

CVT-2512 Series

10/100Base-TX to 100Base-FX OAM Management Converter

CVT-3512 Series

10/100/1000Base-TX to 1000Base-FX OAM Management Converter

Network Management

User's Manual

Version 0.91

Trademarks

CTS is a registered trademark of Connection Technology Systems Inc.

Contents subject to revise without prior notice.

All other trademarks remain the property of their respective owners.

Copyright Statement

Copyright © 2009 Connection Technology Systems Inc., All Rights Reserved.

This publication may not be reproduced as a whole or in part, in any way whatsoever unless prior consent has been obtained from Connection Technology Systems Inc..

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 the equipment is not installed and used in accordance with the instructions, it 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 a different outlet from that 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.

Copyright © 2009 All Rights Reserved.

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.

Revision History

Manual Version	Modification	Firmware Version	Date
0.91	The initial version	1.03.10	2009/10

Note: *This User's Manual is written or revised according to the officially-released Firmware version. The content of this Manual is subject to change without prior notice.*

Table of Contents

1. INTRODUCTION	5
1.1 Connecting the OAM Management Converter	5
2. SNMP NETWORK MANAGEMENT	7
3. WEB MANAGEMENT	8
3.1 System Information	9
3.2 Network Information	10
3.3 Module Setting	12
3.3.1 Network Configuration	12
3.3.2 Password Setting.....	13
3.3.3 Port Configuration.....	14
3.3.4 Traffic Statistics.....	15
3.3.5 SNMP Configuration	16
3.3.6 VLAN Configuration.....	17
3.3.6.1 VLAN Group.....	20
3.3.6.2 VLAN Per Port Setting	21
3.3.7 Q-in-Q Configuration.....	22
3.3.8 VLAN & Q-in-Q Example	23
3.3.9 TS 1000 Loopback Test	25
3.3.10 802.3ah Function	25
3.3.10.1 802.3ah Configuration.....	26
3.3.10.2 802.3ah Loopback.....	27
3.3.10.3 802.3ah Status	28
3.4 Tools	32
3.4.1 System Reboot	32
3.4.2 Save and Restore	33
3.4.3 Firmware Upgrade	33

1. INTRODUCTION

Thank you for purchasing the OAM Management Converter. The built-in management module allows users to configure this OAM Management Converter and monitor the operation status locally or remotely through the network.

1.1 Connecting the OAM Management Converter

It is very important that the proper cables with the correct pin arrangement are used when connecting the OAM Management Converter to other switches, hubs, workstations, etc.

1000Base-X / 100Base-FX SFP Port

The small form-factor pluggable (SFP) is a compact optical transceiver used in optical data communications applications. It interfaces with a network device mother board (for a switch, router or similar device) to a fiber optic or unshielded twisted pair networking cable. It is a popular industry format supported by several fiber optic component vendors.

SFP transceivers are available with a variety of different transmitter and receiver types, allowing users to select the appropriate transceiver for each link to provide the required optical reach over the available optical fiber type. SFP transceivers are also available with a "copper" cable interface, allowing a host device designed primarily for optical fiber communications to also communicate over unshielded twisted pair networking cable.

SFP slot for 3.3V mini GBIC module supports hot swappable SFP fiber transceiver. Before connecting other switches, workstation or media converter, make sure both sides of the SFP transfer are with the same media type, for example, 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX. In addition to that, check the fiber-optic cable type match the SFP transfer model. To connect to 1000Base-SX transceiver, use the multi-mode fiber cable that one side must be male duplex LC connector type. To connect to 1000Base-LX transfer, use the single-mode fiber cable that one side must be male duplex LC connector type.

10/100/1000Base-T RJ-45 Auto-MDI/MDIX Port

The 10/100/1000Base-T RJ-45 Auto-MDI/MDIX port is located in front panel of the OAM Management Converter. This RJ-45 port allows users to connect their traditional copper-based Ethernet/Fast Ethernet devices to the network and support auto-negotiation and MDI/MDIX auto-crossover. In other words, either crossover or straight through CAT-5E UTP or STP cable may be used.

IP Addresses

IP addresses have the format n.n.n.n, (The default factory setting is 192.168.0.1).

IP addresses are made up of two parts:

- The first part (for example 168.168.n.n) refers to network address that identifies the network in which the device resides. Network addresses are assigned by three

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

Remember that none of the two devices on a network can have the same address. If you connect to the outside, you must change all the arbitrary IP addresses to comply with those you have been allocated by the allocation organization. If you do not do this, your outside communications will not be performed.

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

Private MIB (Management Information Bases) is used to manage the OAM Management Converter through the SNMP-based network management system. You must install the private MIB into your SNMP-based network management system first.

The MIB file is shipped together with the OAM Management Converter. The file name extension is “.mib”, allowing SNMP-based compiler to read and compile.

2. 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 of the 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 devices can be switches, hub, etc.

MIB (Management Information Base) defines 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 variable. 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 provides 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 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 report asynchronously 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.

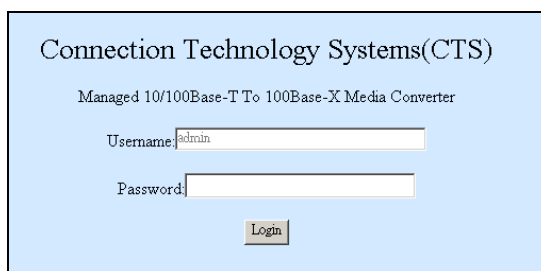
The system built-in management module also supports SNMP management. Users must install the MIB file before using the SNMP based network management system. The MIB file is on a disc or diskette that accompanies the system. The file name extension is “.mib”, allowing SNMP based compiler to read and compile. Please refer to the appropriate documentation for instructions on installing the system private MIB.

3. WEB MANAGEMENT

The OAM Management Converter can be managed via a Web browser. If you want to manage the OAM Management Converter remotely, follow these steps to access the built-in management module of this OAM Management Converter and set up the IP address:

1. When you use the OAM Management Converter for the first time or set the OAM Management Converter back to factory default setting, first connect one end of RJ-45 LAN cable to the RJ-45 port of the OAM Management Converter (as the temporary RJ-45 Management port) and the other end to your computer's RJ-45 port.
2. Then, make sure your computer is set to the same IP subnet address as the OAM Management Converter. For example, the default IP address of this OAM Management Converter is 192.168.0.1. Your computer's IP address must be set to 192.168.1.X (where X denotes a number between 1 and 254) and subset mask to 255.255.255.0.
3. Run a Web browser and then use the default IP address of the OAM Management Converter "**192.168.0.1**" to access the login window which is shown below.
4. Enter the username and password. The default login username is "**admin**" and **without a password**.
5. Select **Network Configuration** from **Module Setting** menu to set up your desired IP address to reach this OAM Management Converter.
6. Once the IP address of this OAM Management Converter is specified, you can access the OAM Management Converter with the new IP address.
7. When you use the specified IP address to access the OAM Management Converter, remember to connect the other end of RJ-45 cable to an Ethernet port and set your computer's IP address back to original settings.

A Login window looks like the one shown below:



Connection Technology Systems(CTS)

Managed 10/100Base-T To 100Base-X Media Converter

Username:

Password:

When you use the OAM Management Converter for the first time or set it back to the factory default settings, enter the login username "**admin**" and press Login. (By default, no password is required. Thus, leave the password field empty.) After a successful login, you will be directed to the Main Menu screen as shown below. Each menu function in the Web Management will be described in the following separate sections.

Note: The login username is set to “admin” permanently and can not be changed. However, the default login password can be changed to the desired one in **Password Setting** under the **Module Setting** menu. It is strongly recommended that the default password is changed to the one that is suitable for your networking environment for security reasons.

System Information Network Information Module Setting Tools logout	System Information	
	Company Name	Connection Technology Systems
	Module Name	CVT-2512
	System Object ID	1.3.6.1.4.1.9304.50.2112
	System Contact	info@ctsyste.com
	System Name	CVT-2512
	System Location	18F-6, No.79, Sec.1, Hsin Tai Wu Rd., Hsichih,
	Software Version	1.03.10
	M/B Version	A03
	Serial Number	026909610000004
Date Code	20091001	
Fiber Typ	SFP --	
Fiber Vendor	--	
Fiber SN	--	
<input type="button" value="Apply"/>		

System Information: Name the Converter, specify the system name and location and check the current version information.

Network Information: Display device information, port status, and SFP status.

Module Setting: Configure DHCP, Port, VLAN, Q-in-Q function and run loopback test.

Tools: Restart the OAM Management Converter, save configurations, restore backup configurations, and upgrade the latest firmware.

3.1 System Information

Select **System Information** from the Main Menu, and then the following screen appears.

System Information Network Information Module Setting Tools logout	System Information	
	Company Name	Connection Technology Systems
	Module Name	CVT-2512
	System Object ID	1.3.6.1.4.1.9304.50.2112
	System Contact	info@ctsyste.com
	System Name	CVT-2512
	System Location	18F-6, No.79, Sec.1, Hsin Tai Wu Rd., Hsichih,
	Software Version	1.03.10
	M/B Version	A03
	Serial Number	026909610000004
Date Code	20091001	
Fiber Typ	SFP --	
Fiber Vendor	--	
Fiber SN	--	
<input type="button" value="Apply"/>		

Company Name: Enter a company name for this OAM Management Converter.

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

System Contact: Enter contact information for this OAM Management Converter.

System Name: Enter a unique name for this OAM Management Converter. Use a descriptive name to identify the OAM Management Converter in relation to your network, for example, “Backbone 1”. This name is mainly used for reference only.

System Location: Enter a brief description of the OAM Management Converter location. The location is for reference only, for example, “13th Floor”.

Software Version: View-only field that shows the product’s firmware version.

M/B Version: View-only field that shows the main board version.

Serial Number: View-only field that shows the serial number of this OAM Management Converter.

Date Code: View-only field that shows the OAM Management Converter Firmware date code.

3.2 Network Information

Select **Network Information** from the Main Menu, then the following screen page appears.

System Information Network Information Module Setting Tools logout	Device Information		
	MAC Address	00:06:19:00:09:30	
	IP Address	192.168.1.197	
	Gateway	192.168.0.254	
	Subnet Mask	255.255.255.0	
	Description	Media Converter	
	Port Status		
	Ports	TP	FX
	Signal detect(SD)	Detected	No
	Link status	On	Down
Speed	100M		
Duplex mode	Full		
Flow control	Disable	Disable	
Auto negotiation	Enable		
SFP Status			
Temperature	--	(C)	
Voltage	--	(V)	
TX Bias	--	(mA)	
TX Power	--	(dBm)	
RX Power	--	(dBm)	

1. Device Information

MAC Address: View-only field that shows the MAC address of this OAM Management Converter. You can not change MAC address of this OAM Management Converter.

IP Address: View-only field that shows the IP address of this OAM Management Converter. You can change the IP address to the desired one in **Network Configuration** under the **Module Setting** Menu.

Gateway: View-only field that shows the Gateway address of this OAM Management Converter. You can change the Gateway address to the desired one in **Network Configuration** under the **Module Setting** Menu.

Subnet Mask: View-only field that shows the Subnet Mask of this OAM Management Converter. You can change the Subnet Mask to the desired one in **Network Configuration** under the **Module Setting** Menu.

Description: View-only field that shows the description you indicate. You can change the description in **Network Configuration** under the **Module Setting** Menu.

2. Port Status

Signal detect (SD): View-only field that shows whether the signal TP and FX is detected or not.

Link status: View-only field that shows the link status of TP and FX. If the link is up, "On" will be shown.

Speed: View-only field that shows the current speed of TP and FX.

Duplex mode: View-only field that shows whether TP and FX are in full-duplex or half-duplex mode.

Flow control: View-only field that shows whether TP and FX's flow control function is enabled or not.

Auto negotiation: View-only field that shows whether TP and FX's auto negotiation function is enabled or not.

3. SFP Status

Temperature: View-only field that shows the slide-in SFP module operation temperature.

Voltage (V): View-only field that shows the slide-in SFP module operation voltage.

TX Power (dbm): View-only field that shows the slide-in SFP module optical Transmission power.

RX Power (dbm): View-only field that shows the slide-in SFP module optical Receiver power.

3.3 Module Setting

Select **Module Setting** and then the following screen page appears.

The screenshot shows a web interface with a left sidebar and a main content area. The sidebar contains a tree view with the following items: System Information, Network Information, **Module Setting** (highlighted in red), Password Setting, Port Configuration, Traffic Statistic, SNMP Configuration, VLAN Configuration, Q-in-Q Configuration, TS1000 Loop Back, 802.3ah Function, and Tools. Under Tools, there is a 'logout' link. The main content area is titled 'NetWork Configuration' and contains a table with the following fields: DHCP Client (set to 'Disable'), IP Address (192.168.1.197), Subnet Mask (255.255.255.0), Gateway (192.168.0.254), and Description (Media Converter). Below the table is a button labeled 'Apply & Save To Flash'.

Network Configuration: To enable or disable DHCP function and specify the desired IP address, subnet mask, gateway and description.

Password Setting: Set up a new password for website access.

Port Configuration: Specify ports' speed, duplex mode, ingress rate limit and egress rate limit and enable or disable flow control function.

Traffic Statistics: Display traffic statistics information of this OAM Management Converter.

SNMP Configuration: To enable or disable SNMP and Trap function.

VLAN Configuration: To enable or disable VLAN mode. If “enabled”, the user can further specify ports' VLAN Group and egress link type.

Q-in-Q Configuration: To enable or disable Q-in-Q. If “enabled”, the user can further specify tag protocol identifier (TPID) and Q-in-Q direction.

TS 1000 Loop Back: Run a loopback test.

3.3.1 Network Configuration

Select **Network Configuration** from **Module Setting** menu, then the following screen page appears.

This screenshot is similar to the previous one, but the 'NetWork Configuration' item in the left sidebar is highlighted in red, indicating it is the active selection. The main content area remains the same, showing the network configuration fields and the 'Apply & Save To Flash' button.

DHCP Client: To enable or disable DHCP function. When “Enabled”, the IP address will be automatically assigned from DHCP Server. When “Disabled”, you need to specify OAM Management Converter’s IP address, subnet mask, and gateway.

IP Address: When DHCP is disabled, you can specify your desired IP address.

Subnet Mask: When DHCP is disabled, you can specify your desired subnet mask.

Gateway: When DHCP is disabled, you can specify your gateway address.

Description: Specify a name or give a brief description to this OAM Management Converter.

Apply & Save To Flash: Click “**Apply & Save To Flash**” to change and save your setting.

3.3.2 Password Setting

Select **Password Setting** from **Module Setting** menu, then the following screen page appears.

Password Setting	
Login Name	<input type="text" value="admin"/>
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm	<input type="password"/>
<input type="button" value="Apply"/>	

Login Name: View-only field. This default login name can not be changed.

Old Password: Type in your old password.

New Password: Type in your new password.

Confirm: Re-type your new password to confirm.

Apply: Click “**Apply**” to change your login password to the one specified.

Note: If you forget the login password, the only way to gain access to the Web Management is to set the OAM Management Converter back to the factory default setting by pressing the Diag. button for 10 seconds (The Diag. button is located on the Front Panel of the OAM Management Converter.). When the OAM Management Converter returns back to the default setting, you can login with the default password (By default, no password is required. Thus, leave the field empty and then press Login.) See Page 8 for login procedure when setting the OAM Management Converter back to the factory default setting.

3.3.3 Port Configuration

Select **Port Configuration** from **Module Setting** menu, then the following screen page appears.

Port Configuration					
Port	Link	Mode	Flow Control	Ingress Rate Limit (kbps)	Egress Rate Limit (kbps)
TP	100F	Auto Speed	Disabled	Not Limit	Not Limit
FX	Down	Auto Mode	Disabled	Not Limit	Not Limit

Apply Refresh

Rate limit is 64kbps as a minimal step

Port: There are two kinds of ports in this OAM Management Converter, these are TP and FX.

Link: This shows the current link status of TP and FX port. For example, when the link is down, it will display “Down”. When the link is connected, it will display the current speed and mode status.

Mode: Select the desired speed or/and duplex mode. For TP port, there are six options available from the pull-down menu, these are “Auto Speed”, “1000 Full”, “100 Full”, “100 Half”, “10 Full”, and “ 10 Half”. For FX port, “Auto mode” and “Force mode” are available.

Flow Control: To enable or disable flow control function.

Ingress Rate Limit (kbps): Select the ingress rate limit from the pull-down menu. “Not Limit” indicates “0” kbps. If you want to specify your own rate limit, you can select “User Setting” and then state your desired rate limit in the corresponding space.

Egress Rate Limit (kbps): Select the egress rate limit from the pull-down menu. “Not Limit” indicates “0” kbps. If you want to specify your own rate limit, you can select “User Setting” and then state your desired rate limit in the corresponding space.

Apply: Click “**Apply**” to change and save the setting.

Refresh: Click “**Refresh**” to refresh the current status.

Note: When DIP 8 (on the Rear Panel of the OAM Management Converter) is set to “ON” (which means that Mode and Flow Control will be set according to configurations in DIP Switch), you can not change TP and FX’s Mode and Flow Control in Web Management. On the other hand, when DIP 8 is set to “OFF” (which means that Mode and Flow Control will be set according to configurations in Web Management), DIP 1~5 setting (set to “ON”) will be ignored.

3.3.4 Traffic Statistics

Select **Traffic Statistics** from **Module Setting** menu, then the following screen page appears.

System Information

Network Information

Module Setting

NetWork Configuration

Password Setting

Port Configuration

Traffic Statistic

SNMP Configuration

VLAN Configuration

Q-in-Q Configuration

TS1000 Loop Back

802.3ah Function

Tools

logout

Traffic Statistic

(The following counter means the port received number)

Port	TP	FX	CPU
Total Bytes	1456275	0	247104
Total Pkts	13075	0	444
Total Error Pkts	0	0	0
Unicast Pkts	570	0	435
Multicast Pkts	941	0	0
Broadcast Pkts	11564	0	9
64	3495	0	265
65-127	8353	0	3
128-255	552	0	7
256-511	667	0	9
512-1023	6	0	18
1024-1518	2	0	142
Undersize Pkts	0	0	0
Oversize Pkts	0	0	0
Fragments	0	0	0
CRC Errors	0	0	0
Jabbers	0	0	0
Drop Events	0	0	0
Pause Frames	0	0	0

Clear

Refresh

Total Bytes: View-only field that shows the number of received frames on each port.

Total Pkts: View-only field that shows the number of total packets received on each port.

Total Error Pkts: View-only field that shows the number of total error packets received on each port.

Unicast Pkts: View-only field that shows the number of unicast packets received.

Multicast Pkts: View-only field that shows the number of multicast packets received.

Broadcast Pkts: View-only field that shows the number of broadcast packets received.

64: View-only field that shows the number of 64byte packets received on each port.

65-127: View-only field that shows the number of packets between 65 and 127 bytes received on each port.

128-288: View-only field that shows the number of packets between 128 and 288 bytes received on each port.

256-511: View-only field that shows the number of packets between 256 and 511 bytes received on each port.

512-1023: View-only field that shows the number of packets between 512 and 1023 bytes received on each port.

1024-1518: View-only field that shows the number of packets between 1024 and 1518 bytes received on each port.

Undersize Pkts: View-only field that shows the number of undersized packets (smaller than 64 bytes) received on each port.

Oversize Pkts: View-only field that shows the number of untagged packets greater than 1518 bytes and tagged packets greater than 1522 bytes received on each port.

Fragments: View-only field that show the number of packets that are less than 64 bytes (excluding framing bits) and have either an FCS error or an alignment error.

CRC Errors: View-only field that show messages of CRC (cyclic redundancy check) data errors.

Jabbers: View-only field that shows the number of packets that are longer than 1522 bytes and have either an FCS error or an alignment error.

Drop Events: View-only field that shows the number of dropped events received on each port.

Pause Frames: View-only field that shows the number of pause frames received on each port.

Clear: Click “Clear” to clear all statistics shown on the table.

Refresh: Click “Refresh” to refresh the counter.

3.3.5 SNMP Configuration

Select **SNMP Configuration** from **Module Setting** menu, then the following screen page appears.

SNMP Configuration	
SNMP Ability	Disable
Trap mode	Disable
SNMP Trap IP Address	0.0.0.0
Read Community	public
Read_Write Community	private
<input type="button" value="Apply"/>	

SNMP Ability: To enable or disable SNMP.

Trap Mode: To enable or disable trap mode. When enabled, a trap will be sent when the following events occur.

Cold Start: When the OAM Management Converter operates cold start, a trap notice will be sent.

Power Down: When the OAM Management Converter is power down, a trap notice will be sent.

Link Up: When TP or FX link is established, a trap notice will be sent.

Link Down: When TP or FX link is disconnected, a trap notice will be sent.

SNMP Trap IP Address: Specify the IP address to which the trap will be sent.

Read Community: Specify a username for SNMP login, up to 31 characters. This allows users to read only.

Read_Write Community: Specify a username for SNMP login, up to 31 characters. This allows users to read and make some setting changes.

Apply: Click “**Apply**”, and then configurations and changes will be saved.

3.3.6 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 Converter 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.

802.1Q VLAN Concept

Port-Based VLAN is simple to implement and use, but it cannot be deployed across converters VLAN. The 802.1Q protocol was developed in order to provide the solution. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large 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.

The 802.1Q frame format is shown below.

PRE	SFD	DA	SA	TCI	P	C	VID	T/L	Payload	FCS
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 Configuration

There are two key concepts to understand.

- The Default Port VLAN ID (**PVID**) specifies the VID to the port that will assign the VID to untagged traffic from that port.
- The VLAN ID (**VID**) specifies the set of VLAN that a given port is allowed to receive and send **labeled** packets.

Both variables can be assigned to a port, but there are significant differences between them. Administrators can only assign one PVID to each port (since the 802.1Q protocol assigns any single packet to just one VLAN). The PVID defines the default VLAN ID tag that will be added to un-tagged frames receiving from that port (ingress traffic).

On the other hand, a port can be defined as a member of multiple VLAN (multiple VID). These VID's constitute an access list for the port. The access list can be used to filter tagged ingress traffic (the converter will drop a tagged packet tagged as belonging in one VLAN if the port on which it was received is not a member of that VLAN). The converter also consults the access list to filter packets it sends to that port (egress traffic). Packets will not be forwarded unless they belong to the VLANs that the port is one of the members.

The differences between **Ingress** and **Egress** configurations can provide network segmentation. Moreover, they allow resources to be shared across more than one VLAN.

Important VLAN Definitions

Ingress

The point at which a frame is received on a converter and the decisions must be made. The converter examines the VID (if present) in the received frames header and decides whether or not and where to forward the frame. If the received frame is untagged, the converter will

tag the frame with the PVID for the port on which it was received. It will then use traditional Ethernet bridging algorithms to determine the port to which the packet should be forwarded.

Next, it checks to see if each destination port is on the same VLAN as the PVID and thus can transmit the frame. If the destination port is a member of the VLAN used by the ingress port, the frame will be forwarded. If the received frame is tagged with VLAN information, the converter checks its address table to see whether the destination port is a member of the same VLAN. Assuming both ports are members of the tagged VLAN, the frame will be forwarded.

Ingress Filtering

The process of checking an incoming frame and comparing its VID with the ingress port VLAN membership is known as Ingress Filtering.

On the OAM Management Converter, it can be either enabled or disabled.

1. When an **untagged** frame is received, the **ingress** port **PVID** will be applied to the frame.
2. When a **tagged** frame is received, the **VID** in the frame tag is used.

When Ingress Filtering is “Enabled”, the OAM Management Converter will first determine,

1. If the **ingress** port itself is a member of the frame VLAN, it will receive the frame.
2. If the **ingress** port is not a member of the frame VLAN, the frame will be dropped.
3. If it is a member of that VLAN, the OAM Management Converter then checks its address table to see whether the destination port is a member of the same VLAN. Assuming both ports are members of that VLAN, the frame will be forwarded.

Administrators should make sure that each port's **PVID** is set up; otherwise, incoming frames may be dropped if **Ingress Filtering** is enabled. On the other hand, when Ingress Filtering is disabled, the OAM Management Converter will not compare the incoming frame **VID** with the **ingress** port VLAN membership. It will only check its address table to see whether the destination VLAN exists.

1. If the VLAN is unknown, it will be broadcasted.
2. If the VLAN and the destination MAC address are known, the frame will be forwarded.
3. If the VLAN is known and the destination MAC address is unknown, the frame will be flooded to all ports in the VLAN.

Tagging

Every port on an 802.1Q compliant converter can be configured as tagging or un-tagging.

Ports with taggings Enable will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has been tagged previously, the port will not alter the packet and keep the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet forwarding decisions.

Un-tagging

Ports with un-taggings Enable will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet does not have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an un-tagging port will have no 802.1Q VLAN information. Un-tagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device. Simply put, un-tagging means that once you set up the port as “U” (untagged), all egress packets (in the same VLAN group) from the port will have no tags.

Select **VLAN Configuration** from **Module Setting** menu, then the following screen page appears.

System Information	802.1Q VLAN Group
Network Information	VLAN Mode [Disable]
Module Setting	Apply
NetWork Configuration	Attention: Before you apply VLAN Group settings, make sure CPU is a member of the management VLAN.
Password Setting	
Port Configuration	
Traffic Statistic	
SNMP Configuration	
<u>VLAN Configuration</u>	
VLAN Group	
VLAN Per Port Setting	
Q-in-Q Configuration	
TS1000 Loop Back	
802.3ah Function	
Tools	
logout	

VLAN Group: To enable or disable VLAN Mode. When enabled, you can further indicate a VID to the selected ports.

VLAN Per Port Setting: To set up each port's egress link type and VID.

3.3.6.1 VLAN Group

Select **VLAN Group**, then the following screen page appears.

System Information	802.1Q VLAN Group
Network Information	VLAN Mode [Disable]
Module Setting	Apply
NetWork Configuration	Attention: Before you apply VLAN Group settings, make sure CPU is a member of the management VLAN.
Password Setting	
Port Configuration	
Traffic Statistic	
SNMP Configuration	
<u>VLAN Configuration</u>	
VLAN Group	
VLAN Per Port Setting	
Q-in-Q Configuration	
TS1000 Loop Back	
802.3ah Function	
Tools	
logout	

VLAN Mode: To enable or disable VLAN Mode. When “enable” is selected, the following screen page will appear to allow you to further indicate a VID to the selected ports.

System Information

Network Information

Module Setting

[NetWork Configuration](#)
[Password Setting](#)
[Port Configuration](#)
[Traffic Statistic](#)
[SNMP Configuration](#)
[VLAN Configuration](#)
[VLAN Group](#)
[VLAN Per Port Setting](#)
[Q-in-Q Configuration](#)
[TS1000 Loop Back](#)
[802.3ah Function](#)

Tools

logout

802.1Q VLAN Group

VLAN Mode Enable

VLAN Group	VID	Member		
		TP	FX	CPU
0	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply

VLAN Group: There are 16 VLAN Groups available from 0 to 15.

VID: Specify a VID (1~4094) to each VLAN Group.

Member: Check the TP, FX, or CPU box in each VLAN Group to enable them to carry the same VID and belong to the same VLAN Group.

3.3.6.2 VLAN Per Port Setting

Select **VLAN Per Port Setting**, then the following screen page appears.

System Information

Network Information

Module Setting

[NetWork Configuration](#)
[Password Setting](#)
[Port Configuration](#)
[Traffic Statistic](#)
[SNMP Configuration](#)
[VLAN Configuration](#)
[VLAN Group](#)
[VLAN Per Port Setting](#)
[Q-in-Q Configuration](#)
[TS1000 Loop Back](#)
[802.3ah Function](#)

Tools

logout

802.1Q VLAN Per Port Setting

Port	Egress Link Type	Port VLAN Entry
TP	Don't Touch Tag	0
FX	Don't Touch Tag	1
CPU	Remove Tag	2
Ingress Filter		Disable

Apply

Attention: Before you apply VLAN Per Port settings, make sure management traffic can go through CPU.

Port: This column indicates the ports available; these are TP, FX, and CPU.

Egress Link Type: Select the needed egress link type from the pull-down menu. Please note that when Q-in-Q is enabled, settings in Egress Link Type will be disabled.

Replace Tag: This will change the VID of packets to the specified one.

Remove Tag: This will remove packets' VID.

Add Tag: This will add the specified VID to packets.

Don't Touch Tag: This will keep packets intact.

Port VLAN Entry: Select each port's corresponding VLAN Group from the pull-down menu.

Ingress Filter: To enable or disable ingress filter.

3.3.7 Q-in-Q Configuration

Select **Q-in-Q Configuration** from **Module Setting** menu, then the following screen page appears.

Q in Q Configuration	
Q in Q Enable	Disable
Out Layer VLAN Tag EtherType (HEX)	0x8100
Out Layer VLAN VID (DEC)	1
Q in Q direction	TP Add QinQ Tag, FX Remove Tag

Apply

Attention: If Q-in-Q is enabled, the VLAN tag may cause Web Management to disconnect.

Q in Q Enable: To enable or disable Q-in-Q function. When Q-in-Q is enabled, settings in Egress Link Type will be disabled.

Out Layer VLAN Tag EtherType (HEX): Specify the tag protocol identifier (TPID) value of VLAN tags.

Out Layer VLAN VID (DEC): Specify the VID (1~4094).

Q in Q Direction: Select Q-in-Q direction from the pull-down menu.

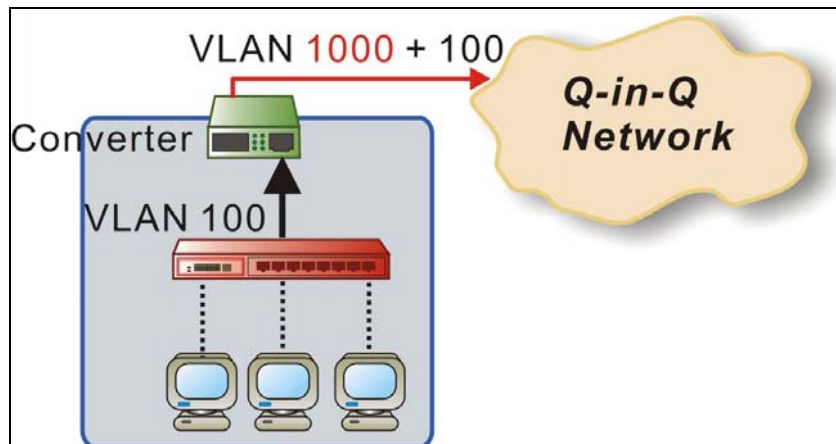
TP Add Q in Q Tag, FX Remove Tag: TP port inserts a Q-in-Q tag and FX port removes a Q-in-Q tag.

FX Add Q in Q Tag, TP Remove Tag: FX port inserts a Q-in-Q tag and FX port removes a Q-in-Q tag.

Note: When traffic is untagged and Q-in-Q is enabled with proper settings, the traffic will be forwarded out with only one tag (Out Layer VLAN VID).

3.3.8 VLAN & Q-in-Q Example

In this section, an example figure is provided to explain the VLAN and Q-in-Q configurations. As illustrated below, TP port is connected to the customer device that has incoming traffic with VLAN 100. If you want traffic forwarded out FX port to be added with a double tag 1000, then follow the steps below to accomplish the process.



VLAN Group

Step 1. By default, VLAN mode is disabled. Make sure you enable VLAN mode before carrying on the following steps.

Step 2. Specify VID 100 and 1000 in VLAN Group 1 and 2 respectively. Select TP, FX, and CPU as member ports in VLAN Group 1 and 2 (When CPU is selected as a member, the VLAN becomes management VLAN.).

System Information
Network Information
Module Setting
NetWork Configuration
Password Setting
Port Configuration
Traffic Statistic
SNMP Configuration
VLAN Configuration
VLAN Group
VLAN Per Port Setting
Q-in-Q Configuration
TS1000 Loop Back
802.3ah Function
Tools
logout

802.1Q VLAN Group
VLAN Mode:

VLAN Group	VID	Member		
		TP	FX	CPU
0	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	1000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Step 3. Click “Apply” to make settings effective.

VLAN Per Port Setting

Step 1. Check whether Q-in-Q is enabled. When enabled, settings in Egress Link Type will be disabled. In this example, Q-in-Q is enabled; thus, this decision ignores Egress Link Type settings.

Step 2. Check whether you have set up 802.1Q VLAN Group Table. When incoming traffic is with a tag, the forwarding process will be executed according to settings in 802.1Q VLAN Group Table. In this example, 802.1Q VLAN Group Table has already set up.

Q-in-Q Configuration

Step 1. By default, Q-in-Q is disabled. Make sure Q-in-Q is enabled before apply the settings.

Step 2. Enter the TPID to identify the frame as the IEEE 802.1q-tagged frame. The value is usually set to 8100. However, you can also enter the TPID (such as 88A8, 9100) that is suitable for your networking environment.

Step 3. Enter the outer VLAN ID. In this example, the outer VLAN ID is 1000.

Step 4. Decide to add a double tag to or remove a double tag from egress traffic. In this example, “FX Add QinQ Tag, TP remove Tag” is selected to accomplish the process of the provided scenario. (Egress traffic from FX port has already had a tag with VID 100. The other tag with VID 1000 will also be added.)

Q in Q Configuration									
System Information	<table><tr><td>Q in Q Enable</td><td>Enable</td></tr><tr><td>Out Layer VLAN Tag EtherType (HEX)</td><td>0x8100</td></tr><tr><td>Out Layer VLAN VID (DEC)</td><td>1000</td></tr><tr><td>Q in Q direction</td><td>FX Add QinQ Tag, TP Remove Tag</td></tr></table>	Q in Q Enable	Enable	Out Layer VLAN Tag EtherType (HEX)	0x8100	Out Layer VLAN VID (DEC)	1000	Q in Q direction	FX Add QinQ Tag, TP Remove Tag
Q in Q Enable	Enable								
Out Layer VLAN Tag EtherType (HEX)	0x8100								
Out Layer VLAN VID (DEC)	1000								
Q in Q direction	FX Add QinQ Tag, TP Remove Tag								
Network Information	<div>Apply</div> <p>Attention: If Q-in-Q is enabled, the VLAN tag may cause Web Management to disconnect.</p>								
Module Setting									
NetWork Configuration									
Password Setting									
Port Configuration									
Traffic Statistic									
SNMP Configuration									
VLAN Configuration									
VLAN Group									
VLAN Per Port Setting									
Q-in-Q Configuration									
TS1000 Loop Back									
802.3ah Function									
Tools									
logout									

3.3.9 TS 1000 Loopback Test

Select **Loopback Test** from **Module Setting** menu, then the following screen page appears.

System Information Network Information Module Setting Network Configuration Password Setting Port Configuration Traffic Statistic SNMP Configuration VLAN Configuration VLAN Group VLAN Per Port Setting Q-in-Q Configuration TS1000 Loop Back 802.3ah Function Tools logout	TS1000 Loop Back Test <div>Send Packet Number: <input type="text" value="100"/> (1~255)</div> <div>Apply</div>
--	--

Send Packet Number: Specify the number of packets for loopback test. By default, the number of packets sent is 100.

Apply: Click “Apply”, then loopback test will be performed.

3.3.10 802.3ah Function

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.

Select **802.3ah Function** from **Module Setting** menu, then the following screen page appears.

System Information Network Information Module Setting NetWork Configuration Password Setting Port Configuration Traffic Statistic SNMP Configuration VLAN Configuration Q-in-Q Configuration TS1000 Loop Back 802.3ah Function 802.3ah Configuration 802.3ah Loopback 802.3ah Status Tools logout	802.3ah OAM Configuration	
	802.3ah Function	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
	802.3ah Mode	<input checked="" type="radio"/> Passive <input type="radio"/> Active
	Remote Loopback	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
	<input type="button" value="Apply"/>	
	802.3ah Status	
	Discovery Status	FAULT
	<input type="button" value="refresh"/>	

802.3ah Configuration: To set up 802.3ah Function, Mode, and Remote Loopback.

802.3ah Loopback: To specify packet number and length for loopback test and view 802.3ah loopback test results.

802.3ah Status: To view 802.3ah status information, including Global Configuration, Flags Field, Discovery Information, and Information TLV.

3.3.10.1 802.3ah Configuration

Select **802.3ah Configuration** from **Module Setting** menu, then the following screen page appears.

System Information Network Information Module Setting NetWork Configuration Password Setting Port Configuration Traffic Statistic SNMP Configuration VLAN Configuration Q-in-Q Configuration TS1000 Loop Back 802.3ah Function 802.3ah Configuration 802.3ah Loopback 802.3ah Status Tools logout	802.3ah OAM Configuration	
	802.3ah Function	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
	802.3ah Mode	<input checked="" type="radio"/> Passive <input type="radio"/> Active
	Remote Loopback	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
	<input type="button" value="Apply"/>	
	802.3ah Status	
	Discovery Status	FAULT
	<input type="button" value="refresh"/>	

1. 802.3ah OAM Configuration

802.3ah Function: Enable or disable 802.3ah function.

802.3ah Mode: Set up 802.3ah Mode for this OAM Management Converter when 802.3ah function is enabled. When this device is set to “Active”, the other device which is 802.3ah-enabled should be set to “Passive” and vice versa. The device in Active mode initiates the exchange of Information OAMPDUs, while the device in Passive mode does not initiate the Discovery process but reacts to the initiation of the Discovery process by the remote 802.3ah-enabled device.

Remote Loopback: Enable or disable remote loopback which is used for fault localization and link performance testing.

2. 802.3ah Status

Discovery Status: View-only field that shows the Discovery process state.

3.3.10.2 802.3ah Loopback

Select **802.3ah Loopback** from **Module Setting** menu, then the following screen page appears.

System Information Network Information Module Setting NetWork Configuration Password Setting Port Configuration Traffic Statistic SNMP Configuration VLAN Configuration Q-in-Q Configuration TS1000 Loop Back 802.3ah Function 802.3ah Configuration 802.3ah Loopback 802.3ah Status Tools logout	802.3ah Loop Back Test	
	Send Packet Number	100 (1~200)
	Packet Length(Not include CRC)	60 (60~1514)
	Apply	

1. 802.3ah Loop Back Test

Send Packet Number: Specify the number of packets that are sent for 802.3ah loopback test.

Packet Length (Not include CRC): Specify the length of each packet that is sent for 802.3ah loopback test.

When appropriate configurations are set and “Apply” is clicked, the 802.3ah loopback result will be shown like the one provided below.

System Information Network Information Module Setting NetWork Configuration Password Setting Port Configuration Traffic Statistic SNMP Configuration VLAN Configuration Q-in-Q Configuration TS1000 Loop Back 802.3ah Function 802.3ah Configuration 802.3ah Loopback 802.3ah Status Tools logout	802.3ah Loop Back Test	
	Send Packet Number	100 (1~200)
	Packet Length(Not include CRC)	60 (60~1514)
	Apply	
Loop Back Test Result		
Result	Pass	
TX Counter	100	
RX Counter	100	
RX Error Counter	0	

2. Loop Back Test Result

Result: View-only field that displays either “Pass” or “Fail”. When “Pass” is displayed, the fields for “TX Counter”, “RX Counter”, and “RX Error Counter” will be shown.

TX Counter: View-only field that shows the number of packets this is transmitted.

RX Counter: View-only field that shows the number of packets that is received.

RX Error Counter: View-only field that shows the number of error packets that is received.

3.3.10.3 802.3ah Status

Select **802.3ah Status** from **Module Setting** menu, then the following screen page appears.

System Information Network Information Module Setting NetWork Configuration Password Setting Port Configuration Traffic Statistic SNMP Configuration VLAN Configuration Q-in-Q Configuration TS1000 Loop Back 802.3ah Function 802.3ah Configuration 802.3ah Loopback 802.3ah Status Tools logout	802.3ah Status Information		
	Global Config		
	Function Enable	ENABLED	
	Local DTE MAC	00-06-19-00-09-30	
	Remote DTE MAC	00-06-19-98-07-1B	
	Flags Field		
		Local	Remote
	Remote Stable	TRUE	TRUE
	Remote Evaluating	FAULT	FAULT
	Local Stable	TRUE	TRUE
Local Evaluating	FAULT	FAULT	
Critical Event	FAULT	FAULT	
Dying Gasp	FAULT	FAULT	
Link Fault	FAULT	FAULT	
Discovery Information			
Discovery State	SEND_ANY		
Local PDU	ANY		
Local Satisfied	TRUE		
Remote State Valid	TRUE		
Local Lost Link Timer Done	FALSE		
Local Link Status	TRUE		

1. Global Config

Function Enable: View-only field that shows whether 802.3ah function is enabled or not.

Local DTE MAC: View-only field that shows the MAC address of this device.

Remote DTE MAC: View-only field that shows the MAC address of the remote DTE device.

Note: If the remote DTE is a device with multiple ports such as a 5-port switch, the remote MAC address field will show its logical MAC address for a particular interface. In other words, the port 1 is assigned the physical MAC address of the device (For example, the physical MAC address is 00-06-19-66-13-17), port 2~5 are assigned the logical MAC address of the device. (Port 2~5 are assigned the logical MAC address 00-06-19-66-13-18~1B.)

2. Flags Field

Remote Stable: Refer to the table below for process definition.

Remote Evaluating: Refer to the table below for process definition.

Local Stable: Refer to the table below for process definition.

Local Evaluating: Refer to the table below for process definition.

VALUE		DEFINITION
Remote/Local Stable	Remote/Local Evaluating	
FALSE	FALSE	Discovery can not complete.
FALSE	TRUE	Remote/Local Discovery process has not completed.
TRUE	FALSE	Remote/Local Discovery process has completed.
TRUE	TRUE	Reserved. If this value is received, it should be ignored.

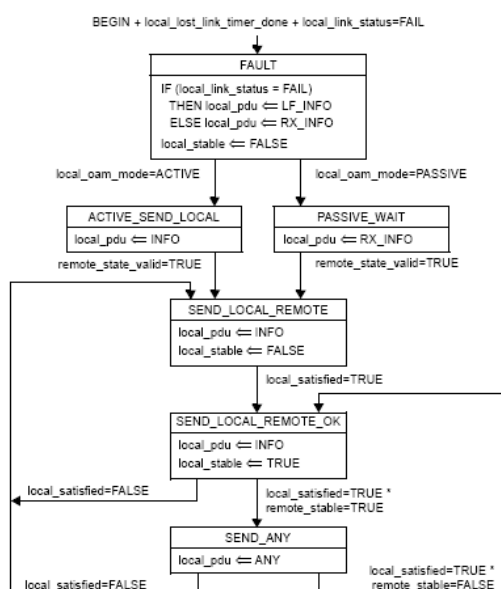
Critical Event: “True” indicates that a critical event has occurred. “Fault” indicates that a critical event has not occurred.

Dying Gasp: “True” indicates that an unrecoverable failure condition (such as power down) has occurred. “Fault” indicates that an unrecoverable failure condition has not occurred.

Link Fault: “True” indicates that the local device’s receive path has detected a fault. “Fault” indicates that the local device’s receive path has not detected a fault.

3. Discovery Information

Discovery State: The Discovery defined in IEEE 802.3ah is used to provide a mechanism to detect the presence of an 802.3ah-capable Network Device on the other end of the Ethernet link. There are six states to complete the Discovery process, these are FAULT state, ACTIVE_SEND_LOCAL state, PASSIVE_WAIT state, SEND_LOCAL_REMOTE state, SEND_LOCAL_REMOTE_OK state, and SEND_ANY state. The following diagram depicts these OAM Discovery states.



OAM Discovery state diagram
(Taken from IEEE Std 802.3ah -2004)

FAULT state: The link can not be established (Local Link Status is False).

ACTIVE_SEND_LOCAL state: When the link is established (Local Link Status is True), the device configured in Active mode sends Information OAMPDUs with Local Information TLVs and waits for Information OAMPDUs received from the remote device.

PASSIVE_WAIT state: A device configured in Passive mode waits until receiving Information OAMPDUs with Local Information TLVs before sending any Information OAMPDUs with Local Information TLVs. Please note that a Passive device cannot complete the Discovery process when connected to another Passive device.

SEND_LOCAL_REMOTE state: Once the device has received Information OAMPDUs with the Local Information TLV from the remote device, the local device begins sending Information OAMPDUs that contain both the local and remote Information TLVs. If settings on the local or remote device are changed resulting in the local OAM client becoming unsatisfied with the settings, the Discovery process returns to the SEND_LOCAL_REMOTE state.

SEND_LOCAL_REMOTE_OK state: If the local OAM client is satisfied with settings on both the local and remote device, it enters the SEND_LOCAL_REMOTE_OK state. If settings on the local OAM client are changed resulting in the remote OAM client becoming unsatisfied with the settings, the Discovery process returns to the SEND_LOCAL_REMOTE state.

SEND_ANY state: The device enters the SEND_ANY state when an OAMPDU has been received indicating the remote device is satisfied with the settings. SEND_ANY is expected to be a normal operating state.

Local PDU: Local PDU consists of four values that are used to govern the transmission and reception of OAMPDUs as part of the Discovery process.

LF_INFO: Only Information OAMPDUs with the Link Fault critical link event set and without Information TLVs are allowed to be transmitted; only Information OAMPDUs are allowed to be received.

RX_INFO: No OAMPDUs are allowed to be transmitted; only Information OAMPDUs are allowed to be received.

INFO: Only Information OAMPDUs are allowed to be transmitted and received.

ANY: Any permissible OAMPDU is allowed to be transmitted and received.

Local Satisfied: View-only field that shows whether OAM Client finds local and remote OAM configuration settings are in agreement or not. "True" indicates that OAM Client is satisfied with local and remote settings, while "False" indicates that OAM Client is not satisfied with local and remote settings.

Remote State Valid: View-only field that shows whether OAM Client has received remote state information. "True" indicates that OAM Client has received remote state information, while "False" indicates that OAM Client has not received remote state information.

Local Lost Link Timer Done: View-only filed that shows whether Local Lost Link Timer expires or not. “True” indicates that Local Lost Link Timer has expired, while “False” indicates that Local Lost Link Timer has not expired.

Local Link Status: View-only filed that shows whether a link fault condition exists or not. “True” indicates that a link fault condition does not exist, while “False” indicates that a link fault condition does exist.

<div>802.3ah Configuration</div> <div>802.3ah Loopback</div> <div>802.3ah Status</div>		
Tools	Information TLV	
logout		
	Local	Remote
State Mux	FWD	FWD
State Par	FWD	FWD
Revision	0x2	0x3
Variable	FAULT	FAULT
Link Events	TRUE	TRUE
Loopback	TRUE	TRUE
Unidir	FAULT	FAULT
Mode	ACTIVE	PASSIVE
Remote Dying Gasp		
Remote Dying Gasp Count: 0		

4. Information TLV

State MUX: View-only field that shows either FWD or DISCARD. “FWD” indicates that Multiplexer passes MAC client frames to subordinate sublayer. “DISCARD” indicates that Multiplexer discards MAC frames.

State Par: View-only field that shows FWD, LB, or DISCARD. “FWD” indicates that Parser passes received non-OAMPDUs to the superior sublayer. “LB” indicates that Parser passes received non-OAMPDUs to Multiplexer during remote loopback test. “DISCARD” indicates that Parser discards received non-OAMPDUs.

Revision: View-only filed that shows the current revision of Information TLVs. The value starts at zero and increments each time when Information TLV changes.

Variable: Currently, this optional function is not supported by the OAM Management Converter.

Link Events: View-only filed that shows whether the device is able to intepret Link Events. “True” indicates that the device is able to intepret Link Events, while “Fault” indicates that the device is unable to intepret Link Events.

Loopback: View-only filed that shows whether the device is able to perform loopback. “True” indicates that the device is able to perform OAM loopback function, while “Fault” indicates that the device is unable to perform OAM loopback function.

Unidir: View only field that shows whether the device is able to send OAMPDUs when the link in the receive path (RX) is not operational. “True” indicates that the device is able to send OAMPDUs when the receive path is not operational, while “Fault” indicates that the device is unable to send OAMPDUs when the receive path is not operational.

Mode: View only field that shows whether the device is configured in Active or Passive mode.

5. Remote Dying Gasp

Remote Dying Gasp Count: The field increments each time when the unrecoverable failure condition occurs (such as power failure).

3.4 Tools

Select **Tools** from the main menu, then the following screen page appears.

The screenshot shows a web interface for the 'TS1000 Loop Back Test'. On the left, a sidebar menu lists 'System Information', 'Network Information', 'Module Setting', and 'Tools' (which is highlighted). Under 'Tools', there are links for 'System Reboot', 'Save and Restore', 'Firmware Upgrade', and 'logout'. The main content area is titled 'TS1000 Loop Back Test' and contains a 'Send Packet Number' input field with the value '100' and a range indicator '(1~255)'. An 'Apply' button is located below the input field.

System Reboot: Restart the OAM Management Converter.

Save and Restore: Save all configurations to flash, load previous configurations, and reset the OAM Management Converter back to factory default settings.

Firmware Upgrade: Upgrade the latest firmware.

3.4.1 System Reboot

Select **System Reboot**, then the following screen page appears.

This screenshot is similar to the previous one, showing the 'TS1000 Loop Back Test' interface. However, a 'Microsoft Internet Explorer' dialog box is overlaid on the screen. The dialog box contains a question mark icon and the text 'Do you want to restart the Converter?'. It has two buttons: 'OK' and 'Cancel'. The 'System Reboot' option in the sidebar is now highlighted in red.

3.4.2 Save and Restore

Select **Save and Restore**, then the following screen page appears.

System Information Network Information Module Setting Tools System Reboot Save and Restore Firmware Upgrade logout	System Configuration Setting
	Press the "SaveToFlash" button, all current configuration will save to converter as backup. <div>SaveToFlash</div>
	Press the "LoadFromFlash" button, the Web Interface may be disconnected for restore to previous backup configuration. <div>LoadFromFlash</div>
	Press the "ResetToFactory" button, the Web Interface will be disconnected. After reset all configuration, the system will back to factory default mode. The default IP address is 192.168.0.1 . Caution: The System will restart automatically after "ResetToFactory" finished. <div>ResetToFactory</div>

3.4.3 Firmware Upgrade

Select **Firmware Upgrade**, then the following screen page appears.

System Information Network Information Module Setting Tools System Reboot Save and Restore Firmware Upgrade logout	Firmware Upgrade
	This mode allows to proceed the firmware upgrade on device. Please select the location of the firmware file on your PC by using the browse button as below, then press the "Upgrade" button. <div><input type="text"/> <div>Browse</div></div>
	Note: 1. Ensure that the "File of type" field in the browse window is set to 'All files(*.*)'. 2. To cancel the Firmware Upgrade process, power cycle the switch without selecting any files. <div>Upgrade</div>
	(Firmware Upgrading may take 60 seconds) Firmware Upgrade process must NOT be interrupted !