ASCENT
Communication Technology

AE208 Series
P2P Gateway

User Guide

Revision B

ACT AE208 Series 8 Port P2P Ethernet CPE Gateway
User Guide

ACT Document Number: AE208 CPE UG Revision A

This document is produced to assist professional and properly trained personnel with installation and maintenance issues for the product. The capabilities, system requirements and/or compatibility with third-party products described herein are subject to change without notice.

For more information, contact ACT: Sales@ascentcomtec.com

Revision History

Revision	Date	Reason for Change
A	08/01/2012	Initial Release
B	10/02/2012	Section Update

Table of Contents

0 Preface

0.1 Audience

This manual is intended for network installers and system administrators who are responsible for installing, configuring or maintaining networks. It assumes that you understand the transmission and management protocols used on your network.

This manual also assumes prior knowledge and understanding of the terminology, theories, practices and specific knowledge about the networking devices, protocols, and interfaces that comprise your network. You should have working experiences of the graphical user interfaces (GUIs), Command Line Interface (CLI), Simple Network Management Protocol (SNMP) and Web browsers.

0.2 Conventions

GUI Convention	Description
Boldface	Keywords on web management page are in **Boldface**
Italic	Tab page name is in *italic*
<>	Button on web management page is in <>

Symbols

Caution	Means reader be careful. Improper operation may cause data loss or damage to equipment.
Note	Means a complementary description.

1 Device Introduction

1.1 Brief Introduction

AE208 P2P Switch series ONU (Optical Network Unit) support data, VoIP (Voice over IP) and CATV "triple play" services in the P2P (point to point) based FTTH (Fiber to the Home) network with high performance and effective cost. The integrated layer 2 Ethernet switch function supports back-pressure in half duplex mode and 802.3x flow control in full duplex mode, and intelligent address recognition algorithm which allows the AE208 Gateway to recognize up to 8096 different MAC addresses and enables filtering and forwarding at full wire speed.

AE208 Gateway provides a wide transparent bandwidth to support CATV analog channels or a combination of analog and digital channels including HDTV broadcast. It has an integrated VoIP function to support SIP-based telephony services. And it supports IGMP Snooping, reducing the bandwidth occupied by IPTV and VoD.

1.2 Features

- One 100Base-FX or 1000Base-X single mode fiber network port with CATV overlay. Eight/Four 10BASE-T/100Base-TX Half/Full duplex layer 2 switch LAN ports with a table up to 8K MAC addresses.
- Store & forward architecture and performs forwarding and filtering at non-blocking full wire speed with auto aging function.
- 802.3x flow control for full duplex and a backpressure function for half duplex operation with bandwidth control function
- Port-based or 802.1Q VLAN of up to 64 active VLAN groups with full 12-bit VLAN ID
- 802.1p, port-base, DiffServ QoS package classification with 4 priority queues
- IGMP Snooping
- By-port egress rate control
- Web-based management interface with both DHCP and static fixed-IP
- Command Line Interface (CLI)
- SNMP v1/v2c/v3
- Telnet management
- Login with the MD5 encrypt automatically
- SNMP trap filter and threshold setting
- Two levels of User Authorization: user and admin
- Broadcast/Multicast Storm Suppression

[Except for 8 port 1000Mbps version]

- Twenty - eight 32 - bit counters and two 64 - bit counters for per port
- Compatible with wireless IEEE802.11b, IEEE802.11g and IEEE 802.11n

- Provides 300Mbps transmission rate
- Wireless Client List
- Supports 64/128-bit WEP, WPA, WPA2, WPA1WPA2, WPA-PSK, WPA2PSK, WPAPSKWPA2PSK and 802.1X encryption
- Supports Hidden SSID and Multiple SSID
- Supports WDS Lazy mode, Bridge mode and Repeater mode
- Supports WPS
- Supports WMM (Wi-Fi Multimedia)
- Supports AP Discovery

[Only for models with CATV module]

- Wide 40 MHz ~ 860 MHz bandwidth supports CATV analog channels or a combination of analog and digital channels including HDTV broadcast
- Excellent RF frequency and distortion characteristics for high linearity
- Internal proprietary impedance matching circuitry with one 75Ω coaxial-cable output port
- High sensitivity of 75 or 88 dBuV RF output at –3dBm optical input
- Single-mode fiber, high return loss optical interface with receptacle Wide range of optical input power of -10 ~ 0 dBm
- Digital diagnostic monitoring interface for optical input level, supply voltage, temperature and RF output level
- Monitoring on CATV Receiver temperature, supply voltage, input optical power and output RF level and send CATV alarm trap

[Only for 1000Mbps uplink PoE model]

- Compatible with IEEE802.3af standard
- Supports PoE power up to 15.4W for each PoE port
- Supports PoE IEEE802.3af compliant PDs, such as IP phones, wireless access point and IP surveillance equipment.

1.3 System Specifications

1.3.1 Software Overview

Network Protocol	• IP/TCP/UDP • IP/ICMP/ARP/RARP • TFTP Client/DHCP Client • HTTP Server
IP Assignment	• Static IP • DHCP

Security	• IEEE 802.1X • HTTP 1.1 basic/digest authentication for Web setup • MD5 for SIP authentication
QoS	• Port based • 802.1p • DiffServ • 802.1p & DiffServ
Configuration	• Web Browser • Telnet • SNMP
Wireless (Not yet available for 1000Mbps uplink version)	• IEEE 802.11b/g/n • 300Mbps transmission rate • 2.400 ~ 2.483 GHz frequency band • 64/128-bit WEP, WPA, WPA2, WPA1WPA2, WPA-PSK, WPA2PSK, WPAPSKWPA2PSK and 802.1X encryption • WPS registration button • Hidden SSID and Multiple SSID • TxPower adjustment • Wireless Client Access Control • WDS Lazy Mode, Bridge Mode and Repeater Mode • WMM (Wi-Fi Multimedia) • AP Discovery
Codec (Only for VoIP option)	• G.711: 64 kb/s (PCM) • G.723.1: 6.3/5.3 kb/s • G.726: 16/24/32/40 kb/s (ADPCM) • G.729A: 8 kb/s (CS-ACELP) • G.729B: adds VAD & CNG to G.729 • GSM: 13 kb/s
Voice Quality (Only for VoIP option)	• Voice activity detection • Comfortable noise generator • Line echo canceller • Packet loss compensation
Call Function (Only for VoIP option)	• Call hold • Call waiting • Call Forwarding • Caller ID • 3-way conference calls

DTMF Function (Only for VoIP option)	• In-band DTMF • Out-of-band DTMF • SIP info
CATV	• Monitoring CATV status • CATV on/off Control • Send CATV alarm trap
PoE (Only for 1000Mbps Uplink PoE)	• IEEE 802.3 af (PoE) standard • Up to 15.4W for each PoE port
Firmware Upgrade	• TFTP

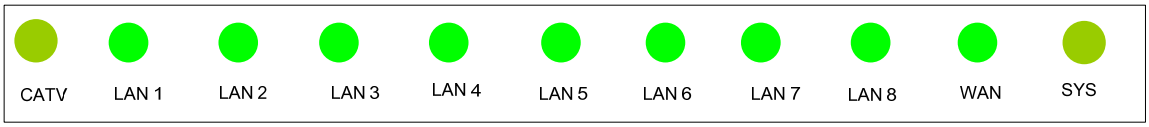
1.3.2 Hardware Overview

WAN Ports	SFP-based Module CATV optical power: -8 to 0 dBm
LAN Ports	Four/Eight RJ-45, Automatic MDI/MDIX crossover for 100BASE-TX and 10BASE-T ports IEEE 802.3u Auto-Negotiation support for automatic speed and duplex selection 10BASE-T/100BASE-TX performance over 100 meters
Telephone Ports (Only for VoIP option)	Two RJ11 FXS POTS ports
CATV	Connector: F-type, 75Ω Frequency: 40 ~ 860MHz RF output > 75dBuV or 84dBuV @ -3dBm CNR > 50dB CSO < -65dBc CTB < -62dBc
Power Supply	DC12V 1.5A using external adaptor
Power Consumption	< 6 W (Not including PoE)
Operating Temperature	0℃～+50℃
Storage Temperature	-20℃～+85℃
Humidity at 85 °C	5%～95%
Size	268mm X 213mm X 56mm with cover 263mm X 183mm X 53mm without cover
Weight	1.3Kg

1.4 LED Panel

About the CATV ports and phone ports, please refer to the table on the cover of this manual.

LED panel behind the cover of 8 port ONU is shown in the following figure.

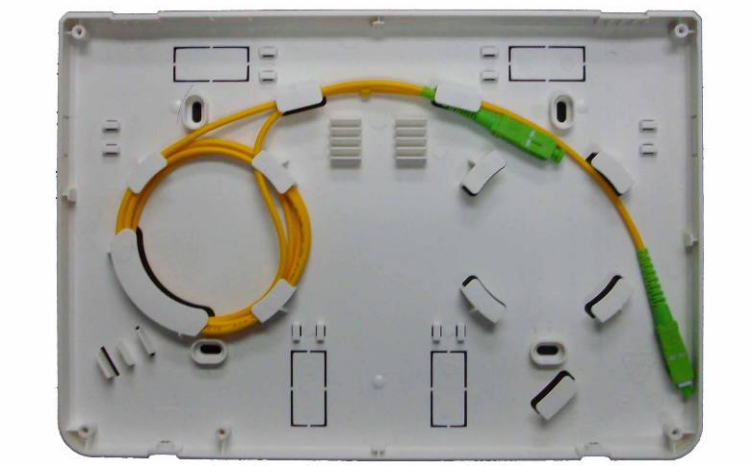


The following table shows the LED panel descriptions for AE208 P2P Switch Series.

LED Name	LED Color		Meaning
CATV	ON	Green	Monitored CATV optical power is from –8dbm to 0dbm.
		Yellow	Monitored CATV optical power is from -10dBm to -8dBm or from -0dBm to +2dBm
		Red	Monitored CATV optical power is beyond the above ranges.
	OFF		CATV is disabled.
LAN1~4/ LAN1~8	Green(100M)		Link and activity: ON = LAN port is connected, OFF = LAN is disconnected, Blinking = Data is transmitting(sending/receiving)
	Yellow (10M)		Link and activity: ON = LAN port is connected, OFF = LAN port is disconnected, Blinking = transmitting data (sending/receiving)
WAN	Green		Link and activity: ON = WAN port is connected, OFF = WAN is disconnected, Blinking = transmitting data (sending/receiving)
Phone1	Green		Phone 1 register and hook status: ON=registered, OFF = unregistered, blink = off-hook
Phone2	Green		Phone 2 register and hook status: ON=registered, OFF =unregistered, blink = off-hook
SYS	Red Yellow		Red ON——power on Yellow ON——start-up is successful.

1.5 Fiber Tray

AE208 P2P Switch series ONU uses standard fiber tray shown as follows. This fiber tray shall be installed firstly.



1.6 Connector Panel

The connector-panel includes an F-type CATV RF output port, RJ45 10BASE-T/100BASE-TX ports, a multi-function reset button and a power receptacle in front of the device and a 100Base-FX optical port at the back. About the CATV ports and Phone ports, please refer the table on the cover of this manual.

1.6.1 100Base-FX Optical Port

AE208 P2P Switch series WAN port uses standard SC / APC or FC / APC port connector to attach 9/125 micron single mode fiber optic cable with 1310nm TX/1490 nm RX data and 1550nm CATV overlay the figure below shows the location of the connectors.

1.6.2 10BASE-T/100BASE-TX Ports

AE208 P2P Switch series LAN ports use 10/100Base-TX RJ-45 (8-pin modular) port connectors. The 10BASE-T/100BASE-TX port connectors are configured as MDI-X (media-dependent interface-crossover). These ports connect over straight cables to the network interface controller (NIC) card in a node or server, similar to a conventional Ethernet repeater hub. If you are connecting it to an Ethernet hub or Ethernet switch, you need a crossover cable unless an MDI connection exists on the associated port of the attached device.

AE208 P2P Switch series LAN ports use auto sense ports that are designed to operate at 10 Mb/s or at 100 Mb/s, depending on the connecting device. These ports support the IEEE 802.3u auto negotiation standard, which means that when a port is connected to another device that also supports the IEEE 802.3u standard; the two devices negotiate for the best speed and duplex mode.

The 10/100Base-TX RJ-45 ports also support half- and full-duplex mode operation.

📖 Note:

Use only Category 5 copper unshielded twisted pair (UTP) cable connections when connecting 10/100Base-TX ports.

1.6.3 POTS Ports

AE208 Gateway uses an RJ-11 (2-pin modular) port connector for POTS connection and provides two TXS POTS ports.

1.6.4 Multi-Function Reset Button

The multi-function reset button performs the following functions:

- Press for (or less than) 3 second during the normal operation to change the device into static fixed IP mode;

```
Static fixed IP Mode Network Information:
IP Address:   192.168.0.253
Subnet:       255.255.255.0
```

- Press and hold for more than 3 seconds during normal operation to reload the factory default settings.

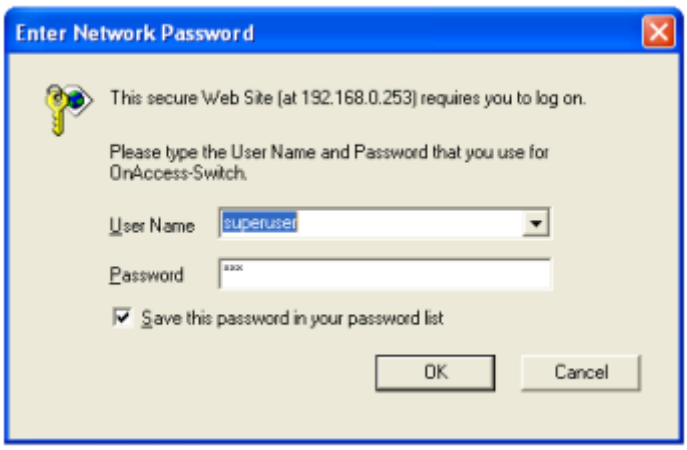
2 Login to AE208 Gateway

To access AE208 Gateway web management function, connect your PC to any LAN port of AE208 Gateway. Open a web-browser and type in the default address http://192.168.0.253 address field of the browser, and then press the **Enter** key.

Note:

To log in to the ONU, the IP address of your PC should be set in the same subnet addresses of the Switch. The IP address is 192.168.0.x ("x" is any number from 2 to 254), Subnet Mask is 255.255.255.0. After you enter the Web configuration page, you can modify the device IP address according to you need. For more details, please refer to 17.1 IP Configuration.

And then a login window will appear, as shown follows. Enter the default User Name and Password. Then click the Login button or press the **Enter** key, so that you can see the device system information.



Note:

You can click before “Remember my password”, and then you don’t need to type the password next time when you re-login.

There are two authorized user levels; the default username and password are shown as follows:

Level	Username	Password

user	superuser	123
admin	manager	123

And you also can use the multi-function reset button to change AE208 P2P Switch series to static fixed IP mode. Press the multi-function reset button for (or less than) 3 second during the normal operation to change the AE208 P2P Switch series into static fixed IP mode (IP address: 192.168.0.253, Subnet Mask: 255.255.255.0).

Note:

- ✧ After clicking <Apply> in the management web pages, all of the changes will be saved automatically.
- ✧ After testing, some supported browsers are listed as follows:
- ■ IE 7.0 or above
- ■ Firefox 3.5 or above
- ✧ Operating System: windows XP or windows vista

---

3 System Information

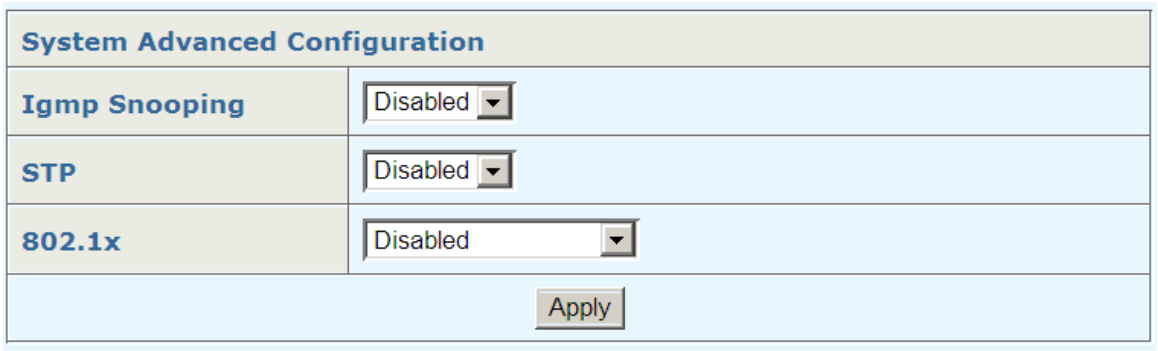
It shows the system information of the ONU as follows.

System Information	
System Name	
System Location	
MAC Address	00-1e-6e-00-56-12
Hardware Version	V1.0
Software Version	1.0.78
Boot Loader Version	1.0.45
Serial Number	r3a0036530
Local Date Time	Tue Nov 20 09:24:19 2012

System name and system address can be changed via SNMP software for available network management.

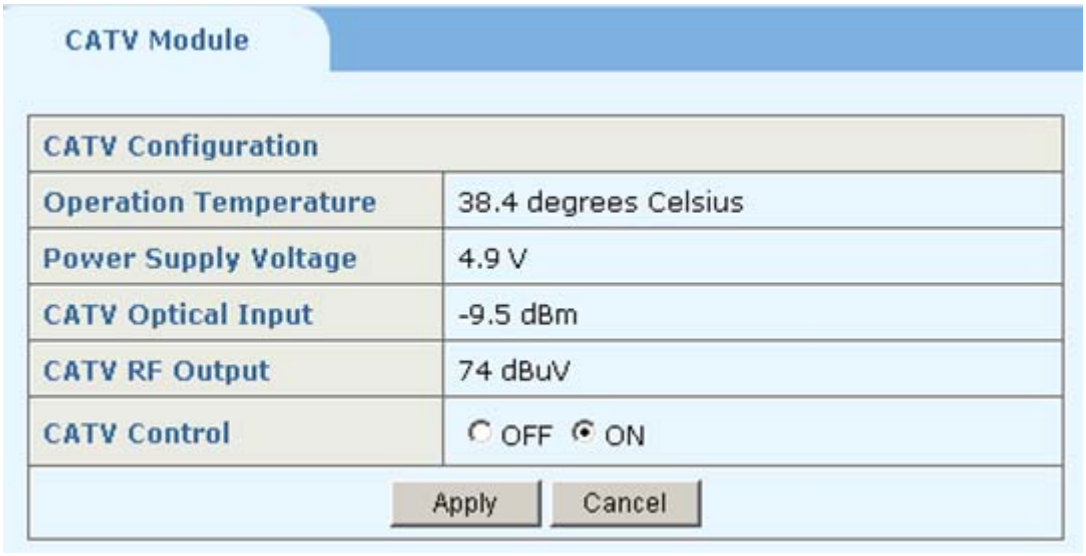
4 Advanced Configuration

On this page, you can enable or disable the following items: IGMP Snooping, STP and 802.1x globally.



5 CATV Configurations

This function is only for the ONUs with CATV option. You can check CATV status and change CATV configuration.



If this module supports the function of monitoring, Operating Temperature, Power Supply Voltage, CATV Optical Input, and CATV RF Output will be shown on this webpage.

If CATV control is set as “OFF”, the CATV module is powered off. If set as “ON”, CATV module is powered on.

6 Port Management

6.1 Port Configuration

Port Configuration page is used to set up the port parameters as shown follows.

State: If set as “Enabled”, the corresponding port will allow the Ethernet packets to pass normally. If set as “Disabled”, any Ethernet packet cannot pass.

Negotiation: The function provides a mechanism for exchanging configuration information between two ends of a link segment, and automatically selecting the highest performance mode of operation supported by both devices if it is enabled.

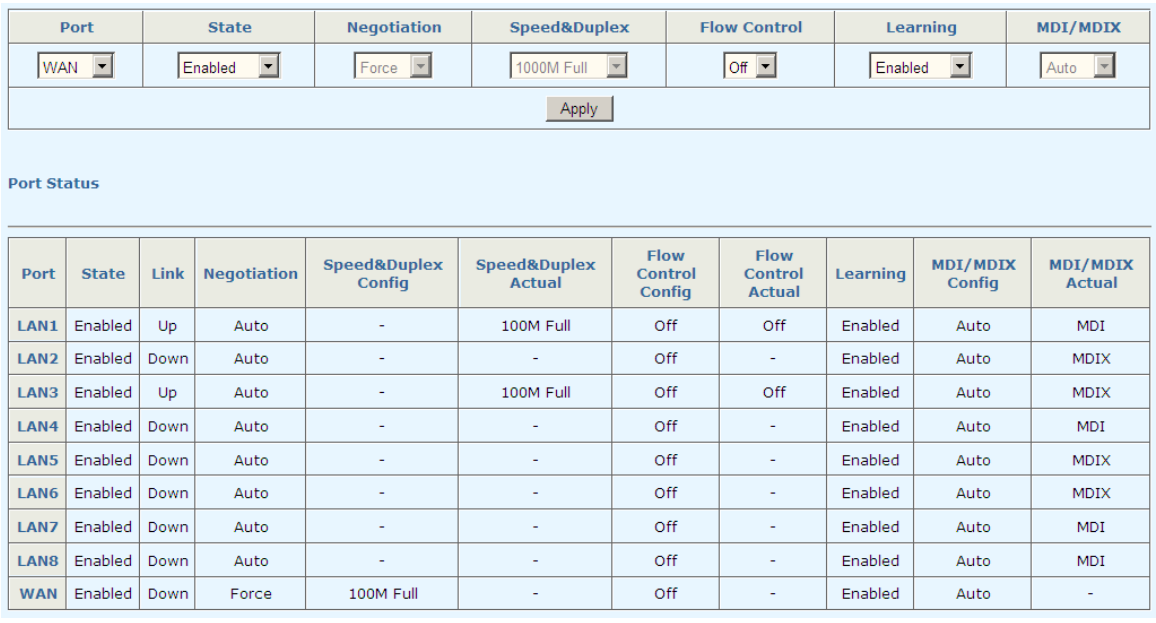
Speed&Duplex:
Speed: Allows the user to choose 100Mbps or 10Mbps mode.
Duplex: Allows the user to choose between full and half duplex mode.

Note: The speed and duplex of the WAN port is fixed to be 1000M Full.

Flow Control: Flow control can eliminate frame loss by “blocking” traffic from end station or segment connected directly to AE200 when it buffers fully. When it is enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade the overall performance of the segment attached to the hub.) The parameter allows flow control to be enabled or disabled.

Learning: To enable or disable the function of learning MAC address on the port.

MDI/MDIX: Select the type of cables: MDI, MDIX or Auto.



Port	State	Negotiation	Speed&Duplex	Flow Control	Learning	MDI/MDIX
WAN	Enabled	Force	1000M Full	Off	Enabled	Auto

Apply

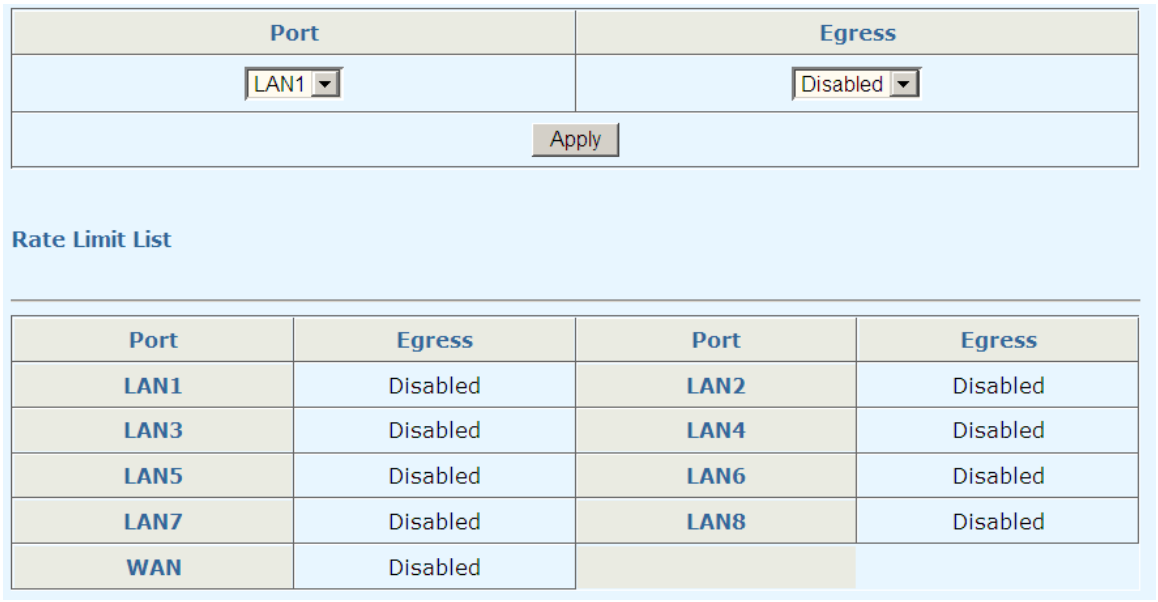
Port Status

Port	State	Link	Negotiation	Speed&Duplex Config	Speed&Duplex Actual	Flow Control Config	Flow Control Actual	Learning	MDI/MDIX Config	MDI/MDIX Actual
LAN1	Enabled	Up	Auto	-	100M Full	Off	Off	Enabled	Auto	MDI
LAN2	Enabled	Down	Auto	-	-	Off	-	Enabled	Auto	MDIX
LAN3	Enabled	Up	Auto	-	100M Full	Off	Off	Enabled	Auto	MDIX
LAN4	Enabled	Down	Auto	-	-	Off	-	Enabled	Auto	MDI
LAN5	Enabled	Down	Auto	-	-	Off	-	Enabled	Auto	MDIX
LAN6	Enabled	Down	Auto	-	-	Off	-	Enabled	Auto	MDIX
LAN7	Enabled	Down	Auto	-	-	Off	-	Enabled	Auto	MDI
LAN8	Enabled	Down	Auto	-	-	Off	-	Enabled	Auto	MDI
WAN	Enabled	Down	Force	100M Full	-	Off	-	Enabled	Auto	-

6.2 Port Bandwidth

You can configure the egress traffic limit on individual ports, so as to keep normal network service.

The bottom of the page will show the rate limit list.



7 VLAN Configurations

The traditional Ethernet is a broadcast network, where all hosts are in the same broadcast domain and connected with each other through hubs or switches. The hub is a physical layer device without the switching function, so it forwards the received packet to all ports. The switch is a link layer device which can forward the packet according to the MAC address of the packet. However, when the switch receives a broadcast packet or an unknown unicast packet whose MAC address is not included in the MAC address table of the switch, it will forward the packet to all the ports except the inbound port of the packet. In this case, a host in the network receives a lot of packets whose destination is not the host itself. Thus, plenty of bandwidth resources are wasted, causing potential serious security problems.

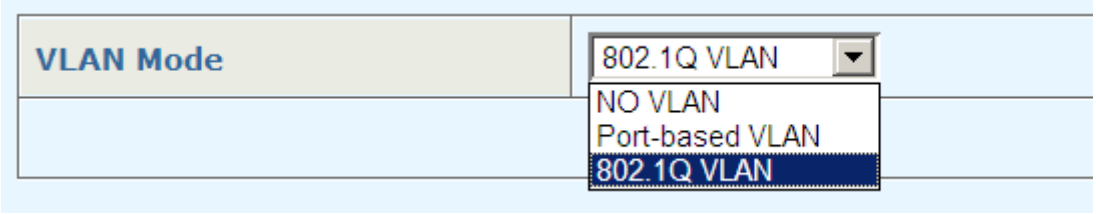
The traditional way to isolate broadcast domains is to use routers. However, routers are expensive and provide few ports, so they cannot subnet the network particularly.

The virtual local area network (VLAN) technology is developed for switches to control broadcast in LANs.

By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate with each other as if they are in a LAN. However, hosts in different VLANs cannot communicate with each other directly.

7.1 Advanced VLAN Mode Configuration

On this page, you can select “NO VLAN” to disable VLAN on the device, “Port-based VLAN” or “802.1Q VLAN”.



7.2 Port-based VLAN

Port-based VLAN technology introduces the simplest way to classify VLANs. You can isolate the hosts and divide them into different virtual workgroups through assigning the ports on the device connecting to hosts to different VLANs.

This way is easy to implement and manage and it is applicable to hosts with relatively fixed positions.

The bottom part of this page lists all port-based VLAN groups that have been set up. As it shows, port 1 and 3 are within VLAN 1, they can communicate with each other, but they cannot communicate with other ports in other VLAN.

Port-based VLAN Setting									
VID	1								
Vlan Name									
Port	Ethernet0/								Ethernet1/
	1	2	3	4	5	6	7	8	1
Member	☐	☐	☐	☐	☐	☐	☐	☐	☐
Create									

VLAN List

VID	Vlan Name	Port List	Modify	Delete
1	VLAN 1	Ethernet0/1,3	Modify	Delete
2	VLAN 2	Ethernet0/5-6	Modify	Delete
3	VLAN 3	Ethernet0/7-8	Modify	Delete

🕮 Note：Select “port-based VLAN” in Advanced VLAN Mode page before configuring port-based VLAN.

7.3 802.1Q VLAN Configuration

🕮 Note：Select “802.1Q VLAN” in Advanced VLAN Mode page before configuring 802.1Q VLAN.

7.3.1 802.1Q VLAN

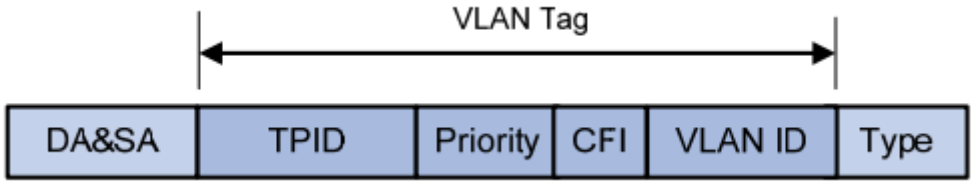
VLAN tags in the packets are necessary for the switch to identify packets of different VLANs. The switch works at Layer 2 and it can identify the data link layer encapsulation of the packet only, so you can add the VLAN tag field into only the data link layer encapsulation if necessary.

In 1999, IEEE issues the IEEE 802.1Q protocol to standardize VLAN implementation, defining the structure of VLAN-tagged packets.

In traditional Ethernet data frames, the type field of the upper layer protocol is encapsulated after the destination MAC address and source MAC address, as shown in the follow figure of Encapsulation format of traditional Ethernet frames.

DA refers to the destination MAC address, SA refers to the source MAC address, and Type refers to the protocol type of the packet. IEEE 802.1Q protocol defines that a 4-byte VLAN tag is encapsulated after the destination MAC address and source MAC address to show the information about VLAN.

As shown in the following figure of Format of VLAN tag, a VLAN tag contains four fields, including TPID, priority, CFI, and VLAN ID.



TPID is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100 in AE200 Ethernet switches.

Priority is a 3-bit field, referring to 802.1p priority. Refer to section “QoS & QoS profile” for details.

CFI is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format in different transmission media. This field is not described in detail in this chapter.

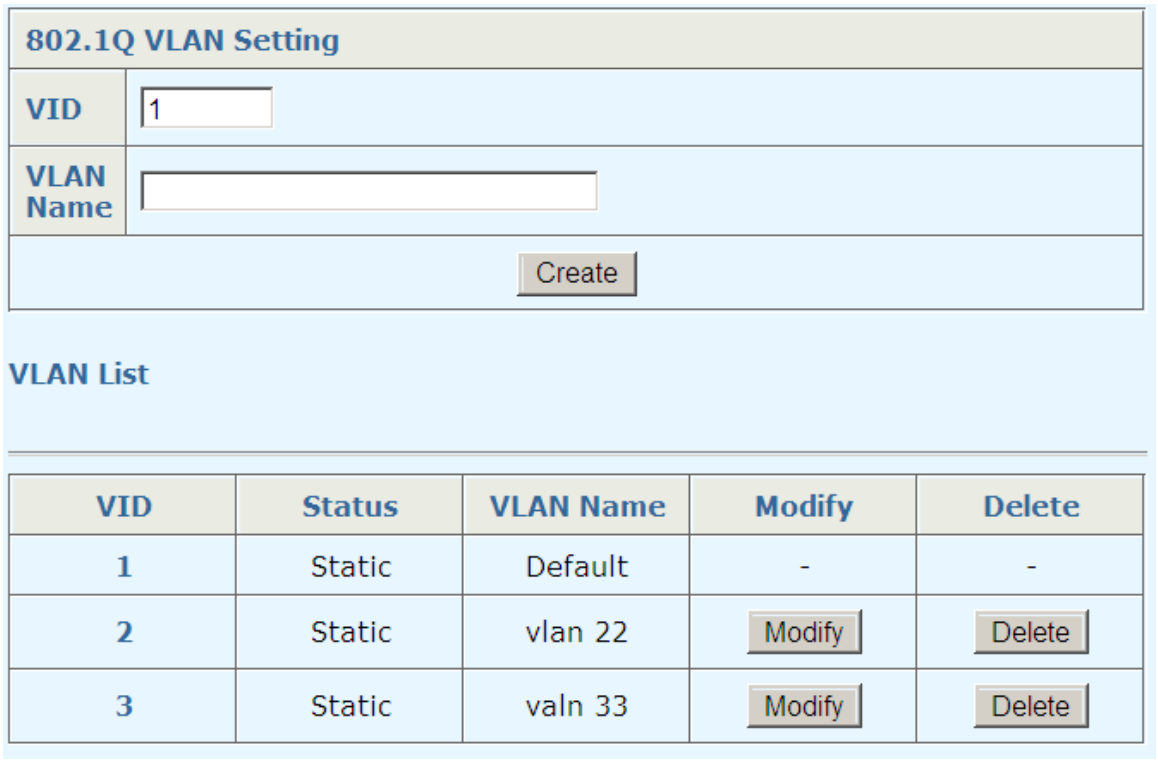
VLAN ID is a 12-bit field, indicating the ID of the VLAN to which this packet belongs. It is in the range of 0 to 4,095. Generally, 0 and 4,095 is not used, so the field is in the range of 1 to 4,094.

VLAN ID identifies the VLAN to which a packet belongs. When the switch receives a packet carrying no VLAN tag, it will encapsulate a VLAN tag with the default VLAN ID of the inbound port for the packet, and the packet will be assigned to the default VLAN of the inbound port for transmission.

The VLAN group with VLAN identifier (VID) of 1 is a default VLAN group. Each port is a member of this group by default, and its value can be modified.

On this tab page, you can create a new VLAN group with specific VID and VLAN group name. Up to 64 VLAN groups can be created; each VLAN group can have an ID number from 1 to 4094.

The bottom part of this page lists all existing VLAN groups, as well as the information of each VLAN group. Users can also modify or delete an existing VLAN group except the default VLAN with VID 1.



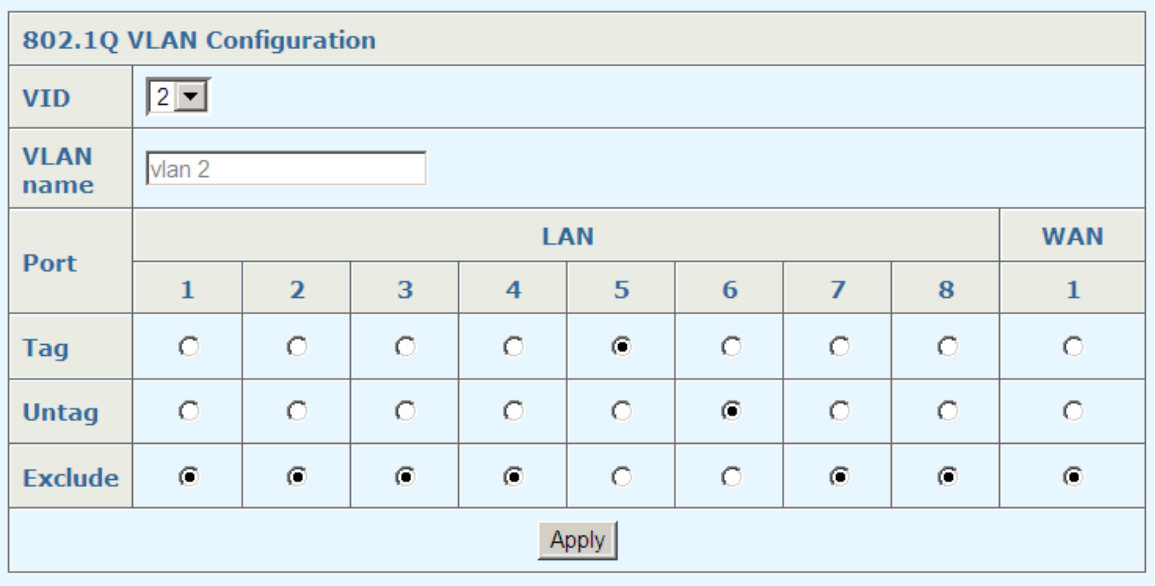
7.3.2 802.1Q Configuration

Configure the member ports of a VLAN to be a specific type.

Tag Indicates the port is a tagged member of the VLAN group. All packets forwarded by the port are tagged. The packets contain VLAN information.

Untag Indicates the port is an untagged VLAN member of the VLAN group. Packets forwarded by the port are untagged.

Exclude Excludes the port from the VLAN group.



7.3.3 802.1Q Port

This tab page configures 802.1Q VLAN port parameters:

PVID: Each port can have only one Port VLAN ID (PVID), an untagged Ethernet package will be tagged a VID of PVID when arriving at the port. The default PVID is 1 for each port.

Link Type: An Ethernet port on an AE208 Gateway device can operate in one of the three link types:

- **Access**: An access port can belong to only one VLAN, and is generally used to connect user PCs. Tag is deleted when transmitting packets.
- **Trunk**: A trunk port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs, and is generally used to connect another switch. A trunk port can belong to multiple VLANs, but it can only be configured as untagged in one VLAN. All packages are tagged, except when an egress package is in a VLAN group with VID the same as PVID.
- **Hybrid**: A hybrid port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs, and can be used to connect either a switch or user PCs. A Hybrid port is similar to a Trunk port, except it leaves the user a flexibility of configuring each port as tagged or untagged.

Frame Type: Select how the port accepts Ethernet package. When **Admit All** is selected, the port accepts all ingress packages; while **Admit Only Tagged** accepts only tagged packages, and discards untagged ones.

VLAN Ingress Filtering: When enabled, an Ethernet package is discarded if this port is not a member of the VLAN with which this package is associated. When being disabled, all packages are forwarded in accordance with the 802.1Q VLAN bridge specification.

Note:

A hybrid port allows the packets of multiple VLANs to be sent without tags, but a trunk port only allows the packets of the default VLAN to be sent without tags.

You can configure all the three types of ports on the same device.

Port	PVID	Link Type	Frame Type	VLAN Ingress Filtering
LAN1	1	Hybrid	Admit All	Disabled
Apply				

Port Status

Port	PVID	Link Type	Frame Type	VLAN Ingress Filtering
LAN1	1	Hybrid	Admit All	Disabled
LAN2	1	Hybrid	Admit All	Disabled
LAN3	1	Access	Admit Only Tagged	Enabled
LAN4	2	Trunk	Admit Only Tagged	Enabled
LAN5	1	Hybrid	Admit All	Disabled
LAN6	2	Hybrid	Admit All	Disabled
LAN7	1	Hybrid	Admit All	Disabled
LAN8	1	Hybrid	Admit All	Disabled
WAN	1	Hybrid	Admit All	Disabled

8 QoS Configuration

In data communications, Quality of Service (QoS) is the ability of a network to provide differentiated service guarantees for diversified traffic in terms of bandwidth, delay, jitter, and drop rate.

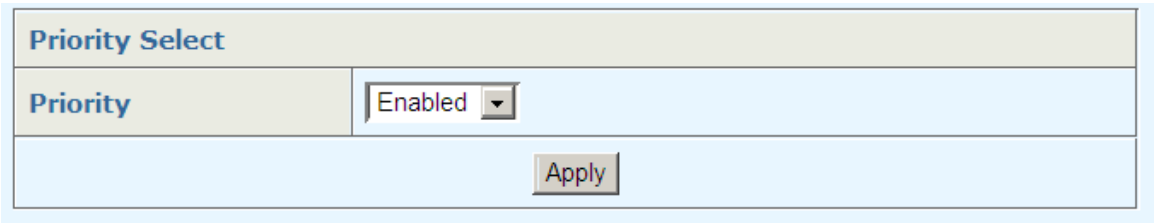
On traditional IP networks, devices treat all packets equally and handle them using the first in first out (FIFO) policy. All packets share the resources of the network and devices. How many resources the packets can obtain completely depends on the time they arrive. This service is called best-effort. It delivers packets to their destinations as possibly as it can, without any guarantee for delay, jitter, packet loss ratio, reliability and so on.

The Internet has been growing along with the fast development of networking technologies. More and more users take the Internet as their data transmission platform to implement various applications. Besides traditional applications such as WWW, e-mail and FTP, network users are experiencing new services, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). The enterprise users expect to connect their regional branches together through VPN technologies to carry out operational applications, for instance, to access the database of the company or to monitor remote devices through Telnet. These new applications have one thing in common, that is, they all have special requirements for bandwidth, delay, and jitter. For instance, videoconference and VoD need large bandwidth, low delay and jitter. As for mission-critical applications, such as transactions and Telnet, they may not require large bandwidth but do require low delay and preferential service during congestion.

8.1 QoS Configuration

8.1.1 General QoS Configuration

You can enable or disable the priority of the device.



8.1.2 Port QoS Configuration

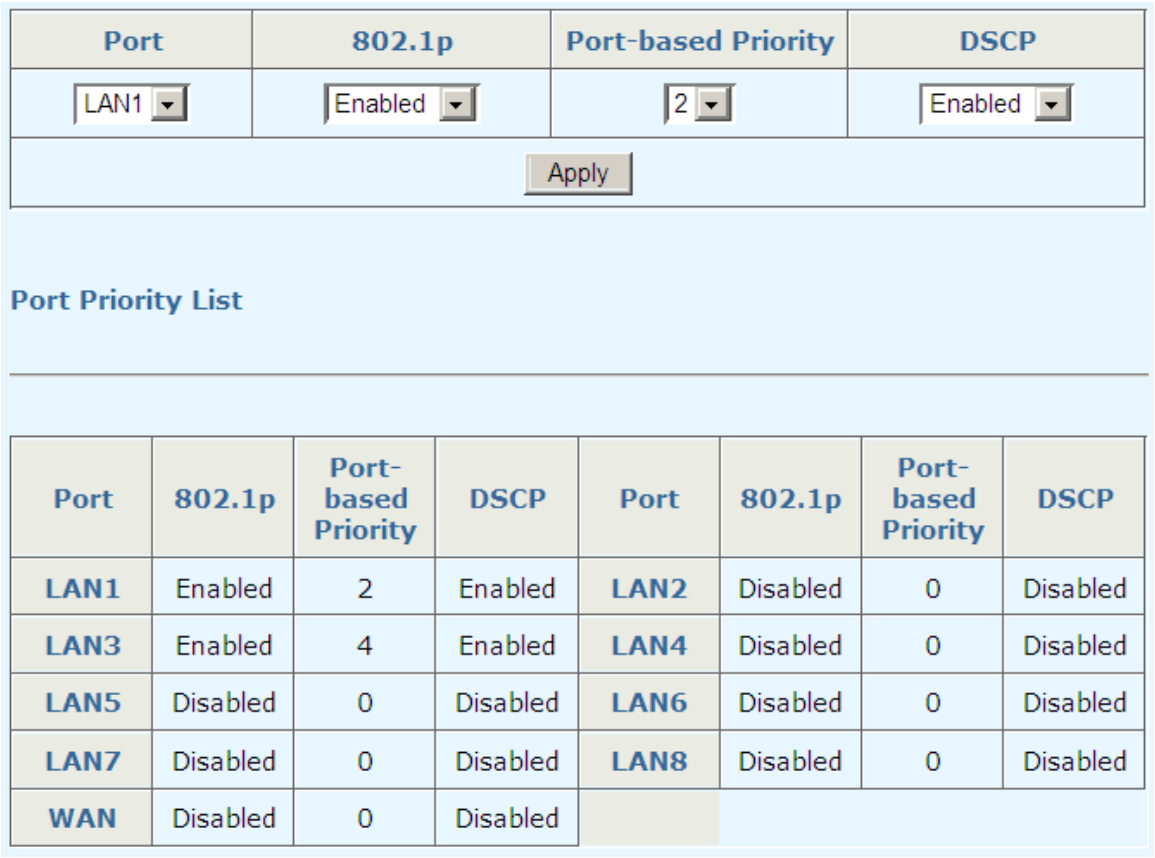
802.1p, port-based priority and DSCP can be configured for each port. And the bottom of the page

shows the port priority list.

802.1P Enable or disable 802.1P.

Port-based Priority There are 8 priorities (0~7) corresponding to 802.1P priority.

DSCP Enable or disable DSCP.



8.2 Scheduling Mechanism

This page sets the queue scheduling mechanism as strict priority or Weighted Round-Robin (8:4:2:1).

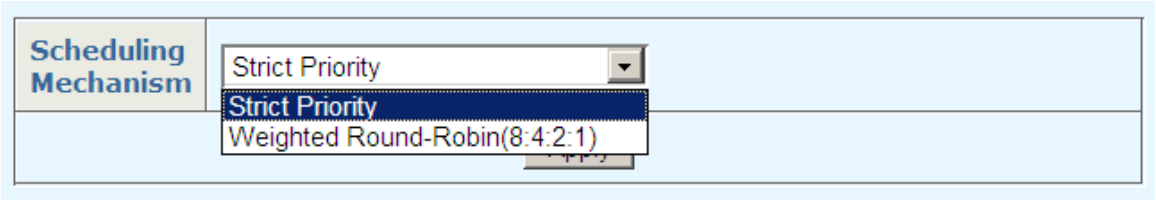
Strict Priority: SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. Assume that there are eight output queues on the port and the preferential queue classifies the eight output queues on the port into eight classes, which are queue7, queue6, queue5, queue4, queue3, queue2, queue1, and queue0. Their priorities decrease in order.

In queue scheduling, SP sends packets in the queue with higher priority strictly following the priority order from high to low. When the queue with higher priority is empty, packets in the queue with lower priority are sent. You can put critical service packets into the queues with higher priority and put non-critical service (such as e-mail) packets into the queues with lower

priority. In this case, critical service packets are sent preferentially and non-critical service packets are sent when critical service groups are not sent.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved” because they are not served.

Weighted Round-Robin (WRR) (8:4:2:1): WRR queue-scheduling algorithm schedules all the queues in turn and every queue can be assured of a certain service time. Assume there are four priority queues on a port. WRR configures a weight value for each queue, which is Q1、Q2、Q3 and Q4. The weight value indicates the proportion of obtaining resources. On a 150 M port, configure the weight value of WRR queue-scheduling algorithm to 1、2、4 and 8 (corresponding to Q1、Q2、Q3 and Q4 in order). In this way, the queue with the lowest priority can get 10 Mbps bandwidth at least, and the disadvantage of SP queue-scheduling that the packets in queues with lower priority may not get service for a long time is avoided. Another advantage of WRR queue is that: though the queues are scheduled in order, the service time for each queue is not fixed; that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use.



8.3 Transmit Queues

This page sets the local precedence for 802.1p priority. The following table lists the default mapping between 802.1p priority and local precedence:

802.1p priority	Local precedence
0	Q0
1	Q0
2	Q1
3	Q1
4	Q2
5	Q2
6	Q3
7	Q3

Transmit Queues Setting								
Priority	0	1	2	3	4	5	6	7
Transmit Queues	◉ Q0	◉ Q0	○ Q0	○ Q0	○ Q0	○ Q0	○ Q0	○ Q0
	○ Q1	○ Q1	◉ Q1	◉ Q1	○ Q1	○ Q1	○ Q1	○ Q1
	○ Q2	○ Q2	○ Q2	○ Q2	◉ Q2	◉ Q2	○ Q2	○ Q2
	○ Q3	○ Q3	○ Q3	○ Q3	○ Q3	○ Q3	◉ Q3	◉ Q3
Apply								

You can change the priority map according to your need, if unnecessary, click <Apply> directly.

8.4 DSCP Map

This page sets the mapping between the DSCP value and the local precedence priority. DSCP (Differentiated Services CodePoint) priority ranges from 0 to 63.

DSCP Map Setting															
DSCP Map	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Queue	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSCP Map	0 1 2 3	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Queue		0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSCP Map	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
Queue	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSCP Map	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
Queue	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSCP Map	60	61	62	63	.										
Queue	0	0	0	0	.										
Apply															

9 Forwarding Configurations

AE208 Gateway series ONU forwarding mechanism has unicast MAC address forwarding and multicast MAC address forwarding, the following is the detailed introduction.

9.1 Unicast MAC Address

MAC address forwarding table: the device forwards the packets to the corresponding port according to the packet destination MAC address. The MAC address forwarding table reflects the relationship between the MAC address and the forwarding port.

A MAC address table is maintained for packet forwarding. Each entry in this table indicates the following information:

- The MAC address of a connected network device
- The interface to which the device is connected
- The VLAN to which the interface belongs

Unicast mode: If an entry is available for the destination MAC address, the device forwards the frame directly from the outgoing port.

Unicast MAC address configuration is for the unicast forwarding mode.

9.1.1 MAC Address Configuration

You can configure the unicast MAC address for each port in each VLAN and the port type. You can follow the following steps:

Step 1 Select a VID.

Step 2 Type unicast MAC address to transmit with the form of xx-xx-xx-xx-xx-xx.

Step 3 Select a port to transmit.

 Caution: The port should belong to the VLAN.

Step 4 Select static, dynamic or blackhole.

Static: Bind a MAC address to a port.
Dynamic: Make a port to learn a MAC address temporarily.
Blackhole: Make a port not learn the MAC address.

After configuration, a MAC address list will be shown at the bottom. And the dynamic MAC address will be shown in the Dynamic Unicast MAC list within the valid time. The port and type in the entries can be modified and the entries can be deleted.

Forwarding Table

VID	Unicast MAC Address[xx-xx-xx-xx-xx-xx]	Port	Type
1		LAN1	Static

Apply

MAC Address Entries

VID	Unicast MAC Address	Port	Type	Modify	Delete
1	00-11-11-11-11-11	LAN1	Static	Modify	Delete
2	00-01-21-21-12-12	LAN6	Blackhole	Modify	Delete
1	00-22-22-22-22-22	LAN1	Dynamic	Modify	Delete

9.1.2 Dynamic Unicast MAC

It shows the dynamic MAC addresses which are learnt by the port and added manually. They can be deleted manually, and it updates the list when the timer is timeout. By default, the timer is 300 seconds.

VID	Unicast MAC Address	Port	Type	Delete
1	00-1e-6e-00-1c-80	LAN4	Dynamic	Delete
1	00-1e-6e-00-58-33	LAN4	Dynamic	Delete
1	00-22-22-22-22-22	LAN1	Dynamic	Delete
1	4c-1f-cc-11-da-c5	LAN4	Dynamic	Delete
1	50-e5-49-e4-44-f7	LAN2	Dynamic	Delete
1	ec-a8-6b-82-ec-6e	LAN4	Dynamic	Delete

9.2 Multicast MAC Address

In the network, packets are sent in three modes: unicast, broadcast and multicast. In unicast, the

source server sends separate copy information to each receiver. When a large number of users require this information, the server must send many pieces of information with the same content to the users. Therefore, large bandwidth will be occupied. In broadcast, the system transmits information to all users in a network. Any user in the network can receive the information, no matter the information is needed or not.

Point-to-multipoint multimedia business, such as video conferences and VoD (video-on-demand), plays an important part in the information transmission field. Suppose a point to multi-point service is required, unicast is suitable for networks with sparsely users, whereas broadcast is suitable for networks with densely distributed users. When the number of users requiring this information is not certain, unicast and broadcast deliver a low efficiency. Multicast solves this problem. It can deliver a high efficiency to send data in the point to multi-point service, which can save large bandwidth and reduce the network load.

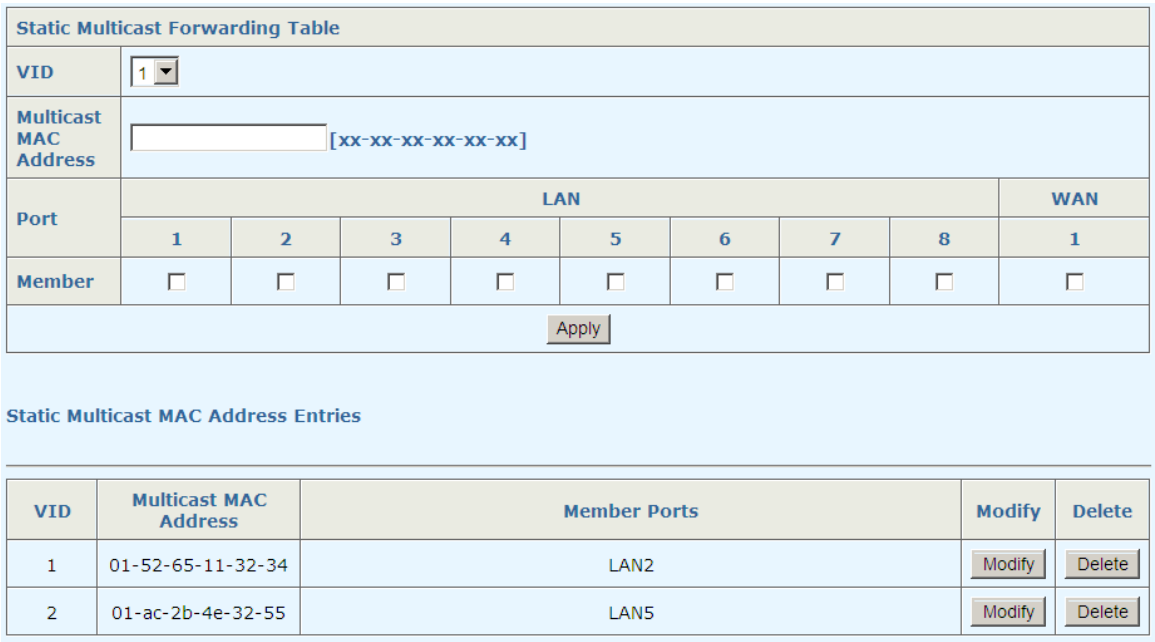
Features of multicast:

- The number of receivers is not certain. Usually point-to-multipoint transmission is needed;
- Multiple users receiving the same information form a multicast group. The multicast information sender just need sends the information to the network device once;
- Each user can join and leave the multicast group at any time;
- Real time is highly demanded and certain packets drop is allowed.

 Caution：

A multicast source does not necessarily belong to a multicast group. A multicast source sends data to a multicast group, and it is not necessarily a receiver. Multiple multicast sources can send packets to the same multicast group at the same time.

You can set to transmit packets with multicast destination MAC address from some ports, and the Static Multicast MAC Address Entries List will be displayed at the bottom, as it shows, the port 2 in VLAN 1 can forward packets to the multicast MAC 01-52-65-11-32-34 and port 5 in VLAN 2 can forward packets to multicast MAC 01-ac-2b-4e-32-55.



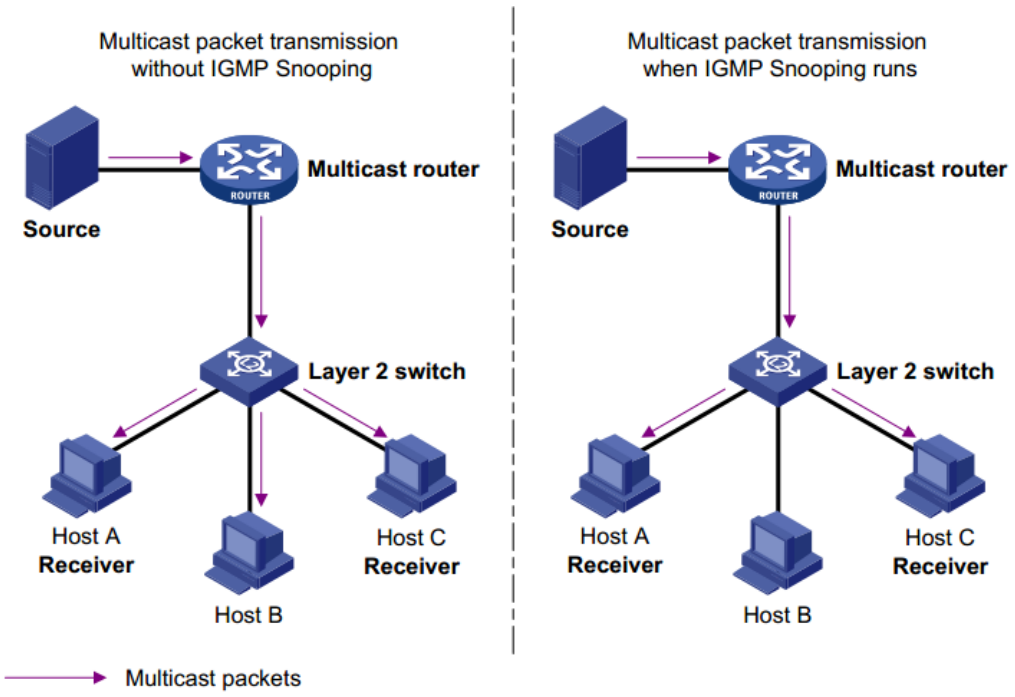
9.3 IGMP Snooping Configuration

📖 Note: Before configuring IGMP Snooping, first enable IGMP Snooping in the Advanced Configuration.

Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

By listening to and analyzing IGMP messages, a Layer 2 device running IGMP Snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

As shown in the following figure, when IGMP Snooping is not running on the device, multicast packets are broadcast to all devices at Layer 2. When IGMP Snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2.



9.3.1 IGMP Snooping

With the wider application of multicast, IGMP V3 is used more and more. It adds the source multicast filtering function, making the receiver not only specify the multicast group to join but also specify to receive the multicast information from certain multicast group.

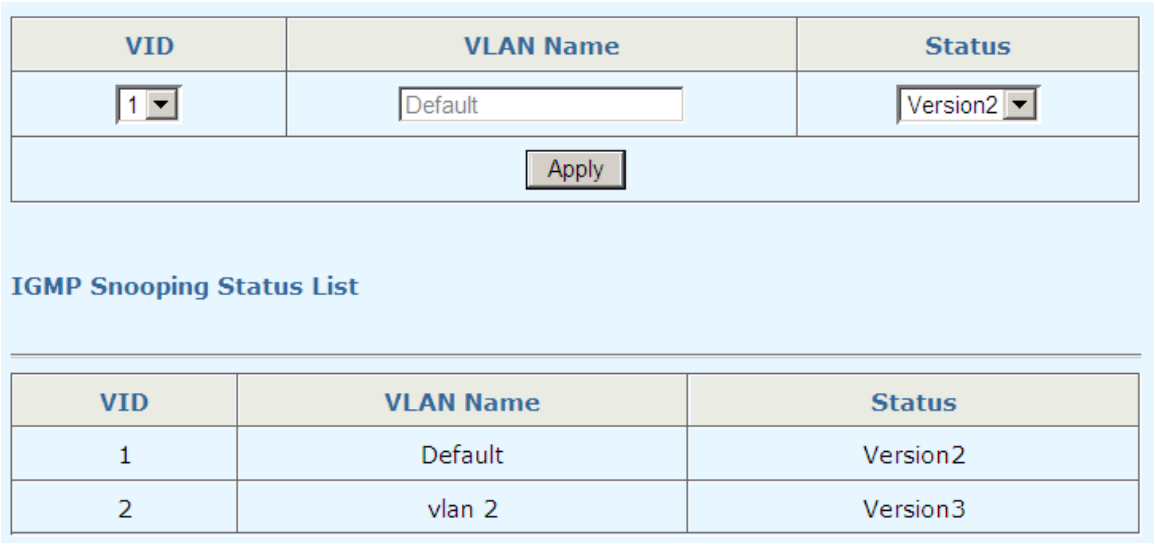
The configuration steps are as follows:

Step 1 Specify the VLAN ID of a multicast group, the VLAN name can be no changed here.

Step 2 Enable or disable IGMP Snooping on the field of Statue, if enable it, select IGMP version 2 or 3. Until now, IGMP has three versions: including IGMP Version 1 (defined by RFC1112), IGMP Version 2 (defined by RFC2236), and IGMP Version 3 (defined by RFC 3376).

On this page, you can enable IGMP Snooping feature for a VLAN group. By default, the IGMP Snooping feature is disabled.

The bottom part of this page lists all VLAN IGMP Snooping status.



9.3.2 Route Port

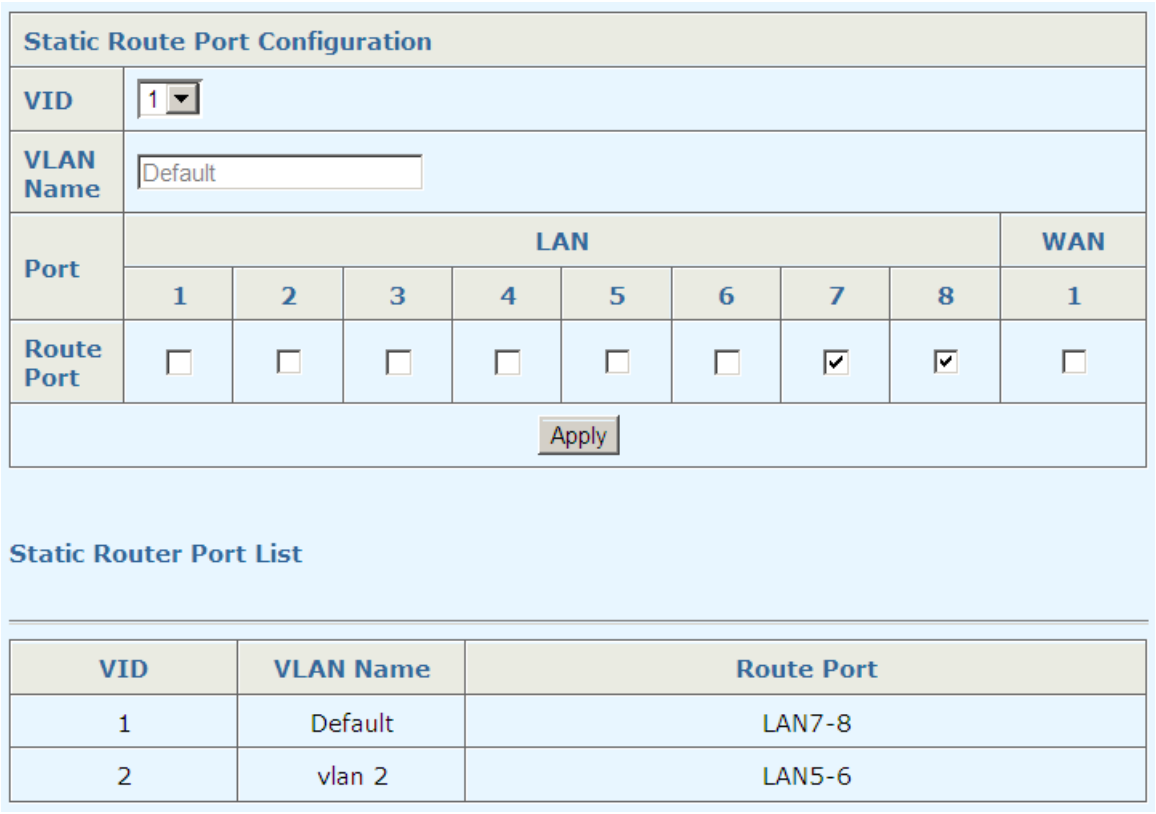
On this page, you can configure a port in a specified VLAN group as a static router port. By default, a port is not a static router port.

If a port is fixed to receive the packets from a multicast group, it can be configured to join in the multicast group statically, so that the device can receive IGMP message by the port from router.

Route port: the port directly connected to multicast devices, which is the IGMP Querier.

The bottom part of this page lists static router ports of all VLANs.

Caution: the router port should be within the VLAN. Please refer to 7 VLAN Configuration.



9.3.3 Misc Configuration

This tab page sets IGMP Snooping Misc configuration parameters: Host Timeout, Route Timeout, IGMP Querier, Query Transmit Interval, Max Response Time, and Fast Leave.

Host Timeout The device starts for a port after the port joins a multicast group. After it time out, the port will be deleted from the group. It is in the range of 200 to 1000; by default, the value is 260 seconds.

Route Timeout The device starts Router Timeout for each router port when it time out, it will be deleted from the router port list. It is in the range of 1 to 1000; by default, the value is 105 seconds.

IGMP QuerierIGMP Querier sends IGMP general query packets to all the hosts and router ports in the network segment to check the multicast group memebers. By default, IGMP Querier is disabled.

Query Transmit Interval The interval IGMP Querier sends IGMP general query packets to all the hosts and router ports. After it times out, it will delete the port form the group. It is in the range of 1 to 255, by default, the value is 125 seconds.

Max Response Time The maximum response time of the IGMP general query packets. After it times out, it will delete the port form the group. It is in the range of 1 to 25, by default, the value is 10 seconds.

Fast Leave If Fast Leave is enabled, when a port receives a leave message from a mulicast

group, the switch will delete the port directly. In this way, when the port has only one user, it can save bandwidth.

10 Security

It includes management security, port authentication, MAC authenticaiton and storm control.

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

10.1 Management Security

📖 Note： Enable 802.1 in Advanced Configuration first.

This page configures the 802.1x system as follows: Authentication RADIUS Server IP, Authentication Port, Authentication Shared Key, Accounting RADIUS Server IP, Accounting Port and Accounting Shared Key.

Authentication RADIUS Server IP: IP address of the radius server to be used, a valid unicast address in dotted decimal notation; the default value is 192.168.0.234.

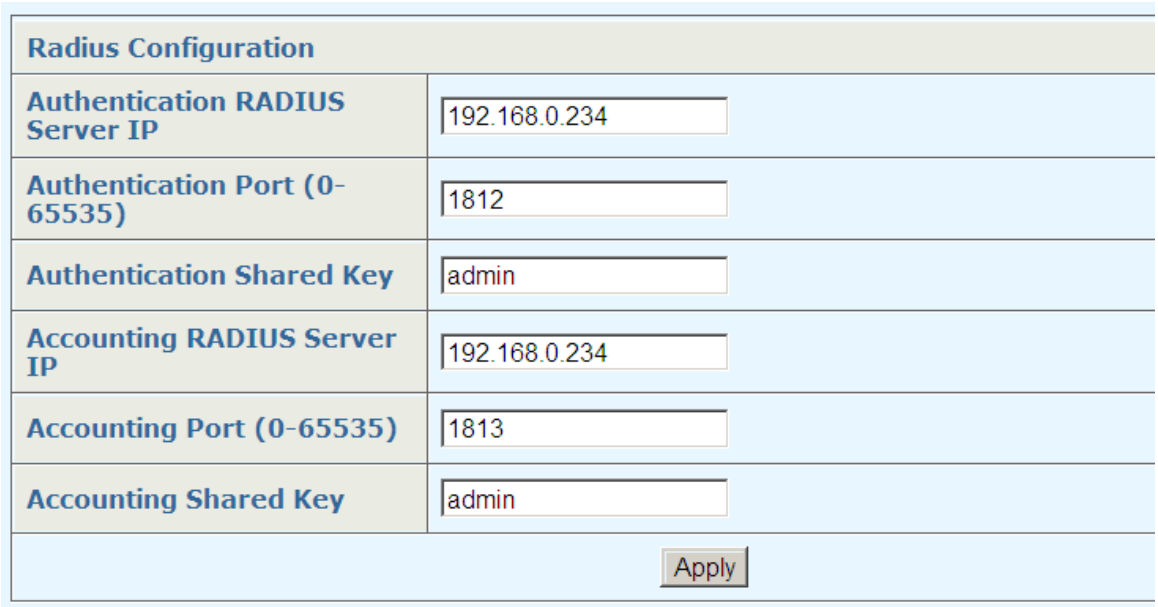
Authentication Port: UDP port number of the radius server, ranging from 0 to 65535; the default value is 1812.

Authentication Shared Key: Sets a shared key for radius messages. String length is 1 to 15 characters.

Accounting RADIUS Server IP: IP address of accounting radius server to be used, a valid unicast address in dotted decimal notation; the default value is 192.168.0.234.

Accounting Port: UDP port number of the radius server, ranging from 0 to 65535; the default value is 1813.

Accounting Shared Key: Sets a shared key for accounting radius. String length is from 1 to 15 characters.



10.2 Port Authentication

IEEE 802.1x authentication system uses EAP protocol to exchange information between a RADIUS client and the RADIUS server. When the client passes the authentication, the server will send user information to the device, and then PAE decides whether to set the port as authorized or unauthorized according to the RADIUS indication: accept or reject.

📖 Note： Enable 802.1 in Advanced Configuration first.

10.2.1 802.1x Port

RADIUS operates in the following manner:

1. The host initiates a connection request carrying the username and password to the RADIUS client.
2. Having received the username and password, the RADIUS client sends an authentication request (Access-Request) to the RADIUS server, with the user password encrypted by using the Message-Digest 5 (MD5) algorithm and the shared key.
3. The RADIUS server authenticates the username and password. If the authentication succeeds, it sends back an Access-Accept message containing the user's authorization information. If the authentication fails, it returns an Access-Reject message.
4. The RADIUS client permits or denies the user according to the returned authentication result. If it permits the user, it sends a start-accounting request (Accounting-Request) to the RADIUS server.
5. The RADIUS server returns a start-accounting response (Accounting-Response) and starts accounting.

6. The user accesses the network resources.
7. The host requests the RADIUS client to tear down the connection and the RADIUS client sends a stop-accounting request (Accounting-Request) to the RADIUS server.
8. The RADIUS server returns a stop-accounting response (Accounting-Response) and stops accounting for the user.
9. The user stops access to network resources.

On this tab page, 802.1x Admin, Re-authentication as well as Guest VLAN can be enabled for a specified Ethernet port, and a specific **PortControl** mode can also be selected. The **PortControl** can be selected among Auto, ForceAuthorized and ForceUnauthorized.

Auto The auto access control mode. When a port operates in this mode, all the unauthenticated hosts connected to it are unauthorized, and only EAPoL packets can be exchanged between the switch and the hosts. And the authenticated hosts connected to the port are authorized to access the network resources.

ForceAuthorized The force-authorized access control mode. When a port operates in this mode, all the hosts connected to it can access the network resources without authentication.

ForceUnauthorized The force-unauthorized access control mode. When a port operates in this mode, the hosts connected to it cannot access the network resources.

Guest VLAN A guest VLAN can be enabled for each IEEE 802.1x port on the switch to provide limited services to the clients.

The bottom part of this page lists all 802.1x port status.

Port	802.1x Admin	PortControl	ReAuth	Guest VLAN
LAN1	Enabled	ForceUnauthorized	Enabled	Disabled

Apply

802.1x Port Status List

Port	802.1x Admin	PortControl	ReAuth	Guest VLAN	Port State
LAN1	Enabled	ForceUnauthorized	Enabled	Disabled	Unauthorized
LAN2	Disabled	ForceAuthorized	Enabled	Disabled	Authorized
LAN3	Enabled	ForceUnauthorized	Enabled	Disabled	Link Down
LAN4	Disabled	ForceAuthorized	Enabled	Disabled	Link Down
LAN5	Disabled	ForceAuthorized	Enabled	Disabled	Link Down
LAN6	Disabled	ForceAuthorized	Enabled	Disabled	Link Down
LAN7	Disabled	ForceAuthorized	Enabled	Disabled	Link Down
LAN8	Disabled	ForceAuthorized	Enabled	Disabled	Link Down
WAN	Disabled	ForceAuthorized	Enabled	Disabled	Link Down

10.2.2 802.1x Misc

This tab page configures 802.1x: Quiet Period, Tx Period, Supplicant Timeout, Server Timeout, Max Request Count, Reauth Period, and Guest VLAN.

Quiet Period Sets the quiet-period, when a supplicant system fails to pass the authentication, the switch quiets for the set period before it processes another authentication request re-initiated by the supplicant system. During this quiet period, the device does not perform any 802.1x authentication-related actions for the supplicant system. The value is in the range of 1 to 65535, and is set to 60 seconds by default.

Tx Period Sets the transmission timer, and is triggered in two cases. The first case is when the client requests authentication, the switch sends a unicast request/identity packet to a supplicant system and then triggers the transmission timer. The device sends another request/identity packet to the supplicant system if it does not receive the reply packet from the supplicant system when this timer times out. The second case is when the device authenticates the 802.1x client which cannot request for authentication actively. The device sends multicast request/identity packets periodically through the port enabled by 802.1x function. In this case, this timer sets the interval to send the multicast request/identity packets. It is in the range of 1 to 65535; the default value is 30 seconds.

Supplicant Timeout: Sets the supplicant system timer, this timer sets the supp-timeout period and is triggered by the device after the device sends a request/challenge packet to a supplicant system. The device sends another request/challenge packet to the supplicant system if the device does not receive any response from the supplicant system when this timer times out. It is in the range of 1 to 300; the default value is 30 seconds.

Server Timeout Sets the radius server timer, this timer sets the server-timeout period. After sending an authentication request packet to the radius server, a device sends another authentication request packet if it does not receive any response from the radius server when this timer times out. It is in the range of 1 to 300; the default value is 30 seconds.

Max Request Count Sets the maximum number of times that a device sends authentication request packets to a user. It is in the range of 1 to 10, and the default value is 2.

Reauth Period Sets re-authentication interval in seconds. After this timer expires, the device indicates: 802.1x re-authentication. It is in the range of 60 to 7200; the default value is 60 seconds.

Guest VLAN Can choose a guest VLAN on the device to provide limited services to clients, such as downloading.

When enabling a guest VLAN on an IEEE 802.1x port, the device assigns the client port to a guest VLAN in case that the device does not receive any response to its EAP request/identity frame, or EAPOL packets are not sent by the client. The device allows the client that is failed in authentication to access the guest VLAN, regardless of whether EAPOL packets have been detected. However, access to external ports out of guest VLAN still needs to be authorized.

802.1x Misc Configuration	
Quiet Period (1-65535)	60 sec
Tx Period (1-65535)	30 sec
Supplicant Timeout (1-300)	30 sec
Server Timeout (1-300)	30 sec
Max Request Count(1-10)	2
Reauth Period (60-7200)	60 sec
Guest VLAN	None
	Apply

10.3 MAC Authentication

Note： Enable MAC Authenticantion in 4 Advanced Configuration first.

MAC address authentication is port and MAC address-based authentication used to control user permissions to access a network. MAC address authentication can be performed without client-side software. With this type of authentication employed, an ONU authenticates a user upon detecting the MAC address of the user for the first time. In the process of authentication, users don't need to input a username or password manually.

10.3.1 Port Configuration

Enable or disable the MAC authentication status on each port and the port status list is shown at the bottom.

Port	MAC Authentication Enable
LAN1	Enabled
Apply	

Port Status List

Port	MAC Authentication Enable	Port	MAC Authentication Enable
LAN1	Enabled	LAN2	Disabled
LAN3	Disabled	LAN4	Disabled
LAN5	Disabled	LAN6	Disabled
LAN7	Disabled	LAN8	Disabled
WAN	Disabled		

10.3.2 Misc Configuration

MAC authentication process is affected by the following timers:

Offline detect time To check whether the client is offline in this time interval. The device will immediately notify the RADIUS server to stop billing from the client when offline is detected. The value ranges from 1 to 65535, and the default value is 300 seconds.

Quiet Period To set the time interval the client must wait after a client authentication fails. During this time interval, the device does not perform the user authentication function. The value ranges from 1 to 3600, and the default value is 60 seconds.

Server Timeout To set the time interval the device waits for a response, when there is a connection request from the authentication server to the client. The value ranges from 1 to 65535, and the default value is 100 seconds.

MAC Authentication Misc Configuration	
Offline detect time (1-65535)	300 sec
Quiet Period (1-3600)	60 sec
Server Timeout (1-65535)	100 sec
Apply	

10.3.3 Authenticate Information

This page lists all the MAC authentication information including **VID**, **MAC Address**, **From Port**, and **Authenticate state**.

VID	MAC Address	From Port	Authenticate State
1	6c-f0-49-82-be-cf	LAN6	Quiet

10.4 Storm Control

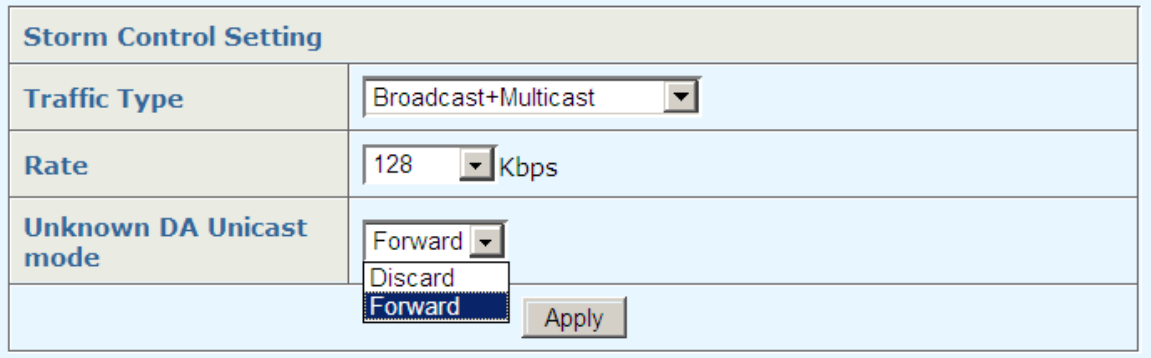
Traffic storm will be generated when there are multiple broadcast / multicast / DLF (Destination Lookup Failed) packets passing through a port, thus it will lead to traffic congestion. If the transmission rate of the three kind packets exceeds the set bandwidth, the packets will be automatically discarded to avoid network broadcast storm.

Traffic Type can be selected from:
None----means to disable storm control;
Broadcast;
Broadcast + Multicast;
Broadcast + Multicast + DLF.

Set thresholds for the specified Traffic Type.

To the Unknown DA Unicast mode, there are two ways to deal with: discard or forward.

This page sets thresholds of the specified **Traffic Type**.



11 Wireless

This function applies to the models with Wireless option.

Wireless Local Area Networks (WLAN) have become very popular because they are very easy to setup and use, and have low maintenance costs. Generally, one or more access points (APs) can cover a building or an area.

The WLAN solution allows you to provide the following wireless LAN services to your customers:

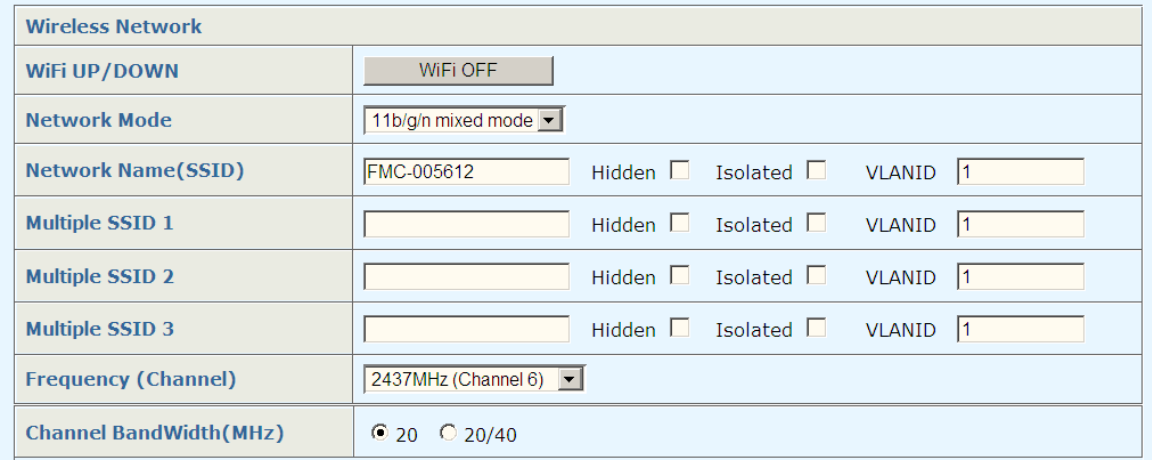
Connectivity to the Internet
WLAN client connectivity to conventional 802.3 LANs
Secured WLAN access with different authentication and encryption methods
Seamless roaming of WLAN clients in the mobility domain

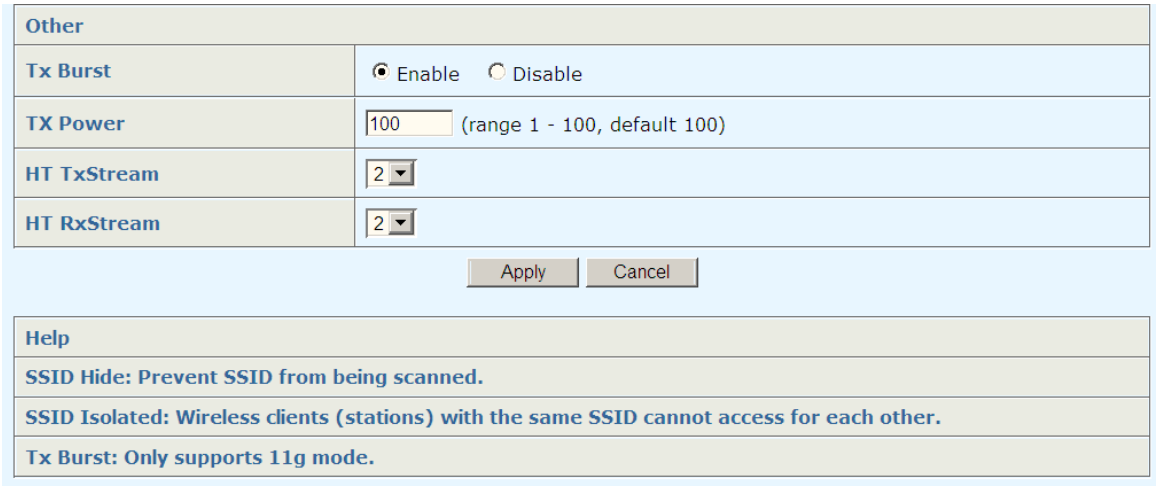
The **Wireless Settings** include the following items:

11.1 Basic Configuration

11.1.1 Basic

This page is used to configure basic wireless parameters like Network Mode, SSID, channel Number and so on.





WiFi UP/DOWN If set to "OFF", the WiFi is powered off. If set to "ON", the WiFi is powered on.

Network Mode AE208 Gateway can connect to 11b/g mixed mode，11b only, 11g only, 11b/g/n mixed mode, and 11n only (2.4G) modes. By default, it is in 11b/g/n mixed mode.

Network Name (SSID) Set a name for AE208 Gateway to be identified.

SSID The service set identifier. A client scans all networks at first, and then selects a specific SSID to connect to a specific wireless network.

Hidden Check it to prevent from wireless sniffing and make it harder for unauthorized clients or stations to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see anything about AE208 Gateway while site surveying. The system allows you to set three sets of SSID for different usage.

Isolated Check this box to make the wireless clients (stations) with the same SSID not have an access to each other.

VLAN ID Add the SSID to the corresponding VLAN. If the VLAN exists, it is added to the VLAN directly, if the VLAN doesn't exist, first create the VLAN and then add the SSID to it. By default the SSID is in VLAN 1.

Frequency（channel） This is the channel frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference.

Channel BandWidth(MHz) Bandwidth is the difference between the upper and lower frequencies in a continuous set of frequencies. It is typically measured in hertz. 802.11n can bond two adjacent 20-MHz channels together to form a 40-MHz channel. During data forwarding, the two 20-MHz channels can work separately with one acting as the primary channel and the other acting as the secondary channel or work together as a 40-MHz channel. This provides a simple way of doubling the data rate. By default, the channel bandwidth of the 802.11n radio (2.4GHz) is 20 MHz.

Tx Burst Frame burst allows a client to burst many frames in a short amount of time to increase overall network speed. Though this is not recommended, it is still useful when large data is being transmitted, but the benefits are not as big as most people hope.

Tx Power This setting will determine the number of milliwatts used to power the radio signal output from the AE208 Gateway.

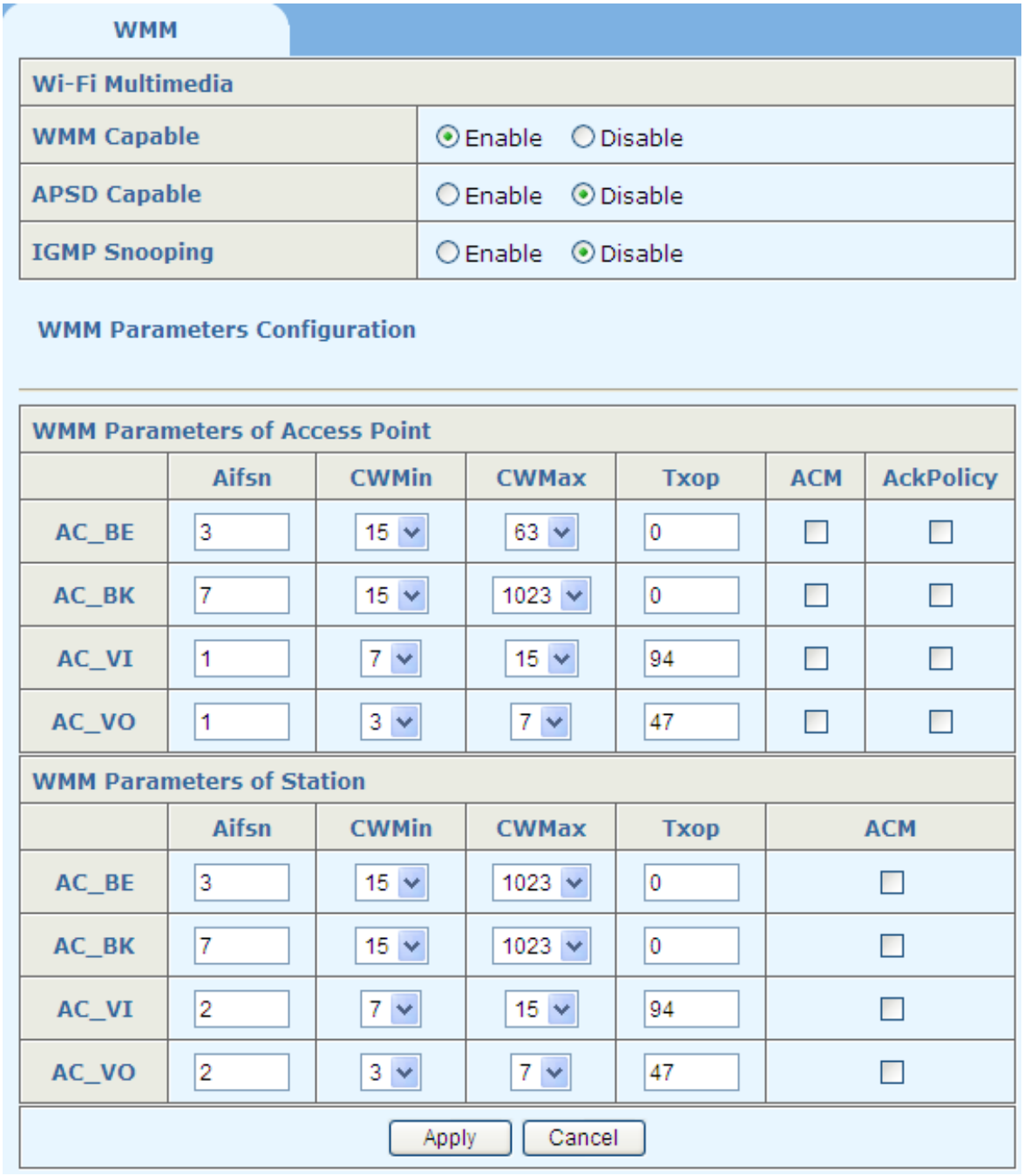
HT TxStream & HT RxStream This is used in conjunction with external antennas to give optimum performance.

After all settings are completed, click <Apply> to activate them.

11.1.2 WMM

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE, AC_BK, AC_VI and AC_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. Such function is designed for mobile and cordless phones that support VoIP mostly.



WMM Capable To apply WMM parameters for wireless data transmission, please click the <Enable> radio button.

APSD Capable The default setting is **Disable**. Click **Enable** to enable the function of automatic power-save delivery (APSD).

IGMP Snooping The default setting is **Disable**. Click **Enable** to enable the function of IGMP Snooping.

Access point (AP) An AP bridges frames between wireless and wired networks.

Aifsn It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing

categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories. As to the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.

CWMin/CWMax CWMin means contention Window-Min and CWMax means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than that of CWMin or equals to it. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.

Txop It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater values for them to get the highest transmission opportunity. Specify the value ranging from 0 to 65535.

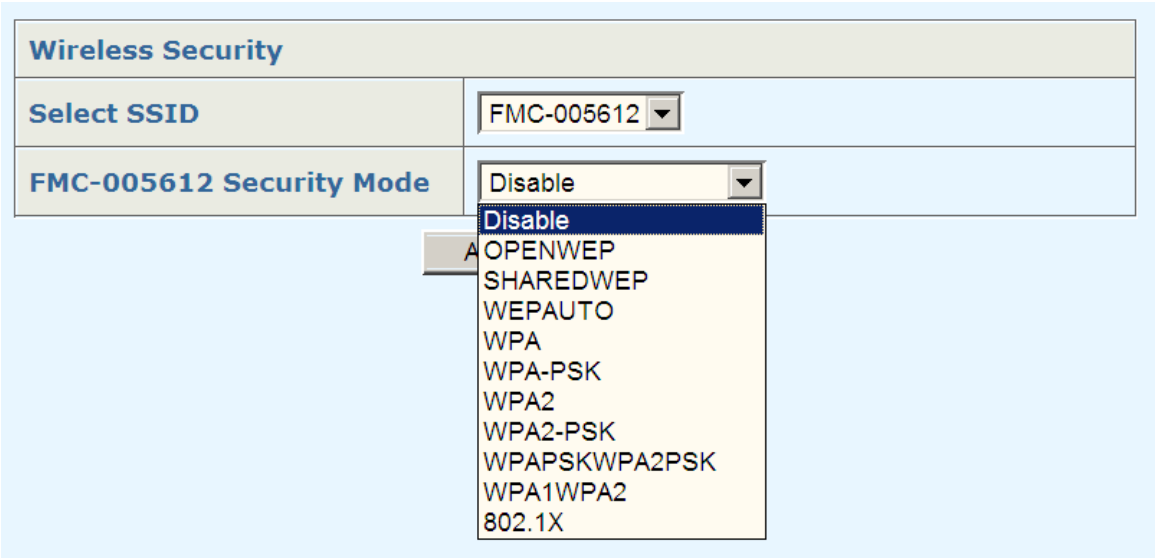
ACM It is an abbreviation of Admission Control Mandatory. It can restrict stations from using specific category class if it is checked.

AckPolicy "Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.

11.2 Security Configuration

11.2.1 Security

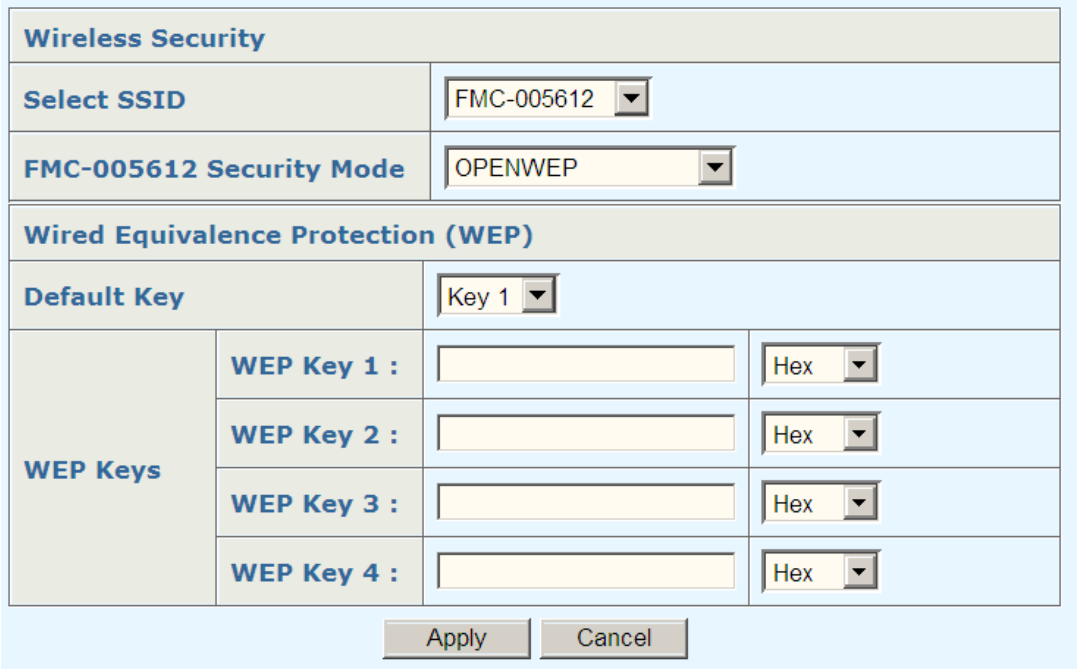
This page allows you to set different security modes for different SSID. Select the SSID in the drop-down menu first, and then select the **Security Mode** in the drop-down menu. The **Security Modes** includes: Disabled, OPENWEP, SHARPWEP, WEPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPAPSK/WPA2PSK, WPA1/WPA2 and 802.1 X.



Security Mode

1) **Disable**: The encryption mechanism is turned off.

2) **OPENWEP**: Accepts only WEP clients. The encryption key should be entered in the **WEP Key** fields. Any client is allowed to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption.

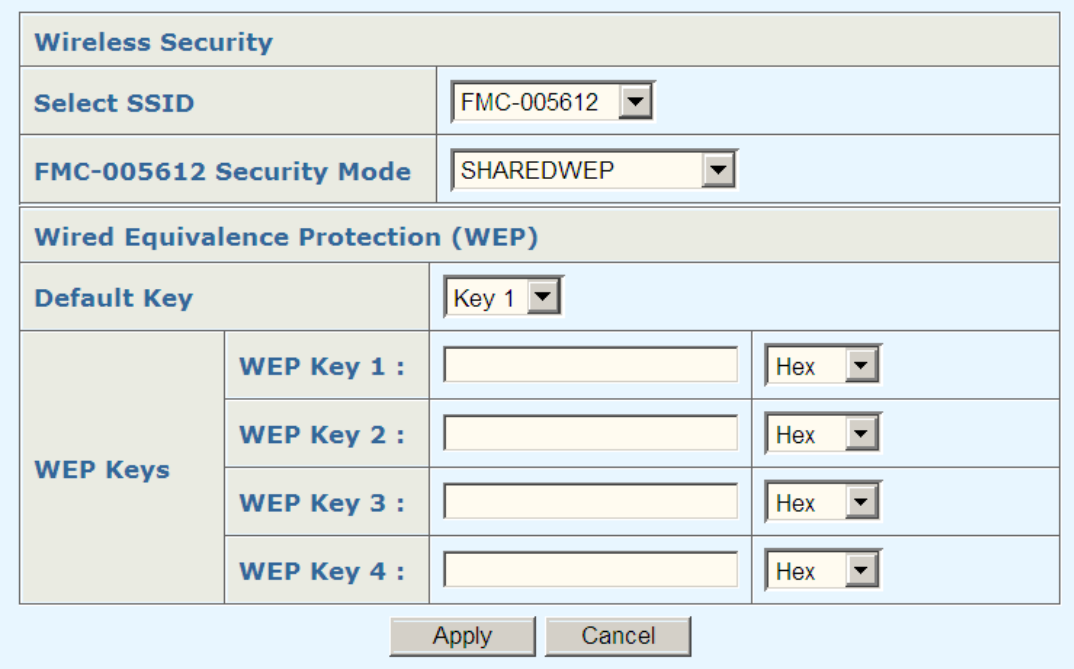


Default WEP Key You may use up to four different keys for four different networks. Select the current key that will be used.

WEP Key1-Key4: Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 10 or 26 Hex characters except '#' and ','.

After all settings are completed, click <Apply> to activate them.

3) **SHARPEDWEP**: Accepts only WEP clients and the encryption key should be entered in the **WEP Key** fields. The AP sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate.

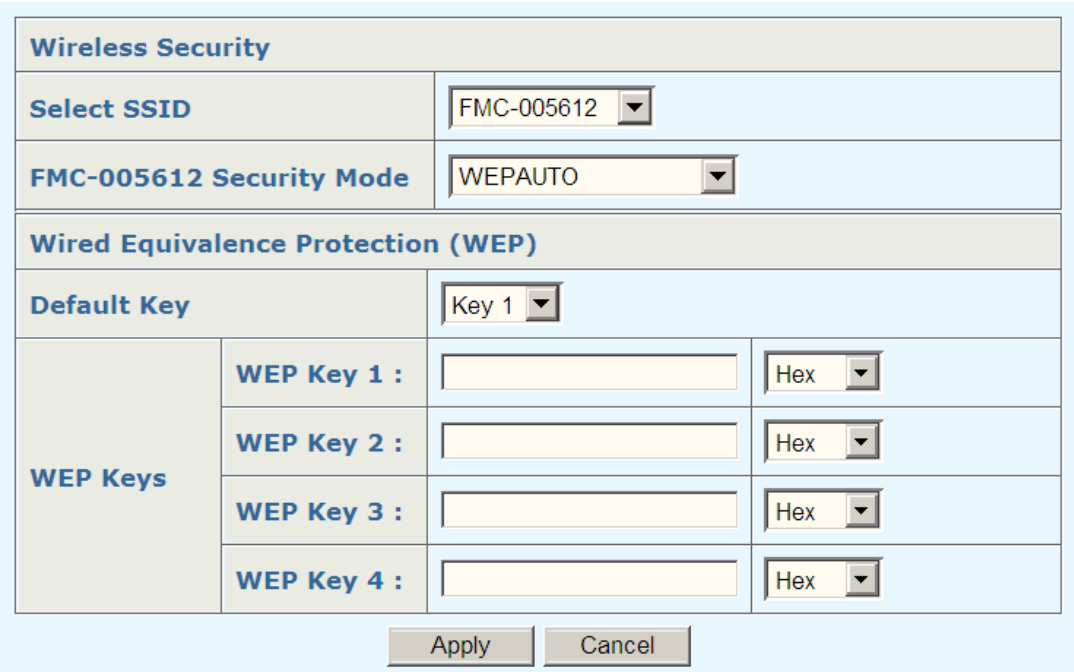


Default WEP Key You may use up to four different keys for four different networks. Select the current key that will be used.

WEP Key1-Key4 Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 10 or 26 Hex characters except '#' and ','.

After all settings are completed, click <Apply> to activate them.

4) **WEPAUTO**: Of OPENWEP and SHAREDWEP, if you are not sure which one to use, choose **WEPAUTO**.

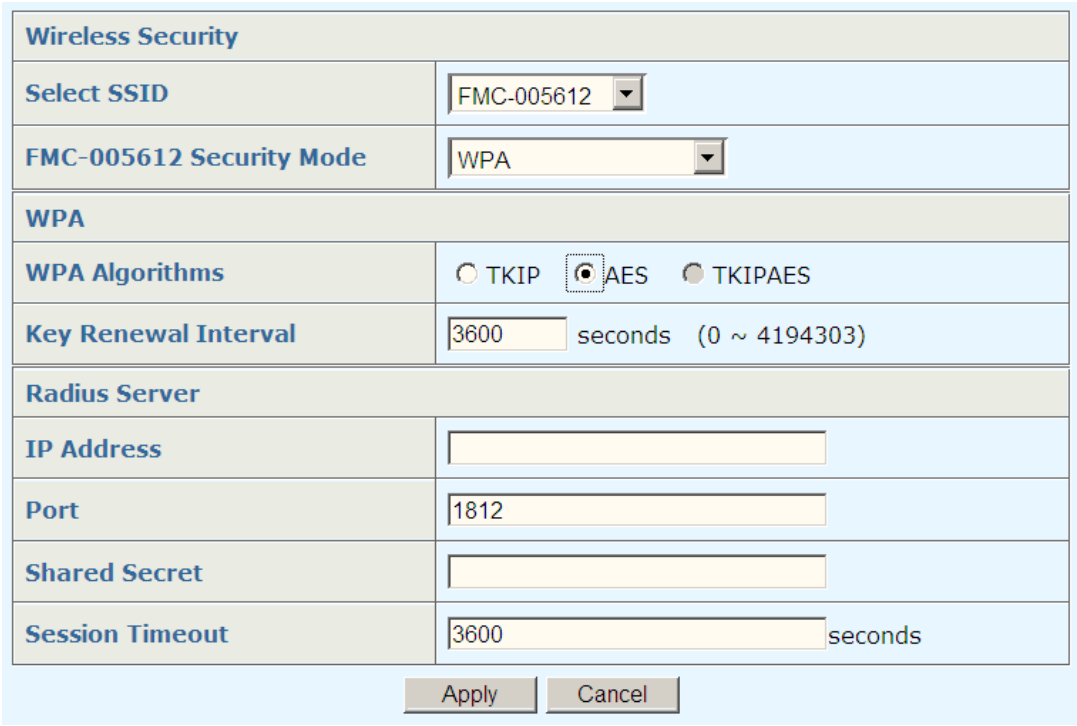


Default WEP Key You may use up to four different keys for four different networks. Select the current key that will be used.

WEP Key1-Key4 Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 10 or 26 Hex characters except '#' and ','.

After all settings are completed, click <Apply> to activate them.

5) **WPA**: The WPA encrypts each frame transmitted from the radio using the key; you can either enter PSK (Pre-Shared Key) manually in the following page or make it automatically negotiate via 802.1x authentication.



WPA Algorithms Select TKIP, AES or TKIP/AES as the algorithm for WPA.

Key Renewal Interval WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

IP Address Enter the IP address of RADIUS Server.

Port The UDP port number that the Radius Server is using. The default value is 1812, based on RFC 2138.

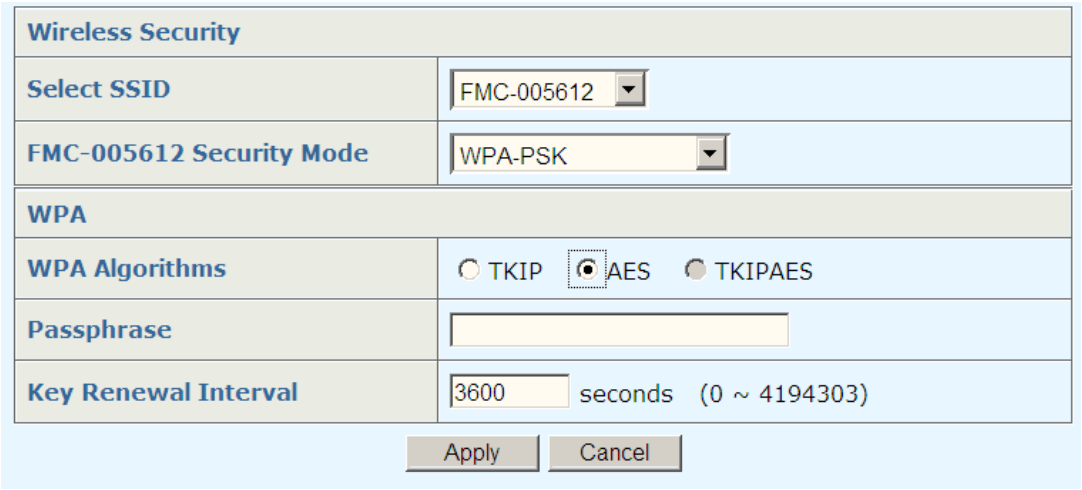
Shared Secret The Radius Server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret

Session Timeout Set the maximum time of service provided before Re-authentication. Set to zero to perform another authentication immediately after the first authentication has

successfully completed. (The unit is second.)

After all settings are completed, click <Apply> to activate them.

6) **WPA-PSK**: One variation of WPA is called WPA Pre Shared Key or WPA-PSK for short. WPA-PSK is a simplified but still powerful form of WPA most suitable for home Wi-Fi networking. To use WPA-PSK, a person sets a static key or "passphrase" as with WEP. But, using TKIP, WPA-PSK automatically changes the keys at a preset time interval, making it much more difficult for hackers to find and exploit them.



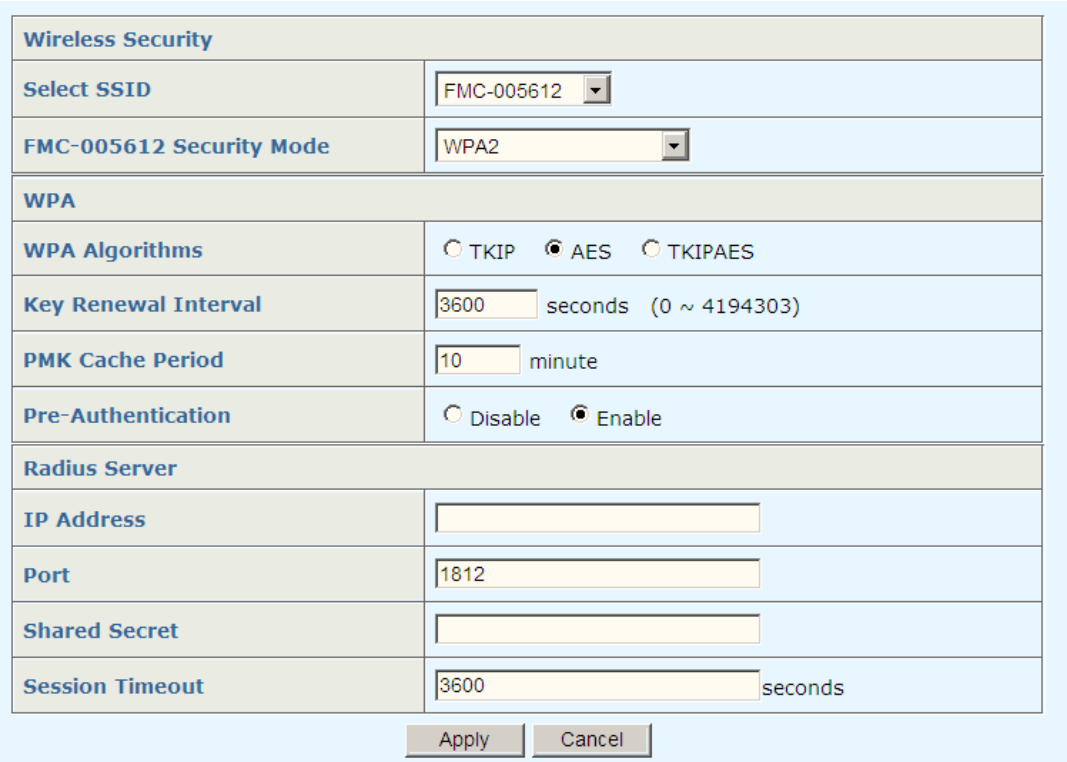
WPA Algorithms Select TKIP, AES or TKIP/AES as the algorithm for WPA.

Pass Phrase If WEP or AES is selected, input 8~64 characters as encrypt key.

Key Renewal Interval WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

After all settings are completed, click <Apply> to activate them.

7) **WPA2**: Just as WPA has replaced WEP, WPA2 has replaced WPA as the most secure protocol at present. WPA2 implements the latest security standards, including "government-grade" data encryption.



WPA Algorithms Select TKIP, AES or TKIP/AES as the algorithm for WPA.

Key Renewal Interval WPA uses shared key for authentication to the network. However, normal network operation uses a different encryption key that is randomly generated. This randomly generated key is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

PMK Cache Period Type PMK cache period.

Pre-Authentication Enable/disable this function.

IP Address Enter the IP address of RADIUS Server.

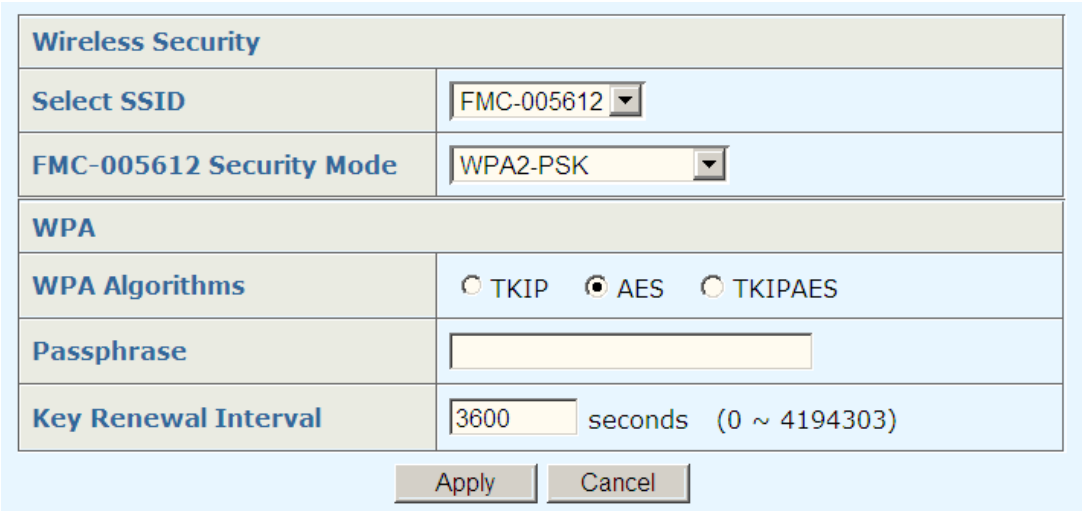
Port The UDP port number that the Radius Server is using. The default value is 1812, based on RFC 2138.

Shared Secret The Radius Server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret

Session Timeout Set the maximum time of service provided before Re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

After all settings completed, click <Apply> to activate them.

8) **WPA2-PSK**: It is a method of securing your network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users without an enterprise authentication server.



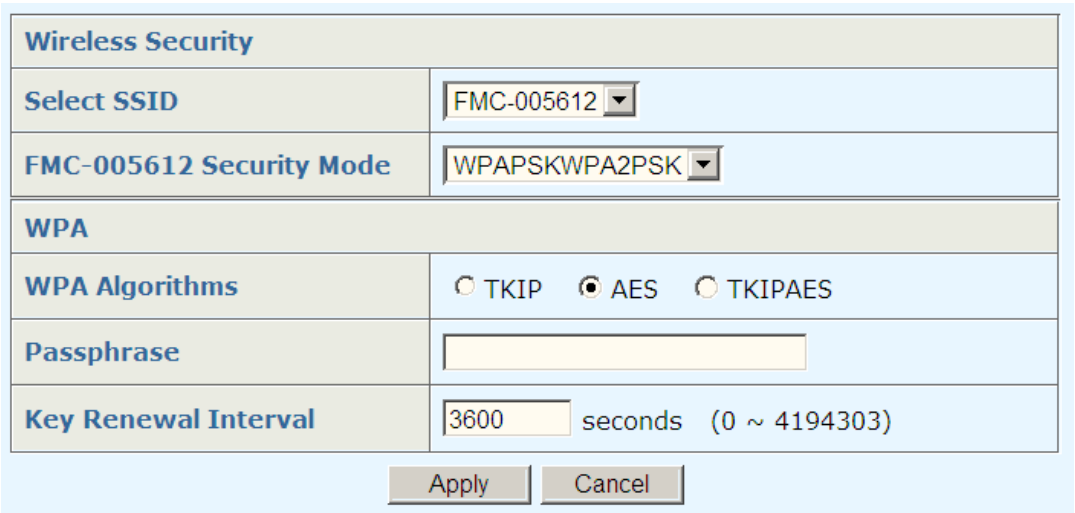
WPA Algorithms Select TKIP, AES or TKIP/AES as the algorithm for WPA.

Pass Phrase Either 8-63 ASCII characters，such as 012345678…(or 64 Hexadecimal digits led by 0x,such as "0x32152fabde…").

Key Renewal Interval WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key ~~that~~ is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

After all settings are completed, click <Apply> to activate them.

9) WPA-PSK/WPA2-PSK: This is a mixed mode, the most secure encryption mode at present.



WPA Algorithms Select TKIP, AES or TKIP/AES as the algorithm for WPA.

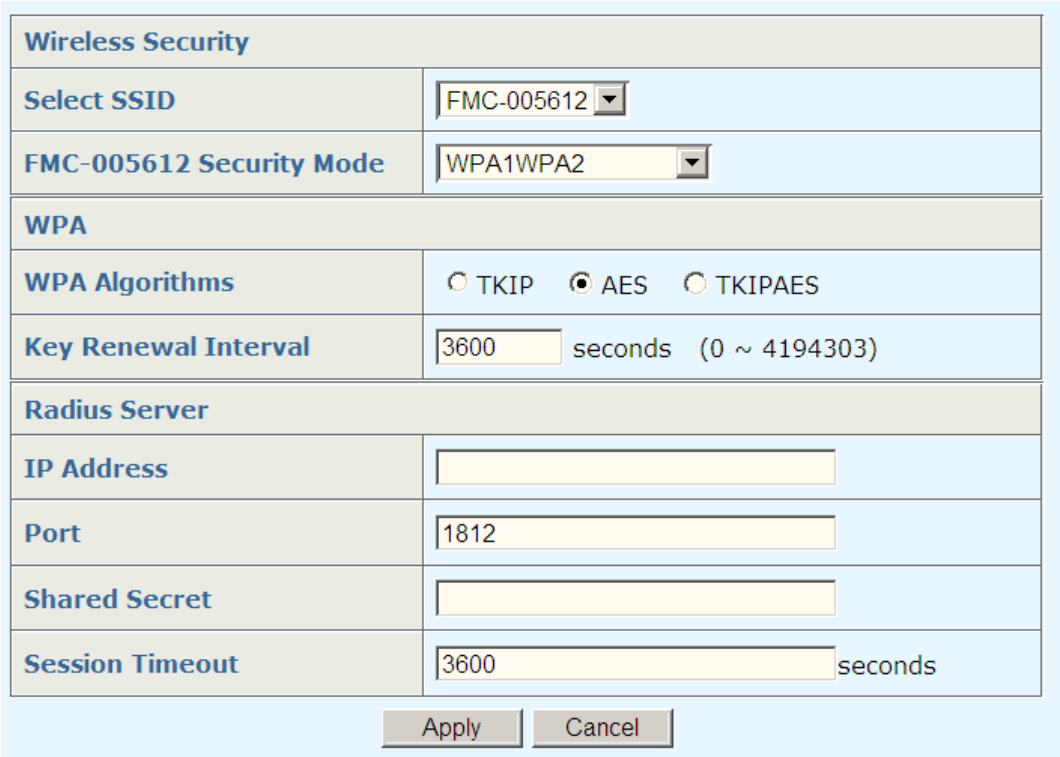
Pass Phrase Either 8-63 ASCII characters，such as 012345678…(or 64 Hexadecimal digits led by 0x,such as "0x32152fabde…").

Key Renewal Interval WPA uses shared key for authentication to the network. However, normal

network operations use a different encryption key that is randomly generated. This randomly generated key ~~that~~ is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

After all settings are completed, click <Apply> to activate them.

10) WPA1/WPA2: Incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.



WPA Algorithms Select TKIP, AES or TKIP/AES as the algorithm for WPA.

Key Renewal Interval WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

IP Address Enter the IP address of RADIUS Server.

Port The UDP port number that the Radius Server is using. The default value is 1812, based on RFC 2138.

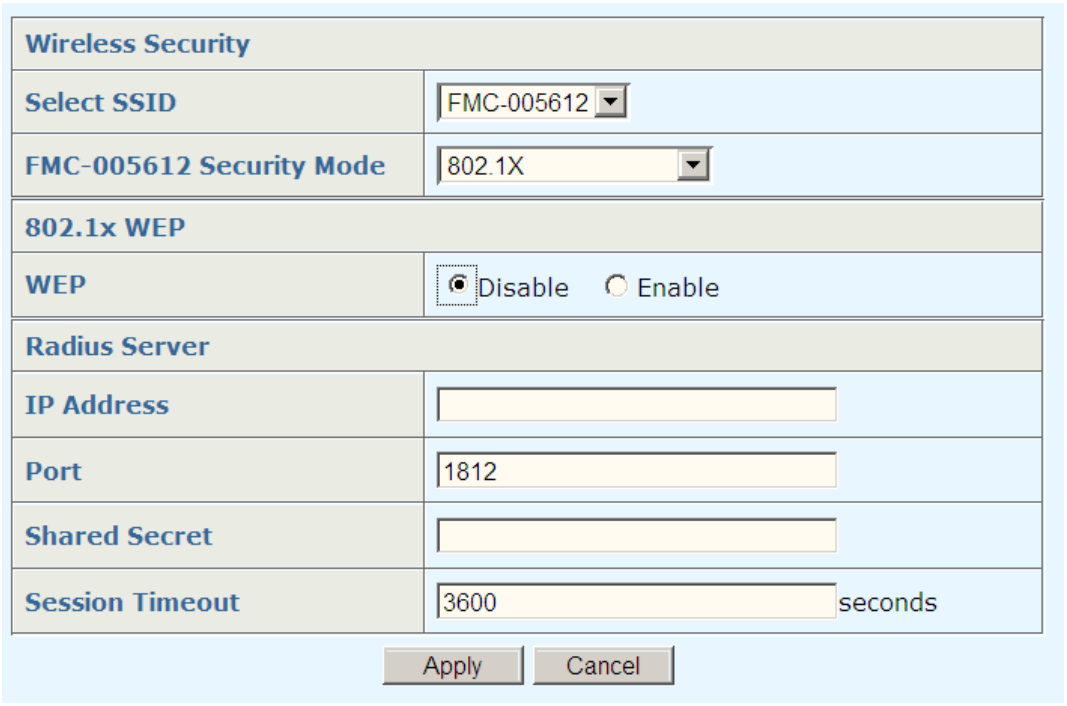
Shared Secret The Radius Server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

Session Timeout Set the maximum time of service provided before Re-authentication. Set to zero to perform another authentication immediately after the first authentication has been

successfully completed. (The unit is second.)

After all settings are completed, click <Apply> to activate them.

11) **802.1X**: 802.1X is an IEEE standard for authenticated network access to wired Ethernet networks and wireless 802.11 networks. IEEE 802.1X enhances security and deployment by providing support for centralized user identification, authentication, dynamic key management and accounting.



802.1x WEP Enable or disable the WEP Encryption. If the WEP encryption is disabled, data sent to the AP will not be encrypted.

IP Address Enter the IP address of RADIUS Server.

Port The UDP port number that the Radius Server is using. The default value is 1812, based on RFC 2138.

Shared Secret The Radius Server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret

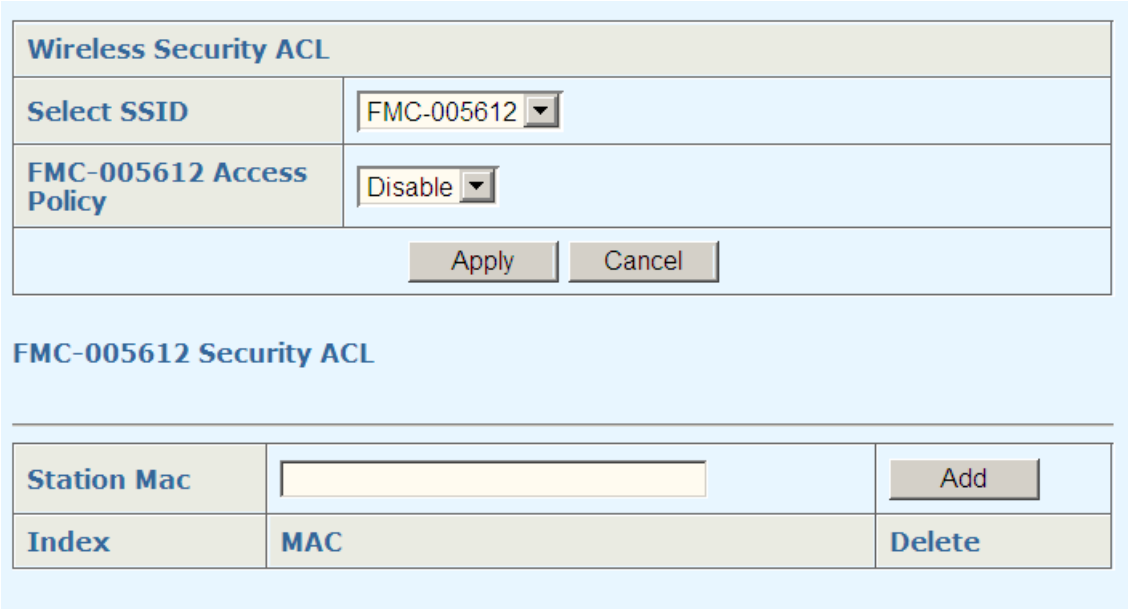
Session Timeout Set the maximum time of service provided before Re-authentication. Set to zero to perform another authentication immediately after the first authentication has been successfully completed. (The unit is second.)

After all settings are completed, click <Apply> to activate them.

11.2.2 ACL

On this page, you can configure wireless security ACL. First select an SSID, and decide to enable or disable FMC-005612 Access Policy, if you enable it, you have to further decide allow it or

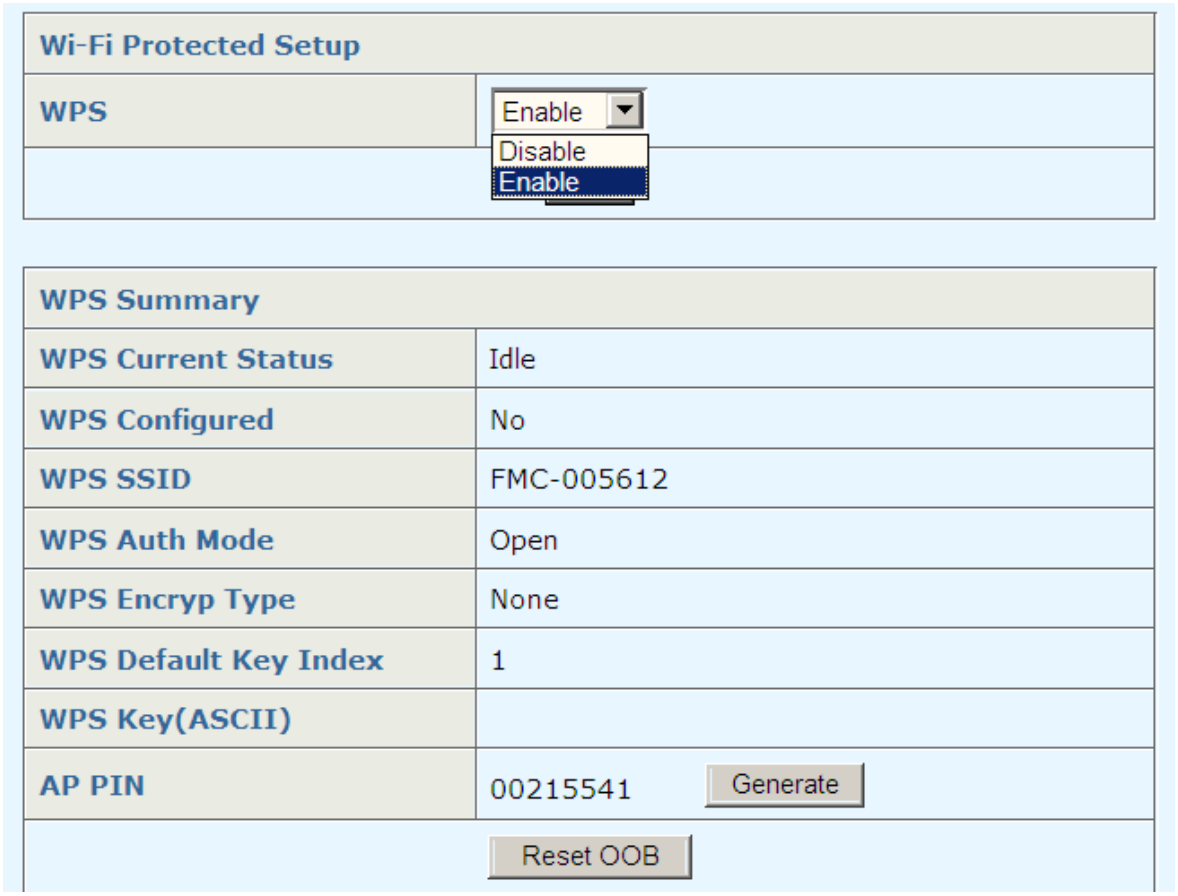
reject it. And you can add the wireless station MAC. On the lower part of the interface, you can see the list, the entries can be deleted.

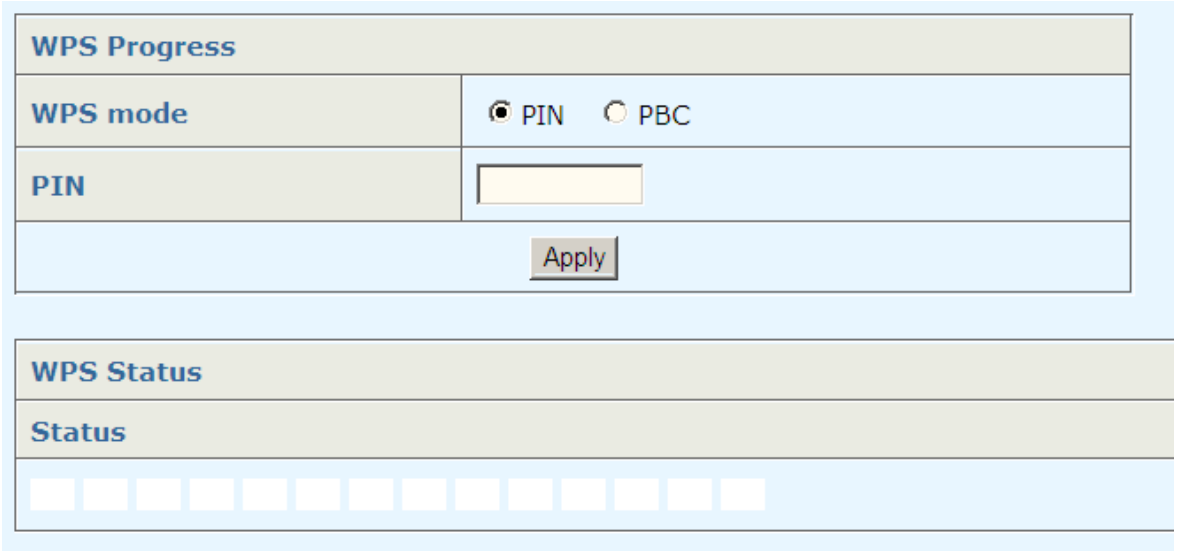


11.2.3 WPS

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point with the encryption of WPA and WPA2.

It is the simplest way to build connection between wireless network clients and AE208 Gateway. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. The user only needs to press a button on wireless client, and WPS will connect for client and AE208 automatically.





WPS Enable/disable WPS setting.

WPS Current Status Display related system information for WPS. If the wireless security (encryption) function of the AE208 Gateway is properly configured, you can see 'Configured' message here.

WPS Configured "No" will be displayed when AE208 Gateway is not connected with any STA by WPS at present, while "Yes" will be displayed while AE208 Gateway is connected with STA by WPS.

WPS SSID Display current selected SSID.

WPS Auth Mode Display current authentication mode. Only WPA2/PSK and WPA/PSK support WPS.

WPS Encrypt Type Display encryption mode (None, WEP, TKIP, AES, etc.) of AE208 Gateway.

WPS Default Key Index The default key index that WPS uses.

WPS Key(ASCII) Display WPS Key by ASCII code.

AP PIN The number displayed here is used for remote client entering the registrar's PIN code in remote station to make a network connection. Clicking <Generate> can generate different AP PIN.

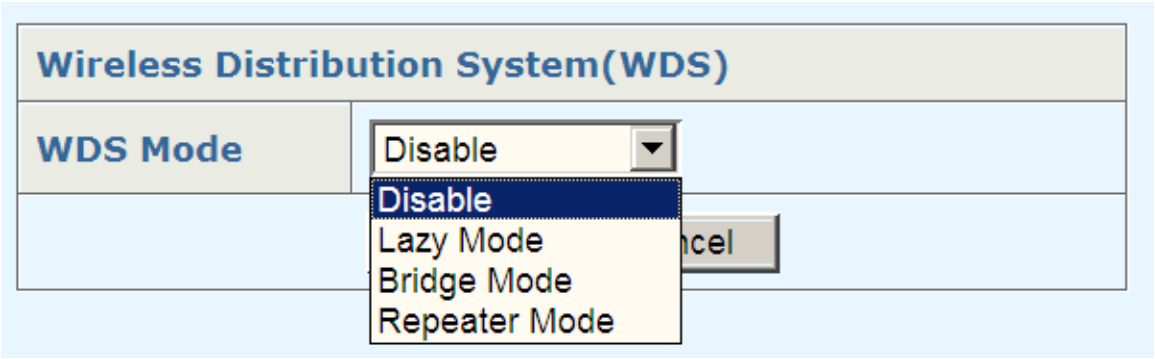
PBC Click **Start PBC** to invoke Push-Button style WPS setup procedure. The AE208 Gateway will wait for WPS requests from wireless clients.

PIN Type the PIN code specified in wireless client you wish to connect, and click <Start PIN>. It will return to normal condition after two minutes. (You need to set up WPS within two minutes.)

11.3 WDS

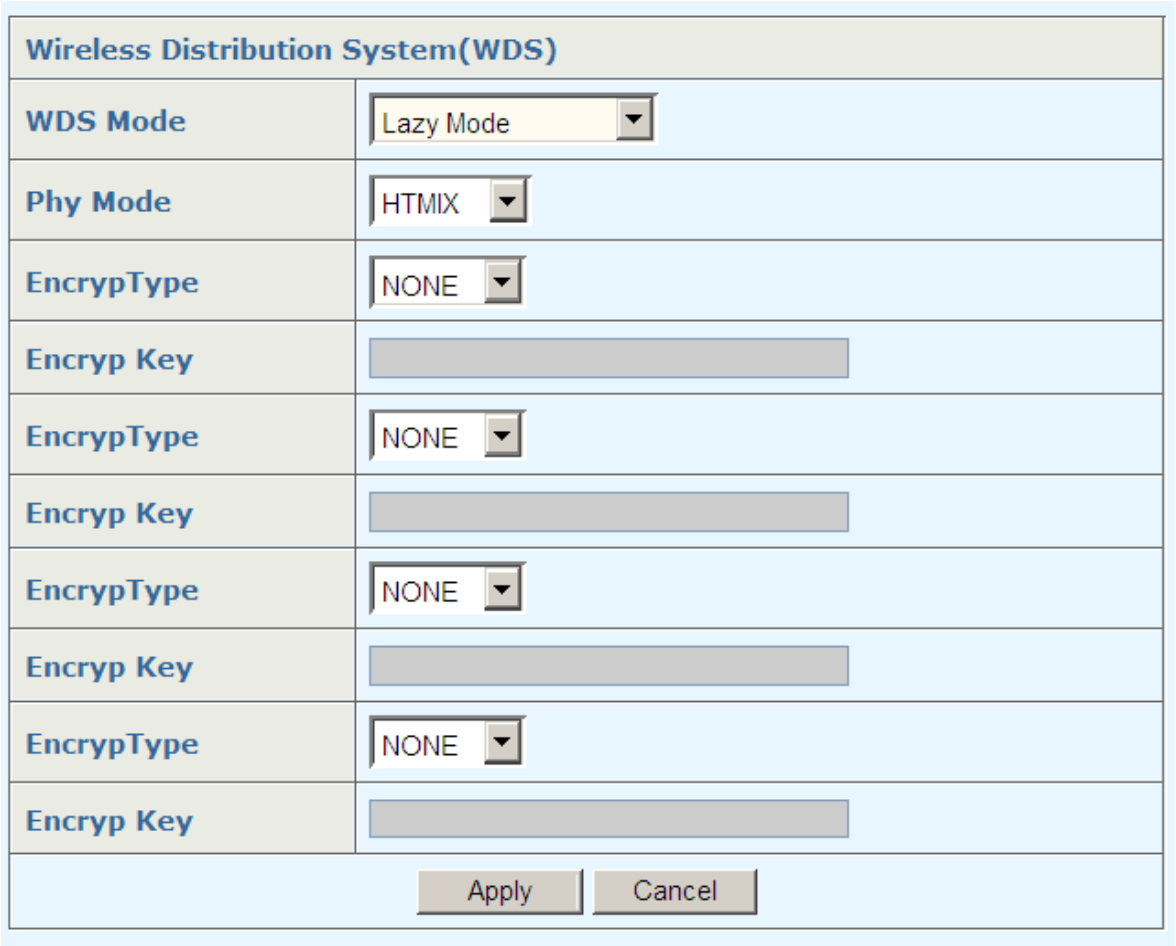
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.



WDS Mode: Select the mode for WDS setting. The **Disable** mode will not invoke any WDS setting.

1) Lazy Mode

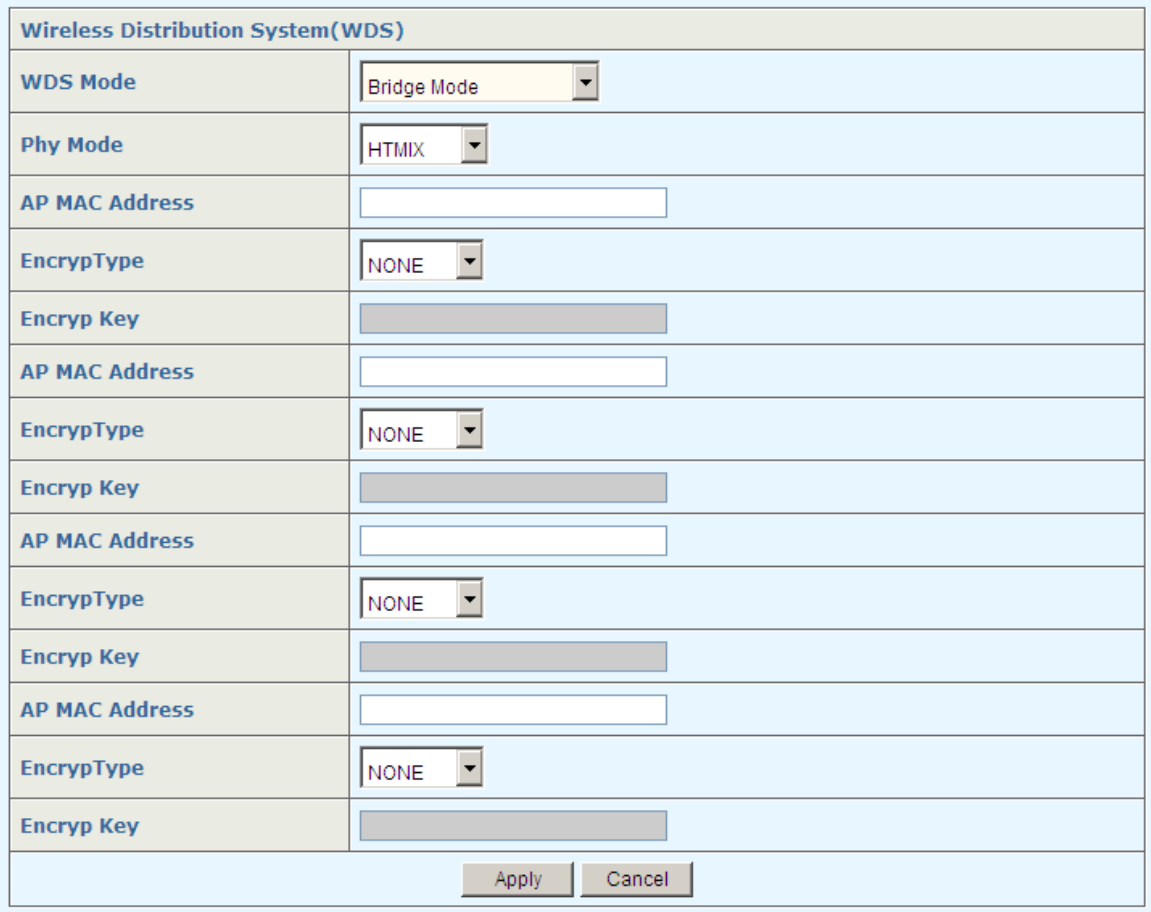


Phy Mode There are three types of transmission rates developed by different techniques for Phy Mode. Data will be transmitted via communication channel.

Encryp Type There are four types for security, Disabled, WEP, TKIP and Key or Peer Mac Address field valid or not. Choose one of the types for the router. Please disable the unused link to get better performance.

Encryp Key If WEP is selected, input 10/26 hexdecimal or 5/13 ascii as encrypt key; If WEP or AES is selected, input 8~64 characters as encrypt key.

2) Bridge Mode



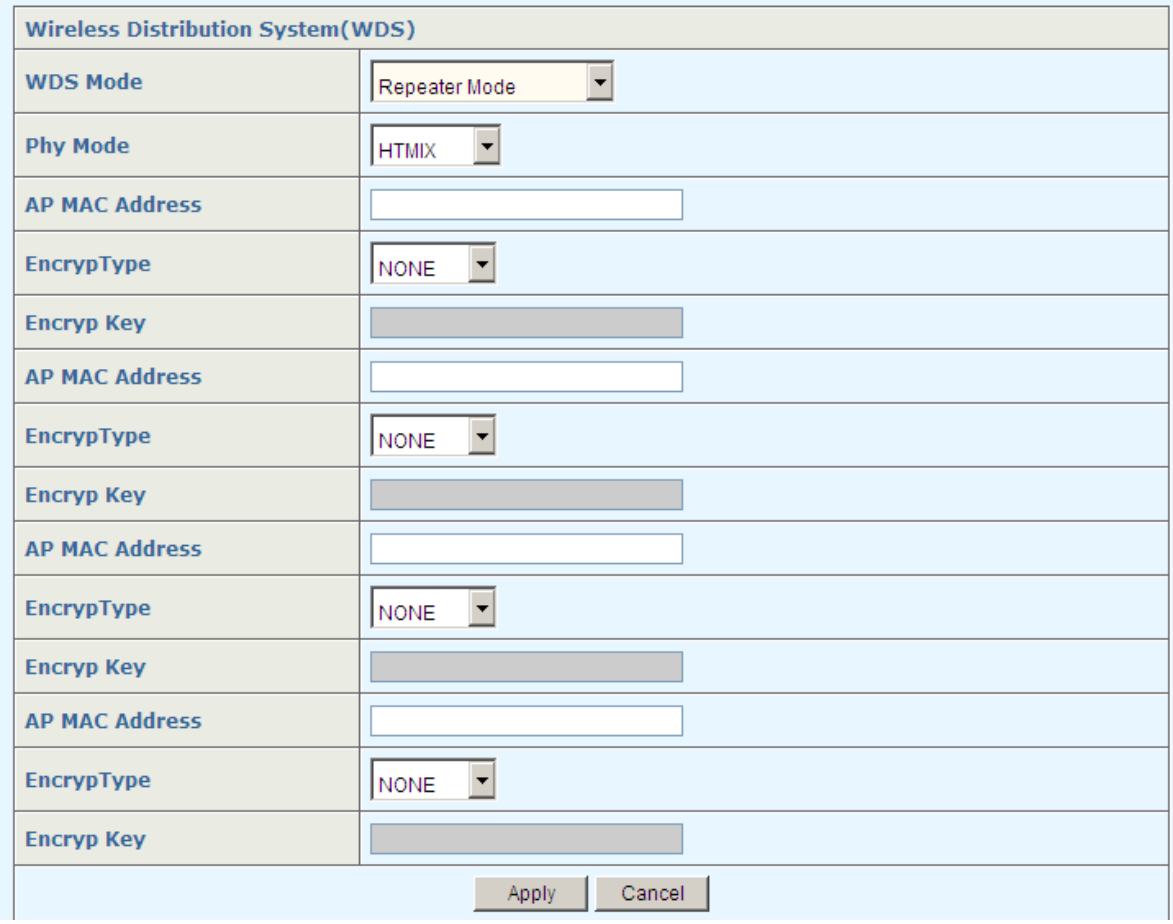
Phy Mode There are three types of transmission rates developed by different techniques for Phy Mode. Data will be transmitted via communication channel.

Encryp Type There are four types for security, Disabled, WEP, TKIP and Key or Peer Mac Address field valid or not. Choose one of the types for the router. Please disable the unused link to get better performance.

Encryp Key If WEP is selected, input 10/26 hexdecimal or 5/13 ascii as encrypt key; If WEP or AES is selected, input 8~64 characters as encrypt key.

AP MAC Address Four AP MAC Addresses are allowed to be entered on this page at one time.

3) Repeater Mode



Phy Mode There are three types of transmission rates developed by different techniques for Phy Mode. Data will be transmitted via communication channel.

Encryp Type There are four types for security, Disabled, WEP, TKIP and Key or Peer Mac Address field valid or not. Choose one of the types for the router. Please disable the unused link to get better performance.

Encryp Key If WEP is selected, input 10/26 hexdecimal or 5/13 ascii as encrypt key; If WEP or AES is selected, input 8~64 characters as encrypt key.

AP MAC Address Four AP MAC Addresses are allowed to be entered on this page at one time.

11.4 APSCAN

11.4.1 AP Scan

AE208 Gateway can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Note that during the scanning process (about 5 seconds); no client is allowed to connect to AE208 Gateway.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found.

	SSID	BSSID	RSSI	Channel	Encryption	Authentication
☐	Mario	68:7f:74:bb:78:49	44	1	AES	WPA2/PSK
☐	airNET-free	00:02:6f:bc:e9:9d	20	1	NONE	OPEN
☐	Abloomy_Listong_VAP5100	00:0e:cb:00:01:49	50	1	NONE	OPEN
☐	Tenda_For_InBi	c8:3a:35:3c:ca:d0	60	1	AES	WPA2/PSK
☐	10.1.1.2-101	00:1e:6e:00:83:88	100	6	AES	WPA2/PSK
☐	TESTESTEST	00:1e:6e:00:94:4c	81	6	TKIP/AES	Mixed (WPA+WPA2)/PSK
☐	FMC-005614	00:1e:6e:00:56:18	100	6	NONE	OPEN
☐	10.1.1.2-301	00:1e:6e:00:83:8a	100	6	AES	WPA2/PSK

Rescan

Add selected BSSID to WDS | ◉ Bridge ○ Repeater Add

SSID Display the SSID of the AP scanned by this router.

BSSID Display the MAC address of the AP scanned by this router.

RSSI Display the signal strength. RSSI is the abbreviation of Receive Signal Strength Indication.

Channel Display the wireless channel used for the AP that is scanned by this router.

Encryption Display the encryption mode for the scanned AP.

Authentication Display the authentication type that the scanned AP applied.

ReScan It is used to discover all the connected AP again.

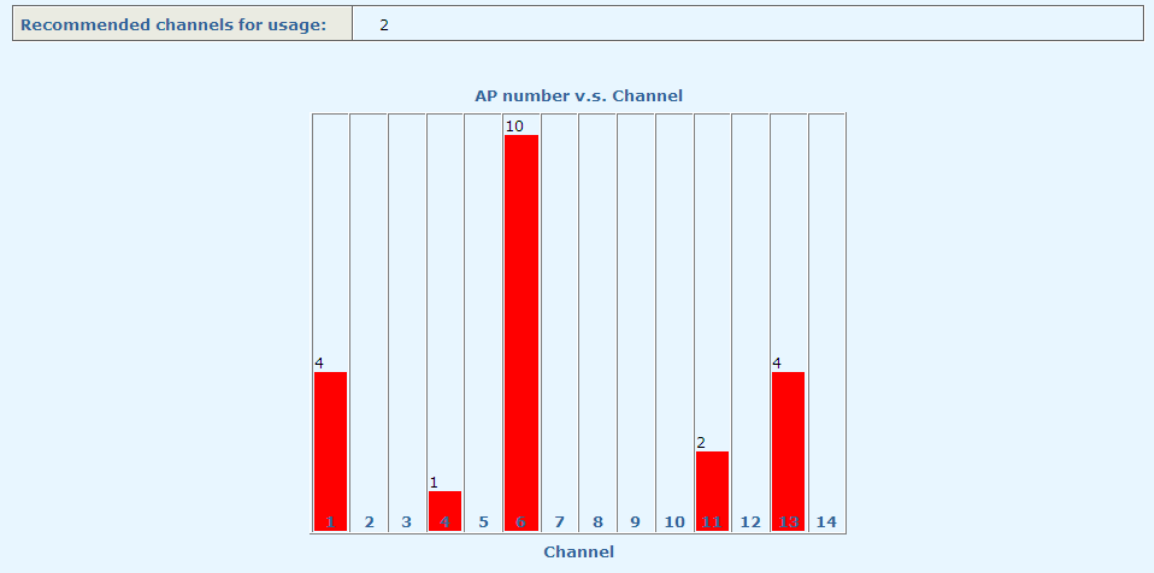
Add selected BSSID to WDS Select the SSID of the Access Point that AE208 Gateway wants to connect to.

Bridge/Repeater AE208 Gateway will connect to the SSID selected as Bridge mode or Repeater mode.

After choosing “Add selected BSSID to WDS” in Bridge or Repeater mode, and then click <Add>, it will turn to WDS page.

11.4.2 AP Channel

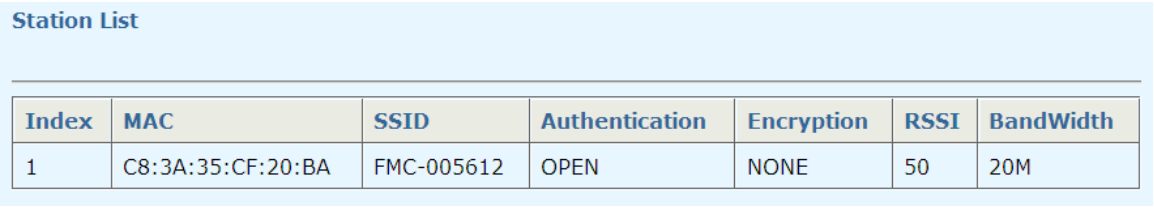
This page is used to display AP number in a different channel.



11.5 Information

11.5.1 Station List

This page is used to display the knowledge of connecting wireless clients along with its status code. The list shows the station information.



Index	MAC	SSID	Authentication	Encryption	RSSI	BandWidth
1	C8:3A:35:CF:20:BA	FMC-005612	OPEN	NONE	50	20M

Index Index number.

MAC Address Display the MAC Address for the connecting client.

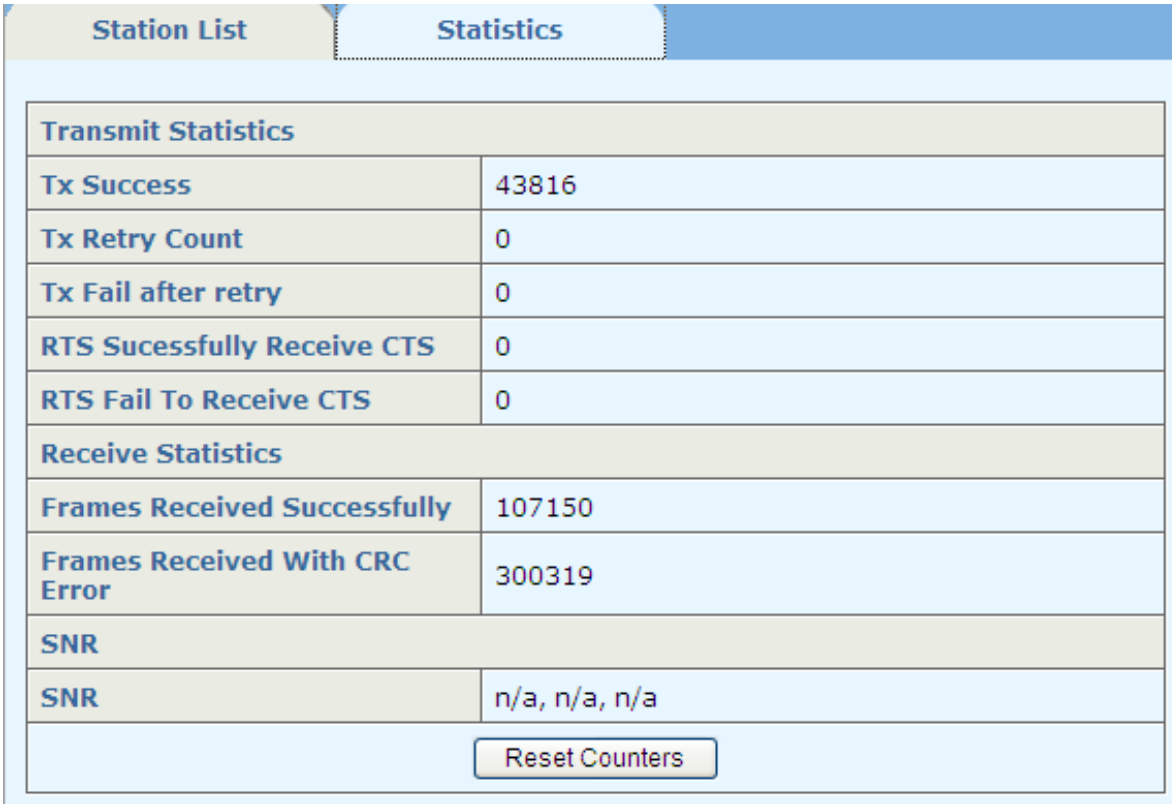
SSID Display the SSID that the wireless client connects to.

Authentication Display the authentication that the wireless client uses for connection with the AP.

Encryption Display the encryption mode used by the wireless client.

11.5.2 Statistics

This page displays all the wireless statistic information of AE208 Gateway.

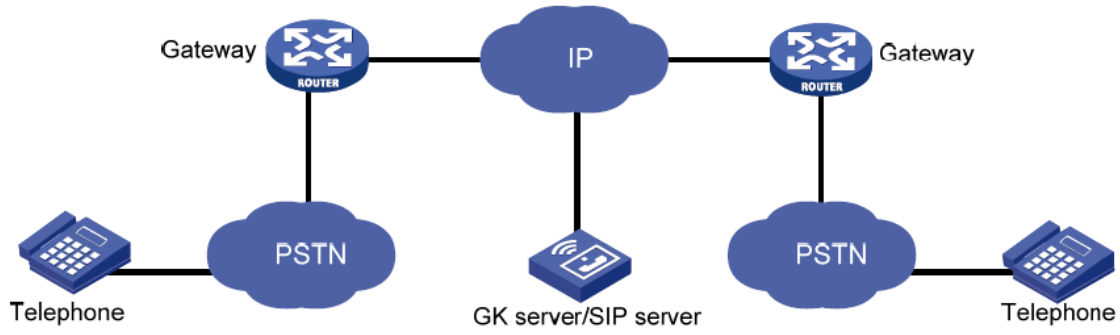


12 VoIP

Voice over IP (VoIP) enables IP networks to provide voice services such as plain old telephone service (POTS). In VoIP, the voice gateway encapsulates voice signals packets to transmit. IP telephony is a typical VoIP application.

Currently, interworking between PSTN and IP is implemented via VoIP gateways. The PC-to-telephone, telephone-to-PC, and telephone-to-telephone technologies are mature and the call quality has been improved greatly. Therefore, VoIP can completely meet the commercial requirements.

For POTS, all functions from the call originator to the call receiver are implemented by the public switched telephone network (PSTN).



In the above figure of VoIP system, the VoIP gateway provides interfaces for communication between the IP network and PSTN/integrated services digital network (ISDN). Users connect to the originating VoIP gateway through PSTN. The originating VoIP gateway converts analog signals into digital signals and compresses them into voice packets that can be transmitted over the IP network. The IP network transmits the voice packets to the terminating VoIP gateway, which converts the voice packets back to recognizable analog signals and transmits them to the receiver. This is a complete telephone-to-telephone communication process. In practice, a gatekeeper (GK) server or SIP server may be applied in the VoIP system to implement the functions such as routing and access control.

The following describes a basic VoIP call flow:

1. A user picks up a telephone and the modular voice card detects the user's off-hook action in real time.
2. The modular voice card transmits the off-hook signal to the VoIP signal processing module on the VoIP gateway.
3. The VoIP signal processing module generates dial tones.
4. The user hears dial tones played by the session application and begins dialing before the dial tone timer expires.
5. The session application collects the digits dialed by the user.

6. The session application compares the collected digits with the match template while collecting digits.

7. After finding a match template for the called number, the originating VoIP gateway maps the number to the terminating VoIP gateway.

8. The originating VoIP gateway initiates a VoIP call to the terminating VoIP gateway over the IP network and establishes a logical channel for the call to send and receive voice data.

9. The terminating VoIP gateway receives the call from the IP network and seeks the destination telephone according to the match template. If the call is to be processed by a private branch exchange (PBX), the terminating VoIP gateway passes the call via PSTN signaling to the PBX for processing until the destination telephone is connected. When the calling party or the called party hangs up, the conversation ends.

12.1 Phone Settings

There are three tab pages in Phone Settings, including *Port Settings*, *Dial Plan Settings* and *Port Function Setting*.

12.1.1 FXS Port Settings

A foreign exchange station (FXS) interface uses a standard RJ-11 connector and a telephone cable to directly connect with an ordinary telephone or a fax machine. An FXS interface accomplishes signaling exchange based on the level changes on the Tip/Ring line and provides ring, voltage, and dial tone.

You can configure the Flash Time, FXS Impedance and Jitter Buffer on this page.

Max Flash Time A PSTN called party can press the flash hook to switch to another incoming call. This setting specifies the maximum time the flash hook is pressed before the call is switched.

Min Flash Time This setting specifies the minimum time the flash hook is pressed before the call is switched.

FXS Port Set the FXS port impedance to meet the requirement of different country

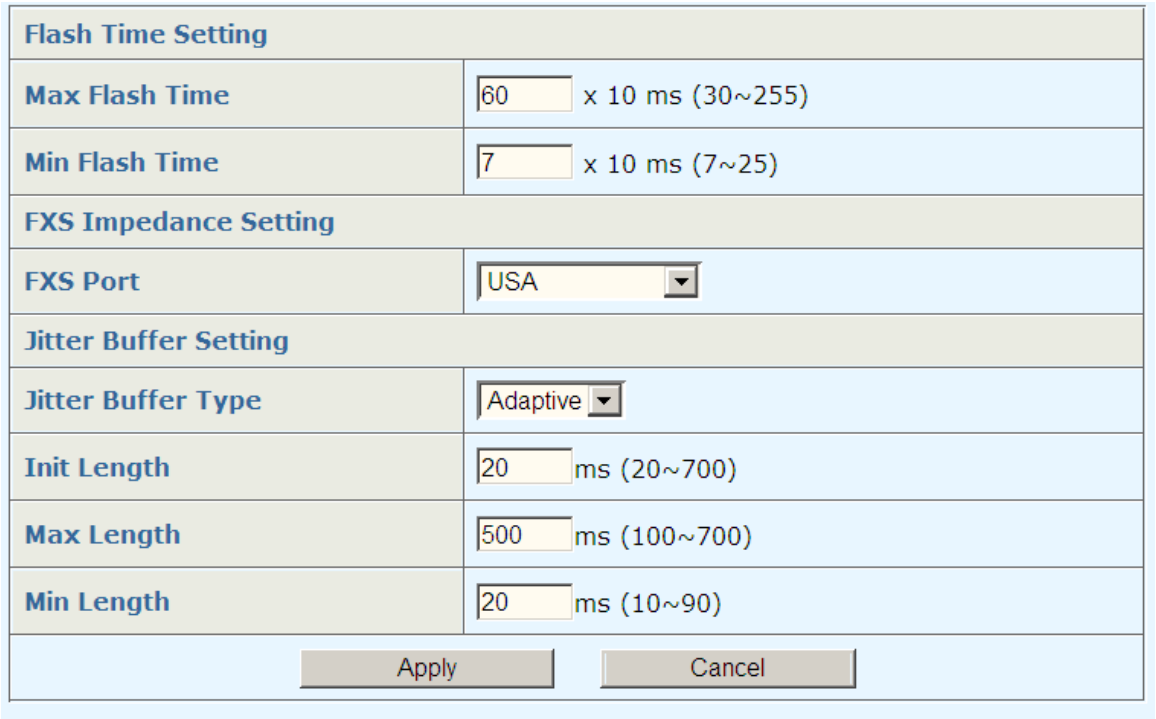
Jitter Buffer Type There are two kinds of jitter buffer: Fixed and Adaptive.

Init Length Specify the initial length of jitter buffer. It ranges from 20 to 700 milliseconds.

If you select adaptive jitter buffer, you should further specify the following parameters.

Max Length Specify the maximum length of jitter buffer. It ranges from 100 to 700 milliseconds.

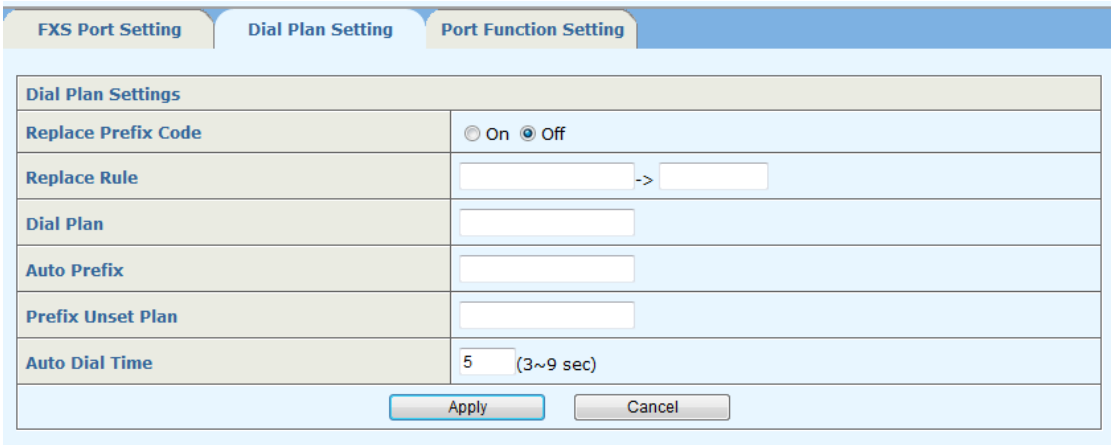
Min Length Specify the minimum length of jitter buffer. It ranges from 10 to 90 milliseconds.



After all settings are completed, click <Apply> to activate them.

12.1.2 Dial Plan Settings

The dial plan can be configured on this page.



Replace Prefix Code This can be set to “on” or “off”. When it is “on”, the Replace Rule will take effect.

Replace Rule The leading digits of an input number will be replaced if they match those specified in the Replace Rule.

There are some examples in the following:

a). If the Replace Rule is 001 -> 005,

The dialing Number “001+86+755+27602040” will be changed to “005-+86+755+27602040”.

b). If the Replace Rule is 001+009+006 -> 005,

The dialing Number “001+86+755+27602040” will become “005-+86+755+27602040”;

The dialing Number “009+86+755+27602040” will be changed to “005-+86+755+27602040”; and

The dialing Number “006+86+755+27602040” will be changed to “005-+86+755+27602040”.

- **Dial Plan**:

There are some examples in the following:

a). If Dial Plan is *xx

Input number (Dial Number) is *0#， System Send out Number is “*0#”.

b). If Dial Plan is 11x

After Input number (Dial Number) is “118”， auto stop to handle input number, system Send out Number is “118”.

digits	description
*0#	If the leading three characters are *0#, only these three characters will be dialed.
*xx	If the leading three characters are *00, *01, …, or *99, only these three characters will be dialed.
#xx	If the leading three characters are #00, #01, …, or #99, only these three characters will be dialed.
10x	If the leading three digits are 100, 101, …, or 109, only these three digits will be dialed.
11x	If the leading three digits are 110, 111,…, or 119, only these three digits will be dialed.
Xxxxxxxx	If the leading characters are eight digits, only these eight digits will be dialed.

- **Auto Prefix**: A number ranging between 0000 and 9999 will be used as a prefix.
- **Prefix Unset Plan**: **Auto Prefix** will not be applied if the leading digit(s) match(es) the **Prefix Unset Plan**.

There are some examples in the following:

a). Auto Prefix is 07, Prefix Unset Plan is 0
If the input number is 0075, 0075 will be dialed.

b). Auto Prefix is 07, Prefix Unset Plan is 1

If the input number is 0075, 070075 will be dialed.
If the input number is 10075, 10075 will be dialed.

c). Auto Prefix is 07, Prefix Unset Plan is 0+1

If the input number is 0075, 0075 will be dialed.

If the input number is 1075, 1075 will be dialed.

If the input number is 2075, 070075 will be dialed.

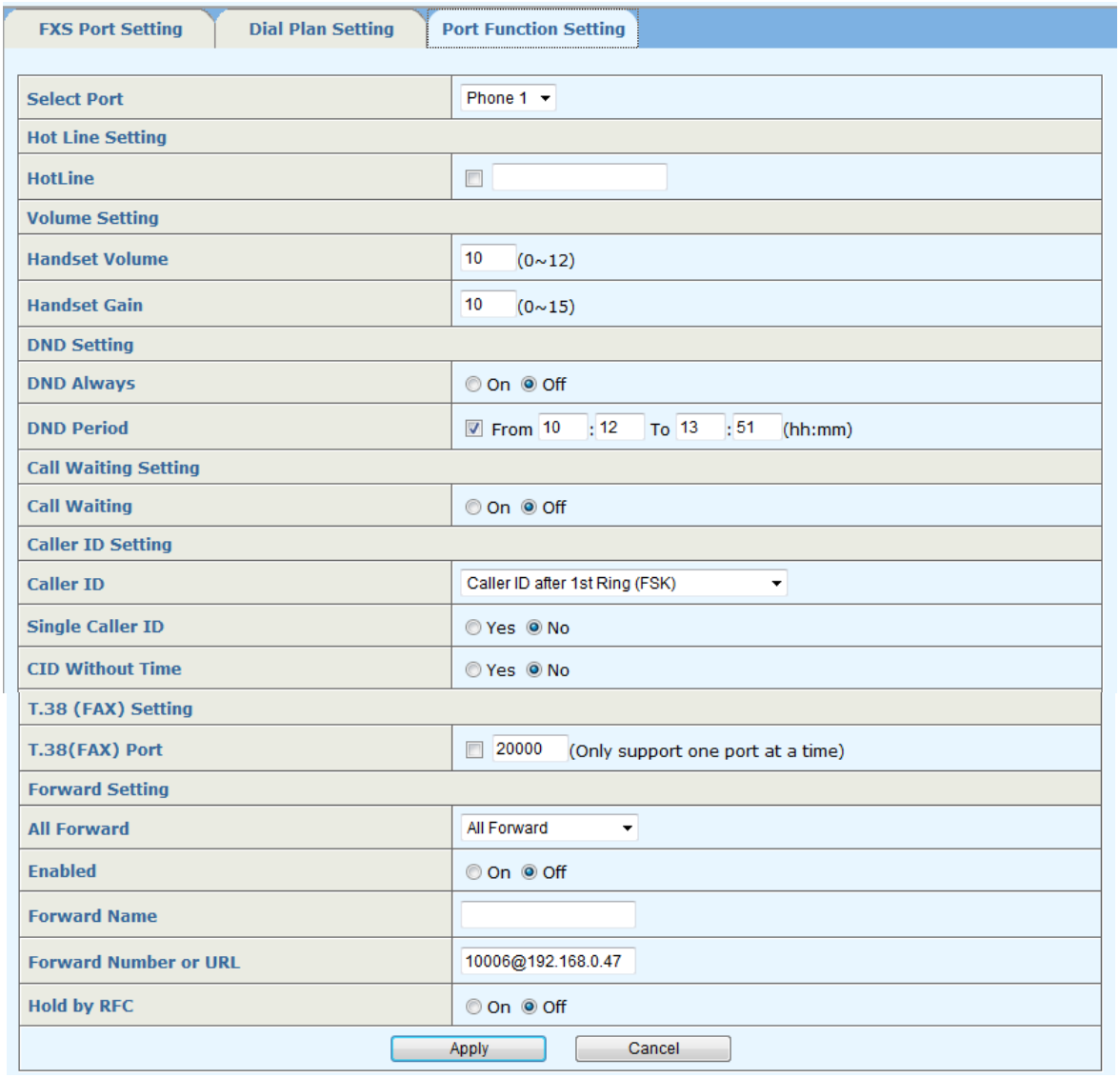
Digits	Description
0	Ignore auto prefix if first digit is '0'
1	Ignore auto prefix if first digit is '1'
xxxx	Ignore auto prefix if input number has 4 leading digits.
xxxxxx	Ignore auto prefix if input number has 6 leading digits.

- **Auto Dial Time**: If the input number does not end with "#", the number will be dialed after **Auto Dial Time** expires.

After all settings are completed, click <Apply> to activate.

12.1.3 Port Function Settings

You can configure Hot Line Settings, Volume Settings, Block, Caller ID, T.38 Fax, Call Waiting and Call forward on this page.



Select Port Select a phone port to be configured.

Hotline Click the checkbox to disable or enable hotline function.

Handset Volume Set the volume of the calling party's handset.

Handset Gain This feature controls the volume of the called party's handset.

DND Always All incoming calls will be blocked until this feature is disabled.

DND Period Set a time period during which incoming calls will be blocked. If the "From" setting is greater than the "To" setting, the "To" setting represents a time of the following day.

Call Waiting Enable or disable call waiting.

Call ID There are four settings of Caller ID. Select an FSK-based or DTMF-based setting that works with your telephone network.

T.38 Port Enable or disable the FAX function and configure the T.38 Fax port.

Call Forward There are three Forward modes: All Forward, Busy Forward and No Answer Forward.

All Forward All incoming calls will be forwarded to a preset number. If a speed dial number is entered in the URL field, all incoming calls will be forwarded to this speed dial number.

Busy Forward If you are on the phone, an incoming call will be forwarded to a specified number. If a speed dial number is entered in the URL field, the incoming calls will be forwarded to this speed dial number.

No Answer Forward If you do not answer the phone until the **Time Out** time expires, the incoming call will be forwarded to a specified number. If a speed dial number is entered in the URL field, the incoming call will be forwarded to this speed dial number. Also you have to set the Time Out rings for system to start to forward the call to the number you choose.

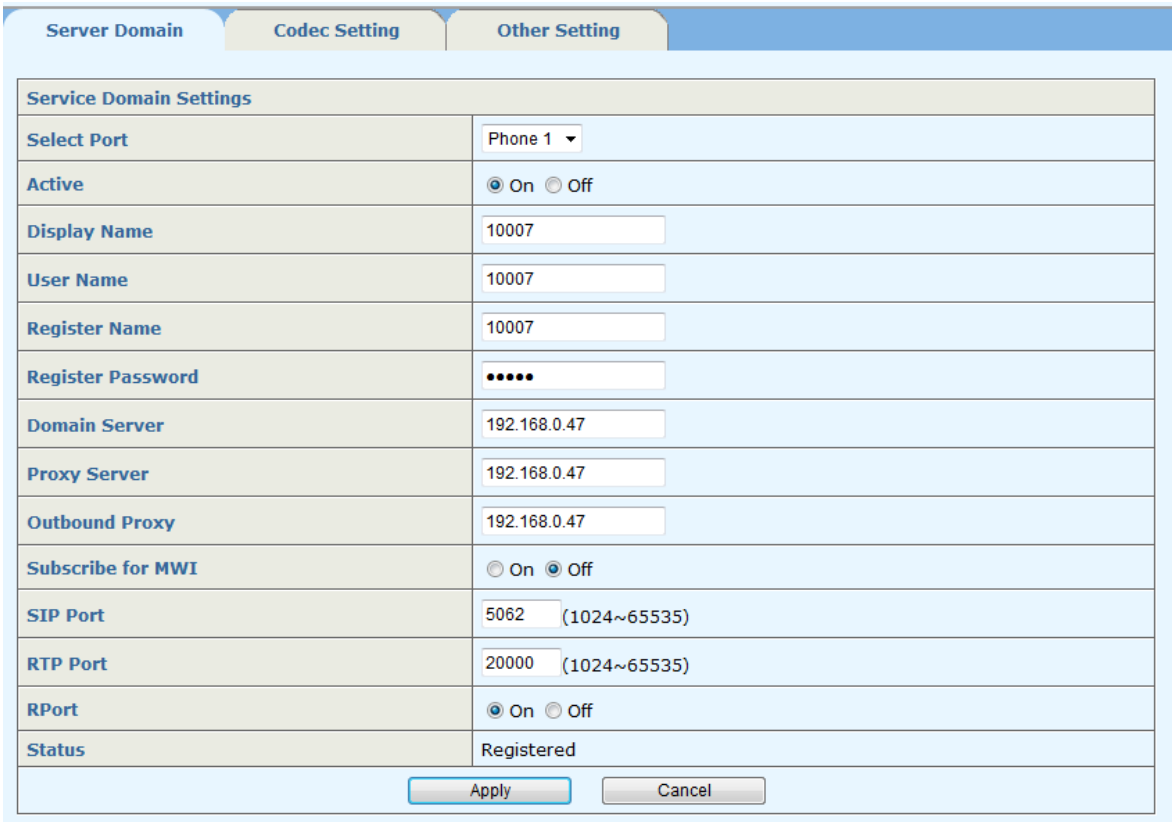
Hold By RFC Enable or disable "Hold by RFC".

After all settings are completed, click <Apply> to activate them.

12.2 SIP Settings

There are three tab pages for **IP Settings**: *Server domain, Codec Settings* and *other Settings*.

12.2.1 Server Domain



Select Port Select a phone port to be configured.

Active Enable or disable SIP phone register.

Display Name Type a display name.

User Name Type the user name assigned by the ISP.

Register Name Type the register name assigned by the ISP.

Register Password Type the register password for the register name.

Domain Server Type the ISP's domain server IP address.

Proxy Server Type the ISP's proxy server IP address.

Outbound Proxy Type the ISP's outbound proxy IP address. Leave this field blank, if you do not have the information.

Subscribe for MWI Enable or disable the message-waiting Indicator.

SIP Port Set up the SIP register port.

RTP Port Set up the RTP port.

Rport Enable or disable the Rport.

Status Display the phone registration status.

After all settings are completed, click <Apply> to activate them.

12.2.2 Codec Settings

You can configure the Codec Priority, RTP Packet Length, VAD and Codec ID on this page.

Codec Priority1~9 Select the codec priority. There are 10 codec options: G.711 u-law, G711 a-law, G.723, G.729, G.726-16, G.726-32, G.726-40, GSM and **Not Used**.

G.711/G.729 RTP Packet Length Select G.711/G.729 RTP packet length. There are 9 options: 10ms, 20ms, 30ms, 40ms, 50ms, 60ms, 70ms, 80ms and 90ms.

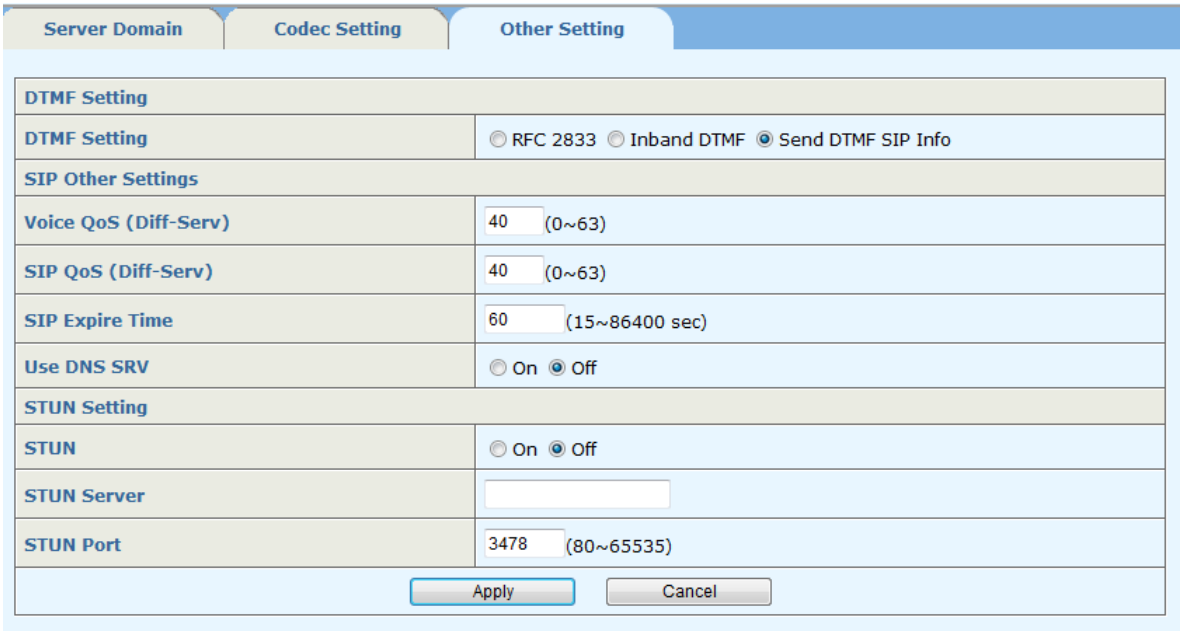
G.723 RTP Packet Length Select G.711/G.729 RTP packet length. There are 3 options: 30ms, 60ms and 90ms.

Codec ID Settings Set the codec ID's.

After all settings are completed, click <Apply> to activate them.

12.2.3 Other Settings

You can set up DTMF, Voice/SIP QoS and SIP expiry time on this page.



DTMF Settings There are 3 options for DTMF, including RFC2833，InBand DTMF and Send DTMF SIP Info.

Voice QoS Set up the quality of service for voice.

SIP Qos Set up the quality of service for SIP.

SIP Expire Time Set the SIP registration expiry time.

Use DNS SRV Disable or enable DNS SRV.

STUN Disable or enable STUN server.

STUN Server Type the STUN server.

STUN Port Specify the STUN port.

After all settings are completed, click <Apply> to activate them.

12.3 Network Settings

VoIP VLANs are configured specially for voice data stream. By configuring VoIP VLANs and adding the ports with voice devices attached to VoIP VLANs, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice data stream and voice quality.

Configuration Steps:

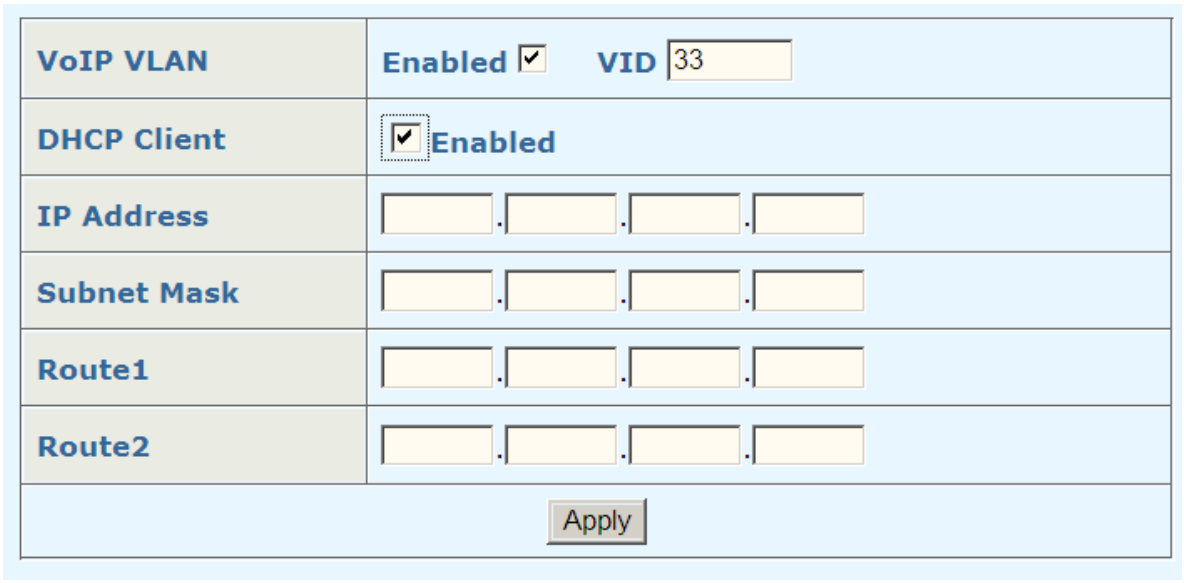
Step 1 Enable/disable VoIP VLAN;

Step 2 If VoIP VLAN is enabled, specify its VID;

Step 3 Set the IP address for VoIP VLAN, if you adopt DHCP for it, enable “DHCP Client”; if you adopt static IP, you should input the IP address, subnet mask, route 1 and route 2. Decide to

enable/disable the DHCP Client role for VoIP VLAN;

Step 4 If DHCP Client is not enabled, you have to specify its IP address, subnet mask, route 1and route 2. If the Phone 1 SIP server can only be reached by a specified route, type the next route IP address in **Phone 1 Route** field, otherwise it will adopt default route to look for the Phone 1 SIP server. And in P**hone 2 Route** field, type the next route IP address of the Phone 2 SIP server.



13 Statistics

It shows the concerned statistic information of the device, including port status, port statistics, VLAN list, MAC address table and IGMP snooping group.

13.1 Port status

This page shows the State, Link, Negotiation, Speed & Duplex, Flow Control, Learning and MDI/MDIX of each Ethernet port.

Port	State	Link	Negotiation	Speed&Duplex	Flow Control	Learning	MDI/MDIX
LAN1	Enabled	Down	Auto	-	-	Enabled	MDI
LAN2	Enabled	Down	Auto	-	-	Enabled	MDIX
LAN3	Enabled	Down	Auto	-	-	Enabled	MDIX
LAN4	Enabled	Down	Auto	-	-	Enabled	MDIX
LAN5	Enabled	Up	Auto	100M Full	Off	Enabled	MDIX
LAN6	Enabled	Down	Auto	-	-	Enabled	MDI
LAN7	Enabled	Down	Auto	-	-	Enabled	MDIX
LAN8	Enabled	Down	Auto	-	-	Enabled	MDI
WAN	Enabled	Down	Force	-	-	Enabled	-

13.2 Port statistics

This page shows the TxGoodPkts, TxBadPkts, RxGoodPkts, RxBadPkts, TxAbort, Collision, and DropPkt of each Ethernet port.

TxGoodPkts The total number of outgoing normal packets on the port, including outgoing normal packets and normal pause frames

TxBadPkts The total byte number of outgoing error frames

RxGoodPkts The total number of incoming normal packets on the port, including incoming normal packets and normal pause frames

RxBadPkts The total number of incoming error frames

TxFCSErr The number of error FCS frames

Collision The number of detected collisions

DropPkt The number of packets dropped for various reasons

Port	TxGoodPkts	TxBadPkts	RxGoodPkts	RxBadPkts	TxFCSErr	Collision	DropPkt
LAN1	0	0	0	0	0	0	0
LAN2	0	0	0	0	0	0	0
LAN3	0	0	0	0	0	0	0
LAN4	0	0	0	0	0	0	0
LAN5	36104	0	20905	0	0	0	0
LAN6	0	0	0	0	0	0	0
LAN7	19330	0	35442	0	0	0	0
LAN8	0	0	0	0	0	0	0
WAN	0	0	0	0	0	0	0

Reset

13.3 VLAN List

This page lists the information of all VLANs, including VID, Name, Type and member port type: Tagged or Untagged **Tagged** lists all ports from which packets are sent tagged; **Untagged** lists all ports from which packets are sent untagged.

VID	Name	Type	Tagged	Untagged
1	Default	Static	-	LAN1-8,WAN
2	vlan 2	Static	LAN5	LAN6

13.4 MAC Address Table

This page shows information of unicast MAC address entries in the MAC address table, including **VID**, **Unicast MAC Address**, **Port**, and **Type**. **Type** includes **Dynamic**, **Static**, and **Blackhole**.

VID	Unicast MAC Address	Port	Type
1	00-11-11-21-21-21	LAN1	Static
1	00-12-11-11-22-22	LAN2	Blackhole
1	00-1e-6e-00-57-c1	LAN7	Dynamic
1	00-1e-6e-6a-7b-8c	CPU	Static
1	4c-1f-cc-11-da-c5	LAN7	Dynamic
1	50-e5-49-e4-44-f7	LAN5	Dynamic
2	00-1e-6e-6a-7b-8c	CPU	Static

13.5 IGMP Snooping Group

This page shows IGMP Snooping multicast group information, including **VID**, **Multicast Group**, **MAC Address**, and **Member Ports**. **Multicast Group** is the IP address of a multicast group, **MAC Address** is the address of a multicast MAC group, and **Member Ports** include all ports belonging to this IGMP Snooping group.

VID	Multicast Group	MAC Address	Member Ports
1	224.8.8.8	01-00-5e-08-08-08	LAN5,8
1	224.9.9.9	01-00-5e-09-09-09	LAN8

14 Spanning Tree

(1) Introduction to STP

STP was developed based on the 802.1d standard of IEEE to eliminate loops at the data link layer in a local area network (LAN). Devices running this protocol detect loops in the network by exchanging information with one another and eliminate loops by selectively blocking certain ports to prune the loop structure into a loop-free tree structure. This avoids proliferation and infinite cycling of packets that would occur in a loop network and prevents decreased performance of network devices caused by duplicate packets received.

In the narrow sense, STP refers to the IEEE 802.1d STP; in the broad sense, STP refers to the IEEE 802.1d STP and various enhanced spanning tree protocols derived from that protocol.

(2) Protocol Packets of STP

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets. STP-enabled network devices exchange BPDUs to establish a spanning tree. BPDUs contain sufficient information for the network devices to complete spanning tree calculation.

In STP, BPDUs have the following types:

- Configuration BPDUs, used for calculating a spanning tree and maintaining the spanning tree topology.
- Topology change notification (TCN) BPDUs, used for notifying the concerned devices of network topology changes, if any.

(3) Basic Concepts in STP

1. Root bridge

A tree network must have a root bridge.

There is only one root bridge in the entire network. The root bridge is not fixed, but can change along with changes of the network topology. Upon initialization of a network, each device generates and sends out BPDUs periodically with itself as the root bridge; after network convergence, only the root bridge generates and sends out configuration BPDUs at a certain interval, and the other devices just forward BPDUs.

2. Root port

On a non-root bridge, the port nearest to the root bridge is the root port. The root port is responsible for communication with the root bridge. Each non-root bridge has one and only one root port. The root bridge has no root port.

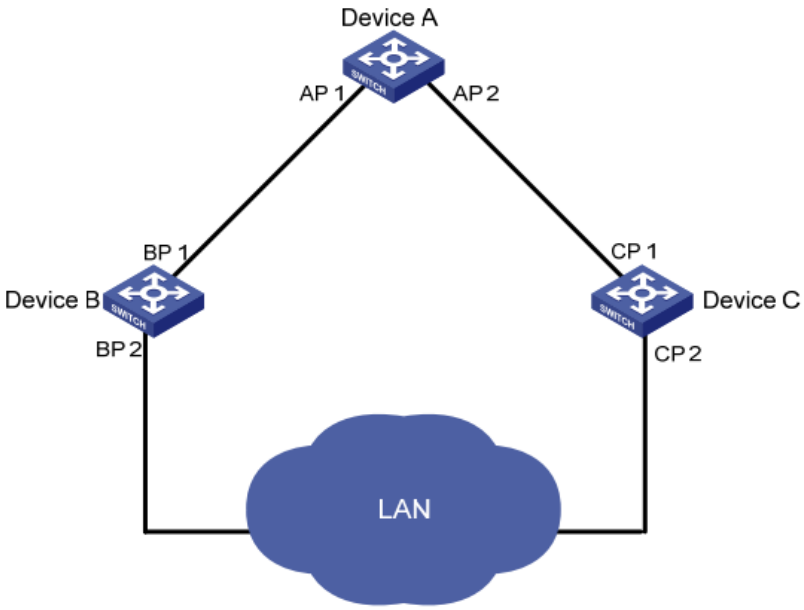
3. Designated bridge and designated port

Classification Designated bridge Designated port

Classification	Designated bridge	Designated port
For a device	A device directly connected to the local device and responsible for forwarding BPDUs to the local device.	The port through which the designated bridge forwards BPDUs to the local device.
For a LAN	The device responsible for forwarding BPDUs to this LAN segment.	The port through which the designated bridge forwards BPDUs to this LAN segment.

As shown in the following figure, AP1 and AP2, BP1 and BP2, and CP1 and CP2 are ports on Device A, Device B, and Device C respectively.

- If Device A forwards BPDUs to Device B through AP1, the designated bridge for Device B is Device A, and the designated port of Device B is port AP1 on Device A.
- Two devices are connected to the LAN: Device B and Device C. If Device B forwards BPDUs to the LAN, the designated bridge for the LAN is Device B, and the designated port for the LAN is the port BP2 on Device B.



4. Path cost

Path cost is a reference value used for link selection in STP. By calculating path costs, STP selects relatively robust links and blocks redundant links, and finally prunes the network into a loop-free tree.

14.1 STP

Note： Enable STP in Advanced Configuration.

14.1.1 Basic STP

The flowing factors should be considered to configure STP.

Priority Configure the priority of the device. It ranges from 0 to 65535, and 32768 by default. The priority is greater with a smaller value.

Hello Time It specifies the interval to send BPDU packets. It is used to test the links. Hello Time ranges from 1 to 10 seconds and is 2 by default.

Max Age It specifies the maximum time the device can wait without receiving a BPDU before attempting to reconfigure. Max. Age ranges from 6 to 40 seconds and is 20s by default.

Forward Delay Time It specifies the time for the port to transit its state after the network topology is changed. Forward Delay ranges from 4 to 30 seconds and is 15 by default.

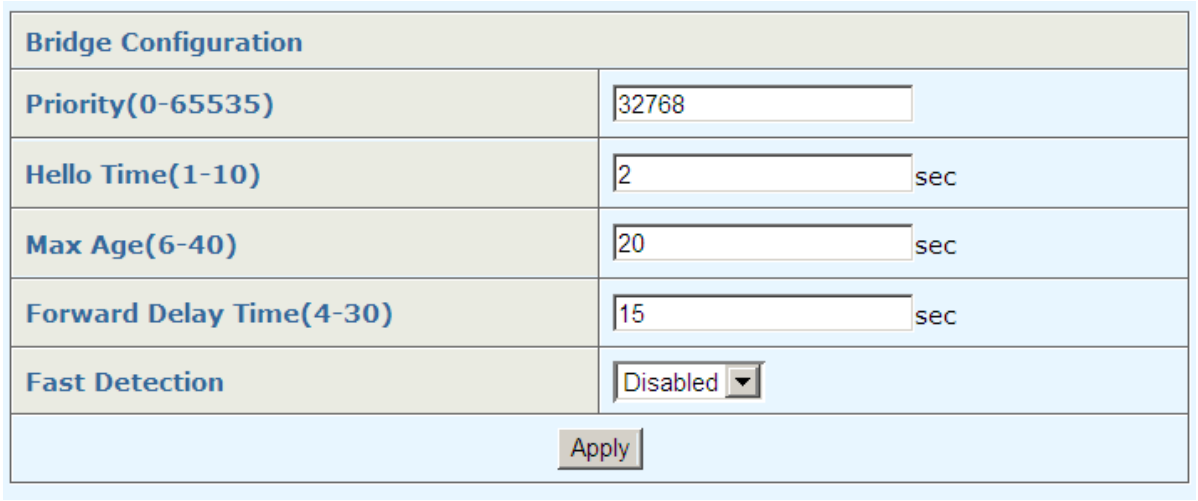
When the STP regeneration caused by network malfunction occurs, the STP structure will get some corresponding change. However, as the new configuration BPDUs cannot be spread in the whole network at once, the temporal loop will occur if the port cannot transits its state immediately. Therefore, STP adopts a state transit mechanism, that is, the new root port and the designated port begins to forward data after twice forward delay, which ensures the new configuration BPDUs are spread in the whole network.

Fast Detection： Enable or disable fast detection funciton. It is disabled by default.

For the above three timers, they should satisfy the following requirement to prevent frequent network jitter:

2 × (Forward Delay Time - 1second) >= Max Age

Max Age >= 2 × (Hello Time + 1second)



14.1.2 STP Information

It shows the bridge information of the device.

Bridge ID Consisting of the priority and MAC address of the bridge. Bridge priority is 32768 by default. With the same bridge priority, the device with the lower bridge ID has the higher priority.

Root Bridge ID Consisting of the priority and MAC address of the root bridge. Bridge priority is 32768 by default. With the same root priority, the device with the lower root bridge MAC has the higher priority.

Root Port Indicates the port that has the lowest path cost from this bridge to the Root Bridge and forwards packets to the root.

Root Path cost The cost of the shortest path to the root bridge.

Designated Bridge	
Bridge ID	32768:00-1e-6e-6a-7b-8c
Root Bridge ID	32768:00-1e-6e-6a-7b-8c
Root Port	0
Root Path Cost	0

14.1.3 STP Port Attributes

You can configure the STP attributes of each port of the device, including the following items:

STP status Select to enable or disable STP on a specified port.

Port Fast In order to allow the port to transit to forwarding state quickly, enable the STP **Port Fast** feature, which can immediately transit the port into STP forwarding state upon linkup. This port still participates in STP. In case that the port forms a loop, it will transit into STP blocking state.

Root Protection It is disabled by default.

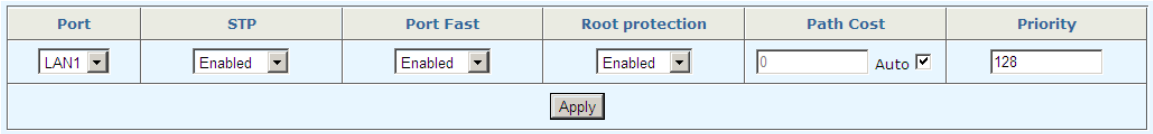
Due to configuration error or malicious attack, the root bridge in a network may receive configuration BPDUs with priorities higher than that of itself, which causes new root bridge to be elected and network topology jitter. In this case, data flows that should have been transmitted along a high-speed link are led to a low-speed link. This problem can be resolved by enabling root protection function. Root-protection-enabled ports can only be kept as designated ports. When a port of this type receives configuration BPDUs with higher priorities, more precisely, when it becomes a non-designated port, it turns to discarding state and stops forwarding packets (as if it is disconnected from the link).

Path Cost Sets the path cost of a specified port. It is in the range of 1 to 200000000, the

default value is 55. You can also make it auto-configured.

Priority Sets a port priority for a specified port. It is in the range of 0 to 255, the default value is 128.

Port attributes are listed at the bottom.



Port Attributes

Port	STP	Port Fast	Root protection	Port State	Port Role	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost
LAN1	Enabled	Enabled	Enabled	Blocking	Disabled	-	128	32768:001e6e6a7b8c	128:1	0
LAN2	Enabled	Enabled	Enabled	Blocking	Disabled	-	128	32768:001e6e6a7b8c	128:2	0
LAN3	Disabled	Disabled	Disabled	Blocking	Disabled	55	128	0:000000000000	0:0	0
LAN4	Disabled	Disabled	Disabled	Blocking	Disabled	55	128	0:000000000000	0:0	0
LAN5	Disabled	Disabled	Disabled	Blocking	Disabled	55	128	0:000000000000	0:0	0
LAN6	Disabled	Disabled	Disabled	Blocking	Disabled	55	128	0:000000000000	0:0	0
LAN7	Disabled	Disabled	Disabled	Blocking	Disabled	55	128	0:000000000000	0:0	0
LAN8	Disabled	Disabled	Disabled	Blocking	Disabled	55	128	0:000000000000	0:0	0
WAN	Disabled	Disabled	Disabled	Blocking	Disabled	55	128	0:000000000000	0:0	0

14.2 RSTP

📖 Note: Enable RSTP in Advanced Configuration before configuration, while the STP parameters are effective.

Developed based on the 802.1w standard of IEEE, RSTP is an optimized version of STP. It achieves rapid network convergence by allowing a newly elected root port or designated port to enter the forwarding state much quicker under certain conditions than in STP.

Point to Point Indicates the link between two devices directly connected.

Protocol Migration When enable Protocol Migration on a specified port, if RSTP is enabled on this port, while the port on the peer device enables STP, and then the BPDU packets sent from this port will be automatically transited from RSTP to STP.

Edge Port Indicates the port connected directly to terminals. Select “Yes” to configure the specified port as an edge port. By default, all ports are edge ports.

If the designated port is an edge port, it can directly transit to forwarding state; if the designated port is connecting to a point-to-point link, it can transit to forwarding state after getting response from the downstream device through handshake. So it is suggested to configure the ports connected with terminals to be edge ports.

Port	Point to Point	Protocol Migration	Edge Port
LAN1	Enabled	Enabled	Yes
Apply			

Port Attributes

Port	Spanning Tree Mode	Port State	Port Role	Point to Point	Protocol Migration	Edge Port
LAN1	RSTP	Blocking	Disabled	Enabled	Enabled	Yes
LAN2	RSTP	Blocking	Disabled	Enabled	Enabled	No
LAN3	RSTP	Blocking	Disabled	Enabled	Enabled	Yes
LAN4	RSTP	Blocking	Disabled	Enabled	Enabled	No
LAN5	RSTP	Blocking	Disabled	Enabled	Enabled	No
LAN6	RSTP	Blocking	Disabled	Enabled	Enabled	No
LAN7	RSTP	Blocking	Disabled	Enabled	Enabled	No
LAN8	RSTP	Blocking	Disabled	Enabled	Enabled	No
WAN	RSTP	Blocking	Disabled	Enabled	Enabled	No

15 SNMP Manager

The Simple Network Management Protocol (SNMP) is an Internet standard protocol, widely used for a network management station (NMS) to access and operate the devices (SNMP agents) on a network, regardless of their vendors, physical characteristics and interconnect technologies.

SNMP enables network administrators to read and set the variables on managed devices to monitor their operating and health state, diagnose network problems, and collect statistics for management purposes.

AE208 Gateway SNMP agents support three SNMP versions: SNMPv1, SNMPv2c, and SNMPv3.

SNMPv1 uses Community Name authentication to control access to SNMP agents. SNMPv1 Community Name fall into read only passwords and read and write passwords.

A read Community Name enables reading data from an SNMP agent.
A read and write Community Name enables reading data and setting variables on an SNMP agent.

SNMPv2c also uses Community Name authentication for SNMP agent access control. It is compatible with SNMPv1, but supports more operation modes, data types, and error codes.

SNMPv3 uses a user-based security model (USM) to secure SNMP communication. You can configure authentication and privacy mechanisms to authenticate access and encrypt SNMP

📖 Note:
An NMS and an SNMP agent must use the same SNMP version to communicate with each other.

SNMP management frame includes three network elements: SNMP Management Station, SNMP Agent and MIB (Management Information Base).

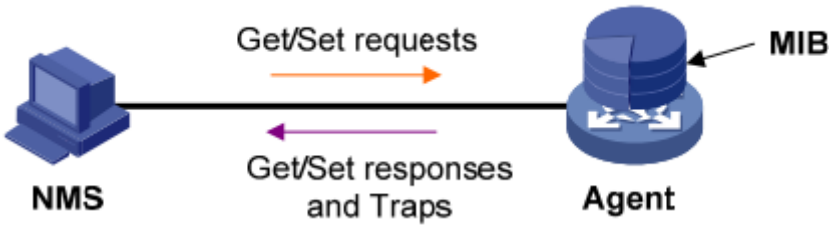
SNMP Management Station: SNMP Management Station is the workstation for running the SNMP client program, providing a friendly management interface for the administrator to manage the most network devices conveniently.

SNMP Agent: Agent is the server software operated on network devices with the responsibility of receiving and processing the request packets from SNMP Management Station. In the meanwhile, Agent will inform the SNMP Management Station of the events whenever the device status changes or the device encounters any abnormalities such as restarting the device.

MIB: MIB is the set of the managed objects. MIB defines a few attributes of the managed objects, including the names, the access rights, and the data types. Every SNMP Agent has its own MIB. The SNMP Management station can read/write the MIB objects basing on its management right.

SNMP Management Station is the manager of SNMP network while SNMP Agent is the managed object. The information between SNMP Management Station and SNMP Agent are exchanged

through SNMP (Simple Network Management Protocol). The relationship among SNMP Management Station, SNMP Agent and MIB is illustrated in the following figure.



15.1 SNMP Account

15.1.1 SNMP Community

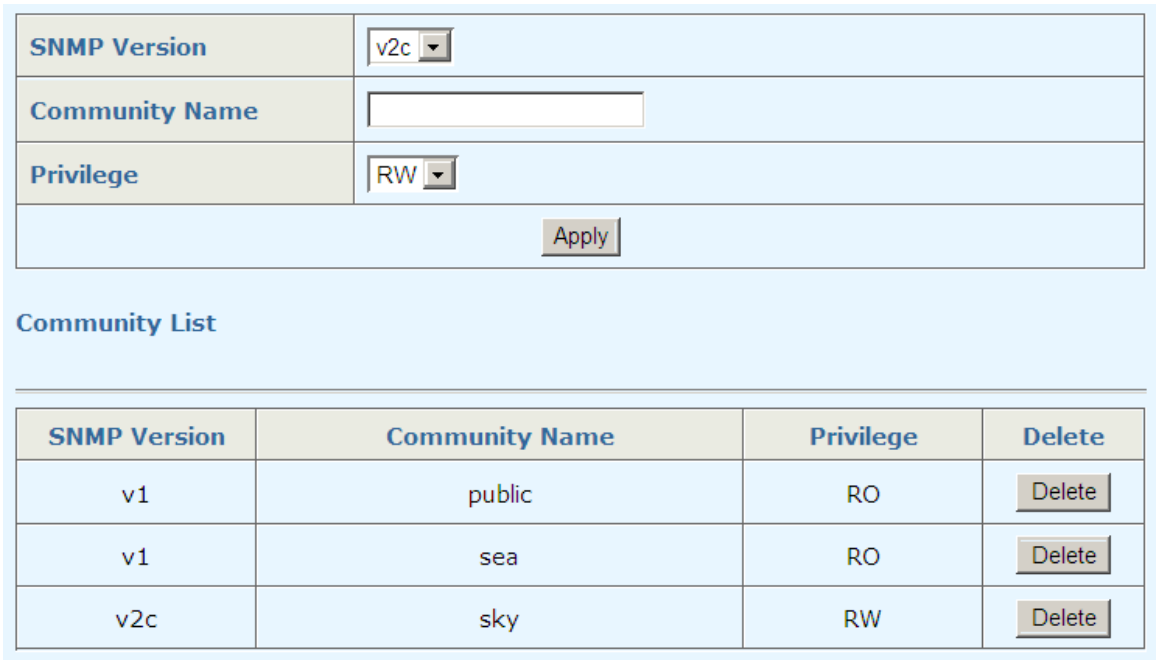
Create SNMP account.

- Select SNMP version (v1 and v2c)
- Type a community name; it is a string of 3 to 16 characters.
- Select the privilege (RW and RO)

RO: Specifies the community that has been created has read-only permission to access MIB objects. Communities of this type can only query MIBs for device information.

RW: Specifies the community that has been created has read-write permission to access MIB objects. Communities of this type are capable of configuring devices.

The community list is shown at the bottom.



15.1.2 SNMP User

The User can manage the device via the management station software. You can configure the SNMP User on this page.

User Name Type the User Name here. It is a string of 3 to 16 characters.

Privilege Select the privilege to be RO or RW.

SNMP V3 Encryption Click to enable SNMP V3 Encryption. If SNMP V3 Encryption is not selected, neither encryption nor authentication will be performed.

Auth Algorithm Select the Authentication Algorithm for the SNMP v3 User.

MD5: The authentication is performed via HMAC-MD5 algorithm.
SHA: The authentication is performed via SHA (Secure Hash Algorithm). This authentication mode has a higher security than MD5 mode.

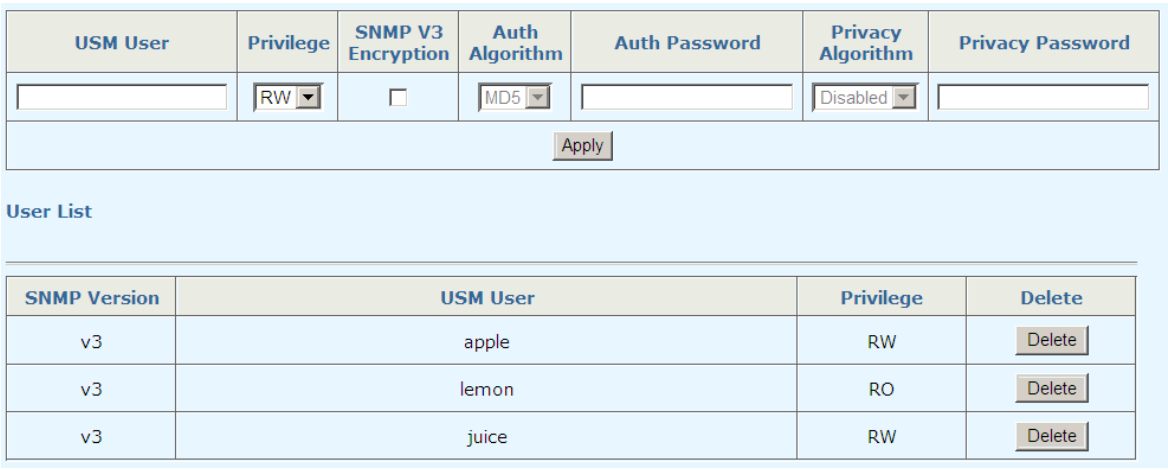
Auth Password Type the password for authentication. It is a string of 9 to 15 characters in plain text, or a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, or a 40-bit hexadecimal number in cipher text if SHA algorithm is used.

Privacy Algorithm Select the Privacy Algorithm for the SNMP v3 User.

Disable: No privacy method is used.
DES: DES encryption method is used.
AES: AES encryption method is used.

Privacy Password Type the privacy password. It is a string of 9 to 15 characters in plain text, or a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, or a 40-bit hexadecimal number in cipher text if SHA algorithm is used.

The user list is displayed at the bottom, the users can be deleted.

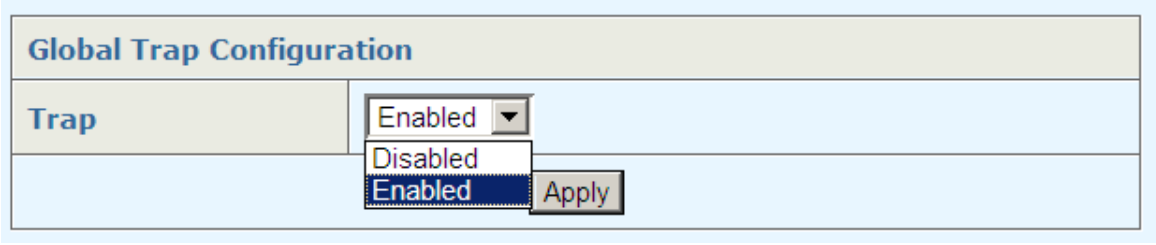


15.2 SNMP Trap

Agent use SNMP Trap to send traps to NMS.

15.2.1 Global Trap

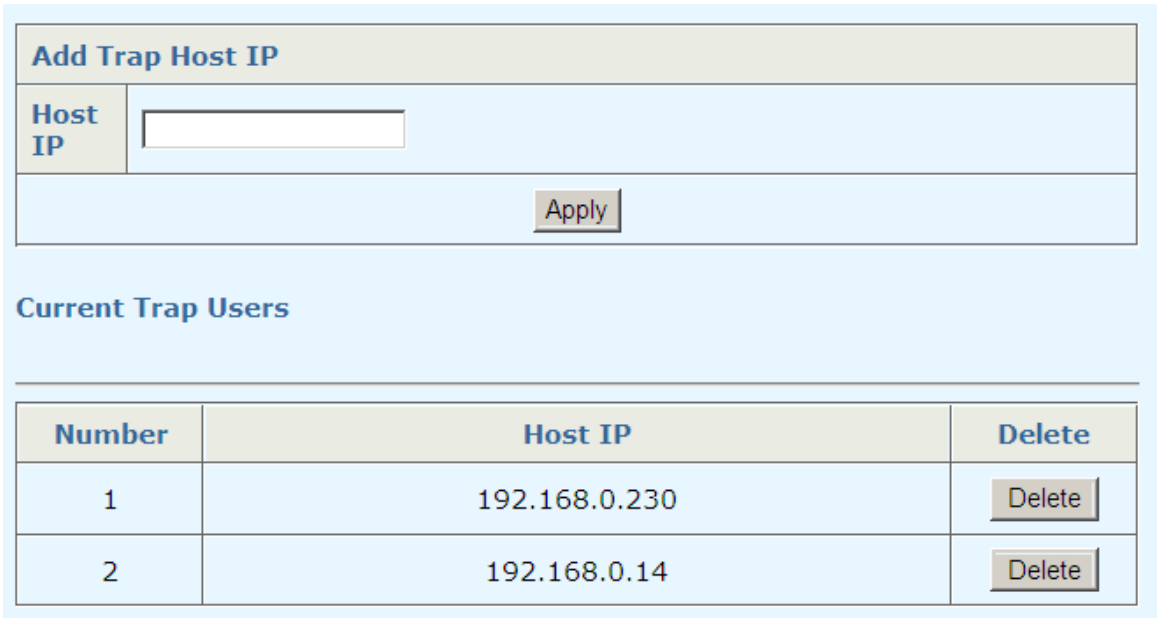
On this page, you can enable or disable Trap globally.



15.2.2 Trap Host IP

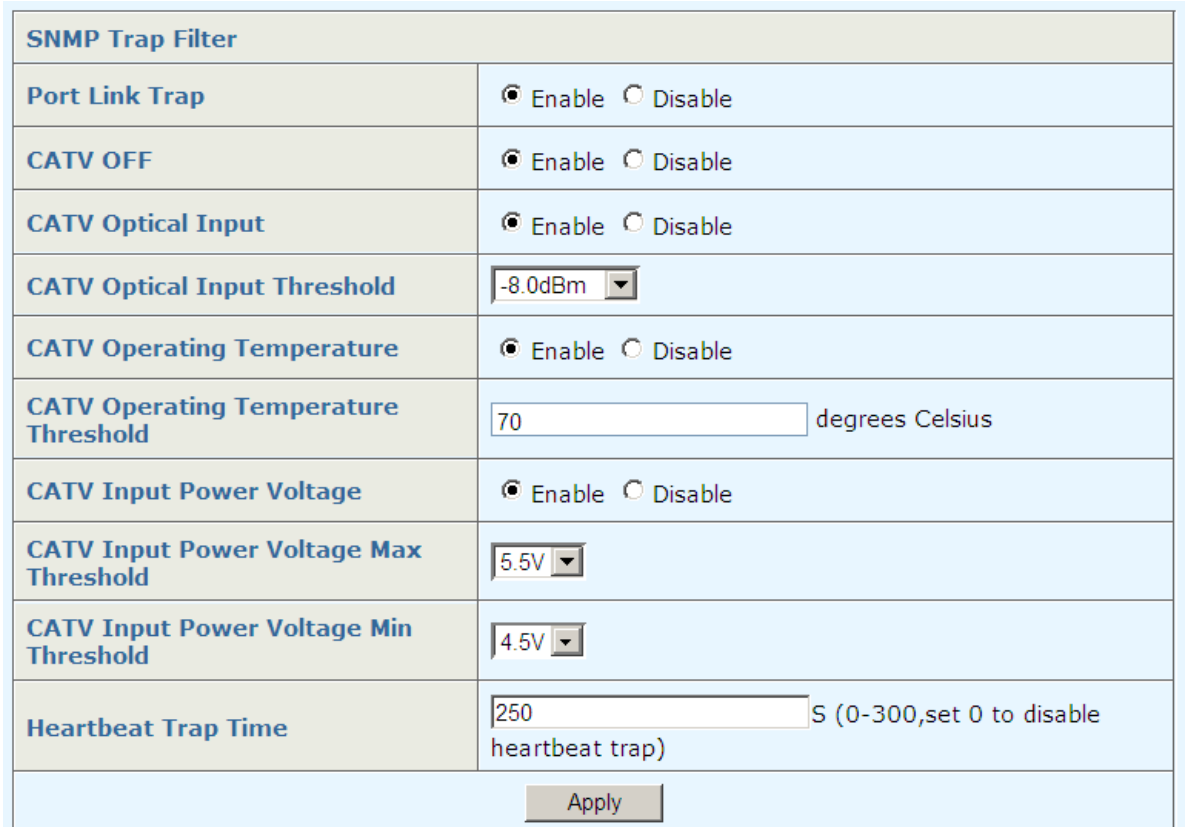
This tab page specifies SNMP trap Host IP. Host IP is the IPv4 address of the host to receive the traps.

The bottom part of this page lists all existing trap host IP addresses. They can be deleted.



15.2.3 Trap Filter

On this page, you can decide to trigger traps in what situations. You can enable or disable the trap and further set the threshold.



Port Link Trap: If enable the port link trap function, the device will send a trap in port link up or link down.

CATV Off: If enable CATV trap function, when CATV module status is changed, trap will be sent.

CATV Optical Input & **CATV Optical Input Threshold**: If “CATV Optical Input” is set as “Enable”, when CATV input optical power is lower than “CATV Optical Input Threshold”, trap will be sent.

CATV Operating Temperature & **CATV Operating Temperature Threshold**: If “CATV Operating Temperature” is set as “Enable”, when CATV operating temperature is higher than “CATV Operating Temperature Threshold”, trap will be sent.

CATV Input Power Voltage & **CATV Input Power Voltage Max Threshold &CATV Input Power Voltage Min Threshold**: If “CATV Input Power Voltage” is set as “Enable”, when CATV input power Voltage is higher than “CATV Input Power Voltage Max Threshold” or lower than the “CATV Input Power Voltage Min Threshold”, trap will be sent.

Heartbeat Trap Time: If it is set as "0", the function of Heartbeat trap will be disabled. If this function is enabled, please set this value to be in the range of 1 to 300 seconds, which indicates the interval of Heartbeat Trap. When “Heartbeat Trap Time” is timeout, trap will be sent.

16 RMON

RMON (Remote Monitoring) based on SNMP (Simple Network Management Protocol) architecture, functions to monitor the network. RMON is currently a commonly used network management standard defined by Internet Engineering Task Force (IETF), which is mainly used to monitor the data traffic across a network segment or even the entire network so as to enable the network administrator to take the protection measures in time to avoid any network malfunction. In addition, RMON MIB records network statistics information of network performance and malfunction periodically, based on which the management station can monitor network at any time effectively. RMON is helpful for network administrator to manage the large-scale network since it reduces the communication traffic between management station and managed agent.

This device supports the following four RMON Groups defined on the RMON standard (RFC1757): History Group, Event Group, Statistic Group and Alarm Group.

RMON Group	Function
History Group	After a history group is configured, the device collects and records network statistics information periodically, based on which the management station can monitor network effectively.
Event Group	Event Group is used to define RMON events. Alarms occur when an event is detected.
Statistic Group	Statistic Group is set to monitor the statistic of alarm variables on the specific ports.
Alarm Group	Alarm Group is configured to monitor the specific alarm variables. When the value of a monitored variable exceeds the threshold, an alarm event is generated, which triggers the device to act in the set way.

16.1 Statistics

This page shows the statistics of Stats Octets, Stats Pkts, Broadcastkts, MulticastPkts, CRC Align Errors, Under size Pkts, Over size Pkts, Fragments, Jabbers, Collisions, Pkts 64 Octets, Pkts 64 to 127 Octets, Pkts 128 to 255 Octets, Pkts 256 to 511 Octets, Pkts512 to 1023 Octets, Pkts1024 to 1518 Octets, and Drop Events of each ethernet port.

Port	LAN2
Stats Octets	3960349
Stats Pkts	26109
Broadcast Pkts	530
Multicast Pkts	160
CRC Align Errors	0
Under size Pkts	0
Over size Pkts	0
Fragments	0
Jabbers	0
Collisions	0
Pkts 64 Octets	13458
Pkts 65 to 127 Octets	27268
Pkts 128 to 255 Octets	2537
Pkts 256 to 511 Octets	2264
Pkts 512 to 1023 Octets	2241
Pkts 1024 to 1518 Octets	12532
Drop Events	0
Reset	

Stats Octets The total number of octets of transmitted data, including bad packets, received from network; it excludes framing bits but includes Frame Check Sequence (FCS) octets.

Stats Pkts The total number of transmitted packets, including bad packets, broadcast packets and multicast packets.

Broadcastkts The total number of the received good packets that are directed to the broadcast address, except the multicast packets.

MulticastPkts The total number of the received good packets that are directed to a multicast address, except the packets directed to the broadcast address.

CRC Align Errors The total number of the received packets that has a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets (both inclusive), and has either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under size Pkts The total number of the received packets that are less than 64 octets long (excluding framing bits, but including FCS octets).

Over size Pkts The total number of the received packets that are longer than 1518 octets

(excluding framing bits, but including FCS octets).

Fragments The total number of the received packets that are less than 64 octets in length (excluding framing bits, but including FCS octets), and has either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Jabbers The total number of the received packets that are longer than 1518 octets (excluding framing bits, but including FCS octets), and has either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Collisions The best estimate of the total number of collisions on this Ethernet segment.

Pkts 64 Octets The total number of received packets, that are 64 octets in length (excluding framing bits, but including FCS octets), including bad packets.

Pkts65 to 127 Octets The total number of received packets, that are between 65 and 127 octets in length inclusive (excluding framing bits, but including FCS octets), including bad packets.

Pkts 128 to255 Octets The total number of received packets, that are between 128 and 255 octets in length inclusive (excluding framing bits, but including FCS octets), including bad packets.

Pkts256 to 511 Octets The total number of packets, including bad packets, received that are between 256 and 511 octets in length inclusive (excluding framing bits, but including FCS octets).

Pkts512 to 1023 Octets The total number of received packets, that are between 512 and 1023 octets in length inclusive (excluding framing bits, but including FCS octets), including bad packets.

Pkts1024 to 1518 Octets The total number of received packets, that are between 102 4and 1518 octets in length inclusive (excluding framing bits, but including FCS octets), including bad packets.

Drop Events The total number of events in which packets are dropped by the probe due to lack of resources.

All of the statistics for each Ethernet port can be reset.

16.2 History

16.2.1 History Control

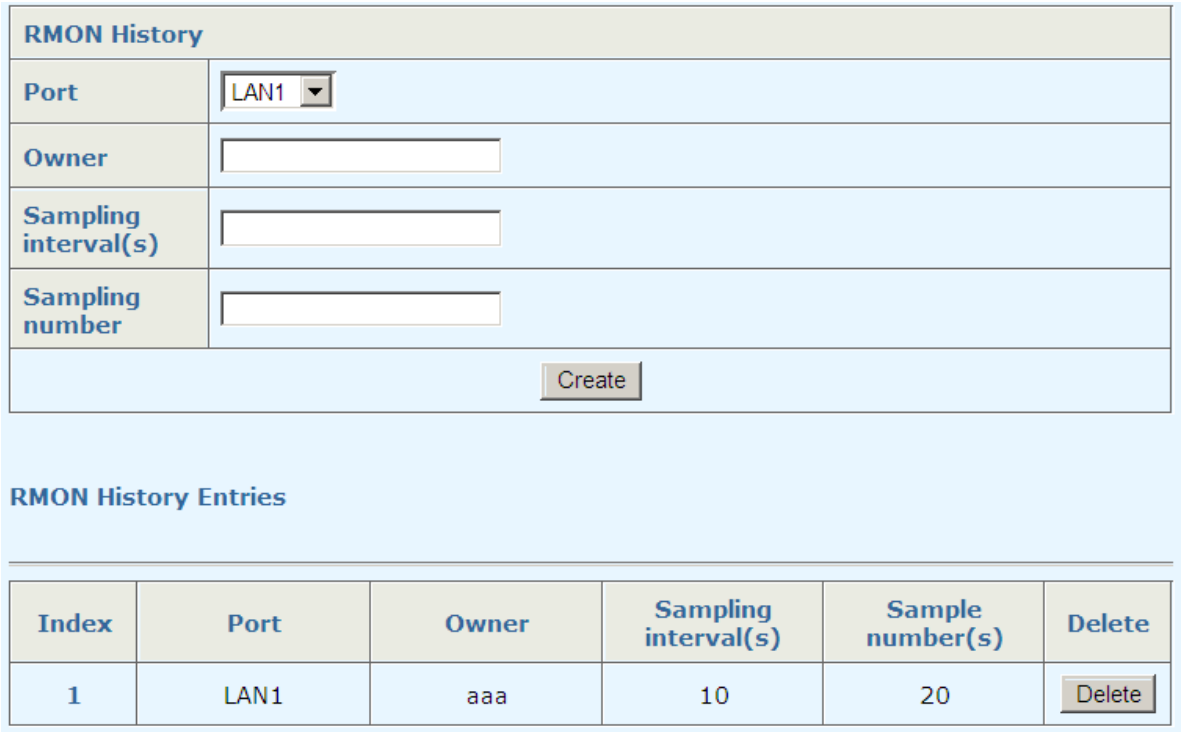
This page sets a history control entry.

Port The Ethernet port for collecting statistics.

Owner The entity that configures this entry and is therefore using the resources assigned to it.

Sampling interval(s) The data sample time interval of each group. The interval range is from 1 and 3600(1 hour).

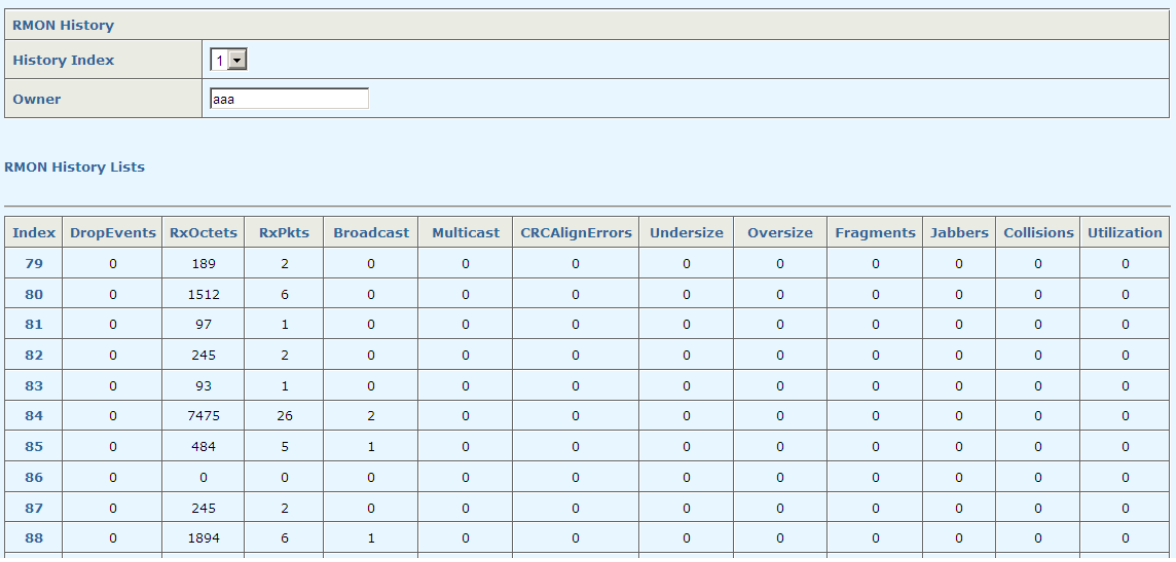
Sampling number The number of discrete sampling intervals over which data shall be saved in the part of the media-specific table associated with this history control entry. It shall be an integer ranging from 1 to 50.



16.2.2 History List

On this page, one of the histories can be selected to show the related statistics.

The bottom part of this page shows the related statistic information: Index, DropEvents RxOctets, RxPkts, Broadcast, Multicast, CRCAlignErrors, Undersize, Oversize, Fragments, Jabbers, Collisions and Utilization.



Index	DropEvents	RxOctets	RxPkts	Broadcast	Multicast	CRCAlignErrors	Undersize	Oversize	Fragments	Jabbers	Collisions	Utilization
79	0	189	2	0	0	0	0	0	0	0	0	0
80	0	1512	6	0	0	0	0	0	0	0	0	0
81	0	97	1	0	0	0	0	0	0	0	0	0
82	0	245	2	0	0	0	0	0	0	0	0	0
83	0	93	1	0	0	0	0	0	0	0	0	0
84	0	7475	26	2	0	0	0	0	0	0	0	0
85	0	484	5	1	0	0	0	0	0	0	0	0
86	0	0	0	0	0	0	0	0	0	0	0	0
87	0	245	2	0	0	0	0	0	0	0	0	0
88	0	1894	6	1	0	0	0	0	0	0	0	0

16.3 Alarm

This page sets an alarm entry.

Port The ethernet port to collect statistics of **Variable**.

Variable Select a variable from the drop-down list.

Sample Type Specify the sampling method for the selected variable and comparing the value against the thresholds.

Absolute Compares the values directly with the thresholds at the end of the sampling interval.

Delta Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

Rising Threshold Type the rising counter value that triggers the Rising Threshold alarm.

Rising Event Index Select the index of the corresponding event which will be triggered if the sampled value is larger than the Rising Threshold.

Falling Threshold Type the falling counter value that triggers the Falling Threshold alarm.

Falling Event Index Select the index of the corresponding event which will be triggered if the sampled value is lower than the Falling Threshold.

Startup Alarm Specify the type of the alarm.

Rising Alarm When the sampled value exceeds the Rising Threshold, an alarm event is triggered.

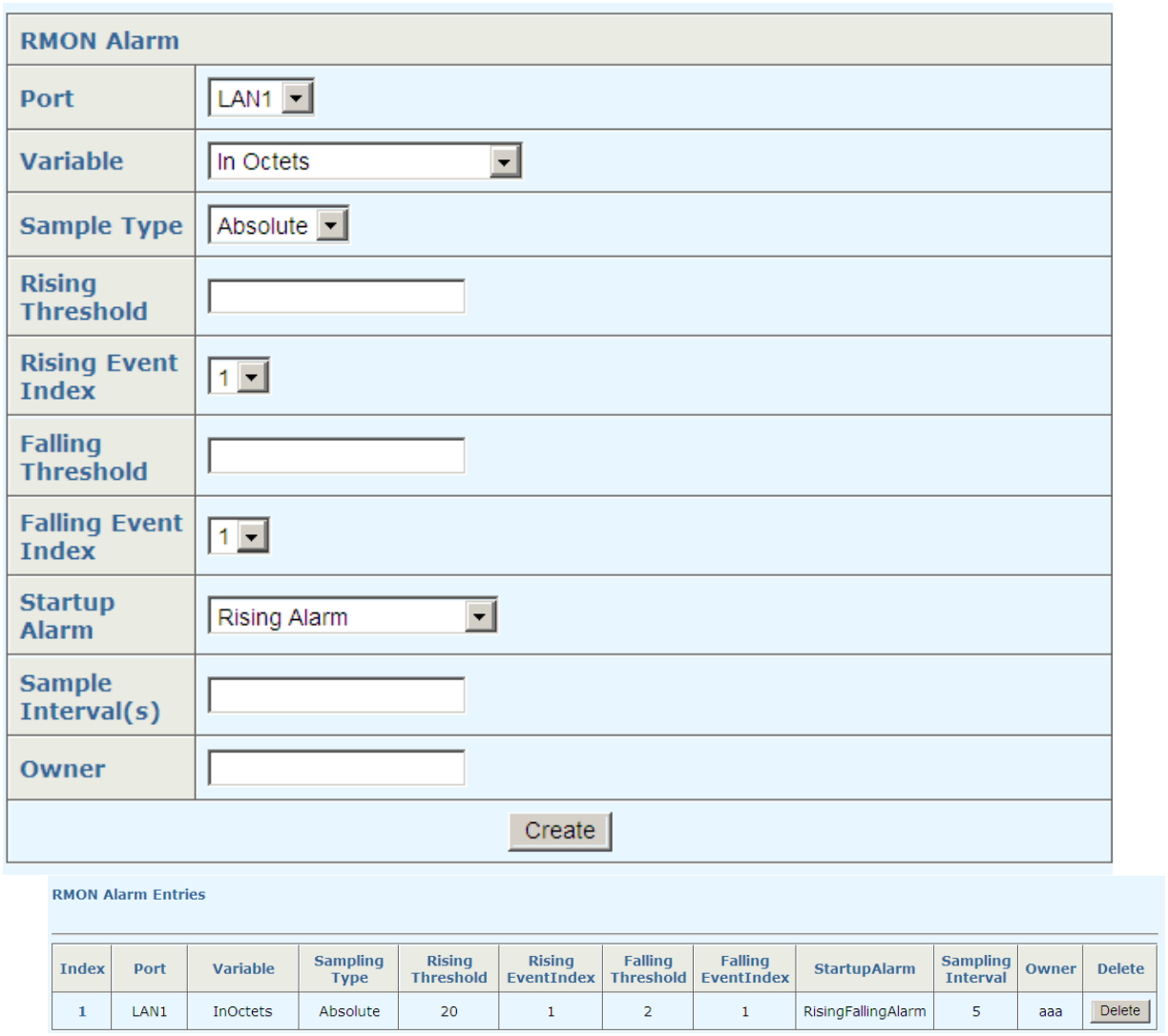
Falling Alarm When the sampled value is under the Falling Threshold, an alarm event is triggered.

Rising or Falling Alarm The alarm event will be triggered either the sampled value exceeds the Rising Threshold or is under the Falling Threshold.

Sample Interval Type the alarm interval time in seconds

Owner Type the user that defined the entry.

The bottom part of this page lists all existing alarm entries.



RMON Alarm Entries

Index	Port	Variable	Sampling Type	Rising Threshold	Rising EventIndex	Falling Threshold	Falling EventIndex	StartupAlarm	Sampling Interval	Owner	Delete
1	LAN1	InOctets	Absolute	20	1	2	1	RisingFallingAlarm	5	aaa	Delete

16.4 Event Configuration

16.4.1 Event

This page sets an event entry for an alarm.

Community If an SNMP trap is to be sent, it will be sent to the SNMP community specified by this octet string.

Description A comment to describe this event entry.

Type The type of notification that the probe makes about this event, in the case of log, an entry is made in the log table for each event; in the case of SNMP-trap, an SNMP trap is sent to one or more management.

Owner The entity that configured this entry and is therefore using the resources assigned to it.

The bottom part of this tab page lists all existing event entries.

RMON Event	
Community	
Description	
Type	None
Owner	
	Create

RMON Event Entries

Index	Community	Description	Type	Owner	Delete
1	abab	bbbb	Log & trap	aaaa	Delete
2	good	very good	Log & trap	Lucy	Delete

16.4.2 Event Log

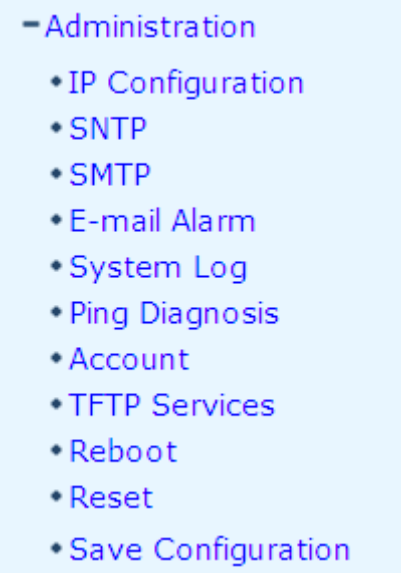
This page shows information about event log entries, including **Event Index**, **Log Index**, **Log Time** and **Description**.

Event Index	Log Index	Log Time	Description
1	1	Sep 13 10:20:52 2012	MIB Var:1.3.6.1.2.1.2.2.1.10.1.0,Absolute,Rising,Actual Val:19990359,Thresh.Set:20,Interval(sec):5

Forward Next

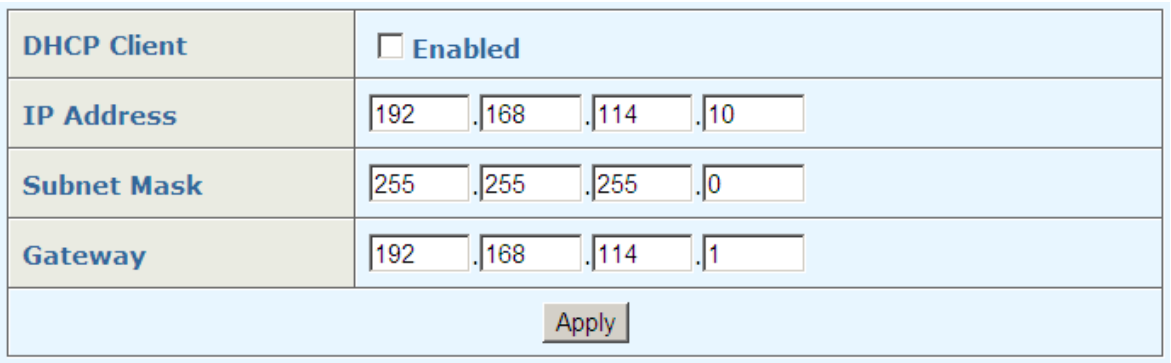
17 Administration

This part covers the following items:



17.1 IP Configuration

The device supports DHCP client and Static IP. **DHCP Client** can be enabled by checking the Enabled checkbox. If static IP is used, **IP Address**, **Subnet Mask**, and **Gateway** shall be specified.



17.2 SNTP

This page configures SNTP (Simple Network Time Protocol).

SNTP Mode Select Server mode or Client mode.

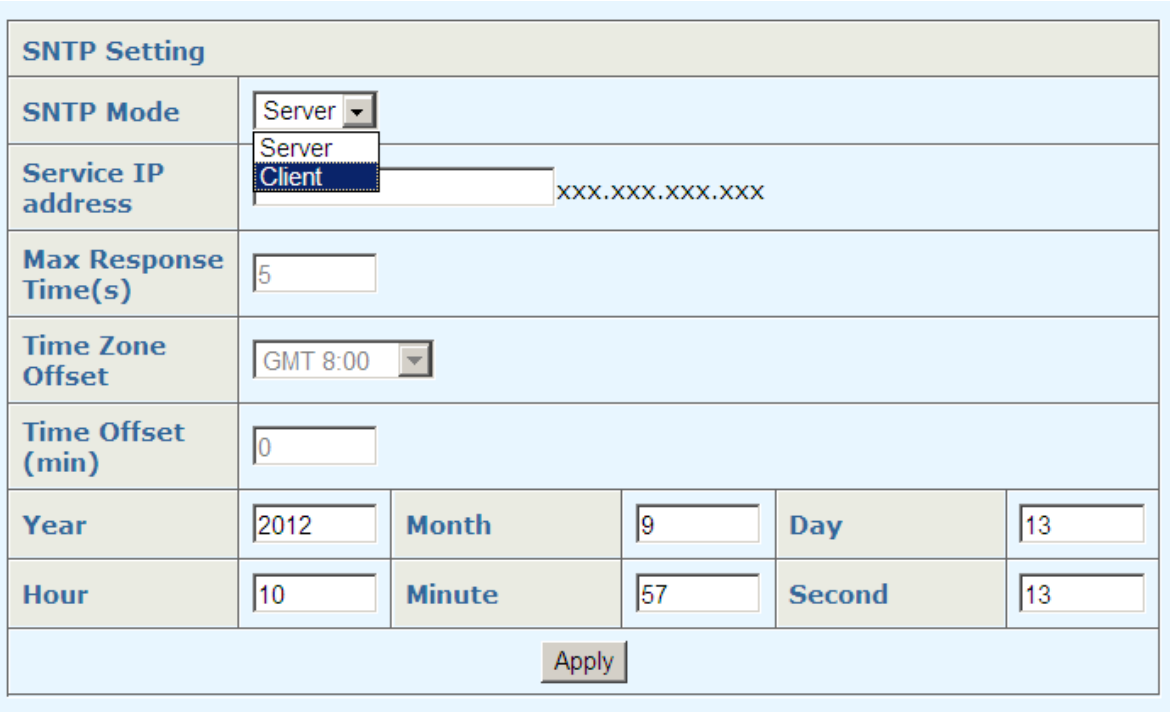
Service IP address If you select Client mode, you should set the device time through the SNTP server for time synchronization IP address of SNTP server.

Response Time Specify the time interval for the device to get a response from the SNTP server, in the unit of second.

Time Zone Offset Time difference between Greenwich standard time and your local time.

Time Offset (min) Time difference in minute between Greenwich standard time and your local time.

In Service Mode, system time can be set with year, month, day, hour, minute and second.

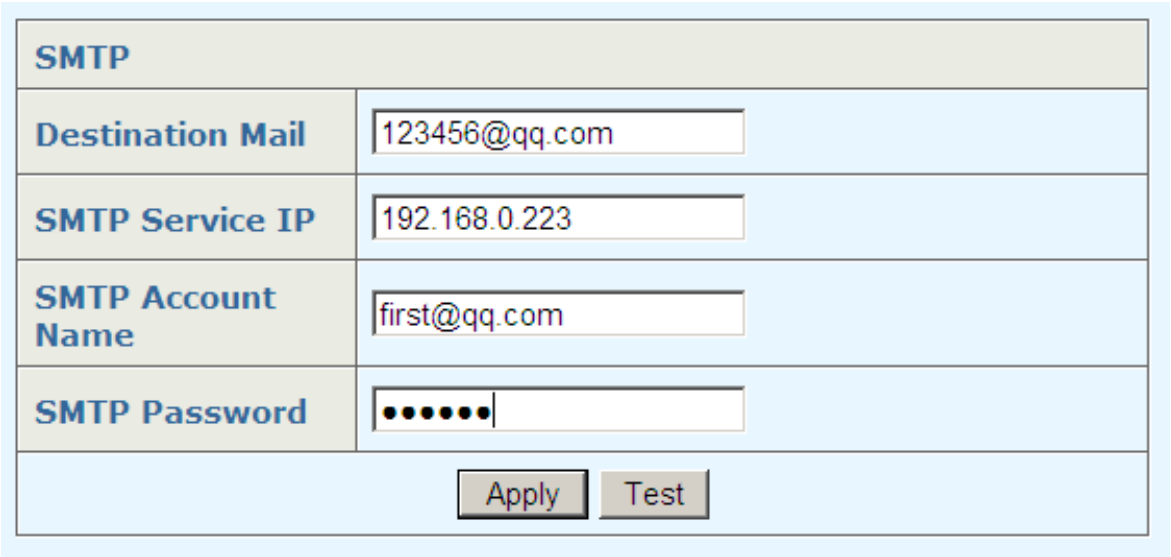


17.3 SMTP

This page sets SMTP (Simple Message Transfer Protocol) configuration. When a pre-defined event occurs, an e-mail will be sent to the following destination mail address.

Destination Mail: The e-mail address to receive the event information.
SMTP Service IP: The IP address of SMTP server.
Source Account Name: Source e-mail account on SMTP server.
SMTP Password: The password for source e-mail account.

📖 Note: click <Test> to check whether the configuration is correct. If it is correct, the destination mail will receive an e-mail.



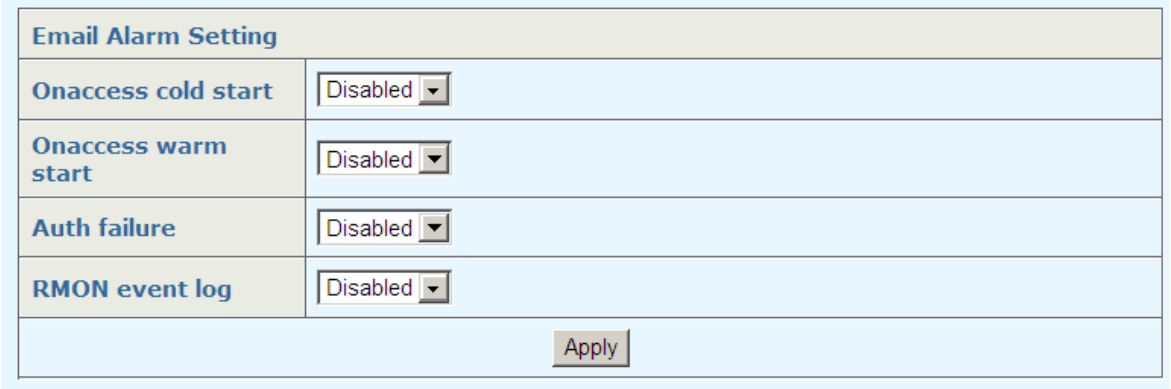
17.4 E-mail Alarm

This page sets the events that will trigger an e-mail described in Section 2.15.3 SMTP, including system events and port events.

17.4.1 System Event

This page sets the following system events. Select <Apply> for an event to trigger e-mail sending when this event occurs.

Onaccess cold start: The device is booted up by turning on the power.
Onaccess warm start: The device is restarted without turning off power.
Auth failure: Fails to login to the device due to incorrect username or password.
RMON event log: see chapter 12 of this manual for details.



17.4.2 Port Event

This page sets the following port events. Select **Enable** for an event to trigger e-mail sending when this event occurs.

Port The port selected for event configuration

Alarm Type If it is enabled, there are three alarm types for the event: **Link Up**, **Link Down**, and **Up & Down**.

Traffic Overload It means that the port traffic exceeds **Traffic Threshold** during a statistics time of **Traffic Duration**.

Traffic Threshold The threshold for port traffic (in percentage of the port speed).

Traffic Duration The statistics duration time for calculating port traffic.

📖 Note: **Traffic Overload**, **Traffic Threshold** and **Traffic Duration** are interrelated. When **Traffic Overload** is enabled, **Traffic Threshold** shall be set with a number between 1% and 99%, and **Traffic Duration** shall be no less than 10 seconds.

The lower part of this page lists all port events.

Port	Alarm Type	Traffic Overload	Traffic Threshold(%)	Traffic Duration(s)
LAN1	Link Up	Enabled	10	15
Apply				

Port Event Status

Port	Alarm Type	Traffic Overload	Traffic Threshold(%)	Traffic Duration(s)
LAN1	Link Up	Enabled	10	15
LAN2	Up & Down	Enabled	5	10
LAN3	Disabled	Disabled	0	0
LAN4	Disabled	Disabled	0	0
LAN5	Disabled	Disabled	0	0
LAN6	Disabled	Disabled	0	0
LAN7	Disabled	Disabled	0	0
LAN8	Disabled	Disabled	0	0
WAN	Disabled	Disabled	0	0

17.5 System Logs

This page shows all of the system logs, clicking <Clear> to clear all the records of the system logs. And you can turn to the next page to go back to the previous page by clicking <Next> and <Forward> respectively.

Log Information

34	2012/9/13 10:55:35 192.168.114.248 has logout the systerm via WEB UI!
35	2012/9/13 10:54:33 192.168.114.248 logins the systerm via WEB UI!
36	2012/9/13 10:53:56 192.168.114.248 has logout the systerm via WEB UI!
37	2012/9/13 10:53:10 192.168.114.248 logins the systerm via WEB UI!
38	2012/9/13 10:50:38 192.168.114.248 has logout the systerm via WEB UI!
39	2012/9/13 10:49:53 192.168.114.248 logins the systerm via WEB UI!
40	2012/9/13 10:45:41 192.168.114.248 has logout the systerm via WEB UI!
41	2012/9/13 10:44:35 192.168.114.248 logins the systerm via WEB UI!
42	2012/9/13 10:40:11 192.168.114.248 has logout the systerm via WEB UI!
43	2012/9/13 10:38:32 192.168.114.248 logins the systerm via WEB UI!
44	2012/9/13 10:33:35 192.168.114.248 has logout the systerm via WEB UI!
45	2012/9/13 10:32:29 192.168.114.248 logins the systerm via WEB UI!
46	2012/9/13 10:26:59 192.168.114.248 has logout the systerm via WEB UI!
47	2012/9/13 10:25:48 192.168.114.248 logins the systerm via WEB UI!
48	2012/9/13 10:23:41 192.168.114.248 has logout the systerm via WEB UI!
49	2012/9/13 10:19:11 192.168.114.248 logins the systerm via WEB UI!
50	2012/9/13 10:18:44 192.168.114.248 has logout the systerm via WEB UI!

Forward Reset Next

17.6 Ping Diagnosis

On this page, you can ping an IP address to check the network connectivity and the reachability of a host.

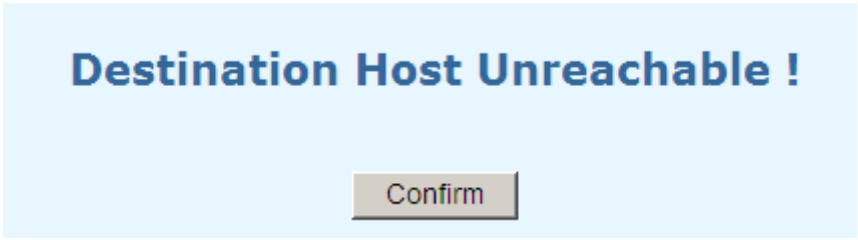
Ping Diagnosis

Ping	192.168.114.248

Apply

If the device is reachable, it will remind you as follows:

If the device is unreachable, it will remind you as follows:



17.7 Account

This page can be used to add a new account. **Username**, **Password**, and **Privilege** for the new account are set on this page.

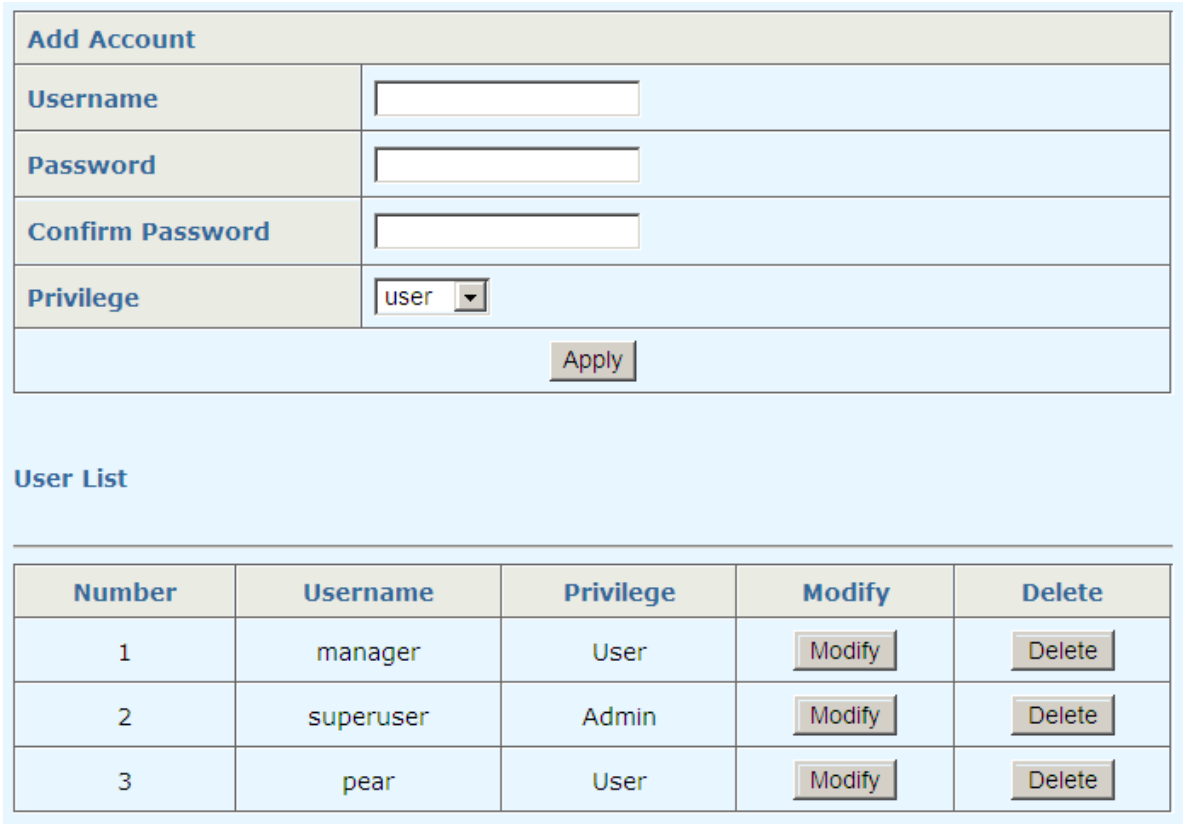
Username Type a username; it is a string of 3 to 16 characters.

Password Type the password; it is a string of 1 to 16 characters.

Privilege It can be set as **user** or **admin**. User cannot add or delete an account, can neither use the TFTP service nor reset function, while admin can check and modify the device configuration.

The bottom part of this page lists all accounts, including **Username** and **Privilege**. An account can be deleted on this page.

Caution: Accounts can be deleted, but at least one admin should be kept.

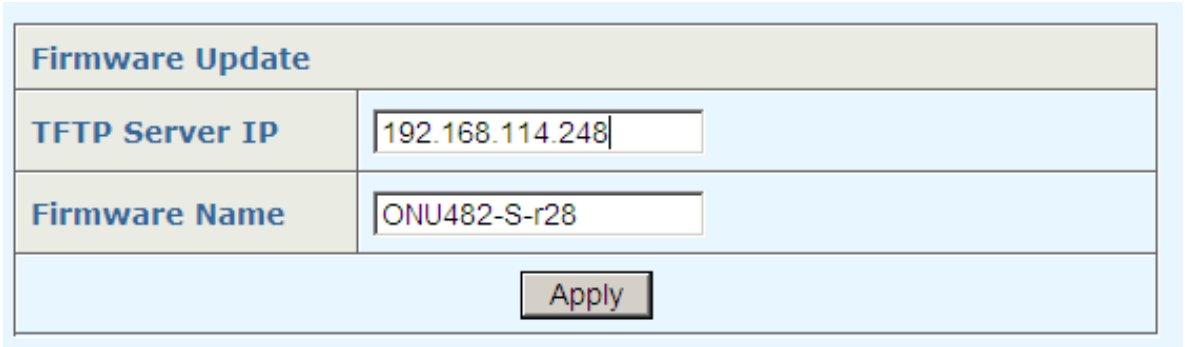


17.8 TFTP Services

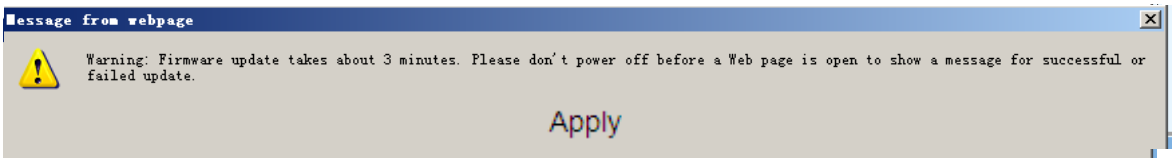
17.8.1 TFTP Firmware

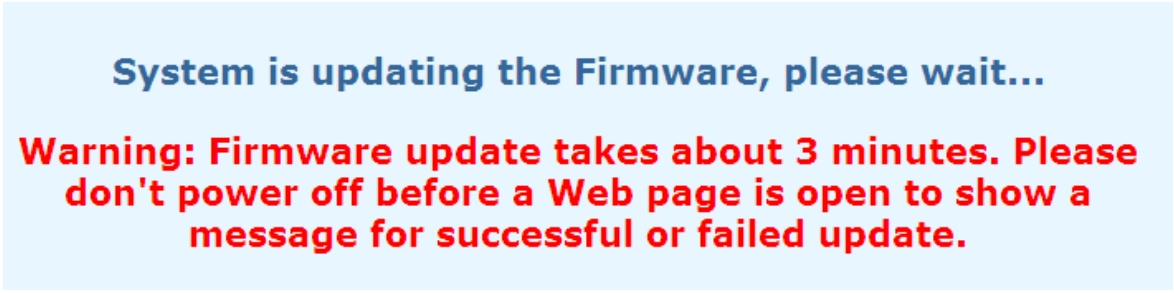
To upgrade the system is to get more functions and better performance. Before upgrading firmware, make sure the device is connected to the TFTP server and the TFTP software is turned on, and new firmware file exists on the server. You can get the newest firmware from Ascent Communication Technology, please contact your sales representative.

The device will begin to update firmware after clicking on <Apply>.

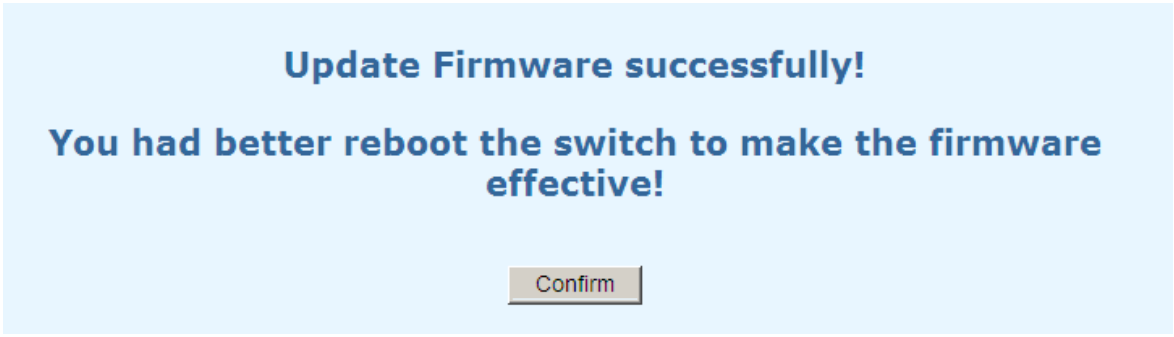


Please pay attention to the following reminds:

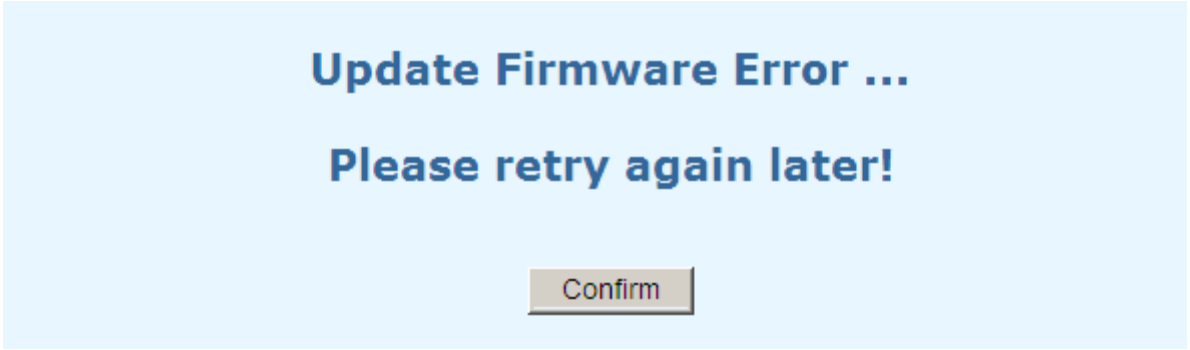




If the upgrade is successful, it will remind you as follows.



If the upgrade fails, it will remind you as follows. Maybe it is because the TFTP software is turned off.



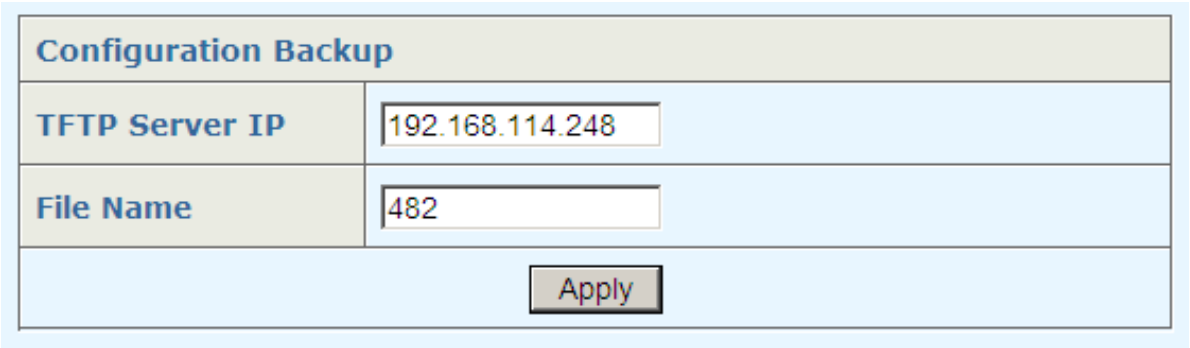
After upgrade, you should reboot the system manually to make upgrade effective.

Caution: please don't cut off the power supply during updating firmware, uploading or downloading a configuration file!

17.8.2 Backup Configuration

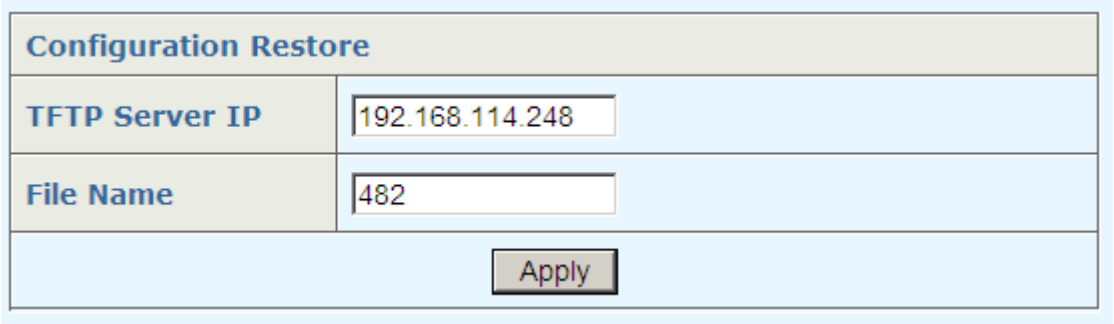
This page sets a **TFTP Server IP** and **File Name**. Before backing up configuration, make sure the device is connected to the TFTP server. The device configuration file will be uploaded to TFTP

server with the specified **File Name** after clicking on <Apply>.



17.8.3 Restore Configuration

This page sets a **TFTP Server IP** and **File Name**. Before restoring a configuration, make sure the device is connected to the TFTP server. The device will download the file with the specified **File Name** and use it as the configuration file after clicking on <Apply>.

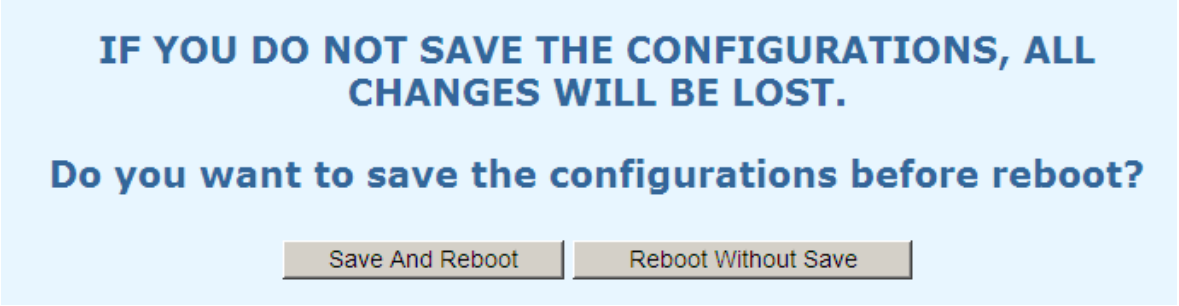


17.9 Reboot

On this page, there are two buttons: <Save And Reboot> and <Reboot Without Save>.

Save And Reboot Saves the current configuration and then reboot

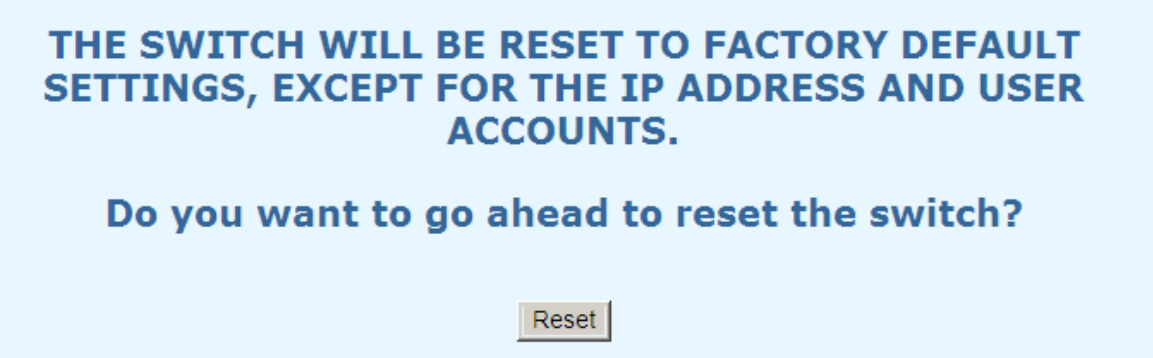
Reboot Without Save Directly reboots without saving the current configuration. All changes may be lost.



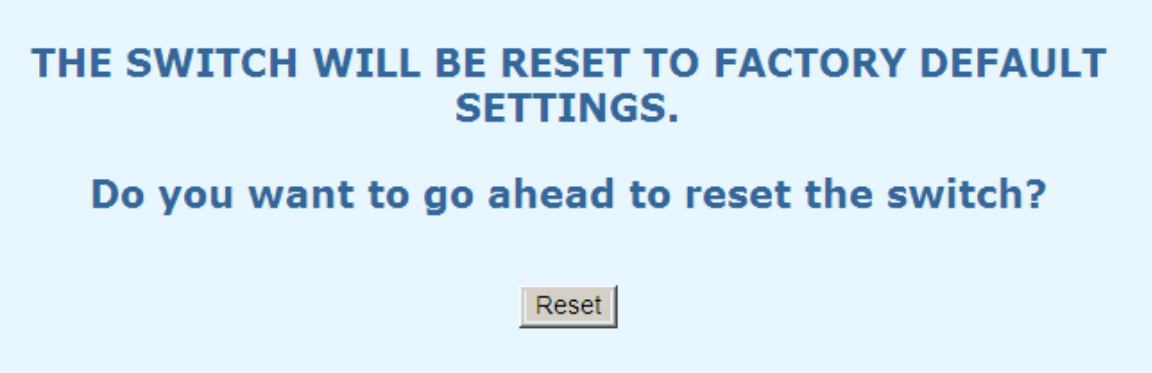
17.10 Reset

There are two tab pages: *Reset* and *Reset To Default*.

Reset: the device will be reset to the factory default setting, except that the IP address and user accounts are kept unchanged.

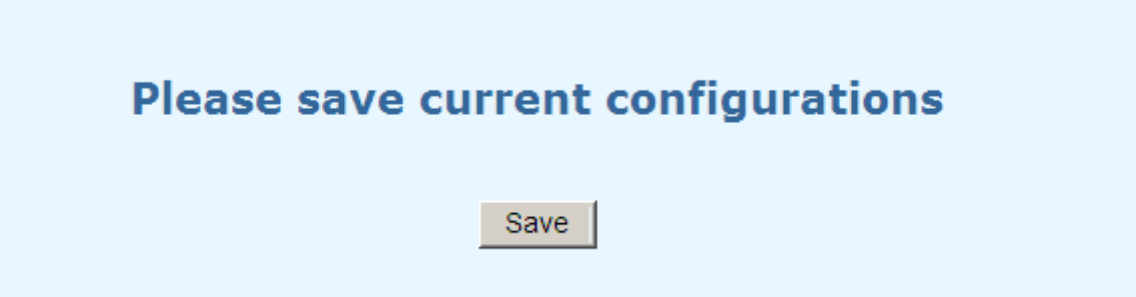


Reset To Default: the device will be reset to the factory default setting.



17.11 Save Configuration

This page saves current configurations.



18 Logout

Click [Logout] in the left menu to log out from the Web interface.

Ascent Communication Technology Ltd.

AUSTRALIA

487 Church St, Richmond, Victoria 3121, Australia

Phone: +61-488 293 682

Email: sales@ascentcomtec.com

CHINA/HONG KONG

13/F., Shum Tower, 268 Des Voeux Road Central, Hong Kong

Phone China: +86-139 0173 4382

Phone Hong Kong: +852-5483 7156

Email: sales@ascentcomtec.com

USA

11B Goodwin St, Stamford CT 06906 USA

Phone: +1-203-816 5188

Email: sales@ascentcomtec.com

Specifications and product availability are subject to change without notice.