MCR-MGT Management Module

User's Guide

Version 1.8

Part #5500310-16

September 2014

Copyright Statement
This document must not be reproduced in any way whatsoever, either printed or electronically, without the consent of:

Perle Systems Limited,
60 Renfrew Drive
Markham, ON
Canada
L3R 0E1

Perle reserves the right to make changes without further notice, to any products to improve reliability, function, or design.
Perle, the Perle logo are trademarks of Perle Systems Limited.

Microsoft and Internet Explorer are trademarks of Microsoft Corporation.

Mozilla Firefox is a trademark of the Mozilla Foundation.

Perle Systems Limited, 2010 - 2014.

Table of Contents

Preface 3

About This Book 3

Intended Audience 3

Contents of CD 3

Typeface Conventions 4

Chapter 1 Introduction 5

About the MCR-MGT Management Module 5

Accessing the MCR-MGT Management Module 5

General Features 5

Management Features 5

Control Features 6

Security Features 6

Additional Features for the MCR1900 6

Additional Features on some media modules 6

Chapter 2 Setting IP Addresses 8

SetIP Utility 8

Using CLI commands 9

Chapter 3 Configuration Methods 11

Introduction 11
Configuration Methods Overview 11
Features 11
MCR Web Manager 11
Connecting to the Management Module for the first time 11
Using WebManager 14
Command Line Interface 15
Overview 15
Access Platforms 15
Using CLI commands 15
Menu 16
Overview 16
Access Platforms 16
Using the Menu 16
SNMP 17
Overview 17
Accessing MCR-MGT using SNMP 17
Chapter 4 MCR1900 Chassis 18
MCR1900 Chassis 18
Power Supplies 18
Temperature Protection Logic 18
Removal Of Management Module From a Chassis 18
Firmware Components 18
Configuration 19
Backplane 19
Media Converter Modules 19
MCR1900 Chassis View 20
Populating Slots In the MCR1900 Chassis 20
Unmanaged modules 20
Empty slot 21
Chapter 5 SMI Media Converter 22
SMI Media Converter 22

Removal Of Management Module From a Chassis **22**
Firmware Components **22**
Configuration **22**
Modules 22
Chassis **23**
Advanced Parameter 23

Chapter 6 MCR-MGT Module 24

MCR-MGT Management Module 24

General Tab **24**
Alert Log Tab **24**
Port Setup Tab **25**
Serial 25
Ethernet 26
Advanced Tab **27**

Management Module View 28

MCR1900 Chassis **28**
Power Schedule 29
Network **30**
Advanced 34
Access **43**
MCR Web Manager 44
SSH 44
SNMP 46
Authorized Hosts 48
Authentication and Accounting **49**
Local 51
RADIUS 52
Kerberos 54
LDAP/Microsoft Active Directory 55
TACACS+ 57
SecurID 59
NIS 60
Alerts **61**
Local Event Log 62
Email Alerts 63
Syslog 65
SNMP Traps 66
Date and Time **68**
Time Zone Settings 68

Display Formats **71**
Files **71**
Firmware 71
MCR 1900 Media Converter Module Firmware Update 73
Manual Update 73
Automatic Update 74
SMI Media Converter Firmware Update 74
Manual Update 74
Automatic Update 75
Configuration 75
Keys and Certificates 75
Diagnostic File 76
Bootup Files 76
TFTP Settings 77

Chapter 7 CM-100 Media Converter Module 78

CM-100 Media Converter Module Parameters 78

General Tab **79**
Copper Port Tab **81**
Fiber Port Tab **82**
Alert Log Tab **82**
Advanced Tab **82**
Slot Tab **83**

Chapter 8 CM-110 Media Converter Module 84

CM-110 Media Converter Module Parameters 84

General Tab **85**
Copper Port Tab **89**
Switch Features **92**
Fiber Port Tab **95**
Switch Features **97**
Alert Port Tab **100**
Advanced Tab **100**
Slot Tab **101**

Chapter 9 CM-1110/CM-1110-SFP Module 102

CM-1110/SPF Media Converter Module Parameters 102

General Tab 103
Copper Port Tab 106
Switch Features 109
Fiber Port Tab 112
Switch Features 115
Alert Log Tab 118
Advanced Tab 118
Slot Tab 119

Chapter 10 CM-1000/CM-1000-SFP Module 120

CM-1000 Media Converter Module Parameters 120

General Tab 121
Copper Port Tab 123
Fiber Port > SFP (Statistics) 126
Alert Log Tab 126
Advanced Tab 126

Chapter 11 CM-100MM Media Converter Module 128

CM-100MM Media Converter Module Parameters 128

General Tab 128
MCR1900 Chassis 128
SMI Chassis 128
Fiber Port 1 Tab 130
Fiber Port 2 Tab 131
Alert Log Tab 131
Advanced Tab 131
Slot Tab 132

Chapter 12 CM-1000MM Media Converter Module 133

CM-1000MM Media Converter Module Parameters 133

General Tab 133
MCR1900 Chassis 133
Fiber Port 1 Tab 136
Fiber Port 2 Tab 137
Alert Log Tab 137

Advanced Tab 138

Chapter 13 CM-10G Media Converter Modules 140

Standard Models 140

High Power Models 140

CM-10G Modules Parameters 141

General Tab 142

Port 1 Tab 144

Port 2 Tab 145

Alert Log Tab 147

Advanced Tab 147

Slot 148

Chapter 14 CM-10GT Media Converter Modules 150

Commercial Model 150

High Power Model 150

CM-10GT Module Parameters 150

General Tab 151

Port 1 Tab (SFP installed) 153

Port 1 Tab (XFP installed) 154

Port 2 Tab (Copper) 156

Alert Log Tab 157

Advanced Tab 158

Slot 159

Chapter 15 eX-1CM110/1110 Media Converter Modules 160

eX-1CM110/1110 Models 160

eX-1CM110/1110 Modules Parameters 160

General Tab 161

Interlink Port > Properties 163

Interlink Port - Advanced VDSL Status 169

Interlink Port - Statistics 170

Alert Log 175

Advanced 176

Slot 176

Chapter 16 CM-4GPT-DSFP Media Converter Module . 178

CM-4GPT-DSFP Media Module Parameters 178

General Tab 179

Port 1 181

Port 1 SFP 182

Port 2 182

Port 2 SFP 183

Alert Log 183

Advanced Tab 184

Slot 184

Appendix A Alert Messages 185

Introduction 185

Format of alerts 185

Severity levels 185

Alert Messages 186

Management Module Alerts 186

Chassis Alerts 187

Power Supply Alerts 188

Media Converter Alerts 188

SFP/XFP Alerts 189

VDSL Line Alerts 200

Appendix B SSL/TLS Ciphers 201

Valid SSL/TLS Ciphers 201

Appendix C Pinouts and Cabling Diagrams 203

Console Port Pinout 203

Appendix D Auto-Config Switch 204

Appendix E Troubleshooting 205

General Troubleshooting 205
Communication Issues 206
Host Problems 206
RADIUS Authentication Problems 206
Unknown IP Address 207
SSL/TLS 207
IPv6 Issues 207
Contacting Technical Support 208
Appendix F Symmetric Key File 209
Symmetric Key File 209

Preface

About This Book

This guide provides the information you need to:

- Configure and manage your MCR-MGT Management Module.

Intended Audience

This guide is for administrators who will be configuring the MCR-MGT Management Module.

Some prerequisite knowledge is needed to understand the concepts and examples in this guide:

- If you are using an external authentication application(s), working knowledge of the authentication application(s).
- Knowledge of TFTP may be required if this is the method you choose to use as the transfer protocol of the MCR-MGT Management Module.

Contents of CD

The following documentation is included on the MCR-MGT Management Module Installation CD:

- *MCR1900 Media Converter 19-Slot Chassis Installation Guide*
- *SMI Media Converter Installation Guide*
- *MCR-MGT Management Module User's Guide*
- *MCR-MGT Management Module CLI Guide*
- *MCR-MGT Management Module Installation Guide*
- *Installation Guides for all supported Media Converter Modules*

The following files are also included on the MCR-MGT Management Module Installation CD:

- *MCR-MGT.MIB file for SNMP*
- *SetIP utility*
- *Firmware for MCR-MGT Management Module*
- *Firmware for all supported Media Converter Modules.*
- *Copyrights notices*

Typeface Conventions

Most text is presented in the typeface used in this paragraph. Other typefaces are used to help you identify certain types of information. The other typefaces are:

Typeface Example	Usage
At the C: prompt, type: `add host`	This typeface is used for code examples and system-generated output. It can represent a line you type in, or a piece of your code, or an example of output.
Set the value to **`TRUE`**.	The typeface used for `TRUE` is also used when referring to an actual value or identifier that you should use or that is used in a code example.
`subscribe` *`project subject`* **`run yourcode.exec`**	The italicized portion of these examples shows the typeface used for variables that are placeholders for values you specify. This is found in regular text and in code examples as shown. Instead of entering *`project`*, you enter your own value, such as `stock_trader`, and for ***`yourcode`***, enter the name of your program.
File, **Save**	This typeface and comma indicates a path you should follow through the menus. In this example, you select **Save** from the **File** menu.
MCR-MGT Management Module	This typeface indicates a book or document title.
See ***About This Book*** on page 3 for more information.	This indicates a cross-reference to another chapter or section that you can click on to jump to that section.

Introduction

About the MCR-MGT Management Module

The following software features are available on the MCR-MGT module.

Accessing the MCR-MGT Management Module

The MCR-MGT Management Module can be accessed through any of the following methods:

- MCR Web Manager, a (http/https) web browser
- Menu, a window-oriented menu interface
- CLI, a Command Line Interface option
- SNMP

General Features

- IPv6 support
- IPv6 Tunneling though an IPv4 network
- Access via Serial, Telnet, SSH, HTTP and HTTPS.
- DHCP/BOOTP for automated network-based setup
- Dynamic DNS with DYNDNS.org
- Domain Name Server (DNS) support
- Display preferences (Date, Time, Temperature formats)
- Backup/Restore module configuration automatically
- Automatically update managed media converter modules to the current firmware version

Management Features

- Console port enable/disable function
- IP and Mac address filtering
- Enable/Disable management services
- Management session inactivity timer
- Multiple Concurrent management sessions
- View and gather link statistics

Control Features

- Remote logging via Syslog
- SNTP (versions 1, 2, 3, and 4 are supported)
- Email alert notification

Security Features

Authentication using any of the following systems:

  - Local Authentication
  - RADIUS
  - Kerberos
  - TACACS+
  - NIS
  - SecurID
  - LDAP/Microsoft Active Directory
- Ability to assign users access level rights to control their access
- Idle timers, which close a connection that has not been active for a specified period of time
- SSH-2 and SSH-1 connections
- SSL/TLS connections.
- Filter network services
- Local event log with filtering per module basis

Additional Features for the MCR1900

- Chassis temperature, voltage and fan monitoring
- ECO power scheduler feature allows you to set power on/off schedules
- Manually power slots off and on
- Define a default power state for each slot

Additional Features on some media modules

Quality of Service (QOS)

- Bandwidth allocation via ingress and egress rate limiting
- IEEE 802.1p tagged frame priority control
- IEEE 802.1p priority tag remapping
- IP TOS (Type of Service) priority for IPv4 Diffserv or IPv6 Traffic Class frames
- Congestion Service Policy through Weighted Fair Queuing or Strict Priority Queuing

VLAN Tagging

- Rate Limiting on ingress or egress packets
- Enable discarding of tagged frames
- Enable discarding of untagged frames
- Removal of existing tag on frames
- Insert tag

- Insert double tag

Other

- Unidirectional Ethernet
- Filtering of unknown multicast frames
- Filtering of unknown unicast frames

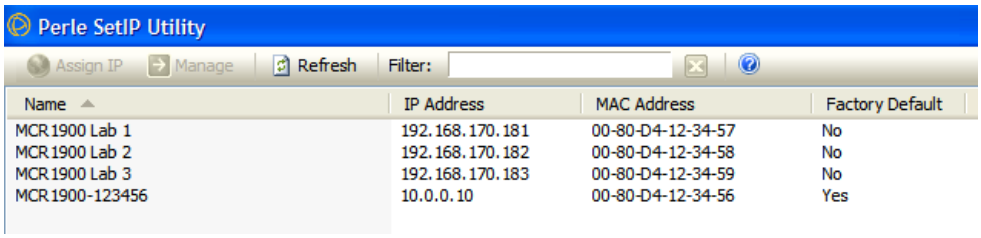
2 Setting IP Addresses

SetIP Utility

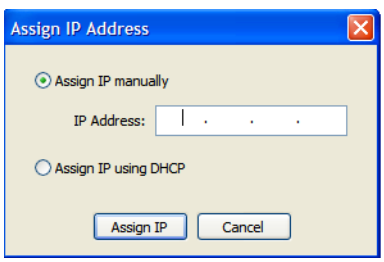
There a several different configurations methods available to configure the MCR-MGT Management Module (Management Module). The most important part of setting up the network is assigning an IP address to the Management Module, whether this is a static IP address, or enabling a DHCP/BOOTP assigned address. The Management Module is pre configured with an IP address of 10.0.0.10 with a subnet mask of 255.0.0.0. This will probably not be the IP address schema for your ethernet network, therefore all of the Management Module configuration methods have the ability to change the IP address on the Management Module. You should also assign a name to the Management Module to make it easier to recognize. By default the Management Module does not require a user to login to configure or manage the module.

This section deals primarily with three ways in which to assign an IP address to the Management Module.

The easiest method to assign an IP address to your MCR-MGT Management Module is to use the Perle SetIP Utility. The Perle SetIP Utility will allow you to assign an IP address and/or manage a predefined Management Module. This utility can be found on the Perle CD that came with your Management Module. Simply run the SetIP utility by double clicking on the SetIP.exe file. For security reasons, the ability to set an IP address to a module is only available when the module is in a factory default state. (i.e. has not yet been configured).



Assign IP address



Using CLI commands

Using a Direct Serial Connection to Specify an IP Address or to Enable DHCP/BOOTP

You can connect to the Management's Module's serial console port using a PC with a terminal emulation package, such as HyperTerminal or a terminal.

1. Using an RJ-45 patch cable and a CISCO RJ45-DB9F-DTE Pinout adapter (Perle part number 04007040), connect your PC or dumb terminal to the console port on the Management Module. See Appendix , "Console Port Pinout" for cabling diagram.
2. Using a PC emulation application, such as HyperTerminal, or from a dumb terminal, set the Port settings to 9600 Baud, 8 Data bits, No Parity, 1 Stop Bits, and No Hardware Flow control.
3. Press **Enter**
4. You should now see a prompt that displays the model type and last 6 numbers of the MAC address for that unit. for example, MCR-MGT-900634.
5. To set the IP address, type the following command:

   ```
   set server internet <ipv4address><netmask>
   ```

   Press **Enter**

   Where ***ipv4address*** is the IP Address being assigned to the Management Module and netmask is the subnet mask to apply to the IP address. ***For example;***

   ```
   set server internet 172.16.4.90 netmask 255.255.0.0
   ```

6. To save the information to non-volatile memory, type the following command:

   ```
   save
   Save config to flash ROM y/n
   Type,
   y
   ```

7. Lastly, type:

   ```
   reboot
   Confirm reboot unit y/n
   ```

   Type,

   ```
   y
   ```

   The management Module will reboot and the IP address will now take affect.

Alternatively, you can enable the DHCP/BOOTP option within the Management Module.

1. Perform the steps above 1 through 4.
2. Using the Command Line Interface (CLI).

   Type the following command:

   ```
   set server internet dhcp/bootp on
   ```

   Press **Enter**
3. Then type the following command:

   ```
   save
   Save config to flash ROM y/n
   Type
   y
   ```

4. Lastly, type:

   ```
   reboot
   ```

```
Confirm reboot unit y/n
Type
y
```

Connecting to the Management Module's Internal IPv6 address

The Management Module has a link local IPv6 address based upon its MAC Address. For example, the link local address is:

Management Module MAC Address: 00-80-D4-AB-CD-EF

Link Local Address: FE80:0280:D4FF:FEAB:CDEF

Using Telnet or SSH you can connect to the Management Module's IPv6 local link address and configure the Management Module. By default, the MCR-MGT Management Module will listen for IPv6 router advertisements to obtain additional IPv6 addresses.

Configuration Methods

Introduction

This chapter provides information about the different methods you can use to configure the MCR-MGT Management Module (Management Module). Before you can configure the Management Module, you must assign an IP address. See Chapter 2, ***Setting IP Addresses*** to find out how to assign an IP address to the Management Module.

Configuration Methods Overview

Following is a list of methods for configuring the Management Module.

- **MCR Web Manager**
- **CLI** using Telnet/SSH or a Direct Serial Console Connection
- **Menu** using Telnet/SSH or a Direct Serial Connection
- **SNMP** using standard based SNMP tools

Features

- Configure Management Module chassis parameters
- Configure Network parameters
- Configure User accounts and Authentication methods
- Configure Alert levels, Email alerts, SMNP parameters and SMNP traps
- Configure Access parameters
- Configure Date and Time parameters
- Configure the Security parameters
- Backup and Restore configuration
- Update firmware
- Reboot the Management Module and any Manageable media converter modules or the Chassis
- View and gather statistics while connected to the Management Module

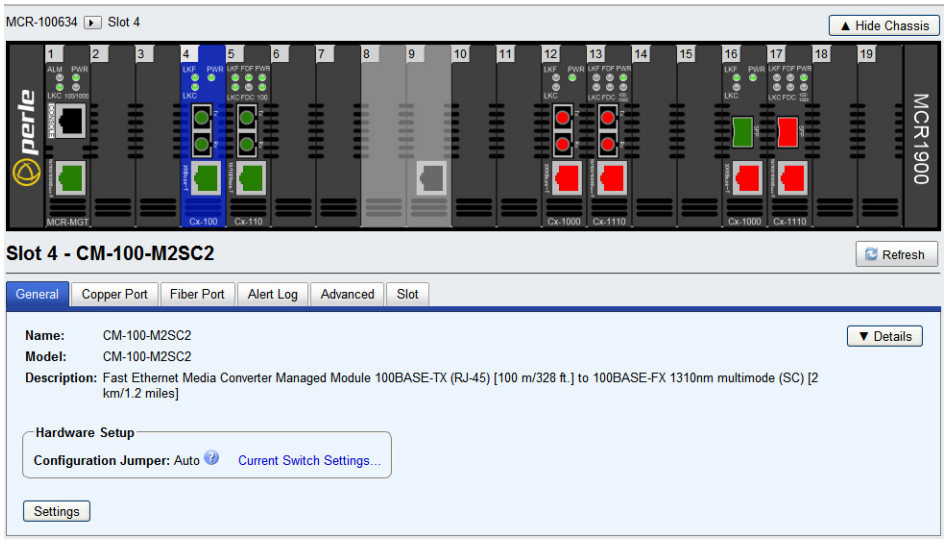
MCR Web Manager

Connecting to the Management Module for the first time

By default, the Management Module requires no login information to gain entry to it. The Management Module supports http/https with common browsers such as Internet Explorer (version 7 or higher), Firefox (version 3.5.10 or higher), Chrome (version 4.0.249 or higher) and Safari (version 4.0.5 or higher).

1. Open your web browser and type in the IP address of the Management Module that you want to manage/configure and press **Enter.** For example: **`http://10.0.0.10 or https://10.0.0.10`**
2. If you successfully connect to the Management Module, either a MCR1900 screen or a SMI Media Converter screen will appear.

MCR1900



The top portion of the screen (chassis view) will display the chassis and all modules detected. This will include;

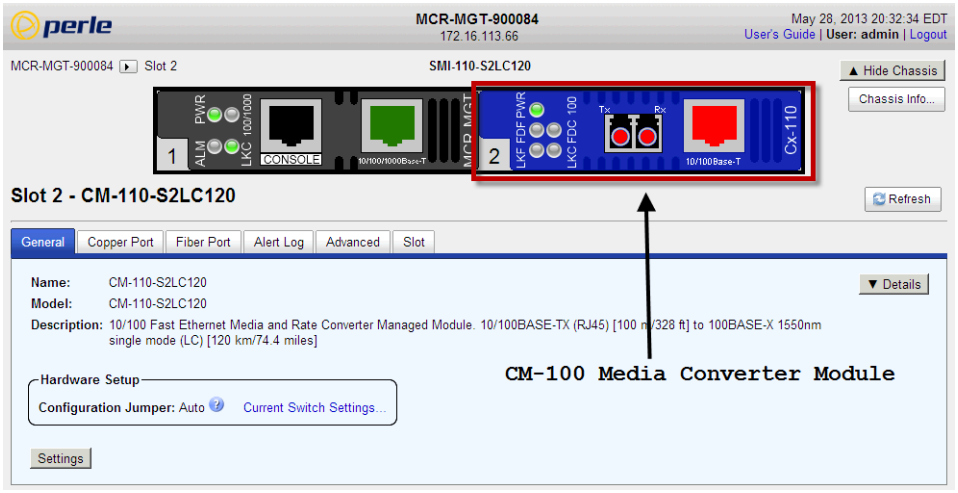
- MCR-MGT Management Module
- Managed Media Converter Modules.
- Unmanaged Media Converter Modules (if any exist).
- Unknown card - Slot powered off when Media Converter Module was inserted.

If any component has an active alarm (severity level “System Level Fault”, “Module level Fault” or “Persistent Error”), a red triangle will show up on that component. If you place your cursor over the triangle, the cause of the alarm will be displayed.

Moving your cursor over any module, will place a “magnifying glass” at the bottom of the module. If you move the cursor to the magnifying glass, you will be presented with a magnified view of the module in that slot.

Clicking on any module on the top portion will bring up the detailed information on the selected module in the bottom half of the screen. If a selected module has active alarms, these will be displayed in the middle of the page. The chassis view automatically refreshes every 30 seconds.

SMI Media Converter



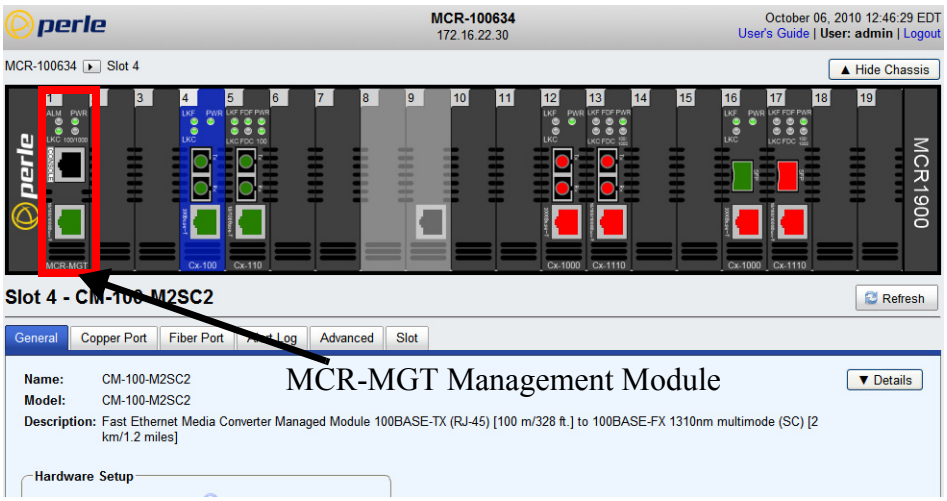
The top portion of the screen will display the installed MCR-MGT module and the detected media converter module.

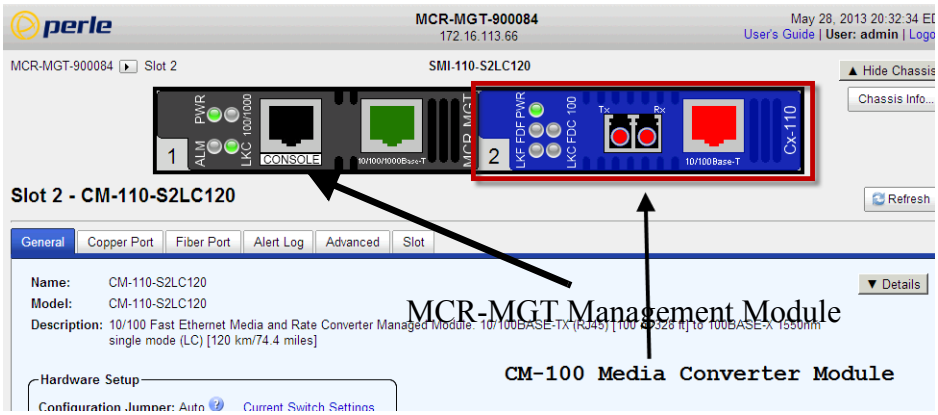
If any module has an active alarm (severity level “System Level Fault”, “Module level Fault” or “Persistent Error”), a red triangle will show up on that module. If you place your cursor over the triangle, the cause of the alarm will be displayed.

Clicking on any module on the top portion will bring up the detailed information on the selected module in the bottom half of the screen. If a selected module has active alarms, these will be displayed in the middle of the page.

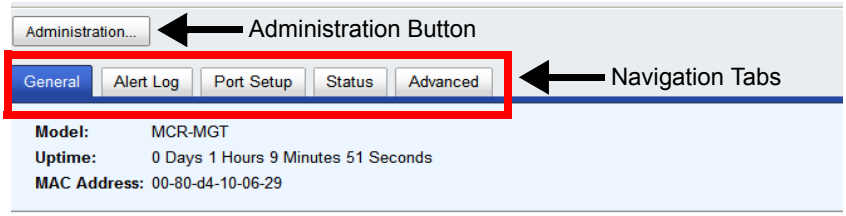
Using WebManager

Click the MCR-MGT Management Module.

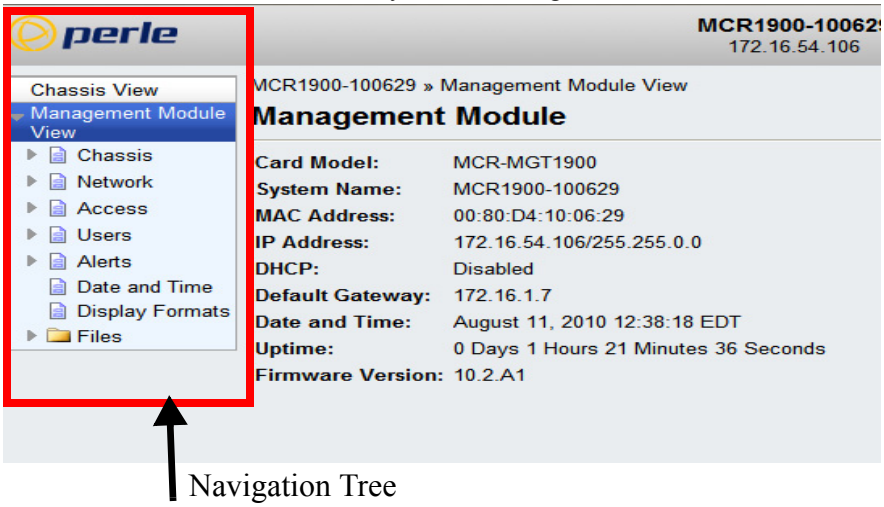




You navigate through the different configuration windows by selecting a navigation tab. Each of the navigation tabs open to more options and windows.



The Administration button will take you to the navigation Tree as shown below.



Note: Remember to click on the Apply button to save your configuration changes.

Command Line Interface

Overview

The Command Line Interface (CLI) is a command line option configuration for the Management Module. See the *Command Line Interface Reference Guide* for a full breakdown of all the CLI commands and their functionality.

Access Platforms

The CLI is accessed by any application that supports a Telnet or SSH session to the Management Module's IP address, such as Putty, SecureCRT, or from a command prompt. You can also access the CLI from a dumb terminal or PC connected to the console port of the Management Module.

Using CLI commands

To connect to the Management Module through the network to configure/manage it using the CLI commands, do the following:

1. Start a Telnet or SSH session to the Management Module's IP address; for example:

   ```
   telnet 10.0.0.10
   ```

2. Press **Enter**
3. Alternatively, you can connect directly to the console serial port.
4. If Require Password is enable you will get a prompt to login, else you will get the following command prompt.

MCR-MGT-<last six digits of your MAC address>#

You can start configuring/managing the Management Module by typing in commands at the prompt. If you are not sure what commands are available, you can type a **?** (question mark) at any time during a command to see your options.

See the *Command Line Interface Reference Guide* for more information about the CLI.

Menu

Overview

The Menu is a graphical representation of the CLI. You can look up Menu parameter explanations in the *Command Line Interface Reference Guide*. The only operations that the Menu does not support are the downloading or uploading of files to/from the Management Module.

Access Platforms

The Menu is accessed by any application that supports a Telnet or SSH session to the Management Module's IP address, such as Putty, SecureCRT, or from a command prompt. You can also access the Menu from a dumb terminal or PC connected to the console port of the Management Module.

Using the Menu

To connect to the Management Module through the network to configure/manage it using the Menu Configurator, do the following:

1. Start a Telnet or SSH session to the Management Module's IP address; for example:

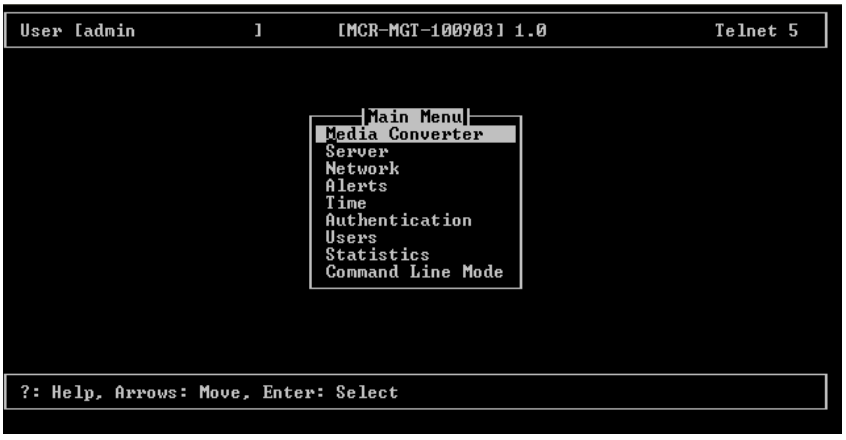
   ```
   telnet 10.0.0.10
   ```

2. Press **Enter**
3. Alternatively, you can connect directly to the console serial port.
4. If Require Password is enable you will get a prompt to login else you will get the following command prompt.

MCR-MGT-<last six digits of your MAC address>#

5. Type **screen**, Press **Enter**

The following Menu will now appear.



To navigate through the Menu options, do the following:

1. Highlight a Menu option by using the keyboard up and down arrows to navigate the list.
2. When the Menu item you want to access is highlighted, press the **Enter** key to either get to the next list of options or to get the configuration screen, depending on what you select.
3. When you are done configuring parameters in a screen, press the **Enter** key and then the **Enter** key again to **Accept and exit the form**.

4. If you want to discard your changes, press the **Esc** key to exit a screen, at which point you will be prompted with **Changes will be lost, proceed? (y/n)**, type **`y`** to discard your changes or **`n`** to return to the screen so you can press **Enter** to submit your changes.
5. If there are a number of predefined options available for a field, you can scroll through those items by pressing the **Space Bar** or you can type **`l`** (lowercase L) to get a list of options, use the up/down arrows to highlight the option you want, and then press **Enter** to select it.

SNMP

Overview

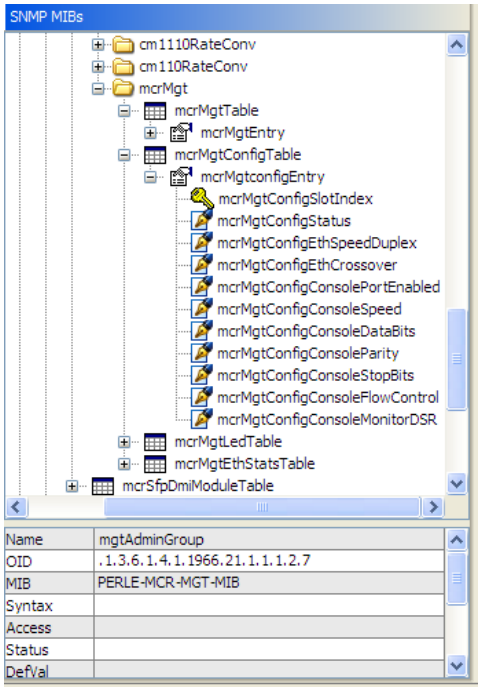
The Management Module supports configuration and management through common standard SNMP Management Tools. You can use SNMP to manage or configure any installed Management Module or Media Converter Modules. The standard SNMP default communities, “public” for read-only access and “private” for read-write access are predefined on the Management Module and will allow you access from any IP address. However, these predefined communities will need to match the communities as configured on your Network Management Software/SNMP MIB browser.

Community=**public**, Permissions=**Readonly**

Community=**private**, Permissions=**Readwrite**

Accessing MCR-MGT using SNMP

1. Load the MCR-MGT.MIB file from the Perle Management Module CD-ROM or Perle website into your SNMP manager.
2. Type in the IP address of the Management Module.
3. You are now ready to start configuring and managing your Management Module and Media Converter Modules using SNMP.



MCR1900 Chassis

General information on the MCR1900 Chassis

MCR1900 Chassis

- The MCR chassis consists of 19 slots.
- Each slot can accommodate either a Management Module or a Media Converter Module.
- This chassis can support 1 Management Module plus 18 Media Converter Modules.
- Each module is hot-pluggable which means it can be inserted or removed without needing to power down the chassis
- The Media Converter Modules do not require the Management Module to be present in order to operate as media converters.

Power Supplies

The chassis supports up to two power supplies. Each supply can power the chassis on its own. When a second power supply is present, “load sharing” is implemented between the two supplies.

The power supply is hot pluggable. When two supplies are powering the chassis, one can be pulled without affecting the operation of the chassis.

Temperature Protection Logic

The chassis has logic which continuously monitors the internal temperature of the chassis. If this temperature ever exceeds 70 degrees Celsius, power to all modules will be cut. This protects the modules from being damaged. The chassis continues to monitor the temperature and when it return back to 55 degrees Celsius, all modules are powered back up.

Removal Of Management Module From a Chassis

You can remove the Management Module from the chassis at any time if needed (i.e for service). All Media Converter Modules will continue to operate normally. What will be lost is the ability to remotely (or locally) connect to the chassis and monitor or control any of its functions. All event notification will be lost as well as any scheduled slot power up/down functionality.

Firmware Components

The MCR1900 chassis has a number of intelligent components, each with supporting firmware. These components are;

- Power supply
- Backplane
- Management module
- Media converter module(s)

All the components are pre-loaded with firmware at the factory. Over time, new updates can become available for any component. Through the Management Module, all components (including the

Management Module itself) can be upgraded.

The firmware residing on Managed Media Converter Modules can be updated manually (user intervention required) or automatically to the latest firmware versions. The Management Module and Media Converter Modules can be at different firmware versions.

The power supply and backplane firmware is embedded in the Management Module image and is updated automatically by the management card so that they always match its firmware.

Configuration

The MCR-MGT Management Module allows for the soft configuration of parameters on the chassis and Media Converter Modules. Some configuration parameters reside only on the Management Module and others reside on the backplane or Media Converter Module.

Backplane

The user can configure a “default power state” for each slot in the chassis. This determines if the slot is powered up or down when the system boots. This information is stored on the backplane so that even if the management card is removed from the chassis, the slots will still power up as per the configured status.

If you ever need to reset this configuration but no longer have a management card with which to do so, you can reset the configuration to factory default (all slots powered up) by doing the following;

1. Power off the chassis.
2. Remove all modules from the chassis.
3. Power up the chassis for at least 30 seconds.
4. Power down the chassis.
5. Re-insert all modules into their respective slots.
6. Power up the chassis.
7. At this point, all slots should have gone back to a “powered up” default state.

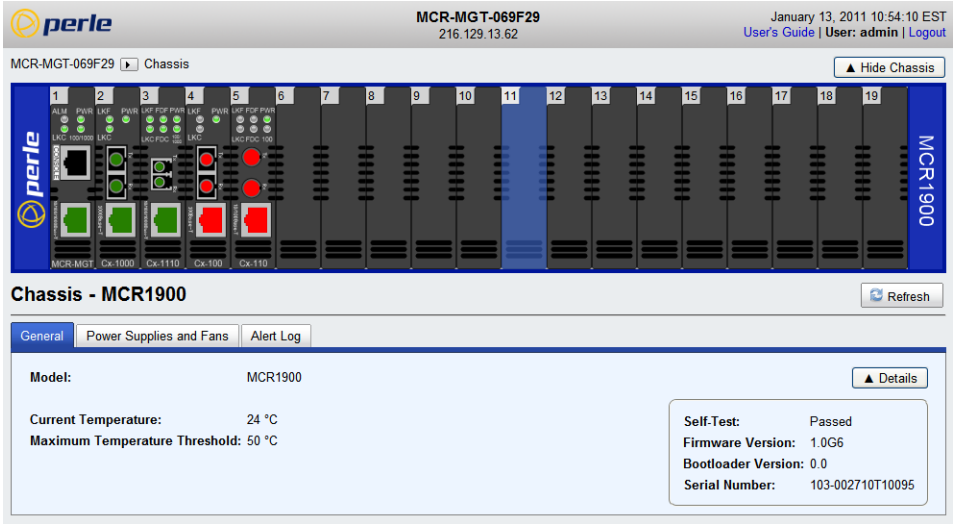
Media Converter Modules

The Media Converter Modules can be configured using the MCR-MGT Management Module. This configuration will be stored on the Media Converter Module in non-volatile memory. Whenever the Media Converter Modules are powered up or re-started, the Media Converter Modules will look first at their Auto-Config Jumper to determine the jumper position see Appendix D, Auto-Config Jumper on page 119 for more information. If the jumper is set to SW the modules will read the settings of the DIP switches and use those as their running configuration. The Media Converter Modules will ignore any configuration information in their flash memory. If the jumper is set to Auto (default), the Media Converter Modules will at power up, check their internal flash memory to see if configuration information has been downloaded to them from a management module. If so, the Media Converter Modules will use this as their running configuration. If there is no configuration in flash, the Media Converter Modules will read the settings of the DIP switches and uses those as their running configuration.

When configuring the Media Converter Module, you have the option to enable the “Backup/Restore Module Configuration Automatically”. When this option is used, the Media Converter configurations are also stored on the Management Module. At any time, if you replace the module in this slot with a different module of the same type, the management card will automatically download the configuration it has for that slot to the new Media Converter Module. This allows you to easily replace a module for servicing purposes.

MCR1900 Chassis View

The Chassis section is used to view the parameters directly associated with the MCR1900 chassis.



General

Model — The Model of the chassis.

Current Temperature — The current temperature of the chassis.

Maximum Temperature Threshold — When the temperature of the chassis exceeds this threshold, alerts will be generated. Once the threshold is exceeded a new alert will be issued each time the temperature raises by 1 degree.

Default: 50 ^{0}C

Power Supplies and Fans

Show details for the Power supplies and fans installed.

Alert Log

Shows any alerts that have been generated.

Populating Slots In the MCR1900 Chassis

Slots in the MCR1900 chassis can be populated with a Management Module and Media Converter Modules. The Media Converter Modules can be of the CM/eX variety (managed) or C variety (unmanaged). You can mix managed and unmanaged Media Converter Modules in the same chassis. Slots can also be left unpopulated.

Unmanaged modules

If a slot is populated with an unmanaged Media Converter Module, the management card can not manage that module however, it can still perform the following actions on this slot;

- Assign a logical name to the slot. This can facilitate the ability for the operator to determine what this card is.
- Power the slot on or off
- Define a default power state for this slot

Empty slot

If a slot is empty the management card can perform the following actions on this slot;

- Power the slot on or off
- Define a default power state for this slot
- Disable the “Backup/Restore Module Configuration Automatically” option.
- This is done to provide the user a method of cancelling or disabling this operation even once the Media Converter Module is no longer in the slot. This would be useful if you plan to place a new Media Converter Module in this slot but do not wish to have its configuration overwritten by the one stored on the management card.

SMI Media Converter

General information on the SMI Media Converter

SMI Media Converter

- This chassis consists of 2 slots.
- One Management Module plus 1 Media Converter Module are supported.
- By default, slot 1 of the SMI Media Converter will be populated with a MCR-MGT management module and slot 2 will be populated with a Media Converter module.
- Each module is hot-pluggable which means it can be inserted or removed without needing to power down the chassis

Removal Of Management Module From a Chassis

You can remove the Management Module from the chassis at any time if needed (i.e for service). The Media Converter Module will continue to operate normally. What will be lost is the ability to remotely (or locally) connect to the chassis and monitor or control any of its functions. All event notifications will be lost.

Firmware Components

Both the MCR-MGT management module and the Media converter module are pre-loaded with firmware at the factory. All modules can be upgraded as new firmware becomes available.

The firmware residing on Managed Media Converter Modules can be updated manually (user intervention required) or automatically to the latest firmware versions. The Management Module and Media Converter Modules can be at different firmware versions.

Configuration

Modules

The two slots in the SMI Media Converter are populated with a Management Module and a Media Converter Module. See ***Advanced Parameter*** on page 23 for information on how to set the slot position for the management module.

The one Media Converter Module can be configured using the MCR-MGT Management Module. This configuration will be stored on the Media Converter Module in non-volatile memory. Whenever the Media Converter Module is powered up or re-started, the Media Converter Module will look first at the Auto-Config Jumper to determine the jumper position see ***Appendix D, Auto-Config Jumper on page 119*** for more information. If the jumper is set to SW the module will read the settings of the DIP switches and use those as its running configuration. It will ignore any configuration information in its flash memory. If the jumper is set to Auto (default), the Media Converter Module will at power up, check its internal flash memory to see if configuration information has been downloaded to it from a management module. If so, the Media Converter Module will use this as its running

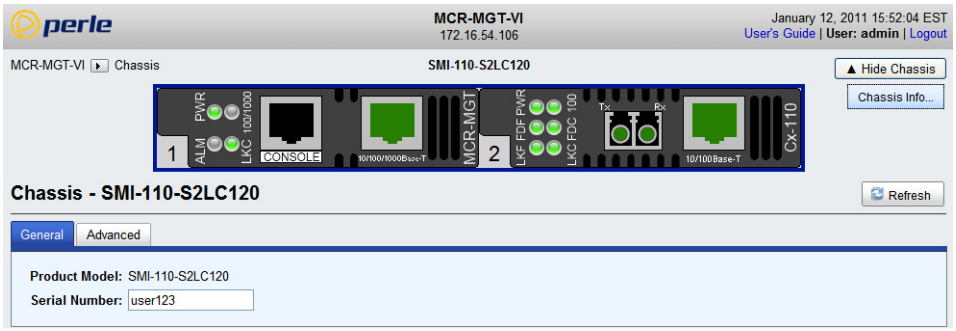
configuration. If there is no configuration in flash, the Media Converter Module will read the settings of the DIP switches and use those as its running configuration.

When configuring the Media Converter Module, you may enable the “Backup/restore Module Configuration Automatically”. When this option is used, the Media Converter configuration is also stored on the Management Module. At any time, if you replace the module in this slot with a different module of the same type, the management card will automatically download the configuration it has for that slot to the new Media Converter Module. This allows you to easily replace a module for servicing purposes.

Chassis

The Chassis section is used to view or configure the parameters directly associated with the SMI Media Converter chassis.

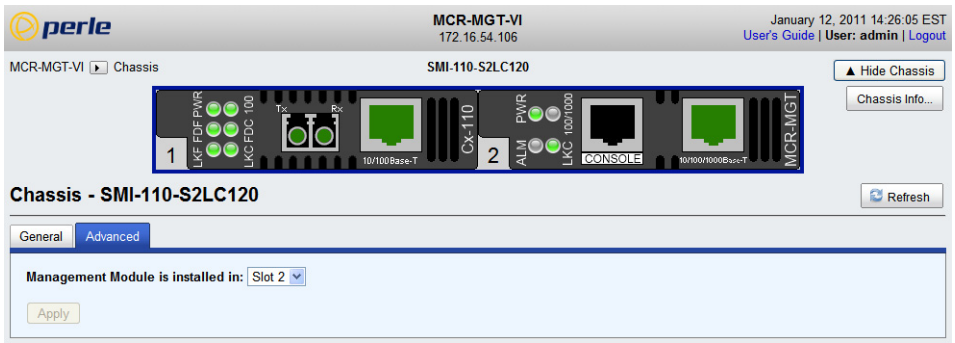
General Parameters



Product Model — The product model.

Serial Number — Sets the chassis serial number.
Field Format: 16 characters

Advanced Parameter



Management Module Slot Number — The management module can be installed in either slot 1 or slot 2.

Note: ***If a change is made to the slot position of the management module, a reboot of the SMI Media Converter is needed for the new slot position to take effect.***

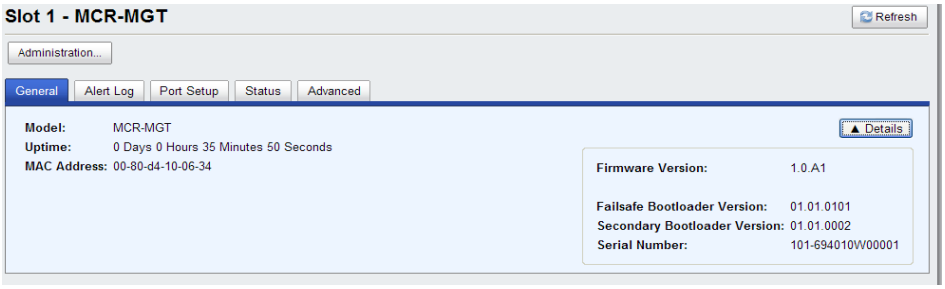
6 MCR-MGT Module

MCR-MGT Management Module

The MCR Web Manager screens will be used to explain the various parameters associated with each component of the system. The parameters have the same meaning in all configuration tools.

General Tab

Field Descriptions

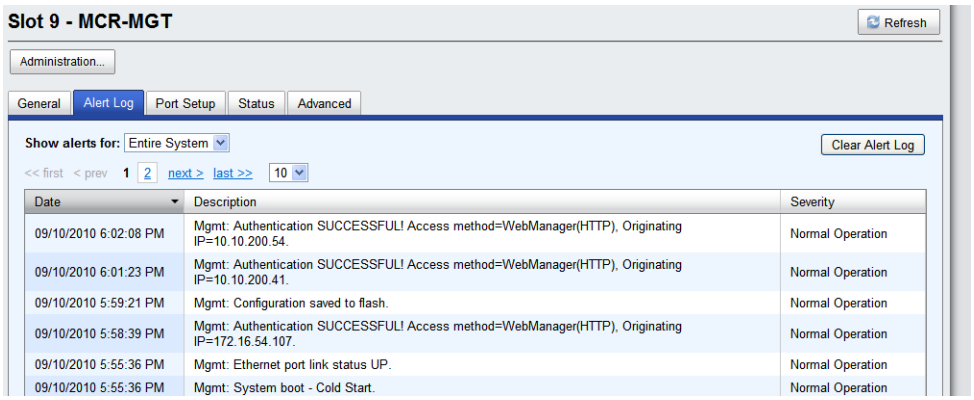


Model	Displays the module's model information.
Uptime	Displays the amount of time the MCR-MGT Management Module has been running since its last reboot.
MAC Address	Displays the MCR-MGT Management Module's MAC Address.
Details	Displays the Management Module's firmware and serial number information.

Alert Log Tab

The MCR-MGT Management Module monitors the status of the various components in the system and when a note worthy event occurs, it records this event in its local event log. This log is kept in a circular buffer which means that once the log is full (around 200 entries), the oldest entries will be replaced with new entries. The date and time of when the alert occurred is recorded with each alert. Clicking on any column will cause the log to be sorted based on the selected column.

Field Descriptions

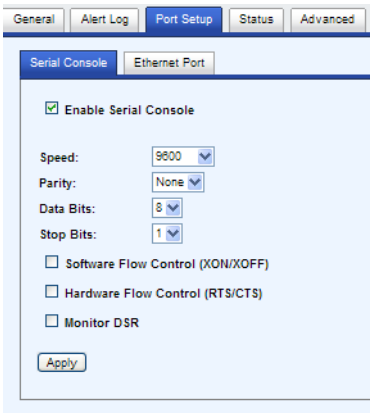


Configure the following parameters:

Show Alerts	Shows Alerts for the Entire System, Chassis or a specific slot.
Clear Alerts	Clears the Alert Log for the Entire System.

Port Setup Tab

Serial



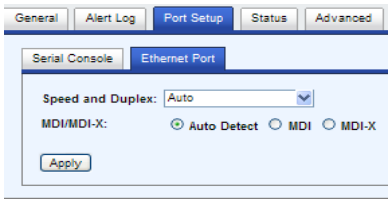
The serial console port is used to obtain local access to the MCR-MGT module. The port allows the user to configure, monitor and/or control the system modules via CLI (Command Line Interface) or Menu (a series of menus). This tab allows for the configuration of the serial parameters used for the port. This tab also allows the system administrator to disable the console port if they do not want to grant access to the Management Module via this port.

Field Descriptions

Enable Serial Console	Enables/Disables the serial console port. **Default:** Enabled
Speed	Specifies the baud rate of the serial console port. **Data Options:** 9600, 19200, 38400, 57600 or 115200 **Default:** 9600
Parity	Specifies the type of parity being used for the data communication on the serial port. **Data Options:** Even, Odd, None **Default:** None
Data Bits	Specifies the number of bits in a transmitted character. **Data Options:** 7, 8 **Default:** 8
Stop Bits	Specifies the number of stop bits that follow a byte. **Data Options:** 1, 2 **Default:** 1
Software Flow Control	The data flow is handled by the Software Flow Control (XON/OFF). **Default:** Off
Hardware Flow Control	The data flow is handled by the Hardware Flow Control (RTS/CTS). **Default:** Off
Monitor DSR	Specifies whether the EIA-232 signal DSR (Data Set Ready) should be monitored. on the serial console port. When the DSR signal is dropped (turn off terminal), the session is terminated. If login is required, will force user to login next time terminal is powered up. **Default:** Off

Ethernet

The Ethernet port is used to both provide access to the MCR-MGT Management Module from the LAN or Internet as well as allowing the Management Module to access hosts and servers on the LAN or beyond. The port allows the user to configure, monitor and/or control the system modules by Telneting, SSHing, HTTPing or HTTPSing into the IP address associated with this port.



Field Descriptions

Speed and Duplex Define the Ethernet connection.

Data Options:

- **Auto**—automatically detects the Ethernet interface speed and duplex
- 10 Mbps/Half Duplex
- 10 Mbps/Full Duplex
- 100 Mbps/Half Duplex
- 100 Mbps/Full Duplex
- 1000 Mbps/Half Duplex

Default: Auto

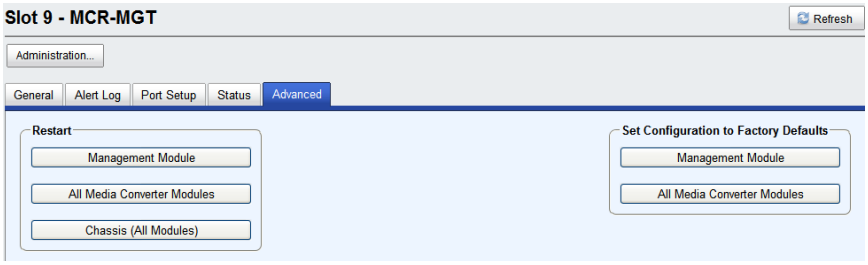
MDI/MDI-X

- **Auto-Detect**— automatically detects the Ethernet's cable polarity
- **MDI** —the cable's polarity is straight-through
- **MDI-X** —the cable's polarity is crossovered

Default: Auto

Advanced Tab

This tab allows the user to reset/restart modules or to reset the configuration of modules back to a factory default state.



Field Descriptions

Restart

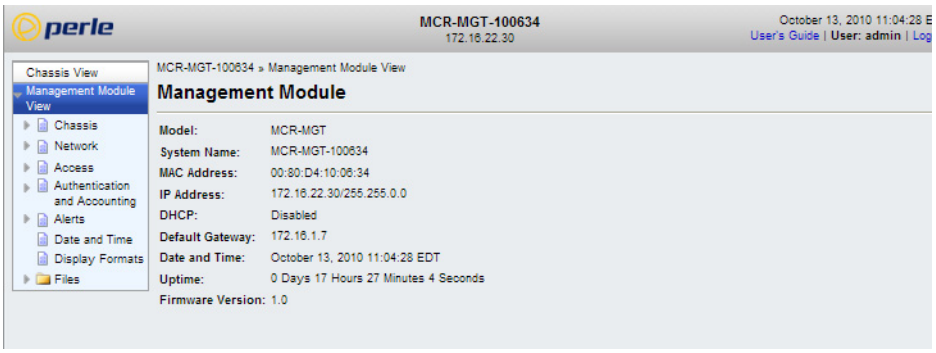
- Restart the Management Module
- Restarts all Media Converter Modules
- Restarts all Modules (including the Management Module)

Set Configuration to Factory Defaults

- Sets the Management Module back to factory default, erasing all configuration, SSL keys and certificates.
- Sets all Media Converter Modules back to factory defaults.

Management Module View

To configure the “system wide” parameters associated with the MCR-MGT module, click on the “Administration” button. This will take you to the following screen where you can navigate to the various parameters which can be set.



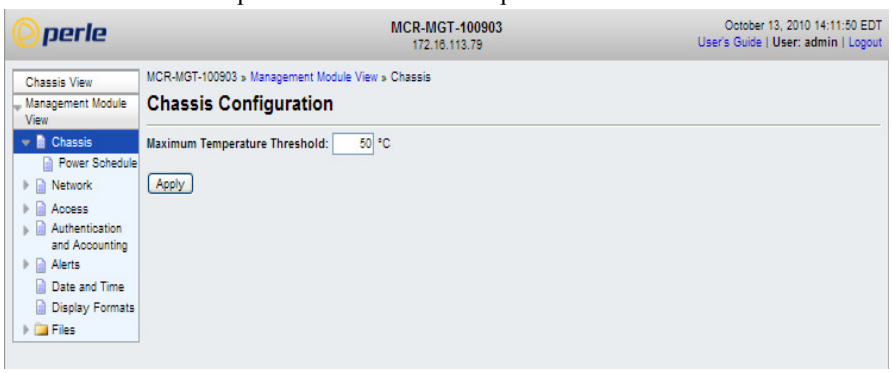
The main screen is divided into two sections. On the left is the “navigation tree” and on the right is the information associated with a specific selection on the navigation tree.

Click on the desired item on the navigation tree and then review or update the information in the window on the right of it.

To get back to the “Chassis” view, click on the “Chassis View” item on the top of the navigation tree. This will return you to the screen with the graphical representation of the chassis.

MCR1900 Chassis

The Chassis section is used to configure the parameters directly associated with the chassis. Maximum Threshold parameter as well as the parameters for the Power Scheduler.



Configure the following parameters:

Maximum Temperature Threshold

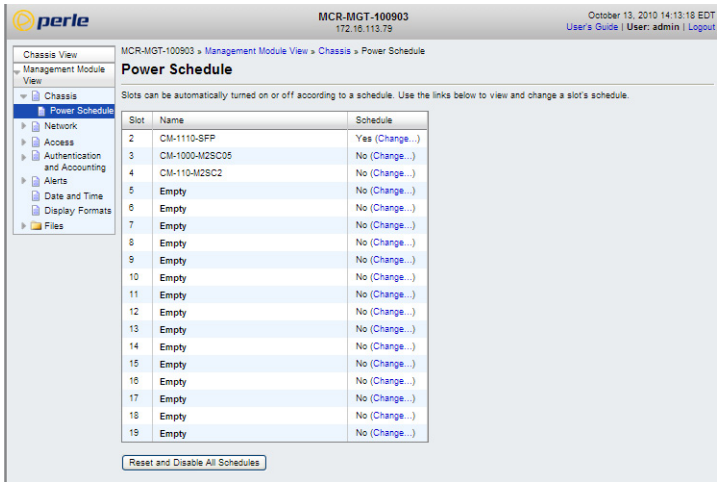
When the temperature of the chassis exceeds this threshold, alerts will be generated. Once the threshold is exceeded a new alert will be issued each time the temperature raises by 1 degree.

Field Format: 0 ^{0}C to 70 ^{0}C (32 ^{0}F to 158 ^{0}F)

Default: 50 ^{0}C

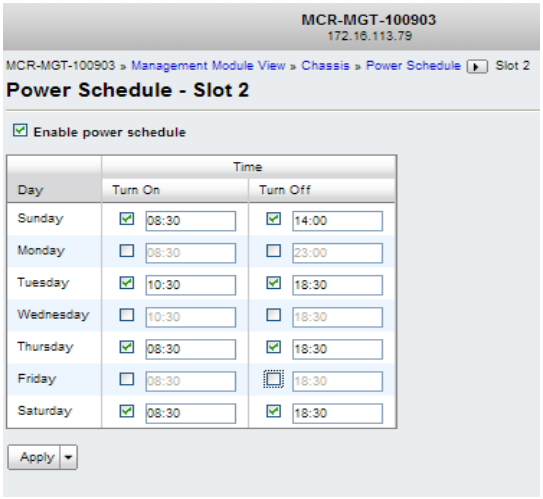
Power Schedule

The parameters in Power Scheduler allow you to configure each slot within the Chassis to be automatically turned On or Off according to a user pre-defined schedule. This feature is available on the MCR1900 chassis only.



Schedule Field Descriptions

Clicking on “Change” for a specific slot above, you will be presented with the following screen;



Configure the following parameters:

Enable Power Scheduler

Enable the scheduler feature for this slot. The power scheduler can be enabled or disabled individually for each slot.

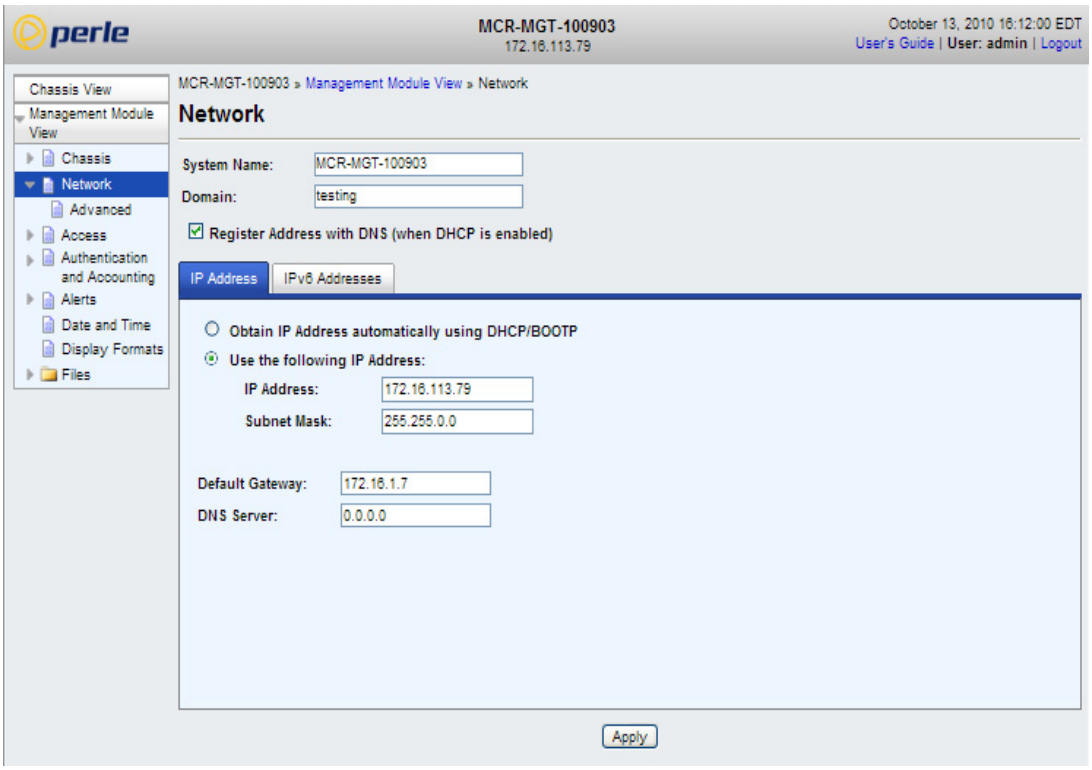
Default: Disabled

Turn On/Turn Off

For each day of the week, you can select an "ON" time and/or an "OFF" time. You can cross over one or more days. For example you could configure an "OFF" time on Friday at 17:00 (5 P.M.) and an "ON" time of Monday at 9:00. This would power the slot off on Friday afternoon until Monday morning.

Network

The Network node allows you to set up your IPv4 or IPv6 network permeates to be used on the Ethernet port of the MCR-MGT Management Module. These are used by the Management Module to access the network.



Configure the following parameters:

System Name
The **System Name** is used for informational purposes by such tools as the MCR Web Manager and is also used in conjunction with the Domain field to construct a fully qualified domain name (FQDN).

Default: MCR-MGT-xxxxxx (where xxxxxx is the last 6 digits of the Management Module's MAC address).

Domain
This field is combined with the **System Name** to construct the fully qualified domain name (FQDN). For example, if the domain is **mycompany.com** and the **Server Name** is set to **accounting**, the FQDN would be **accounting.mycompany.com**.

Register Address in DNS
When this parameter is set, the MCR-MGT Management Module will provide the DHCP server with a fully qualified domain name (FQDN), so that the DHCP server can update the network's DNS server with the newly assigned IP address.

Default: Disabled

Obtain IP Address automatically using DHCP/BOOTP
When enabled, the MCR-MGT Management Module will request an IP address from the DHCP/BOOTP server. When this option is enabled, the MCR-MGT Management Module will also attempt to retrieve the DNS server and default gateway from the DHCP/BOOTP server.

Default: Disabled

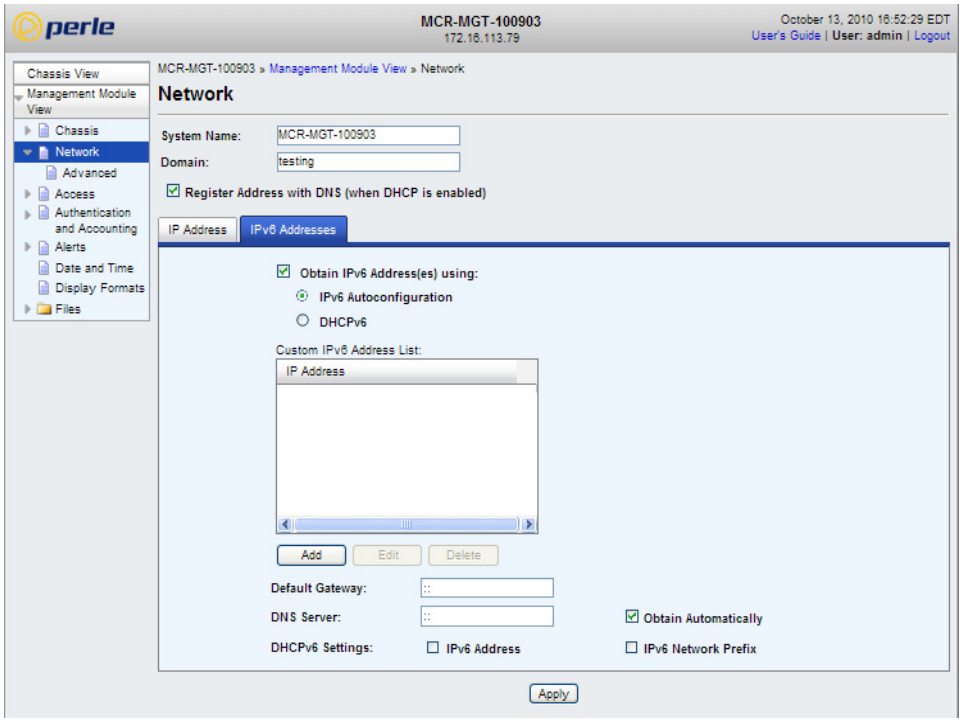
Use the following IP Address
Assign a specific IP address and subnet to the MCR-MGT Management Module's Ethernet interface.

IP Address	The IPv4 network address you wish to assign to the MCR-MGT management module's Ethernet port. For example: 172.16.113.79
Subnet Mask	The IPv4 subnet mask you wish to assign to the MCR-MGT management module's Ethernet port. For example, 255.255.0.0
Default Gateway	Specify the gateway IP address that will provide general access beyond the local network. **Field Format:** IPv4 address
DNS Server	Specify the IP address of a DNS host in your network for host name resolution. **Field Format:** IPv4

IPv6 Addresses

Configure IPv6 settings when the Management Module resides in an IPv6 network.

Field Descriptions



Configure the following parameters:

Obtain IPv6 Address(es) using	When enabled, you can configure the MCR-MGT Management Module to obtain the IPv6 address using IPv6 Autoconfiguration or a DHCPv6 server. **Default:** Enabled

IPv6 Autoconfiguration
When enabled, the MCR-MGT Management Module will send out a Router Solicitation message. If a Router Advertisement message is received, the MCR-MGT Management Module will configure the IPv6 address and configuration parameters based on the information contained in the advertisement. If no Router Advertisement message is received, the MCR-MGT Management Module will attempt to connect to a DHCPv6 server to obtain IPv6 addresses and other configuration parameters.

Default: Enabled

DHCPv6
When enabled, requests IPv6 address and configuration information from the DHCPv6 server.

Default: Disabled

Custom IPv6 Address list
You can manually assign one or more IPv6 addresses to the MCR-MGT management module's Ethernet port using this table. Use the "Add", "Delete" or "Edit" buttons to manipulate the table entries.

Default Gateway
Specify the IPv6 address of a gateway that will provide general access beyond the local network.

Field Format: IPv6 address

DNS Server
Specify the IPv6 address of a DNS host in your network for host name resolution.

Field Format: IPv6 address

Obtain Automatically
When DHCPv6 is enabled, you can enable this option to have the MCR-MGT Management Module receive the DNS IP address from the DHCPv6 server.

Default: Enabled

DHCPv6 Settings

IPv6 Address
When enabled, the MCR-MGT Management Module will accept IPv6 address from the DHCPv6 server.

Default: Disabled

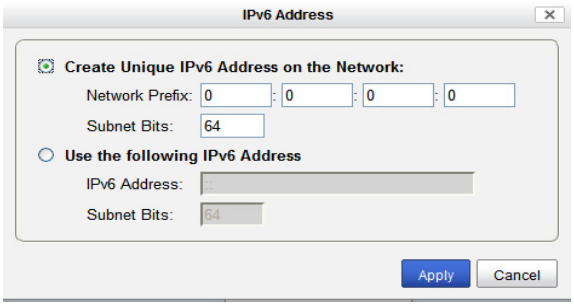
IPv6 Network Prefix
When enabled, the MCR-MGT Management Module will accept the network prefix from the DHCPv6 server.

Default: Disabled

Adding/Editing a Custom IPv6 Address

You can manually add one of the following:

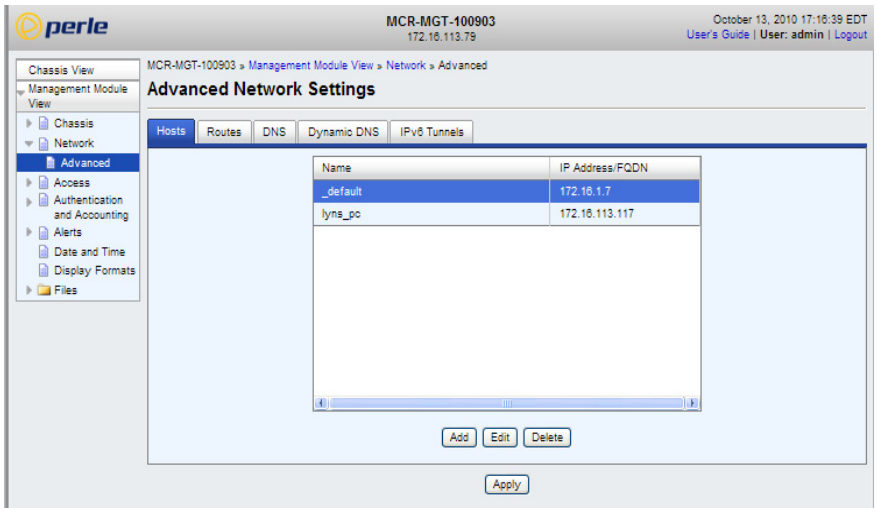
- The IPv6 network prefix (and the Management Module will determine an IPv6 address based on the network prefix and the Management Module MAC address).
- The complete IPv6 address.



Configure the following parameters:

Create a unique IPv6 address on the network	When enabled, the MCR-MGT Management Module will derive an IPv6 address from the entered network prefix and the MCR-MGT Management Module's MAC address. **Default:** Enabled
Network Prefix	Specify the IPv6 network prefix. The MCR-MGT Management Module will derive the complete IPv6 address from the entered network prefix and the MCR-MGT Management Module's MAC address. **Default:** Enabled
Subnet Bits	Specify the network prefix bits for the IPv6 address. **Range:** 0-128 **Default:** 64
Use the following IPv6 address	Enable this option when you want to enter a specific IPv6 address. **Default:** Disabled
IPv6 Address	Specify the complete IPv6 address. **Field Format:** IPv6 address
Subnet Bits	Specify the network prefix bits for the IPv6 address. **Range:** 0-128 **Default:** 64

Advanced

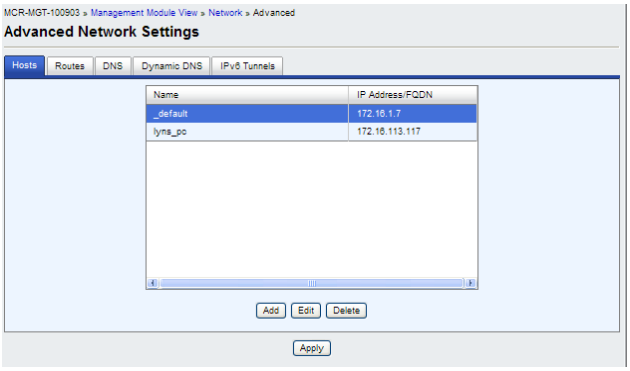


The **Advanced** node configures Host Table entries, Routes, DNS, Dynamic DNS and IPv6 Tunnels.

Configure the parameters in the **Advanced** node if you want to

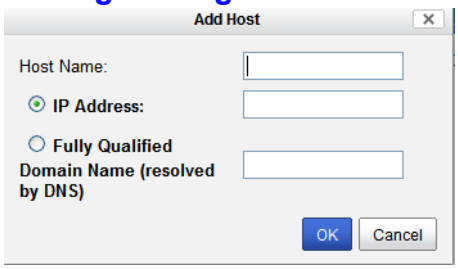
- add a specific host
- modify the host table
- add a route to an external network or host
- specify a DNS server to perform host resolution
- configure an IPv6 tunnel

Host tab



The **host** tab configures Host Table entries. This can include any type of host the MCR-MGT Management Module will need to communicate with. The host is given a local name and an IP address or a fully qualified domain name which will need to be resolved using a DNS server.

Adding/Editing a Host



Configure the appropriate parameters.

Host Name	The name of the host. This is used only for the MCR-MGT Management Module configuration. **Field Format:** Up to 14 characters, no spaces.
IP Address	The IP address of the Host you want to add. **Field Format:** IPv4 or IPv6 address
Fully Qualified Domain Name	You can configure up to four DNS servers. **Field Format:** IPv4 or IPv6 address

Routes tab

Entering routes in the routing list enables the identification of gateways to be used for accessing specific hosts or external networks from the Management Module's local network.

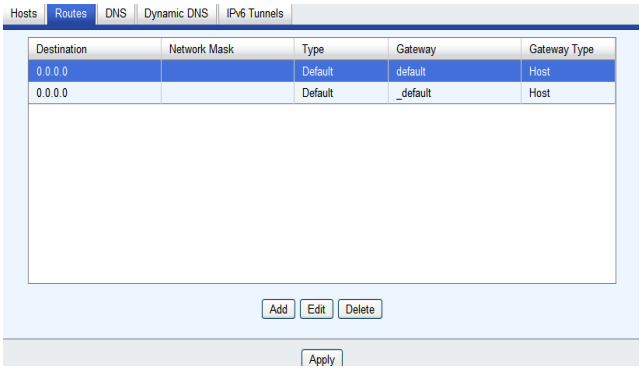
There are three types of routes:

- **Default**—A route that provides general access beyond your local network.
- **Host**—A route defined for accessing a specific host external to your local network.
- **Network**—A route defined for accessing a specific network external to your local network.

Two types or gateways (method of accessing specific hosts or external networks) can be configured:

- **Host**—Specify a specify host that will provide access to the route destination.
- **Interface**—Specify the IPv6 tunnel that will provide access to the route destination.

Field Descriptions

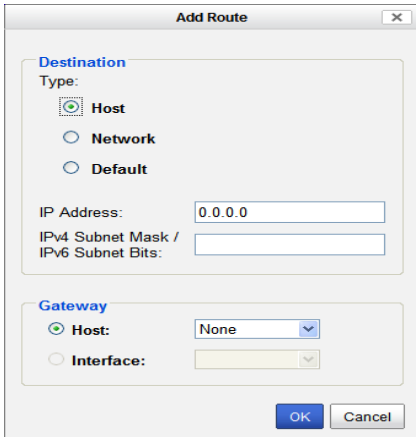


The following buttons are available on this window:

Add Button	Adds a route to the Route List.
Edit Button	Changes an existing route in the Route List.
Delete Button	Deletes a route from the Route List.

Adding/Editing Routes

From the **Route List** tab, if you click the **Add** or **Edit** button, you will be able to add a new or edit an existing route.



Configure the appropriate parameters.

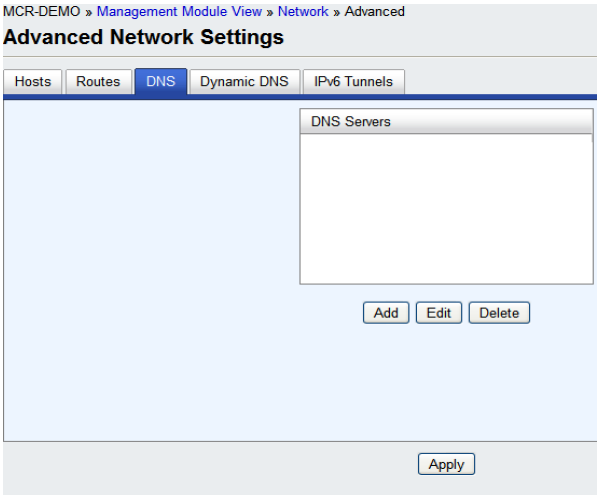
Type	Specify the type of route you want to configure. **Data Options:** ● **Host**—A route defined for accessing a specific host external to your local network. ● **Network**—A route defined for accessing a specific network external to your local network. ● **Default**—A route which provides general access beyond your local network. **Default:** Default

IP Address	When the route **Type** is defined as **Host**, this field will contain the IP address of the host. If the route **Type** is defined as **Network**, the network portion of the IP address must be specified and the Host port of the address will be set to 0. Example: to access network 10.10.20, the address 10.10.20.0 would be specified in this field. **Format:** IPv4 or IPv6 address
IPv4 Subnet Mask	When the route is a **Network** route, you must specify the network's subnet mask.
IPv6 Prefix Bits	If the IP address is IPv6, then you must specify the network's prefix bits. **Range:** 0-128
Host	Select this option when a host is being used at the route gateway. **Default:** Enabled, None
Interface	The Interface list is comprised of configured IPv6 tunnels. Select this option when you want to use the specified interface as the gateway to the destination. **Field Option(s):** IPv6 tunnels **Default:** Disabled

DNS tab

You can configure up to four DNS servers. If you specified a DNS server on the **Network**, **Advanced, DNS** tab (either IPv4 or IPv6), it will be automatically be entered into the appropriate list. If the DNS server is provided by a DHCP server, these will NOT be viewable in the list, however, you can add DNS servers to supplement the DHCP supplied server.

Field Descriptions

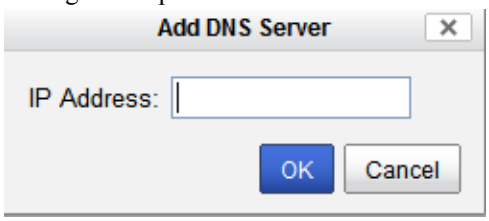


The following buttons are available on this window:

Add DNS Button	Adds a DNS server.
Edit DNS Button	Edits an existing DNS server.
Delete DNS Button	Deletes a DNS server.

Editing/Adding DNS Servers

Configure the parameter:



DNS IP Address	You can configure up to four DNS servers. **Field Format:** IPv4 or IPv6 address

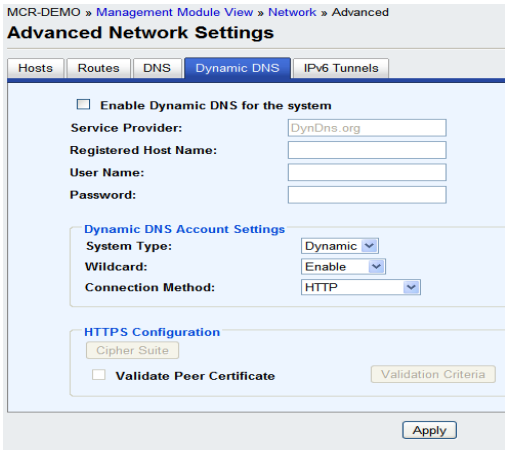
Dynamic DNS

Dynamic DNS Service providers enable users to access a server connected to the internet that has been assigned a dynamic IP address. The Management Module has built-in support for the DynDNS.com service provider. Refer to **`www.DynDNS.com`** for information on setting up an account.

When the Management Module is assigned a dynamic IP address, it will inform the DynDNS.com service provider of its new IP address. Users can then use DynDNS.com as a DNS service to get the IP address of the Management Module. In order to take advantage of this service, the following steps need to be taken.

1. Create an account with DynDNS.com and configure the name your Management Module will be known by on the internet (the **Host** name). For example, create a host name such as **`yourcompanySCS.DynDNS.org`**.
2. Enable the **Network Dynamic DNS** feature and configure the Management Module's dynamic DNS parameters to match the **Host**'s configuration on the DynDNS.com server. Every time the Management Module gets assigned a new IP address, it will update DynDNS.com with the new IP address.
3. Users accessing the Management Module via the internet can now access it via its fully qualified host name. For example, **`telnet yourcompanySCS.DynDNS.org`**.

Field Descriptions



Configure the appropriate parameters:

Enable Dynamic DNS for the system Enables/disables the dynamic DNS feature. When **Dynamic DNS** is enabled, the MCR-MGT Management Module will automatically update its IP address with DynDNS.org if it changes.

Default: Disabled

Service Provider Displays the Dynamic DNS service provider.

Default: DynDNS.org (permanent)

Register Host Name Specify the registered hostname with DynDNS.org that will be updated with the MCR-MGT Management Module's IP address should it change. Put in the full name; for example, mymediaconverter`.dyndns.org`.

User Name Specify the user name used to access the account set up on the DynDNS.org server.

Password Specify the password used to access the account set up on the DynDNS.org server.

Dynamic DNS Account Settings

System Type Specify how your account IP address schema was set up with DynDNS.org. Refer to www.DynDNS.org for information about this parameter.

Data Options: Dynamic, Static, Custom

Default: Dynamic

Wildcard Specifies whether to add an alias such as `*to your Registered Host Name .yourcompanySCS.dyndns.org` pointing to the same IP address as entered for `yourcompanySCS.dyndns.org`.

Data Options: Enable, Disable, Nochange

Default: Enable

Connection Method Specify how the MCR-MGT Management Module is going to connect to the DynDNS.org server.

Data Options:

- HTTP
- HTTP through Port 8245
- HTTPS—for a secure connection to the DynDNS server

Default: HTTPS

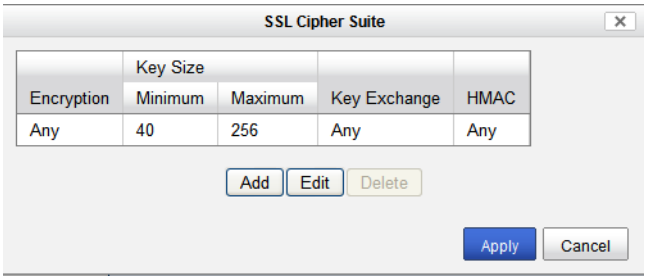
Cipher Suite Button Launches the cipher information window so you can specify the type of encryption that will be used for data that is transferred between the DynDNS.org server and the MCR-MGT Management Module.

See Appendix B, SSL/TLS Ciphers for more information.

Validate Peer Certificate	Enables/disables peer validation between the DynDNS.org server and the MCR-MGT Management Module. This may be desirable, since the DynDNS user name and password are sent from the management module to the DynDNS server when the IP address needs to be updated and when an account refresh is performed. Account refreshes are done periodically to ensure that DynDNS accounts do not auto-delete should the IP address change infrequently. This parameter will only take effect if **HTTPS** is selected as the connection method. **Default:** Disabled
Validation Criteria Button	Launches the peer validation criteria window so you can specify the information used to validate the connection between the DynDNS.org server and the MCR-MGT Management Module.

Cipher Suite Field Descriptions

The SSL/TLS cipher suite is used to encrypt data between the Management Module and the client. You can specify up to five cipher groups.

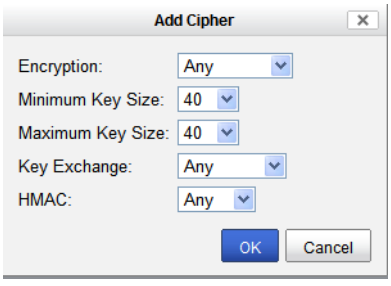


The following buttons are available:

Add Button	Adds a cipher to the cipher list.
Edit Button	Edits a cipher to the cipher list.
Delete Button	Deletes a cipher to the cipher list.

Adding/Editing a Cipher Suite

To see a list of valid cipher suite combinations, see Appendix B, SSL/TLS Ciphers.



Configure the following parameters:

Encryption

Select the type of encryption that will be used for the SSL connection.

Data Options:

- Any—Will use the first encryption format that can be negotiated.
- AES
- 3DES
- DES
- ARCFOUR
- ARCTWO

Default: Any

Min Key Size

The minimum key size value that will be used for the specified encryption type.

Data Options: 40, 56, 64, 128, 168, 256

Default: 40

Max Key Size

The maximum key size value that will be used for the specified encryption type.

Data Options: 40, 56, 64, 128, 168, 256

Default: 256

Key Exchange

The type of key to exchange for the encryption format.

Data Options:

- **Any**—Any key exchange that is valid is used (this does not, however, include ADH keys).
- **RSA**—This is an RSA key exchange using an RSA key and certificate.
- **EDH-RSA**—This is an EDH key exchange using an RSA key and certificate.
- **EDH-DSS**—This is an EDH key exchange using a DSA key and certificate.
- **ADH**—This is an anonymous key exchange which does not require a private key or certificate. Choose this key if you do not want to authenticate the peer device, but you want the data encrypted on the SSL/TLS connection.

Default: Any

HMAC

Select the key-hashing for message authentication method for your encryption type.

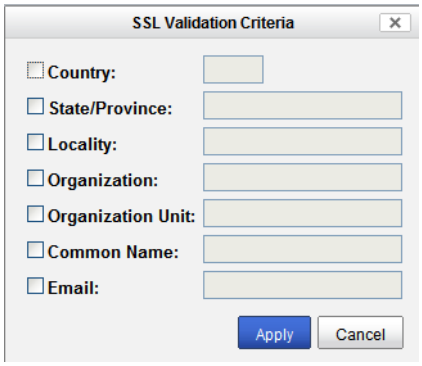
Data Options:

- Any
- MD5
- SHA1

Default: Any

Validation Criteria Field Descriptions

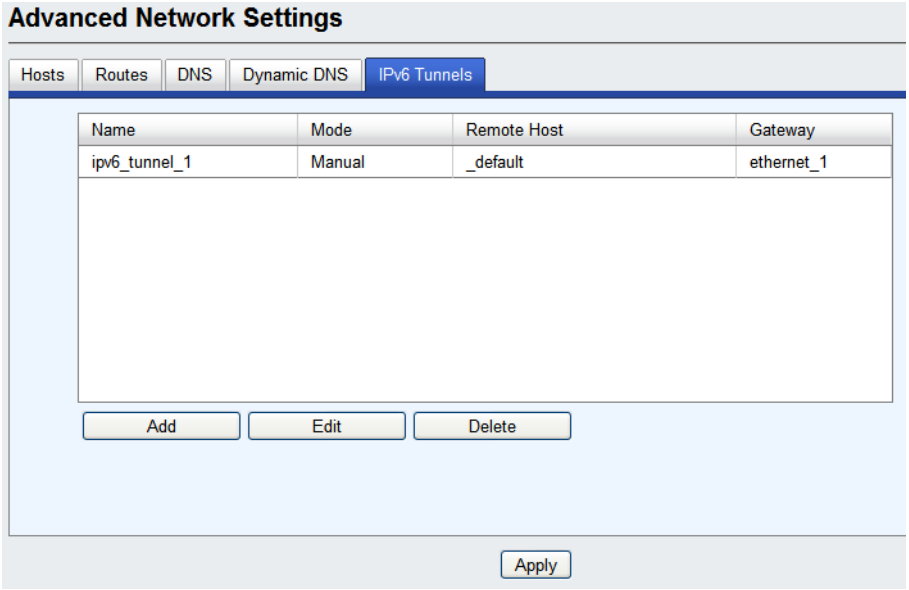
If you choose to configure validation criteria, the information in the peer SSL/TLS certificate must match exactly the information configured in this window in order to pass peer authentication and create a valid SSL/TLS connection.



IPv6 Tunnels

IPv6 tunnels transport IPv6 data packets from one IPv6 network to another IPv6 network over an IPv4 network. In addition to creating the IPv6 tunnel, you must also create the route that will transport the data packets through the IPv4 network in the Route List (see***Advanced*** on page 35) for more information.

Field Descriptions

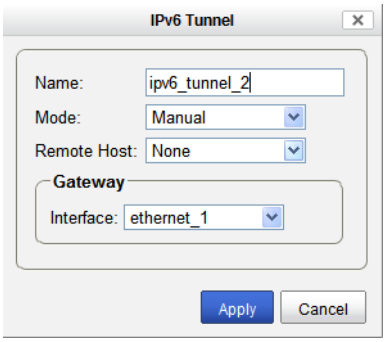


The following buttons are available:

Add Button	Adds an IPv6 tunnel.
Edit Button	Edits an existing IPv6 tunnel.
Delete Button	Deletes an IPv6 tunnel. If a tunnel is associated with a route, it cannot be deleted until the route is either changed or deleted.

Adding/Editing an IPv6 Tunnel

When you add/edit an IPv6 tunnel, you are determining how an IPv6 message will reach an IPv6 device through an IPv4 network.



Configure the following parameters:

Name
The name of the IPv6 tunnel.
Field Format: Maximum 16 alphanumeric characters
Default: ipv6_tunnel1

Mode
The method or protocol that is used to create the IPv6 tunnel.

- **Manual**—When enabled, the MCR-MGT Management Module will manually create the IPv6 tunnel to the specified **Remote Host** through the specified **Interface**.
- **6to4**—When enabled, the MCR-MGT Management Module will broadcast to the multicast address 192.88.99.1 through the specified **Interface**. When the closest 6to4 router responds, it will create the IPv6 tunnel, encapsulating and decapsulating IPv6 traffic sent to and from the MCR-MGT Management Module.
- **Teredo**—When enabled, the Teredo protocol encapsulates the IPv6 packet as an IPv4 UDP message, allowing it to pass through most network address translator (NAT) boxes and create an IPv6 tunnel to the specified **Remote Host** (a Teredo server) through the specified **Interface**.

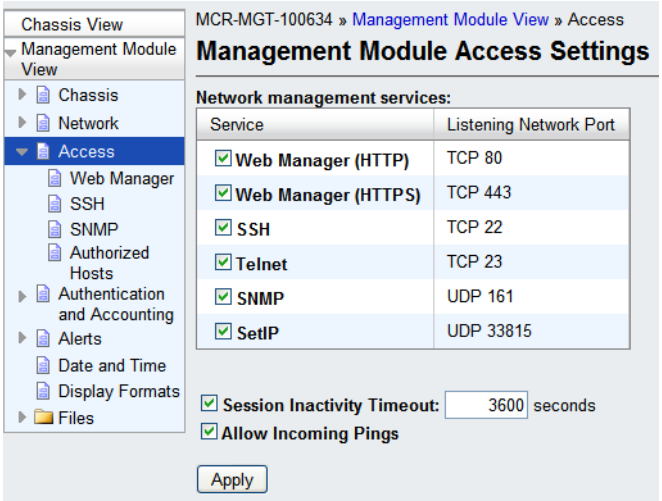
Default: Manual

Remote Host
The IPv4 host that can access the IPv6 network when the **Mode** is **Manual**.
The Teredo server when the **Mode** is **Teredo**.
Default: None

Interface
The interface that the MCR-MGT Management Module is going to use to access the Remote Host.
Default: Ethernet 1

Access

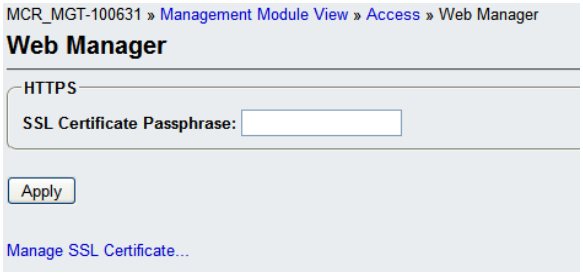
The **Access** node allows you to configure which services can be used to access the MCR-MGT module as well as configuring specific parameters for Web, SSH and SNMP access. It also allows for the configuration of a filter to determine which hosts will be granted access to the Management Module.



Unchecking the box next to each of the services listed above, will disable this service and users will no longer be able to reach the MCR-MGT module using that service.

The session inactivity timer is only used when “Bypass login” is not enabled (i.e. login is required). If no activity is detected on the session for the amount of time configured here, the session will be terminated.

MCR Web Manager



Configure the following parameter.

SSL Certificate Passphrase — This is the SSL/TLS passphrase used to generate an encrypted RSA/DSA private key. This private key and passphrase are required for both HTTPS and SSL/TLS connections, unless an unencrpyted private key was generated, then the SSL passphrase is not required. Make sure that you download the SSL private key and certificate if you are using the secure HTTP option (HTTPS) or SSL/TLS. If both RSA and DSA private keys are downloaded to the MCR-MGT Management Module, they need to be generated using the same SSL passphrase for both to work.

SSH

The Management Module contains SSH Server software that you need to configure if the Management Module is going to be accessed via SSH. If you specify more than one **Authentication** method and/or **Cipher**, the Management Module will negotiate with the client and use the first authentication method and cipher that is compatible with both systems.

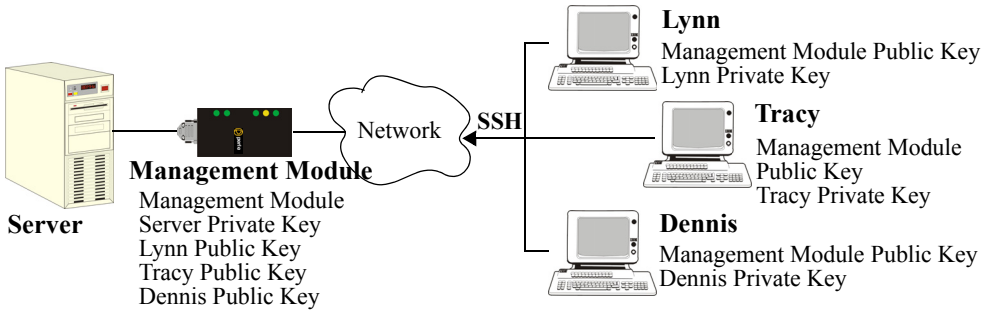
Functionality

When you are using the SSH connection protocol, keys need to be distributed to all users and the Management Module. Below is an example scenario for key/certificate distribution.

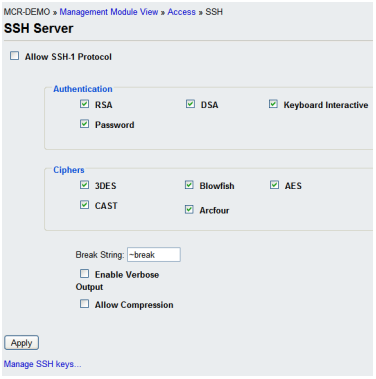
Users Logging into the Management Module Using SSH

In the following example, users are connecting to the Management Module via SSH from the LAN. Therefore, the following keys need to be exchanged:

- Install Management Module **SSH Public Key** to each user's host machine who is connecting and logging into the Management Module using SSH.
- Get the **SSH Public Key** from each user's host machine who is connecting and logging into the Management Module using SSH.



Field Descriptions



Configure the following parameters:

Allow SSH-1 Protocol	Allows the user's client to negotiate an SSH-1 connection, in addition to SSH-2. **Default:** Disabled
RSA	When a client SSH session requests RSA authentication, the Management Module's SSH server will authenticate the user via RSA. **Default:** Enabled
DSA	When a client SSH session requests DSA authentication, the Management Module's SSH server will authenticate the user via DSA. **Default:** Enabled
Keyboard-Interactive	The user types in a password for authentication. **Default:** Enabled

Password	The user types in a password for authentication. **Default:** Enabled
3DES	The Management Module SSH server's 3DES encryption is enabled/disabled. **Default:** Enabled
CAST	The Management Module SSH server's CAST encryption is enabled/disabled. **Default:** Enabled
Blowfish	The Management Module SSH server's Blowfish encryption is enabled/disabled. **Default:** Enabled
Arcfour	The Management Module SSH server's Arcfour encryption is enabled/disabled. **Default:** Enabled
AES	The Management Module SSH server's AES encryption is enabled/disabled. **Default:** Enabled
Enable Verbose Output	Displays debug messages on the terminal. **Default:** Disabled
Allow Compression	Requests compression of all data. Compression is desirable on modem lines and other slow connections, but will only slow down things on fast networks. **Default:** Disabled

SNMP

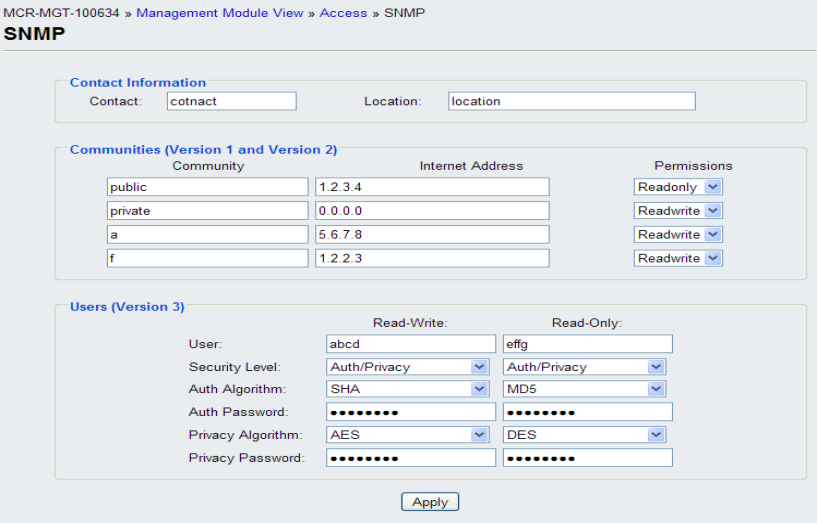
If you are using SNMP to manage/configure the Management Module, or to view statistics or traps, you can connect to the Management Module using either of the two pre-defined communities.

Community = **public**, IP address = **0.0.0.0** (any), Permissions = **Readonly**

Community = **private**, IP address = **0.0.0.0** (any), Permissions =**Readwrite**

You must load the management.MIB (found on the CD-ROM packaged with the Management Module) file into your SNMP manager before you connect to the Management Module.

Field Descriptions



Configure the following parameters.

Contact — The name and contract information of the person who manages this SMNP node.

Location — The physical location of the SNMP node.

Community — The name of the group that devices and management stations running SNMP belong to.

Internet Address — The IP address of the SNMP manager that will send requests to the MCR-MGT module. If the address is `0.0.0.0`, any SNMP manager matching the **Community** name configured, can access the MCR-MGT module. If you specify a network address, for example `172.16.0.0`, any SNMP manager residing on the 172.16.x.x subnet with a matching **Community** name can access the MCR-MGT module.

Field Format: IPv4 or IPv6 address

Permissions — Defines the level of access this community has.

Data Options:

- **None**—No access will be granted to members of this community.
- **Readonly**—Read access will be granted to members of this community.
- **Readwrite**—Read and write access will be granted to members of this community.

Default: None

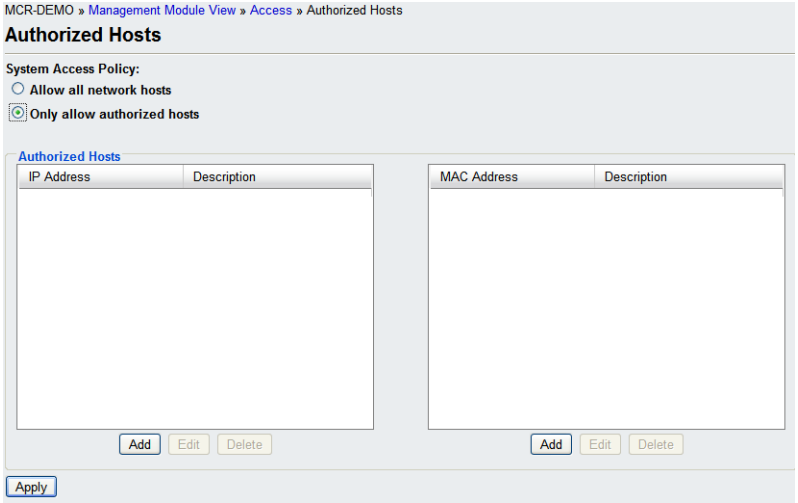
Users (Version 3) — This section is used to configure the attributes associated with a "read-only" type user and a "read-write" type user. For each parameter you configure an entry in either or both of these columns. It is only used to define V3 users.

Users — Enter the user name for the SNMP v3 user. This name must match the v3 user name configured in the SNMP manager.

Security Level	Select the security level for the user. This must match the configuration set up in the SNMP manager. **Data Options:** • **None**—No security is used. • **Auth**—User authentication is used. • **Auth/Priv**—User authentication and privacy (encryption) settings are used. **Default:** None
Authentication Algorithm	Specify the authentication algorithm that will be used for the user. **Data Options:** MD5, SHA **Default:** MD5
Authentication Password	Type in the user's authentication password.
Privacy Algorithm	Specify the authentication algorithm that will be used for the user. **Data Options:** MD5, SHA **Default:** MD5
Privacy Password	Type in the user's privacy password.

Authorized Hosts

You can configure which hosts will be permitted access to the MCR-MGT module. Up to 16 hosts can be defined by IP address and an additional 16 hosts can be defined by MAC address. When enabled, only hosts matching the IP address or MAC address of an entry in this table will be allowed to access the MCR-MGT Management Module.

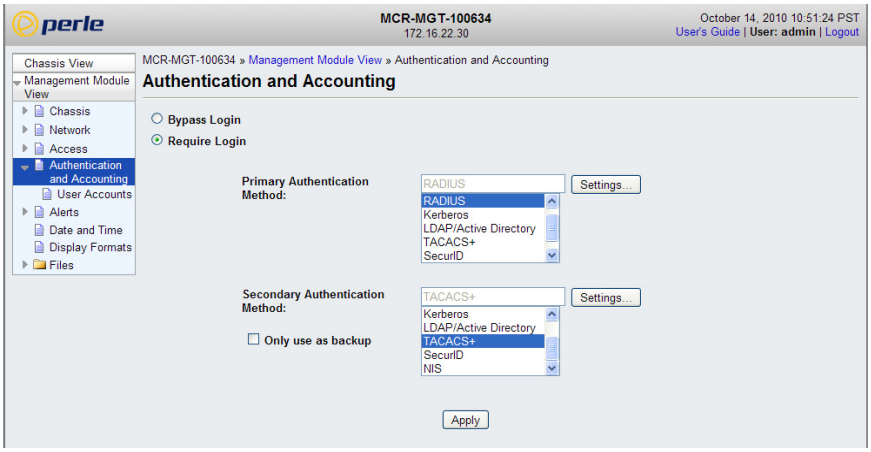


Field Descriptions

System Access Policy	**Data Options:** ● **Allow all network hosts**— Allows any host to connect to the MCR-MGT Management Module. ● **Only allow authorized hosts**—A security feature that when enabled, the Management Module will only accept data from or send data to hosts configured in this table.
Add Authorized Host	Adds an authorized host.
Edit Authorized Host	Edits an authorized host.
Delete Authorized Host	Deletes an authorized host.

Authentication and Accounting

This node allows the administrator to configure the security and accounting methods which will be used by the MCR-MGT module.



The default settings are not to have any security or accounting enabled ("Bypass login"). It is up to the administrator to lock down the access to the module if desired. When "Bypass login" is enabled, the user is never prompted with a login prompt.

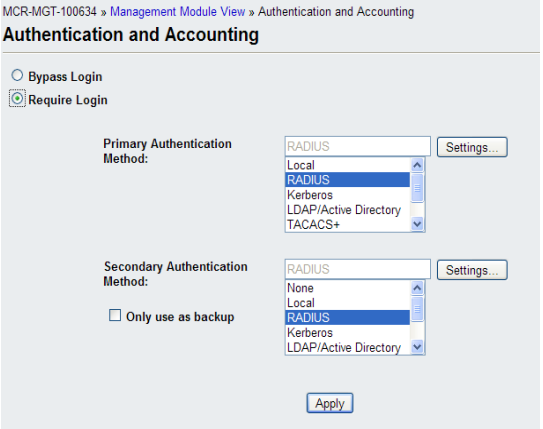
If "Require Login" is enabled, users will be prompted to login to the MCR-MGT module before access is granted. The default username and password are;

User name --> admin

Password --> superuser

You can define additional users via the "User Accounts" node. The "admin" user cannot be deleted. however the password ("superuser") can be changed.

Field Descriptions



Configure the following parameters.

Bypass login

When “Bypass login” is selected (enabled), a user accessing the MCR-MGT module is not asked to login.

Default: Enabled

Require Login

When "Require Login" is selected (enabled), a user accessing the MCR-MGT module is presented with a login prompt or screen before they can obtain access to the management module. The default user name is "admin" and the default password is "superuser". The "admin" user can not be deleted, however the password for this user can be changed.

Default: Disabled

Primary Authentication Method

Select the primary (or only if "none" is selected for the secondary) authentication method to be used to authenticate users attempting to access the MCR-MGT management module.

Data Options:

- **Local**
- **Radius**
- **Kerberos**
- **LDAP/Active Directory**
- **TACACS+**
- **SecureID**
- **NIS**

Default: Local

Only use as backup

If this option is selected (enabled), the secondary authentication method will only be attempted if the MCR-MGT module can not reach the primary authentication host. (i.e. if the primary authentication host indicates that the user does not have access, the secondary authentication method will not be attempted). In other words, the secondary is only used as a backup to the primary in case the primary is not available.

If this options is not selected (disabled), the secondary authentication will always be tried if the primary authentication is not successful (for any reason including an indication from the primary that the user is not authenticated).

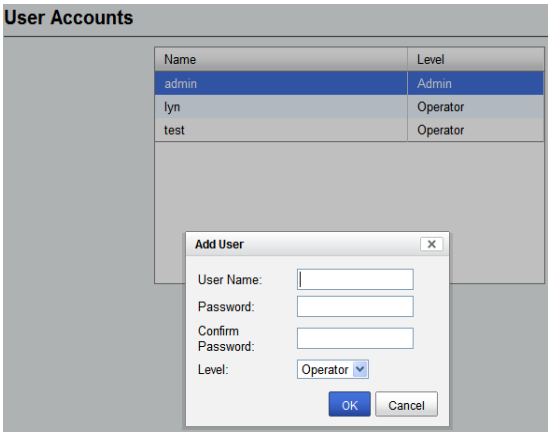
Default: Disabled (not selected).

Specific authentication methods

Local

When **Local** authentication is selected, the user must be configured in the Management Module's **User Accounts** list. A maximum of 31 users can be configured in the list.

Field Descriptions



Configure the following parameters:

User Name

The name of the user.

Restrictions: Do not use spaces.

Password

The password the user will need to login into the Management Card.

Level

The access that a user is allowed.

Data Options:

- **Admin**—The admin level user has total access to the Management Module. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the Management Module.
- **Operator**—The Operator level user has no write access to make configuration changes to the Management Module. They are able to read all management module configuration and to control and reset media converter modules, the management module and the chassis.

When the admin user logs into the Management Module using CLI (via Telnet or SSH), the prompt ends with a **#**, whereas all other users' prompts ends with a **$** or **£**, depending on the character set.

Default: Operator

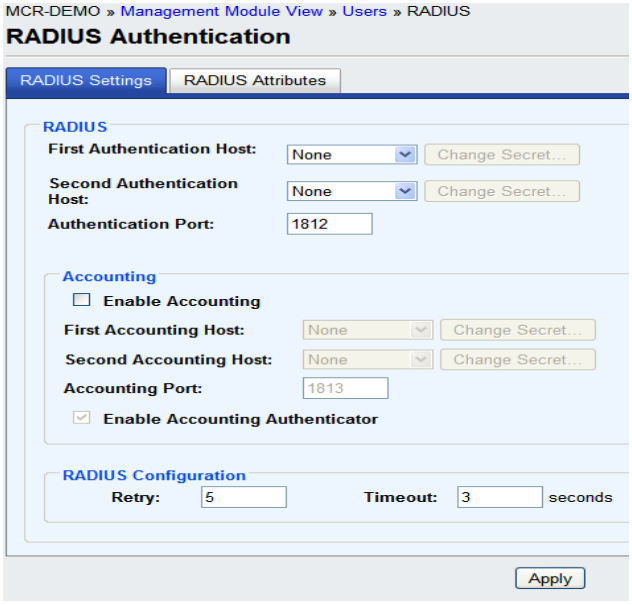
RADIUS

When setting up users on the Radius host, you can specify the permission level this user will have on the MCR-MGT Management Module (i.e. admin or operator). To do this, you need to set the radius parameter "Service_Type" to one of the following values;

Service_Type Value	Permission
1 - Login	Operator
3 - Callback-Login	Operator
6 - Administrative User	Admin
11- Callback Administrative User	Admin

If the "Service_Type" parameter is not returned by the Radius server or if it contains any other value from the one defined above, the firmware will look for a user record in the local data base. If one is found, the permission level will be extracted from this record. If no matching user is found in the local database, the user will be given the default permission of "Operator"

General Field Descriptions



Configure the following parameters:

First Authentication Host Name of the primary RADIUS authentication host.
Default: None

Second Authentication Host Name of the secondary RADIUS authentication host, should the first RADIUS host fail to respond.
Default: None

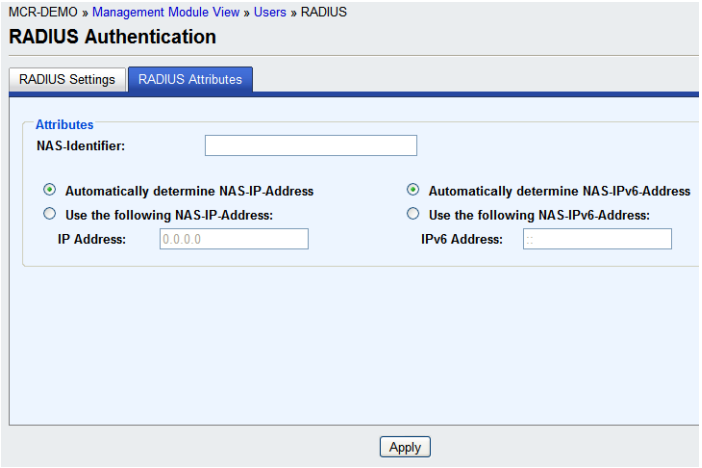
Authentication Port The port that the RADIUS host listens to for authentication requests.
Default: 1812

Change Secret The secret (password) shared between the Management Module and the RADIUS authentication host.

Enable Accounting Enables/disables RADIUS accounting.
Default: Disabled

First Accounting Host	Name of the primary RADIUS accounting host. **Default:** None
Second Accounting Host	Name of the secondary RADIUS accounting host. **Default:** None
Accounting Port	The port that the RADIUS host listens to for accounting requests. **Default:** 1813
Change Secret	The secret (password) shared between the Management Module and the RADIUS accounting host.
Enable Accounting Authentication	Enables/disables whether or not the Management Module validates the RADIUS accounting response. **Default:** Enabled
Retry	The number of times the Management Module tries to connect to the RADIUS server before erroring out. **Range:** 0-255 **Default:** 5
Timeout	The time, in seconds, that the Management Module waits to receive a reply after sending out a request to a RADIUS accounting or authentication host. If no reply is received before the timeout period expires, the Management Module will retry the same host up to and including the number of retry attempts. **Range:** 1-255 **Default:** 3 seconds

Attribute Field Descriptions



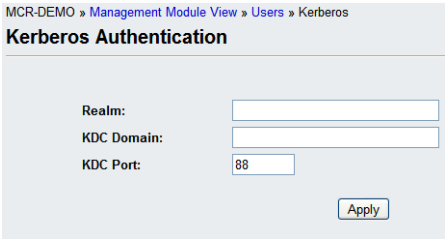
Configure the following parameters:

NAS-Identifier	This is the string that identifies the Network Address Server (NAS) that is originating the Access-Request to authenticate a user. **Field Format:** Maximum 31 characters, including spaces
Automatically determine NAS-IP-Address	When enabled, the Management Module will send the Management Module's Ethernet IPv4 address to the RADIUS server. **Default:** Enabled

Use the following NAS-IP-Address	When enabled, the Management Module will send the specified IPv4 address to the RADIUS server. **Default:** Disabled
IP Address	The IPv4 address that the Management Module will send to the RADIUS server. **Default:** 0.0.0.0
Automatically determine NAS-IPv6-Address	When enabled, the Management Module will send the Management Module's IPv6 address to the RADIUS server. **Default:** Enabled
Use the following NAS-IPv6-Address	When enabled, the Management Module will send the specified IPv6 address to the RADIUS server. **Default:** Disabled
IPv6 Address	The IPv6 address that the Management Module will send to the RADIUS server. **Field Format:** IPv6 address

Kerberos

Field Descriptions



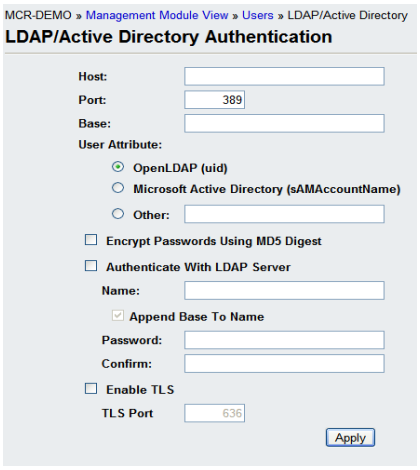
Configure the following parameters.

Realm	The Kerberos realm is the Kerberos host domain name, in upper-case letters.
KDC Domain	The name of a host running the KDC (Key Distribution Center) for the specified realm. The host name that you specify must either be defined in the Management Module's **Host Table** before the last reboot or be resolved by DNS.
KDC Port	The port that the Kerberos server listens to for authentication requests. **Default:** 88

LDAP/Microsoft Active Directory

LDAP (Lightweight Directory Access Protocol) is an application protocol for querying and modifying directory services running over TCP/IP. It is also used as a method of authenticating users. Microsoft Active Directory is an LDAP like directory service. It can be used for authenticating users in a similar fashion to LDAP. In this manual, the use of LDAP is synonymous with Microsoft Active Directory.

Field Descriptions



Configure the following parameters.

Host Name

The name or IP address of the LDAP/Microsoft Active Directory host. If you use a host name, that host must either have been defined in the Management Module's **Host Table** before the last reboot or be resolved by DNS. If you are using **TLS**, you must enter the same string you used to create the LDAP certificate that resides on your LDAP/Microsoft Active Directory server.

Port

The port that the LDAP/Microsoft Active Directory host listens to for authentication requests.

Default: 389

Base

The domain component (dc) that is the starting point for the search for user authentication.

User Attribute

This defines the name of the attribute used to communicate the user name to the server.

Options:

- **OpenLDAP(uid)**—Chose this option if you are using an OpenLDAP server. The user attribute on this server is "uid".
- **Microsoft Active Directory(sAMAccountName)**—Chose this option if your LDAP server is a Microsoft Active Directory server. The user attribute on this server is "sAMAccountName".
- **Other**—If you are running something other than a OpenLDAP or Microsoft Active Directory server, you will have to find out from your system administrator what the user attribute is and enter it in this field.

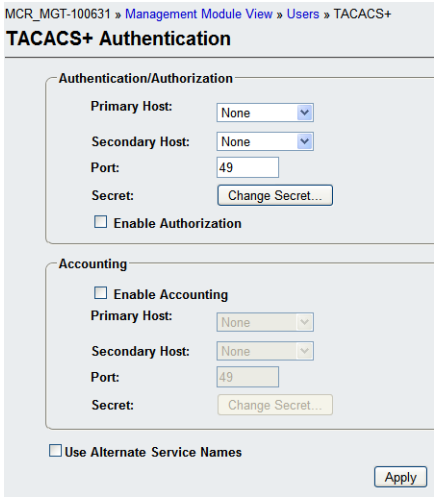
Default: OpenLDAP(uid)

Encrypt Passwords Using MD5 digest	Checking this parameter will cause the Management Module to encrypt the password using MD5 digest before sending it to server. If this option is not checked, the password is sent to the server in the clear. **Default:** Disabled
Authenticate with LDAP server	This option will cause the Management Module to authenticate with the LDAP server before the user authentication takes place. The user name/password to use for this authentication is configured below. **Default:** Disabled
Name	The user name associated with the Management Module.
Append Base to Name	When checked, this causes the domain component configured in the “base” parameter to be appended to the user name. This allows for a fully qualified name to be used when authenticating the Management Module. **Default:** Enabled but if the base parameter is not configured, it does not modify the name.
Password	The password associated with the user name for authenticating the Management Module. **Default:** Blank
Confirm	You must enter the exact same value as the password field. Since the password is not echoed, this ensures that the field was entered correctly. **Default:** Blank
Enable TLS	Enables/disables the Transport Layer Security (TLS) with the LDAP/Microsoft Active Directory host. **Default:** Disabled.
TLS Port	Specify the port number that LDAP/Microsoft Active Directory will use for **TLS**. **Default:** 636

If you are using LDAP or Microsoft Active Directory with **TLS**, you need to Install a CA list to the Management Module that includes the certificate authority (CA) that signed the LDAP certificate on the LDAP host by selecting **Files**, **Keys and Certificates**. See Appendix B, SSL/TLS Ciphers for more information on the LDAP certificate.

TACACS+

Field Descriptions



Configure the following parameter.

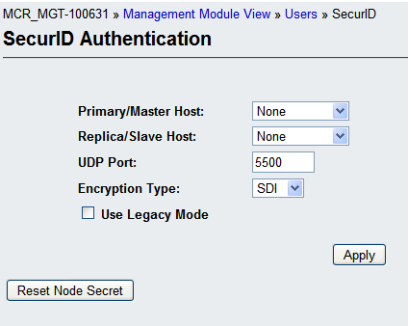
Authentication/ Authorization Primary Host	The primary TACACS+ host that is used for authentication. **Default:** None
Authentication/ Authorization Secondary Host	The secondary TACACS+ host that is used for authentication, should the primary TACACS+ host fail to respond. **Default:** None
Authentication/ Authorization Port	The port number that TACACS+ listens to for authentication requests. **Default:** 49
Authentication/ Authorization Secret	The TACACS+ shared secret is used to encrypt/decrypt TACACS+ packets in communications between two devices. The shared secret may be any alphanumeric string. Each shared secret must be configured on both client and server sides.
Enable Authorization	Enables authorization on the TACACS+ host, meaning that Management Module-specific parameters set in the TACACS+ configuration file can be passed to the Management Module after authentication. **Default:** Disabled
Enable Accounting	Enables/disables TACACS+ accounting. **Default:** Disabled
Accounting Primary Host	The primary TACACS+ host that is used for accounting. **Default:** None
Accounting Secondary Host	The secondary TACACS+ host that is used for accounting, should the primary accounting TACACS+ host fail to respond. **Default:** None

Accounting Port	The port number that TACACS+ listens to for accounting requests. **Default:** 49
Accounting Secret	The TACACS+ shared secret is used to encrypt/decrypt TACACS+ packets in communications between two devices. The shared secret may be any alphanumeric string. Each shared secret must be configured on both client and server sides.
Use Alternate Service Names	The TACACS+ service name for Telnet or SSH is normally “raccess”. The service name for MCR Web Manager is “EXEC”. In some cases, these service names conflicted with services used by Cisco devices. If this is the case, checking this field will cause the service name for Telnet or SSH to be “perlecli” and the service name for MCR Web Manager to be “perleweb”.

SecurID

If you need to reset the SecurID secret, select **Administration, Authentication, Securid, Settings**, **Reset SecurID Node Secret**.

Field Descriptions

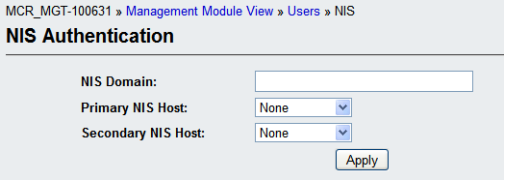


Configure the following parameters.

Primary/Master Host	The first SecurID server that is tried for user authentication. **Default:** None
Replica/Slave Host	If the first SecurID server does not respond to an authentication request, this is the next SecurID server that is tried for user authentication. **Default:** None
UDP Port	The port number that SecurID listens to for authentication requests. **Default:** 5500
Encryption Type	The type of encryption that will be used for SecurID server communication. **Data Options:** DES, SDI **Default:** SDI
Legacy	If you are running SecurID 3.x or 4.x, you need to run in **Legacy Mode**. If you are running SecurID 5.x or above, do not select **Legacy Mode**. **Default:** Disabled
Reset Node Secret	Resets the SecurID secret (password) in the Management Module.

NIS

Field Descriptions



Configure the following parameters.

NIS Domain The NIS domain name.

Primary NIS Host The primary NIS host that is used for authentication.
Default: None

Secondary NIS Host The secondary NIS host that is used for authentication, should the primary NIS host fail to respond.
Default: None

Alerts

The MCR-MGT Management Module supports the ability to provide notification of important events occurring in the system. The events can be communicated via one or more of the following methods;

- Local Event Log
- Email
- Syslog
- SNMP traps

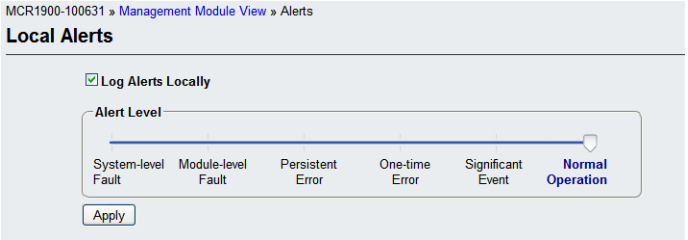
For a complete list of all alerts and their associated level, please see Appendix A, Alert Messages.

Local Event Log

The MCR-MGT Management Module has a built-in local event log. The event log is a circular buffer that can hold up to 200 local event messages. Once the log is full, the oldest entries will be replaced with new entries. The date and time of when the event occurred is recorded with each event.

The local event log buffer will be cleared if the Management Module is rebooted.

Field Descriptions



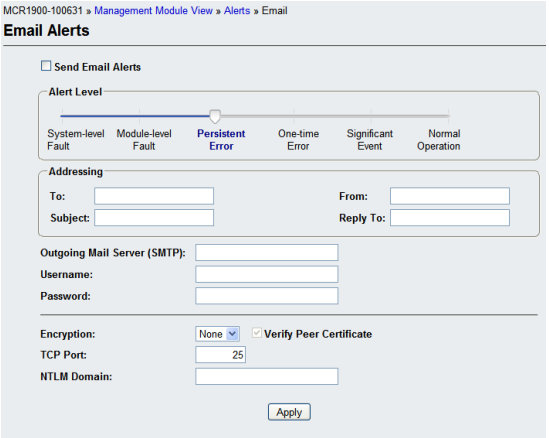
Configure the following parameters:

Log Alerts Locally	When enabled, alert events are logged to the built-in local event log.
Alert Level	Choose the alert level that will trigger a notification to be sent to the local log. **Data Options:** System-level Fault Module Level Fault Persistent Error One-time error Significant Event Normal Operation. **The level selected is the minimum trigger level with the "Normal Operation" being the least severe and "System-level Fault" being the most severe. The level selected will include alerts of that level and all more severe levels above it.** **Default:** Normal Operation

Email Alerts

Email notification requires an SMTP host that is accessible by the Management Module to process the email messages sent by the Management Module.

Field Descriptions



Configure the following parameters:

Send Email Alert
Enables/disables Email Alerts.
Default: Disabled

Email Alert Level
Choose the alert level that will trigger a notification to be sent to the local log.
Data Options:
System-level Fault
Module Level Fault
Persistent Error
One-time error
Significant Event
Normal Operation.
The level selected is the minimum trigger level with the "Normal Operation" being the least severe and "System-level Fault" being the most severe. The level selected will include alerts of that level and all more severe levels above it.
Default: Normal Operation

To
An email address or list of email addresses that will receive the email notification.

Subject
A text string, which can contain spaces, that will display in the **Subject** field of the email notification.

Reply To
The email address to whom all replies to the email notification should go.

Outgoing Mail Server
The SMTP host (email server) that will process the email notification request. This can be either a host name defined in the Management Module host table or the SMTP host IP address.

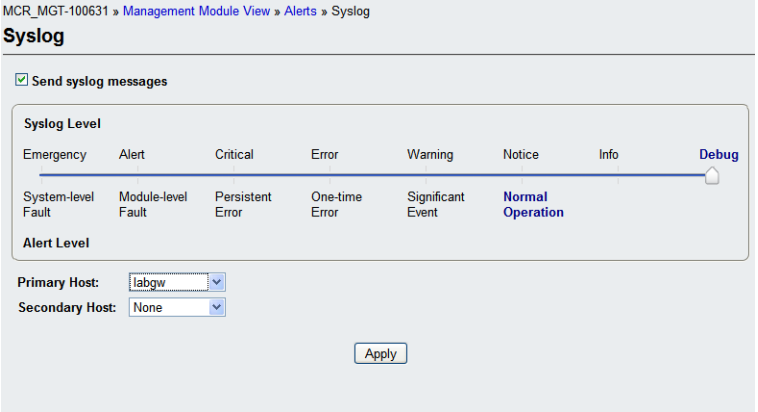
Username
If your mail server requires you to authenticate with it before it will accept email messages, use this field to configure the authorized user name. Maximum size of user name is 64 characters.

Password	Enter the password associated with the user configured in “Username”. Maximum size of password is 64 characters.
Encryption	Choose the type of encryption desired. Valid options are; None - All information is sent in the clear. ● TLS - Select this if your email server requires TLSAll data from previous connections on that serial port has drained ● SSL - Select this if your email server requires SSL
Verify Peer Certificate	When checked this will enable the validation of the certificate presented by the email server. To validate the certificate, you will need to download the appropriate CA list into the Management Module. If the certificate is not found to be valid, the communication with the email server will be terminated. No authentication will take place and the email message will not be forwarded to the email server. If this option is not checked, the certificate validation will still be attempted but if it fails, a syslog message will be generated but the authentication and forwarding of the email will still take place. **Default:** Enabled if SSL or TLS encryption is selected. Disabled if no encryption is selected.
TCP Port	This is the TCP port used to communicate with the email server. **Default:** 25 for non-SSL, 465 if SSL/TLS is used
NTLM Domain	This field is only used if SPA authentication is performed with the email server. It may or may not be required. If the email server does not expect this field, it can be left blank.

Syslog

The Management Module can be configured to send system log messages to a syslog daemon running on a remote host if the **Syslog** service is activated. You can configure a primary and secondary host for the syslog information and specify the level for which you want syslog information sent.

Field Descriptions



Configure the following parameters:

Send Syslog Alert
Enable/disable syslog alert settings.
Default: Disabled

Syslog Level
Choose the alert level that will trigger a syslog message to be sent.
Data Options:

- Emergency (System-level Fault)
- Alert (Module Level Fault)
- Critical (Persistent Error)
- Error (One-time error)
- Warning (Significant Event)
- Notice (Normal Operation)
- Info
- Debug

The level selected is the minimum trigger level with the "Debug" being the least severe and "System-level Fault" being the most severe. The level selected will include alerts of that level and all more severe levels above it.
Default: Normal Operation

Primary Host
The Primary Host where syslog alerts will be send.

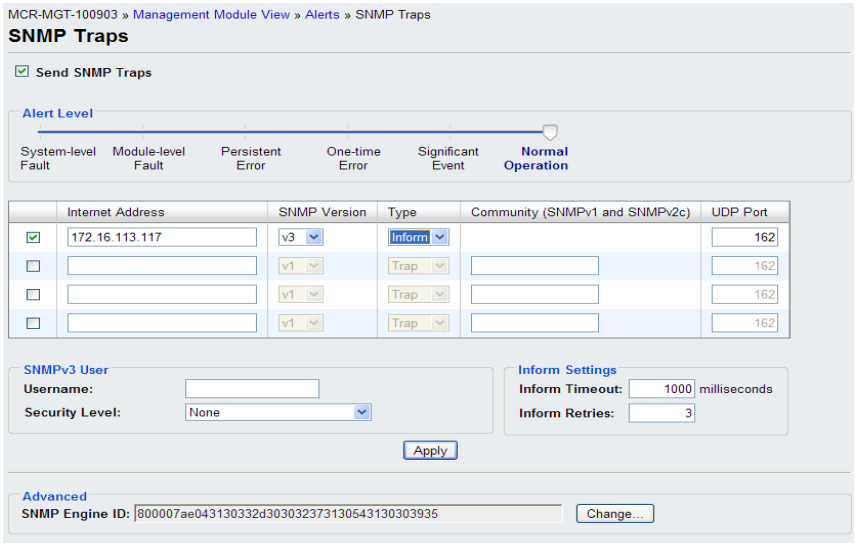
Secondary Host
The Secondary Host where the syslog alerts will be send.

SNMP Traps

If MCR-MGT Management Module supports the use of SNMP traps to communicate significant events to an SNMP trap host. Up to 4 trap hosts can be defined to receive the traps. Each host can be configured independently for the version of traps that it supports.

The MCR-MGT Management Module supports v1, v2c and v3 traps.

Field Descriptions



Configure the following parameters:

Send SNMP Traps Enables/Disables SNMP Alerts.

Default: Disabled

Alert level

Choose the alert level that will trigger an SNMP trap to be sent.

Data Options:

- System-level Fault
- Module Level Fault
- Persistent Error
- One-time error
- Significant Event
- Normal Operation.

The level selected is the minimum trigger level with the "Normal Operation**" being the least severe and "System-level Fault" being the most severe. The level selected will include alerts of that level and all more severe levels above it.**

Default: Normal Operation

Trap checkbox Check this box to enable the entry for this trap host.

Default: Disabled

Internet Address Enter the IP address of the host you wish to send the trap to.

Field Format: IPv4 or IPv6 address

SNMP Version	Defines the SNMP version of the traps sent to the specified host. If v3 is selected then the SNMP trap v3 user will be used to authenticate the trap with the specified host. Valid options are v1, v2c or v3. **Default:** v1
Type	This field is ignored for trap host version v1" Data Options: Trap -Management module will send traps via a TRAP_PDU or TRAP2-PDU not expecting any response from the specified host. Inform -Management module will send traps via an INFORM_PDU, expecting a response from the specified host. Default: Trap
Community	The name of the group that devcies and management stations running SNMP belong to. This applies to SNMP version 1 and version 2c.
UDP Port	Enter the UDP port number that the SNMP trap host is listening on for UDP traps. **Default:** 162
SNMP V3 User	This section is used to configure the attributes associated with a trap "user". It is only used if the trap version is set to V3.
User Name	This field identifies the system sending the traps to the host receiving the traps. Same user name is used for all V3 traps sent by this system.
Security Level	Select the security level for the user. This must match the configuration set up in the SNMP manager. **Data Options:** ● **None**—No security is used. ● **Auth**—User Authtication is used. ● **Auth/Priv**—User authentication and privacy (encryption) settings are used. **Default:** None
Authentication Algorithm	Specify the authentiation algorithm that will be used for the user. **Data Options:** MD5, SHA **Default:** MD5
Authentication Password	Type in the user's authentication password.
Confirm Authentication Password	Retype the user's authentication password.
PrivacyAlgorithm	Specifiy the encryption algorithm to be used with this user. **Data Options:** DES, AES **Default:** DES
Privacy Password	Type in the user's privacy password.

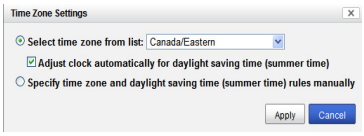
Confirm Password	Retype the privacy password.
Inform Retires	This is only used for "Inform" traps. Select the number of seconds to wait for the acknowledgement of the trap. **Default:** 1 second
Inform Retries	This is only used for "Inform" traps. Select the number of times the trap will be sent if no acknowledgement is received. **Default:** 3
SNMP Engine ID	The engine ID is used to help identify the trap sender to the trap receiver when using v3 traps. It is a unique identifier of the SNMP agent in the domain. By default the Engine ID is composed using the serial number of the Management Module which should make it unique. If you wish to assign a different engine ID to this node, click on the "Change" button. When changing the engine ID, the string entered in this field will be combined with other required elements to form the EngineID. It is up to the user to ensure that this will be a unique string.

Date and Time

The Management Module has a real-time internal clock, allowing the date and time to be set and viewed. It will maintain the time over a short power outage and after reboots of the Management Module. If you do not set the time, it will start the clock at the factory set time.

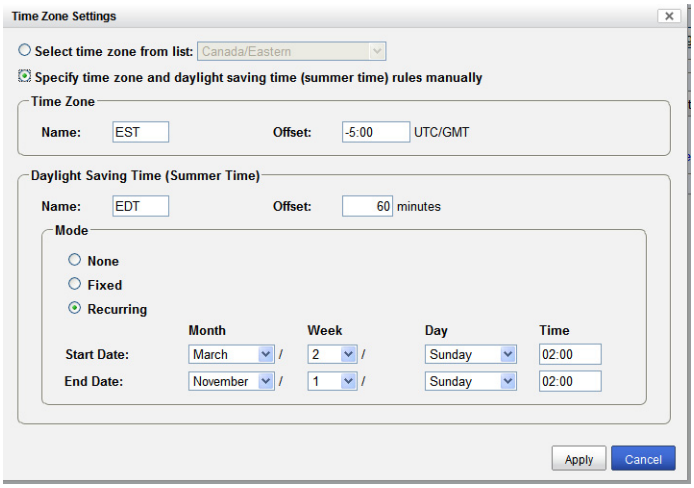
Time Zone Settings

You can set standard and summer time (daylight savings time) in the Management Module. You can specify the summer time settings as absolute, on a fixed date and time, or relative, on something like the third day of the third week at this time in June.



- Select time zone from list:
- Adjust clock automatically for daylight saving time
- Specific time zone and daylight saving time rules manually Time Zone/Summer Time Tab Field Descriptions

Field Descriptions



Configure the following parameters:

Time Zone Name

The name of the time zone to be displayed during standard time.

Field Format: Maximum 4 characters and minimum 3 characters (do not use angled brackets < >)

Time Zone Offset

The offset from UTC for your local time zone.

Field Format: Hours *hh* (valid -12 to +14) and minutes *mm* (valid 0 to 59 minutes)

Summer Time Name

The name of the configured summer time zone; this will be displayed during the summer time setting. If this parameter is not set, then the summertime feature will not work.

Field Format: Maximum 4 characters and minimum 3 characters (do not use angled brackets < >)

Summer Time Offset

The offset from standard time in minutes. Valid values are 0 to 180.

Range: 0-180

Default: 60

Summer Time Mode

You can configure the summer time to take effect:

- **None**—No summer time change.
- **Fixed**—The summer time change goes into effect at the specified time every year. For example, April 15 at 1:00 pm.
- **Recurring**—The summer time changes goes into effect every year at same relative time. For example, on the third week in April on a Tuesday at 1:00 pm.

Default: None

Fixed Start Date

Sets the exact date and time in which the Management Module's clock will change to summer time (daylight saving time) hours.

Fixed End Date

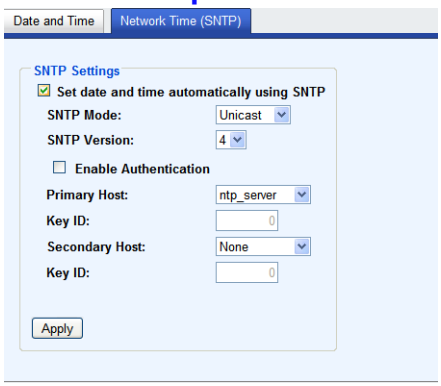
Sets the exact date and time in which the Management Module's clock will end summer time hours and change to standard time.

Recurring Start Date	Sets the relative date and time in which the Management Module's clock will change to summer time (daylight saving time) hours. Sunday is considered the first day of the week.
Recurring End Date	Sets the relative date and time in which the Management Module's clock will end summer time hours and change to standard time. Sunday is considered the first day of the week.

Network Time Tab

You can configure your SNTP client in the Management Module to automatically synchronize the Management Module's time.

Field Descriptions



Configure the following parameters.

SNTP Mode — The SNTP mode. The SNTP client listens on UDP port 123.

Data Options:

- **None**—SNTP is turned off.
- **Unicast**—Sends a request packet periodically to the Primary host. If communication with the Primary host fails, the request will be sent to the Secondary host.
- **Multicast**—Listen for any broadcasts from an SNTP server and then synchronizes its internal clock to the message.
- **Anycast**—Sends a request packet as a broadcast on the LAN to get a response from any SNTP server. The first response that is received is used to synchronize its internal clock and then operates in **Unicast** mode with that SNTP server.

Default: None

SNTP Version — Version of SNTP.

Range: 1-4

Default: 4

Enable Authentication — Sets SNTP server authentication on or off

Default: Off

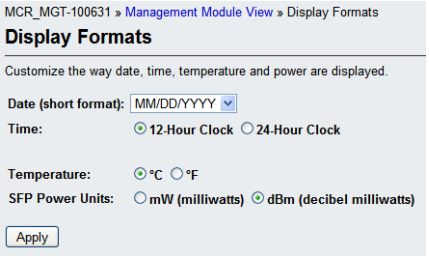
Primary Host — The name of the primary SNTP server from the Management Module host table. Valid with **Unicast** and **Multicast** modes, although in **Multicast** mode, the Management Module will only accept broadcasts from the specified host SNTP server.

Secondary Host	The name of the secondary SNTP server from the Management Module host table. Valid with **Unicast** and **Multicast** modes, although in **Multicast** mode, the Management Module will only accept broadcasts from the specified host SNTP server.
Key ID	Specify the key id associated with this host. This key must exist in the sntp (symmetric key) file that was downloaded to the MCR-MGT management card. **Valid Key ID's: 1-65534** (**Note:** the structure for the sntp (symmetric key) file can be found in this guide. Appendix F, Symmetric Key File

Display Formats

The Display Format tab allows you to customize the way date, time, temperature and power are displayed.

Field Descriptions



Configure the following parameters:

Date	The Date can be express in the following formats: ● MM/DD/YYYY ● DD/MM/YYYY ● YYYY-MM-DD **Default**: MM/DD/YYYY
Date	Time can be express in the following formats: ● 12-Hour Clock ● 24-Hour Clock **Default**: 12-Hour Clock
Temperature	Temperature can be expressed as Celsius or Fahrenheit
SFP Power Units	Power can be expressed in mW(milliwatts) or dBm (decibel milliwatts) for SFP modules.

Files

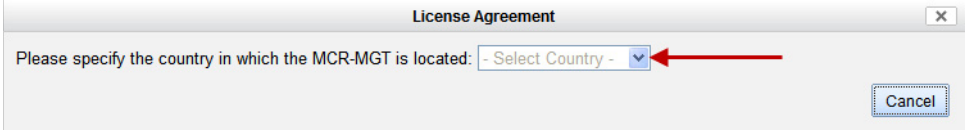
Firmware

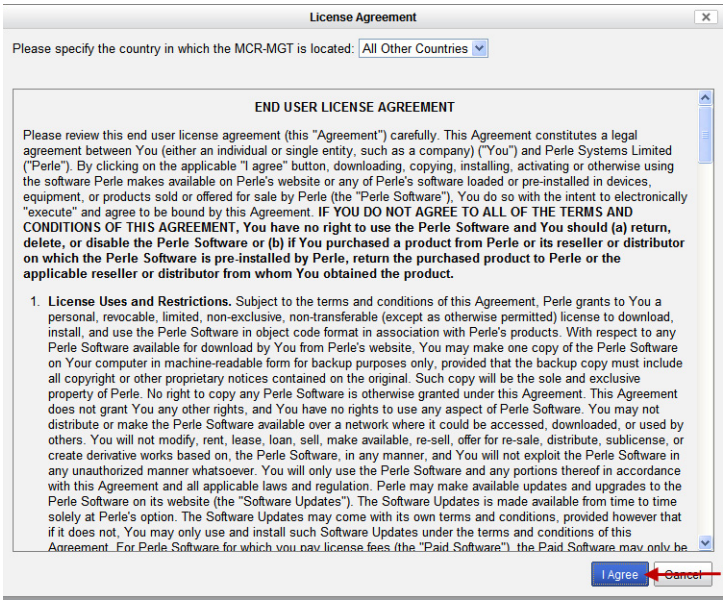
Allows you to update new firmware to the Management Module and any installed Media Converter Modules.

You can choose to use TFTP or HTTP as the method of transferring the files. If TFTP is used, you must have a TFTP server set up with the firmware files residing on it. With HTTP, you can use the same PC as the one which your browser is running on without the need for any additional software.

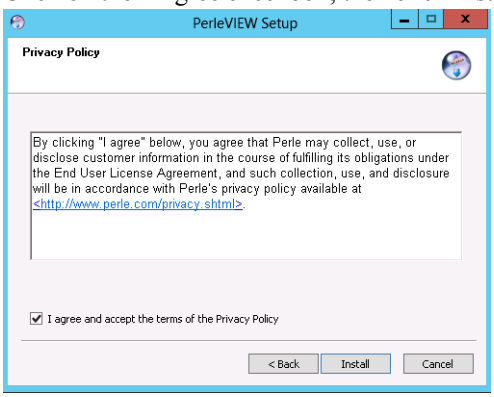
You must agree to the Perle Licensing Agreement and the Privacy Policy in order to download firmware.

When the Licensing Agreement window appears, specify your country. If you reside in Germany you must select “Germany” as your country. Germany has unique licensing requirements. After selecting your country click on the I Agree button.



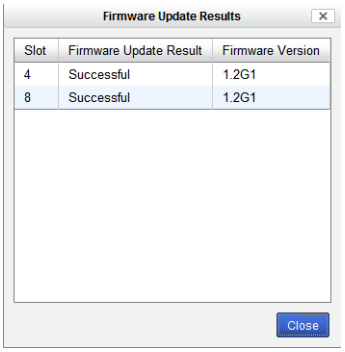


Click on the I Agree checkbox, then click Install.



The download will now continue and firmware will be downloaded to each of the modules specified.

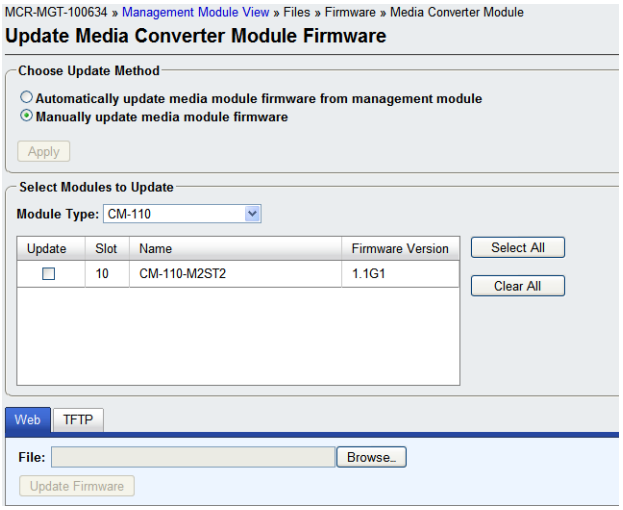
After the download has completed, a status dialog will appear.



MCR 1900 Media Converter Module Firmware Update

Manual Update

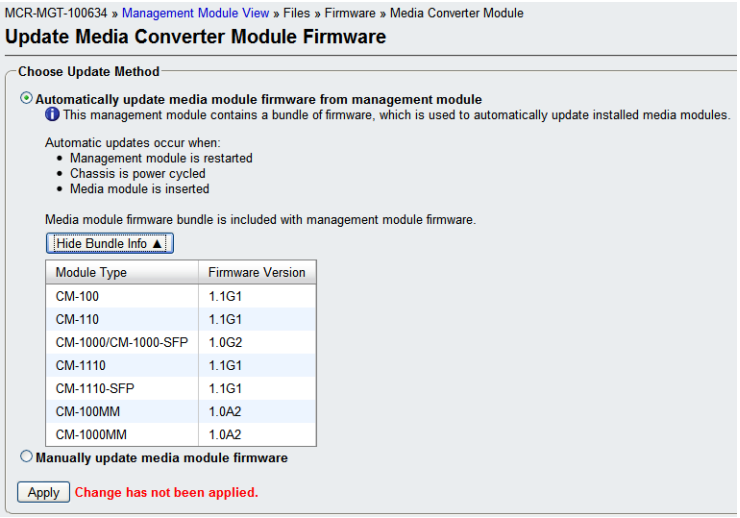
Manually update one or more managed Media Converter Modules of the same type.



1. From the drop down box, select the Module Type.
2. Displayed is a list of slots which contain this Module Type.
3. Select Update for each module to be upgraded.
4. Either select Web or TFTP to perform the firmware update.

Automatic Update

Automatically update managed Media Converter Modules. Only media converter modules that are running older versions of the firmware will be updated.



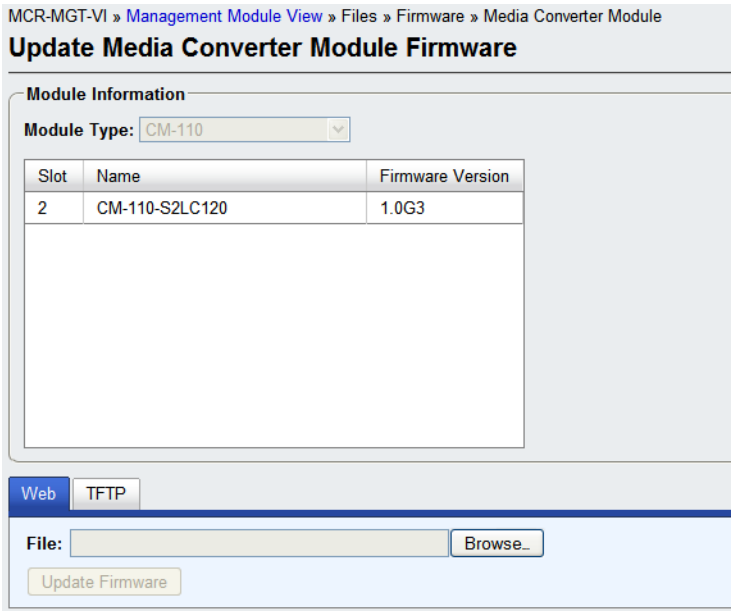
The Media Converter Module firmware bundle is included with management module firmware. Automatic updates will occur when the:

- Management Module is restarted
- Chassis is power cycled
- Media Converter Module is inserted

Note: Remember to click the Apply button to save your configuration changes.

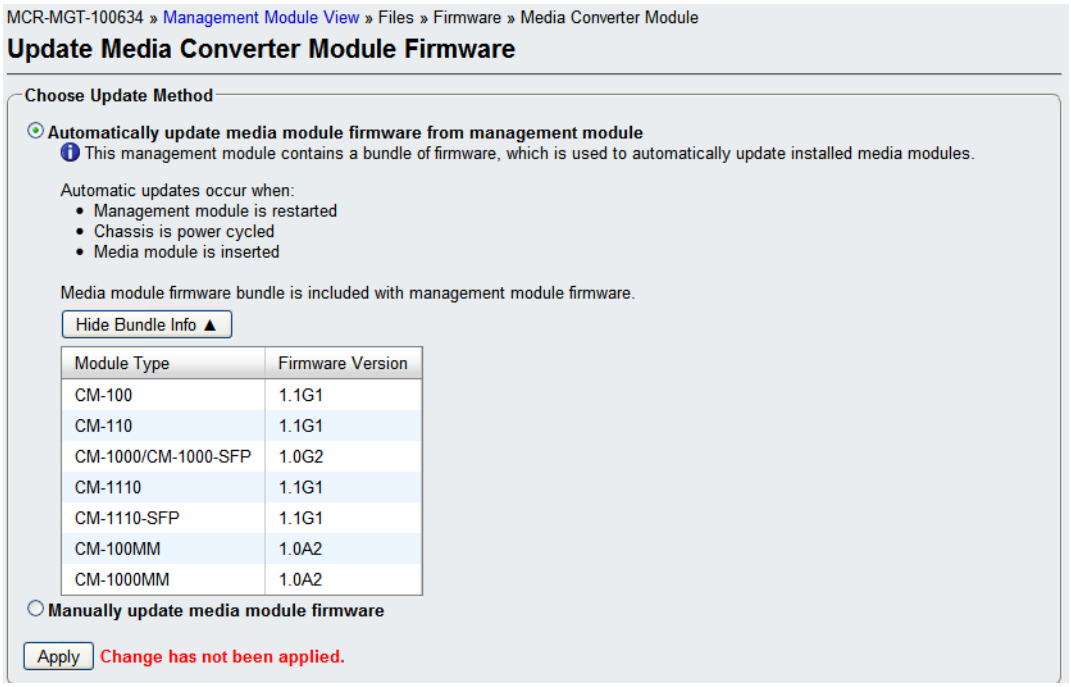
SMI Media Converter Firmware Update

Manual Update



The managed Media Converter Module to be updated will be shown. Either select Web or TFTP to perform the firmware update.

Automatic Update



The Media Converter Module firmware bundle is included with management module firmware. Automatic updates will occur when the:

- Management Module is restarted
- Chassis is power cycled
- Managed Media Converter Module is inserted

Note: Remember to click the Apply button to save your configuration changes.

Configuration

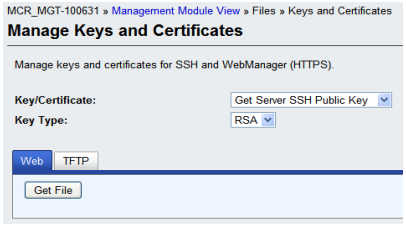
This option allows you to Backup and Restore configuration files. You can choose to backup the configuration in Binary (native) format or as a text file. The text file can be viewed and edited with a standard text editor.

Keys and Certificates

Allows you to install Keys and Certificates to the Management Module. See Appendix B, SSL/TLS Ciphers for more information.

Manage SSL Keys

Field Descriptions



Configure the following parameter

Key/Certificate — Select key or certificate to be transferred to or from the management module.

Data Options:

- Get Server SSH Public Key.
- Install SSH User Public Key.
- Install SSL/TLS Private Key, required if using HTTPS and/or SSL/TLS
- Install SSL/TLS Certificate, required if using HTTPS and/or SSL/TLS.
- Install SSL/TLS CA, required if using LDAP/Microsoft Active Directory with TLS, SSL/TLS.
- Install SNTP Keys File, required if using SNTP authentication.

Key Type — Specify the key type that will be used for SSH/SSL.

Data Options:

- **RSA**
- **DSA**

Web/TFTP — Choose the method by which to download/upload keys/certificates. TFTP requires a TFTP server to be accessible by the MCR-MGT management module.

Diagnostic File

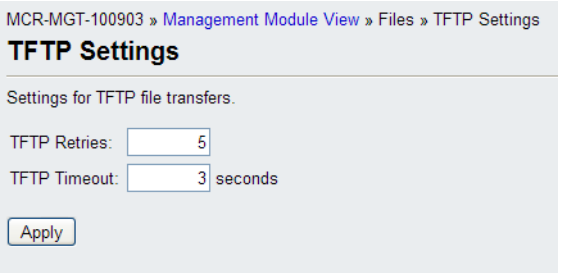
Should the Management Module experience any problems, a Perle Technical support representative may ask you to get this file and sent it to us. Uploading this file will permanently remove it from the non-volatile memory on the MCR-MGT Management Module.

Bootup Files

Provides the ability to configure the host and file name from which the firmware and/or configuration for the MCR-MGT Management Module can be retrieved from when the module is booted. A check will be made to determine if the filename has changed since the previous load. If it matches the name of the file downloaded previously, no download will occur. The files must reside on a TFTP server which is accessible to the MCR-MGT Management Module.

TFTP Settings

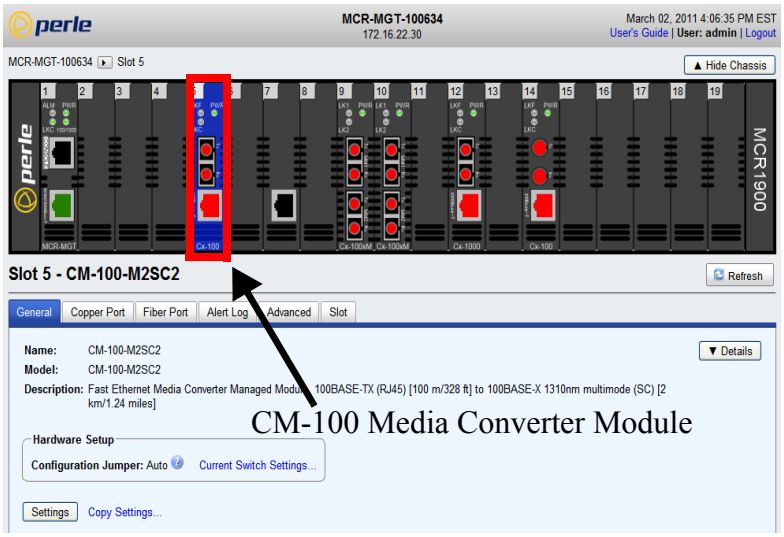
Provides the ability to configure the timeout and number of retires when doing a TFTP file transfer.



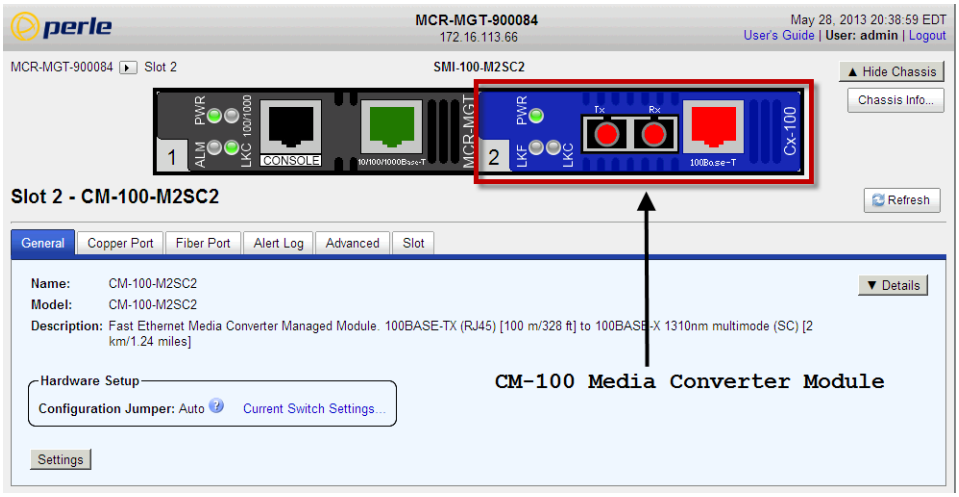
7 CM-100 Media Converter Module

CM-100 Media Converter Module Parameters

MCR1900 Chassis

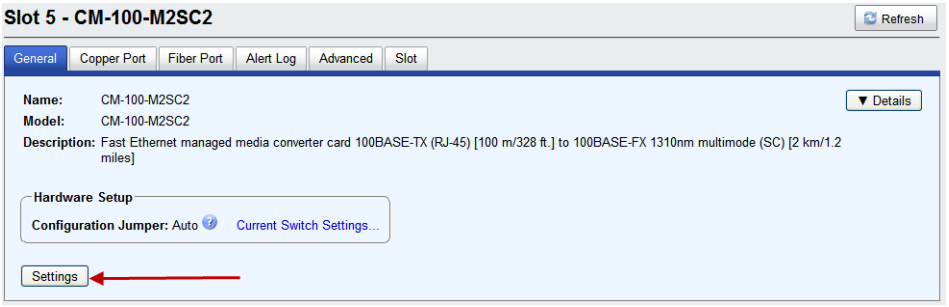


SMI Chassis



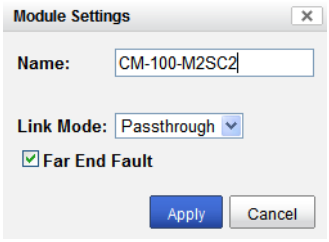
General Tab

Field Descriptions



Name	Displays the configured name for this Module.
Model	Displays the module's model information.
Description	Displays a description of the Module that is inserted in this slot.
Configuration Jumper	**Auto:** Use software configuration if present, otherwise use hardware DIP switch settings. **Switch:** Use hardware DIP switch settings. For detailed information on hardware DIP switch settings, see the Hardware Installation Guide.
Current Switch Settings	Displays the current DIP switch settings. For detailed information on hardware jumpers and DIP settings, see the Hardware Installation Guide.
Details	Displays the firmware's details.

Settings



Name	Displays the configured name for this Module.

Link Mode

Smart Link Pass-Through: In this mode, the link state on one connection is directly reflected through the Media Converter Module to the other connection. If link is lost on one of the connections, then the other link will be brought down by the Media Converter.

Standard: In this mode, the links on the fiber and copper sides can be brought up and down independently of each other. A loss of link on either the fiber or copper port can occur without affecting the other connection.

Default: Smart Link Passthrough

Far End Fault

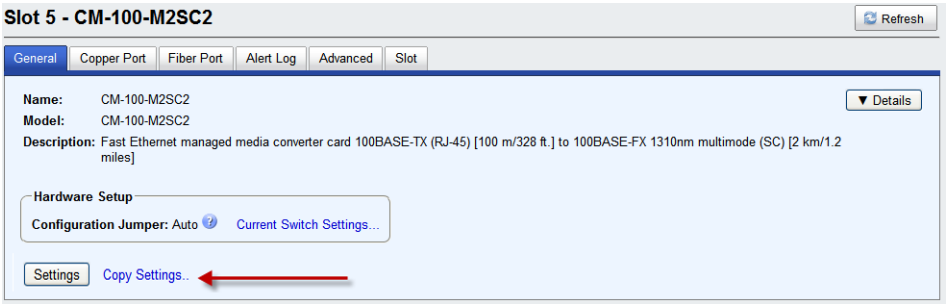
When enabled, if the Media Converter Module detects a loss of signal on the fiber receiver, it will transmit a FEF signal to the remote Media Converter Module. This, in effect, notifies the fiber link partner that an error condition exists on the fiber connection.

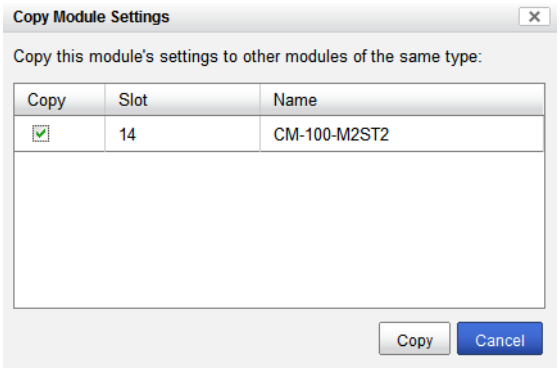
Note: This feature only takes effect if Auto Negotiation has been turned off.

When disabled, the Media Converter Module will not monitor for or generate Far End Fault.

Default: On

Copy Settings



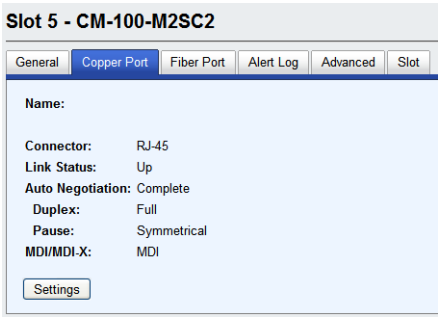


Copy Module Settings

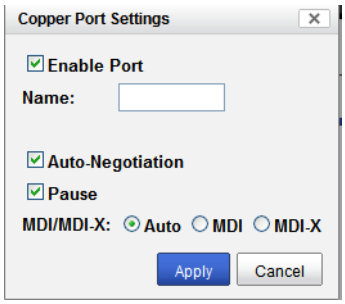
Copy this module's settings to other modules of the same type.

Copper Port Tab

Copper Port > Settings



Settings



Configure the following parameter.

Enable Port
Enables/Disables the copper port.
Default: Enable

Name
The name of the copper port.
Field Format: 8 characters

Auto-Negotiation
When enabled, the Media Converter Module will negotiate with its link partner to determine the most optimal parameters for this connection.

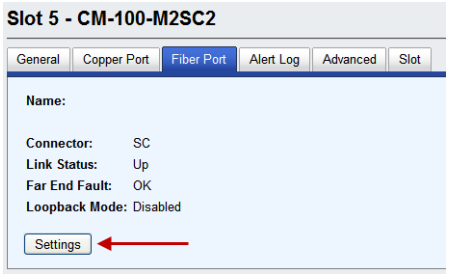
Pause
When enabled, the Media Converter Module will advertise its Pause capabilities.

MDI/MDXI
- **Auto-Detect—** automatically detects the Ethernet's cable polarity
- **MDI —**the cable's polarity is straight-through
- **MDI-X** —the cable's polarity is crossovered

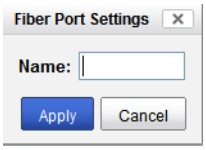
Default: Auto-Detect

Fiber Port Tab

Fiber Port Settings



Settings

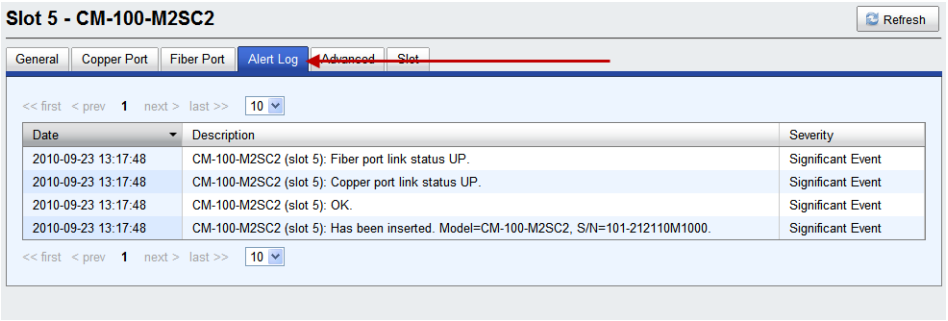


Configure the following parameter:

Name — The name of the fiber port.
Field Format: 8 characters

Alert Log Tab

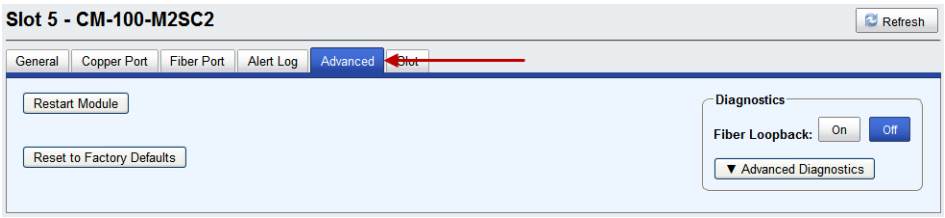
Field Descriptions



Displays the current local Alerts. The local Alert buffer contains the last 200 alerts and displays these events in a wrap around fashion.

Advanced Tab

Field Descriptions

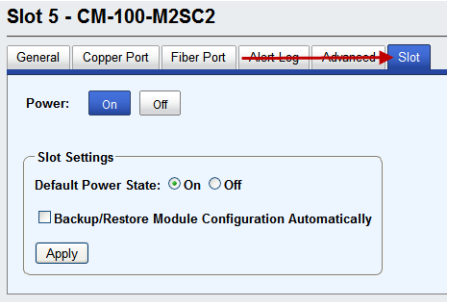


Configure the following parameter:

Restart Module	Restarts this Media Converter Module.
Reset to Factory Defaults	Resets this Media Converter Module back to factory defaults.
Diagnostics	
Fiber Loopback	**Off:** This is the normal setting. In this setting, data received on the fiber port will be passed through the Media Converter Module. **On:** This is a test mode. All data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection. **Default:** Off
Advanced Diagnostics, Read/Write Register	This feature should only be used if guided by a Perle Technical Support Representative. Use of this feature without guidance from a Perle Technical Support Representative could make your Media Converter Module inoperable.

Slot Tab

Field Descriptions



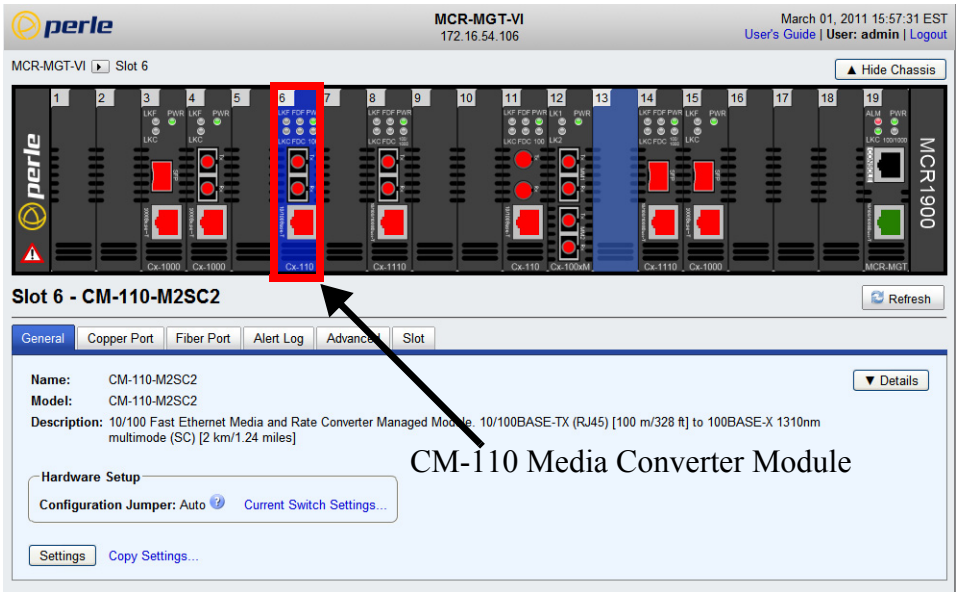
Configure the following parameters:

Power	Immediately power the slot on or off. The current state of the slot is highlighted in BLUE. Press the "ON" button to immediately power the slot on. Press the "OFF" button to immediately power the slot off.
Default Power State	This is the default power state of the slot when the chassis is powered up or restarted. **Default:** On
Backup/Restore	**Enabled:** The configuration information associated with this slot is saved on the Management Module and will be downloaded to the Media Converter Module whenever the Media Converter Module is inserted into this slot. **Disabled:** The Media Converter Module configuration information is only kept on this Module. **Default**: Disabled

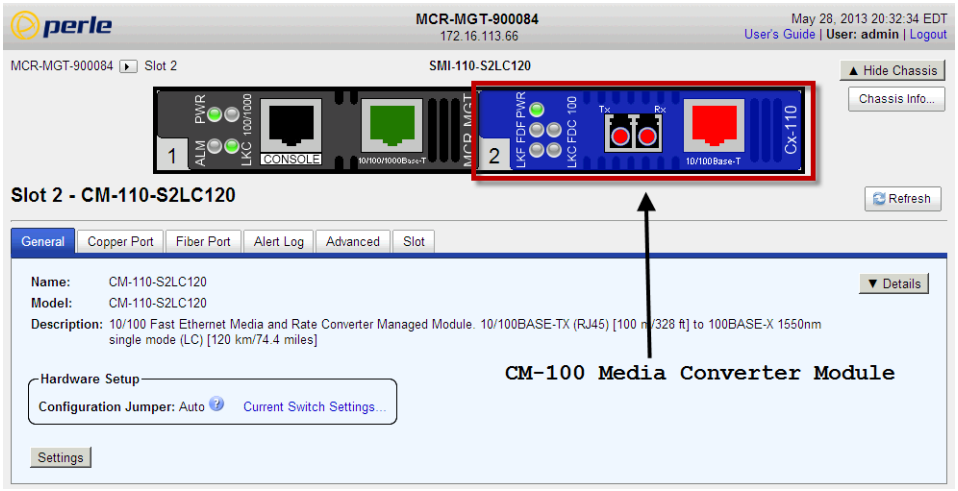
8 CM-110 Media Converter Module

CM-110 Media Converter Module Parameters

MCR1900 Chassis

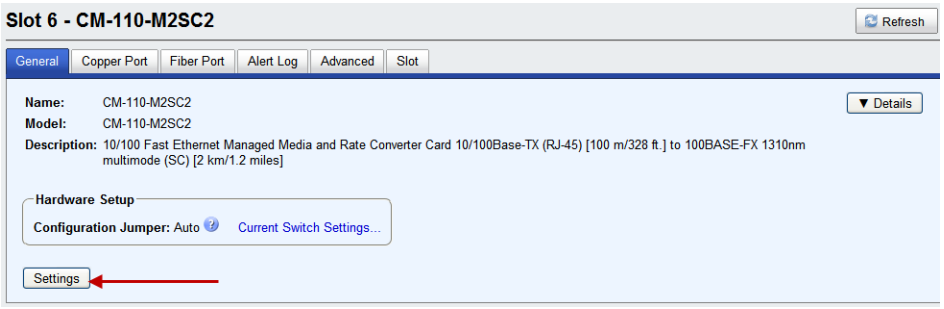


SMI Chassis

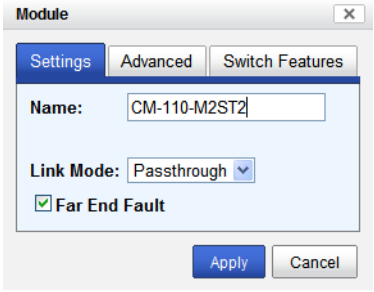


General Tab

General > Settings



Name	Displays the configured name for this Module.
Model	Displays the module's model information.
Description	Displays a description of the Module that is inserted in this slot.
Configuration Jumper	**Auto:** Use software configuration if present, otherwise use hardware DIP switch settings. **Switch:** Use hardware DIP switch settings. For detailed information on hardware DIP switch settings, see the Hardware Installation Guide.
Current Switch Settings	Displays the current DIP switch settings. For detailed information on hardware jumpers and DIP settings, see the Hardware Installation Guide.
Details	Displays the firmware's details.



Configure the following parameters.

Name — Displays the configured name for this Module.

Link Mode — **Standard:** In this mode, the links on the fiber and copper sides can be brought up and down independently of each other. A loss of link on either the fiber or copper port can occur without affecting the other connection.

Smart Link Pass-Through: In this mode, the link state on one connection is directly reflected through the Media Converter Module to the other connection. If link is lost on one of the connections, then the other link will be brought down by the Media Converter.

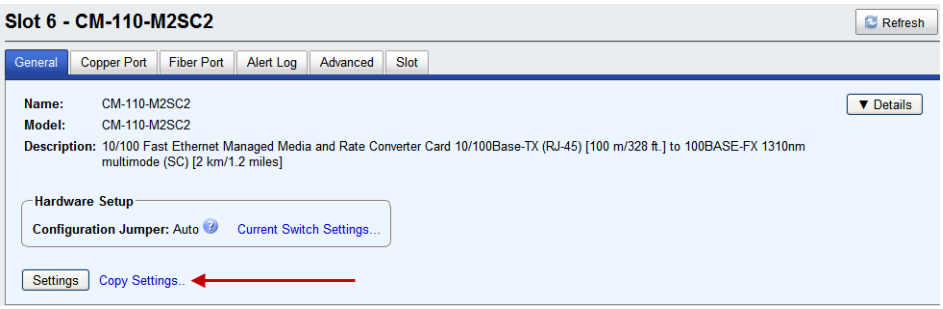
Default: Smart Link Pass-Through

Far End Fault — When enabled, if the Media Converter Module detects a loss of signal on the fiber receiver, it will trasmit a FEF signal to the remote Media Converter Module. This, in effect, notifies the fiber link partner that an error conditiion exists on the fiber connection.

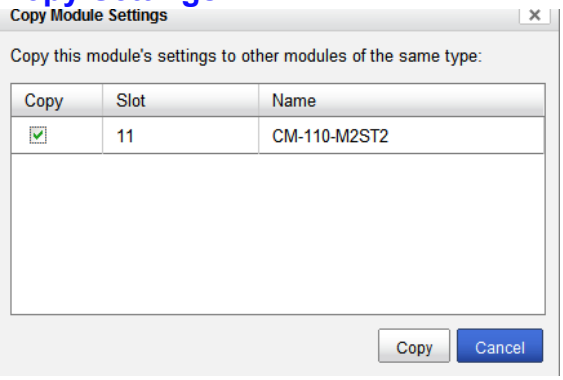
Note: This feature only takes effect if Auto Negotiation has been turned off.

When disabled, the Media Converter Module will not monitor for or generate Far End Fault.

Default: Enabled



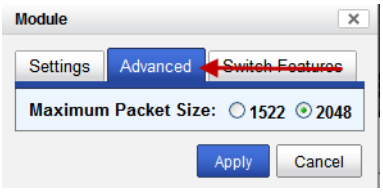
Copy Settings



Copy Module Settings

Copy this module's settings to other modules of the same type.

General > Settings > Advanced



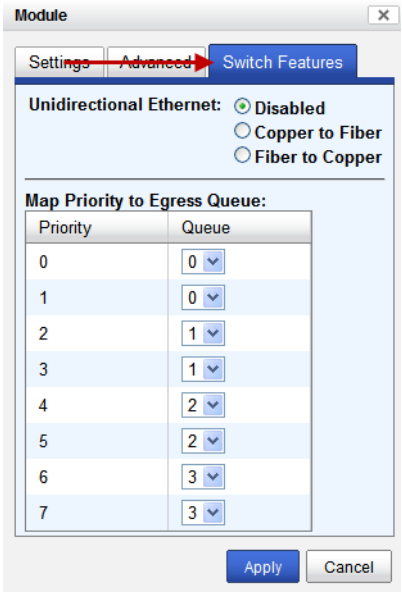
Maximum Packet Size

Select the maximum packet size.

Options: 1522 bytes or 2048 bytes

Default: 2048

General > Settings > Switch Features



Configure the following parameters.

Unidirectional Ethernet

When enabled, this feature provides the ability to restrict the flow of data between the Copper and fiber ports.

Values:

- Disabled
- Copper to Fiber
- Fiber to Copper

Default: Disabled

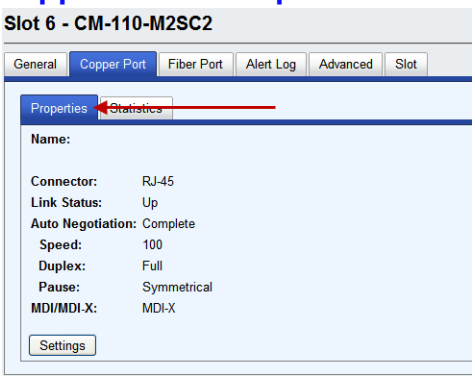
Map Priority to Egress

This is the **default** egress priority mapping for both the copper and fiber ports.

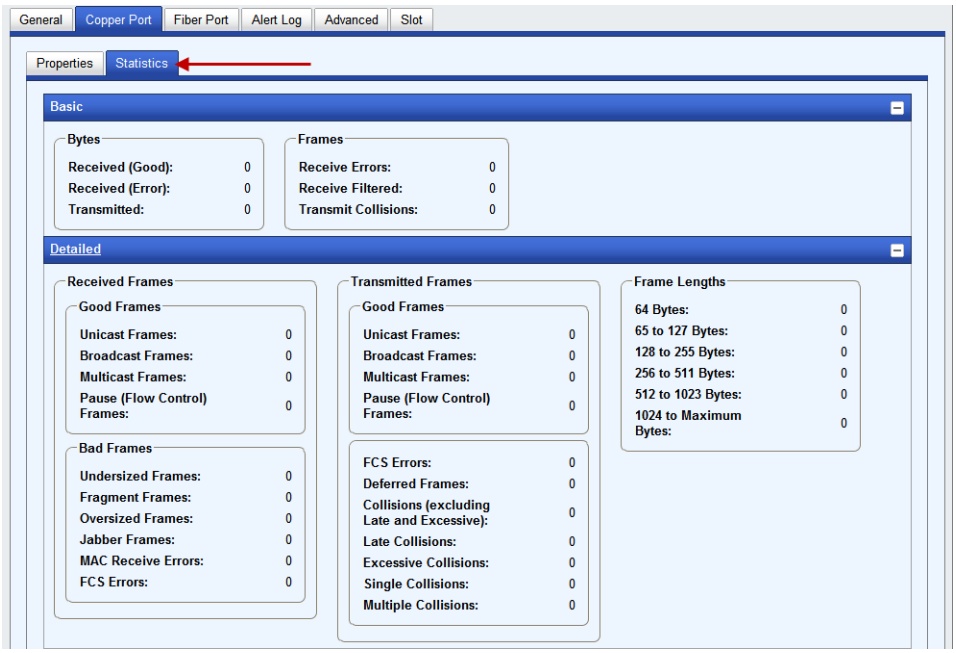
- Priority 0 (lowest priority).....Queue 0
- Priority 1 .....Queue 0
- Priority 2 .....Queue 1
- Priority 3 .....Queue 1
- Priority 4 .....Queue 2
- Priority 5 .....Queue 2
- Priority 6 .....Queue 3
- Priority 7 (highest priority) ....Queue 3

Copper Port Tab

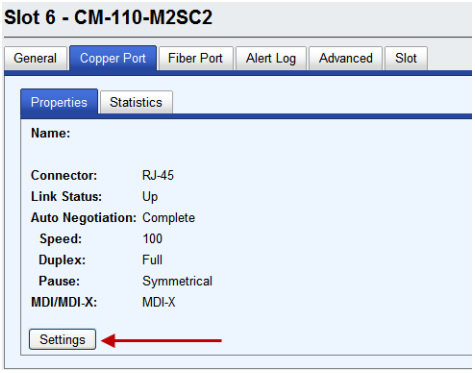
Copper Port > Properties



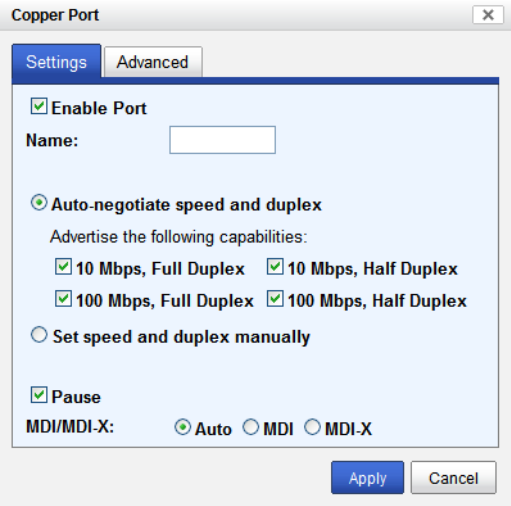
Copper Port - Statistics



Copper Port > Properties



Copper Port > Settings (Auto negotiate speed and duplex)



Configure the following parameters.

Enable Port
Enables/Disables the copper port.
Default: Enable

Name
The name of the copper port.
Field Format: 8 characters

Auto Negotiate Speed and Duplex
When enabled, the Media Converter Module will negotiate with its link partner to determine the most optimal parameters for this connection.
Advertise capabilities of:

- 10 Mbps, Full Duplex
- 100 Mbps, Full Duplex
- 10 Mbps, Half Duplex
- 100 Mbps, Half Duplex

Set Speed and Duplex Manually
When enabled, the following selections are available:
Speed: 100 Mbps, 10 Mbps
Duplex: Full, Half

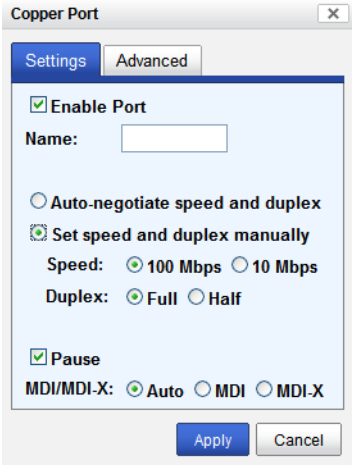
Pause
When enabled, the Media Converter Module will advertise its Pause capabilities.

MDI/MDI-X

- **Auto-Detect—** automatically detects the Ethernet's cable polarity
- **MDI —**the cable's polarity is straight-through
- **MDI-X** —the cable's polarity is crossovered

Default: Auto

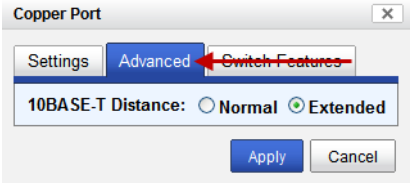
Copper Port > Settings (Set speed and duplex manually)



Configure the following parameters.

Set Speed and Duplex Manually	When enabled, the following selections are available: **Speed:** 100 Mbps, 10 Mbps **Duplex:** Full, Half

Copper Port > Advanced



Configure the following parameters.

10BASE-T Distance	**Normal:** the Media Converter copper link is in normal operating mode. **Extended:** the Media Converter will boost the signal strength on its copper link.

Switch Features

Copper Port > Switch Features > Priority

Configure the following parameters.

Enable 802.1p Priority — When enabled, the media converter module will use IEEE 802.1p tagged frame priority control to assign ingress frames to the appropriate priority egress queue.
Default: Enabled

Enable IP TOS Priority — When enabled, the media converter module will use IPv4 Diffserv or IPv6 traffic class field to assign ingress frames to the appropriate priority egress queue.
Default: Enabled

Priority Precedence — When both 802.1p priority and IP TOS priority are selected, you can select which of the two priorities takes precedence.
Default: 802.1p

Remap Priority

Remap IEEE 802.1p ingress frames with a new priority tag. This new priority tag will be used to determine which queue the frame gets posted to.

Original Priority -----> New Priority

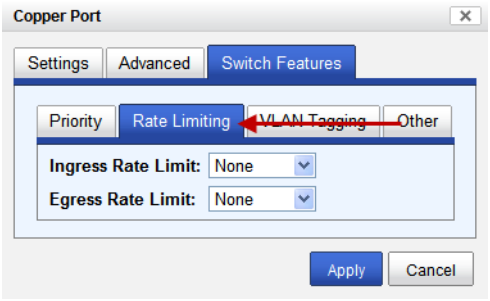
Values: 0-7

Congestion Policy

Select a method to be used when determining the order by which frames are sent from the four egress queues. Setting the congestion policy on either the fiber or copper port will change the policy on both ports.
Strict Priority Queuing - The order is determined strictly by the priority of the queue. Frames in higher priority queues are always sent ahead of frames in lower priority queues.
Weighted Fair Queuing - This method allows lower priority frames to be inter-mixed with higher priority frames in the ratio of (**8, 4, 2, 1**).
The ratio for 8 highest priority sent frames will be as follows:
8 highest priority frames from queue 3
4 frames from queue 2
2 frames from queue 1
1 frame from queue 0

Default: Strict Priority Queuing

Copper Port > Switch Features > Rate Limiting



Configure the following parameters.

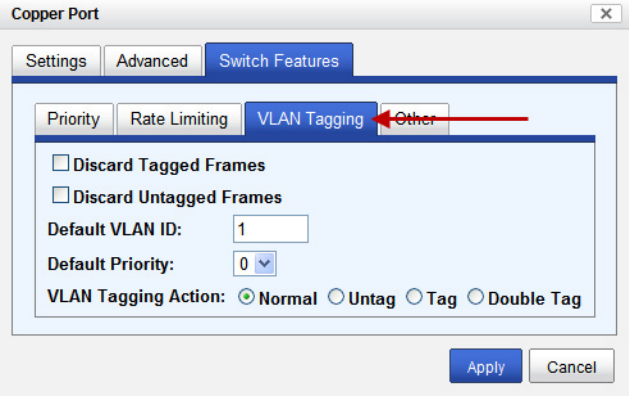
Ingress Rate Limit

Restricts ingress frames on the copper port.
Default: None
Data Options: 64 kbps to 90 Mbps

Egress Rate Limit

Restricts egress frames on the copper port.
Default: None
Data Options: 64 kbps to 90 Mbps

Copper Port > Switch Features- VLAN Tagging



Configure the following parameters.

Discard Tagged Frames
When enabled, discards all VLAN tagged frames.
Default: Off

Discard Untagged Frames
When enabled, discards all VLAN untagged frames.
Default: Off

Default VLAN ID
Specify a default VLAN ID to insert when tagging frames.
Default: 1
Data Options: 0-4095

Default Priority
Specify a default VLAN priority to insert when tagging frames.
Default: 0
Data Options: 0-7

VLAN Tagging Actions
Define the VLAN tagging action to take on a egress frame.

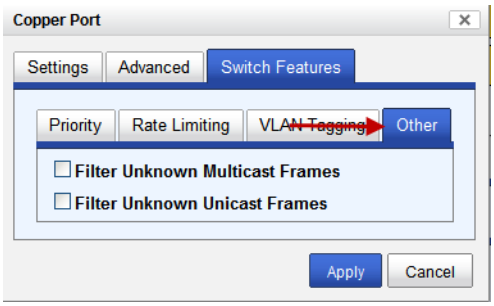
- Normal -Take no action.
- Untag - Remove any existing tag.
- Tag

  Insert tag with configured VLAN ID and VLAN priority if original frame is untagged.

  Replace tag with configured VLAN ID and VLAN priority if original frame is tagged.
- Double tag - Append a tag with configured VLAN ID and VLAN priority.

Default: Normal

Copper Port > Switch Features > Other

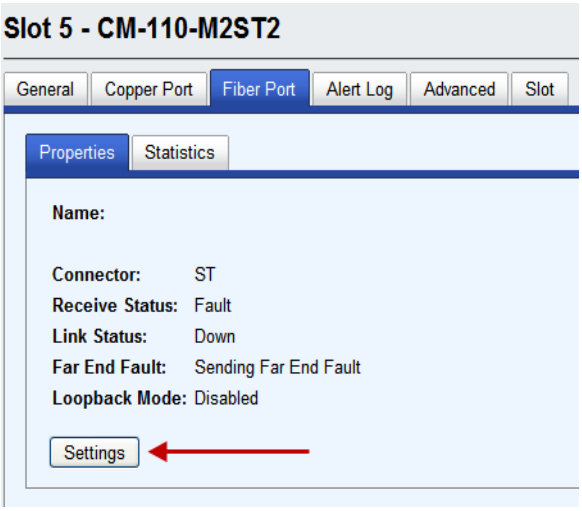


Configure the following parameters.

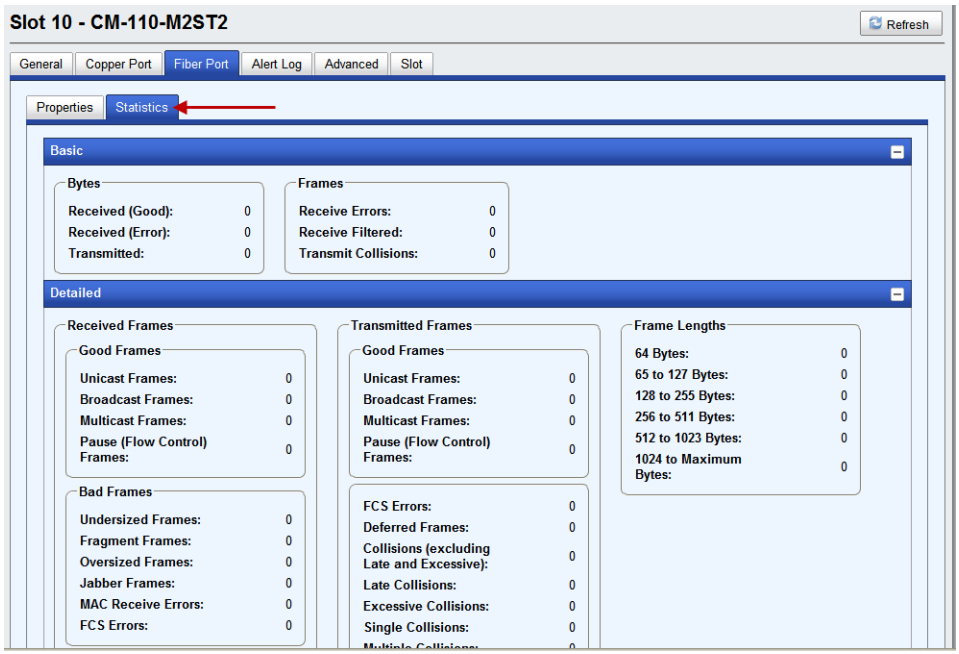
Filter Unknown Multicast Frames	When enabled, multicast frames with unknown destination addresses are not allowed to egress this port. **Default:** Disabled
Filter Unknown Unicast Frames	When enabled, unicast frames with unknown destination addresses are not allowed to egress this port. **Default:** Disabled

Fiber Port Tab

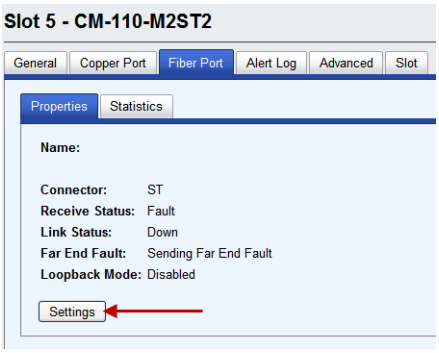
Field Descriptions > Properties



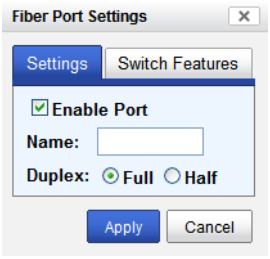
Fiber Port > Statistics



Fiber Port > Properties



Fiber Port Settings

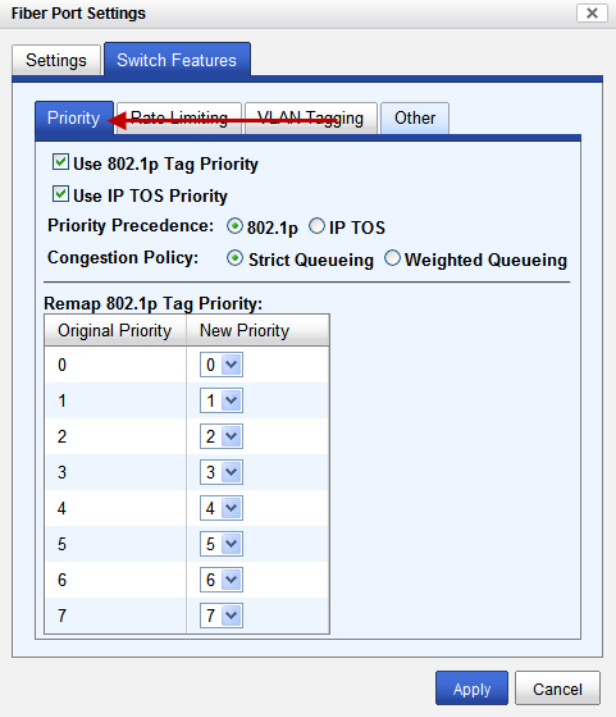


Configure the following parameters.

Enable Port	Enables/Disables the fiber port.
Name	The name of fiber port 1. **Field Format:** 8 characters
Duplex	The following Duplex modes are available: **Duplex:** Full, Half **Default:** Full

Switch Features

Switch Features > Priority



Configure the following parameters.

Enable 802.1p Priority
When enabled, the media converter module will use IEEE 802.1p tagged frame priority control to assign ingress frames to the appropriate priority egress queue.
Default: Enabled

Enable IP TOS Priority
When enabled, the media converter module will use IPv4 Diffserv or IPv6 traffic class field to assign ingress frames to the appropriate priority egress queue.
Default: Enabled

Priority Precedence
When both 802.1p priority and IP TOS priority are selected, you can select which of the two priorities takes precedence.
Default: 802.1p

Congestion Policy

Select a method to be used when determining the order by which frames are sent from the four egress queues. Setting the congestion policy on either the fiber or copper port will change the policy on both ports.
Strict Priority Queuing - The order is determined strictly by the priority of the queue. Frames in higher priority queues are always sent ahead of frames in lower priority queues.
Weighted Fair Queuing - This method allows lower priority frames to be inter-mixed with higher priority frames in the ratio of (**8, 4, 2, 1**).
The ratio for 8 highest priority sent frames will be as follows:
8 highest priority frames from queue 3
4 frames from queue 2
2 frames from queue 1
1 frame from queue 0

Default: Strict Priority Queuing

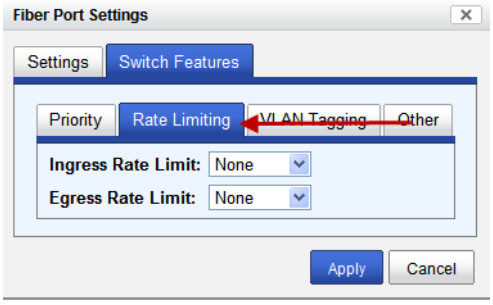
Remap Priority

Remap IEEE 802.1p ingress frames with a new priority tag. This new priority tag will be used to determine which queue the frame gets posted to.

Original Priority -----> New Priority

Values: 0-7

Switch Features > Rate Limiting



Configure the following parameters.

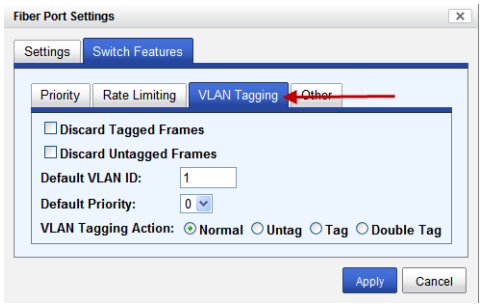
Ingress Rate Limit

Restricts ingress frames on the fiber port.
Default: None
Data Options: 64 kbps to 90 Mbps

Egress Rate Limit

Restricts egress frames on the fiber port.
Default: None
Data Options: 64 kbps to 90 Mbps

Switch Features > VLAN Tagging



Configure the following parameters.

Discard Tagged Frames
When enabled, discards all VLAN tagged frames.
Default: Off

Discard Untagged Frames
When enabled, discards all VLAN untagged frames.
Default: Off

Default VLAN ID
Specify a default VLAN ID to insert when tagging frames.
Default: 1
Data Options: 0-4095

Default Priority
Specify a default VLAN priority to insert when tagging frames.
Default: 0
Data Options: 0-7

VLAN Tagging Actions
Define the VLAN tagging action to take on a egress frame.

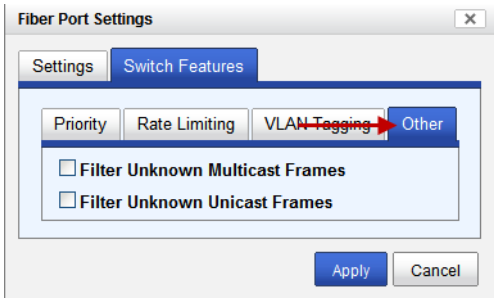
- Normal -Take no action.
- Untag - Remove any existing tag.
- Tag

  Insert tag with configured VLAN ID and VLAN priority if original frame is untagged.

  Replace tag with configured VLAN ID and VLAN priority if original frame is tagged.
- Double tag - Append a tag with configured VLAN ID and VLAN priority.

Default: Normal

Switch Features > Other



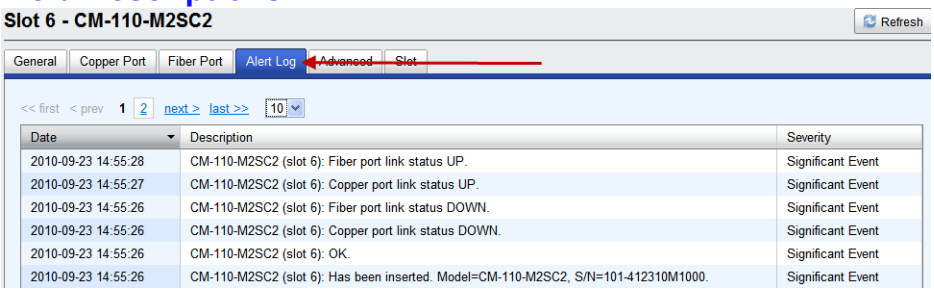
Configure the following parameters.

Filter Unknown Multicast Frames
When enabled, multicast frames with unknown destination addresses are not allowed to egress this port.
Default: Disabled

Filter Unknown Unicast Frames
When enabled, unicast frames with unknown destination addresses are not allowed to egress this port.
Default: Disabled

Alert Port Tab

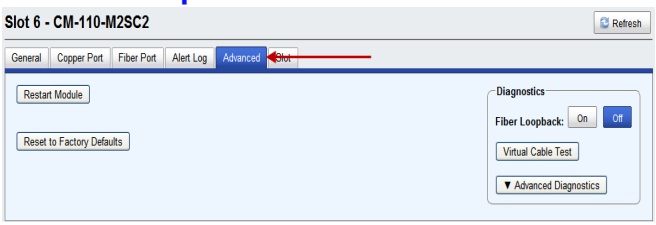
Field Descriptions



Displays the current local Alerts. The local Alert buffer contains the last 200 alerts and displays these events in a wrap around fashion.

Advanced Tab

Field Descriptions



Configure the following parameter:

Restart Module — Restarts this Media Converter Module.

Reset to Factory Defaults — Resets this Media Converter Module back to factory defaults.

Diagnostics

Fiber Loopback — **Off:** This is the normal setting. In this setting, data received on the fiber port will be passed through the Media Converter Module.

On: This is a test mode. All data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection.

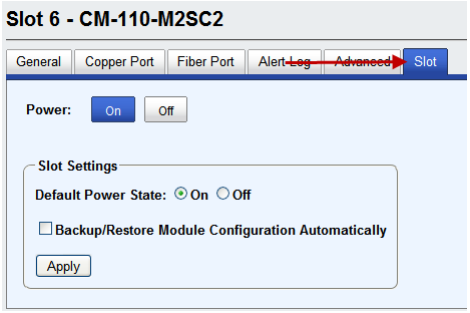
Default: Off

Virtual Cable Test — Performs a Virtual Cable Test to remotely and non-evasively diagnose the quality and characteristics of the attached ethernet cable. This test can detect issues such as cable opens, cable shorts or any impedance mismatch in the cable and then accurately report (within one meter) the distance of the fault. In addition, this Virtual Cable Test will detect pair swaps, pair polarity reversal and excessive pair skew.

Advanced Diagnostics, Read/Write Register — This feature should only be used if guided by a Perle Technical Support Representative. Use of this feature without guidance from a Perle Technical Support Representative could make your Media Converter Module inoperable.

Slot Tab

Field Descriptions



Configure the following parameters:

Power — Immediately power the slot on or off. The current state of the slot is highlighted in BLUE.

Press the "ON" button to immediately power the slot on.

Press the "OFF" button to immediately power the slot off.

Default Power State — This is the default power state of the slot when the chassis is powered up or restarted.

Default: On

Backup/Restore — **Enabled:** The configuration information associated with this slot is saved on the Management Module and will be downloaded to the Media Converter Module whenever the Media Converter Module is inserted into this slot.

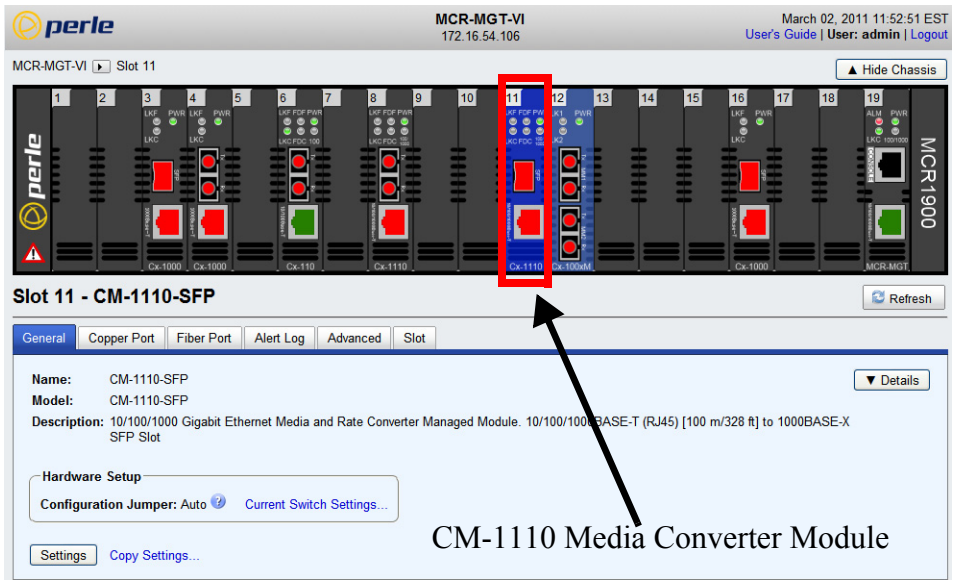
Disabled: The Media Converter Module configuration information is only kept on this Module.

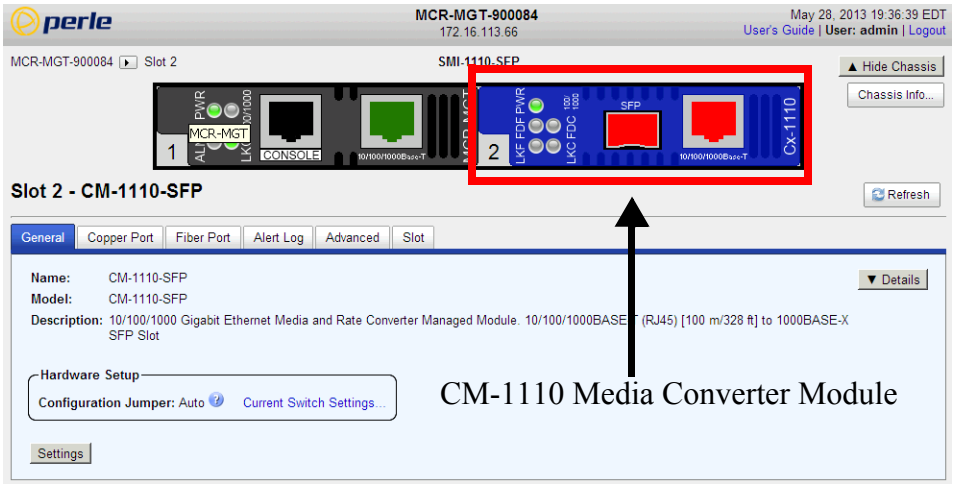
Default: Disabled

9 CM-1110/CM-1110-SFP Module

CM-1110/SPF Media Converter Module Parameters

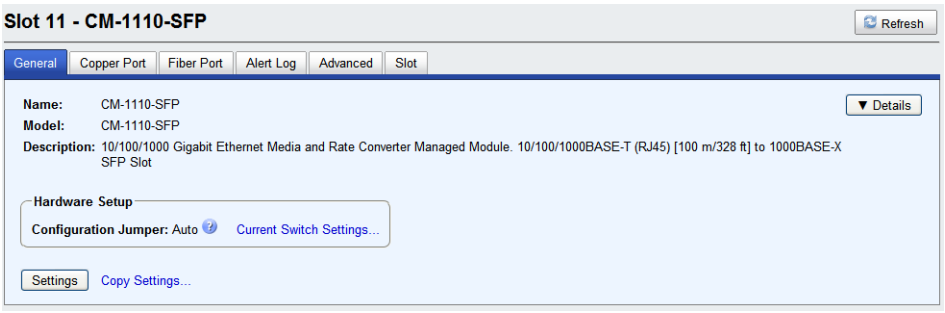
MCR1900 Chassis





General Tab

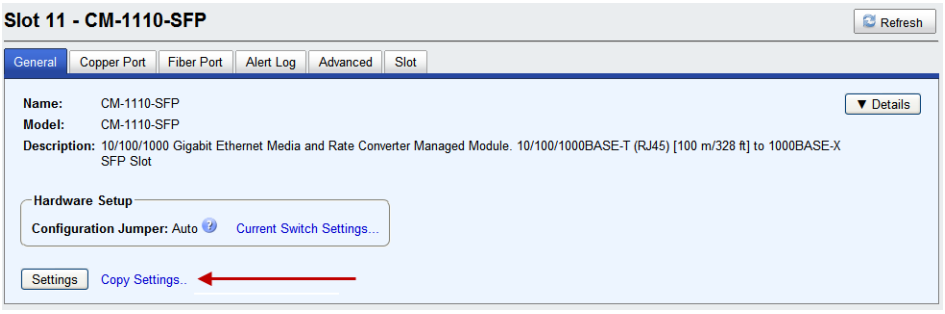
Field Descriptions

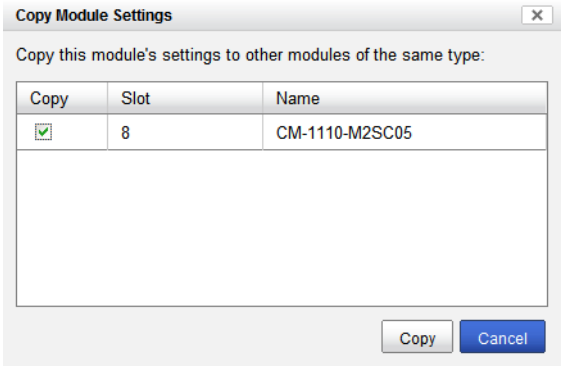


Configure the following parameters.

Name	Displays the configured name for this Module.
Description	Displays a description of the Module that is inserted in this slot.
Configuration Jumper	**Auto:** Use software configuration if present, otherwise use hardware DIP switch settings. **Switch:** Use hardware DIP switch settings. For detailed information on hardware DIP switch settings, see the Hardware Installation Guide.
Current Switch Settings	Displays the current DIP switch settings. For detailed information on hardware jumpers and DIP settings, see the Hardware Installation Guide.
Details	Displays the firmware's details.

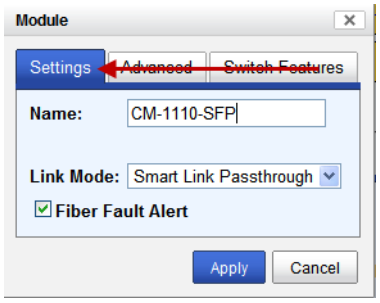
Copy Settings





Copy Module Settings Copy this module's settings to other modules of the same type.

Settings



Configure the following parameters.

Name Displays the configured name for this Module.

Link Mode

Smart Link Pass-Through: In this mode, the link state on one connection is directly reflected through the Media Converter Module to the other connection. If link is lost on one of the connections, then the other link will be brought down by the Media Converter.

Standard: In this mode, the links on the fiber and copper sides can be brought up and down independently of each other. A loss of link on either the fiber or copper port can occur without affecting the other connection.

Default: Smart Link Passthrough

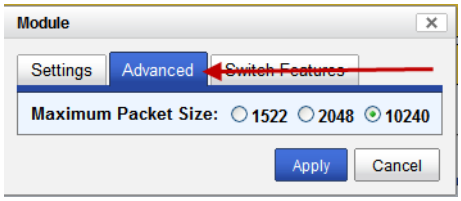
Fiber Fault Alert When enabled, if the Media Converter Module detects a loss of signal on the fiber receiver, it will immediately disable its fiber transmitter signal. This in effect, notifies the fiber link partner that an error condition exists on the fiber connection.

Note: This feature only takes effect if Fiber Negotiation has been turned off.

When disabled, the Media Converter Module will not monitor for or generate Fiber Fault Alert.

Default: On

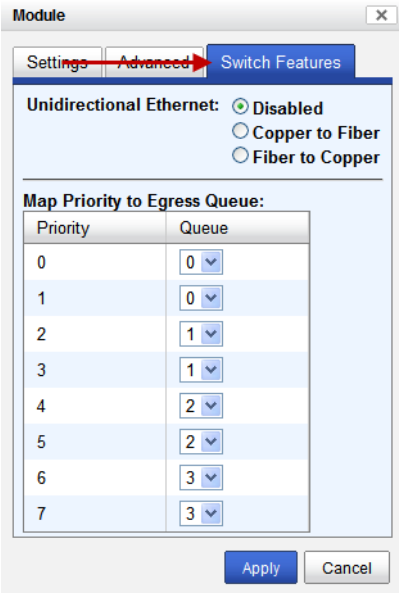
Advanced



Configure the following parameter.

Maximum Packet Size	Select the maximum packet size. **Options:** 1522, 2048, 10240 **Default:** 10240

Switch Features



Configure the following parameters:

Unidirectional Ethernet	When enabled, this feature provides the ability to restrict the flow of data between the Copper and fiber ports. **Values:** • Disabled • Copper to Fiber • Fiber to Copper **Default:** Disabled

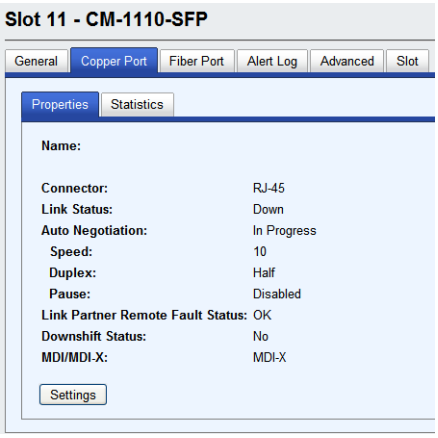
Map Priority to Egress Queue

This is the **default** egress priority mapping for both the copper and fiber ports.

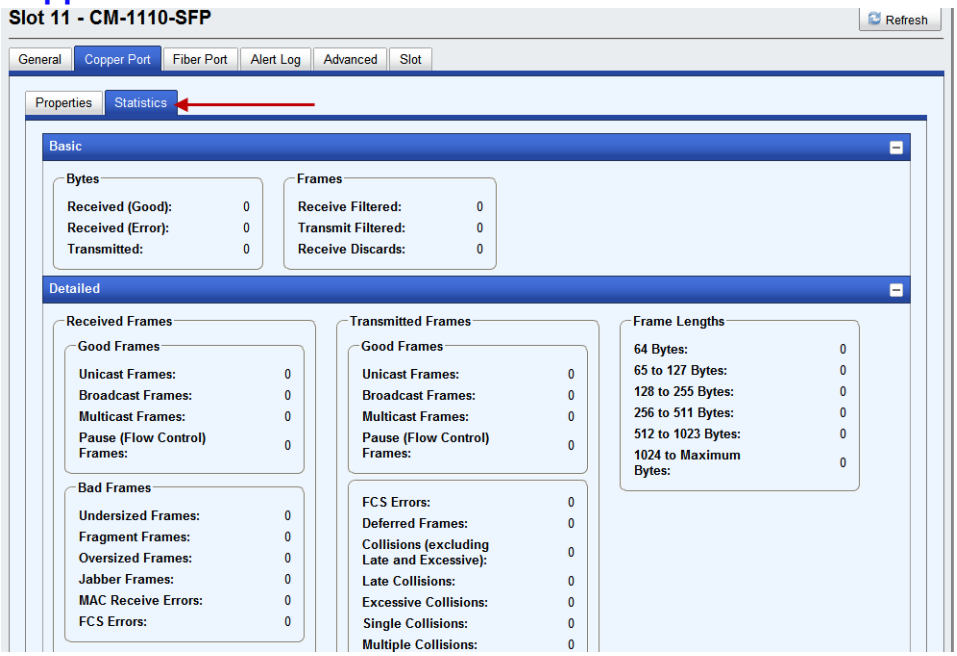
- Priority 0 (lowest priority).....Queue 0
- Priority 1 .....Queue 0
- Priority 2 .....Queue 1
- Priority 3 .....Queue 1
- Priority 4 .....Queue 2
- Priority 5 .....Queue 2
- Priority 6 .....Queue 3
- Priority 7 (highest priority) ....Queue 3

Copper Port Tab

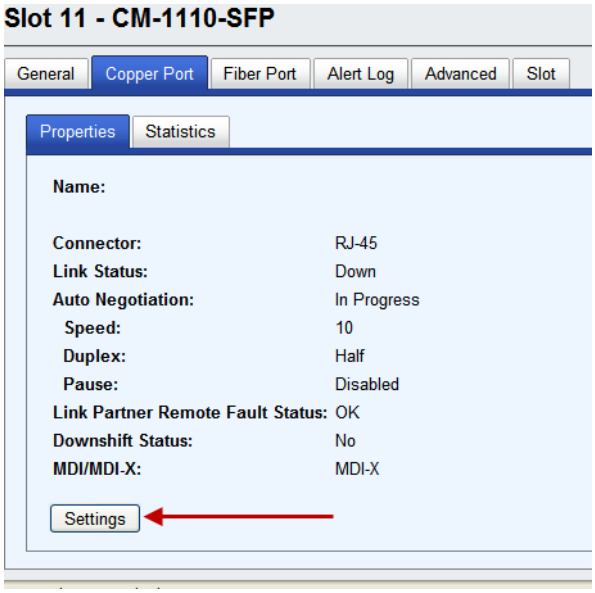
Copper Port > Properties



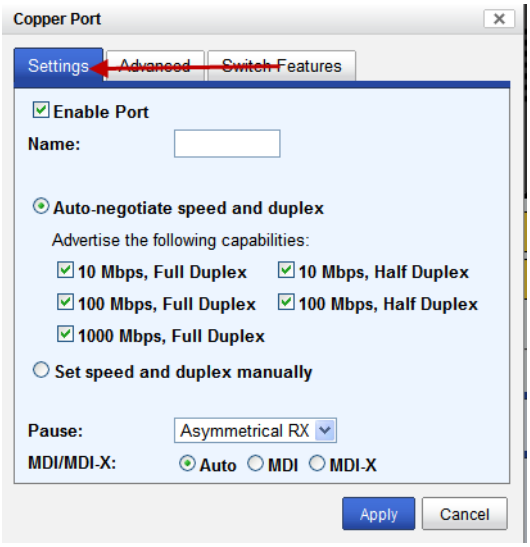
Copper > Port Statistics



Copper Port Settings



Copper Port > Settings (Auto negotiation speed and duplex)



Configure the following parameters.

Enable Port	Enables/Disables the copper port. **Default:** Enable
Name	The name of the copper port. **Field Format:** 8 characters

Auto negotiate speed and duplex

When enabled, the Media Converter Module will negotiate with its link partner to determine the most optimal parameters for this connection.

Advertise capabilities of:

- 10 Mbps, Full Duplex
- 100 Mbps, Full Duplex
- 10Mbps, Half Duplex
- 100Mbps, Half Duplex
- 1000Mbps, Full Duplex

Set speed and duplex manually

When enabled, the following selections are available:

Speed: 100 Mbps, 10 Mbps

Duplex: Full, Half

Pause

When enabled, the Media Converter Module will advertise the following Pause capabilities:

- Symmetrical
- Asymmetrical TX
- Asymmetrical RX

Note: Pause feature will only work if Auto Negotiation is set to OFF on the fiber port and Duplex is set to Full.

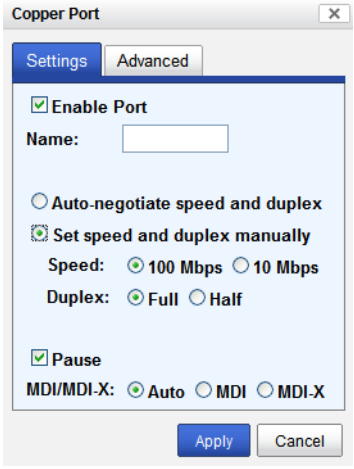
Default: Off

MDI/MDI-X

- **Auto-Detect—** automatically detects the Ethernet's cable polarity
- **MDI —**the cable's polarity is straight-through
- **MDI-X** —the cable's polarity is crossovered

Default: Auto

Copper Port > Settings (Set speed and duplex manually)



Configure the following parameters.

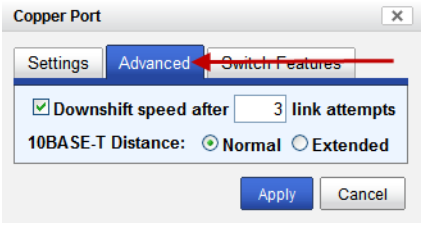
Set Speed and Duplex Manually

When enabled, the following selections are available:

Speed: 100 Mbps, 10 Mbps

Duplex: Full, Half

Copper Port > Advanced

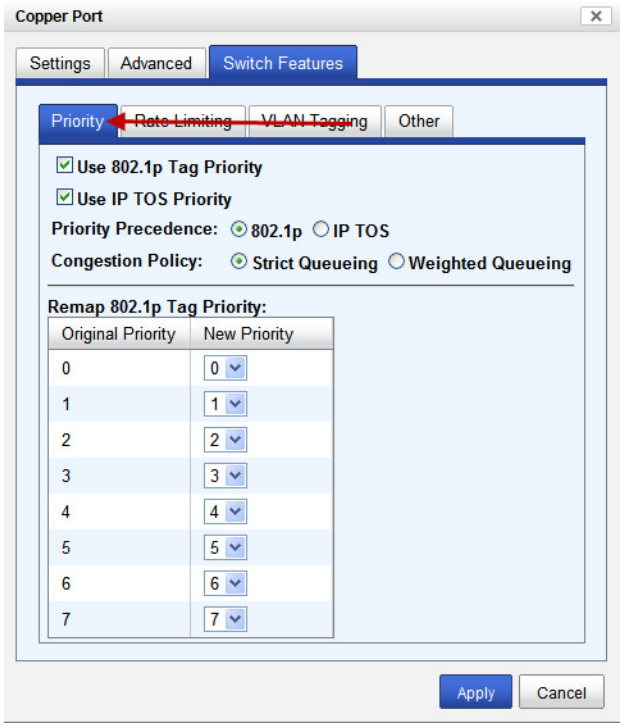


Configure the following parameter.

Downshift speed after number of link attempts	When enabled, the number of retries the Media Converter Module will attempt to establish a fiber connection at 1000 Mbps before attempting a lower speed. **Default:** On **Link attempts:** 1-8
10BASE-T Distance	**Normal:** the Media Converter copper link is in normal operating mode. **Extended:** the Media Converter will boost the signal strength on its copper link.

Switch Features

Switch Features > Priority



Configure the following parameters.

Enable 802.1p Priority	When enabled, the media converter module will use IEEE 802.1p tagged frame priority control to assign ingress frames to the appropriate priority egress queue. **Default:** Enabled
Enable IP TOS Priority	When enabled, the media converter module will use IPv4 Diffserv or IPv6 traffic class field to assign ingress frames to the appropriate priority egress queue. **Default:** Enabled

Priority Precedence When both 802.1p priority and IP TOS priority are selected, you can select which of the two priorities takes precedence.
Default: 802.1p

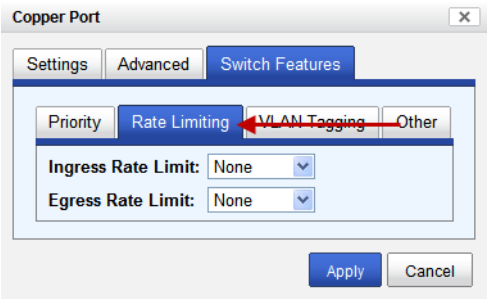
Congestion Policy Select a method to be used when determining the order by which frames are sent from the four egress queues.
Strict Priority Queuing - The order is determined strictly by the priority of the queue. Frames in higher priority queues are always sent ahead of frames in lower priority queues.
Weighted Fair Queuing - This method allows lower priority frames to be inter-mixed with higher priority frames in the ratio of (**8, 4, 2, 1**).
The ratio for 8 highest priority sent frames will be as follows:
8 highest priority frames from queue 3
4 frames from queue 2
2 frames from queue 1
1 frame from queue 0

Remap Priority Remap IEEE 802.1p ingress frames with a new priority tag. This new priority tag will be used to determine which queue the frame gets posted to.

Original Priority -----> New Priority

Values: 0-7

Switch Features > Rate Limiting

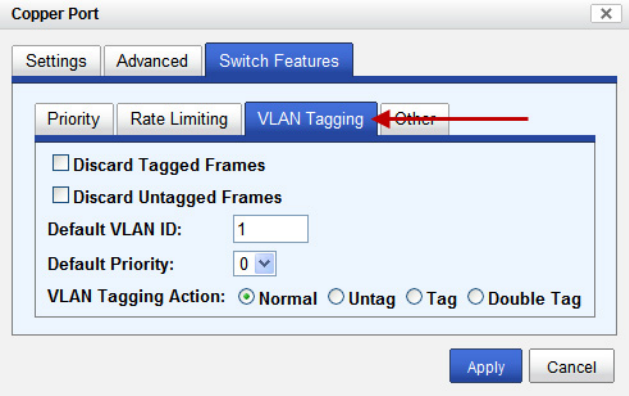


Configure the following parameters.

Congestion Policy Restricts ingress frames on the copper port.
Default: None
Data Options: 64 kbps to 900 mbps

Remap Priority Restricts egress frames on the copper port.
Default: None
Data Options: 64kbps to 900 mbps

Switch Features > VLAN Tagging



Configure the following parameters.

Discard Tagged Frames
When enabled, discards all VLAN tagged frames.
Default: Off

Discard Untagged Frames
When enabled, discards all VLAN untagged frames.
Default: Off

Default VLAN ID
Specify a default VLAN ID to insert when tagging frames.
Default: 1
Data Options: 0-4095

Default Priority
Specify a default VLAN priority to insert when tagging frames.
Default: 0
Data Options: 0-7

VLAN Tagging Actions
Define the VLAN tagging action to take on a egress frame.

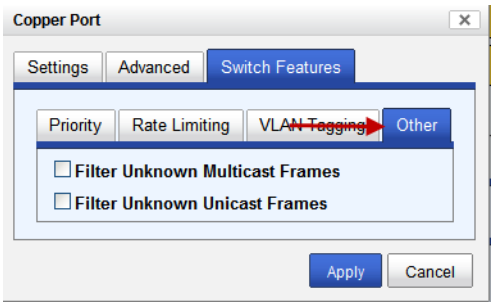
- Normal -Take no action.
- Untag - Remove any existing tag.
- Tag

  Insert tag with configured VLAN ID and VLAN priority if original frame is untagged.

  Replace tag with configured VLAN ID and VLAN priority if original frame is tagged.
- Double tag - Append a tag with configured VLAN ID and VLAN priority.

Default: Normal

Switch Features > Other

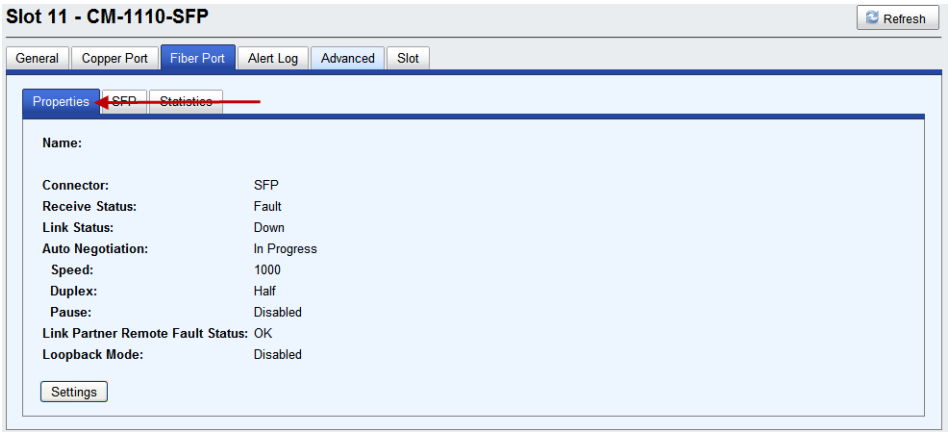


Configure the following parameters.

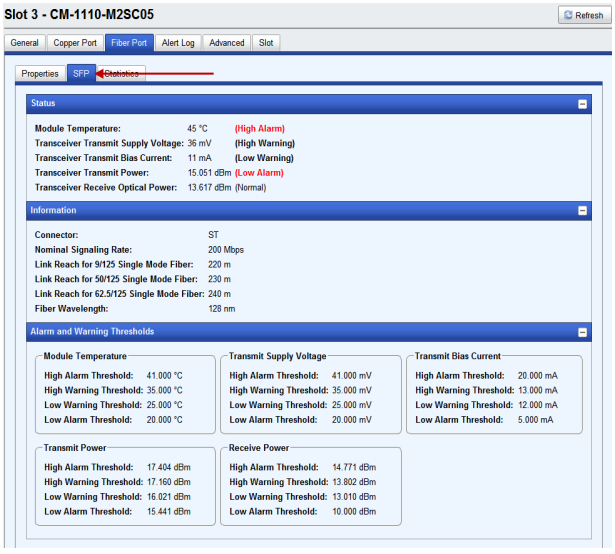
Filter Unknown Multicast Frames	When enabled, multicast frames with unknown destination addresses are not allowed to egress this port. **Default:** Disabled
Filter Unknown Unicast Frames	When enabled, unicast frames with unknown destination addresses are not allowed to egress this port. **Default:** Disabled

Fiber Port Tab

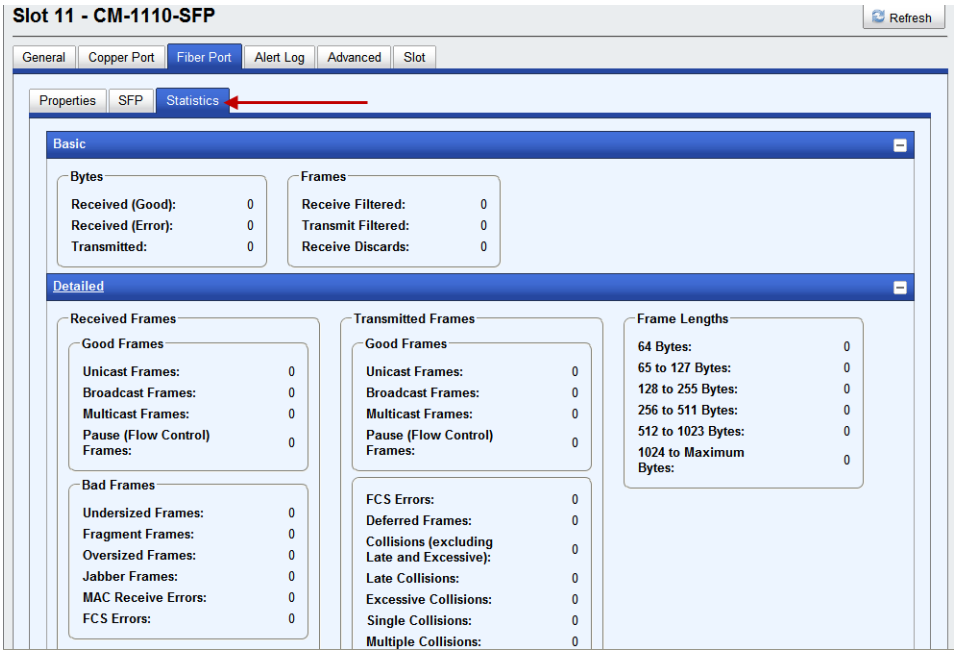
Fiber Port > Properties



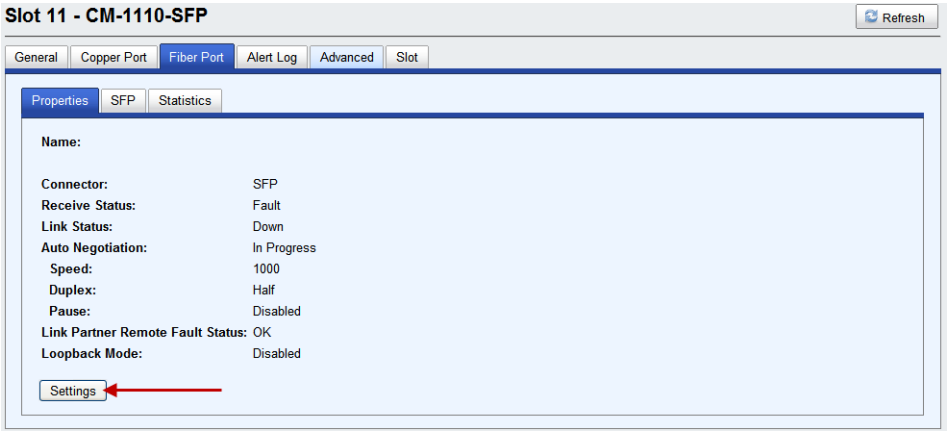
Fiber Port > SFP



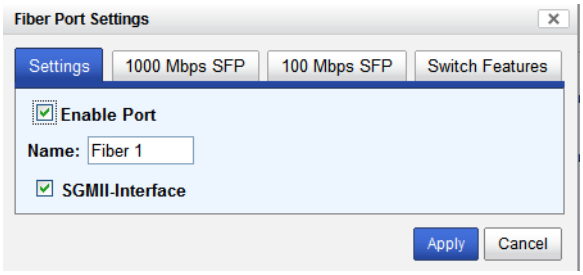
Fiber Port > Statistics



Fiber Port > Properties



Fiber Port > Settings



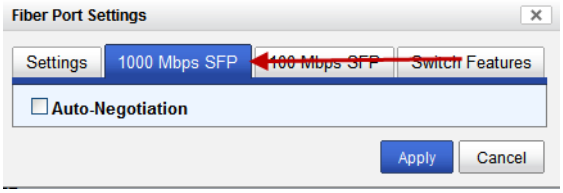
Configure the following parameter.

Enable Port Enables/Disables the fiber port.

Name The name of the fiber port.
Field Format: 8 characters

SGMII-Interface Select the checkbox if your SFP has a SGMII interface.

Fiber Port > 1000 MBPS SFP



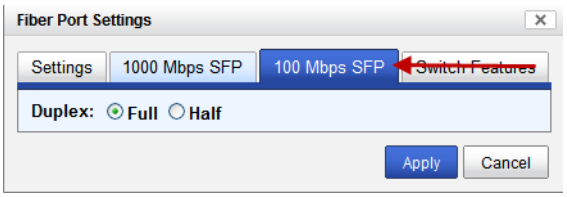
Configure the following parameter.

Auto Negotiation **Enabled:** The Media Converter Module will negotiate Ethernet parameters on the fiber connection. This will ensure that the most optimal connection parameters will be in effect. If connecting to another Perle Media Converter, this parameter should be set to Auto. The Media converter module will advertise 1000 Mbps, Full and Half Duplex, no Pause.

Disabled: The Media Converter Module's fiber will be fixed to 1000 Mbps, Full Duplex.

Default: Disabled

Fiber Port > 100 MBPS SFP



Configure the following parameter.

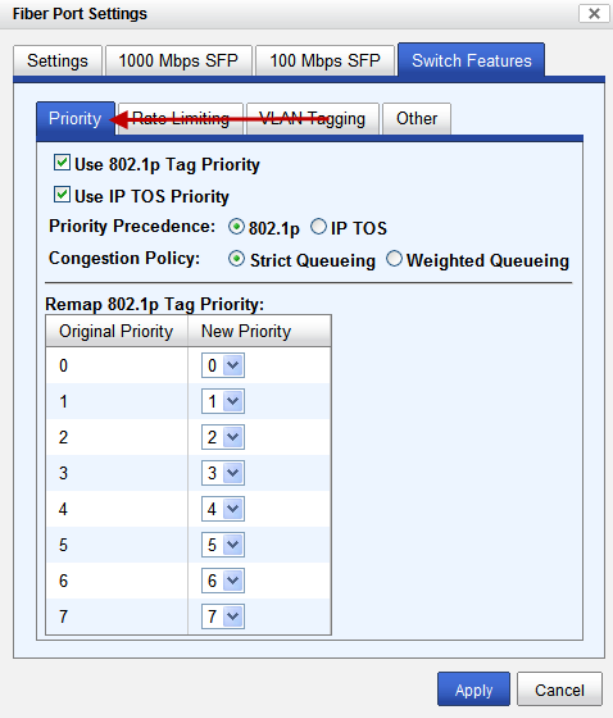
Duplex The following Duplex modes are available:

Duplex: Full, Half

Default: Full

Switch Features

Switch Features > Priority



Configure the following parameters.

Enable 802.1p Priority
When enabled, the media converter module will use IEEE 802.1p tagged frame priority control to assign ingress frames to the appropriate priority egress queue.
Default: Enabled

Enable IP TOS Priority
When enabled, the media converter module will use IPv4 Diffserv or IPv6 traffic class field to assign ingress frames to the appropriate priority egress queue.
Default: Enabled

Priority Precedence
When both 802.1p priority and IP TOS priority are selected, you can select which of the two priorities takes precedence.
Default: 802.1p

Congestion Policy

Select a method to be used when determining the order by which frames are sent from the four egress queues.
Strict Priority Queuing - The order is determined strictly by the priority of the queue. Frames in higher priority queues are always sent ahead of frames in lower priority queues.
Weighted Fair Queuing - This method allows lower priority frames to be inter-mixed with higher priority frames in the ratio of (**8, 4, 2, 1**).
The ratio for 8 highest priority sent frames will be as follows:
8 highest priority frames from queue 3
4 frames from queue 2
2 frames from queue 1
1 frame from queue 0

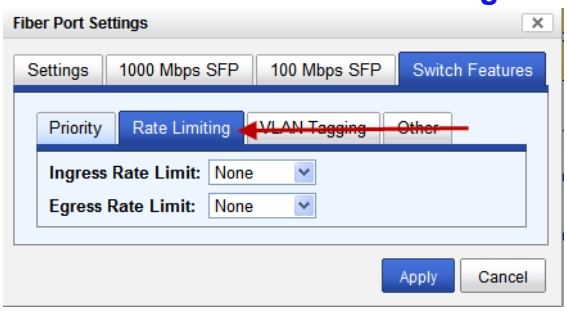
Remap Priority

Remap IEEE 802.1p ingress frames with a new priority tag. This new priority tag will be used to determine which queue the frame gets posted to.

Original Priority -----> New Priority

Values: 0-7

Switch Features > Rate Limiting



Configure the following parameters.

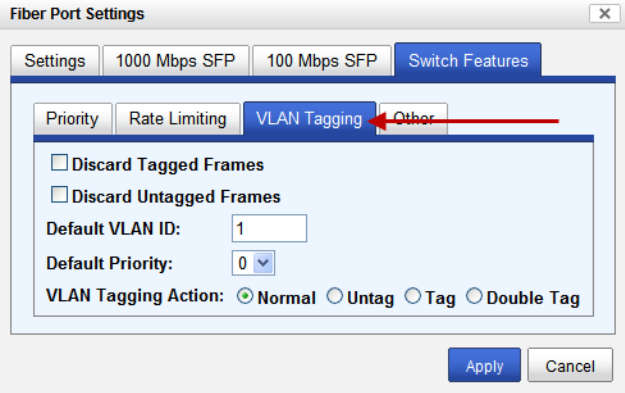
Ingress Rate Limit

Restricts ingress frames on the fiber port.
Default: None
Data Options: 64 kbps to 900 mbps

Egress Rate Limit

Restricts egress frames on the fiber port.
Default: None
Data Options: 64 kbps to 900 mbps

Switch Features > VLAN Tagging



Configure the following parameters.

Discard Tagged Frames
When enabled, discards all VLAN tagged frames.
Default: Off

Discard Untagged Frames
When enabled, discards all VLAN untagged frames.
Default: Off

Default VLAN ID
Specify a default VLAN ID to insert when tagging frames.
Default: 1
Data Options: 0-4095

Default Priority
Specify a default VLAN priority to insert when tagging frames.
Default: 0
Data Options: 0-7

VLAN Tagging Actions
Define the VLAN tagging action to take on a egress frame.

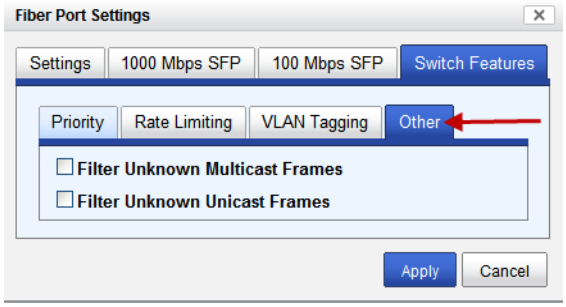
- Normal -Take no action.
- Untag - Remove any existing tag.
- Tag

  Insert tag with configured VLAN ID and VLAN priority if original frame is untagged.

  Replace tag with configured VLAN ID and VLAN priority if original frame is tagged.
- Double tag - Append a tag with configured VLAN ID and VLAN priority.

Default: Normal

Switch Features > Other

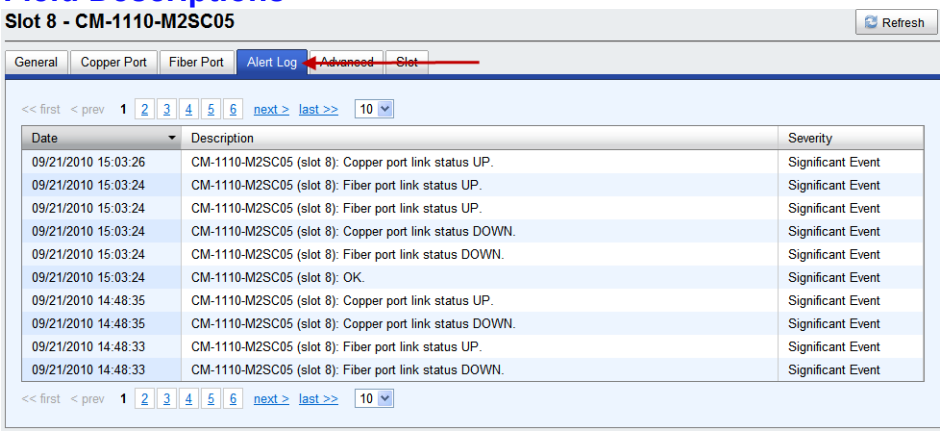


Configure the following parameters.

Filter Unknown Multicast Frames	When enabled, multicast frames with unknown destination addresses are not allowed to egress this port. **Default:** Disabled
Filter Unknown Unicast Frames	When enabled, unicast frames with unknown destination addresses are not allowed to egress this port. **Default:** Disabled

Alert Log Tab

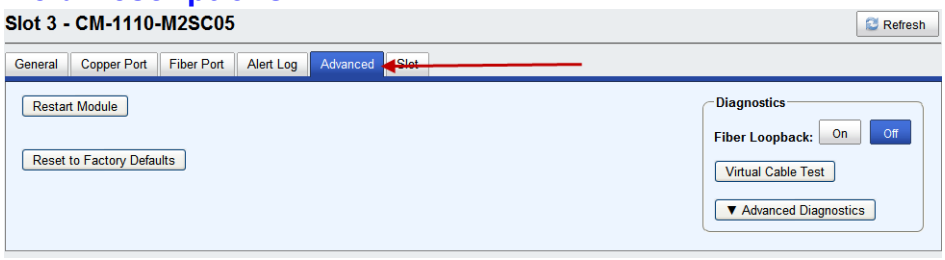
Field Descriptions



Displays the current local Alerts. The local Alert buffer contains the last 200 alerts and displays these events in a wrap around fashion.

Advanced Tab

Field Descriptions



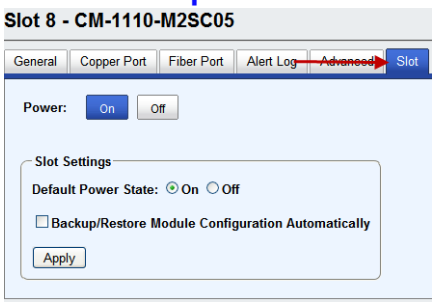
Configure the following parameter:

Restart Module	Restarts this Media Converter Module.
Reset Factory Defaults	Resets this Media Converter Module back to factory defaults.
Diagnostics	

Fiber Loopback	**Off:** This is the normal setting. In this setting, data received on the fiber port will be passed through the Media Converter Module. **On:** This is a test mode. All data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection. **Default:** Off
Virtual Cable Test	Performs a Virtual Cable Test to remotely and non-evasively diagnose the quality and characteristics of the attached ethernet cable. This test can detect issues such as cable opens, cable shorts or any impedance mismatch in the cable and then accurately report (within one meter) the distance of the fault. In addition, this Virtual Cable Test will detect pair swaps, pair polarity reversal and excessive pair skew.
Advanced Diagnostics, Read/Write Register	This feature should only be used if guided by a Perle Technical Support Representative. Use of this feature without guidance from a Perle Technical Support Representative could make your Media Converter Module inoperable.

Slot Tab

Field Descriptions



Configure the following parameters:

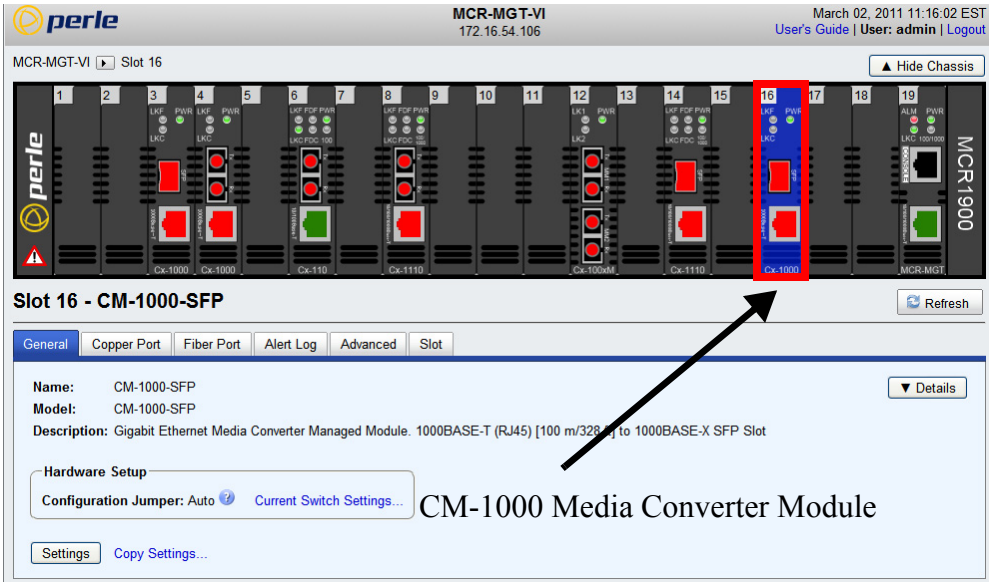
Power	Immediately power the slot on or off. The current state of the slot is highlighted in BLUE. Press the "ON" button to immediately power the slot on. Press the "OFF" button to immediately power the slot off.
Default Power State	This is the default power state of the slot when the chassis is powered up or restarted. **Default:** On
Backup/Restore Automatically	**Enabled:** The configuration information associated with this slot is saved on the Management Module and will be downloaded to the Media Converter Module whenever the Media Converter Module is inserted into this slot. **Disabled:** The Media Converter Module configuration information is only kept on this Module. **Default**: Disabled

.

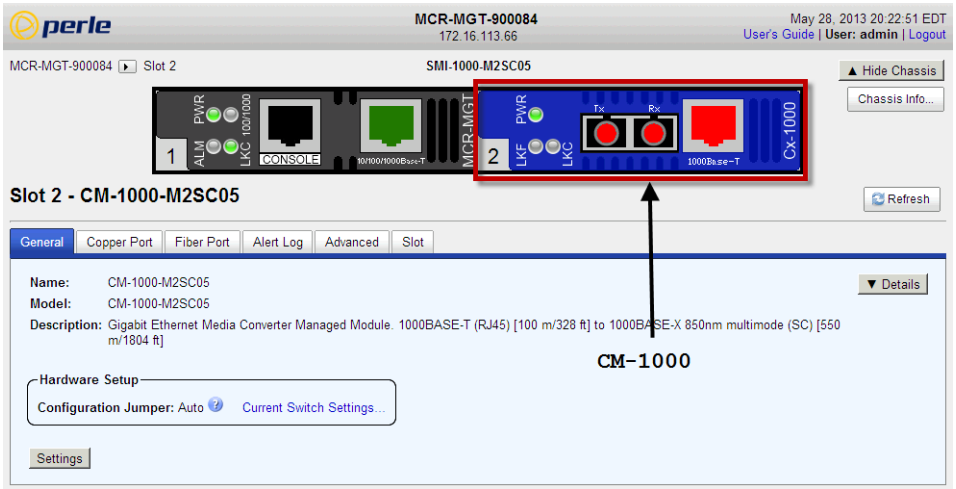
10 CM-1000/CM-1000-SFP Module

CM-1000 Media Converter Module Parameters

MCR1900 Chassis

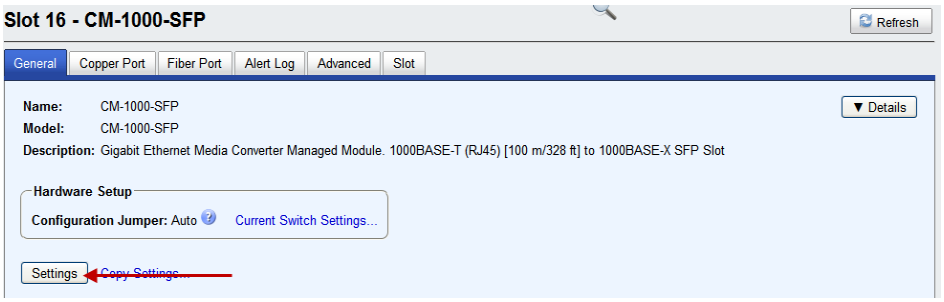


SMI Chassis



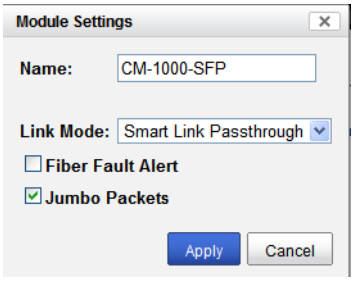
General Tab

Field Descriptions



Name	Displays the configured name for this Module.
Model	Displays the module's model information.
Description	Displays a description of the Module that is inserted in this slot.
Configuration Jumper	**Auto:** Use software configuration if present, otherwise use hardware DIP switch settings. **Switch:** Use hardware DIP switch settings. For detailed information on hardware DIP switch settings, see the Hardware Installation Guide.
Current Switch Settings	Displays the current DIP switch settings. For detailed information on hardware jumpers and DIP settings, see the Hardware Installation Guide.

Settings



Configure the following parameters:

Name	Displays the configured name for this Module.
Link Mode	**Smart Link Pass-Through:** In this mode, the link state on one connection is directly reflected through the Media Converter Module to the other connection. If link is lost on one of the connections, then the other link will be brought down by the Media Converter. **Standard:** In this mode, the links on the fiber and copper sides can be brought up and down independently of each other. A loss of link on either the fiber or copper port can occur without affecting the other connection. **Default:** Smart Link Passthrough

Fiber Fault Alert

When enabled, if the Media Converter Module detects a loss of signal on the fiber receiver, it will immediately disable its fiber transmitter signal. This in effect, notifies the fiber link partner that an error condition exists on the fiber connection.

Note: This feature only takes effect if Fiber Negotiation has been turned off.

When disabled, the Media Converter Module will not monitor for or generate Fiber Fault Alert.

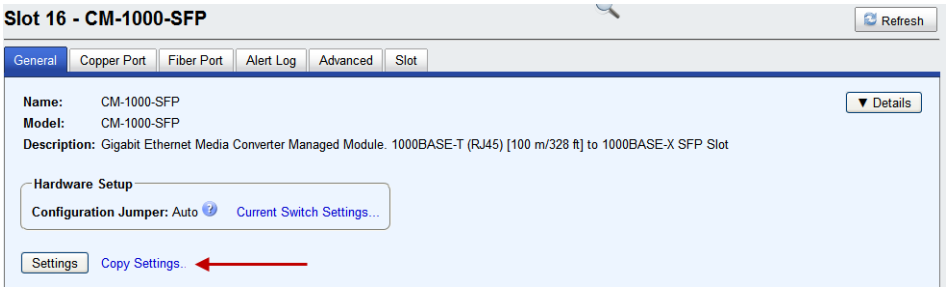
Default: On

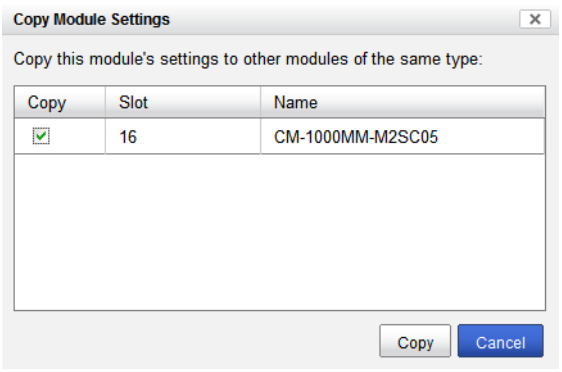
Jumbo Packets

Enable Jumbo Packet support.

Default: Enabled

Copy Settings



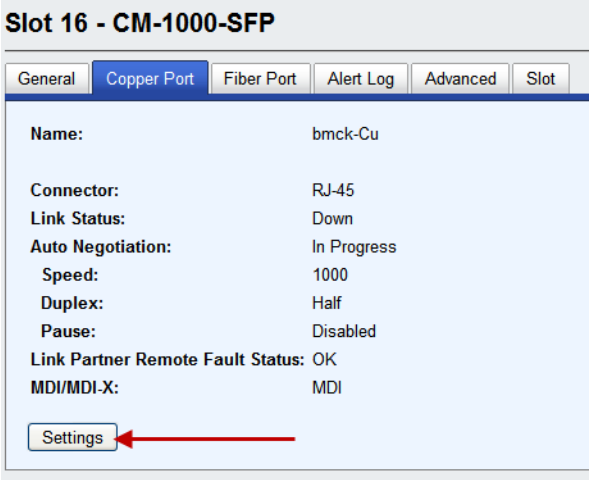


Copy Module Settings

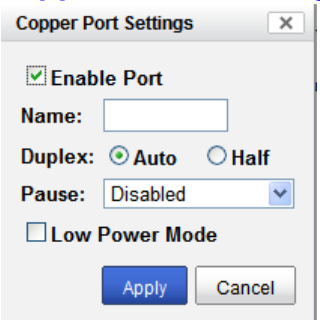
Copy this module's settings to other modules of the same type.

Copper Port Tab

Field Descriptions



Copper Port > Settings



Configure the following parameters:

Enable Port — Enables/Disables the copper port.
Default: Enable

Name — The name of the copper port.
Field Format: 8 characters

Duplex — The following selections are available:
Duplex: Auto, Half
Default: Auto
The following selections are available:
Duplex: Auto, Half
Default: Auto

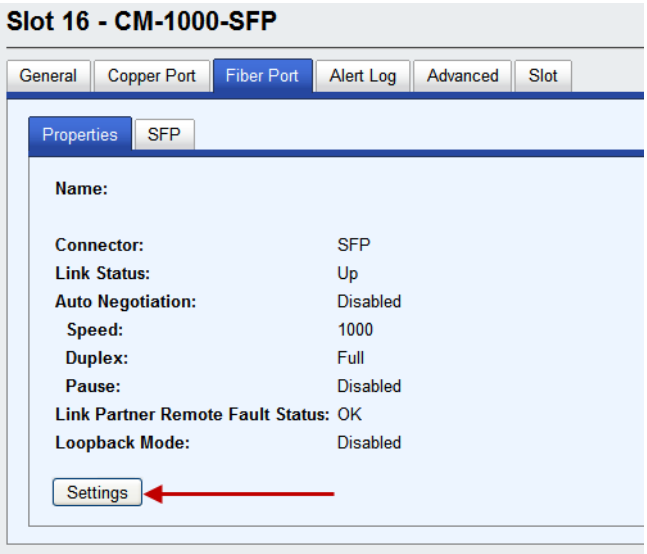
Pause — When enabled, the Media Converter Module will advertise the following Pause capabilities:

- Symmetrical
- Asymmetrical TX
- Asymmetrical RX

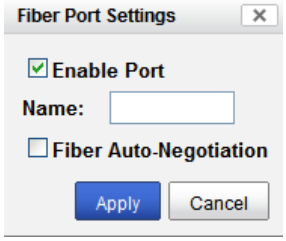
Note: Pause feature will only work if Auto Negotiation is set to OFF on the fiber port and Duplex is set to Full.
Default: Off

Low Power Mode — If enabled, the Gigabit copper transceiver is set into low power mode which reduces the strength of the copper signal.
Default: Off

Field Descriptions



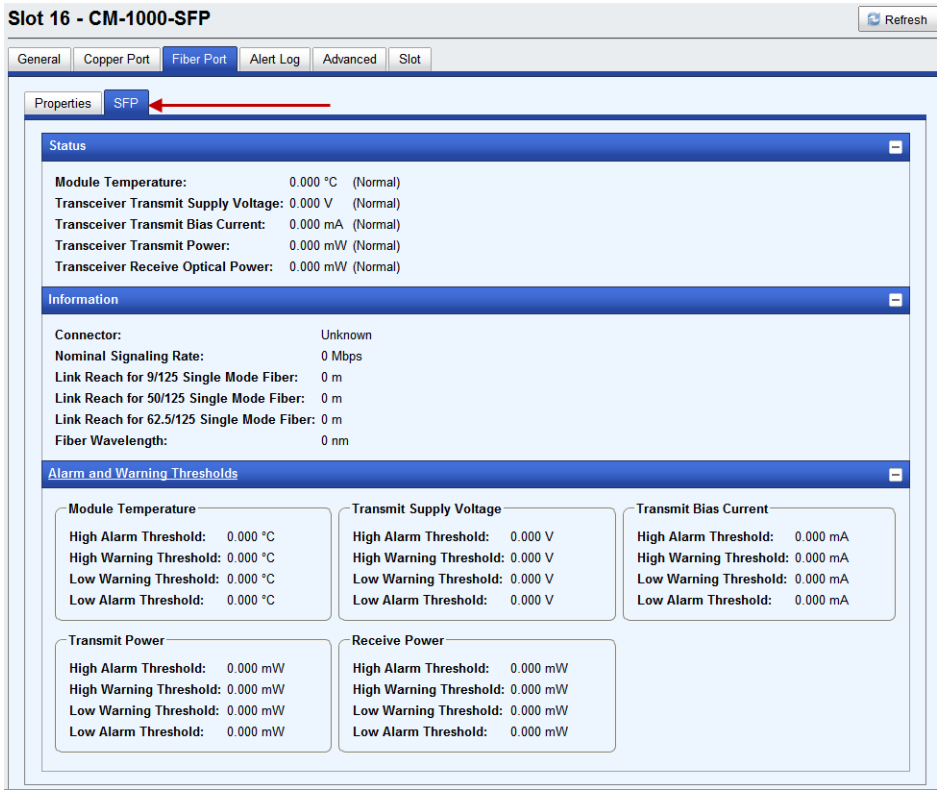
Fiber Port > Settings



Configure the following parameter:

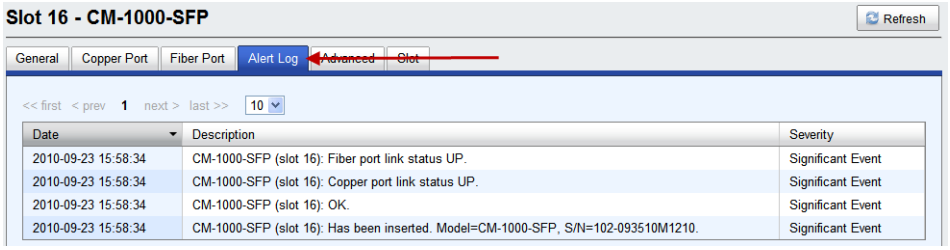
Enable Port	Enables/Disables the fiber port.
Name	The name of the fiber port. **Field Format:** 8 characters
Fiber Auto-Negotiation	**Enabled:** The Media Converter Module will negotiate Ethernet parameters on the fiber connection. This will ensure that the most optimal connection parameters will be in effect. If connecting to another Perle Media Converter, this parameter should be set to Auto. The Media converter module will advertise 1000 Mbps, Full and Half Duplex, no Pause. **Disabled:** The Media Converter Module's fiber will be fixed to 1000 Mbps, Full Duplex. **Default:** Disabled

Fiber Port > SFP (Statistics)



Alert Log Tab

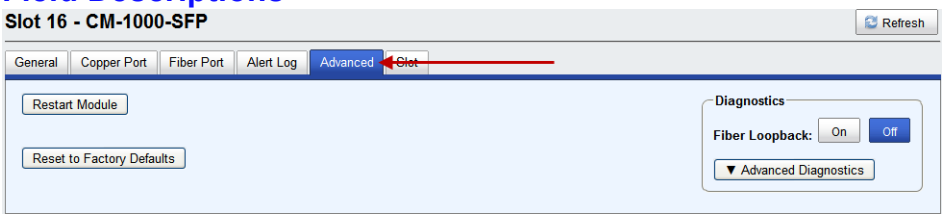
Field Descriptions



Displays the current local Alerts. The local Alert buffer contains the last 200 alerts and displays these events in a wrap around fashion.

Advanced Tab

Field Descriptions

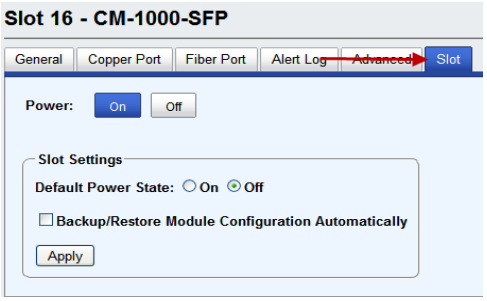


Configure the following parameter:

Restart Module	Restarts this Media Converter Module.
Reset Factory Defaults	Resets this Media Converter Module back to factory defaults.
Diagnostics	
Fiber Loopback	**Off:** This is the normal setting. In this setting, data received on the fiber port will be passed through the Media Converter Module. **On:** This is a test mode. All data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection. **Default:** Off
Advanced Diagnostics, Read/Write Register	This feature should only be used if guided by a Perle Technical Support Representative. Use of this feature without guidance from a Perle Technical Support Representative could make your Media Converter Module inoperable.

Slot

Field Descriptions



Configure the following parameters:

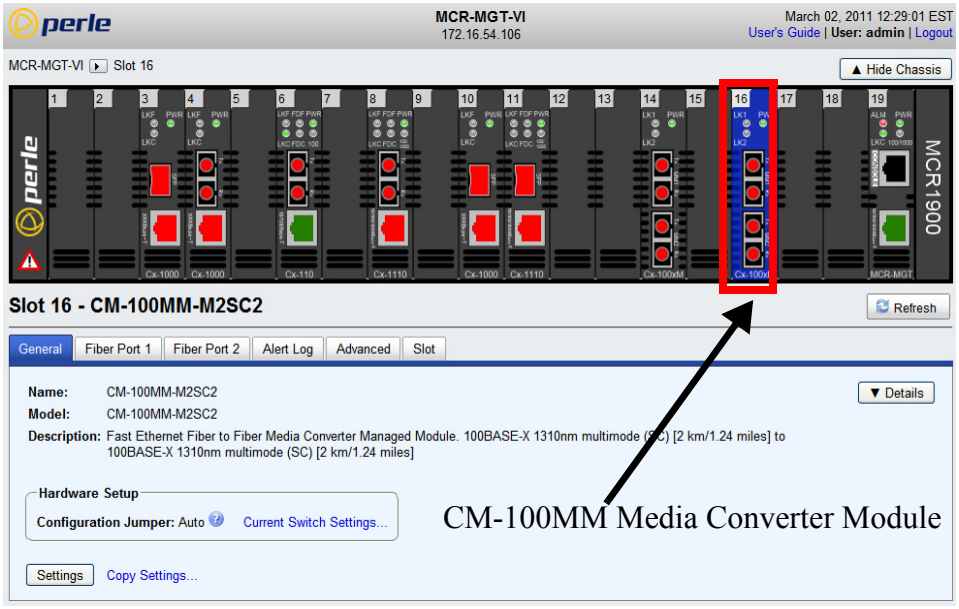
Power State	Immediately power the slot on or off. The current state of the slot is highlighted in BLUE. Press the "ON" button to immediately power the slot on. Press the "OFF" button to immediately power the slot off.
Default Power State	This is the default power state of the slot when the chassis is powered up or restarted. **Default:** On
Backup/Restore Module Configuration Automatically	**Enabled:** The configuration information associated with this slot is saved on the Management Module and will be downloaded to the Media Converter Module whenever the Media Converter Module is inserted into this slot. **Disabled:** The Media Converter Module configuration information is only kept on this Module. **Default**: Disabled

11 CM-100MM Media Converter Module

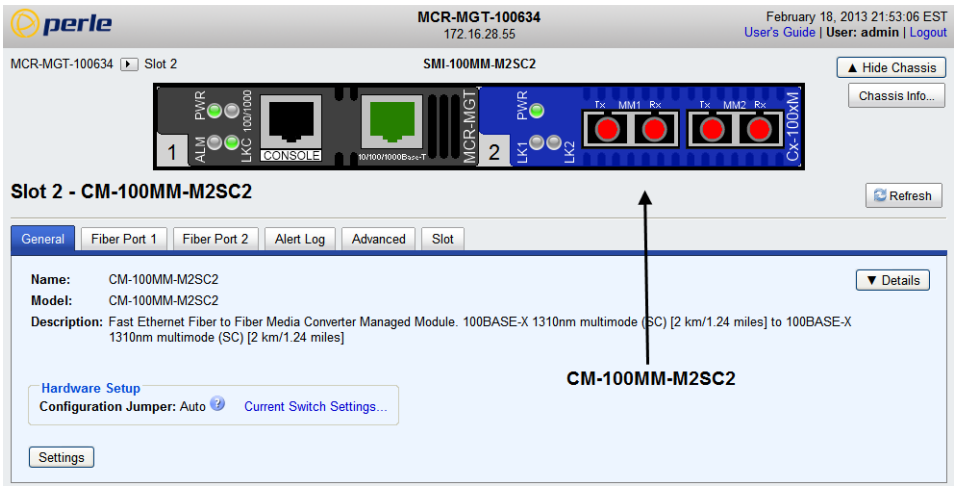
CM-100MM Media Converter Module Parameters

General Tab

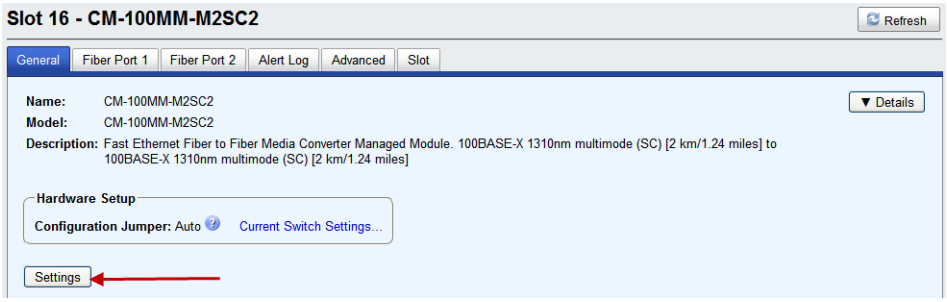
MCR1900 Chassis



SMI Chassis



Field Descriptions



Name — Displays the configured name for this Module.

Model — Displays the module's model information.

Description — Displays a description of the Module that is inserted in this slot.

Configuration Jumper — **Auto:** Use software configuration if present, otherwise use hardware DIP switch settings.

Switch: Use hardware DIP switch settings.

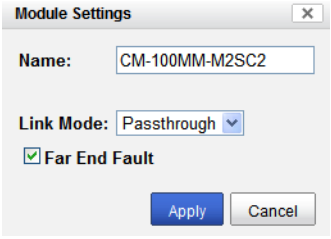
For detailed information on hardware DIP switch settings, see the Hardware Installation Guide.

Current Switch Settings — Displays the current DIP switch settings.

For detailed information on hardware jumpers and DIP settings, see the Hardware Installation Guide.

Details — Displays the firmware's details.

Settings



Name — Displays the configured name for this Module.

Link Mode — **Link Pass-Through:** In this mode, the link state on one fiber connection is directly reflected through the Media Converter Module to the other fiber connection. If link is lost on one of the fiber connections, then the other fiber link will be brought down by the Media Converter.

Standard: In this mode, each fiber link can be brought up and down independently of each other. A loss of signal on either fiber connection can occur without affecting the other fiber connection.

Default: Link Pass-Through

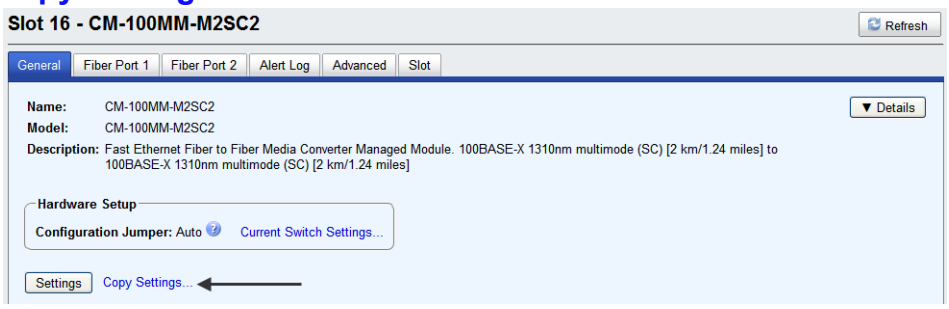
Far End Fault — When enabled, if the Media Converter Module detects a loss of signal on the fiber receiver, it will transmit a FEF signal to the remote Media Converter Module. This, in effect, notifies the fiber link partner that an error condition exists on the fiber connection.

Note: This feature only takes effect if Auto Negotiation has been turned off.

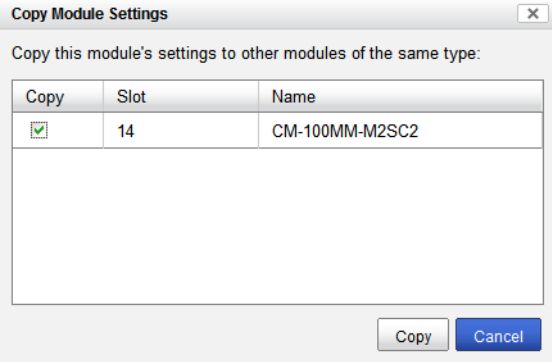
When disabled, the Media Converter Module will not monitor for or generate Far End Fault.

Default: On

Copy Settings

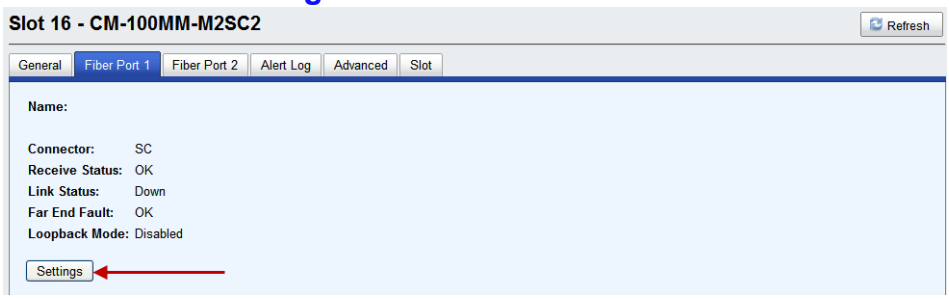


Copy Module Settings — Copy this module's settings to other modules of the same type.

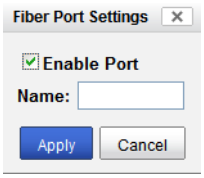


Fiber Port 1 Tab

Fiber Port 1 > Settings



Settings



Configure the following parameters:

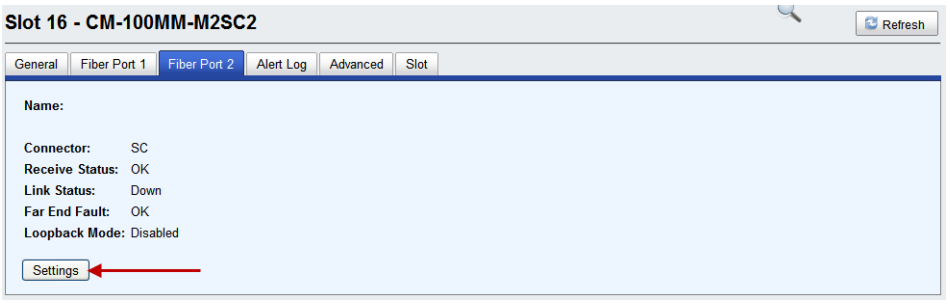
Settings

Enable Port — Enables/Disables fiber port 1.

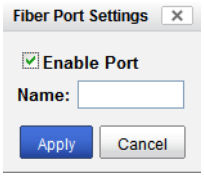
Name — The name of fiber port 1.
Field Format: 8 characters

Fiber Port 2 Tab

Fiber Port 2 > Settings



Settings

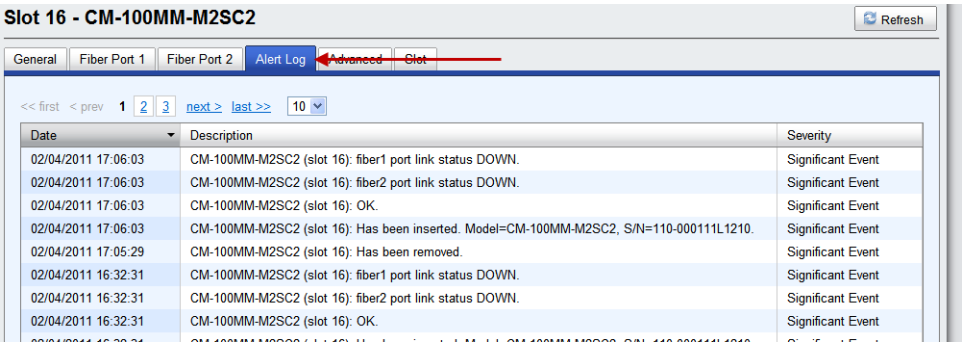


Configure the following parameters:

Enable Port	Enables/Disables fiber port 2.
Name	The name of fiber port 2. **Field Format:** 8 characters

Alert Log Tab

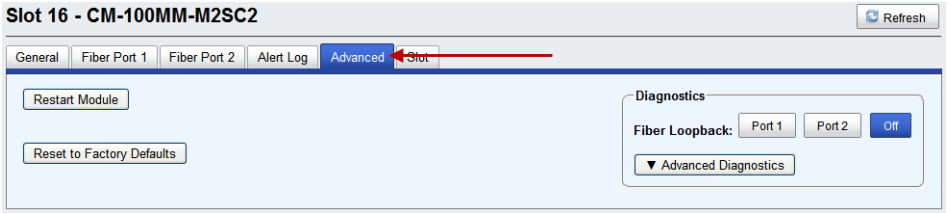
Field Descriptions



Displays the current local Alerts. The local Alert buffer contains the last 200 alerts and displays these events in a wrap around fashion.

Advanced Tab

Field Descriptions

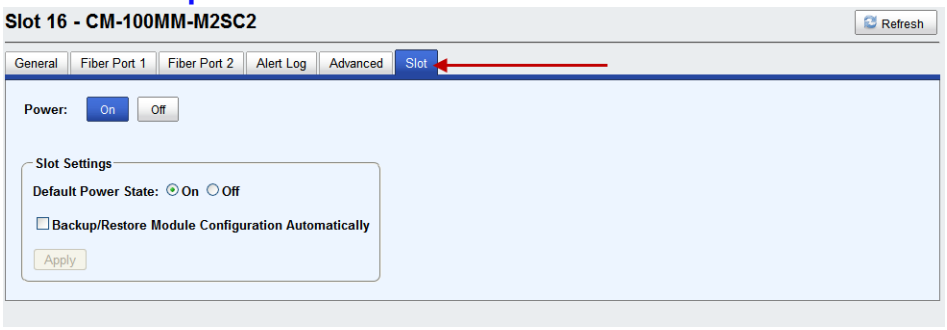


Configure the following parameter:

Restart Module	Restarts this Media Converter Module.
Reset to Factory Defaults	Resets this Media Converter Module back to factory defaults.
Diagnostics	
Fiber Loopback	**Off:** This is the normal setting. In this setting, data received on the fiber port will be passed through the Media Converter Module. Select either Port 1 or Port 2. Only one fiber port can be in loopback at one time. **Port 1:** This is a test mode. All data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection. **Port 2:** This is a test mode. All data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection. **Default:** Off
Advanced Diagnostics, Read/Write Register	This feature should only be used if guided by a Perle Technical Support Representative. Use of this feature without guidance from a Perle Technical Support Representative could make your Media Converter Module inoperable.

Slot Tab

Field Descriptions



Configure the following parameters:

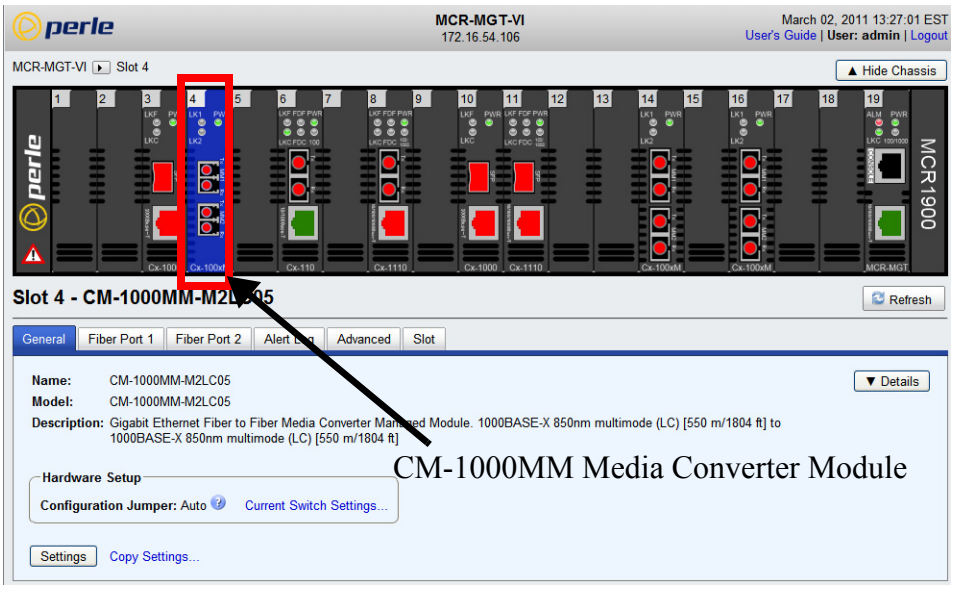
Power	Immediately power the slot on or off. The current state of the slot is highlighted in BLUE. Press the "ON" button to immediately power the slot on. Press the "OFF" button to immediately power the slot off.
Default Power State	This is the default power state of the slot when the chassis is powered up or restarted. **Default:** On
Backup/Restore Module Configuration Automatically	**Enabled:** The configuration information associated with this slot is saved on the Management Module and will be downloaded to the Media Converter Module whenever the Media Converter Module is inserted into this slot. **Disabled:** The Media Converter Module configuration information is only kept on this Module. **Default**: Disabled

12 CM-1000MM Media Converter Module

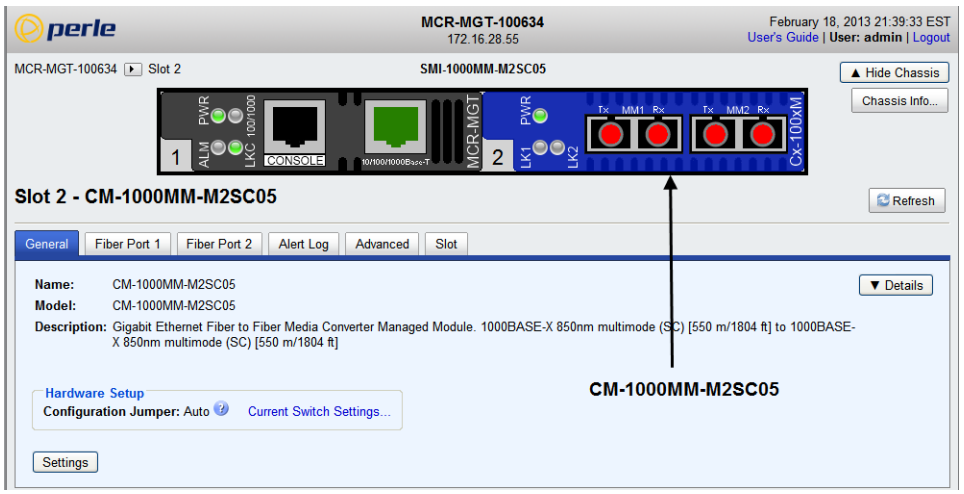
CM-1000MM Media Converter Module Parameters

General Tab

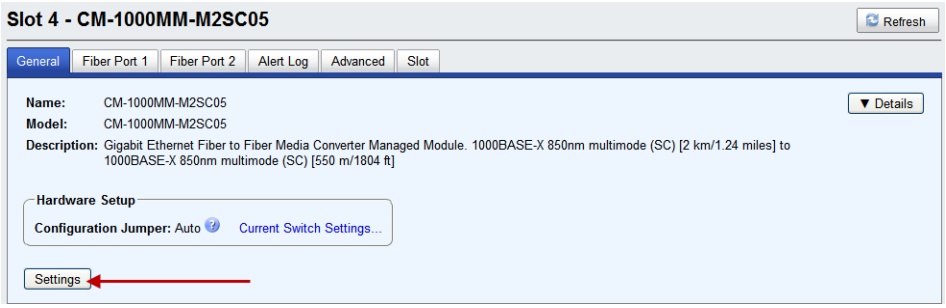
MCR1900 Chassis



SMI Chassis

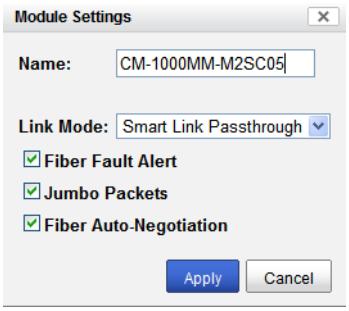


Field Descriptions



Name	Displays the configured name for this Module.
Model	Displays the module's model information.
Description	Displays a description of the Module that is inserted in this slot.
Configuration Jumper	**Auto:** Use software configuration if present, otherwise use hardware DIP switch settings. **Switch:** Use hardware DIP switch settings. For detailed information on hardware DIP switch settings, see the Hardware Installation Guide.
Current Switch Settings	Displays the current DIP switch settings. For detailed information on hardware jumpers and DIP settings, see the Hardware Installation Guide.

Settings



Configure the following parameters:

Name	Displays the configured name for this Module.
Link Mode	**Smart Link Pass-Through:** In this mode, the link state on one connection is directly reflected through the Media Converter Module to the other connection. If link is lost on one of the connections, then the other link will be brought down by the Media Converter. **Standard:** In this mode, the links on the fiber and copper sides can be brought up and down independently of each other. A loss of link on either the fiber or copper port can occur without affecting the other connection. **Default:** Smart Link Passthrough

Fiber Fault Alert

When enabled, if the Media Converter Module detects a loss of signal on the fiber receiver, it will immediately disable its fiber transmitter signal. This in effect, notifies the fiber link partner that an error condition exists on the fiber connection.

Note: This feature only takes effect if Fiber Negotiation has been turned off.

When disabled, the Media Converter Module will not monitor for or generate Fiber Fault Alert.

Default: On

Jumbo Packets

Enable Jumbo Packet support.

Default: Enabled

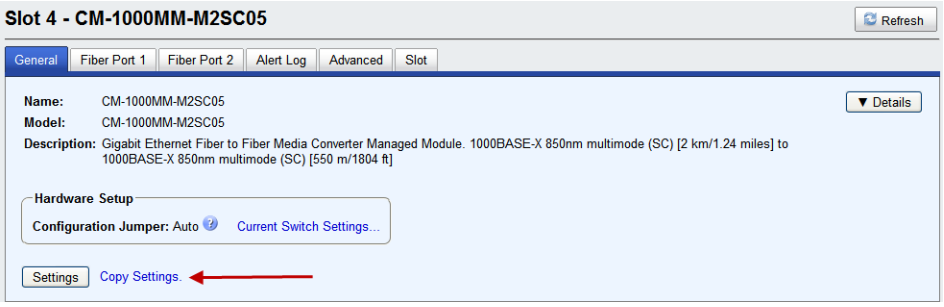
Fiber Auto-Negotiation

Auto: In this mode, the Media Converter will negotiate fiber parameters on both fiber connections. This will ensure the most optimal connection parameters will be in effect. If connecting to another Perle Media Converter this parameter should be set to Auto.

Off: Fiber negotiation on both fiber ports will be disabled. The switch settings for Link Mode and Fiber Fault Alert will be determined by the Module Settings parameters.

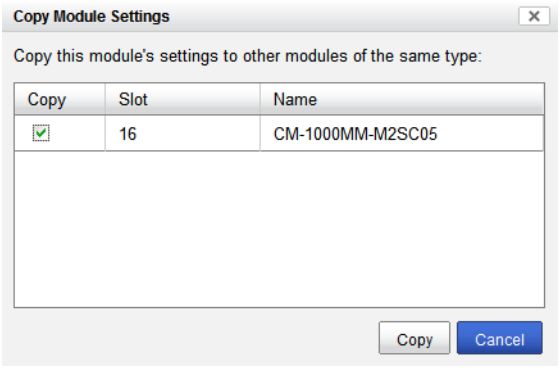
Default: Auto

Copy Settings



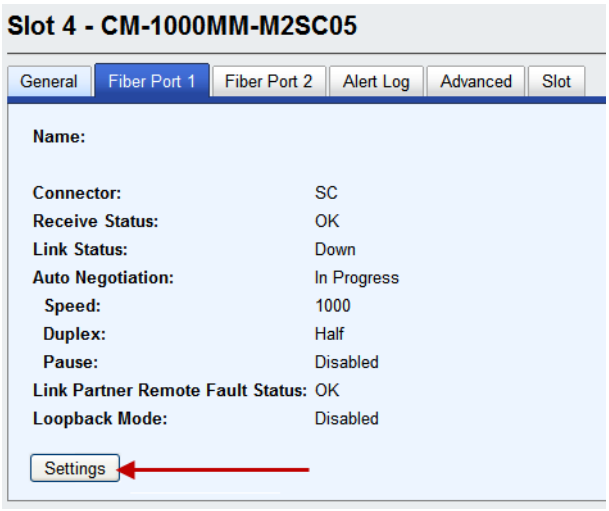
Copy Module Settings

Copy this module's settings to other modules of the same type.

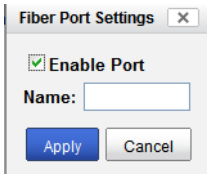


Fiber Port 1 Tab

Fiber Port 1 > Settings



Settings

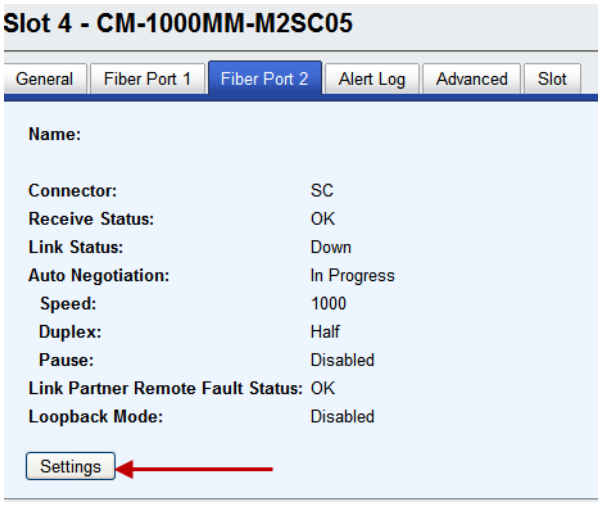


Configure the following parameter:

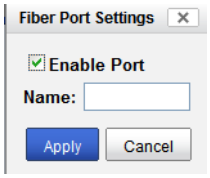
Enable Port	Enables/Disables fiber port 1.
Port Name	The name of fiber port 1. **Field Format:** 8 characters

Fiber Port 2 Tab

Fiber Port 2 > Settings



Settings

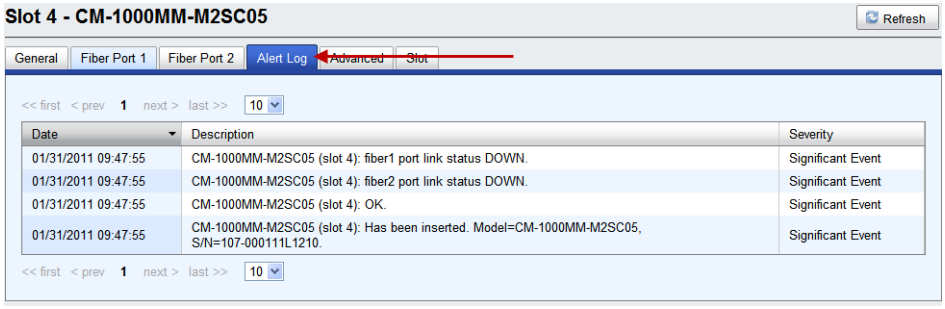


Configure the following parameter:

Enable Port	Enables/Disables fiber port 2.
Name	The name of fiber port 2. **Field Format:** 8 characters

Alert Log Tab

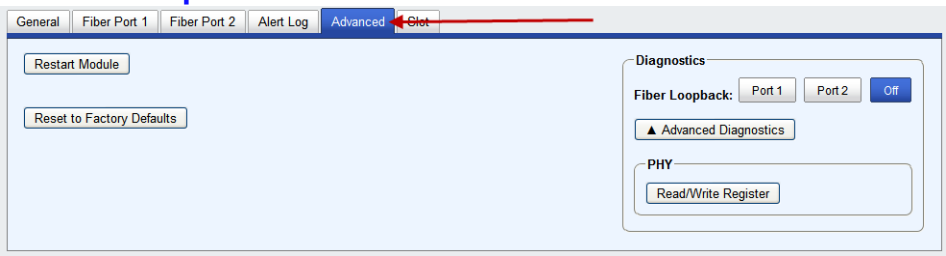
Field Descriptions



Displays the current local Alerts. The local Alert buffer contains the last 200 alerts and displays these events in a wrap around fashion.

Advanced Tab

Field Descriptions

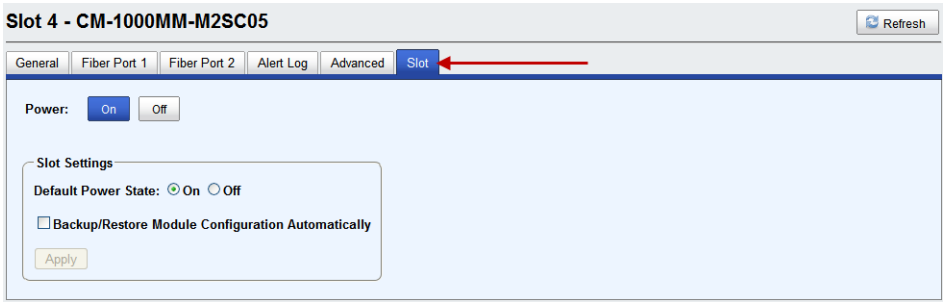


Configure the following parameter:

Restart Module	Restarts this Media Converter Module.
Reset Factory Defaults	Resets this Media Converter Module back to factory defaults.
Diagnostics	
Fiber Loopback	**Off:** This is the normal setting. In this setting, data received on the fiber port will be passed through the Media Converter Module. Select either Port 1 or Port 2. Only one fiber port can be in loopback at one time. **Port 1:** This is a test mode. All data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection. **Port 2:** This is a test mode. All data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection. **Default:** Off
Advanced Diagnostics, Read/Write Register	This feature should only be used if guided by a Perle Technical Support Representative. Use of this feature without guidance from a Perle Technical Support Representative could make your Media Converter Module inoperable.

Slot

Field Descriptions



Configure the following parameters:

Power State	Immediately power the slot on or off. The current state of the slot is highlighted in BLUE. Press the "ON" button to immediately power the slot on. Press the "OFF" button to immediately power the slot off.
Default Power State	This is the default power state of the slot when the chassis is powered up or restarted. **Default:** On
Backup/Restore Module Configuration Automatically	**Enabled:** The configuration information associated with this slot is saved on the Management Module and will be downloaded to the Media Converter Module whenever the Media Converter Module is inserted into this slot. **Disabled:** The Media Converter Module configuration information is only kept on this Module. **Default**: Disabled

13 CM-10G Media Converter Modules

Standard Models

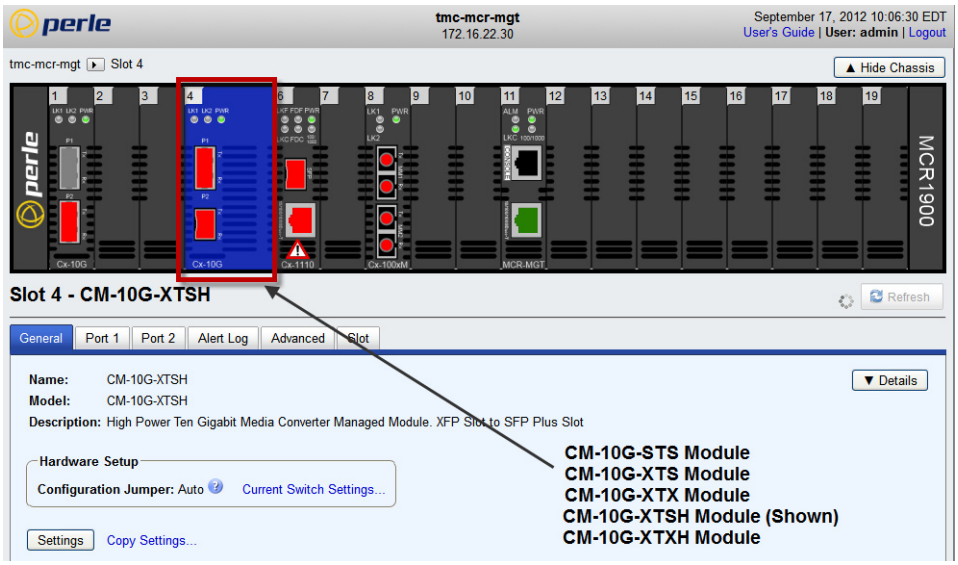
- CM-10G-STS - This model contains two SFP+ pluggable transceivers. These pluggable transceiver ports can be populated with either:
  - two (1 gigabit SFP modules)
  - two (10 gigabit SFP+ modules).
- CM-10G-XTS - This model contains one SFP+ pluggable transceiver port and one XFP pluggable transceiver port.
- CM-10G-XTX - This model contains two XFP pluggable transceiver ports.

High Power Models

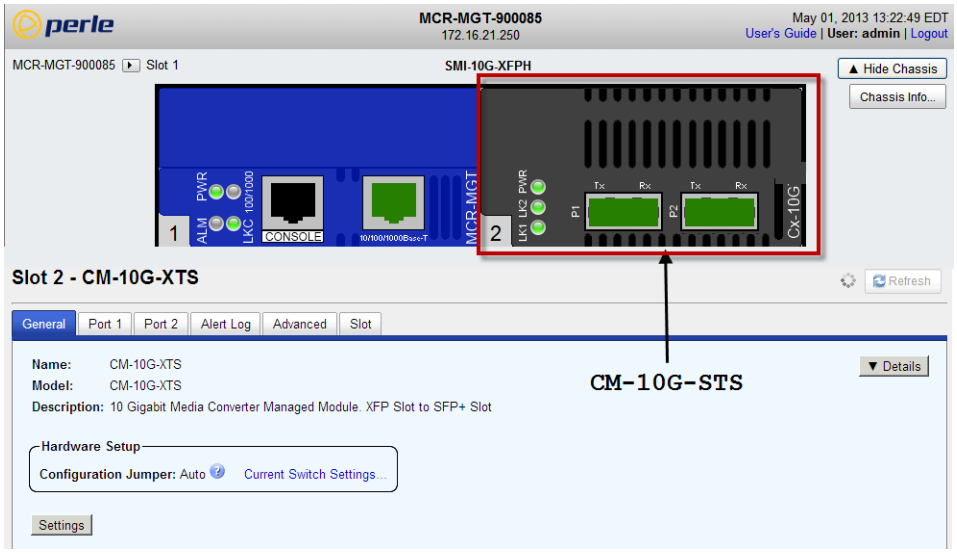
- CM-10G-XTSH - This model contains one SFP+ pluggable transceiver port and one XFP pluggable transceiver port. This module takes 2 slots within a Perle chassis.
- CM-10G-XTXH - This model contains two high power XFP pluggable transceiver ports. parameters. This module takes 2 slots within a Perle chassis.

CM-10G Modules Parameters

MCR1900 Chassis

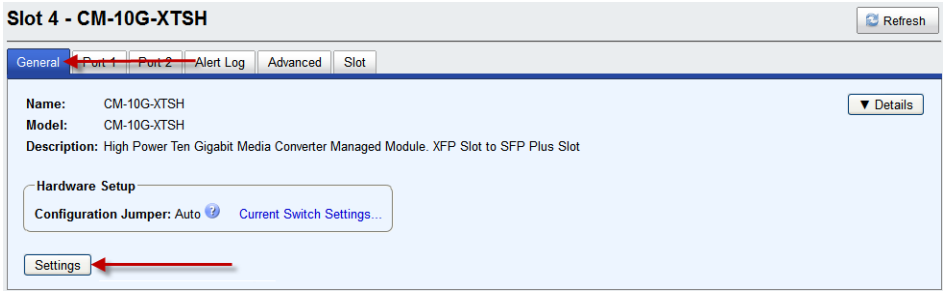


SMI Chassis



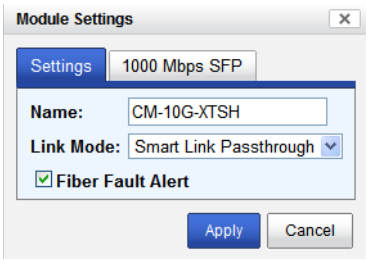
General Tab

Field Descriptions



Name	Displays the configured name for this Module.
Model	Displays the module's model information.
Description	Displays a description of the Module that is inserted in this slot.
Configuration Jumper	**Auto:** Use software configuration if present, otherwise use hardware DIP switch settings. **Switch:** Use hardware DIP switch settings. For detailed information on hardware DIP switch settings, see the Hardware Installation Guide.
Current Switch Settings	Displays the current DIP switch settings. For detailed information on hardware jumpers and DIP settings, see the Hardware Installation Guide.

Settings



Configure the following parameters:

Name	Displays the configured name for this Module.
Link Mode	**Smart Link Pass-Through:** In this mode, the link state on one connection is directly reflected through the Media Converter Module to the other connection. If link is lost on one of the connections, then the other link will be brought down by the Media Converter. **Standard:** In this mode, the links on the fiber and copper sides can be brought up and down independently of each other. A loss of link on either the fiber or copper port can occur without affecting the other connection. **Default:** Smart Link Passthrough

Fiber Fault Alert

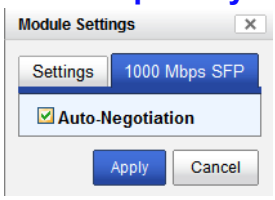
When enabled, if the Media Converter Module detects a loss of signal on the fiber receiver, it will immediately disable its fiber transmitter signal. This in effect, notifies the fiber link partner that an error condition exists on the fiber connection.

Note: This feature only takes effect if Fiber Negotiation has been turned off.

When disabled, the Media Converter Module will not monitor for or generate Fiber Fault Alert.

Default: On

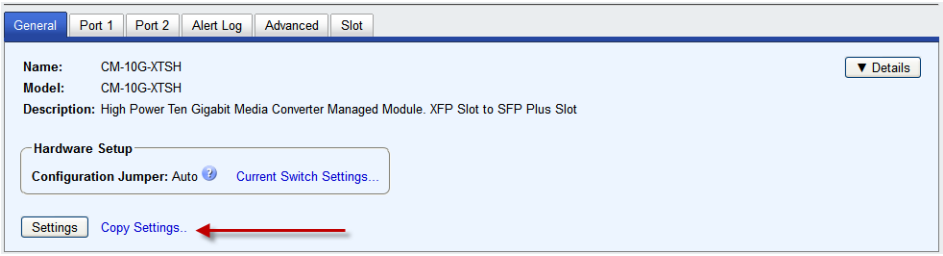
1000 Mbps only SFP



Auto-Negotiation

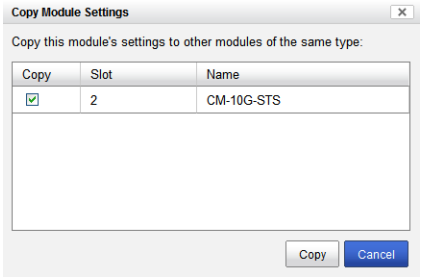
When enabled, the Media Converter Module will negotiate with its link partner to determine the most optimal parameters for this connection.

Copy Settings



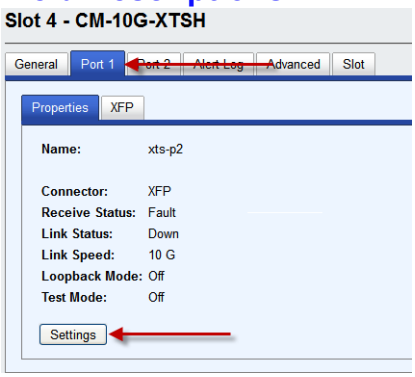
Copy Module Settings

Copy this module's settings to other modules of the same type.

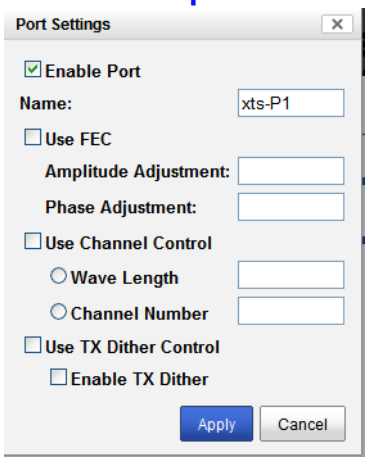


Port 1 Tab

Field Descriptions



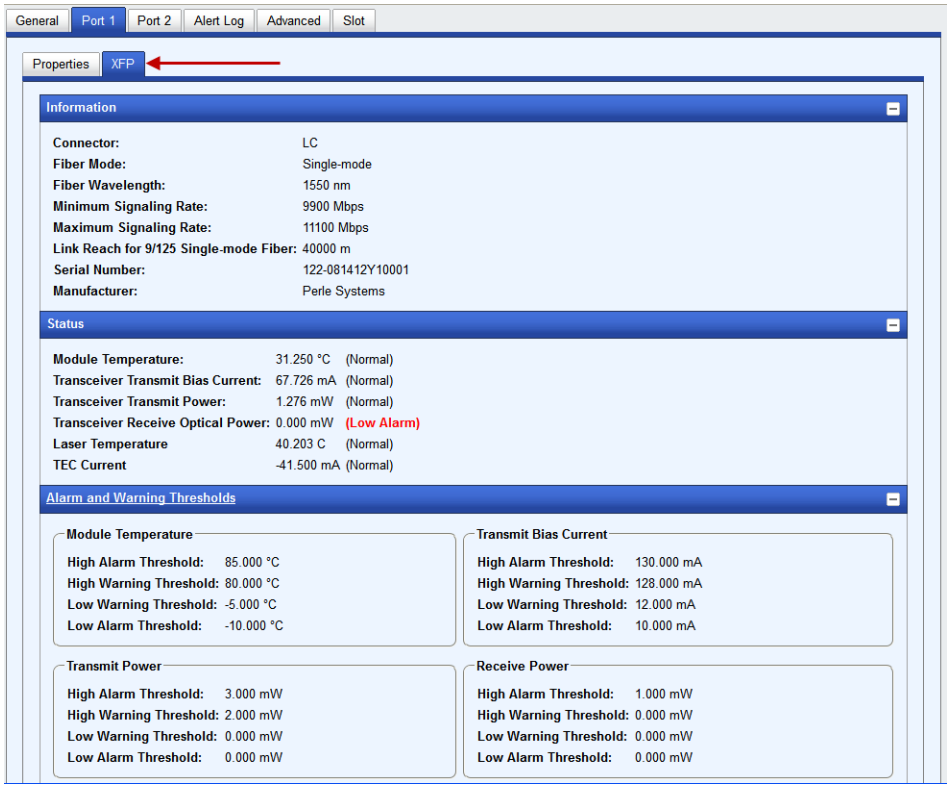
Port 1 > Properties



Configure the following parameter:

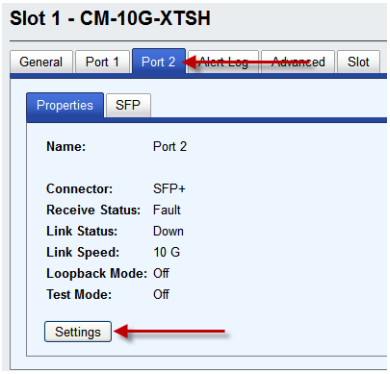
Enable Port	Enables/Disables the fiber port.
Name	The name of the fiber port. **Field Format:** 8 characters
Use FEC*	*** Note: See manufacturers documentation for parameter settings.**
Use Channel Control*	*** Note: See manufacturers documentation for parameter settings.**
Use TX Dither Control*	*** Note: See manufacturers documentation for parameter settings.**

Port 1 > XFP

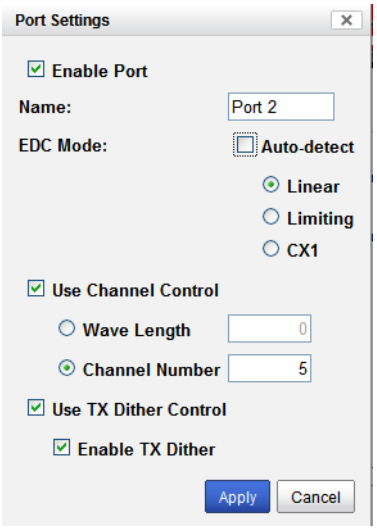


Port 2 Tab

Field Descriptions

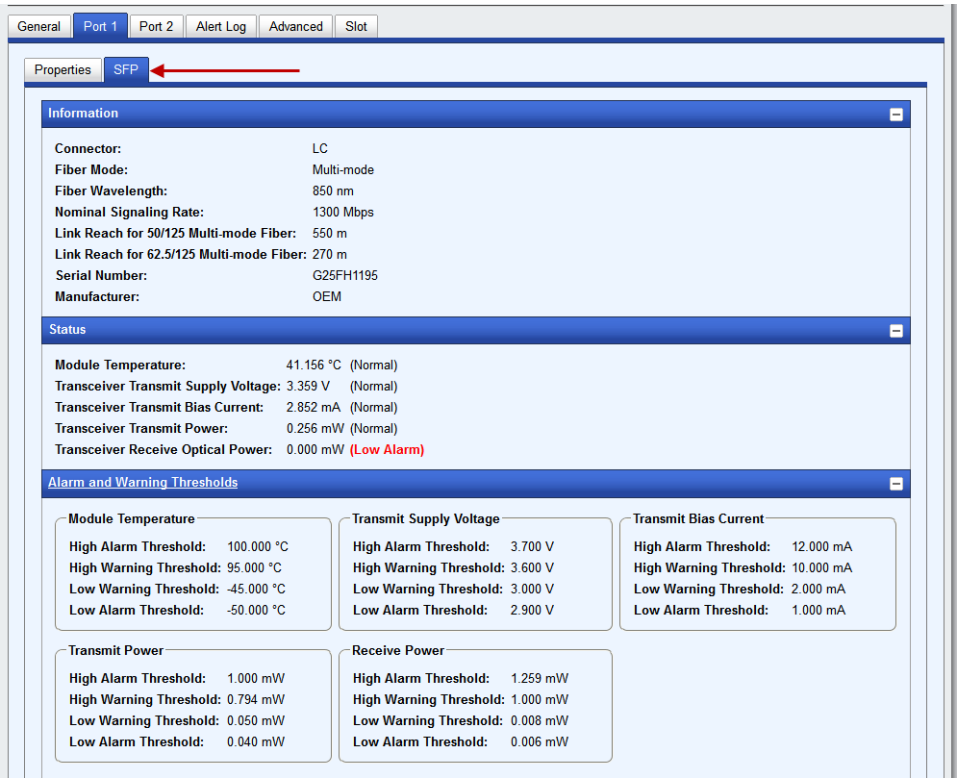


Port 2 > Settings



Enable Port	Enables/Disables the fiber port.
Name	The name of the fiber port. **Field Format:** 8 characters
EDC Mode*	*** Note: See manufacturers documentation for parameter settings.**
Use Channel Control*	*** Note: See manufacturers documentation for parameter settings.**
Use TX Dither Control*	*** Note: See manufacturers documentation for parameter settings.**

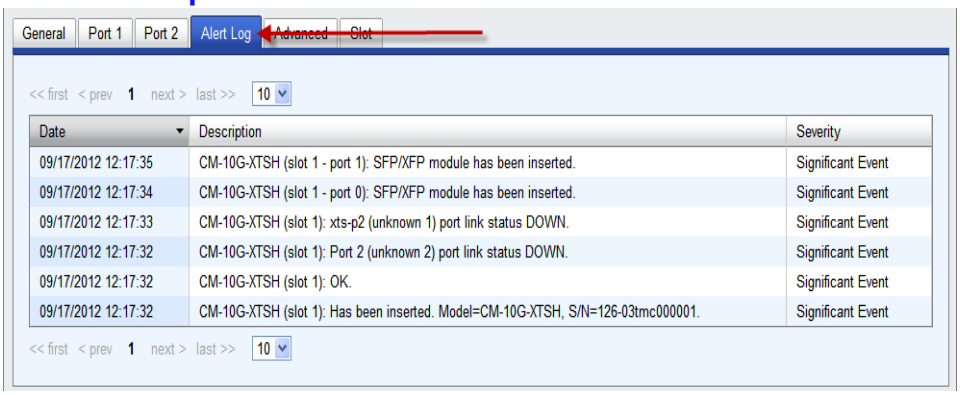
Port 2 > SFP



Note: The View Module Memory feature should only be used if guided by a Perle Technical Support Representative.

Alert Log Tab

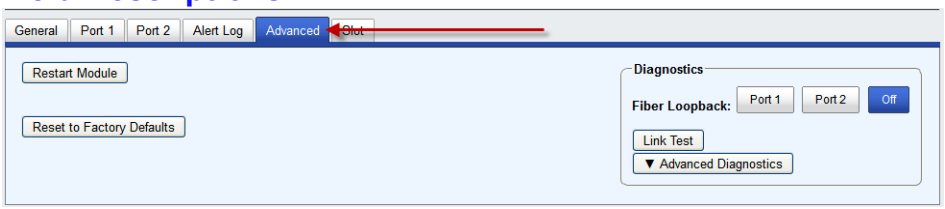
Field Descriptions



Displays the current local Alerts. The local Alert buffer contains the last 200 alerts and displays these events in a wrap around fashion.

Advanced Tab

Field Descriptions



Configure the following parameter:

Restart Module — Restarts this Media Converter Module.

Reset Factory Defaults — Resets this Media Converter Module back to factory defaults.

Diagnostics

Fiber Loopback — **Port 1:** Port 1 will be in loopback mode. All data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection.

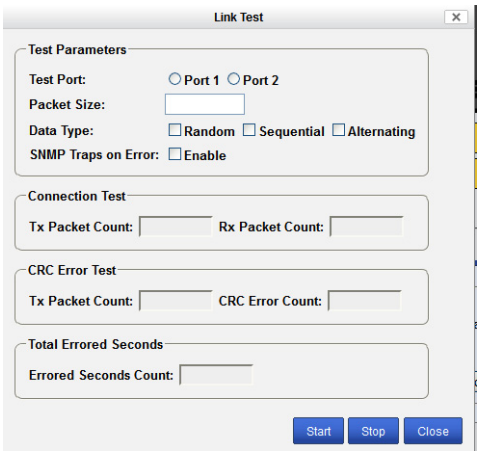
Port 2: Port 2 will be in loopback mode. All data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection.

Off: Loop back mode is off.

(**Note**: only one port can be in loopback mode at a time)

Link Test — This command enables a port on a Perle 10G media converter module to generate test patterns to a remote media converter module. If the remote media converter module is a Perle 10G then the remote end will automatically be put into loopback mode. This test is used to help identify link issues.

Link Test



Test Port

This is the port that will generate the test patterns to be sent to the remote media converter. The other port will be disabled during the running of these tests.

Values: port 1 or port 2

Packet Size

The test will use this packet size when running the tests.

Values: 256-8960 bytes

Default: 256 bytes

Data Type

Specify how the tests will run.

Values: Random, Sequential, Alternating (0101)

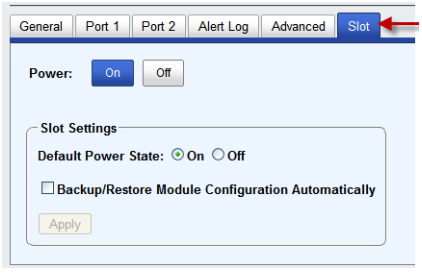
Default: 256 bytes

Advanced Diagnostics, Read/Write Register

This feature should only be used if guided by a Perle Technical Support Representative. Use of this feature without guidance from a Perle Technical Support Representative could make your Media Converter Module inoperable.

Slot

Field Descriptions



Configure the following parameters:

Power State	Immediately power the slot on or off. The current state of the slot is highlighted in BLUE. Press the "ON" button to immediately power the slot on. Press the "OFF" button to immediately power the slot off.
Default Power State	This is the default power state of the slot when the chassis is powered up or restarted. **Default:** On
Backup/Restore Module Configuration Automatically	**Enabled:** The configuration information associated with this slot is saved on the Management Module and will be downloaded to the Media Converter Module whenever the Media Converter Module is inserted into this slot. **Disabled:** The Media Converter Module configuration information is only kept on this Module. **Default**: Disabled

14 CM-10GT Media Converter Modules

Commercial Model

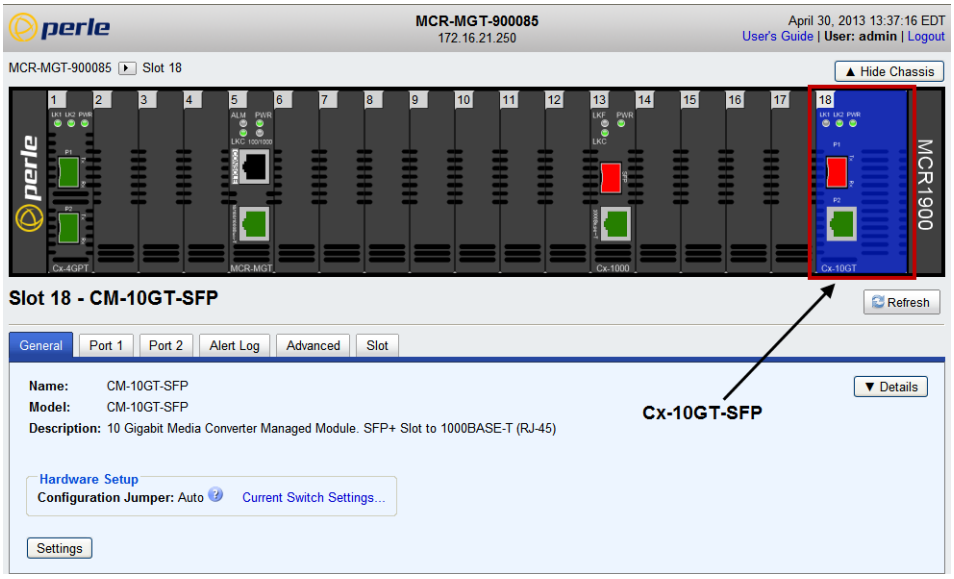
- CM-10GT-SFP - This model contains one pluggable transceiver port that permits insertion of one low power SFP+ fiber module and one intergrated RJ-45 (copper) port.

High Power Model

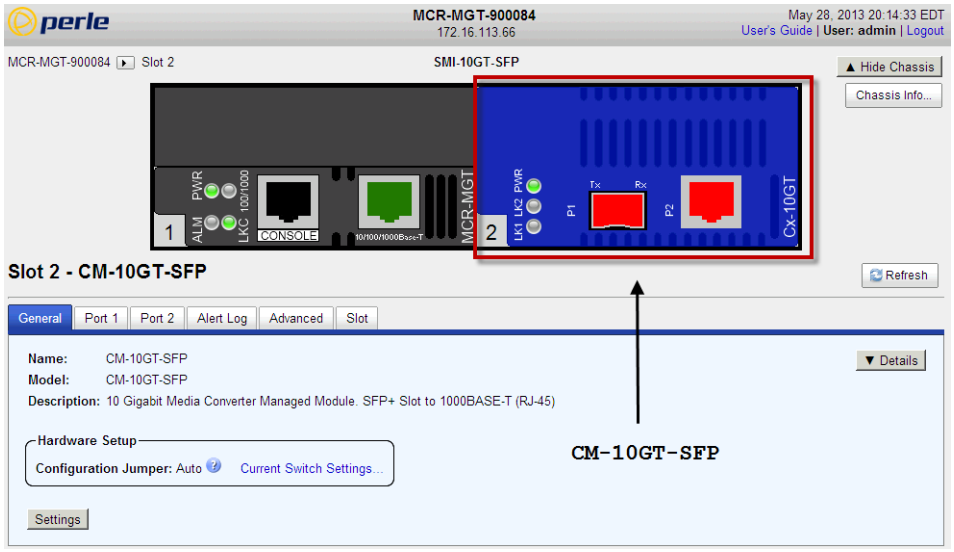
- CM-10GT-XFPH - This model contains one pluggable transceiver port that permits insertion of one high powered XFP fiber module and one intergrated RJ-45 (copper) port.

CM-10GT Module Parameters

MCR1900 Chassis

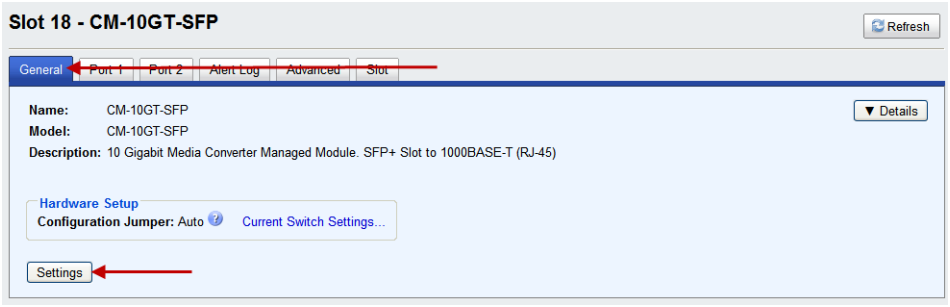


SMI Chassis



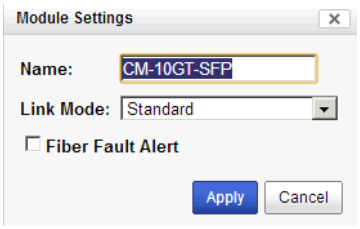
General Tab

Field Descriptions



Name	Displays the configured name for this Module.
Model	Displays the module's model information.
Description	Displays a description of the Module that is inserted in this slot.
Configuration Jumper	**Auto:** Use software configuration if present, otherwise use hardware DIP switch settings. **Switch:** Use hardware DIP switch settings. For detailed information on hardware DIP switch settings, see the Hardware Installation Guide.
Current Switch Settings	Displays the current DIP switch settings. For detailed information on hardware jumpers and DIP settings, see the Hardware Installation Guide.

General > Settings > Module Settings



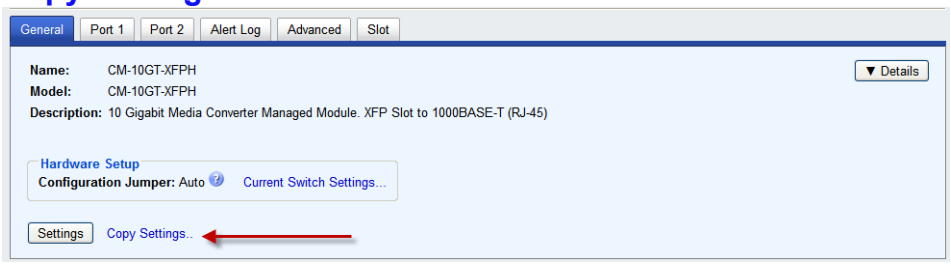
Configure the following parameters:

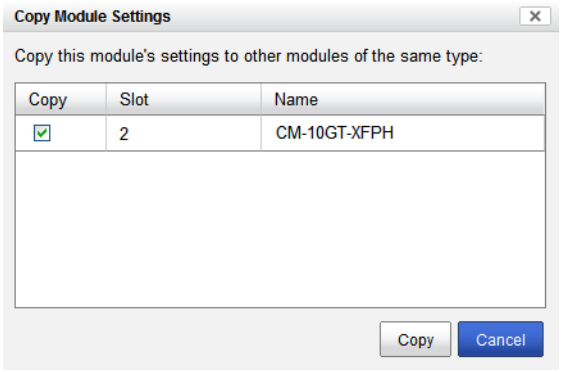
Name — Displays the configured name for this Module.

Link Mode — **Smart Link Passthrough:** In this mode, the link state on one port connection is directly reflected through the media converter to the other port. If the link is lost on one of the connections, then the other link will be brought down by the media converter.
Standard Mode: In this mode, the links can be brought up and down independently of each other. A loss of link on either connection can occur without affecting the other fiber connection.
Default: Smart Link Pass-through

Fiber Fault Alert — **Enabled:** If the media converter detects a loss of signal on the fiber port, the media converter notifies the link partner on that same port that an error condition exists by bringing down the link.
Disabled: The media converter will not monitor for fiber fault.
Default: Disabled

Copy Settings

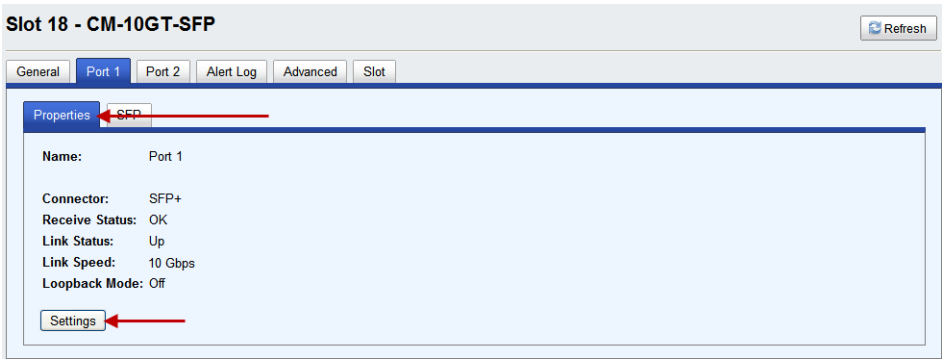




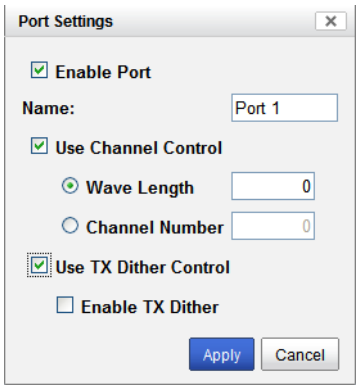
Copy Module Settings — Copy this module's settings to other modules of the same type.

Port 1 Tab (SFP installed)

Port 1 > Properties > Settings

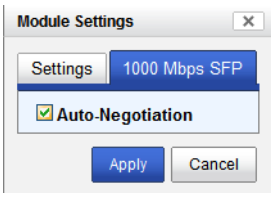


Port 1 Settings (SFP)



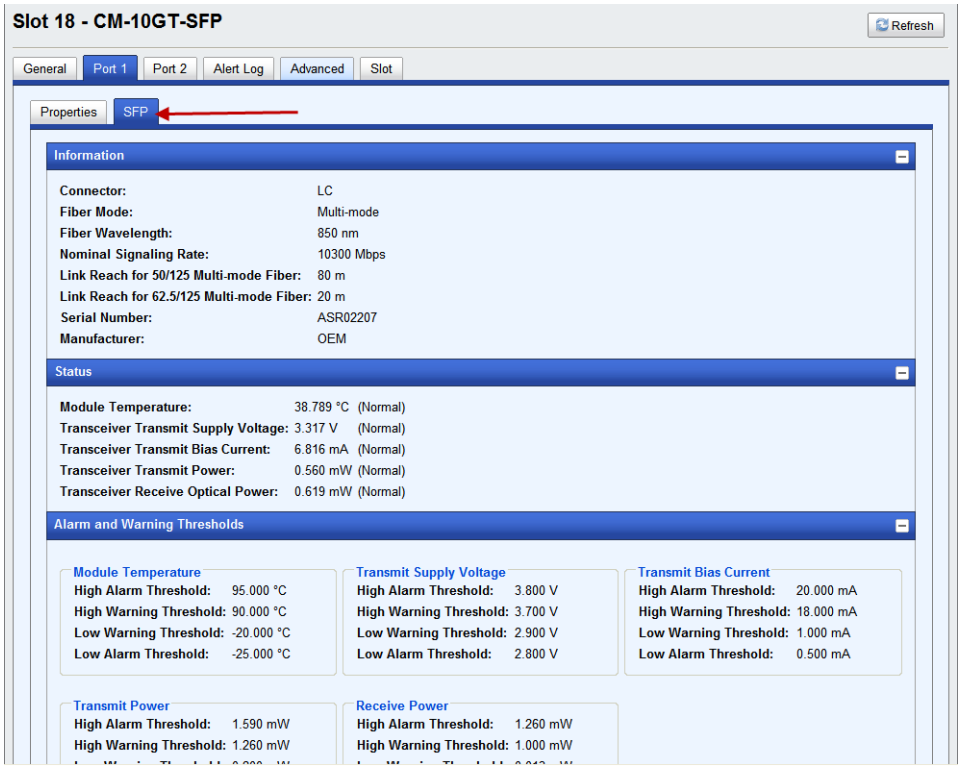
Enable Port	Enables/Disables the fiber port.
Name	The name of the fiber port. **Field Format:** 8 characters
Use Channel Control	**Settings:** **Wave length:** 0-65535 **Channel Number:** 1-65535 **Default:** Off *** Note: See manufacturers documentation for parameter settings.**
Use Dither Control	**Default:** Disable *** Note: See manufacturers documentation for parameter settings.**

Settings > 1000 Mbps SFP



Auto-Negotiation When enabled, the Media Converter Module will negotiate with its link partner to determine the most optimal parameters for this connection. This applies to 1000 SFP modules only.
Default: Enabled

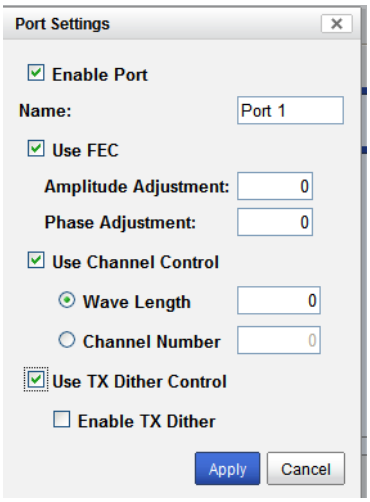
Port 1 > SFP



Port 1 Tab (XFP installed)

Port 1 > Properties > Settings

Port 1 Settings (XFP)



Enable Port — Enables/Disables the fiber port.

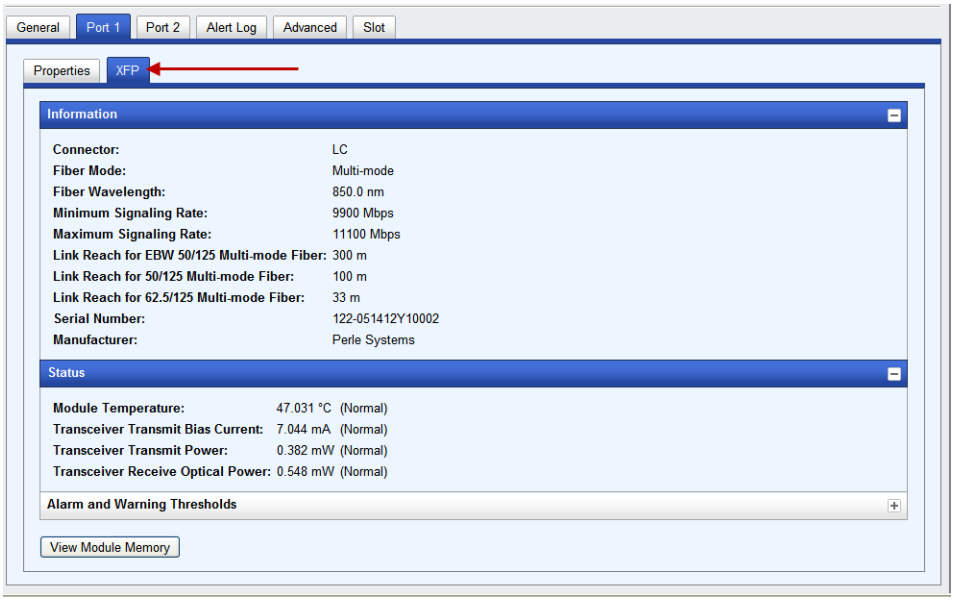
Name — The name of the fiber port.
Field Format: 8 characters

Use FEC
Settings:
Amplitude Adjustment: -128 to 127
Phase Adjustment: -128 to 127
Default: Disabled
*** Note: See manufacturers documentation for parameter settings.**

Use Channel Control
Settings:
Wave length: 0-65535
Channel Number: 1-65535
Default: Off
*** Note: See manufacturers documentation for parameter settings.**

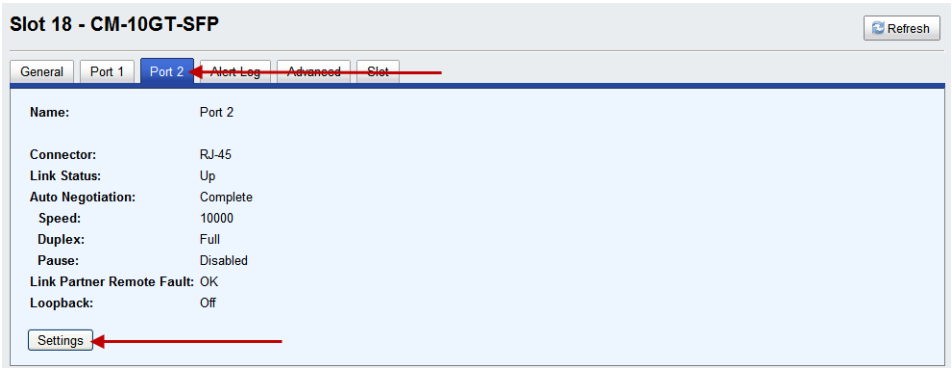
Use TX Dither
Default: Disable
*** Note: See manufacturers documentation for parameter settings.**

Port 1 > XFP

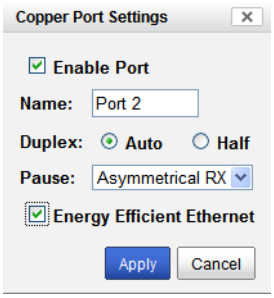


Port 2 Tab (Copper)

Port 2 > Settings



Port 2 > Copper Port Settings

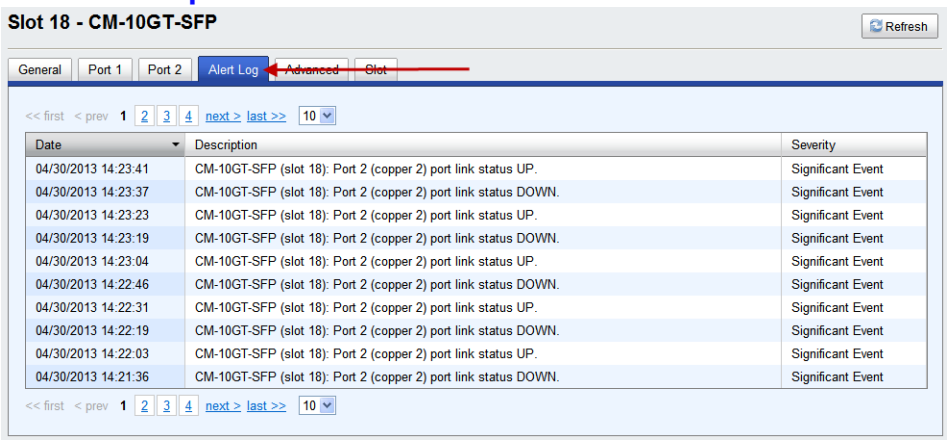


Enable Port	Enables/Disables the copper port. **Default:** Enable
Name	The name of the copper port. **Field Format:** 8 characters

Duplex	**The following selections are available:** **Duplex:** Auto, Half **Default:** Auto This duplex configuration parameter will only be used for 1 gigabit SPF modules. For 10 gigabit modules, full duplex will always be advertised
Pause	When enabled, the Media Converter Module will advertise the following Pause capabilities: ● Symmetrical ● Asymmetrical TX ● Asymmetrical RX **Note: Pause feature will only work if Auto Negotiation is set to OFF on the fiber port and Duplex is set to Full.** **Default:** Off
Energy Efficient Ethernet (EEE)	**Enabled:** When enabled, the media converter module will auto negotiate EEE with the attached EEE compliant devices/servers. **Disabled:** The media converter module will not auto negotiate EEE with attached the EEE compliant devices/servers. **Default:** Enabled

Alert Log Tab

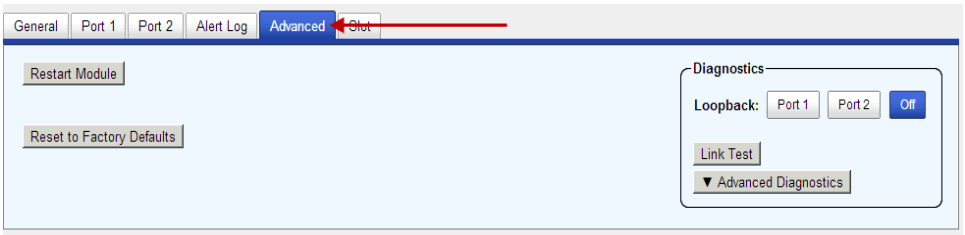
Field Descriptions



Displays the current local Alerts. The local Alert buffer contains the last 200 alerts and displays these events in a wrap around fashion.

Advanced Tab

Field Descriptions



Restart Module — Restarts this Media Converter Module.

Reset Factory Defaults — Resets this Media Converter Module back to factory defaults.

Diagnostics

Loopback — **Port 1:** Port 1 (fiber) will be in loopback mode. Data received on the receive (RX) fiber connection is looped back to the transmit (TX) fiber connection.

Port 2: Port 2 (copper) will be in loopback mode. Data received on the TXD lines are looped back to the RXD lines.

Off: Loop back mode is off.

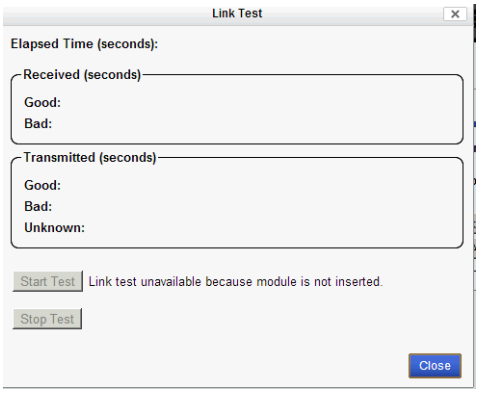
(**Note**: only one port can be in loopback mode at a time)

Link Test — The Link Test involves sending a pattern to the remote peer, having him validate the pattern and send back a response indicating whether he received the pattern correctly or not. Based on the response from the peer, the local module is able to obtain one of three statuses for that transaction (which is repeated every second). See ***Link Test Responses***.

Advanced Diagnostics, Read/Write Register — This feature should only be used if guided by a Perle Technical Support Representative. Use of this feature without guidance from a Perle Technical Support Representative could make your Media Converter Module inoperable.

Note: The View Module Memory feature under the Advanced Diagnostics menu should only be used if guided by a Perle Technical Support Representative.

Link Test



Link Test Responses

Received

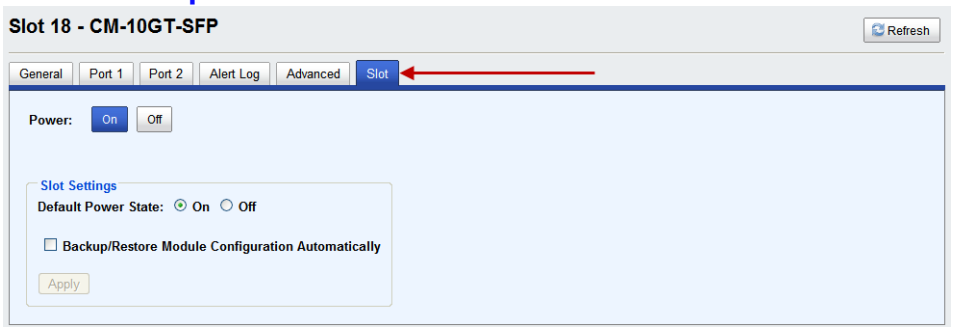
- **Good -** The local module received a “good” response from the peer.
- **Bad -** The response received from the peer was received in error or not received at all

Transmitted:

- **Good** - The remote peer indicated that the data sent by the local module was received correctly.
- **Bad -** The remote peer indicated that the data sent by the local module was received in error
- **Unknown -** The local module was unable to decode the message sent by the remote peer (this is a “bad” receive status). Since the local module is unable to decode what the peer sent back, it is unable to determine if the data it transmitted to the peer was received correctly.

Slot

Field Descriptions



Power State

Immediately power the slot on or off. The current state of the slot is highlighted in BLUE.

Press the "ON" button to immediately power the slot on.

Press the "OFF" button to immediately power the slot off.

Default Power State

This is the default power state of the slot when the chassis is powered up or restarted.

Default: On

Backup/Restore Module

Enabled: The configuration information associated with this slot is saved on the Management Module and will be downloaded to the Media Converter Module whenever the Media Converter Module is inserted into this slot.

Disabled: The Media Converter Module configuration information is only kept on this Module.

Default: Disabled

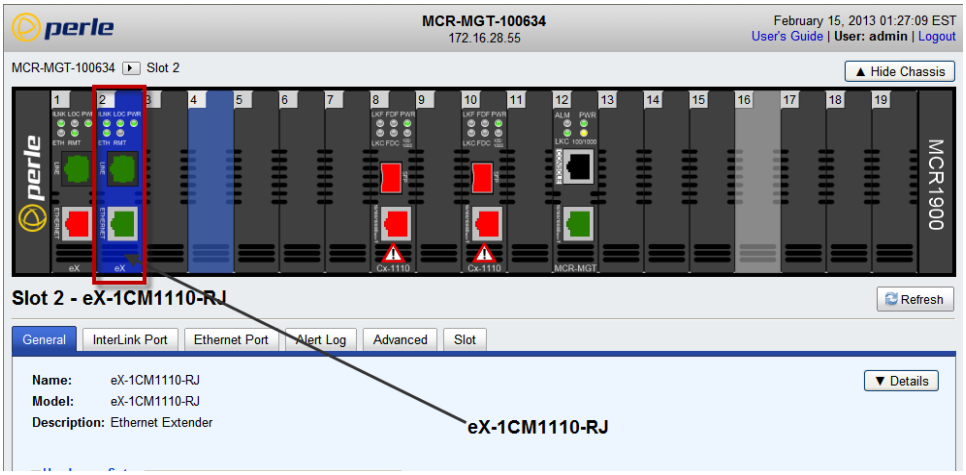
15 eX-1CM110/1110 Media Converter Modules

eX-1CM110/1110 Models

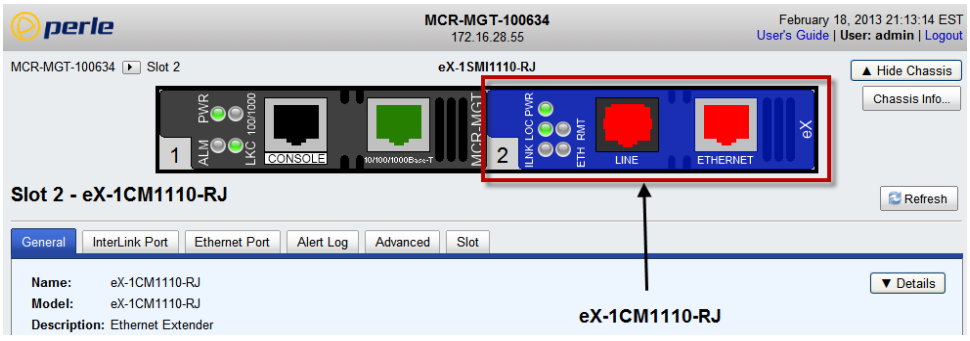
- eX-CM110 - This model contains one Ethernet port and one VDSL Line port with Ethernet speeds of 10/100 megabits.
- eX-CM1110 - This model contains one Ethernet port and one VDSL Line port with Ethernet speeds of 10/100/1000 megabits.
- Both models can be ordered either with an RJ-45, BNC or Terminal Block connector for the VDSL line port.

eX-1CM110/1110 Modules Parameters

MCR1900 Chassis

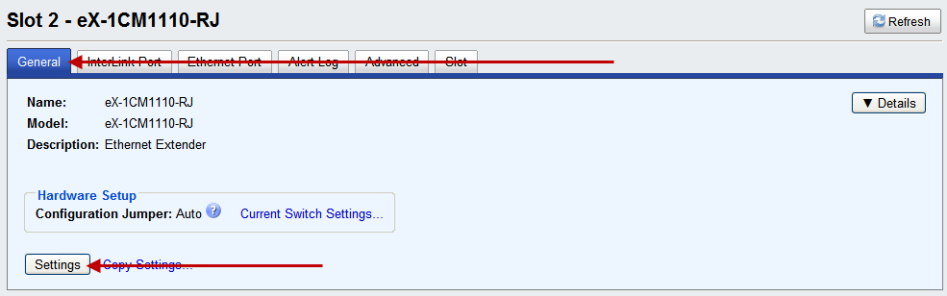


SMI Chassis



General Tab

Field Descriptions



Name — Displays the configured name for this Module.

Model — Displays the module's model information.

Description — Displays a description of the Module that is inserted in this slot.

Configuration Jumper — **Auto:** Use software configuration if present, otherwise use hardware DIP switch settings.

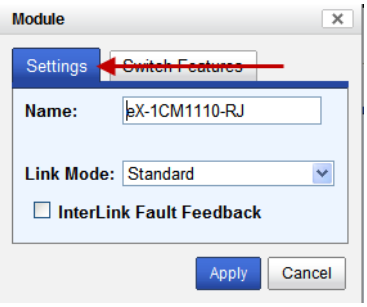
Switch: Use hardware DIP switch settings.

For detailed information on hardware DIP switch settings, see the Hardware Installation Guide.

Current Switch Settings — Displays the current DIP switch settings.

For detailed information on hardware jumpers and DIP settings, see the Hardware Installation Guide.

General > Settings



Name — Displays the configured name for this Module.

Link Mode — **Standard Mode:** In this mode, the Ethernet Extender module will not pass the state of the Ethernet interface across the Line connection to its peer. A loss on the Ethernet interface can occur without affecting the peer connection.

Link Pass-Through: In this mode, the Ethernet Extender will pass the state of the Ethernet interface across the Line connection to its peer. If link is lost on the Ethernet connection, then the peer Ethernet connection will be brought down by the remote Ethernet Extender. This is accomplished by signalling Link Pass-Through across the VDSL line without bringing down the link.

Default: Standard Mode

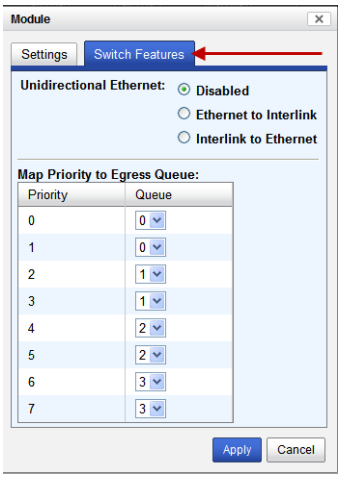
Interlink Fault Feedback

The status of the VDSL interface will be passed to its Ethernet interface. If the VDSL line link is lost the Ethernet link will be brought down.

When Interlink Fault Feedback is unchecked the status of the VDSL interface will not be passed to its Ethernet interface.

Default: unchecked

General >Switch Settings



Unidirectional Ethernet

When enabled, this feature provides the ability to restrict the flow of data between the Ethernet and Interlink port.

Values:

- Disabled
- Ethernet to Interlink
- Interlink to Ethernet

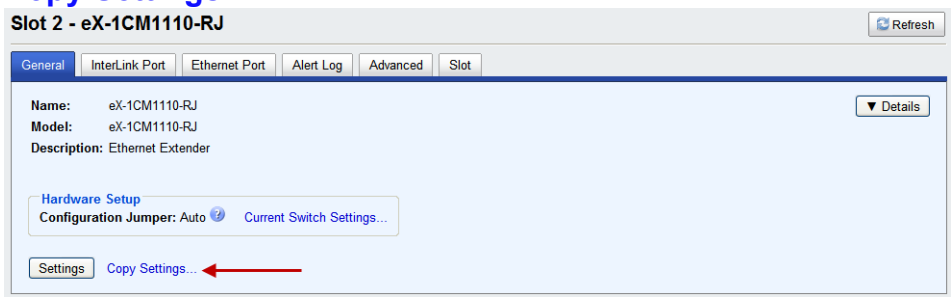
Default: Disabled

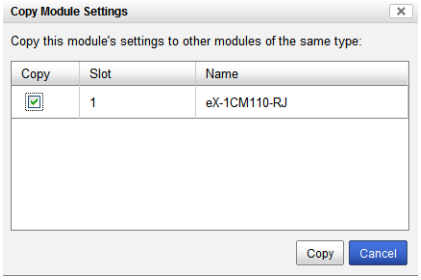
Map Priority to Egress Queue

This is the **default** egress priority mapping for both the Ethernet and Interlink port.

- Priority 0 (lowest priority)... Queue 0
- Priority 1... Queue 0
- Priority 2... Queue 1
- Priority 3... Queue 1
- Priority 4... Queue 2
- Priority 5... Queue 2
- Priority 6... Queue 3
- Priority 7... (highest priority)...Queue 3

Copy Settings

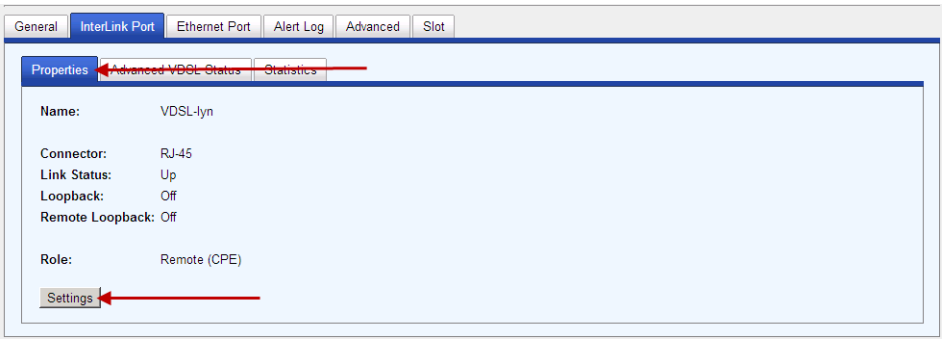




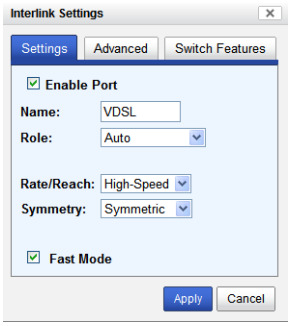
Copy Module Settings — Copy this module's settings to other modules of the same type.

Interlink Port > Properties

Interlink Port > Properties > Settings



Settings



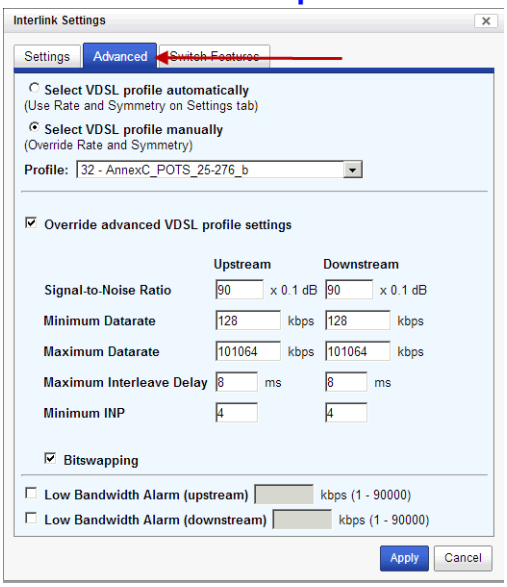
Enable Port — Enable/Disable Interlink port.
Default: Enabled

Name — The name of the Interlink port.
Length: characters (1-8)

Role	**Auto:** If at least one Ethernet Extender is configured for Auto mode, a proprietary method of detection is implemented for each attempt to synchronize one side of the link to local and the other side of the link to remote. However, it is preferable to configure one Ethernet Extender to Local and the other Ethernet Extender to Remote since this may result in slightly faster training times and direct control over their roles. **Local (C0)**: This Ethernet Extender is set to the Local mode of operation. **Remote (CPE):** This Ethernet Extender is set to the Remote mode of operation. **Note:** Ethernet Extender modules work in pairs. If both Ethernet Extenders are not set to Auto, then one side of the link must be set to Local/Auto and the other end must be set to Remote/CPE.
Rate/Reach	**High Speed:** In this mode, the VDSL connection will be optimized for maximum attainable speeds. **Long Range:** In this mode, the VDSL connection will be optimized for distance and the achievable distance will be up to 1 mile (3 km).
Symmetry	**Symmetric:** Set this mode to Symmetric if your network data needs are almost equal for uploads and downloads (both directions). **Asymmetric:** Set this mode to Asymmetric if your network data needs are primarily for downloads. Data direction is towards the remote Ethernet Extender.
Fast Mode	Fast mode reduces frame latency when using shorter cable distances. **Default:** Enabled **Note:** Using Interlink override values for upstream and downstream SNR and/or INP may disable Fast Mode.

Note: The actual distance and rates may vary depending on the environment and type/gauge of wire used. There will always be a compromise between speed and range. For more information on hardware specifications see the Perle website at www.perle.com.

Interlink Port > Properties > Settings > Advanced



Select VDSL Profile Automatically "Select VDSL profile automatically" to use the configured settings for Rate and Symmetry on the settings tab.

Select VDSL Profile Manually "Select VDSL profile manually" to override the configured settings for Rate and Symmetry on the settings tab. Then select a profile from the drop down list. For a description of the VDSL profiles, refer to the ITU-T recommendation G.993.2.

Override advanced VDSL profile settings Select this checkbox to override specific parameters associated with the VDSL line.

Note: Advanced settings for VDSL are only valid if your Ethernet Extender has been configured with a role of Local.

Signal to Noise Ratio Configure the value to be used for Signal to Noise Ratio.

The Ethernet Extender module will attempt to maintain the desired SNR value by adjusting line settings. A larger dB number will result in less line errors and a more stable connection, but may result in slower speeds.

If Rate/Reach is set to High Speed the default value is 90dB for both upstream and downstream data.

If Rate/Reach is set to Long Range the default value is 60dB for both upstream and downstream data.

Values: Upstream/Downstream: 30 - 240 (3 - 24 dB)

Minimum Data Rate The minimum data rate of the VSDL link.

Values: Upstream/Downstream 128 - 101064 kbps

Maximum Data Rate The maximum data rate of the VSDL link.

Values: Upstream/Downstream 128 - 101064 kbps

Maximum Interleave Delay Interleaving is a method of taking packets, chopping them up into smaller bits and then rearranging them so that once contiguous data is now spaced further apart into a noncontinuous stream. This provides better noise protection but increases latency.

Enter the maximum acceptable gap in the data.

Values: Upstream/Downstream 0-16 ms

Minimum Impulse Noise Protection (INP)
This is a measure of minimum amount of protection, in terms of the discrete multi-tone (DMT) symbols that can be recovered if impulse noise occurs in a burst.

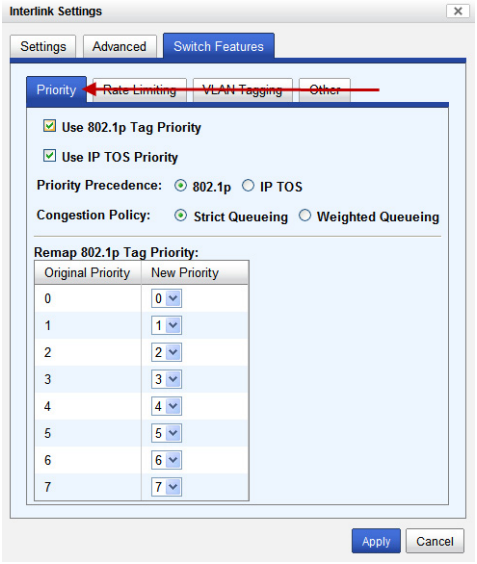
Fast Mode
Values: Upstream/Downstream 1-18

Bitswapping
As line conditions change, bit swapping allows the modem to swap bits around different channels without retraining as each channel becomes more or less capable. If bit swapping is disabled, the modem will need to retrain in order to adapt to changing line conditions.

Low Bandwidth Alarm (up)
When the Upstream link is established the Ethernet Extender module will check the low bandwidth value. If the data rate is below the threshold value, an SNMP trap will be generated.
Values: 1-90000 kbps

Low Bandwidth Alarm (down)
When the Downstream link is established the Ethernet Extender module will check the low bandwidth value. If the data rate is below the threshold value, an SNMP trap will be generated.
Values: 1-90000 kbps

Interlink Port > Properties > Settings > Switch Features > Priority



Enable 802.1p Priority
When enabled, the media converter module will use IEEE 802.1p tagged frame priority control to assign ingress frames to the appropriate priority egress queue.
Default: Enabled

Enable IP TOS Priority
When enabled, the media converter module will use IPv4 Diffserv or IPv6 traffic class field to assign ingress frames to the appropriate priority egress queue.
Default: Enabled

Priority Precedence
When both 802.1p priority and IP TOS priority are selected, you can select which of the two priorities takes precedence.
Default: 802.1p

Remap 802.1p Tag Priority

Remap IEEE 802.1p ingress frames with a new priority tag. This new priority tag will be used to determine which queue the frame gets posted to.

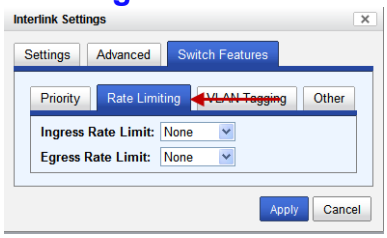
Original Priority -----> New Priority

Values: 0-7

Congestion Policy

Select a method to be used when determining the order by which frames are sent from the four egress queues. Setting the congestion policy on either the Interlink or Ethernet port will change the policy on both ports.
Strict Priority Queuing - The order is determined strictly by the priority of the queue. Frames in higher priority queues are always sent ahead of frames in lower priority queues.
Weighted Fair Queuing - This method allows lower priority frames to be inter-mixed with higher priority frames in the ratio of (**8, 4, 2, 1**).
The ratio for 8 highest priority sent frames will be as follows:
8 highest priority frames from queue 3
4 frames from queue 2
2 frames from queue 1
1 frame from queue 0

Interlink Port > Properties > Settings > Switch Features > Rate Limiting



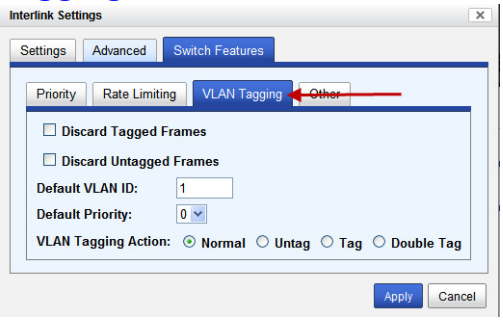
Ingress Rate Limit

Restricts ingress frames on the Interlink port.
Default: None
Data Options: none to 90 Mbps

Egress Rate Limit

Restricts egress frames on the Interlink port.
Default: None
Data Options: none to 90 Mbps

Interlink Port > Properties > Settings > Switch Features > VLAN Tagging



Discard Tagged Frames
When enabled, discards all VLAN tagged frames.
Default: Off

Discard Untagged Frames
When enabled, discards all VLAN untagged frames.
Default: Off

Default VLAN ID
Specify a default VLAN ID to insert when tagging frames.
Default: 1
Data Options: 0-4095

Default Priority
Specify a default VLAN priority to insert when tagging frames.
Default: 0
Data Options: 0-7

VLAN Tagging Actions
Define the VLAN tagging action to take on a egress frame.

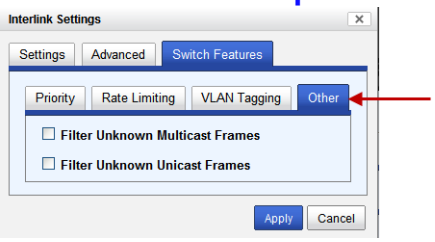
- Normal -Take no action.
- Untag - Remove any existing tag.
- Tag

  Insert tag with configured VLAN ID and VLAN priority if original frame is untagged.

  Replace tag with configured VLAN ID and VLAN priority if original frame is tagged.
- Double tag - Append a tag with configured VLAN ID and VLAN priority.

Default: Normal

Interlink Port > Properties > Settings > Switch Features > Other

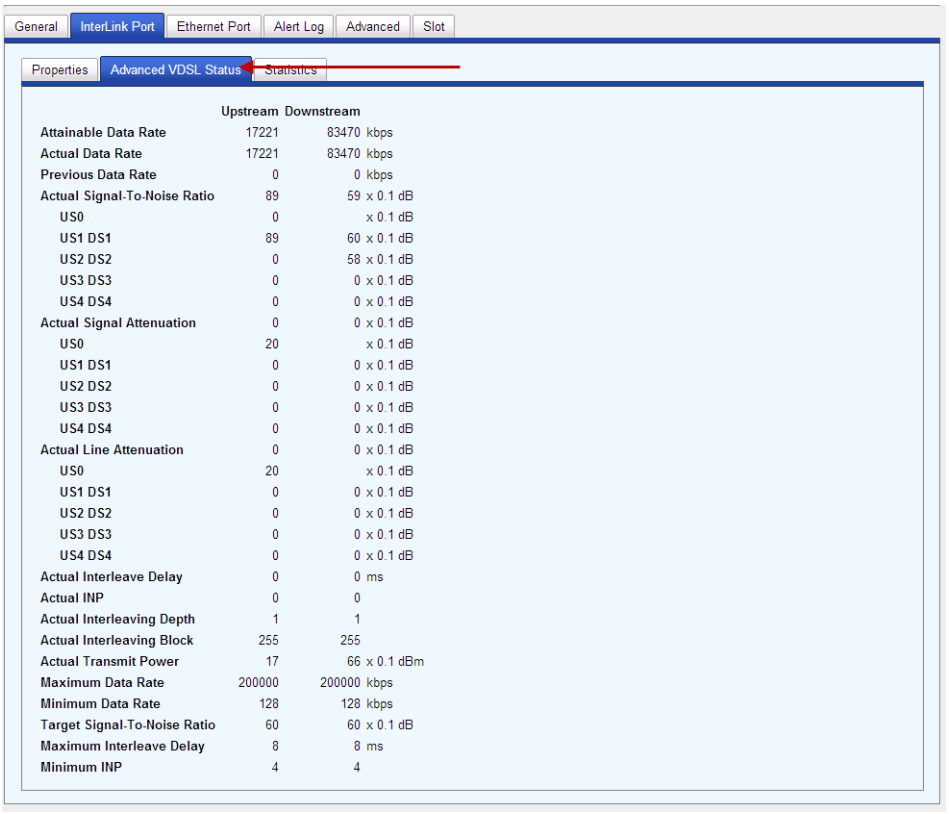


Filter Unknown Multicast Frames
When enabled, multicast frames with unknown destination addresses are not allowed to egress this port.
Default: Disabled

Filter Unknown Unicast Frames
When enabled, unicast frames with unknown destination addresses are not allowed to egress this port.
Default: Disabled

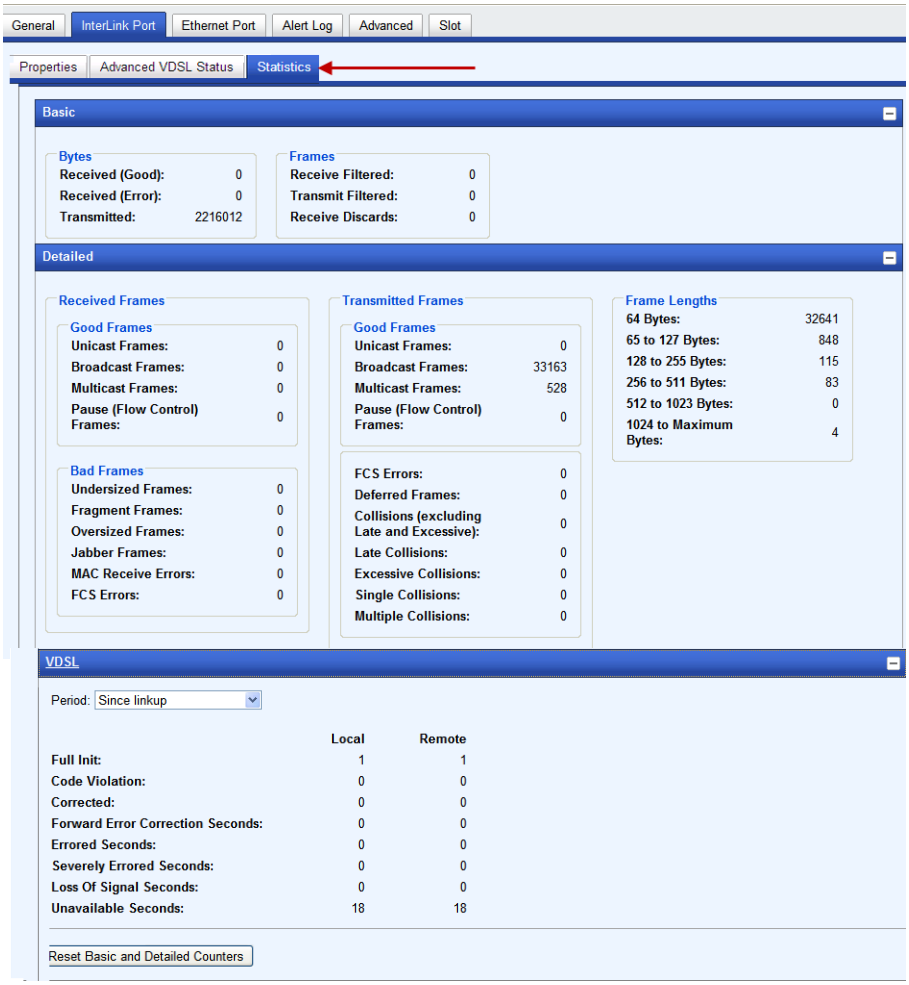
Interlink Port - Advanced VDSL Status

Displays the current statuses for the VDSL port.



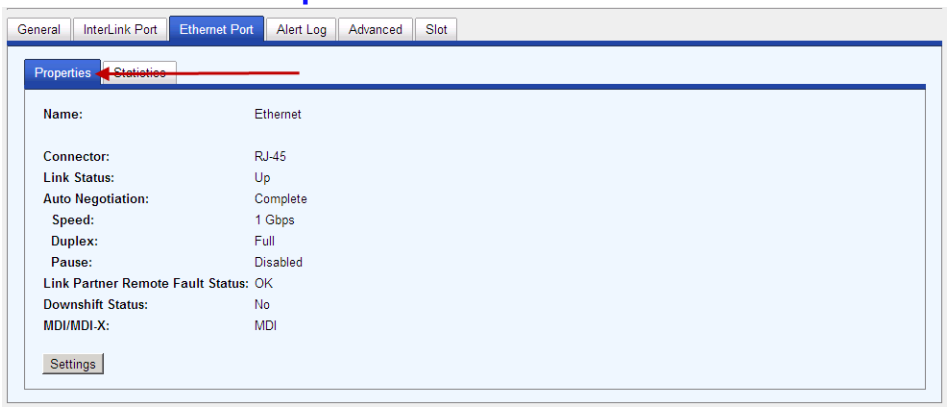
	Upstream	Downstream	
Attainable Data Rate	17221	83470	kbps
Actual Data Rate	17221	83470	kbps
Previous Data Rate	0	0	kbps
Actual Signal-To-Noise Ratio	89	59	x 0.1 dB
US0	0		x 0.1 dB
US1 DS1	89	60	x 0.1 dB
US2 DS2	0	58	x 0.1 dB
US3 DS3	0	0	x 0.1 dB
US4 DS4	0	0	x 0.1 dB
Actual Signal Attenuation	0	0	x 0.1 dB
US0	20		x 0.1 dB
US1 DS1	0	0	x 0.1 dB
US2 DS2	0	0	x 0.1 dB
US3 DS3	0	0	x 0.1 dB
US4 DS4	0	0	x 0.1 dB
Actual Line Attenuation	0	0	x 0.1 dB
US0	20		x 0.1 dB
US1 DS1	0	0	x 0.1 dB
US2 DS2	0	0	x 0.1 dB
US3 DS3	0	0	x 0.1 dB
US4 DS4	0	0	x 0.1 dB
Actual Interleave Delay	0	0	ms
Actual INP	0	0	
Actual Interleaving Depth	1	1	
Actual Interleaving Block	255	255	
Actual Transmit Power	17	66	x 0.1 dBm
Maximum Data Rate	200000	200000	kbps
Minimum Data Rate	128	128	kbps
Target Signal-To-Noise Ratio	60	60	x 0.1 dB
Maximum Interleave Delay	8	8	ms
Minimum INP	4	4	

Interlink Port - Statistics

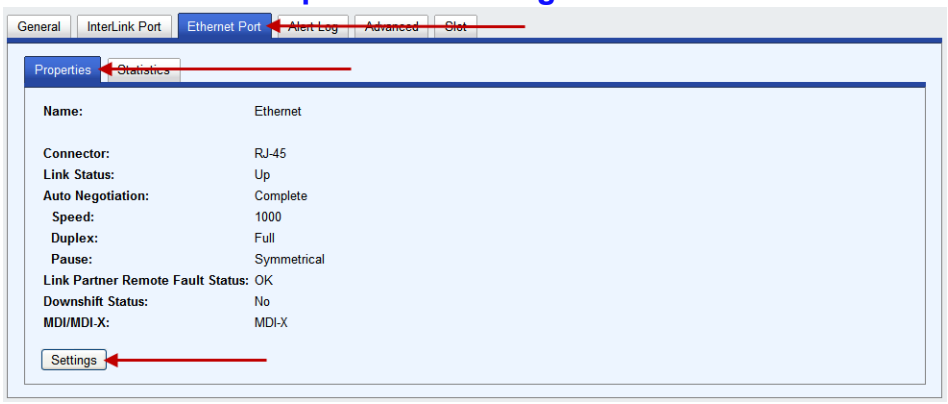


Note: Resetting Basic and Detailed counters will not reset the VDSL counters. The VDSL counters are automatically reset when the VDSL link is reset.

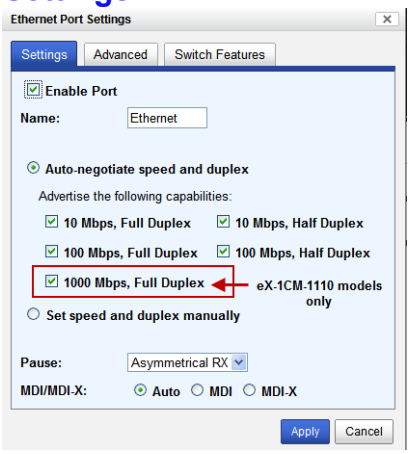
Ethernet Port > Properties



Ethernet Port > Properties > Settings



Settings



Enable Port
Enables/Disables the Ethernet port.
Default: Enable

Name
The name of the Ethernet port.
Data Values: 1-8 characters

Auto Negotiate Speed and Duplex
Define the Ethernet connection.
Data Options:

- **Auto**—automatically detects the Ethernet interface speed and duplex
- 10 Mbps/Half Duplex
- 10 Mbps/Full Duplex
- 100 Mbps/Half Duplex
- 100 Mbps/Full Duplex
- 1000 Mbps/Half Duplex (applies to eX-1CM-1110 models only)

Default: Auto

Set Speed and Duplex Manually
When enabled, the following selections are available:
Speed: 100 Mbps, 10 Mbps
Duplex: Full, Half

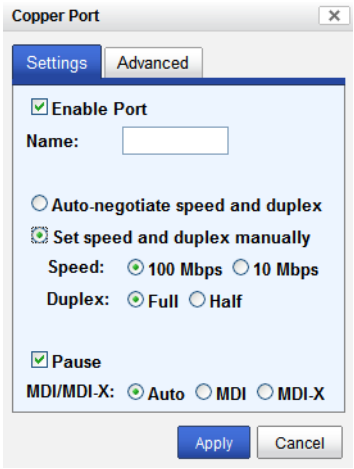
Pause — When enabled, the Media Converter Module will advertise its Pause capabilities.

MDI/MDI-X

- **Auto-Detect—** automatically detects the Ethernet's cable polarity
- **MDI** —the cable's polarity is straight-through
- **MDI-X** —the cable's polarity is crossovered

Default: Auto

Ethernet Port > Properties > Settings > Set speed and duplex manually

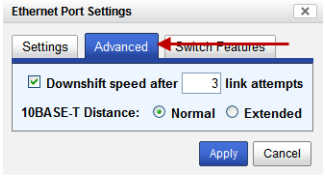


Set Speed and Duplex Manually — When enabled, the following selections are available:

Speed: 100 Mbps, 10 Mbps

Duplex: Full, Half

Ethernet Port > Properties > Settings > Advanced



Downshift speed after number of link attempts — When enabled, the number of retries the Media Converter Module will attempt to establish a fiber connection at 1000 Mbps before attempting a lower speed.

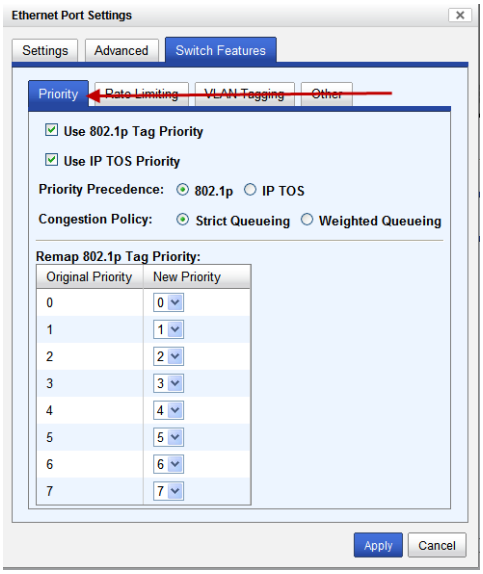
Default: On

Link attempts: 1-8

10BASE-T Distance **Normal:** the Media Converter copper link is in normal operating mode.

Extended: the Media Converter will boost the signal strength on its copper link.

Ethernet Port > Properties > Settings > Switch Features >Priority



Enable 802.1p Priority

When enabled, the media converter module will use IEEE 802.1p tagged frame priority control to assign ingress frames to the appropriate priority egress queue.
Default: Enabled

Enable IP TOS Priority

When enabled, the media converter module will use IPv4 Diffserv or IPv6 traffic class field to assign ingress frames to the appropriate priority egress queue.
Default: Enabled

Priority Precedence

When both 802.1p priority and IP TOS priority are selected, you can select which of the two priorities takes precedence.
Default: 802.1p

Remap 802.1p Tag Priority

Remap IEEE 802.1p ingress frames with a new priority tag. This new priority tag will be used to determine which queue the frame gets posted to.

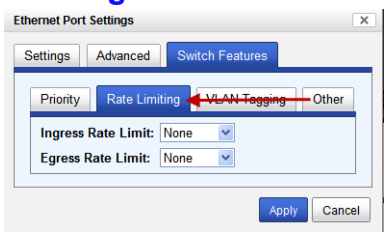
Original Priority -----> New Priority

Values: 0-7

Congestion Policy

Select a method to be used when determining the order by which frames are sent from the four egress queues. Setting the congestion policy on either the Interlink or Ethernet port will change the policy on both ports.
Strict Priority Queuing - The order is determined strictly by the priority of the queue. Frames in higher priority queues are always sent ahead of frames in lower priority queues.
Weighted Fair Queuing - This method allows lower priority frames to be inter-mixed with higher priority frames in the ratio of (**8, 4, 2, 1**).
The ratio for 8 highest priority sent frames will be as follows:
8 highest priority frames from queue 3
4 frames from queue 2
2 frames from queue 1
1 frame from queue 0

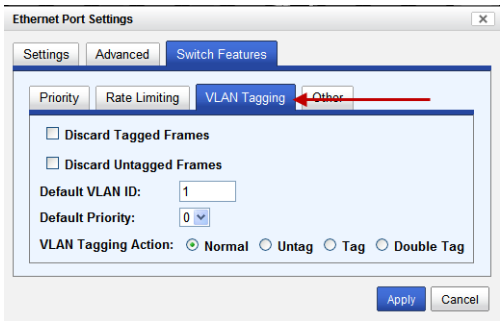
Ethernet Port > Properties > Settings > Switch Features > Rate Limiting



Ingress Rate Limit Restricts ingress frames on the Interlink port.
Default: None
Data Options: none to 90 Mbps

Egress Rate Limit Restricts egress frames on the Interlink port.
Default: None
Data Options: none to 90 Mbps

Ethernet Port > Properties > Settings > Switch Features > VLAN Tagging



Discard Tagged Frames When enabled, discards all VLAN tagged frames.
Default: Off

Discard Untagged Frames When enabled, discards all VLAN untagged frames.
Default: Off

Default VLAN ID Specify a default VLAN ID to insert when tagging frames.
Default: 1
Data Options: 0-4095

Default Priority

Specify a default VLAN priority to insert when tagging frames.
Default: 0
Data Options: 0-7

VLAN Tagging Actions

Define the VLAN tagging action to take on a egress frame.

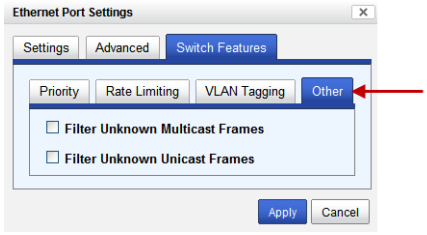
- Normal -Take no action.
- Untag - Remove any existing tag.
- Tag

  Insert tag with configured VLAN ID and VLAN priority if original frame is untagged.

  Replace tag with configured VLAN ID and VLAN priority if original frame is tagged.
- Double tag - Append a tag with configured VLAN ID and VLAN priority.

Default: Normal

Ethernet Port > Properties > Settings > Switch Features > Other



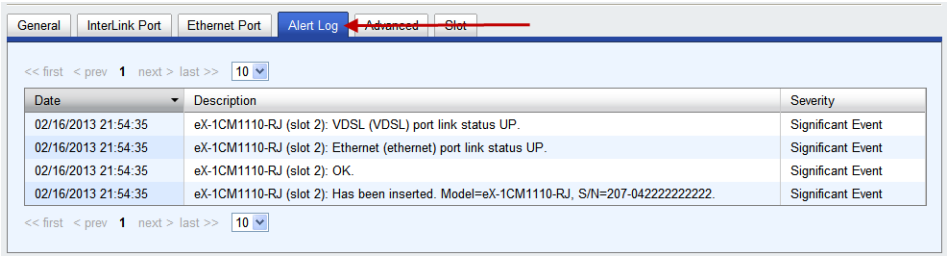
Filter Unknown Multicast Frames

When enabled, multicast frames with unknown destination addresses are not allowed to egress this port.
Default: Disabled

Filter Unknown Unicast Frames

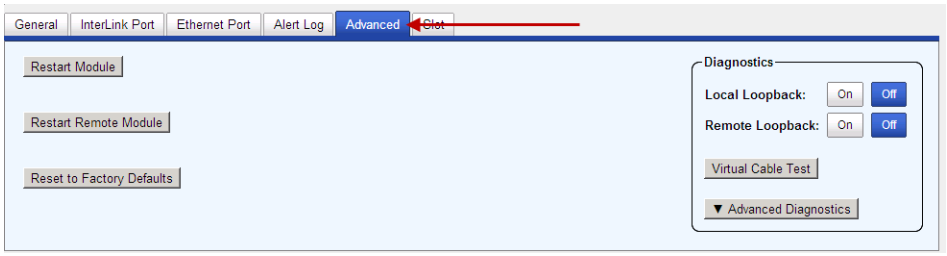
When enabled, unicast frames with unknown destination addresses are not allowed to egress this port.
Default: Disabled

Alert Log



Displays the current local Alerts. The local Alert buffer contains the last 200 alerts and displays these events in a wrap around fashion.

Advanced



Restart Module Restarts this Media Converter Module.

Restart Remote Module The local Ethernet Extender module sends a restart sequence to the remote Ethernet Extender to restart.

Reset to Factory Defaults Resets this Media Converter Module back to factory defaults.

Diagnostics

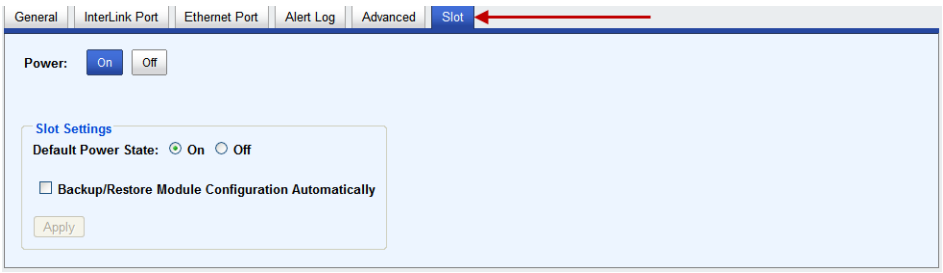
(Local) Loopback In local loopback mode any data received on the VDSL line from the remote Ethernet Extender module will be looped back to the remote Ethernet Extender module.

(Remote) Loopback In remote loopback mode any data received on the VDSL line from the local Ethernet Extender module will be looped back to the local Ethernet Extender module.

Virtual Cable Test Performs a Virtual Cable Test to remotely and non-evasively diagnose the quality and characteristics of the attached ethernet cable. This test can detect issues such as cable opens, cable shorts or any impedance mismatch in the cable and then accurately report (within one meter) the distance of the fault. In addition, this Virtual Cable Test will detect pair swaps, pair polarity reversal and excessive pair skew.

Advanced Diagnostics, Read/Write Register This feature should only be used if guided by a Perle Technical Support Representative. Use of this feature without guidance from a Perle Technical Support Representative could make your Media Converter Module inoperable.

Slot



Power Immediately power the slot on or off. The current state of the slot is highlighted in BLUE.

Press the "ON" button to immediately power the slot on.

Press the "OFF" button to immediately power the slot off.

Default Power State This is the default power state of the slot when the chassis is powered up or restarted.

Default: On

Backup/Restore

Enabled: The configuration information associated with this slot is saved on the Management Module and will be downloaded to the Media Converter Module whenever the Media Converter Module is inserted into this slot.

Disabled: The Media Converter Module configuration information is only kept on this Module.

Default: Disabled

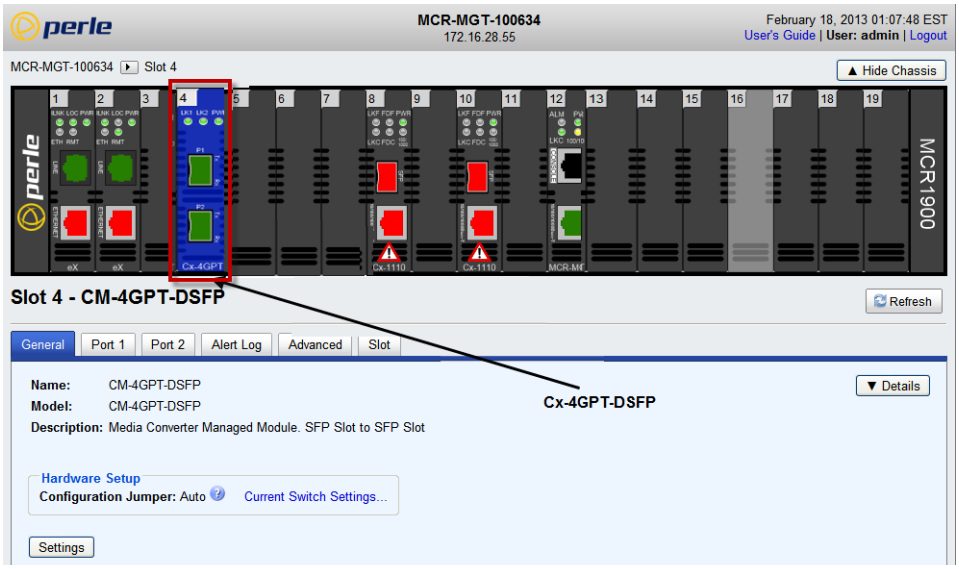
16 CM-4GPT-DSFP Media Converter Module

This module allows connections and cross connections of fiber networks of different types to each other.

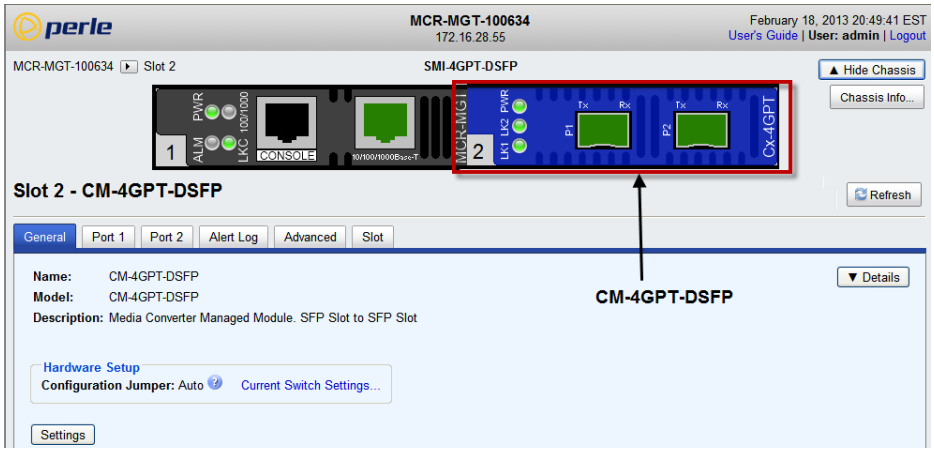
- protocol independent module using two standard SFP+ modules with speeds up to 4.25 Gbps.

CM-4GPT-DSFP Media Module Parameters

MCR1900 Chassis

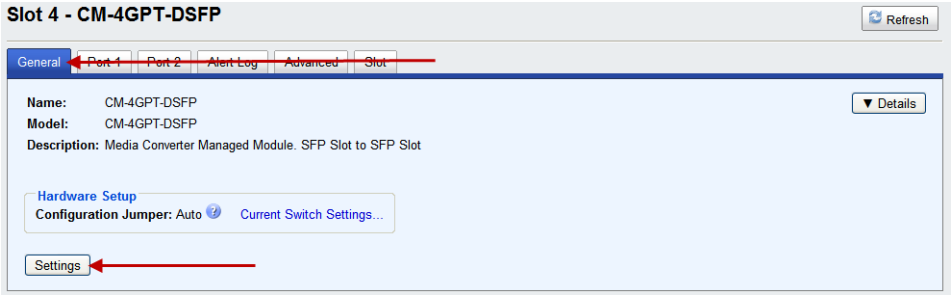


SMI Chassis



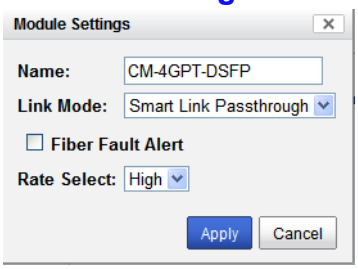
General Tab

Field Descriptions



Name	Displays the configured name for this Module.
Model	Displays the module's model information.
Description	Displays a description of the Module that is inserted in this slot.
Configuration Jumper	**Auto:** Use software configuration if present, otherwise use hardware DIP switch settings. **Switch:** Use hardware DIP switch settings. For detailed information on hardware DIP switch settings, see the Hardware Installation Guide.
Current Switch Settings	Displays the current DIP switch settings. For detailed information on hardware jumpers and DIP settings, see the Hardware Installation Guide.

Module Settings



Name

Displays the configured name for this Module.

Link Mode

Smart Link Pass-Through: In this mode, the fiber link state on one fiber connection is directly reflected through the media converter module to the other fiber connection. Since this media converter module is protocol independent, it monitors the Signal Detect indicator from the SFP and reflects this on the TX port of the other SFP by turning off the transmitter. When the signal (Link) gets restored and Signal Detect becomes active, the affected transmitter will get re-enabled.

Standard Mode: In Standard Mode the media converter module will monitor the fiber link in the same manner. If Signal Detect goes down the media converter module will output a 25MHz signal on the TX port of the other SFP.

Default: Smart-Link Passthrough

Fiber Fault Alert

Enabled: If the media converter module detects a loss of fiber signal on its fiber receiver, it will disable its fiber transmitter on the same SFP. This, in effect, notifies the fiber link partner that an error condition exists on the fiber connection.
Disabled: The module will take no action when a loss of signal is detected.
Default: Disabled

Note: If two media converters are connected to each other, FFA should not be enabled on both since this could create a "deadlock" state.

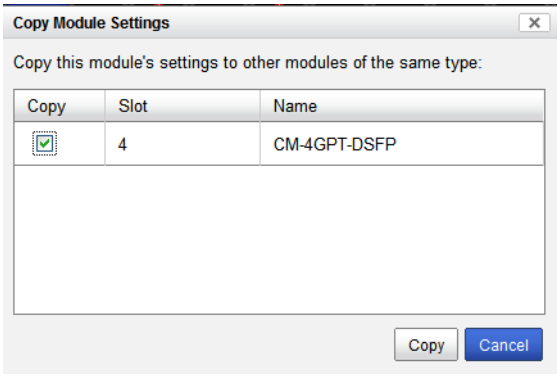
Rate Select

High Speed: when a multi-rate SFP is inserted, it is enabled for the higher speed of operation.

Low Speed: when a multi-rate SFP is inserted, it is enabled for the slower speed of operation.

Default: High

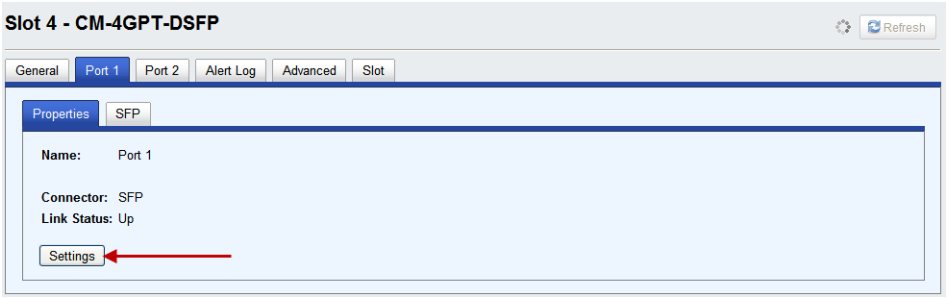
Copy Settings



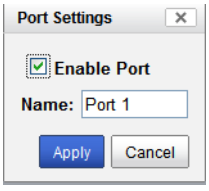
Copy Module Settings Copy this module's settings to other modules of the same type.

Port 1

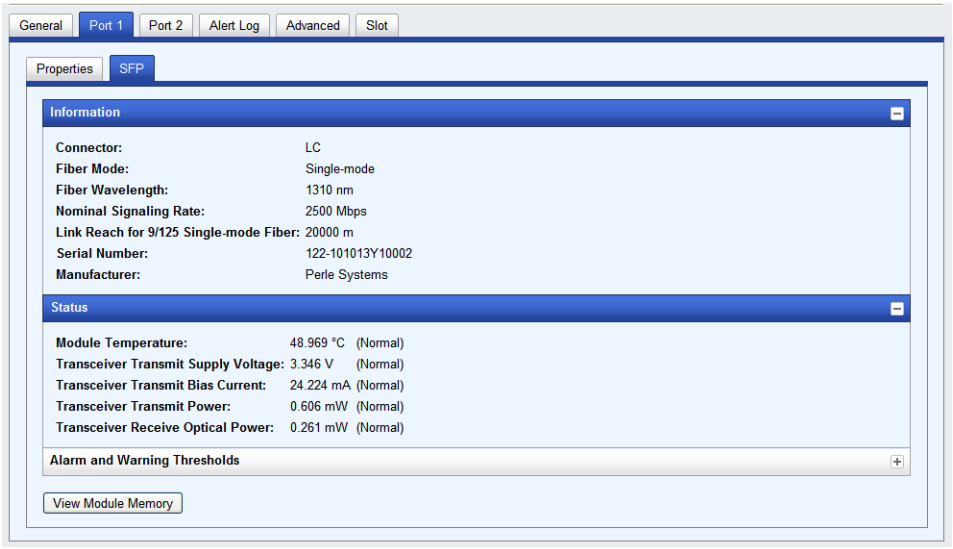
Port 1 > Properties > Settings



Settings



Port 1 SFP

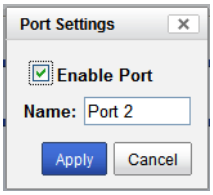


Note: The View Module Memory feature should only be used if guided by a Perle Technical Support Representative.

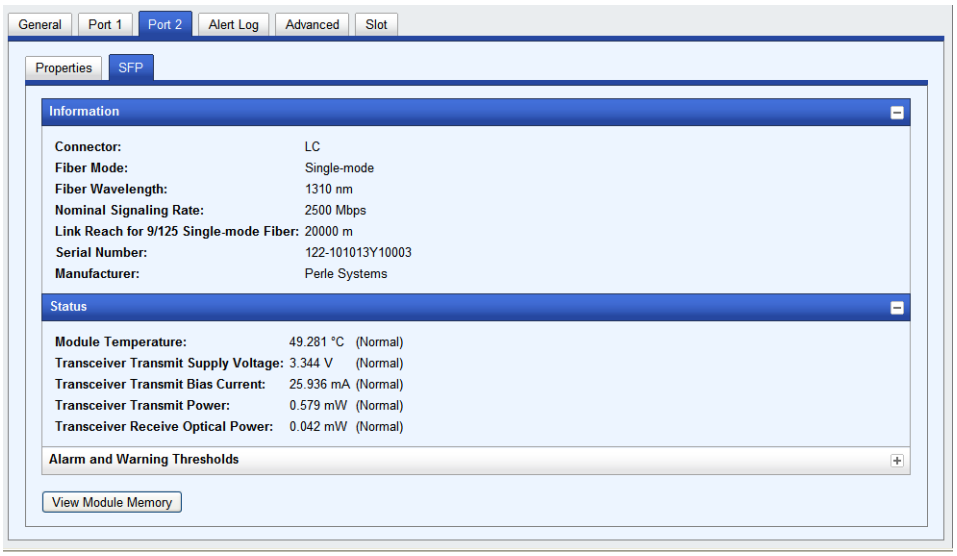
Port 2

Port 2 > Properties > Settings

Settings

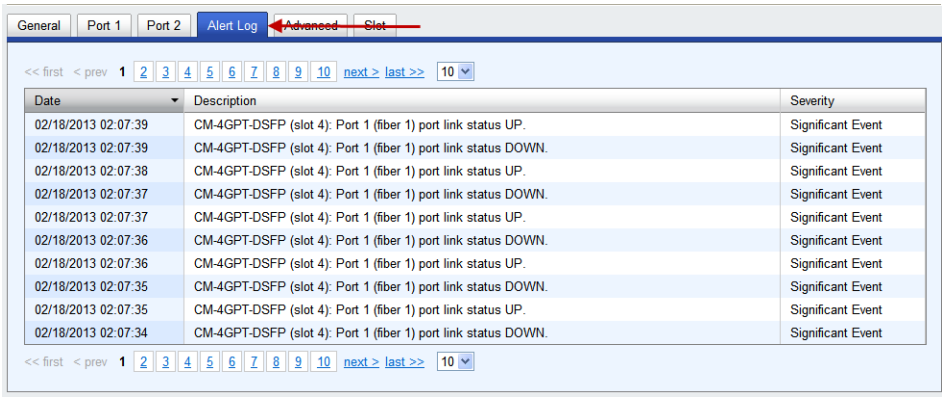


Port 2 SFP



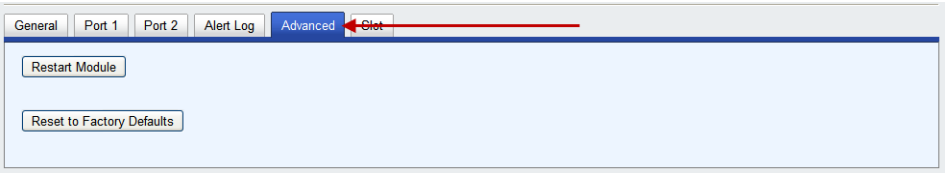
Note: The View Module Memory feature should only be used if guided by a Perle Technical Support Representative.

Alert Log



Displays the current local Alerts. The local Alert buffer contains the last 200 alerts and displays these events in a wrap around fashion.

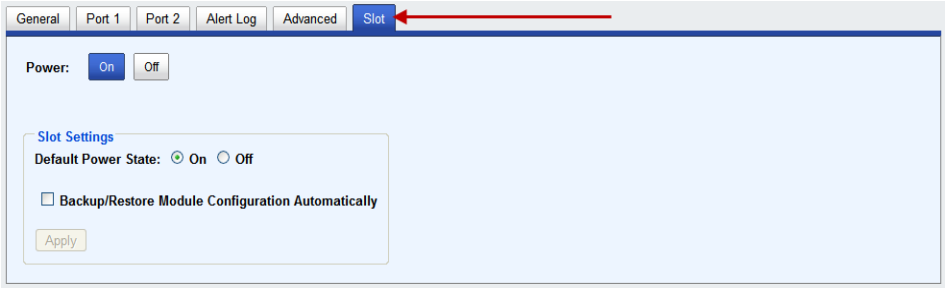
Advanced Tab



Restart Module Restarts this Media Converter Module.

Reset Factory Defaults Resets this Media Converter Module back to factory defaults.

Slot



Power State Immediately power the slot on or off. The current state of the slot is highlighted in BLUE.

Press the "ON" button to immediately power the slot on.

Press the "OFF" button to immediately power the slot off.

Default Power State This is the default power state of the slot when the chassis is powered up or restarted.

Default: On

Backup/Restore Module Configuration Automatically

Enabled: The configuration information associated with this slot is saved on the Management Module and will be downloaded to the Media Converter Module whenever the Media Converter Module is inserted into this slot.

Disabled: The Media Converter Module configuration information is only kept on this Module.

Default: Disabled

Alert Messages

Introduction

This appendix contains the list of alerts which can be generated by the MCR-MGT Management Module.

The alerts are grouped in the following sections;

- Management Module alerts
- Chassis alerts
- Power supply alerts
- Media converter alerts
- SFP related alerts

Format of alerts

Each alert consists of the following items;

- Date alert occurred
- Time alert occurred
- Name of instance of object (i.e Media Converter Module name and slot number)
- Description of event which triggered the alert
- Severity of the alert

Severity levels

Alerts are assigned a specific severity level. This enables the user to set a filter for alerts at an appropriate severity level.

The following are the severity levels defined on the MCR-MGT Management Module in decreasing severity level. Also included is the syslog equivalent level.

Severity level		Syslog equivalent
System Level Fault	-	Emergency
Module Level Fault	-	Alert
Persistent Error	-	Critical
One Time Error	-	Error
Significant Event	-	Warning
Normal Operation	-	Notice

Alert Messages

Management Module Alerts

Mgmt: Management module has been inserted in slot ***x***, Model=***model***, S/N=***s/n***.
Severity --> Significant Event
Mgmt: System boot - Cold Start (System diagnostic file available).
Severity --> Normal Operation
Mgmt: System boot - Warm start, System crash (System diagnostic file available).
Severity --> Normal Operation
Mgmt: Has been reset.
Severity --> Significant Event
Mgmt: Has been reset to factory default.
Severity --> Significant Event
Mgmt: Ethernet port link status UP.
Severity --> Normal Operation
Mgmt: Ethernet port link status DOWN.
Severity --> Significant Event
Mgmt: Console port monitored signal changed. DSR now inactive.
Severity --> Significant Event
Mgmt: Authentication SUCCESSFUL! Access method=Serial Console, Originating IP=***Unknown***.
Severity --> Normal Operation
Mgmt: Authentication SUCCESSFUL! Access method=SNMP, Originating IP= ***ip***.
Severity --> Normal Operation
Mgmt: Authentication SUCCESSFUL! Access method=Telnet, Originating IP= ***ip***.
Severity --> Normal Operation
Mgmt: Authentication SUCCESSFUL! Access method=SSH, Originating IP= ***ip***.
Severity --> Normal Operation
Mgmt: Authentication SUCCESSFUL! Access method=WebManager(HTEMPP), Originating IP= ***ip***.
Severity --> Normal Operation
Mgmt: Authentication SUCCESSFUL! Access method=WebManager(HTEMPPS), Originating IP= ***ip***.
Severity --> Normal Operation
Mgmt: Authentication FAILED! Access method=Serial Console, Originating IP=***Unknown***.
Severity --> One Time Error
Mgmt: Authentication FAILED! Access method=SNMP, Originating IP= ***ip***.
Severity --> One Time Error
Mgmt: Authentication FAILED! Access method=Telnet, Originating IP= ***ip***.
Severity --> One Time Error
Mgmt: Authentication FAILED! Access method=SSH, Originating IP= ***ip***.
Severity --> One Time Error
Mgmt: Authentication FAILED! Access method=WebManager(HTEMPP), Originating IP= ***ip***.
Severity --> One Time Error
Mgmt: Authentication FAILED! Access method=WebManager(HTEMPPS), Originating IP= ***ip***.

```
     Severity --> One Time Error
Mgmt: System date/time has been set. Current date/time is now mm dd, yyyy hh:mm:ss
tz (GMT -hhh).
     Severity --> Significant Event
Mgmt: Communication with Secondary SNTP server ip recovered.
     Severity --> Significant Event
Mgmt: Communication with Primary SNTP server ip FAILED.
     Severity --> One Time Error
Mgmt: Communication with SNMP trap host 5 IP=ip recovered.
     Severity --> Significant Event
Mgmt: Communication with SNMP trap host 2 IP=ip FAILED.
     Severity --> One Time Error
Mgmt: Communication with email server ip recovered.
     Severity --> Significant Event
Mgmt: Communication with email server ip FAILED.
     Severity --> One Time Error
Mgmt: Configuration saved to flash.
     Severity --> Normal Operation
Mgmt: System IP address has been dynamically changed from ip to ip.
     Severity --> Significant Event
Mgmt: TFTP file transfer of file fileName1 to remote host ip was successful.
     Severity --> Normal Operation
Mgmt: TFTP file transfer of file fileName2 to remote host ip failed.
     Severity --> One Time Error
Mgmt: TFTP file transfer of file fileName3 from remote host ip was successful.
     Severity --> Normal Operation
Mgmt: TFTP file transfer of file fileName4 from remote host ip failed.
     Severity --> One Time Error
Mgmt: Chassis configuration mismatch! Backup Media Converter Module
configurations reset to factory default.
     Severity --> Significant Event
```

Chassis Alerts

```
Chassis: Has been reset.
     Severity --> Significant Event
Chassis: High Temperature alarm cleared! Temperature temp C/F.
     Severity --> Significant Event
Chassis: High temperature alarm! Temperature temp C/F, alarm threshold temp C/F.
Alarm Relay Engaged."
     Severity --> System Level Fault
Chassis: Slot 5 has been powered ON. Model=model, S/N=s/n, Module name=name."
     Severity --> Significant Event
Chassis: Slot 7 has been powered OFF.
     Severity --> Significant Event
Chassis: OK.
     Severity --> Significant Event
Chassis: Failed! Reason code=33. Alarm Relay Engaged.
     Severity --> System Level Fault
Chassis: Communication with temperature sensor has been restored.
```

```
     Severity --> Significant Event
Chassis: Communication with temperature sensor failed.
     Severity --> One Time Error
```

Power Supply Alerts

```
POWER SUPPLY A: Power Supply Monitoring Unit has been inserted. Model=model,
S/N=s/n."
     Severity --> Significant Event
POWER SUPPLY A: Has been removed from chassis.
     Severity --> Significant Event
POWER SUPPLY A: Power supply OK.
     Severity --> Significant Event
POWER SUPPLY A: Power supply failed! Reason code=22. Alarm Relay Engaged.
     Severity --> System Level Fault
POWER SUPPLY B: Voltage from power supply restored.
     Severity --> Significant Event
POWER SUPPLY B: No voltage being supplied from power supply. Alarm Relay Engaged.
     Severity --> System Level Fault
POWER SUPPLY B: Fan OK.
     Severity --> Normal Operation
POWER SUPPLY B: Fan failed! Alarm Relay Engaged.
     Severity --> System Level Fault
```

Media Converter Alerts

```
Mod. Name (slot x,): Has been inserted. Model=model, S/N=s/n."
     Severity --> Significant Event
Mod. Name (slot x): Has been removed.
     Severity --> Significant Event
Mod. Name (slot x): Has been reset.
     Severity --> Significant Event
Mod. Name (slot x): Recovered communication with Management module.
     Severity --> Significant Event
Mod. Name (slot x): No longer communicating with Management module.
     Severity --> Module Level Fault
Mod. Name (slot x): OK.
     Severity --> Significant Event
Mod. Name (slot x): Failed! Reason code=44.
     Severity --> Module Level Fault
Mod. Name  (slot x): Fiber port link status UP.
     Severity --> Significant Event
Mod. Name  (slot x): Copper port link status DOWN.
     Severity --> Significant Event
Mod. Name (slot x): Configuration update failed.
     Severity --> One Time Error
Mod. Name (slot x): Configuration update successful.
     Severity --> Normal Operation
Mod. Name (slot x): Configuration mismatch resolved. Type inserted model, type
configured model.
```

```
     Severity --> Significant Event
Mod. Name (slot x): Backup media configuration mismatch. Module type inserted
model, module type configured model.
     Severity --> Persistent Error
Mod. Name (slot x): Firmware update successful.
     Severity --> Normal Operation
Mod. Name (slot x): Firmware update failed!
     Severity --> One Time Error
Mod. Name (slot x): Module has been powered down due to detection of a hardware
failure.
     Severity --> Module Level Fault
Mod. Name (slot x): The image on this Media Converter Module is invalid.
     Severity --> Module Level Fault
Mod. Name (slot x): Module not fully supported. Please download latest firmware to
     MCR-MGT module.
     Severity --> Significant Event
Mod. Name (slot x): Module firmware is being updated.
     Severity --> Significant Event
```

SFP/XFP Alerts

```
Mod. Name (slot x, port y): SFP/XFP module has been inserted.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP module has been removed.
     Severity --> Significant Event
Mod. Name (slot x, port y): Recovered communication with SFP/XFP module.
     Severity --> Significant Event
Mod. Name (slot x, port y): Unable to communicate with SFP/XFP module.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI High temperature warning recovered.
Temperature temp C/F
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High temperature warning. Temperature temp
C/F, warning threshold temp C/F."
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI High temperature alarm recovered.
Temperature temp C/F.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High temperature alarm! Temperature temp
C/F, alarm Threshold temp C/F."
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI Low temperature warning recovered.
Temperature temp C/F.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low temperature warning. Temperature temp
C/F, warning threshold temp C/F."
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI Low temperature alarm recovered.
Temperature temp C/F.
```

```
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low temperature alarm! Temperature temp
C/F, alarm Threshold temp C/F."
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI High voltage warning recovered. Voltage
value Volts.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High voltage warning. Voltage value Volts,
warning threshold value Volts."
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI High voltage alarm recovered. Voltage
value Volts.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High voltage alarm! Voltage value Volts,
alarm threshold value Volts."
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI Low voltage warning recovered. Voltage
value Volts.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low voltage warning. Voltage value Volts,
warning threshold value Volts."
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI Low voltage alarm recovered. Voltage value
Volts.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low voltage alarm! Voltage value Volts,
alarm threshold value Volts."
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI High TX bias current warning recovered. TX
Bias: value mA
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High TX bias current warning. TX Bias
value mA, warning threshold value mA."
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI High TX bias current alarm recovered. TX
Bias: value mA.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High TX bias current alarm! TX Bias value
mA, alarm threshold value mA."
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI Low TX bias current warning recovered. TX
Bias value mA.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low TX bias current warning. TX Bias value
mA, warning threshold value mA."
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI Low TX bias current alarm recovered. TX
Bias value mA.
     Severity --> Significant Event
```

```
Mod. Name (slot x, port y): SFP/XFP DMI Low TX bias current alarm! TX Bias value
mA, alarm threshold value mA."
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI High TX power warning recovered. TX power
value mW.
     Severity --> Significant Event
Mod. Name (slot x, Slot y): SFP/XFP DMI High TX power warning. TX power value mW,
warning threshold value mW."
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI High TX power alarm. TX power value mW,
alarm threshold value mW."
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI High TX power alarm recovered. TX power
value mW.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low TX power warning recovered. TX power
value mW
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low TX power warning. TX power value mW,
warning threshold value mW."
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI Low TX power alarm recovered. TX power
2000.001 mW.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low TX power alarm. TX power value mW,
alarm threshold value mW."
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI High RX power warning recovered. RX power
value mW.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High RX power warning. RX power value mW,
warning threshold value mW."
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI High RX power alarm recovered. RX power
3000.001 mW.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High RX power alarm! RX power value mW,
alarm threshold value mW."
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI Low RX power warning recovered. RX power
value mW.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low RX power warning. RX power value mW,
warning threshold value mW.
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI Low RX power alarm recovered. RX power
value mW.
     Severity --> Significant Event
```

```
Mod. Name (slot x, port y): SFP/XFP DMI Low RX power alarm! RX power value mW,
alarm threshold value mW.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP module has been shutdown due to high
     temperature.
     Severity --> Module level Fault"
Mod. Name (slot x, port y): SFP/XFP module has been recovered from shutdown due to
     high temperature.
     Severity --> Significant Event
Mod. Name (slot x, port y): Module port XFP High APD Bias voltage warning. Voltage
     value mV, warning threshold value mV.
     Severity --> Persistent Error
Mod. Name (slot x, port y): Module port XFP High APD Bias voltage warning
     recovered. Voltage value mV.
     Severity --> Persistent Error
Mod. Name (slot x, port y): Module port XFP High APD Bias voltage alarm! Voltage
     value mV, alarm threshold value mV.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High APD Bias voltage alarm recovered. Voltage
     value mV.
     Severity --> Significant Event
Mod. Name (slot x - port y): XFP Low APD Bias voltage warning. Voltage value mV,
     warning threshold value mV.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low APD Bias voltage warning recovered. Voltage
     value mV. Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low APD Bias voltage alarm! Voltage value mV,
     alarm threshold value mV.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP Low APD Bias voltage alarm recovered. Voltage
     value mV.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP High TEC current warning. Current value mA,
     warning threshold value mA. Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High TEC current warning recovered. Current value
     mA.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High TEC current alarm! Current value mA, alarm
     threshold value mA. Severity --> Module Level Fault
Mod Name (slot x, port y: XFP High TEC current alarm recovered. Current value mA.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low TEC current warning. Current value mA, warning
     threshold value mA. Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low TEC current warning recovered. Current value
     mA.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low TEC current alarm! Current value mA, alarm
     threshold value mA. Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP Low TEC current alarm recovered. Current value mA.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP High Laser temperature warning. Temperature,
     warning threshold.
     Severity --> Persistent Error
```

```
Mod. Name (slot x, port y): XFP High Laser temperature warning recovered.
     Temperature Severity --> Significant Event
Mod. Name (slot x, port y): XFP High Laser temperature alarm! Temperature, alarm
     threshold Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High Laser temperature alarm recovered.
     Temperature. Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low Laser temperature warning. Temperature,
     warning threshold.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low Laser temperature warning recovered.
     Temperature Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low Laser temperature alarm! Temperature, alarm
     threshold Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP Low Laser temperature alarm recovered. Temperature
     Severity -->Significant Event
Mod. Name (slot x, port y): XFP High Laser wavelength warning. Wavelength nm,
     warning threshold nm.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High Laser wavelength warning recovered.
     Wavelength nm. Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High Laser wavelength alarm! Wavelength nm, alarm
     threshold nm.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High Laser wavelength alarm recovered. Wavelength
     nm. Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low Laser wavelength warning. Wavelength nm,
     warning threshold nm.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low Laser wavelength warning recovered. Wavelength
     nm. Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low Laser wavelength alarm! Wavelength nm, alarm
     threshold nm.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP Low Laser wavelength alarm recovered. Wavelength
     nm. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +5V supply voltage warning. Voltage value
     Volts, warning threshold value Volts.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +5V supply voltage warning recovered. Voltage
     value Volts. Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +5V supply voltage alarm! Voltage value
     Volts, alarm threshold value Volts.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High +5V supply voltage alarm recovered. Voltage
     value Volts. Severity --. Significant Event
Mod. Name (slot x, port y): XFP Low +5V supply voltage warning. Voltage value
     Volts, warning threshold value Volts.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low +5V supply voltage warning recovered. Voltage
     value Volts. Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low +5V supply voltage alarm! Voltage value Volts,
     alarm threshold value Volts.
     Severity --> Module Level Fault
```

```
Mod. Name (slot x, port y): XFP Low +5V supply voltage alarm recovered. Voltage
     value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +3.3V supply voltage warning. Voltage value
     Volts, warning threshold value Volts.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +3.3V supply voltage warning recovered.
     Voltage value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +3.3V supply voltage alarm! Voltage value
     Volts, alarm threshold value Volts.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High +3.3V supply voltage alarm recovered. Voltage
     value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low +3.3V supply voltage warning. Voltage value
     Volts, warning threshold value Volts.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low +3.3V supply voltage warning recovered.
     Voltage value Volts. Severity Significant Event
Mod. Name (slot x, port y): XFP Low +3.3V supply voltage alarm! Voltage value
     Volts, alarm threshold value Volts.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP Low +3.3V supply voltage alarm recovered. Voltage
     value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +1.8V supply voltage warning. Voltage value
     Volts, warning threshold value Volts.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +1.8V supply voltage warning recovered.
     Voltage value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +1.8V supply voltage alarm! Voltage value
     Volts, alarm threshold value Volts.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High +1.8V supply voltage alarm recovered. Voltage
     value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low +1.8V supply voltage warning. Voltage value
     Volts, warning threshold value Volts.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low +1.8V supply voltage warning recovered.
     Voltage value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low +1.8V supply voltage alarm! Voltage value
     Volts, alarm threshold value Volts.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP Low +1.8V supply voltage alarm recovered. Voltage
     value Volts. Severity --. Significant Event
Mod. Name (slot x, port y): XFP High -5.2V supply voltage warning. Voltage value
     Volts, warning threshold value Volts.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High -5.2V supply voltage warning recovered.
     Voltage value Volts. Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High -5.2V supply voltage alarm! Voltage value
     Volts, alarm threshold value Volts.
     Severity --> Module Level Alert
Mod. Name (slot x, port y): XFP High -5.2V supply voltage alarm recovered.
     Voltages value Volts. Severity --. Significant Event
Mod. Name (slot x, port y): XFP Low -5.2V supply voltage warning. Voltage value
     Volts, warning threshold value Volts.
```

```
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low -5.2V supply voltage warning recovered.
     Voltage value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low -5.2V supply voltage alarm! Voltage value
     Volts, alarm threshold value Volts.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP Low -5.2V supply voltage alarm recovered. Voltage
     value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +5V supply current warning. Current value mA,
     warning threshold value mA.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +5V supply current warning recovered. Current
     value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +5V supply current alarm! Current value mA,
     alarm threshold value mA.
     Severity --> Module Event Error
Mod. Name (slot x, port y): XFP High +5V supply current alarm recovered. Current
     value mA. Severity --> Significant Error
Mod. Name (slot x, port y): XFP High +5V supply current warning. Current value mA,
     warning threshold value mA.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +5V supply current warning recovered. Current
     value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +5V supply current alarm! Current value mA,
     alarm threshold value mA.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High +5V supply current alarm recovered. Current
     value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +3.3V supply current warning. Current value
     mA, warning threshold value mA.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +3.3V supply current warning recovered.
     Current value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +3.3V supply current alarm! Current value mA,
     alarm threshold value mA.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High +3.3V supply current alarm recovered. Current
     value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +3.3V supply current warning. Current value
     mA, warning threshold value mA.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +3.3V supply current warning recovered.
     Current value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +3.3V supply current alarm! Current value mA,
     alarm threshold value mA.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High +3.3V supply current alarm recovered.
     Currents value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +1.8V supply current warning. Current value
     mA, warning threshold value mA.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +1.8V supply current warning recovered.
     Current value mA. Severity --> Significant Events
```

```
Mod. Name (slot x, port y): XFP High +1.8V supply current alarm! Current value mA,
     alarm threshold value mA.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High +1.8V supply current alarm recovered. Current
     value mA. Severity -->Significant Event
Mod. Name (slot x, port y): XFP High +1.8V supply current warning. Current value
     mA, warning threshold value mA.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +1.8V supply current warning recovered.
     Current value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +1.8V supply current alarm! Current value mA,
     alarm threshold value mA.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High +1.8V supply current alarm recovered. Current
     Value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High -5.2V supply current warning. Current value
     mA, warning threshold value mA.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High -5.2V supply current warning recovered.
     Current value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High -5.2V supply current alarm! Current value mA,
     alarm threshold value mA.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High -5.2V supply current alarm recovered. Current
     value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High -5.2V supply current warning. Current value
     mA, warning threshold value mA.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High -5.2V supply current warning recovered.
     Current value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High -5.2V supply current alarm! Current value mA,
     alarm threshold value mA.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High -5.2V supply current alarm recovered. Current
     value mA. Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +5V supply voltage warning
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +5V supply voltage warning recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +5V supply voltage alarm!
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High +5V supply voltage alarm recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low +5V supply voltage warning.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low +5V supply voltage warning recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low +5V supply voltage alarm!
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP Low +5V supply voltage alarm recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +3.3V supply voltage warning
     Severity -->Persistent Error
Mod. Name (slot x, port y): XFP High +3.3V supply voltage warning recovered.
```

```
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +3.3V supply voltage alarm!
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High +3.3V supply voltage alarm recovered.
     Severity --> Significant Error
Mod. Name (slot x, port y): XFP Low +3.3V supply voltage warning.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low +3.3V supply voltage warning recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low +3.3V supply voltage alarm! Severity -->
     Module Level Fault
Mod. Name (slot x, port y): XFP Low +3.3V supply voltage alarm recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +1.8V supply voltage warning
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP High +1.8V supply voltage warning recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP High +1.8V supply voltage alarm! Severity -->
     Module Level Fault
Mod. Name (slot x, port y): XFP High +1.8V supply voltage alarm recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low +1.8V supply voltage warning. Severity -->
     Persistent Error
Mod. Name (slot x, port y): XFP Low +1.8V supply voltage warning recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low +1.8V supply voltage alarm! Severity -->
     Module Level Fault
Mod. Name (slot x, port y): XFP Low +1.8V supply voltage alarm recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP High -5.2V supply voltage warning Severity --
     >Persistent Error
Mod. Name (slot x, port y): XFP High -5.2V supply voltage warning recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP High -5.2V supply voltage alarm!
     Severity --> Module Level Fault
Mod. Name (slot x, port y): XFP High -5.2V supply voltage alarm recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low -5.2V supply voltage warning.
     Severity --> Persistent Error
Mod. Name (slot x, port y): XFP Low -5.2V supply voltage warning recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): XFP Low -5.2V supply voltage alarm! Severity -->
     Module Level Fault
Mod. Name (slot x, port y): XFP Low -5.2V supply voltage alarm recovered.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP module has been inserted.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP module has been removed.
     Severity --> Significant Event
Mod. Name (slot x, port y): Unable to communicate with SFP/XFP module.
     Severity --> Significant Event
Mod. Name (slot x, port y): Recovered communication with SFP/XFP module.
     Severity --> Significant Event
```

```
Mod. Name (slot x, port y): SFP/XFP DMI High temperature warning. Temperature,
     warning threshold.
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI High temperature warning recovered.
     Temperature. Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High temperature alarm! Temperature, alarm
     Threshold.
     Severity --> Module Level Faults
Mod. Name (slot x, port y): SFP/XFP DMI High temperature alarm recovered.
     Temperature. Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low temperature warning. Temperature,
     warning threshold.
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI Low temperature warning recovered.
     Temperature. Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low temperature alarm! Temperature, alarm
     Threshold.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI Low temperature alarm recovered.
     Temperature Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High voltage warning. Voltage value Volts,
     warning threshold value Volts.
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI High voltage warning recovered. Voltage
     value Volts.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High voltage alarm! Voltage value Volts,
     alarm threshold value Volts.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI High voltage alarm recovered. Voltage
     value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low voltage warning. Voltage value Volts,
     warning threshold value Volts.
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI Low voltage warning recovered. Voltage
     value Volts. Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low voltage alarm! Voltage value Volts,
     alarm threshold value Volts.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI Low voltage alarm recovered. Voltage value
     Volts.
     Severity -->Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High TX bias current warning. TX Bias
     value mA, warning threshold value mA."
Mod. Name (slot x, port y): SFP/XFP DMI High TX bias current warning recovered. TX
     Bias: value mA Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High TX bias current alarm! TX Bias value
     mA, alarm threshold value mA.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI High TX bias current alarm recovered. TX
     Bias: value mA. Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low TX bias current warning. TX Bias value
     mA, warning threshold value mA.
     Severity --> Persistent Error
```

```
Mod. Name (slot x, port y): SFP/XFP DMI Low TX bias current warning recovered. TX
     Bias value mA. Severity --> Significant Events
Mod. Name (slot x, port y): SFP/XFP DMI Low TX bias current alarm! TX Bias value
     mA, alarm threshold value mA.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI Low TX bias current alarm recovered. TX
     Bias value mA. Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High TX power warning. TX power, warning
     threshold Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI High TX power warning recovered. TX power.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High TX power alarm. TX power, alarm
     threshold. Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI High TX power alarm recovered. TX power.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low TX power warning. TX power, warning
     threshold Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI Low TX power warning recovered. TX power
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP DMI Low TX power alarm. TX power, alarm threshold.
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI Low TX power alarm recovered. TX power.
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High RX power warning. RX power, warning
     threshold
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI High RX power warning recovered. RX power
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI High RX power alarm! RX power, alarm
     threshold Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI High RX power alarm recovered. RX power
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low RX power warning. RX power, warning
     threshold
     Severity --> Persistent Error
Mod. Name (slot x, port y): SFP/XFP DMI Low RX power warning recovered. RX power
     Severity --> Significant Event
Mod. Name (slot x, port y): SFP/XFP DMI Low RX power alarm! RX power, alarm
     threshold
     Severity --> Module Level Fault
Mod. Name (slot x, port y): SFP/XFP DMI Low RX power alarm recovered. RX power
     Severity --> Significant Event
Mod. Name (slot x,): Speed Mismatch between SFP and the other SFP/XFP module
     Severity --> Persistent Error
Mod. Name (slot x,): SFP speed mismatch has recovered.
     Severity --> Significant Event
Mod. Name (slot x,): An XFP module's power requirements has exceeded card capacity
     Severity --> Module Level Fault
Mod. Name (slot x,): XFP excessive power alarm has recovered
     Severity --> Significant Event
Mod. Name (slot x, port y): Low upstream bandwidth alarm! Bandwidth (Upstream
     Bandwidth kbps) dropped below threshold (UpstreamBandwidthThreshold kbps).
     Severity --> Persistent Error
Mod. Name (slot x, port y): Recovered from low upstream bandwidth condition.
```

```
     Severity --> Significant Error
Mod. Name (slot x, port y): Low downstream bandwidth alarm! Bandwidth
     (DownstreamBandwidth kbps) dropped below threshold
     (DownstreamBandwidthThreshold kbps).
     Severity --> Persistent Error
Mod. Name (slot x, port y): Recovered from low downstream bandwidth condition.
     Severity --> Significant Error
```

VDSL Line Alerts

```
Mod. Name (slot x,): Peer was reset
Severity --> Significant Event
```

SSL/TLS Ciphers

Valid SSL/TLS Ciphers

Full Name	SSL Ver.	Key-Exchange	Authentication	Encryption	Key-Size	HMAC
ADH-AES256-SHA	SSLv3	Kx=DH	Au=None	Enc=AES	256	Mac=SHA1
DHE-RSA-AES256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES	256	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES	256	Mac=SHA1
AES256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES	256	Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3	Kx=DH	Au=RSA	Enc=3DES	168	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3	Kx=DH	Au=DSS	Enc=3DES	168	Mac=SHA1
DES-CBC3-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=3DES	168	Mac=SHA1
DES-CBC3-MD5	SSLv2	Kx=RSA	Au=RSA	Enc=3DES	168	Mac=MD5
ADH-AES128-SHA	SSLv3	Kx=DH	Au=None	Enc=AES	128	Mac=SHA1
DHE-RSA-AES128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES	128	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES	128	Mac=SHA1
AES128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES	128	Mac=SHA1
RC2-CBC-MD5	SSLv2	Kx=RSA	Au=RSA	Enc=RC2	128	Mac=MD5
DHE-DSS-RC4-SHA	SSLv3	Kx=DH	Au=DSS	Enc=RC4	128	Mac=SHA1
RC4-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=RC4	128	Mac=SHA1
RC4-MD5	SSLv3	Kx=RSA	Au=RSA	Enc=RC4	128	Mac=MD5
RC4-MD5	SSLv2	Kx=RSA	Au=RSA	Enc=RC4	128	Mac=MD5
RC4-64-MD5	SSLv2	Kx=RSA	Au=RSA	Enc=RC4	64	Mac=MD5
EDH-RSA-DES-CBC-SHA	SSLv3	Kx=DH	Au=RSA	Enc=DES	56	Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3	Kx=DH	Au=DSS	Enc=DES	56	Mac=SHA1
DES-CBC-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=DES	56	Mac=SHA1
DES-CBC-MD5	SSLv2	Kx=RSA	Au=RSA	Enc=DES	56	Mac=MD5
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	Kx=DH(512)	Au=RSA	Enc=DES	40	Mac=SHA1
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	Kx=DH(512)	Au=DSS	Enc=DES	40	Mac=SHA1
EXP-DES-CBC-SHA	SSLv3	Kx=RSA(512)	Au=RSA	Enc=DES	40	Mac=SHA1

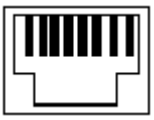
Full Name	SSL Ver.	Key-Exchange	Authentication	Encryption	Key-Size	HMAC
EXP-RC2-CBC-MD5	SSLv3	Kx=RSA(512)	Au=RSA	Enc=RC2	40	Mac=MD5
ADH-DES-CBC3-SHA	SSLv3	Kx=DH	Au=None	Enc=3DES	168	Mac=SHA1
ADH-DES-CBC-SHA	SSLv3	Kx=DH	Au=None	Enc=DES	56	Mac=SHA1
EXP-ADH-DES-CBC-SHA	SSLv3	Kx=DH(512)	Au=None	Enc=DES	40	Mac=SHA1
ADH-RC4-MD5	SSLv3	Kx=DH	Au=None	Enc=RC4	128	Mac=MD5
EXP-ADH-RC4-MD5	SSLv3	Kx=DH(512)	Au=None	Enc=RC4	40	Mac=MD5
EXP-RC2-CBC-MD5	SSLv2	Kx=RSA(512)	Au=RSA	Enc=RC2	40	Mac=MD5
EXP-RC4-MD5	SSLv3	Kx=RSA(512)	Au=RSA	Enc=RC4	40	Mac=MD5
EXP-RC4-MD5	SSLv2	Kx=RSA(512)	Au=RSA	Enc=RC4	40	Mac=MD5

C Pinouts and Cabling Diagrams

Console Port Pinout

The RJ-45 console port on the MCR-MGT Management Module has a standard “Cisco” pinout as defined below.

Pin order:

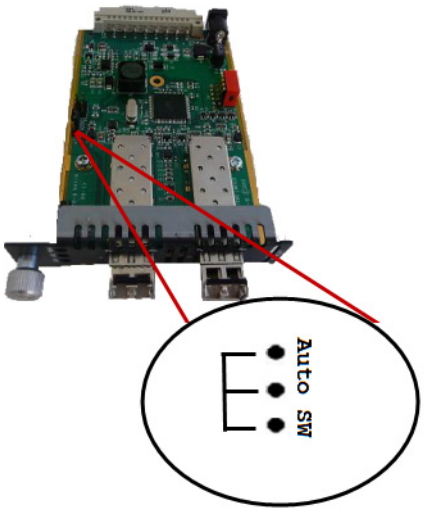
Pin 1  Pin 8

Pinout:

Pin #	Pin Description
1	RTS (out)
2	DTR (out)
3	TxD (out)
4	GND
5	GND
6	RxD (in)
7	DSR (in)
8	CTS (in)

Auto-Config Switch

The default jumper setting is Auto mode. Jumper the top and middle Pin to select Auto mode. Jumper the middle and bottom Pin to select SW mode.



Troubleshooting

General Troubleshooting

- Ensure that any Media Converter Modules and MCR-MGT Management Modules are securely seated in the Chassis of the MCR1900 or the SMI Media Converter.
- If the media converter module is a managed module and it is detected as an unmanaged module, then carefully pull the module out of the chassis and re-insert the module securing it to the front face plate of the chassis.
- Ensure all cabling is of the correct type and is in good working order.
- Ensure the remote device's fiber connection type is compatible with the Media Converter Module. If using a simplex fiber connection, ensure that you have both an Upstream (U) and Downstream (D) Media Converter Module.
- For duplex fiber connections, ensure the RX and TX has been reversed between the two Media Converter Modules.

No Connectivity

If unable to get full connectivity with the Media converter Modules and all their DIP switches are in the UP position, then this procedure is recommended for troubleshooting.

Method 1

1. Set the Link mode to Standard to ON on both Media Converter Modules. Leave all other switches in the UP position.
2. Connect the near end device to the copper connection. The LKC LED indicates good copper connection. If the LKC LED is not lit, then check the copper cable and the attached device.
3. Repeat for the far end Media Converter Module.
4. Connect the fiber cable to both Media Converter Modules. The LKF LED indicates good fiber connection. If no LKF LED then check the fiber cabling. Ensure the transmitter and receiver pairs are crossed.
5. Return modules to their desired configuration.

Method 2

The fiber connection can also be verified by configuring the remote Media Converter Module for loopback mode. The LKF LEDs on both Media Converter Modules should be lit. Data should pass through the local converter, over the fiber connection to the remote Media Converter. At the remote Media Converter Module, the data will be looped back and passed through the fiber, back to the local Media Converter Module and passed to the copper link.

Communication Issues

Webmanager screen appears garbled.

- Press and hold Ctrl, then press F5 or clear the cache memory on your browser.

General communication checks and practices are as follows:

- Are your cables connected and correctly configured? If you are using EIA-232, see to verify that your cables are correctly configured.
- Can you ping your host? If you can ping but packet loss is reported, ping another host/device on the same network. This will tell you whether the problem is specific to the host/device or general to the network.
- After entering or changing IP information for your MCR-MGT Management Module, *reboot* the MCR-MGT Management Module does not apply when using BOOTP or DHCP). Once the Management Module has rebooted, other network devices should be able to communicate with it (ping, telnet, etc.). Also, protocols such as ARP and proxy-ARP will work properly.
- Use the **`show routes`** command (command line only). Is there a route to the host?
- If the MCR Web Manager cannot communicate with the Management Module, verify that the service is enabled under Administration, Access**, HTTP** and/or **HTTPS** are enabled for the MCR Web Manager. If you are using only HTTPS, the connection URL must start with **`https://`**.

Host Problems

Cannot access a host by name:

- If using DNS or if DNS is required, ensure a nameserver is configured on your MCR-MGT Management Module and is accessible (ping it).
- If not using DNS, verify that the host is configured in the **Host Table**. Check access to the host by pinging it using the host's IP address.

Cannot access a host on a local network, verify:

- The network address is correct.
- The subnet mask is set correctly and reflects the network configuration.
- The broadcast address is set correctly and reflects the network configuration.

Cannot access a host on a remote network:

- Use the **`show route`** command to verify that there is a route to the remote host. If no gateway is specified, verify that a default gateway is specified. Ping the default gateway to check if it is working.
- Consider the situation beyond the gateway; for example, are intermediate gateways and the remote host available? Also, check the messages returned by the **`ping`** command; for example, that a particular host or gateway is unreachable.

Access to host lost after a few minutes.

- If the route to this host goes through routers, make sure those routers are all sending RIP packets across the networks.

RADIUS Authentication Problems

User is waiting up to 60 seconds before login is accepted or denied and Authentication is set to RADIUS. User has entered User Name and Password, and has pressed Enter.

- Check RADIUS configuration of primary and secondary authentication/accounting hosts specified, if you have retry and timeout values greater than the default, the Management Module be spending time trying each of these hosts and keeping the user waiting.

- Adjust RADIUS configuration: specify just one host, reduce **Timeout** and **Retry** values to the default or less than default.

You cannot progress beyond the login and password prompts when authentication is set to RADIUS:

- On the RADIUS host, check the secret (password), you should see it displayed in clear text in the RADIUS clients file. If you are unsure whether it is the same secret which you entered in the Management Module, go to the Management Module and re-enter a new secret.
- On the RADIUS host, verify that there is only one entry for a particular user; do not have multiple entries of the same user name (even if the passwords are different).

Unknown IP Address

You don't know the IP address of the Management Module so you cannot obtain a successful login.

- Review Chapter 2, "Setting IP Addresses".

SSL/TLS

Could not obtain peer's certificate.

- You have selected a cipher key exchange of ADH (anonymous Diffie-Hellman) and enabled Peer verification. ADH does not use certificates so they will not be sent in an SSL/TLS handshake. Disable Peer Verification or change to a cipher suite that uses certificates.
- You have selected Peer Verification on the configured SSL/TLS server and have not configured a certificate for the client. Either disable peer verification on the SSL/TLS server or configure a certificate for the SSL/TLS client.

Certificate did not match configuration

- The message is displayed when **Validate Peer Certificate** has been enabled, but the configured **Validation Criteria** does not match the corresponding data in the certificate received from the peer. The data configured must match exactly to the data in the certificate. The data is also case sensitive.

tlsv1 alert handshake failure or **sslv3 alert handshake failure**

- The remote site has an SSL/TLS error and is sending this message with an alert message. Look at the error messages on the remote end and fix the problem indicated.

IPv6 Issues

You are not seeing the IPv6 address value when you attempt to connect to the MCR-MGT Management Module.

Windows Vista and Server 2008 operating systems have IPv6 support already enabled, however, you will have to install IPv6 support for Windows XP.

To install IPv6 support in Windows XP, do the following:

1. In Control Panel, double-click the **Network Connections** icon.
2. Double-click the **Local Area Connection** entry.
3. In the Local Area Connection Status window, click the **Properties** button on the **General tab**.
4. In the Local Area Connections window, click the **Install** button on the **General** tab.
5. In the Select Network Component Type window, select **Protocol** and click the **Add** button.
6. In the Select Network Protocol window, select **Microsoft TCP/IP version 6** and click the **OK** button.

Contacting Technical Support

Making a Technical Support Query

Contact information for the Perle Technical Assistance Center (PTAC) can be found at the link below. A Technical Support Query may be made via this web page.

http://www.perle.com/support_services/support_request.shtml

Warranty / Registration

Perle's standard Lifetime Warranty provides customers with return to factory repairs for Perle products that fail under the conditions of the warranty coverage. Details can be found at

http://www.perle.com/support_services/warranty.shtml

Feedback on this Manual

If you have any comments or suggestions for improving this manual please email Perle using the following address:

Email: ptac@perle.com

Please include the **title**, **part number** and **date** of the manual (you can find these on the title page at the front of this manual).

Symmetric Key File

Symmetric Key File

This section defines the layout of the SNTP Symmetric Key file that must be downloaded to the management card in order to use the SNTP server authentication feature. Each line of the SNTP symmetric key file consists of three fields: a key ID in the range 1 to 65,534, inclusive, a key type and a message digest key consisting of a printable ASCII string equal to or less than 20 characters or a 40 character hex digit string.

key ID	key type	message digest key	
1	MD5	CeR{+’9LRTY:a0=P?GOA	ascii string
2	MD5	POE)+’9KRMY:P0-PZOQ	ascii string
3	MD5	E)+’9KRRTS {+’9LRTpp	ascii string
4	MD5	ECeE)+’9KRDSRuurQPiw	ascii string
5	SHA1	0e9e44502940294fa788aafaac34ccb126347d34	hex digit string
6	SHA1	f4e9e4454e9e4450294faccb126309ff4ccb1200	hex digit string
7	SHA1	e9e44502949e4450294ccb12634e9e447d3489	hex digit string
8	SHA1	40294fa7894faccb126502944fac4e9e788aafaa	hex digit string

Note: **Note:1-10 key ID entries are allowed in this SNTP key file. Both MD5 and SHA1 are supported. Key ID 0 is excluded.**