval

Displays the default frame interval.

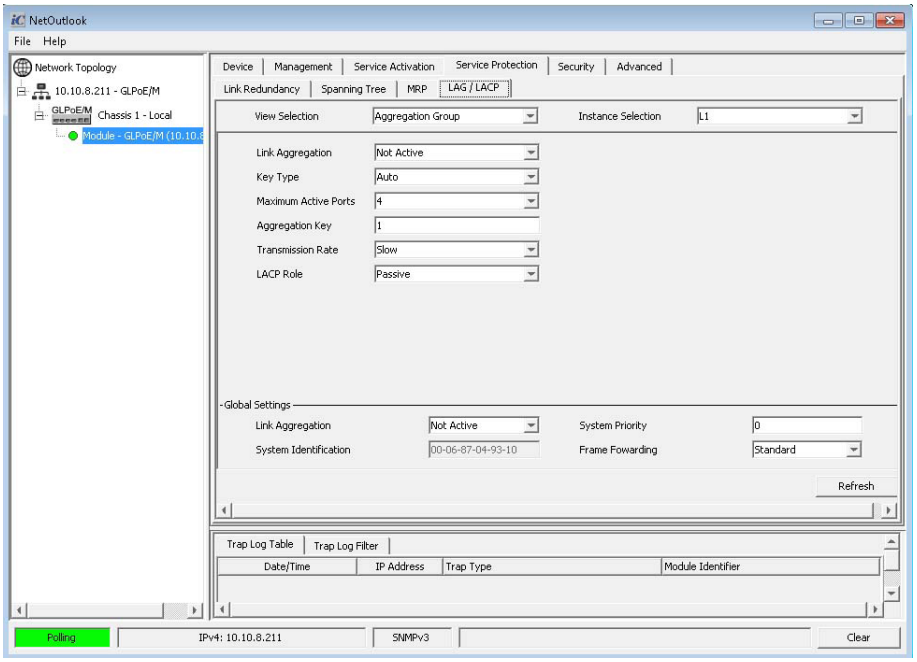
To save the changes, click on the ***Apply*** button.

5.6.5.4 LAG / LACP Tab

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

Use the View Selection to select Aggregation Group, Port Configuration or Port Statistics. Select Aggregation Group.

Use the Instance Selection to select the logical port number for a Link Aggregation Group.



LAG / LACP Tab

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.

Aggregation Group

Link Aggregation

Use the Link Aggregation pull-down menu to enable (active) or disable (not active) LAG on the selected logical port number.

Key Type

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

Maximum Active Ports

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

Aggregation Key

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

Transmission Rate

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

LACP Role

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

Global Settings

Link Aggregation

Use the Link Aggregation pull-down menu to enable (active) or disable (not active) Link Agregation on the module.

System Identification

Displays the System Identification (MAC address).

System Priority

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

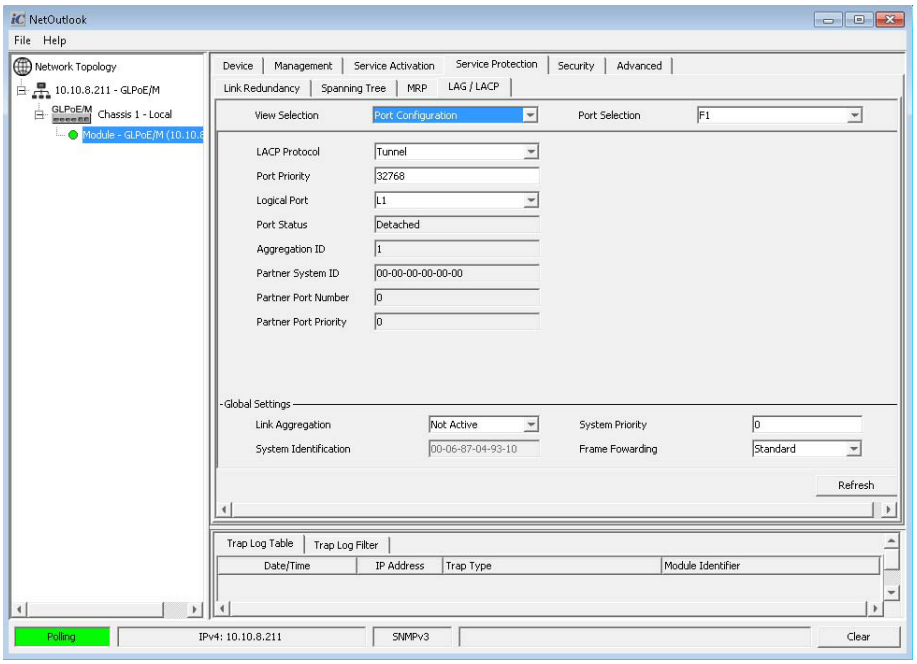
Frame Forwarding

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

To save the changes, click on the ***Apply*** button.

Use the View Selection pull-down menu to select Aggregation Group, Port Configuration or Port Statistics. Select Port Configuration.

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



LAG / LACP Tab - Port Configuration Option

LACP Protocol

Use the LACP Protocol pull-down menu to configure the LACP protocol for Discard, Peer, Static or Tunnel on the selected port.

NOTE: Ports 1-4 do not support Static LAG manual configuration, also known as no LACP LAG.

Port Priority

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

Logical Port

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

Port Status

Displays the port status as Detached or Attached.

Aggregation ID

Displays the Aggregation ID.

Partner System ID

Displays the partner system ID.

Partner Port Number

Displays the partner port number.

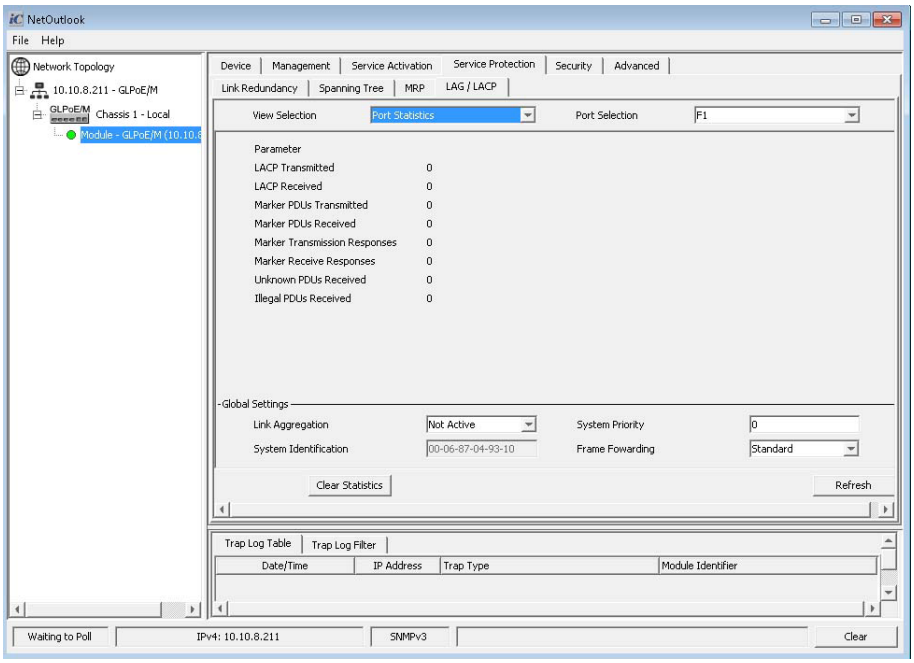
Partner Port Priority

Displays the partner port priority.

To save the changes, click on the ***Apply*** button.

Use the View Selection pull-down menu to select Aggregation Group, Port Configuration or Port Statistics. Select Port Statistics.

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



LAG / LACP Tab - Port Statistics Option

LACP Transmitted

Displays the number of LACP PDU transmitted.

LACP Received

Displays the number of LACP PDU received.

Marker PDUs Transmitted

Displays the number of Marker PDU transmitted.

Marker PDUs Received

Displays the number of Marker PDU received.

Marker Transmission Responses

Displays the number of transmitted Marker responses.

Marker Receive Responses

Displays the number of received Marker responses.

Unknown PDUs Received

Displays the number of unknown PDUs received.

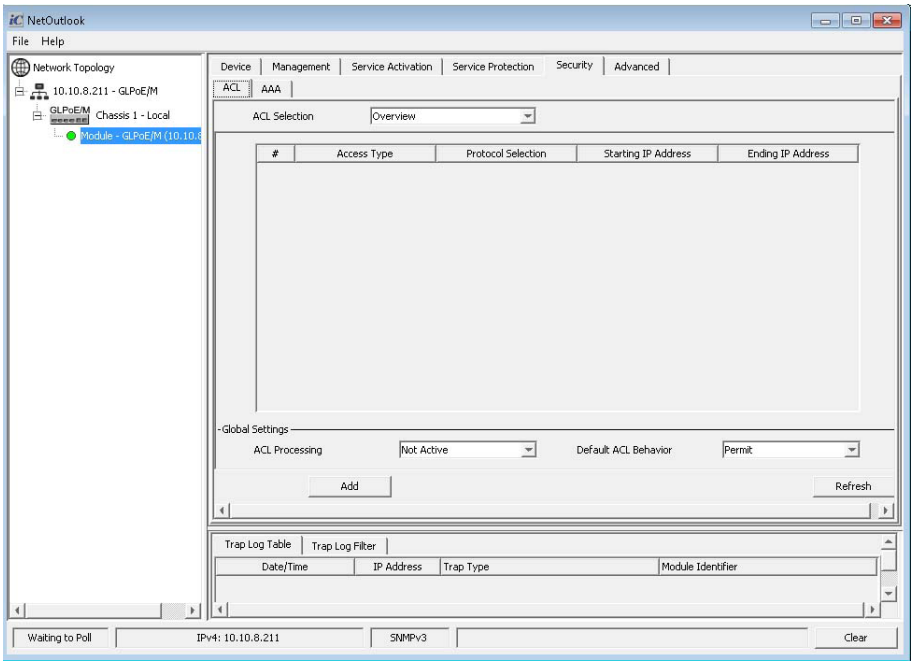
Illegal PDUs Received

Displays the number of illegal PDUs received.

The ***Clear Statistics*** button clears the statistics.

5.6.6 Security Tab

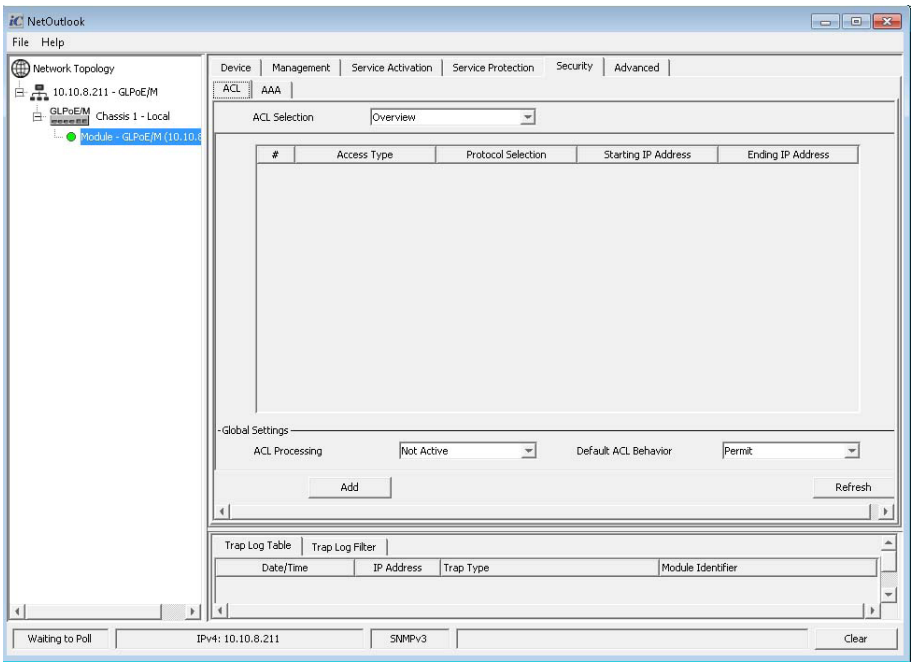
The Security tab provides the ability to configure and display Access Control List (ACL), Authentication, Authorization and Accounting (AAA), Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+) and Port Based Network Access Control (IEEE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



Security Tab

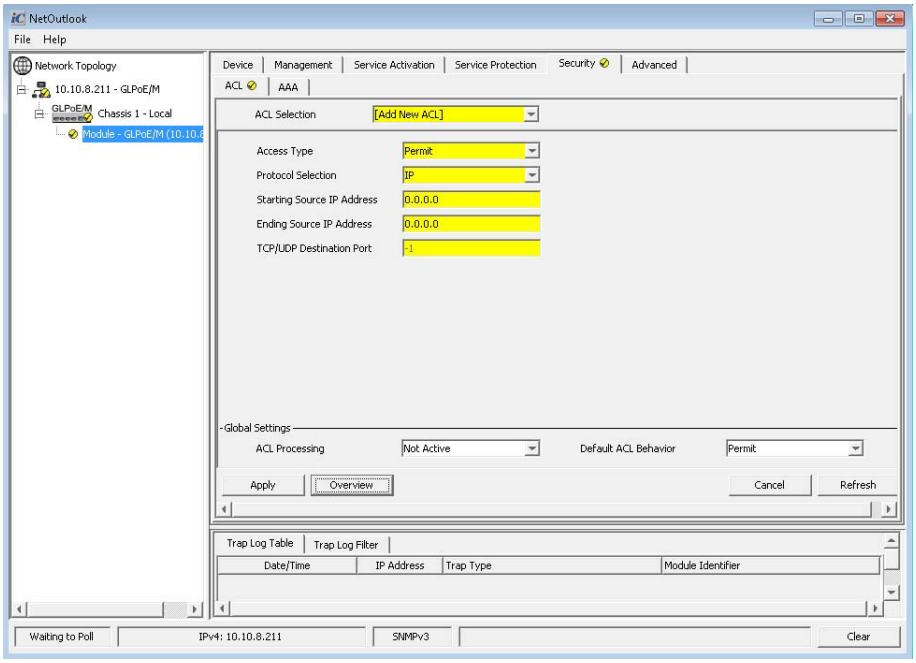
5.6.6.1 ACL Tab

The ACL tab provides basic traffic filtering capabilities with Access Control Lists (ACL). 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. Two hundred individual ACLs can be configured at one time.



ACL Tab

To configure an ACL, click on the ***Add*** button.



ACL Tab - Add ACL

Access Type

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

Protocol Selection

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

Starting Source IP Address

Enter the starting source IP Address in the text box.

Ending Source IP Address

Enter the ending source IP Address in the text box.

TCP/UDP Destination Port

Enter the destination port number in the text box.

Global Settings

ACL Processing

Use the ACL Processing pull-down menu to globally enable (active) or disable (not active) ACL processing.

Default ACL Behavior

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

Use the ACL Selection pull-down menu to select one of the configured or [Add New ACL] ACLs.

To save the changes, click on the ***Apply*** button.

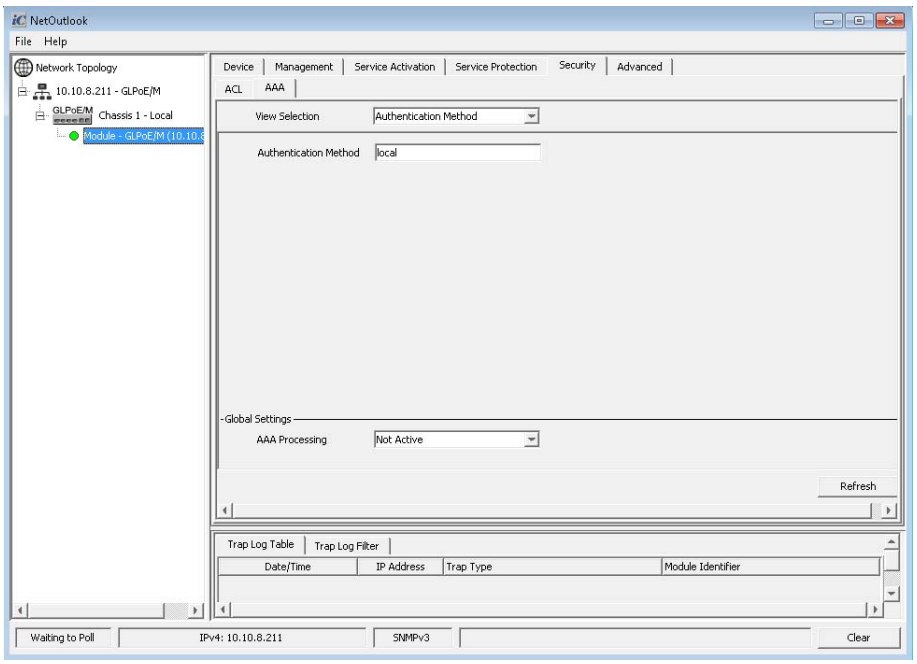
To delete the configured ACL, click the ***Delete*** button.

To delete all ACL instances, click the ***Delete All*** button.

To add another ACL, click the ***Add*** button.

5.6.6.2 AAA Tab

The AAA tab 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).



AAA Tab

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

Authentication Method

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

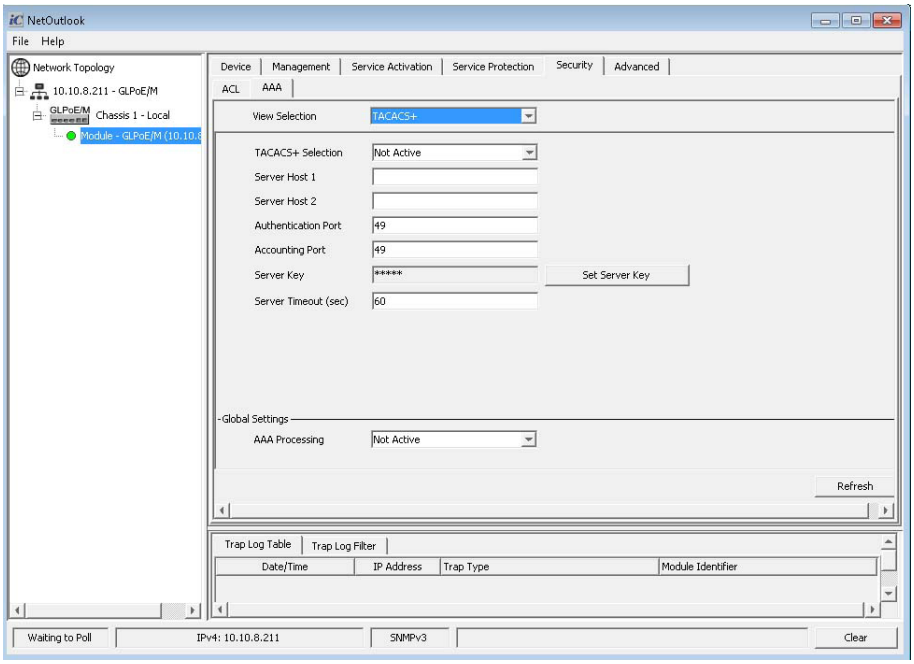
Global Settings

AAA Processing

Use the AAA Processing pull-down menu to enable (active) or disable (not active) AAA.

To save the changes, click on the ***Apply*** button.

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



AAA Tab - TACACS+

TACACS+ Selection

Use the TACACS+ Selection pull-down menu to enable (active) or disable (not active) TACACS+.

Server Host 1

Enter the IP Addresses of the TACACS+ servers host 1 in the text box.

Server Host 2

Enter the IP Addresses of the TACACS+ servers host 2 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

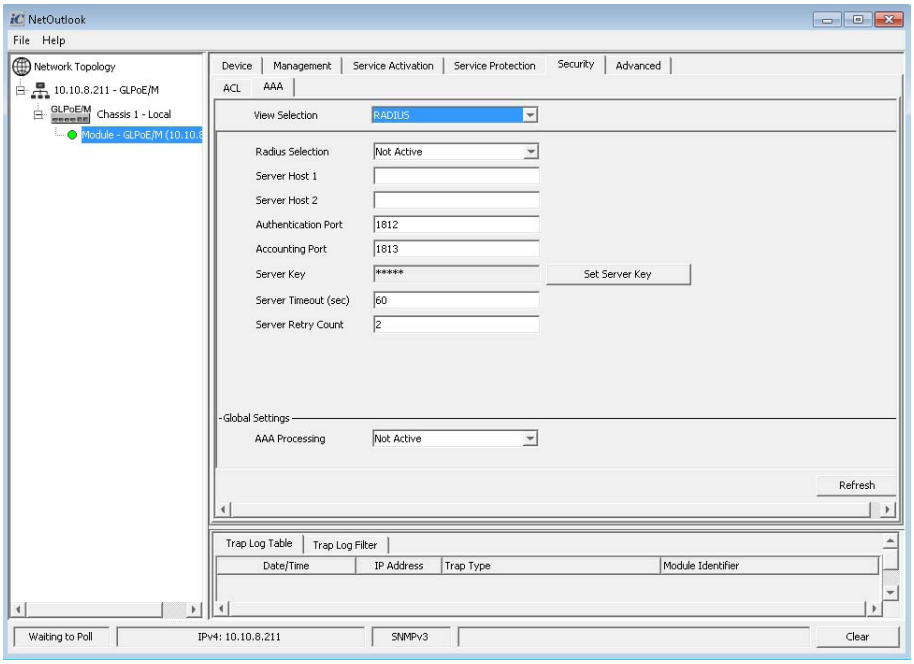
Click the ***Set Server Key*** button to configure the key. A TACACS+ Server Key dialog box is displayed. Enter the new Server Key and confirm the entry.

Server Timeout (sec)

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

To save the changes, click on the ***Apply*** button.

Use the View Selection pull-down menu to select authentication method or type of authentication as Authentication Method, TACACS+, RADIUS or Port Authentication (802.1x). Select RADIUS.



AAA Tab - RADIUS

RADIUS Selection

Use the RADIUS Selection pull-down menu to enable (active) or disable (not active) RADIUS.

Server Host 1

Enter the IP Addresses of the RADIUS servers host 1 in the text box.

Server Host 2

Enter the IP Addresses of the RADIUS servers host 2 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 1812.

Server Key

Click the ***Set Server Key*** button to configure the key. A RADIUS Server Key dialog box is displayed. Enter the new Server Key and confirm the entry.

Server Timeout (sec)

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

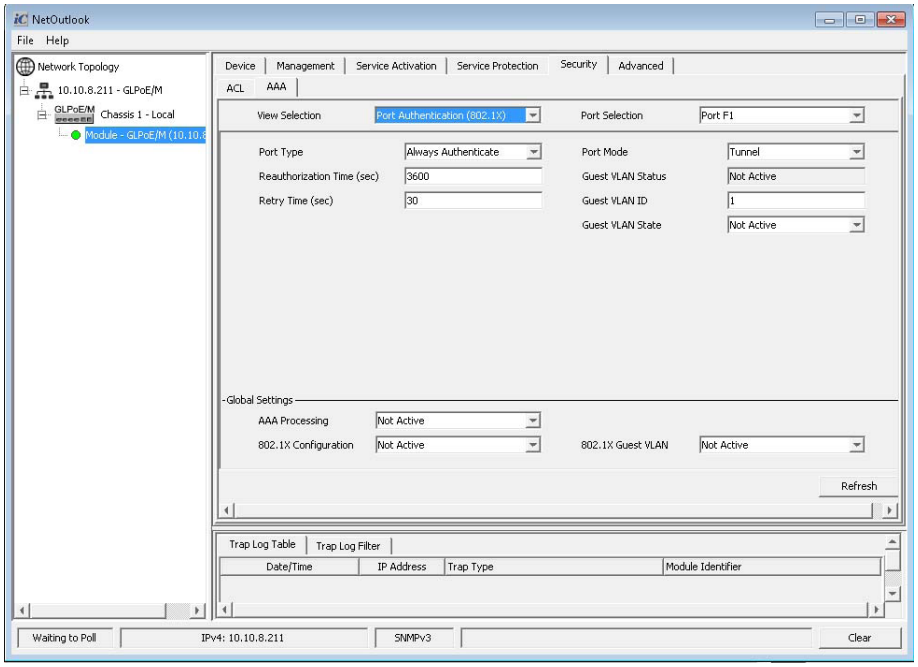
Server Retry Count

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

To save the changes, click on the ***Apply*** button.

Use the View Selection pull-down menu to select authentication method or type of authentication as Authentication Method, TACACS+, RADIUS or Port Authentication (802.1x). Select Port Authentication.

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



AAA Tab - Port Authentication

Port Type

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

Always Authenticate	Port is always authorized, 802.1X disabled.
Automatic	Standard 802.1X authentication on a port.
Always Unauthorized	Port is always unauthorized.
Mac Bypass	802.1X MAC bypass authentication on a port.

Reauthorize Time (s)

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

Retry Time (s)

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

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.

Guest VLAN Status

The Guest VLAN Status is displayed.

Guest VLAN ID

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

Guest VLAN State

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

Global Settings

AAA Processing

Use the AAA Processing pull-down menu to enable (active) or disable (not active) AAA.

802.1x Configuration

Use the 802.1x Configuration pull-down menu to enable (active) or disable (not active) 802.1x processing.

802.1x Guest VLAN

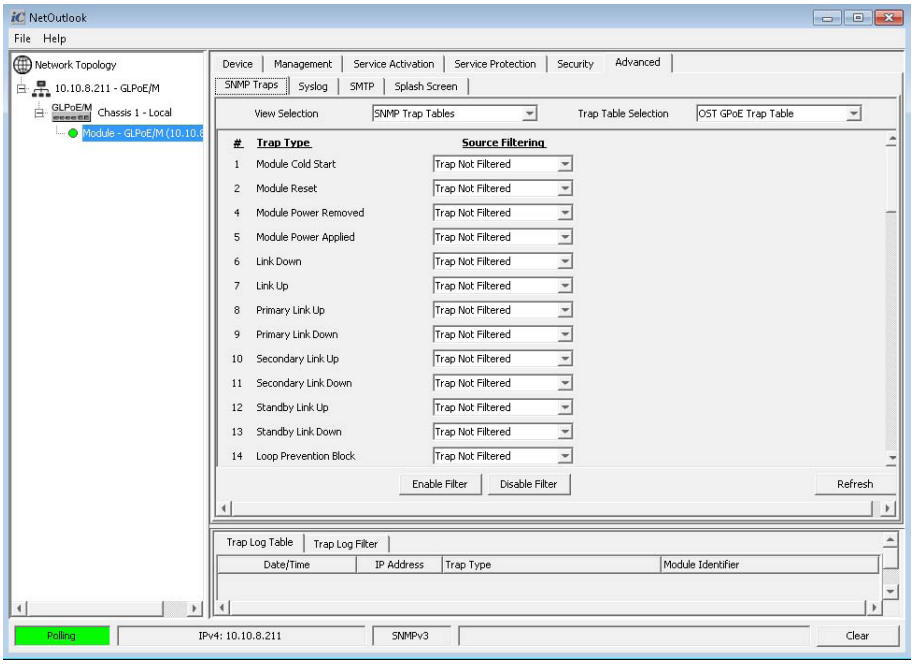
Use the 802.1x Guest VLAN pull-down menu to enable (active) or disable (not active) Guest VLAN.

To save the changes, click on the ***Apply*** button.

5.6.7 Advanced Tab

The Advanced tab provides a second row of tabular options to configure and display information on the specific module type.

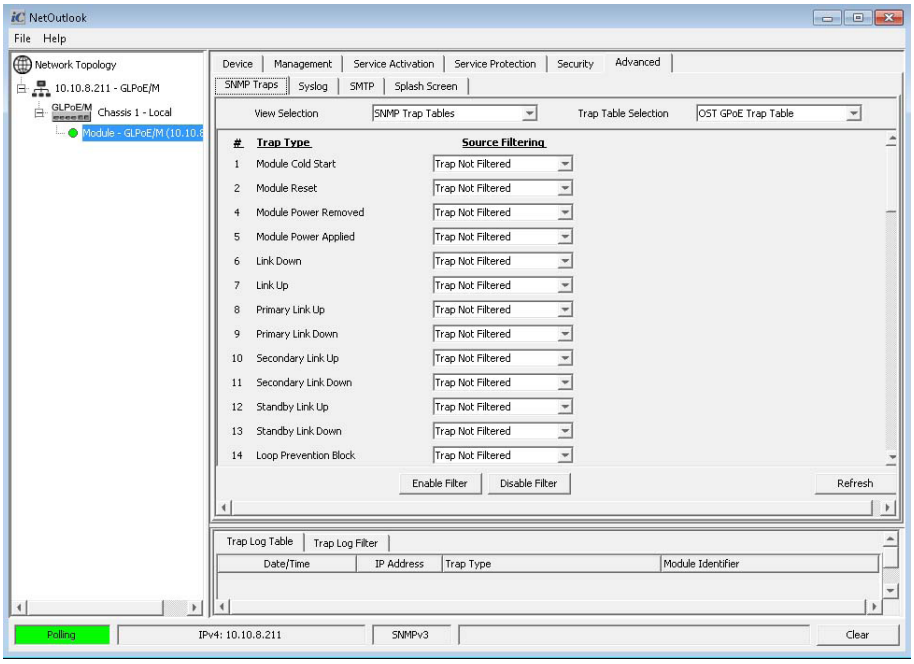
The order of tabs described in this section are: SNMP Traps, Syslog SMTP and Splash Screen.



Advanced Tab

5.6.7.1 SNMP Traps Tab

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



Advanced Tab - SNMP Traps

Use the View Selection pull-down menu to select SNMP Trap Table.

Use the Trap Table Selection to select OST GPoE Trap Table.

The SNMP Trap Table provides a list of traps that can be generated by the module. Each individual trap can be enabled (Trap Filtered) or disabled (Trap Not Filtered) by using the pull-down menu next to each trap type.

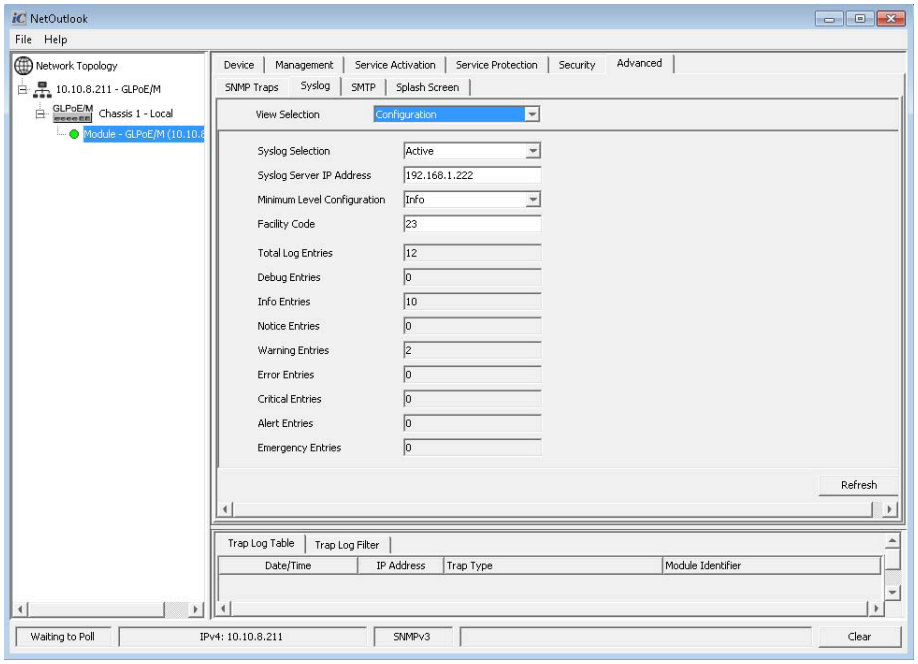
Once a change has been made, use the ***Apply*** button to save the changes.

Use the ***Enable Filter*** button to enable (Trap Filtered) for all trap types.

Use the ***Disable Filter*** button to disable (Trap Not Filtered) for all trap type.

5.6.7.2 Syslog Tab

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



Syslog Tab

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 View Selection pull-down menu to select Configuration or Syslog Table. Select Configuration.

Syslog Selection

Use the Syslog Selection pull-down menu to select enable (active) or disable (inactive) syslog functionality.

Syslog Server IP Address

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

Minimum Level Configuration

Use the Minimum Level Configuration 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

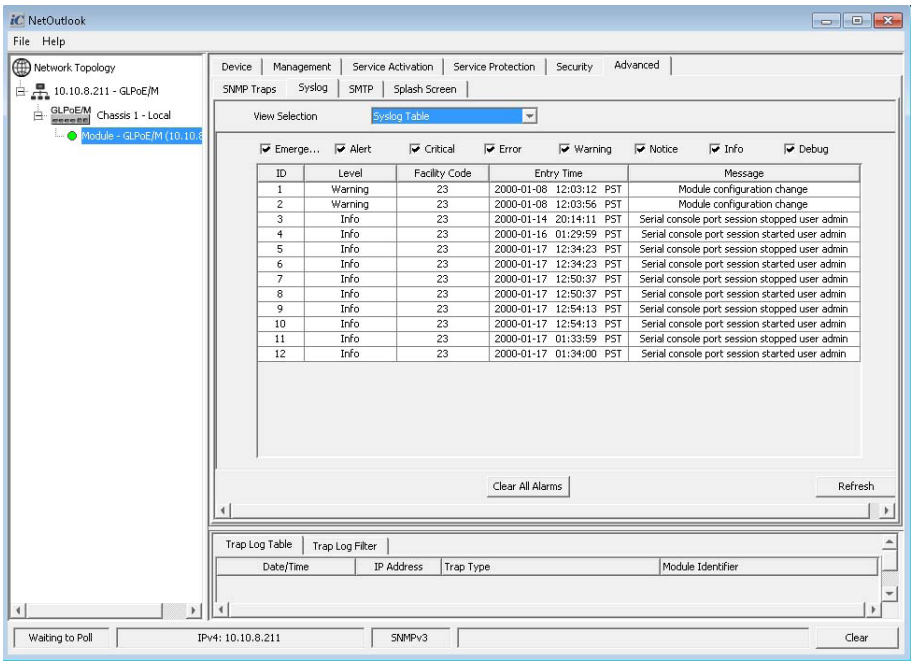
A facility code is used to specify the type of program that is logging the message. Enter the Facility code in the text box.

Entries

The status of the different entries are displayed.

To save the changes, click on the ***Apply*** button.

Use the View Selection pull-down menu to select Configuration or Syslog Table. Select Syslog Table.



Syslog Tab - Syslog Table

The Syslog Table displays the number of each severity level at has been received.

The Syslog Table also displays each message with ID, Level, Facility Code, Entry Time and Message.

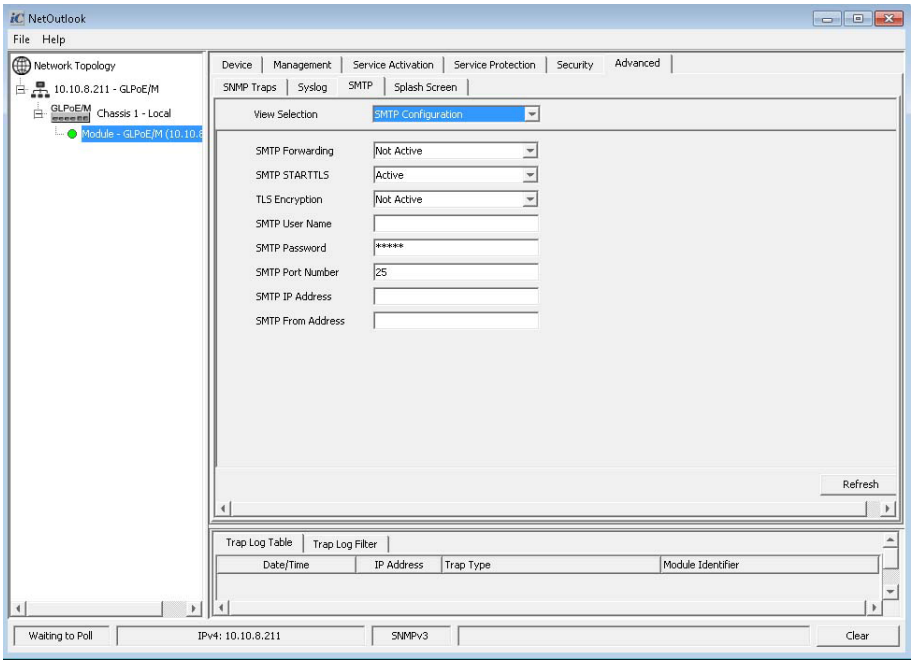
The severity level displayed in the log is based on which severity boxes are checked boxes.

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

The module retains the last 1000 entries.

5.6.7.3 SMTP Tab

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



SMTP Tab

Simple Mail Transfer Protocol (SMTP) uses a combination of STARTTLS and Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt the mail. STARTTLS is a protocol command used to inform the email server that the email client wants to upgrade from an insecure connection to a secure one using TLS or SSL.

Use the Selection pull-down menu to select SMTP Configuration or SMTP Recipients. Select SMTP Configuration.

SMTP Forwarding

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

SMTP STARTTLS

Use the SMTP STARTTLS pull-down menu to Enable or Disable STARTTLS.

TLS Encryption

Use the TLS Encryption pull-down menu to Enable or Disable TLS Encryption.

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.

SMTP IP Address

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

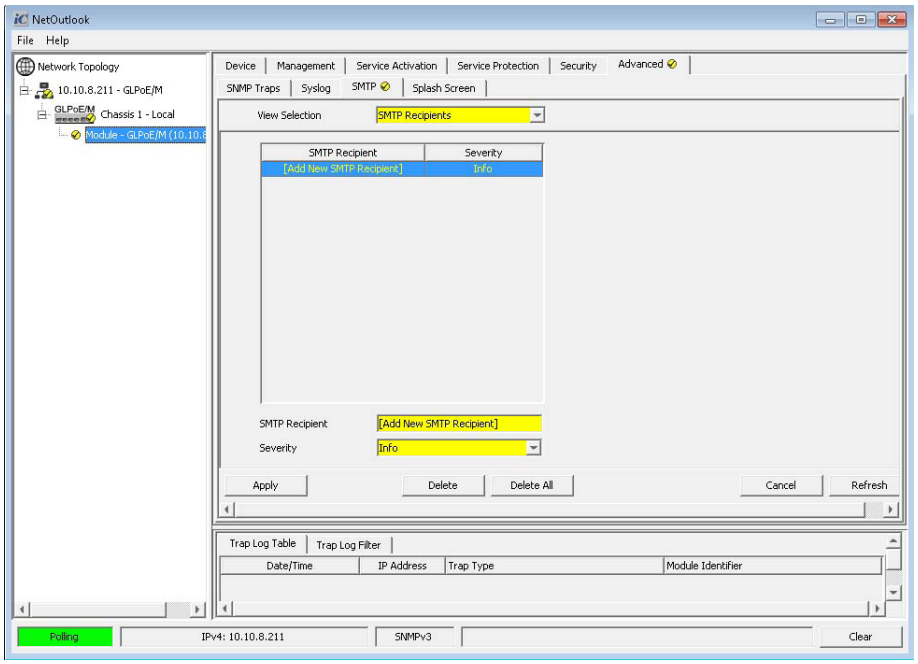
SMTP From Address

Enter the email address of the person the messages are from in the text box.

To save the changes, click on the ***Apply*** button.

Use the Selection pull-down menu to select SMTP Configuration or SMTP Recipients. Select SMTP Recipients.

Click the ***Add*** button to configure the recipients.



SMTP Tab - Configure Recipients

SMTP Recipients

Enter the email address of the recipient of the messages in the text box.

Security

Use the Security 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 ***Apply*** button to add the new recipient. Once the ***Apply*** button has been clicked, a new entry will be displayed.

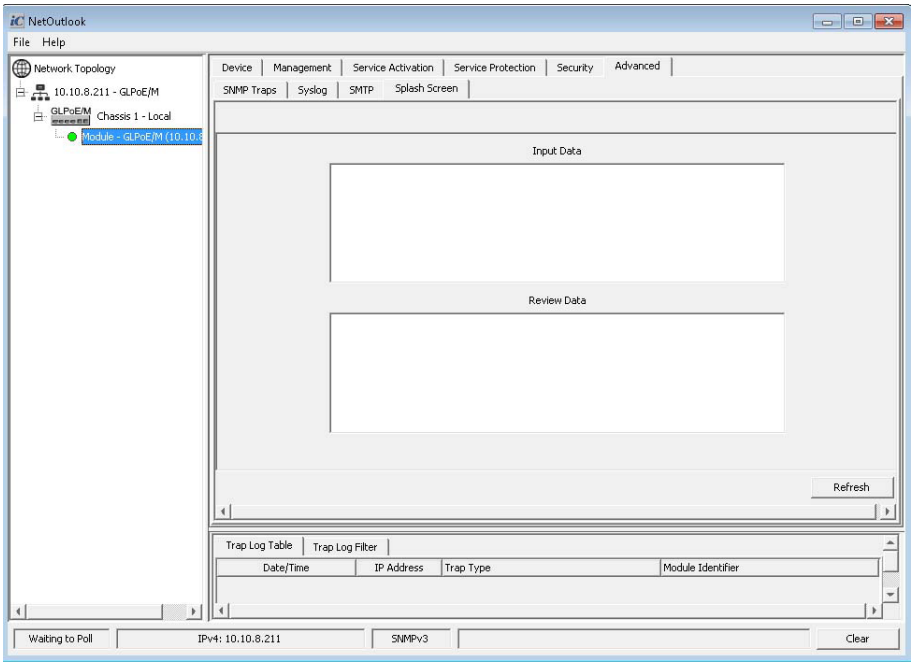
To save the changes, click on the ***Apply*** button.

Click the ***Delete*** button to delete the selected entries.

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

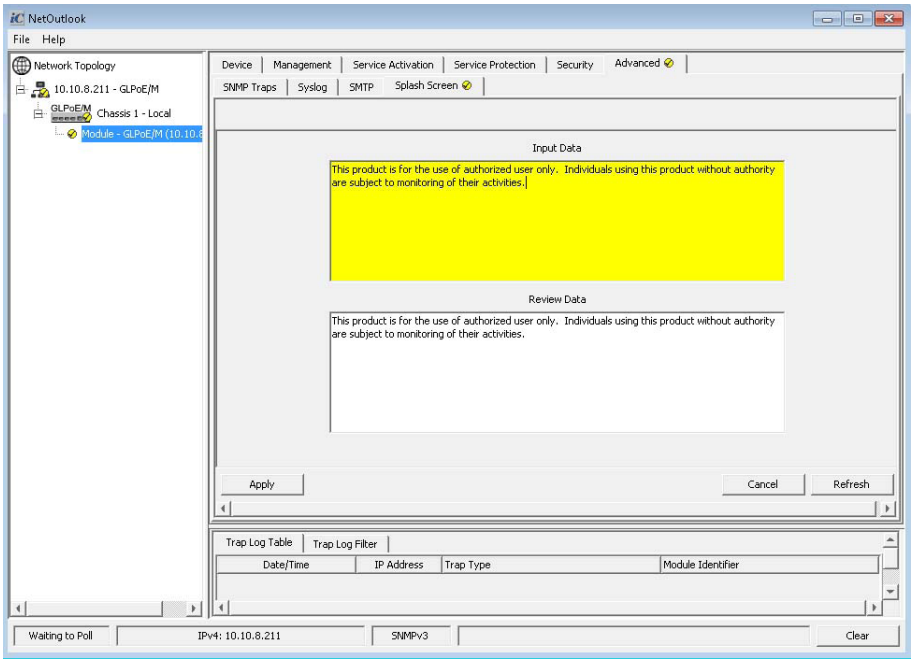
5.6.7.4 Splash Screen Tab

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.



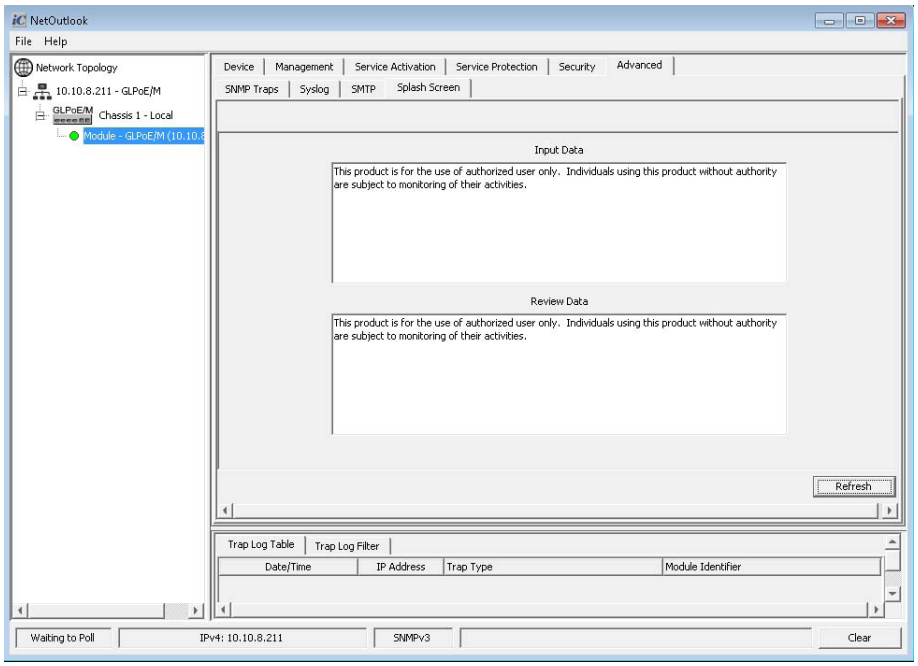
Splash Screen Tab

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



Splash Screen Tab - with Entry

To save the changes, click on the ***Apply*** button.



Splash Screen Tab - with Entry

6.0 APPENDIX B: DIP-SWITCH DEFINITIONS

Each managed and management module has DIP-Switches available to configure specific functions on the module. The following information is provided to outline the functions on each module.

6.1 OmniConverter Switches - DIP-Switches

6.1.1 GL/M Switch

Switch Mode

The module operates as a standard layer 2 switch. Data flow will follow MAC address mapping.

Directed Switch Mode

Data traffic from SPE ports are only forwarded to the uplink port F1, preventing the broadcast traffic from flooding other network ports. Incoming traffic from F1 follows MAC address mapping.

Dual Device Mode)

The module is configured as two logically independent Layer 2 switches.

Port F1 to Ports 1 and 2 and Port F2 to Ports 3 and 4.

Fiber Redundancy

Enables Port F1/F2 redundancy; Normal, Redundant No Return, Redundant Return.

MAC Learning

Enables or disables MAC learning.

6.1.2 GLPoE/M Switch

Switch Mode

The module operates as a standard layer 2 switch. Data flow will follow MAC address mapping.

Directed Switch Mode

Data traffic from SPE ports are only forwarded to the uplink port F1, preventing the broadcast traffic from flooding other network ports. Incoming traffic from F1 follows MAC address mapping.

Dual Device Mode)

The module is configured as two logically independent Layer 2 switches.

Port F1 to Ports 1 and 2 and Port F2 to Ports 3 and 4.

Fiber Redundancy

Enables Port F1/F2 redundancy; Normal, Redundant No Return, Redundant Return.

MAC Learning

Enables or disables MAC learning.

SPoE Reset

Enable or disable PSE reset. When enabled, the PoE output power will be removed for 5 seconds after a loss of receive link on any uplink port.

6.2 RuggedNet Switches - DIP-Switches

6.2.1 GL/Mi Switch

Switch Mode

The module operates as a standard layer 2 switch. Data flow will follow MAC address mapping.

Directed Switch Mode

Data traffic from SPE ports are only forwarded to the uplink port F1, preventing the broadcast traffic from flooding other network ports. Incoming traffic from F1 follows MAC address mapping.

Dual Device Mode

The module is configured as two logically independent Layer 2 switches.

Port F1 to Ports 1 and 2 and Port F2 to Ports 3 and 4.

Fiber Redundancy

Enables Port F1/F2 redundancy; Normal, Redundant No Return and Redundant Return.

MAC Learning

Enables or disables MAC learning.

6.2.2 GLPoE/Mi Switch

Switch Mode

The module operates as a standard layer 2 switch. Data flow will follow MAC address mapping.

Directed Switch Mode

Data traffic from SPE ports are only forwarded to the uplink port F1, preventing the broadcast traffic from flooding other network ports. Incoming traffic from F1 follows MAC address mapping.

Dual Device Mode

The module is configured as two logically independent Layer 2 switches.

Port F1 to Ports 1 and 2 and Port F2 to Ports 3 and 4.

Fiber Redundancy

Enables Port F1/F2 redundancy; Normal, Redundant No Return and Redundant Return.

MAC Learning

Enables or disables MAC learning.

SPoE Reset

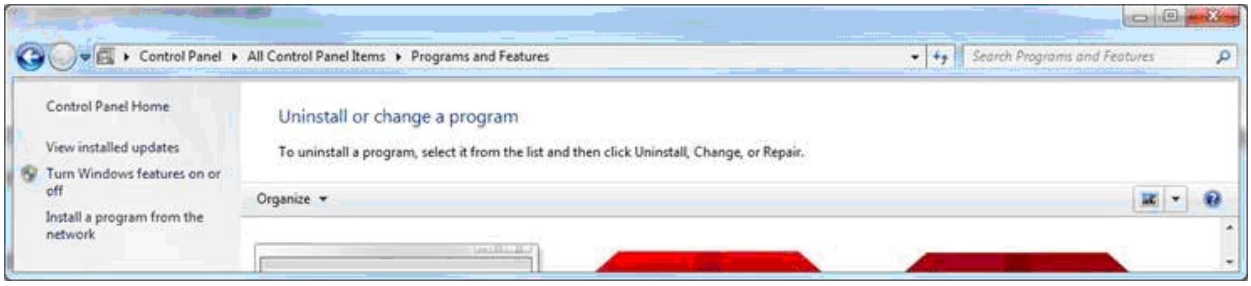
Enable or disable PoE output power (PSE) reset. When enabled, the PoE output power will be removed for 5 seconds after a loss of receive link on any uplink port.

7.0 APPENDIX B: SNMP SERVICE FOR WINDOWS 7

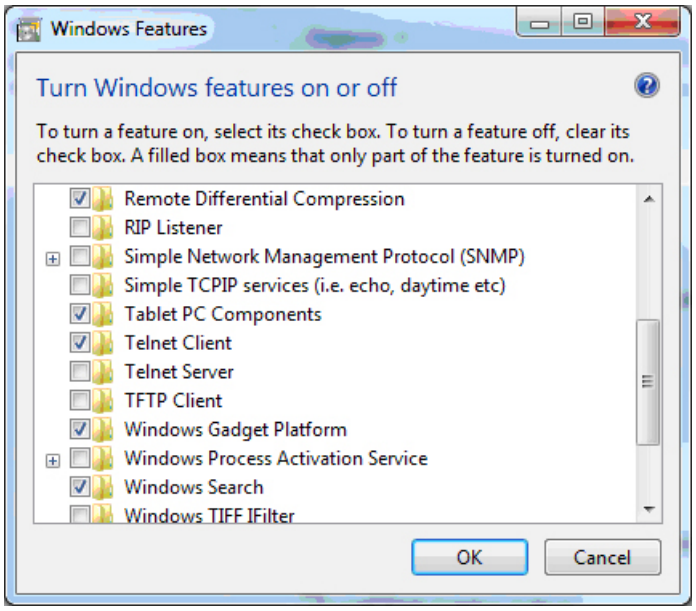
To fully support SNMP and SNMP traps when using Windows7, SNMP services needs to be enabled.

From the control panel select the “Programs and Features”

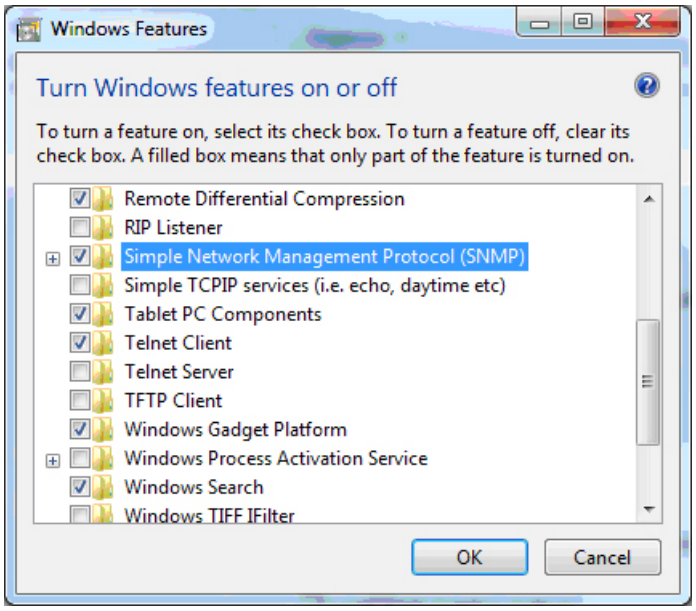
Select “Turn Windows features on or off”



Find “Simple Network Management Protocol (SNMP)”

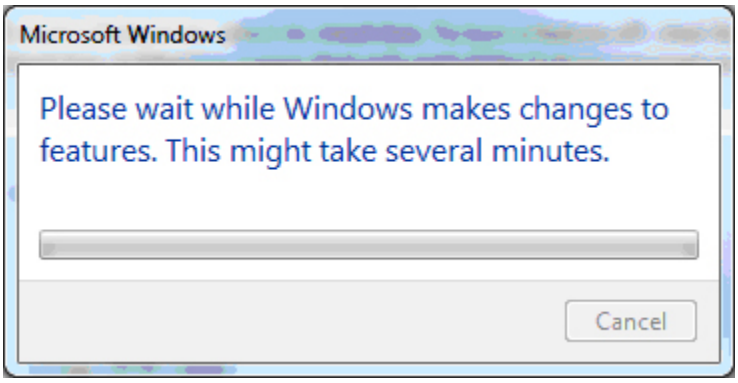


Check the box for “Simple Network Management Protocol (SNMP)”



Select “OK”

Wait if necessary …



Exit control panel and if prompted reboot the computer.

8.0 APPENDIX C: DEFINITION OF TERMS

8.1 Power over Ethernet Terms

Power over Ethernet (PoE) describes a method of passing electrical power along with data over copper UTP Ethernet cabling. This allows a single cable to provide both data connection and electrical power to Powered Devices (PDs) such as small cells, wireless access points or IP cameras.

8.1.1 Power Sourcing Equipment (PSE)

Power Sourcing Equipment are devices such as a media converter or switch that provides (sources) power on the Ethernet cable.

The main functions of the PSE are to automatically detect a PD, classify the PD and supply power to the link (only if a PD is detected). The PSE detects a PD by applying a voltage in the range of -2.8 to -10V on the cable to detect a 25K ohm signature resistor from the attached PD. A compliant PD is required to have this level of resistance between its twisted pairs. Classification of the PD determines the maximum power levels required by the PD. The PSE applies a fixed voltage between -15.5 and 20V with a current limit of 100ma on the cable. The PSE measures the PD load current to determine the proper classification and power requirements of the PD. After the PD is classified, the PD is powered up according to the detected classification.

8.1.2 Powered Device (PD)

A powered device is a device powered by a PSE. Wireless access points, IP Phones and IP cameras are examples of PDs.

8.1.3 Single Pair Power over Ethernet (SPoE)

Single-Pair Power over Ethernat (SPoE) is defined to work with the 10BASE-T1L 10Mb/s protocol. SPoE enables data and power to reach devices at a distance of up to 1km. It is design to operate over a single-pair Ethernet (SPE) cabling, IEC 61156-13 (fixed) or IEC 61156-14 (flexible) 18AWG, at a distance of up to 1km. However, other cabling types can be used but the distance will vary due to cabling resistance and class of end device.

SPoE deployments use two operating line voltages (24V and 55V DC) depending on the distance and the Class of the end device. There are six Classes defined for SPE networks. Classes 10, 11, and 12 use 24V DC power and Classes 13, 14, and 15 use 55V DC power.

The table below shows the operating parameters for the six Classes.

Operating Parameters	Classes					
	10	11	12	13	14	15
Supply Voltage V_{PSE}(min/typ/max)	20/24/30			50/55/58		
Voltage @ PD V_{PD}(min)	14VDC	14VDC	14VDC	35VDC	35VDC	35VDC
Power @ PD P_{PD}(max)	1.23 Watts	3.2 Watts	8.4 Watts	7.7 Watts	20 Watts	52 Watts
Current across cabling I_{CABLE}(max)	0.092A	0.240A	0.632A	0.230A	0.600A	1.579A

The table below shows actual test data for the different cable types using a bookend configuration (Class 13 - 15).

Cable Type	Cable Gauge	Max Cable Length with no data errors	Max SPoE Power at PSE for V_{PD} min (35V)	SPoE Power Available at PD after Max Cable Length	Power Available for PoE or Splitter
CAT5e	24 AWG	700m	8W	5W	n/a
CAT6a	23 AWG	900m	7W	4W	n/a
SPE101	18 AWG	1000m	23W	15W	10W
3090A	16 AWG	1000m	63W	40W	35W

The data shown for the 3090A cable is based on theoretical calculations.

9.0 CUSTOMER SERVICE 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

041-029XX-001A 7/25