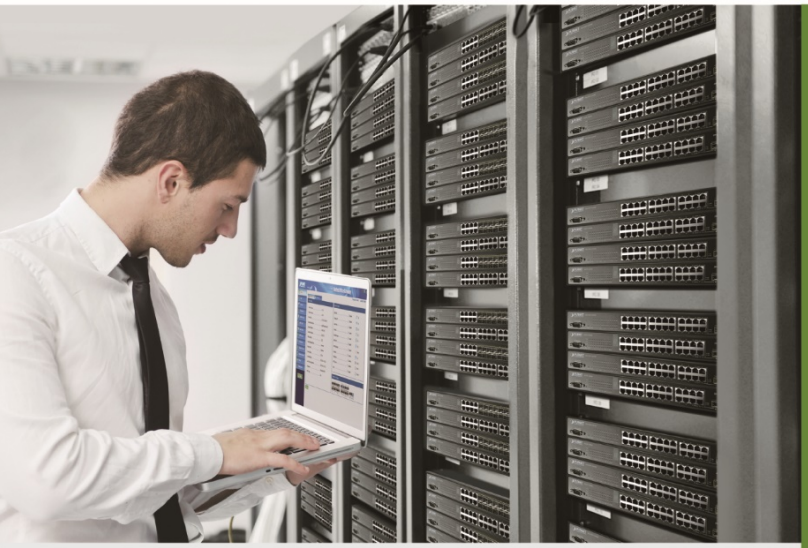
PLANET
Networking & Communication

User's Manual

10/100/1000BASE-T to 100/1000BASE-X SFP Managed Media Converter

GT-915A



www.PLANET.com.tw

Trademarks

Copyright © PLANET Technology Corp. 2023.
Contents are subject to revision without prior notice.
PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

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 limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

This device is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy saving, please remove the power cable to disconnect the device from the power circuit. In view of saving the energy and reducing the unnecessary power consumption, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

PLANET 10/100/1000BASE-T to 100/1000BASE-X SFP Managed Media Converter User's Manual

FOR MODELS: GT-915A

REVISION: 1.0 (February, 2023)

Part No: EM-GT-915A_v1.0

TABLE OF CONETNTS

1. INTRODUCTION 6

1.2 Product Description 7

1.3 How to Use This Manual 10

1.4 Product Features 11

1.5 Product Specifications 13

2. INSTALLATION 16

2.1 Hardware Description 16

2.1.1 Converter Front Panel 16

2.1.2 Converter LED Indicators 17

2.1.3 Rear Panel 18

2.1.4 Power Information 18

2.2 Media Converter Installation 19

2.2.1 Stand-alone Installation 19

2.2.2 Wall-mount Installation 19

2.2.3 Media Chassis Installation 20

2.2.4 Installing the SFP Transceiver 21

3. MEDIA CONVERTER MANAGEMENT 24

3.1 Requirements 24

3.2 Management Access Overview 24

3.3 Web Management 25

3.4 SNMP-Based Network Management 26

3.5 PLANET Smart Discovery Utility 27

4. WEB CONFIGURATION 29

4.1 Main Web Page 32

4.2 System 35

4.2.1 Management 36

4.2.1.1 System Information 36

4.2.1.2 System Configuration 37

4.2.1.3 Device Information 38

4.2.1.4 Users Configuration 38
4.2.1.5 CPU Resource Utilization 39
4.2.1.6 Syslog Settings 40
4.2.1.7 System Log 41
4.2.2 IP Configuration 42
4.2.2.1 IPv4 42
4.2.2.2 IPv6 42
4.2.3 SNMP Settings 43
4.2.3.1 SNMP Configuration 44
4.2.3.2 SNMP View Table 44
4.2.3.3 SNMP Group Table 46
4.2.3.4 SNMP User Table 47
4.2.3.5 SNMP Community Table 48
4.2.3.6 SNMP Host Table 49
4.2.4 NTP Configuration 50
4.2.5 Remote Management 51

4.3 Switching 53
4.3.1 Port Management 54
4.3.1.1 Port Configuration 54
4.3.1.2 SFP Module Information 55
4.3.2 OAM TS-1000 56
4.3.2.1 Local OAM TS-1000 Configuration 56
4.3.2.2 Remote OAM TS-1000 Configuration 57
4.3.2.3 OAM TS-1000 Loop Back 58
4.3.3 OAM 802.3ah 60
4.3.3.1 Common OAM 802.3ah Configuration 60
4.3.3.2 Remote OAM 802.3ah Configuration 61
4.3.3.3 OAM 802.3ah Loop Back 62
4.3.4 VLAN Configuration 64
4.3.4.1 VLAN Overview 64
4.3.4.2 IEEE 802.1Q VLAN 65
4.3.4.3 VLAN Mode 68
4.3.4.4 VLAN Tag-based Entry Config 69
4.3.4.5 VLAN Port Config 71
4.3.4.6 Q-in-Q Port Config 74
4.3.4.7 Q-in-Q Index Config 76
4.3.5 LLDP 78
4.3.5.1 LLDP Global Setting 78
4.3.5.2 LLDP Port Setting 79
4.3.5.3 LLDP Remote MIB 81

4.3.6 Link Fault Passthrough 82

4.4 QoS 83

4.4.1 Understanding QoS 83

4.4.2 General 84

4.4.2.1 QoS Mode Set 84

4.4.2.2 Class of Service 85

4.4.2.3 802.1p-based QoS 86

4.4.2.4 DSCP-based Priority 87

4.4.2.5 IP Addr Base 88

4.4.3 Bandwidth Control 89

4.4.4 Storm Control 90

4.5 Security 92

4.5.1 Access Security 92

4.5.1.1 Access Management 92

4.5.1.2 HTTPS 93

4.6 Maintenance 94

4.6.1 Configuration 94

4.6.1.1 Backup 94

4.6.1.2 Restore 94

4.6.1.3 Save 94

4.6.2 Firmware Update 95

4.6.3 Factory Default 95

4.6.4 System Reboot 96

5. TROUBLESHOOTING 97

Appendix A Networking Connection 99

A.1 Device's RJ-45 Pin Assignments 99

A.2 RJ-45 cable pin assignment 100

1. INTRODUCTION

Thank you for purchasing PLANET Managed Media Converter. In the following sections, unless specified, the term "**Managed Media Converter**" mentioned in this manual refers to the GT-915A.

Open the box of the Managed Media Converter and carefully unpack it. The box should contain the following items:

XST-705A Smart Media Converter x 1	Quick Start QR code sheet x 1	SFP Dust Cap x 1
Power adapter (5V,2A) x 1		

If any of these are missing or damaged, please contact your dealer immediately; if possible, retain the carton including the original packing material, and use them again to repack the product in case there is a need to return it to us for repair.

1.2 Product Description

Remotely Managed Gigabit Converter

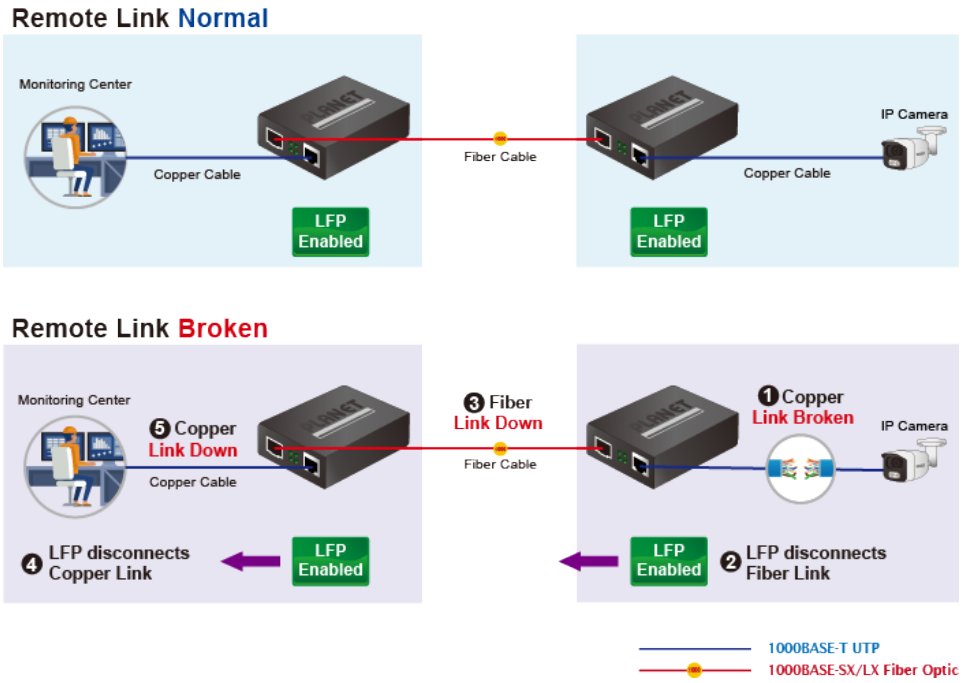
PLANET GT-915A 10/100/1000BASE-T to 100/1000BASE-X Managed Media Converter is developed to meet the advanced demand of network applications but it comes with the easy Plug and Play feature. The GT-915A provides all kinds of 10/100/1000Mbps Ethernet Media on RJ45 port and offers highly-stable Gigabit SFP fiber performance. It supports conversion between 10/100/1000BASE-T and 100/1000BASE-X Ethernet, which includes SFP slot with single-mode or multi-mode media as required. The Ethernet signal allows three types of segments to connect easily, efficiently and inexpensively.

Enhanced Smart Management Features

The GT-915A provides auto MDI/MDI-X on its TP port and built-in **Link Fault Pass-through** function (**LFP**). The LFP function includes **Link Loss Carry Forward** (**LLCF**) and **Link Loss Return** (**LLR**), both of which can immediately alarm administrators the problem of the link media and provide efficient solution to monitoring the net.

- LLCF means when a device connected to the converter and the TP line loses the link, the converter's fiber port will disconnect the link of transmission.
- LLR means when a device connected to the converter and the fiber line loses the link, the converter's fiber port will disconnect the link of transmission.

Therefore, the GT-915A greatly supports the administrators to manage the network efficiently.



Network with Cybersecurity Helps Minimize Security Risks

The GT-915A comes with enhanced cybersecurity to fend off cyberthreats and cyberattacks. It supports SSHv2, TLSv1.2 and SNMPv3 protocols to provide strong protection against advanced threats. Served as a key point to transmit data to customer's critical equipment in a business network, the cybersecurity feature of the IGT-900-Series protects the management and enhances the security of the mission-critical network without any extra deployment cost and effort.

User-friendly and Centralized Web Management Interface

For efficient management, the GT-915A is equipped with a remote Web/SNMP interface. With its built-in Web-based management, PLANET GT-915A acts as an easy-to-use, platform-independent management and configuration facility. The GT-915A also supports standard Simple Network Management Protocol (SNMP) and can be managed via any standard-based management software.

OAM Management

TS-1000/802.3ah OAM protocol (operation, administration, and maintenance) supported enables remote OAM compliant device to be managed and monitored by the GT-915A.

Remotely Manage Solution

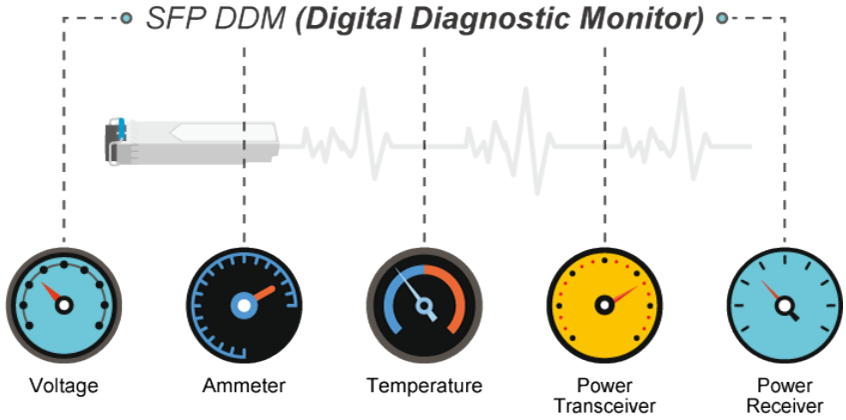
PLANET's Universal Network Management System (**UNI-NMS**) and **CloudViewer App** support IT staff to remotely manage all network devices and monitor the GT-915A operation statuses. Thus, they're designed for both the enterprises and industries where deployments of the GT-915A can be as remote as possible, without having to go to the actual location once a bug or faulty condition is found. With the UNI-NMS or CloudViewer app, all kinds of businesses can now be speedily and efficiently managed from one platform.

Enhanced Traffic Control

The GT-915A can be programmed for advanced management functions such as IP address configuration, DHCP client function, port configuration, converter configuration, 802.1Q tag VLAN, Q-in-Q VLAN, ingress/egress bandwidth control, QoS and Layer protocol filter, and broadcast storm and bandwidth control to enhance bandwidth utilization.

Intelligent SFP Diagnosis Mechanism

The GT-915A supports SFP-DDM (digital diagnostic monitor) function that greatly helps network administrator to easily monitor real-time parameters of the SFP transceivers, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.



Easy Chassis Installation

The GT-915A Media Converter can be used as a stand-alone unit or as a slide-in module to the PLANET Media Converter Chassis (**MC-700, MC-1500 and MC-1500R series**). The media chassis can assist in providing DC power to the GT-915A Media Converter to maintain the fiber-optic network at one centralized location. It can be DIN-rail or wall mounted for efficient use of cabinet space.

1.3 How to Use This Manual

This User's Manual is structured as follows:

Section 2, **INSTALLATION**

The section explains the functions of the Managed Media Converter and how to physically install the Managed Media Converter.

Section 3, **SWITCH MANAGEMENT**

The section contains the information about the software function of the Managed Media Converter.

Section 4, **WEB CONFIGURATION**

The section explains how to manage the Managed Media Converter by Web interface.

Section 5, **TROUBLESHOOTING**

The chapter explains how to do troubleshooting of the Managed Media Converter.

Appendix A

GLOSSARY

1.4 Product Features

Physical Port

- One 1G/100/10BASE-T RJ45 interface with auto MDI/MDI-X function
- One 1G/100BASE-X SFP interface

Layer 2 Features

- Supports VLAN
  - IEEE 802.1Q tagged VLAN
  - Supports provider bridging (VLAN Q-in-Q, IEEE 802.1ad)
  - VLAN transparent
- Storm Control support
  - Broadcast/Multicast/DLF (Destination Lookup Failure)/ARP/ICMP
- Store-and-Forward mechanism
- Non-blocking full wire-speed forwarding rate
- **16K** jumbo frame size support
- Prevents packet loss with back pressure (half-duplex) and IEEE 802.3x pause frame flow control (full-duplex)
- Automatic address learning and address aging
- Supports port status/Ethernet statistics on both TP and fiber interfaces
- Supports Link Fault Passthrough (LFP) and Link Layer Discovery Protocol (LLDP)

OAM Compliant

- TS-1000 OAM / IEEE 802.3ah OAM / Loop Back Test

Quality of Service

- Ingress Shaper and Egress Rate Limit per port bandwidth control
- 8 priority queues on all converter ports
- Strict priority and Weighted Round Robin (WRR) CoS policies
- Traffic classification
  - IEEE 802.1p CoS
  - IP DSCP
  - IP Address

Management

- IPv4 and IPv6 dual stack management
- Management Interfaces
  - Web HTTP management
  - Telnet Command Line Interface
  - SNMP v1, v2c monitoring
  - SSHv2, TLSv1.2 and SNMP v3 secure access
- System Maintenance
  - Firmware upload/download via HTTP
  - Reset button for system reboot or reset to factory default

- Network Time Protocol (NTP)
- SNMP Management
  - − SNMP trap for interface link up and link down notification
  - − Four RMON groups (history, statistics, alarms and events)
- Network Diagnostic
  - SFP-DDM (Digital Diagnostic Monitor)
- Syslog remote alarm
- Local system Log
- PLANET Smart Discovery Utility for deploy management
- PLANET Remote Management
  - − PLANET NMS Controller and CloudViewer for deployment management

Case and Installation

- External 5V DC, 2A power supply
- 0 to 50 degrees C operating temperature
- Supports 6000 VDC Ethernet ESD protection
- Wall mounting and DIN-rail installation supported
- Works with PLANET's 10"/19" Media Converter Chassis (MC-700/MC-1500/MC-1500R/MC-1500R48)
- Plug and Play installation

1.5 Product Specifications

Model	GT-915A
Hardware Specifications	
Copper Interface	1 x 10/100/1000BASE-T RJ45 port (Auto-MDI/MDI-X) twisted pair
Fiber Interface	1 x 100/1000BASE-X SFP Slot
Reset Button	< 10 sec.: System reboot > 10 sec.: Factory default
ESD Protection	6KV DC
Enclosure	Compact-sized metal case
Installation	Wall mountable Media convert Chassis installation Optional DIN-rail kit
Dimensions (W x D x H)	94 x 70 x 26mm
Weight	201g (device only)
Power Input	DC 5V, 2A
Power Consumption	3.4 watts/11.6 BTU (maximum)
LED Indicator	PWR, (**Green**) TP LINK/ACT, 1000 (**Green**) Fiber LINK/ACT (**Green**)
Network Cables	**10/100/1000BASE-T：** 10BASE-T: 2-pair UTP Cat. 3,4,5, up to 100 m 100BASE-TX: 2-pair UTP Cat. 5, up to 100 m 1000BASE-T: 4-pair STP Cat 5 up to 100m **100/1000GBASE-SX/LX：** 50/125μm or 62.5/125μm multi-mode fiber cable, up to 220/550m. 9/125μm single-mode cable, extending long distance to 10/20/40/60/80/120km (vary on fiber transceiver or SFP module)
Switching Specifications	
Switch Processing Scheme	Store and Forward
Fabric	4Gbps
Throughput (packet per second)	2.98Mpps@64bytes
Address Table	1K entries, automatic source address learning and aging
Flow Control	Back pressure for half duplex IEEE 802.3x pause frame for full duplex
Jumbo Frame	16K
Shared Buffer	512Kb
Layer 2 Function	
Port Configuration	Port disable/enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow control disable/enable
Port Status	Display each port's speed duplex mode, link status, flow control status, auto negotiation status

VLAN	IEEE 802.1Q tag-based VLAN IEEE 802.1ad Q-in-Q tunneling Up to 16 VLAN groups, out of 4094 VLAN IDs Management VLAN
Bandwidth Control	Per port bandwidth control Ingress: 1~1000,000Kbps Egress: 1~1000,000Kbps
QoS	Traffic classification based, strict priority and WRR 8-level priority for switching Traffic classification: - 802.1p priority - IP DSCP - IP Address
Security Function	
Access Security	Remote management protocols control by SSH, Telnet, HTTP ans HTTPs
System Management	
Basic Management Interfaces	Telnet; Web browser; SNMP v1, v2c
Secure Management Interfaces	SSHv2, TLS v1.2, SNMP v3
System Management	Firmware upgrade by HTTP protocol through Ethernet network Configuration upload/download through HTTP LLDP protocol NTP PLANET Smart Discovery Utility PLANET CloudViewer app
Event Management	Remote syslog Local system log SNMP trap
Standards Conformance	
Regulatory Compliance	FCC Class A, CE Class A
Standards Compliance	IEEE 802.3, 10BASE-T IEEE 802.3u, 100BASE-TX/FX IEEE 802.3ab, 1000BASE-T IEEE 802.3z, 1000BASE-SX/LX IEEE 802.3x full-duplex flow control IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1ad Q-in-Q VLAN stacking IEEE 802.1ab LLDP IEEE 802.3ah OAM RFC 768 UDP RFC 783 TFTP RFC 791 IP

	RFC 792 ICMP RFC 2068 HTTP
Environment	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

2. INSTALLATION

This section describes the hardware features and installation of the Managed Media Converter on the desktop or rack mount. For easier management and control of the Managed Media Converter, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the Managed Media Converter, please read this chapter completely.

2.1 Hardware Description

2.1.1 Converter Front Panel

The front panel provides a simple interface monitoring the Managed Media Converter. Figure 2-1 shows the front panels of the Managed Media Converter.

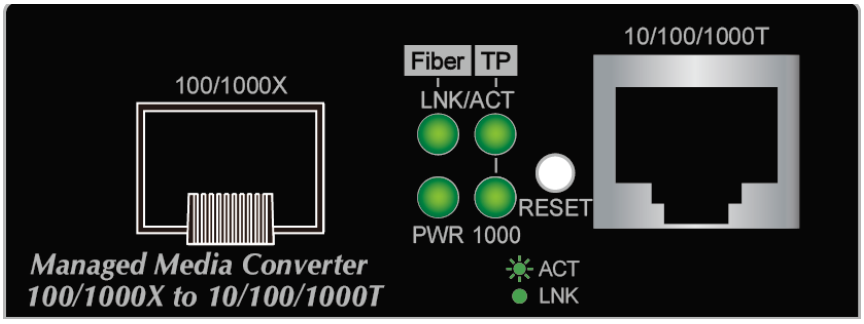


Figure 2-1: Front Panels of Managed Media Converter

■ **Gigabit TP interface**

10/100/1000BASE-T Copper, RJ45 Twisted-pair: Up to 100 meters.

■ **SFP slots**

100/1000BASE-X mini-GBIC slot, SFP (Small Factor Pluggable) transceiver module: From 550 meters to 2km (Multi-mode fiber), up to above 10/20/30/40/50/60/70/120 kilometers (Single-mode fiber).

■ **Reset button**

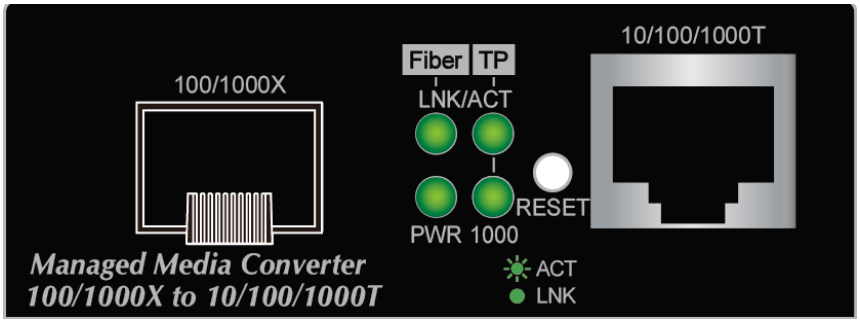
At the left of the front panel, the reset button is designed for rebooting the Managed Media Converter without turning off and on the power. The following is the summary table of Reset button functions:

Reset Button Pressed and Released	Function
< 5 sec: System Reboot	Reboot the Managed Media Converter.

> 5 sec: Factory Default	Reset the Managed Media Converter to Factory Default configuration. The Managed Media Converter will then reboot and load the default settings as below: ◦ Default Username: **admin** ◦ Default Password: **admin** ◦ Default IP address: **192.168.0.100** ◦ Subnet mask: **255.255.255.0** ◦ Default Gateway: **192.168.0.254**

2.1.2 Converter LED Indicators

Figure 2-2 shows the LED indications of the Managed Media Converter.



■ **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate that the Media Converter has power.

■ **1000BASE-X Fiber Optic interface (SFP, SC & WDM)**

LED	Color	Function
LNK/ACT	**Green**	**Lights** to indicate that the fiber optic link is established.
		Blinks to indicate that the fiber optic link is actively sending or receiving data over that fiber port.

■ **10/100/1000BASE-T Port**

LED	Color	Function
LNK/ACT	**Green**	**Lights** to indicate the link through TP port is successfully established.
		Blinks to the TP port is actively sending or receiving data
1000 **Speed**	**Green**	**Lights** to indicate that the port is operating at **1000Mbps.**
		Off to indicate that the port is link down or **10Mbps** or **100Mbps**.

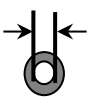
2.1.3 Rear Panel

The rear panel of the Managed Media Convertere consists of one DC jack, which accepts input power with 5V DC, 2A.

2.1.4 Power Information

The central pole of the Managed Media Convertere's power jacks measures 2.5mm wide that require +5VDC power input. It conforms to the bundled AC-DC adapter and PLANET's media chassis. Should you have the issue of power connection, please contact your local sales representative.

Please keep the AC-DC adapter as a spare part when the GT-915A is installed in a media chassis.



2.5mm

Width of DC Receptacle: **2.5mm**

+5V for each slot

DC receptacle is 2.5mm wide that matches the central pole; the width of the Media Converter DC jack also measures 2.5mm.

Warning: Do not install any improper unit.

The device is a power-required device, meaning it will not work till it is powered. If your networks should be active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime.

In some areas, installing a surge suppression device may also help to protect your Media Converter from being damaged by unregulated surge or current to the converter or the power adapter.

2.2 Media Converter Installation

This section describes the functionalities of the Media Converter's components and guides you to how to install it on the desktop. Basic knowledge of networking is assumed. Please read this chapter completely before continuing.

2.2.1 Stand-alone Installation

Step 1: Unpack the Media Converter.

Step 2: Connect the 5V DC power adapter to the GT-915A and verify that the Power LED lights up.
(Please refer to the **2.1.4 Power Information** section for power input.)

Step 3:

3-1: Prepare a twisted-pair, straight-through **Category 5e/6/7 UTP cable** for Ethernet connection.

3-2: Prepare a fiber cable for connection to the SFP slot, and make sure both sides of the SFP transceiver are with the same media type.
(Please refer to the **3.5 Cable Connection** section for the type of connection.)

Step 4:

4-1: Insert one side of **Category 5e/6/7 cable** into the Media Converter Ethernet port (RJ45) while the other side of Category 5e/6/7 cable into the network devices' Ethernet port (RJ45), e.g., switch, PC or server.
The UTP port (RJ45) LED on the Media Converter will light up when the cable is connected with the network device.
(Please refer to the **2.1.2 LED Indicators** section for the functions of LED lights.)

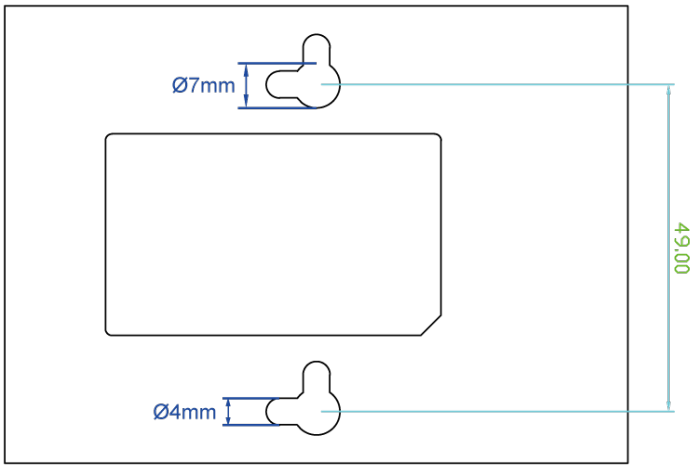
4-2: Connect the **fiber cable**. Attach the duplex LC connector on the network cable to the SFP transceiver. Attach the fiber cable from the GT-915A to the fiber network. TX, RX must be paired at both ends.

Step 5: When all the connections are all set and the LED lights all show normally, the installation is complete.

2.2.2 Wall-mount Installation

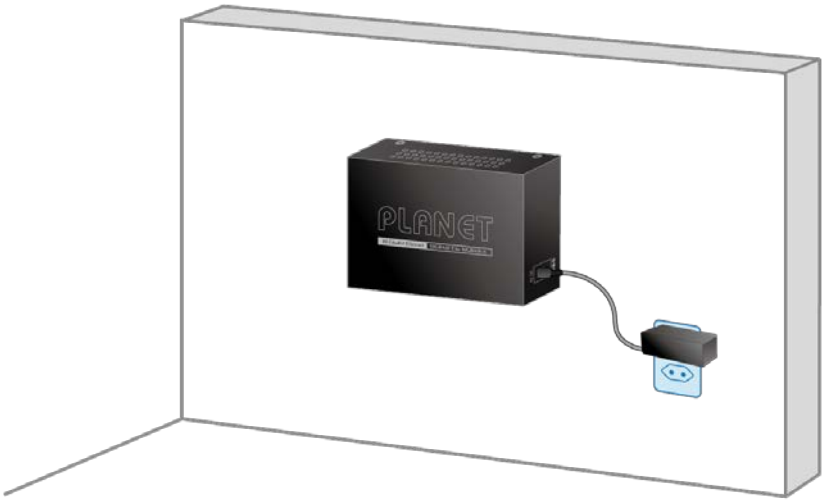
Step 1: Please find the wall that can mount the Managed Media Converter

Step 2: Screw two screws on the wall.



Step 3: Hang the Managed Media Converter on the screws from the wall.

Step 4: Refer to Chapter **2.1.4 Power Information** on power supply to the Managed Media Converter.



Note

Before mounting the device to the wall, please check the location of the electrical outlet and the length of the Ethernet cable.

2.2.3 Media Chassis Installation

To install the Media Converter in a **10-inch** or **19-inch** standard rack, follow the instructions described below.

Step 1: Place your Managed Media Converter on a hard flat surface, with the front panel positioned towards your front side.

Step 2: Carefully slide in the module until it is fully and firmly fitted into the slot of the chassis; the Power LED of the Media Converter will turn ON.

Figure 2-2: Insert Managed Media Converter into an available slot

1. Never push the converter into the slot with force; it could damage the chassis.

Caution:

2. The Media Converter Chassis supports hot-swap; there is no need to turn off the whole chassis before sliding in the new converter.

2.2.4 Installing the SFP Transceiver

The sections describe how to insert an SFP transceiver into an SFP slot.

The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Managed Media Converter, as the Figure 2-3 shows..

Figure 2-3: Plug-in the SFP Transceiver

■ Approved PLANET SFP Transceivers

PLANET Managed Media Converter supports both Single mode and Multi-mode SFP transceiver. The following list of approved PLANET SFP transceivers is correct at the time of publication:

Gigabit SFP Transceiver Modules

MGB-GT	SFP-Port 1000BASE-T Module
MGB-SX	SFP-Port 1000BASE-SX mini-GBIC module - 550m
MGB-SX2	SFP-Port 1000BASE-SX mini-GBIC module - 2km
MGB-LX	SFP-Port 1000BASE-LX mini-GBIC module - 20km
MGB-L40	SFP-Port 1000BASE-LX mini-GBIC module - 40km
MGB-L80	SFP-Port 1000BASE-LX mini-GBIC module - 80km
MGB-L120	SFP-Port 1000BASE-LX mini-GBIC module - 120km
MGB-LA10	SFP-Port 1000BASE-LX (WDM,TX:1310nm) mini-GBIC module - 10km
MGB-LB10	SFP-Port 1000BASE-LX (WDM,TX:1550nm) mini-GBIC module - 10km
MGB-LA20	SFP-Port 1000BASE-LX (WDM,TX:1310nm) mini-GBIC module - 20km
MGB-LB20	SFP-Port 1000BASE-LX (WDM,TX:1550nm) mini-GBIC module - 20km
MGB-LA40	SFP-Port 1000BASE-LX (WDM,TX:1310nm) mini-GBIC module - 40km
MGB-LB40	SFP-Port 1000BASE-LX (WDM,TX:1550nm) mini-GBIC module - 40km
MGB-LA80	SFP-Port 1000BASE-LX (WDM,TX:1490nm) mini-GBIC module - 80km

MGB-LB80	SFP-Port 1000BASE-LX (WDM,TX:1550nm) mini-GBIC module - 80km

Fast Ethernet SFP Transceiver Modules

MFB-FX	SFP-Port 100BASE-FX Transceiver (1310nm) -2km
MFB-F20	SFP-Port 100BASE-FX Transceiver (1310nm) - 20km
MFB-F40	SFP-Port 100BASE-FX Transceiver (1310nm) - 40KM
MFB-F60	SFP-Port 100BASE-FX Transceiver (1310nm) - 60KM
MFB-TFX	SFP-Port 100BASE-FX Transceiver (1310nm) -2km (-40~75 degrees C)
MFB-TF20	SFP-Port 100BASE-FX Transceiver (1310nm) - 20km (-40~75 degrees C)

It is recommended to use PLANET SFP on the Managed Media Converter. If you insert an SFP transceiver that is not supported, the Managed Media Converter will not recognize it.

1. Before we connect Managed Media Converter to the other network device, we have to make sure both sides of the SFP transceivers are with the same media type, for example: 1000BASE-SX to 1000BASE-SX, 1000BASE-LX to 1000BASE-LX.
2. Check whether the fiber-optic cable type matches with the SFP transceiver requirement.
1. To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
2. To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

■ Connect the Fiber Cable

1. Insert the duplex LC connector into the SFP transceiver.
2. Connect the other end of the cable to a device with SFP transceiver installed.
3. Check the LNK/ACT LED of the SFP slot on the front of the Managed Media Converter. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to **"1000 Force"**.

■ Remove the Transceiver Module

1. Make sure there is no network activity any more.
2. Remove the Fiber-Optic Cable gently.
3. Lift up the lever of the MGB module and turn it to a horizontal position.
4. Pull out the module gently through the lever.

Figure 2-4: How to Pull Out the SFP Transceiver

Note

Never pull out the module without lifting up the lever of the module and turning it to a horizontal position. Directly pulling out the module could damage the module and the SFP module slot of the Managed Media Converter.

3. MEDIA CONVERTER MANAGEMENT

This chapter explains the methods that you can use to configure management access to the Managed Media Converter. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Administration Console Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- Workstations running Windows XP/2003/2008/Vista/7/8/10/11, MAC OS X or later, Linux, UNIX, or other platforms are compatible with TCP/IP protocols.
- Workstations are installed with Ethernet NIC (Network Interface Card)
- **Ethernet Port Connection**
  - Network cables -- Use standard network (UTP) cables with RJ45 connectors.
  - The above PC is installed with Web browser.

It is recommended to use Chrome 98.0.xxx or above to access the Managed Media Converter.

3.2 Management Access Overview

The Managed Media Converter gives you the flexibility to access and manage it using any or all of the following methods:

- An administration **console**
- **Web browser** interface
- An external **SNMP-based network management application**

The administration console and Web browser interface support are embedded in the Managed Media Converter software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Command Line	• Text-based • Telnet and SSH protocols functionality	
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1: Comparison of Management Methods

3.3 Web Management

The Managed Media Converter offers management features that allow users to manage the Managed Media Converter from anywhere on the network through a standard browser such as Microsoft Internet Explorer or Google Chrome. After set up your IP address for the Managed Media Converter, you can access the Managed Media Converter 's Web interface applications directly in your Web browser by entering the IP address of the Managed Media Converter.

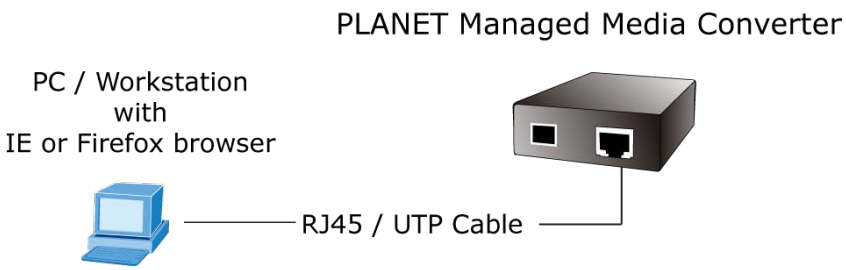


Figure 3-3: Web Management

You can then use your Web browser to list and manage the Managed Media Converter configuration parameters from one central location, just as if you were directly connected to the Managed Media Converter's RJ45 console port. Web Management requires either **Microsoft Internet Explorer 8.0** or later.

Figure 3-4: Web Main Screen of Managed Media Converter

3.4 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the Managed Media Converter, such as SNMP Network Manager, HP Openview Network Node Management (NNM) or What's Up Gold. This management method requires the SNMP agent on the Managed Media Converter and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string. If the SNMP Net-work management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default getting and setting community strings for the Managed Media Converter is public.

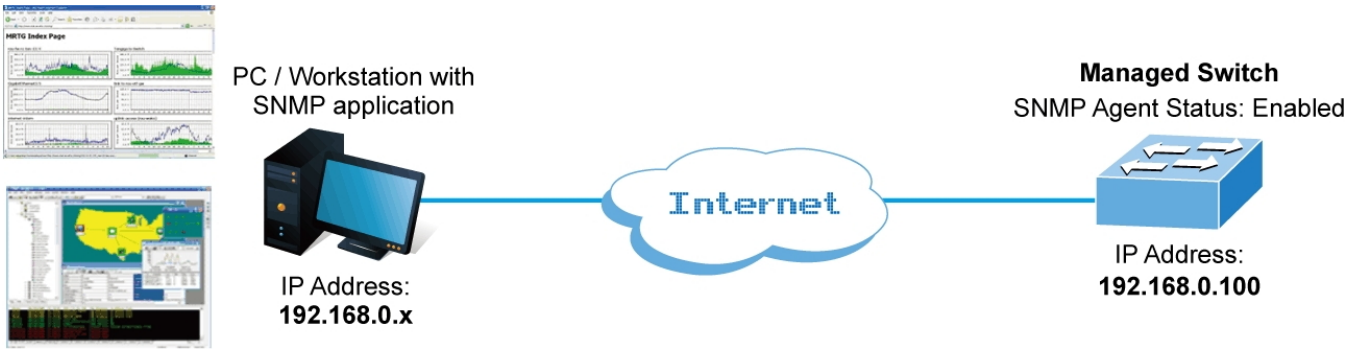


Figure 3-5: SNMP Management

3.5 PLANET Smart Discovery Utility

For easily listing the Managed Media Converter in your Ethernet environment, the PLANET Smart Discovery Utility is an ideal solution. The following installation instructions are to guide you to running the PLANET Smart Discovery Utility.

1. Deposit the PLANET Smart Discovery Utility in administrator PC.
2. Run this utility as the following screen appears.

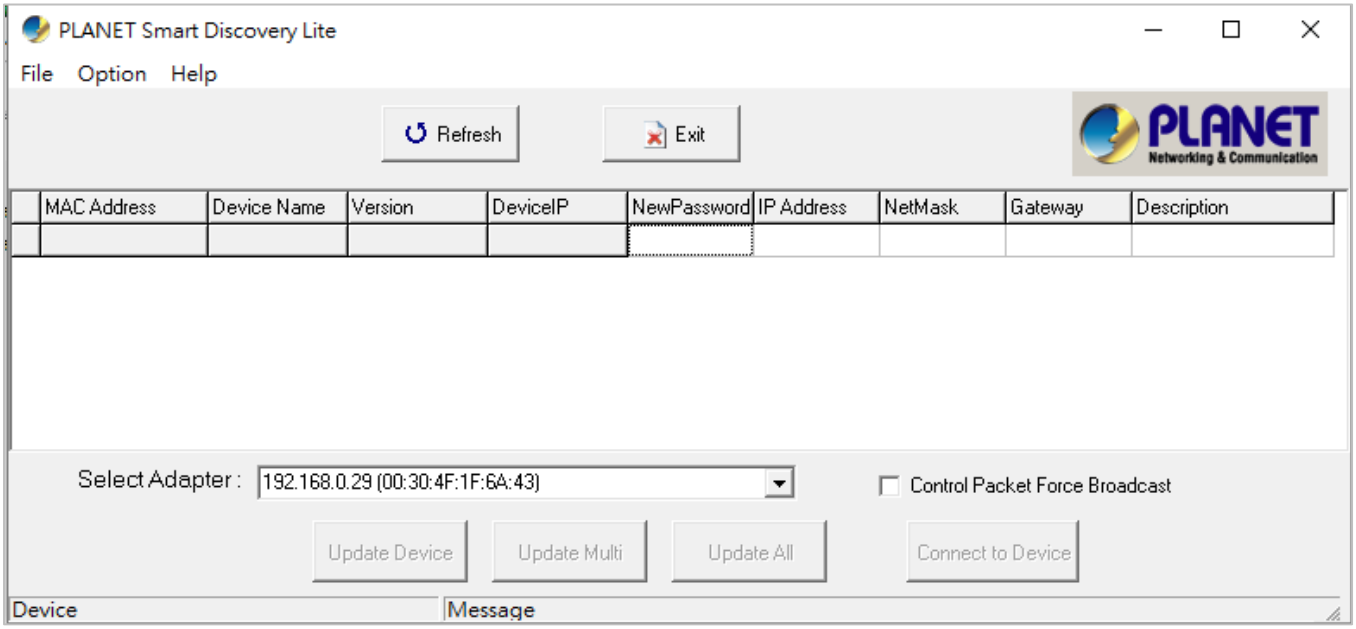


Figure 3-6: Planet Smart Discovery Utility Screen

Note

If there are two LAN cards or above in the same administrator PC, choose different LAN card by using the **"Select Adapter"** tool.

3. Press **"Refresh"** button for the currently connected devices in the discovery list as the screen shows below:

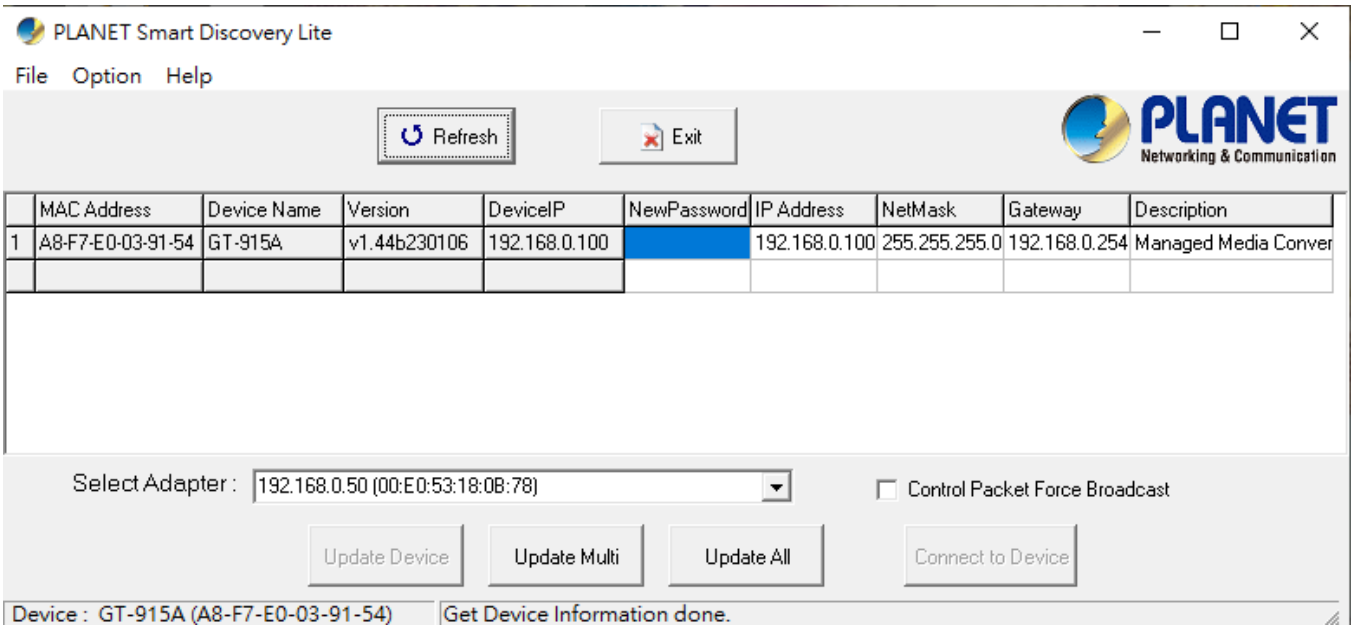


Figure 3-7: Planet Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC Address, Device Name, firmware version, and Device IP Subnet address. It can also assign new password, IP Subnet address and description for the devices.
2. After setup is completed, press **"Update Device"**, **"Update Multi"** or **"Update All"** button to take effect. The meaning of the 3 buttons above are shown as below:
   - **Update Device**: use current setting on one single device.
   - **Update Multi:** use current setting on choose multi-devices.
   - **Update All:** use current setting on whole devices in the list.

   The same functions mentioned above also can be found in **"Option"** tools bar.
3. To click the **"Control Packet Force Broadcast"** function, it can allow assign new setting value to the Web Smart Switch under a different IP subnet address.
4. Press **"Connect to Device"** button and the Web login screen appears in Figure 3-4.
5. Press **"Exit"** button to shut down the Planet Smart Discovery Utility.

4. WEB CONFIGURATION

This section introduces the configuration and functions of the Web-based management from Managed Media Converter.

About Web-based Management

The Managed Media Converter offers management features that allow users to manage the Managed Media Converter from anywhere on the network through a standard browser such as Microsoft Internet Explorer or Google Chrome.

The Managed Media Converter can be configured through an Ethernet connection, making sure the manager PC must be set on the same IP subnet address with the Managed Media Converter.

For example, the default IP address of the Managed Media Converter is ***192.168.0.100***, then the manager PC should be set at **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the Managed Media Converter to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.

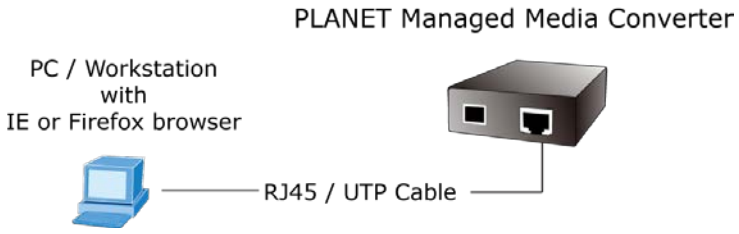


Figure 4-1: Web Management

- **Logging on the Managed Media Converter**

1. Use Internet Explorer 8.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address is shown as follows:

   http://192.168.0.100

2. When the following login screen appears, please enter the default username **"admin"** with password "**admin**" (or the username/password you have changed via console) to login the main screen of Managed Media Converter. The login screen in Figure 4-1-2 appears.

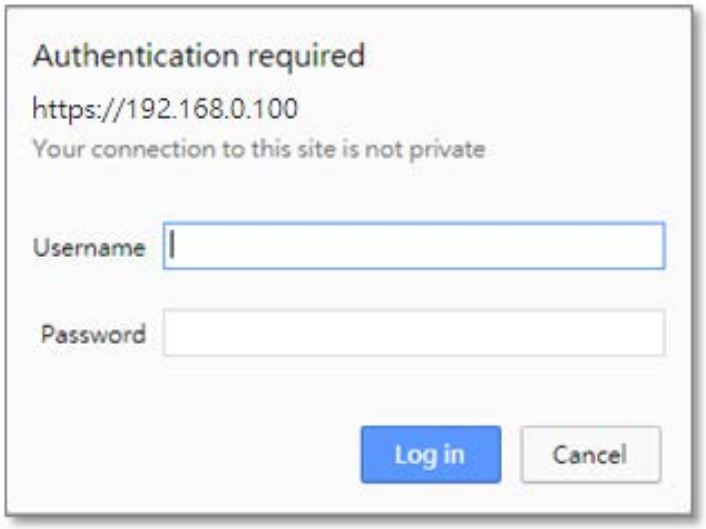


Figure 4-2: Login Screen

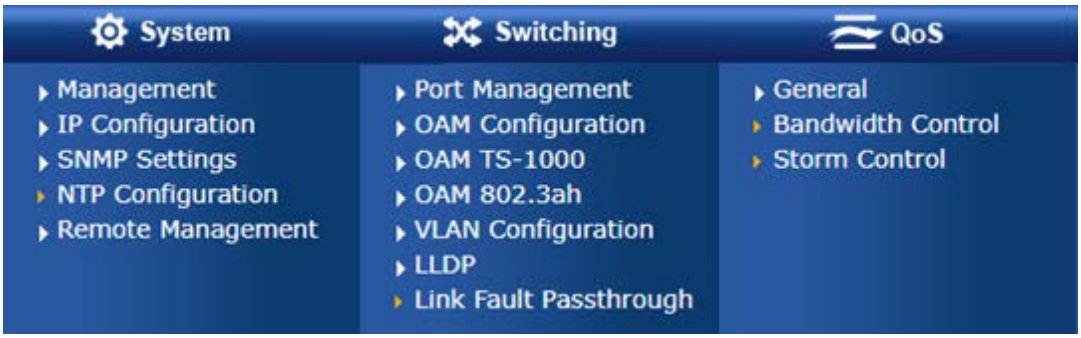
Default User name: **admin**

Default Password: **admin**

After entering the username and password, the main screen appears as shown in Figure 4-1-3.

Figure 4-3: Web Main Page

Now, you can use the Web management interface to continue the switch management or manage the Managed Media Converter by Web interface. The Switch Menu on the left of the web Page let you access all the commands and statistics the Managed Media Converter provides.



Note

1. It is recommended to use Chrome 98.0.xxx or above to access the Managed Media Converter.
2. The changed IP address take effect immediately after clicking the **Save** icon on the top Switch Menu bar. You need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.

4.1 Main Web Page

The Managed Media Converter provides a Web-based browser interface for configuring and managing it. This interface allows you to access the Managed Media Converter using the Web browser of your choice. This chapter describes how to use the Managed Media Converter's Web browser interface to configure and manage it.

Figure 4-4: Web Main Page

Panel Display

The web agent displays an image of the Managed Media Converter's ports. The Mode can be set to display different information for the ports, including Link up or Link down. The port status are illustrated as follows:

State	Disabled	Down	Link
RJ45 Ports			
SFP Ports			

System Hot Key Icons

The system hot keys icons are in the right side of the Managed Media Converter's web page, from left to right side is System Up Time, refresh button, save config button, reboot button and logout button.

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the Managed Media Converter, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the Managed Media Converter by selecting the functions those listed in the Main Function. The screen in Figure 4-1-5 appears.

Figure 4-5: Managed Media Converter Main Functions Menu

Device Information

Access Device Information web page, you can view device informations of the Managed Media Converter, the screen in Figure 4-6 appears and table 4-1-1 show the items of Device Information.

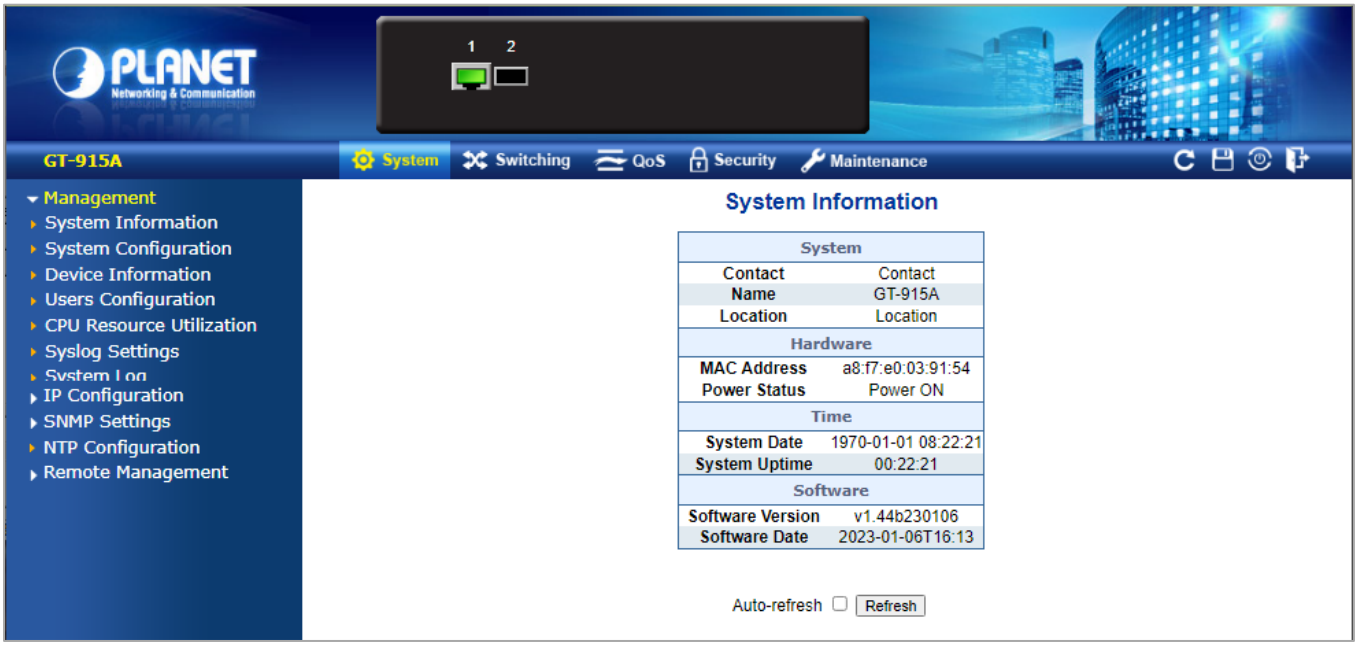


Figure 4-6: Managed Media Converter Device Information Web Page

Object	Description
• **Contact**	The system contact configured in SNMP | System Information | System Contact.
• **Name**	The system name configured in SNMP | System Information | System Name.
• **Location**	The system location configured in SNMP | System Information | System Location.
• **MAC Address**	The MAC Address of this **Managed Media Converter**.
• **Power Status**	The status of power input

• **System Date**	The current (GMT) system time and date. The system time is obtained through the configured NTP Server, if any.
• **System Uptime**	The period of time the device has been operational.
• **Software Version**	The software version of the **Managed Media Converter**.
• **Software Date**	The date when the **Managed Media Converter** software was produced.

Table 4-1-1: Item Desciptions of Device Information

4.2 System

Use the system menu items to display and configure basic administrative details of the Managed Media Converter. Under the system the following topics are provided to configure and view the system information. This section has the following items:

Access system web page, you can view system functions of the Managed Media Converter, the screen in Figure 4-7 appears and table 4-2-1 show the items of System.

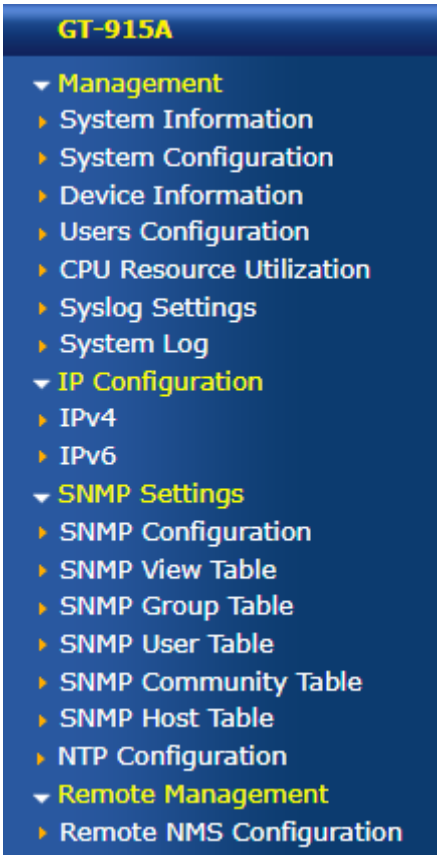


Figure 4-7: Managed Media Converter System Web Page

System Configuration	
Item	**Description**
System Information	The Managed Media Converter system information is provided here.
System Configuration	Configuration the Managed Media Converter's system information
Device Information	Device Information
User Configuration	Configure new user name and password on this page
CPU Resource Utilization	This page displays the CPU load, using an SVG graph.
Syslog Settings	Configure remote syslog on this page.
System Log	The system log information of the Managed Media Converter system is provided here.
IP Configuration	Configure the Managed Media Converter-managed IP4/IPv6 information on this

	page.
SNMP Settings	Configure the Managed Media Converter-SNMP functions on this web page.
NTP Configuration	Configure the Managed Media Converter-NTP function on this web page.
Remote Management	Configure the Planet NMS Configuration

Table 4-2-1: Item Desciptions of System Web Page

4.2.1 Management

4.2.1.1 System Information

The System Infomation Page provides information for the current device information. System Information Page helps a switch administrator to identify the hardware MAC address, firmware version and system uptime and also config the device name, comment, location and contact information. The screen in Figure 4-8 appears.

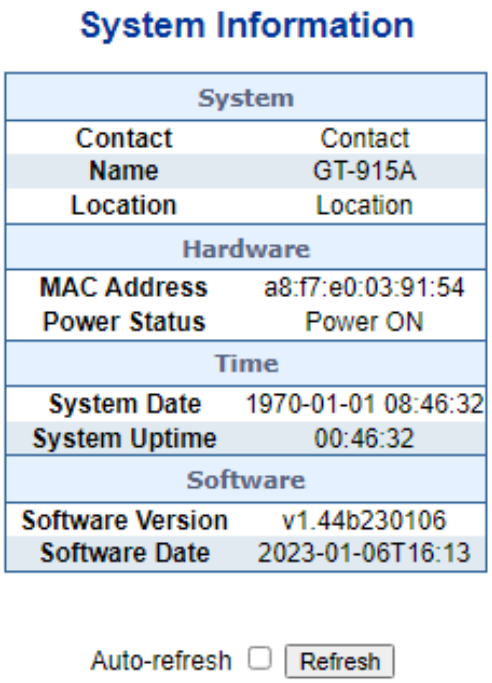


Figure 4-8: System Information Page Screenshot

The page includes the following fields:

Object	Description
• **Contact**	Display the current system contact
• **Name**	The system name configured in SNMP | System Information | System Name.
• **Location**	The system location configured in SNMP | System Information | System Location.
• **MAC Address**	The MAC Address of this **Managed Media Converter**.
• **Power Status**	The status of power input

• **System Date**	The current (GMT) system time and date. The system time is obtained through the configured NTP Server, if any.
• **System Uptime**	The period of time the device has been operational.
• **Software Version**	The software version of the **Managed Media Converter**.
• **Software Date**	The date when the **Managed Media Converter** software was produced.

Button

Apply: press this button to take affect.

4.2.1.2 System Configuration

Configure System informations on this page.

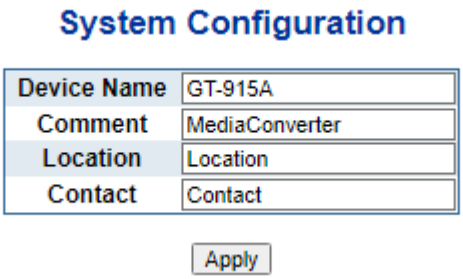


Figure 4-9: System Configuration Page Screenshot

The Current column is used to show the System Configuration.

Object	Description
• **Device Name**	Configured the system name.
• **Comment**	Define device's type.
• **Location**	The system location configured in SNMP | System Information | System Location.
• **Contact**	Display the current system contact

Button

Apply: press this button to take affect.

4.2.1.3 Device Information

Access Device Information web page, you can view device informations of the Managed Media Converter, the screen in Figure 4-10.

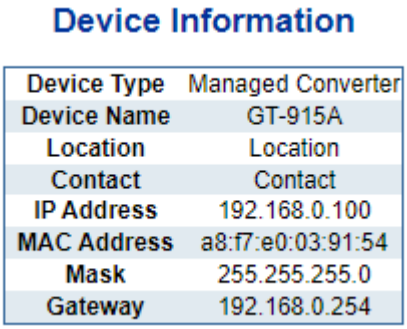


Figure 4-10: Device Information Page Screenshot

The page includes the following fields:

Object	Description
• **Device Type**	The type of the device.
• **Device Name**	The name of the device.
• **Location**	The system location configured in SNMP | System Information | System Location.
• **Contact**	Display the current system contact
• **IP Address**	The IP address of this Managed Media Converter.
• **MAC Address**	The MAC Address of this Managed Media Converter.
• **Mask**	The mask of this Managed Media Converter.
• **Gateway**	The gateway of this Managed Media Converter.

4.2.1.4 Users Configuration

The User configuration includes the User Name,Password and Confirm Password. The configured column is used to view or change the User Name and Password. The screen in Figure 4-9 appears.

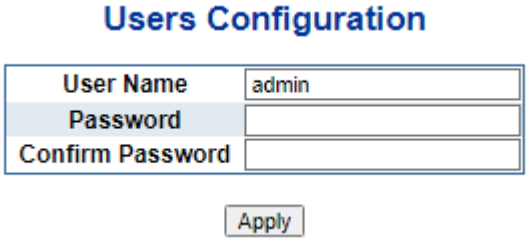


Figure 4-11: Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	The name identifying the user. This is also a link to Add/Edit User.
• **Password**	Enter the user's new password here. (Range: 0-32 characters plain text, case sensitive)
• **Confirm Password**	Please enter the user's new password here again to confirm.

Buttons

Add New User: Click to add a new user.

4.2.1.5 CPU Resource Utilization

This page allows you to view the CPU resource utilization of Managed Media Converter as the screen in Figure 4-12 appears.

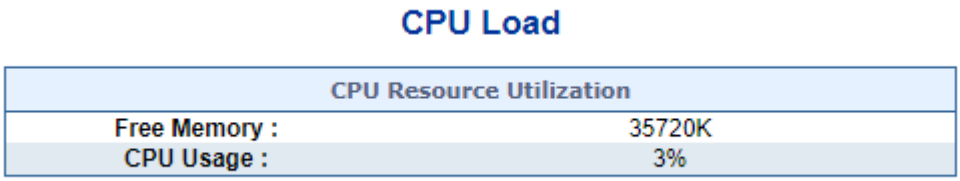


Figure 4-12: CPU Resource Utilization Page Screenshot

The page includes the following fields:

Object	Description
• **Free Memory**	This column provides displaying the free memory status.
• **CPU Usage**	This column provides displaying the CPU Usgae status.

4.2.1.6 Syslog Settings

The Syslog settings provide to set system log settings, the configured column is used to select the related settings of Syslog settings as the screen in Figure 4-13 appears.

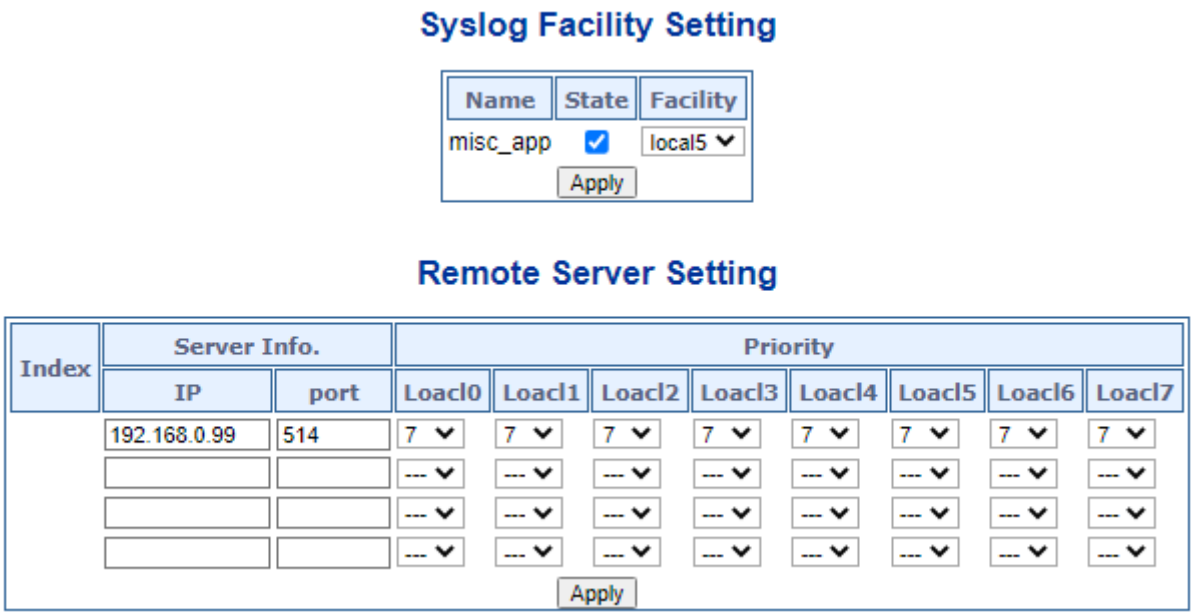


Figure 4-13: Syslog Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Syslog State**	Enable or disable the Syslog function.
• **Name**	Display the available protocol for facility setting on this page.
• **State**	Click to enable the available protocol for facility setting on this page.
• **Facility**	Selelct the local device number and the range is 0 to 7.
• **IP**	Input the IP address of remote server
• **Port**	The port number of remote server.
• **Priority**	Log priority range 0 to 7.

Button

Apply: press this button to take effect.

4.2.1.7 System Log

The Managed Media Converter system log information is provided here. The System Log screen in Figure 4-14 appears.

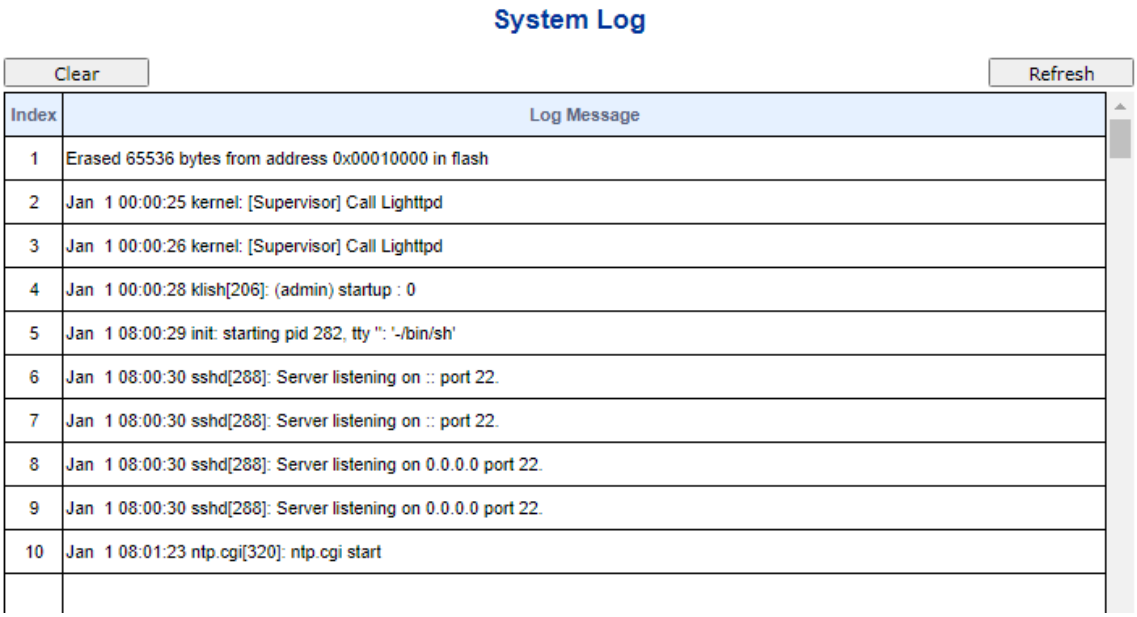


Figure 4-14: System Log Page Screenshot

The page includes the following fields:

Object	Description
• **Index**	This column provides displaying per index list.
• **Log Message**	This column provides displaying log message information of per index.

Button

Refresh: press this button to refresh current Syslog log message information.

4.2.2 IP Configuration

The IP configuration includes the IPv4 subnet address setting and IPv6 subnet address setting, the configured column is used to view or change the IP configuration.

4.2.2.1 IPv4

The IPv4 configuration includes the IPv4 Address, Subnet Mask, Default Gateway and DNS Server, also the DHCPv4 Client Enable function. The configured column is used to view or change the IPv4 Address, Subnet Mask, Default Gateway and DNS Server. Fill up the IPv4 Address, Subnet Mask and Default Gateway or enable the DHCPv4 Client function for the Managed Media Converter. The screen in Figure 4-15 appears.

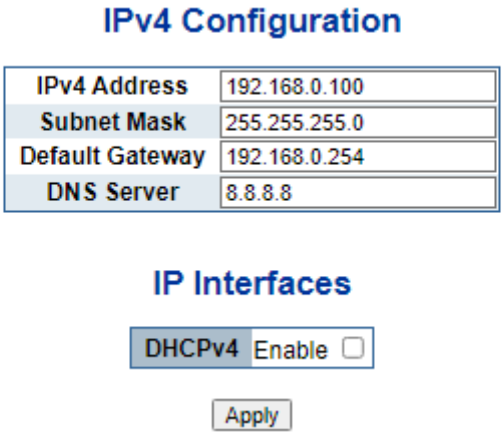


Figure 4-15: IPv4 Page Screenshot

4.2.2.2 IPv6

The IPv4 Configuration includes the IPv6 Address, Subnet Prefix Length, Default Gateway and DNS Server, also the DHCPv6 Client Enable function. The configured column is used to view or change the IPv6 Address, Subnet Prefix Length, Default Gateway and DNS Server. Fill up the IPv6 Address, Subnet Prefix Length and Default Gateway or enable the DHCPv6Client function for the Managed Media Converter. The screen in Figure 4-16 appears.

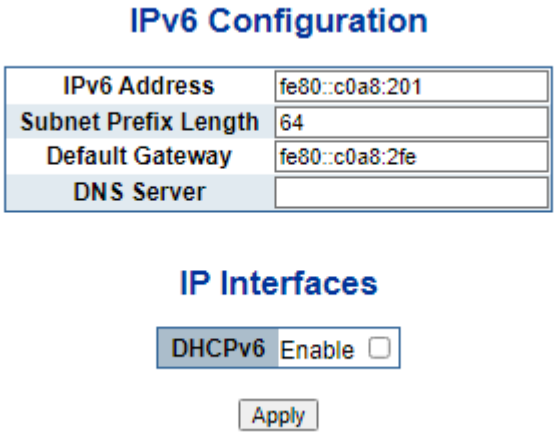


Figure 4-16: IPv6 Page Screenshot

Button

Apply: press this button to take affect.

4.2.3 SNMP Settings

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 Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of three key components: Network management stations (NMSs), SNMP agents, Management information base (MIB) and network-management protocol：

- **Network management stations (NMSs)：**Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents：**Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)：**A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **network-management protocol：**A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- **Get --** Allows the NMS to retrieve an object instance from the agent.
- **Set --** Allows the NMS to set values for object instances within an agent.
- **Trap --** Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- **Write** = private
- **Read** = public

Use the SNMP Menu to display or configure the Managed Media Converter's SNMP function. This section has the following items:

■ **SNMP Configuration**	Configure SNMP configuration on this web page.
■ **SNMP View Table**	Configure SNMP view table settings on this web page.
■ **SNMP Group Table**	Configure SNMP group settings on this web page.
■ **SNMP User Table**	Configure SNMP user table settings on this web page.
■ **SNMP Community Table**	Configure SNMP community table on this web page.
■ **SNMP Host Table**	Configure SNMP host table on this web page.

4.2.3.1 SNMP Configuration

The SNMP Host Table provides to set SNMP settings; the configured column is used to input the selected operation modes of SNMP State, SNMP Trap and SNMP Link Change Traps as the screen in Figure 4-17 appears.

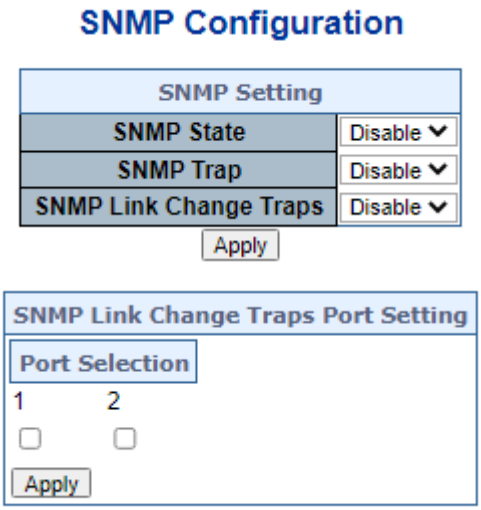


Figure 4-17: SNMP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **SNMP State**	Enable or Disable the Managed Media Converter SNMP function on this page.
• **SNMP Trap**	Enable or Disable the Managed Media Converter SNMP trap function on this page.
• **SNMP Link Change Traps**	Enable or Disable the Managed Media Converter SNMP Link Change trap function on this page.

Button

Apply: press this button to take effect.

4.2.3.2 SNMP View Table

The SNMP View Table provide to set view rules for allow or deny access to certain MIB objects, the configured column is used to input the view name, subtree OID and change the view type. The screen in Figure 4-18 appears.

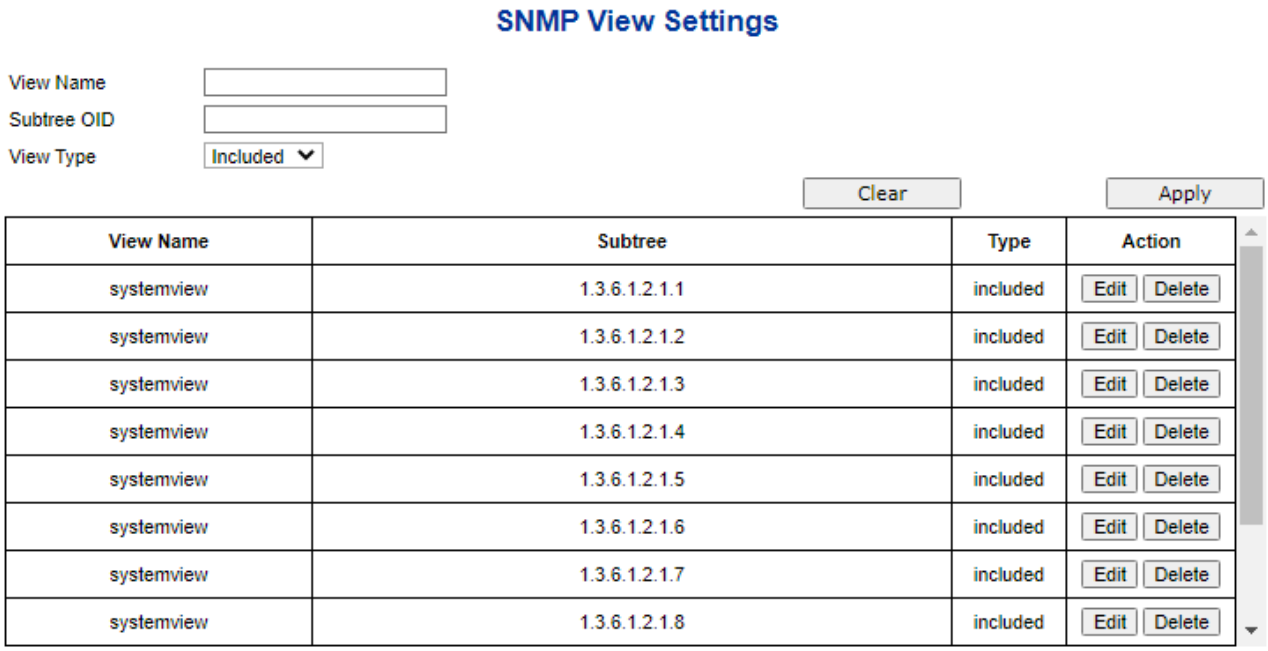


Figure 4-18: SNMP View Table Configuration Page Screenshot\

The Current column is used to show the SNMP View Table configuration.

Object	Description
• **View Name**	Configure the Managed Media Converter view name information on this web page, the maximum length is 20 characters.
• **Subtree OID**	Configure the Managed Media Converter Subtree OID information on this web page.
• **View Type**	Configure the Managed Media Converter view type mode on this web page, the available options are **Included** and **Excluded**.

Buttons

Apply: press this button to take affect.

Delete: press this button to delete.

Note

Each view need to configure a view rule, otherwise it will affect the SNMP function.

4.2.3.3 SNMP Group Table

The SNMP View Table provide to set SNMP Group settings, the configured column is used to input the group name, change the Read, Write, Notify view type and Security Model /Level. The screen in Figure 4-19 appears.

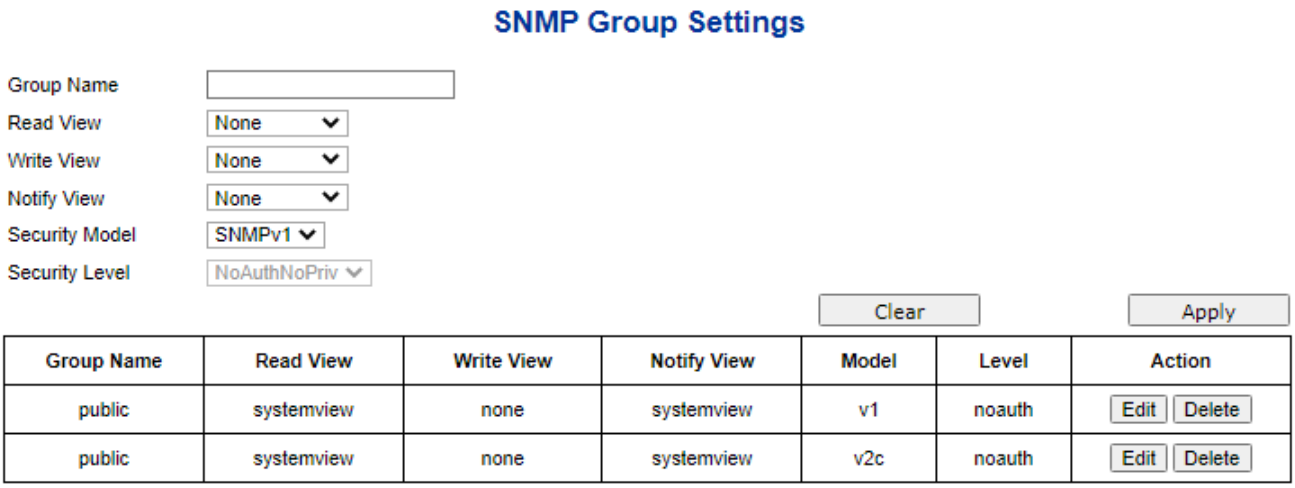


Figure 4-19: SNMP Group Table Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Group Name**	Configure the Managed Media Converter group name information on this page, the maximum length is 20 characters.
• **Read View**	Choose the Read View and available options are: ■ **None**: Set none for Read View status. ■ **systemview**: Set systemview for Read View status.
• **Write View**	Choose the Write View and available options are: ■ **None**: Set none for Read View status. ■ **systemview**: Set systemview for Write View status.
• **Notify View**	Choose the Notify View and available options are: ■ **None**: Set none for Read View status. ■ **systemview**: Set systemview for Notify View status.
• **Security Model**	Indicates the SNMP supported version. Possible versions are: ■ **SNMP v1**: Set SNMP supported version 1. ■ **SNMP v2**: Set SNMP supported version 2c. ■ **SNMP v3**: Set SNMP supported version 3.
• **Security Level**	Available when choose the SNMPv3 in Security Model. Possible versions are: ■ **NoAuthNoPriv**: None authentication and none privacy. ■ **AuthNoPriv**: Authentication and none privacy. ■ **AuthPriv**: Authentication and privacy.

Buttons

Apply: press this button to take affect.

Delete: press this button to delete.

Note

The SNMP group needs to create the view before group create.

4.2.3.4 SNMP User Table

The SNMP User Table provide to set SNMP user settings, the configured column is used to input the user name, select the group name and input the password for Auth-Protocol MD5 /Priv-Protocol DES. The screen in Figure 4-20 appears.

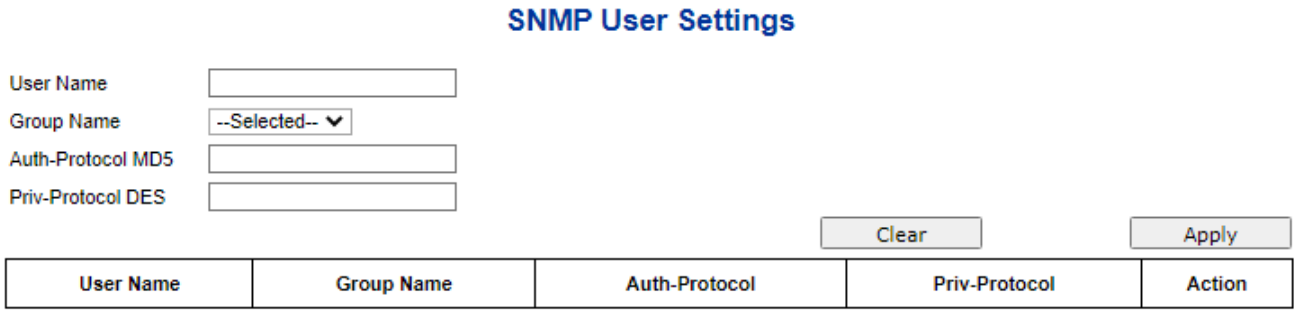


Figure 4-20: SNMP User Table Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	Configure the Managed Media Converter user name information on this page, the maximum length is 20 characters.
• **Group Name**	Select the exist SNMP group.
• **Auth-Protocol MD5**	Set the authorization password with using the MD5 authentication level, the available length is 8 to16 characters.
• **Priv-Protocol DES**	Set the authorization password with using the standard DES private encryption protocol, the available length is 8 to16 characters.

Buttons

Apply: press this button to take affect.

Delete: press this button to delete.

Note

Create SNMP views and groups are required to use, the security level of the user needs to be the same as the security level of the group.

4.2.3.5 SNMP Community Table

The SNMP User Table provides to set SNMP community settings; the configured column is used to input the community name, and select the group name for access group as the screen in Figure 4-21 appears.

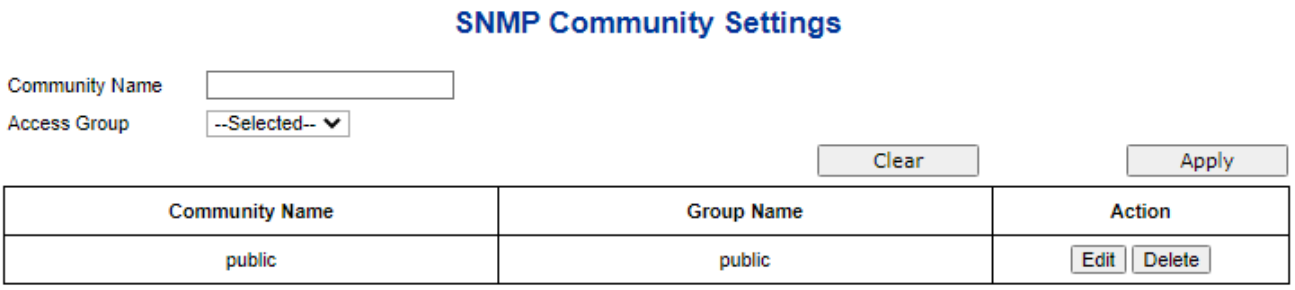


Figure 4-21: SNMP Community Table Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Community Name**	Configure the Managed Media Converter community name information on this page, the maximum length is 20 characters.
• **Access Group**	Select the exist access group.

Buttons

Apply: press this button to take effect.

Delete: press this button to delete.

4.2.3.6 SNMP Host Table

The SNMP Host Table provides to set SNMP host settings. The configured column is used to input the host IP address, and select the security model, security level and community string for SNMPv3 user as the screen in Figure 4-22 appears.

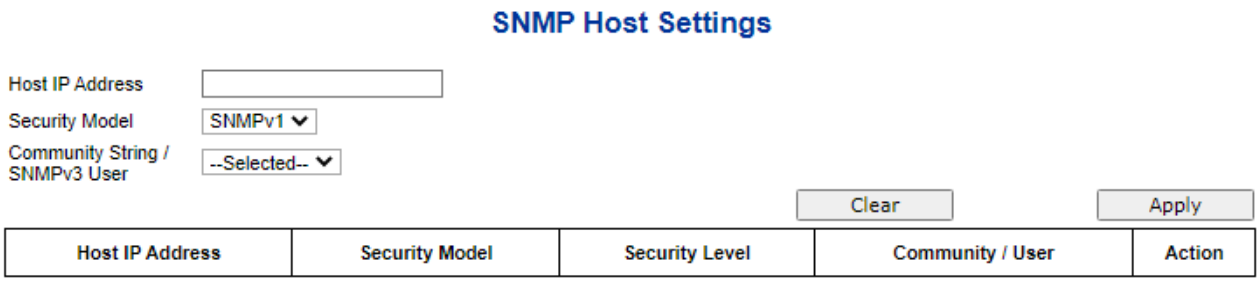


Figure 4-22: SNMP Host Table Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Host IP Address**	Configure the Managed Media Converter IPv4 Host Ip address on this page.
• **Security Model**	Indicates the SNMP supported version. Possible versions are: ■ **SNMP v1**: Set SNMP supported version 1. ■ **SNMP v2**: Set SNMP supported version 2c. ■ **SNMP v3**: Set SNMP supported version 3.
• **Security Level**	Available when choose the SNMPv3 in Security Model. Possible versions are: ■ **NoAuthNoPriv**: None authentication and none privacy. ■ **AuthNoPriv**: Authentication and none privacy. ■ **AuthPriv**: Authentication and privacy.
• **Community String/SNMPv3 User**	Select the exist community string for SNMPv3 user.

Button

Apply: press this button to take effect.

4.2.4 NTP Configuration

On this page. **NTP**, an acronym for **Network Time Protocol**, is for synchronizing the clocks of computer systems. NTP uses UDP (data grams) as transport layer. You can specify NTP Servers and set GMT time zone. The NTP configuration screen in Figure 4-23 appears.

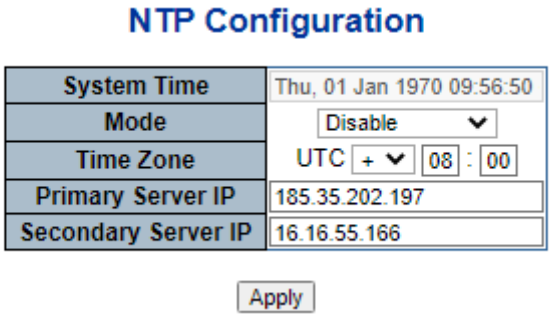


Figure 4-23: NTP Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **System Time**	Display current system time of Managed Media Converter.
• **State**	Indicates the NTP mode operation. Possible modes are: ■ **Enable**: Enable NTP mode operation. When enable NTP mode operation, the agent forward and to transfer NTP messages between the clients and the server when they are not on the same subnet domain. ■ **Disable**: Disable NTP mode operation.
• **Time Zone**	Allow selecting the time zone according to current location of Managed Media Converter.
• **Primary Server IP**	Configure the NTP server IPv4 IP address on this page.
• **Secondary Server IP**	Configure the NTP server IPv4 IP address on this page.

Button

Apply: press this button to take effect.

4.2.5 Remote Management

The Managed Media Converter can support both NMS contoleer and CloudViewer Sever for remote management. PLANET's **NMS Controller** is a Network Management System can monitor all kinds of deployed network devices, such as managed switches, media converters, routers, smart APs, VoIP phones, IP cameras, etc., compliant with the SNMP Protocol, ONVIF Protocol and PLANET Smart Discovery utility. The **CloudViewer** is a free networking service just for PLANET Products. This service provides simplified network monitoring and real-time network status. Working with PLANET CloudViewer app, user can easily check network status, device information, Port and PoE status from Internet. Any other services are not included.

The Remote NMS Configuration screens in Figure 4-24 appear.

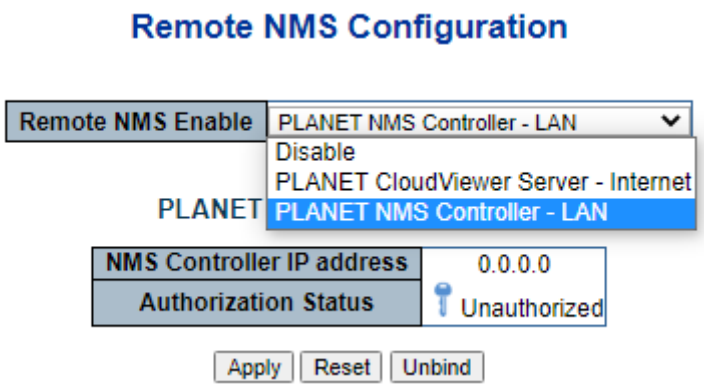


Figure 4-24: Fault Alarm Control Configuration Page Screenshot

The NMS Controller – LAN Configuration screens in Figure 4-25 appear.

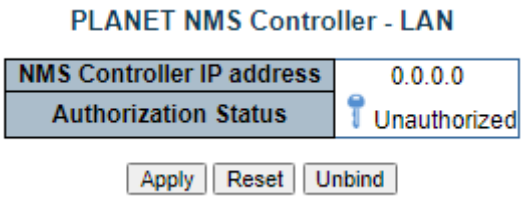


Figure 4-25 NMS Controller – LAN Configuration Page Screenshot

Object	Description
• **Remote NMS Enable**	Enable NMS management
• **NMS Controller IP address**	The IP address of NMS Controller
• **Authorization Status**	Indicate the authorization status of the switch to NMS Controller

The CloudViewer Server – Internet screens in Figure 4-26 appear.

Figure 4-26 CloudViewer Server – Internet Configuration Page Screenshot

Object	Description
• **Remote NMS Enable**	Enable NMS management
• **Subscriber email**	The email registered on CloudViewer Server
• **Password**	The password of your CloudViewer account
• **Status**	Indicate the status of connecting CloudViewer Server

4.3 Switching

On the Access Basic configuration web page, you can view Port management function informations of the Managed Media Converter as the screen in Figure 4-27 appears.

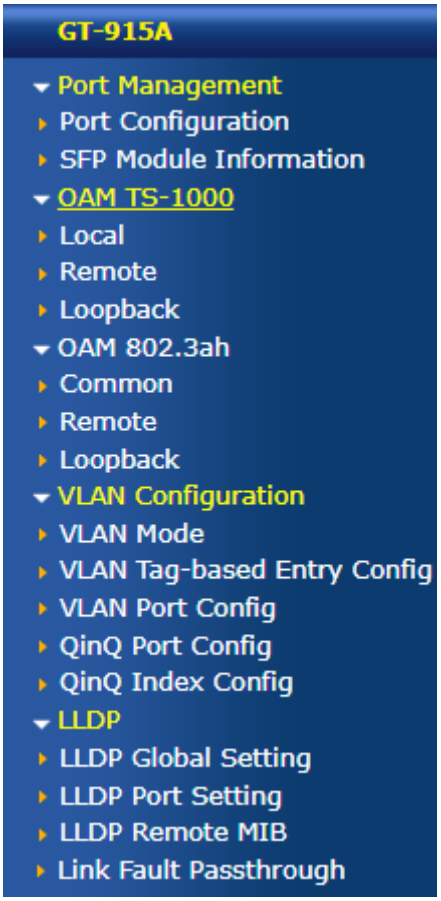


Figure 4-27: Managed Media Converter Basic Configuration Web Page

Basic Configuration	
Item	**Description**
Port Configuration	Display and configure per Port configuration settings.
SFP Module Information	Display SFP Module information
OAM TS-1000	Display and configure OAM TS-1000 function.
OAM 802.3ah	Display and configure OAM 802.3ah function.
VLAN Configuration	Display and configure VLAN function.
LLDP	Display and configure LLDP function.

Table 4-28: Descriptions of Basic Configuration

4.3.1 Port Management

4.3.1.1 Port Configuration

This page displays current port configurations and each port can also be configured here as the Port configuration screen in Figure 4-29 appears.

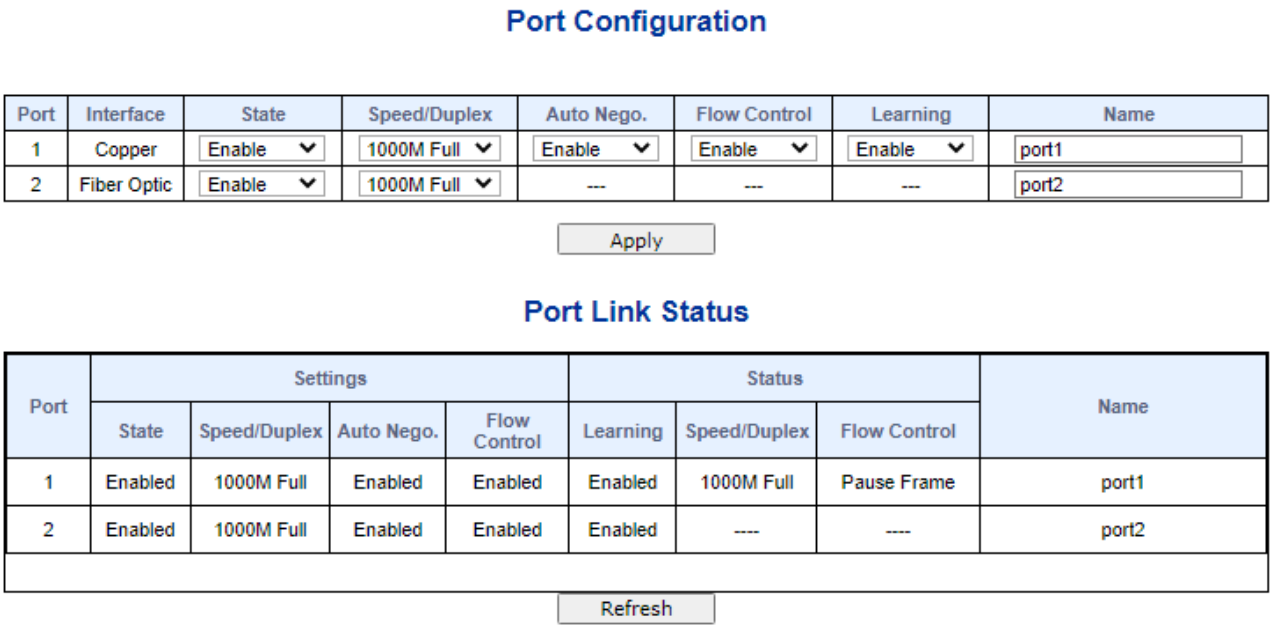


Figure 4-29 : Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Display per port list.
• **Interface**	Select specific port for further configuration.
• **State**	Enable or disable specific Port function.
• **Speed/Duplex**	Change specific Port speed duplex and the available optios are shown below: Top Speed/10M Half/10M Full/100M Half/100M Full/1000M Full.
• **Auto Negotiation**	Enable or disable auto negotiation function on specific Port.
• **Flow Control**	Enable or disable flow control function on specific Port.
• **Learning**	Display per port current learning setting mode.
• **Name**	Configure the Managed Media Converter per port description information on this page; the maximum length is 20 characters.

Buttons

Apply **: press this button to take effect.**

Refresh **: press this button to refresh information.**

4.3.1.2 SFP Module Information

This page shows the operational status, such as the transceiver type, speed, wavelength, optical output power, optical input power, temperature, laser bias current and transceiver supply voltage in real time. The SFP Module Information page is shown in Figure 4-30.

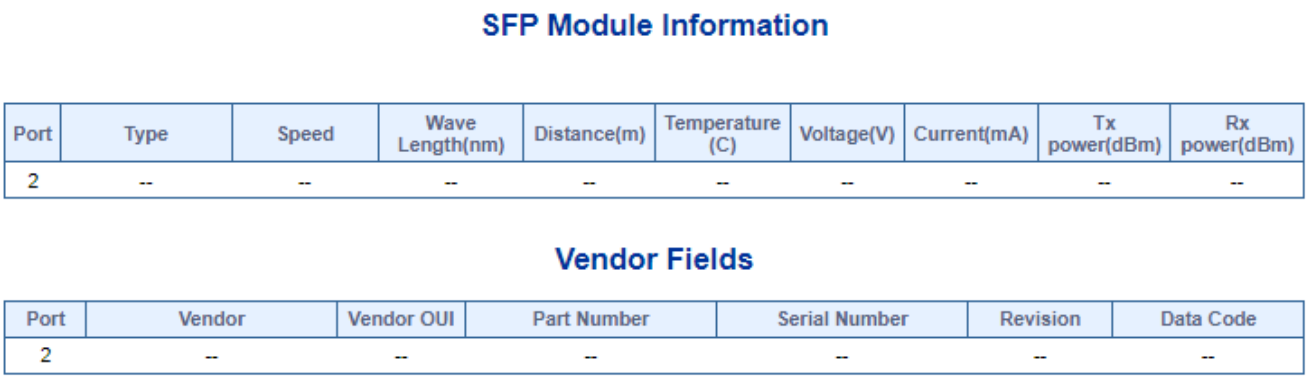


Figure 4-30: SFP Module Information

Object	Description
• **Port**	Display per port list.
• **Type**	Display the type of current SFP module; the possible types are: ■ 1000BASE-SX/LX ■ 100BASE-TX
• **Speed**	Display the speed of current SFP module; the speed value or description is obtained from the SFP module. Different vendors SFP modules might show different speed information.
• **Wave Length(nm)**	Display the wavelength of current SFP module; the wavelength value is obtained from the SFP module. Use this column to check if the wavelength values of two nodes match while the fiber connection fails.
• **Distance (m)**	Display the support distance of current SFP module; the distance value is obtained from the SFP module.
• **Temperature (C)** **– SFP DDM Module Only**	Display the temperature of current SFP DDM module; the temperature value is gotten from the SFP DDM module.
• **Voltage (V)** **– SFP DDM Module Only**	Display the voltage of current SFP DDM module; the voltage value is gotten from the SFP DDM module.
• **Current (mA)** **– SFP DDM Module Only**	Display the ampere of current SFP DDM module; the ampere value is gotten from the SFP DDM module.
• **TX power (dBm)** **– SFP DDM Module Only**	Display the TX power of current SFP DDM module; the TX power value is gotten from the SFP DDM module.
• **RX power (dBm)** **– SFP DDM Module Only**	Display the RX power of current SFP DDM module; the RX power value is gotten from the SFP DDM module.

4.3.2 OAM TS-1000

4.3.2.1 Local OAM TS-1000 Configuration

This function provides Local TS-1000 OAM Setup of Managed Media Converter. Press the **"Apply"** button to save the current configuration of Managed Media Converter. The screen in Figure 4-35 appears and Table 4-13 describes the Local TS-1000 OAM Setup object of Managed Media Converter.

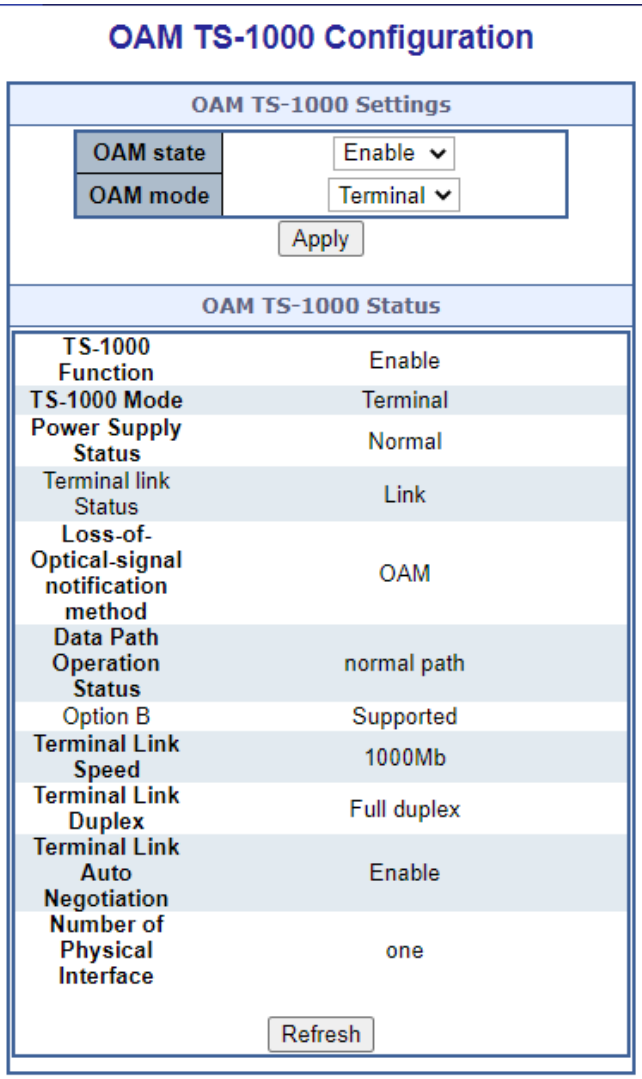


Figure 4-31 Local TS-1000 OAM Setup Web Page screen

The Local TS-1000 OAM Setup Web page includes the following configurable data:

Object	Description
• **TS-1000 OAM State**	Provide disable or enable the TS-1000 OAM operation mode. Default mode is Disable
• **TS-1000 Mode**	Provide two TS-1000 modes for operation, the available options are: Terminal Center Default mode is Terminal.

• **Link Transparent**	Provide disable or enable the Link Transparent function. Default mode is Disable.
• **Link Transparent Result**	Display the link transparent result.
• **Apply button**	Press this button for save current configuration of Managed Media Converter.

Table 4-32 Descriptions of the Local TS-1000 OAM Setup Web Page Screen Objects

4.3.2.2 Remote OAM TS-1000 Configuration

The Remote TS-1000 OAM Setup is an advanced remote device monitor feature that allows you to Remote monitor and automatic notify status indication.

Remote monitor

1. User instructs center Media Converter to issue a status notification request frame defined in TS-1000 to get status of terminal Media Converter.
2. Terminal Media Converter receives the status notification request frame and sends out status response frame, which carries its current status.

Autonomous notification

1. Terminal Media Converter notifies the center Media Converter autonomously with a status notification indication, if any change occurs in the status monitored internally by the terminal Media Converter.
2. Center Media Converter if support Option A, notifies the terminal Media Converter autonomously with a status notification indication, if any change occurs in the status monitored internally by the center Media Converter.

This function provides Remote TS-1000 OAM Setup of Managed Media Converter. Press the **"Apply"** button to save the current configuration of Managed Media Converter. The screen in Figure 4-33 appears.

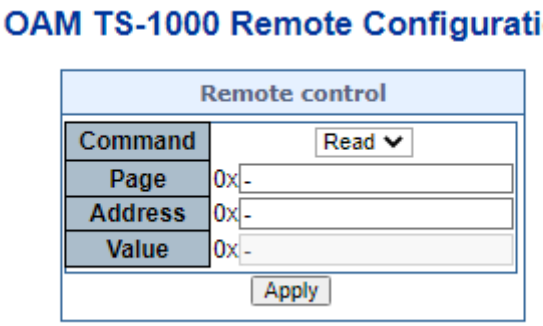
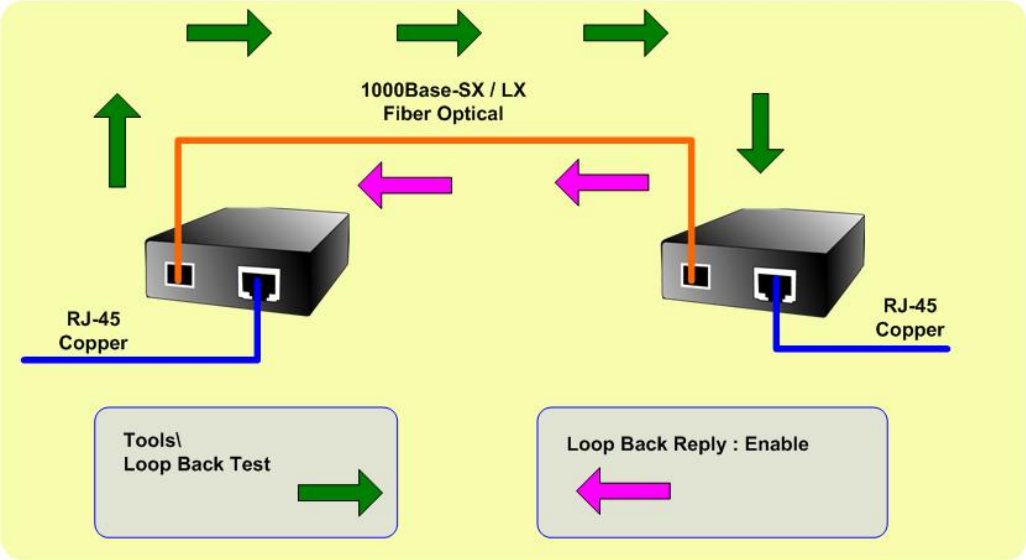


Figure 4-33 GT-915A Remote TS-1000 OAM Setup Web Page screen

Notice: Please use the PLANET GST-80x and GT-91x as the Remote device.

4.3.2.3 OAM TS-1000 Loop Back

The TS-1000 Loop Back Test allows manual run this loop back test to check the interconnection between two Media Converter devices. To assure the Remote TS-1000 OAM function can work correctly.



In-band and out-band Loop back

1. Instruct center Media Converter to issue an OAM frame to request a loop back test. Terminal return start response OAM frame to center Media Converter.

2. Terminal Media Converter runs at loop back mode.

3. Central Media Converter send test frame and terminal Media Converter loop back the frames. Test frame can be generated from central Media Converter's UTP port (Out-Band) or from central Media Converter (In-Band) automatically.

4. Center Media Converter check the loop back test result after sending all test frames

5. Instruct the central Media Converter to end loop back test.

This function provides TS-1000 Loop Back Test of Managed Media Converter. Press the **"Apply"** button to run Loop Back Test and see the TS-1000 Loop Back Test Result of Managed Media Converter, also press the **"Refresh"** button to renew the Web screen. The screen in Figure 4-34 appears and Table 4-35 describes the TS-1000 Loop Back Test object of Managed Media Converter.

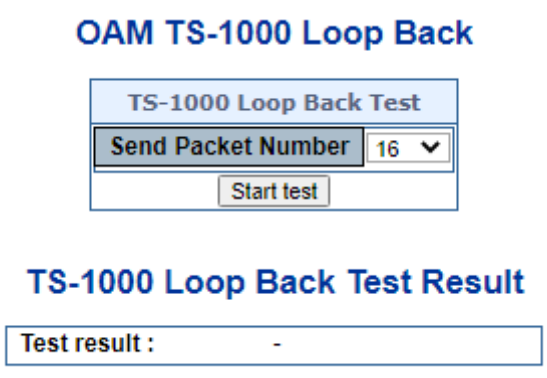


Figure 4-34 Remote TS-1000 Loop Back Test Web Page screen

The TS-1000 Loop Back Test Web page includes the following configurable data:

Object	Description
TS-1000 Loop Back Test	
Send Packet Number	Allow input the number for packet send and the available options is 1 to 255. Default is 16.
Apply button	Press this button for save current configuration of Managed Media Converter.
Refresh button	Press "Refresh" button to refresh current status.
TS-1000 Loop Back Test Result	
Result	Display the TS-1000 Loop Back Test Result. Fail or Pass.
Result counter	Display the value of Counter Result.

Table 4-35 Descriptions of the TS-1000 Loop Back Test Web Page Screen Objects

Notice: Please use the PLANET GST-80x and GT-91x as the Remote device.

4.3.3 OAM 802.3ah

4.3.3.1 Common OAM 802.3ah Configuration

When enable 802.3ah OAM function, all 802.3ah OAMPDU packets will trap to embedded CPU.
Software will implement auto discovery procedure. With hardware support, software controls the 802.3ah remote loop back procedure. Hardware can also detect dying gasp even and interrupt CPU to send dying gasp even notification OAMPDU. All other functions defined by 802.3ah are implemented using embedded CPU.

When remote device is in loop back mode, hardware can support change looped test frame's DA, SA or both as user defined. Hardware can also set to don't change looped test frame.

This function provides 802.3ah Setup of Managed Media Converter. Press the **"Apply"** button to save the current configuration of Managed Media Converter. The screen in Figure 4-36 appears and Table 4-37 describes the 802.3ah Setup object of Managed Media Converter.

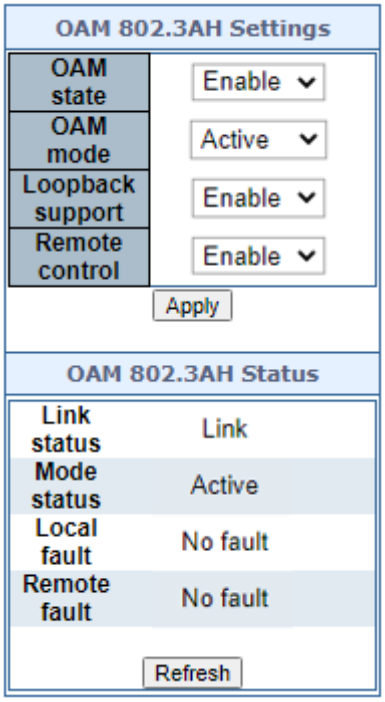


Figure 4-36 802.3ah Setup Web Page screen

The 802.3ah Setup Web page includes the following configurable data:

Object	Description
802.3ah OAM State	Provide disable or enable the 802.3ah OAM State function. Default mode is Enable.
802.3ah OAM Mode	Allow to choose **"Active"** or **"Passive"** for 802.3ah OAM Mode. Default mode is **Passive**.
Loopback Reply	Provide disable or enable the Loopback Reply function. Default mode is **Enable**.
Remote OAM Configure	Provide disable or enable the Remote OAM Configure function. Default mode is **Enable**.
Remote OAM Configuration Result	Display the Remote OAM Configuration Result.
Apply button	Press this button for save current configuration of Managed Media Converter.

Table 4-37 Descriptions of the 802.3ah Setup Web Page Screen Objects

Notice:

1. The 802.3ah function must work with manageable device that supports 802.3ah function.
2. Please use the PLANET GT-90x as the Remote device.

4.3.3.2 Remote OAM 802.3ah Configuration

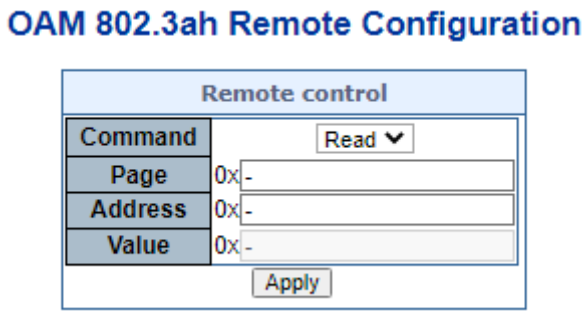
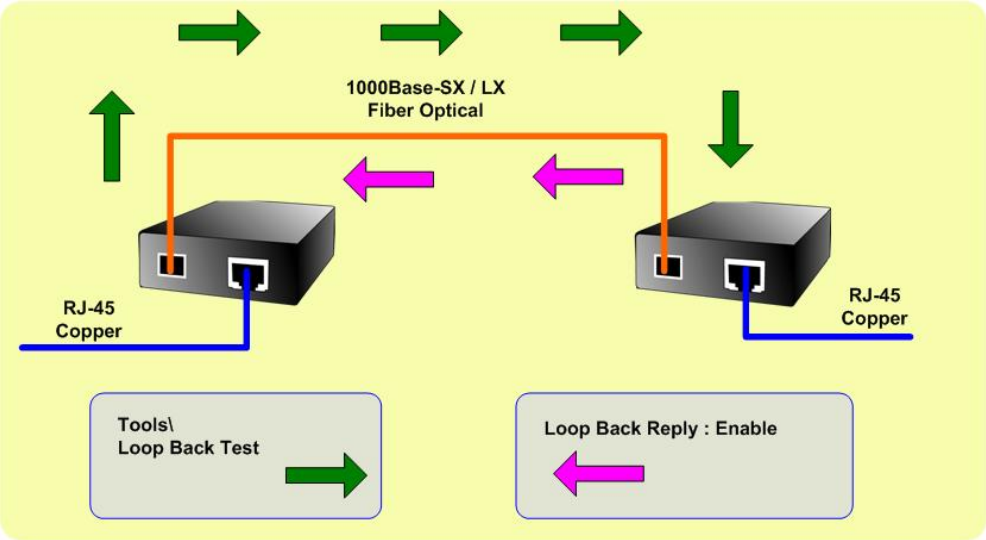


Figure 4-37 802.3ah Setup Web Page screen

4.3.3.3 OAM 802.3ah Loop Back

The 802.3ah Loop Back Test allows manual run this loop back test to check the interconnection between two Media Converter devices. To assure the Remote 802.3ah function can work correctly.



This function provides 802.3ah Loop Back Test of Managed Media Converter. Press the **"Apply"** button to run 802.3ah Loop Back Test and see the 802.3ah Loop Back Test Result of Managed Media Converter, also press the **"Refresh"** button to renew the Web screen. The screen in Figure 4-38 appears and Table 4-39 describes the 802.3ah Loop Back Test object of Managed Media Converter.

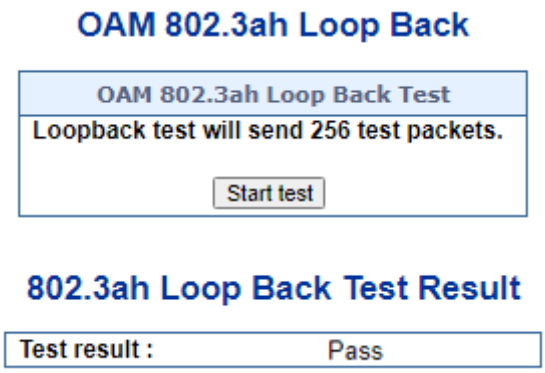


Figure 4-38 802.3ah Loop Back Test Web Page screen

The 802.3ah Loop Back Test Web page includes the following configurable data:

Object	Description
802.3ah Loop Back Test	
Send Packet Number	Allow input the number for packet send and the available options is 1 to 255. Default is **16**.
Packet Length (Not include CRC)	Allow input the number for Packet Length and the available options is 60 to 1514. Default is **60**.
Apply button	Press this button for save current configuration of Managed Media Converter.
Refresh button	Press **"Refresh"** button to refresh current status.
802.3ah Loop Back Test Result	
Result	Display the 802.3ah Loop Back Test Result. Fail or Pass.

Table 4-39 Descriptions of the 802.3ah Loop Back Test Web Page Screen Objects

Notice:

1. The 802.3ah function must work with manageable device that supports 802.3ah function.
2. Please use the PLANET GT-90x as the Remote device.

4.3.4 VLAN Configuration

4.3.4.1 VLAN Overview

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 collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

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 logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Note

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLANs.
2. The Managed Media Converter supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

Note

The Managed Media Converter 's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_ VLAN port member list. The DEFAULT_VLAN has a VID = 1.

On the Access VLAN configuration web page, you can view VLAN management function information of the Managed Media Converter as the screen in Figure 4-40 appears.

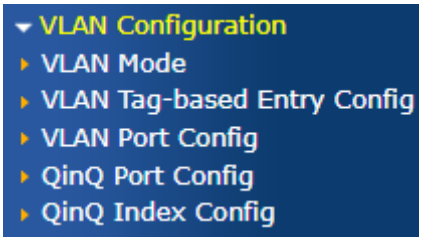


Figure 4-40: Managed Media Converter VLAN Configuration Web Page

VLAN Configuration	
Item	**Description**
VLAN Mode	Configure VLAN Mode configuration settings on this web page.
VLAN Tag-based Entry Config	Display and configure VLAN Tag-based Entry Config function on this web page.
VLAN Port Config	Display and configure VLAN Port Config function on this web page.

QinQ Port Config	Display and configure QinQ Port Config function on this web page.
QinQ Index Config	Display and configure QinQ Index Config function on this web page.

Table 4-41: Descriptions of VLAN Configuration

4.3.4.2 IEEE 802.1Q VLAN

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This Managed Media Converter provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This Managed Media Converter supports the following VLAN features:

- Up to 26 VLANs based on the IEEE 802.1Q standard
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

IEEE 802.1Q Standard

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLAN allows a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either **tagging** or **untagging**.:

- The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.
- The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

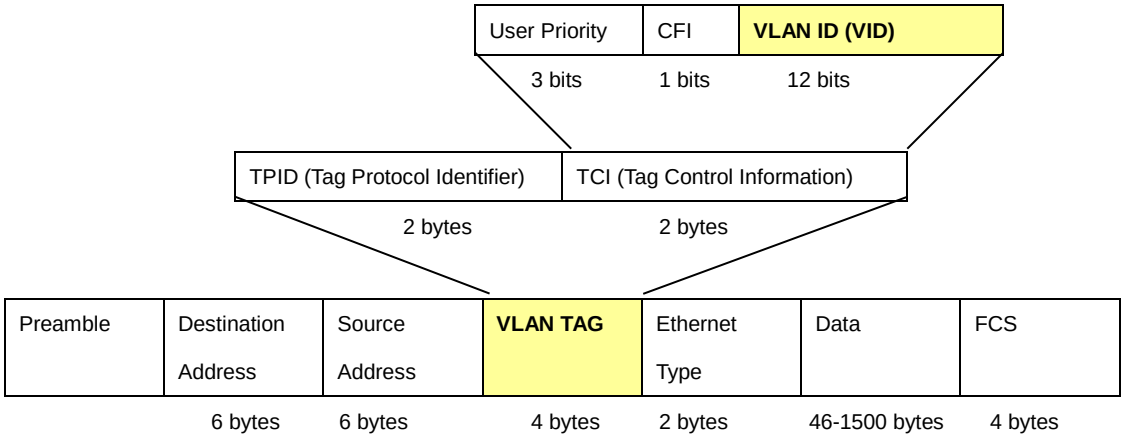
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of **0x8100** in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of **VLAN ID (VID)**. The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

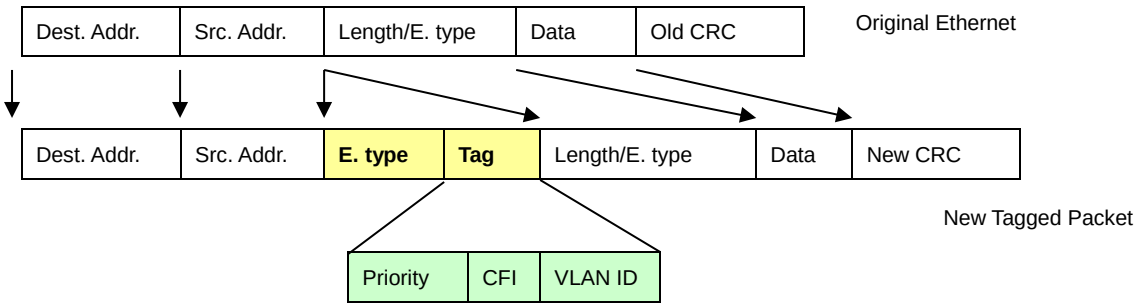
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag



Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLAN are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VID as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called **"Default."** The factory default setting assigns all ports on the Switch to the **"Default"**. As new VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

4.3.4.3 VLAN Mode

The VLAN Mode Page provide VLAN Mode configuration supported by the Managed Media Converter as the VLAN Mode screen in Figure 4-42 appears.

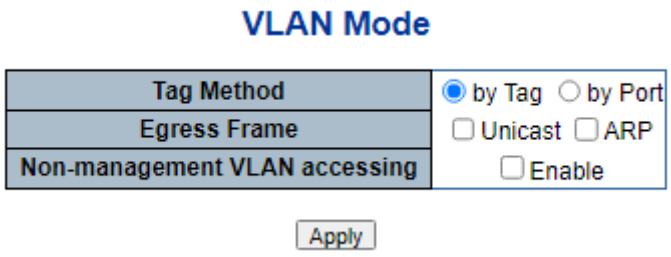


Figure 4-42: VLAN Mode Configuration Page Screenshot

The Page includes the following fields:

Object	Description
• **VLAN Mode**	Display the current VLAN mode used by this Managed Media Converter. ■ **Tag VLAN** determines the VID of each entry and those ports are VLAN members of which VLAN based on the settings of the Tag-based Entry. ■ **Group VLAN** determines which port in each group is its VLAN member based on the settings of the Group-based Entry.
• **Tag Method**	This option only available in Tag VLAN mode. ■ **By Tag-** whether packet sent out add/remove tag is judged on the basis of the value set by the port in the Tag-based entry. ■ **By Port-**whether the port sent out the packet add/remove tag is judged by the tagging value set by the port in the VLAN port config web page
• **Egress Frame**	It could connect the selected packet type via engress rule to transport between different VLAN groups. The available options are shown below: Unicast ARP

Button

Apply: press this button to take effect.

4.3.4.4 VLAN Tag-based Entry Config

Use the VLAN Tag-based entry config to configure port members function for the selected VLAN index. The VLAN Tag-based Entry config configuration can be monitored and modified here. Up to 26 VLANs are supported. This page allows for adding and deleting VLANs as well as configure port members function of each VLAN as the VLAN Tag-based Entry Config screen in Figure 4-43 appears.

Figure 4-43: VLAN Tag-based Entry Config Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Name**	Display the name of specific VLAN group.
• **Static**	Display the state of specific VLAN group.
• **VID**	Display the VLAN ID of specific VLAN group.
• **Don't care**	Display the per port Don't care information of specific VLAN group.
• **Add Tag**	Display the per port Add Tag state of specific VLAN group.
• **Remove Tag**	Display the per port Remove Tag state of specific VLAN group.
• **Forbidden**	Display the per port Forbidden state of specific VLAN group.
• **Priority**	Display the Priority state of specific VLAN group.
• **Action**	Edit: press this button to edit specific VLAN group. Delete: press this button to delete specific VLAN group.

Buttons

Add: press this button to create a new specific VLAN group.

Edit: press this button to edit specific VLAN group.

Delete: press this button to delete specific VLAN group.

Press the Edit button to edit per member port state and the screen in Figure 4-44 appears.

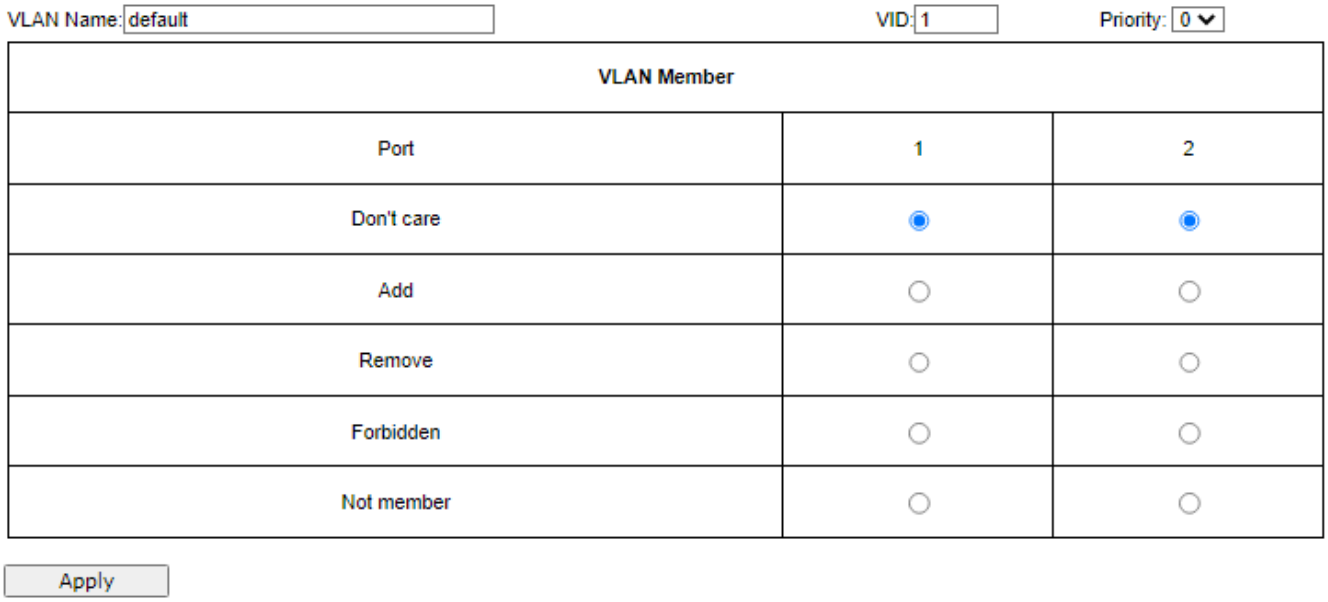


Figure 4-44: Edit VLAN Tag-based Entry Config Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN Name**	Display and configure the name of specific VLAN group; the maximum length is 20 characters.
• **VID**	Display and configure the VLAN ID of specific VLAN group.
• **Priority**	Display and configure the Priority value of specific VLAN group.
• **Port**	Display per port list of Managed Media Converter.
• **Don't care**	As a VLAN member of specific VLAN group without any action.
• **Add**	As a VLAN member, add the Tag action to the packet sent out by this port.
• **Remove**	As a VLAN member, remove the Tag action to the packet sent out by this port.
• **Forbidden**	Configure that this port cannot register this Tag VLAN dynamically through GVRP.
• **Not Member**	Not a member of the VLAN.

Button

Apply: press this button to take effect.

GVRP (GARP VLAN Registration Protocol) maintains VLAN dynamic registration information for GVRP devices based on the working mechanism of GARP to maintain VLAN dynamic registration information that supports GVRP devices.

And propagate this information to other devices in order to achieve agreement on VLAN information for all devices supporting GVRP in the same LAN.

The VLAN registration information propagated by GVRP includes both local manual static registration information and dynamic registration information from other switches.

4.3.4.5 VLAN Port Config

This page is used for configuring the Managed Media Converter port VLAN. The VLAN per port configuration page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN port configuration page. All untagged packets arriving to the device are tagged by the ports PVID.

Understanding Nomenclature of the Switch

IEEE 802.1Q Tagged and Untagged

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

- **Tagged:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping 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.
- **Untagged:** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Frame Income / Frame Leave	Income Frame is **tagged**	Income Frame is **untagged**
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remains untagged

Table 4-45: Ingress / Egress Port with VLAN VID Tag / Untag table

The VLAN Port configuration screen in Figure 4-46 is shown below.

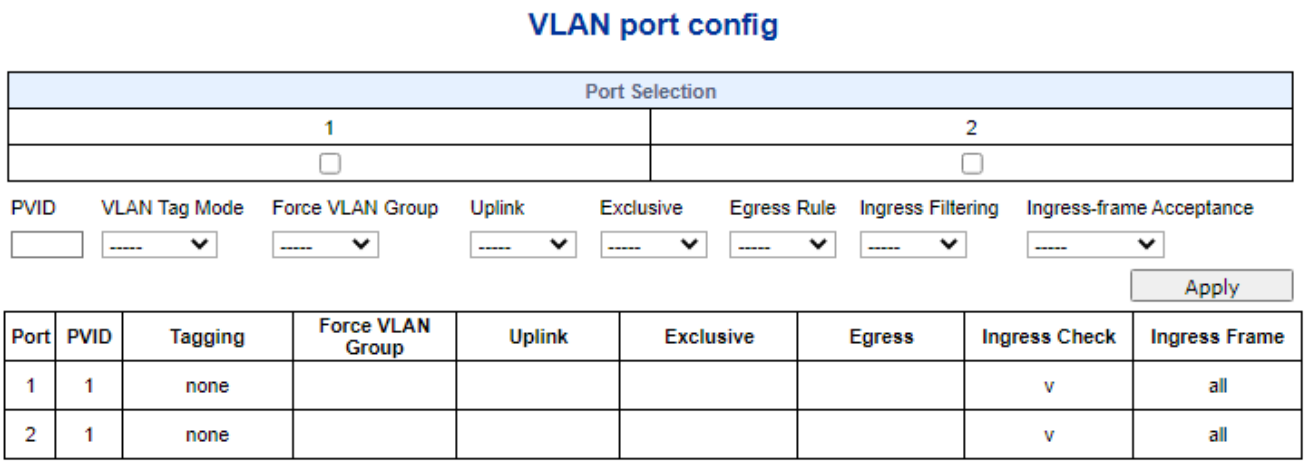


Figure 4-46 : VLAN Port Config Configuration Page Screenshot

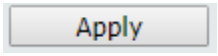
The page includes the following fields:

Object	Description
• **Port Selection**	Select specific port for VLAN settings.
• **PVID**	Allow assigned PVID for selected port. The range for the PVID is 1-4094. The PVID will be inserted into all untagged frames entering the ingress port. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.
• **Tagging**	Set whether VLAN Tag is added or removed from the packet sent out by selected port. The available options are **"Add"**, **"RMV"** and **"None"**.
• **Force VLAN Group**	Whether or not to set priority according to the group VLAN setting for the action.
• **Uplink**	Set up the Uplink port, which automatically sends the packet out of the Uplink Port when the destination Port is not the same as the VLAN.
• **Exclusive**	Enable or disable the exclusive function on specific port, the exclusive port unable to transfer packets.
• **Egress**	Enable or disable the exgress function on specific port, when the destination port of the packet is not in the same VLAN, it can still be transmitted to the destination port via the egress rule.
• **Ingress-Check**	Enable or disable the ingress check function, check whether port is member of this VLAN through VID.
• **Ingress-Frame Acceptance**	Setting allows the specified frame to do the forwarding action. The available options are **"Tag-Frame"** and **"All"**.
• **Port**	Display per port list.
• **PVID**	Display per port PVID information.
• **Tagging**	Display per port Tagging information.
• **Force VLAN Group**	Display per port Force VLAN Group information.
• **Uplink**	Display per port Uplink information.

• **Exclusive**	Display per port Exclusive information.
• **Egress**	Display per port Egress information.
• **Ingress Check**	Display per port Ingress Check information.
• **Ingress-Frame**	Display per port Ingress Frame information.

The port must be a member of the same VLAN as the Port VLAN ID.

Button



: press this button to take effect.

4.3.4.6 Q-in-Q Port Config

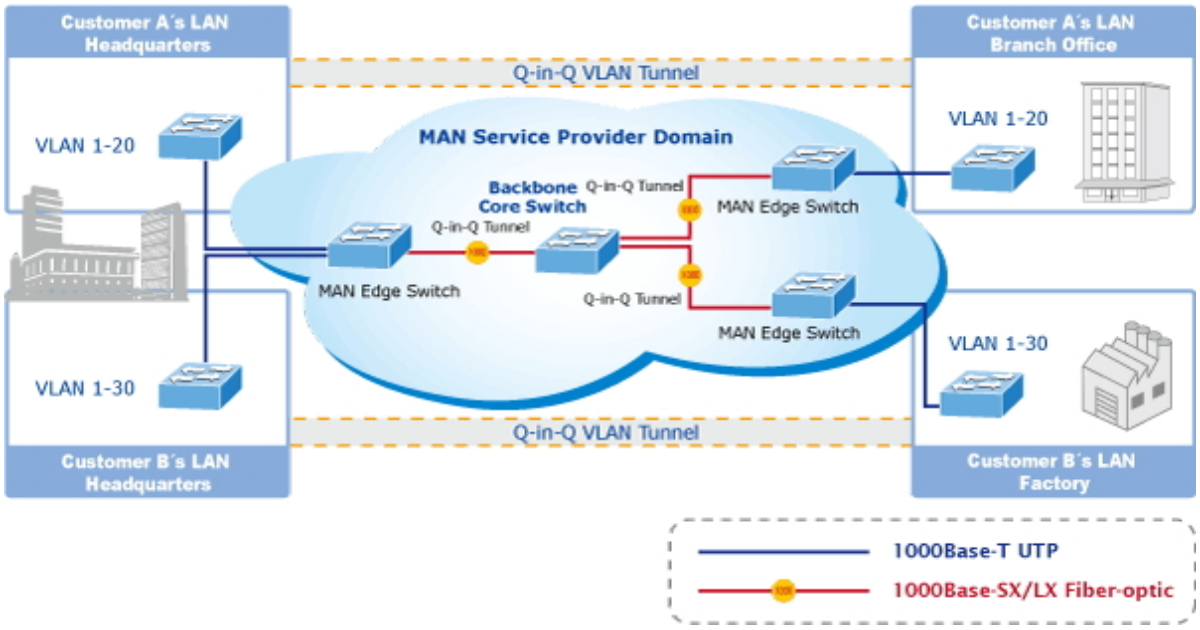
This page is used for configuring the Managed Media Converter Q-in-Q port VLAN function; the Q-in-Q port VLAN function configuration page contains fields for managing ports that are part of Q-in-Q VLAN.

Understanding Nomenclature of the Switch

IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (Q-in-Q) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



The Managed Media Converter supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

Q-in-Q Port Configuration

The Q-in-Q Port configuration screen in Figure 4-47 is shown below.

Figure 4-47 : Q-in-Q Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection/Port**	Select specific port for Q-in-Q Port configuration./ List per port numbers.
• **Index**	Choose to use the set of indexes in which the service Tag value is placed in the Q-in-Q Index config web page setting. Also display current Index information.
• **Tagging**	Set whether VLAN Tag is added or removed from the packet sent out by selected port. The available options are **"Add"**, **"RMV"** and **"None"**. **Add:** Do the new service Tag action on the incoming and outgoing packet from this port, if the incoming packet itself has service tag, modify or directly replace the service Tag action depending on whether the RX detect is opened or not. **RMV:** RX detect enable state to remove service Tag. Also display current Tagging information.
• **RX Detect**	Enable or disable the packet that enters the port to do the service Tag check. Also display current RX Detect information.
• **Keep PCP/DEI**	Set whether to retain the original PCP and DEI values when modifying the service Tag entered into the packet. Also display current Keep PCP/DEI information.

Button

Apply : press this button to take effect.

4.3.4.7 Q-in-Q Index Config

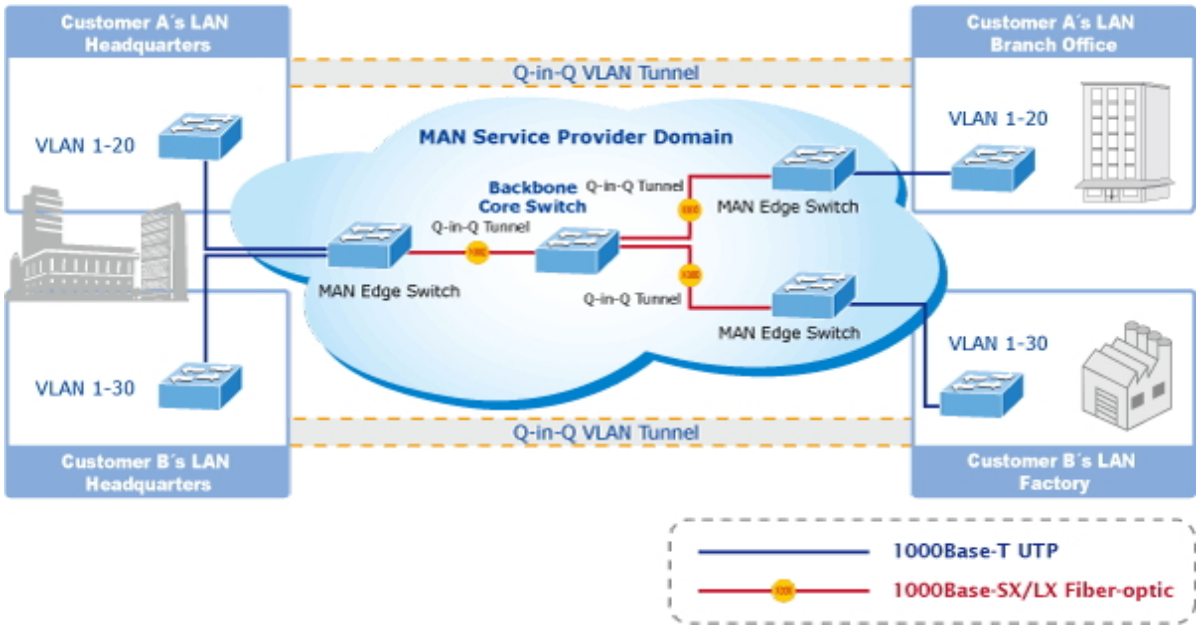
This page is used for configuring the Managed Media Converter Q-in-Q port VLAN function; the Q-in-Q port VLAN function configuration page contains fields for managing ports that are part of Q-in-Q VLAN.

Understanding Nomenclature of the Switch

IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (Q-in-Q) is designed for service providers carrying traffic for multiple customers across their networks. Q-in-Q tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



The Managed Media Converter supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available. This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

Q-in-Q Index Configuration

The Q-in-Q Index configuration screen in Figure 4-48 appears.

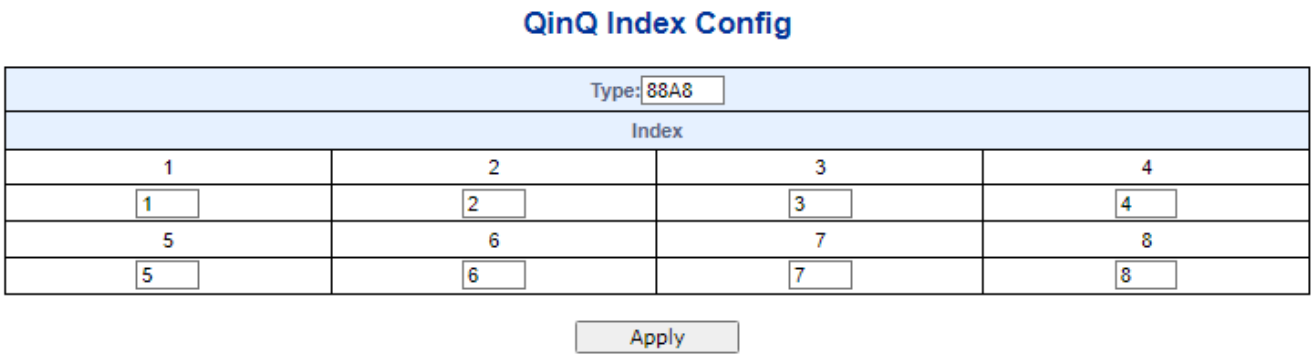


Figure 4-48 : Q-in-Q Index Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Type**	Set the type value of service Tag.
• **Index**	Set the service Tag value for each index.

Button

Apply : press this button to take effect.

4.3.5 LLDP

On this page, **Link Layer Discovery Protocol (LLDP)** is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in **Type Length Value (TLV)** format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

The LLDP setting configuration includes the LLDP Global Setting, LLDP Port Setting and table 4-49 show the items of LLDP setting functions.

LLDP Configuration	
Item	**Description**
LLDP Global Setting	Configure and display LLDP Global Settings on this web page.
LLDP Port Setting	Configure and display LLDP Port Settings on this web page.
LLDP Remote MIB	Configure and display LLDP Remote MIB on this web page.

Table 4-49: Descriptions of LLDP Setting Configuration

4.3.5.1 LLDP Global Setting

This page allows you to configure the LLDP Global settings for Managed Media Converter as the screen in Figure 4-50 appears.

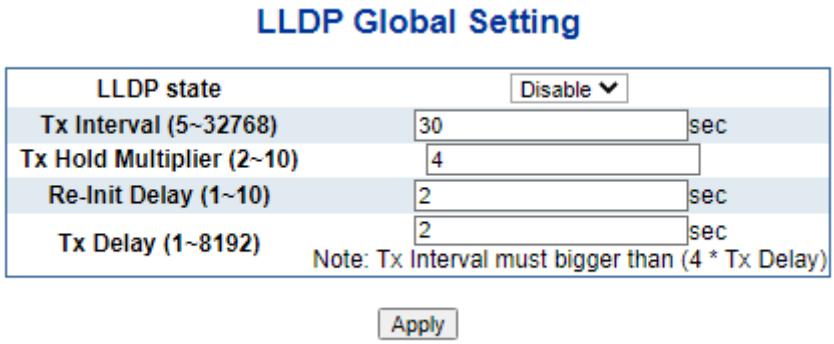


Figure 4-50: LLDP Global Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **LLDP State**	This column provides configuring enable or disable the LLDP function.
• **Tx Interval (5-32768)**	This column provides configuring Tx Interval settings; the default value is 30 and the available range is **5** to **32678**. Unit is second. The Managed Media Converter is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission

	Interval >= (4 * Delay Interval)
• **Tx Hold Multiplier (2-10)**	This column provides configuring the value for Tx Hold Multiplier; the default value is 4 minute and the available range is **2** to **10**. Each LLDP frame contains information about how long the information in the LLDP frame will be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
• **Re-Init Delay (1-10)**	This column provides configuring Re-Init Delay settings; the default value is 2 and the available range is **1** to **10**. Unit is second. When a port is disabled, LLDP is disabled or the Managed Media Converter is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Re-init Delay** controls the amount of seconds between the shutdown frame and a new LLDP initialization.
• **Tx Delay (1-8192)**	This column provides configuring Tx Delay settings; the default value is 2 and the available range is **1** to **8192**. Unit is second. If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval

Button

Apply: press this button to take effect

4.3.5.2 LLDP Port Setting

This page allows you to configure the LLDP Port settings for Managed Media Converter as the screen in Figure 4-51 appears.

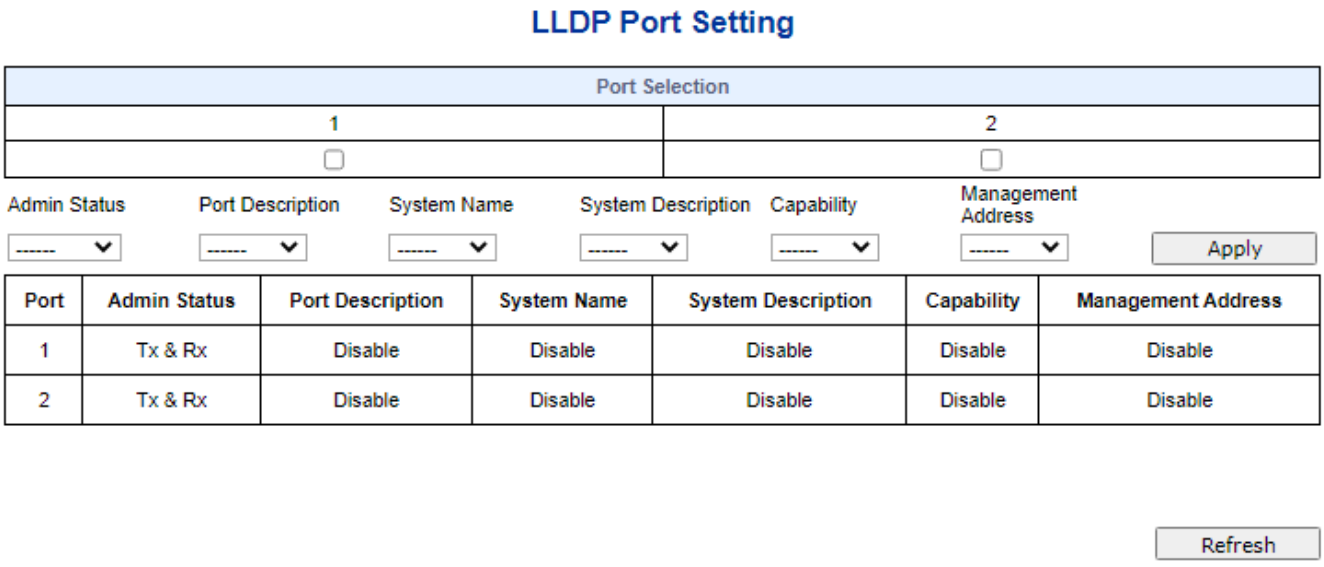


Figure 4-51: LLDP Port Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	This column provides selecting specific port for LLDP Port Settings function.
• **Admin Status**	This column provides displaying and selecting the Admin status of LLDP and the available options are : **Disable** The Managed Media Converter will not send out LLDP information, and will drop LLDP information received from neighbors. **Rx Only** The Managed Media Converter will not send out LLDP information, but LLDP information from neighbor units is analyzed. **Tx Only** The Managed Media Converter will drop LLDP information received from neighbors, but will send out LLDP information. **Tx & Rx** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
• **Port Description**	This column provides displaying and configuring enable or disable the Port Description function. When enabling the "Port Description", the LLDP information will be transmitted.
• **System Name**	This column provides displaying and configuring enable or disable the System Name function. When enabling the "System Name", the LLDP information will be transmitted.
• **System Description**	This column provides displaying and configuring enable or disable the System Description function. When enabling the "System Description", the LLDP information will be transmitted.
• **Capability**	This column provides displaying and configuring enable or disable the Capability function. When enabling the "Capability", the LLDP information will be transmitted.
• **Management Address**	This column provides displaying and configuring enable or disable the Management Address function. When enabling the "Management Address", the LLDP information will be transmitted.
• **Port**	Display per port list.

Buttons

Apply: press this button to take effect.

Refresh: press this button to refresh current status.

4.3.5.3 LLDP Remote MIB

This page allows you to configure the LLDP Remote MIB settings for Managed Media Converter as the screen in Figure 4-52 appears.

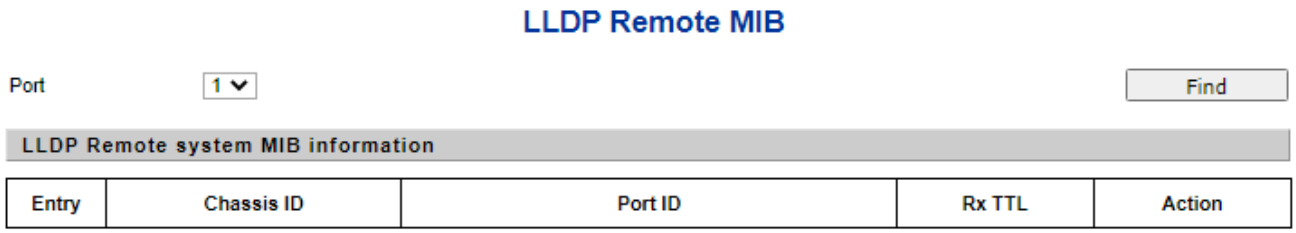


Figure 4-52: LLDP Remote MIB Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	This column provides selecting specific port for LLDP Remote MIB function.
LLDP Remote System MIB Information	
• **Enrty**	This column provides displaying entry number of LLDP Remote MIB information.
• **Chassis ID**	This column provides displaying chassis ID of LLDP Remote MIB information.
• **Port ID**	This column provides displaying Port ID of LLDP Remote MIB information.
• **Rx TTL**	This column provides displaying Rx TTL of LLDP Remote MIB information.
• **Action**	Delete: press this button to delete specific LLDP Remote MIB information.

Button

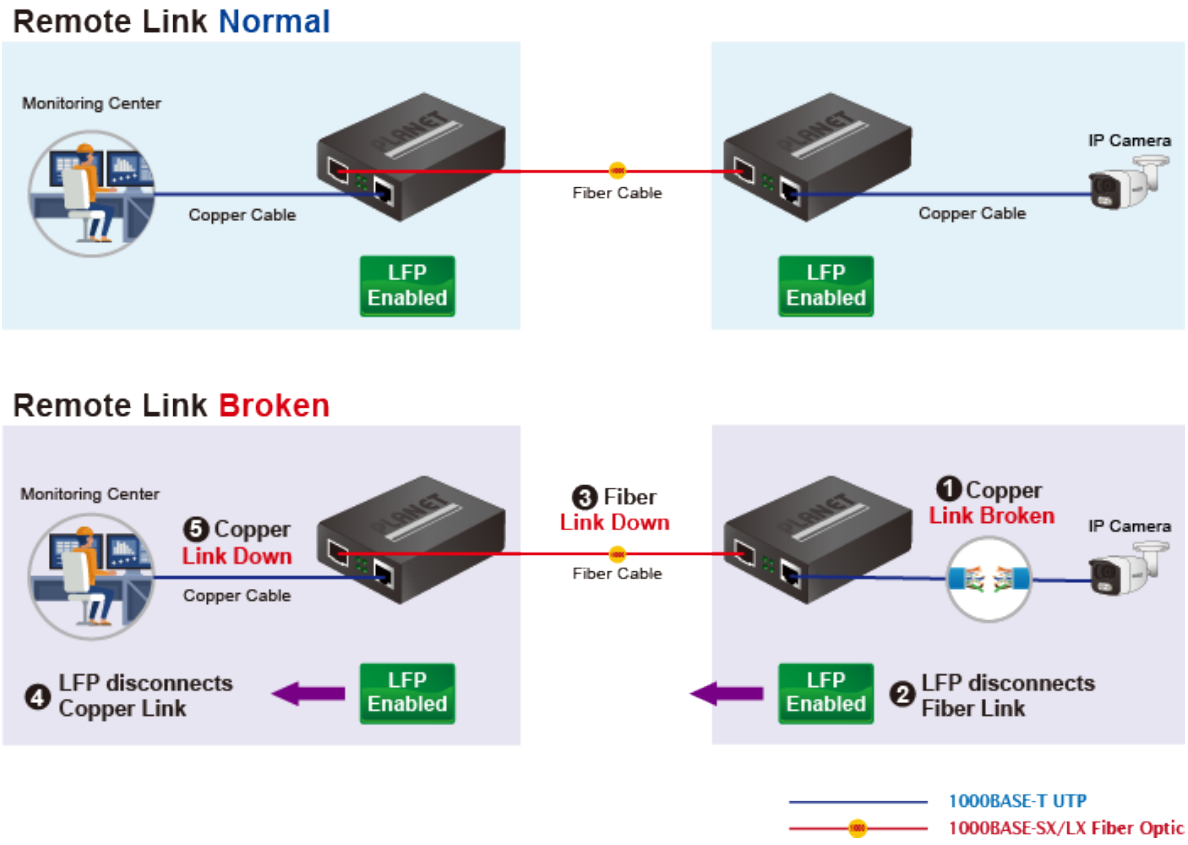
Find: press this button to find LLDP Remote MIB information of specific port.

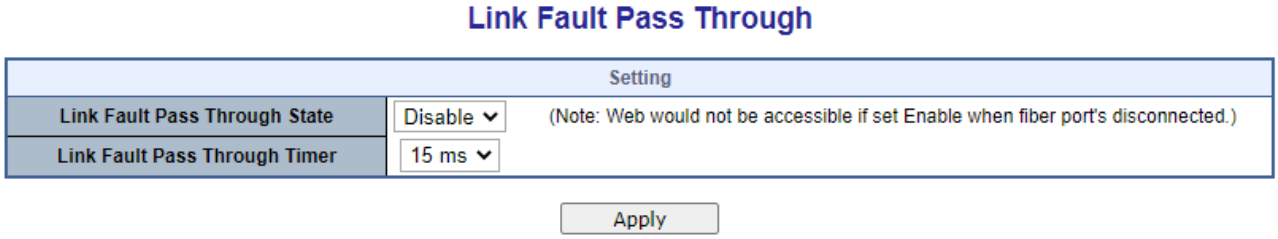
4.3.6 Link Fault Passthrough

The GT-915A provides auto MDI/MDI-X on its TP port and built-in **Link Fault Pass-through** function (**LFP**). The LFP function includes **Link Loss Carry Forward** (**LLCF**) and **Link Loss Return** (**LLR**), both of which can immediately alarm administrators the problem of the link media and provide efficient solution to monitoring the net.

- LLCF means when a device connected to the converter and the TP line loses the link, the converter's fiber port will disconnect the link of transmission.
- LLR means when a device connected to the converter and the fiber line loses the link, the converter's fiber port will disconnect the link of transmission.

Therefore, the GT-915A greatly supports the administrators to manage the network efficiently.





4.4 QoS

4.4.1 Understanding QoS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic. You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

QoS Terminology

- **Classifier**—classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The Switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** — is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- **Service Level**—defines the priority that will be given to a set of classified traffic. You can create and modify service levels.
- **Policy**—comprises a set of "rules" that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- **QoS Profile**—consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- **Rules**—comprises a service level and a classifier to define how the Switch will treat certain types of traffic. Rules are associated with a QoS Profile (see above).

To implement QoS on your network, you need to carry out the following actions:

1. Define a service level to determine the priority that will be applied to traffic.
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Switch.
3. Create a QoS profile which associates a service level and a classifier.
4. Apply a QoS profile to a port(s).

On the Access QoS configuration web page, you can view QoS management function informations of the Managed Media Converter as the screen in Figure 4-53 appears.

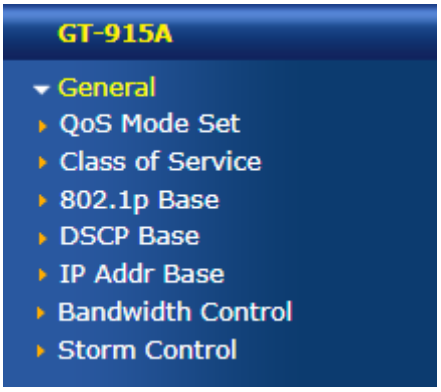


Figure 4-53: Managed Media Converter QoS Configuration Web Page

QoS Configuration	
Item	**Description**
QoS Mode Set	Configure QoS Mode Set configuration settings on this web page.
Class of Service	Display and configure QoS Class of Service settings on this web page.
802.1p-based QoS	Display and configure 802.1p-based QoS settings on this web page.
DSCP Based	Display and configure DSCP-based Priority settings on this web page.
IP Addr Base	Display and configure IP Addr Base settings on this web page.
Bandwidth Control	Display and configure Bandwidth Control function.
Storm Control	Display and configure Broadcast Storm Control function.

Table 4-54: Descriptions of QoS Configuration

4.4.2 General

4.4.2.1 QoS Mode Set

This page allows you to configure the QoS mode settings for Managed Media Converter as the QoS mode settings screen in Figure 4-54 appears.

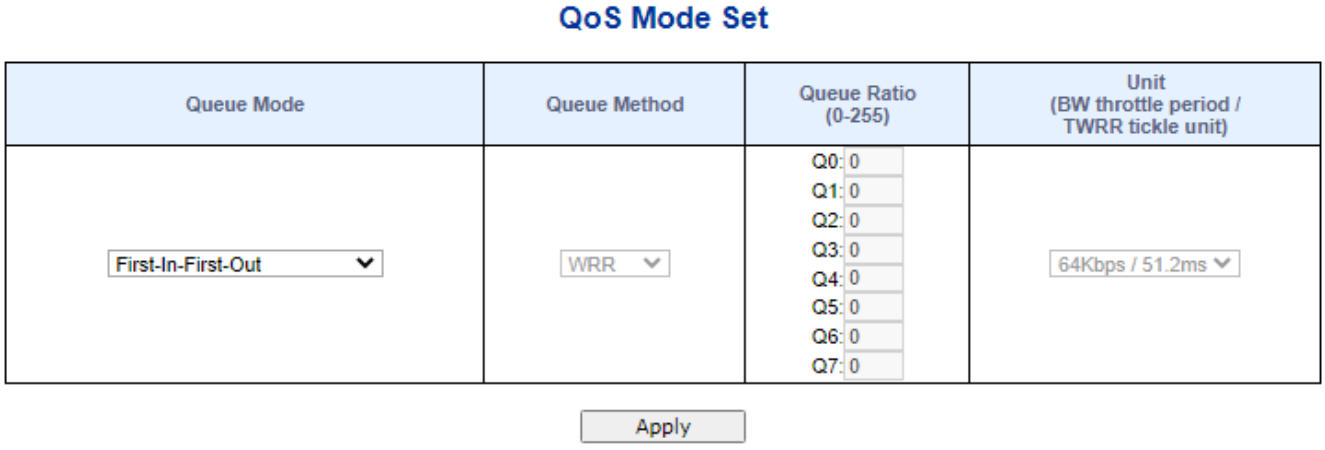


Figure 4-54 : QoS Mode Set Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Queue Mode**	Select the Queue Mode for QoS and the available options are shown below: **First-In-First-Out** **WRR/WFQ/Bwassure/Bwlimit/TWRR** **SPx1 WRR/WFQ/Bwassure/Bwlimit/TWRRx7** **SPx2 WRR/WFQ/Bwassure/Bwlimit/TWRRx6** **SPx4 WRR/WFQ/Bwassure/Bwlimit/TWRRx4** **SPx8**
• **Queue Method**	Select the Queue Method for QoS and the available options are shown below: **WRR** **WFQ** **Bwassure** **Bwlimit** **TWRR**
• **Queue Ratio (0-255)**	Set Queue Ratio for each mode and the available range is **0-255**.
• **Unit (BW Throttle Period/TWRR Tickle Unit)**	Set Queue Ratio Unit for each mode and the available options are shown below: **64Kbps/51.2ms** **1Mbps/3.1ms** **2Mbps/1.55ms** **4Mbps/0.82ms**

Button

Apply: press this button to take effect.

4.4.2.2 Class of Service

This page allows you to configure the QoS Class of Service settings for all switch ports as the QoS Class of Servic screen in Figure 4-55 appears.

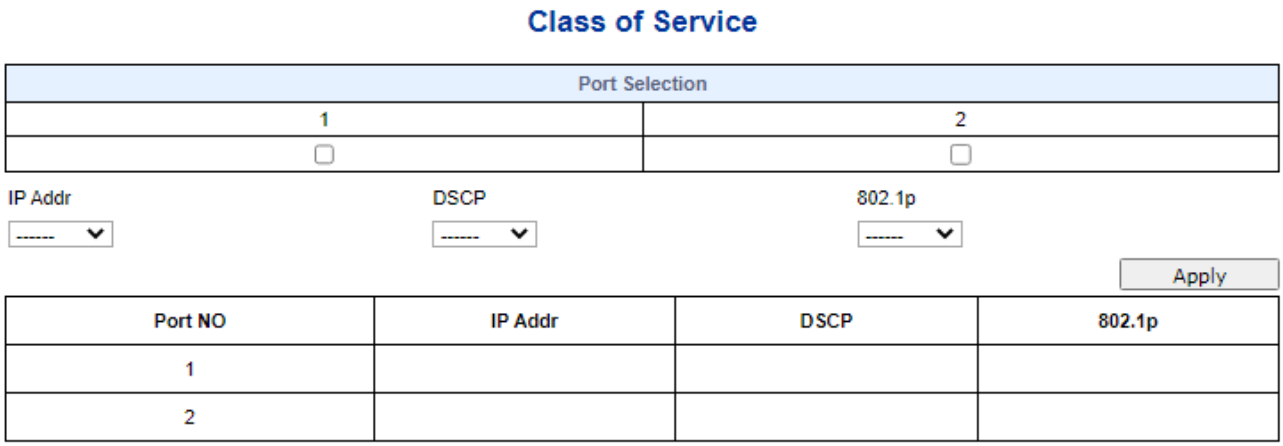


Figure 4-55: QoS Class of Service Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific port for QoS Class of Service settings.
• **Port No.**	Display per port list.
• **IP Addr**	Enable or disable the IP Address function for specific port. Also display per port IP Address status.
• **DSCP**	Enable or disable the DSCP function for specific port. Also display per port DSCP status.
• **802.1p**	Enable or disable the 802.1p function for specific port. Also display per port 802.1p status.

Button

Apply : press this button to take effect.

4.4.2.3 802.1p-based QoS

This page allows you to configure the 802.1p-based QoS settings for Managed Media Converter as the 802.1p-based QoS screen in Figure 4-56 appears.

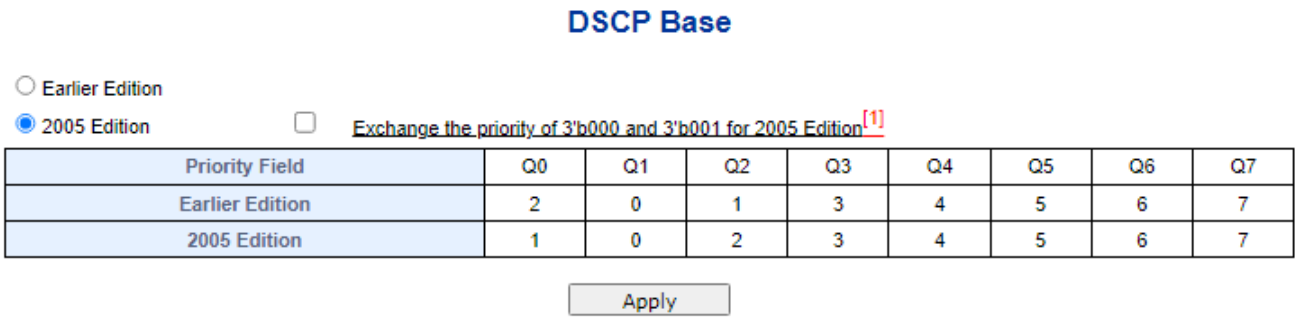


Figure 4-56: 802.1p-based QoS Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Earlier Edition**	Click to select the Eariler Edition for 802.1p-based QoS.
• **2005 Edition**	Click to select the 2005 Edition for 802.1p-based QoS.
• **Exchange the priority of 3'b001 for 2005 Edition**	Click to select the Exchange the priority of 3'b001 for 2005 Edition for 802.1p-base QoS.
• **Priority Field**	Display priority field of Q0 to Q7.
• **Earlier Edition**	Display earlier edition for 802.1p-based QoS.
• **2005 Edition**	Display 2005 edition for 802.1p-based QoS.

Button

Apply : press this button to take effect.

4.4.2.4 DSCP-based Priority

This page allows you to configure the DSCP-based Priority settings for Managed Media Converter as the DSCP-based Priority screen in Figure 4-57 appears.

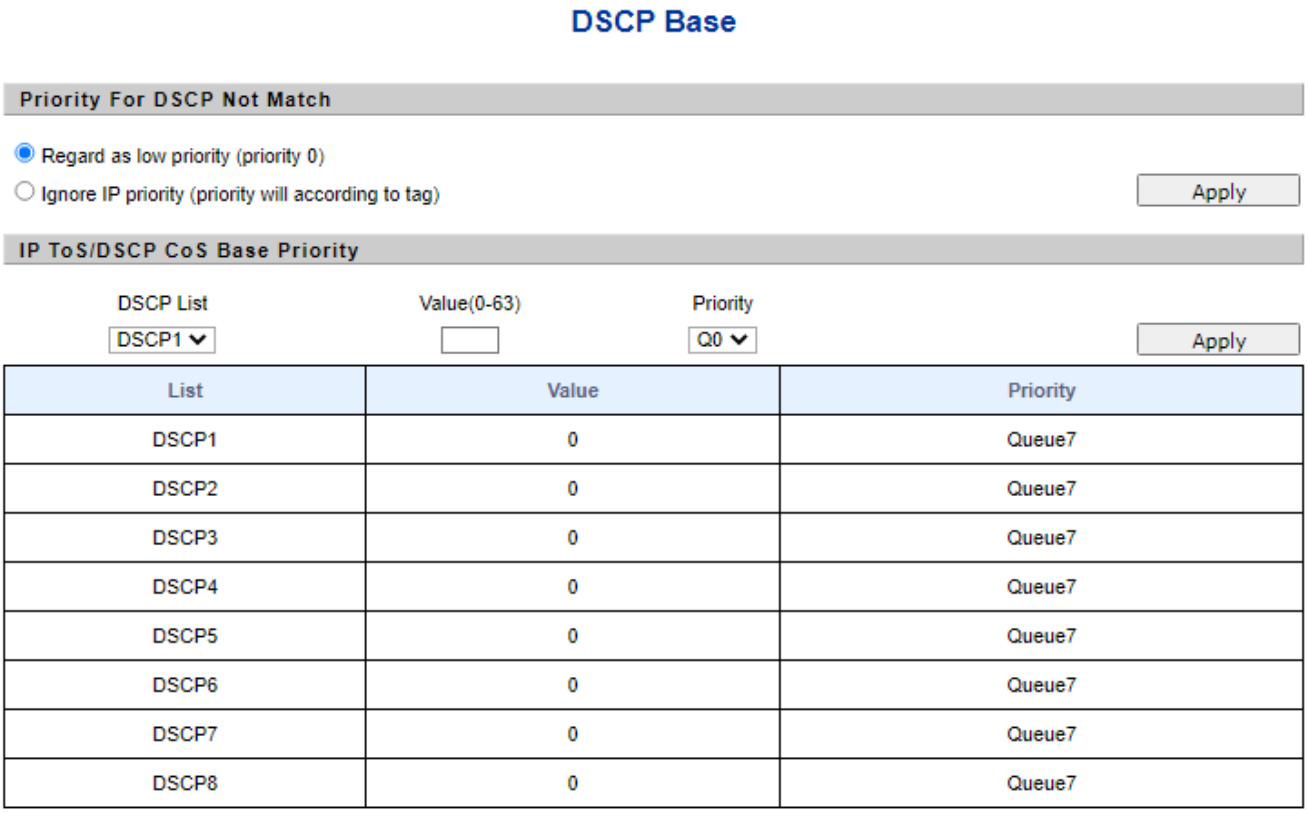


Figure 4-57: DSCP-based Priority Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Priority For DSCP Not Match**	Provide two options for selection. Regard as low priority (priority 0) Ignore IP priority (priority will according to tag/port)
• **IP ToS/DSCP CoS Base Priority**	Provide three functions for setting. **DSCP List**: provide DSCP1 to DSCP8 options to choose. **Value(0-63):**allow input the value range from 0 to 63. **Priority:** provide Q0 to Q7 options to choose.
• **List**	Display DSCP1 to DSCP8.
• **Value**	Display the value setting of per DSCP1 to DSCP8.
• **Priority**	Display the priority setting of per DSCP1 to DSCP8.

Button

Apply: press this button to take effect.

4.4.2.5 IP Addr Base

This page allows you to configure the IP Addr Base settings for Managed Media Converter as the IP Addr Base screen in Figure 4-58 appears.

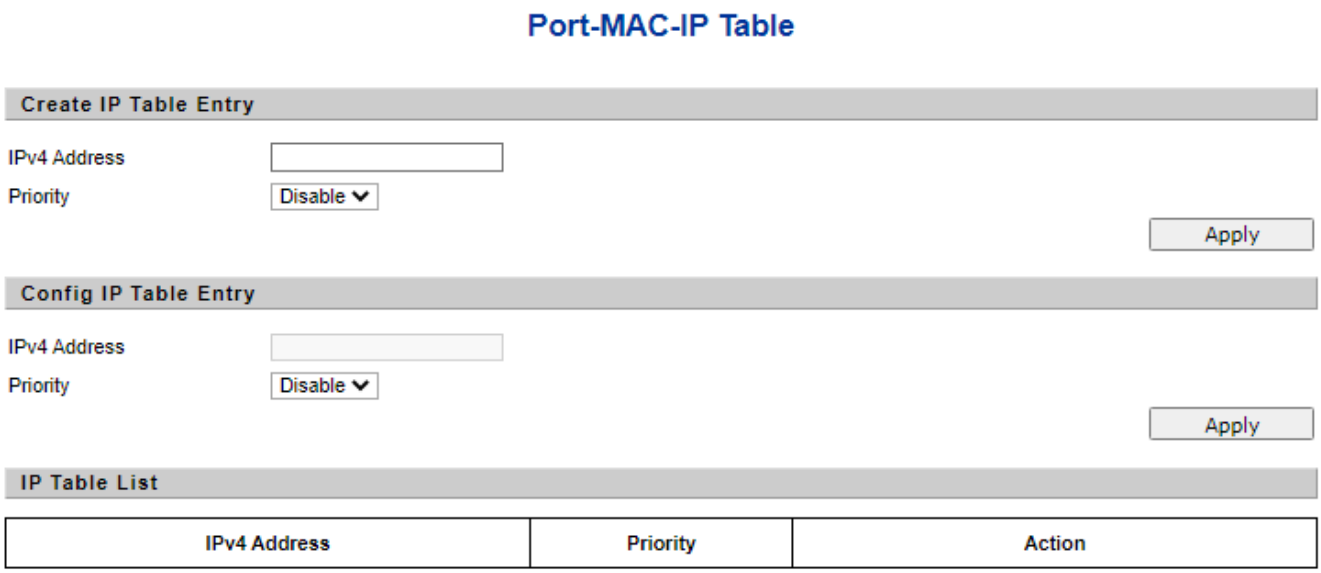


Figure 4-58: IP Addr Base Configuration Page Screenshot

The page includes the following fields:

Object	Description
Create IP Table Entry	
• **IPv4 Address**	Configure the IP Address.
• **Priority**	Configure the priority (0-7)
Config IP Table Entry	
• **IPv4 Address**	Display the IP Address you select
• **Priority**	Change the priority (0-7)

Button

Apply: press this button to take effect.

4.4.3 Bandwidth Control

This page allows you to configure the incoming and outgoing bandwidth control settings for all switch ports as the bandwidth control screen in Figure 4-59 appears.

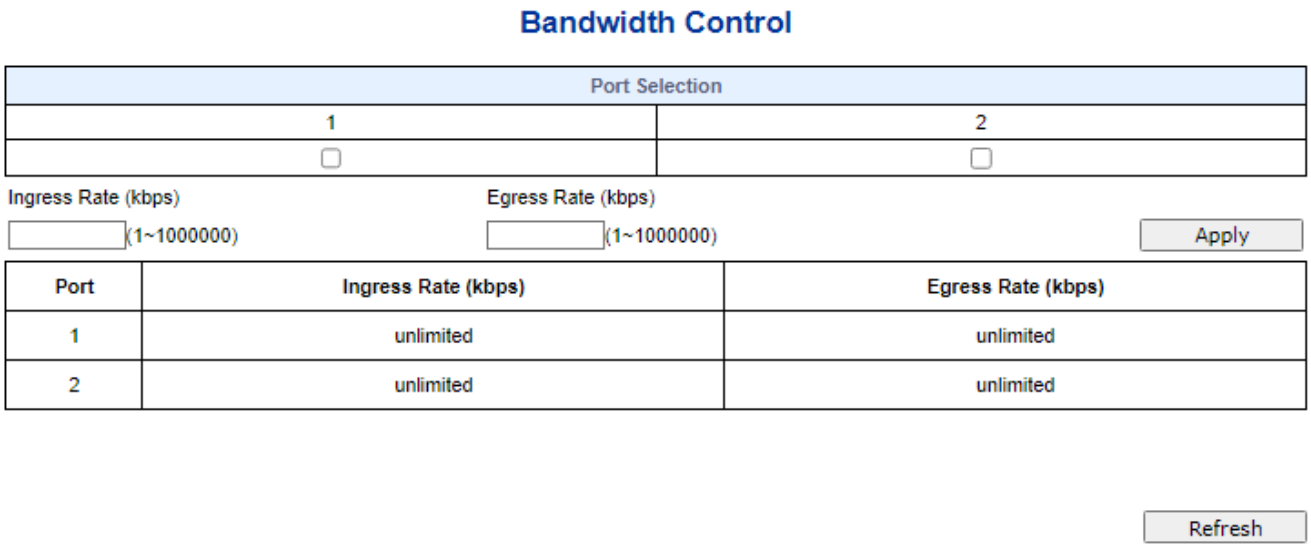


Figure 4-59: Bandwidth Control Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific port for incoming and outgoing bandwidth control settings.
• **Ingress Rate (kbps)** • **(1-1000000)**	Controls the rate (unit: kbps) for the ingress rate. This value is restricted to 1-1000000. The default value is **Unlimited**.
• **Egress Rate (kbps)** • **(1-1000000)**	Controls the rate (unit: kbps) for the egress rate. This value is restricted to 1-1000000. The default value is **Unlimited**.
• **Port**	Display per port list.
• **Ingress Rate (kbps)**	Display per port ingress rate setting value.
• **Egress Rate (kbps)**	Display per port egress rate setting value.

Buttons

Apply: press this button to take effect.

Refresh: press this button to refresh information.

4.4.4 Storm Control

Storm control for the switch is configured on this page. There are a broadcast storm rate control, multicast storm rate control, and unicast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch as the Storm Control configuration screen in Figure 4-60 appears.

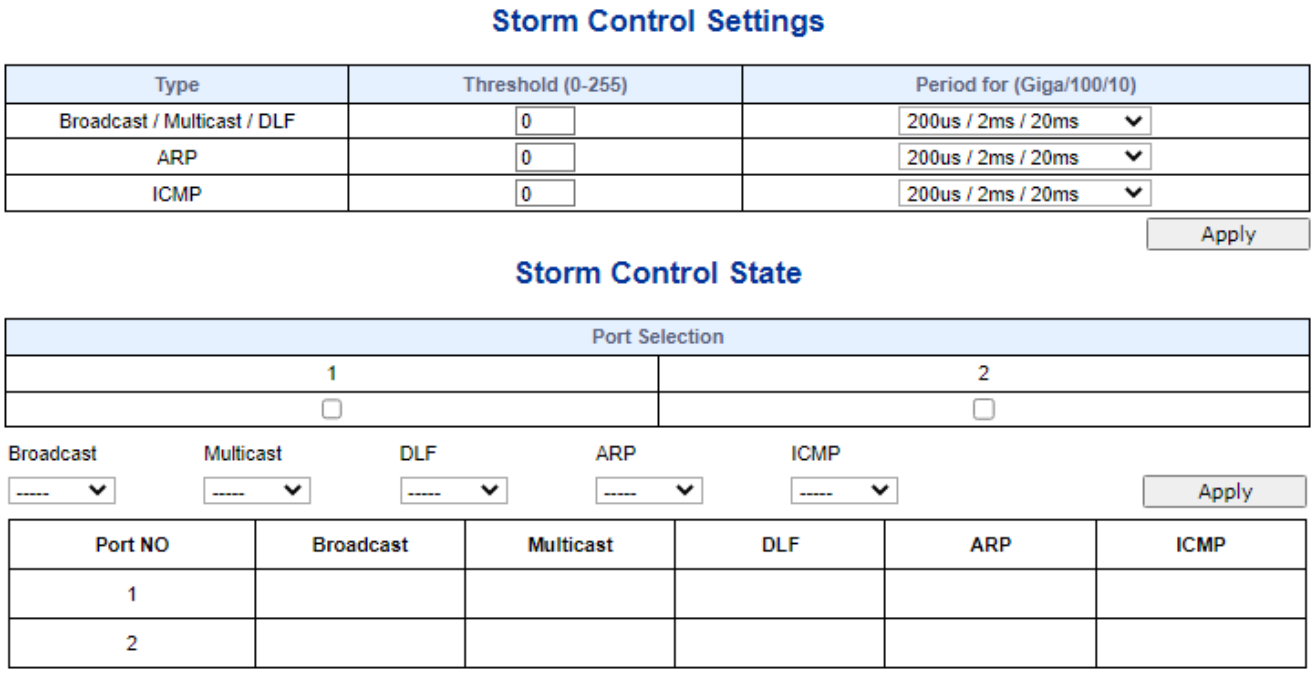


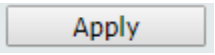
Figure 4-60: Broadcast Storm Control Configuration Page Screenshot

The page includes the following fields:

Object	Description
Storm Control Settings	
• **Type**	Types of storm control: Broadcast: Broadcast packet. Multicast: Multicast packet, 40th bit in the destination MAC is 1 DLF: The destination address in the MAC table does not exist ARP: ARP packet. ICMP: ICMP packet.
• **Threshold (0-255)**	During the receive period, the port receives an upper limit for the specified packet type
• **Period for (Giga/100/10)**	Set reception period and the available options are shown below: 200us/2ms/20ms 1ms/10ms/100ms 10ms/10ms/10ms 100ms/100ms/100ms
Storm Control State	
• **Port Selection**	Select specific port for further configuration.
• **Broadcast**	Enable or disable the broadcast storm control function.

• **Multicast**	Enable or disable the multicast storm control function.
• **DLF**	Enable or disable the unknown destination MAC packets control function.
• **ARP**	Enable or disable the ARP packets control function.
• **ICMP**	Enable or disable the ICMP packets control function.
• **Port No.**	Display per port list.
• **Broadcast**	Display per port broadcast storm control setting.
• **Multicast**	Display per port multicast storm control setting.
• **DLF**	Display per port unknown destination MAC packets control setting.
• **ARP**	Display per port ARP packets control setting.
• **ICMP**	Display per port ICMP packets control setting.

Button



: press this button to take effect.

4.5 Security

On the Access Security configuration web page, you can view and configure Security functions of the Managed Media Converter as the screen in Figure 4-61 appears:

Figure 4-61: Managed Media Converter Security Configuration Web Page

Security Configuration	
Item	**Description**
Access Managament	Configure and display Access Management configuration settings on this web page.
HTTPS	Configure and display HTTPS configuration settings on this web page.

Table 4-62: Descriptions of Security Configuration

4.5.1 Access Security

4.5.1.1 Access Management

This page allows you to configure the Access Security settings for Managed Media Converter as the Access Security configuration screen in Figure 4-63 appears.

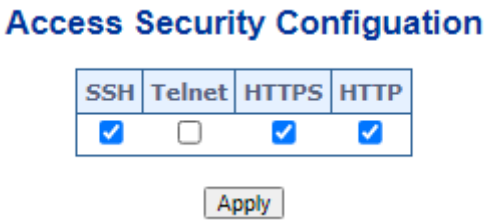


Figure 4-63: Access Security Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **SSH**	Configure enable or disable the SSH function and default mode is enable.
• **Telnet**	Configure enable or disable the Telnet function and default mode is enable.
• **HTTPS**	Configure enable or disable the HTTPS function and default mode is enable.
• **HTTP**	Configure enable or disable the HTTP function and default mode is enable.

Button

Apply: press this button to take effect.

4.5.1.2 HTTPS

Configure HTTPS on this page. The HTTPS Configuration screen in Figure 4-64 appears.

Figure 4-64: HTTPS Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Certificate Upload**	Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39. Possible methods are: **`Web Browser`**: Upload a certificate via Web browser. **`URL`**: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

Button

Apply: press this button to take effect.

4.6 Maintenance

4.6.1 Configuration

The configuration includes backup and reload the current configuration of the Managed Media Converter to/from the local management station.

4.6.1.1 Backup

The backup configuration provides downloading the Managed Media Converter configuration file (Current.tar.gz) to local management station as the screen in Figure 4-65 appears.

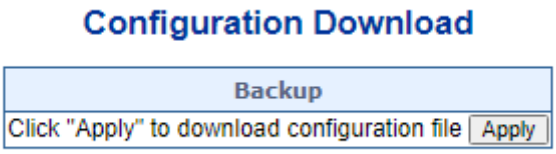


Figure 4-65: Backup Configuration Page Screenshot

4.6.1.2 Restore

The restore configuration provides upload the Managed Media Converter configuration file (Current.tar.gz) to other Managed Media Converter from local management station as the screen in Figure 4-66 appears.

Figure 4-66: Restoring Configuration Page Screenshot

Note

The Managed Media Converter configures restoration as **the IP address setting is excluded**.

Button

Apply: press this button to take effect.

4.6.1.3 Save

This function allows to save the current configuration, thereby ensuring that the current active configuration can be used at the next reboot as the screen in Figure 4-67 appears.

Figure 4-67: Restoring Configuration Page Screenshot

Button

Apply: press this button to take effect

4.6.2 Firmware Update

This page facilitates an update on the firmware controlling the switch as the Web Firmware Upgrade screen in Figure 4-68 appears.

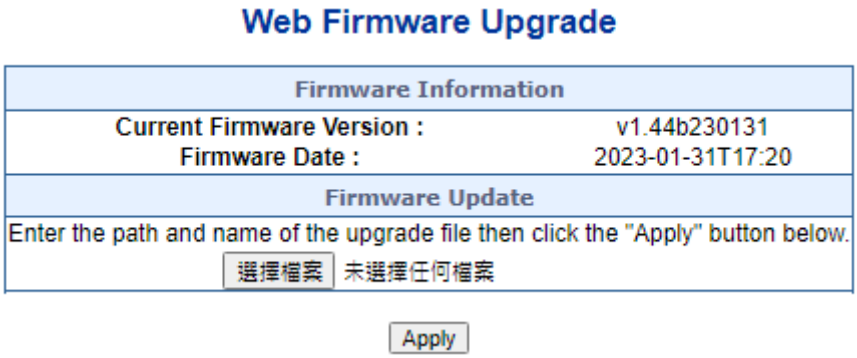


Figure 4-68: Web Firmware Update Page Screenshot

Once the software is loaded to the system successfully, the following screen appears. The system will load the new software after reboot.

Note

DO NOT Power OFF the Managed Media Converter until the update progress is complete.

4.6.3 Factory Default

You can reset the configuration of the Managed Media Converter on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in Figure 4-69 appears.

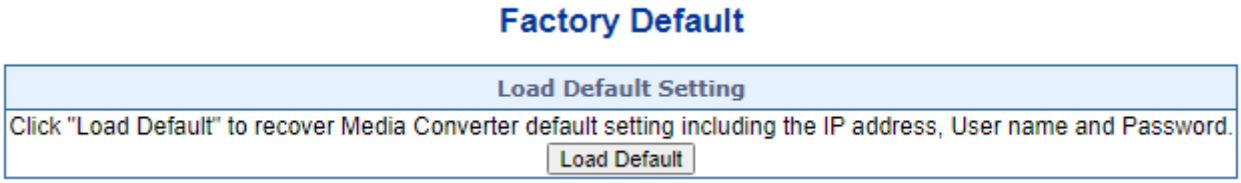


Figure 4-69: Factory Default Configuration Page Screenshot

Button

Load Default : Click to reset the configuration to Factory Defaults.

Note To reset the Managed Media Converter to the Factory default setting, you can also press the hardware-based reset button at the front panel about 5 seconds.

4.6.4 System Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user has to re-login the Web interface about 60 seconds later; the System Reboot screen in Figure 4-70 appears.

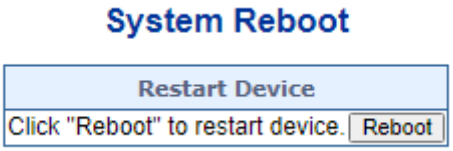


Figure 4-70: System Reboot Page Screenshot

5. TROUBLESHOOTING

This chapter contains information to help you solve issues. If the Managed Media Converter is not functioning properly, make sure the Managed Media Converter was set up according to instructions in this manual.

■ **The Link LED is not lit**

Solution:

Check the cable connection and remove duplex mode of the Managed Media Converter

■ **Some stations cannot talk to other stations located on the other port**

Solution:

Please check the VLAN settings, trunk settings, or port enabled / disabled status.

■ **Performance is bad**

Solution:

Check the full duplex status of the Managed Media Converter. If the Managed Media Converter is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

■ **Why the device doesn't connect to the network**

Solution:

1. Check the LNK/ACT LED on the switch
2. Try another port on the Switch
3. Make sure the cable is installed properly
4. Make sure the cable is the right type
5. Turn off the power. After a while, turn on power again

■ **10/100/1000BASE-T port link LED is lit, but the traffic is irregular**

Solution:

Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

■ **Device does not power up**

Solution:

1. AC power cord not inserted or faulty
2. Check that the AC power cord is inserted correctly
3. Replace the power cord If the cord is inserted correctly, check that the AC power source is working by connecting a different device in place of the switch.
4. If that device works, refer to the next step.
5. If that device does not work, check the AC power

■ **IP address has been changed or admin password has been forgotten –**

Solution:

To reset the IP address to the default IP address **"192.168.0.100"** or reset the login password to default value, press the hardware-based **reset button** on the front panel for about **5 seconds.** After the device is rebooted, you can log in to the management Web interface within the same subnet of 192.168.0.xx.

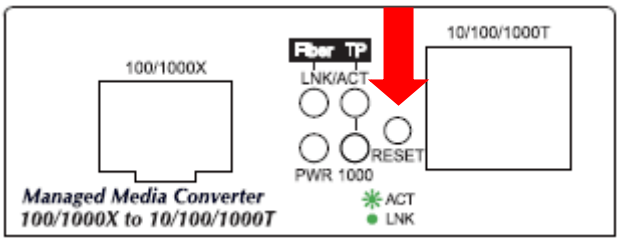


Figure 9-1: GT-915A Reset Button

Appendix A Networking Connection

A.1 Device's RJ-45 Pin Assignments

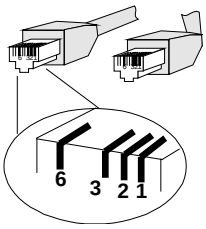
■ **1000Mbps, 1000Base T**

RJ-45 Connector pin assignment		
Contact	**MDI**	**MDI-X**
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

10/100Mbps, 10/100Base-TX

RJ-45 Connector pin assignment		
Contact	MDI Media Dependant Interface	MDI-X Media Dependant Interface -Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

A.2 RJ-45 cable pin assignment



The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

Figure A-1: Straight-Through and Crossover Cable

Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.