CONNECTION TECHNOLOGY SYSTEMS

MCT-RACK-12-MGM

12 SLOTS COMPACT MEDIA CONVERTER CENTER

Network Management

User's Manual

Version 0.91

.

Revision History

Version	F/W	Date	Description
0.90	0.99.02	2016/03/17	First release
0.91	1.02.0l	2020/03/11	Add DI/DO Feature Add CLI terminal length Add remark on Digital Output Configuration Add Remote Module section Add Appendix C, D and E Add Appendix F for MCT-5002FSMSFP+ Add the new description of TACACS+ authentication Add CTS branches' contact information

Trademarks

CTS is a registered trademark of Connection Technology Systems Inc..
Contents are subject to revision without prior notice.
All other trademarks remain the property of their owners.

Copyright Statement

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limitations are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult your local distributors or an experienced radio/TV technician for help.
- Shielded interface cables must be used in order to comply with emission limits.

Changes or modifications to the equipment, which are not approved by the party responsible for compliance, could affect the user's authority to operate the equipment.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:
All trade names and trademarks are the properties of their respective companies.

CTS Contact Information

■ Headquarters/Manufacturer:

Connection Technology Systems Inc.

18F-6, No.79, Sec.1, Xintai 5th Rd.,

Xizhi Dist., New Taipei City 221, Taiwan(R.O.C.)

Tel: +886-2-2698-9661

Fax: +886-2-2698-3960

Sales Direct Line:+886-2-2698-9201

www.ctsystem.com

■ Global Offices:

Connection Technology USA

40538 La Purissima Way,

Fremont, CA 94539, USA

Tel: +1-510-509-0304

Sales Direct Line: +1-510-509-0305

E-mail:cts_us@ctsystem.com

Connection Technology Systems Japan

Higobashi Bldg. No.3 R201, 1-23-13,

Edobori, Nishi-ku, Osaka 550-0002, Japan

Tel: +81-6-6450-8890

E-mail: cts_japan@ctsystem.com

Connection Technology Systems NE AB

August Barks Gata 21,

421 32 Västra Frölunda, Sweden

Tel: +46-31-221980

E-mail: info@ctsystem.se

Connection Technology Systems Central Europe (COMPONET Handels GmbH)

Hirschstettner Straße 19-21/Stiege I

A-1220 Vienna, Austria

Tel: +43-1-235 05 66-0

E-mail: cts_ce@ctsystem.com

Table of Content

1. INTRODUCTION

Thank you for purchasing the CHASSIS, the 12-slot converter management rack. The CHASSIS, with advanced management to increase network performance, is designed to be the carrier's conversion chassis aiming at the application that require monitoring point-to-point connection for the deployment of FTTX. In order to ease administrators' daily maintenance and operation load, a network management converter is equipped within the CHASSIS. The real-time operational status of the CHASSIS and any of the installed slide-in converter can be monitored locally and remotely through this network management converter.

1.1 Management Options

You can manage the CHASSIS and any of the installed slide-in converter modules in-band or out-of-band. "In-band" management refers to managing the CHASSIS through the 10/100Base-T RJ-45 LAN port. "Out-of-band" management means going through the RS-232 (RJ-45) port.

Following is a list of management options available in this CHASSIS:

- Local Console Management
- Telnet Management
- SSH Management
- SNMP Management
- Web Management

Local Console Management

Local Console Management is done through the RS-232 (RJ-45) console port. This RS-232 (RJ-45) port is located at the front panel of the CHASSIS. Managing the CHASSIS in this mode requires a direct connection between a PC and the CHASSIS.

Telnet Management

Telnet is done through the 10/100Base-T network. A RJ-45 connector is located at the back panel of the CHASSIS. Once the CHASSIS is on the network, users can use Telnet to login and monitor its status remotely.

SSH Management

SSH Management supports encrypted data transfer to prevent the data from being "stolen" for remote management. You can use PuTTY, a free and open source terminal emulator application which can act as a client for the SSH, to gain access to the CHASSIS.

SNMP Management

SNMP is done over the network. The CHASSIS private Management Information Base (MIB) is provided for SNMP-based network management system.

You can use standard SNMP-based network management system, such as HP OpenView, to manage the CHASSIS and any of the installed slide-in converter modules remotely through the 10/100Base-T network correction. When you use a SNMP-based network management system, the CHASSIS becomes one of the managed devices (network elements) in that system. The CHASSIS network management module contains a SNMP agent that will respond to the requests from the SNMP-based network management system. These requests, which you can control, include and may vary from getting system information to setting the device attribute's values.

Web Management

Web is done over the network. Once the CHASSIS is on the network, you can log in and monitor the status remotely through a web browser.

1.2 Management Preparation

After you have decided how you would like to manage your CHASSIS, you need to do the cable connection, determine the CHASSIS IP address and, in some cases, install the MIB shipped on disc or diskette with the CHASSIS.

Connecting the CHASSIS

It is very important that the proper cables with correct pin arrangement are being used when connecting CHASSIS to the switches, hubs, workstations and other devices.

10/100Base-T RJ-45 Auto-MDI/MDIX Port

The 10/100Base-T RJ-45 Auto-MDI/MDI port is located on the front panel of the CHASSIS. The 10/100Base-T port is used for remote, in-band network management. It uses Category 3, 4, or 5 straight-through UTP or STP cable with the maximum distance up to 328 feet (i.e. 100 meters).

RS-232 (RJ-45) Port

The RS-232 (RJ-45) port is located at the front of the CHASSIS. The RS-232 (RJ-45) port is used for local, out-of-band management. By connecting the CHASSIS and a PC via RS-232 (RJ-45) port, it allows you to configure the CHASSIS and check its status even when the network is down.

Since the RS-232 (RJ-45) port of the CHASSIS is a DTE, a null modem is required to connect the CHASSIS and PC.

IP Addresses

IP addresses have the format of n.n.n.n, where n is a decimal number between 0 and 255. For example, an IP address could be: 168.168.8.100

IP addresses are made up in two parts:

- The first part (168.168 in the example) refers as the network address identifying the network on which the device resides. Network addresses are assigned by three allocation organizations. Depending on your location, each allocation organization assigns a globally unique network number to each network that wishes to connect to the Internet.

- The second part (8.100 in the example) identifies the device within the network. Assigning unique device numbers is your responsibility. If you are unsure of the IP addresses being allocated to you, consult the allocation organization from which your IP addresses were obtained.

Remember that no two devices on a network can have the same address. If you connect to the outside world, you must change all the arbitrary IP addresses to comply with those you have been allocated by the network allocation organization. Otherwise, your outward communications might not work.

A subnet mask is a filtering system for IP addresses. It allows you to further subdivide your network. You must use the proper subnet mask for proper operation of a network with subnets defined.

MIB for Network Management Systems

The CHASSIS private MIB (Management Information Base) is provided for managing the CHASSIS through a SNMP-based network management system. You must install the MIB before using that SNMP-based network management system.

The MIB file is on a disc or diskette shipped with the CHASSIS. It is a file with file extension ".mib", which a SNMP-based compiler can read and compile.

2. Command Line Interface (CLI)

This chapter describes how to use your CHASSIS Console Program, specifically in:

- Local Console Management (out-of-band)
- Telnet Management (in-band)
- Configuring the system
- Resetting the system

The interface and options are mostly the same in both Local Console and Telnet Management. The only difference is the type of connection and the port that are used to manage the CHASSIS.

2.1 Local Console Management

Local Console Management is always done through the RS-232 (RJ-45) port and requires a direct connection between the CHASSIS and a PC. This type of management is very useful especially when the network is down and the CHASSIS cannot be reached by any other means.

You also need to use the Local Console Management to set up the CHASSIS network configuration for the first time. You can set up the IP address and change the default configuration to the desired setting to enable Telnet or SNMP.

Follow these steps to begin a management session using Local Console Management:

1. Attach the serial cable to the console RJ-45 port located at the front of the CHASSIS with a null modem.

2. Attach the other end to the serial port of a PC or workstation.

3. Run a terminal emulation program using the following settings:

    - **Emulation** VT-100/ANSI compatible
    - **BPS** 9600
    - **Data bits** 8
    - **Parity** None
    - **Stop bits** 1
    - **Flow Control** None
    - **Enable** Terminal keys

4. Press Enter to reach the Main menu.

2.2 Remote Console Management - Telnet

You can use Command Line Interface to manage the Chassis via Telnet session. For first-time users, you must first assign a unique IP address to the CHASSIS before you can manage it remotely. Use any one of the RJ-45 ports on the front panel as the temporary management console port to login to the device with the default username & password and then assign the IP address using IP command in Global Configuration mode.

Follow steps described below to access the CHASSIS through Telnet session:

Step 1. Use any one of the RJ-45 ports on the front panel as a temporary management console port to login to the CHASSIS.

Step 2. Run Telnet client and connect to *192.168.0.1*. For first-time users, make sure the IP address of your PC or workstation is assigned to an IP address between 192.168.0.2 and 192.168.0.254 with subnet mask 255.255.255.0.

Step 3. When asked for a username, enter "***admin***". When asked for a password, *leave the password field blank* and press Enter (by default, no password is required.)

Step 4. If you enter CLI successfully, the prompt display *MCT-RACK*> (the model name of your device together with a greater than sign) will appear on the screen.

Step 5. Once you enter CLI successfully, you can set up the CHASSIS' IP address, subnet mask and the default gateway using "IP" command in Global Configuration mode. The telnet session will be terminated immediately once the IP address of the CHASSIS has been changed.

Step 6. Use new IP address to login to the CHASSIS via Telnet session again.

Limitation: Only four active Telnet sessions can access the CHASSIS at a time.

2.3 Navigating CLI

After you successfully access to the CHASSIS, you will be asked for a login username. Enter your authorized username and password, and then you will be directed to the User Mode. In CLI management, the User Mode only provides users with basic functions to operate the CHASSIS. If you would like to configure advanced features of the CHASSIS, you must enter the Configuration Mode. The following table provides an overview of modes available in this CHASSIS.

Command Mode	Access Method	Prompt Displayed	Exit Method
User Mode	Login username & password	MCT-RACK>	logout
Privileged Mode	From user mode, enter the *enable* command	MCT-RACK#	disable, exit, logout
Configuration Mode	From the enable mode, enter the *config* or *configure* command	MCT-RACK(config)#	exit

NOTE: *By default, the model name will be used for the prompt display. For convenience, the prompt display "MCT-RACK" will be used throughout this user's manual.*

2.3.1 General Commands

This section introduces you some general commands that you can use in all modes, including "help", "exit", "history" and "logout".

Entering the command…	To do this…	Available Modes
help	Obtain a list of available commands in the current mode.	User Mode Privileged Mode Configuration Mode
exit	Return to the previous mode or login screen.	User Mode Privileged Mode Configuration Mode
history	List all commands that have been used.	User Mode Privileged Mode Configuration Mode
logout	Logout from the CLI or terminate Telnet session.	User Mode Privileged Mode

2.3.2 Quick Keys

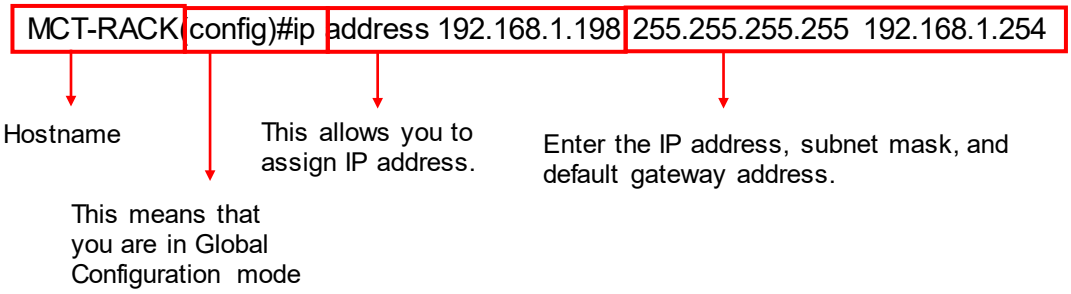
In CLI, there are several quick keys that you can use to perform several functions. The following table summarizes the most frequently used quick keys in CLI.

Keys	Purpose
tab	Enter an unfinished command and press “Tab” key to complete the command.
?	Press “?” key in each mode to get available commands.
Unfinished command followed by ?	Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help. Examples: MCT-RACK#h? help Show available commands history Show history commands MCT-RACK#he? <cr> MCT-RACK#help
Up arrow	Use Up arrow key to scroll through the previous entered commands, beginning with the most recent key-in commands.
Down arrow	Use Down arrow key to scroll through the previous entered commands, beginning with the commands that are entered first.

2.3.3 Command Format

While in CLI, you will see several symbols very often. As mentioned above, you might already know what “>”, “#” and (config)# represent. However, to perform what you intend the device to do, you have to enter a string of complete command correctly. For example, if you want to assign IP address for the CHASSIS, you need to enter the following command with the required parameter and IP, subnet mask and default gateway:

IP command syntax: MCT-RACK(config)#ip address [A.B.C.D] [255.X.X.X] [A.B.C.D]



The following table lists common symbols and syntax that you will see very frequently in this User's Manual for your reference:

Symbols	Brief Description
>	Currently, the device is in User Mode.
#	Currently, the device is in Privileged Mode.
(config)#	Currently, the device is in Global Configuration Mode.
Syntax	**Brief Description**
[ ]	Brackets mean that this field is required information.
[A.B.C.D]	Brackets represent that this is a required field. Enter an IP address or gateway address.
[255.X.X.X]	Brackets represent that this is a required field. Enter the subnet mask.
[port-based | 802.1p | dscp | vid]	There are four options that you can choose. Specify one of them.
[1-8191]	Specify a value between 1 and 8191.
[0-7] 802.1p_list [0-63] dscp_list	Specify one or more values or a range of values. For example: specifying one value MCT-RACK(config)#qos 802.1p-map 1 0 MCT-RACK(config)#qos dscp-map 10 3 For example: specifying three values (separated by commas) MCT-RACK(config)#qos 802.1p-map 1,3 0 MCT-RACK(config)#qos dscp-map 10,13,15 3 For example: specifying a range of values (separating by a hyphen) MCT-RACK(config)#qos 802.1p-map 1-3 0 MCT-RACK(config)#qos dscp-map 10-15 3

2.3.4 Login Username & Password

Default Login

After you enter Telnet session, a login prompt will appear to request a valid and authorized username and password combination. For first-time users, enter the default login username "**admin**" and "**press Enter key**" in password field (no password is required for default

setting). When system prompt shows “MCT-RACK>”, it means that the user has successfully entered the User Mode.

For security reasons, it is strongly recommended that you add a new login username and password using User command in Configuration Mode. When you create your own login username and password, you can delete the default username (admin) to prevent unauthorized accesses.

Forgot Your Login Username & Password?

If you forgot your login username and password, you can use the “reset button” to set all configurations back to factory defaults. Once you have performed system reset to defaults, you can login with default username and password. Please note that if you use this method to gain access to the CHASSIS, all configurations saved in Flash will be lost. It is strongly recommended that a copy of configurations is backed up in your local hard-drive or file server from time to time so that previously-configured settings can be restored to the CHASSIS for use after you gain access again to the device.

2.4 User Mode

In User mode, only a limited set of commands are provided. Please note that in Use Mode, you have no authority to configure advanced settings. You need to enter Privileged mode and Configuration mode to set up advanced functions of a CHASSIS feature. For a list of commands available in User Mode, enter the question mark (?) or “help” command after the system prompt displays “MCT-RACK>”.

Command	Description
exit	Quit the User mode or close the terminal connection.
help	Display a list of available commands in User mode.
history	Display the command history.
logout	Logout from the CHASSIS.
ping	Used to test the reachability of a host on an Internet Protocol (IP) network
enable	Enter the Privileged mode.

2.5 Privileged Mode

The only place where you can enter the Privileged (Enable) Mode is in User Mode. When you successfully enter Enable mode, the prompt will be changed to MCT-RACK# (the model name of your device together with a pound sign). Enter the question mark (?) or help command to view a list of commands available for use.

Command	Description
copy-cfg	Restore or backup configuration file via FTP or TFTP server.
disable	Exit Enable Mode and return to User Mode
exit	Exit Enable Mode and return to User Mode.
firmware	Upgrade Firmware via FTP or TFTP server.
help	Display a list of available commands in Enable Mode.
history	Show commands that have been used.
logout	Logout from the Chassis.
ping	Used to test the reachability of a host on an Internet Protocol (IP) network
reload	Restart the Chassis.
write	Save your configurations to Flash.
configure	Enter Global Configuration mode
show	Show a list of commands or show the current setting of each listed command.

2.5.1 Copy-cfg Command

Use “copy-cfg” command to backup a configuration file via FTP or TFTP server or restore the Chassis back to the defaults or to the defaults without changing IP configurations.

1. Restore a configuration file via FTP or TFTP server.

Command	Parameter	Description
MCT-RACK# copy-cfg from ftp [A.B.C.D] [file name] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file_name]	Enter the configuration file name that you want to restore.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
MCT-RACK# copy-cfg from tftp [A.B.C.D] [file_name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file_name]	Enter the configuration file name that you want to restore.
Example		
MCT-RACK# copy-cfg from ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz		
MCT-RACK# copy-cfg from tftp 192.168.1.198 HS_0600_file.conf		

2. Restore the Chassis back to default settings.

Command / Example
MCT-RACK# copy-cfg from default

NOTE: *There are two ways to set the Chassis back to the factory default settings. Users can use the “copy-cfg from default” command in CLI or simply press the “Reset Button” located*

on the front panel to restore the device back to the initial state.

3. Restore the Chassis back to default settings but keep IP configurations.

Command / Example
MCT-RACK# copy-cfg from default keep-ip

4. Backup a configuration file to TFTP server.

Command	Parameter	Description
MCT-RACK# copy-cfg to ftp [A.B.C.D] [file_name] [running | default | startup] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file_name]	Enter the configuration file name that you want to backup.
	[running | default | startup]	Specify the type of backup config. **Running-config:** Back up the data you're processing **Default-config:** Back up the data same as factory setting. **Start-up-config:** Back up the data same as last saved data.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
MCT-RACK# copy-cfg to tftp [A.B.C.D] [file_name] [running | default | startup]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file_name]	Enter the configuration file name that you want to backup.
	[running | default | startup]	Specify the type of backup config.
Example		
MCT-RACK# copy-cfg to ftp 192.168.1.198 HS_0600_file.conf default misadmin1 abcxyz		
MCT-RACK# copy-cfg to tftp 192.168.1.198 HS_0600_file.conf running		

2.5.2 Firmware Command

To upgrade Firmware via FTP or TFTP server.

Command	Parameter	Description
MCT-RACK# firmware upgrade ftp [A.B.C.D] [file_name] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file_name]	Enter the firmware file name that you want to upgrade.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.

MCT-RACK# firmware upgrade tftp [A.B.C.D] [file_name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file_name]	Enter the firmware file name that you want to upgrade.
Example		
MCT-RACK# firmware upgrade ftp 192.168.1.198 HS_0600_file.bin edge10 abcxyz		
MCT-RACK# firmware upgrade tftp 192.168.1.198 HS_0600_file.bin		

2.5.3 Ping Command

Command	Parameter	Description
MCT-RACK> ping [A.B.C.D] [-s size (1-65500)bytes] [-t timeout (1-99)secs]	[A.B.C.D]	Enter the IP address that you would like to ping.
	[-s size (1-65500)bytes]	Enter the packet size that would be sent. The allowable packet size is from 1 to 65500 bytes. (optional)
	[-t timeout (1-99) secs]	Enter the timeout value when the specified IP address is not reachable. (optional)
Example		
MCT-RACK> ping 8.8.8.8 MCT-RACK> ping 8.8.8.8 –s 128 –t 10		

2.5.4 Reload Command

To restart the Chassis, enter the reload command.

Command / Example
MCT-RACK# reload

2.5.5 Write Command

To save running configurations to startup configurations, enter the write command. All unsaved configurations will be lost when you restart the Chassis.

Command / Example
MCT-RACK# write

2.5.6 Configure Command

You can enter Global Configuration Mode only from Privileged Mode. You can type in “configure” or “config” to enter Global Configuration Mode. The display prompt will change from “MCT-RACK#” to “MCT-RACK(config)#” once you successfully enter Global Configuration Mode.

Command / Example
MCT-RACK# config MCT-RACK(config)#
MCT-RACK# configure MCT-RACK(config)#

2.5.7 Show Command

The “show” command is very important for network administrators to get information about the device, receive outputs to verify a command’s configurations or troubleshoot a network configuration error. It can be used in Privileged or Configuration mode. The following describes different uses of “show” command.

1. Display system information

Enter “show switch-info” command in Privileged or Configuration mode, and then the following information will appear.

Company Name: Display a company name for this CHASSIS. Use “switch-info company-name [company-name]” command to edit this field.

System Object ID: Display the predefined System OID.

System Contact: Display contact information for this CHASSIS. Use “switch-info sys-contact [sys-contact]” command to edit this field.

System Name: Display a descriptive system name for this CHASSIS. Use “switch-info sys-name [sys-name]” command to edit this field.

System Location: Display a brief location description for this CHASSIS. Use “switch-info sys-location [sys-location]” command to edit this field.

Model Name: Display the product’s model name.

Host Name: Display the product’s host name.

DHCP Vendor ID: Display the product’s DHCP Vendor ID.

Firmware Version1: Display the firmware version 1 (image-1) used in this device.

Firmware Version2: Display the firmware version 2 (image-2) used in this device.

M/B Version: Display the main board version.

Serial Number: Display the serial number of this CHASSIS.

Up Time: Display the up time since last restarting.

Local Time: Display local time.

Current Run In: Display the current running firmware image.

Reboot Run To: Display the firmware image which will run after next restarting.

Fan State: Display the status of case fans.

Power (A-B): Display the status of powers.

2. Display or verify currently-configured settings

Refer to the following sub-sections for more information.

2.6 Configuration Mode

When you enter “configure” or “config” and press “Enter” in Privileged Mode, you will be directed to Global Configuration Mode where you can set up advanced functions,. Any command entered will be applied to running-configuration and the device’s operation. From this level, you can also enter different sub-configuration modes to set up specific configurations.

Command	Description
chassis	Enable or disable power supply for installed media converters.
exit	Exit the Configuration Mode.
help	Display a list of available commands in Configuration Mode.
history	Show commands that have been used.
ip	Set up the IP address.
management	Set up the system service type.
ntp	Set up required configurations for Network Time Protocol.
snmp-server	Create a new SNMP community and trap destination and specify the trap types.
switch-info	Specify company name, host name, system location, etc.
syslog	Enable or disable syslog server and assign server IP address.
user	Create a new user account.
no	Disable a command or set it back to its default setting.
slot	Set up media converter configuration.
show	Show a list of commands or show the current setting of each listed command.

2.6.1 No Command

Most commands that you enter in Configuration mode can be negated using “no” command followed by the same or original command. The purpose of “no” command is to disable a function, remove a command, or set the setting back to the default value. In each sub-section below, the use of no command to fulfill different purposes will be introduced.

2.6.2 Show Command

The command “show” is very important for network administrators to get information about the device, receive outputs to verify a command’s configurations or troubleshoot a network configuration error. “Show” command can be used in Privileged or Configuration mode. The following describes different uses of “show” command.

2.6.3 Chassis Command

This is to enable or disable power supply on a corresponding slot.

Command	Parameter	Description
MCT-RACK(config)# chassis power [slot_list]	[slot_list]	Enable power supply on specified slots.
No Command		
MCT-RACK(config)# no chassis power [slot_list]	[slot_list]	Disable power supply on specified slots.

Show Command		
MCT-RACK(config)# show chassis		Show chassis power supply status.
Chassis command example		
MCT-RACK(config)# chassis power 8		Enable power supply on slot 8

2.6.4 Digital Command

This is a way serving as an alarm via relay that is an electrically operated switch used where it is necessary to control a circuit by a low-power signal, or where several circuits must be controlled by one signal, thus helping us understand immediate status on a circuit with fault relay feature from remote site. This section gives the instruction how to set up relay configuration.

Digital command	Parameter	Description
MCT-RACK(config)# digital input 1 [open | close]	[open | close]	Set up digital input 1 circuit normal status. Under normal status, determine the electrical circuit should be open or close. Normal Status refers to where the contacts remain in one state unless actuated. The contacts can either be normally open until closed by operation of the switch, or normally closed and opened by the switch action.
MCT-RACK(config)# digital output 1		Enter Digital Output interface
MCT-RACK(config-output-No.)# normal [open | close]	[open | close]	Under normal status, determine the electrical circuit should be open or close. This is where the contacts remain in one state unless actuated by one of events in Digital Output Event.
MCT-RACK(config-output-No.)# event digital-input 1		Specify digital number 1 and enable the alarm of digital input specified.
MCT-RACK(config-output-No.)# event slot [slot_list]	[slot_list]	Specify slots and enable slot alarm.
MCT-RACK(config-output-No.)# event slot [slot_list] [por_list]	[slot_list] [port_list]	Specify TP or FO port alarm on media converters. Where 1 is TP port and 2 is FO port.
MCT-RACK(config-output-No.)# event lan-port		Enable LAN port alarm

MCT-RACK(config-output-No.)# event power [a | b]	[a | b]	Specify power source and enable power alarm.
MCT-RACK(config-output-No.)# trigger		Enable digital output event.
No command		
MCT-RACK (config)# no digital input 1		Undo the status of electrical circuit for the digital input number specified.
MCT-RACK (config)# no digital output 1		Undo the status of electrical circuit for the digital number specified.
MCT-RACK (config-output-No.)# no event digital-input 1		Specify digital number and disable the alarm of digital output specified.
MCT-RACK (config-output-No.)# no event lan-port		Specify LAN port and disable the alarm of digital output specified.
MCT-RACK (config-output-No.)# no event slot [slot_list]	[slot_list]	Specify slots and disable slot alarm.
MCT-RACK (config-output-No.)# no event slot [slot_list] [port_list]	[slot_list] [port_list]	Specify TP/FO port on media converters and disable port alarm.
MCT-RACK (config-output-No.)# no event power [a | b]	[a | b]	Specify power source and disable power alarm.
MCT-RACK(config-output-No.)# no normal		Undo the status of electrical circuit for the digital output number specified.
MCT-RACK(config-output-No.)# no trigger		Disable digital output event.
Show command		
MCT-RACK (config)# show digital input		Show digital input configuration.
MCT-RACK (config)# show digital input status		Show digital input status.
MCT-RACK (config)# show digital output		Show digital output configuration.
MCT-RACK (config)# show digital output status		Show digital output status.
MCT-RACK (config-output-No.)# show		Show the designated digital output status.

2.6.5 IP Command

This is to configure IP address.

1. Set up or remove the IP address.

IP command	Parameter	Description
MCT-RACK(config)# ip address [A.B.C.D] [255.X.X.X] [A.B.C.D]	[A.B.C.D]	Enter the desired IP address for the Chassis.
	[255.X.X.X]	Enter subnet mask of your IP address.
	[A.B.C.D]	Enter the default gateway address.
No command		
MCT-RACK(config)# no ip address		Remove the CHASSIS's IP address.
Show command		
MCT-RACK(config)# show ip address		Show the current IP configurations or verify the configured IP settings.
IP command example		
MCT-RACK(config)# ip address 192.168.1.198 255.255.255.0 192.168.1.254		Set up the CHASSIS's IP to 192.168.1.198, subnet mask to 255.255.255.0, and default gateway to 192.168.1.254.

2. Enable the Chassis to automatically get IP address from the DHCP server.

Command / Example	Description
MCT-RACK(config)# ip address dhcp	Enable DHCP mode.
No command	
MCT-RACK(config)# no ip address dhcp	Disable DHCP mode.
Show command	
MCT-RACK(config)# show ip address	Show the current IP configurations or verify the configured IP settings.

2.6.6 Management Command

Management command	Parameter	Description
MCT-RACK(config)# management console timeout [0 | 5-300]	[0 | 5-300]	Under RS-232 interface commands, specify session aging time within the range: zero or 5-300 seconds. ("0" indicates never aging out)
MCT-RACK(config)# management [ssh | telnet | web]	[ssh | telnet | web]	Select the system service type, SSH, telnet or web.
MCT-RACK(config)# management telnet port [1-65535]	[1-65535]	Specify telnet port number.

No command		
MCT-RACK(config)# no management [ssh | telnet | web]	[ssh | telnet | web]	Set system service type to Disabled.
MCT-RACK(config)# no management telnet port		Disable telnet port number specified.
Show command		
MCT-RACK(config)# show management		Show the current system service type.
Management command example		
MCT-RACK(config)# management ssh		Enable SSH system service type.

2.6.7 NTP Command

Set up required configurations for Network Time Protocol.

Command	Parameter	Description
MCT-RACK(config)# ntp		Enable the Chassis to synchronize the clock with a time server.
MCT-RACK(config)# ntp daylight-saving [recurring | date]	[recurring | date]	Enable the day light savings.
MCT-RACK(config)# ntp offset [Mm,w,d,hh:mm-Mm,w,d,hh:mm]	[Mm,w,d,hh:mm-Mm,w,d,hh:mm]	Offset setting for daylight saving function of recurring mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat)** **Hh=0-23, mm=0-59, Days=1-365**
MCT-RACK(config)# ntp offset [Days,hh:mm-Days,hh:mm]	[Days,hh:mm-Days,hh:mm]	Offset setting for daylight saving function of date mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat)** **Hh=0-23, mm=0-59, Days=1-365**
MCT-RACK(config)# ntp server1 [A.B.C.D]	[A.B.C.D]	Specify the primary time server IP address.
MCT-RACK(config)# ntp server2 [A.B.C.D]	[A.B.C.D]	Specify the secondary time server IP address.
MCT-RACK(config)# ntp syn-interval [1-8]	[1-8]	Specify the interval time to synchronize from NTP time server. The meanings of the value: **1:1hr, 2:2hrs 3:3hrs 4:4hrs** **5:6hrs 6:8hrs 7:12hrs 8:24hrs**
MCT-RACK(config)# ntp time-zone [0-132]	[0-132]	Specify the time zone to that the Chassis belongs. Use any key to view the complete code list of 132 time zones. For example, "MCT-RACK(config)# ntp time-zone ?"
No command		
MCT-RACK(config)# no ntp		Disable the Chassis to synchronize the clock with a time server.
MCT-RACK(config)# no ntp daylight-saving		Disable the daylight saving function.
MCT-RACK(config)# no ntp offset		Set the offset value back to the default setting.
MCT-RACK(config)# no ntp server1		Delete the primary time server IP address.
MCT-RACK(config)# no ntp server2		Delete the secondary time server IP address.
MCT-RACK(config)# no ntp syn-interval		Set the synchronization interval back to the default setting.

MCT-RACK(config)# no ntp time-zone	Set the time-zone setting back to the default setting.
Show command	
MCT-RACK(config)# show ntp	Show or verify current time server settings.
NTP command example	
MCT-RACK(config)# ntp	Enable the Chassis to synchronize the clock with a time server.
MCT-RACK(config)# ntp server1 192.180.0.12	Set the primary time server IP address to 192.180.0.12.
MCT-RACK(config)# ntp server2 192.180.0.13	Set the secondary time server IP address to 192.180.0.13.
MCT-RACK(config)# ntp syn-interval 8	Set the synchronization interval to 24 hrs.
MCT-RACK(config)# ntp time-zone 4	Set the time zone to GMT-8:00 Vancouver.

2.6.8 SNMP-Server Command

1. Create a SNMP community and set up detailed configurations for this community.

Snmp-server command	Parameter	Description
MCT-RACK(config)# snmp-server community [community]	[community]	Specify a SNMP community name up to 20 alphanumeric characters.
MCT-RACK(config-community-NAME)# active		Enable this SNMP community account.
MCT-RACK(config-community-NAME)# description [Description]	[Description]	Enter the description up to 35 alphanumerical characters for this SNMP community.
MCT-RACK(config-community-NAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify the access privilege for this SNMP account. By default, when you create a community, the access privilege for this account is set to “read only”. **Admin:** Full access right, including maintaining user account, system information, loading factory settings, etc.. **rw:** Read & Write access privilege. Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware. **Ro:** Read Only access privilege.
No command		
MCT-RACK(config)# no snmp-server community [community]	[community]	Delete the specified community.
MCT-RACK(config-community-NAME)# no active		Disable this SNMP community account.
MCT-RACK(config-community-NAME)# no description		Remove the entered SNMP community descriptions.
MCT-RACK(config-community-NAME)# no level		Remove the configured level. This will set this community’s level to read only.
Show command		
MCT-RACK(config)# show snmp-server community [community]	[community]	Show the specified SNMP server account’s settings.
MCT-RACK(config)# show snmp-server community		Show SNMP community account’s information in Global Configuration Mode.
MCT-RACK(config-community-NAME)# show		View or verify the configured SNMP community account’s information.
Exit command		
MCT-RACK(config-community-NAME)# exit		Return to Global Configuration Mode.

Snmp-server example	
MCT-RACK(config)# snmp-server community mycomm	Create a new community “mycomm” and edit the details of this community account.
MCT-RACK(config-community-mycomm)# active	Activate the SNMP community “mycomm”.
MCT-RACK(config-community-mycomm)# description rddeptcomm	Add a description for “mycomm” community.
MCT-RACK(config-community-mycomm)# level admin	Set “mycomm” community level to admin.

2. Set up a SNMP trap destination.

Trap-dest command	Parameter	Description
MCT-RACK(config)# snmp-server trap-destination [1-10]	[1-10]	Create a trap destination account.
MCT-RACK(config-trap-ACCOUNT)# active		Enable this SNMP trap destination account.
MCT-RACK(config-trap-ACCOUNT)# community [community]	[community]	Enter the community name of network management system.
MCT-RACK(config-trap-ACCOUNT)# destination [A.B.C.D]	[A.B.C.D]	Enter the SNMP server IP address.
No command		
MCT-RACK(config)# no snmp-server trap-destination [1-10]	[1-10]	Delete the specified trap destination account.
MCT-RACK(config-trap-ACCOUNT)# no active		Disable this SNMP trap destination account.
MCT-RACK(config-trap-ACCOUNT)# no community		Delete the configured community name.
MCT-RACK(config-trap-ACCOUNT)# no destination		Delete the configured trap destination.
Show command		
MCT-RACK(config)# show snmp-server trap-destination [1-10]	[1-10]	Show the specified trap destination information.
MCT-RACK(config)# show snmp-server trap-destination		Show SNMP trap destination information in Global Configuration mode.
MCT-RACK(config-trap-ACCOUNT)# show		View this trap destination account’s information.
Exit command		
MCT-RACK(config- trap-ACCOUNT)# exit		Return to Global Configuration Mode.
Trap-destination example		
MCT-RACK(config)# snmp-server trap-destination 1		Create a trap destination account.
MCT-RACK(config-trap-1)# active		Activate the trap destination account.

MCT-RACK(config-trap-1)# community mycomm	Refer this trap destination account to the community “mycomm”.
MCT-RACK(config-trap-1)# description redepttrapdest	Add a description for this trap destination account.
MCT-RACK(config-trap-1)# destination 172.168.1.254	Set trap destination IP address to 192.168.1.254.

3. Set up SNMP trap types that will be sent.

Trap-type command	Parameter	Description
MCT-RACK(config)# snmp-server trap-type [all |auth-fail | case-fan | cold-start | digital | module-port-link | power-down | warm-start]	[all |auth-fail | case-fan | cold-start | digital | module-port-link | power-down | warm-start]	Specify the trap type that will be sent when a certain situation occurs. **all:** A trap will be sent when authentication fails, the device cold /warm starts, port link is up or down, power is down. **auth-fail:** A trap will be sent when any unauthorized user attempts to login. **case-fan:** A trap will be sent when any case fan fails. **cold-start:** A trap will be sent when the device boots up. **digital:** A trap will be sent when there is a discrepancy on digital input/output. **module-port-link:** A trap will be sent when the link is up or down. **power-down:** A trap will be sent when the device’s power is down. **warm-start:** A trap will be sent when the device restarts.
No command		
MCT-RACK(config)# no snmp-server trap-type auth-fail		Authentication failure trap will not be sent.
Show command		
MCT-RACK(config)# show snmp-server trap-type		Show the current enable/disable status of each type of trap.
Trap-type example		
MCT-RACK(config)# snmp-server trap-type all		All types of SNMP traps will be sent.

4. Set up detailed configurations for SNMPv3 USM User

Simple Network Management Protocol Version 3, SNMPv3 in short, features stronger security mechanism, including authentication and encryption that helps ensure that the message is from a valid source and scramble the content of a packet, to prevent from being learned by an unauthorized source.

Note: The SNMPv3 community user account is generated from "User Command" (Section 2.6.11)

Snmp-server command	Parameter	Description
MCT-RACK(config)# snmp-server user [user_name]	[user_name]	Specify an existing SNMPv3 community name for configuration.
MCT-RACK(config-v3-community- user_name)# authentication [md5 | sha]	[md5 | sha]	Specify the method to ensure the identity of users. **md5(message-digest algorithm):** A widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. **sha(Secure Hash Algorithm):** A 160-bit hash function which resembles the said MD5 algorithm.
MCT-RACK(config-v3-community- user_name)# authentication password [password]	[password]	Specify the passwords, up to 20 characters.
MCT-RACK(config-v3-community- user_name)# private [des]	[des]	Specify the method to ensure confidentiality of data. **des(data encryption standard):** An algorithm to encrypt critical information such as message text message signatures…etc.
MCT-RACK(config-v3-community- user_name)# private password [password]	[password]	Specify the passwords, up to 20 characters.
No Command		
MCT-RACK(config-v3-community-user_name)# no authentication		Disable authentication function.
MCT-RACK(config-v3-community-user_name)# no authentication password		Delete authentication password.
MCT-RACK(config-v3-community-user_name)# no private		Disable data encryption function.
MCT-RACK(config-v3-community-user_name)# no private password		Delete private password.

Show Command	
MCT-RACK(config-v3-community-user_name)# show	Show the current status of SNMPv3 community.

A combination of a security event as below indicates which security mechanism is used when handling an SNMP packet.

Authentication	Private	Result
None	None	Uses a username match for authentication
Message Digest Algorithm(MD5) or Secure Hash Algorithm(SHA)	None	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms.
MD5 or SHA	Data Encryption Standard(DES)	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms. What's more, enables DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES standard.

2.6.9 System-Info Command

Set up the Chassis's basic information including company name, hostname, system name, etc..

Switch-info Command	Parameter	Description
MCT-RACK(config)# system-info company-name [company_name]	[company_name]	Enter a company name for this Chassis, up to 55 alphanumeric characters.
MCT-RACK(config)# system-info dhcp-vendor-id [dhcp_vendor_id]	[dhcp_vendor_id]	Enter the user-defined DHCP vendor ID up to 55 alphanumeric characters. Please make sure you have an exact DHCP Vendor ID with the value specified in "vendor-classes" in your dhcp.conf file.
MCT-RACK(config)# system-info system-contact [system_contact]	[system_contact]	Enter contact information up to 55 alphanumeric characters for this Chassis.
MCT-RACK(config)# system-info system-location [system_location]	[system_location]	Enter a brief description of the Chassis location up to 55 alphanumeric characters. Like the name, the location is for reference only, for example, "13th Floor".
MCT-RACK(config)# system-info system-name [system_name]	[system_name]	Enter a unique name up to 55 alphanumeric characters for this Chassis. Use a descriptive name to identify the Chassis in relation to your network, for example, "Backbone 1". This name is mainly used for reference only.
MCT-RACK(config)# system-info host-name [host_name]	[host_name]	Enter a new hostname up to 15 alphanumeric characters for this Chassis. By default, the hostname prompt shows the model name of this Chassis. You can change the factory-assigned hostname prompt to the one that is easy for you to identify during network configuration and maintenance.

No command	
MCT-RACK(config)# no system-info company-name	Delete the entered company name information.
MCT-RACK(config)# no system-info dhcp-vendor-id	Delete the entered DHCP vendor ID information.
MCT-RACK(config)# no system-info system-contact	Delete the entered system contact information.
MCT-RACK(config)# no system-info system-location	Delete the entered system location information.

MCT-RACK(config)# no system-info system-name	Delete the entered system name information.
MCT-RACK(config)# no system-info host-name	Set the hostname to the factory default.
Show command	
MCT-RACK(config)# show system-info	Show CHASSIS information including company name, system contact, system location, system name, model name, firmware version and fiber type.
Switch-info example	
MCT-RACK(config)# system-info company-name telecomxyz	Set the company name to “telecomxyz”.
MCT-RACK(config)# system-info system-contact info@company.com	Set the system contact field to “info@compnay.com”.
MCT-RACK(config)# system-info system-location 13thfloor	Set the system location field to “13thfloor”.
MCT-RACK(config)# system-info system-name backbone1	Set the system name field to “backbone1”.

2.6.10 Syslog Command

Syslog command	Parameter	Description
MCT-RACK(config)# syslog		Enable syslog server
MCT-RACK(config)# syslog server1/server2/server3 [A.B.C.D]	[A.B.C.D]	Configure syslog server1/server2/server3
No command		
MCT-RACK(config)# no syslog		Disable syslog server
Show command		
MCT-RACK(config)#show syslog		Show syslog status
Syslog example		
MCT-RACK(config)# syslog MCT-RACK(config)# syslog server1 192.168.0.222		Enable syslog and assign server1 IP address 192.168.0.222

2.6.11 Terminal Command

Command	Parameter	Description
Switch(config)# terminal length [0-512]	[0-512]	Specify how many the event lines show up at a time for “show running-config”, “show default-config” and “show start-up-config” commands.
No Command		
Switch(config)# no terminal length		Return terminal length to default value 20.
Show Command		
Switch(config)# show terminal		Show the current status of terminal length.

2.6.12 User Command

1. Create a new login account.

User command	Parameter	Description
MCT-RACK(config)# user name [user_name]	[user_name]	Enter the new account’s username. The authorized user login name is up to 20 alphanumeric characters. Only 10 login accounts can be registered in this device.
MCT-RACK(config-user-USERNAME)# active		Activate this user account.
MCT-RACK(config-user-USERNAME)# description [description]	[description]	Enter the brief description for this user account.

MCT-RACK(config-user-USERNAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify user account level. By default, when you create a community, the access privilege for this account is set to “read only”. **Admin:** Full access right, including maintaining user account, system information, loading factory settings, etc.. **rw:** Read & Write access privilege. Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware. **Ro:** Read Only access privilege.
MCT-RACK(config-user-USERNAME)# password [password]	[password]	Enter the password for this user account up to 20 alphanumeric characters.
No command		
MCT-RACK(config)# no user name [user_name]	[user_name]	Delete the specified user account.
MCT-RACK(config-user-USERNAME)# no description		Remove the configured description.
MCT-RACK(config-user-USERNAME)# no level		Remove the configured level value. The account level will return to the default setting.
MCT-RACK(config-user-USERNAME)# no password		Remove the configured password value.
Show command		
MCT-RACK(config)# show user name [user_name]	[user_name]	Show the specified account’s information.
MCT-RACK(config)# show user name		List all user accounts.
MCT-RACK(config-user-USERNAME)# show		Show or verify the newly-created user account’s information.
User command example		
MCT-RACK(config)# user name miseric		Create a new login account “miseric”.
MCT-RACK(config-user-USERNAME)# description misengineer		Add a description to this new account “miseric”.
MCT-RACK(config-user-USERNAME)# level rw		Set this new account’s access privilege to “read & write”.
MCT-RACK(config-user-USERNAME)# password mis2256i		Set up a password for this new account “miseric”

2. Configure RADIUS server settings.

User command	Parameter	Description
MCT-RACK(config)# user radius		Enable RADIUS authentication.
MCT-RACK(config)# user radius radius-port [1025-	[1025-65535]	Specify RADIUS server port number.

65535]		
MCT-RACK(config)# user radius retry-time [0-2]	[0-2]	Specify the retry value. This is the number of times that the CHASSIS will try to reconnect if the RADIUS server is not reachable.
MCT-RACK(config)# user radius secret [secret]	[secret]	Specify a secret up to 30 alphanumeric characters for RADIUS server. This secret key is used to validate communications between RADIUS servers.
MCT-RACK(config)# user radius server1 [A.B.C.D]	[A.B.C.D]	Specify the primary RADIUS server IP address.
MCT-RACK(config)# user radius server2 [A.B.C.D]	[A.B.C.D]	Specify the secondary RADIUS server IP address.
No command		
MCT-RACK(config)# no user radius		Disable RADIUS authentication.
MCT-RACK(config)# no user radius radius-port		Reset the radius port setting back to the default.
MCT-RACK(config)# no user radius retry-time		Reset the retry time setting back to the default.
MCT-RACK(config)# no user radius secret		Remove the configured secret value.
MCT-RACK(config)# no user radius server1		Delete the specified IP address.
MCT-RACK(config)# no user radius server2		Delete the specified IP address.
Show command		
MCT-RACK(config)#show user radius		Show current RADIUS settings.
User command example		
MCT-RACK(config)# user radius		Enable RADIUS authentication.
MCT-RACK(config)# user radius radius-port 1812		Set RADIUS server port number to 1812.
MCT-RACK(config)# user radius retry-time 2		Set the retry value to 2. The CHASSIS will try to reconnect twice if the RADIUS server is not reachable.
MCT-RACK(config)# user radius secret abcxyzabc		Set up a secret for validating communications between RADIUS clients.
MCT-RACK(config)# user radius server1 192.180.3.1		Set the primary RADIUS server address to 192.180.3.1.
MCT-RACK(config)# user radius server2 192.180.3.2		Set the secondary RADIUS server address to 192.180.3.2.

3. Configure TACACS server settings.

User command	Parameter	Description
MCT-RACK(config)# user tacacs		Enable TACACS+ authentication.
MCT-RACK(config)# user tacacs tacacs-port [49, 1025-65535]	[49, 1025-65535]	Specify TACACS server port number. The default setting is at 49 port.
MCT-RACK(config)# user tacacs retry-time [0-2]	[0-2]	Specify the retry time value. This is the number of times that the CHASSIS will try to reconnect if the TACACS server is not reachable.
MCT-RACK(config)# user tacacs secret [secret]	[secret]	Specify a secret, up to 30 alphanumeric characters, for TACACS server. This secret key is used to validate communications between TACACS servers.
MCT-RACK(config)# user tacacs server1 [A.B.C.D]	[A.B.C.D]	Specify the primary TACACS server IPv4 address.
MCT-RACK(config)# user tacacs server2 [A.B.C.D]	[A.B.C.D]	Specify the secondary TACACS server IPv4 address.
No command		
MCT-RACK(config)# no user tacacs		Disable TACACS+ authentication.
MCT-RACK(config)# no user tacacs tacacs-port		Reset the tacacs port setting back to the default.(49 port)
MCT-RACK(config)# no user tacacs retry-time		Reset the retry time setting back to the default.
MCT-RACK(config)# no user tacacs secret		Remove the configured secret value.
MCT-RACK(config)# no user tacacs server1		Delete the IPv4 address of the primary TACACS server.
MCT-RACK (config)# no user tacacs server2		Delete the IPv4 address of the secondary TACACS server.
Show command		
MCT-RACK(config)# show user tacacs		Show the current TACACS+ configuration.

2.6.13 Remote Command

Slot command	Parameter	Description
MCT-RACK(config)# remote [remote_list]	[remote_list]	Specify any remote converter you want to configure.
MCT-RACK(config-remote-No.)# firmware upgrade		Upgrade the firmware of remote converter.
MCT-RACK(config-remote-No.)# module link-alarm		Enable link alarm function.
MCT-RACK(config-remote-No.)# module-info description [description]	[description]	Type any remark for the remote converter.
MCT-RACK(config-remote-No.)# reload		Reset the remote converter.
MCT-RACK(config-remote-No.)# security storm-protection		Enable Broadcast Storm Control.
MCT-RACK(config-remote-No.)# security storm-protection rates [32-1000000] kbps	[32-1000000]	Set up storm rate value. Packets exceeding the value will be dropped. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)
MCT-RACK(config-remote-No.)# vlan dot1q-vlan		Globally enable 802.1q VLAN
MCT-RACK(config-remote-No.)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VID number to create a 802.1q VLAN. **Note :** 802.1q VLAN ID need to be created under interface command. In here you can only modify it instead of creating a new VLAN ID.
MCT-RACK(config-remote-No.-vlan-No.)# name [vlan_name]	[vlan_name]	Specify the VLAN a name, up to 15 characters.
MCT-RACK(config-remote-No.)# vlan qinq-vlan		Globally enable QinQ VLAN.
MCT-RACK(config-remote-No.)# vlan qinq-vlan bypass-ctag		Ignore the C-tag checking.
MCT-RACK(config-remote-No.)# vlan qinq-vlan isp-port [port_list]	[port_list]	Configure ISP Port (Q-in-Q Port) **ISP(Internet Service Provider) Port:** This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.

MCT-RACK(config-remote-No.)# vlan qinq-vlan stag-ethertype [0xWXYZ]	[0xWXYZ]	Specify service tag ether type. **Ether Type:** A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).
MCT-RACK(config-remote-No.)# interface [port_list]	[port_list]	Select TP or FX port to configure. Where: 1=TP, 2=FX
MCT-RACK(config-remote-No.-if-No.)# auto-negotistion		Enable Auto-Negotiation on TP port.
MCT-RACK(config-remote-No.-if-No.)# duplex [full]	[full]	Set the duplex to full mode. **Note:** Duplex can be set when Auto-Negotiation is disabled.
MCT-RACK(config-remote-No.-if-No.)# qos rate-limit ingress [0 | 32-1000000]Kbps	[0 | 32-1000000]	Configure **ingress** rate limit, set zero or from 32Kbps to 1000Mbps.
MCT-RACK(config-remote-No.-if-No.)# qos rate-limit egress [0 | 32-1000000]Kbps	[0 | 32-1000000]	Configure **egress** rate limit, set zero or from 32Kbps to 1000Mbps.
MCT-RACK(config-remote-No.-if-No.)# shutdown		Administratively disable the selected ports' status.
MCT-RACK(config-remote-No.-if-No.)# speed [1000 |100 | 10 | auto_sense]	[1000 |100 | 10 | auto_sense]	Set up the selected interfaces' speed. Manual speed configuration only works when "no auto-negotiation" command is issued.
MCT-RACK(config-remote-No.-if-No.)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
MCT-RACK(config-remote-No.-if-No.)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
MCT-RACK(config-remote-No.-if-No.)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
MCT-RACK(config-remote-No.-if-No.)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
MCT-RACK(config-remote-No.-if-No.)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note :** When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.

Chassis(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid [1-4094]	[1-4094]	Specify the service tag VID for the selected port(s)
No Command		
MCT-RACK(config-remote-No.)# no module link-alarm		Disable Link Alarm function.
MCT-RACK(config-remote-No.)# no module-info description		Clear the description of the remote converter.
MCT-RACK(config-remote-No.)# no security storm-protection		Disable Storm Control.
MCT-RACK(config-remote-No.)# no security storm-protection rates		Return Storm Rate to default.
MCT-RACK(config-remote-No.)# no vlan dot1q-vlan		Disable 802.1q VLAN.
MCT-RACK(config-remote-No.)# no vlan qinq-vlan		Disable QinQ VLAN.
MCT-RACK(config-remote-No.)# no vlan dot1q-vlan		Disable IEEE 802.1q Tag VLAN mode.
MCT-RACK(config-remote-No.)# no vlan qinq-vlan		Disable Q-in-Q VLAN
MCT-RACK(config-remote-No.)# no vlan qinq-vlan bypass-ctag		Not ignore the C-tag checking.
MCT-RACK(config-remote-No.)# no vlan qinq-vlan isp-port		Undo ISP port (Q-in-Q port)
MCT-RACK(config-remote-No.)# no vlan qinq-vlan stag-ethertype		Delete service tag ether type.
MCT-RACK(config-remote-No.-if-No.)# no auto-negotiation		Disable auto-negotiation function.
MCT-RACK(config-remote-No.-if-No.)# no duplex		Set the selected ports' duplex mode to the default setting. **Note :** Auto-negotiation needs to be disabled before configuring duplex mode.
MCT-RACK(config-remote-No.-if-No.)# no qos rate-limit ingress		Undo **ingress** rate limit.
MCT-RACK(config-remote-No.-if-No.)# no qos rate-limit egress		Undo **egress** rate limit.
MCT-RACK(config-remote-No.-if-No.)# no shutdown		Administratively enable the selected ports' status.
MCT-RACK(config-remote-		Set the selected ports' speed to the default

No.-if-No.)# no speed		setting.
MCT-RACK(config-remote-No.-if-No.)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
MCT-RACK(config-remote-No.-if-No.)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
MCT-RACK(config-remote-No.-if-No.)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
MCT-RACK(config-remote-No.-if-No.)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
MCT-RACK(config-remote-No.)# no vlan qinq-vlan stag-vid		Clear the service tag VID specified.
Show Command		
MCT-RACK(config-remote-No.)# show dip-switch		Show DIP Switch information.
MCT-RACK(config-remote-No.)# show interface		Show all the interface information.
MCT-RACK(config-remote-No.)# show module		Show the current status of link alarm.
MCT-RACK(config-remote-No.)# show module-info		Show all the basic converter information.
MCT-RACK(config-remote-No.)# show qos interface		Show all the current status of bandwidth control.
MCT-RACK(config-remote-No.)# show qos interface [port_list]	[port_list]	Show the TP or FX current status of bandwidth control. Where: 1=TP, 2=FX
MCT-RACK(config-remote-No.)# show security storm-protection		Show the current status of broadcast storm configuration.
MCT-RACK(config-remote-No.)# show vlan dot1q-vlan tag-vlan		Show the current 802.1q tag VLAN table.
MCT-RACK(config-remote-No.)# show vlan dot1q-vlan trunk-vlan		Show the current trunk VLAN table.

2.6.14 Slot Command

This section is intended to introduce the configuration of specified media converters.

Note: *Make sure that media converts are firmly installed and powered on.*

1. Specify any slots to configure

Slot command	Parameter	Description
MCT-RACK(config)# slot [slot_list]	[slot_list]	Specify any slots you want to configure.

2. Upgrade media converter firmware.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# firmware upgrade		Upgrade firmware. **Note:** Upgrade one media converter at a time.

3. Configure link alarm

When UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module link-alarm		Enable link alarm function.
No Command		
MCT-RACK(config-slot-slot-slot)# no module link-alarm		Disable link alarm function.
Show Command		
MCT-RACK(config-slot-slot-slot)# show module		Show the status of link alarm.

4. Set up module description

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module-info description [description]	[description]	Specify user-defined information. Up to 55 characters are available.
No Command		
MCT-RACK(config-slot-slot-slot)# no module-info description		Delete user-defined information.

Show Command	
MCT-RACK(config-slot-slot-slot)# show module-info	Show the module information.
Module Description Example	
MCT-RACK(config-slot-slot-slot)# module-info description 123	The description of the converter is named “123”.

5. Reset converter

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# reload		Reboot the media converters.

6. Set up security protection

When a device on the network is malfunctioning or application programs are not well designed or properly configured, broadcast storms may occur, which may degrade network performance or in the worst situation cause a complete halt. The Chassis allows users to set a threshold rate for broadcast traffic so as to protect network from broadcast storms. Any broadcast packet exceeding the specified value will then be dropped.

Security command	Parameter	Description
MCT-RACK(config)# security storm-protection		Enable storm protection function.
MCT-RACK(config)# security storm-protection rates [32-1000000] kbps	[32-1000000] kbps	Specify the maximum broadcast packet rate.
No command		
MCT-RACK(config)# no security storm-protection		Disable storm protection globally.
MCT-RACK(config)# no security storm-protection rates		Set broadcast packet rate back to the default.
Show command		
MCT-RACK(config)# show security storm-protection		Show storm control settings.

7. Set up VLAN configuration

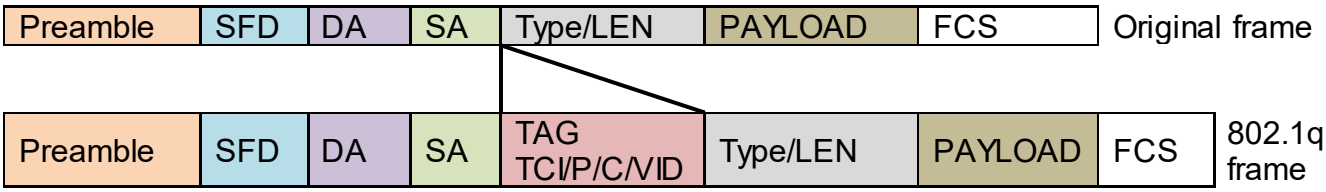
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the device on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of

physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

IEEE 802.1Q VLAN Concepts

Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes		User data	
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**

Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.

Example : PortX configuration

Configuration	Result
Trunk-VLAN = 10, 11, 12 Access-VLAN = 20 **Mode = Access**	PortX is an **Access Port** PortX's **VID** is ignored PortX's **PVID** is 20 PortX sends **Untagged** packets (PortX takes away VLAN tag if the PVID is 20) PortX receives **Untagged** packets only
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Trunk**	PortX is a **Trunk Port** PortX's **VID** is 10,11 and 12 PortX's **PVID** is ignored PortX sends and receives **Tagged** packets VID 10,11 and 12
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Trunk-native**	PortX is a **Trunk-native Port** PortX's **VID** is 10,11 and 12 PortX's **PVID** is 20 PortX sends and receives **Tagged** packets VID 10,11 and 12 PortX receives **Untagged** packets and add PVID 20

The CHSSSIS supports two types of VLAN, these are: **IEEE 802.1q Tag VLAN** and **Q in Q VLAN.**

VLAN Command	Parameter	Description
MCT-RACK(config-slot-slot-slot)#		Enable IEEE 802.1q Tag VLAN mode.

vlan dot1q-vlan		
MCT-RACK(config-slot-slot-slot)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VID number to create a 802.1q VLAN. **Note :** 802.1q VLAN ID need to be created under interface command. In here you can only modify it instead of creating a new VLAN ID.
MCT-RACK(config-slot-slot-slot)# vlan qinq-vlan		Enable Q-in-Q VLAN
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan bypass-ctag		Ignore the C-tag checking.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan isp-port [port_list]	[port_list]	Configure ISP Port (Q-in-Q Port) **ISP(Internet Service Provider) Port:** This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan stag-ethertype [0xWXYZ]	[0xWXYZ]	Specify service tag ether type. **Ether Type:** A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).
No Command		
MCT-RACK(config-slot-slot-slot)# no vlan dot1q-vlan		Disable IEEE 802.1q Tag VLAN mode.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan		Disable Q-in-Q VLAN
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan bypass-ctag		Not ignore the C-tag checking.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan isp-port		Undo ISP port (Q-in-Q port)
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan management-stag		Clear management service tag VID.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan stag-ethertype		Delete service tag ether type.
Show Command		
MCT-RACK(config-slot-slot-slot)# show vlan dot1q-vlan		Show dot1q VLAN configuration.
MCT-RACK(config-slot-slot-slot)# show vlan interface		Show all interfaces on a media converter
MCT-RACK(config-slot-slot-slot)# show vlan interface [port_list]	[port_list]	Show specific interfaces on a media converter
MCT-RACK(config-slot-slot-slot)#		Show Q-in-Q VLAN configuration.

show vlan qinq-vlan		

8. Use "Interface" command to configure 802.1q VLAN settings on a port.

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid [1-4094]	[1-4094]	Specify the service tag VID for the selected port(s)
No Command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
MCT-RACK(config-slot-slot-slot-if-port-port)# no	[1-4094]	Remove the selected ports' from the specified trunk VLAN.

vlan dot1q-vlan trunk-vlan [1-4094]		
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid		Clear the service tag VID specified.

2.6.15 Interface Command

This command is to configure TP port or fiber port on a converter.

Interface command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.

1. Configure auto-negotiation function.

Interface command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# auto-negotiation		Set the selected interfaces' to auto-negotiation. When auto-negotiation is enabled, speed configuration will be ignored.
No command		**No command**
MCT-RACK(config-slot-slot-slot-if-port-port)# no auto-negotiation		Disable auto-negotiation function.

2. Set up Duplex Mode

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# duplex [full]	[full]	Configure port duplex to **full.**
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no duplex		Set the selected ports' duplex mode to the default setting. **Note :** Auto-negotiation needs to be disabled before configuring duplex mode.

3. Qos configuration

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# qos rate-limit ingress [0|32-1000000]	[0|32-1000000]	Configure **ingress** rate limit, set zero or from 32Kbps to 1000Mbps.
MCT-RACK(config-slot-slot-slot-if-port-port)# qos rate-limit egress [0|32-1000000]	[0|32-1000000]	Configure **egress** rate limit, set zero or from 32Kbps to 1000Mbps.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no qos rate-limit ingress		Undo **ingress** rate limit.

MCT-RACK(config-slot-slot-slot-if-port-port)# no qos rate-limit egress		Undo **egress** rate limit.

4. Shutdown interface

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# shutdown		Administratively disable the selected ports' status.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no shutdown		Administratively enable the selected ports' status.

5. Speed configuration

Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# speed [1000 |100 | 10 | auto_sense]	[1000 |100 | 10 | auto_sense]	Set up the selected interfaces' speed. Manual speed configuration only works when "no auto-negotiation" command is issued.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no speed		Set the selected ports' speed to the default setting.

6. Configure 802.1q VLAN settings on a port.

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note : When you assign a default Access-**

		VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid [1-4094]	[1-4094]	Specify the service tag VID for the selected port(s)
No Command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid		Clear the service tag VID specified.

3. SNMP NETWORK MANAGEMENT

The Simple Network Management Protocol (SNMP) is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP consists following key components,

Managed device is a network node that contains SNMP agent. Managed devices collect and store management information and make this information available to NMS using SNMP. Managed device can be switches/Hub, etc.

MIB (Management Information Base) define the complete manageable entries of the managed device. These MIB entries can be either read-only or read-write. For example, the System Version is read-only variables. The Port State Enable or Disable is a read-write variable and a network administrator can not only read but also set its value remotely.

SNMP Agent is a management module resides in the managed device that responds to the SNMP Manager request.

SNMP Manager/NMS executes applications that monitor and control managed devices. NMS provide the bulk of the processing and memory resources required for the complete network management. SNMP Manager often composed by desktop computer/work station and software program such like HP OpenView.

Totally 4 types of operations are used between SNMP Agent & Manager to change the MIB information. These 4 operations all use the UDP/IP protocol to exchange packets.

GET: This command is used by an SNMP Manager to monitor managed devices. The SNMP Manager examines different variables that are maintained by managed devices.

GET Next: This command provides traversal operation and is used by the SNMP Manager to sequentially gather information in variable tables, such as a routing table.

SET: This command is used by an SNMP Manager to control managed devices. The NMS changes the values of variables stored within managed devices.

Trap: Trap is used by the managed device to asynchronously report a specified event to the SNMP Manager. When certain types of events occur, a managed device will send a trap to alert the SNMP Manager.

The system built-in management module also supports SNMP management. User must install the MIB file before using the SNMP based network management system. The MIB file is on a diskette that accompanies the system. The file name extension is .mib, which SNMP based compiler can read.

Please refer to the appropriate documentation for instructions on installing the system private MIB.

4. WEB MANAGEMENT

The CHASSIS can be accessed and managed via a Web browser. However, you must first assign a unique IP address to it before doing so. Use a RJ45 LAN cable and 10/100Base-T RJ-45 port of the CHASSIS (as the temporary RJ-45 Management console port) to login to the CHASSIS and set up the IP address for the first time. (The default IP of the CHASSIS can be reached at **"http://192.168.0.1"**. You can change the CHASSIS's IP address to the needed one in its **Network Management** menu.)

Follow these steps to manage the CHASSIS through a Web browser:

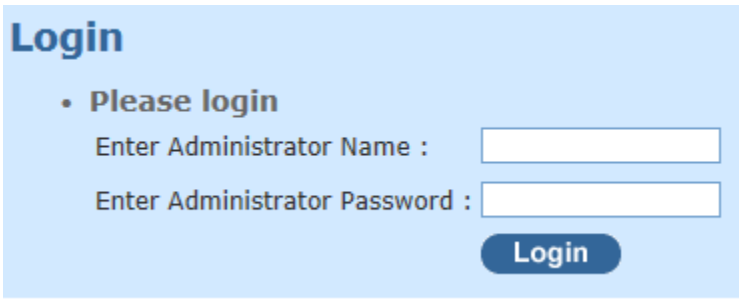
1. Use the 10/100Base-T RJ-45 ports (as the temporary RJ-45 Management console port) to set up the following IP parameters for the CHASSIS:

    - IP address
    - Subnet Mask
    - Default CHASSIS IP address, if required

2. Run a Web browser and specify the CHASSIS's IP address to reach it. (The default IP address is **"http://192.168.0.1"**)

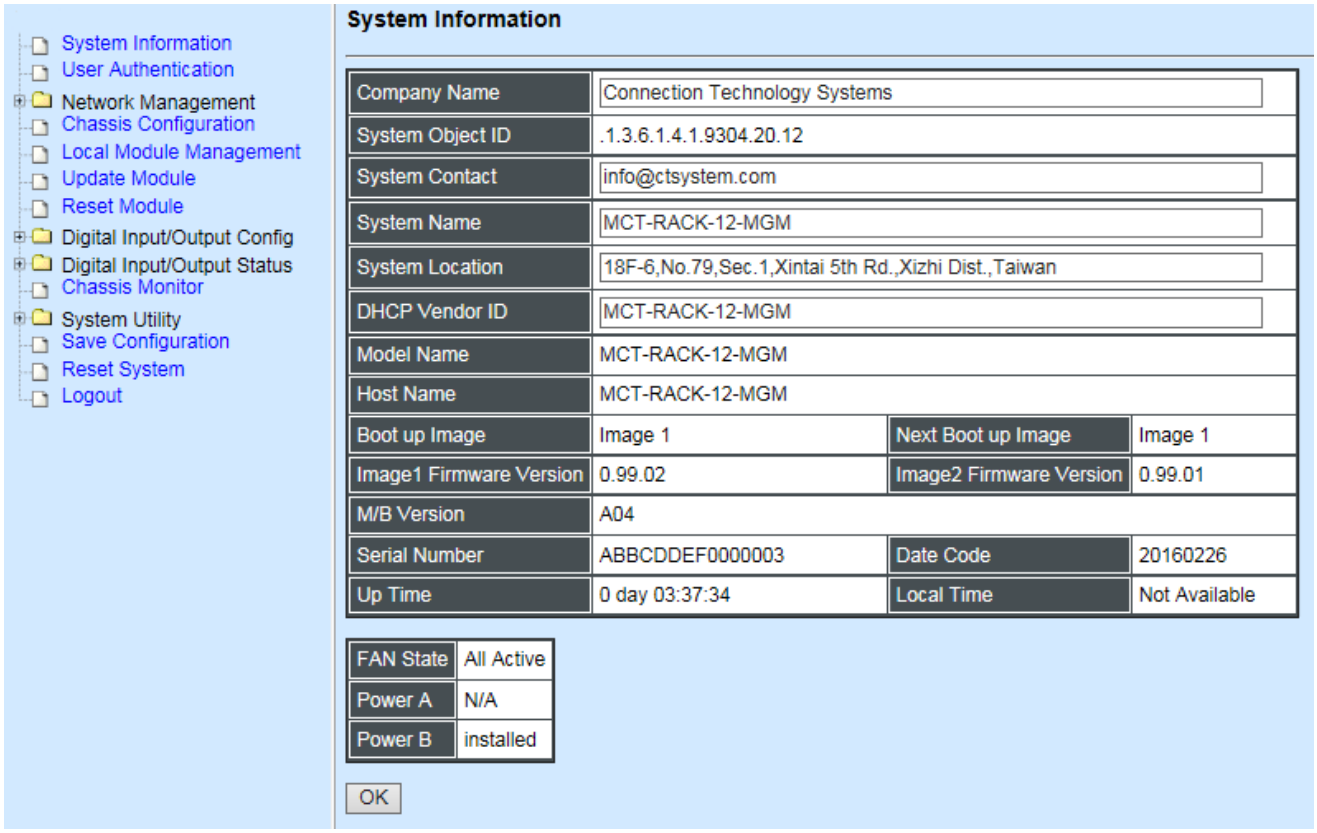
3. Login to reach the Main Menu.

Once you gain the access, a Login window shows up like the one shown below.



Enter the user name and password then select "OK" to login to the main screen page. By default, the username is **"admin"** and **without a password**.

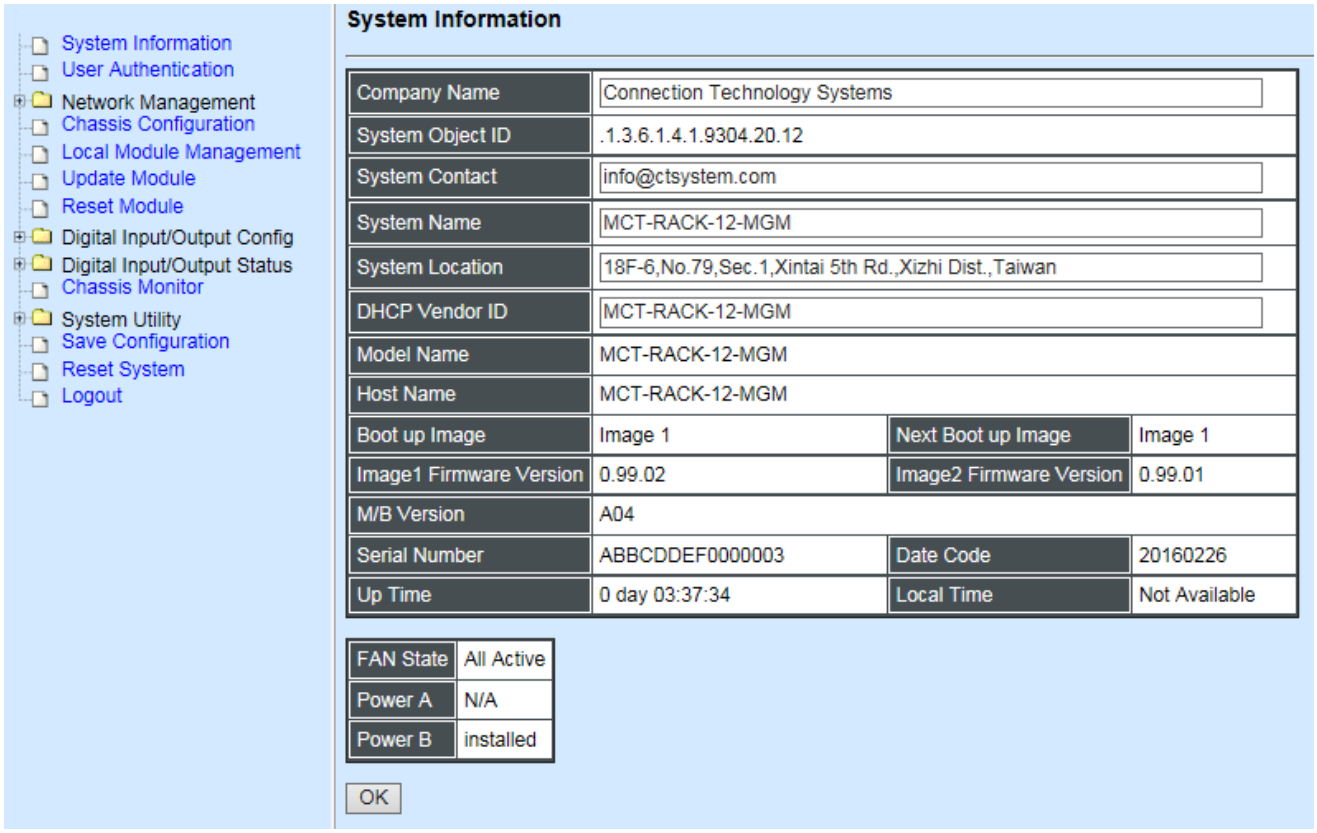
After a successful login, the Main Menu screen shows up. The menu functions in the Web Management are similar to those described at the Console Management and are also described below.



1. **System Information:** Name the CHASSIS, specify the location and check the current version information.
2. **User Authentication:** View the registered user list. Add a new user or remove an existing user.
3. **Network Management:** Set up or view the required IP address and related information of the CHASSIS for network management application.
4. **Local Module Management:** Set up CHASSIS local module's port configuration, bandwidth control, QoS priority, VLAN Configuration and other functions.
5. **Reset Module:** Reset the local and remote module.
6. **CHASSIS Monitor:** Display local and remote module state.
7. **System Utility:** View Event Log, Load Factory Settings …etc.
8. **Save Configuration:** Save all changes to the system.
9. **Reset System:** Reset the CHASSIS.
10. **Logout:** Logout the system.

4.1 System Information

Click **System Information** from **Main Menu**, then the **System Information** page shows up.



Company Name: Enter a company name for this CHASSIS of up to 55 alphanumeric characters.

System Object ID: View only field that shows the predefined System OID.

System Contact: Enter the contact information for this CHASSIS of up to 55 alphanumeric characters.

System Name: Enter the unique name of this CHASSIS of up to 55 alphanumeric characters. Use a descriptive name to identify the CHASSIS in relation to your network, for example “Backbone Rack 1”. This name is mainly used for reference purpose only.

System Location: Enter a brief description of the CHASSIS location of up to 55 alphanumeric characters. The location is for reference only, for example “13th Floor”.

DHCP Vendor ID: Enter the Vendor ID used for DHCP relay agent function.

Model Name: View-only field that shows the product model name.

Host Name: Display the product’s host name.

Boot up image: The first image used for boot up.

Next Boot up image: The second image used for boot up.

Image1 Firmware Version: Display the firmware version 1 (image-1) used in this device.

Image2 Firmware Version2: Display the firmware version 2 (image-2) used in this device.

M/B Version: Display the main board version.

Serial Number: View-only field that shows the product's serial number

Date Code: Display the CHASSIS Firmware date code.

Up Time: View-only field that shows how long the CHASSIS has been up**.**

Local Time: View-only field that shows the local time of the device.

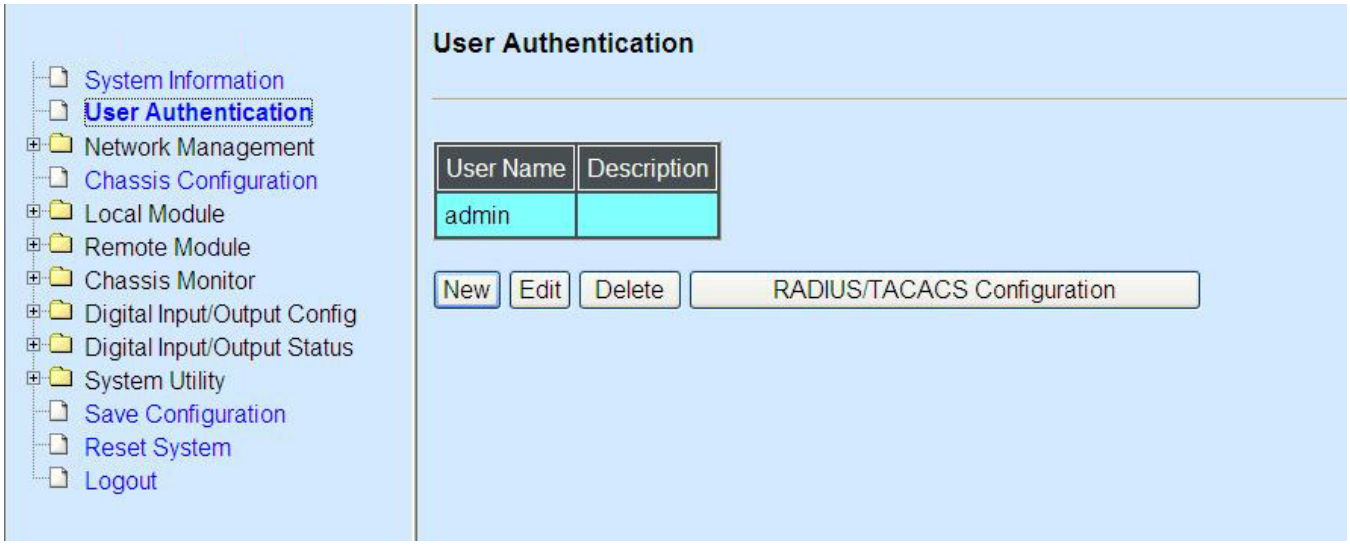
Fan State: View-only field that shows the fans' current status.

Power A / B: View-only field that shows the status of power.

4.2 User Authentication

To prevent any un-authorized operation, only registered users are allowed to operate the CHASSIS. Users who want to access and operate the CHASSIS need to register into the users list first.

To view or change current registered users, select **User Authentication** from **Main Menu**, then the **User Authentication** page shows up.

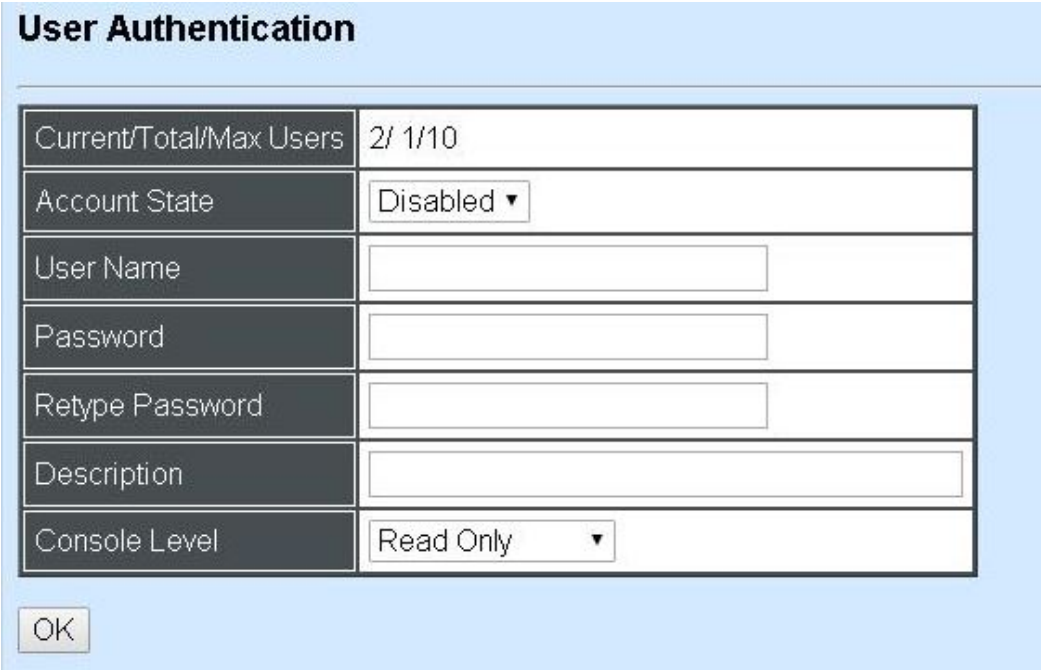


Click **New** to add a new user and then the following screen page appears. Up to 10 users can be registered.

Click **Edit** to modify a registered user's settings.

Click **Delete** to remove the selected registered user from the user list.

Click **RADIUS/TACACS Configuration** for authentication setting via RADIUS/TACACS+. For more details on these settings, please refer to Section 4.2.1.



Current/Total/Max Users: View-only field.

Current: This shows the number of current registered user.

Total: This shows the amount of total users who have already registered.

Max: This shows the maximum number available for registration. The maximum number is 10.

Account State: Enable or disable this user account.

User Name: Specify the authorized user login name. Up to 20 alphanumeric characters can be accepted.

Password: Enter the desired user password. Up to 20 alphanumeric characters can be accepted.

Retype Password: Enter the password again for double-checking.

Description: Enter a unique description for this user. Up to 35 alphanumeric characters can be accepted. This is mainly used for reference only.

Console Level: Select the desired privilege level for the management operation from the pull-down menu. Three operation levels of privilege are available in the CHASSIS.

Administrator: Own the full-access right. The user can maintain user account as well as system information, load the factory default settings, and so on.

Read & Write: Own the partial-access right. The user is unable to modify user account, system information and items under System Utility menu.

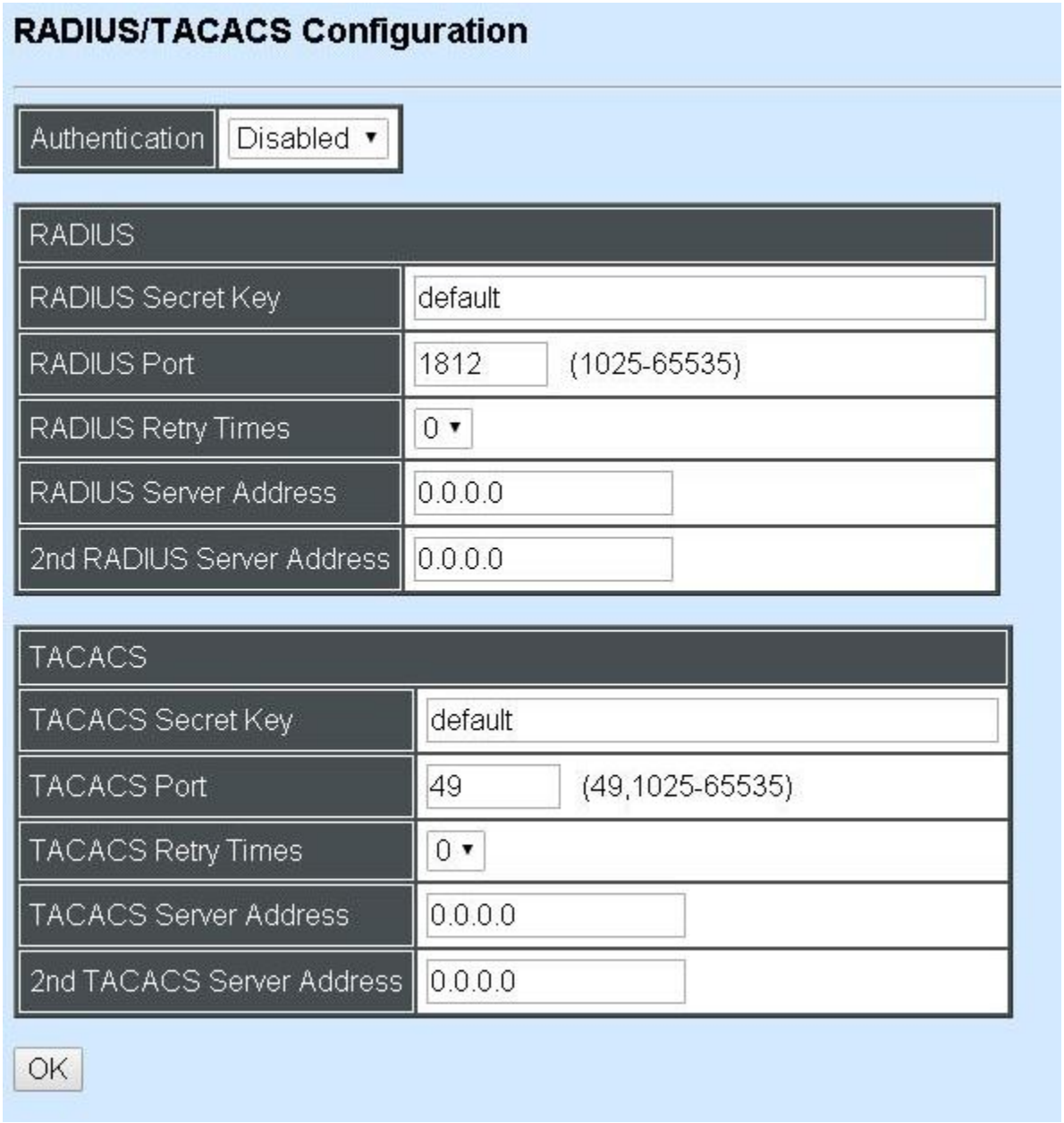
Read Only: Allow to view only.

NOTE:

1. To prevent incautious operations, users cannot delete their own account, modify their own user name and change their own account state.

4.2.1 RADIUS/TACACS+ Configuration

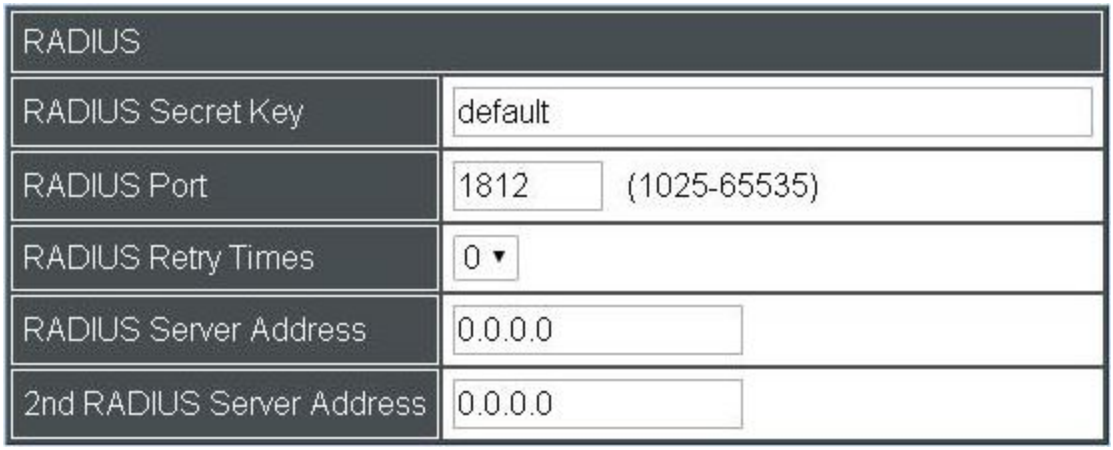
Click **RADIUS/TACACS Configuration** in the User Authentication webpage and then the following screen page appears.



Authentication: From the **Authentication** pull-down menu, you can choose **RADIUS** or **TACACS** option to respectively enable authentication via RADIUS or TACACS+. To disable the authentication, just select **Disabled** option from this menu.

When **RADIUS Authentication** is selected, the user login will be upon those settings on the RADIUS server(s).

NOTE: *For advanced RADIUS Server setup, please refer to APPENDIX B or the "free RADIUS readme.txt" file on the disc provided with this product.*



RADIUS Secret Key: The word to encrypt data of being sent to RADIUS server.

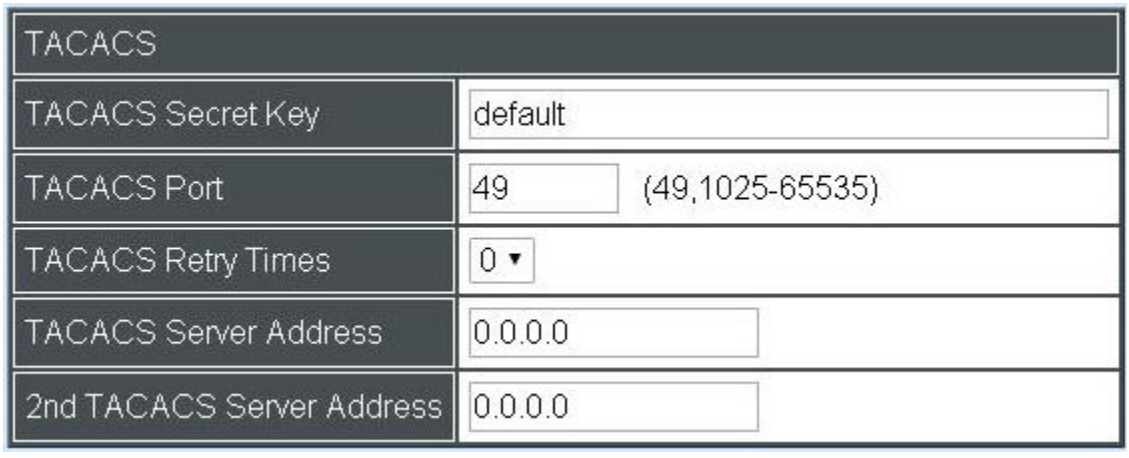
RADIUS Port: The RADIUS service port on RADIUS server.

RADIUS Retry Times: Times of trying to reconnect if the RADISU server is not reachable.

RADIUS Server Address: IPv4 address of the primary RADIUS server.

2nd RADIUS Server Address: IPv4 address of the secondary RADIUS server.

When **TACACS Authentication** is selected, the user login will be upon those settings on the TACACS server(s).



TACACS Secret Key: The word to encrypt data of being sent to TACACS server.

TACACS Port: The TACACS service port on TACACS server.

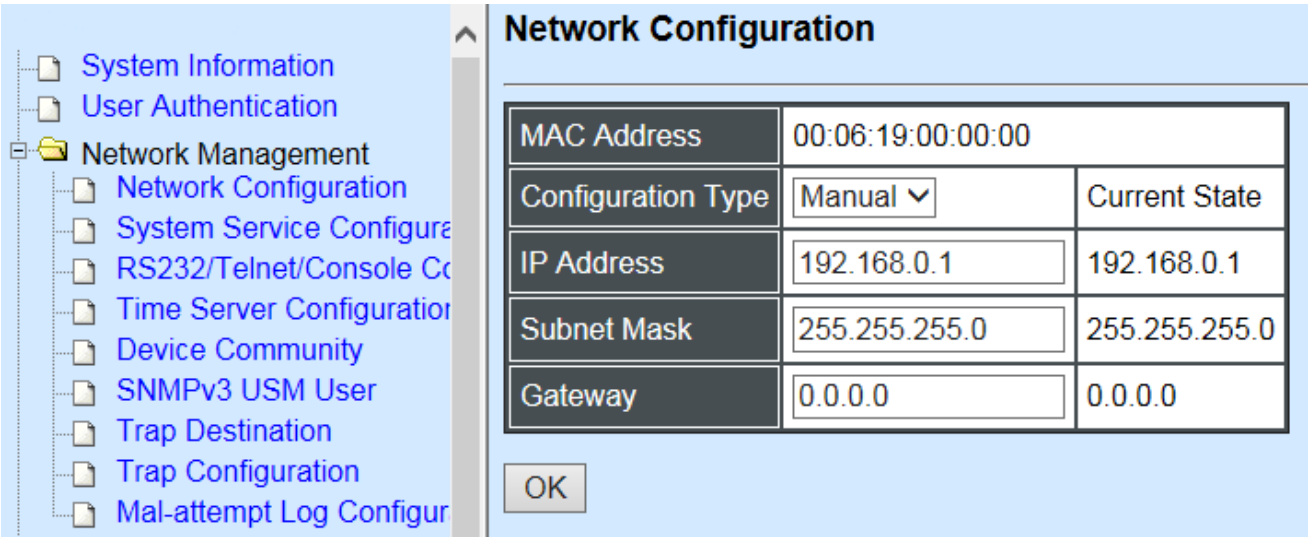
TACACS Retry Times: Times of trying to reconnect if the TACACS server is not reachable.

TACACS Server Address: IPv4 address of the primary TACACS server.

2nd TACACS Server Address: IPv4 address of the secondary TACACS server.

4.3 Network Management

In order to enable the network management of the CHASSIS, a proper network configuration is required. Click the folder **Network Management**, then **Network Management** sub-folders show up.



1. **Network Configuration:** Set up the required IP configuration of the CHASSIS.

2. **System Service Configuration:** Enable or disable the specified network services.

3. **RS232/Telnet/Console Configuration:** View the RS-232 port setting, and the specified Telnet & Console services.

4. **Time Server Configuration:** Set up the time server's configuration

5. **Device Community:** View the registered SNMP community name list. Add a new community name or remove an existing community name.

6. **SNMPv3 USM User:** View the registered SNMPv3 user name list. Edit an existing user name.

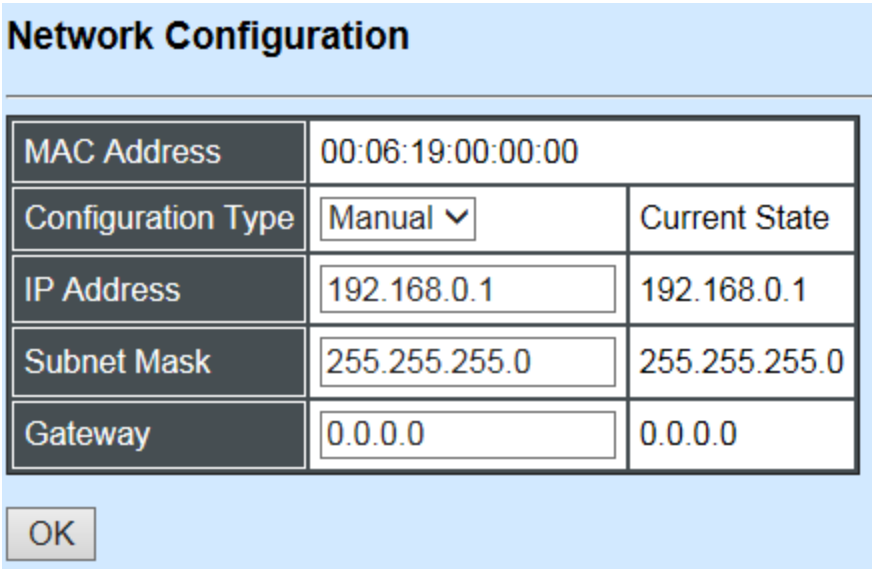
7. **Trap Destination:** View the registered SNMP trap destination list. Add a new trap destination or remove an existing trap destination.

8. **Trap Configuration:** View the CHASSIS trap configuration. Enable or disable a specified trap.

9. **Mal-attempt Log Configuration:** Set up the Mal-attempt Log server's configuration.

4.3.1 Network Configuration

Select the option **Network Configuration** from the **Network Management** menu, then the **Network Configuration** page shows up.



MAC Address: This view-only field shows the unique and permanent MAC address assigned to the CHASSIS. You cannot change the MAC address of your CHASSIS.

Configuration Type: There are two configuration types that users can select from the pull-down menu; these are "**DHCP**" and "**Manual**". When "**DHCP**" is selected and a DHCP server is also available on the network, the CHASSIS will automatically get the IP address from the DHCP server. If "**Manual**" is selected, users need to specify the IP address, Subnet Mask and Gateway.

IP Address: Enter the unique IP address of this CHASSIS. You can use the default IP address or specify a new one when the situation of address duplication occurs or the address does not match up with your network. (The default factory setting is 192.168.0.1.)

Subnet Mask: Specify the subnet mask. The default subnet mask values for the three Internet address classes are as follows:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

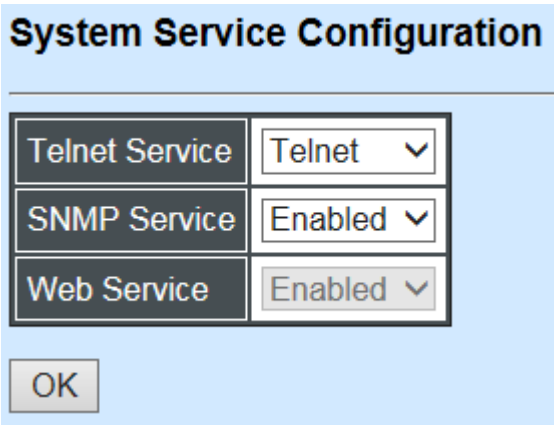
Gateway: Specify the IP address of a gateway or a router, which is responsible for the delivery of the IP packets sent by the CHASSIS. This address is required when the CHASSIS and the network management station are on different networks or subnets. The default value of this parameter is 0.0.0.0, which means no gateway exists and the network management station and CHASSIS are on the same network.

Current State: This View-only field shows currently assigned IP address (by DHCP or manual), Subnet Mask and Gateway of the CHASSIS.

NOTE: *This Wireless Gateway also supports DHCP auto-provisioning function that enables DHCP clients to automatically download the latest Firmware and Configuration image. For information about how to set up a DHCP server, please refer to Appendix A.*

4.3.2 System Service Configuration

Select the option **System Service Configuration** from the **Network Management** menu, then the **System Service Configuration** screen page shows up.



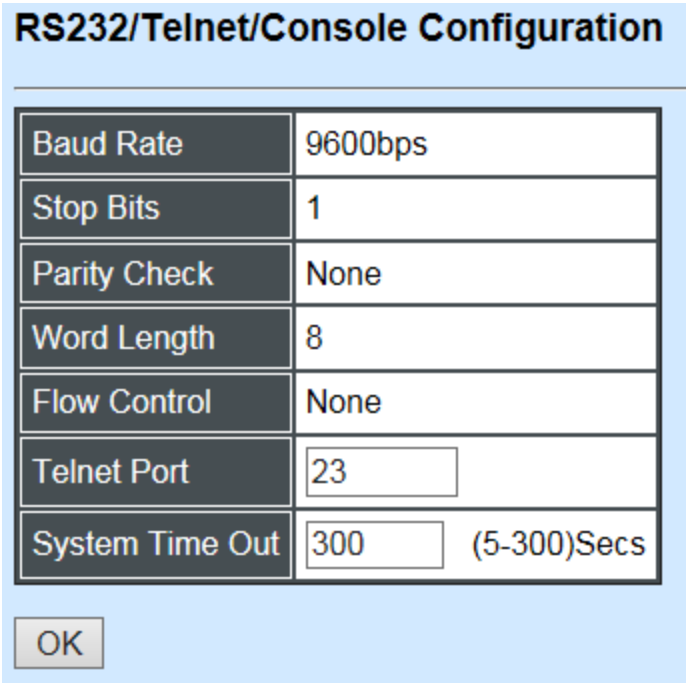
Telnet Service: To enable or disable the Telnet Management service.

SNMP Service: To enable or Disable the SNMP Management service.

Web Service: To enable or Disable the Web Management service.

4.3.3 RS232/Telnet/Console Configuration

Select the option **RS232/Telnet/Console Configuration** from the **Network Management** menu, then the **RS232/Telnet/Console Configuration** screen page shows up.



Baud Rate: 9600 bps, RS-232 setting, view-only field.

Stop Bits: 1, RS-232 setting, view-only field.

Parity Check: None, RS-232 setting, view-only field.

Word Length: 8, RS-232 setting, view-only field.

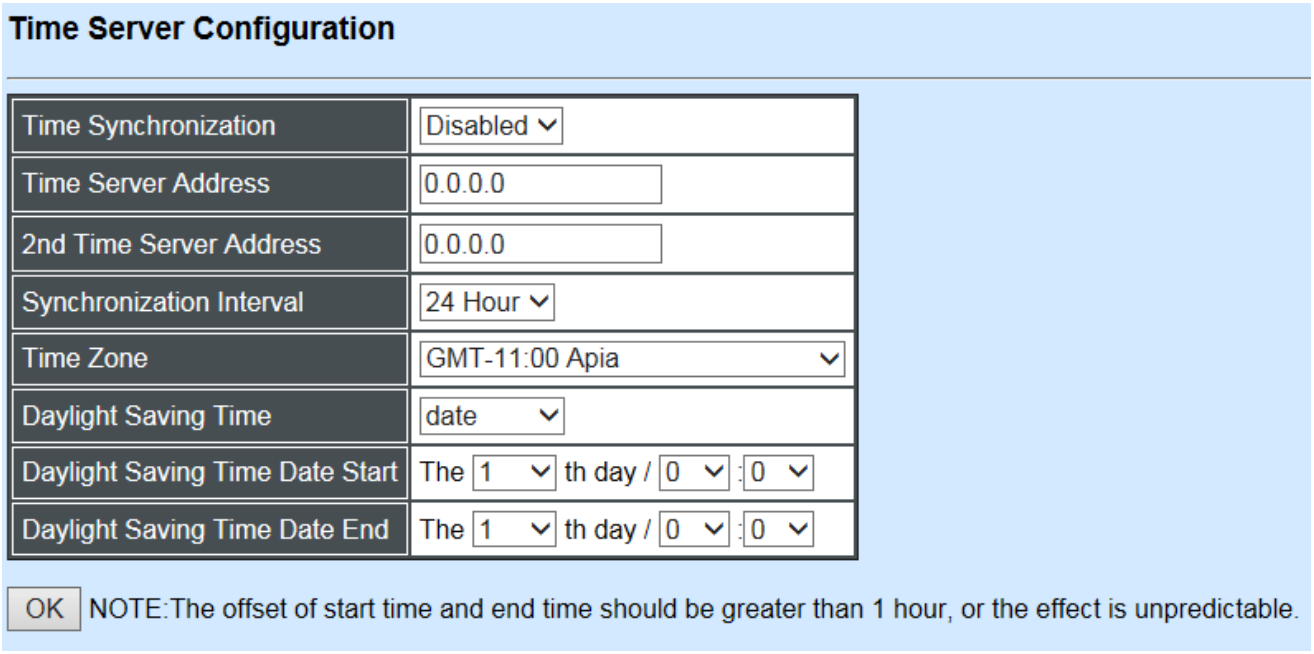
Flow Control: None, RS-232 setting, view-only field.

Telnet Port: Specify the desired TCP port number for the Telnet console. The default TCP port number of the Telnet is 23.

System Time Out: Specify the desired time that the CHASSIS will wait before disconnecting an inactive console/telnet. Specifying “0” means an inactive connection will never be disconnected.

4.3.4 Time Server Configuration

Select the option **Time Server Configuration** from the **Network Management** menu, then the **Time Server Configuration** screen page shows up.



Time Synchronization: To enable or disable time synchronization.

Time Server Address: NTP time server address.

2nd Time Server Address: When the default time server is down, the CHASSIS will automatically connect to the 2nd time server.

Synchronization Interval: The time interval to synchronize from NTP time server.

Time Zone: Select the appropriate time zone from the pull-down menu.

Daylight Saving Time: To enable or disable the daylight saving time function. It is a way of getting more daytime hour(s) by setting the time to be hour(s) ahead in the morning.

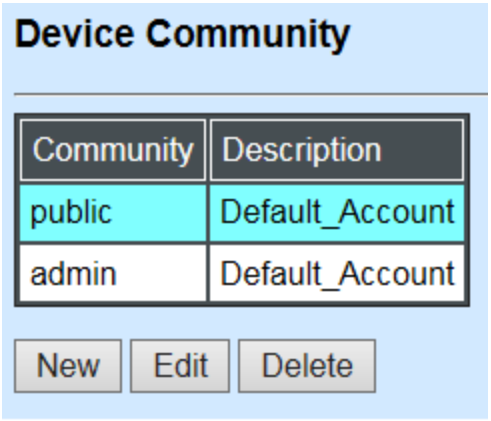
Daylight Saving Time Date Start: Click the pull-down menu to select the start date of daylight saving time.

Daylight Saving Time Date End: Click the pull-down menu to select the end date of daylight saving time.

NOTE: *We use SNTP to get the time from those NTP servers. It is recommended that the time server is in the same LAN with the CHASSIS or at least not too far away. In this way, the time will be more accurate.*

4.3.5 Device Community

Select the option **Device Community** from the **Network Management** menu, then the **Device Community** page shows up.

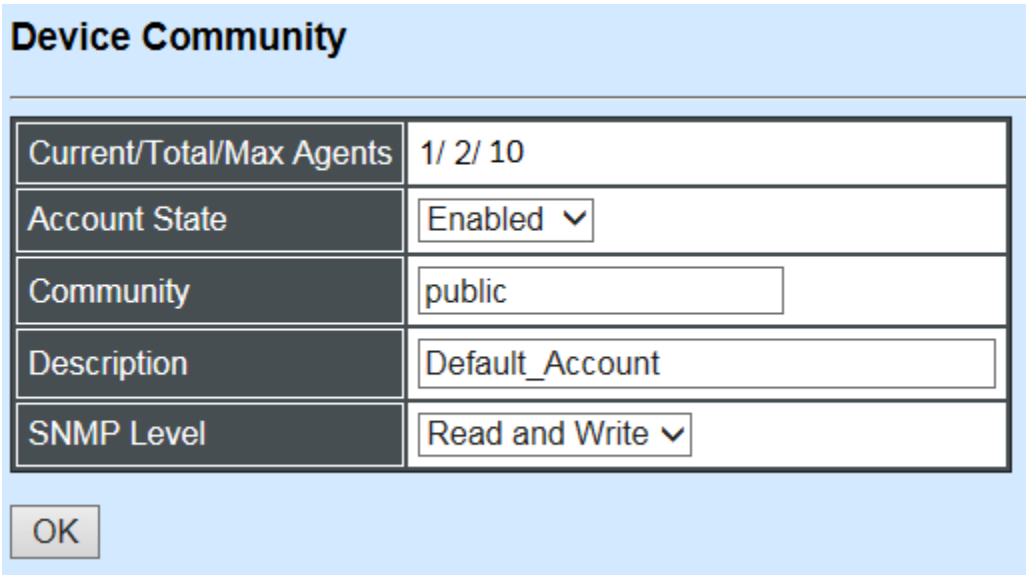


Up to 10 Device Communities can be set up.

Click **New** to add a new community and then the following screen page appears.

Click **Edit** to view the current community settings.

Click **Delete** to remove a registered community.



Current/Total/Max Agents: View-only field.

Current: This shows the number of currently registered communities.

Total: This shows the number of total registered community users.

Max Agents: This shows the number of maximum number available for registration. The default maximum number is 10.

Account State: Enable or disable this Community Account.

Community: Specify the authorized SNMP community name, up to 20 alphanumeric characters.

Description: Enter a unique description for this community name, up to 35 alphanumeric characters. This is mainly for reference only.

SNMP Level: Click the pull-down menu to select the desired privilege for the SNMP operation.

Administrator: Full access right including maintaining user account & system information, load factory settings …etc.

Read & Write: Full access right but cannot modify user account & system information, cannot load factory settings.

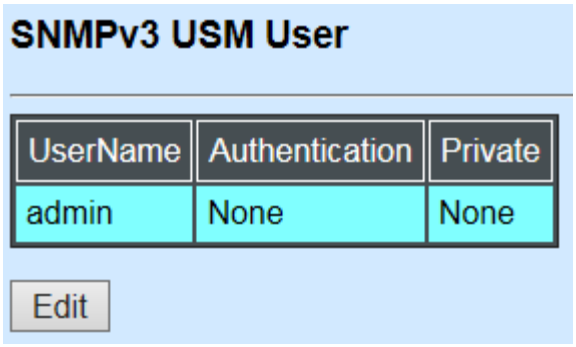
Read Only: Allow to view only.

NOTE: *When the community accesses the CHASSIS without proper access right, the CHASSIS will respond nothing. For example, if a community only has Read & Write privilege, then it cannot browse the CHASSIS's user table.*

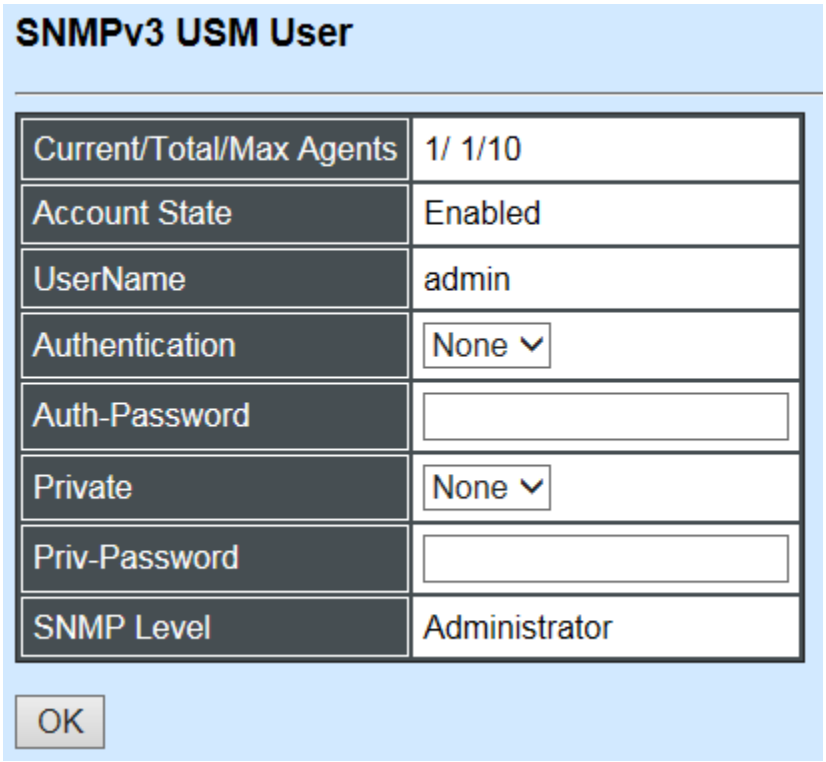
4.3.6 SNMPv3 USM User

Simple Network Management Protocol Version 3, SNMPv3 in short, features stronger security mechanism, including authentication and encryption that helps ensure that the message is from a valid source and scramble the content of a packet, to prevent from being learned by an unauthorized source. Select the option SNMPv3 USM User from the **Network Management** menu, then the **SNMPv3 USM User** page shows up.

Note: *The SNMPv3 user account is generated from "User Authentication" (Section 4.2)*



Click **"Edit"** for further settings.



Current/Total/Max Agents: View-only field.

Current: This shows the number of currently registered communities.

Total: This shows the number of total registered community users.

Max Agents: This shows the number of maximum number available for registration. The default maximum number is 10.

Account State: View-only field that shows this user account is enabled or disabled.

User Name: View-only field that shows the authorized user login name.

Authentication: This is used to ensure the identity of users. The following is the method to perform authentication.

None: Disable authentication function. Click "None" to disable it.

MD5(Message-Digest Algorithm): A widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. Click "MD5" to enable authentication.

SHA(Secure Hash Algorithm): A 160-bit hash function which resembles the said MD5 algorithm. Click "SHA" to enable authentication.

Auth-Password: Specify the passwords, up to 20 characters.

Private: It allows for encryption of SNMP v3 messages to ensure confidentiality of data. The following is the method to perform encryption.

None: Disable Private function. Click "None" to disable it.

DES(Data Encryption Standard): An algorithm to encrypt critical information such as message text message signatures…etc. Click "DES" to enable it.

Priv-Password: Specify the passwords, up to 20 characters.

SNMP-Level: View-only field that shows user's authentication level.

Administrator: Full access right including maintaining user account & system information, load factory settings …etc.

Read & Write: Full access right but cannot modify user account & system information, cannot load factory settings.

Read Only: Allow to view only.

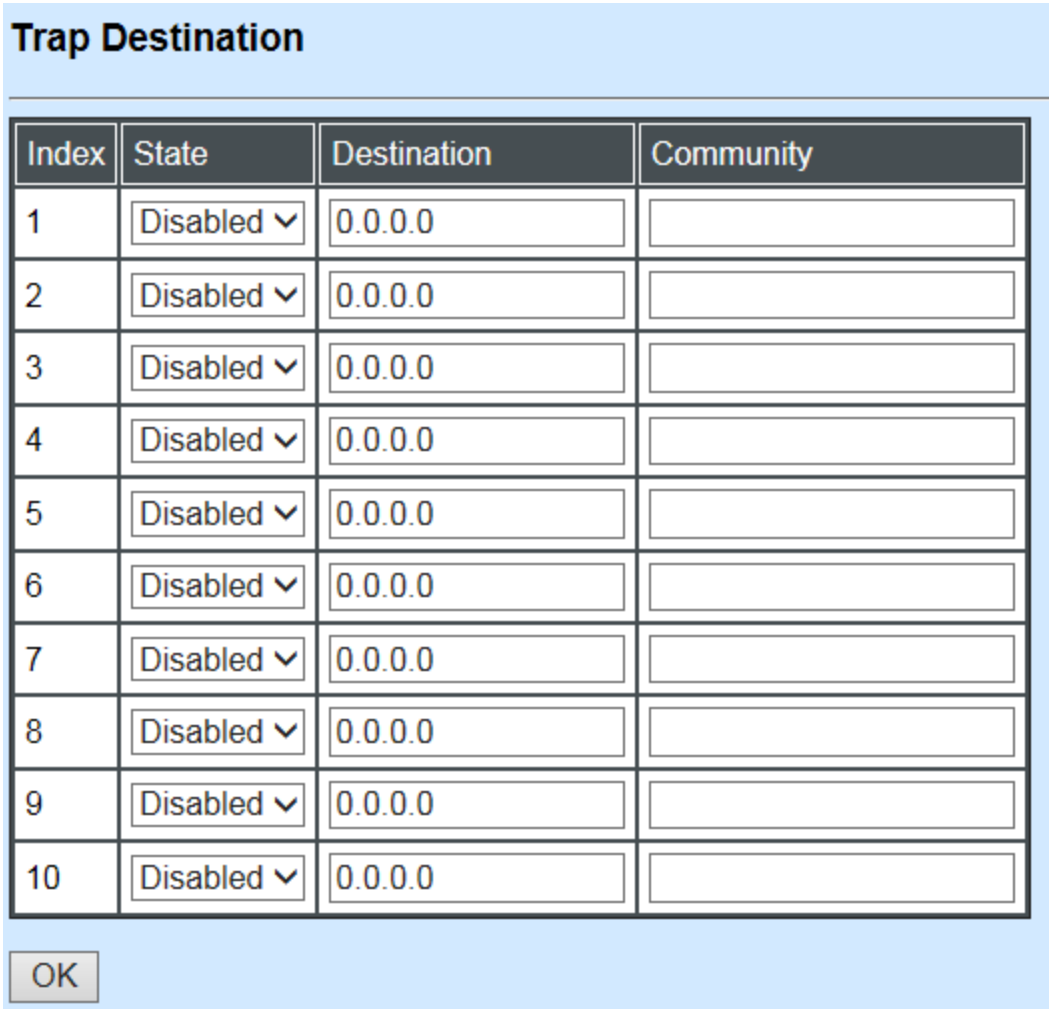
A combination of a security event as below indicates which security mechanism is used when handling an SNMP packet.

Authentication	Private	Result
None	None	Uses a username match for authentication
Message Digest Algorithm(MD5) or	None	Provides authentication based on the Hashed Message

Secure Hash Algorithm(SHA)		Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms.
MD5 or SHA	Data Encryption Standard(DES)	Provides authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms. What's more, provides DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES standard.

4.3.7 Trap Destination

Select the option **Trap destination** from the **Network Management** menu, then the **Trap Destination** screen page shows up.



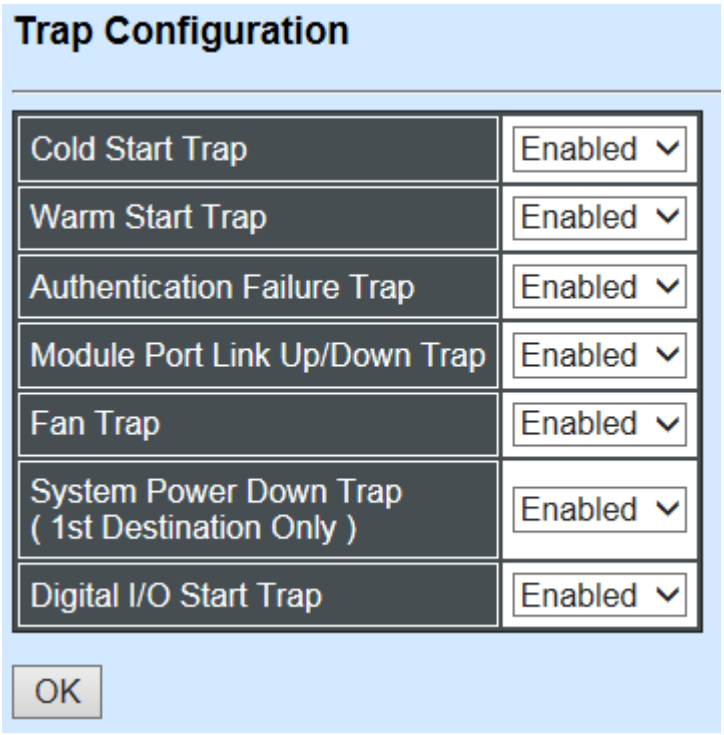
State: Enable or disable the function of sending trap to the specified destination.

Destination: Enter the specific IP address of the network management system that will receive the trap.

Community: Enter the community name of the network management system.

4.3.8 Trap Configuration

Select the option **Trap Configuration** from the **Network Management** menu, then the **Trap Configuration** screen page shows up.



Cold Start Trap: Enable or disable the CHASSIS to send the cold start trap.

Warm Start Trap: Enable or disable the CHASSIS to send a trap after a system reset.

Authentication Failure Trap: Enable or disable the CHASSIS to send the Authentication Failure trap when any unauthorized login attempts are made.

Module Port Link Up/Down Trap: Enable or disable the CHASSIS to send the module port link up/down traps.

Fan Trap: Enable or disable the CHASSIS to send a trap when the fan is not working.

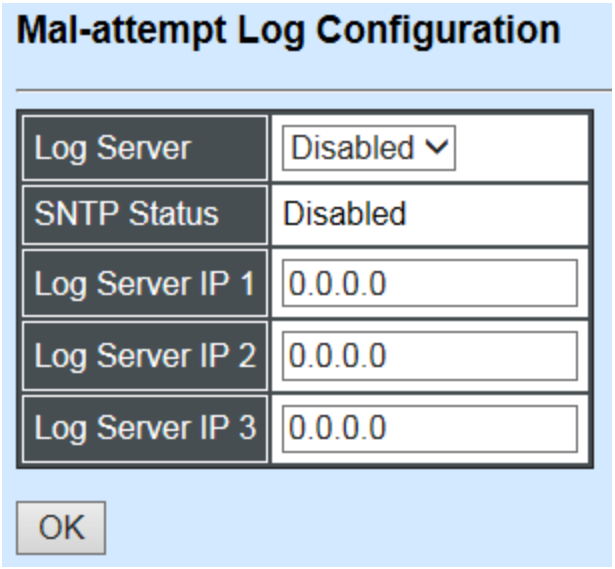
System Power Down Trap (the 1st destination only): Enable or disable the port power-down trap notice sending.

Digital I/O Start Trap: Select Disabled or Enabled for the SNMP trap.

Click the **"OK"** button to apply the settings.

4.3.9 Mal-attempt Log Configuration

Click the option **Mal-attempt Log Configuration** from the **Network Management** menu and then the following screen page appears.



When DHCP snooping filters unauthorized DHCP packets on the network, the Mal-attempt log will allow the CHASSIS to send event notification message to Log server.

Log Server: Enable or disable Mal-attempt log function.

SNTP Status: View-only field that shows the SNTP server status.

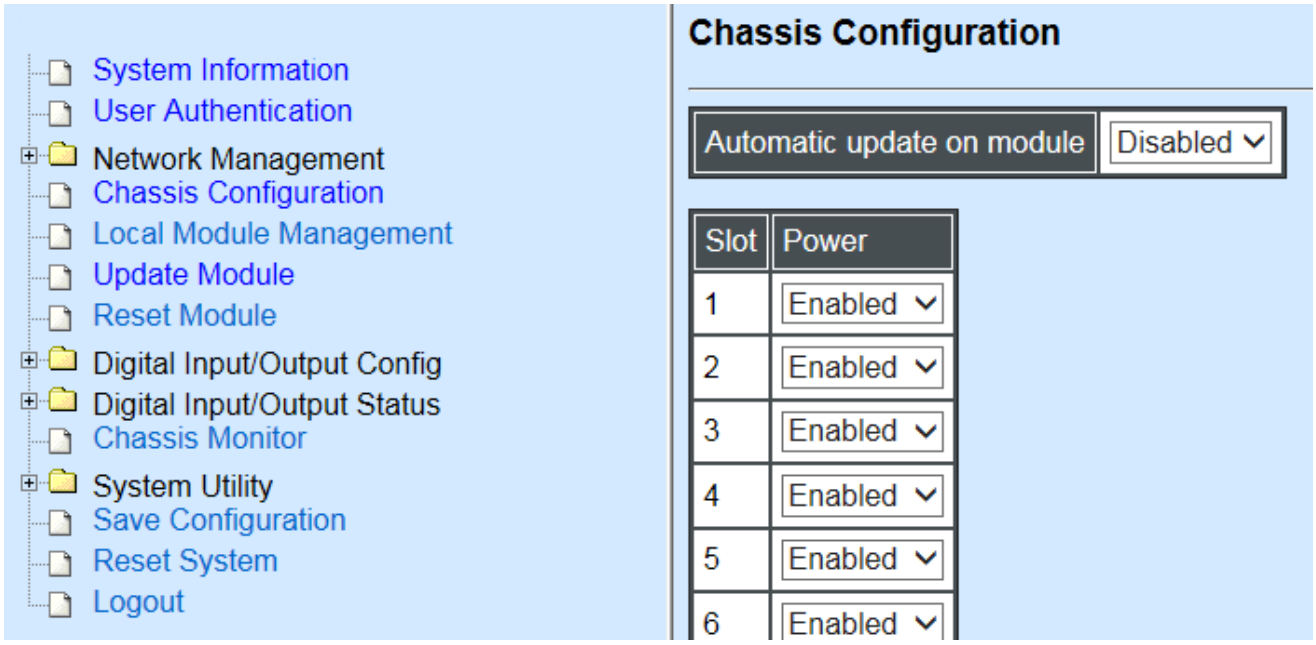
Log Server IP 1: Specify the default Log server IP address.

Log Server IP 2: Specify the second Log server IP address. When the default Log Server is down, the CHASSIS will automatically contact the second or third Log server.

Log Server IP 3: Specify the third Log server IP address. When the default Log Server is down, the CHASSIS will automatically contact the second or third Log server.

4.4 Chassis Configuration

This section is to set up power through web interface. Select the option **Chassis Configuration** from **Main Menu**, then **Chassis Configuration** screen page shows up.



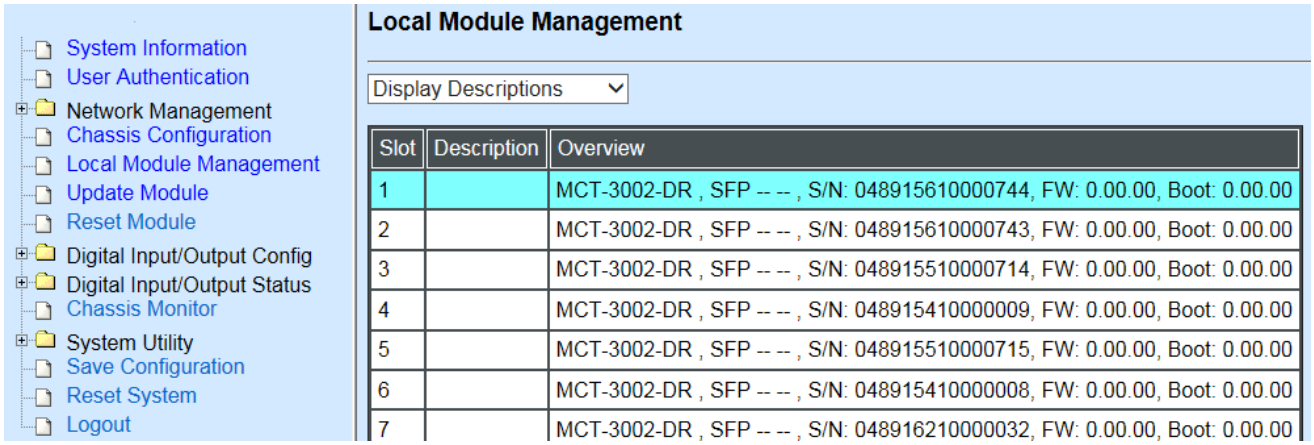
Automatic update on module: Click drop-down box to enable or disable automatic update on module. The Chassis will update media converter automatically once enabling it.

Click drop-down box to enable or disable power supply on a corresponding slot.

Click “OK” to apply.

4.5 Local Module Management

In order to manage the installed converters and set up required functions, select the option **Local Module Management** from **Main Menu**, then **Local Module Management** screen page shows up.



Overview: Shows product information.

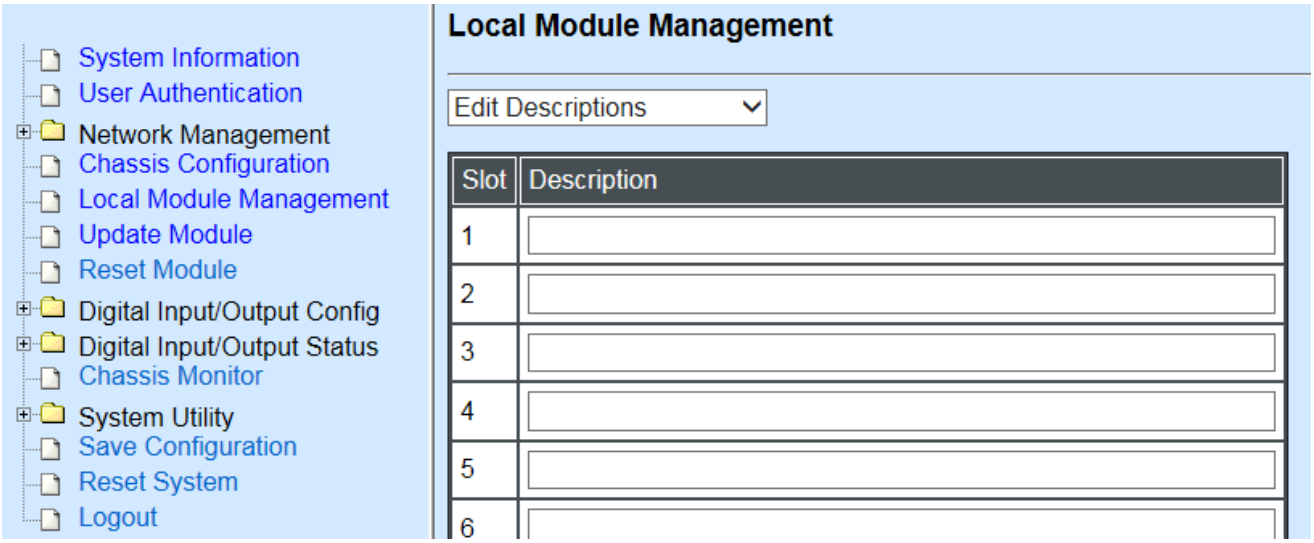
Description: Shows the user-specified message.

The drop-down box is to edit or show the message you specify. There are three options:

Not Display Descriptions: Hide the user-specified message.

Display Descriptions: Show up the user-specified message.

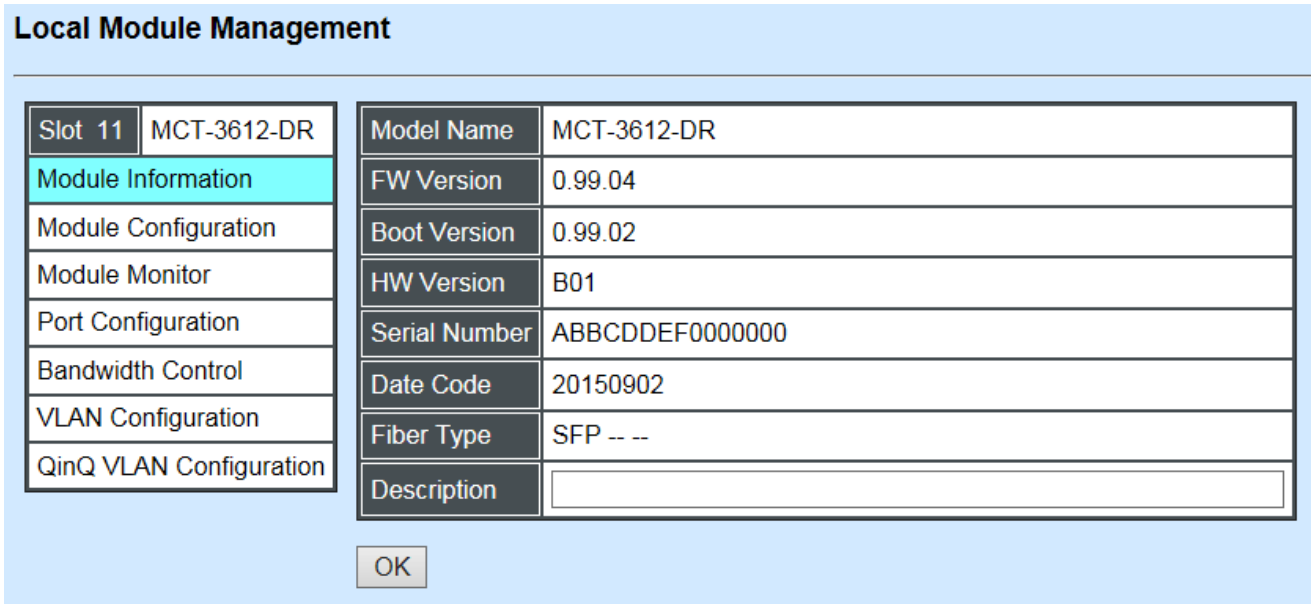
Edit Descriptions: Change the user-specified message.



To edit description, click drop-down box and select **Edit Descriptions**.

Click "**OK**" to save edited message.

Click on the available modules and then the following screen page appears.



Module Information: Display vender Name, model name, H/W Version, serial Number, Fiber Type, Wavelength information**.**

Module Configuration: Set up Link Alarm function.

Module Monitor: Display information about Media Type, Port State, Link State, Auto-Negotiation status, Speed, Duplex, Flow Control.

Port Configuration: Set up Media Type, Port State, Port Type, Port Speed, Duplex, Flow, Control, MDI/MDIX, Link Path Through, Power State, Egress PPPoE Only.

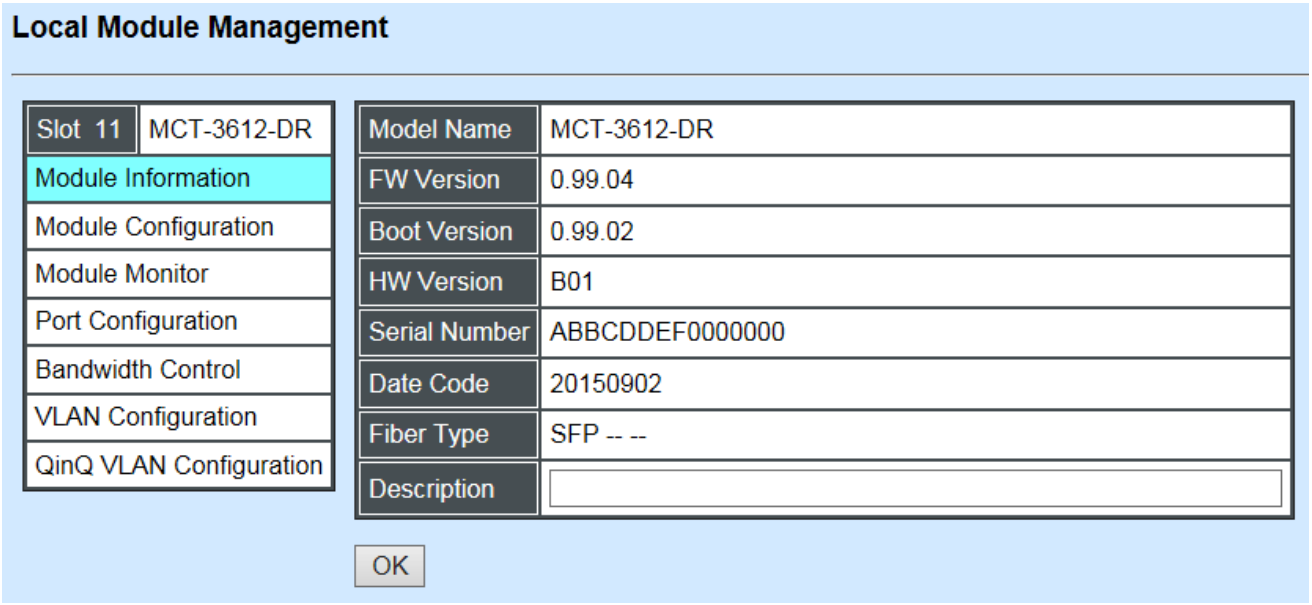
Bandwidth Control: Set up Egress Rate Limit, Broadcast Storm Blocking.

VLAN Configuration: Set up TP/FX default PVID, Egress Mode.

Firmware Upgrade: Upgrade the current firmware version.

4.5.1 Module Information

Select the option **Module Information** from the **Local Module Management** menu, then the **Module Information** fields show up on the right to provide you information about the module.



Vender Name: View-only field that shows the product's vender name.

Model Name: View-only field that shows the product's model name.

FW Version: View-only field that shows the product's firmware version.

HW Version: View-only field that shows the product's hardware version.

Serial Number: View-only field that shows the product's serial number.

Date Code: View-only field that shows the date of EEPROM burned.

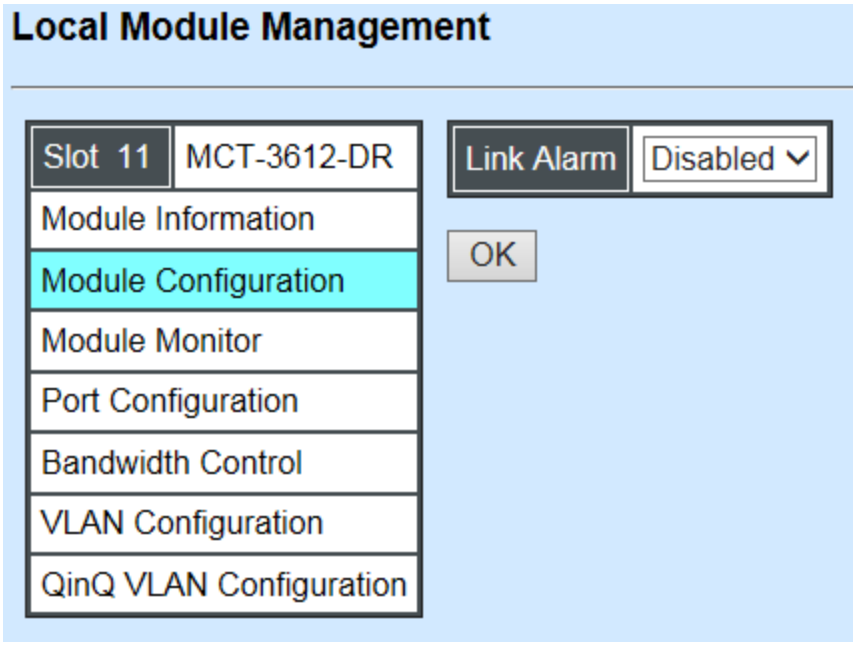
Fiber Type: View-only field that shows the product's fiber connector type, speed, and distance.

Description: Specify the appropriate brief description for the slide-in converter module.

4.5.2 Module Configuration

Select the option **Module Configuration** from the **Local Module Management** menu, then **Module Configuration** fields show up on the right to let you view the configuration of the converter.

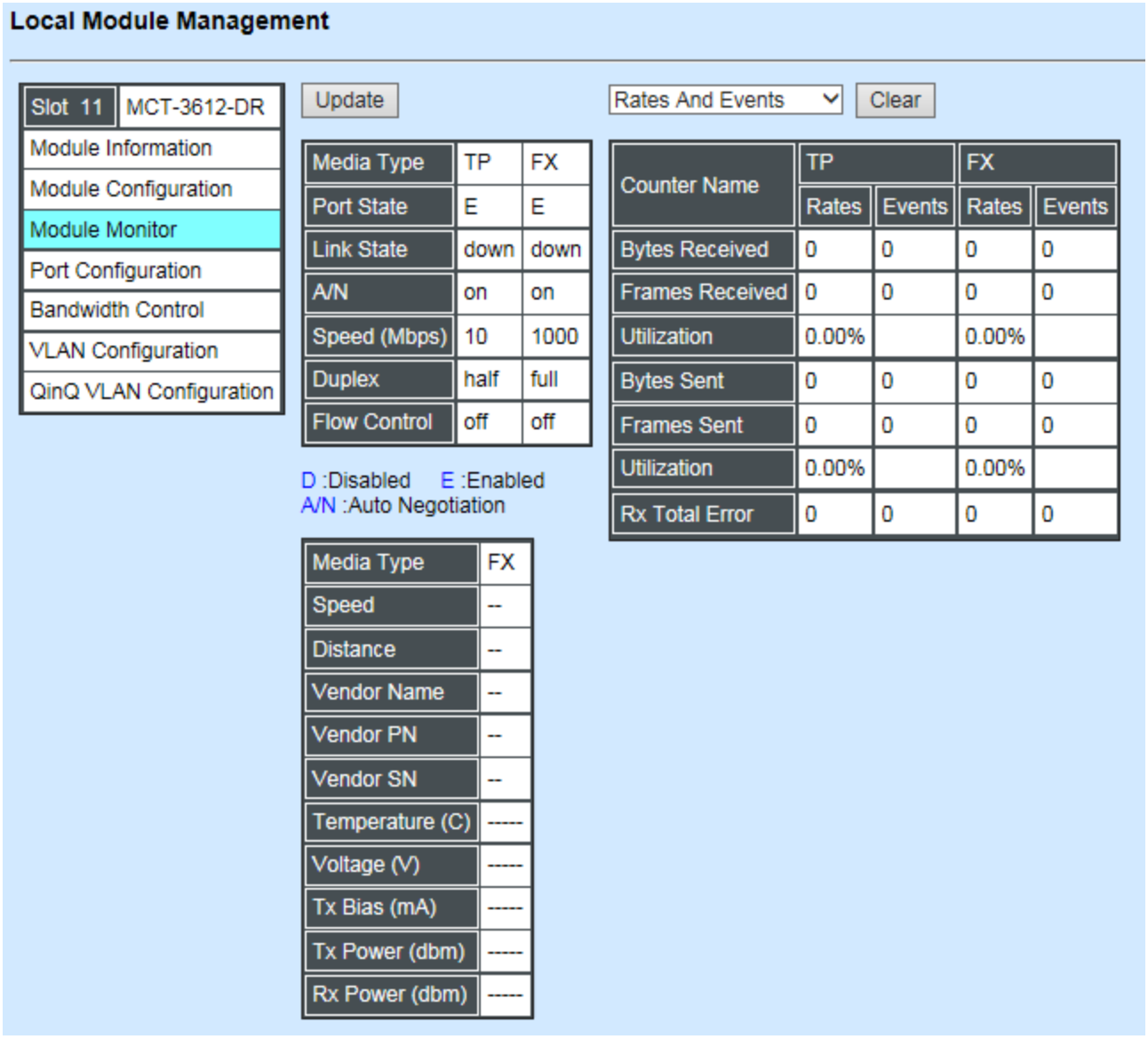
Link Alarm: This function is used under the circumstance that when UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.



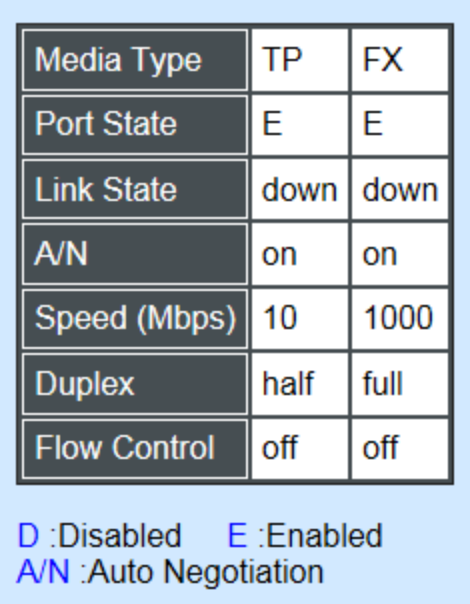
Click the drop-down box to enable or disable link alarm of the converter.

4.5.3 Module Monitor

Select the option **Module Monitor** from the **Local Module Management** menu, then **Module Monitor** fields show up on the right to let you view the configuration of the module.



Port Status



Media Type	TP	FX
Port State	E	E
Link State	down	down
A/N	on	on
Speed (Mbps)	10	1000
Duplex	half	full
Flow Control	off	off

D :Disabled E :Enabled
A/N :Auto Negotiation

Media Type: TP (copper, 10/100Base-T, RJ-45) and FX (fiber).

Port State: View-only field that shows traffic is Disabled or Forwarding.

Link State: View-only field that shows the link is up or down.

A/N: View-only field that shows Auto-negotiation is on or off.

Speed: View-only field that shows the port speed.

Duplex: View-only field that shows the duplex mode is half or full.

Flow Control: View-only field that shows the flow control is on or off.

SFP Status

Media Type	FX
Speed	--
Distance	--
Vendor Name	--
Vendor PN	--
Vendor SN	--
Temperature (C)	-----
Voltage (V)	-----
Tx Bias (mA)	-----
Tx Power (dbm)	-----
Rx Power (dbm)	-----

Media Type: Shows the type of FX (fiber).

Speed: Data rate of the slide-in SFP Transceiver.

Distance: Transmission distance of the slide-in SFP Transceiver.

Vendor Name: Vendor name of the slide-in SFP Transceiver.

Vendor PN: Vendor PN of the slide-in SFP Transceiver.

Vendor SN: Vendor SN of the slide-in SFP Transceiver.

Temperature (C): The Slide-in SFP module operation temperature.

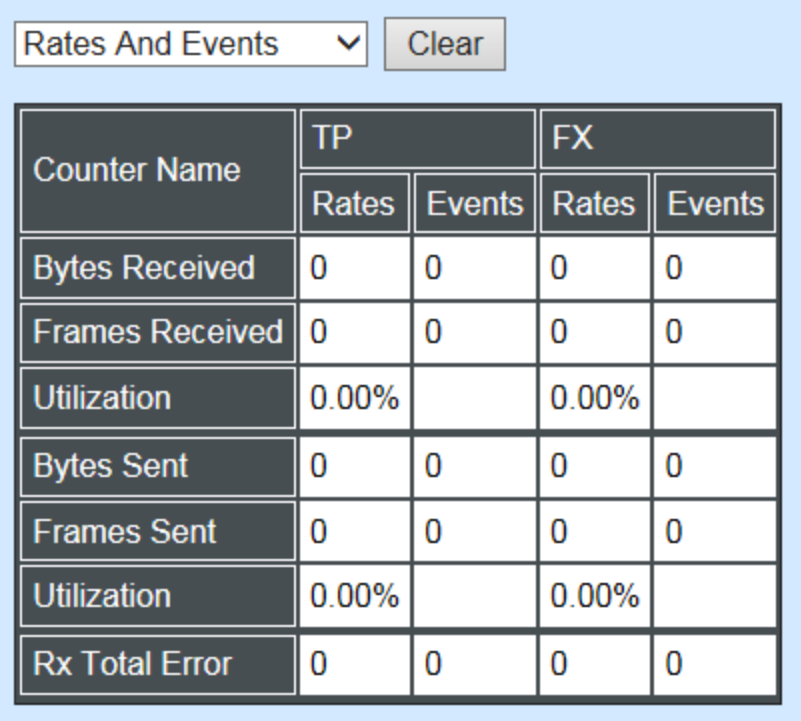
Voltage (V): The Slide-in SFP module operation voltage.

TX Bias (mA): The Slide-in SFP module operation current.

TX Power (dbm): The Slide-in SFP module optical Transmission power.

RX Power (dbm): The Slide-in SFP module optical Receiver power.

Select **"Rates and Events"** option from the Counters Display pull-down menu to view the detailed traffic statistics (counters' information).



Rates: Counters displayed and updated once per second.

Events: The count is cumulative (i.e. cumulated count).

Bytes Received: The total number of bytes received from this port.

Frames Received: The total number of frames received from this port.

Utilization: The utilization of receiving bandwidth from this port.

Bytes Sent: The total number of bytes sent from this port.

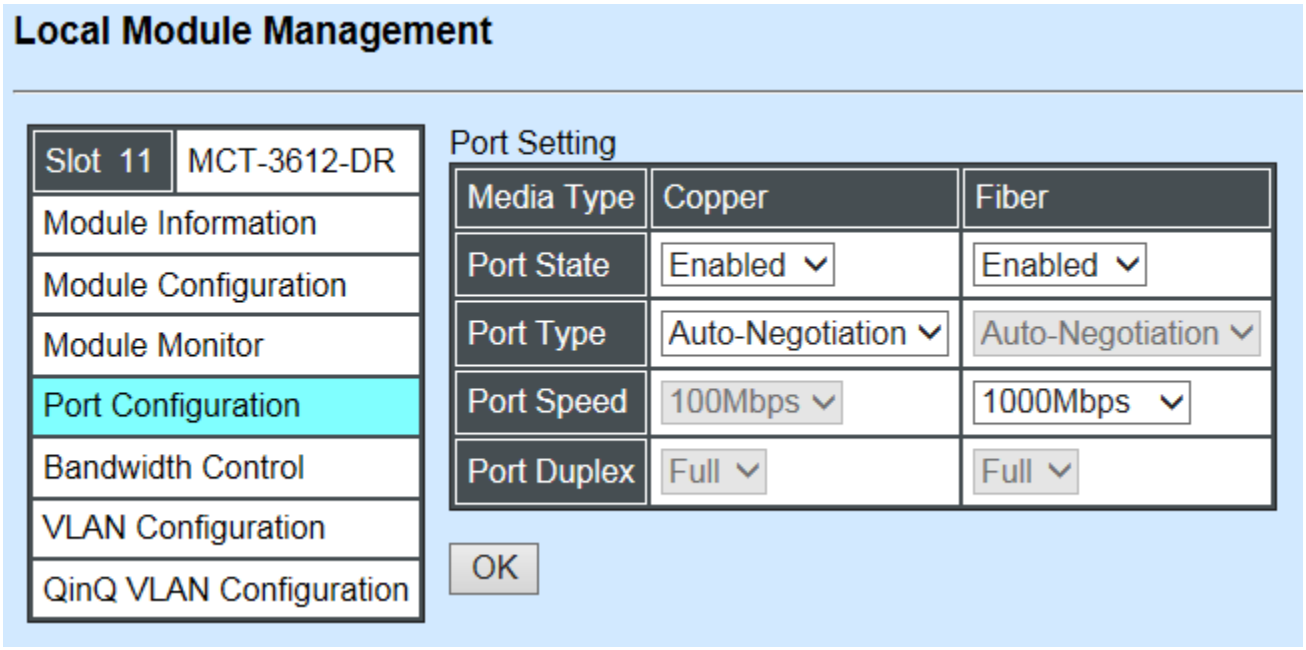
Frames Sent: The total number of frames sent from this port.

Utilization: The utilization of sending bandwidth from this port.

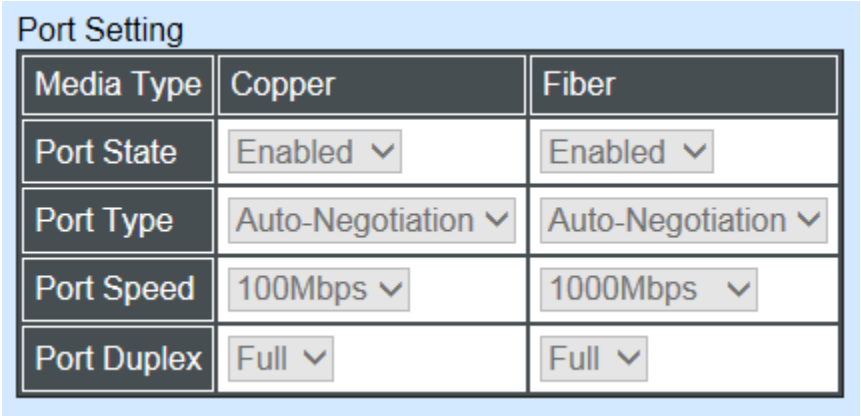
RX Total Errors: The total number of errors frames from this port.

4.5.4 Port Configuration

Select the option **Port Configuration** from the **Local Module Management** menu, then the **Port Configuration** fields show up on the right to let you configure them accordingly.



Port Setting



Media Type: Select between Copper (UTP, RJ-45) and Fiber

Port State: Enable or disable port state.

Port Type: View-only field that shows the port type configuration is manual or auto-negotiation.

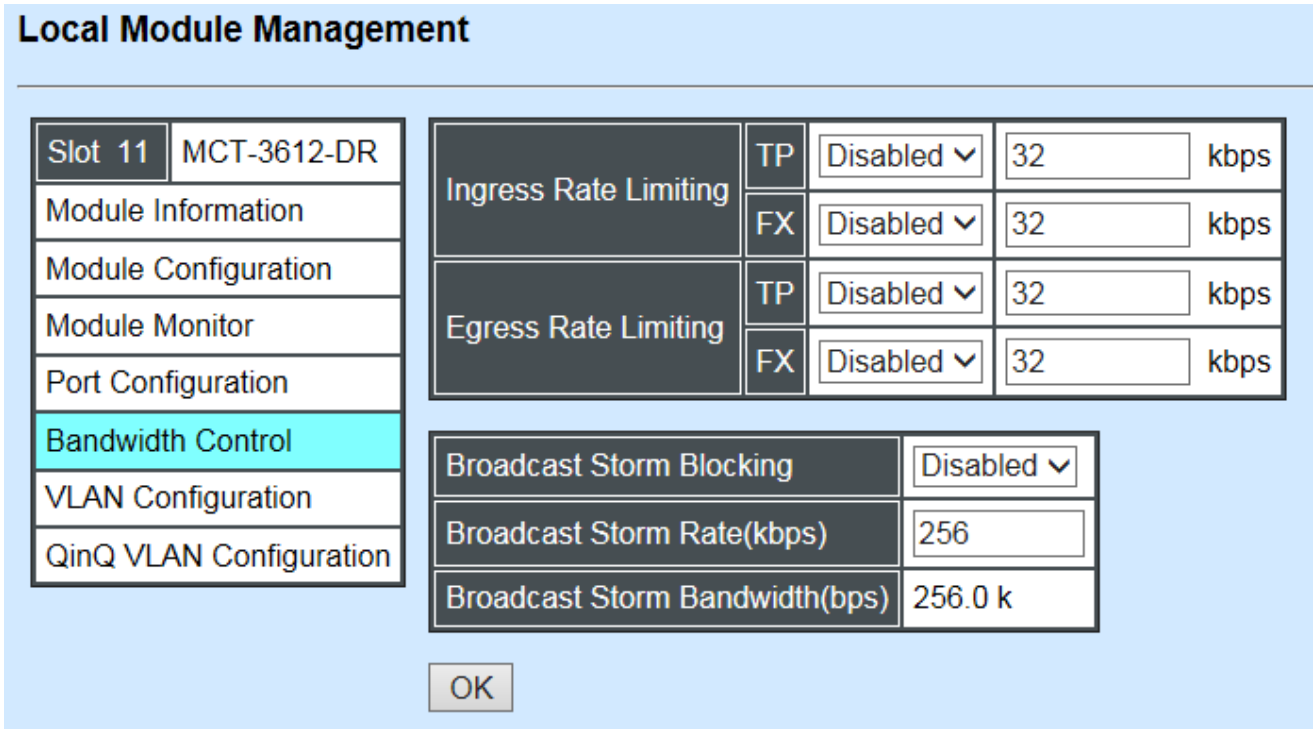
Port Speed: View-only field that shows the port speed of the selected media type.

Port Duplex: View-only field that show the duplex mode is half or full.

Click “**OK**” to apply.

4.5.5 Bandwidth Control

Select the option **Bandwidth Control** from the **Local Module Management** menu, then the **Bandwidth Control’s** Ingress/Egress Rate Limit and Broadcast Storm fields show up on the right to let you enable/disable TP/FX, specify the rate in kbps, enable/disable broadcast Storm settings and specify the rate in kbps in broadcast storm blocking.



Inress Rate Limiting: Enable or disable TP/FX ingress rate limiting in kbps and set up current configured ingress bandwidth in kbps. (The Ingress Rate Limiting range can be configured within 32~1000000kbps)

Egress Rate Limiting: Enable or disable TP/FX egress rate limiting in kbps and set up current configured egress bandwidth in kbps. (The Egress Rate Limiting range can be configured within 32~1000000kbps)

Broadcast Storm Blocking: Enable or disable broadcast storm blocking function.

Broadcast Storm Rate(kbps): Set up storm rate value. Packets exceeding the value will be dropped. (The Egress Rate Limiting range can be configured within 32~1000000kbps)

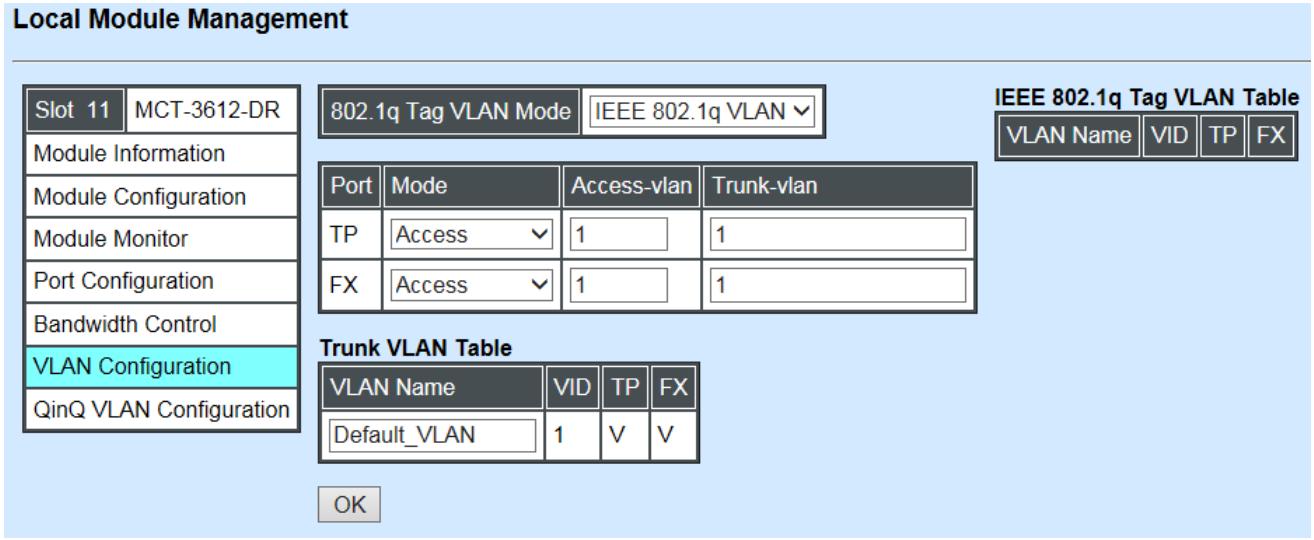
Broadcast Storm Rate Bandwidth(bps): Display the current configured storm rate bandwidth.

4.5.6 VLAN Configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the CHASSIS on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

Select the option **VLAN Configuration** from the **Local Module Management** menu, then the **VLAN Configuration's** Default VLAN Mode and Table fields show up on the right to let you specify the TP/FX of VLAN settings.

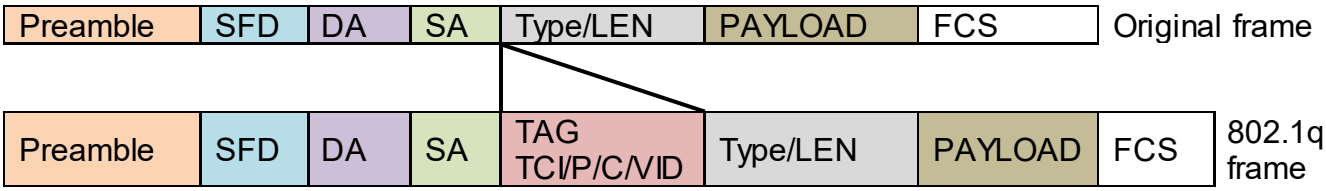


The Managed Media Converter supports **IEEE 802.1q Tag VLAN.**

IEEE 802.1Q VLAN Concepts

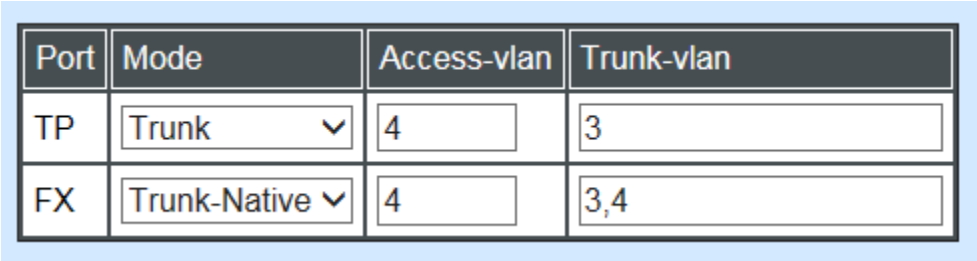
Port-Based VLAN is simple to implement and use, but it cannot be deployed cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution to this problem. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large switched networks into smaller segments so that broadcast and multicast traffic will not occupy too much available bandwidth as well as provide a higher level security between segments of internal networks.

Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes		User data	
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

IEEE 802.1q Tag VLAN Mode: Enable or disable IEEE 802.1q Tag VLAN mode, or select Bypass Ctag Mode which ignore C-tag checking.



Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

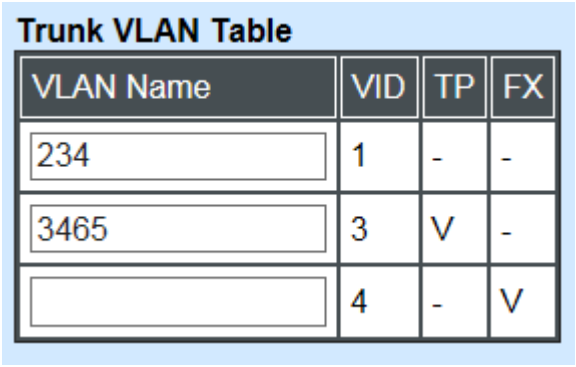
A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.



Trunk VLAN table: To edit 802.1Q Tag VLAN Name.

VLAN Name: User-specified field to give VLAN a name.

VID: The VLAN ID (**VID**) specifies the set of VLAN that a given port is allowed to receive and send **labeled** packets.

TP: It shows whether the TP port that is included in a given VID.

FX: It shows whether the Fiber port that is included in a given VID.

Click “OK” to apply.

IEEE 802.1q Tag VLAN Table

VLAN Name	VID	TP	FX
234	1	V	V

IEEE 802.1q Tag VLAN Table: It shows the status of IEEE 802.1q Tag VLAN.

VLAN Name: View-only filed that shows the VLAN name.

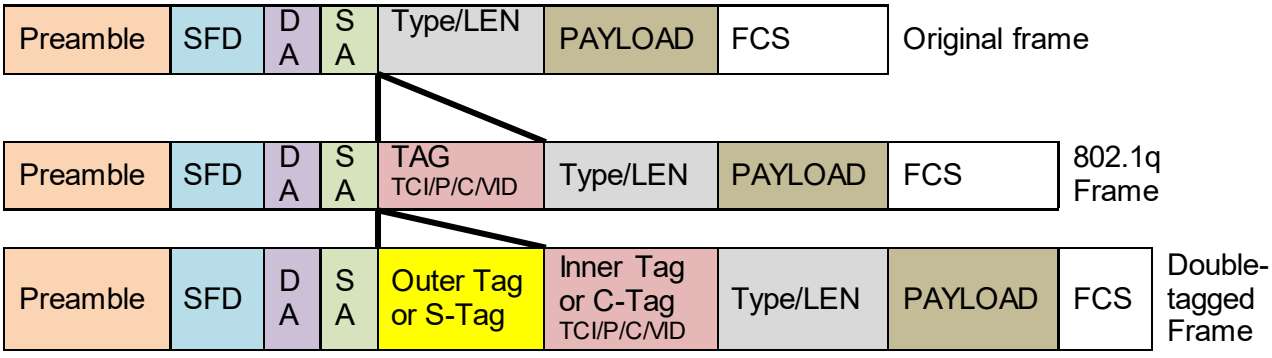
VID: View-only filed that shows the VID.

TP: View-only filed that shows whether the TP port that is included in a given VID.

FX: View-only filed that shows whether the fiber port that is included in a given VID.

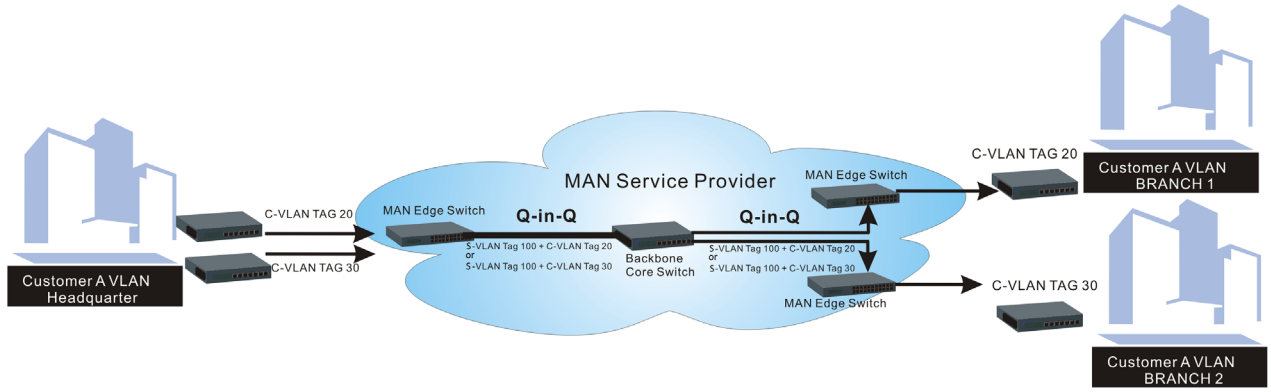
4.5.7 Q-in-Q VLAN Configuration

The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a “double-tagged” frame is created so as to separate customer traffic within a service provider network. As shown below in “Double-Tagged Frame” illustration, an outer tag is added between source destination and inner tag at the provider network’s edge. This can support C-VLAN (Customer VLAN) over Metro Area Networks and ensure complete separation between traffic from different user groups. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single S-VLAN (Service VLAN) tag per customer over the Metro Ethernet network.



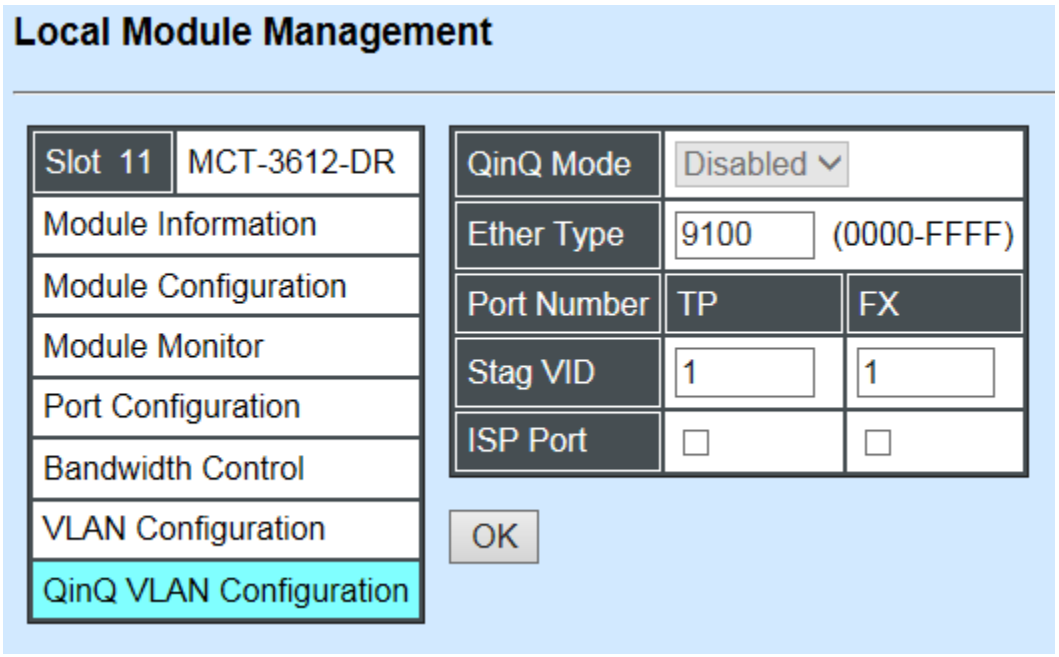
Double-Tagged Frame

As shown below in “Q-in-Q Example” illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider’s backbone, there is a possibility that traffic might be forwarded insecurely, for example due to the same VLAN ID used. Therefore, in order to get the information from Headquarter to Branch 1, the easiest way for the carrier to ensure security to customers is to encapsulate the original VLAN with a second VLAN ID of 100. This second VLAN ID is known as S-VLAN (Service VLAN) that is added as data enters the service provider’s network and then removed as data exits. Eventually, with the help of S-Tag, the information sent from Headquarter to Branch 1 can be delivered with customers’ VLANs intactly and securely.



Q-in-Q Example

This section allows you to set up QinQ VLAN. Select the option **QinQ VLAN Configuration** from the **Local Module Management** menu, the **Firmware Upgrade’s** fields show up on the right.



QinQ Mode: Enable or disable the function by clicking drop-down box.

Ether Type: A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).

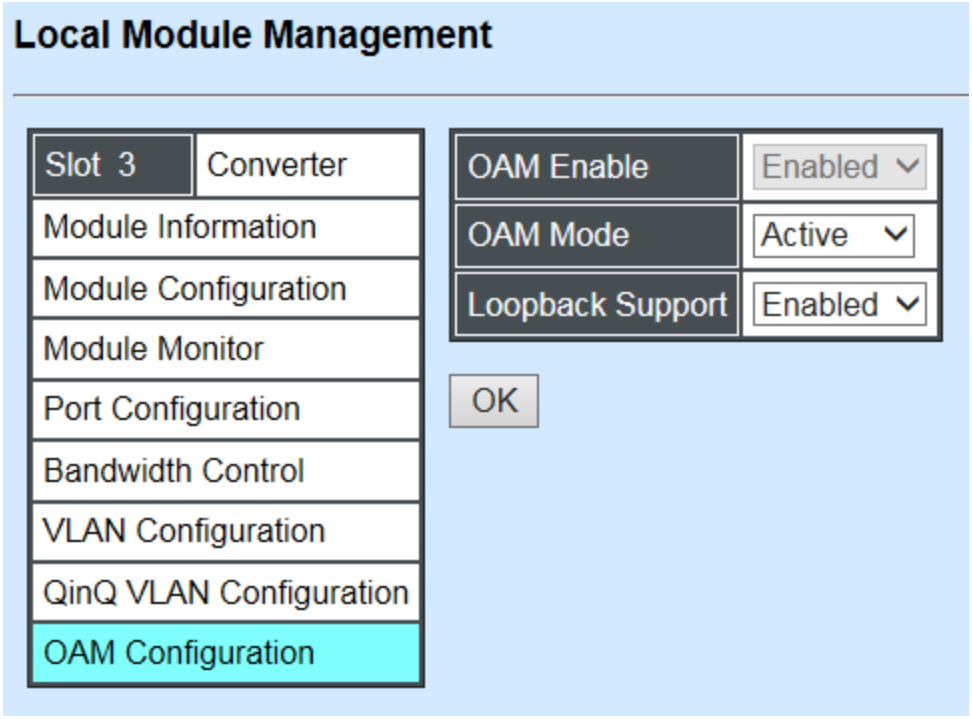
Port Number: Two kinds of ports are available, TP port or Fiber port.

Stag(Service Tag) VID: Specify a VID for the service tag (Outer Tag).

ISP(Internet Service Provider) Port: This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.

Click the **"OK"** button to apply the settings.

4.5.8 OAM Configuration (For OAM Converter Only)



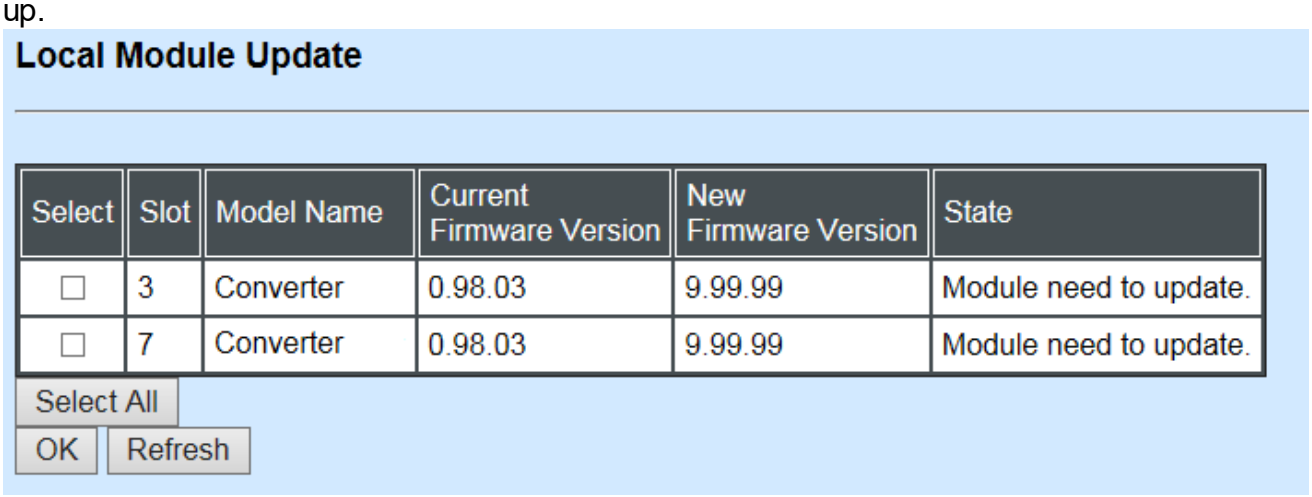
OAM Enable: The module is fixed at "Enabled" only.

OAM Mode: Click drop-down box to select OAM mode, either Active or Passive. To perform remote management, it's strongly recommended that OAM Mode be set "Active".

Loopback Support: Click drop-down box to enable or disable the function. A loopback test is a test in which a signal in sent from a communications device and returned (looped back) to it as a way to determine whether the device is working right or as a way to pin down a failing node in a network. The default setting is Disabled.

4.6 Local Update Module

Select **Local Update Module** from the **Main Menu**, then the following screen page shows up.



Select: Check the box to upgrade firmware on specified converters or check Select All box to upgrade firmware on all converters.

Slot: Shows which slot the converter is inserted into.

Model Name: Shows the current model name of the converter.

Current Firmware Version: Shows the current firmware version used for each converter.

New Firmware Version: The upcoming firmware version to be installed.

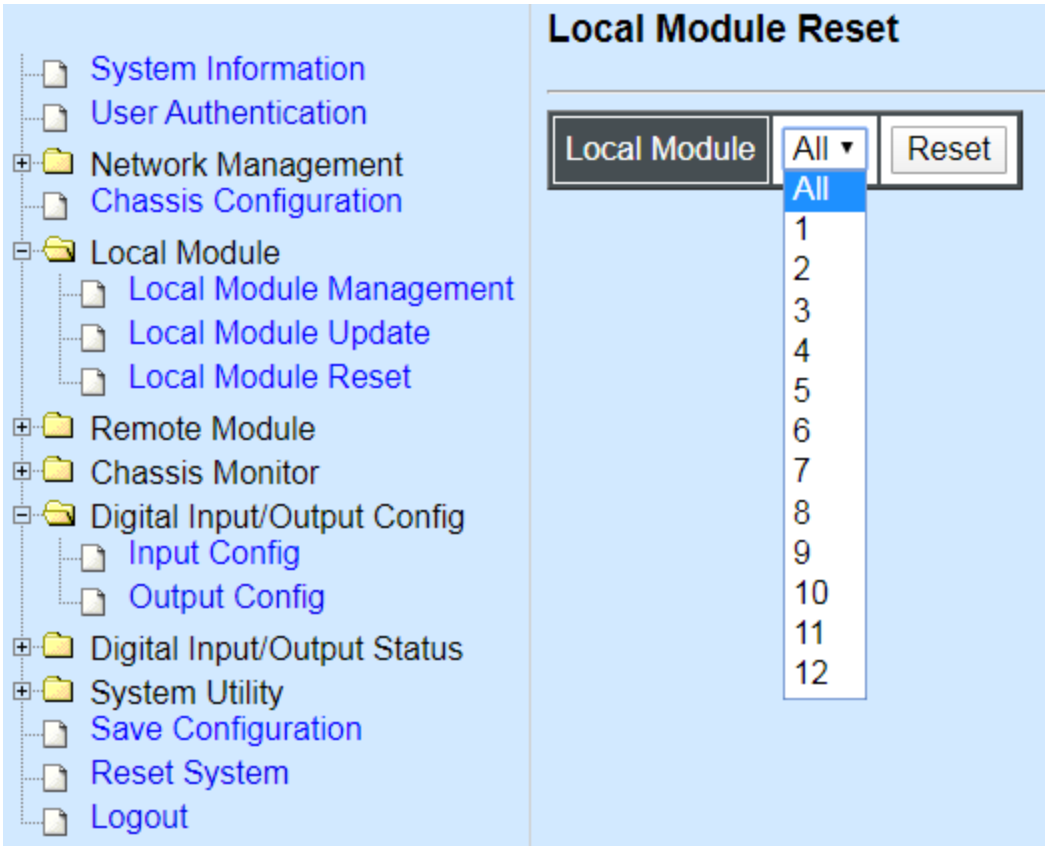
State: Shows the current status of firmware upgrade.

Click **"OK"** to start module update procedure.

Click **"Refresh"** to renew all update module information.

4.7 Local Reset Module

Select **Local Reset Module** from the **Main Menu**, then the following screen page shows up.

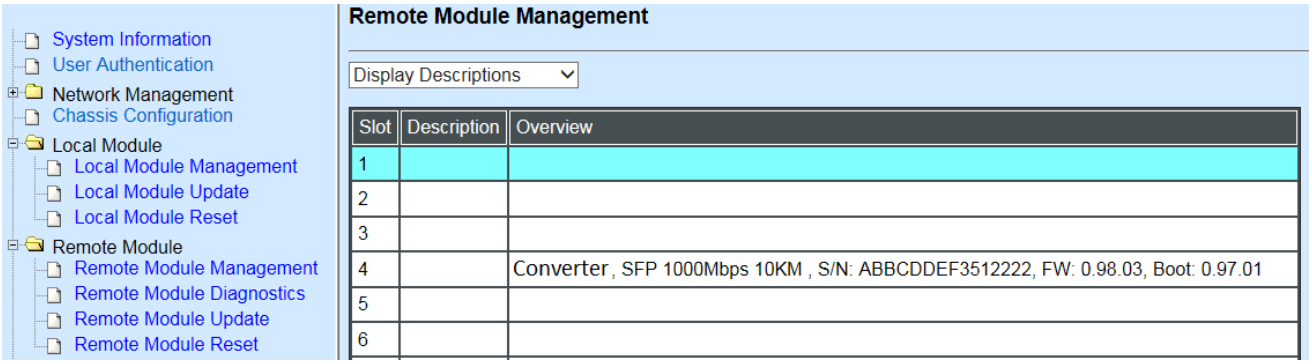


Local Module: Select **"All"** to reset all modules or select the individual module. When you decide which module to reset, select **"Reset"** to begin the reset process.

4.8 Remote Module Management

Note: This section is for reference only. For specific converter setting, please refer to Appendix C, D and E.

In order to manage the installed converters and set up required functions, select the option **Remote Module Management** from **Main Menu**, then **Remote Module Management** screen page shows up.



Overview: Shows product information.

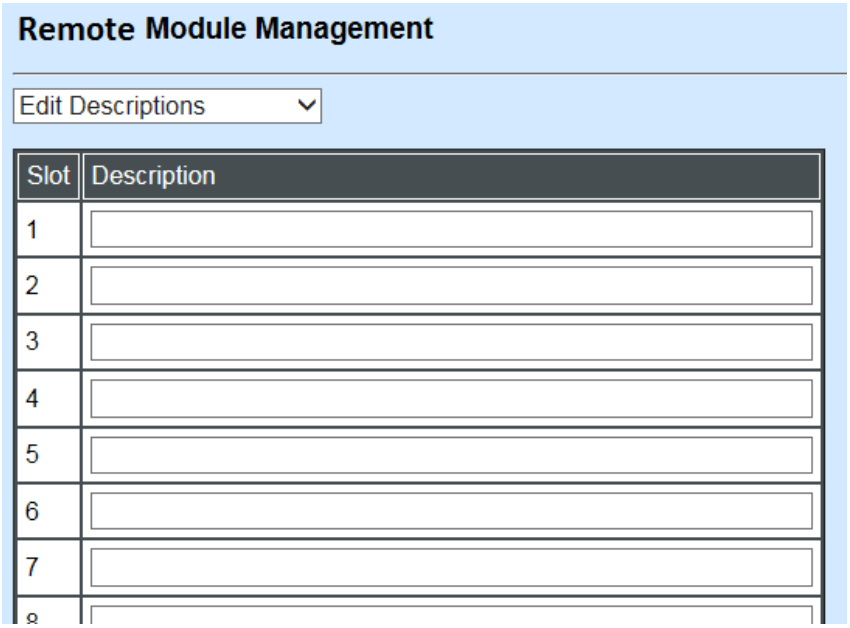
Description: Shows the user-specified message.

The drop-down box is to edit or show the message you specify. There are three options:

Not Display Descriptions: Hide the user-specified message.

Display Descriptions: Show up the user-specified message.

Edit Descriptions: Change the user-specified message.



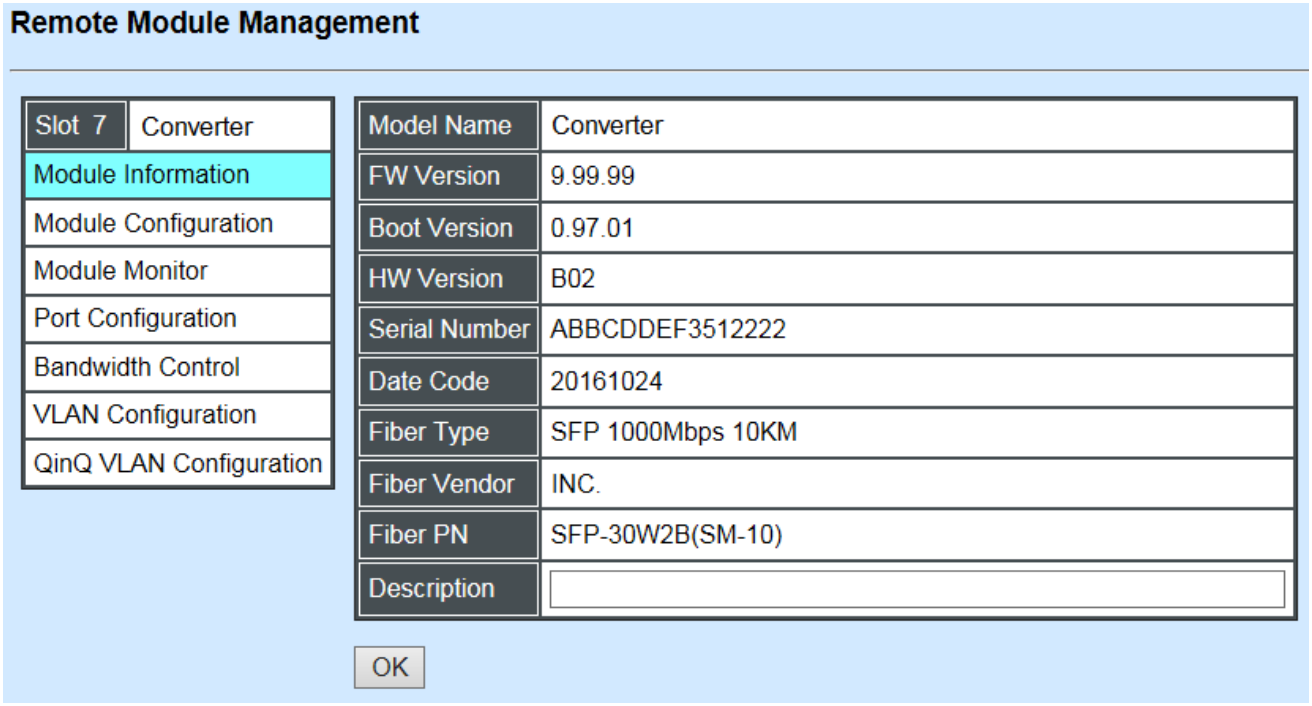
To edit description, click drop-down box and select **Edit Descriptions**.

Click “**OK**” to save edited message.

Click on the available modules and then the following screen page appears.

4.8.1 Module Information

Select the option **Module Information** from the **Local Module Management** menu, then the **Module Information** fields show up on the right to provide you information about the module.



Model Name: View-only field that shows the product's model name.

FW Version: View-only field that shows the product's firmware version.

Boot Version: View-only field that shows the product's boot loader version.

HW Version: View-only field that shows the product's hardware version.

Serial Number: View-only field that shows the product's serial number.

Date Code: View-only field that shows the date of EEPROM burned.

Fiber Type: View-only field that shows the product's fiber connector type, speed, and distance.

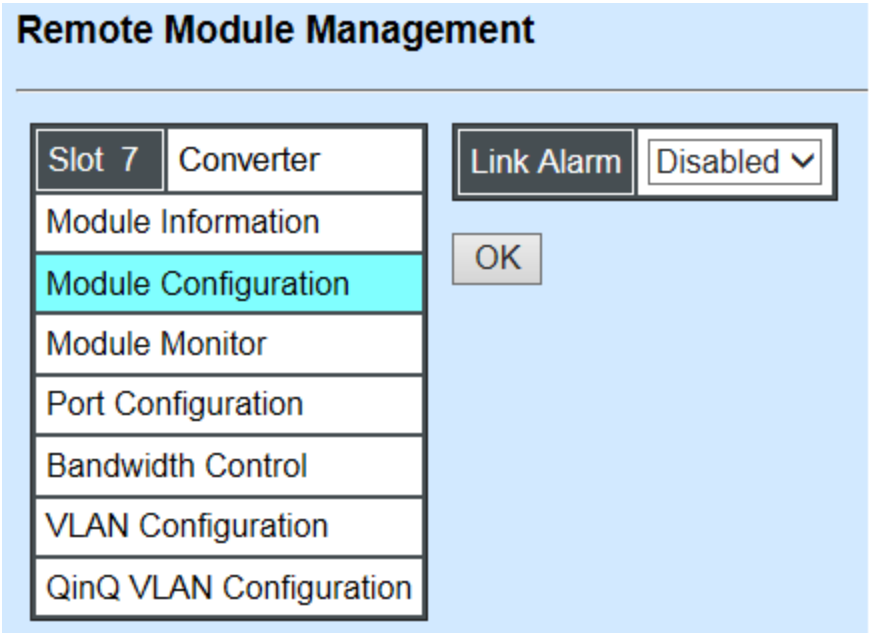
Fiber Vendor: View-only field that shows the vendor name.

Fiber PN: View-only field that shows the fiber PN.

Description: Specify the appropriate brief description for the slide-in converter module.

4.8.2 Module Configuration

Select the option **Module Configuration** from the **Remote Module Management** menu, then **Module Configuration** fields show up on the right to let you view the configuration of the converter.

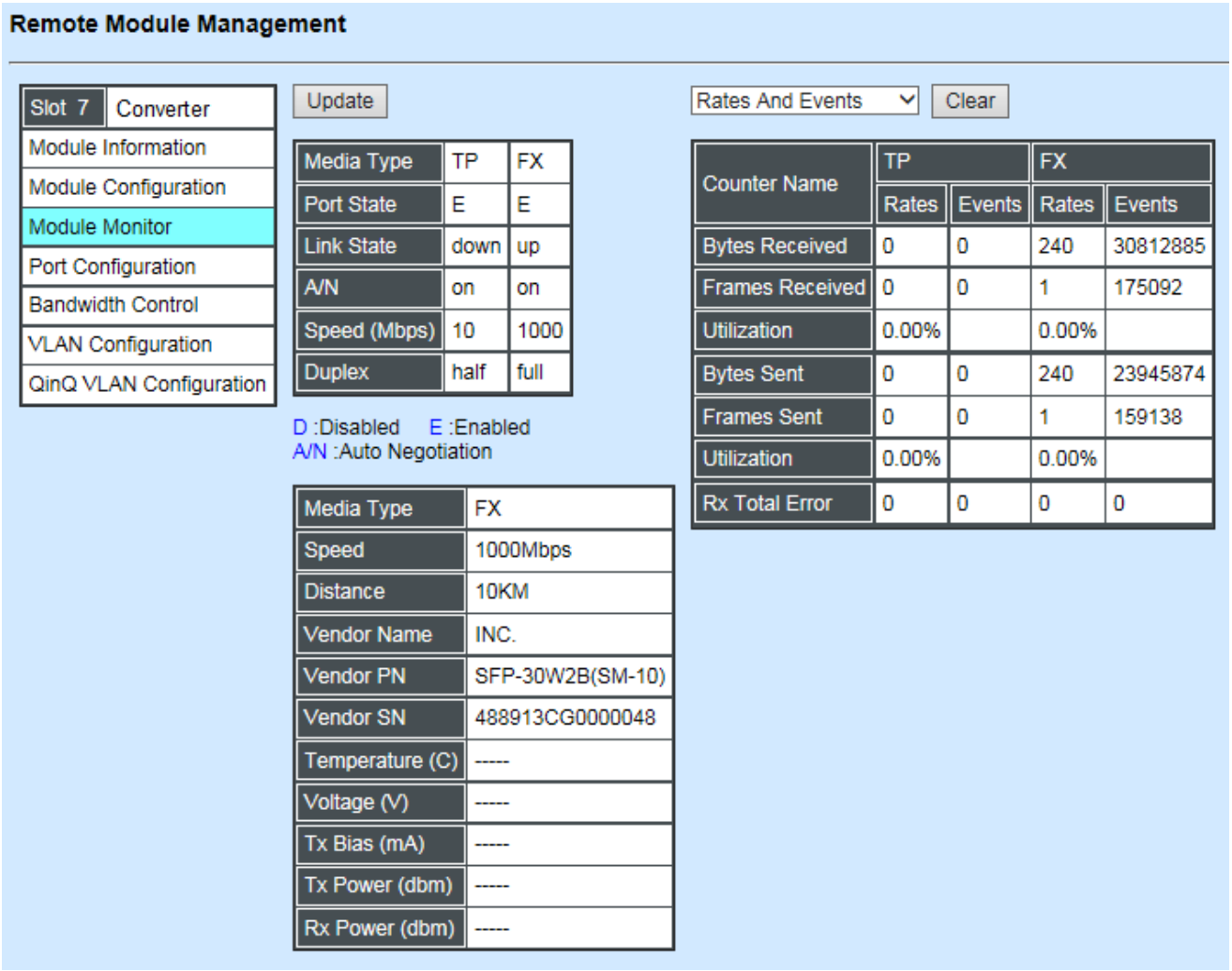


Link Alarm: This function is used under the circumstance that when UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.

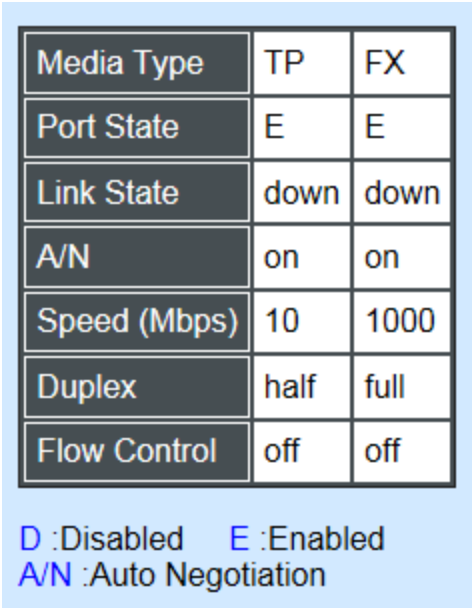
Click the drop-down box to enable or disable link alarm of the converter.

4.8.3 Module Monitor

Select the option **Module Monitor** from the **Remote Module Management** menu, and then **Module Monitor** fields show up on the right to let you view the configuration of the module.



Port Status



Media Type	TP	FX
Port State	E	E
Link State	down	down
A/N	on	on
Speed (Mbps)	10	1000
Duplex	half	full
Flow Control	off	off

D :Disabled E :Enabled
A/N :Auto Negotiation

Media Type: TP (copper, 10/100Base-T, RJ-45) and FX (fiber).

Port State: View-only field that shows traffic is Disabled or Forwarding.

Link State: View-only field that shows the link is up or down.

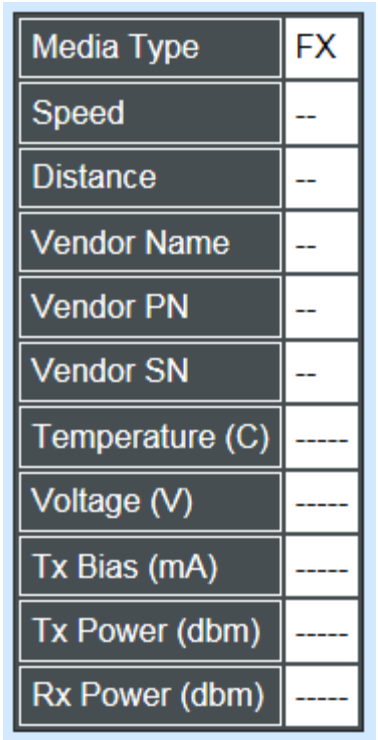
A/N: View-only field that shows Auto-negotiation is on or off.

Speed: View-only field that shows the port speed.

Duplex: View-only field that shows the duplex mode is half or full.

Flow Control: View-only field that shows the flow control is on or off.

SFP Status



Media Type	FX
Speed	--
Distance	--
Vendor Name	--
Vendor PN	--
Vendor SN	--
Temperature (C)	-----
Voltage (V)	-----
Tx Bias (mA)	-----
Tx Power (dbm)	-----
Rx Power (dbm)	-----

Media Type: Shows the type of FX (fiber).

Speed: Data rate of the slide-in SFP Transceiver.

Distance: Transmission distance of the slide-in SFP Transceiver.

Vendor Name: Vendor name of the slide-in SFP Transceiver.

Vendor PN: Vendor PN of the slide-in SFP Transceiver.

Vendor SN: Vendor SN of the slide-in SFP Transceiver.

Temperature (C): The Slide-in SFP module operation temperature.

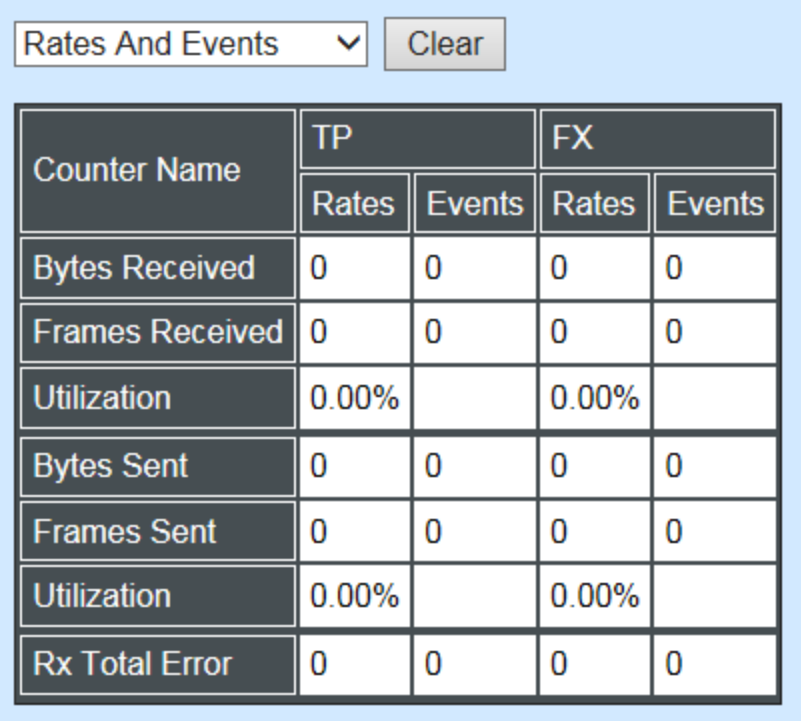
Voltage (V): The Slide-in SFP module operation voltage.

TX Bias (mA): The Slide-in SFP module operation current.

TX Power (dbm): The Slide-in SFP module optical Transmission power.

RX Power (dbm): The Slide-in SFP module optical Receiver power.

Select **"Rates and Events"** option from the Counters Display pull-down menu to view the detailed traffic statistics (counters' information).



Rates: Counters displayed and updated once per second.

Events: The count is cumulative (i.e. cumulated count).

Bytes Received: The total number of bytes received from this port.

Frames Received: The total number of frames received from this port.

Utilization: The utilization of receiving bandwidth from this port.

Bytes Sent: The total number of bytes sent from this port.

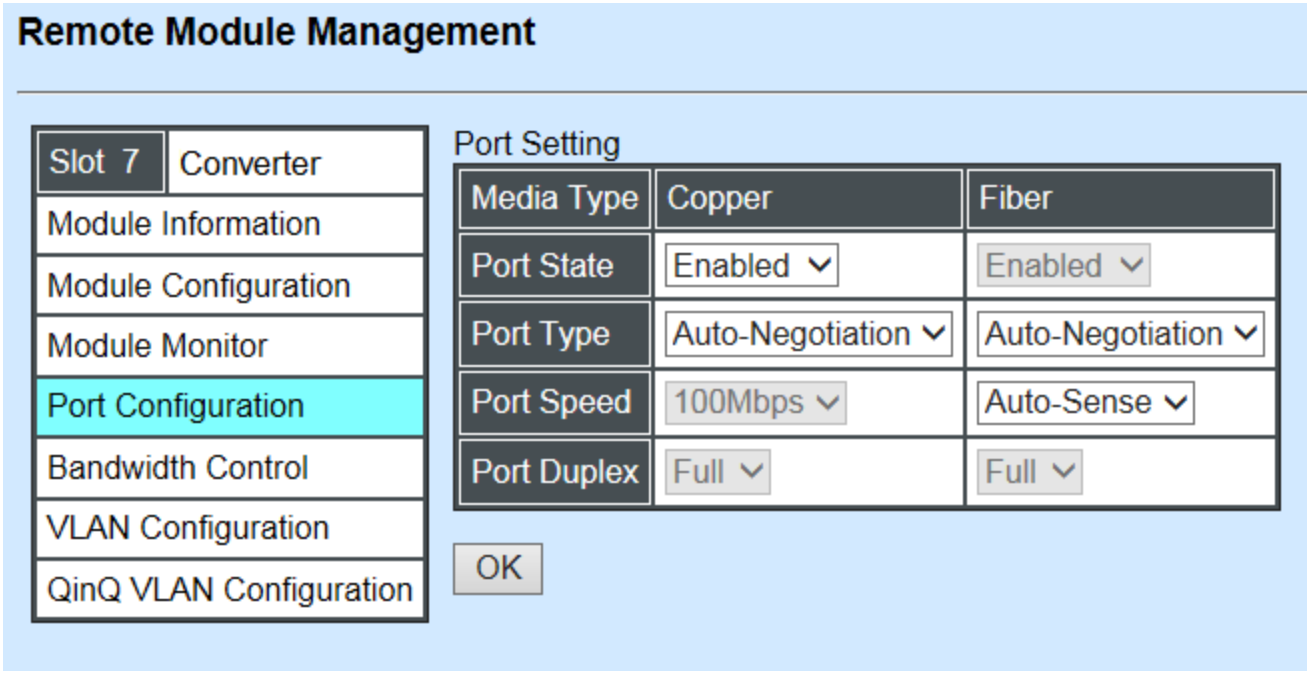
Frames Sent: The total number of frames sent from this port.

Utilization: The utilization of sending bandwidth from this port.

RX Total Errors: The total number of errors frames from this port.

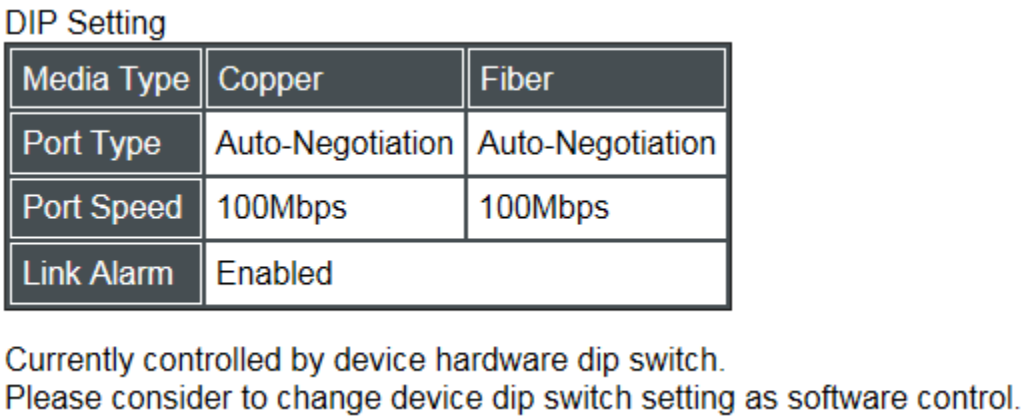
4.8.4 Port Configuration

Select the option **Port Configuration** from the **Remote Module Management** menu, then the **Port Configuration** fields show up on the right to let you configure them accordingly.



DIP Setting

You are allowed to view the DIP switch configuration via WEB UI if PIN 8 of the converter is switched "ON".



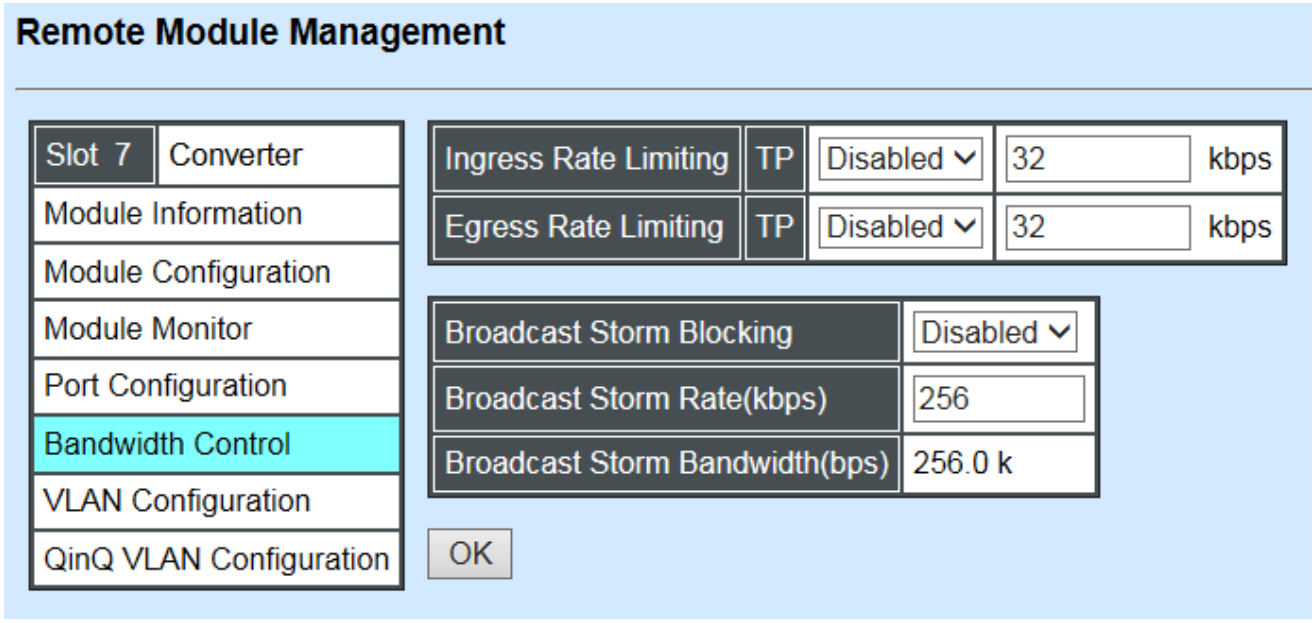
Port Type: View-only field that shows the port type configuration is manual or auto-negotiation.

Port Speed: View-only field that shows the port speed of the selected media type.

Link Alarm: View-only field that shows the link alarm is enabled or disabled.

4.8.5 Bandwidth Control

Select the option **Bandwidth Control** from the **Remote Module Management** menu, then the Bandwidth Control's Ingress/Egress Rate Limit and Broadcast Storm fields show up on the right to let you enable/disable TP/FX, specify the rate in kbps, enable/disable broadcast Storm settings and specify the rate in kbps in broadcast storm blocking.



Ingress Rate Limiting: Enable or disable TP ingress rate limiting in kbps and set up current configured ingress bandwidth in kbps. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

Egress Rate Limiting: Enable or disable TP egress rate limiting in kbps and set up current configured egress bandwidth in kbps. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

Broadcast Storm Blocking: Enable or disable broadcast storm blocking function.

Broadcast Storm Rate(kbps): Set up storm rate value. Packets exceeding the value will be dropped. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

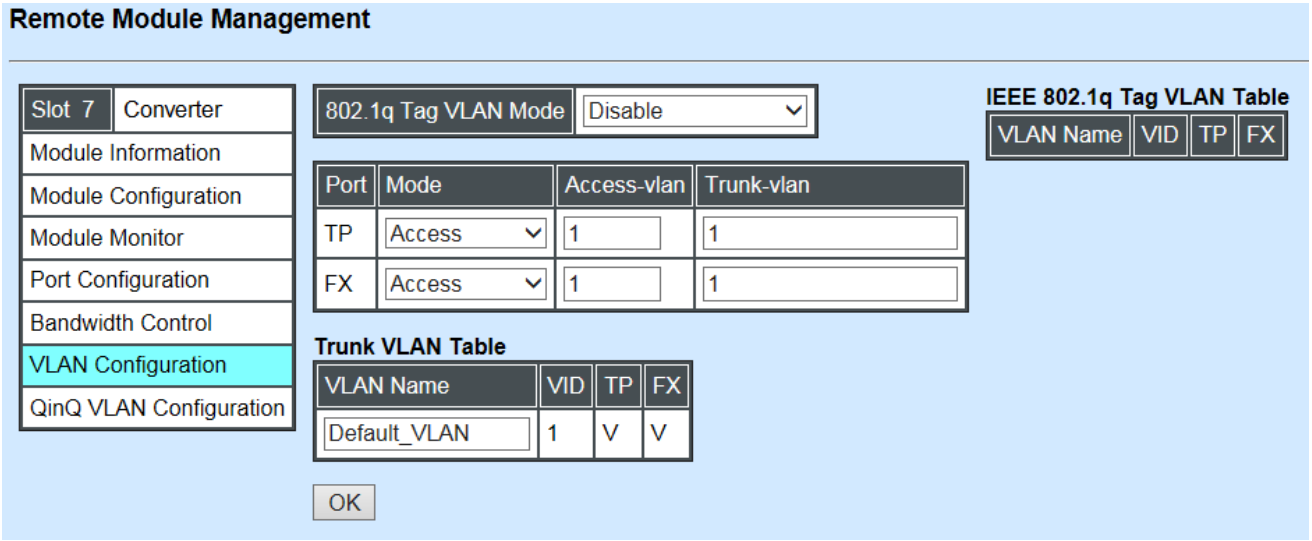
Broadcast Storm Rate Bandwidth(bps): Display the current configured storm rate bandwidth.

4.8.6 VLAN Configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the CHASSIS on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

Select the option **VLAN Configuration** from the **Local Module Management** menu, then the **VLAN Configuration's** Default VLAN Mode and Table fields show up on the right to let you specify the TP/FX of VLAN settings.

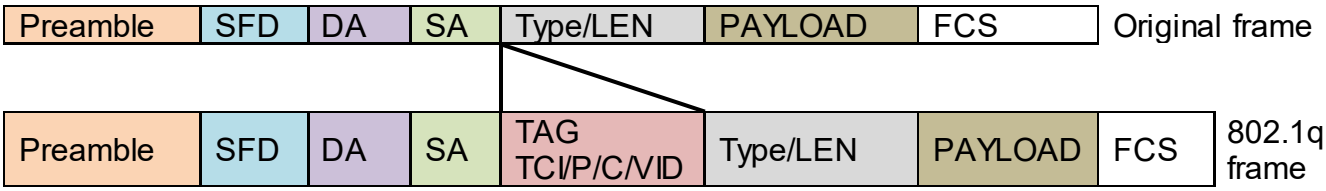


The Managed Media Converter supports **IEEE 802.1q Tag VLAN.**

IEEE 802.1Q VLAN Concepts

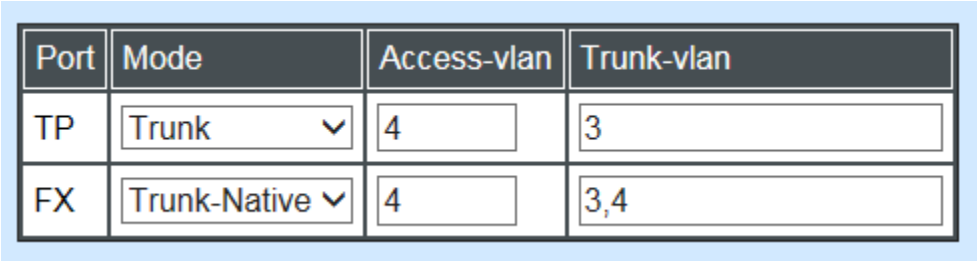
Port-Based VLAN is simple to implement and use, but it cannot be deployed cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution to this problem. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large switched networks into smaller segments so that broadcast and multicast traffic will not occupy too much available bandwidth as well as provide a higher level security between segments of internal networks.

Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes		User data	
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

IEEE 802.1q Tag VLAN Mode: Enable or disable IEEE 802.1q Tag VLAN mode, or select Bypass Ctag Mode which ignore C-tag checking.



Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

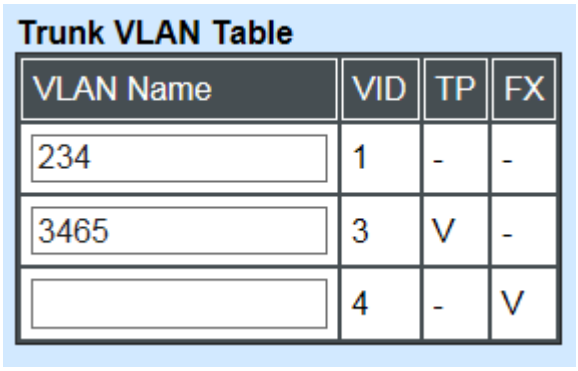
A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode:**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode:**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.



Trunk VLAN table: To edit 802.1Q Tag VLAN Name.

VLAN Name: User-specified field to give VLAN a name.

VID: The VLAN ID (**VID**) specifies the set of VLAN that a given port is allowed to receive and send **labeled** packets.

TP: It shows whether the TP port that is included in a given VID.

FX: It shows whether the Fiber port that is included in a given VID.

Click “OK” to apply.

IEEE 802.1q Tag VLAN Table

VLAN Name	VID	TP	FX
234	1	V	V

IEEE 802.1q Tag VLAN Table: It shows the status of IEEE 802.1q Tag VLAN.

VLAN Name: View-only filed that shows the VLAN name.

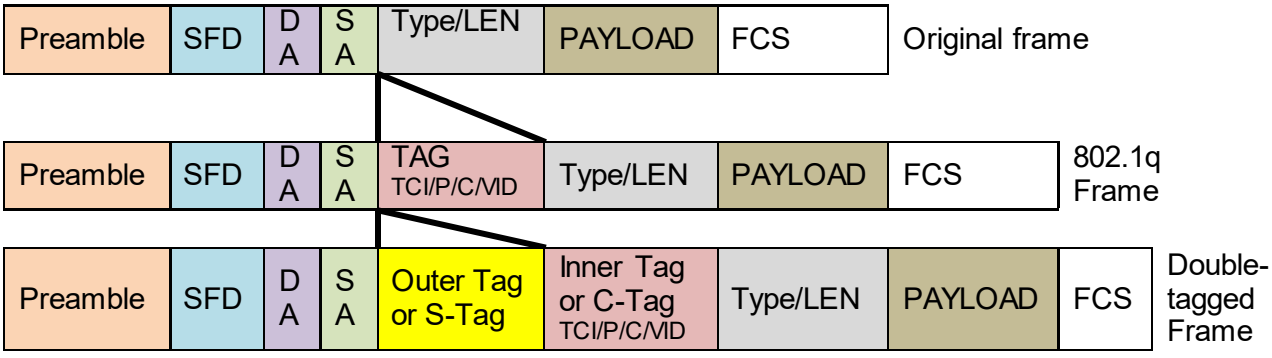
VID: View-only filed that shows the VID.

TP: View-only filed that shows whether the TP port that is included in a given VID.

FX: View-only filed that shows whether the fiber port that is included in a given VID.

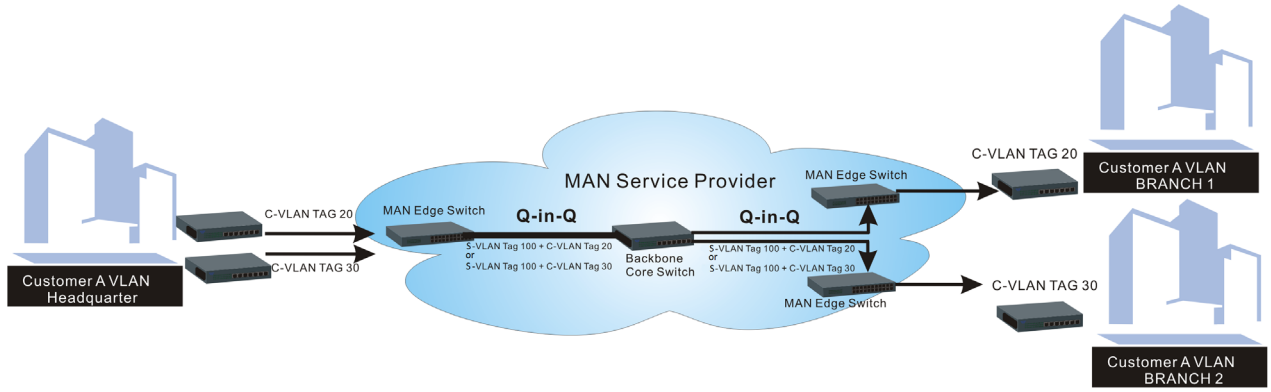
4.8.7 Q-in-Q VLAN Configuration

The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a “double-tagged” frame is created so as to separate customer traffic within a service provider network. As shown below in “Double-Tagged Frame” illustration, an outer tag is added between source destination and inner tag at the provider network’s edge. This can support C-VLAN (Customer VLAN) over Metro Area Networks and ensure complete separation between traffic from different user groups. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single S-VLAN (Service VLAN) tag per customer over the Metro Ethernet network.



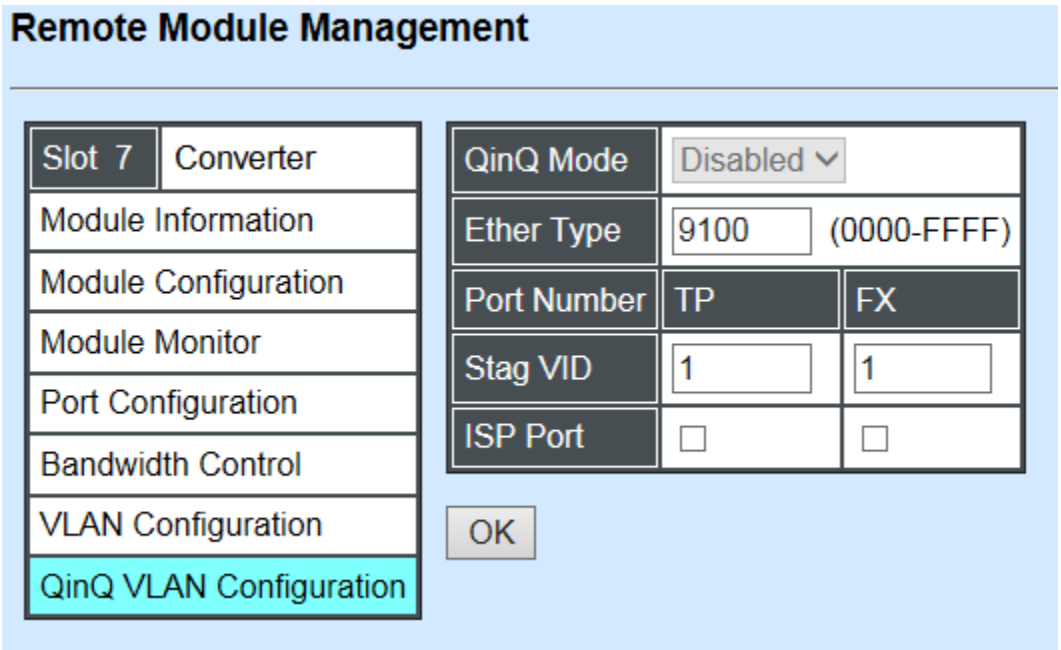
Double-Tagged Frame

As shown below in “Q-in-Q Example” illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider’s backbone, there is a possibility that traffic might be forwarded insecurely, for example due to the same VLAN ID used. Therefore, in order to get the information from Headquarter to Branch 1, the easiest way for the carrier to ensure security to customers is to encapsulate the original VLAN with a second VLAN ID of 100. This second VLAN ID is known as S-VLAN (Service VLAN) that is added as data enters the service provider’s network and then removed as data exits. Eventually, with the help of S-Tag, the information sent from Headquarter to Branch 1 can be delivered with customers’ VLANs intactly and securely.



Q-in-Q Example

This section allows you to set up QinQ VLAN. Select the option **QinQ VLAN Configuration** from the **Remote Module Management** menu, the **Firmware Upgrade’s** fields show up on the right.



QinQ Mode: Enable or disable the function by clicking drop-down box.

Ether Type: A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).

Port Number: Two kinds of ports are available, TP port or Fiber port.

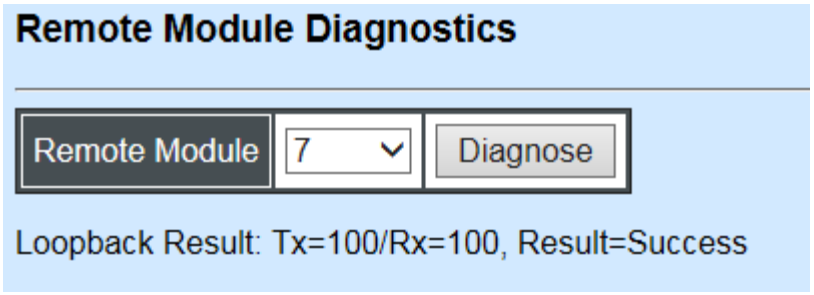
Stag(Service Tag) VID: Specify a VID for the service tag (Outer Tag).

ISP(Internet Service Provider) Port: This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.

Click the **"OK"** button to apply the settings.

4.9 Remote Module Diagnostics

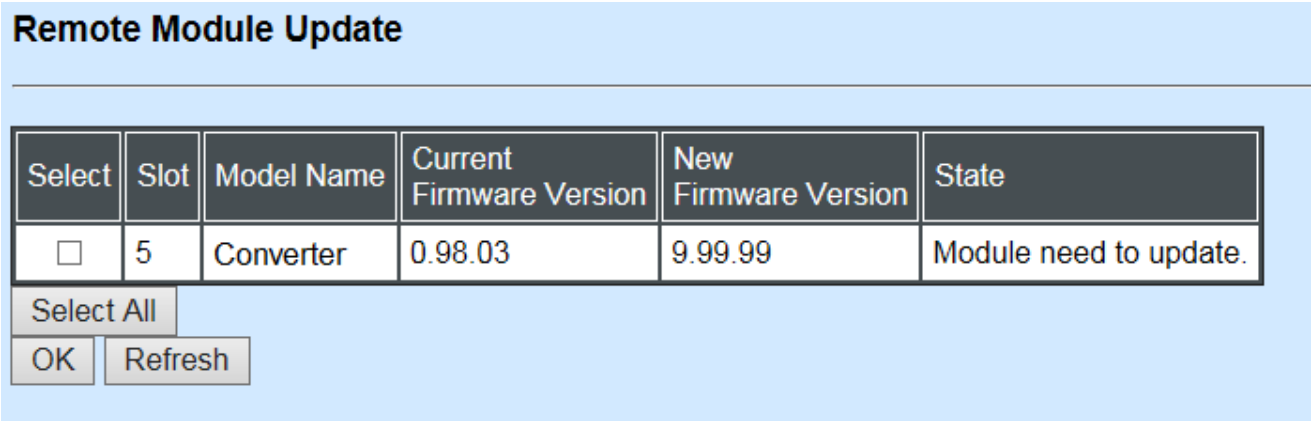
This is to conduct loopback test to check if the external converter is link up properly. Select the slot that the external converter is connected with and click “Diagnose”. After a while, the test result will pop out as below:



That the Packet of Tx is equal to that of Rx indicates the link is working normal and the result of test shows “Success”. If the Tx is not the same as Rx, which means some packet are dropped during the link transmission, the result of test shows “Fail”.

4.10 Remote Module Update

Select **Local Update Module** from the **Main Menu**, then the following screen page shows up.



Select: Check the box to upgrade firmware on specified converters or check Select All box to upgrade firmware on all converters.

Slot: Shows which slot the converter is inserted into.

Model Name: Shows the current model name of the converter.

Current Firmware Version: Shows the current firmware version used for each converter.

New Firmware Version: The upcoming firmware version to be installed.

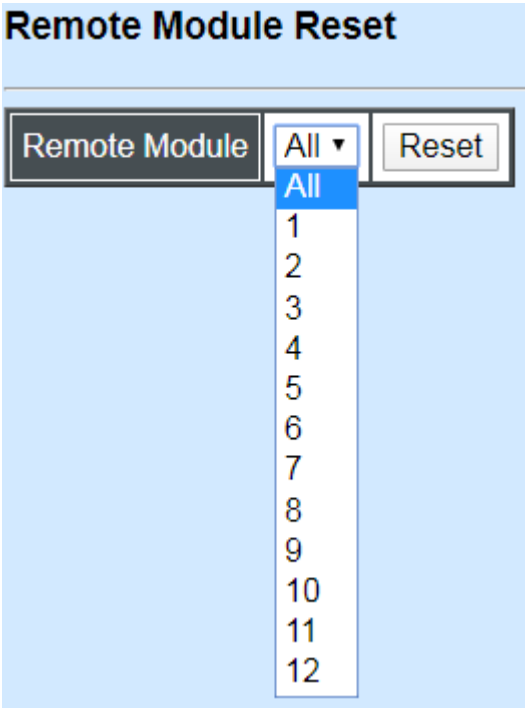
State: Shows the current status of firmware upgrade.

Click **"OK"** to start module update procedure.

Click **"Refresh"** to renew all update module information.

4.11 Remote Module Reset

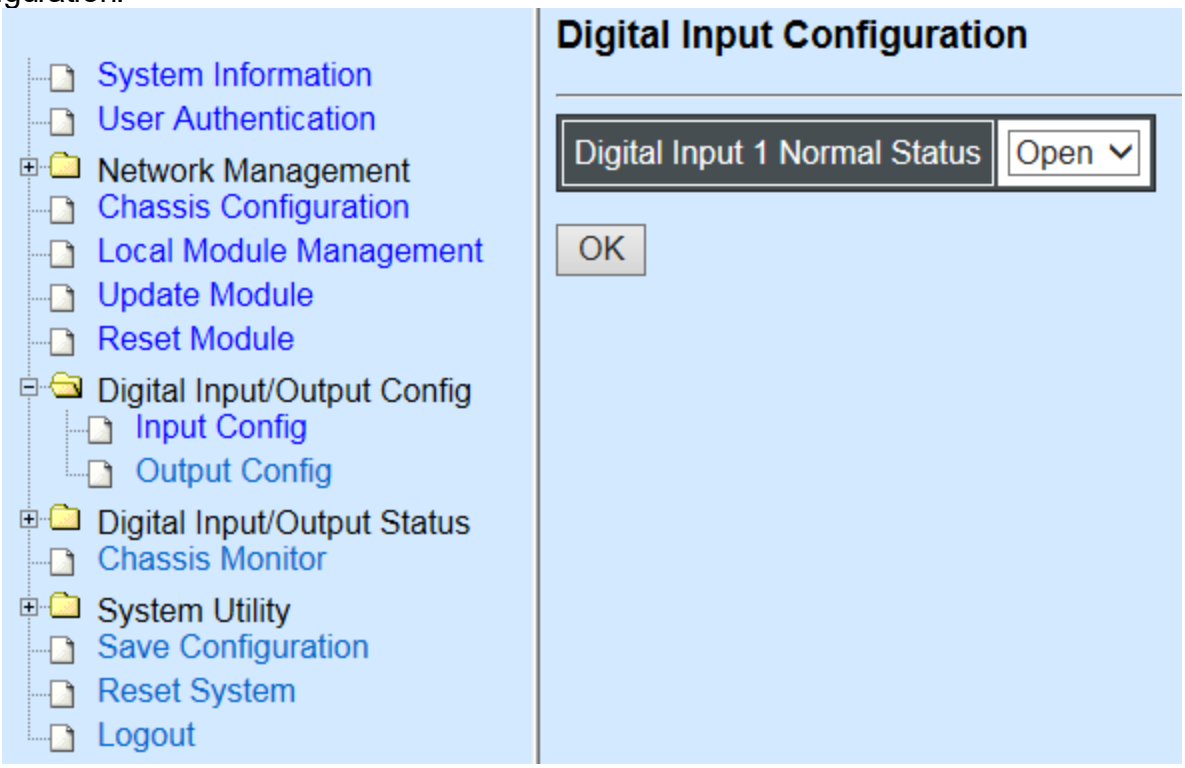
Select **Remote Module Reset** from the **Main Menu**, then the following screen page shows up.



Remote Module: Select **"All"** to reset all modules or select the individual module. When you decide which module to reset, select **"Reset"** to begin the reset process.

4.12 Digital Input/Output Config

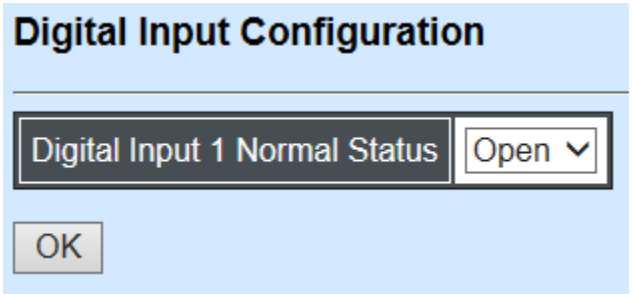
This is a way serving as an alarm via relay that is an electrically operated switch used where it is necessary to control a circuit by a low-power signal, or where several circuits must be controlled by one signal, thus helping us understand immediate status on a circuit with fault relay feature from remote site. This section gives the instruction how to set up relay configuration.



Input Config: Set up Digital Input Configuration.

Output Config: Set up Digital Output Configuration.

4.12.1 Digital Input Configuration



Digital Input 1 Normal Status is shown on the screen. Normal Status refers to where the contacts remain in one state unless actuated. The contacts can either be normally open until closed by operation of the switch, or normally closed and opened by the switch action. You may choose either open or close status of electrical circuit by clicking drop-down box.

Note: *The Event Trigger and Digital Input event must be enabled to activate alarm for Digital Input. Refer to Digital Output Configuration for more information.*

4.12.2 Digital Output Config

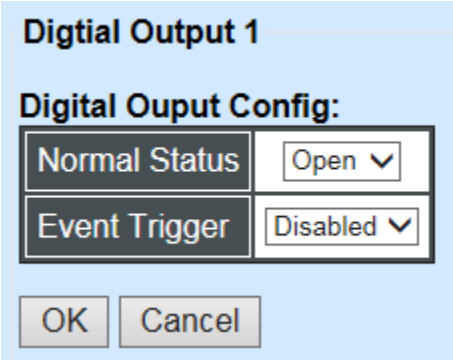
The following shows the current Digital Output Configuration.

Digital Output Configuration

Digital Output	Config		Event					Action
	Normal	Event Trigger	Digital Input 1	Power A	Power B	LAN Port	Slot Number	
1	Open	Disabled	Disabled	Disabled	Disabled	Disabled	None	Edit

Digital Output	Event											
	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9	Slot 10	Slot 11	Slot 12
1												

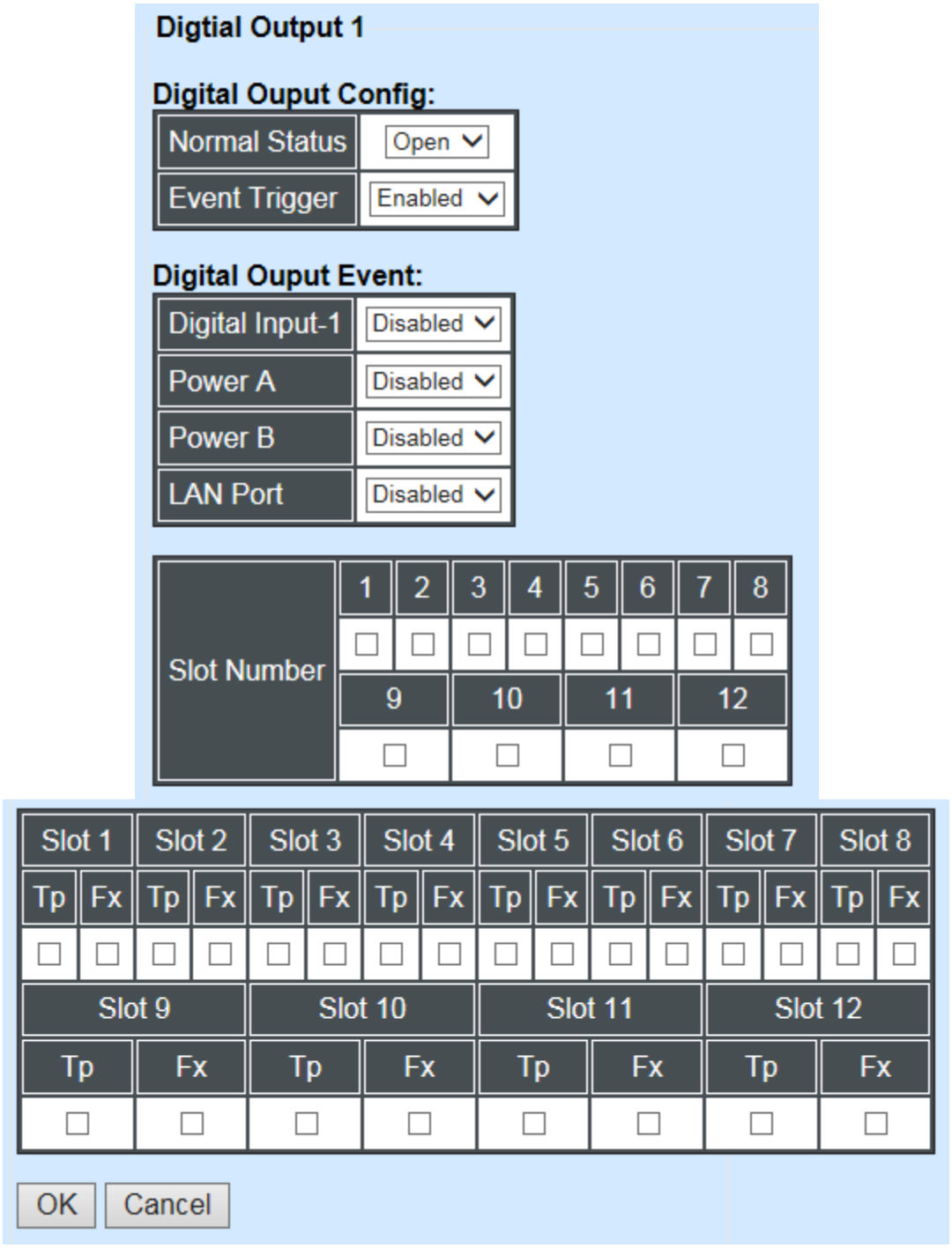
Click **"Edit"** under Action column, Digital Output section will appear.



Normal Status: This is where the contacts remain in one state unless actuated by one of events in Digital Output Event. You may choose either open or close status of electrical circuit by clicking drop-down box.

Event Trigger: This is Digital Output event settings.

Click Event Trigger drop-down box and select "**Enabled**", the following section appears.



Digital Input 1: Enable or disable the alarm transmission for Digital Input-1.

Power A: Enable or disable the alarm transmission for Power A.

Power B: Enable or disable the alarm transmission for Power B.

LAN Port: Enable or disable the alarm transmission for LAN Port

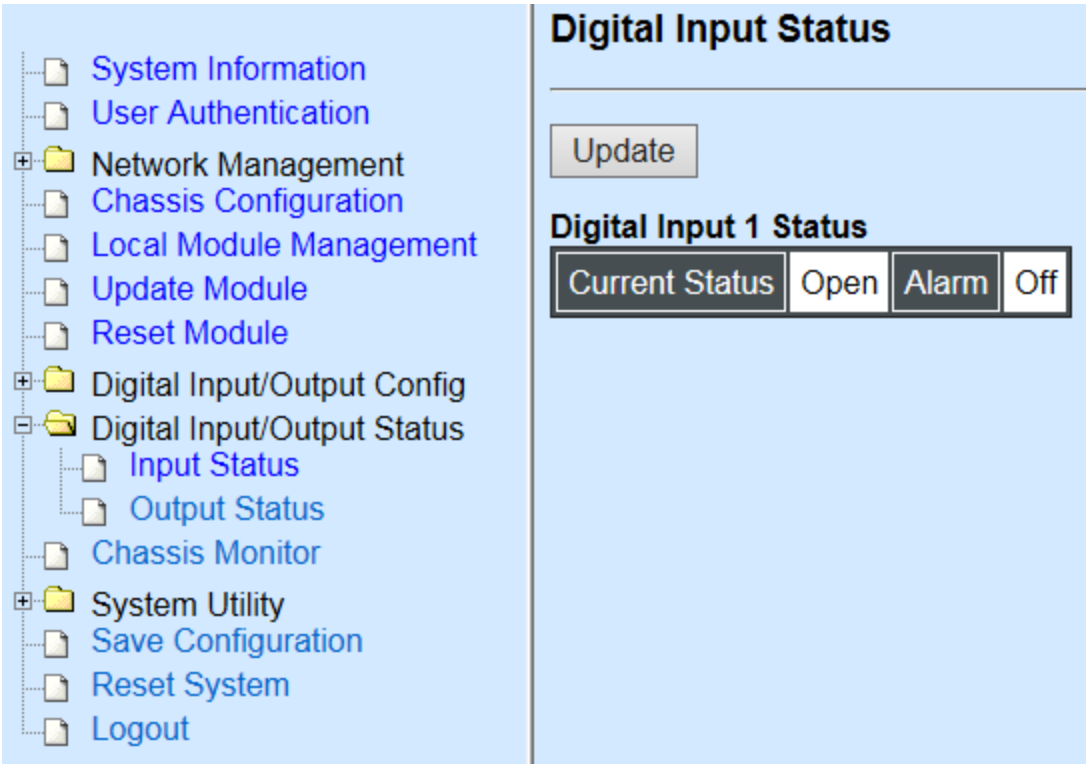
Slot Number: Enable the alarm transmission by checking Port Number box or disable it by unchecking.

Tp/Fx Port: Enable the alarm transmission by checking Tp/Fx box or disable it by unchecking.

Click **OK** to save the setting or **Cancel** to undo it.

Digital Output Event	Alarm is triggered when..
Digital Input 1	Normal status and current status are different from each other.
Power A	Power is disconnected.
Power B	Power is disconnected.
LAN Port	LAN port is disconnected.
Slot Number	Any checked slot is disconnected.
Tp/Fx Port	Tp/Fx Port is disconnected.
Note: *Make sure that the designated event is enabled or checked before triggering alarm.*	

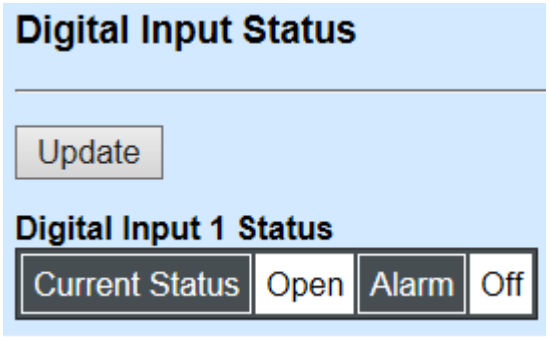
4.13 Digital Input/Output Status



Input Status: It shows the current status of digital Input.

Output Stastus: It shows the current status of digital Output.

4.13.1 Digital Input Status



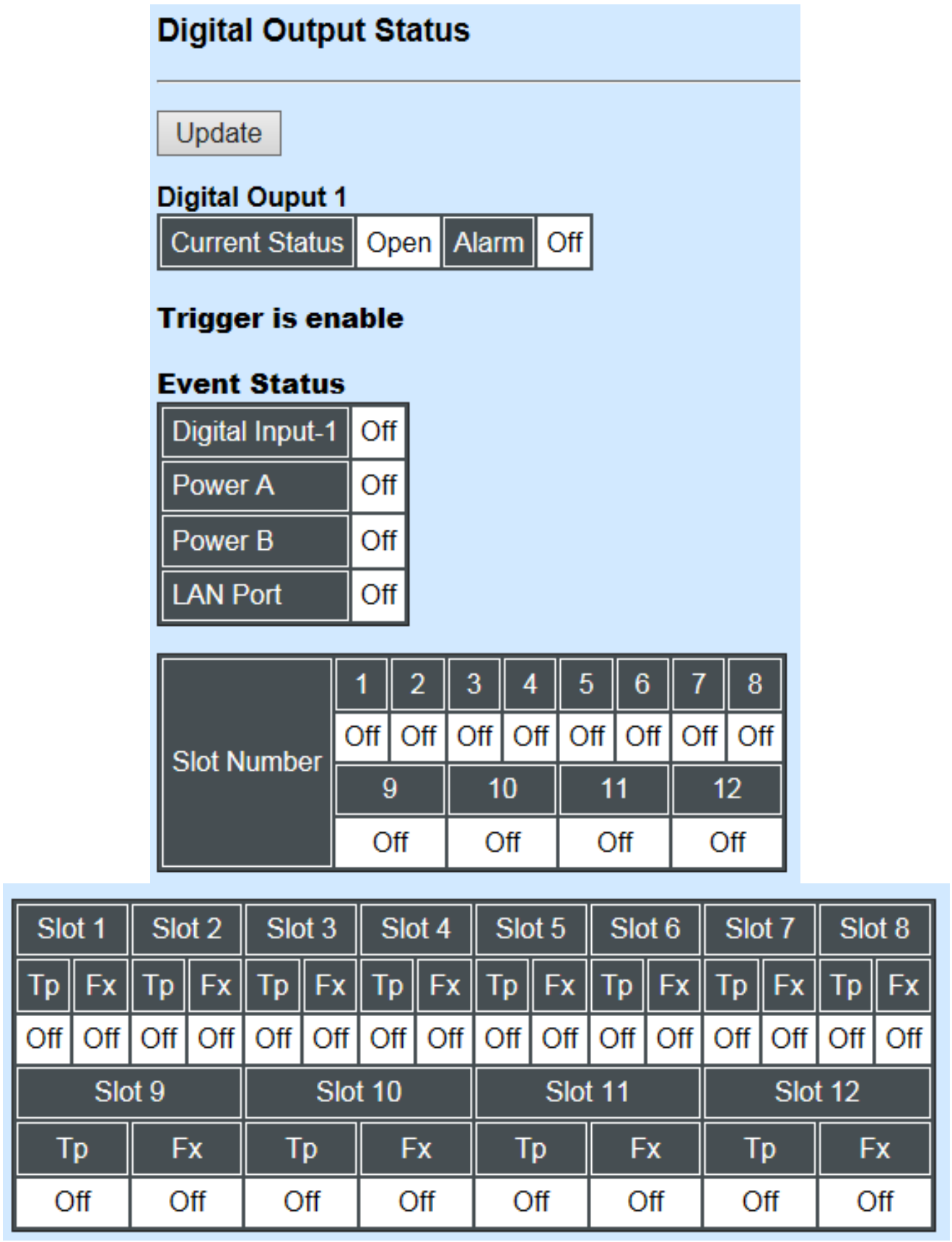
Current Status: Status at present is either Open or Close on electrical circuit.

Alarm: Shows whether the alarm is triggered. "On" indicates "triggered" and "Off" indicates "not triggered".

Note: *Remember to enable the desired Digital Output Event. Otherwise, the alarm status always shows OFF.*

Click **"Update"** to renew current status.

4.13.2 Digital Output Status



Digital Output Status

Update

Digital Ouput 1

Current Status	Open	Alarm	Off

Trigger is enable

Event Status

Digital Input-1	Off
Power A	Off
Power B	Off
LAN Port	Off

Slot Number	1	2	3	4	5	6	7	8
	Off	Off	Off	Off	Off	Off	Off	Off
	9		10		11		12	
	Off		Off		Off		Off	

Slot 1		Slot 2		Slot 3		Slot 4		Slot 5		Slot 6		Slot 7		Slot 8	
Tp	Fx	Tp	Fx	Tp	Fx	Tp	Fx	Tp	Fx	Tp	Fx	Tp	Fx	Tp	Fx
Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off
Slot 9				Slot 10				Slot 11				Slot 12			
Tp		Fx		Tp		Fx		Tp		Fx		Tp		Fx	
Off		Off		Off		Off		Off		Off		Off		Off	

Current Status: Status at present is either Open or Close on electrical circuit.

Alarm: Shows whether the alarm is triggered. “On” indicates “triggered” and “Off” indicates “not triggered”.

Event Status: This shows alarm status for each event. “On” indicates “triggered” and “Off” indicates “not triggered”.

Digital Input-1: The status of whether the alarm for Digital Input-1 has been triggered.

Power A: The status of whether the alarm for Power A has been triggered.

Power B: The status of whether the alarm for Power B has been triggered.

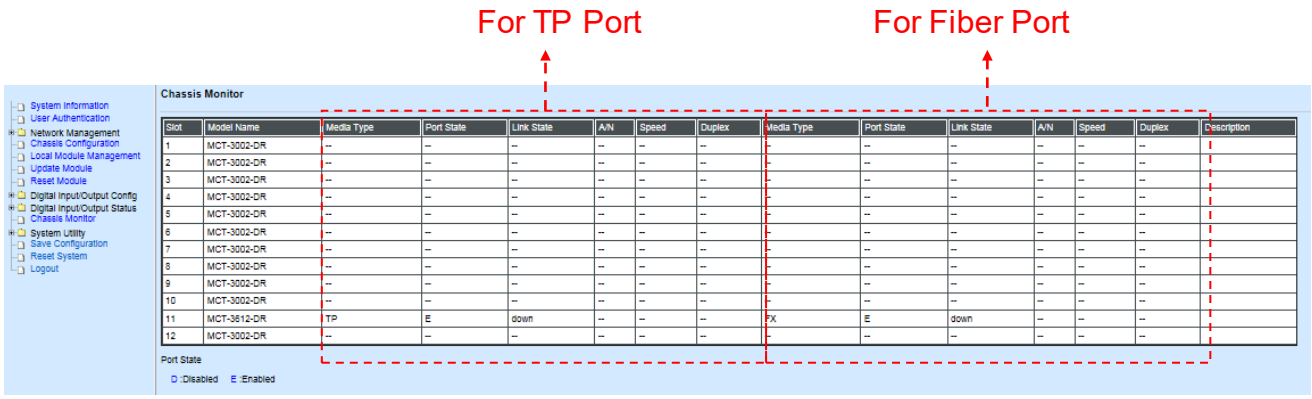
Slot Number: The status of whether the alarm for slots has been triggered.

Tp/Fx Port: The status of whether the alarm for Tp/Fx ports has been triggered.

***NOTE*:** *Remember to enable the desired Digital Output Event. Otherwise, the alarm status always shows OFF.*

4.14 Chassis Monitor

Select **Chassis Monitor** from the **Main Menu**, then the following screen page appears. This is intended to show overall status of converters.
The Chassis Monitor is mainly divided into two sections as below. The left squared section is for TP port while the right is for fiber port.



1. **Model Name:** Display the name of connected unit.
2. **Media Type:** TP (copper, 10/100Base-T, RJ-45) and FX (fiber).
3. **Port State:** View-only field that shows traffic is Disabled or Forwarding.
4. **Link State:** View-only field that shows the link is up or down.
5. **A/N:** View-only field that shows Auto-negotiation is on or off.
6. **Speed:** View-only field that shows the port speed.
7. **Duplex:** View-only field that shows the duplex mode is half or full.
8. **Description:** Specify the appropriate brief description for the slide-in converter module.

4.15 System Utility

System Utility allows users to easily operate and maintain the system. Select the option **System Utility** from the **Main Menu**, then the **System Utility** screen page shows up.

1. **Ping:** Ping can help you test the network connectivity between the CHASSIS and the host. You can also specify count s, timeout and size of the Ping packets.

2. **Event Log:** Event log can keep a record of system's log events such as system warm start, cold start, link up/down, user login/logout, etc. They will be kept only when your CPU version is A06 with Boot ROM version A08 or later version. If your CPU or Boot ROM version is older than the one mentioned above, all events will lose when the system is shut down or rebooted.

3. **HTTP Upgrade:** Users may save or restore their configuration and update their Firmware off-line.

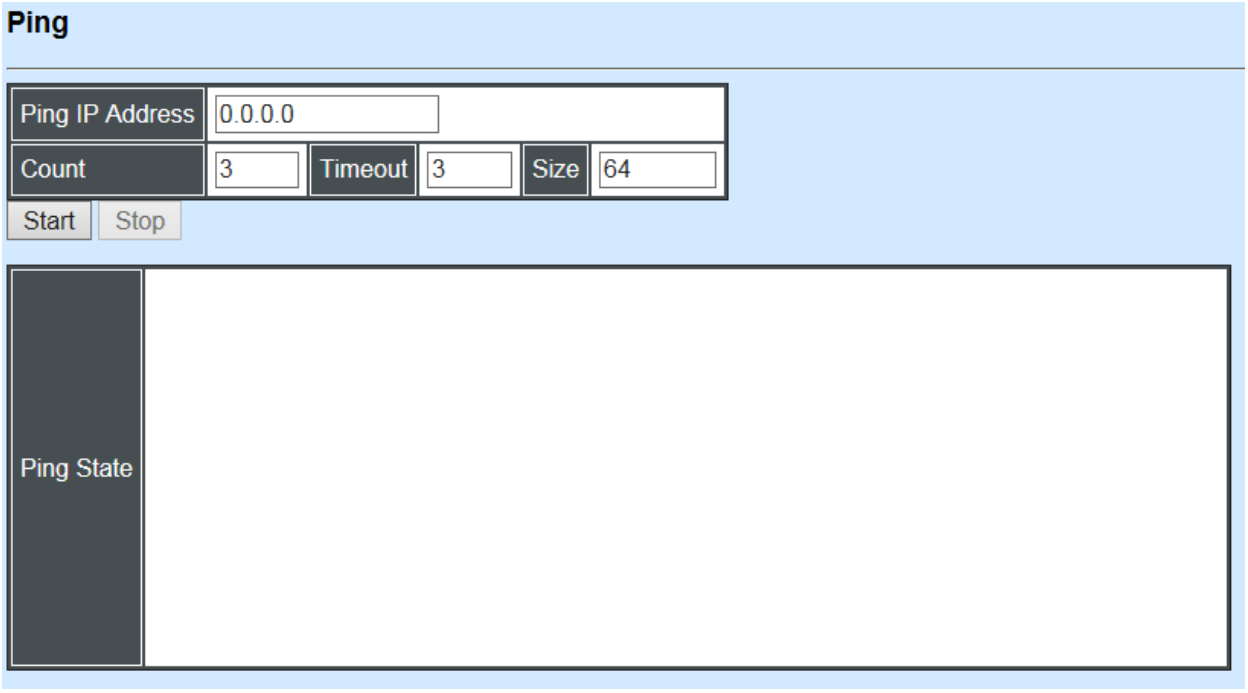
4. **FTR/TFTP Upgrade:** This allows users to update the latest firmware, save current configuration or restore previous configuration to the CHASSIS.

5. **Load Factory Setting:** Load Factory Setting will set the configuration of the CHASSIS back to the factory default settings. The IP and Gateway addresses will be set to the factory default as well.

6. **Load Factory Setting Except Network Configuration:** Selecting this function will also restore the configuration of the CHASSIS to its original factory default settings. However, this will not reset the IP and Gateway addresses to the factory default.

4.15.1 Ping

Ping can help you test the network connectivity between the CHASSIS and the host. Select **Ping** from the **System Utility** menu and then the following screen page appears.



You can also specify counts, timeout and size of the Ping packets.
Click **Start** to start the Ping process.

4.15.2 Event Log

Event Log will display all the CHASSIS system-related events recorded, including login, logout, time-out …etc. information Select **Event Log** from the **System Utility** menu, the following screen page shows up,

Event Log

Index	Type	Time	Up Time	Description	Source	Event	Name/Community	Address
1	I		0 day 00:01:13	System cold start.	local	cold start		
2	I		0 day 00:01:17	Case fan1 fan ok.	local	fan ok		
3	I		0 day 00:01:17	Case fan2 fan ok.	local	fan ok		
4	I		0 day 00:01:17	Case fan3 fan ok.	local	fan ok		
5	I		0 day 00:01:17	Case fan4 fan ok.	local	fan ok		
6	I		0 day 00:01:41	User from web login succeeded.	web	login	admin	192.168.0.2
7	I		0 day 00:15:02	Local slot 8 module up.	local	module up		
8	W		0 day 00:17:47	Local slot 8 module down.	local	module down		
9	I		0 day 00:17:56	Local slot 8 module up.	local	module up		
10	I		0 day 00:19:52	User from web logout.	web	logout	admin	192.168.0.2
11	I		0 day 00:20:01	User from web login succeeded.	web	login	admin	192.168.0.2
12	W		0 day 00:27:07	Local slot 8 module down.	local	module down		

This page records system-related events including link up/down, power supply status, case fan status, etc. You can remove all events from the table by clicking the **"Clear All"** button at the bottom of the table.

4.15.3 HTTP Update

Users may save or restore their configuration and update their Firmware off-line. Select **HTTP Upgrade** from the **System Utility** menu and then the following screen page appears.

HTTP Upgrade

Configuration Update

Backup	Config Type	Running-config
	device configuration to local file	Backup
Restore		Browse.. Restore

Firmware Update

Upgrade Image Option	Image1
Select File	Browse.. Upload

To backup or restore data, click **HTTP Upgrade**

Config Type

There are three types of Config Type: Running-config, Default-config and Start-up-config

Running-config: Back up the data you're processing

Default-config: Back up the data same as factory setting.

Start-up-config: Back up the data same as last saved data.

Device Configuration to Local File: Click **Backup** and define the route where you intend to save data.

Restore: Click **Browse**, select the designated data and then click **Restore**.

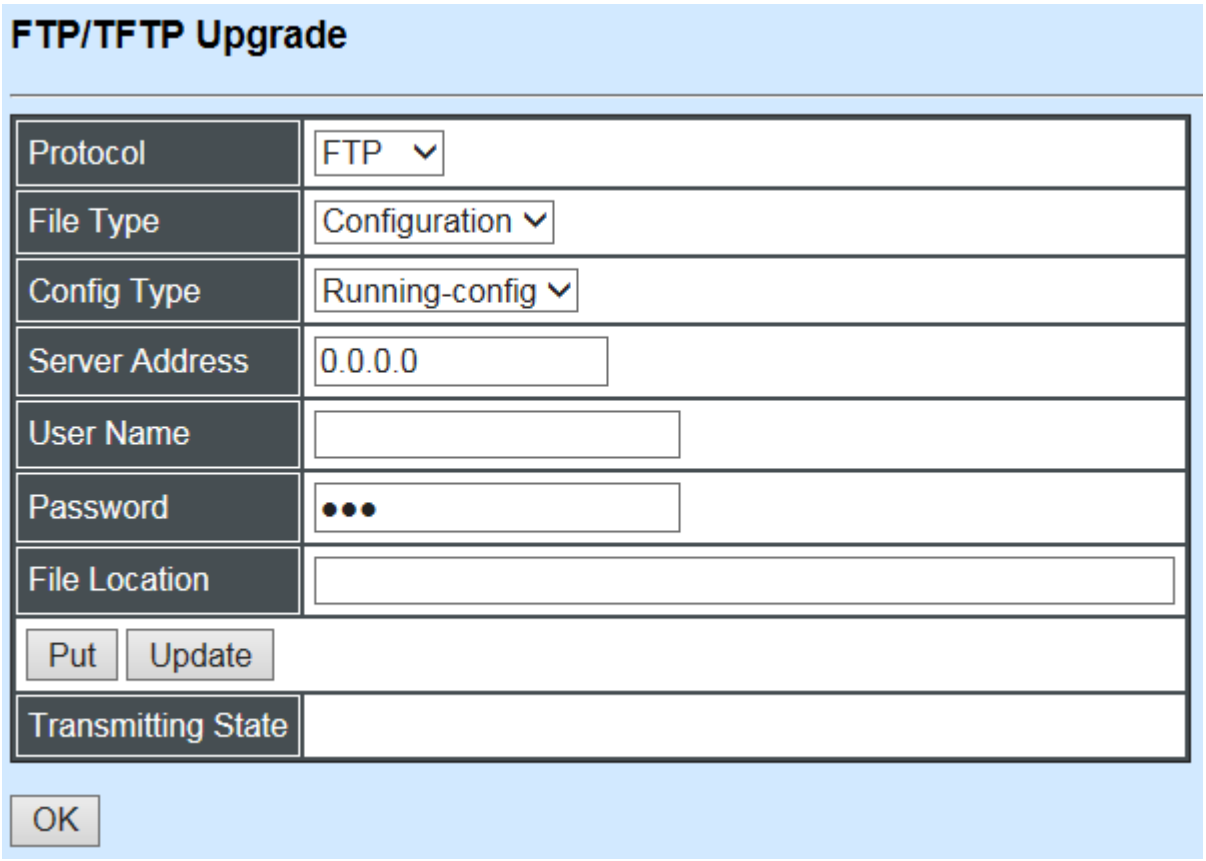
Firmware Update

Upgrade Image Option: Choose the image you want to upgrade.

Select File: Click browse, select the desired file and click **Upload.**

4.15.4 FTP/TFTP Upgrade

Select **FTP/TFTP Upgrade** from the **System Utility** folder, then the following screen page appears.



Protocol: Select the preferred protocol, either FTP or TFTP.

File Type: Select the appropriate file type that you would like to process. Select **"Configuration"**, if you would like to restore a configuration file. Select **"Firmware"**, if you would like to upgrade Firmware.

Config Type

There are three types of Config Type: Running-config, Default-config and Start-up-config

Running-config: Back up the data you're processing

Default-config: Back up the data same as factory setting.

Start-up-config: Back up the data same as last saved data.

Server Address: Enter the specific IP address of the File Server.

User Name: Enter the specific username to access the File Server.

Password: Enter the specific password to access the File Server.

File Location: Enter the specific path and filename within the File Server.

Click **OK** to start the download process and receive files from the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind the user.

Click **Put** to start the upload process and transmit files to the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind users.

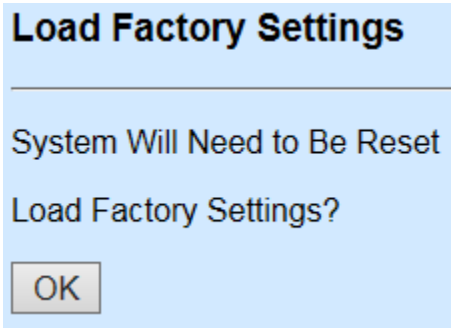
Select **Update** then press **Enter** to instruct the CHASSIS to update existing firmware/configuration to the latest firmware/configuration received. After a successful update, a message will pop up. The CHASSIS will need a reset to make changes effective.

4.15.5 Load Factory Settings

Load Factory Setting will set all the configuration of the CHASSIS back to the factory default settings, including the IP and Gateway address. **Load Factory Setting** is useful when network administrator needs to re-configure the system.

A system reset is required to make all changes effective after **Load Factory Setting**.

Select **Load Factory Settings** from the **System Utility** menu, then the following screen page shows up.



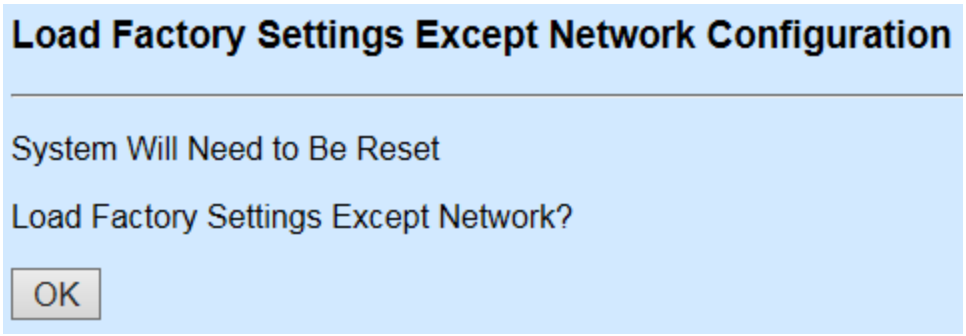
To load Factory Setting, press **OK**.

4.15.6 Load Factory Setting Except Network Configuration

Load Factory Setting Except Network Configuration will set all the configuration of the CHASSIS back to the factory default settings. However, the IP and Gateway addresses will not be changed back to the factory default settings.

Load Factory Setting Except Network Configuration is very useful when a network administrator needs to re-configure the system "REMOTELY". Because traditional Factory Reset will set the network setting back to the default and all current network connections might be lost then.

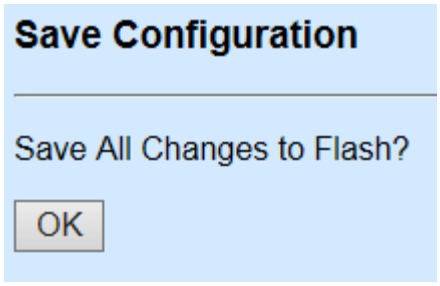
Select **Load Factory Setting Except Network Configuration** from the **System Utility** menu, then the following screen page shows up.



To load Factory Setting Except Network Configuration, press **OK**.

4.16 Save Configuration

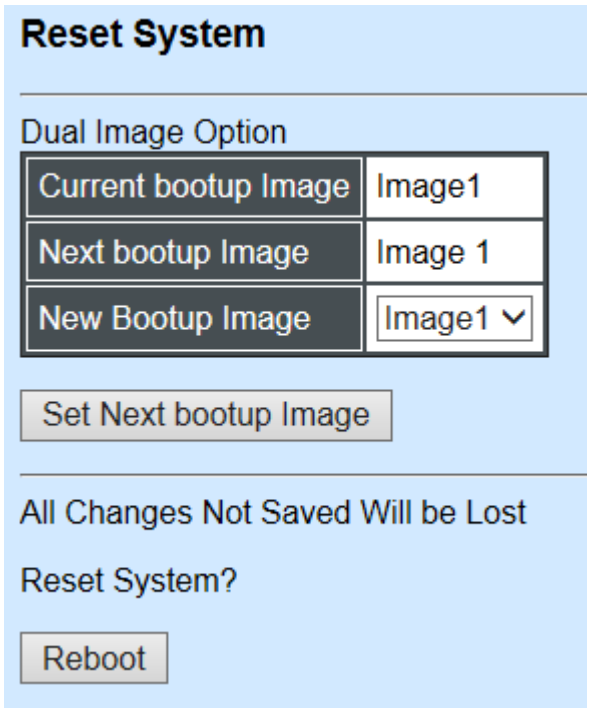
In order to save configuration setting permanently, user needs to **Save Configuration** first before resetting the CHASSIS. Select **Save Configuration** from the **Main Menu**, the following screen page shows up.



To save Configuration before resetting system, press **OK**.

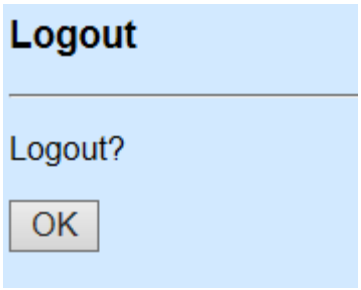
4.17 Reset System

After any configuration changes, **Reset System** can make changes effective. Select **Reset System** from the **Main Menu** and then the following screen page appears.



To perform System Reset, press **OK**.
This pop-up message alerts the user that the configuration change will take effect after a reset. However, before performing System Reset, users must save the configuration change first.

4.18 Logout



Click **“OK”** to log out.

APPENDIX A: DHCP Auto-Provisioning Setup

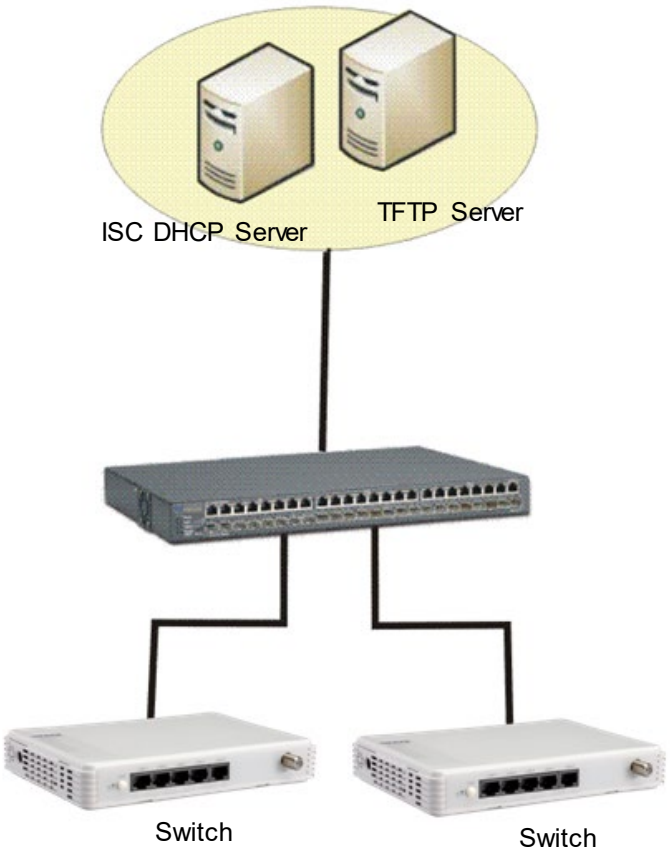
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Chassis that you purchased supports DHCP Auto-provisioning. Setup procedures and auto-provisioning process are described below for your reference.

A. Setup Procedures

Follow the steps below to set up Auto Provisioning server, modify dhcpd.conf file and generate a copy of configuration file.

Step 1. Set Up Environment

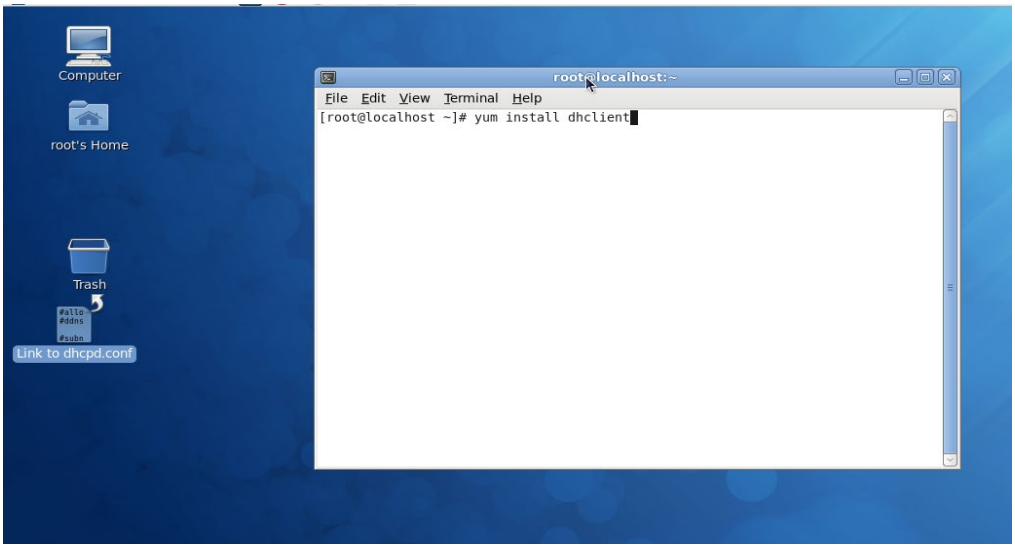
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

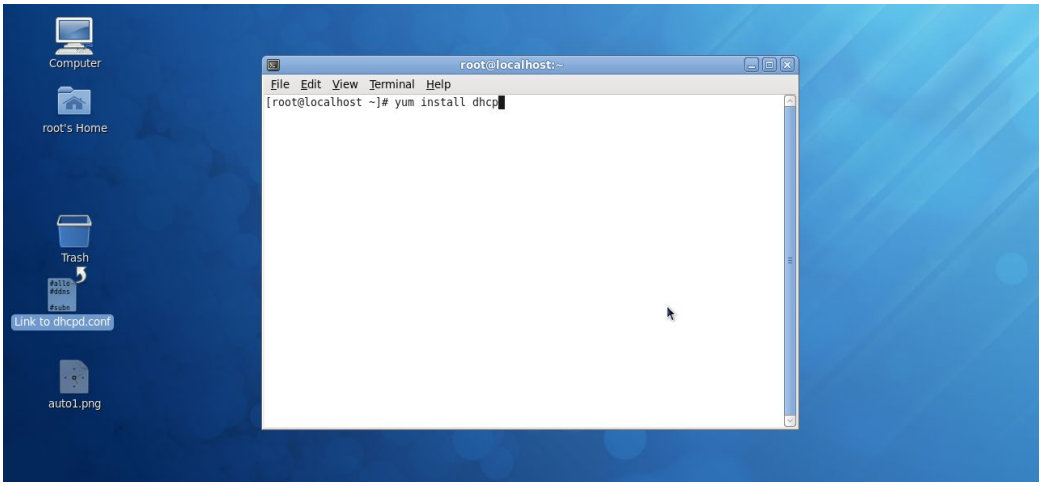
Step 2. Set Up Auto Provision Server

- **Update DHCP client**



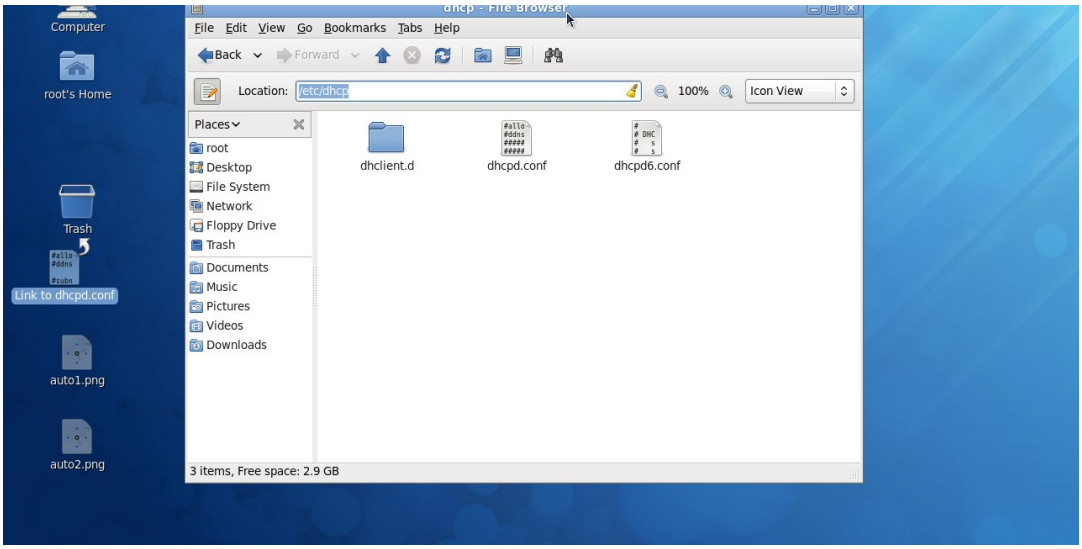
Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

- **Install DHCP server**



Issue “yum install dhcp” command to install DHCP server.

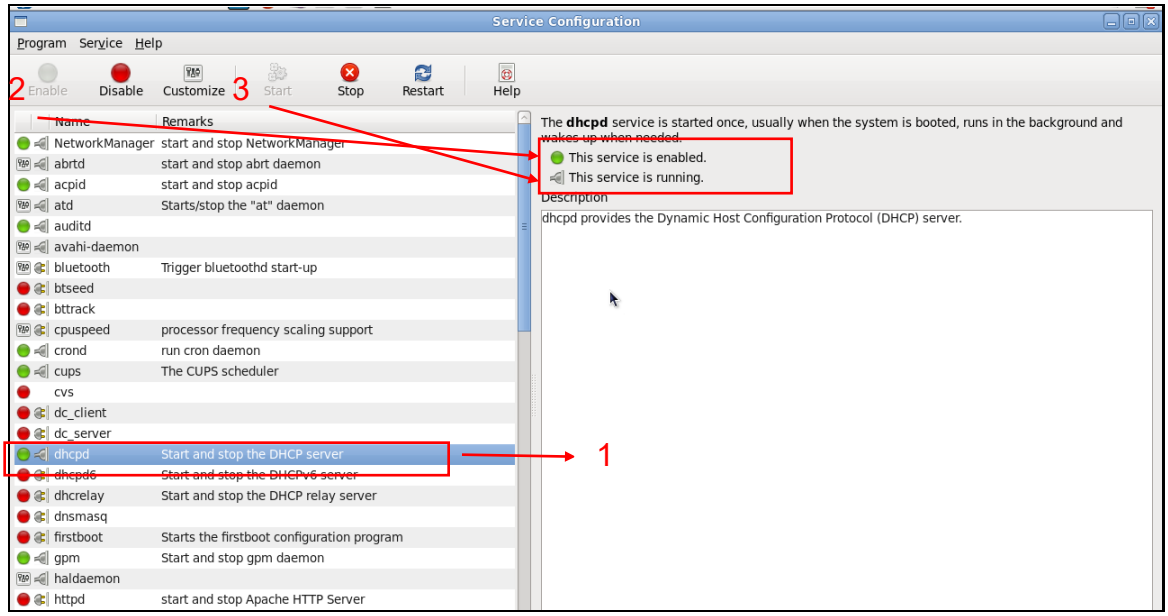
- **Copy dhcpd.conf to /etc/dhcp/ directory**



Copy dhcpd.conf file provided by the vendor to /etc/dhcp/ directory.

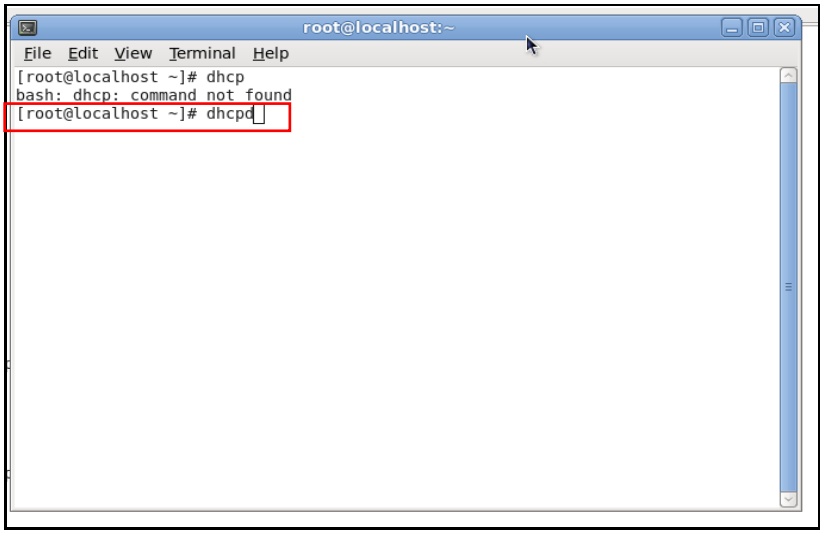
Please note that each vendor has its own way to define auto-provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



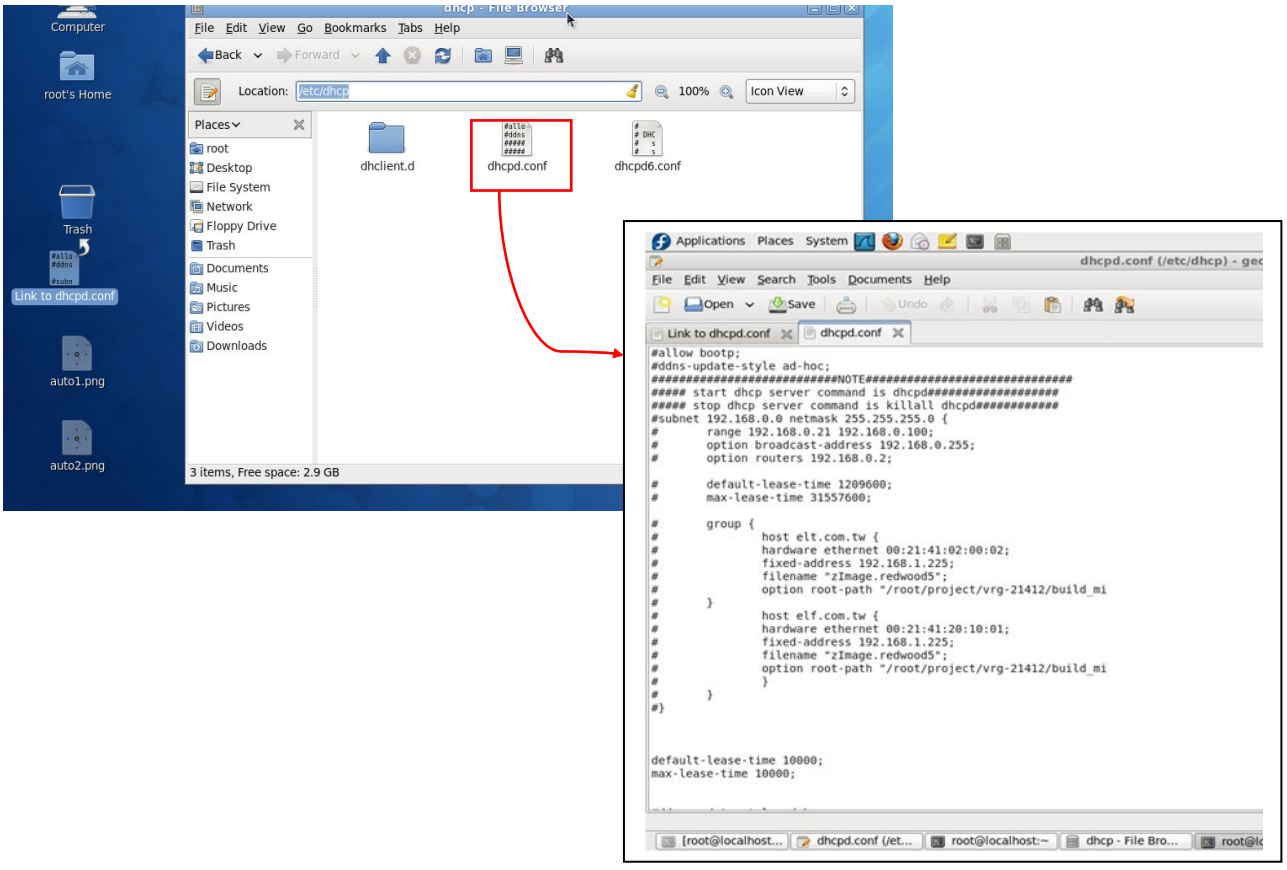
1. Choose dhcpd.
2. Enable DHCP service.
3. Start running DHCP service.

NOTE: *DHCP service can also be enabled using CLI. Issue "dhcpd" command to enable DHCP service.*



Step 3. Modify dhcpd.conf File

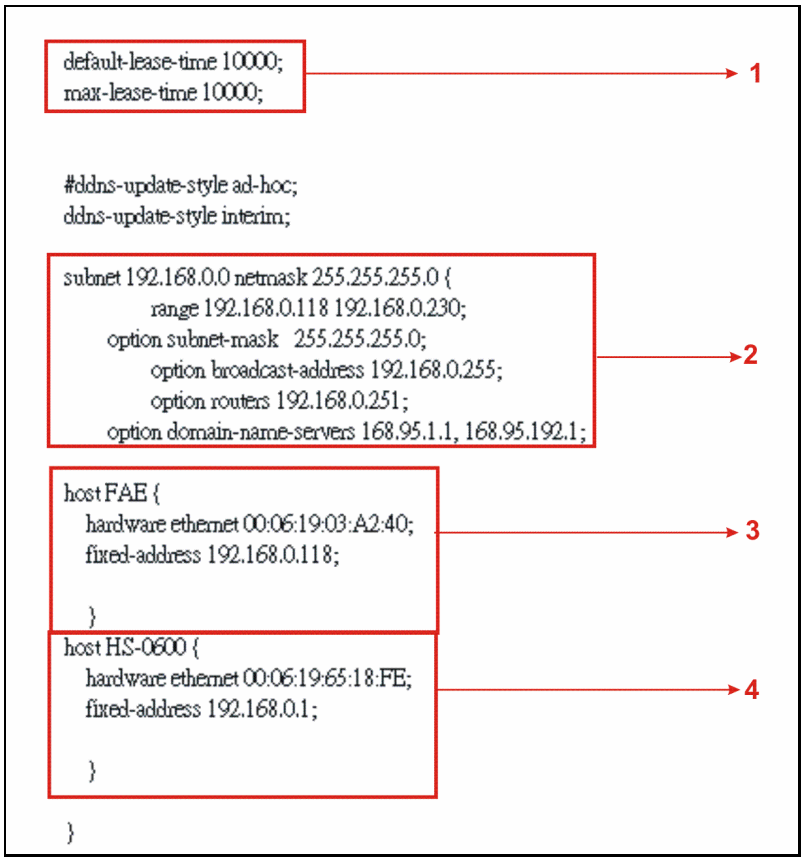
- **Open dhcpd.conf file in /etc/dhcp/ directory**



Double-click dhcpd.conf placed in /etc/dhcp/ directory to open it.

Modify dhcpd.conf file

The following marked areas in dhcpd.conf file can be modified with values that work with your networking environment.



1. Define DHCP default and maximum lease time in seconds.

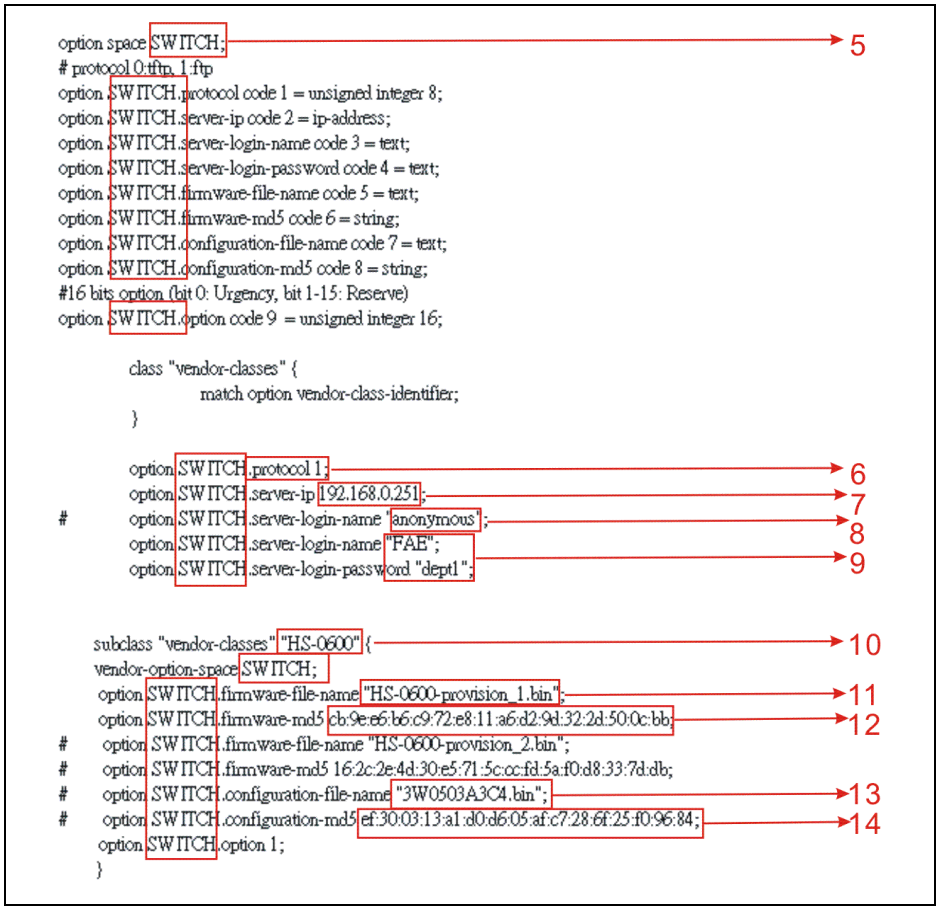
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

   Maximum lease time: This is the maximum length of time that the server will lease for.

2. Define subnet, subnet mask, IP range, broadcast address, router address and DNS server address.

3. Map a host's MAC address to a fixed IP address.

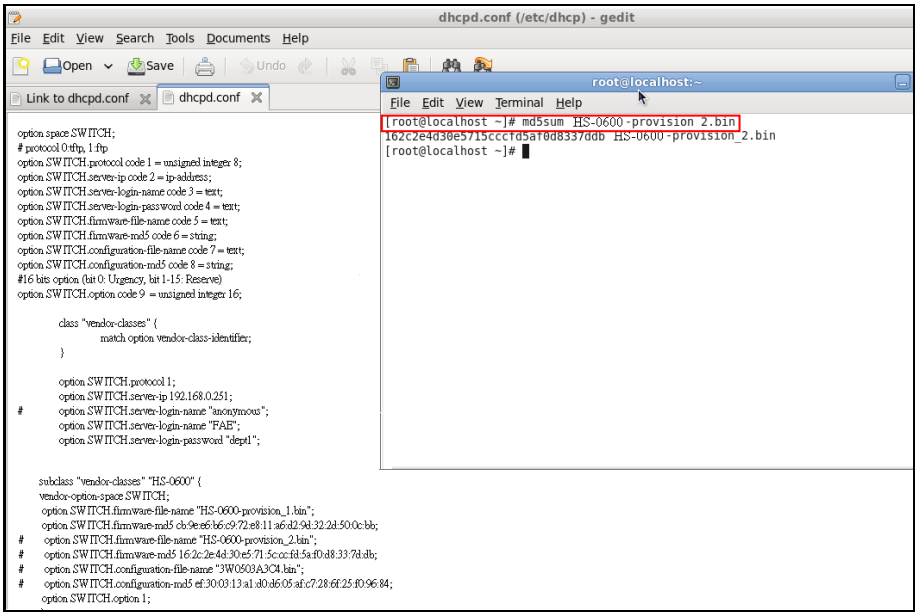
4. Map a host's MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.



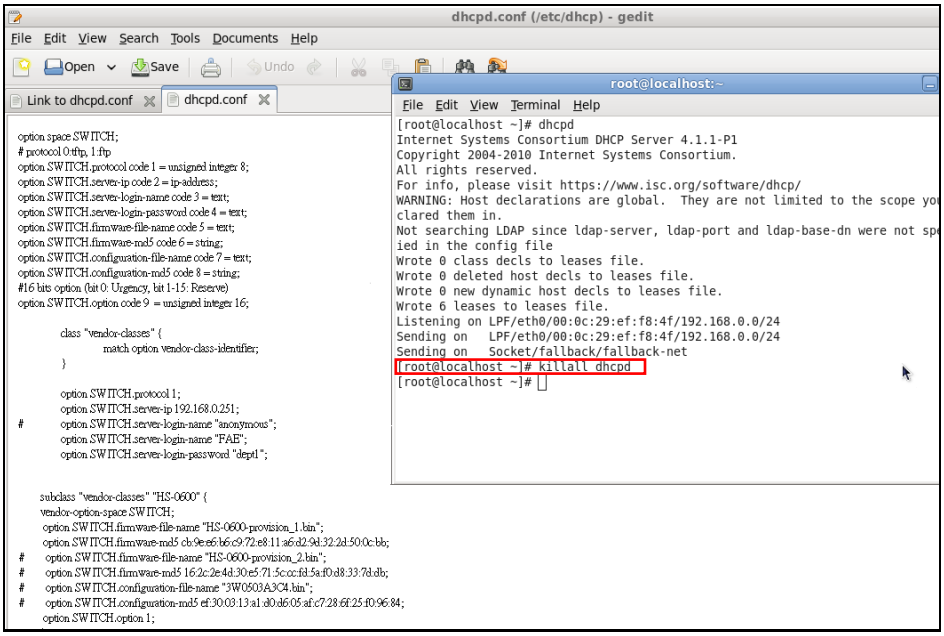
5. This value is configurable and can be defined by users.
6. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
7. Specify the FTP or TFTP IP address.
8. Login TFTP server anonymously (TFTP does not require a login name and password).
9. Specify FTP Server login name and password.
10. Specify the product model name.
11. Specify the firmware filename.
12. Specify the MD5 for firmware image.
13. Specify the configuration filename.
14. Specify the MD5 for configuration file.

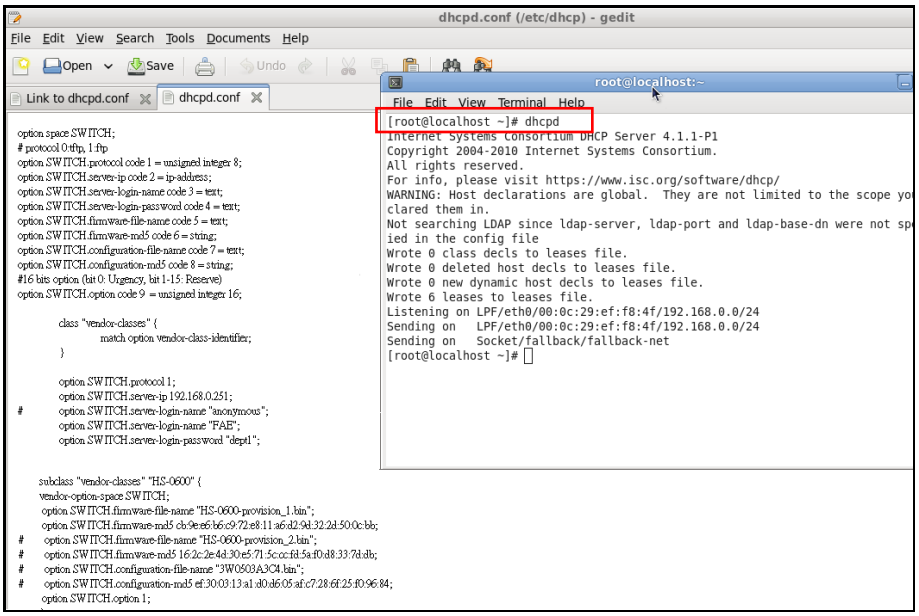
NOTE 1: *The text beginning with a pound sign (#) will be ignored by the DHCP server. For example, in the figure shown above, firmware-file-name "HS-0600-provision_2.bin" and firmware-md5 (line 5 & 6 from the bottom) will be ignored. If you want DHCP server to process these two lines, remove pound signs in the initial of each line.*

NOTE 2: *You can use either free software program or Linux default md5sum function to get MD5 checksum for firmware image and configuration file.*



- **Restart DHCP service**





Every time you modify dhcpd.conf file, DHCP service must be restarted. Issue “killall dhcpd” command to disable DHCP service and then issue “dhcpd” command to enable DHCP service.

Step 4. Backup a Configuration File

Before preparing a configuration file in TFTP/FTP Server, make sure the device generating the configuration file is set to **“Get IP address from DHCP”** assignment. DHCP Auto-provisioning is running under DHCP mode, so if the configuration file is uploaded by the network type other than DHCP mode, the downloaded configuration file has no chance to be equal to DHCP when provisioning, and it results in MD5 never matching and causes the device to reboot endlessly.

In order to have your Chassis retrieve the correct configuration image in TFTP/FTP Server, please make sure the filename of your configuration file is defined exactly the same as the one specified in **dhcpd.conf**. For example, if the configuration image’s filename specified in dhcpd.conf is “metafile”, the configuration image filename should be named to “metafile” as well.

Step 5. Place a Copy of Firmware and Configuration File in TFTP/FTP

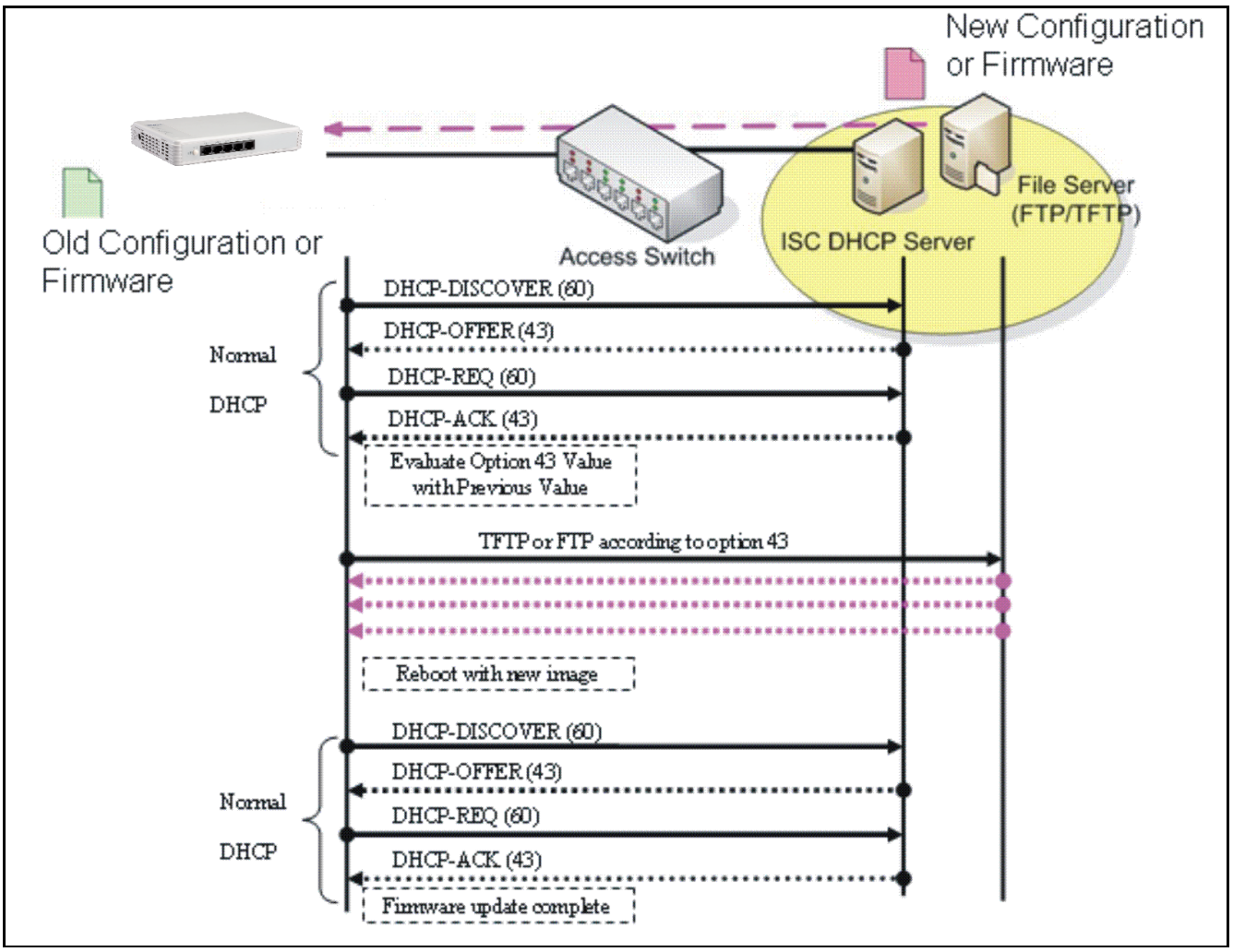
The TFTP/FTP File server should include the following items:

1. Firmware image (This file is provided by the vendor.)
2. Configuration file (This file is generally created by users.)
3. User account for your device (For FTP server only.)

B. Auto-Provisioning Process

This switching device is setting-free (through auto-upgrade and configuration) and its upgrade procedures are as follows:

1. ISC DHCP server will recognize the device when it receives an IP address request sent by the device, and it will tell the device how to get a new firmware or configuration.
2. The device will compare the firmware and configuration MD5 code form of DHCP option every time it communicates with DHCP server.
3. If MD5 code is different, the device will then upgrade the firmware or configuration. However, it will not be activated immediately.
4. If the Urgency Bit is set, the device will be reset to activate the new firmware or configuration immediately.
5. The device will retry for 3 times if the file is incorrect, and then it gives up until getting another DHCP ACK packet again.



APPENDIX B: Free RADIUS readme

The advanced RADIUS Server Set up for **RADIUS Authentication** is described as below.

When free RADIUS client is enabled on the device,

On the server side, it needs to put this file "**dictionary.sample**" under the directory **/raddb**, and modify these three files - "**users**", "**clients.conf**" and "**dictionary**", which are on the disc shipped with this product.

* Please use any text editing software (e.g. Notepad) to carry out the following file editing works.

In the file "**users**",

Set up user name, password, and other attributes.

In the file "**clients.conf**",

Set the valid range of RADIUS client IP address.

In the file "**dictionary**",
Add this following line -

$INCLUDE dictionary.sample

APPENDIX C: MCT-3512 Converter

This section is used to introduce 10/100/1000BASE-T to 100/1000BASE-X with 802.3ah OAM compliance standalone Media Converter which is specifically designed to fulfill emerging deployment needs of fiber Ethernet networks. The OAM Media Converter has built-in management module that allows users to configure the device and monitor the operation status both locally and remotely through the network.

The Ethernet OAM (802.3ah) protocol for installing, monitoring, and troubleshooting Metro Ethernet networks and Ethernet WANs relies on an optional sublayer in the data link layer of the Normal link operation. Ethernet OAM can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link for a network or part of a network.
IEEE 802.3ah provides the following features:

Auto-discovery: IEEE 802.3ah provides a mechanism to detect the presence of an 802.3ah-capable Network Device (ND) on the other end of the Ethernet link. To this end, the 802.3ah-capable ND sends specified OAMPDUs in a periodic fashion, normally once a second. During the OAM Discovery process, the 802.3ah-capable ND monitors received OAMPDUs from the remote ND and allows 802.3ah OAM functionality to be enabled on the link based upon local and remote state and configuration settings. In other words, it supports OAM capability discovery function and hence eliminates the need for operators" configurations.

Remote loopback: IEEE 802.3ah provides a mechanism to support a data link layer frame-level loopback mode. With this function, the operator may test the performance of the link prior to placing a link in service. Once the Ethernet physical link is verified to be operational and error-free, the operator takes the link out of remote loopback and places it in service.

C.1 CLI Command

This is to how the OAM converter is presented via CLI Command.

C.1.1 Local OAM Module Configuration

This section is intended to introduce the configuration of specified OAM media converters.

Note: *Make sure that media converts are firmly installed and powered on.*

1. Specify any slots to configure

Slot command	Parameter	Description
MCT-RACK(config)# slot [slot_list]	[slot_list]	Specify any slots you want to configure.

2. Upgrade media converter firmware

Slot command	Parameter	Description
MCT-RACK(config-slot-		Upgrade the firmware.

slot-slot)# firmware upgrade		**Note:** Upgrade one media converter at a time.

3. Configure link alarm

When UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module link-alarm		Enable link alarm function.
No Command		
MCT-RACK(config-slot-slot-slot)# no module link-alarm		Disable link alarm function.
Show Command		
MCT-RACK(config-slot-slot-slot)# show module		Show the status of link alarm.

4. Set up module description

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module-info description [description]	[description]	Specify user-defined information. Up to 55 characters are available.
No Command		
MCT-RACK(config-slot-slot-slot)# no module-info description		Delete user-defined information.
Show Command		
MCT-RACK(config-slot-slot-slot)# show module-info		Show the module information.
Module Description Example		
MCT-RACK(config-slot-slot-slot)# module-info description 123		The description of the converter is named “123”.

5. Reset converter

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# reload		Reboot the media converters.

6. Set up security protection

When a device on the network is malfunctioning or application programs are not well designed or properly configured, broadcast storms may occur, which may degrade network performance or in the worst situation cause a complete halt. The Chassis allows users to set a threshold rate for broadcast traffic so as to protect network from broadcast storms. Any broadcast packet exceeding the specified value will then be dropped.

Security command	Parameter	Description
MCT-RACK(config)# security storm-protection		Enable storm protection function.
MCT-RACK(config)# security storm-protection rates [32-1000000] kbps	[32-1000000] kbps	Specify the maximum broadcast packet rate.
No command		
MCT-RACK(config)# no security storm-protection		Disable storm protection globally.
MCT-RACK(config)# no security storm-protection rates		Set broadcast packet rate back to the default.
Show command		
MCT-RACK(config)# show security storm-protection		Show storm control settings.

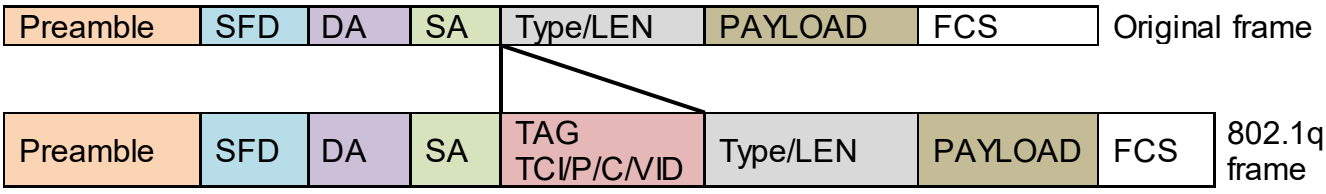
7. Set up VLAN configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the device on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be ‘moved’ to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

IEEE 802.1Q VLAN Concepts

Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes		User data	
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During

data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.

Example : PortX configuration

Configuration	Result
Trunk-VLAN = 10, 11, 12 Access-VLAN = 20 **Mode = Access**	PortX is an **Access Port** PortX's **VID** is ignored PortX's **PVID** is 20 PortX sends **Untagged** packets (PortX takes away VLAN tag if the PVID is 20) PortX receives **Untagged** packets only
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Trunk**	PortX is a **Trunk Port** PortX's **VID** is 10,11 and 12 PortX's **PVID** is ignored PortX sends and receives **Tagged** packets VID 10,11 and 12
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Trunk-native**	PortX is a **Trunk-native Port** PortX's **VID** is 10,11 and 12 PortX's **PVID** is 20 PortX sends and receives **Tagged** packets VID 10,11 and 12 PortX receives **Untagged** packets and add PVID 20

The CHSSSIS supports two types of VLAN, these are: **IEEE 802.1q Tag VLAN** and **Q-in-Q VLAN.**

VLAN Command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# vlan dot1q-vlan		Enable IEEE 802.1q Tag VLAN mode.
MCT-RACK(config-slot-slot-slot)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VID number to create an 802.1q VLAN. **Note :** 802.1q VLAN ID needs to be created under interface command. In here you can only modify it instead of creating a new VLAN ID.

MCT-RACK(config-slot-slot-slot)# vlan qinq-vlan		Enable Q-in-Q VLAN.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan bypass-ctag		Ignore the C-tag checking.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan isp-port [port_list]	[port_list]	Configure ISP Port (Q-in-Q Port). **ISP(Internet Service Provider) Port:** This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan stag-ethertype [0xWXYZ]	[0xWXYZ]	Specify service tag ether type. **Ether Type:** A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).
No Command		
MCT-RACK(config-slot-slot-slot)# no vlan dot1q-vlan		Disable IEEE 802.1q Tag VLAN mode.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan		Disable Q-in-Q VLAN.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan bypass-ctag		Not ignore the C-tag checking.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan isp-port		Undo ISP port (Q-in-Q port).
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan management-stag		Clear management service tag VID.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan stag-ethertype		Delete service tag ether type.
Show Command		
MCT-RACK(config-slot-slot-slot)# show vlan dot1q-vlan		Show dot1q VLAN configuration.
MCT-RACK(config-slot-slot-slot)# show vlan interface		Show all interfaces on a media converter
MCT-RACK(config-slot-slot-slot)# show vlan interface [port_list]	[port_list]	Show specific interfaces on a media converter
MCT-RACK(config-slot-slot-slot)# show vlan qinq-vlan		Show Q-in-Q VLAN configuration.

8. Use "Slot" command to configure 802.1q VLAN settings on a port.

Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.

MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid [1-4094]	[1-4094]	Specify the service tag VID for the selected port(s).
No Command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid		Clear the service tag VID specified.

9. Use "Slot" command set up OAM function.

Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# oam mode [active | passive]	[port_list]	Specify OAM mode, either Active or Passive. To perform remote management, it's strongly recommended that OAM Mode be set "Active".
MCT-RACK(config-slot-slot-slot-if-port-port)# oam loopback		Enable Loopback function. A loopback test is a test in which a signal in sent from a communications device and returned (looped back) to it as a way to determine whether the device is working right or as a way to pin down a failing node in a network.
MCT-RACK(config-slot-slot-slot-if-port-port)# oam loopback diagnostics		Execute loopback test. That the Packet of Tx is equal to that of Rx indicates the link is working normal and the result of test shows "Success". If the Tx is not the same as Rx, which means some packet are dropped during the link transmission, the result of test shows "Fail".
No Command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no oam		Globally disable OAM function.
MCT-RACK(config-slot-slot-slot-if-port-port)# no oam mode		Return OAM mode to default.
MCT-RACK(config-slot-slot-slot-if-port-port)# no oam loopback		Disable Loopback function.

C.1.2 Local OAM Module Port Configuration

This is to configure port via "interface" command.

This command is to configure TP port or fiber port on a converter.

Interface command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.

1. Configure auto-negotiation function.

Interface command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# auto-		Set the selected interfaces' to auto-negotiation. When auto-negotiation is

negotiation		enabled, speed configuration will be ignored.
No command		**No command**
MCT-RACK(config-slot-slot-slot-if-port-port)# no auto-negotiation		Disable auto-negotiation function.

2. Set up Duplex Mode

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# duplex [full]	[full]	Configure port duplex to **full**.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no duplex		Set the selected ports' duplex mode to the default setting. **Note :** Auto-negotiation needs to be disabled before configuring duplex mode.

3. QoS configuration

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# qos rate-limit ingress [0|32-1000000]	[0|32-1000000]	Configure **ingress** rate limit, set zero or from 32Kbps to 1000Mbps.
MCT-RACK(config-slot-slot-slot-if-port-port)# qos rate-limit egress [0|32-1000000]	[0|32-1000000]	Configure **egress** rate limit, set zero or from 32Kbps to 1000Mbps.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no qos rate-limit ingress		Undo **ingress** rate limit.
MCT-RACK(config-slot-slot-slot-if-port-port)# no qos rate-limit egress		Undo **egress** rate limit.

4. Shutdown interface

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# shutdown		Administratively disable the selected ports' status.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no shutdown		Administratively enable the selected ports' status.

5. Speed configuration

Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# speed [1000 |100 | 10 | auto_sense]	[1000 |100 | 10 | auto_sense]	Set up the selected interfaces' speed. Manual speed configuration only works when "no auto-negotiation" command is issued.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no speed		Set the selected ports' speed to the default setting.

6. Configure 802.1q VLAN settings on a port.

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid [1-4094]	[1-4094]	Specify the service tag VID for the selected port(s).
No Command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan access-		Set the selected ports' PVID to the default setting.

vlan		
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid		Clear the service tag VID specified.

C.1.3 Remote OAM Module Configuration

This section is intended to introduce the configuration of specified remote media converters.

Note: *Make sure that media converts are firmly installed and powered on.*

1. Specify any remote converter to configure

Command	Parameter	Description
MCT-RACK(config)# remote [remote_list]	[remote_list]	Specify any remote converter you want to configure.

2. Upgrade media converter firmware

Command	Parameter	Description
MCT-RACK(config-remote-No.)# firmware upgrade		Upgrade the firmware of remote converter.

3. Configure link alarm

When UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.

Command	Parameter	Description
MCT-RACK(config-remote-No.)# module link-alarm		Enable link alarm function.
No Command		
MCT-RACK(config-remote-No.)# no module link-alarm		Disable link alarm function.
Show Command		
MCT-RACK(config-remote-No.)# show module		Show the status of link alarm.

4. Set up module description

Command	Parameter	Description
MCT-RACK(config-remote-No.)# module-info description [description]	[description]	Specify user-defined information. Up to 55 characters are available.
No Command		
MCT-RACK(config-remote-No.)# no module-info description		Delete user-defined information.
Show Command		
MCT-RACK(config-remote-No.)# show module-info		Show the module information.
Module Description Example		
MCT-RACK(config-remote-No.)# module-info description 123		The description of the converter is named “123”.

5. Reset converter

Command	Parameter	Description
MCT-RACK(config-remote-No.)# reload		Reboot the media converters.

6. Set up security protection

When a device on the network is malfunctioning or application programs are not well designed or properly configured, broadcast storms may occur, which may degrade network performance or in the worst situation cause a complete halt. The Chassis allows users to set a threshold rate for broadcast traffic so as to protect network from broadcast storms. Any broadcast packet exceeding the specified value will then be dropped.

Security command	Parameter	Description
MCT-RACK(config-remote-No.)# security storm-protection		Enable storm protection function.
MCT-RACK(config-remote-No.)# security storm-protection rates [32-1000000] kbps	[32-1000000] kbps	Specify the maximum broadcast packet rate.
No command		
MCT-RACK(config-remote-No.)# no security storm-protection		Disable storm protection globally.
MCT-RACK(config-remote-No.)# no security storm-protection rates		Set broadcast packet rate back to the default.
Show command		
MCT-RACK(config-remote-No.)# show security storm-protection		Show storm control settings.

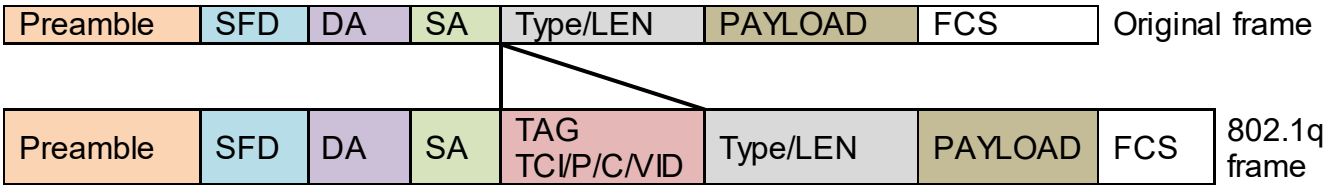
7. Set up VLAN configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the device on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

IEEE 802.1Q VLAN Concepts

Introduction to 802.1Q frame format:



PRE Preamble	62 bits	Used to synchronize traffic
SFD Start Frame Delimiter	2 bits	Marks the beginning of the header
DA Destination Address	6 bytes	The MAC address of the destination
SA Source Address	6 bytes	The MAC address of the source
TCI Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P Priority	3 bits	Indicates 802.1p priority level 0-7
C Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes	User data	
FCS Frame Check Sequence	4 bytes	Cyclical Redundancy Check

Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a

time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.

Example : PortX configuration

Configuration	Result
Trunk-VLAN = 10, 11, 12 Access-VLAN = 20 **Mode = Access**	PortX is an **Access Port** PortX's **VID** is ignored PortX's **PVID** is 20 PortX sends **Untagged** packets (PortX takes away VLAN tag if the PVID is 20) PortX receives **Untagged** packets only
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Trunk**	PortX is a **Trunk Port** PortX's **VID** is 10,11 and 12 PortX's **PVID** is ignored PortX sends and receives **Tagged** packets VID 10,11 and 12
Trunk-VLAN = 10,11,12	PortX is a **Trunk-native Port**

Access-VLAN = 20 **Mode = Trunk-native**	PortX's **VID** is 10,11 and 12 PortX's **PVID** is 20 PortX sends and receives **Tagged** packets VID 10,11 and 12 PortX receives **Untagged** packets and add PVID 20

The CHSSSIS supports two types of VLAN, these are: **IEEE 802.1q Tag VLAN** and **Q-in-Q VLAN.**

VLAN Command	Parameter	Description
MCT-RACK(config-remote-No.)# vlan dot1q-vlan		Enable IEEE 802.1q Tag VLAN mode.
MCT-RACK(config-remote-No.)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VID number to create an 802.1q VLAN. **Note :** 802.1q VLAN ID needs to be created under interface command. In here you can only modify it instead of creating a new VLAN ID.
MCT-RACK(config-remote-No.-vlan-No.)# name [vlan_name]	[vlan_name]	Specify the VLAN a name, up to 15 characters.
MCT-RACK(config-remote-No.)# vlan qinq-vlan		Enable Q-in-Q VLAN.
MCT-RACK(config-remote-No.)# vlan qing-vlan bypass-ctag		Ignore the C-tag checking.
MCT-RACK(config-remote-No.)# vlan qing-vlan isp-port [port_list]	[port_list]	Configure ISP Port (Q-in-Q Port). **ISP(Internet Service Provider) Port:** This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.
MCT-RACK(config-remote-No.)# vlan qing-vlan stag-ethertype [0xWXYZ]	[0xWXYZ]	Specify service tag ether type. **Ether Type:** A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).
No Command		
MCT-RACK(config-remote-No.)# no vlan dot1q-vlan		Disable IEEE 802.1q Tag VLAN mode.
MCT-RACK(config-remote-No.)# no vlan qinq-vlan		Disable Q-in-Q VLAN.
MCT-RACK(config-remote-No.)# no vlan qinq-vlan bypass-ctag		Not ignore the C-tag checking.
MCT-RACK(config-remote-No.)# no vlan qinq-vlan isp-port		Undo ISP port (Q-in-Q port).

MCT-RACK(config-remote-No.)# no vlan qinq-vlan stag-ethertype		Delete service tag ether type.
Show Command		
MCT-RACK(config-remote-No.)# show vlan dot1q-vlan		Show dot1q VLAN configuration.
MCT-RACK(config-remote-No.)# show vlan interface		Show all interfaces on a media converter.
MCT-RACK(config-remote-No.)# show vlan interface [port_list]	[port_list]	Show specific interfaces on a media converter.
MCT-RACK(config-remote-No.)# show vlan qinq-vlan		Show Q-in-Q VLAN configuration.

C.1.4 Remote OAM Module Port Configuration

This is to configure port via “interface” command.

This command is to configure TP port or fiber port on a remote converter.

Interface command	Parameter	Description
MCT-RACK(config-remote-No.)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port “1” represents TP port while port “2” fiber port.

1. Configure auto-negotiation function.

Interface command	Parameter	Description
MCT-RACK(config-remote-No.-if-No.)# auto-negotiation		Set the selected interfaces’ to auto-negotiation. When auto-negotiation is enabled, speed configuration will be ignored.
No command		**No command**
MCT-RACK(config-remote-No.-if-No.)# no auto-negotiation		Disable auto-negotiation function.

2. Set up Duplex Mode

Interface Command	Parameter	Description
MCT-RACK(config-remote-No.-if-No.)# duplex [full]	[full]	Configure port duplex to **full**.
No command		
MCT-RACK(config-remote-No.-if-No.)# no duplex		Set the selected ports’ duplex mode to the default setting. **Note :** Auto-negotiation needs to be disabled before configuring duplex mode.

3. QoS configuration

Interface Command	Parameter	Description
MCT-RACK(config-remote-No.-if-No.)# qos rate-limit ingress [0|32-1000000]	[0|32-1000000]	Configure **ingress** rate limit, set zero or from 32Kbps to 1000Mbps.
MCT-RACK(config-remote-No.-if-No.)# qos rate-limit egress [0|32-1000000]	[0|32-1000000]	Configure **egress** rate limit, set zero or from 32Kbps to 1000Mbps.
No command		
MCT-RACK(config-remote-No.-if-No.)# no qos rate-limit ingress		Undo **ingress** rate limit.
MCT-RACK(config-remote-No.-if-No.)# no qos rate-limit egress		Undo **egress** rate limit.

4. Shutdown interface

Interface Command	Parameter	Description
MCT-RACK(config-remote-No.-if-No.)# shutdown		Administratively disable the selected ports' status.
No command		
MCT-RACK(config-remote-No.-if-No.)# no shutdown		Administratively enable the selected ports' status.

5. Speed configuration

Command	Parameter	Description
MCT-RACK(config-remote-No.-if-No.)# speed [1000 |100 | 10 | auto_sense]	[1000 |100 | 10 | auto_sense]	Set up the selected interfaces' speed. Manual speed configuration only works when "no auto-negotiation" command is issued.
No command		
MCT-RACK(config-remote-No.-if-No.)# no speed		Set the selected ports' speed to the default setting.

6. Configure 802.1q VLAN settings on a port.

Interface Command	Parameter	Description
MCT-RACK(config-remote-No.-if-No.)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
MCT-RACK(config-remote-No.-if-No.)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
MCT-RACK(config-remote-No.-if-No.)# vlan dot1q-		Set the selected ports to access mode (untagged).

vlan mode access		
MCT-RACK(config-remote-No.-if-No.)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
MCT-RACK(config-remote-No.-if-No.)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged). **Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
MCT-RACK(config-remote-No.-if-No.)# vlan qinq-vlan stag-vid [1-4094]	[1-4094]	Specify the service tag VID for the selected port(s).
No Command		
MCT-RACK(config-remote-No.-if-No.)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
MCT-RACK(config-remote-No.-if-No.)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
MCT-RACK(config-remote-No.-if-No.)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
MCT-RACK(config-remote-No.-if-No.)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
MCT-RACK(config-remote-No.-if-No.)# no vlan qinq-vlan stag-vid		Clear the service tag VID specified.

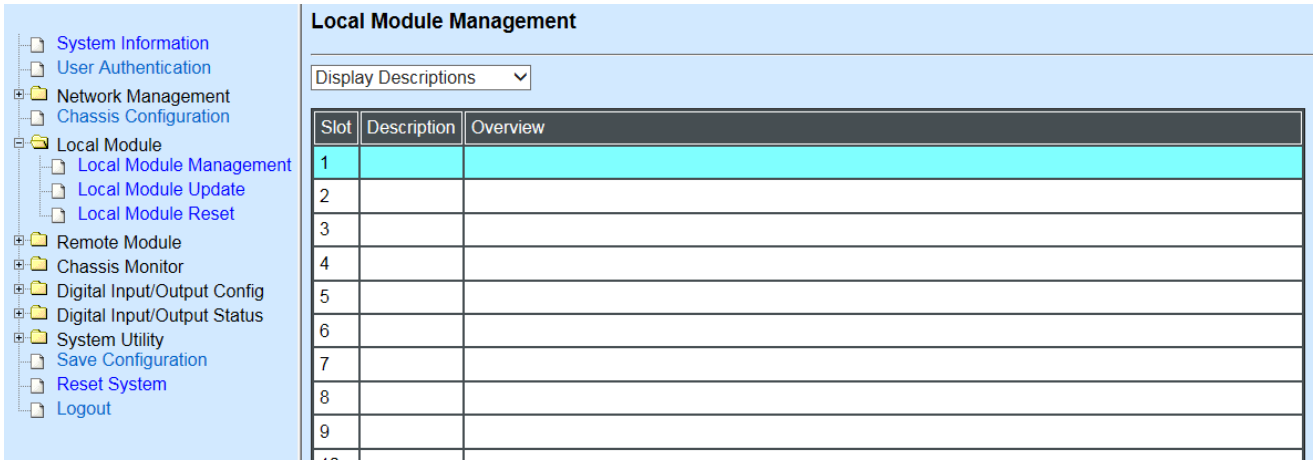
C.2 Web Management

This is to how the OAM converter is presented via Chassis on Web UI.

C.2.1 Local Module Management

In order to manage the installed converters and set up required functions, select the option **Local Module Management** from **Main Menu**, then **Local Module Management** screen page shows up.

Note: The slot configuration will return to the default if we replace Gigabit media converter with Fast media converter.



Overview: Show the product information of each slide-in converter.

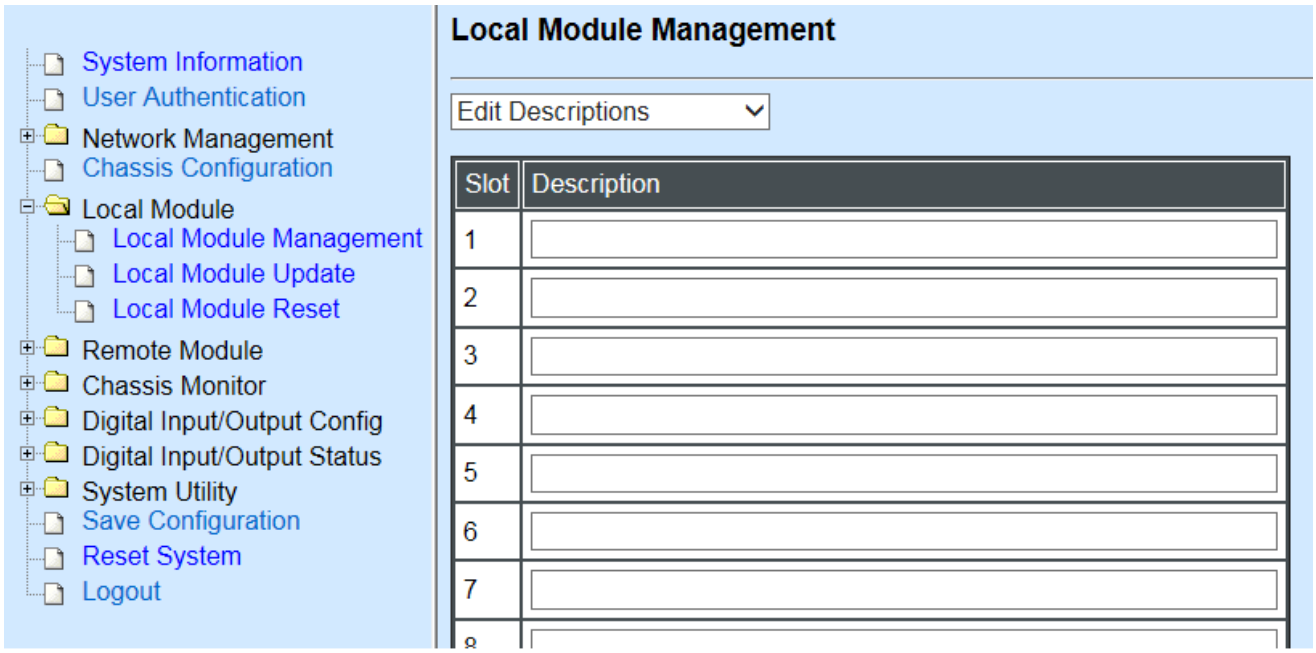
Description: Show the user-specified message of each slide-in converter.

The drop-down box is to modify or show the message you specify. There are three options:

Not Display Descriptions: Hide the user-specified message in the Description field of each slide-in converter.

Display Descriptions: Show the product information and the user-specified message of each slide-in converter both in the fields of Description and Overview.

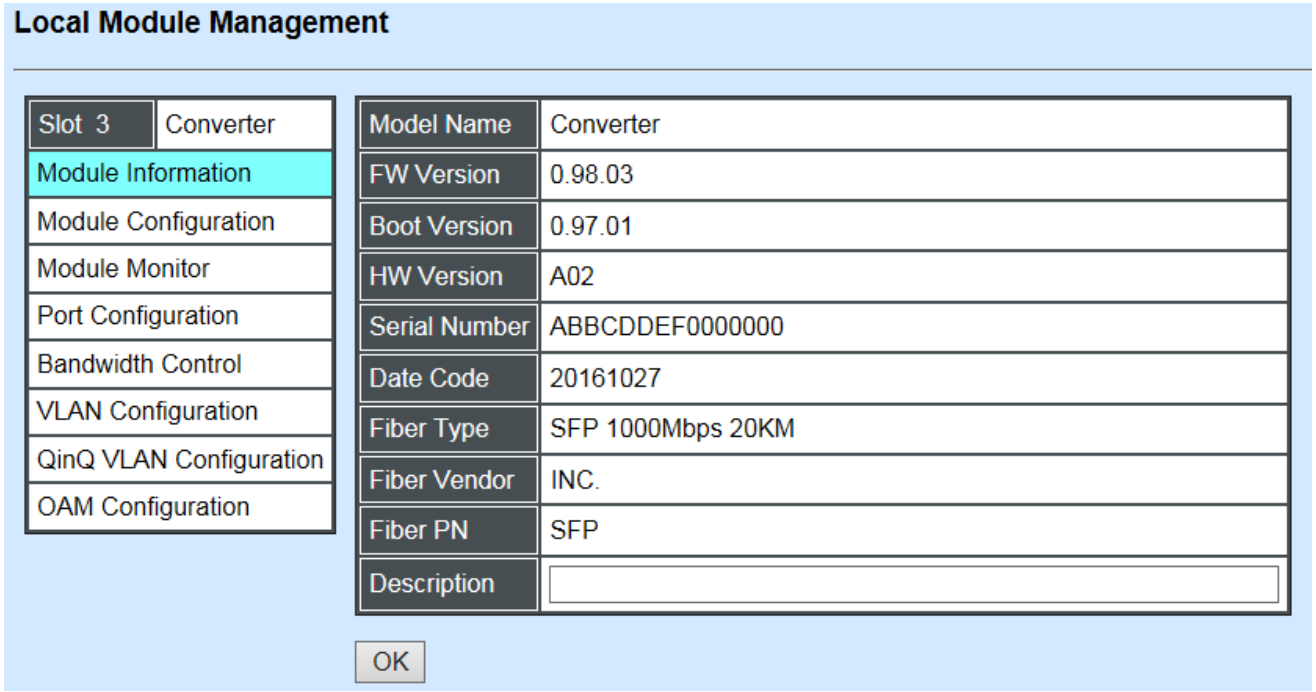
Edit Descriptions: Change the user-specified message of each slide-in converter separately.



To modify the description, click drop-down box and select **Edit Descriptions**.

Click **"OK"** to save edited message.

Click on the available modules and then the following screen page appears.



Module Information: Display the model name, version of FW/Boot/HW, serial number, date code, fiber type, fiber vendor, fiber PN and description.

Module Configuration: Set up Link Alarm function.

Module Monitor: Display information about Media Type, Port State, Link State, Auto-Negotiation status, Speed, Duplex, and Flow Control.

Port Configuration: Set up Media Type, Port State, Port Type, Port Speed, and Duplex.

Bandwidth Control: Set up Egress Rate Limit, Broadcast Storm Blocking.

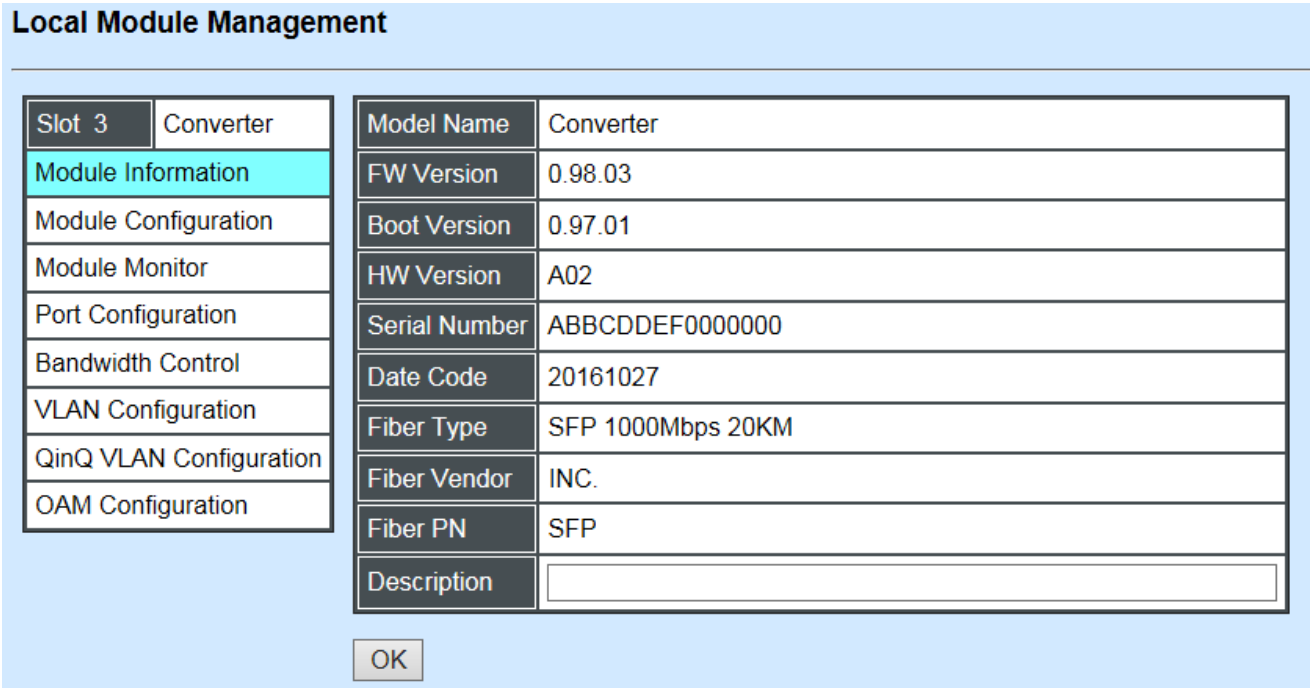
VLAN Configuration: Set up TP/FX default PVID, Egress Mode.

QinQ VLAN Configuration: Configure Q-in-Q (double tag) VLAN settings.

OAM Configuration: Set up OAM function.

C.2.1.1 Module Information

Select the option **Module Information** from the **Local Module Management** menu, then the **Module Information** fields show up on the right to provide you information about the module.



Model Name: View-only field that shows the product's model name.

FW Version: View-only field that shows the product's firmware version.

Boot Version: View-only field that shows the product's boot loader version.

HW Version: View-only field that shows the product's hardware version.

Serial Number: View-only field that shows the product's serial number.

Date Code: View-only field that shows the date of EEPROM burned.

Fiber Type: View-only field that shows the product's fiber connector type, speed, and distance.

Fiber Vendor: View-only field that shows the vendor name.

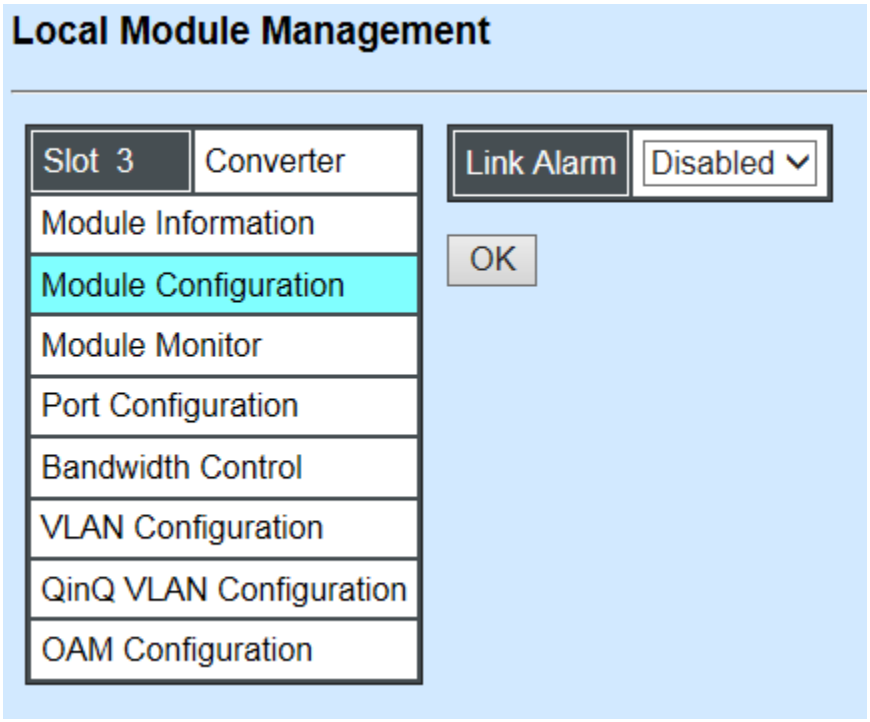
Fiber PN: View-only field that shows the fiber PN.

Description: Specify the appropriate brief description for the slide-in converter module.

C.2.1.2 Module Configuration

Select the option **Module Configuration** from the **Local Module Management** menu, then **Module Configuration** fields show up on the right to let you view the configuration of the converter.

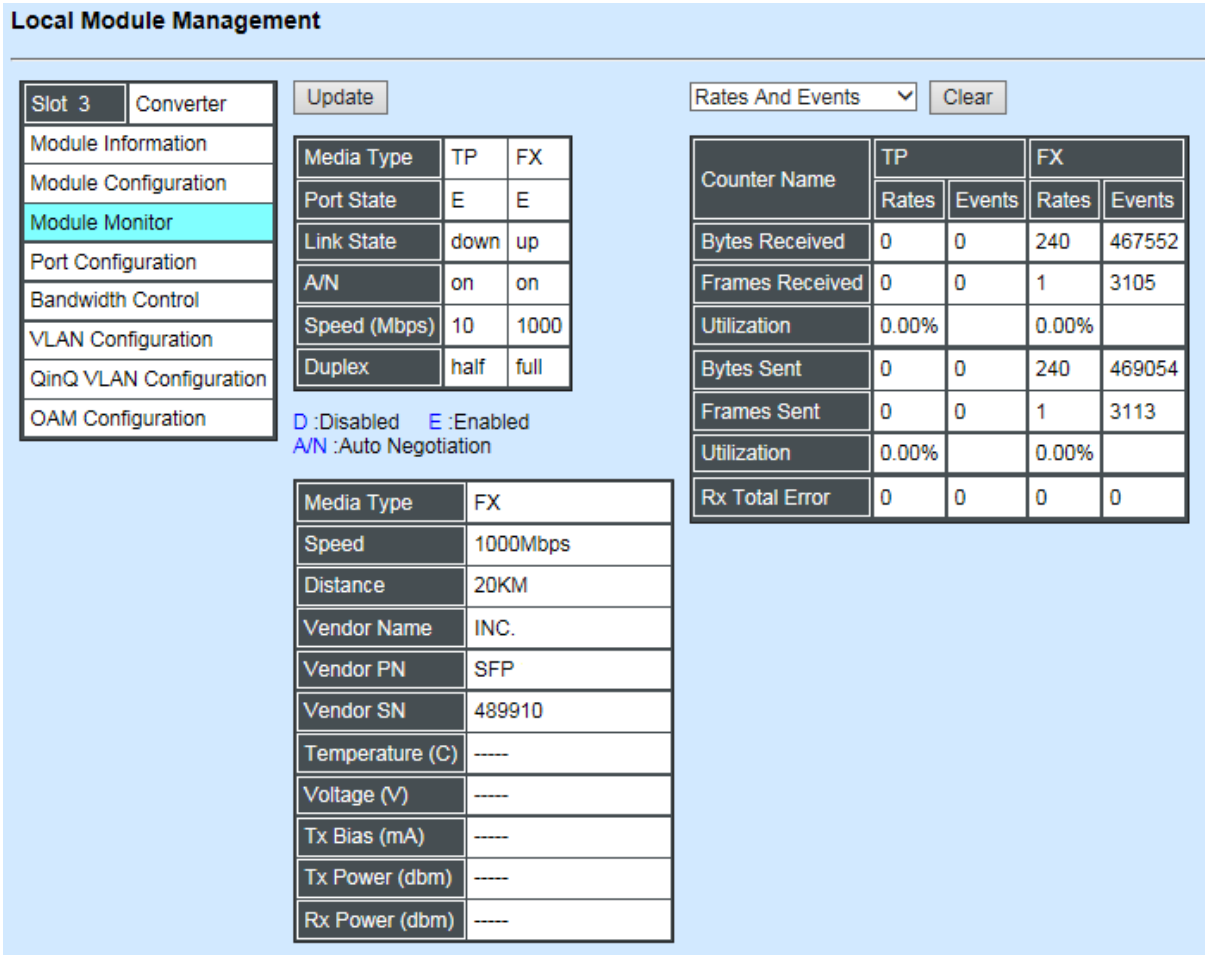
Link Alarm: This function is used under the circumstance that when UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.



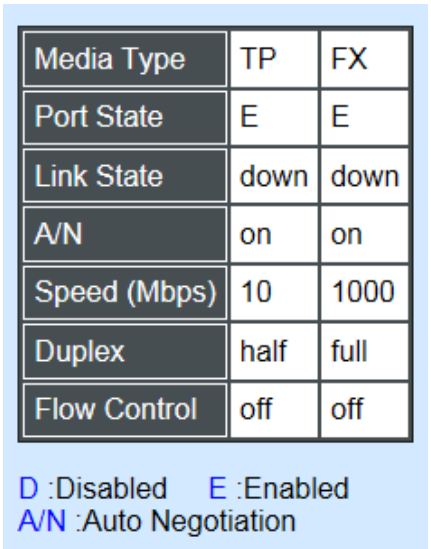
Click the drop-down box to enable or disable link alarm of the converter.

C.2.1.3 Module Monitor

Select the option **Module Monitor** from the **Local Module Management** menu, then **Module Monitor** fields show up on the right to let you view the configuration of the module.



Port Status



Media Type: TP (copper, 10/100Base-T, RJ-45) and FX (fiber).

Port State: View-only field that shows traffic is Disabled or Forwarding.

Link State: View-only field that shows the link is up or down.

A/N: View-only field that shows Auto-negotiation is on or off.

Speed: View-only field that shows the port speed.

Duplex: View-only field that shows the duplex mode is half or full.

Flow Control: View-only field that shows the flow control is on or off.

SFP Status

Media Type	FX
Speed	--
Distance	--
Vendor Name	--
Vendor PN	--
Vendor SN	--
Temperature (C)	-----
Voltage (V)	-----
Tx Bias (mA)	-----
Tx Power (dbm)	-----
Rx Power (dbm)	-----

Media Type: Show the type of FX (fiber).

Speed: Data rate of the slide-in SFP Transceiver.

Distance: Transmission distance of the slide-in SFP Transceiver.

Vendor Name: Vendor name of the slide-in SFP Transceiver.

Vendor PN: Vendor PN of the slide-in SFP Transceiver.

Vendor SN: Vendor SN of the slide-in SFP Transceiver.

Temperature (C): The slide-in SFP module operation temperature.

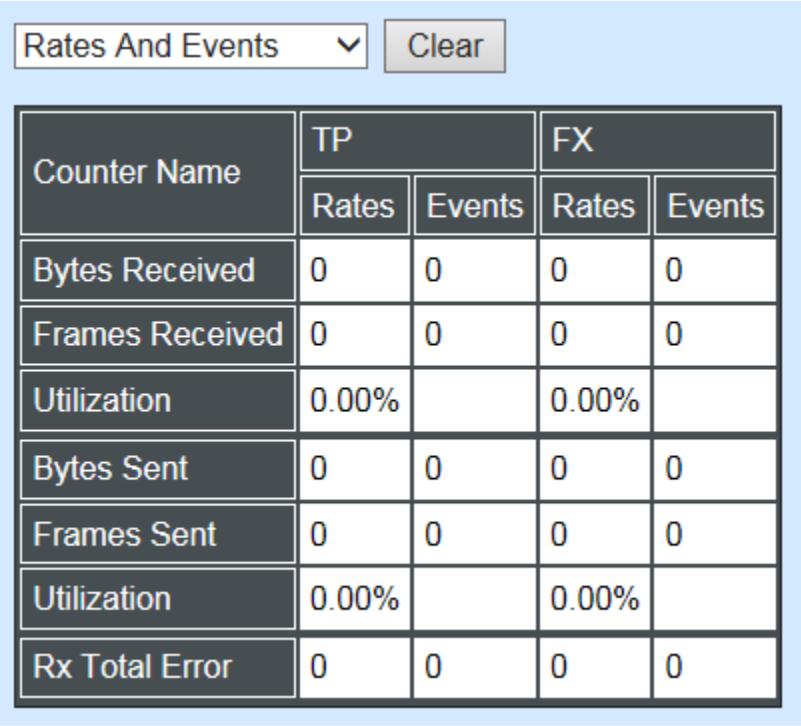
Voltage (V): The slide-in SFP module operation voltage.

TX Bias (mA): The slide-in SFP module operation current.

TX Power (dbm): The slide-in SFP module optical Transmission power.

RX Power (dbm): The slide-in SFP module optical Receiver power.

Select **"Rates and Events"** option from the Counters Display pull-down menu to view the detailed traffic statistics (counters' information).



Rates: Counters displayed and updated once per second.

Events: The count is cumulative (i.e. cumulated count).

Bytes Received: The total number of bytes received from this port.

Frames Received: The total number of frames received from this port.

Utilization: The utilization of receiving bandwidth from this port.

Bytes Sent: The total number of bytes sent from this port.

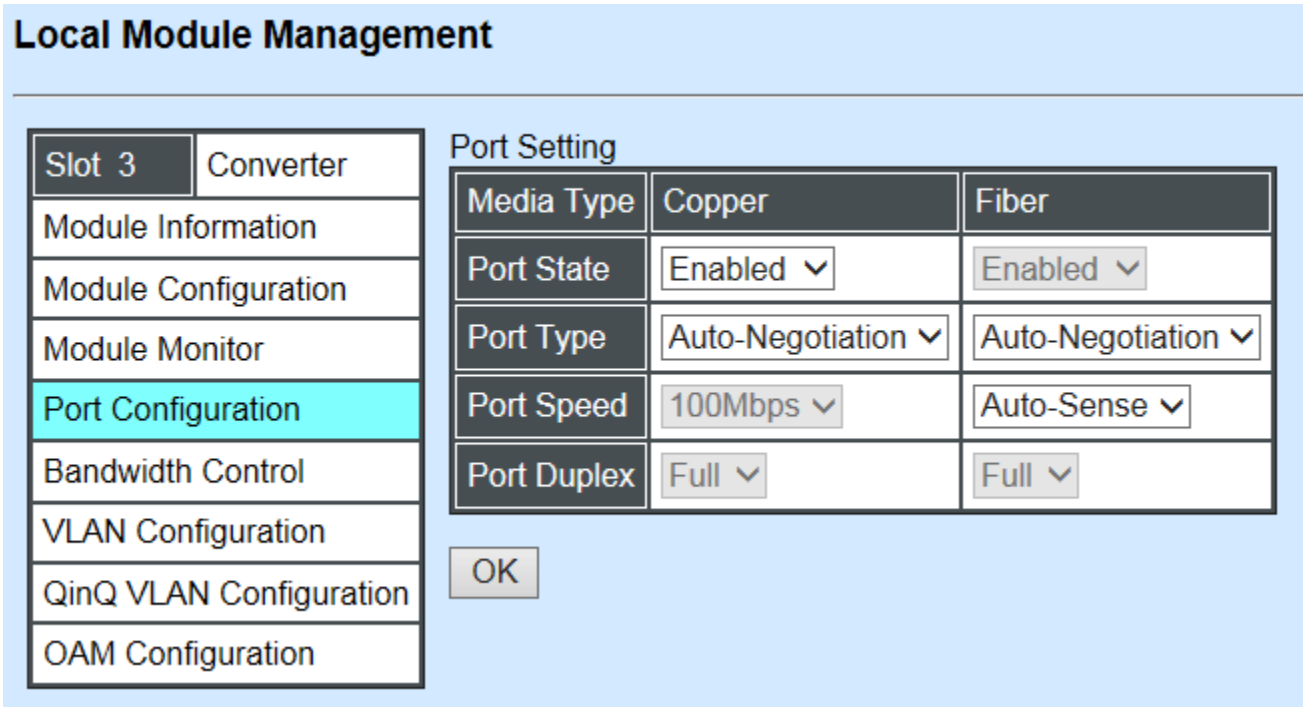
Frames Sent: The total number of frames sent from this port.

Utilization: The utilization of sending bandwidth from this port.

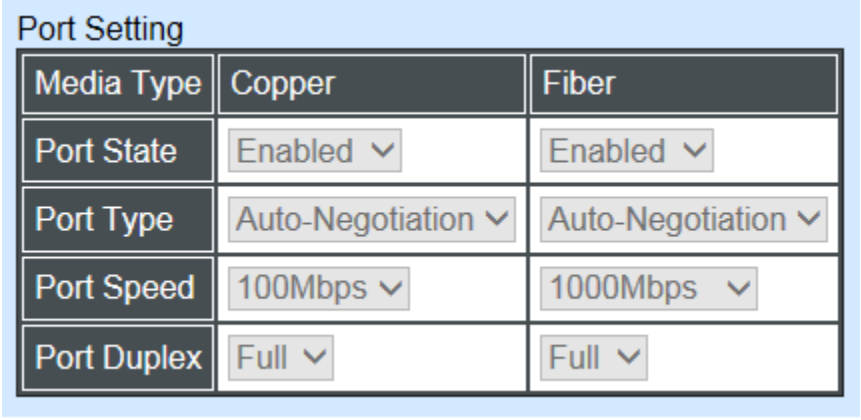
RX Total Errors: The total number of errors frames from this port.

C.2.1.4 Port Configuration

Select the option **Port Configuration** from the **Local Module Management** menu, then the **Port Configuration** fields show up on the right to let you configure them accordingly.



Port Setting



Media Type: Select between Copper (UTP, RJ-45) and Fiber

Port State: Enable or disable port state.

Port Type: Show the port type configuration is manual or auto-negotiation.

Port Speed: Show the port speed of the selected media type.

Port Duplex: Show the duplex mode is half or full.

Click **"OK"** to apply.

DIP Setting
You are allowed to view the DIP switch configuration via WEB UI.

DIP Setting

Media Type	Copper	Fiber
Port Type	Auto-Negotiation	Auto-Negotiation
Port Speed	100Mbps	100Mbps
Link Alarm	Enabled	

Currently controlled by device hardware dip switch.
Please consider to change device dip switch setting as software control.

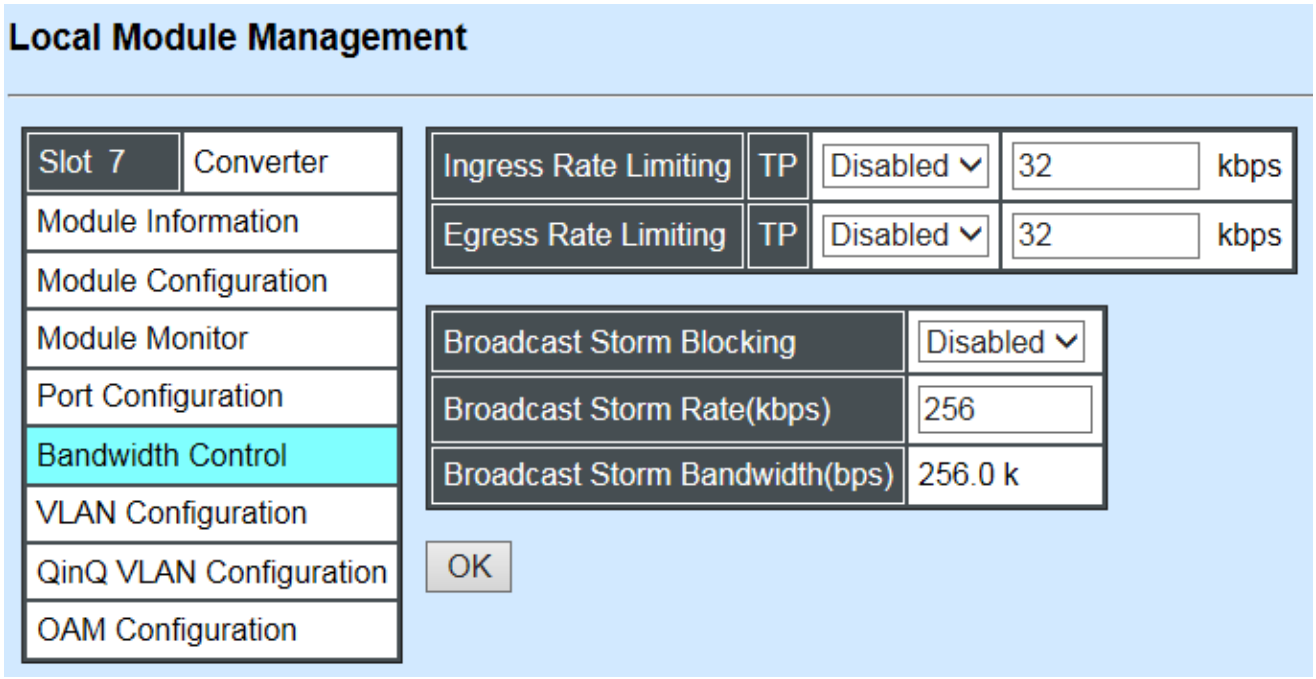
Port Type: View-only field that shows the port type configuration is manual or auto-negotiation.

Port Speed: View-only field that shows the port speed of the selected media type.

Link Alarm: View-only field that shows the link alarm is enabled or disabled.

C.2.1.5 Bandwidth Control

Select the option **Bandwidth Control** from the **Local Module Management** menu, then the **Bandwidth Control's** Ingress/Egress Rate Limit and Broadcast Storm fields show up on the right to let you enable/disable TP/FX, specify the rate in kbps, enable/disable broadcast Storm settings and specify the rate in kbps in broadcast storm blocking.



Ingress Rate Limiting: Enable or disable TP ingress rate limiting in kbps and set up current configured ingress bandwidth in kbps. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

Egress Rate Limiting: Enable or disable TP egress rate limiting in kbps and set up current configured egress bandwidth in kbps. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

Broadcast Storm Blocking: Enable or disable broadcast storm blocking function.

Broadcast Storm Rate(kbps): Set up storm rate value. Packets exceeding the value will be dropped. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

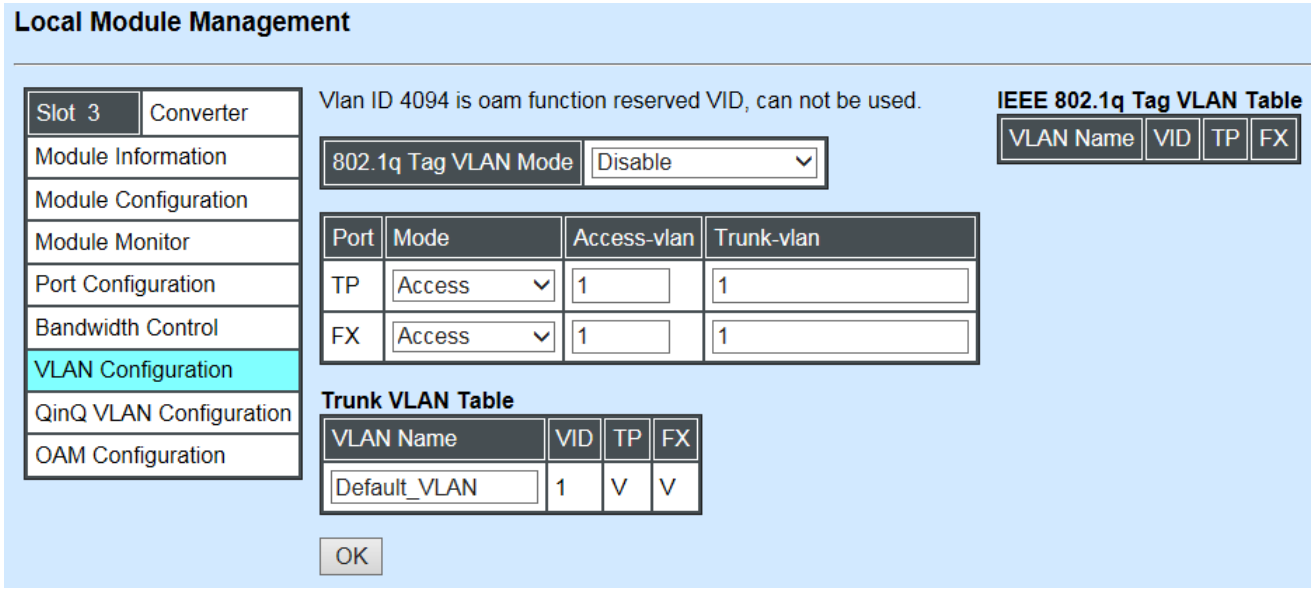
Broadcast Storm Rate Bandwidth(bps): Display the current configured storm rate bandwidth.

C.2.1.6 VLAN Configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the CHASSIS on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

Select the option **VLAN Configuration** from the **Local Module Management** menu, then the **VLAN Configuration's** Default VLAN Mode and Table fields show up on the right to let you specify the TP/FX of VLAN settings.



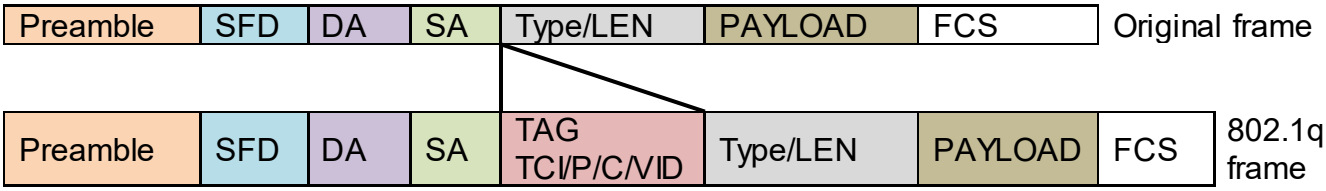
The Managed Media Converter supports **IEEE 802.1q Tag VLAN**.

IEEE 802.1Q VLAN Concepts

Port-Based VLAN is simple to implement and use, but it cannot be deployed cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution to this problem. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large switched networks into smaller segments so that

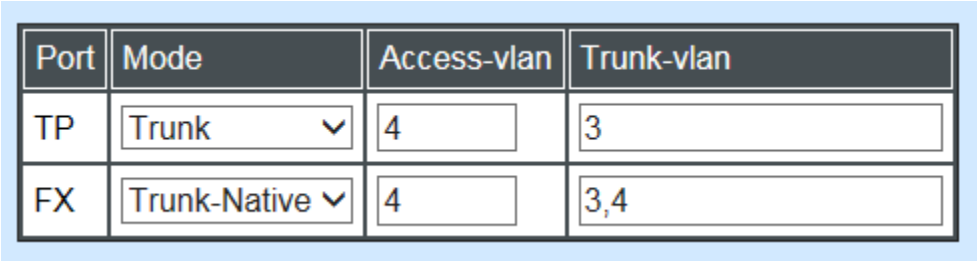
broadcast and multicast traffic will not occupy too much available bandwidth as well as provide a higher level security between segments of internal networks.

Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes		User data	
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

IEEE 802.1q Tag VLAN Mode: Enable or disable IEEE 802.1q Tag VLAN mode, or select Bypass Ctag Mode which ignore C-tag checking.



Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When

the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

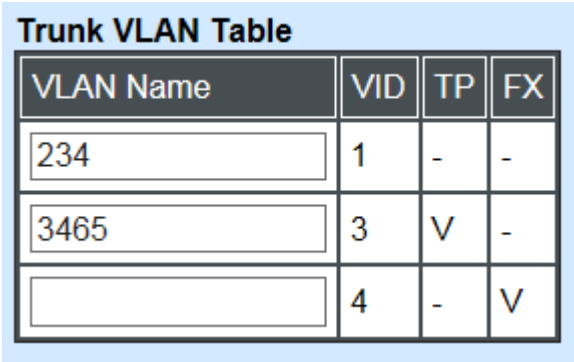
A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.



Trunk VLAN table: To edit 802.1Q Tag VLAN Name.

VLAN Name: User-specified field to give VLAN a name.

VID: The VLAN ID (**VID**) specifies the set of VLAN that a given port is allowed to receive and send **labeled** packets.

TP: It shows whether the TP port that is included in a given VID.

FX: It shows whether the Fiber port that is included in a given VID.

Click **"OK"** to apply.

IEEE 802.1q Tag VLAN Table

VLAN Name	VID	TP	FX
234	1	V	V

IEEE 802.1q Tag VLAN Table: It shows the status of IEEE 802.1q Tag VLAN.

VLAN Name: View-only filed that shows the VLAN name.

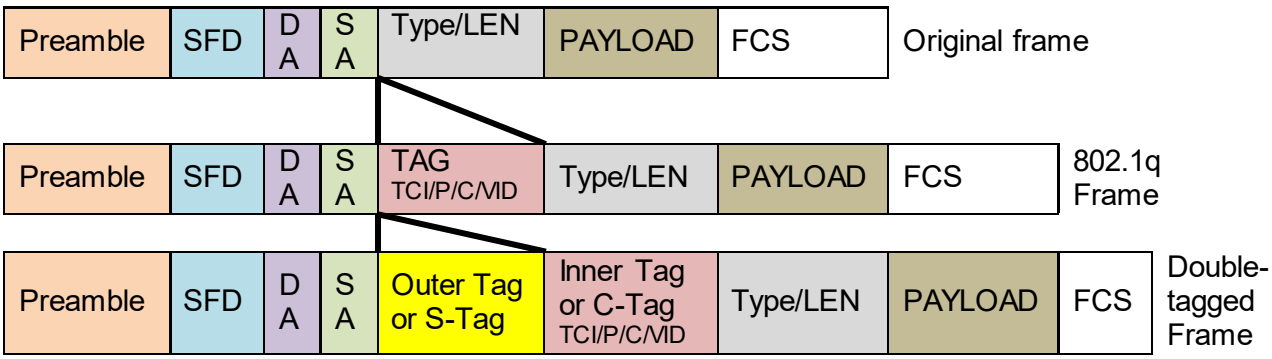
VID: View-only filed that shows the VID.

TP: View-only filed that shows whether the TP port that is included in a given VID.

FX: View-only filed that shows whether the fiber port that is included in a given VID.

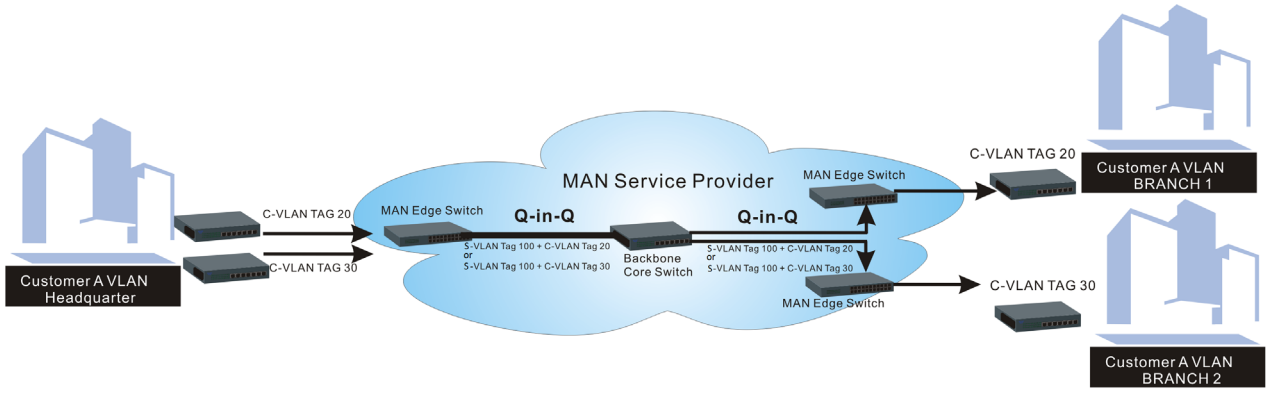
C.2.1.7 Q-in-Q VLAN Configuration

The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a "double-tagged" frame is created so as to separate customer traffic within a service provider network. As shown below in "Double-Tagged Frame" illustration, an outer tag is added between source destination and inner tag at the provider network's edge. This can support C-VLAN (Customer VLAN) over Metro Area Networks and ensure complete separation between traffic from different user groups. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single S-VLAN (Service VLAN) tag per customer over the Metro Ethernet network.



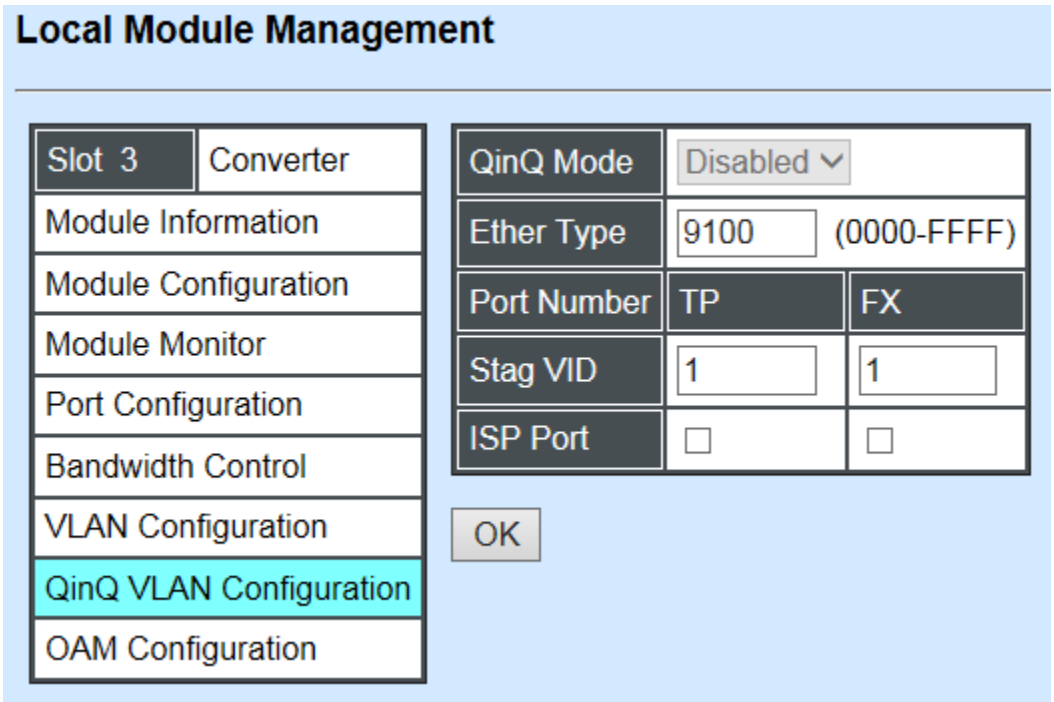
Double-Tagged Frame

As shown below in “Q-in-Q Example” illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider’s backbone, there is a possibility that traffic might be forwarded insecurely, for example due to the same VLAN ID used. Therefore, in order to get the information from Headquarter to Branch 1, the easiest way for the carrier to ensure security to customers is to encapsulate the original VLAN with a second VLAN ID of 100. This second VLAN ID is known as S-VLAN (Service VLAN) that is added as data enters the service provider’s network and then removed as data exits. Eventually, with the help of S-Tag, the information sent from Headquarter to Branch 1 can be delivered with customers’ VLANs intactly and securely.



Q-in-Q Example

This section allows you to set up Q-in-Q VLAN. Select the option **QinQ VLAN Configuration** from the **Local Module Management** menu, the **Q-in-Q VLAN** fields show up on the right.



QinQ Mode: Enable or disable the function by clicking drop-down box.

Ether Type: A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).

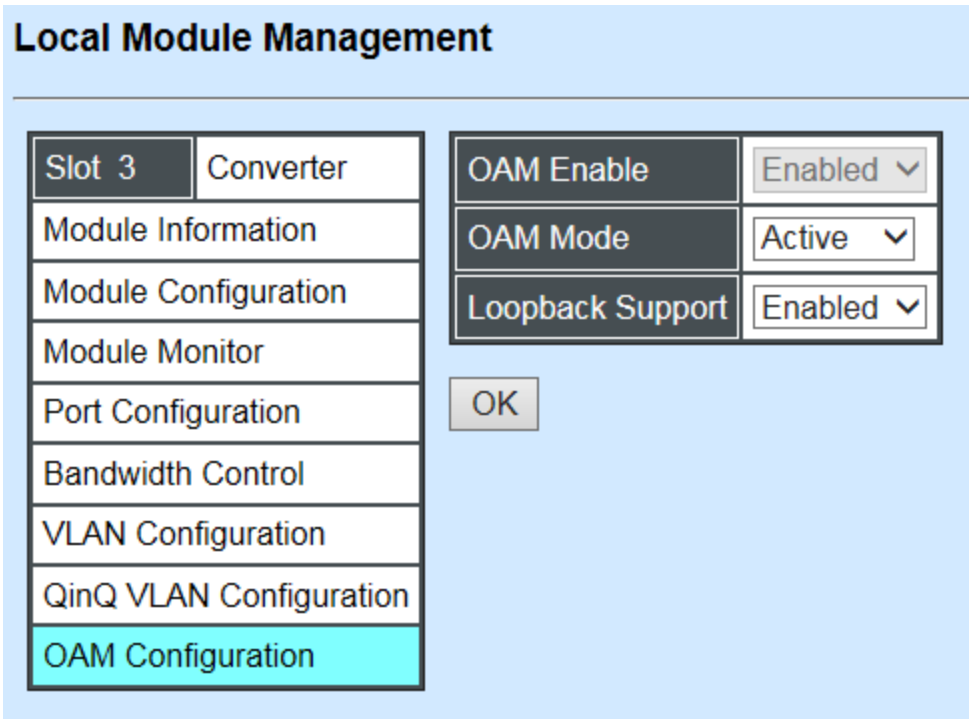
Port Number: Two kinds of ports are available, TP port or Fiber port.

Stag(Service Tag) VID: Specify a VID for the service tag (Outer Tag).

ISP(Internet Service Provider) Port: This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.

Click the **"OK"** button to apply the settings.

C.2.1.8 OAM Configuration



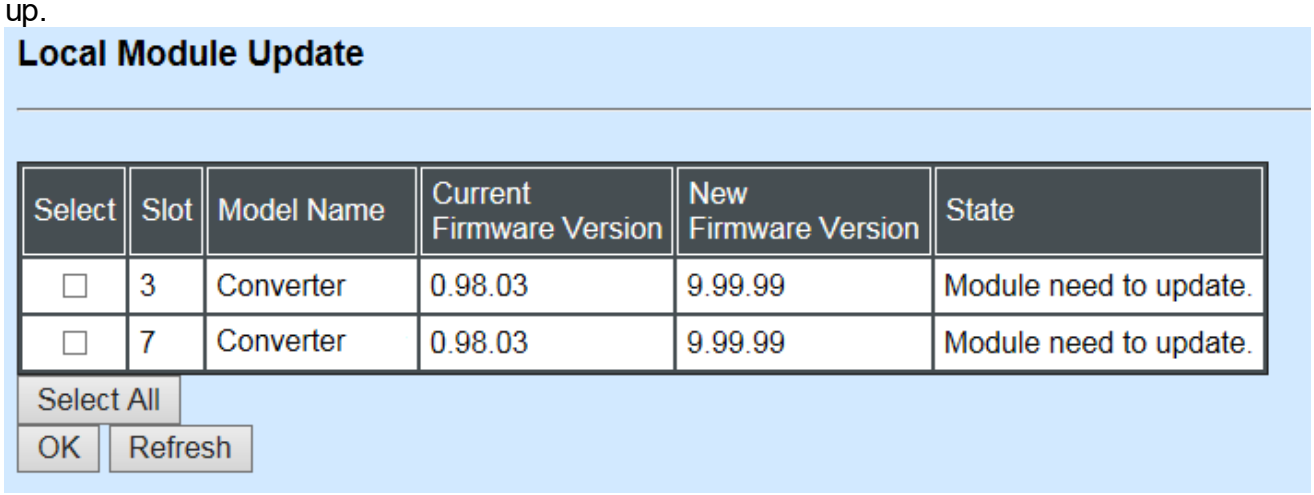
OAM Enable: The module is fixed at "Enabled" only.

OAM Mode: Click drop-down box to select OAM mode, either Active or Passive. To perform remote management, it's strongly recommended that OAM Mode be set "Active".

Loopback Support: Click drop-down box to enable or disable the function. A loopback test is a test in which a signal in sent from a communications device and returned (looped back) to it as a way to determine whether the device is working right or as a way to pin down a failing node in a network. The default setting is "Disabled".

C.2.2 Local Module Update

Select **Local Module Update** from the **Main Menu**, then the following screen page shows up.



Select: Check the box to upgrade the firmware on specified converters or click **Select All** button to upgrade the firmware on all converters.

Slot: Show which slot the converter is inserted into.

Model Name: Show the current model name of the converter.

Current Firmware Version: Show the current firmware version used for each converter.

New Firmware Version: The upcoming firmware version to be installed.

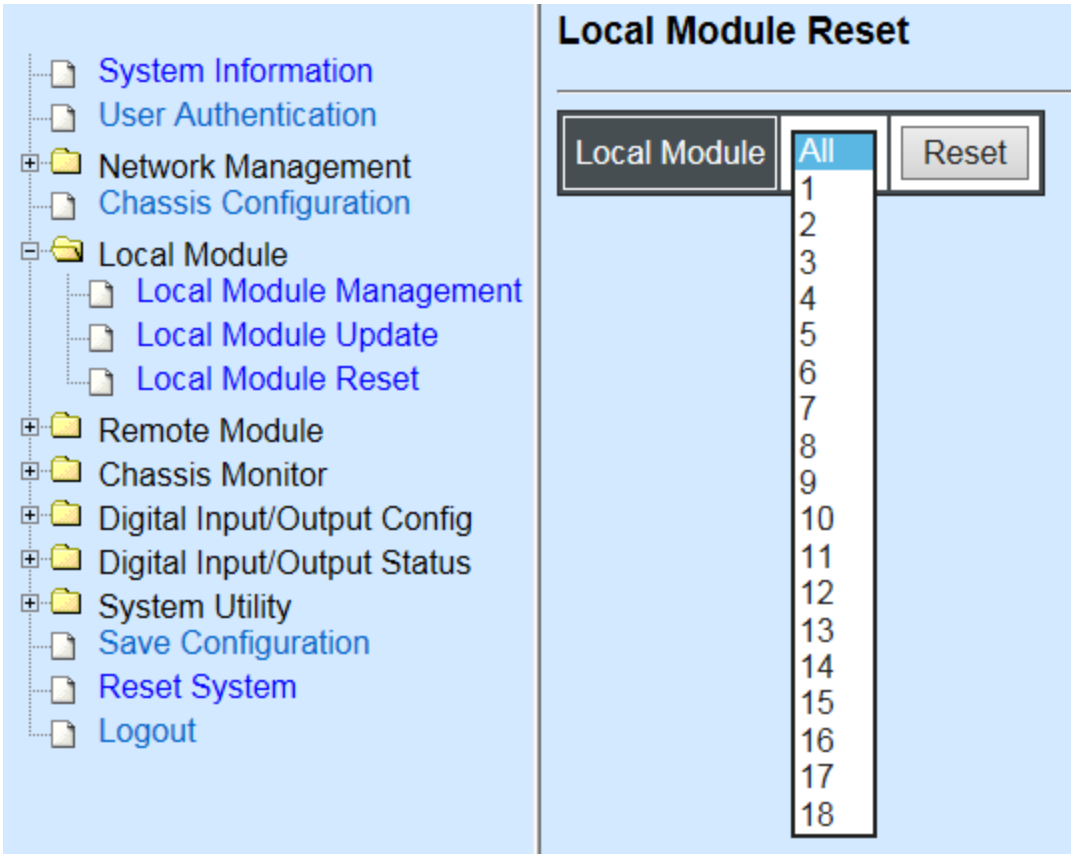
State: Show the current status of firmware upgrade.

Click **"OK"** to start module update procedure.

Click **"Refresh"** to renew all update module information.

C.2.3 Local Module Reset

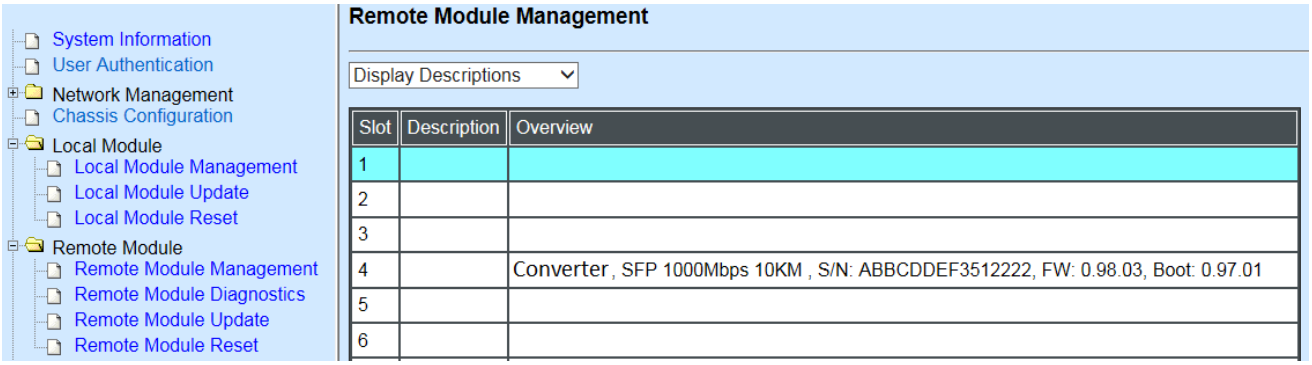
Select **Local Module Reset** from the **Main Menu**, then the following screen page shows up.



Local Module: Select **"All"** to reset all modules or select the individual module. When you decide which module to be reset, click **Reset** button to begin the reset process.

C.2.4 Remote Module Management

In order to manage the installed converters and set up required functions, select the option **Remote Module Management** from **Main Menu**, then **Remote Module Management** screen page shows up.



Overview: Show the product information of each slide-in converter.

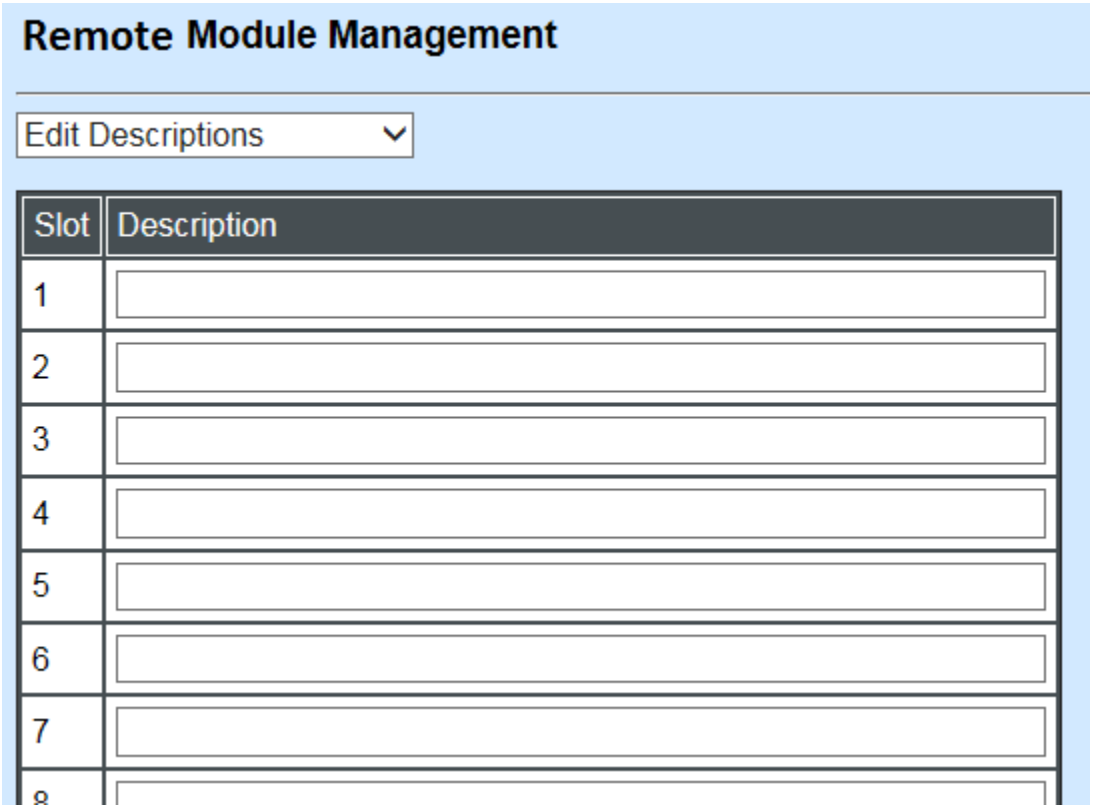
Description: Show the user-specified message of each slide-in converter.

The drop-down box is to modify or show the message you specify. There are three options:

Not Display Descriptions: Hide the user-specified message in the Description field of each slide-in converter.

Display Descriptions: Show the product information and the user-specified message of each slide-in converter both in the fields of Description and Overview.

Edit Descriptions: Change the user-specified message of each slide-in converter separately.



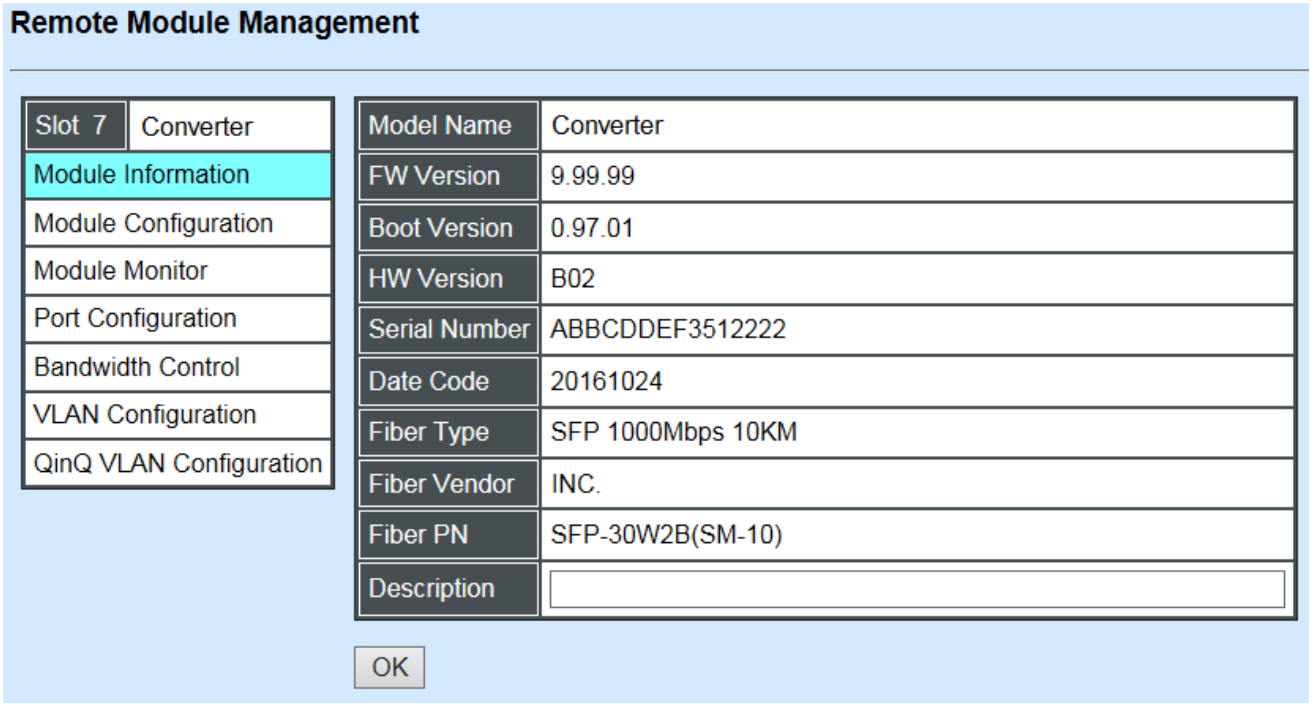
To modify the description, click drop-down box and select **Edit Descriptions**.

Click **"OK"** to save edited message.

Click on the available modules and then the following screen page appears.

C.2.4.1 Module Information

Select the option **Module Information** from the **Remote Module Management** menu, then the **Module Information** fields show up on the right to provide you information about the module.



Model Name: View-only field that shows the product's model name.

FW Version: View-only field that shows the product's firmware version.

Boot Version: View-only field that shows the product's boot loader version.

HW Version: View-only field that shows the product's hardware version.

Serial Number: View-only field that shows the product's serial number.

Date Code: View-only field that shows the date of EEPROM burned.

Fiber Type: View-only field that shows the product's fiber connector type, speed, and distance.

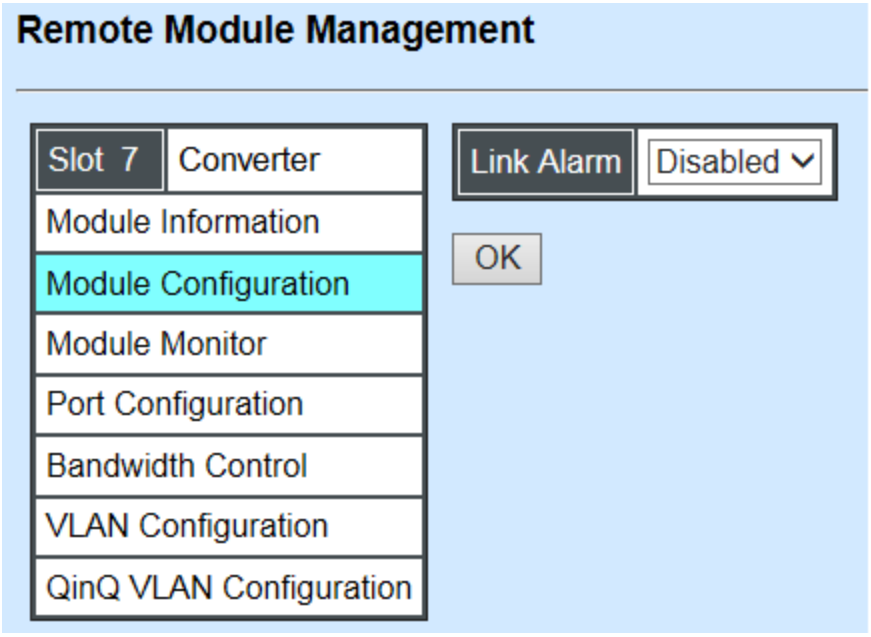
Fiber Vendor: View-only field that shows the vendor name.

Fiber PN: View-only field that shows the fiber PN.

Description: Specify the appropriate brief description for the slide-in converter module.

C.2.4.2 Module Configuration

Select the option **Module Configuration** from the **Remote Module Management** menu, then **Module Configuration** fields show up on the right to let you view the configuration of the converter.

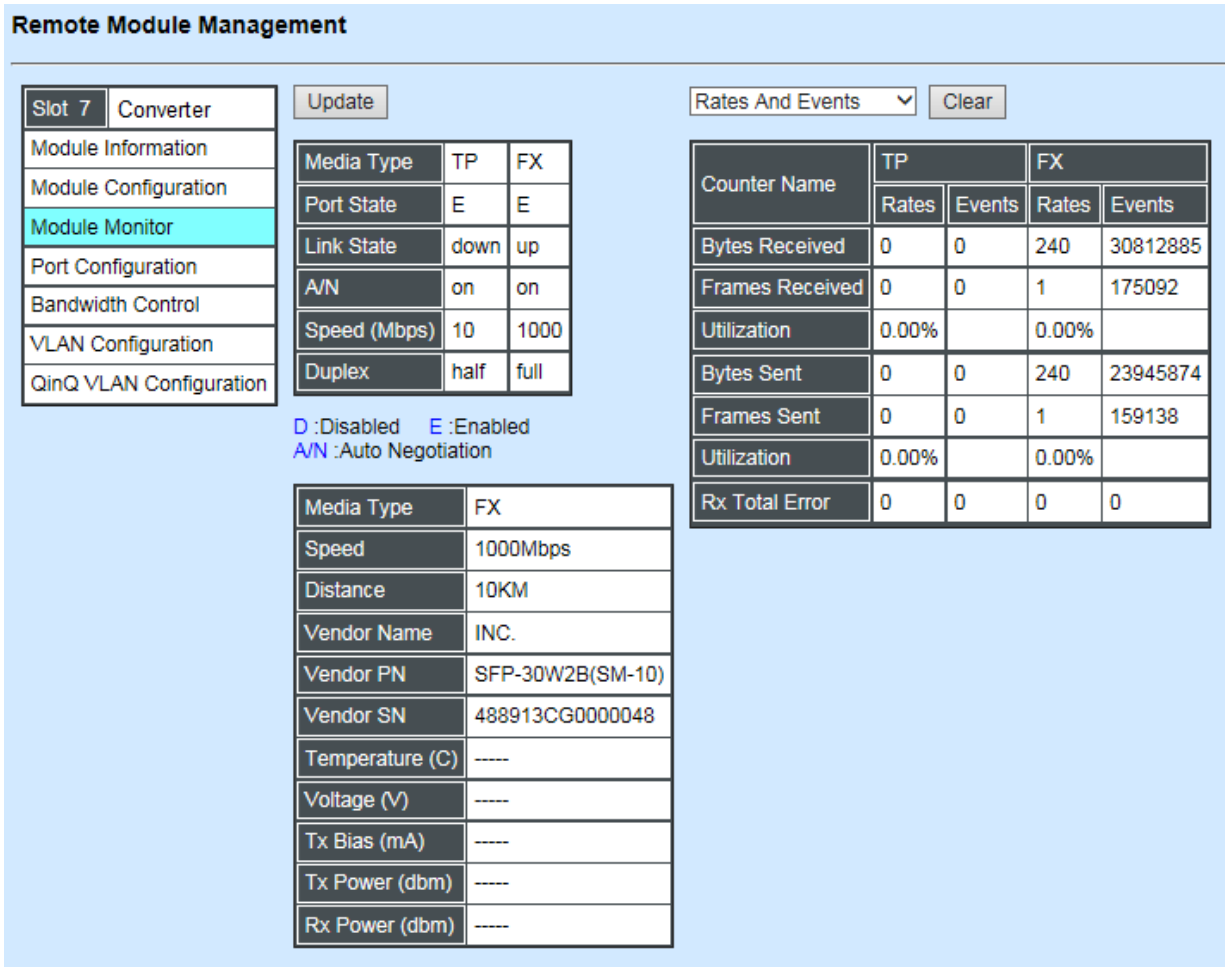


Link Alarm: This function is used under the circumstance that when UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.

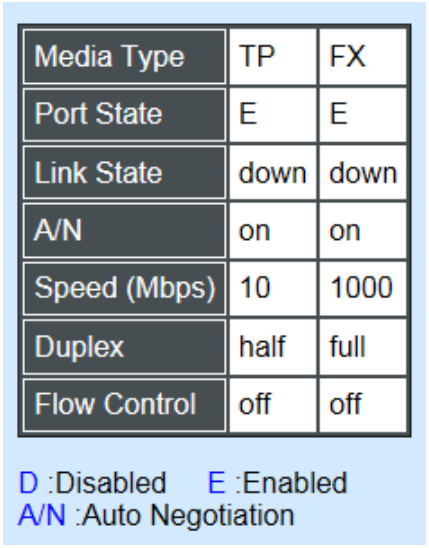
Click the drop-down box to enable or disable link alarm of the converter.

C.2.4.3 Module Monitor

Select the option **Module Monitor** from the **Remote Module Management** menu, and then **Module Monitor** fields show up on the right to let you view the configuration of the module.



Port Status



Media Type: TP (copper, 10/100Base-T, RJ-45) and FX (fiber).

Port State: View-only field that shows traffic is Disabled or Forwarding.

Link State: View-only field that shows the link is up or down.

A/N: View-only field that shows Auto-negotiation is on or off.

Speed: View-only field that shows the port speed.

Duplex: View-only field that shows the duplex mode is half or full.

Flow Control: View-only field that shows the flow control is on or off.

SFP Status

Media Type	FX
Speed	--
Distance	--
Vendor Name	--
Vendor PN	--
Vendor SN	--
Temperature (C)	-----
Voltage (V)	-----
Tx Bias (mA)	-----
Tx Power (dbm)	-----
Rx Power (dbm)	-----

Media Type: Show the type of FX (fiber).

Speed: Data rate of the slide-in SFP Transceiver.

Distance: Transmission distance of the slide-in SFP Transceiver.

Vendor Name: Vendor name of the slide-in SFP Transceiver.

Vendor PN: Vendor PN of the slide-in SFP Transceiver.

Vendor SN: Vendor SN of the slide-in SFP Transceiver.

Temperature (C): The slide-in SFP module operation temperature.

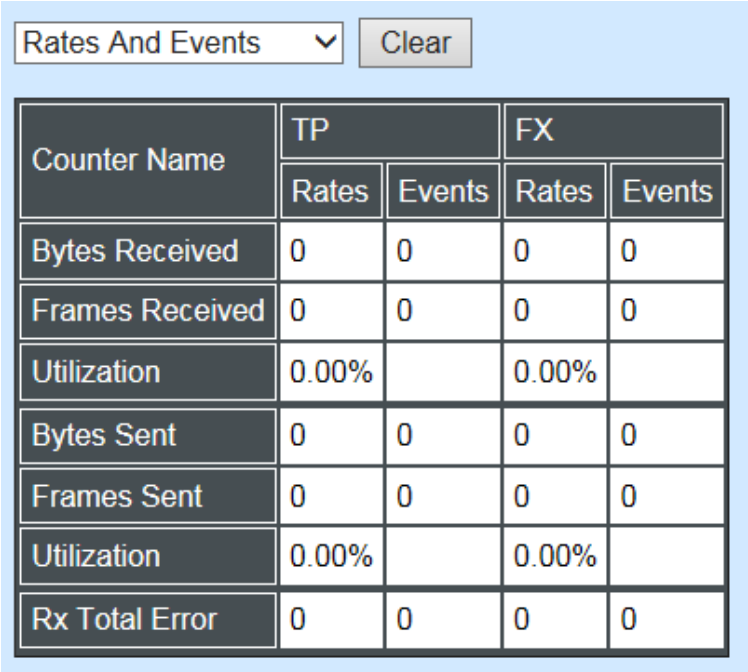
Voltage (V): The slide-in SFP module operation voltage.

TX Bias (mA): The slide-in SFP module operation current.

TX Power (dbm): The slide-in SFP module optical Transmission power.

RX Power (dbm): The slide-in SFP module optical Receiver power.

Select **"Rates and Events"** option from the Counters Display pull-down menu to view the detailed traffic statistics (counters' information).



Rates: Counters displayed and updated once per second.

Events: The count is cumulative (i.e. cumulated count).

Bytes Received: The total number of bytes received from this port.

Frames Received: The total number of frames received from this port.

Utilization: The utilization of receiving bandwidth from this port.

Bytes Sent: The total number of bytes sent from this port.

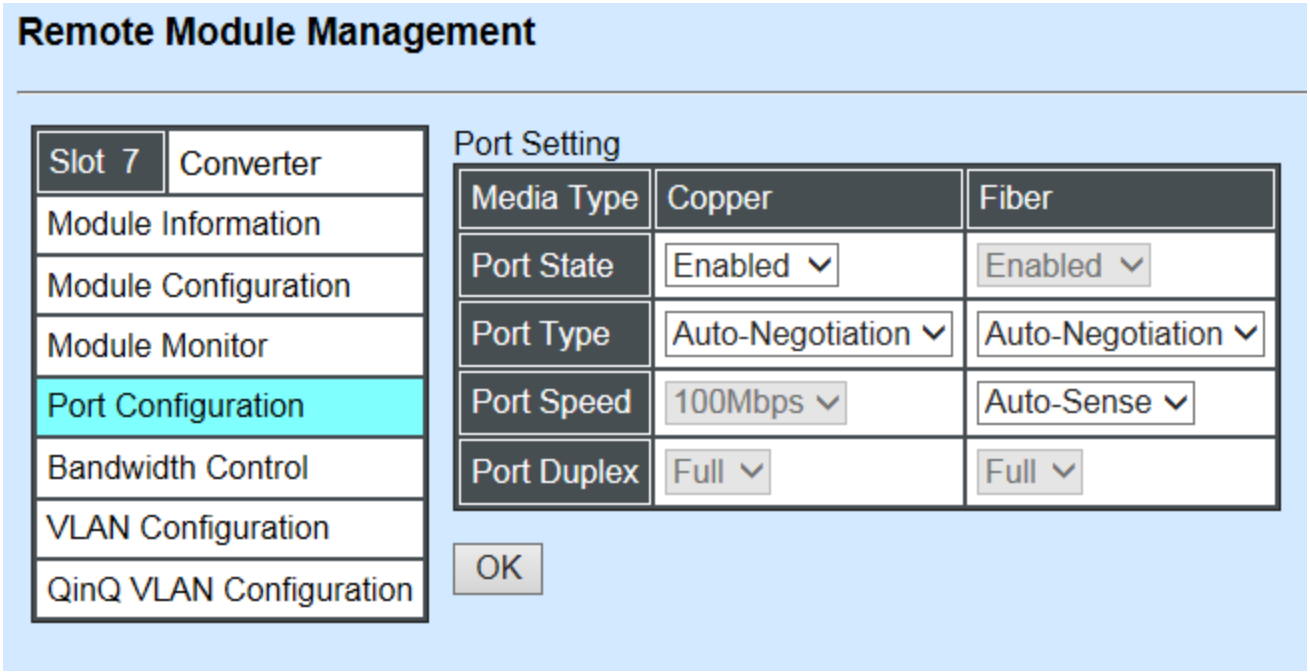
Frames Sent: The total number of frames sent from this port.

Utilization: The utilization of sending bandwidth from this port.

RX Total Errors: The total number of errors frames from this port.

C.2.4.4 Port Configuration

Select the option **Port Configuration** from the **Remote Module Management** menu, then the **Port Configuration** fields show up on the right to let you configure them accordingly.



DIP Setting
You are allowed to view the DIP switch configuration via WEB UI if PIN 8 of the converter is switched "ON".

DIP Setting

Media Type	Copper	Fiber
Port Type	Auto-Negotiation	Auto-Negotiation
Port Speed	100Mbps	100Mbps
Link Alarm	Enabled	

Currently controlled by device hardware dip switch.
Please consider to change device dip switch setting as software control.

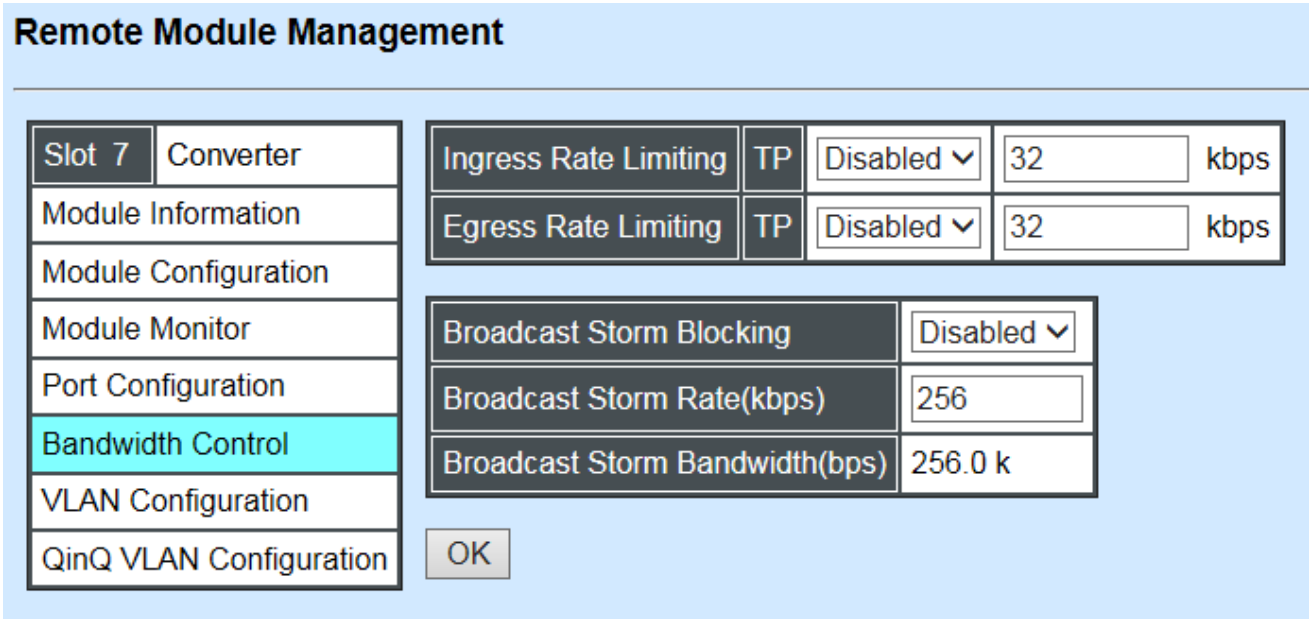
Port Type: View-only field that shows the port type configuration is manual or auto-negotiation.

Port Speed: View-only field that shows the port speed of the selected media type.

Link Alarm: View-only field that shows the link alarm is enabled or disabled.

C.2.4.5 Bandwidth Control

Select the option **Bandwidth Control** from the **Remote Module Management** menu, then the Bandwidth Control's Ingress/Egress Rate Limit and Broadcast Storm fields show up on the right to let you enable/disable TP/FX, specify the rate in kbps, enable/disable broadcast Storm settings and specify the rate in kbps in broadcast storm blocking.



Ingress Rate Limiting: Enable or disable TP ingress rate limiting in kbps and set up current configured ingress bandwidth in kbps. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

Egress Rate Limiting: Enable or disable TP egress rate limiting in kbps and set up current configured egress bandwidth in kbps. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

Broadcast Storm Blocking: Enable or disable broadcast storm blocking function.

Broadcast Storm Rate(kbps): Set up storm rate value. Packets exceeding the value will be dropped. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

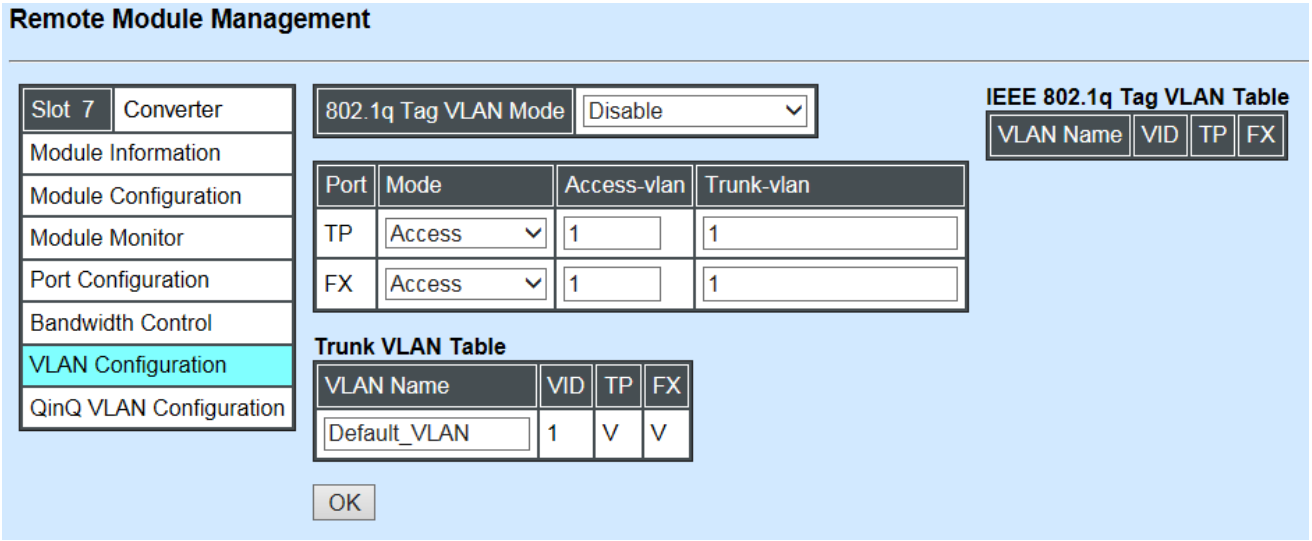
Broadcast Storm Rate Bandwidth(bps): Display the current configured storm rate bandwidth.

C.2.4.6 VLAN Configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the CHASSIS on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

Select the option **VLAN Configuration** from the **Remote Module Management** menu, then the **VLAN Configuration's** Default VLAN Mode and Table fields show up on the right to let you specify the TP/FX of VLAN settings.

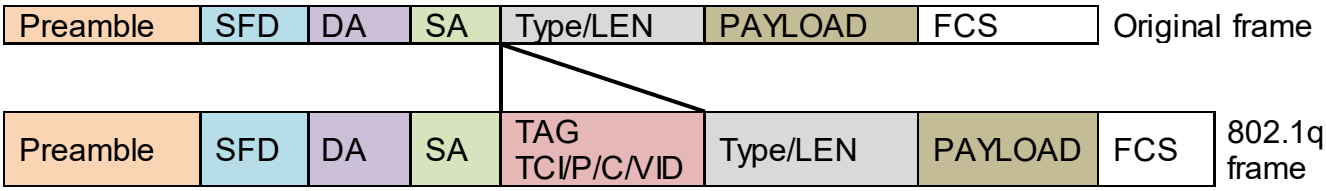


The Managed Media Converter supports **IEEE 802.1q Tag VLAN**.

IEEE 802.1Q VLAN Concepts

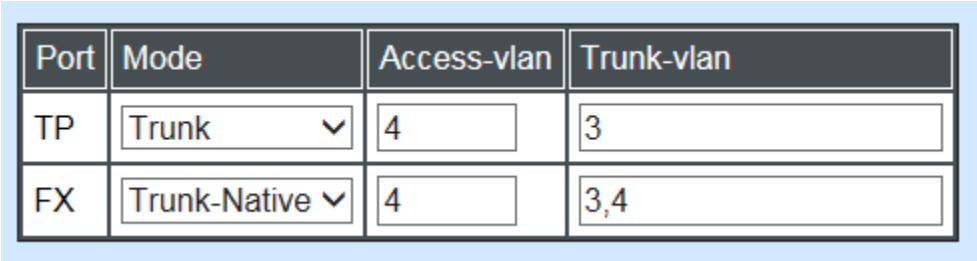
Port-Based VLAN is simple to implement and use, but it cannot be deployed cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution to this problem. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large switched networks into smaller segments so that broadcast and multicast traffic will not occupy too much available bandwidth as well as provide a higher level security between segments of internal networks.

Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes		User data	
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

IEEE 802.1q Tag VLAN Mode: Enable or disable IEEE 802.1q Tag VLAN mode, or select Bypass Ctag Mode which ignore C-tag checking.



Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

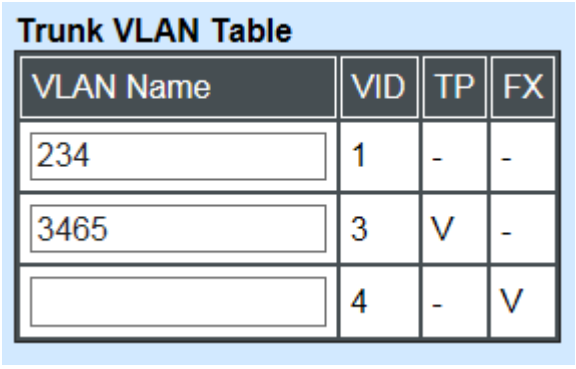
A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode:**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode:**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.



Trunk VLAN table: To edit 802.1Q Tag VLAN Name.

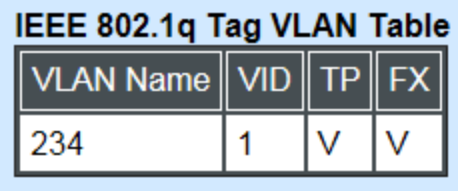
VLAN Name: User-specified field to give VLAN a name.

VID: The VLAN ID (**VID**) specifies the set of VLAN that a given port is allowed to receive and send **labeled** packets.

TP: It shows whether the TP port that is included in a given VID.

FX: It shows whether the Fiber port that is included in a given VID.

Click **“OK”** to apply.



IEEE 802.1q Tag VLAN Table

VLAN Name	VID	TP	FX
234	1	V	V

IEEE 802.1q Tag VLAN Table: It shows the status of IEEE 802.1q Tag VLAN.

VLAN Name: View-only filed that shows the VLAN name.

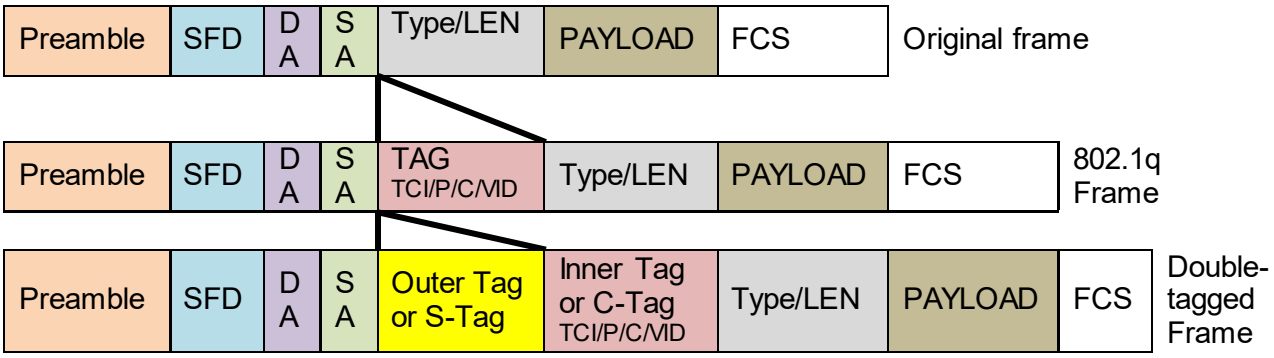
VID: View-only filed that shows the VID.

TP: View-only filed that shows whether the TP port that is included in a given VID.

FX: View-only filed that shows whether the fiber port that is included in a given VID.

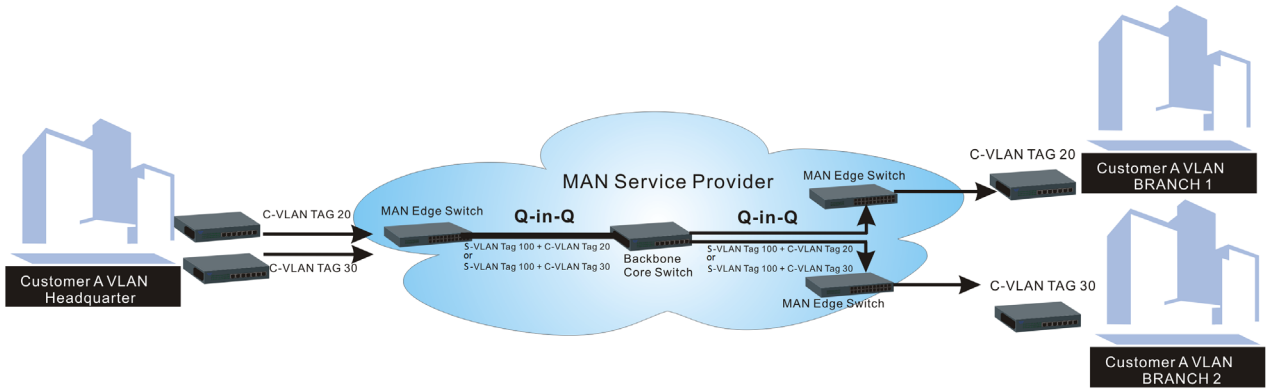
C.2.4.7 Q-in-Q VLAN Configuration

The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a “double-tagged” frame is created so as to separate customer traffic within a service provider network. As shown below in “Double-Tagged Frame” illustration, an outer tag is added between source destination and inner tag at the provider network’s edge. This can support C-VLAN (Customer VLAN) over Metro Area Networks and ensure complete separation between traffic from different user groups. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single S-VLAN (Service VLAN) tag per customer over the Metro Ethernet network.



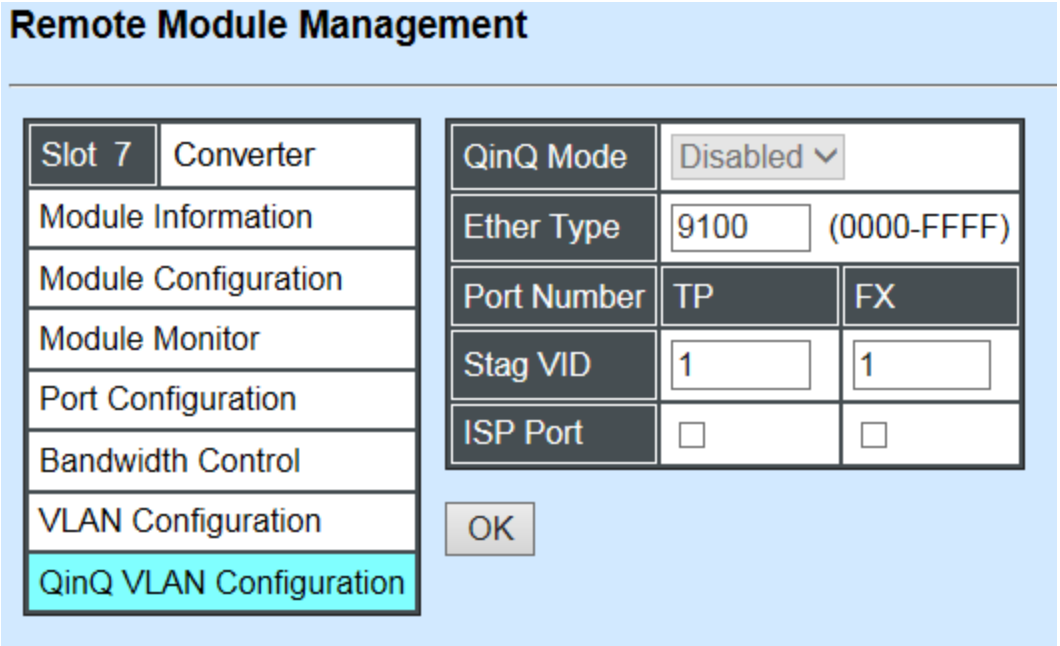
Double-Tagged Frame

As shown below in “Q-in-Q Example” illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider’s backbone, there is a possibility that traffic might be forwarded insecurely, for example due to the same VLAN ID used. Therefore, in order to get the information from Headquarter to Branch 1, the easiest way for the carrier to ensure security to customers is to encapsulate the original VLAN with a second VLAN ID of 100. This second VLAN ID is known as S-VLAN (Service VLAN) that is added as data enters the service provider’s network and then removed as data exits. Eventually, with the help of S-Tag, the information sent from Headquarter to Branch 1 can be delivered with customers’ VLANs intactly and securely.



Q-in-Q Example

This section allows you to set up Q-in-Q VLAN. Select the option **QinQ VLAN Configuration** from the **Remote Module Management** menu, the **Q-in-Q VLAN** fields show up on the right.



QinQ Mode: Enable or disable the function by clicking drop-down box.

Ether Type: A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).

Port Number: Two kinds of ports are available, TP port or Fiber port.

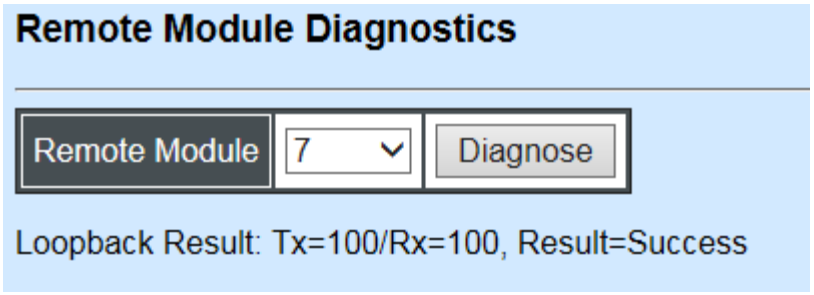
Stag(Service Tag) VID: Specify a VID for the service tag (Outer Tag).

ISP(Internet Service Provider) Port: This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.

Click the **"OK"** button to apply the settings.

C.2.5 Remote Module Diagnostics

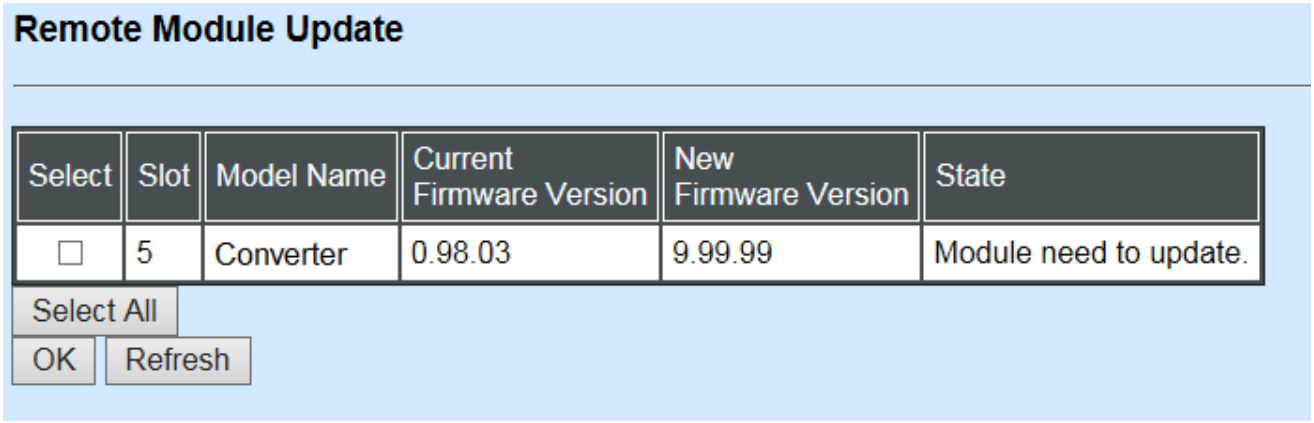
This is to conduct loopback test to check if the external converter is link up properly. Select the slot that the external converter is connected with and click "Diagnose". After a while, the test result will pop out as below:



That the Packet of Tx is equal to that of Rx indicates the link is working normal and the result of test shows "Success". If the Tx is not the same as Rx, which means some packet are dropped during the link transmission, the result of test shows "Fail".

C.2.6 Remote Module Update

Select **Remote Module Update** from the **Main Menu**, then the following screen page shows up.



Select: Check the box to upgrade the firmware on specified converters or click **Select All** button to upgrade the firmware on all converters.

Slot: Show which slot the converter is inserted into.

Model Name: Show the current model name of the converter.

Current Firmware Version: Show the current firmware version used for each converter.

New Firmware Version: The upcoming firmware version to be installed.

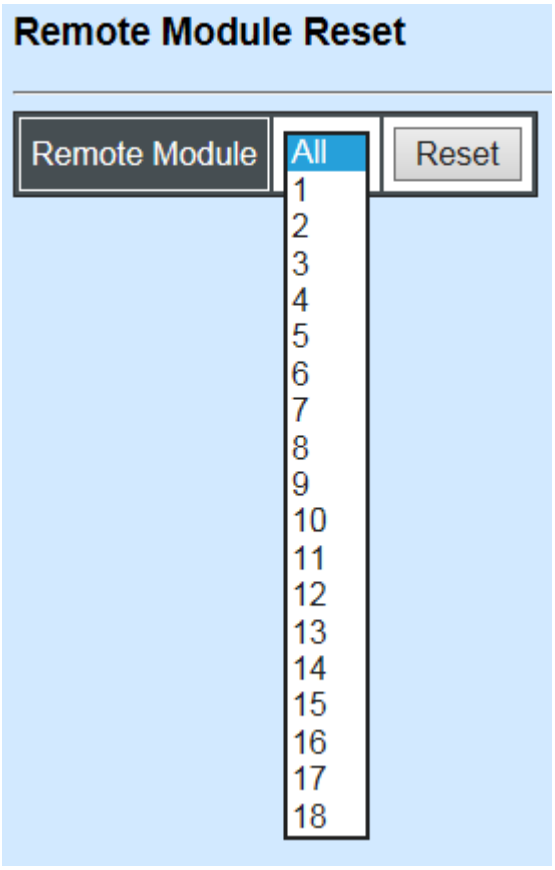
State: Show the current status of firmware upgrade.

Click **"OK"** to start module update procedure.

Click **"Refresh"** to renew all update module information.

C.2.7 Remote Module Reset

Select **Remote Module Reset** from the **Main Menu**, then the following screen page shows up.



Remote Module: Select **"All"** to reset all modules or select the individual module. When you decide which module to be reset, click **Reset** button to begin the reset process.

APPENDIX D: MCT-3612 Converter

This section is used to introduce 10/100/1000BASE-T to 100/1000BASE-X standalone Media Converter which is specifically designed to fulfill emerging deployment needs of fiber Ethernet networks.

D.1 CLI Command

This is to how the converter is presented via CLI Command.

D.1.1 Local Module Configuration

This section is intended to introduce the configuration of specified media converters.

Note: *Make sure that media converts are firmly installed and powered on.*

1. Specify any slots to configure

Slot command	Parameter	Description
MCT-RACK(config)# slot [slot_list]	[slot_list]	Specify any slots you want to configure.

2. Upgrade media converter firmware.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# firmware upgrade		Upgrade the firmware. **Note:** Upgrade one media converter at a time.

3. Configure link alarm

When UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module link-alarm		Enable link alarm function.
No Command		
MCT-RACK(config-slot-slot-slot)# no module link-alarm		Disable link alarm function.
Show Command		
MCT-RACK(config-slot-slot-slot)# show module		Show the status of link alarm.

4. Set up module description

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module-info description [description]	[description]	Specify user-defined information. Up to 55 characters are available.
No Command		
MCT-RACK(config-slot-slot-slot)# no module-info description		Delete user-defined information.
Show Command		
MCT-RACK(config-slot-slot-slot)# show module-info		Show the module information.
Module Description Example		
MCT-RACK(config-slot-slot-slot)# module-info description 123		The description of the converter is named “123”.

5. Reset converter

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# reload		Reboot the media converters.

6. Set up security protection

When a device on the network is malfunctioning or application programs are not well designed or properly configured, broadcast storms may occur, which may degrade network performance or in the worst situation cause a complete halt. The Chassis allows users to set a threshold rate for broadcast traffic so as to protect network from broadcast storms. Any broadcast packet exceeding the specified value will then be dropped.

Security command	Parameter	Description
MCT-RACK(config)# security storm-protection		Enable storm protection function.
MCT-RACK(config)# security storm-protection rates [32-1000000] kbps	[32-1000000] kbps	Specify the maximum broadcast packet rate.
No command		
MCT-RACK(config)# no security storm-protection		Disable storm protection globally.
MCT-RACK(config)# no security storm-protection rates		Set broadcast packet rate back to the default.
Show command		
MCT-RACK(config)# show security storm-protection		Show storm control settings.

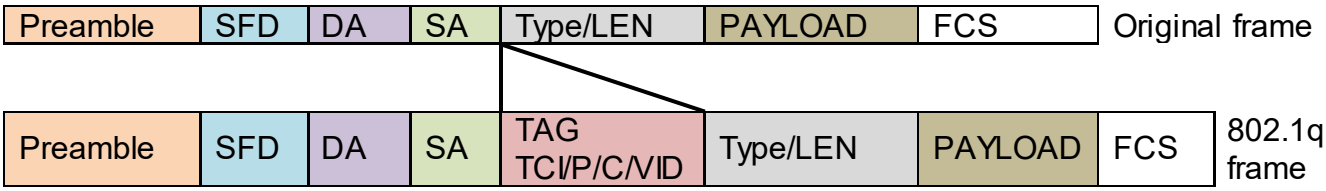
7. Set up VLAN configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the device on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

IEEE 802.1Q VLAN Concepts

Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes		User data	
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a

time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.

Example : PortX configuration

Configuration	Result
Trunk-VLAN = 10, 11, 12 Access-VLAN = 20 **Mode = Access**	PortX is an **Access Port** PortX's **VID** is ignored PortX's **PVID** is 20 PortX sends **Untagged** packets (PortX takes away VLAN tag if the PVID is 20) PortX receives **Untagged** packets only
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Trunk**	PortX is a **Trunk Port** PortX's **VID** is 10,11 and 12 PortX's **PVID** is ignored PortX sends and receives **Tagged** packets VID 10,11 and 12
Trunk-VLAN = 10,11,12	PortX is a **Trunk-native Port**

Access-VLAN = 20 **Mode = Trunk-native**	PortX's **VID** is 10,11 and 12 PortX's **PVID** is 20 PortX sends and receives **Tagged** packets VID 10,11 and 12 PortX receives **Untagged** packets and add PVID 20

The CHSSSIS supports two types of VLAN, these are: **IEEE 802.1q Tag VLAN** and **Q-in-Q VLAN**.

VLAN Command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# vlan dot1q-vlan		Enable IEEE 802.1q Tag VLAN mode.
MCT-RACK(config-slot-slot-slot)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VID number to create an 802.1q VLAN. **Note :** 802.1q VLAN ID need to be created under interface command. In here you can only modify it instead of creating a new VLAN ID.
MCT-RACK(config-slot-slot-slot)# vlan qinq-vlan		Enable Q-in-Q VLAN.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan bypass-ctag		Ignore the C-tag checking.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan isp-port [port_list]	[port_list]	Configure ISP Port (Q-in-Q Port). **ISP(Internet Service Provider) Port:** This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan stag-ethertype [0xWXYZ]	[0xWXYZ]	Specify service tag ether type. **Ether Type:** A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).
No Command		
MCT-RACK(config-slot-slot-slot)# no vlan dot1q-vlan		Disable IEEE 802.1q Tag VLAN mode.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan		Disable Q-in-Q VLAN.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan bypass-ctag		Not ignore the C-tag checking.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan isp-port		Undo ISP port (Q-in-Q port).
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan management-stag		Clear management service tag VID.

MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan stag-ethertype		Delete service tag ether type.
Show Command		
MCT-RACK(config-slot-slot-slot)# show vlan dot1q-vlan		Show dot1q VLAN configuration.
MCT-RACK(config-slot-slot-slot)# show vlan interface		Show all interfaces on a media converter.
MCT-RACK(config-slot-slot-slot)# show vlan interface [port_list]	[port_list]	Show specific interfaces on a media converter.
MCT-RACK(config-slot-slot-slot)# show vlan qinq-vlan		Show Q-in-Q VLAN configuration.

8. Use "Slot" command to configure 802.1q VLAN settings on a port.

Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid [1-4094]	[1-4094]	Specify the service tag VID for the selected port(s).
No Command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.

MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid		Clear the service tag VID specified.

D.1.2 Local Module Port Configuration

This is to configure port via "interface" command.

This command is to configure TP port or fiber port on a converter.

Interface command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.

1. Configure auto-negotiation function.

Interface command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# auto-negotiation		Set the selected interfaces' to auto-negotiation. When auto-negotiation is enabled, speed configuration will be ignored.
No command		**No command**
MCT-RACK(config-slot-slot-slot-if-port-port)# no auto-negotiation		Disable auto-negotiation function.

2. Set up Duplex Mode

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# duplex [full]	[full]	Configure port duplex to **full**.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no duplex		Set the selected ports' duplex mode to the default setting. **Note :** Auto-negotiation needs to be

		disabled before configuring duplex mode.

3. Qos configuration

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# qos rate-limit ingress [0|32-1000000]	[0|32-1000000]	Configure **ingress** rate limit, set zero or from 32Kbps to 1000Mbps.
MCT-RACK(config-slot-slot-slot-if-port-port)# qos rate-limit egress [0|32-1000000]	[0|32-1000000]	Configure **egress** rate limit, set zero or from 32Kbps to 1000Mbps.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no qos rate-limit ingress		Undo **ingress** rate limit.
MCT-RACK(config-slot-slot-slot-if-port-port)# no qos rate-limit egress		Undo **egress** rate limit.

4. Shutdown interface

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# shutdown		Administratively disable the selected ports' status.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no shutdown		Administratively enable the selected ports' status.

5. Speed configuration

Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# speed [1000 |100 | 10 | auto_sense]	[1000 |100 | 10 | auto_sense]	Set up the selected interfaces' speed. Manual speed configuration only works when "no auto-negotiation" command is issued.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no speed		Set the selected ports' speed to the default setting.

6. Configure 802.1q VLAN settings on a port.

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.
MCT-RACK(config-slot-	[1-4094]	Specify the selected ports' Access-VLAN ID

slot-slot-if-port-port)# vlan dot1q-vlan access-vlan [1-4094]		(PVID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid [1-4094]	[1-4094]	Specify the service tag VID for the selected port(s).
No Command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid		Clear the service tag VID specified.

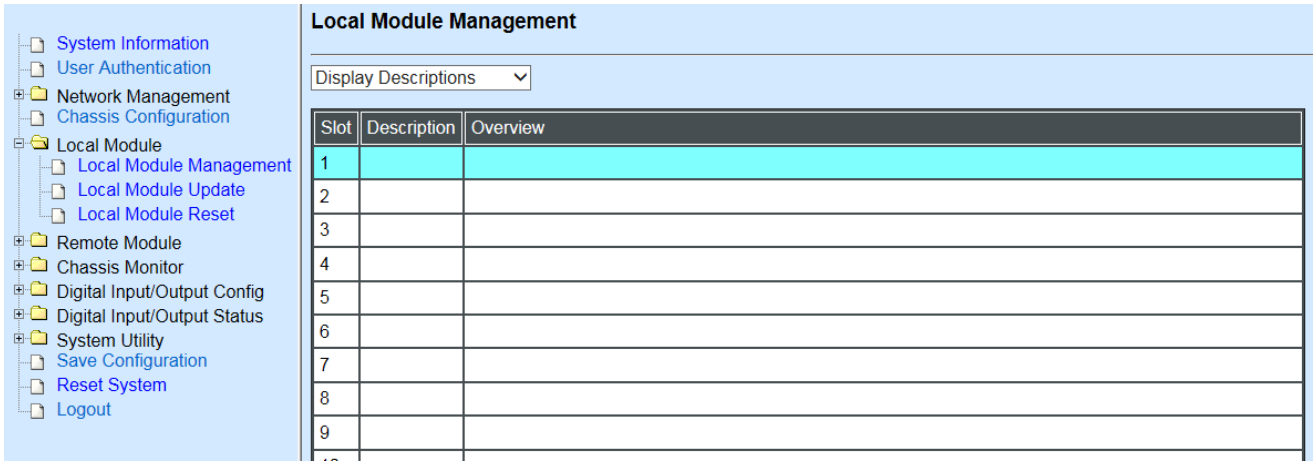
D.2 Web Management

This is to how the converter is presented via Chassis on Web UI.

D.2.1 Local Module Management

In order to manage the installed converters and set up required functions, select the option **Local Module Management** from **Main Menu**, then **Local Module Management** screen page shows up.

Note: The slot configuration will return to the default if we replace Gigabit media converter with Fast media converter.



Overview: Show the product information of each slide-in converter.

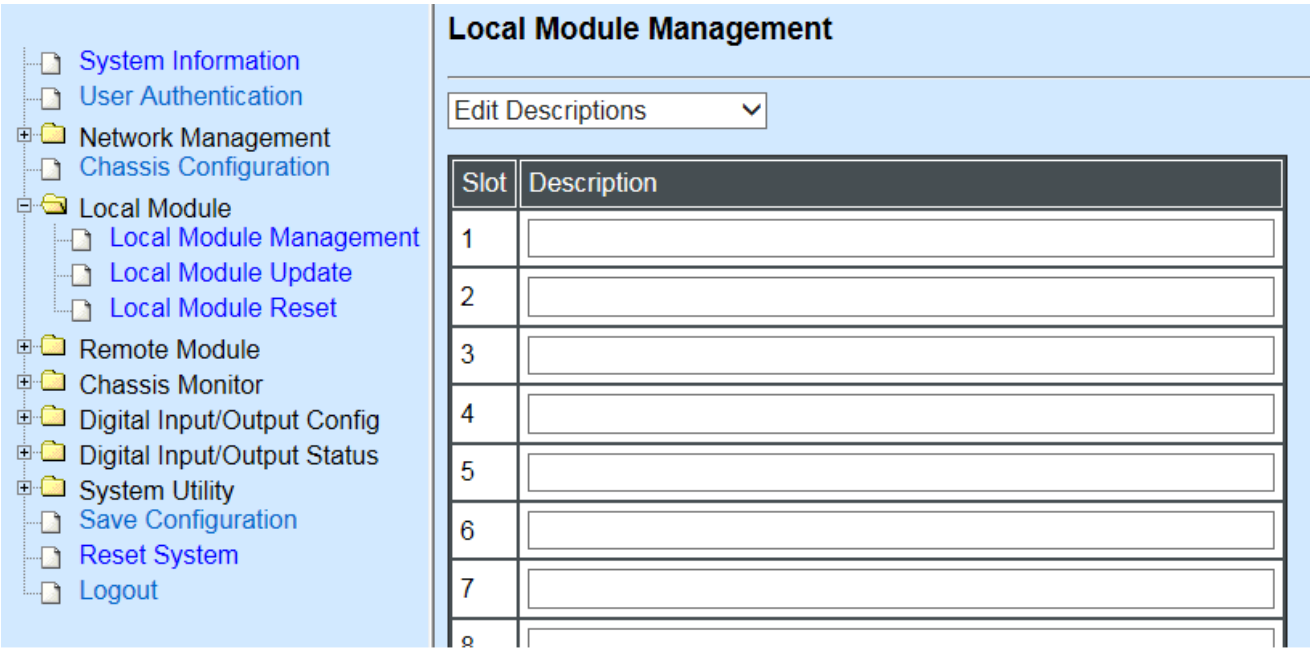
Description: Show the user-specified message of each slide-in converter.

The drop-down box is to modify or show the message you specify. There are three options:

Not Display Descriptions: Hide the user-specified message in the Description field of each slide-in converter.

Display Descriptions: Show the product information and the user-specified message of each slide-in converter both in the fields of Description and Overview.

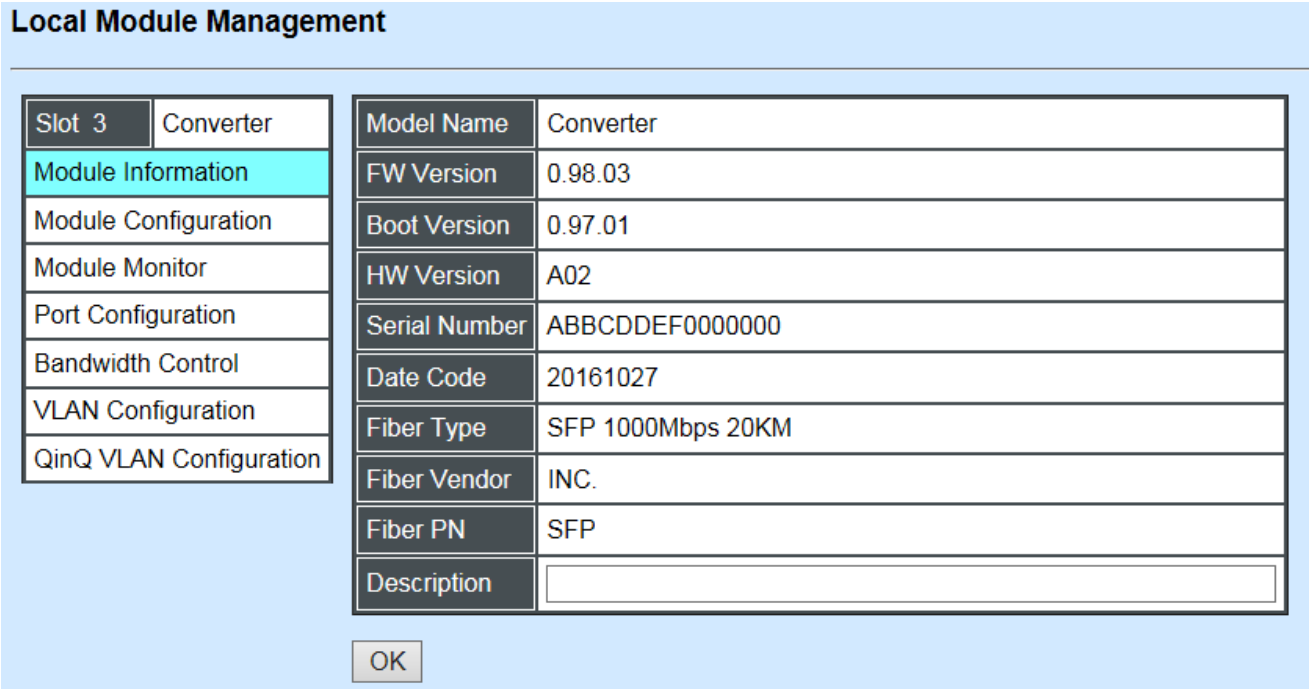
Edit Descriptions: Change the user-specified message of each slide-in converter separately.



To modify the description, click drop-down box and select **Edit Descriptions**.

Click "**OK**" to save edited message.

Click on the available modules and then the following screen page appears.



Module Information: Display the model name, version of FW/Boot/HW, serial number, date code, fiber type, fiber vendor, fiber PN and description.

Module Configuration: Set up Link Alarm function.

Module Monitor: Display information about Media Type, Port State, Link State, Auto-Negotiation status, Speed, Duplex, Flow Control.

Port Configuration: Set up Media Type, Port State, Port Type, Port Speed, Duplex.

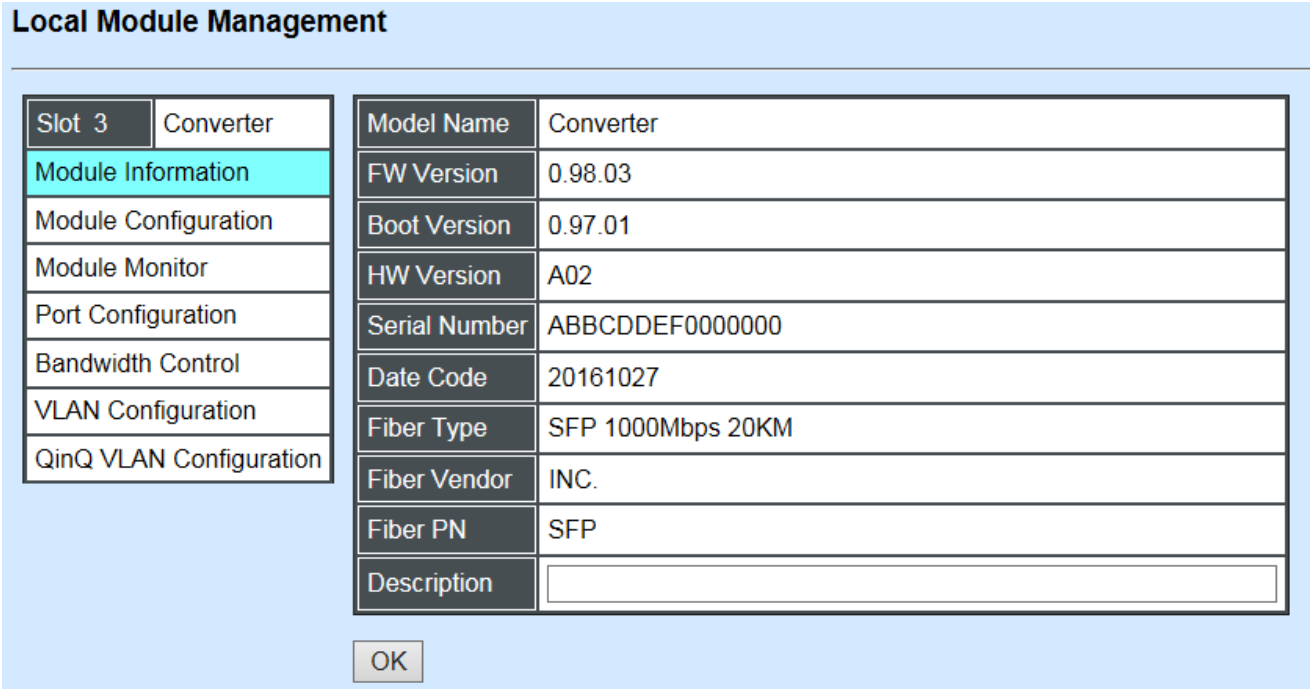
Bandwidth Control: Set up Egress Rate Limit, Broadcast Storm Blocking.

VLAN Configuration: Set up TP/FX default PVID, Egress Mode.

QinQ VLAN Configuration: Configure Q-in-Q (double tag) VLAN settings.

D.2.1.1 Module Information

Select the option **Module Information** from the **Local Module Management** menu, then the **Module Information** fields show up on the right to provide you information about the module.



Model Name: View-only field that shows the product's model name.

FW Version: View-only field that shows the product's firmware version.

Boot Version: View-only field that shows the product's boot loader version.

HW Version: View-only field that shows the product's hardware version.

Serial Number: View-only field that shows the product's serial number.

Date Code: View-only field that shows the date of EEPROM burned.

Fiber Type: View-only field that shows the product's fiber connector type, speed, and distance.

Fiber Vendor: View-only field that shows the vendor name.

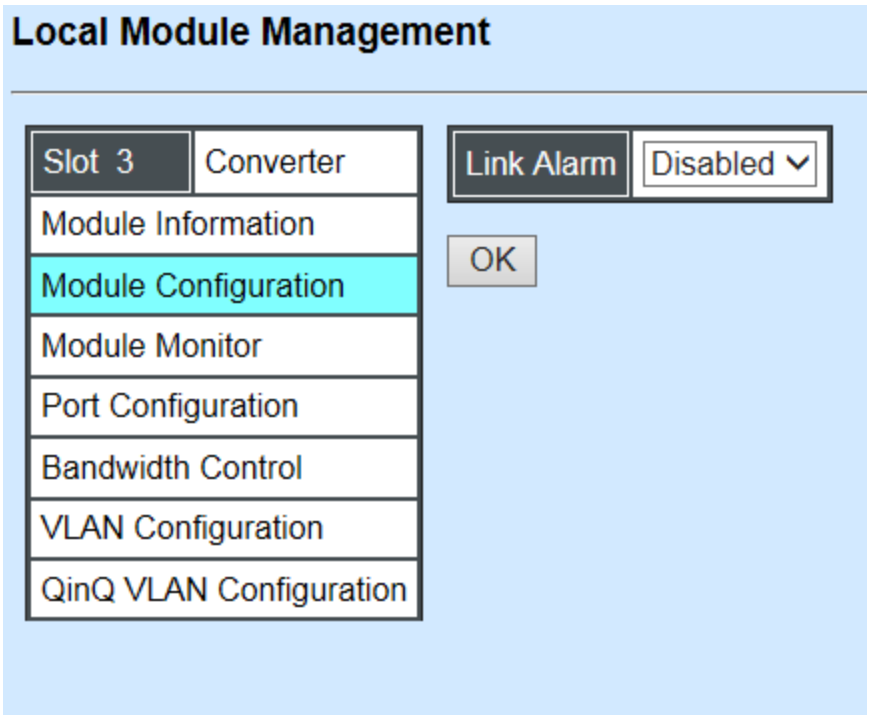
Fiber PN: View-only field that shows the fiber PN.

Description: Specify the appropriate brief description for the slide-in converter module.

D.2.1.2 Module Configuration

Select the option **Module Configuration** from the **Local Module Management** menu, then **Module Configuration** fields show up on the right to let you view the configuration of the converter.

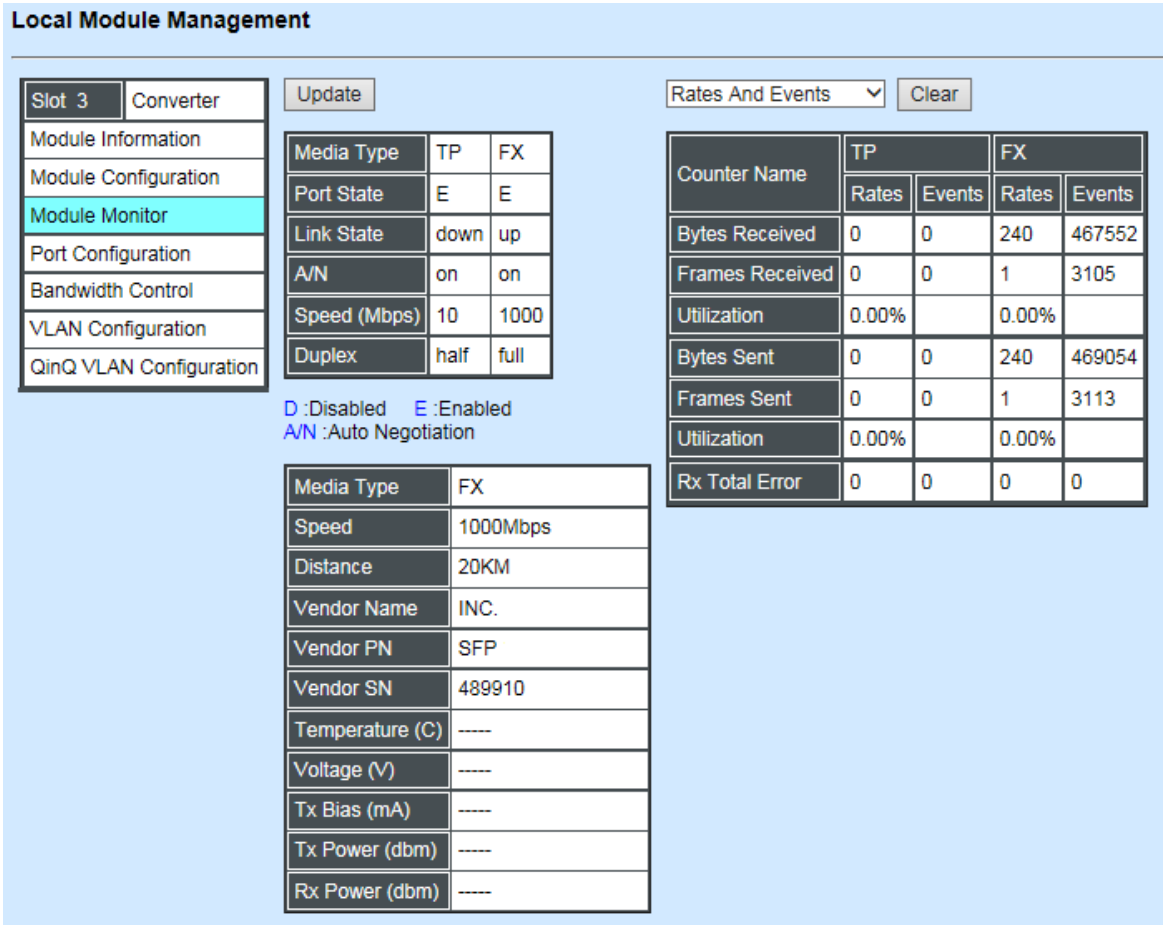
Link Alarm: This function is used under the circumstance that when UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.



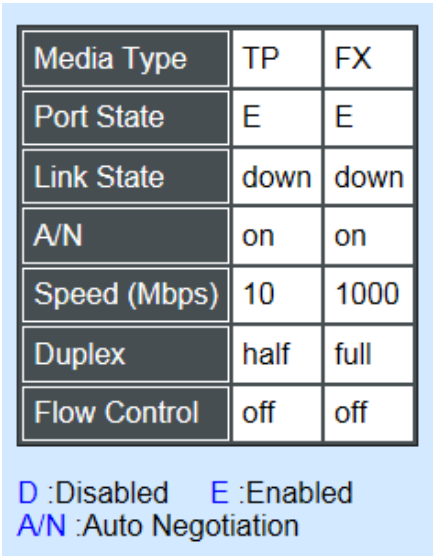
Click the drop-down box to enable or disable link alarm of the converter.

D.2.1.3 Module Monitor

Select the option **Module Monitor** from the **Local Module Management** menu, then **Module Monitor** fields show up on the right to let you view the configuration of the module.



Port Status



Media Type: TP (copper, 10/100Base-T, RJ-45) and FX (fiber).

Port State: View-only field that shows traffic is Disabled or Forwarding.

Link State: View-only field that shows the link is up or down.

A/N: View-only field that shows Auto-negotiation is on or off.

Speed: View-only field that shows the port speed.

Duplex: View-only field that shows the duplex mode is half or full.

Flow Control: View-only field that shows the flow control is on or off.

SFP Status

Media Type	FX
Speed	--
Distance	--
Vendor Name	--
Vendor PN	--
Vendor SN	--
Temperature (C)	-----
Voltage (V)	-----
Tx Bias (mA)	-----
Tx Power (dbm)	-----
Rx Power (dbm)	-----

Media Type: Show the type of FX (fiber).

Speed: Data rate of the slide-in SFP Transceiver.

Distance: Transmission distance of the slide-in SFP Transceiver.

Vendor Name: Vendor name of the slide-in SFP Transceiver.

Vendor PN: Vendor PN of the slide-in SFP Transceiver.

Vendor SN: Vendor SN of the slide-in SFP Transceiver.

Temperature (C): The Slide-in SFP module operation temperature.

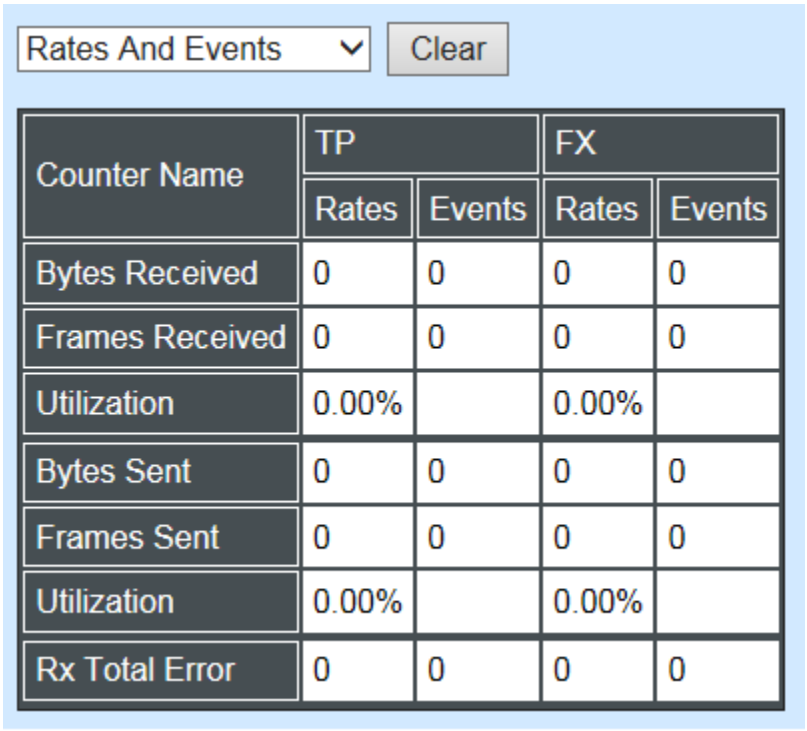
Voltage (V): The Slide-in SFP module operation voltage.

TX Bias (mA): The Slide-in SFP module operation current.

TX Power (dbm): The Slide-in SFP module optical Transmission power.

RX Power (dbm): The Slide-in SFP module optical Receiver power.

Select **"Rates and Events"** option from the Counters Display pull-down menu to view the detailed traffic statistics (counters' information).



Counter Name	TP		FX	
	Rates	Events	Rates	Events
Bytes Received	0	0	0	0
Frames Received	0	0	0	0
Utilization	0.00%		0.00%	
Bytes Sent	0	0	0	0
Frames Sent	0	0	0	0
Utilization	0.00%		0.00%	
Rx Total Error	0	0	0	0

Rates: Counters displayed and updated once per second.

Events: The count is cumulative (i.e. cumulated count).

Bytes Received: The total number of bytes received from this port.

Frames Received: The total number of frames received from this port.

Utilization: The utilization of receiving bandwidth from this port.

Bytes Sent: The total number of bytes sent from this port.

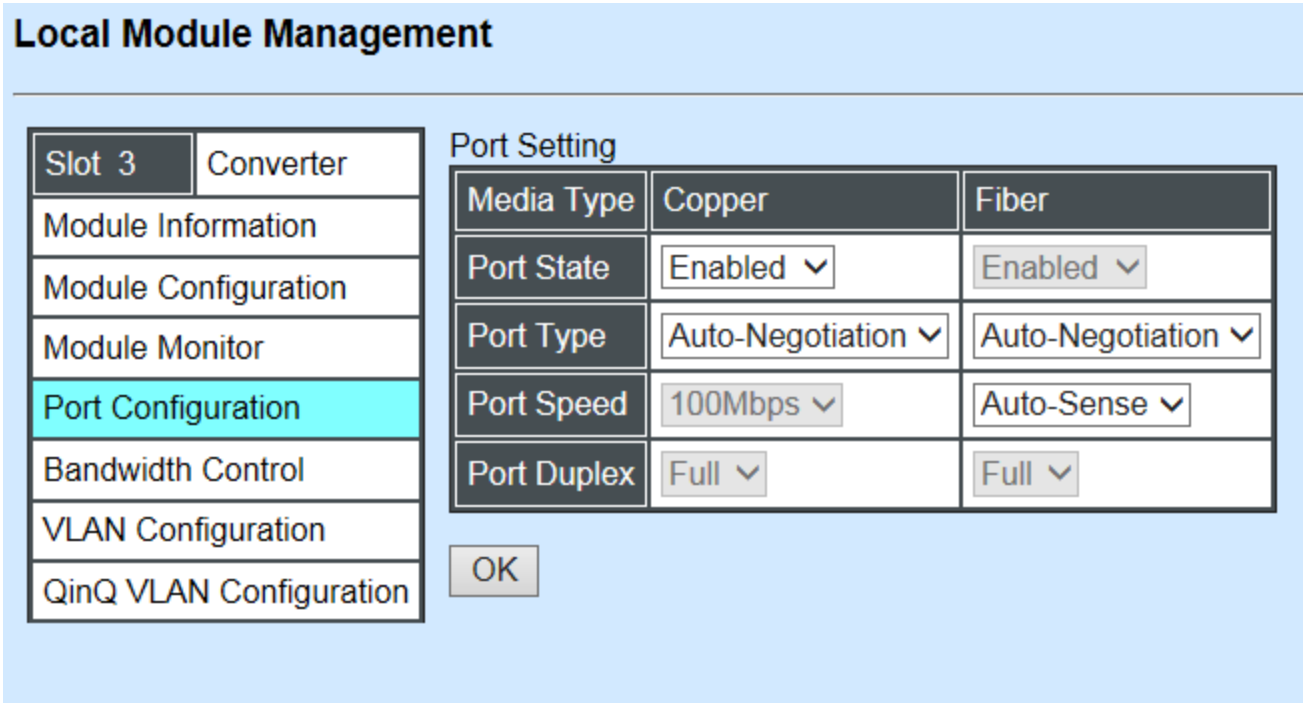
Frames Sent: The total number of frames sent from this port.

Utilization: The utilization of sending bandwidth from this port.

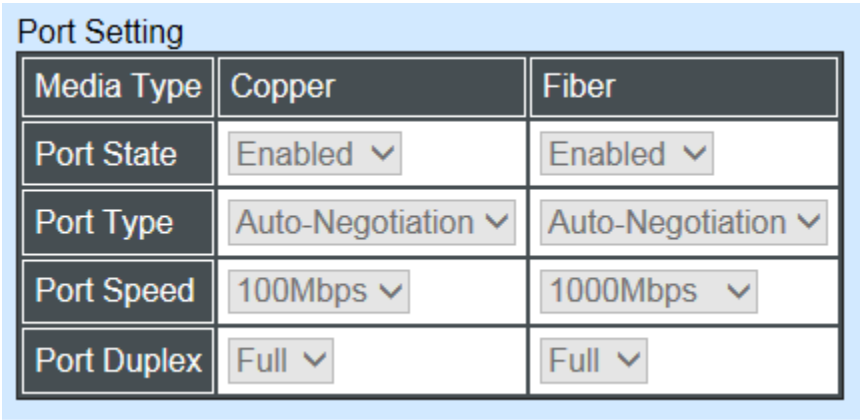
RX Total Errors: The total number of errors frames from this port.

D.2.1.4 Port Configuration

Select the option **Port Configuration** from the **Local Module Management** menu, then the **Port Configuration** fields show up on the right to let you configure them accordingly.



Port Setting



Media Type: Select between Copper (UTP, RJ-45) and Fiber

Port State: Enable or disable port state.

Port Type: Show the port type configuration is manual or auto-negotiation.

Port Speed: Show the port speed of the selected media type.

Port Duplex: Show the duplex mode is half or full.

Click "**OK**" to apply.

DIP Setting
You are allowed to view the DIP switch configuration via WEB UI.

DIP Setting

Media Type	Copper	Fiber
Port Type	Auto-Negotiation	Auto-Negotiation
Port Speed	100Mbps	100Mbps
Link Alarm	Enabled	

Currently controlled by device hardware dip switch.
Please consider to change device dip switch setting as software control.

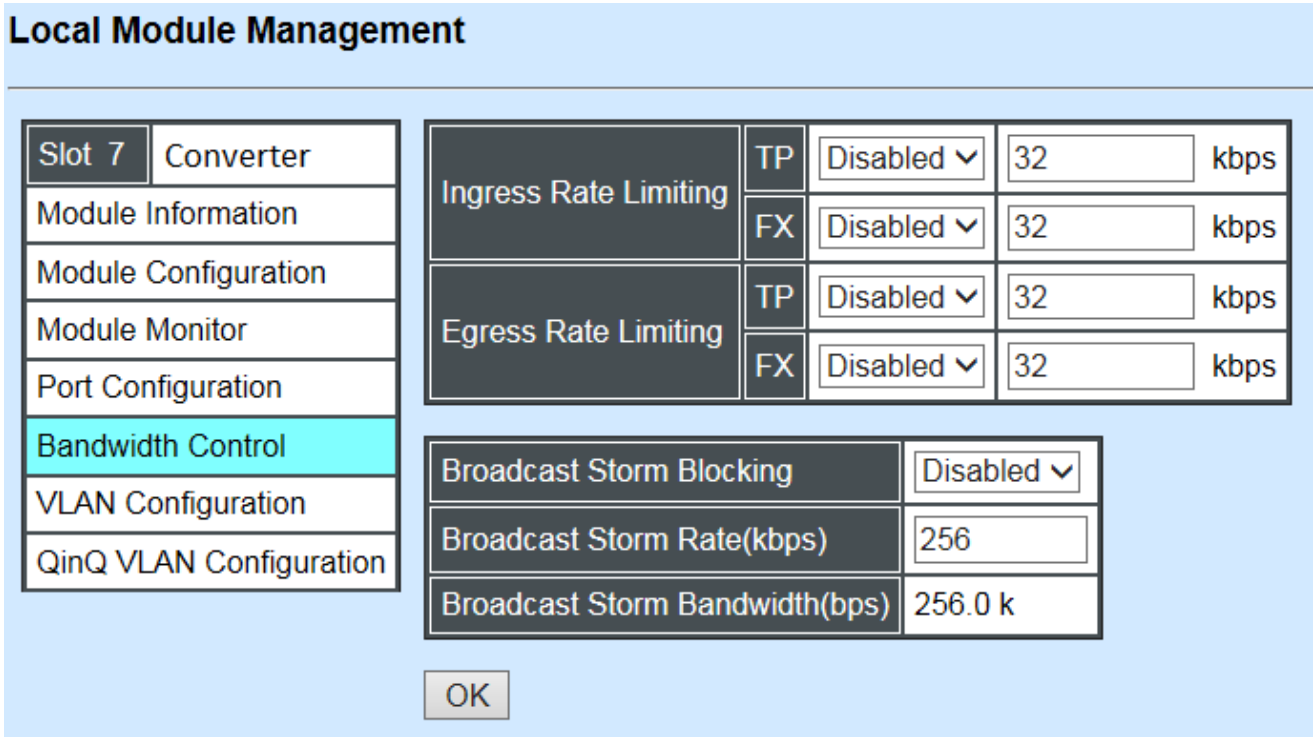
Port Type: View-only field that shows the port type configuration is manual or auto-negotiation.

Port Speed: View-only field that shows the port speed of the selected media type.

Link Alarm: View-only field that shows the link alarm is enabled or disabled.

D.2.1.5 Bandwidth Control

Select the option **Bandwidth Control** from the **Local Module Management** menu, then the **Bandwidth Control's** Ingress/Egress Rate Limit and Broadcast Storm fields show up on the right to let you enable/disable TP/FX, specify the rate in kbps, enable/disable broadcast Storm settings and specify the rate in kbps in broadcast storm blocking.



Ingress Rate Limiting: Enable or disable TP ingress rate limiting in kbps and set up current configured ingress bandwidth in kbps. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

Egress Rate Limiting: Enable or disable TP egress rate limiting in kbps and set up current configured egress bandwidth in kbps. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

Broadcast Storm Blocking: Enable or disable broadcast storm blocking function.

Broadcast Storm Rate(kbps): Set up storm rate value. Packets exceeding the value will be dropped. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

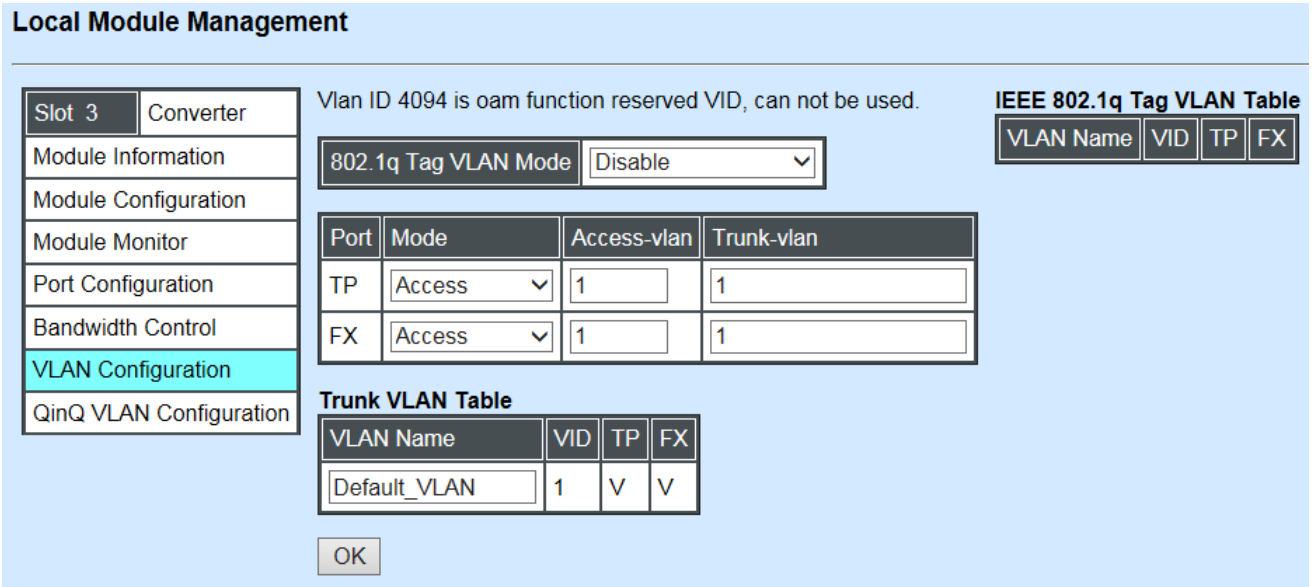
Broadcast Storm Rate Bandwidth(bps): Display the current configured storm rate bandwidth.

D.2.1.6 VLAN Configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the CHASSIS on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

Select the option **VLAN Configuration** from the **Local Module Management** menu, then the **VLAN Configuration's** Default VLAN Mode and Table fields show up on the right to let you specify the TP/FX of VLAN settings.



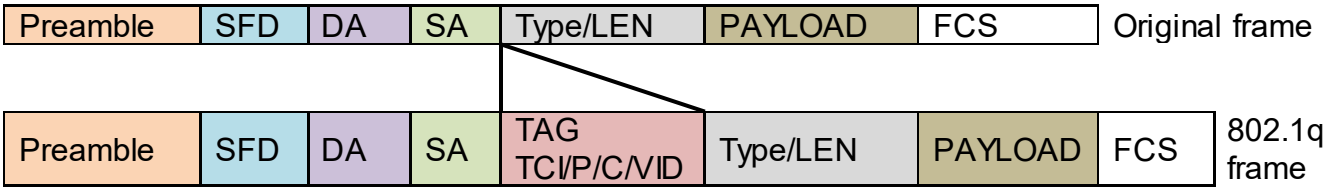
The Managed Media Converter supports **IEEE 802.1q Tag VLAN**.

IEEE 802.1Q VLAN Concepts

Port-Based VLAN is simple to implement and use, but it cannot be deployed cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution to this problem. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large switched networks into smaller segments so that

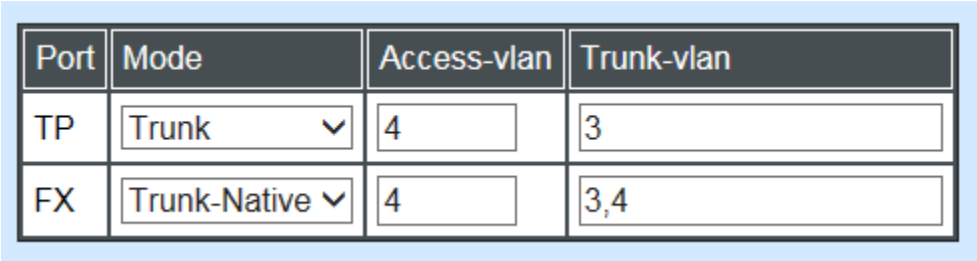
broadcast and multicast traffic will not occupy too much available bandwidth as well as provide a higher level security between segments of internal networks.

Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes		User data	
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

IEEE 802.1q Tag VLAN Mode: Enable or disable IEEE 802.1q Tag VLAN mode, or select Bypass Ctag Mode which ignore C-tag checking.



Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When

the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

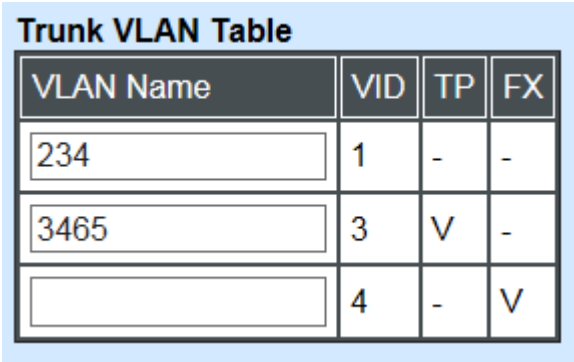
A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.



Trunk VLAN table: To edit 802.1Q Tag VLAN Name.

VLAN Name: User-specified field to give VLAN a name.

VID: The VLAN ID (**VID**) specifies the set of VLAN that a given port is allowed to receive and send **labeled** packets.

TP: It shows whether the TP port that is included in a given VID.

FX: It shows whether the Fiber port that is included in a given VID.

Click **"OK"** to apply.

IEEE 802.1q Tag VLAN Table

VLAN Name	VID	TP	FX
234	1	V	V

IEEE 802.1q Tag VLAN Table: It shows the status of IEEE 802.1q Tag VLAN.

VLAN Name: View-only filed that shows the VLAN name.

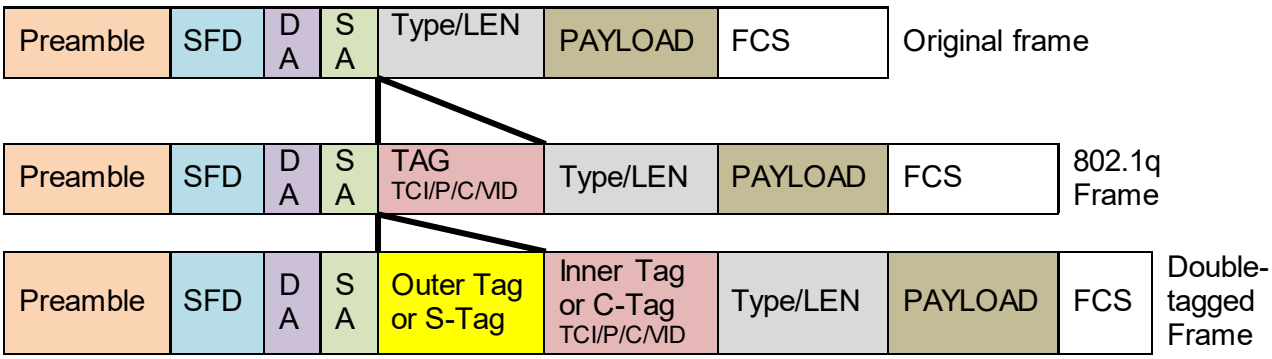
VID: View-only filed that shows the VID.

TP: View-only filed that shows whether the TP port that is included in a given VID.

FX: View-only filed that shows whether the fiber port that is included in a given VID.

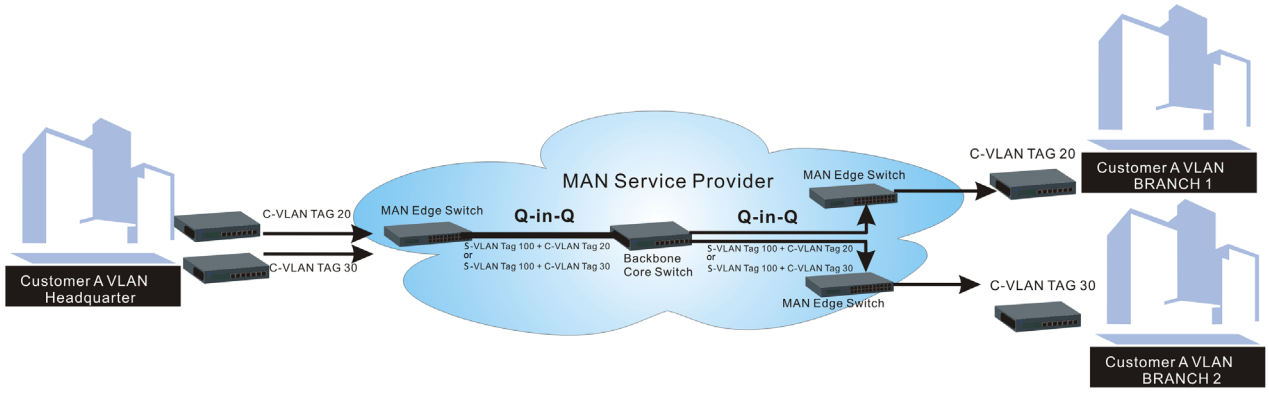
D.2.1.7 Q-in-Q VLAN Configuration

The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a "double-tagged" frame is created so as to separate customer traffic within a service provider network. As shown below in "Double-Tagged Frame" illustration, an outer tag is added between source destination and inner tag at the provider network's edge. This can support C-VLAN (Customer VLAN) over Metro Area Networks and ensure complete separation between traffic from different user groups. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single S-VLAN (Service VLAN) tag per customer over the Metro Ethernet network.



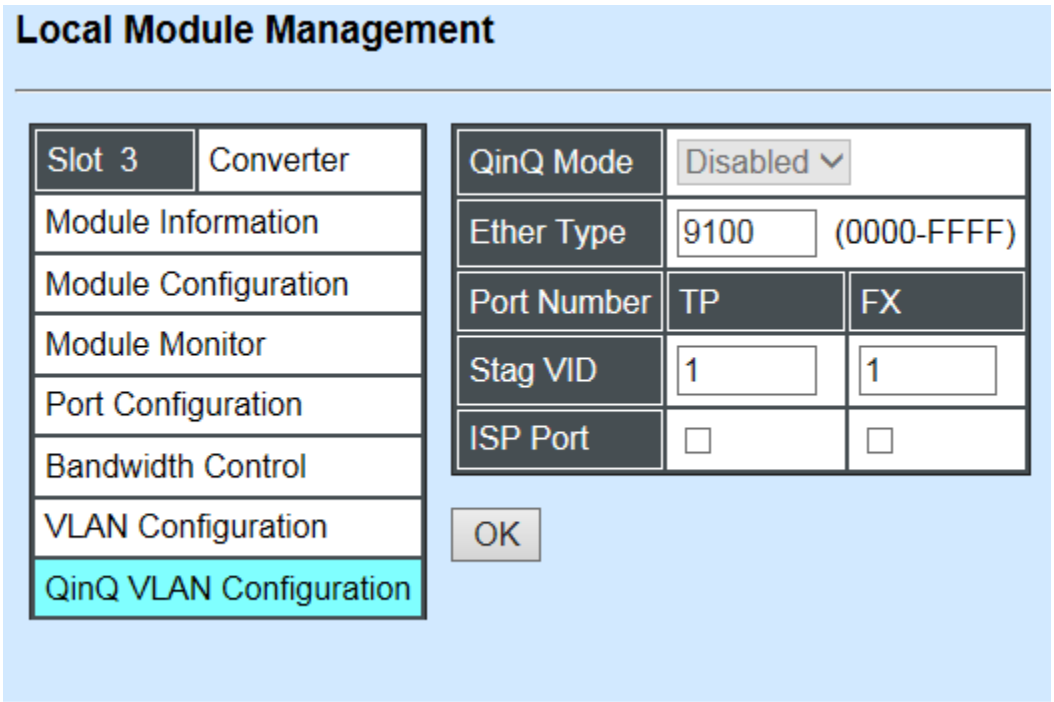
Double-Tagged Frame

As shown below in “Q-in-Q Example” illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider’s backbone, there is a possibility that traffic might be forwarded insecurely, for example due to the same VLAN ID used. Therefore, in order to get the information from Headquarter to Branch 1, the easiest way for the carrier to ensure security to customers is to encapsulate the original VLAN with a second VLAN ID of 100. This second VLAN ID is known as S-VLAN (Service VLAN) that is added as data enters the service provider’s network and then removed as data exits. Eventually, with the help of S-Tag, the information sent from Headquarter to Branch 1 can be delivered with customers’ VLANs intactly and securely.



Q-in-Q Example

This section allows you to set up Q-in-Q VLAN. Select the option **QinQ VLAN Configuration** from the **Local Module Management** menu, **Q-in-Q VLAN** fields show up on the right.



QinQ Mode: Enable or disable the function by clicking drop-down box.

Ether Type: A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).

Port Number: Two kinds of ports are available, TP port or Fiber port.

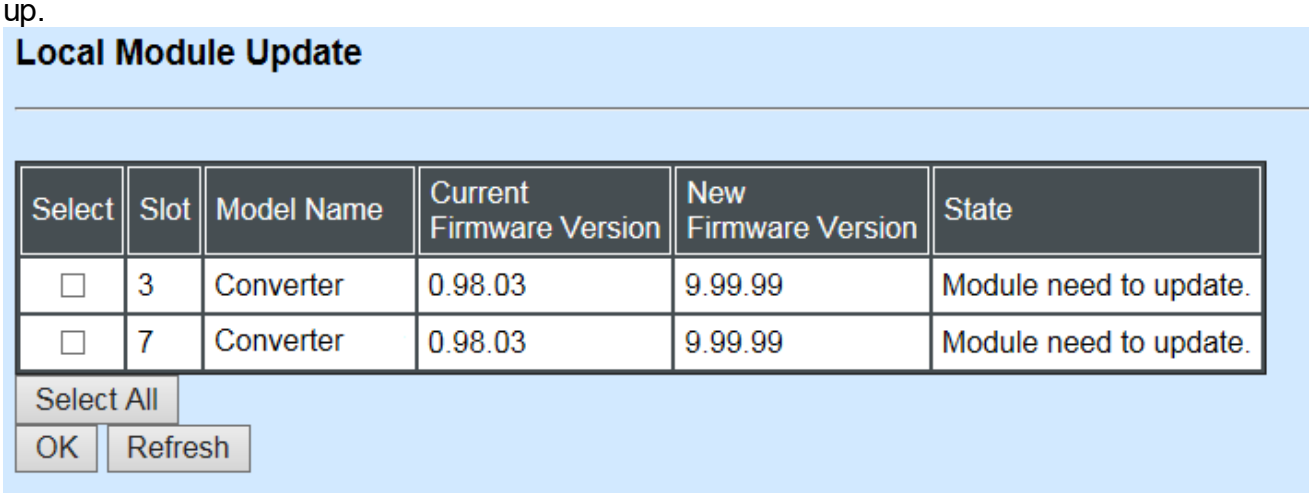
Stag(Service Tag) VID: Specify a VID for the service tag (Outer Tag).

ISP(Internet Service Provider) Port: This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.

Click the **"OK"** button to apply the settings.

D.2.2 Local Module Update

Select **Local Module Update** from the **Main Menu**, then the following screen page shows up.



Select: Check the box to upgrade the firmware on specified converters or click **Select All** button to upgrade the firmware on all converters.

Slot: Show which slot the converter is inserted into.

Model Name: Show the current model name of the converter.

Current Firmware Version: Show the current firmware version used for each converter.

New Firmware Version: The upcoming firmware version to be installed.

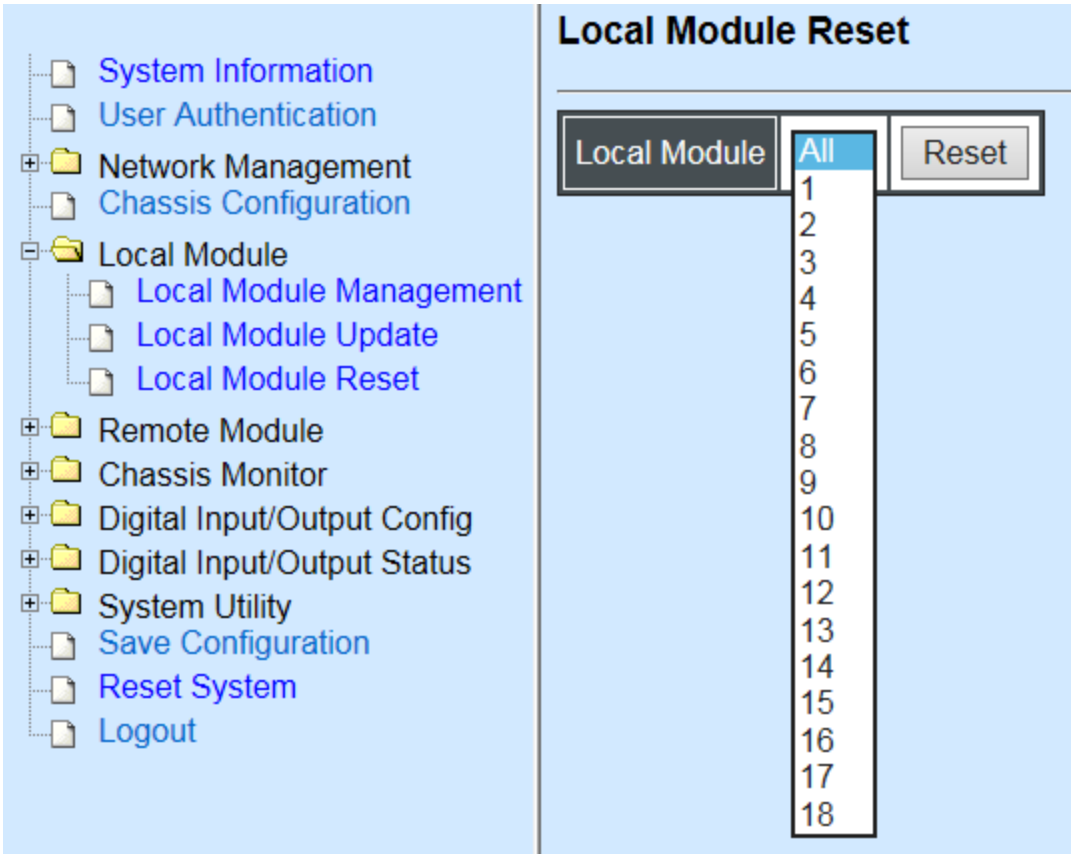
State: Show the current status of firmware upgrade.

Click **"OK"** to start module update procedure.

Click **"Refresh"** to renew all update module information.

D.2.3 Local Module Reset

Select **Local Module Reset** from the **Main Menu**, then the following screen page shows up.



Local Module: Select **"All"** to reset all modules or select the individual module. When you decide which module to be reset, click **Reset** button to begin the reset process.

APPENDIX E: MCT-2612 Converter

This section is used to introduce 10/100BASE-T to 100BASE-X standalone Media Converter which is specifically designed to fulfill emerging deployment needs of fiber Ethernet networks.

E.1 CLI Command

This is to how the converter is presented via CLI Command.

E.1.1 Local Module Configuration

This section is intended to introduce the configuration of specified media converters.

Note: *Make sure that media converts are firmly installed and powered on.*

1. Specify any slots to configure

Slot command	Parameter	Description
MCT-RACK(config)# slot [slot_list]	[slot_list]	Specify any slots you want to configure.

2. Upgrade media converter firmware.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# firmware upgrade		Upgrade the firmware. **Note:** Upgrade one media converter at a time.

3. Configure link alarm

When UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module link-alarm		Enable link alarm function.
No Command		
MCT-RACK(config-slot-slot-slot)# no module link-alarm		Disable link alarm function.
Show Command		
MCT-RACK(config-slot-slot-slot)# show module		Show the status of link alarm.

4. Set up module description

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module-info description [description]	[description]	Specify user-defined information. Up to 55 characters are available.
No Command		
MCT-RACK(config-slot-slot-slot)# no module-info description		Delete user-defined information.
Show Command		
MCT-RACK(config-slot-slot-slot)# show module-info		Show the module information.
Module Description Example		
MCT-RACK(config-slot-slot-slot)# module-info description 123		The description of the converter is named “123”.

5. Reset converter

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# reload		Reboot the media converters.

6. Set up security protection

When a device on the network is malfunctioning or application programs are not well designed or properly configured, broadcast storms may occur, which may degrade network performance or in the worst situation cause a complete halt. The Chassis allows users to set a threshold rate for broadcast traffic so as to protect network from broadcast storms. Any broadcast packet exceeding the specified value will then be dropped.

Security command	Parameter	Description
MCT-RACK(config)# security storm-protection		Enable storm protection function.
MCT-RACK(config)# security storm-protection rates [32-1000000] kbps	[32-1000000] kbps	Specify the maximum broadcast packet rate. **Note:** For Fast Ethernet model, specify the rates no more than 100000 kbps.
No command		
MCT-RACK(config)# no security storm-protection		Disable storm protection globally.
MCT-RACK(config)# no security storm-protection rates		Set broadcast packet rate back to the default.

Show command	
MCT-RACK(config)# show security storm-protection	Show storm control settings.

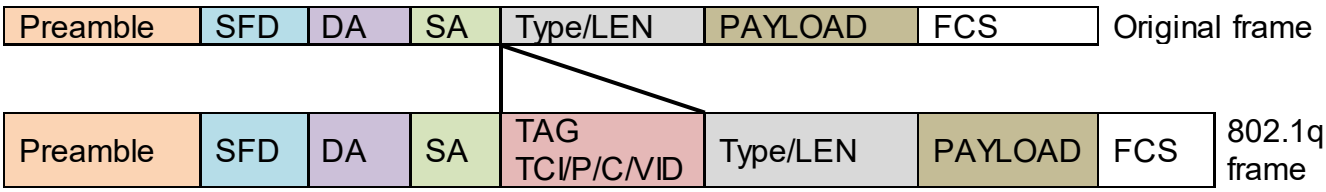
7. Set up VLAN configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the device on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

IEEE 802.1Q VLAN Concepts

Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes		User data	
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.

Example : PortX configuration

Configuration	Result
Trunk-VLAN = 10, 11, 12 Access-VLAN = 20 **Mode = Access**	PortX is an **Access Port** PortX's **VID** is ignored PortX's **PVID** is 20 PortX sends **Untagged** packets (PortX takes away VLAN tag if the PVID is 20) PortX receives **Untagged** packets only
Trunk-VLAN = 10,11,12	PortX is a **Trunk Port**

Access-VLAN = 20 **Mode = Trunk**	PortX's **VID** is 10,11 and 12 PortX's **PVID** is ignored PortX sends and receives **Tagged** packets VID 10,11 and 12
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Trunk-native**	PortX is a **Trunk-native Port** PortX's **VID** is 10,11 and 12 PortX's **PVID** is 20 PortX sends and receives **Tagged** packets VID 10,11 and 12 PortX receives **Untagged** packets and add PVID 20

The CHSSSIS supports two types of VLAN, these are: **IEEE 802.1q Tag VLAN** and **Q-in-Q VLAN**.

VLAN Command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# vlan dot1q-vlan		Enable IEEE 802.1q Tag VLAN mode.
MCT-RACK(config-slot-slot-slot)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VID number to create an 802.1q VLAN. **Note :** 802.1q VLAN ID need to be created under interface command. In here you can only modify it instead of creating a new VLAN ID.
MCT-RACK(config-slot-slot-slot)# vlan qinq-vlan		Enable Q-in-Q VLAN.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan bypass-ctag		Ignore the C-tag checking.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan isp-port [port_list]	[port_list]	Configure ISP Port (Q-in-Q Port). **ISP(Internet Service Provider) Port:** This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.
MCT-RACK(config-slot-slot-slot)# vlan qing-vlan stag-ethertype [0xWXYZ]	[0xWXYZ]	Specify service tag ether type. **Ether Type:** A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).
No Command		
MCT-RACK(config-slot-slot-slot)# no vlan dot1q-vlan		Disable IEEE 802.1q Tag VLAN mode.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan		Disable Q-in-Q VLAN.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan bypass-ctag		Not ignore the C-tag checking.

MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan isp-port		Undo ISP port (Q-in-Q port).
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan management-stag		Clear management service tag VID.
MCT-RACK(config-slot-slot-slot)# no vlan qinq-vlan stag-ethertype		Delete service tag ether type.
Show Command		
MCT-RACK(config-slot-slot-slot)# show vlan dot1q-vlan		Show dot1q VLAN configuration.
MCT-RACK(config-slot-slot-slot)# show vlan interface		Show all interfaces on a media converter.
MCT-RACK(config-slot-slot-slot)# show vlan interface [port_list]	[port_list]	Show specific interfaces on a media converter.
MCT-RACK(config-slot-slot-slot)# show vlan qinq-vlan		Show Q-in-Q VLAN configuration.

8. Use "Slot" command to configure 802.1q VLAN settings on a port.

Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid [1-4094]	[1-4094]	Specify the service tag VID for the selected port(s).

No Command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid		Clear the service tag VID specified.

E.1.2 Local Module Port Configuration

This is to configure port via "interface" command.

This command is to configure TP port or fiber port on a converter.

Interface command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.

1. Configure auto-negotiation function.

Interface command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# auto-negotiation		Set the selected interfaces' to auto-negotiation. When auto-negotiation is enabled, speed configuration will be ignored.
No command		**No command**
MCT-RACK(config-slot-slot-slot-if-port-port)# no auto-negotiation		Disable auto-negotiation function.

2. Set up Duplex Mode

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# duplex [full]	[full]	Configure port duplex to **full**.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no duplex		Set the selected ports' duplex mode to the default setting. **Note :** Auto-negotiation needs to be disabled before configuring duplex mode.

3. QoS configuration

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# qos rate-limit ingress [0|32-1000000]	[0|32-1000000]	Configure **ingress** rate limit, set zero or from 32Kbps to 1000Mbps. **Note:** For Fast Ethernet model, specify no more than 100000kbps.
MCT-RACK(config-slot-slot-slot-if-port-port)# qos rate-limit egress [0|32-1000000]	[0|32-1000000]	Configure **egress** rate limit, set zero or from 32Kbps to 1000Mbps. **Note:** For Fast Ethernet model, specify no more than 100000kbps.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no qos rate-limit ingress		Undo **ingress** rate limit.
MCT-RACK(config-slot-slot-slot-if-port-port)# no qos rate-limit egress		Undo **egress** rate limit.

4. Shutdown interface

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# shutdown		Administratively disable the selected ports' status.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no shutdown		Administratively enable the selected ports' status.

5. Speed configuration

Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-	[1000 |100 |	Set up the selected interfaces' speed.

if-port-port)# speed [1000 |100 | 10 | auto_sense]	10 | auto_sense]	**Note:** For TP port, manual speed configuration only works when "no auto-negotiation" command is issued. For Fast Ether net model, the speed of TP port is available in 100 or 10 Mbps only; the speed of FX port is available in 100 Mbps only.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no speed		Set the selected ports' speed to the default setting.

6. Configure 802.1q VLAN settings on a port.

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port "1" represents TP port while port "2" fiber port.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid [1-4094]	[1-4094]	Specify the service tag VID for the selected port(s).
No Command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan access-		Set the selected ports' PVID to the default setting.

vlan		
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
MCT-RACK(config-slot-slot-slot-if-port-port)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
MCT-RACK(config-slot-slot-slot-if-port-port)# vlan qinq-vlan stag-vid		Clear the service tag VID specified.

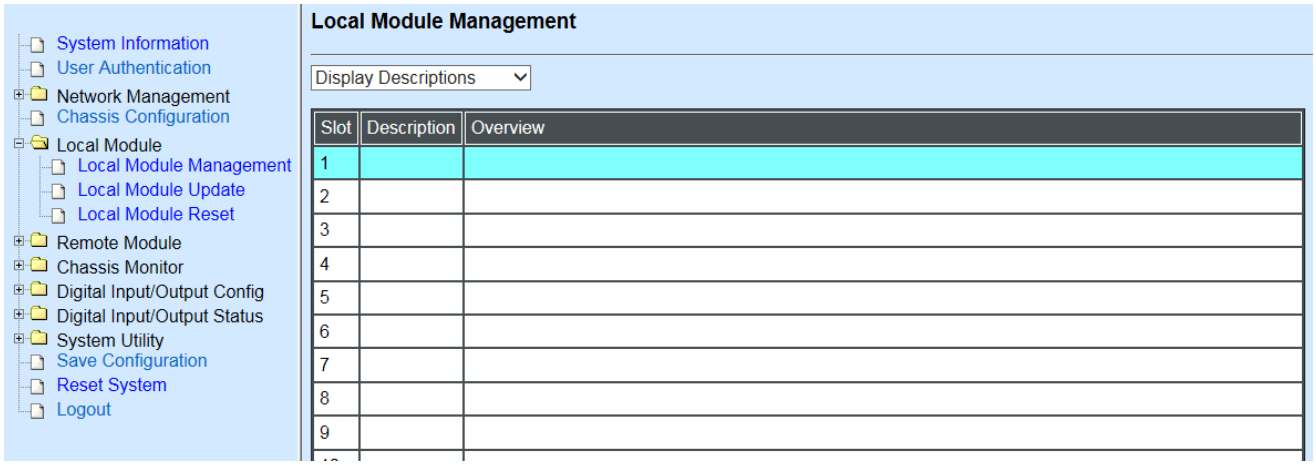
E.2 Web Management

This is to how the converter is presented via Chassis on Web UI.

E.2.1 Local Module Management

In order to manage the installed converters and set up required functions, select the option **Local Module Management** from **Main Menu**, then **Local Module Management** screen page shows up.

Note: The slot configuration will return to the default if we replace Gigabit media converter with Fast media converter.



Overview: Show the product information of each slide-in converter.

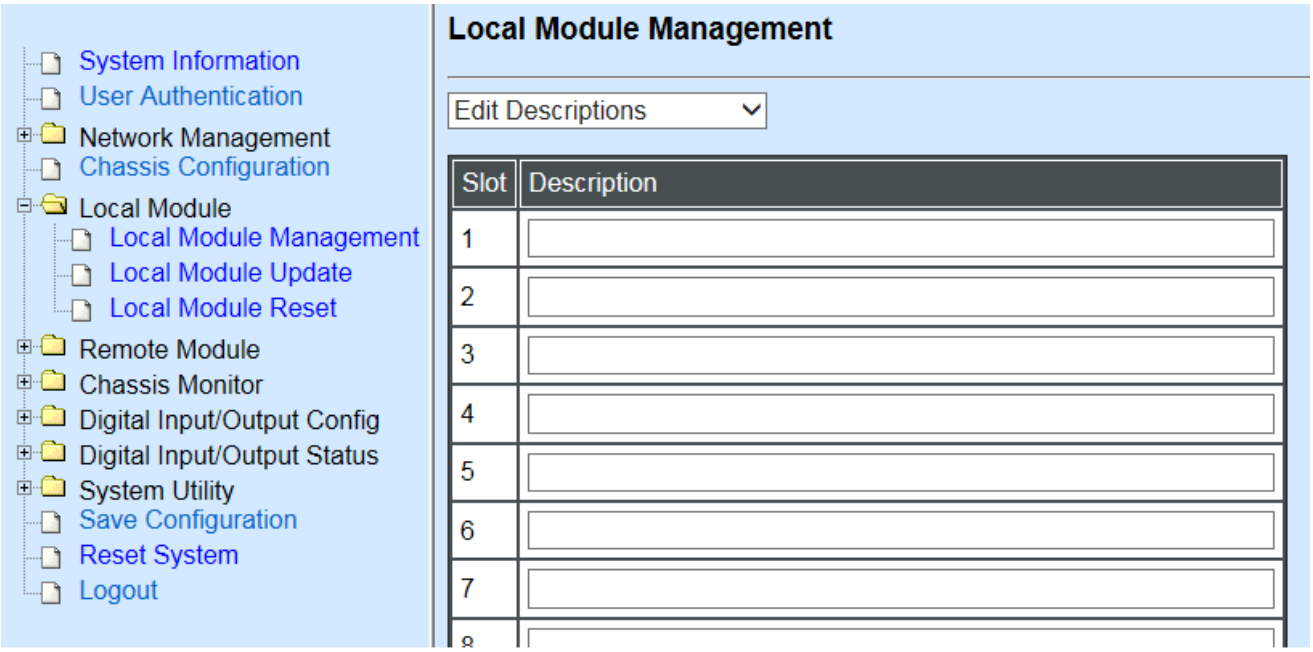
Description: Show the user-specified message of each slide-in converter.

The drop-down box is to modify or show the message you specify. There are three options:

Not Display Descriptions: Hide the user-specified message in the Description field of each slide-in converter.

Display Descriptions: Show the product information and the user-specified message of each slide-in converter both in the fields of Description and Overview.

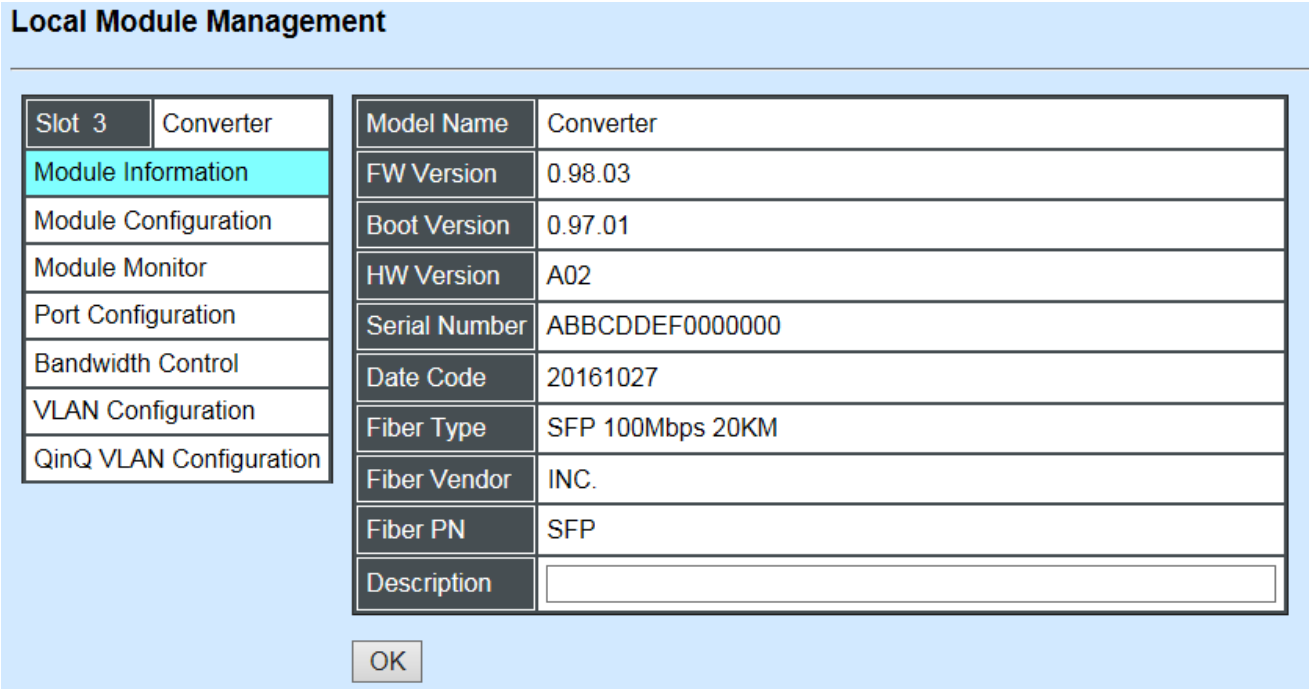
Edit Descriptions: Change the user-specified message of each slide-in converter separately.



To modify the description, click drop-down box and select **Edit Descriptions**.

Click **"OK"** to save edited message.

Click on the available modules and then the following screen page appears.



Module Information: Display the model name, version of FW/Boot/HW, serial number, date code, fiber type, fiber vendor, fiber PN and description.

Module Configuration: Set up Link Alarm function.

Module Monitor: Display information about Media Type, Port State, Link State, Auto-Negotiation status, Speed, Duplex, Flow Control.

Port Configuration: Set up Media Type, Port State, Port Type, Port Speed, Duplex.

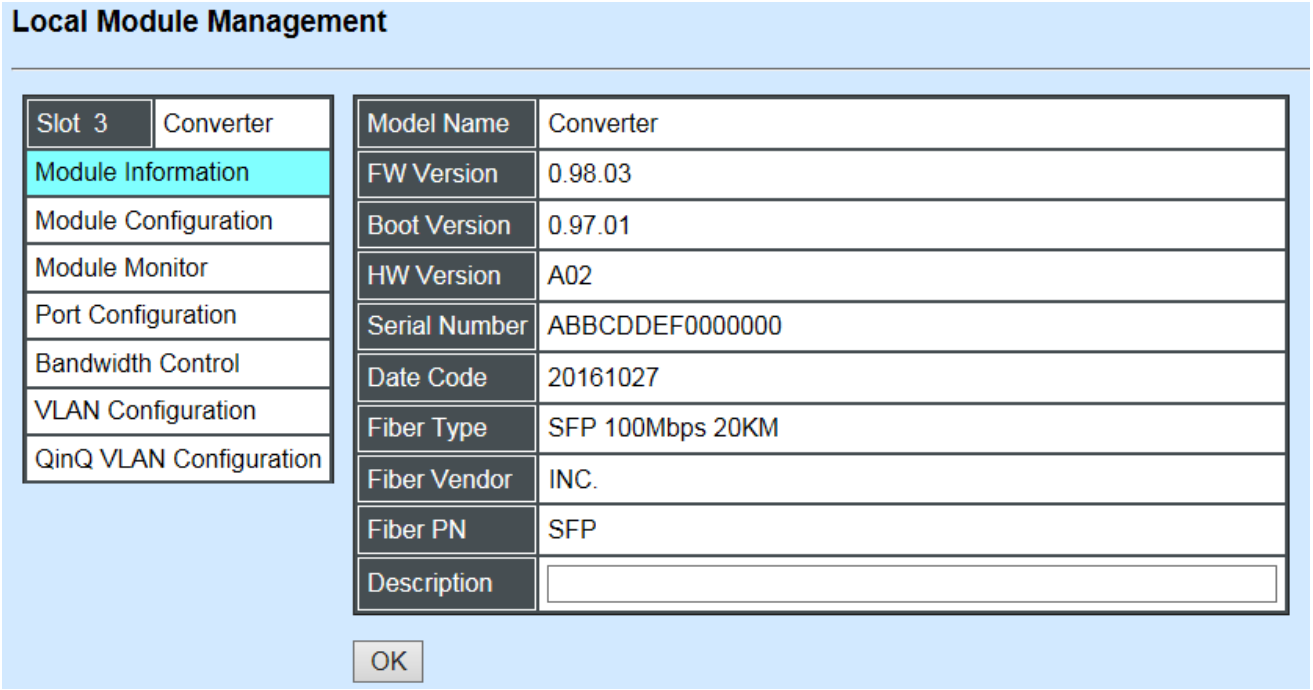
Bandwidth Control: Set up Egress Rate Limit, Broadcast Storm Blocking.

VLAN Configuration: Set up TP/FX default PVID, Egress Mode.

QinQ VLAN Configuration: Configure Q-in-Q (double tag) VLAN settings.

E.2.1.1 Module Information

Select the option **Module Information** from the **Local Module Management** menu, then the **Module Information** fields show up on the right to provide you information about the module.



Model Name: View-only field that shows the product's model name.

FW Version: View-only field that shows the product's firmware version.

Boot Version: View-only field that shows the product's boot loader version.

HW Version: View-only field that shows the product's hardware version.

Serial Number: View-only field that shows the product's serial number.

Date Code: View-only field that shows the date of EEPROM burned.

Fiber Type: View-only field that shows the product's fiber connector type, speed, and distance.

Fiber Vendor: View-only field that shows the vendor name.

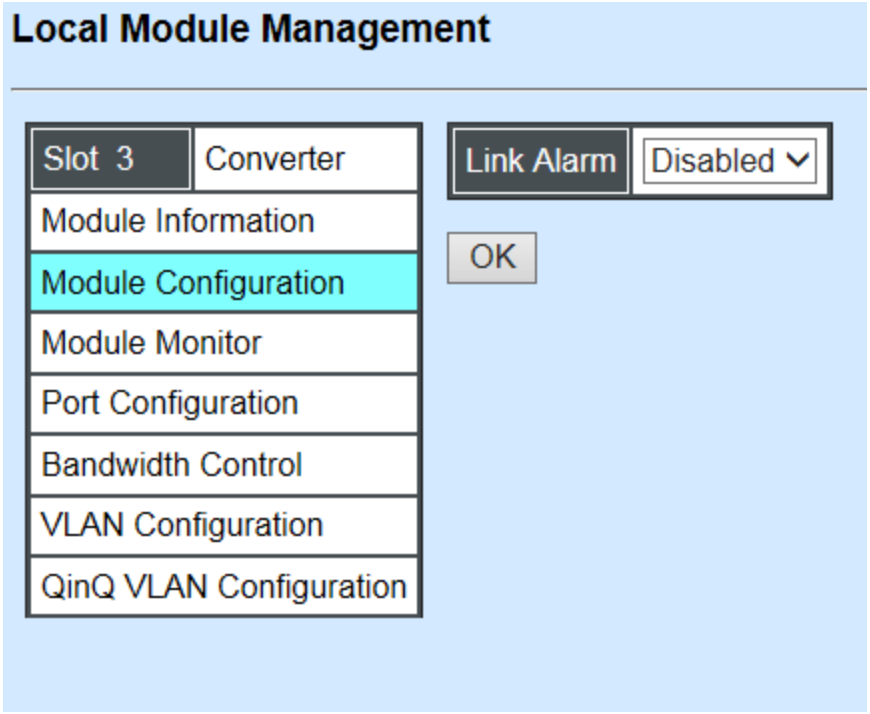
Fiber PN: View-only field that shows the fiber PN.

Description: Specify the appropriate brief description for the slide-in converter module.

E.2.1.2 Module Configuration

Select the option **Module Configuration** from the **Local Module Management** menu, then **Module Configuration** fields show up on the right to let you view the configuration of the converter.

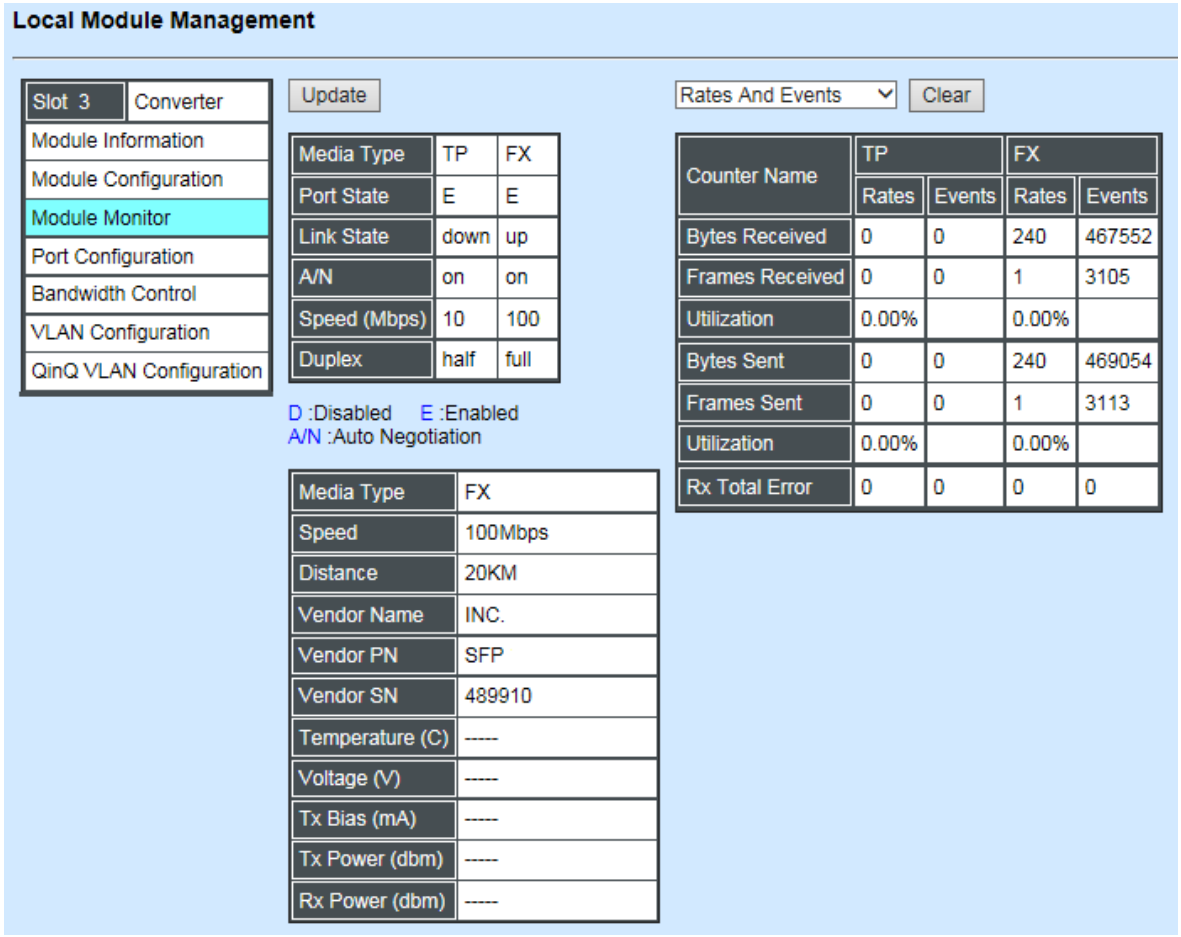
Link Alarm: This function is used under the circumstance that when UTP or fiber port is down during operation, the other port will be automatically turned off to alert the user.



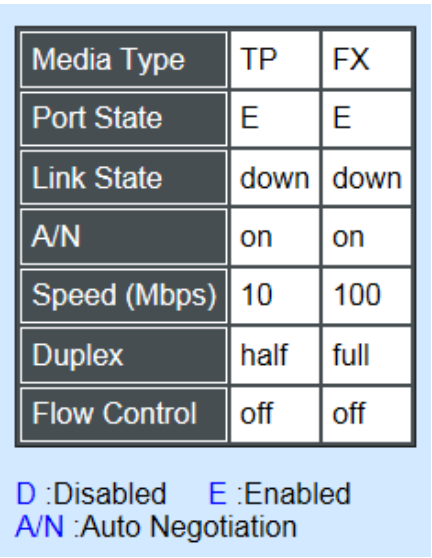
Click the drop-down box to enable or disable link alarm of the converter.

E.2.1.3 Module Monitor

Select the option **Module Monitor** from the **Local Module Management** menu, then **Module Monitor** fields show up on the right to let you view the configuration of the module.



Port Status



Media Type: TP (copper, 10/100Base-T, RJ-45) and FX (fiber).

Port State: View-only field that shows traffic is Disabled or Forwarding.

Link State: View-only field that shows the link is up or down.

A/N: View-only field that shows Auto-negotiation is on or off.

Speed: View-only field that shows the port speed.

Duplex: View-only field that shows the duplex mode is half or full.

Flow Control: View-only field that shows the flow control is on or off.

SFP Status

Media Type	FX
Speed	--
Distance	--
Vendor Name	--
Vendor PN	--
Vendor SN	--
Temperature (C)	-----
Voltage (V)	-----
Tx Bias (mA)	-----
Tx Power (dbm)	-----
Rx Power (dbm)	-----

Media Type: Show the type of FX (fiber).

Speed: Data rate of the slide-in SFP Transceiver.

Distance: Transmission distance of the slide-in SFP Transceiver.

Vendor Name: Vendor name of the slide-in SFP Transceiver.

Vendor PN: Vendor PN of the slide-in SFP Transceiver.

Vendor SN: Vendor SN of the slide-in SFP Transceiver.

Temperature (C): The slide-in SFP module operation temperature.

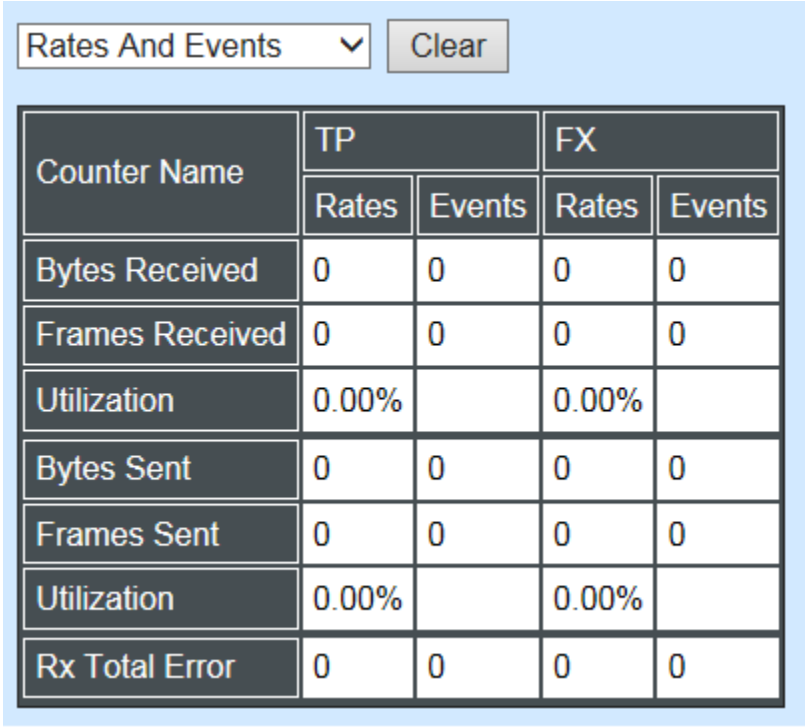
Voltage (V): The slide-in SFP module operation voltage.

TX Bias (mA): The slide-in SFP module operation current.

TX Power (dbm): The slide-in SFP module optical Transmission power.

RX Power (dbm): The slide-in SFP module optical Receiver power.

Select **"Rates and Events"** option from the Counters Display pull-down menu to view the detailed traffic statistics (counters' information).



Counter Name	TP		FX	
	Rates	Events	Rates	Events
Bytes Received	0	0	0	0
Frames Received	0	0	0	0
Utilization	0.00%		0.00%	
Bytes Sent	0	0	0	0
Frames Sent	0	0	0	0
Utilization	0.00%		0.00%	
Rx Total Error	0	0	0	0

Rates: Counters displayed and updated once per second.

Events: The count is cumulative (i.e. cumulated count).

Bytes Received: The total number of bytes received from this port.

Frames Received: The total number of frames received from this port.

Utilization: The utilization of receiving bandwidth from this port.

Bytes Sent: The total number of bytes sent from this port.

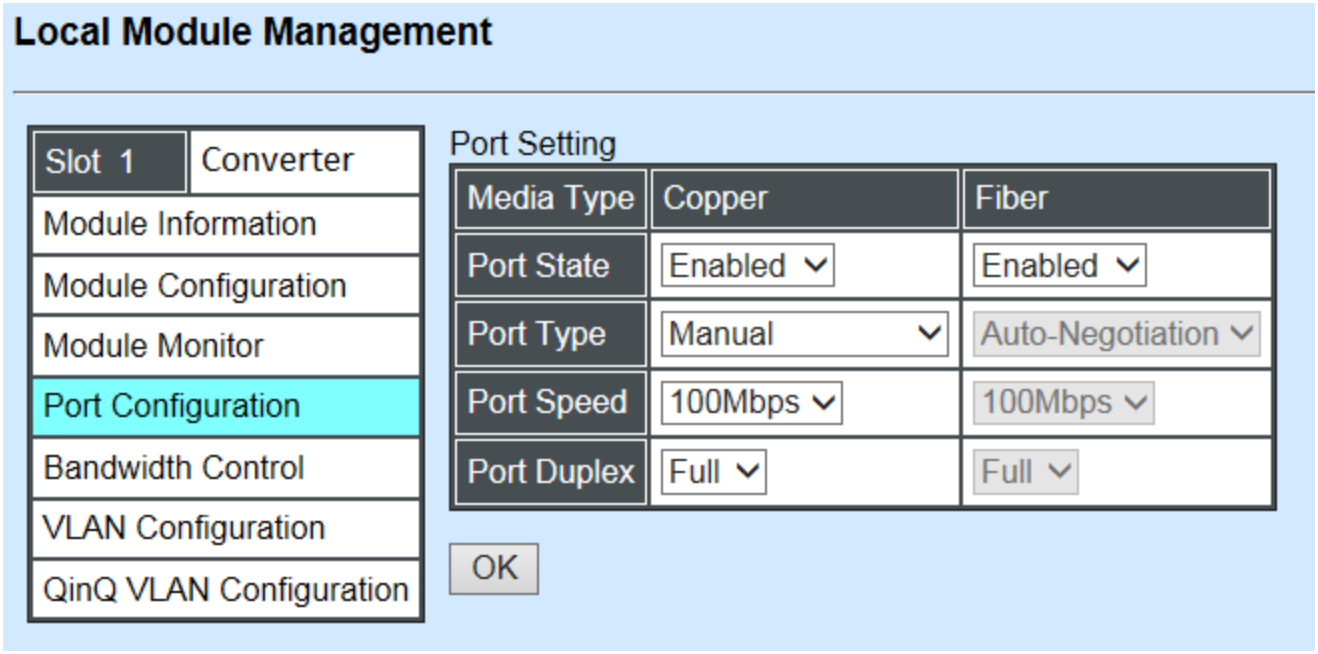
Frames Sent: The total number of frames sent from this port.

Utilization: The utilization of sending bandwidth from this port.

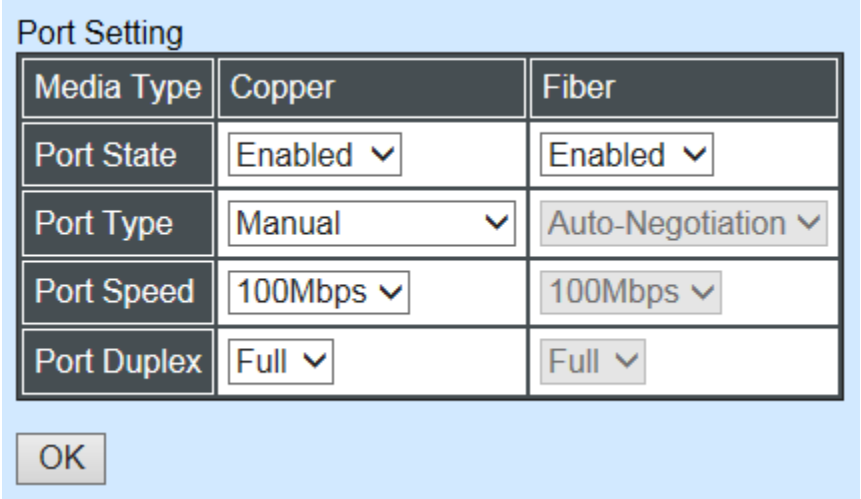
RX Total Errors: The total number of errors frames from this port.

E.2.1.4 Port Configuration

Select the option **Port Configuration** from the **Local Module Management** menu, then the **Port Configuration** fields show up on the right to let you configure them accordingly.



Port Setting



Media Type: Select between Copper (UTP, RJ-45) and Fiber

Port State: Enable or disable port state.

Port Type: Show the port type configuration is manual or auto-negotiation.

Port Speed: Show the port speed of the selected media type.

Port Duplex: Show the duplex mode is half or full.

Click "**OK**" to apply.

DIP Setting
You are allowed to view the DIP switch configuration via WEB UI.

DIP Setting

Media Type	Copper	Fiber
Port Type	Auto-Negotiation	Auto-Negotiation
Port Speed	100Mbps	100Mbps
Link Alarm	Enabled	

Currently controlled by device hardware dip switch.
Please consider to change device dip switch setting as software control.

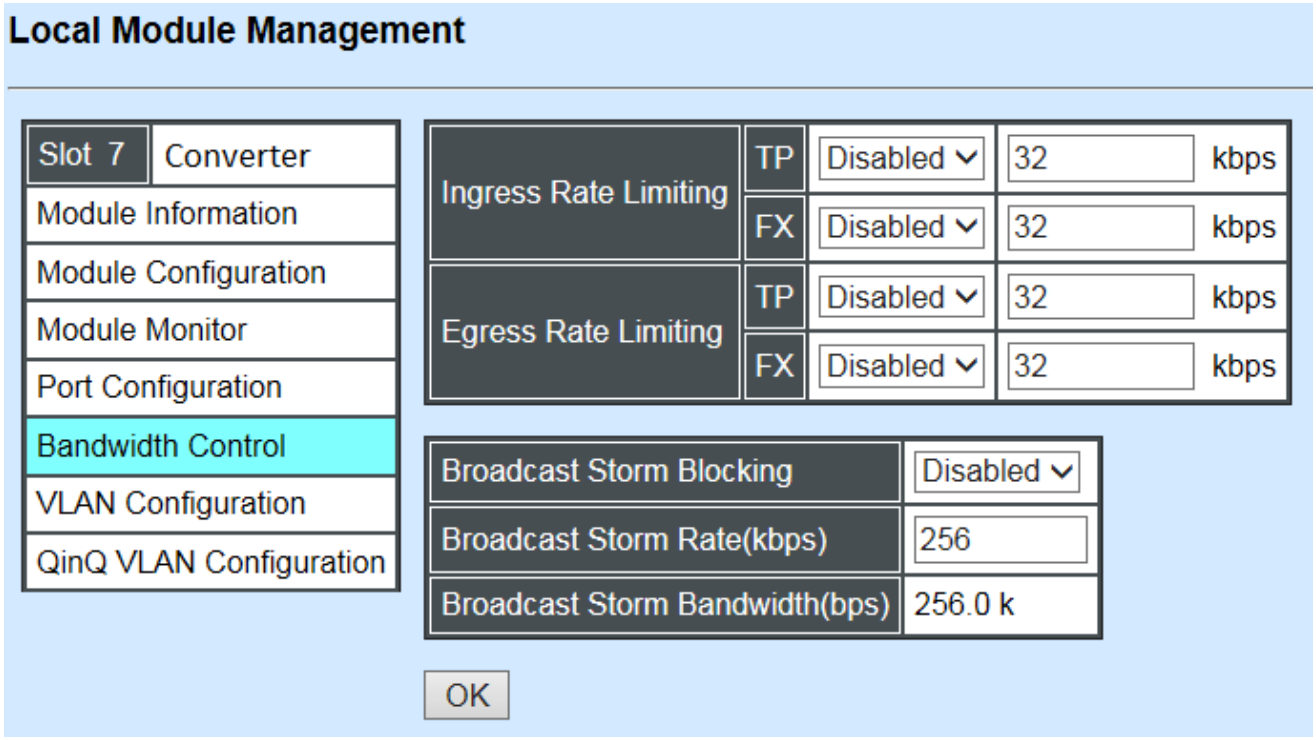
Port Type: View-only field that shows the port type configuration is manual or auto-negotiation.

Port Speed: View-only field that shows the port speed of the selected media type.

Link Alarm: View-only field that shows the link alarm is enabled or disabled.

E.2.1.5 Bandwidth Control

Select the option **Bandwidth Control** from the **Local Module Management** menu, then the **Bandwidth Control's** Ingress/Egress Rate Limit and Broadcast Storm fields show up on the right to let you enable/disable TP/FX, specify the rate in kbps, enable/disable broadcast Storm settings and specify the rate in kbps in broadcast storm blocking.



Ingress Rate Limiting: Enable or disable TP ingress rate limiting in kbps and set up current configured ingress bandwidth in kbps. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

Egress Rate Limiting: Enable or disable TP egress rate limiting in kbps and set up current configured egress bandwidth in kbps. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

Broadcast Storm Blocking: Enable or disable broadcast storm blocking function.

Broadcast Storm Rate(kbps): Set up storm rate value. Packets exceeding the value will be dropped. (The rate range can be configured within 32~1000000kbps for Gigabit Ethernet media converter; as for Fast Ethernet media converter, it can be configured within 32~100000kbps only.)

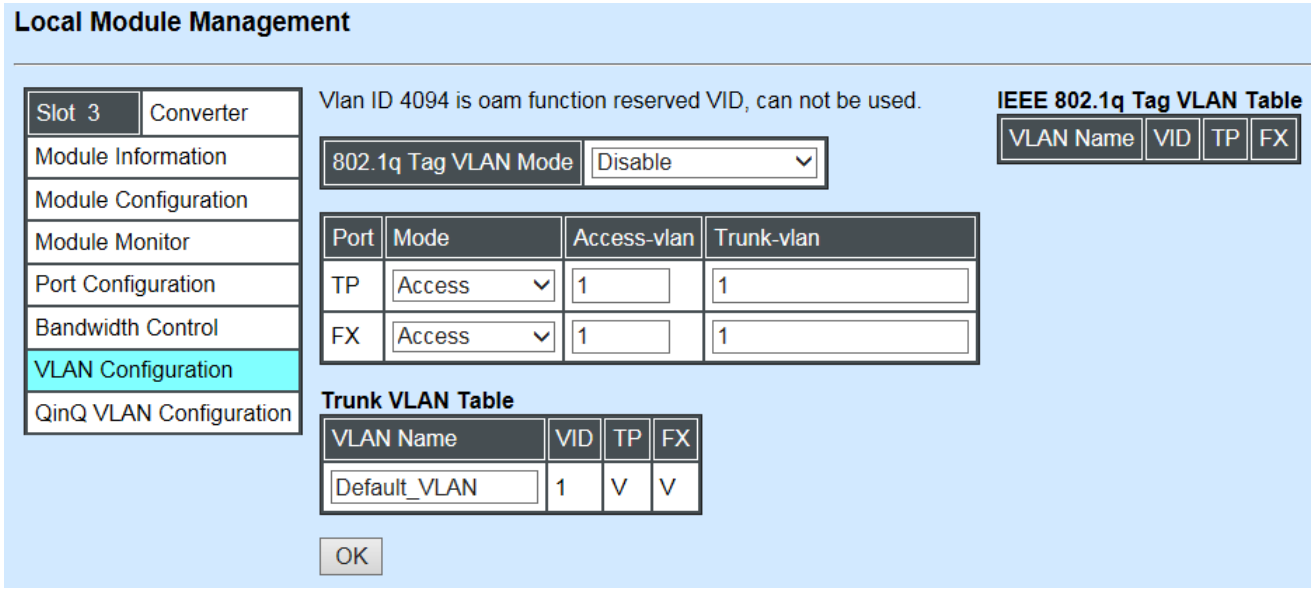
Broadcast Storm Rate Bandwidth(bps): Display the current configured storm rate bandwidth.

E.2.1.6 VLAN Configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the CHASSIS on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

Select the option **VLAN Configuration** from the **Local Module Management** menu, then the **VLAN Configuration's** Default VLAN Mode and Table fields show up on the right to let you specify the TP/FX of VLAN settings.



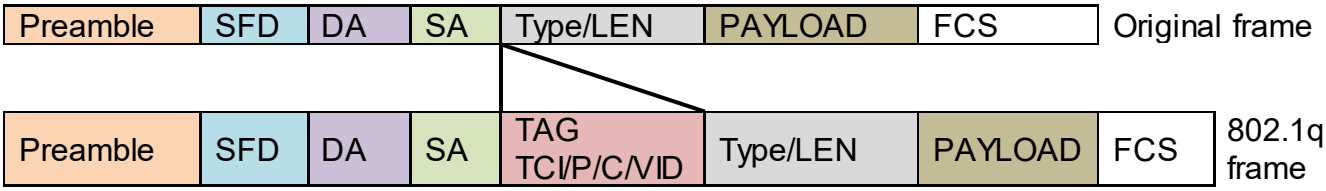
The Managed Media Converter supports **IEEE 802.1q Tag VLAN**.

IEEE 802.1Q VLAN Concepts

Port-Based VLAN is simple to implement and use, but it cannot be deployed cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution to this problem. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large switched networks into smaller segments so that

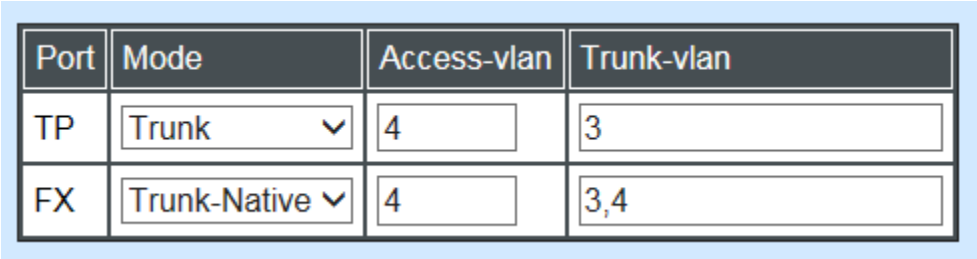
broadcast and multicast traffic will not occupy too much available bandwidth as well as provide a higher level security between segments of internal networks.

Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to	8100 for 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format – Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes		User data	
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

IEEE 802.1q Tag VLAN Mode: Enable or disable IEEE 802.1q Tag VLAN mode, or select Bypass Ctag Mode which ignore C-tag checking.



Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When

the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

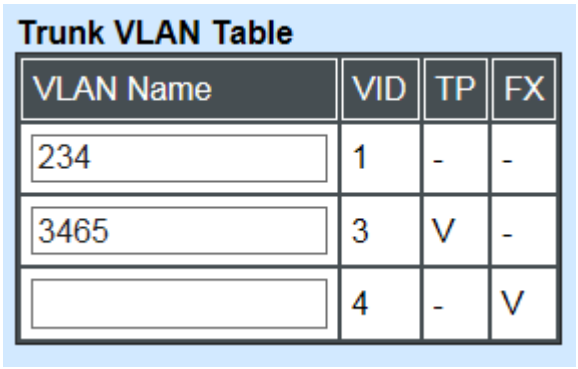
A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN. All **network hosts (such as PCs)** connect to the Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal device. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between devices. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple devices.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.



Trunk VLAN table: To edit 802.1Q Tag VLAN Name.

VLAN Name: User-specified field to give VLAN a name.

VID: The VLAN ID (**VID**) specifies the set of VLAN that a given port is allowed to receive and send **labeled** packets.

TP: It shows whether the TP port that is included in a given VID.

FX: It shows whether the Fiber port that is included in a given VID.

Click “OK” to apply.

IEEE 802.1q Tag VLAN Table

VLAN Name	VID	TP	FX
234	1	V	V

IEEE 802.1q Tag VLAN Table: It shows the status of IEEE 802.1q Tag VLAN.

VLAN Name: View-only filed that shows the VLAN name.

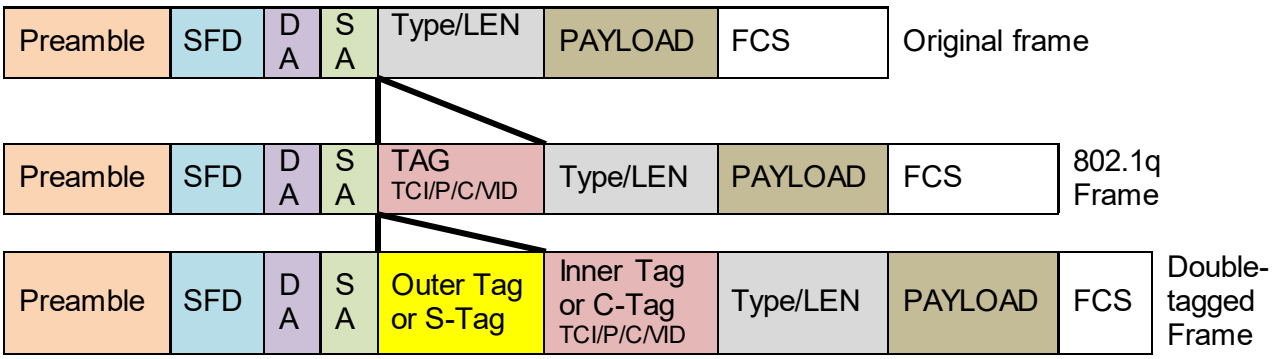
VID: View-only filed that shows the VID.

TP: View-only filed that shows whether the TP port that is included in a given VID.

FX: View-only filed that shows whether the fiber port that is included in a given VID.

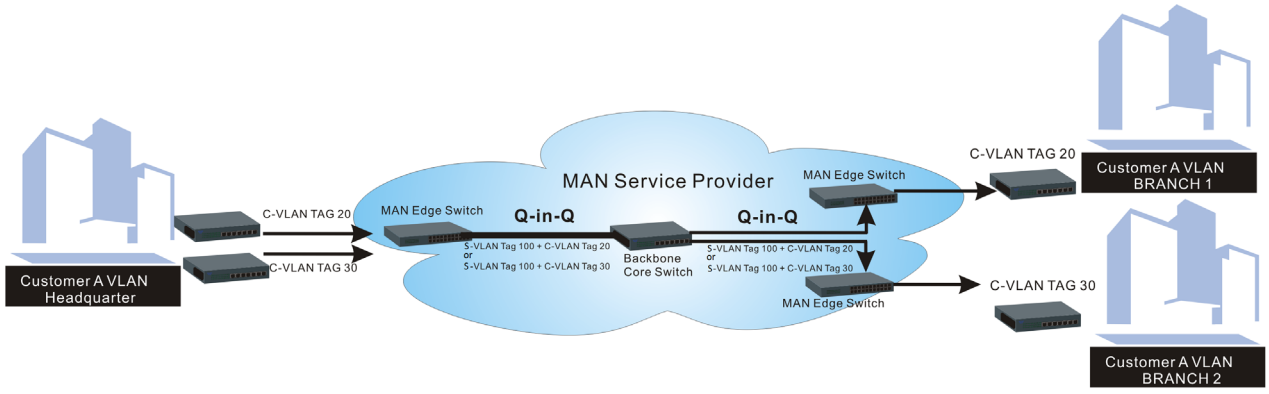
E.2.1.7 Q-in-Q VLAN Configuration

The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a “double-tagged” frame is created so as to separate customer traffic within a service provider network. As shown below in “Double-Tagged Frame” illustration, an outer tag is added between source destination and inner tag at the provider network’s edge. This can support C-VLAN (Customer VLAN) over Metro Area Networks and ensure complete separation between traffic from different user groups. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single S-VLAN (Service VLAN) tag per customer over the Metro Ethernet network.



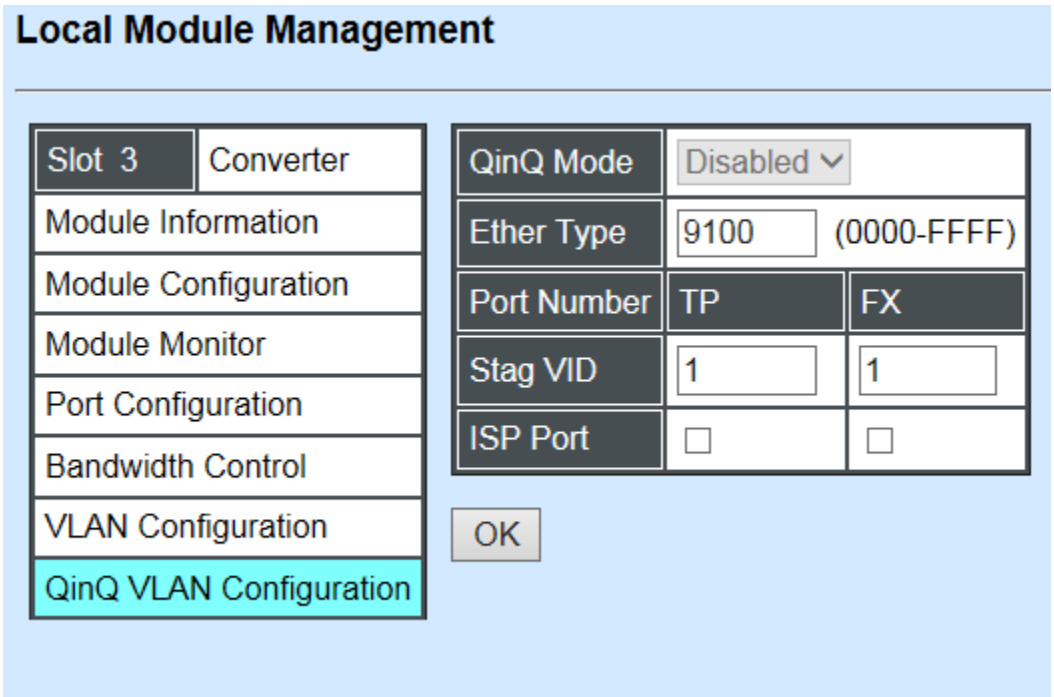
Double-Tagged Frame

As shown below in “Q-in-Q Example” illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider’s backbone, there is a possibility that traffic might be forwarded insecurely, for example due to the same VLAN ID used. Therefore, in order to get the information from Headquarter to Branch 1, the easiest way for the carrier to ensure security to customers is to encapsulate the original VLAN with a second VLAN ID of 100. This second VLAN ID is known as S-VLAN (Service VLAN) that is added as data enters the service provider’s network and then removed as data exits. Eventually, with the help of S-Tag, the information sent from Headquarter to Branch 1 can be delivered with customers’ VLANs intactly and securely.



Q-in-Q Example

This section allows you to set up Q-in-Q VLAN. Select the option **QinQ VLAN Configuration** from the **Local Module Management** menu, the **Q-in-Q VLAN** fields show up on the right.



QinQ Mode: Enable or disable the function by clicking drop-down box.

Ether Type: A two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame. Specify the Ether type for the service tag (S-tag).

Port Number: Two kinds of ports are available, TP port or Fiber port.

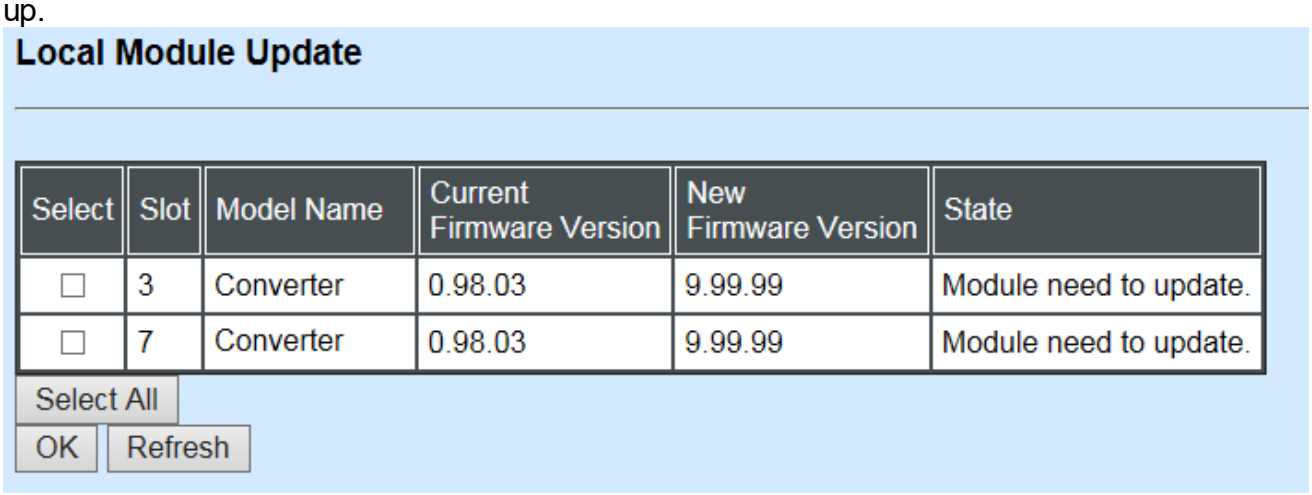
Stag(Service Tag) VID: Specify a VID for the service tag (Outer Tag).

ISP(Internet Service Provider) Port: This is to determine whether the port receives and forwards double-tagged packet. Check the port and it receives and forwards double-tagged packet only.

Click the **"OK"** button to apply the settings.

E.2.2 Local Module Update

Select **Local Module Update** from the **Main Menu**, then the following screen page shows up.



Select: Check the box to upgrade the firmware on specified converters or click **Select All** button to upgrade the firmware on all converters.

Slot: Show which slot the converter is inserted into.

Model Name: Show the current model name of the converter.

Current Firmware Version: Show the current firmware version used for each converter.

New Firmware Version: The upcoming firmware version to be installed.

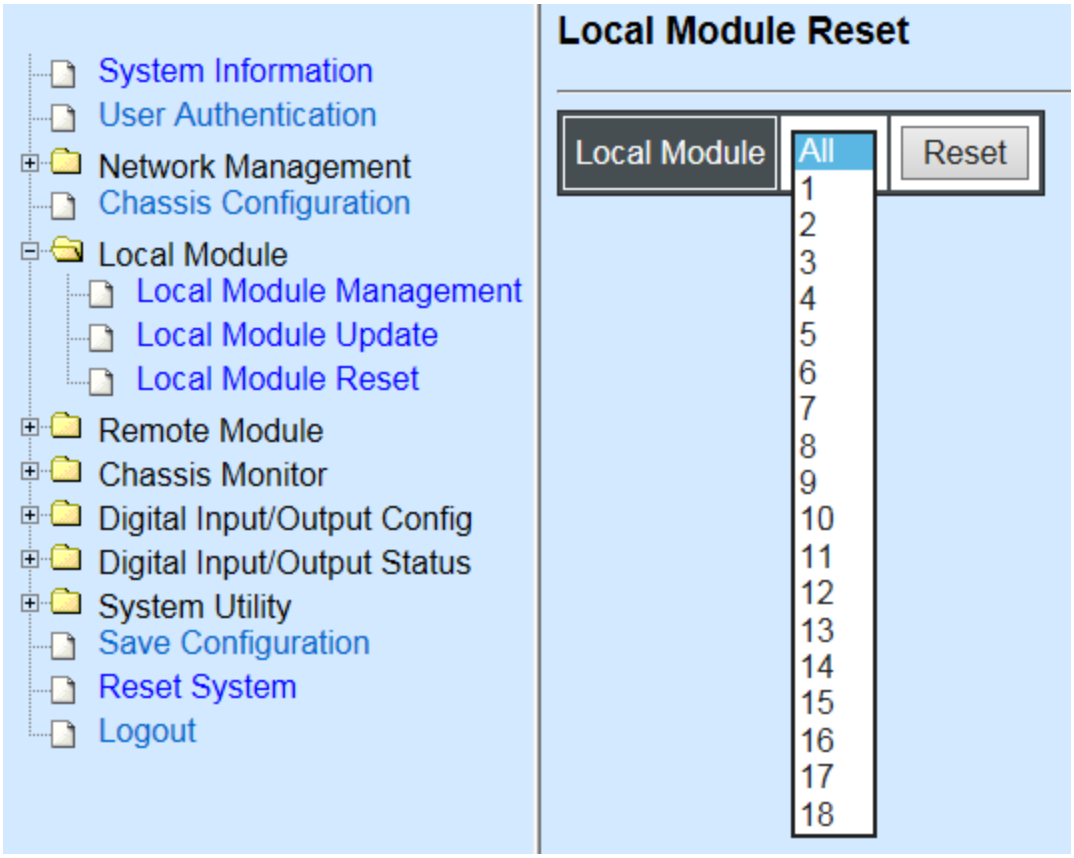
State: Show the current status of firmware upgrade.

Click **"OK"** to start module update procedure.

Click **"Refresh"** to renew all update module information.

E.2.3 Local Module Reset

Select **Local Module Reset** from the **Main Menu**, then the following screen page shows up.



Local Module: Select **"All"** to reset all modules or select the individual module. When you decide which module to be reset, click **Reset** button to begin the reset process.

APPENDIX F: MCT-5002FSMSFP+ Converter

This section is used to introduce 10G Base-R to SFP standalone MCT-5002FSMSFP+ Media Converter which is specifically designed to fulfill emerging deployment needs of fiber Ethernet networks.

F.1 CLI Command

This is to how the converter is presented via CLI Command.

F.1.1 Local Module Configuration

This section is intended to introduce the configuration of specified media converters.

Note: *Make sure that media converts are firmly installed and powered on.*

1. Specify any slots to configure

Slot command	Parameter	Description
MCT-RACK(config)# slot [slot_list]	[slot_list]	Specify any slots you want to configure.

2. Upgrade media converter firmware.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# firmware upgrade		Upgrade the firmware. **Note:** Upgrade one media converter at a time.

3. Configure signal loss alarm

MCT-5002FSMSFP+ will simultaneously stop the optical signal transmission at both sides when the signal loss occurs at one side. The fiber port links will be down to alert the user even the output of optical power exists.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module signal-loss-alarm		Enable signal loss alarm.
No Command		
MCT-RACK(config-slot-slot-slot)# no module link-alarm		Disable signal loss alarm.

Show Command	
MCT-RACK(config-slot-slot-slot)# show module	Show the status of signal loss alarm.

4. Configure loopback mode

When the fiber loopback mode is enabled, the MCT-5002FSMSFP+ will loopback the received packets (The packets are generated from the testing packets generator) to ensure the circuit quality.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module loopback-mode		Enable loopback mode.
No Command		
MCT-RACK(config-slot-slot-slot)# no module link-alarm		Disable loopback mode.
Show Command		
MCT-RACK(config-slot-slot-slot)# show module		Show the status of loopback mode.

5. Set up module description

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module-info description [description]	[description]	Specify user-defined information. Up to 55 characters are available.
No Command		
MCT-RACK(config-slot-slot-slot)# no module-info description		Delete user-defined information.
Show Command		
MCT-RACK(config-slot-slot-slot)# show module-info		Show the module information.
Module Description Example		
MCT-RACK(config-slot-slot-slot)# module-info description 123		The description of the converter is named “123”.

6. Reset converter

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# reload		Reboot the media converters.

F.1.2 Local Module Port Configuration

This is to configure port via “interface” command.

This command is to configure fiber ports on a converter.

1. Specify any interface to configure

Interface command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# interface [port_list]	[port_list]	Specify any ports you want to configure. There are two ports available. Port “1” represents FX1 port while port “2” FX2 port.

2. Shutdown interface

Interface Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# shutdown		Administratively disable the selected ports’ status.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no shutdown		Administratively enable the selected ports’ status.

3. Speed configuration

Command	Parameter	Description
MCT-RACK(config-slot-slot-slot-if-port-port)# speed [force_10g | 1000]	[force_10g | 1000]	Set up the selected interfaces’ speed. Manual speed configuration only works when “no auto-negotiation” command is issued.
No command		
MCT-RACK(config-slot-slot-slot-if-port-port)# no speed		Set the selected ports’ speed to the default setting.

4. Configure loopback mode

When the loopback mode is enabled to the specified fiber port, it will loopback the received packets from the specified fiber port (The packets are generated from the testing packets generator) to ensure the circuit quality.

Slot command	Parameter	Description
MCT-RACK(config-slot-slot-slot)# module loopback-mode interface [port_list]	[port_list]	Enable loopback mode to the specified interface.

No Command	
MCT-RACK(config-slot-slot-slot)# no module link-alarm	Disable loopback mode to the specified interface.
Show Command	
MCT-RACK(config-slot-slot-slot)# show module	Show the status of loopback mode.

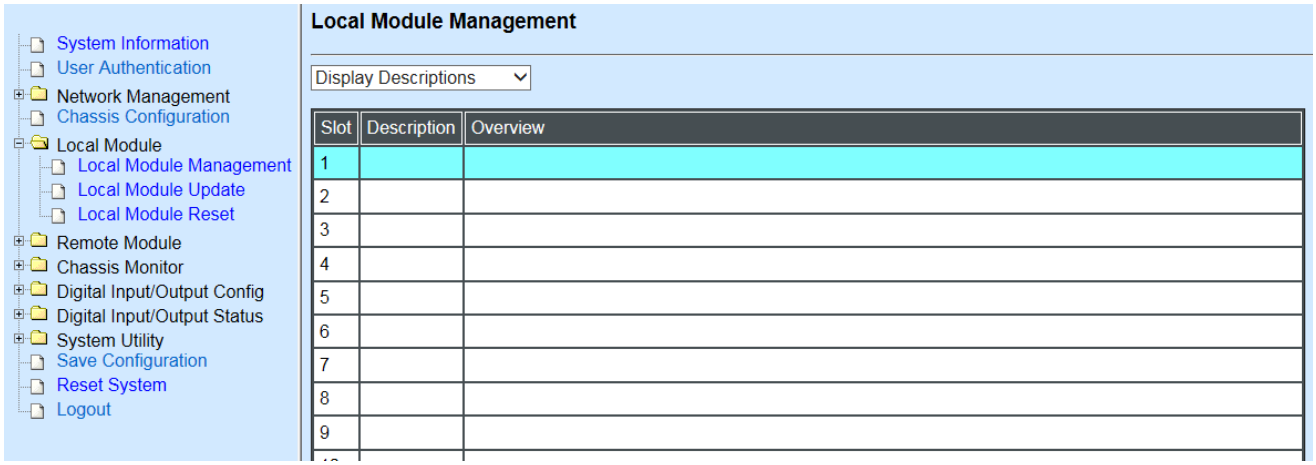
F.2 Web Management

This is to how the MCT-5002FSMSFP+ Media Converter is presented via Chassis on Web UI.

F.2.1 Local Module Management

In order to manage the installed converters and set up required functions, select the option **Local Module Management** from **Main Menu**, and then **Local Module Management** screen page shows up.

Note: The slot configuration will return to the default if we replace Gigabit media converter with Fast media converter.



Overview: Show the product information of each slide-in converter.

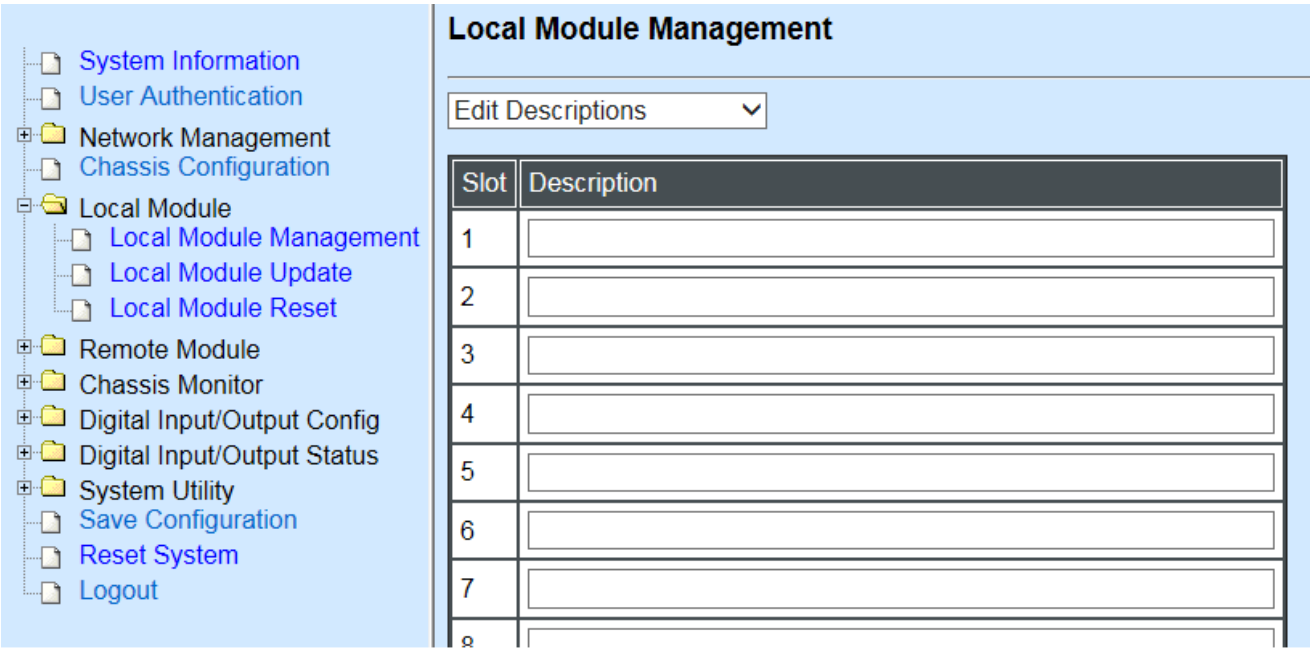
Description: Show the user-specified message of each slide-in converter.

The drop-down box is to modify or show the message you specify. There are three options:

Not Display Descriptions: Hide the user-specified message in the Description field of each slide-in converter.

Display Descriptions: Show the product information and the user-specified message of each slide-in converter both in the fields of Description and Overview.

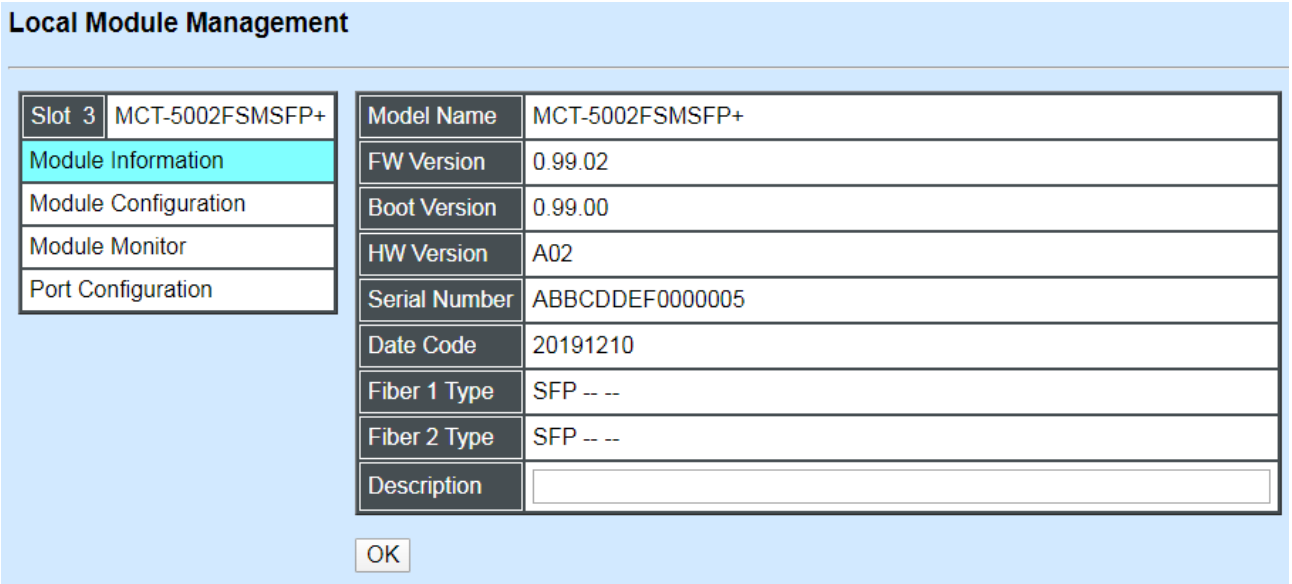
Edit Descriptions: Change the user-specified message of each slide-in converter separately.



To modify the description, click drop-down box and select **Edit Descriptions**.

Click **"OK"** to save edited message.

Click on the available modules for MCT-5002FSMSFP+ converter and then the following screen page appears.



Module Information: Display the model name, version of FW/Boot/HW, serial number, date code, fiber type, and description.

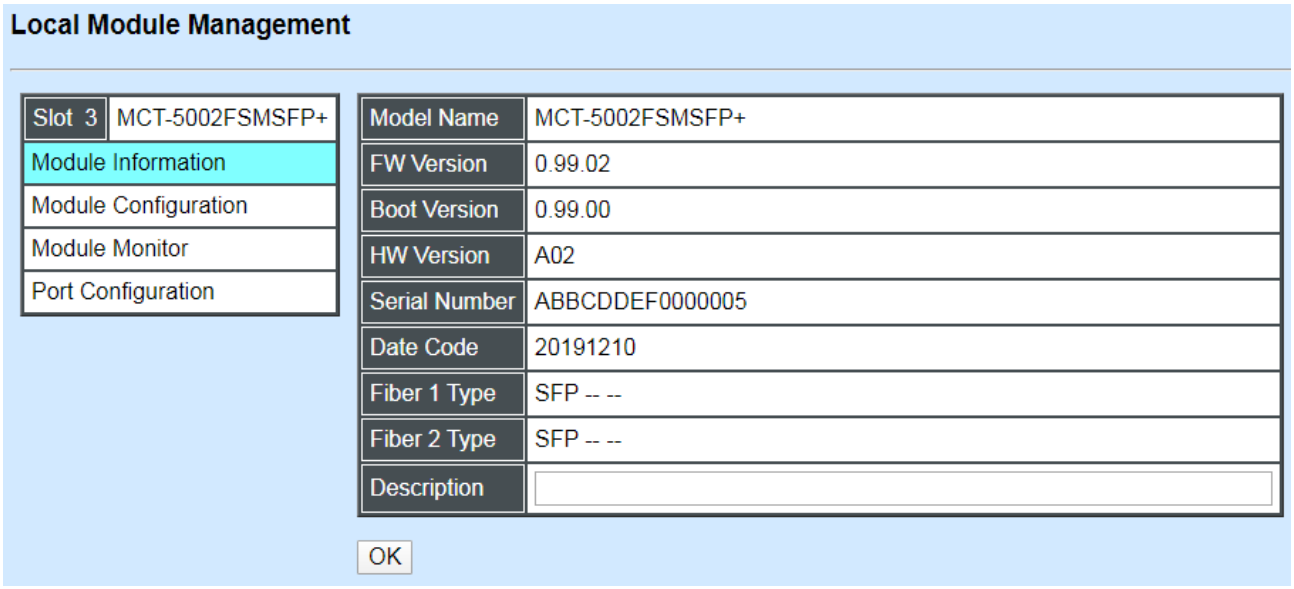
Module Configuration: Set up Signal Loss Alarm function and LoopBack Mode.

Module Monitor: Display information about Media Type, Port State, Link Status, Speed, and LoopBack.

Port Configuration: Set up the port state, and the port speed.

F.2.1.1 Module Information

Select the option **Module Information** from the **Local Module Management** menu, and then the **Module Information** fields show up on the right to provide you information about the module.



Model Name: View-only field that shows the product's model name.

FW Version: View-only field that shows the product's firmware version.

Boot Version: View-only field that shows the product's boot loader version.

HW Version: View-only field that shows the product's hardware version.

Serial Number: View-only field that shows the product's serial number.

Date Code: View-only field that shows the date of EEPROM burned.

Fiber 1/2 Type: View-only field that shows the product's fiber connector type, speed, and distance.

Description: Specify the appropriate brief description for the slide-in converter module.

F.2.1.2 Module Configuration

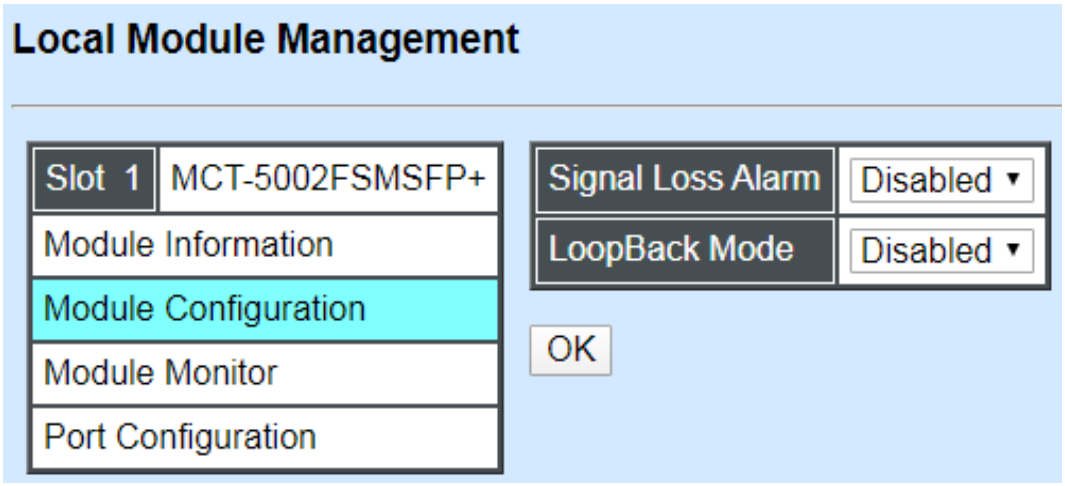
Select the option **Module Configuration** from the **Local Module Management** menu, then **Module Configuration** fields show up on the right to let you view the configuration of the converter.

Signal Loss Alarm: This function is used under the circumstance when the signal loss occurs at one side, MCT-5002FSMSFP+ will simultaneously stop the optical signal transmission at both sides to allow users to easily identify and diagnose the linking status.

Click the drop-down box to enable or disable Signal Loss Alarm of the converter.

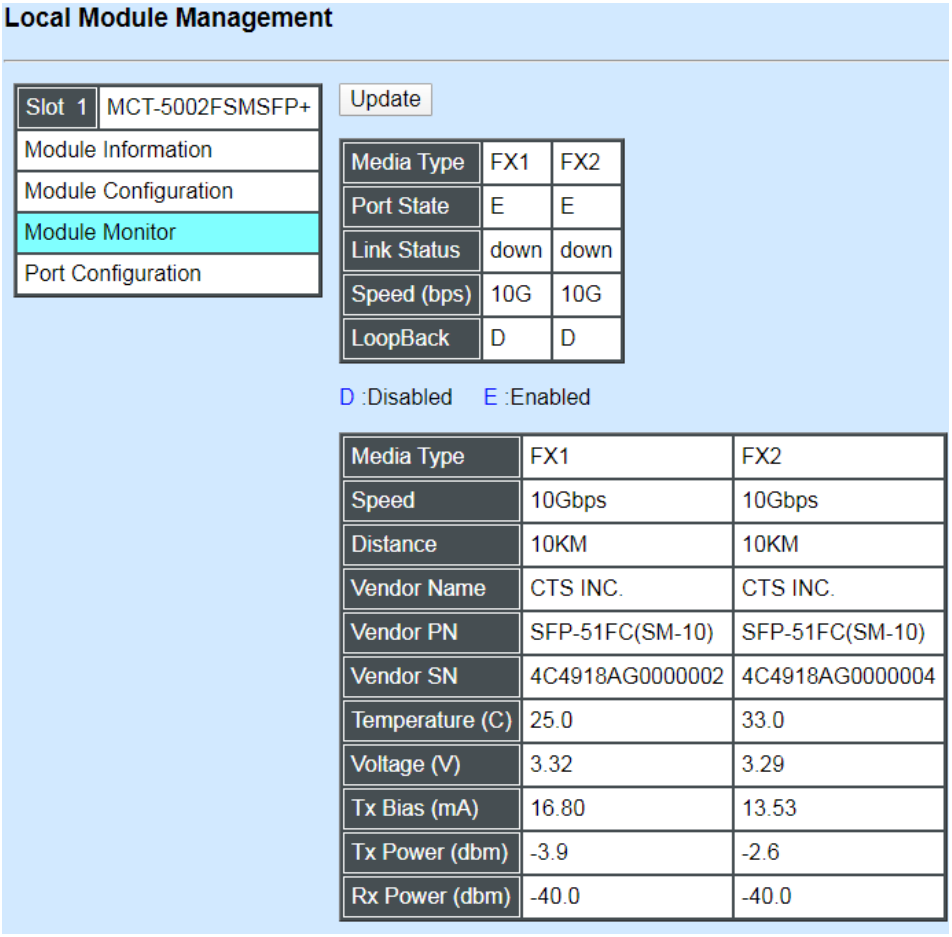
LoopBack Mode: This function is used under the circumstance when the media converter will loopback the received packets (The packets are generated from the testing packets generator) to ensure the circuit quality.

Click the drop-down box to enable or disable LoopBack Mode of the converter.



F.2.1.3 Module Monitor

Select the option **Module Monitor** from the **Local Module Management** menu, then **Module Monitor** fields show up on the right to let you view the configuration of the module.



Local Module Management

Slot 1	MCT-5002FSMSFP+
Module Information	
Module Configuration	
Module Monitor	
Port Configuration	

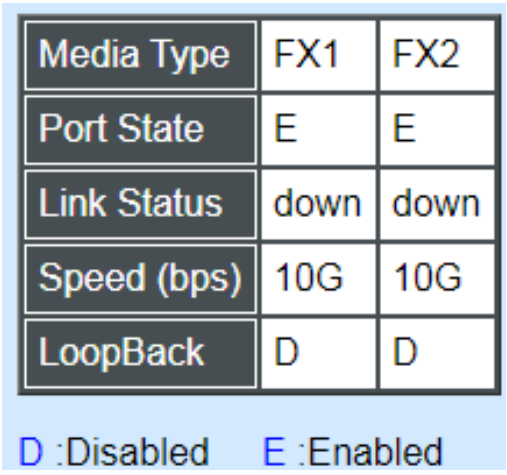
Update

Media Type	FX1	FX2
Port State	E	E
Link Status	down	down
Speed (bps)	10G	10G
LoopBack	D	D

D :Disabled E :Enabled

Media Type	FX1	FX2
Speed	10Gbps	10Gbps
Distance	10KM	10KM
Vendor Name	CTS INC.	CTS INC.
Vendor PN	SFP-51FC(SM-10)	SFP-51FC(SM-10)
Vendor SN	4C4918AG0000002	4C4918AG0000004
Temperature (C)	25.0	33.0
Voltage (V)	3.32	3.29
Tx Bias (mA)	16.80	13.53
Tx Power (dbm)	-3.9	-2.6
Rx Power (dbm)	-40.0	-40.0

Port Status



Media Type	FX1	FX2
Port State	E	E
Link Status	down	down
Speed (bps)	10G	10G
LoopBack	D	D

D :Disabled E :Enabled

Media Type: FX1 and FX2 (fibers).

Port State: View-only field that shows traffic is Disabled or Forwarding.

Link State: View-only field that shows the link is up or down.

Speed: View-only field that shows the port speed.

LoopBack: View-only field that shows the loopback mode is on or off.

SFP Status

Media Type	FX1	FX2
Speed	10Gbps	10Gbps
Distance	10KM	10KM
Vendor Name	CTS INC.	CTS INC.
Vendor PN	SFP-51FC(SM-10)	SFP-51FC(SM-10)
Vendor SN	4C4918AG0000002	4C4918AG0000004
Temperature (C)	25.0	33.0
Voltage (V)	3.32	3.29
Tx Bias (mA)	16.80	13.53
Tx Power (dbm)	-3.9	-2.6
Rx Power (dbm)	-40.0	-40.0

Media Type: Show the type of FX (fiber).

Speed: Data rate of the slide-in SFP Transceiver.

Distance: Transmission distance of the slide-in SFP Transceiver.

Vendor Name: Vendor name of the slide-in SFP Transceiver.

Vendor PN: Vendor PN of the slide-in SFP Transceiver.

Vendor SN: Vendor SN of the slide-in SFP Transceiver.

Temperature (C): The slide-in SFP module operation temperature.

Voltage (V): The slide-in SFP module operation voltage.

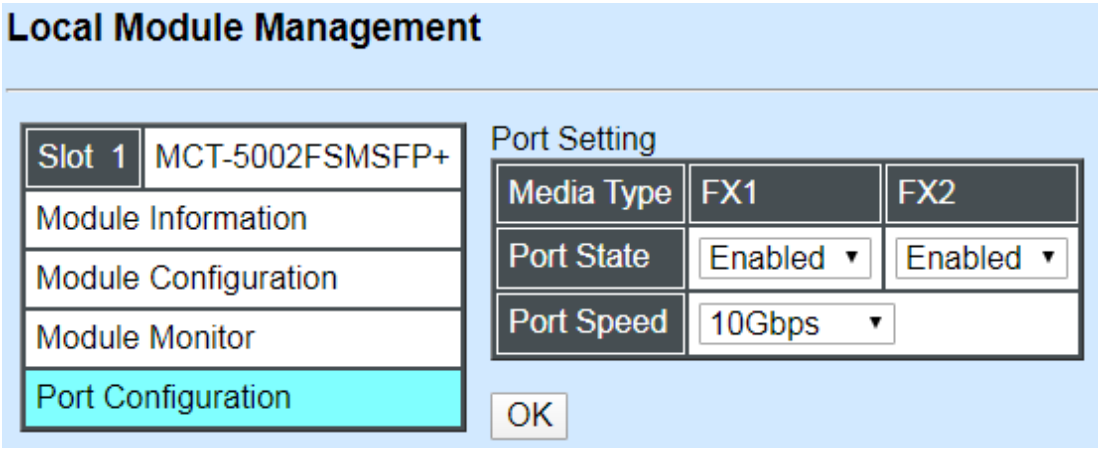
TX Bias (mA): The Slide-in SFP module operation current.

TX Power (dbm): The Slide-in SFP module optical Transmission power.

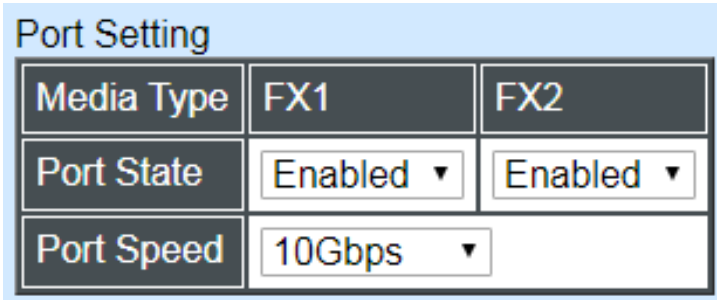
RX Power (dbm): The Slide-in SFP module optical Receiver power.

F.2.1.4 Port Configuration

Select the option **Port Configuration** from the **Local Module Management** menu, then the **Port Configuration** fields show up on the right to let you configure them accordingly.



Port Setting



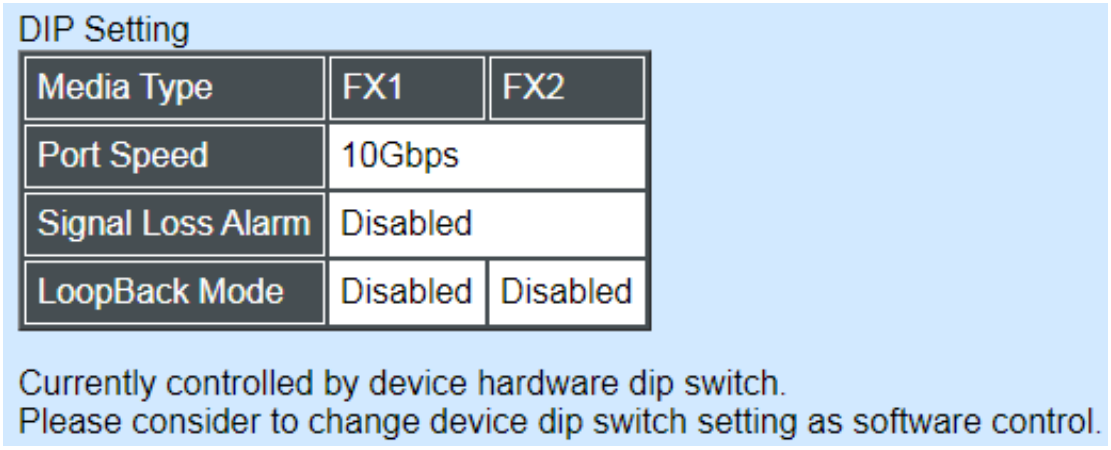
Media Type: Select between FX1 or FX2(fiber)

Port State: Enable or disable port state.

Port Speed: Show the port speed of the selected media type.

Click **"OK"** to apply.

DIP Setting
You are allowed to view the DIP switch configuration via WEB UI.



Media Type: View-only field that shows the selected media type configuration.

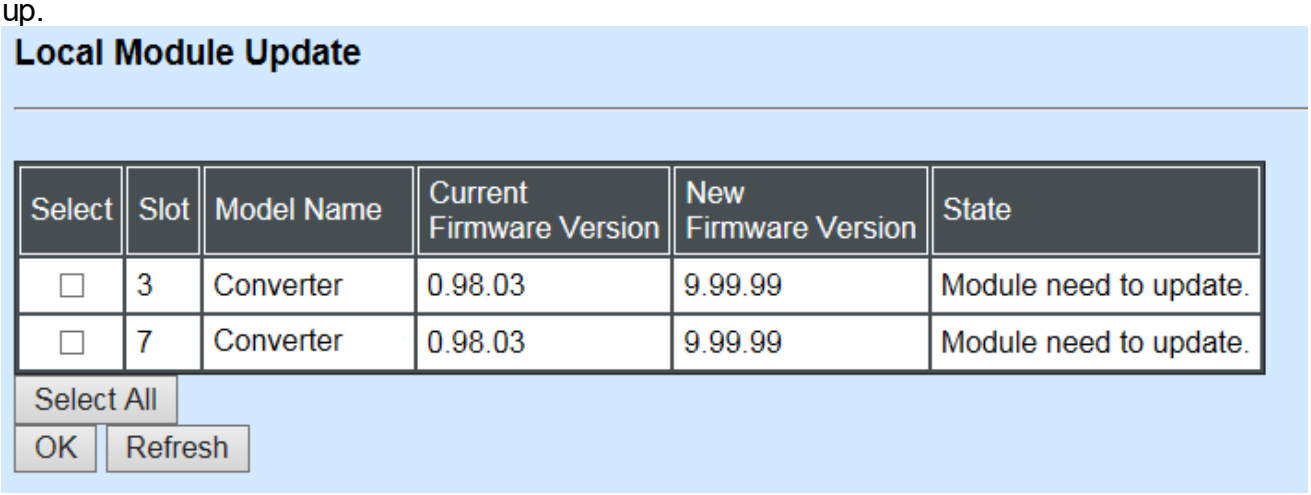
Port Speed: View-only field that shows the port speed.

Signal Link Alarm: View-only field that shows the signal link alarm is enabled or disabled.

LoopBack Mode: View-only field that shows the loopback mode is enabled or disabled of the selected media type.

F.2.2 Local Module Update

Select **Local Module Update** from the **Main Menu**, then the following screen page shows up.



Select: Check the box to upgrade the firmware on specified converter(s) or click **Select All** button to upgrade the firmware on all converters.

Slot: Show which slot the converter is inserted into.

Model Name: Show the current model name of the converter.

Current Firmware Version: Show the current firmware version used for each converter.

New Firmware Version: The upcoming firmware version to be installed.

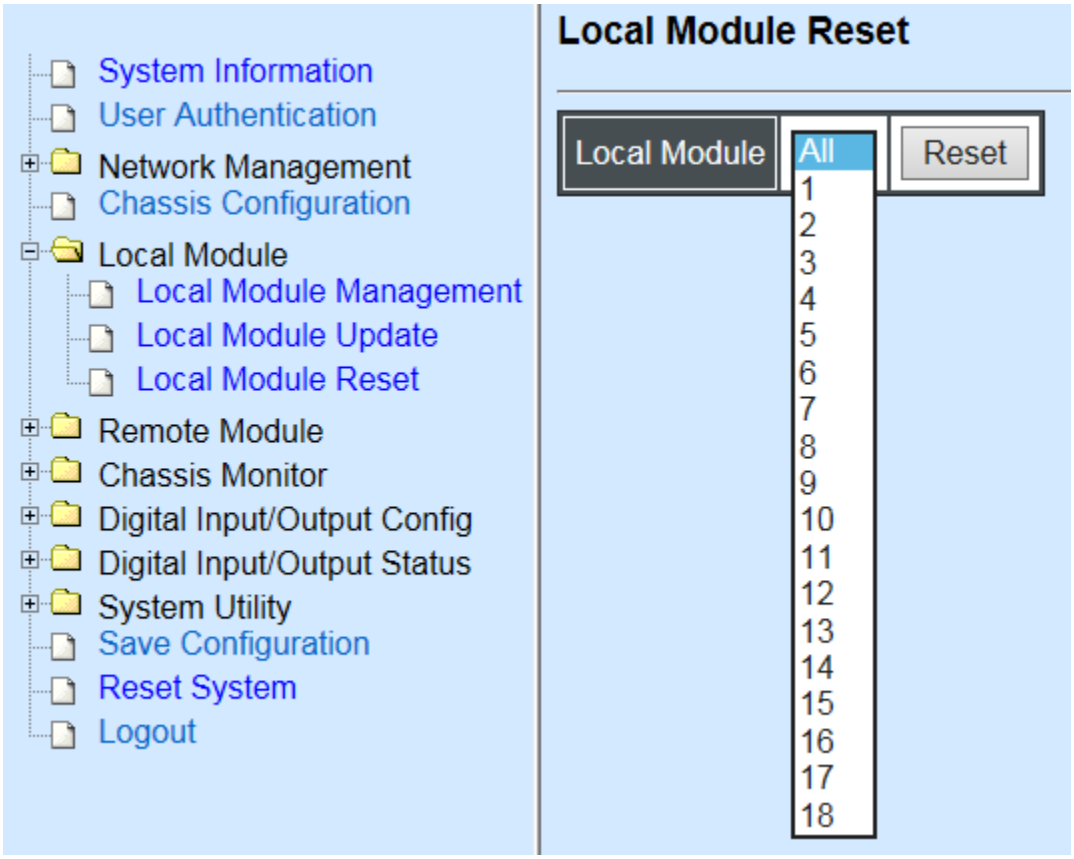
State: Shows the current status of firmware upgrade.

Click **"OK"** to start module update procedure.

Click **"Refresh"** to renew all update module information.

F.2.3 Local Module Reset

Select **Local Module Reset** from the **Main Menu**, then the following screen page shows up.



Local Module: Select **"All"** to reset all modules or select the individual module. When you decide which module to be reset, then click **Reset** button to begin the reset process.