barox

PD-VDSL-2402

User Manual

Version 1.1

TABLES OF CONTENTS

TABLES OF CONTENTS 3

CHAPTER 1 INTRODUCTION 8

1.1 FEATURES 9

1.2 SPECIFICATION 13

CHAPTER 2 HARDWARE INSTALLATION 14

2.1 FRONT PANEL 14

2.1.1 Connectors *14*

2.1.2 LED Indicators *15*

2.1.3 Reset Button *16*

2.2 PIN ASSIGNMENT OF RJ21 CABLE 16

CHAPTER 3 WEB CONFIGURATION 17

3.1 ADMINISTRATION 21

3.1.1 IP Address *22*

3.1.2 Switch Setting *23*

3.1.3 Console Port Information *26*

3.1.4 Port Configuration *27*

3.1.5 SNMP Configuration *33*

3.1.6 Syslog Setting *41*

3.1.7 Alarm Configuration *41*

3.1.8 Temperatures & Fan Status *42*

3.1.9 Firmware Update *43*

3.1.10 Configuration Backup *43*

3.1.11 SNTP Setting *44*

3.2 L2 FEATURES 46

3.2.1 VLAN Configuration *47*

3.2.1.1 Static VLAN 48

3.2.1.2 GVRP VLAN 52

3.2.1.3 QinQ VLAN 54

3.2.2 Trunking *57*

3.2.3 Forwarding & Filtering *60*

3.2.4 IGMP Snooping *63*

3.2.5 Spanning Tree *64*

3.2.5.1 System Configuration 66

3.2.5.2 PerPort Configuration 68

3.2.5.3 Instance 68

3.2.5.4 Interface 69

3.2.6 DHCP Relay & Opt.82 ..... *70*

3.2.6.1 DHCP Option 82 71

3.2.6.2 DHCP Relay 71

3.2.6.3 DHCP Option 82 Router Port 71

3.2.6.4 DHCP Opt. 82 Port Table 72

3.3 ACL 73

3.3.1 IPv4 ..... *74*

3.3.2 Non-IPv4 ..... *76*

3.3.3 Binding *76*

3.4 SECURITY 78

3.4.1 Security Manager *79*

3.4.2 MAC Limit *80*

3.4.3 802.1x Configuration *81*

3.5 QOS 84

3.5.1 QoS Configuration *84*

3.5.2 ToS/DSCP *86*

3.6 MONITORING 88

3.6.1 Port Status *88*

3.6.2 Port Statistics *89*

3.7 VDSL 90

3.7.1 Configuration *90*

3.7.2 Profile Table *93*

3.8 RESET SYSTEM 94

3.9 REBOOT 94

CHAPTER 4 CONFIGURATION VIA CONSOLE 95

CHAPTER 5 COMMAND LINE INTERFACE 96

5.1 OPERATION NOTICE 96

5.1.1 Command Line Editing *98*

5.1.2 Command Help *99*

5.2 SYSTEM COMMANDS 99

5.3 SWITCH STATIC CONFIGURATION 101

5.4 TRUNK CONFIGURATION 104

5.4.1 Trunking Commands *104*

5.4.2 LACP Commands *105*

5.5 VLAN CONFIGURATION 106

5.5.1 Virtual LANs *106*

5.6 GVRP COMMANDS 111

5.7 QINQ COMMANDS 113

5.8 MISC CONFIGURATION 114

5.9 ADMINISTRATION CONFIGURATION 116

5.10 PORT MIRRORING CONFIGURATION 117

5.11 QUALITY OF SERVICE 118

5.12 MAC ADDRESS CONFIGURATION 120

5.12.1 Commands for MAC *120*

5.12.2 MAC Limits *121*

5.13 PROTOCOL RELATED COMMENDS 122

5.13.1 STP/RSTP *122*

5.13.2 MSTP *126*

5.14 SNMP 132

5.15 IGMP 138

5.16 802.1X PROTOCOL 139

5.17 DHCP RELAY & OPTION 82 142

5.18 SYSLOG 143

5.19 REBOOT SWITCH 143

5.20 TFTP FUNCTION 143

5.21 ACCESS CONTROL LIST 144

5.22 BINDING 149

5.22.1 SIP/SMAC binding commands *149*

5.23 VDSL2 COMMANDS 150

5.23.1 VDSL2 interface commands *150*

APPENDIX **157**

CHAPTER 1 INTRODUCTION

Barox PD-DSLAM-724 presents the ideal and efficient solution for Telecom, ISP (Internet Service Provider), or SI (System Integration) with 24-port VDSL2 and 2-port gigabit Ethernet combo interfaces (TP and SFP) in the 1.5U height design. The PD-DSLAM-724 offers the benefits of high speed connectivity with an efficient management system, robust layer 2 features with advanced security system, and reliable hardware design with monitoring system.

Package Contents:

- PD-DSLAM-724 x1
- User Manual CD x1
- Power Cord x1
- Rubber Feet x4
- Console Cable (DB9-RJ45) x1
- 19” Rack Mount Brackets and Screws x1

1.1 FEATURES

- 24 10/100BaseX Ethernet ports and 2 10/100/1000BaseX Ethernet ports Ethernet switch controller
- Supports SMII or SS-SMII for 10/100BaseX ports
- Supports GMII/MII/TBI for 10/100/1000BaseX ports
- All packet buffer and control data memory embedded
- Flow control support:
  - 802.3x pause frame used for full-duplex ports
  - Collision-based back-pressure for half-duplex ports, carrier-based back-pressure not supported
- Half- and full-duplex operations:
  - Full-duplex operation supported on 10/100/1000 Mbps ports
  - Half-duplex operation supported on 10/100 Mbps ports only
- Supports 802.1D bridge self-learning, storing up to 8K+ 256 unicast or multicast addresses
- Supports automatic age-out period between 1 to 1,000,000 seconds
- Broadcast storm filtering based on ingress port bandwidth
- HOL blocking prevention
- Deadlock relief
- Auto-polling via MDC/MDIO management interface for auto-configuration of speed, duplex mode, and flow control capability of all Ethernet ports
- 9K+ jumbo packets supported on per port and per VLAN basis
- Supports layer 2 source filtering
- Supports 802.1D Spanning Tree Algorithm and Protocol, and 802.1w Rapid Reconfiguration
- Flexible per-port VLAN classification option supports port-based VLAN domain and 802.1Q VLAN domain simultaneously
- Supports Independent VLAN Learning (IVL) and Shared VLAN Learning (SVL)

- Supports 802.1X Port-based Network Access Control
- Supports 802.3ad Aggregation of Multiple Link Segments
  - Statistical load-balancing algorithm may be configured to be function of source and destination MAC addresses, ingress port ID, source and destination IP addresses, and TCP/UDP source and destination ports
- Supports BPDU, LACP, EAPOL suppression based on per port configuration
- Supports 64 VLAN-dependent Spanning Trees
- Supports IP multicast and snooping of IGMP and IP multicast routing protocol PDU
  - Including IGMP, CBT, OSPF, and PIM v2
- IP multicast packets may be forwarded within single VLAN or across multiple VLANs
  - Cross-VLAN mode allows each egress port to have its own tag rule and VID for IP multicast packets
- Port mirroring
- Supports 802.1p Traffic Priority
- ToS-to-802.1p priority mapping is enabled on per-VLAN basis
- Flexible per-port prioritization option:
  - The prioritization result can be made available to other switches in the network by replacing priority field in VLAN tag
- Four priority egress queues per port
- Scheduling algorithms: strict priority or weighted round robin
- Four RMON groups (1,2,3,9)
- Supports MIB of RFC1213, 1573, 1757, 1643, 2233
- Programmable LED output provides:
  - Serial LED output provides basic status of all Ethernet ports, or
  - Port 24/25 link status and broadcast storm indicator
- MAC address table synchronization assistance
- Asymmetric VLAN membership for better network security:
  - Distinguish ingress VLAN member and egress VLAN member

- Prevents a station to sneak in VLANs set up for common servers

- Improved VLAN ingress rules may specify:
  - Filtering untagged packets or VLAN tagged packets
  - Filtering packets received on non-ingress VLAN member ports
- Supports insertion of 2nd tag with different TPID to VLAN-tagged packets
- Port-based ingress rate policing and egress rate pacing
- Supports Layer 2/3/4 (Layer 2+) classification:
  - Standard-length IPv4 packets can use layer 2 VLAN-tag ID, IP protocol, Source IP, Destination IP, TCP/UDP Destination Port and Source Port, and TCP SYN field for classification
  - Non-standard or non-IPv4 packets use part of layer 2/3 header for classification
  - Up to 256 different classification rules supported
  - Each classification rule is associated with an action code
  - Packet and byte counters for all classification rules to record match statistics
- Supports Layer 2+ based VLAN classification scheme:
  - IP subnet based and Protocol-based VLAN achievable by means of layer 2+ classification
  - May override VID in VLAN-tag
- Supports filtering, redirecting, and/or mirroring of packets based on Layer 2+ classification result
  - Redirects IPv6 packets to IPv6-capable network devices
- SMAC/SIP bindings for IPv4 packets can be implemented
- Layer 2+ packet classification result may be used to define packet priority
- Priority adjustment based on per port profile and per VLAN property
  - Priority of a packet can be upgraded or downgraded based on setting of the ingress port and VLAN
- Supports protected port, protected port group, and unprotected port group
- VID in transmitted packets can be replaced by a fixed VID associated with the egress port
  - The VID to be swapped in by egress port can be different than the default VID for untagged ingress packets
- CPU interface: alternatively

- 32-bit 33 MHz PCI interface
- 16-bit PIO interface with three DMA controllers

- Programmable byte-swap capability for MIB counter memory access
- Programmable event triggered interrupts allowing software to respond to or ignore an array of exceptions
- 332-ball PBGA package
- 1.8V core and SRAM voltage, and 3.3V pad voltage

1.2 SPECIFICATION

Hardware

Case:

- 1.5U High Pizza-Box Type

Interfaces:

- 24 VDSL2 Ports
- Two RJ-45 100/1000Mbps Ethernet Combo Ports
- Management Ethernet
- 1 x RS-232 Serial Console
- POTS Splitter

LED Indicators:

- SYS, ALM, LINK, ACT
- 24 x VDSL LEDs

Standards Support:

- VDSL2 ITU-T G.993.2
- VDSL2 Profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a and 30a
- 802.1d L2 Bridging
- DHCP Server/Client/Relay
- IEEE 802.1q VLAN (Port-based VLAN and Protocol-Based VLAN)
- VLAN Stacking (Q-in-Q)
- IEEE 802.1p Spanning Tree Protocol (STP)
- IEEE 802.3ad Link Aggregation

Protocol Support:

- IGMP Snooping/Proxy v1, v2 and v3
- Multicast Forwarding with IGMP Snooping v1 and v2 (RFC 1112 and RFC 2236)
- Multicast MAC address mapping
- Up to 512 Multicast Channels
- Profile-based Multicast Access Control (up to 24 profiles)
- Fast and Normal Leave Modes

Security:

- L2 Frame Filtering by MAC Addresses
- L3 Frame Filtering by IP Addresses, protocol ID, and TCP/UDP
- DHCP and ARP Broadcasting Frames Filtering
- Support Secured Forwarding

Management:

- Support OAM&P Functions
- Support VLAN Priority Queue (IEEE 802.1p)
- Support CoS, ToS, DSCP, etc.
- Support SNMP v1/v2/v3 and MIB I/II
- Web-based Graphical User Interface, Telnet, CLI

Operating Requirements:

- Operating Temperature: -10°C to 50°C
- Storage Temperature: -40°C to 70°C
- Relative Humidity: Up to 95% (non-condensing)

* Barox reserves the right to change specifications without prior notice. All brand names and trademarks are property of their respective owners. All rights reserved.

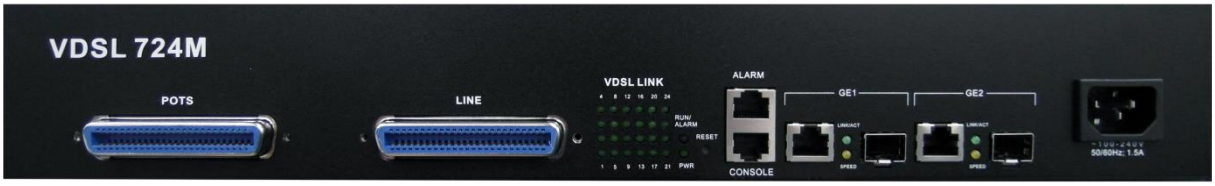
CHAPTER 2 HARDWARE INSTALLATION

This chapter shows the front panel and how to install the hardware.

2.1 FRONT PANEL

724M includes all connectors and LED indicators on its front panel so only a few installations are required in order to build the network solution.

2.1.1 CONNECTORS



- POTS

  PD-DSLAM-724 includes 24 build-in splitters, POTS, with a Telco-50/ RJ-21 cable for telephone services.

- LINE

  LINE is for connecting 24 VDSL2 ports with a Telco-50/ RJ-21 cable.

- ALARM

  For alarm inputs and outputs.

- CONSOLE

  Users are able to access 724M locally with CONSOLE port. Via CONSOLE, users are able to configure 724M with menu-driven interface with any terinal emulation program, such as, Hyperterminal and Teraterm. (115200, 8, None, 1, None)

- GE1 & GE2

  For connecting Gigabit Ethernet, 724M provides Gigabit Ethernet combo interfaces, TP and SPF.

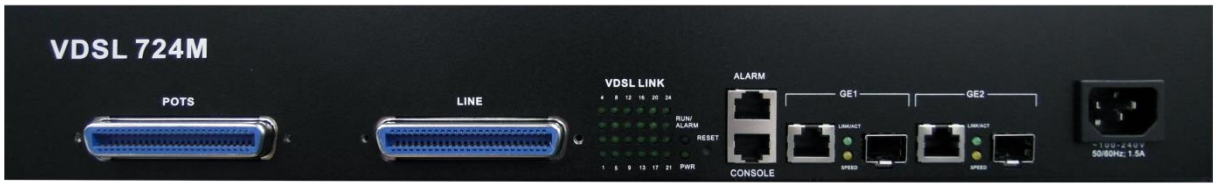
  TP: 10/100/1000 BaseT copper (RJ-45 connector).

  SFP: 1000 Base-SX/LX mini-GBIC slot.

- POWER

  The connector is for 100V ~ 240V AC power inputs (50Hz~60Hz, 1.5A).

2.1.2 LED INDICATORS



	Blinking	On	Off
VDSL LINK (1 ~ 24)	VDSL2 link is active (transmitting data or training)	VDSL2 link is ready	VDSL2 link is down
RUN/ALARM	System up	Alarm is detected	No alarm
PWR		Power On	Power Off
GE1/GE2 LINK/ACT			
SPEED			

2.1.3 RESET BUTTON

The reset buttons allows users to reboot the VDSL2 IP DSLAM or load the default settings.

Press the reset button for	Action
1 ~ 5 seconds	Reboot the IP DSLAM
	Load the default settings

2.2 PIN ASSIGNMENT OF RJ21 CABLE

PIN	COLOR	PORT	PIN	COLOR	PORT	PIN	COLOR	PORT
1	Black	P24	9	White	P16	17	White	P8
26	Orange		34	Brown		42	Gray	
2	Black	P23	10	White	P15	18	Red	P7
27	Blue		35	Green		43	Blue	
3	Red	P22	11	White	P14	19	Red	P6
28	Gray		36	Orange		44	Orange	
4	Red	P21	12	White	P13	20	Red	P5
29	Brown		37	Blue		45	Green	
5	Red	P20	13	White	P12	21	Red	P4
30	Green		38	Blue		46	Brown	
6	Red	P19	14	White	P11	22	Red	P3
31	Orange		39	Orange		47	Gray	
7	Red	P18	15	White	P10	23	Black	P2
62	Blue		40	Green		48	Blue	
8	White	P17	16	White	P9	24	Black	P1
33	Gray		41	Brown		49	Orange	

CHAPTER 3 WEB CONFIGURATION

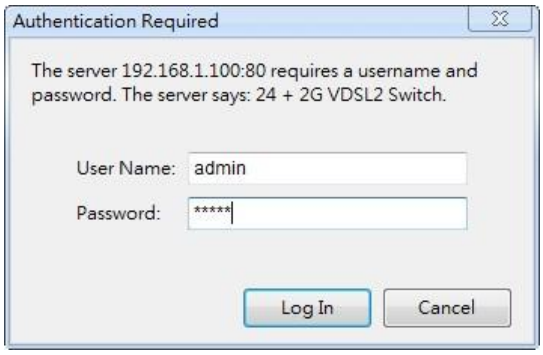
The VDSL2 IP DSLAM allows users to manage and change its configurations with web browsers. Users are able to login the web management system with any standard web browser, such as, Internet Explorer, Firefox, etc.

Default IP Address	192.168.0.100
Default User Name	admin
Default Password	admin

TABLE 1 DEFAULT LOGIN INFORMATION

Please make sure the IP address is correct once the IP of the management web site is changed.

Once users are able to login the web management page successfully, the login message box will pop up as the following image.



Please key in the correct login information and the main page of the management will be showed as the following image.

HOME page of the management system includes three major sections.

1. Title section

This section indicates the model name of the device.

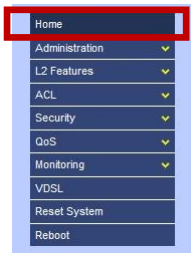
2. Menu section

"Menu" section is located on the left hand side of the page and users are allowed to change the configuration and review the status of the device by interacting this section.

3. Information section

"Information" section presents the real-time LED status and the current status of the IP DSLAM.

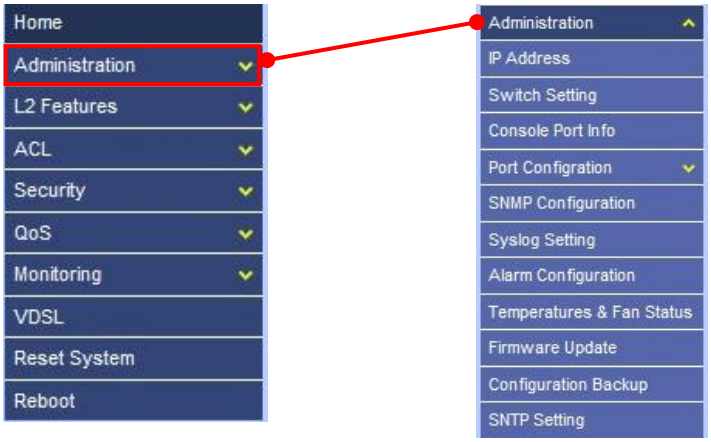
Users are able to go back HOME page anytime by clicking on "Home" on the menu section.



The following sections will introduce users the features of the VDSL2 IP DSLAM.

- Administration (3.1)
- L2 Features (3.2)
- ACL (3.3)
- Security (3.4)
- QoS (3.5)
- Monitoring (3.6)
- VDSL (3.7)
- Reset System 3.8)
- Reboot (3.9)

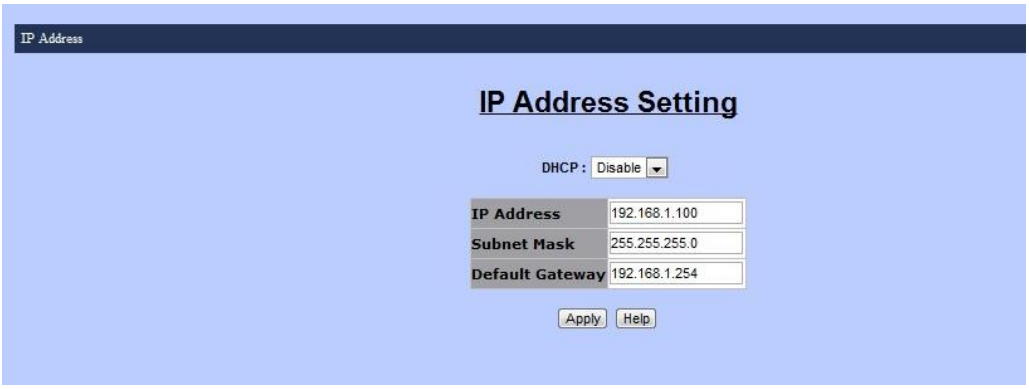
3.1 ADMINISTRATION



"Administration" section is for users to manage the VDSL2 IP DSLAM, including the IP address, switch settings, etc. It includes the following detail functions.

- IP Address
- Switch Setting
- Console Port Info
- Port Configuration
- SNMP Configuration
- Syslog Setting
- Alarm Configuration
- Temperatures & Fan Status
- Firmware Update
- Configuration Backup
- SNTP Setting

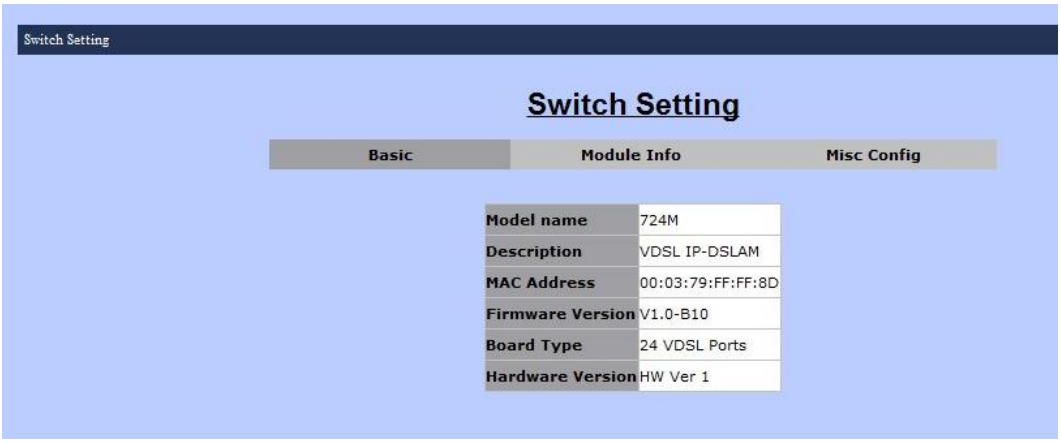
3.1.1 IP ADDRESS



"IP Address" function includes four information and users are allowed to change these information:

- DHCP mode
  - Disable or enable DHCP mode
  - The value of this mode will decide whether the IP address is a static IP address or a dynamic IP address.
- IP address
- Subnet mask
- Default gateway

3.1.2 SWITCH SETTING



"Switch Setting" presents information of the switch in the following sub-functions.

Only "Misc Config" section allows users to change the settings of the switch.

- Basic

In "Basic" tab, the basic information of the VDSL2 IP DSLAM is presented.

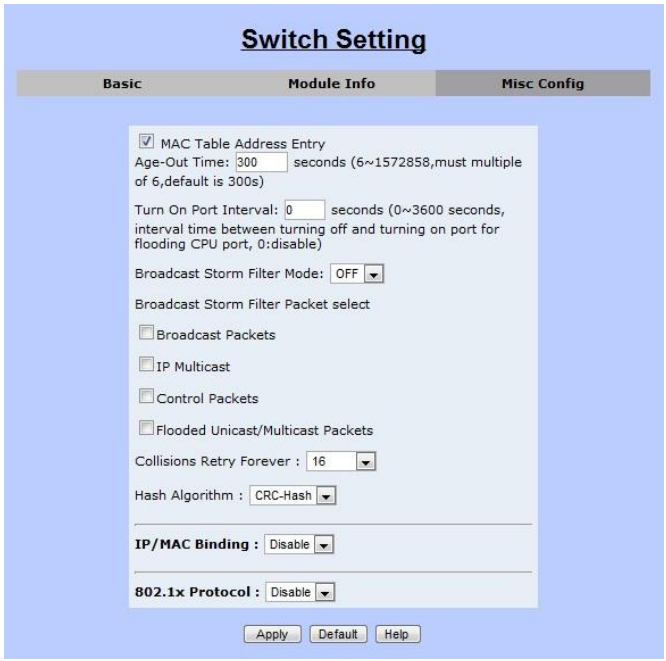
- Model name
- Description
- MAC address
- Firmware version
- Board type
- Hardware version

- Module Info

This section shows the information of uplinks, Gigabit Ethernet 1 and Gigabit Ethernet 2.

In the following contents, these two uplinks will be called Mod1 and Mod2.

- Misc Config



Users are allowed to modify the following details of the switch.

- MAC address age-out time
  - This value is for setting up how many seconds that an inactive MAC address remains.
- Turn on port interval

- This value for setting up the time interval that the CPU port should be enabled after flooding attacks.

0 means never enable the CPU port.

- Broadcast storm filter mode

  - This feature is to set up the threshold value of broadcast traffic for ports.
  - Options: off, 1/2, 1/4, 1/8 or 1/16

The value is the percentage of the port's ingress bandwidth used by broadcast traffic.

- Broadcast storm filter packets select

  - This option allows users to choose the type of the target packet for broadcast storm filter mode.
  - If there is no type is chosen, this means broadcast storm filter mode is off.
  - Options: broadcast packets, IP multicast, control packets, and flooded unicast/multicast packets.

- Collisions retry forever

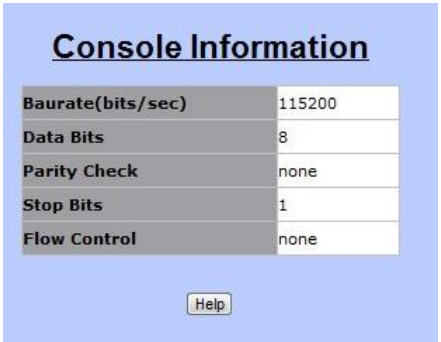
  - This function will allow users to choose how many times the IP DSLAM should retry when a packet meets a collision.
  - Disable, 16, 32 or 48 collision number

When the function is disabled, this means the IP DSLAM will retry for 6 times before packets are dropped. Otherwise, it will retry continuously until the packet is sent successfully.

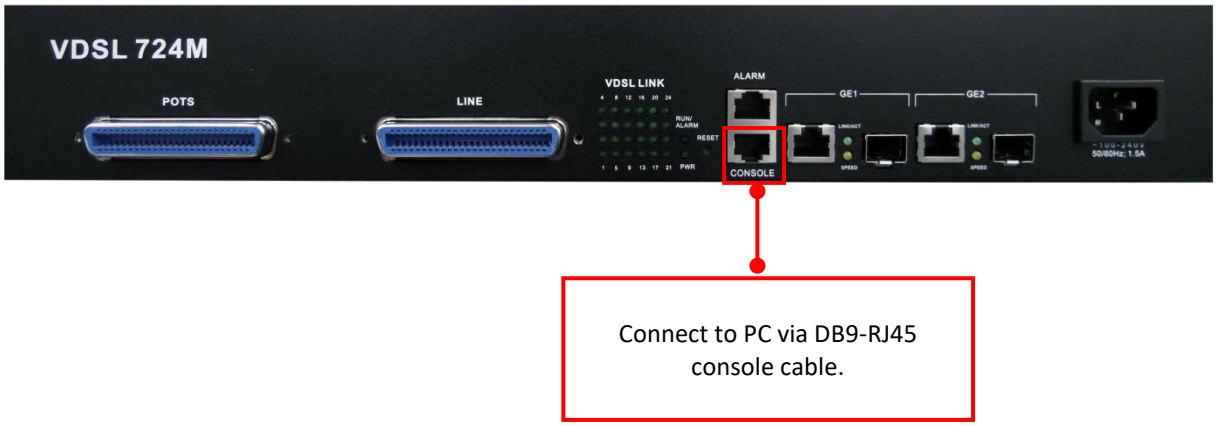
- Hash algorithm
  - This option is for choosing a hash algorithm for MAC address table.
  - CRC-Hash or DirectMap.
- IP/MAC binding
  - This feature allows user to enable or disable IP/MAC binding function.
  - Enable or disable.
- 802.1x protocol
  - 802.1x protocol is able to enable or disable via this option.
  - Enable or Disable.

Users are able to save the modified settings by clicking on "Apply" button. "Default" button is for restore the default settings; and "Help" button will provide some information about the features with another window.

3.1.3 CONSOLE PORT INFORMATION



The section is for users to review the settings of console port, which lets users to connect and manage the VDSL2 IP DSLAM in Command Line Interface (CLI) mode.



3.1.4 PORT CONFIGURATION

"Port Configuration" section includes four detail functions of VDSL2 ports and Gigabit Ethernet ports:

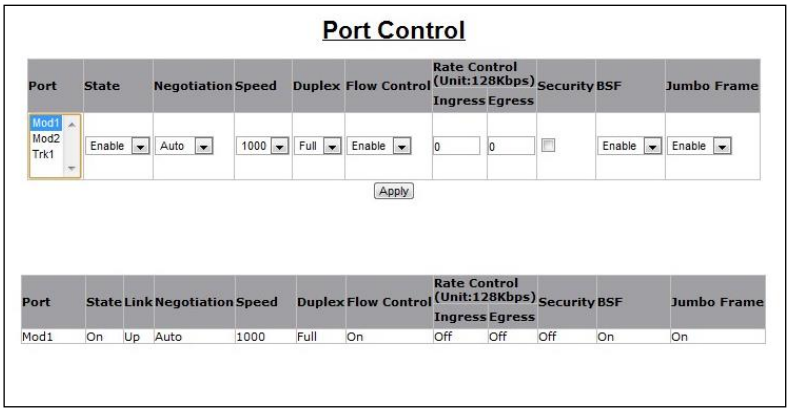
i. Port Controls

ii. Port Sniffer

iii. Protected Port

iv. VDSL Port Status

- **Port Controls**



"Port Control" is for users to setting up the details of Gigabit Ethernet ports and trunking ports if there exists any trunking ports. Users are allowed to configure the following parameters.

- State
  - This option will enable or disable the selected port.
  - Enable or Disable

"Disable" means to turn off the selected port; and this means there will be no traffic going through this port.

- Negotiation
  - Users are able to decide whether Gigabit Ethernet ports should be auto-negotiable or not.
  - Options: auto or force

If "force" mode is selected, users have to provide the information of "Speed" and "Duplex".

- Speed
  - Users can setup the speed of Gigabit Ethernet ports in this function.
  - 10, 100 or 1000
- Duplex
  - Half or Full
- Flow Control
  - Options: enable or disable
  - Enable: send a PAUSE signal to the sender and halts the traffic for a period of time.
  - Disable: drop the exceed packets when there are too much packets to process.
- Rate Control
  - Users are able to set up the specific rate for both ingress and egress ports. Therefore, the VDSL2 IP DSLAM will control the rate to meet the specified rate.

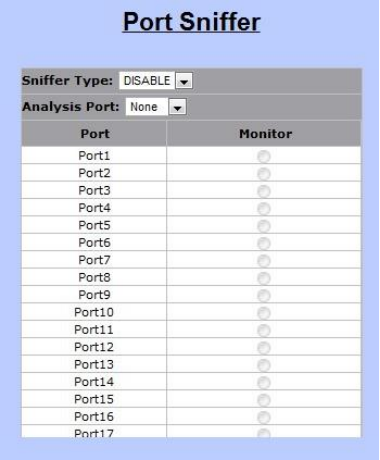
The valid rate range is 0 ~ 8000; and the unit is 128Kbps.

- Security
  - This function is to decide whether the IP DSLAM will forward all incoming packets from both secured MAC addresses and unknown MAC addresses.
  - Options: enable or disable
  - Enable: only packets from secured MAC addresses will be forwarded.
  - Disable: all packets will be forwarded.
- BSF

- BSF stands for "Broadcast Storm Filtering". It is able to enable or disable this function by port.
- Options: enable or disable

- Jumbo Frame
  - Users are able to choose whether the IP DSLAM forwards jumbo frame packets or not.
  - Options: enable or disable

- **Port Sniffer**

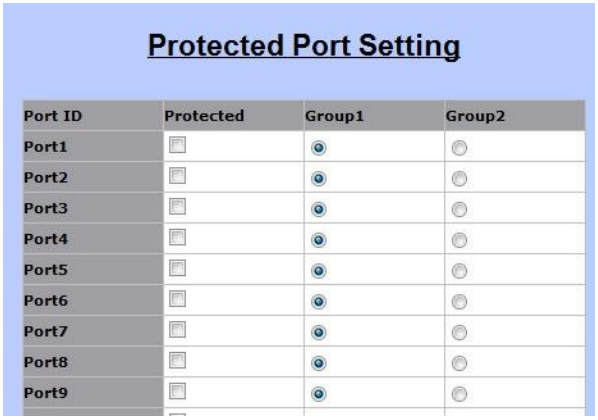


"Port Sniffer" is for monitoring a target port by mirroring or copying the data of the port and forwarding to an assigned port.

- Sniffer Type
  - Options: Disable, Rx, TT, or Both.
  - Users are able to choose what kind of data they would like to monitor.
- Analysis Port
  - This port is for assigning the port which should receive the data.
  - The analysis port will accept only copied packets from the monitored port.
- Port & Monitor

- This port is for assigning the port users would like to monitor.

- **Protected Port**



"Protected Port" isolates a protected port from its neighbor ports and other ports in different protected groups. However, it is allowed for a protected port to communicate with other unprotected ports. By setting up protected ports, it is able to ensure that there is no traffic, such as unicast, broadcast, or multicast, between protected ports on the VDSL2 IP DSLAM.

This function provides two protected port groups. Users are able to choose ports and assign to either group 1 or group 2.

- Options:

  - Protected

    - Click on the corresponding checkbox to select a port.

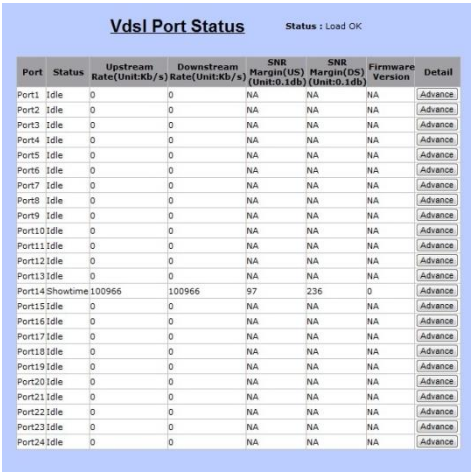
  - Group1

    - Click on the corresponding radio button for assigning a group.

  - Group2

    - Click on the corresponding radio button for assigning a group.

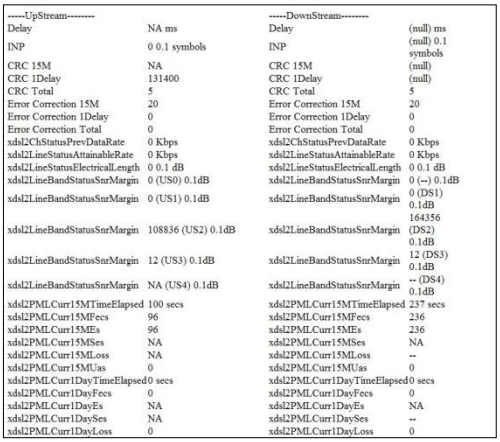
- **VDSL Port Status**



Vdsl Port Status Status : Load OK

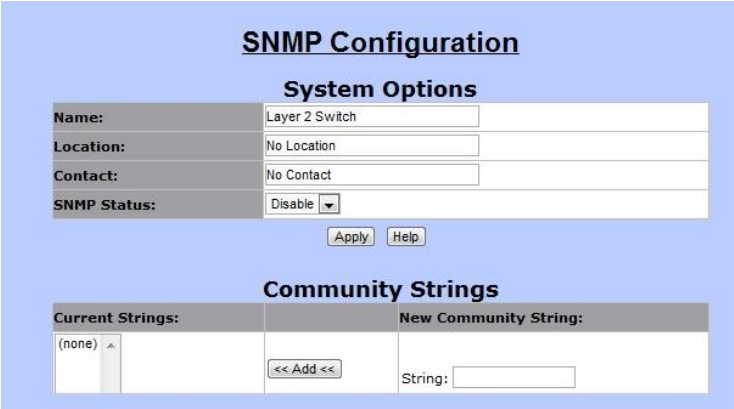
Port	Status	Upstream Rate(Unit:Kb/s)	Downstream Rate(Unit:Kb/s)	SNR Margin(US) (Unit:0.1db)	SNR Margin(DS) (Unit:0.1db)	Firmware Version	Detail
Port1	Idle	0	0	NA	NA	NA	Advance
Port2	Idle	0	0	NA	NA	NA	Advance
Port3	Idle	0	0	NA	NA	NA	Advance
Port4	Idle	0	0	NA	NA	NA	Advance
Port5	Idle	0	0	NA	NA	NA	Advance
Port6	Idle	0	0	NA	NA	NA	Advance
Port7	Idle	0	0	NA	NA	NA	Advance
Port8	Idle	0	0	NA	NA	NA	Advance
Port9	Idle	0	0	NA	NA	NA	Advance
Port10	Idle	0	0	NA	NA	NA	Advance
Port11	Idle	0	0	NA	NA	NA	Advance
Port12	Idle	0	0	NA	NA	NA	Advance
Port13	Idle	0	0	NA	NA	NA	Advance
Port14	Showtime	100966	100966	97	236	0	Advance
Port15	Idle	0	0	NA	NA	NA	Advance
Port16	Idle	0	0	NA	NA	NA	Advance
Port17	Idle	0	0	NA	NA	NA	Advance
Port18	Idle	0	0	NA	NA	NA	Advance
Port19	Idle	0	0	NA	NA	NA	Advance
Port20	Idle	0	0	NA	NA	NA	Advance
Port21	Idle	0	0	NA	NA	NA	Advance
Port22	Idle	0	0	NA	NA	NA	Advance
Port23	Idle	0	0	NA	NA	NA	Advance
Port24	Idle	0	0	NA	NA	NA	Advance

"VDSL Port Status" allows users to monitor the current information of each VDSL port, such as, status, upstream rate, downstream rate, SNR margins for upstream and downstream, and firmware version. In addition, it includes "Advance" button for checking the details of the selected port in another window, as the following.



-----UpStream--------		-----DownStream--------	
Delay	NA ms	Delay	(null) ms
INP	0 0.1 symbols	INP	(null) 0.1 symbols
CRC 15M	NA	CRC 15M	(null)
CRC 1Delay	131400	CRC 1Delay	(null)
CRC Total	5	CRC Total	5
Error Correction 15M	20	Error Correction 15M	20
Error Correction 1Delay	0	Error Correction 1Delay	0
Error Correction Total	0	Error Correction Total	0
xdsl2ChStatusPrevDataRate	0 Kbps	xdsl2ChStatusPrevDataRate	0 Kbps
xdsl2LineStatusAttainableRate	0 Kbps	xdsl2LineStatusAttainableRate	0 Kbps
xdsl2LineStatusElectricalLength	0 0.1 dB	xdsl2LineStatusElectricalLength	0 0.1 dB
xdsl2LineBandStatusSnrMargin	0 (US0) 0.1dB	xdsl2LineBandStatusSnrMargin	0 (--) 0.1dB
xdsl2LineBandStatusSnrMargin	0 (US1) 0.1dB	xdsl2LineBandStatusSnrMargin	0 (DS1) 0.1dB
xdsl2LineBandStatusSnrMargin	108836 (US2) 0.1dB	xdsl2LineBandStatusSnrMargin	164356 (DS2) 0.1dB
xdsl2LineBandStatusSnrMargin	12 (US3) 0.1dB	xdsl2LineBandStatusSnrMargin	12 (DS3) 0.1dB
xdsl2LineBandStatusSnrMargin	NA (US4) 0.1dB	xdsl2LineBandStatusSnrMargin	-- (DS4) 0.1dB
xdsl2PMLCurr15MTimeElapsed	100 secs	xdsl2PMLCurr15MTimeElapsed	237 secs
xdsl2PMLCurr15MFecs	96	xdsl2PMLCurr15MFecs	236
xdsl2PMLCurr15MEs	96	xdsl2PMLCurr15MEs	236
xdsl2PMLCurr15MSes	NA	xdsl2PMLCurr15MSes	NA
xdsl2PMLCurr15MLoss	NA	xdsl2PMLCurr15MLoss	--
xdsl2PMLCurr15MUas	0	xdsl2PMLCurr15MUas	0
xdsl2PMLCurr1DayTimeElapsed	0 secs	xdsl2PMLCurr1DayTimeElapsed	0 secs
xdsl2PMLCurr1DayFecs	0	xdsl2PMLCurr1DayFecs	0
xdsl2PMLCurr1DayEs	NA	xdsl2PMLCurr1DayEs	NA
xdsl2PMLCurr1DaySes	NA	xdsl2PMLCurr1DaySes	--
xdsl2PMLCurr1DayLoss	0	xdsl2PMLCurr1DayLoss	0

3.1.5 SNMP CONFIGURATION



"SNMP" stands for "Simple Network Management Protocol", which is a standard protocol for managing network devices. SNMP is used commonly in Network Management Systems (as known as, NMS) to monitor network devices. In addition, MIBs (Management Information Bases) is a kind of file which is used to store all the data of managed network devices in NMS according to SNMP standard protocols.

VDSL2 IP DSLAM supports three versions of SNMP: SNMPv1, SNMPv2c and SNMPv3. In SNMP Configuration page, it includes the followings sections.

- **System Options**

- Name
  - The name of the VDSL2 IP DSLAM

- Location
  - The location of the switch
- Contact
  - The contact information (the name of a person or organization)
- SNMP Status
  - Options: Enable or Disable
  - This option is for enabling or disabling SNMP function.

- **Community Strings**

This section is for setting up the password for accessing SNMP system.

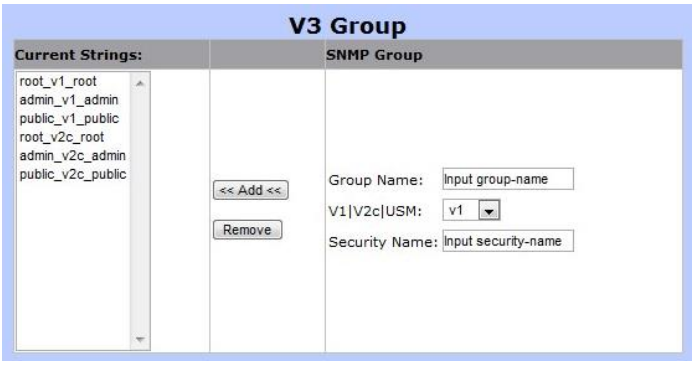
- Current Strings
  - The list of existing password strings
- New Community String
  - For the information of a new password
  - String: password
  - Options: RO (read only) or RW (read and write)
- Add
  - Add button: for adding new information on the right hand side of the table to the community list.
- Remove

- Remove button: for removing a password from the left hand side of the table.

- **Trap Manager**

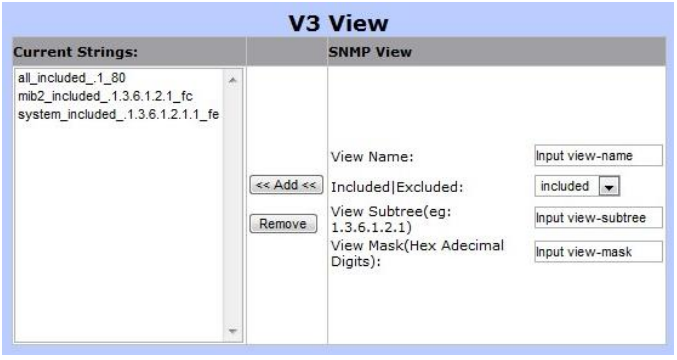
- Current Managers
  - The list of existing SNMP servers.
- New Manager
  - The information of new trap manager.
  - IP Address: the IP address of the trap manager.
  - Community: the password for accessing the trap manager.
- Add
  - For adding new manager.
- Remove
  - For removing the information of existing manager.

- **SNMPv3 Group**



- Current Strings
  - The list of current SNMPv3 groups.
- SNMP Group
  - Group Name: the name of the SNMPv3 group.
  - V1/V2c/USM: the security model of this group.
  - Security Name: the security name string of this group.
- Add
  - For adding new SNMPv3 group.
- Remove
  - For removing an existing SNMPv3 group.

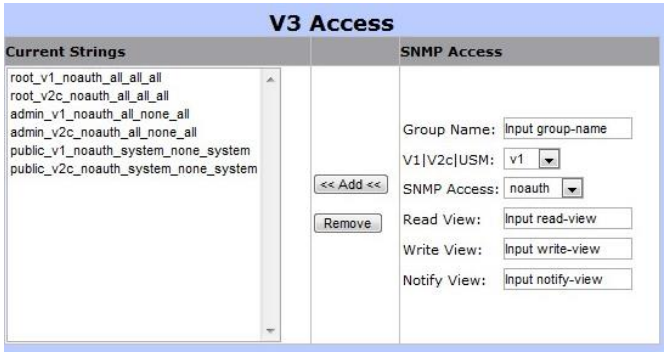
- **SNMPv3 View**



"SNMPv3 view" is to offer or deny access to the complete features or parts of features of the VDSL2 IP DSLAM.

- Current Strings
  - The name of current SNMPv3 views.
- SNMP View
  - View Name: the name of the new SNMPv3 view.
  - Included/Excluded: the OID should be included or excluded from the SNMP view.
  - View Subtree: the feature OID of this view.
  - View Mask: the subnet mask of this view.
- Add
  - For adding the new SNMPv3 view.
- Remove
  - For removing a selected SNMPv3 view from the current strings table.

- **SNMPv3 Access**



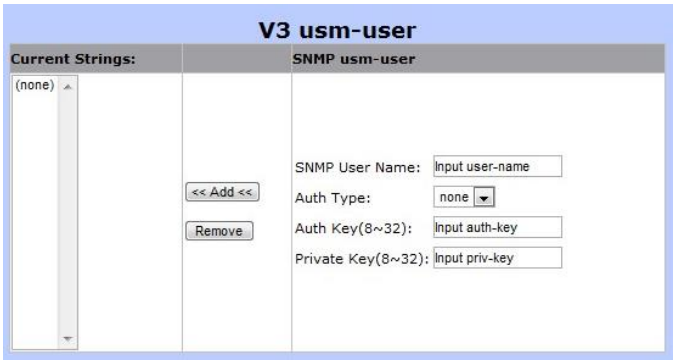
"SNMPv3 Access" section is for managing SNMPv3 access control, which is different from the access control defined by SNMPv1 and SNMPv2. SNMPv3 access sets up

SNMP access levels based on contexts, groups and users, rather than on IP addresses and community strings.

- Current Strings
  - The list of current SNMPv3 access list
- SNMP Access
  - Group Name: the group name of the new SNMPv3 access
  - V1/V2c/USM: the security model
    - V1: Reserved for SNMPv1
    - V2c: Reserved for SNMPv2c
    - USM: User-based Security Model
  - SNMP Access: the security model
    - Options: NoAuth/ Auth/ Authpriv
    - NoAuth: None authentication and none privacy
    - Auth: Authentication and none privacy
    - Authpriv: Authentication and privacy
  - Read View: the view name for each group that defines the list of OIDs that are accessible for reading by users belonging to the group.
  - Write View: the view name for each group that defines the list of OIDs that are able to be created or modified by users of the group.
  - Notify View: the view name for each group that defines the list of notifications that can be sent to each user in the group.
- Add
  - For adding the new SNMPv3 access
- Remove

- For removing an access from Current Strings list

- **SNMPv3 USM-User**



"SNMPv3 USM-User" section is for setting up the details of USM (User-based Security Model) security model. USM provides different types of security levels using various authentication and privacy protocols.

- Current Strings
  - The list of current SNMPv3 USM-user.
- SNMP usm-user
  - SNMP User Name
    - the name of new USM user
  - Auth Type
    - The authentication type
    - Options: none or md5
  - Auth Key
    - The authentication password of the USM user
  - Private Key
    - The password for the privacy protocol type
- Add

- For adding the new SNMPv3 USM-user

- Remove

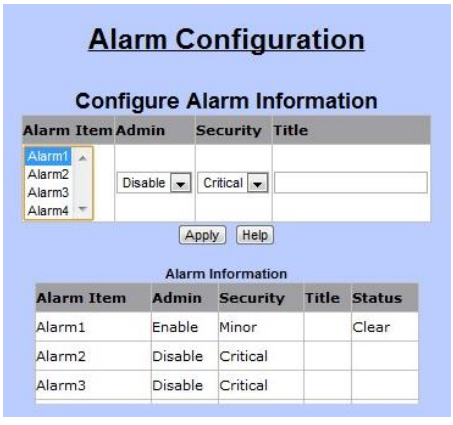
  - For removing a SNMPv3 USM-user from the current list

3.1.6 SYSLOG SETTING

"Syslog" function is supported in this VDSL2 IP DSLAM system. The system will send logs to a remote log system. In this system, three events will be reported to the remote log system: cold start, warm start and link change. The followings are necessary for connecting the remote syslog server.

- Syslog server IP: the IP address of the remote syslog server IP.
- Log level:
  - Options: None, Major, or All

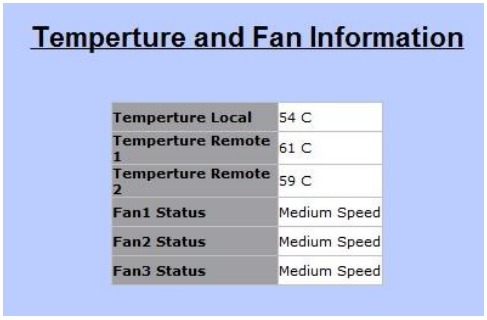
3.1.7 ALARM CONFIGURATION



"Alarm Configuration" is distinguished into two tables: Configure Alarm Information and Alarm Information. Users are able to setup alarms and monitor alarm status.

- **Configure Alarm Information (configuration section)**
  - Alarm Item
    - Total of four alarms can be set in the VDSL2 IP DSLAM
  - Admin
    - Options: Disable or Enable
  - Security
    - The level of the alarm
  - Title
    - The name of the alarm
- **Alarm Information (monitor section)**
  - Alarm Item
  - Admin
  - Security
  - Title

3.1.8 TEMPERATURES & FAN STATUS



"Temperatures & Fan Status" allows users to monitor the real-time information of the VDSL2 IP DSLAM's temperatures and FANs.

3.1.9 FIRMWARE UPDATE

"Firmware Update" allows users to upgrade firmware by themselves. Users are able to choose upgrading firmware through TFTP or HTTP.

3.1.10 CONFIGURATION BACKUP

Users are able to load or backup configurations via "Configuration Restore" function. This function includes two tabs: "TFTP Restore Configuration" and "TFTP Backup Configuration".

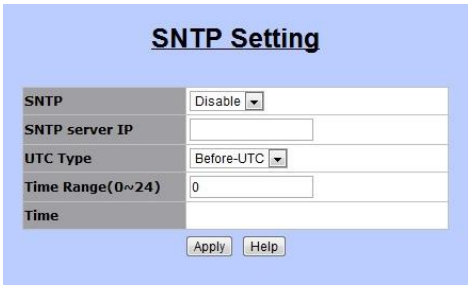
- **TFTP Restore Configuration**

This section is for load the settings from a configuration file. Users are able to upload the settings by TFTP or HTTP.

- **TFTP Backup Configuration**

This area allows users to download the current configuration through TFTP or HTTP.

3.1.11 SNTP SETTING



SNTP stands for "Simple Network Time Protocol". SNTP is a simpler version of "Network Time Protocol" (NTP), which is a system for synchronizing the clocks of network computer systems. By enabling SNTP function, users are able to configure this switch to send time synchronization requests to the assigned servers with servers' IP addresses.

- SNTP
  - To enable or disable SNTP feature.
  - Options: Enable or Disable.
- SNTP server IP
  - The IP address of the assigned SNTP server.
- UTC Type

- To decide the time zone.
- Options:
  - After-UTC: UTC+hh (hh: hours)
    - For example, Taipei (UTC+08), choose “After-UTC”.
  - Before-UTC: UTC-hh (hh: hours)
    - For example, San Francisco (UTC-08), choose “Before-UTC”.

- Time Range
  - This field is for setting up the hour data in “UTC-hh/UTC+hh”.
    - For example, UTC-08, then, choose “Before-UTC” in UTC type and fill in “8” in Time Range.

- Time
  - This section is for displaying the current time once the switch is connected to the assigned NTP server.

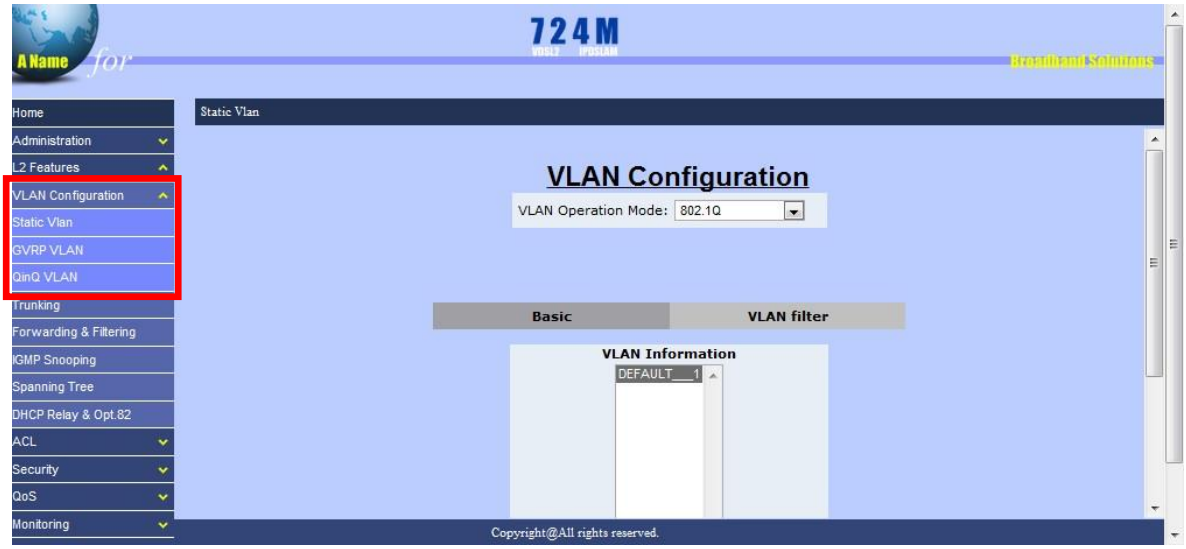
3.2 L2 FEATURES

VDSL2 724M IP DSLAM offers a flexible L2 features, as the following functions:

- VLAN Configuration
- Trunking
- Forwarding & Filtering
- IGMP Snooping
- Spanning Tree
- DHCP Relay & Opt.82

3.2.1 VLAN CONFIGURATION

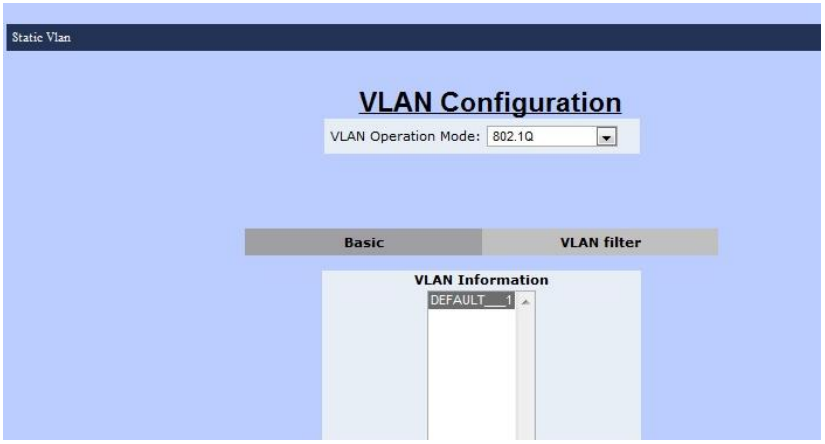
"VLAN" stands for "Virtual Local Area Network" or "virtual LAN". It is a concept of separating and grouping LAN segments by a common set of requirements. VLAN presents couple benefits, such as, simplifying network design, enhancing bandwidth performance and improving, etc.



The VDSL2 IP DSLAM supports three kinds of VLAN algorithms:

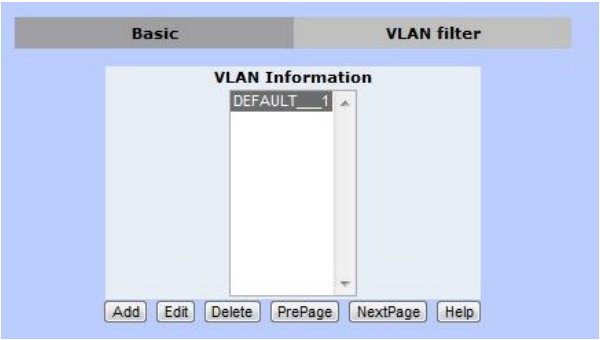
- Static VLAN
- GVRP VLAN
- QinQ VLAN

3.2.1.1 STATIC VLAN



Static VLAN function allows users to setup and manage VLAN groups manually.

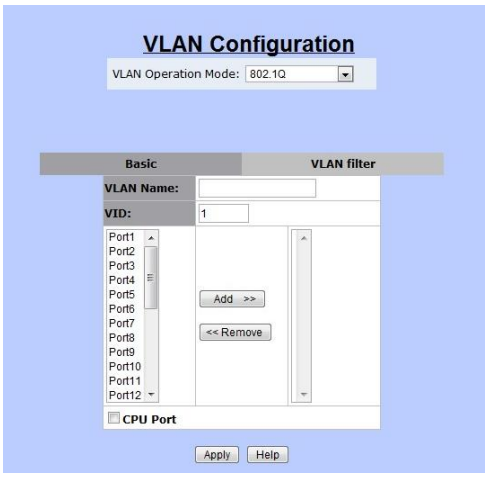
- **VLAN Operation Mode**
  - No VLAN
    - To disable VLAN mode.
  - Port-Based VLAN
    - To setup VLAN groups by ports.
  - 802.1Q VLAN
    - To setup VLAN groups by 802.1Q VLAN tags.
- **Basic**



"VLAN Information" displays all VLAN groups stored already. The following buttons allow users to manage VLAN groups.

The VLAN mode of VLAN operation mode is the global setting of "Basic" and "VLAN Filter".

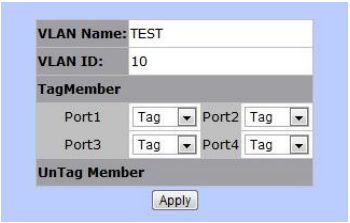
- Add



■ To create a new VLAN group.

Name	Description
VLAN Name	The name of this VLAN group
VID	VLAN ID
VLAN Members	There are three columns in this section. ➢ Ports (left-hand side): Port1 ~ Port24, Mod1, Mod2 ➢ Add or Remove (middle): for adding or removing a port ➢ Selected Ports (right-hand side): the VLAN group members
CPU Port	Click on this checkbox to choose this VLAN group as the management group of this VDSL2 IP DSLAM.

- Click "Apply" to set up tag mode.



- Edit

  - To change the settings of an existing VLAN group.

- Delete

  - To remove an existing VLAN group.

- PrePage

  - To move to the previous page of VLAN information table.

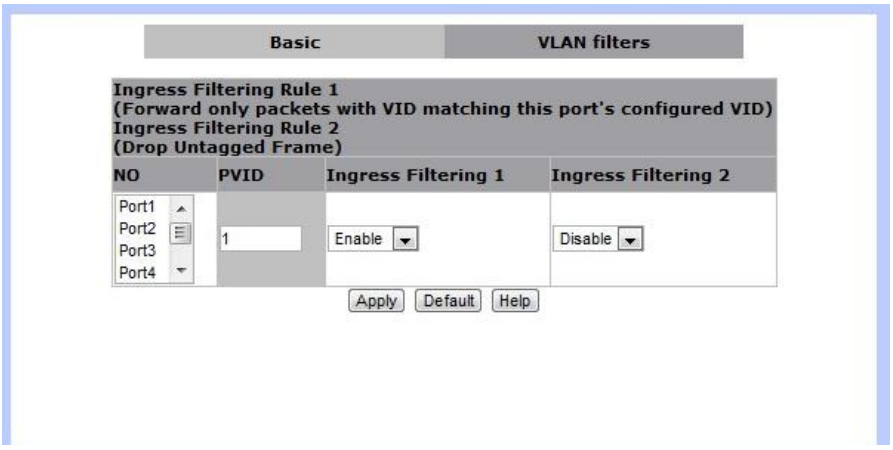
- NextPage

  - To move to the following page of VLAN information table.

- Help

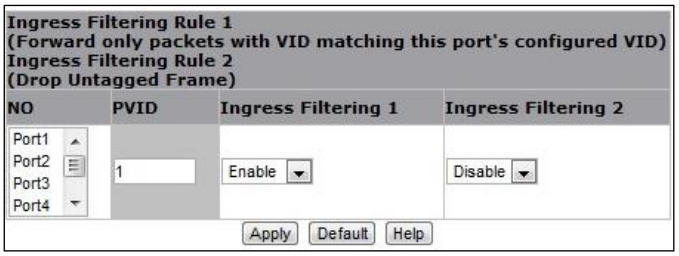
  - To open FAQ page of VLAN configuration.

- **VLAN filter**



VLAN filter function is for setting the filtering rules for all ports (Port1 ~ Port24, Mod1 and Mod2).

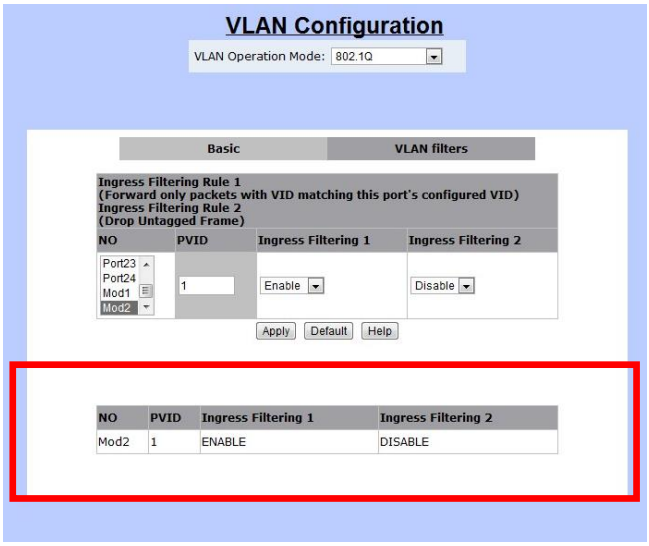
Users are able to define filtering rules for each port.



- NO

  - The list of available ports.

  - Click on a port to change the details. In addition, the current setups will be showed in a different table right next to the setup table.



- PVID

  - The VLAN ID of ingress packets.

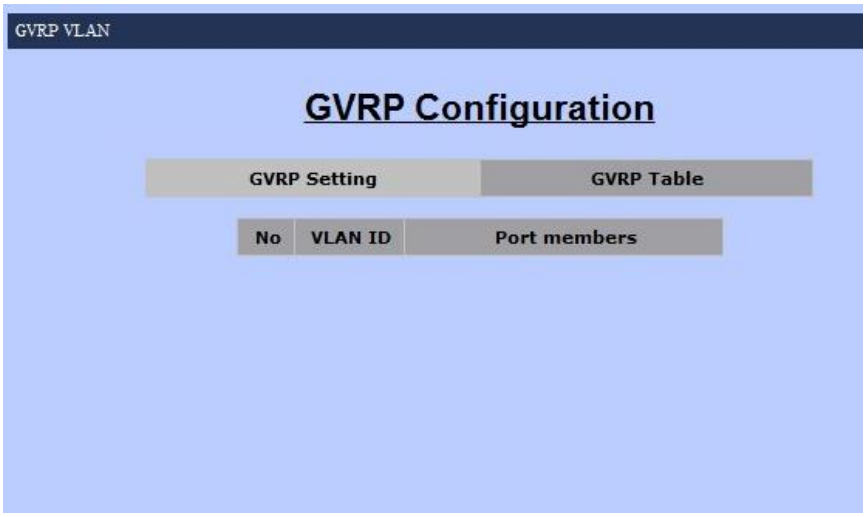
Two filtering rules are available in VLAN Filtering function of this VDSL2 IP DSLAM.

- Ingress Filtering 1

- Only these ingress packets with the assigned VLAN ID are able to pass through this port.
- Options: Enable or Disable (disable filtering function)

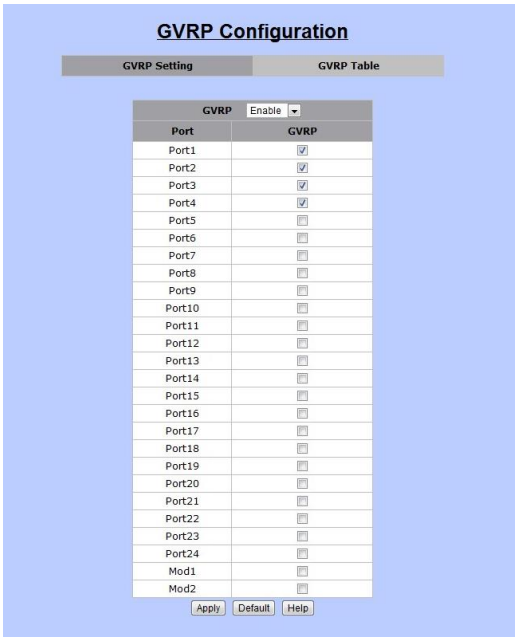
- Ingress Filtering 2
  - Enabling this rule will drop all untagged packets.
  - Options: Enable (only packets with the assigned VLAN ID can pass through this port) or Disable (accept all packets)

3.2.1.2 GVRP VLAN



GVRP stands for "GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol" or "Generic VLAN Registration Protocol". GVRP VLAN method follows IEEE 802.1Q specification and defines tagging frames with VLAN configuration data. This meaning allows VDSL2 IP DSLAM to exchange VLAN configuration information with other network devices dynamically.

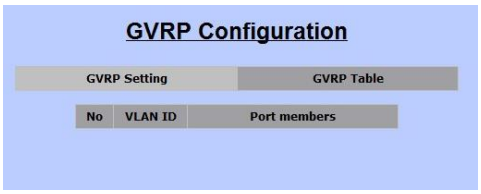
- GVRP Setting
  - For setting up GVRP configurations



- GVRP
  - Options: Enable or Disable
- Port & GVRP
  - Port1 ~ Port24, Mod1, Mod2 & corresponding checkbox.
  - Click on the checkboxes to choose GVRP group members.
- Apply
  - To save the modifications.
- Default
  - To restore default settings.
- Help
  - To open the FAQ page of GVRP VLAN.

- GVRP Table

  ■ This table is for displaying current GVRP VLAN information.



  - GVRP will learn VLAN ID and its group member automatically. This table will show this information.

3.2.1.3 QINQ VLAN

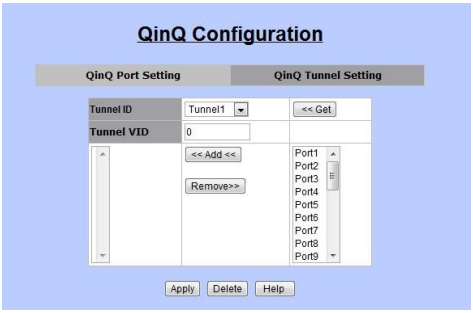
QinQ VLAN function allows users or service providers to separate traffic service for different customers by adding service provide VLAN tags and customer VLAN IDs. In this function, settings are divided into two parts:

- QinQ Port Setting
- QinQ Tunnel Setting

- **QinQ Port Setting**

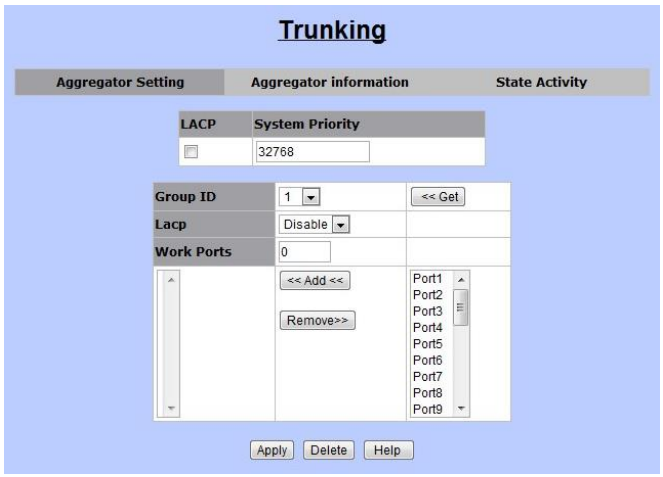
- This section is for setting up QinQ mode, TPID, and group members.
- The followings are the details that are required to be filled in for setting QinQ function.
  - QinQ: Disable or Enable
  - QinQ TPID:
    - TPID stands for "Tag Protocol Identifier".
    - TPID is the Ethertype value for 802.1Q encapsulation.
    - Standard Ethertype value: 0x8100 (Default value)
    - Range: 0x0800 ~ 0xFFFF (hexadecimal value).
  - Port Table:
    - QinQ: for choosing which port should be enabled with QinQ mode.
    - QinQ Uplink: for setting up an uplink port of this QinQ group.

- **QinQ Tunnel Setting**



- Tunnel ID
- Tunnel VID

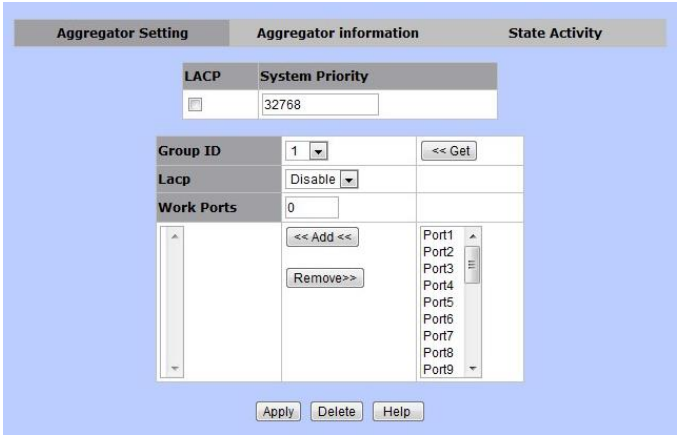
3.2.2 TRUNKING



Trunking function allows users to combine several ports or connections together to create one single connection which has a higher and faster connection speed. "Trunking" is also called "Link Aggregation". Two trunking techniques are available in this VDSL2 IP DSLAM:

- Static Trunk
- LACP

- Aggregator Setting

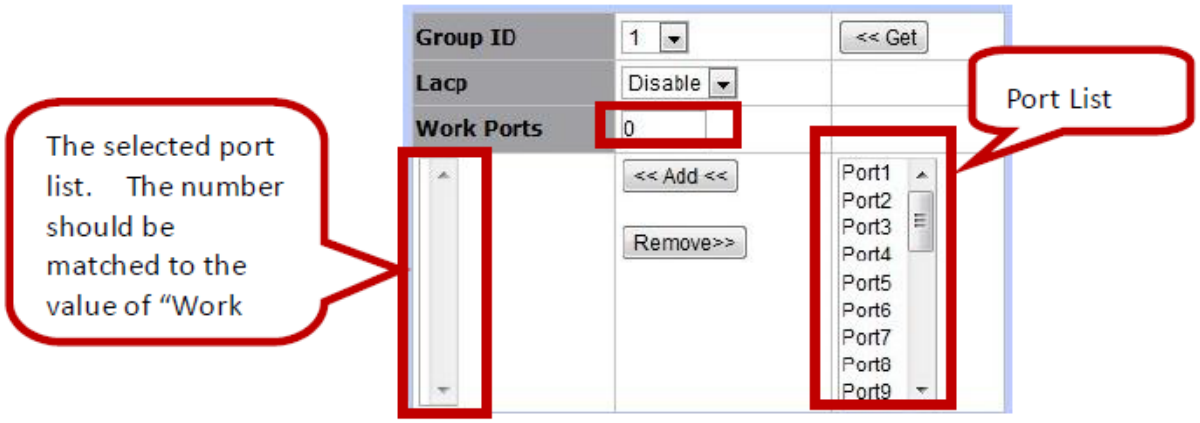


- This section allows users to setup trunking groups and details.
- The following information is needed for setting up a trunk group.

- LACP (checkbox): for enable or disable LACP algorithm by check on the checkbox.
- System Priority: this value is for identifying the active LACP of this VDSL2 IP DSLAM.

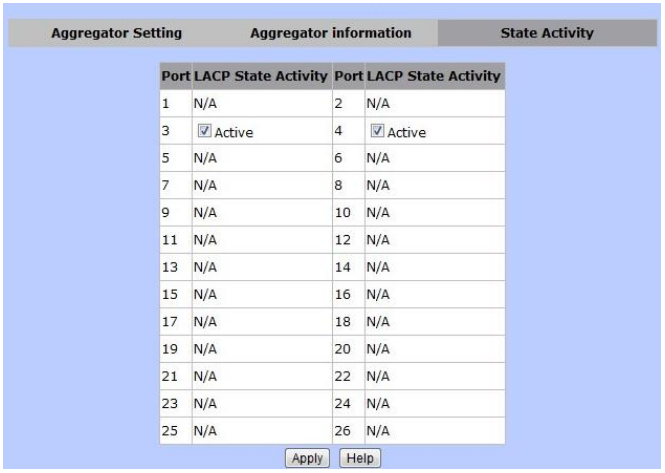
The lowest value presents the highest priority.

- Trunk Group Table
  - Group ID: the trunk group ID (1~13)
  - LACP: Enable or Disable LACP algorithm for this trunk group.
  - Work Ports: the total port number of the group member. (Please select the group number in the following port list.)



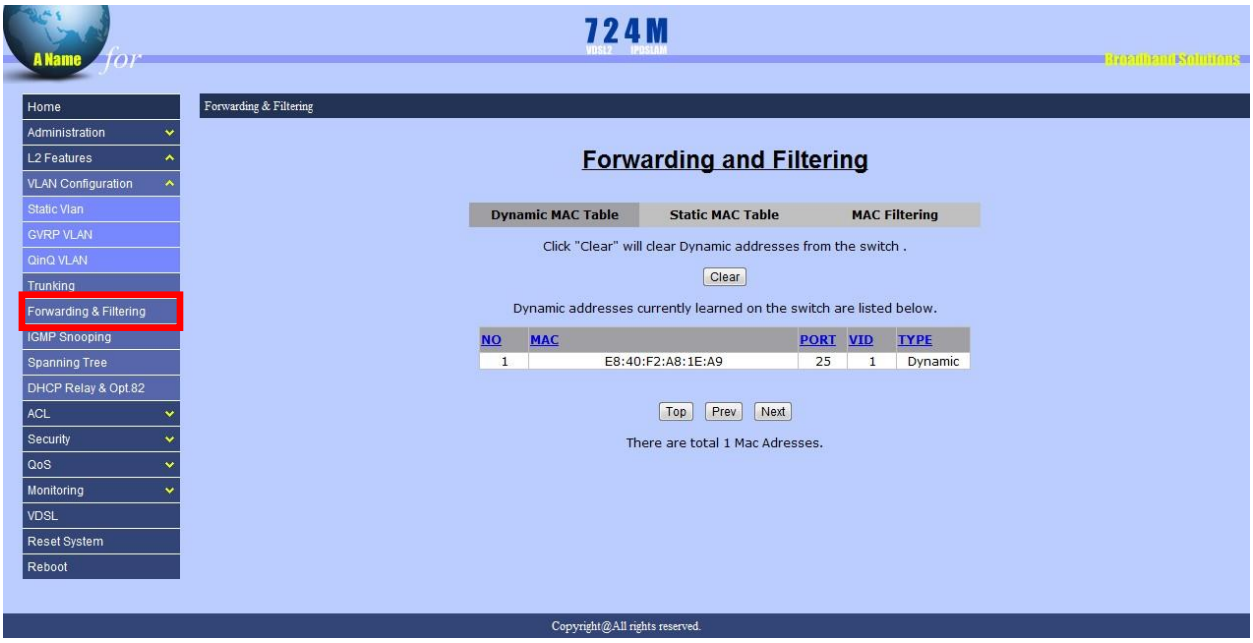
- Aggregator information
  - This section allows users to review trunk information.
  - Two data are reviewed in this section:
    - Group Key: the trunk group ID.
    - Port No: the port member of this trunk group. (Port1 ~ Port24, Mod1, Mod2)

- Static Activity



- This area is for setting up LACP mode (active or passive)
  - Active: the active port will send LACP packets automatically.
  - Passive: the passive port will not send LACP packets but it will respond if and only if it receives LACP packets from the other end.

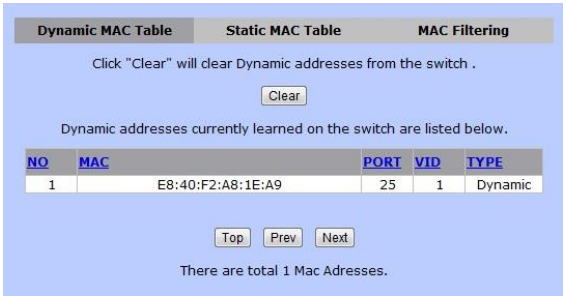
3.2.3 FORWARDING & FILTERING



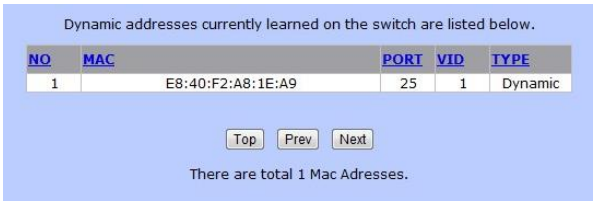
"Forwarding & Filtering" function is for users to setup rules about packets. Four ways to setup these rules:

- Dynamic MAC Table
- Static MAC Table
- MAC Filtering

- Dynamic MAC Table



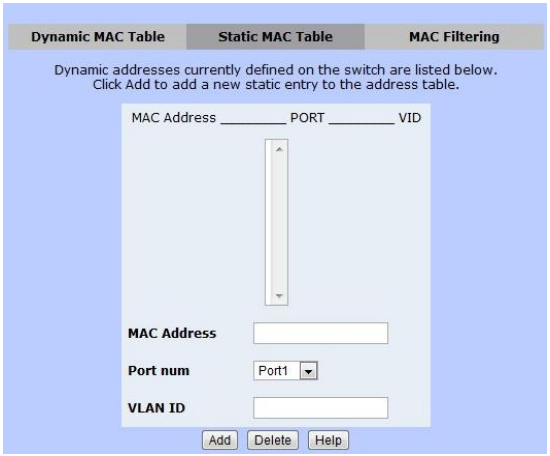
- The VDSL2 IP DSLAM will learn devices' MAC addresses dynamically and record these addresses into MAC address table. This section will show all the found MAC addresses as the following table.



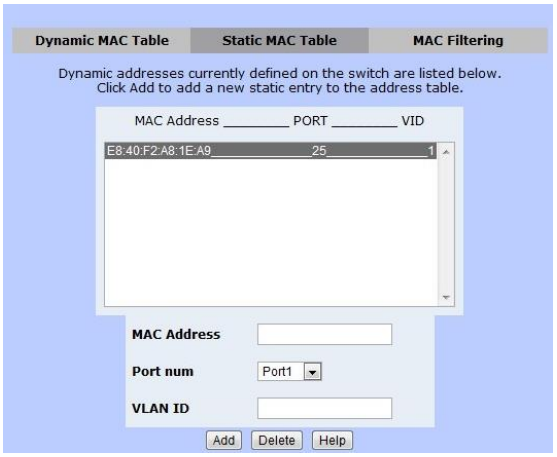
- Clear: to clear the dynamic MAC address table.
- Top: to show the first page of the MAC address table.
- Prev: to go to the previous page of the MAC address table.
- Next: to go to the next page of the MAC address table.

If there is nothing showed, it means this is the end page.

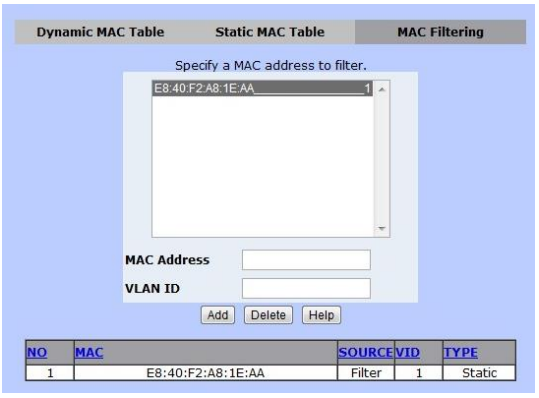
- Static MAC Table



- Users are able to fill up the MAC addresses of devices connected to the switch. By adding a static MAC address, the switch will save the information permanently and will not attend to learn the MAC address of this device when the device is online.



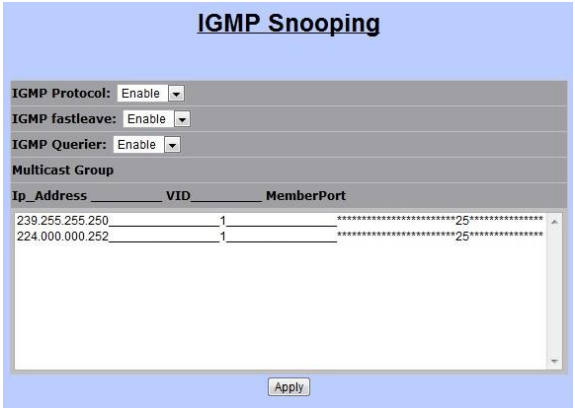
- MAC Filtering



■ Users are able to define and drop unwanted traffic in “MAC Filtering” function.

3.2.4 IGMP SNOOPING

"IGMP" stands for "Internet Group Management Protocol". IGMP allows hosts and routers to build multicast group memberships. IGMP snooping presents the process of IGMP network traffic listening. With this feature, VDSL2 IP DSLAM is able to listen to IGMP conversation between hosts and routers. The switch is able to maintain a relation map of links and IP multicast streams.

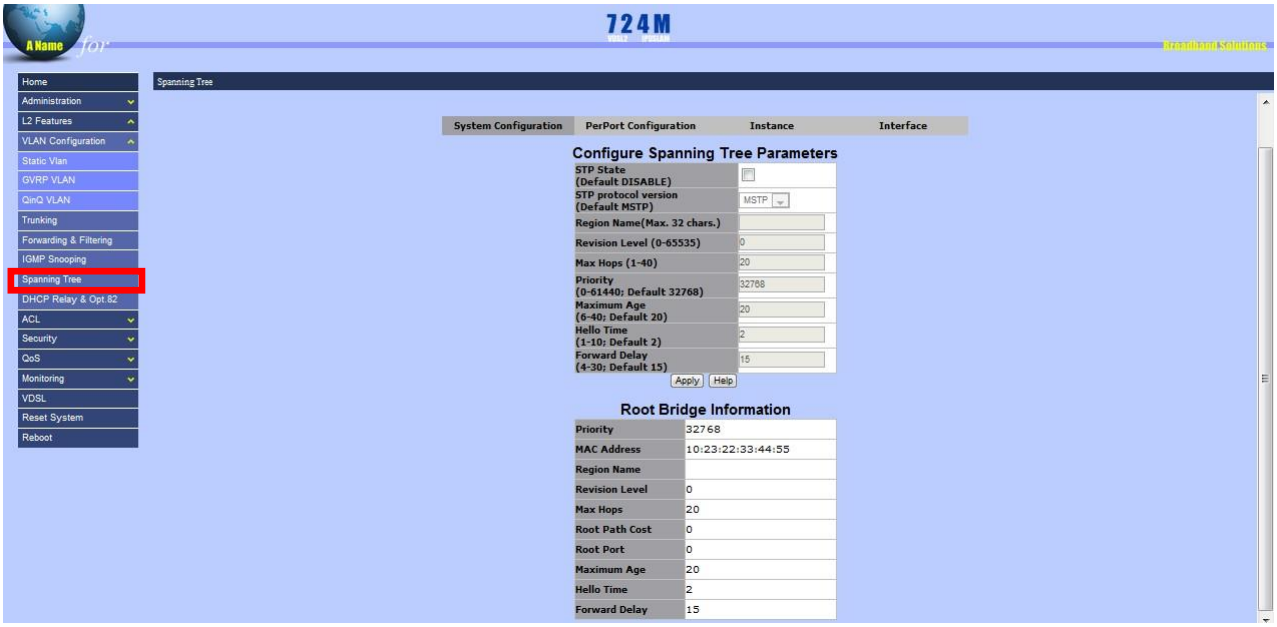


The following settings are needed in order to allow IGMP snooping work properly.

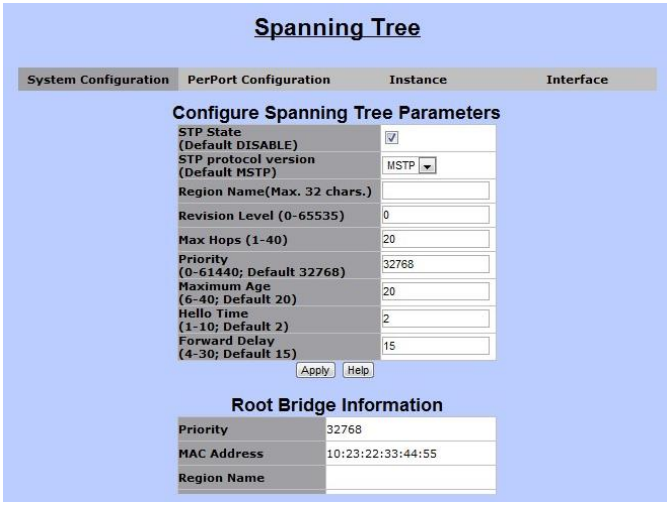
- IGMP Protocol: to enable or disable IGMP function.
- IGMP Fastleave: to enable or disable IGMP Fastleave mode.

- IGMP Querier: to enable or disable IGMP Querier mode.
- Multicast Group: the multicast group list table.

3.2.5 SPANNING TREE



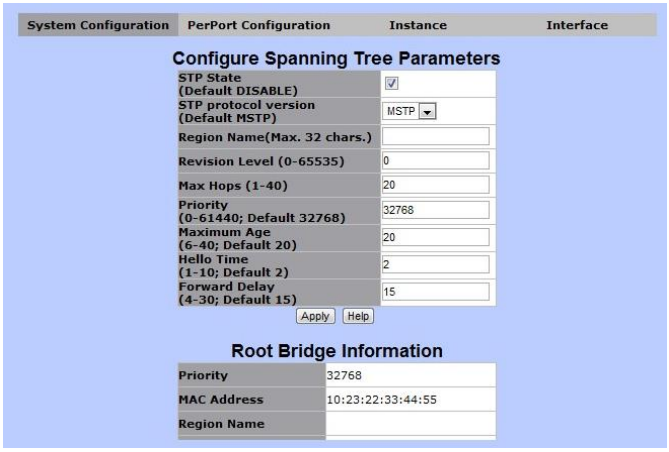
Spanning Tree (also known as, STP) is a network protocol which is defined by IEEE 802.1 D standards for preventing bridge loops and broadcast radiation. In addition, STP allows redundant links to provide automatic backups. Most commonly known STP algorithms are STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol), and MSTP (Multiple Spanning Tree Protocol). This VDSL2 IP DSLAM supports both STP and MSTP. In addition, in this Switch, users are able to set up STP either for the whole system of the Switch or for each individual port.



In Spanning Tree function, there are four major setup pages as the following sections.

- System Configuration
- PerPort Configuration
- Instance
- Interface

3.2.5.1 SYSTEM CONFIGURATION



"System Configuration" allows users setting up the details of STP function. In addition, the information of the root node of the STP will be displayed in this page.

- Configure Spanning Tree Parameters

  - STP State

    - To enable or disable STP function.

    To enable STP function, users are required to click on this checkbox and press "Apply" button. Then, after the saving process is completed, users are able to fill up the rest of the information.

  - STP protocol version

    - STP or MSTP

  - Region Name

    - Name of STP tree

  - Revision Level

    - The level of STP tree

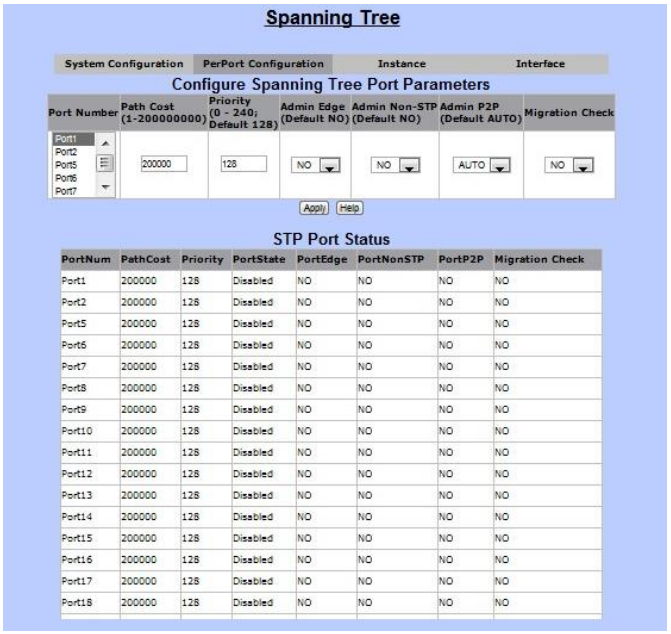
  - Max Hops

- Hop number

- Priority
- Maximum Age
  - The waiting time (seconds) before the switch attempts to reconfigure.
- Hello Time
  - The time (seconds) the switch will send BPDU packets to check STP current status.
- Forward Delay

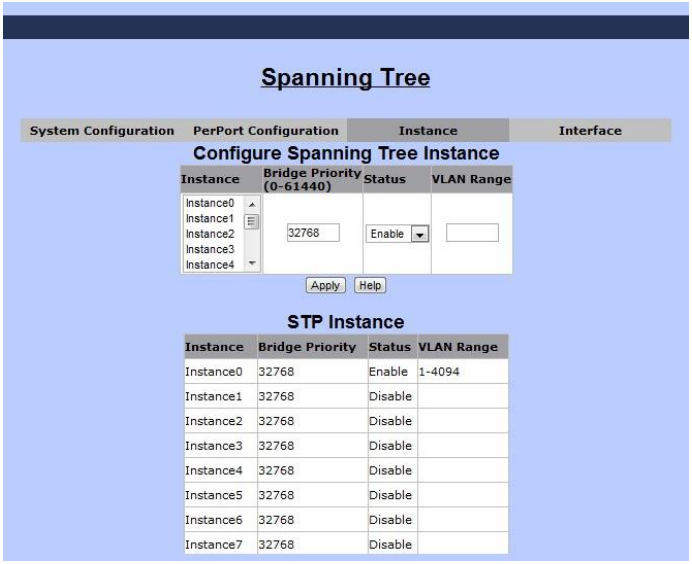
- Root Bridge Information
  - Priority
  - MAC Address
  - Region Name
  - Revision Level
  - Max Hops
  - Root Path Cost
  - Maximum Age
  - Hello Time
  - Forward Delay

3.2.5.2 PERPORT CONFIGURATION

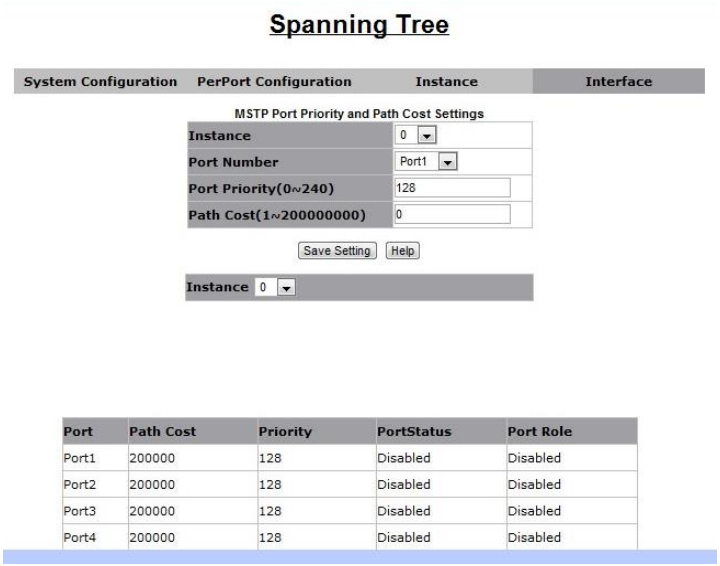


"PerPort Configuration" is for setting up Spanning Tree mode for each individual port.

3.2.5.3 INSTANCE

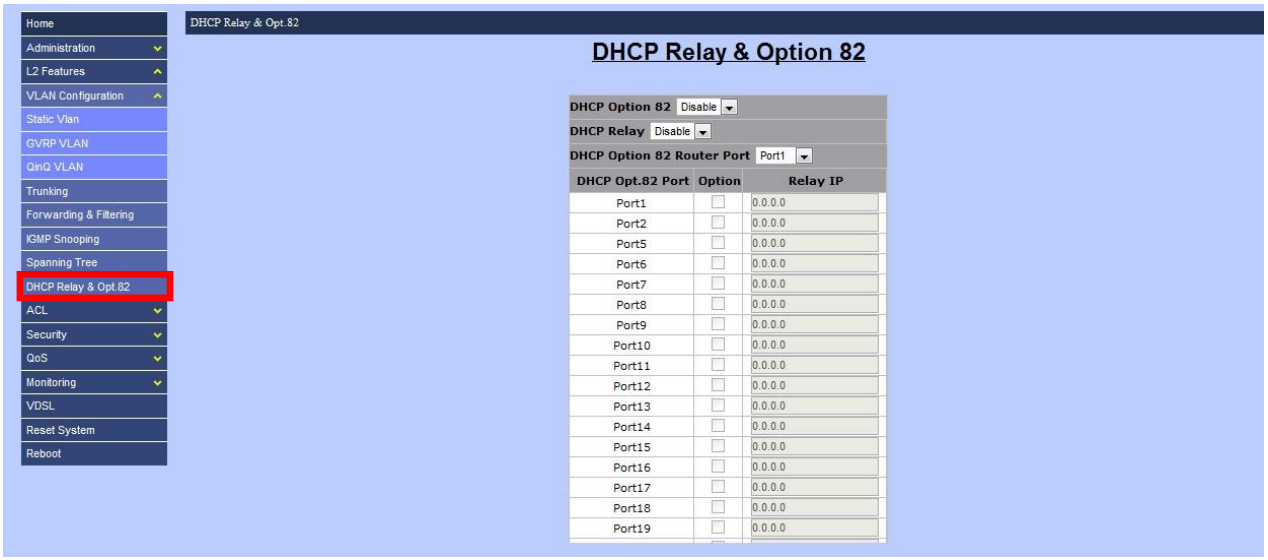


3.2.5.4 INTERFACE



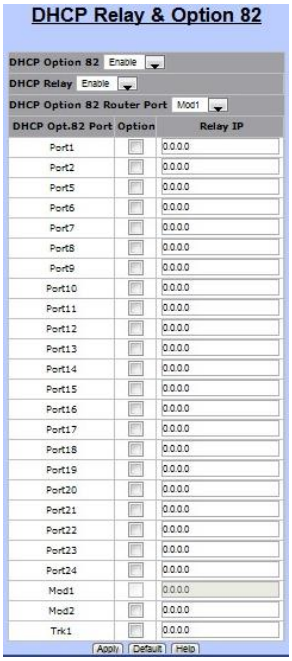
Port	Path Cost	Priority	PortStatus	Port Role
Port1	200000	128	Disabled	Disabled
Port2	200000	128	Disabled	Disabled
Port3	200000	128	Disabled	Disabled
Port4	200000	128	Disabled	Disabled

3.2.6 DHCP RELAY & OPT.82



"DHCP" stands for "Dynamic Host Configuration Protocol", which is a network protocol that is for configuring network devices dynamically so these devices can communicate on an IP network. It is a service that runs at the application layer of TCP/IP protocol stack to assign IP addresses to its clients dynamically.

"DHCP Relay" will forward DHCP broadcasts to multiple DHCP servers in different subnets using unicasts. By doing so, DHCP clients on subnets not directly served by DHCP servers can communicate with DHCP servers. In addition, "DHCP Relay Information Options 82", is defined in RFC 3046 and RFC 3993, allows a DHCP Relay agent to insert circuit specific information to a request which is forwarded to a DHCP server.



3.2.6.1 DHCP OPTION 82

Users are allowed to enable or disable DHCP Option 82 by choosing the options in the drop-down menu. To setup DHCP Option 82 for this switch, users are required to enable this option first.

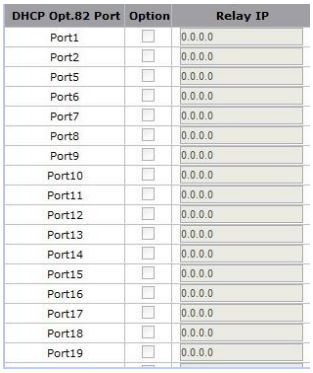
3.2.6.2 DHCP RELAY

DHCP Relay is for enabling or disabling DHCP Relay function.

3.2.6.3 DHCP OPTION 82 ROUTER PORT

"DHCP Option 82 Router Port" allows users to choose the relay port for DHCP Option 82 feature. Users are able to specific one port between Port1 to Port24 or Mod1 to Mod2.

3.2.6.4 DHCP OPT. 82 PORT TABLE



DHCP Opt.82 Port	Option	Relay IP
Port1	☐	0.0.0.0
Port2	☐	0.0.0.0
Port5	☐	0.0.0.0
Port6	☐	0.0.0.0
Port7	☐	0.0.0.0
Port8	☐	0.0.0.0
Port9	☐	0.0.0.0
Port10	☐	0.0.0.0
Port11	☐	0.0.0.0
Port12	☐	0.0.0.0
Port13	☐	0.0.0.0
Port14	☐	0.0.0.0
Port15	☐	0.0.0.0
Port16	☐	0.0.0.0
Port17	☐	0.0.0.0
Port18	☐	0.0.0.0
Port19	☐	0.0.0.0

This section is for defining DHCP Option 82 and port information.

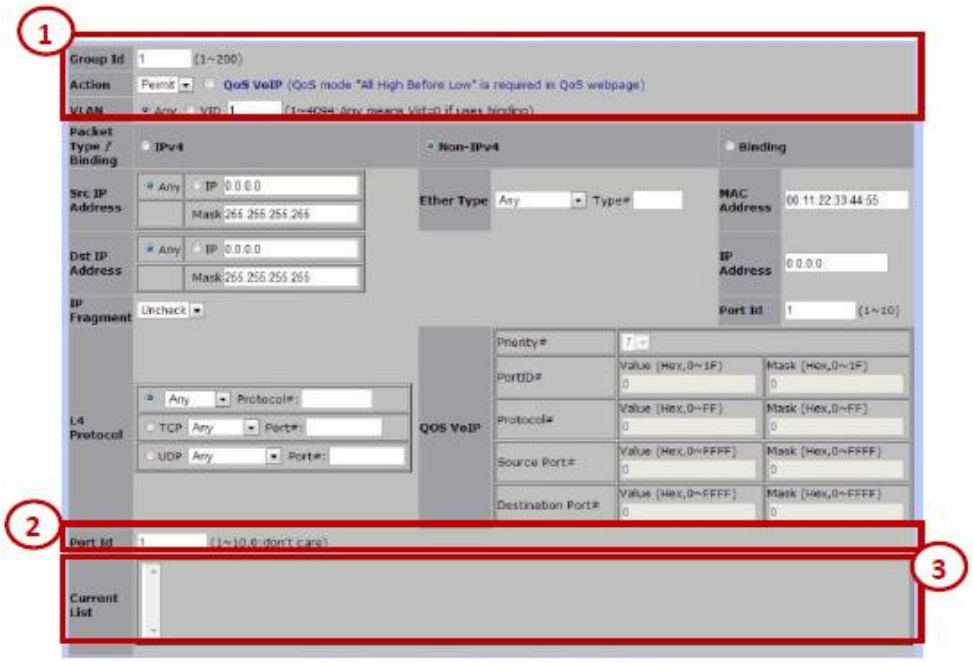
- Option: the checkbox for enabling or disabling DHCP Relay Information Option 82 function.

- Relay IP: for assign the IP address of the port.

3.3 ACL

Packets can be forwarded or dropped by ACL rules include IPv4 or non-IPv4. The switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

There are 2 main ACL rule types to setup: Packet Type (IPv4 and Non-IPv4) and Binding (SIP-SMAC-Port).



Section 1:

- Group ID: the ID of this Access Control List (1 ~ 200).
- Action: Permit or Deny the access
- VLAN: Any or VID (a specific VLAN ID)

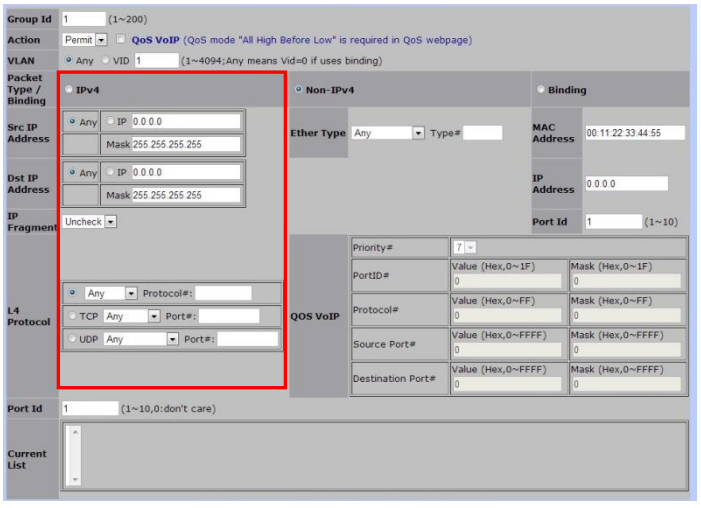
Section 2:

- Port ID: the target port of this access control list should be applied to. (0: don't care/1 ~ 10)

Section 3:

- Current List: the current list of all access control lists.

3.3.1 IPV4



- Packet Type/ Binding
  - The option of "IPv4" is selected.
- SRC IP Address

- Options: Any or a specific IP address
- The rule should be applied on these packets from which IP address or any IP address.

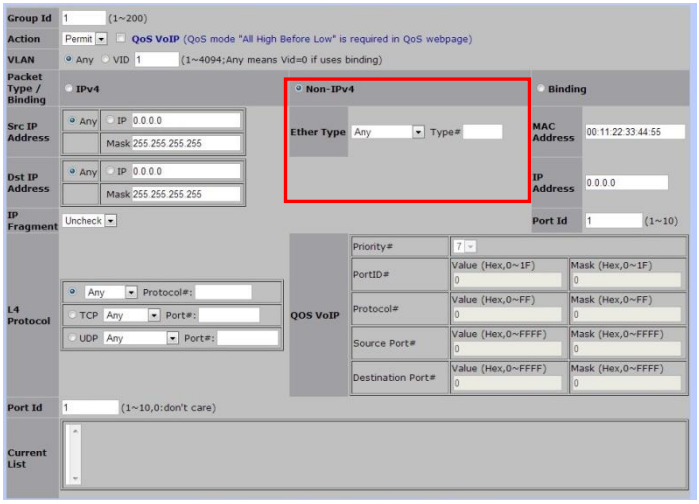
- DST IP Address
  - Options: Any or a specific IP address
  - The rule should be applied on these packets with an assigned destination IP address or any IP address.

- IP Fragment
  - Options: Uncheck or Check
  - To decide whether IP fragment should be checked or not.

- L4 Protocol
  - Options are as the following table

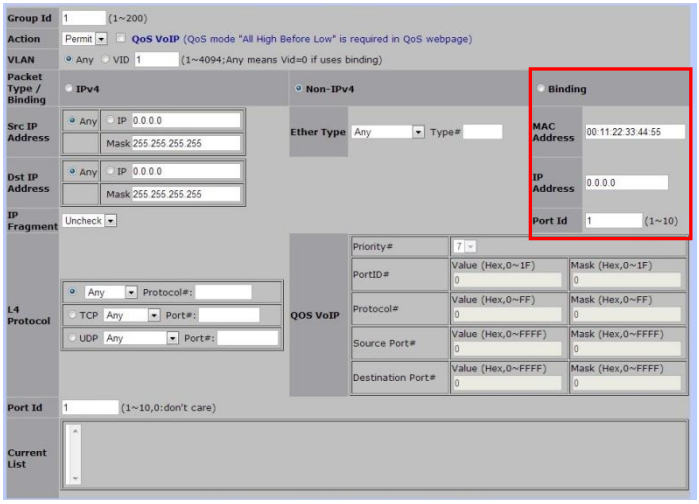
L4 Protocol Type	Options	Data
Any	Any, ICMP, or IGMP	Protocol No.
TCP	Any, FTP, or HTTP	Port No.
UDP	Any, DHCP, TFTP, NetBIOS	Port No.

3.3.2 NON-IPV4



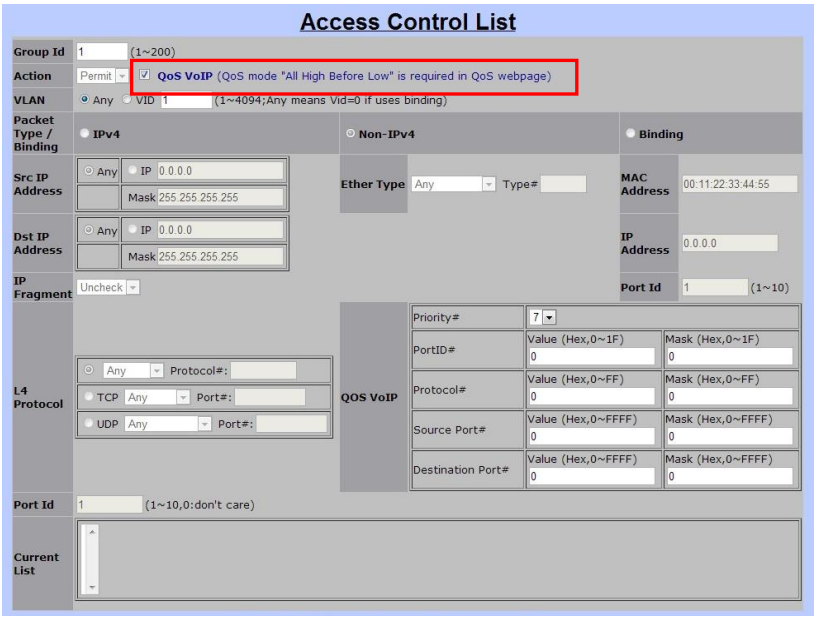
- Ether Type
  - Options: Any, ARP, or IPX

3.3.3 BINDING

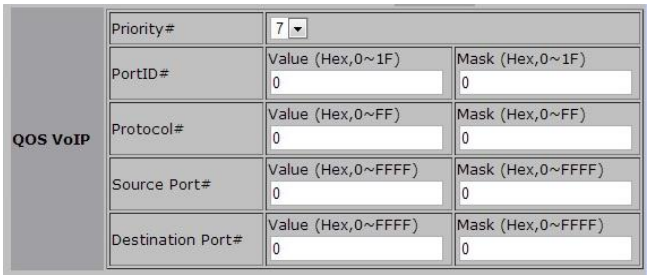


- MAC Address
- IP Address
- Port ID (1 ~ 10)

If the checkbox of QoS VoIP is selected, the following information should be provided.



QoS VoIP:



- Priority
  - The priority of QoS VoIP
  - Options: 0 ~ 7
- Port ID
  - Value
  - Mask
- Protocol
  - Value

- Mask

- Source Port
  - Value
  - Mask
- Destination Port
  - Value
  - Mask

All values are in HEX format.

3.4 SECURITY

"Security" section allows users to enhance the security level of this VDSL2 IP DSLAM. It includes the following functions:

- Security Manager
- MAC Limit
- 802.1x Configuration

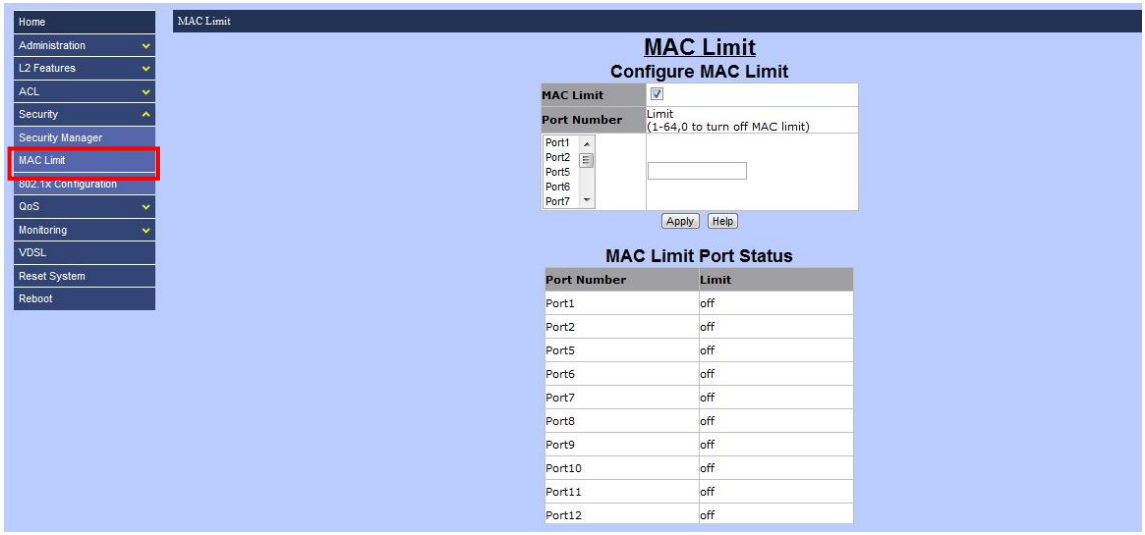
3.4.1 SECURITY MANAGER

"Security Manager" allows users to change the user name and password for login purpose. Only one set of user name and password is stored in the Switch. The followings are the necessary information for this section.

- User Name
- Assign/Change Password
- Reconfirm Password

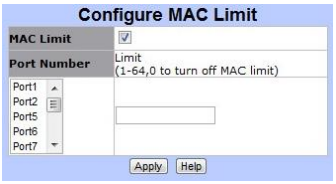
The default user name and password are "admin" and "admin".

3.4.2 MAC LIMIT



MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an "opening" is available, the switch stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked. Two sections are in MAC Limit page:

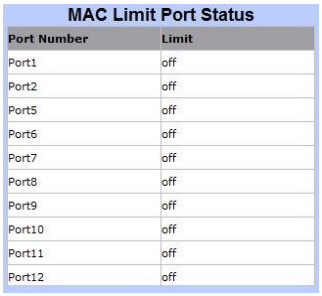
- Configure MAC Limit



Users are able to setup MAC limit rules for each port in this section by providing the information as the followings:

- MAC Limit: enable or disable MAC limit function.
- Limit: the maximum number of MAC addresses should be blocked.

- MAC Limit Port Status

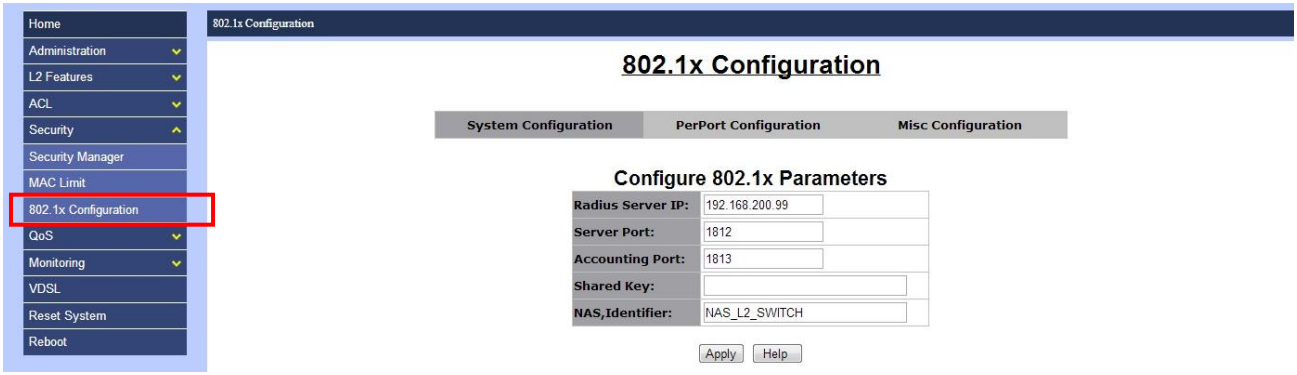


MAC Limit Port Status

Port Number	Limit
Port1	off
Port2	off
Port5	off
Port6	off
Port7	off
Port8	off
Port9	off
Port10	off
Port11	off
Port12	off

- This section allows users to review the status of ports and MAC limits.

3.4.3 802.1X CONFIGURATION

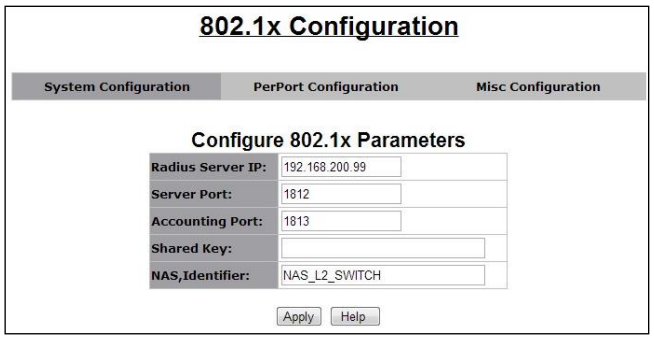


802.1x makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

The default 802.1x setup is disabled, hence, users will not be able to see "802.1x Configuration" page as showed above. To enable 802.1x, go to "Administration → Switch setting → Misc Configs" page to enable the 802.1x protocol field. After enable the function, the 802.1x configuration page will be shown up.

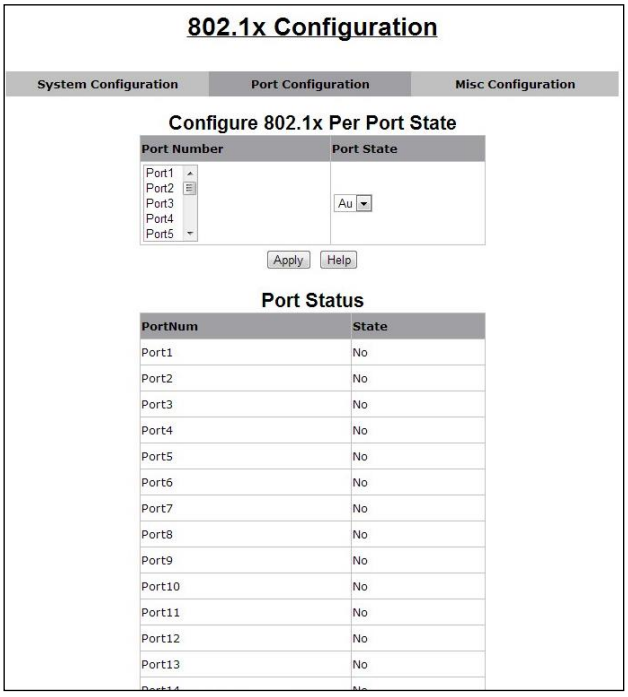
Three sections are in 802.1x configuration function:

- **System Configuration**



- Radius Server IP: the IP address of the authentication server.
- Server Port: the UDP port number used by the authentication server to authenticate (default: 1812).
- Accounting Port: the UDP port number used by the authentication server to retrieve accounting information (default: 1813).
- Shared Key: the password between the switch and the authentication server.
- NAS, Identifier: the name of this switch.

- **PerPort Configuration**

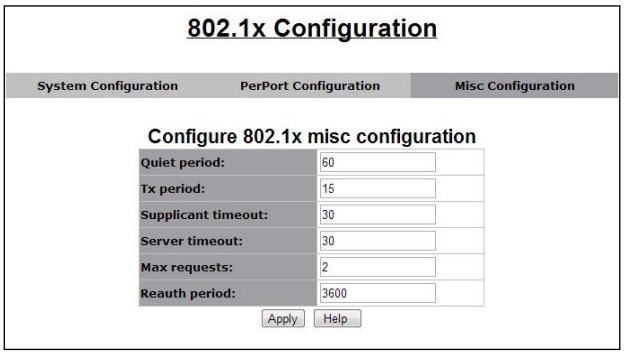


"PerPort Configuration" allows users to setup the authorization mode of 802.1x for each port and review the authorization status of each port.

The VDSL2 IP DSLAM allows users to setup four authorization modes:

- FU: force the specific port to be unauthorized.
- FA: force the specific port to be authorized.
- AU: the state of the selected port was determined by the outcome of the authentication.
- NO: the selected port didn't support 802.1x function.

- **Misc Configuration**



"Misc Configuratioin" page allows users to change miscellaneous setups of 802.1x function.

- Quiet Period: Used to define periods of time during which it will not attempt to acquire a supplicant (default time: 60 seconds).
- Tx Period: Used to determine when an EAPOL PDU is to be transmitted (Default value is 30 seconds).
- Supplicant Timeout: Used to determine timeout conditions in the exchanges between the supplicant and authentication server (default value: 30 seconds).
- Server Timeout: Used to determine timeout conditions in the exchanges between the authenticator and authentication server (default value: 30 seconds).

- ReAuthMax: Used to determine the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (default value: 2 times).
- Reauth Period: Used to determine a nonzero number of seconds between periodic re-authentication of the supplications (default value: 3600 seconds).

3.5 QOS

This switch provides quality of service (QoS) to prioritize the packet forwarding when traffic congestion happens. This switch supports two QoS functions: port-based (4-level output queue) and 802.1p (8-level priority to 4-level queue mapping). In addition, Strict and weight Round Robin (WRR) QoS modes are supported.

3.5.1 QOS CONFIGURATION

"QoS Configuration" page includes two sections as the followings:

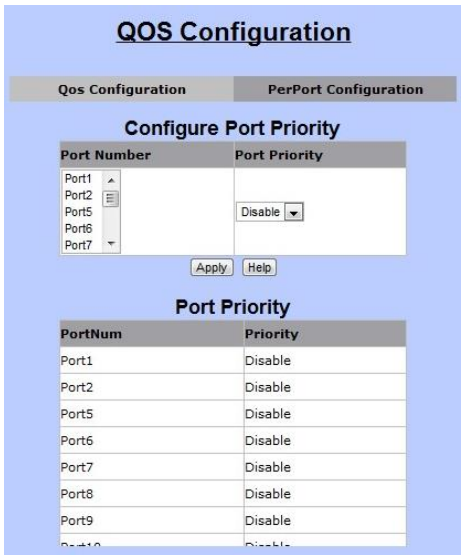
- QoS Configuration

Three QoS modes are supported in this switch:

- First Come First Service
  - The sequence of packets sent is depending on arrive orders. This mode can be regarded as QoS is disabled.
- All High before Low
  - The high priority packets sent before low priority packets.
- WRR
  - Weighted Round Robin. Select the preference given to packets in the switch's high-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent.
  - For example, 8 Highest：4 second-high means that the switch sends 8 highest-priority packets before sending 4 second-high priority packets.

- 802.1p priority
  - The switch supports 8 802.1p priority queues with 4 priority levels (Highest, Second-High, Second-Low, and Lowest). This section is for setting up the maps of priority queues and priority levels.

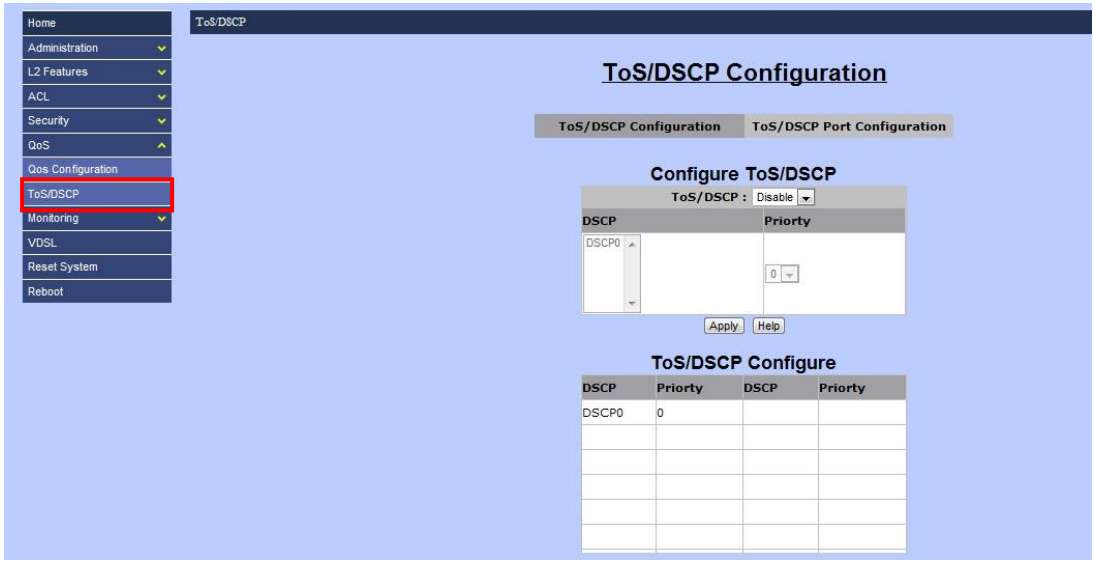
- PerPort Configuration



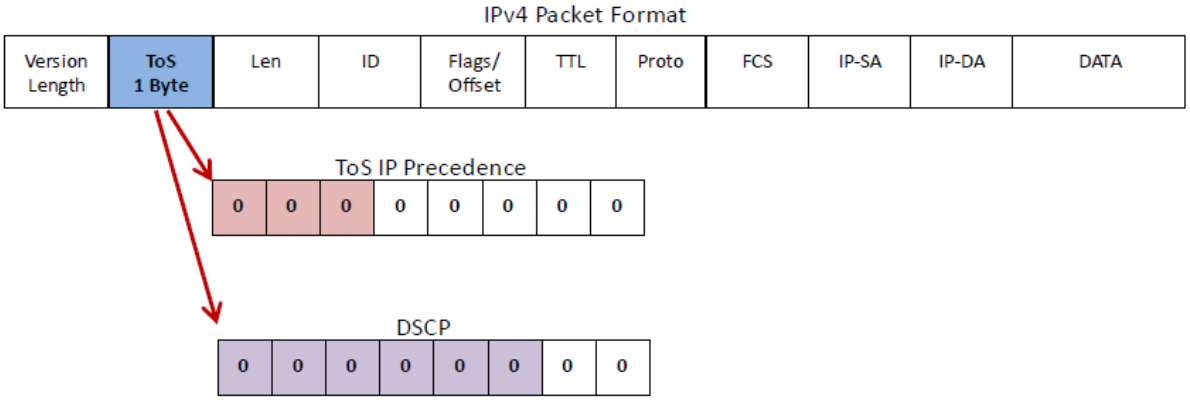
"PerPort Configuration" section allows users to setup the priority level for each port. Users are able to setup QoS algorithm with Port-Based algorithm in this page.

- Port Priority:
  - Options: Disable, 0 ~ 7.
  -

3.5.2 TOS/DSCP



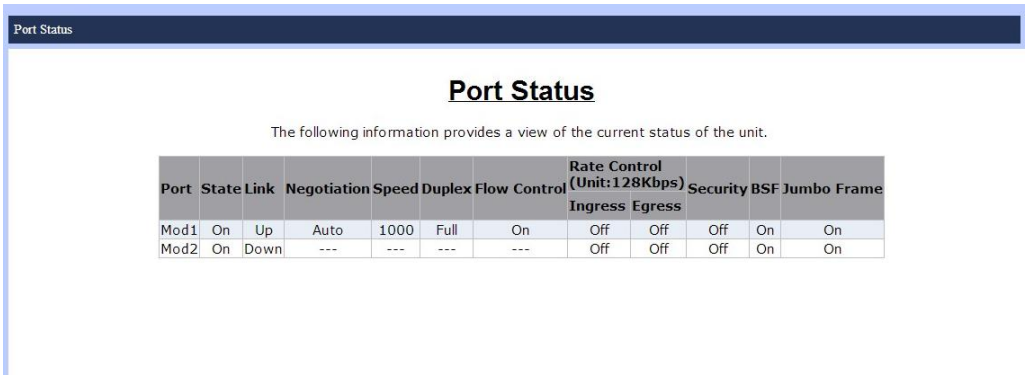
"ToS/DSCP" page is where users can set up priority algorithm for each queue and packets. In IPv4 packet header, there is a ToS byte. "ToS" stands for "Type of Service", and ToS algorithm uses first 3 bits for priority level. However, for DSCP algorithm, it will take first 6 bits for priority level.



3.6 MONITORING

"Monitoring" function is for users to review current status and statistics of each port (Port1 ~ Port24, Mod1 and Mod2).

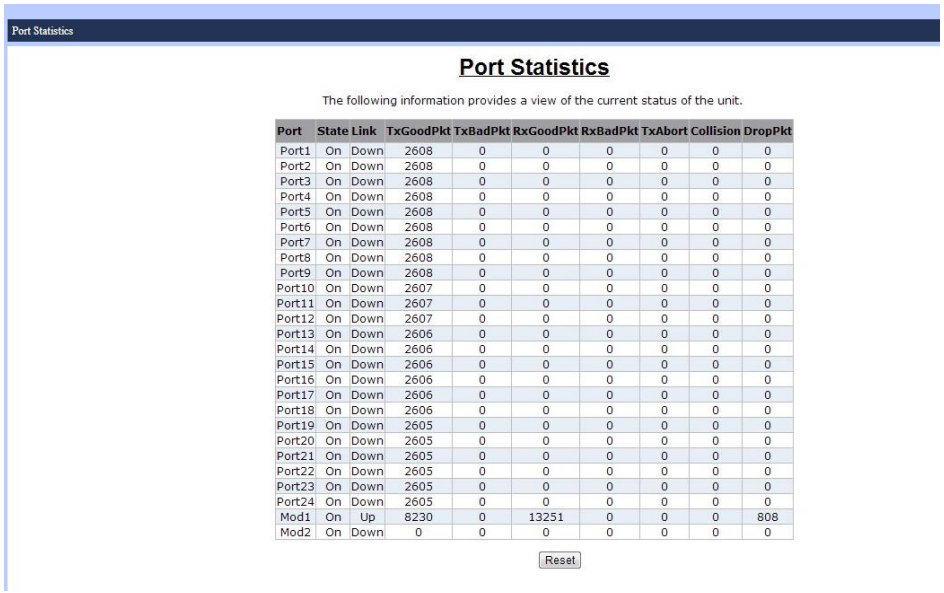
3.6.1 PORT STATUS



"Port Status" displays current status of linked ports. This page is for review only. The information will be showed are as the followings.

Item	Data
Port	Port No.
State	On (Only linked port will be showed)
Link	Up / Down
Negotiation	Auto / Force
Speed	10 / 100 Mbps (Port1 ~ Port24) 10 / 100 / 1000 Mbps (Mod1 ~ Mod2)
Duplex	Full / Half
Rate Control (both Ingress and Egress)	On / Off
Security	On / Off
BSF	On / Off
Jumbo Frame	On / Off

3.6.2 PORT STATISTICS



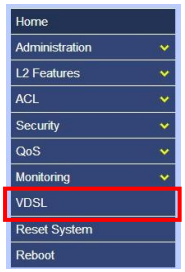
Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
Port1	On	Down	2608	0	0	0	0	0	0
Port2	On	Down	2608	0	0	0	0	0	0
Port3	On	Down	2608	0	0	0	0	0	0
Port4	On	Down	2608	0	0	0	0	0	0
Port5	On	Down	2608	0	0	0	0	0	0
Port6	On	Down	2608	0	0	0	0	0	0
Port7	On	Down	2608	0	0	0	0	0	0
Port8	On	Down	2608	0	0	0	0	0	0
Port9	On	Down	2608	0	0	0	0	0	0
Port10	On	Down	2607	0	0	0	0	0	0
Port11	On	Down	2607	0	0	0	0	0	0
Port12	On	Down	2607	0	0	0	0	0	0
Port13	On	Down	2606	0	0	0	0	0	0
Port14	On	Down	2606	0	0	0	0	0	0
Port15	On	Down	2606	0	0	0	0	0	0
Port16	On	Down	2606	0	0	0	0	0	0
Port17	On	Down	2606	0	0	0	0	0	0
Port18	On	Down	2606	0	0	0	0	0	0
Port19	On	Down	2605	0	0	0	0	0	0
Port20	On	Down	2605	0	0	0	0	0	0
Port21	On	Down	2605	0	0	0	0	0	0
Port22	On	Down	2605	0	0	0	0	0	0
Port23	On	Down	2605	0	0	0	0	0	0
Port24	On	Down	2605	0	0	0	0	0	0
Mod1	On	Up	8230	0	13251	0	0	0	808
Mod2	On	Down	0	0	0	0	0	0	0

"Port Statistics" allows users to review the statistics data of each port with the following details.

Item	Data
Port	Port No
State	On / Down
Link	On / Down
TxGoodPkt	The total bytes of good packets which were transmitted
TxBadPkt	The total bytes of bad packets which were transmitted
RxGoodPkt	The total bytes of good packets which were received
RxBadPkt	The total bytes of bad packets which were received
TxAbort	The total bytes of packets which were aborted.
Collision	Collision

DropPkt	The total bytes of packets dropped

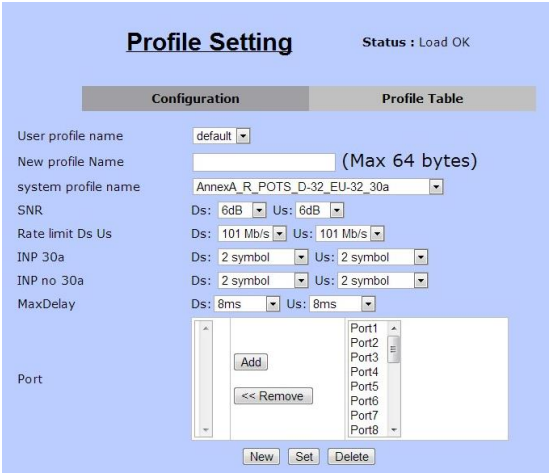
3.7 VDSL



"VDSL" page is where users are able to setup and review VDSL profiles. Two sections are included in VDSL page:

- Configuration
- Profile Table

3.7.1 CONFIGURATION

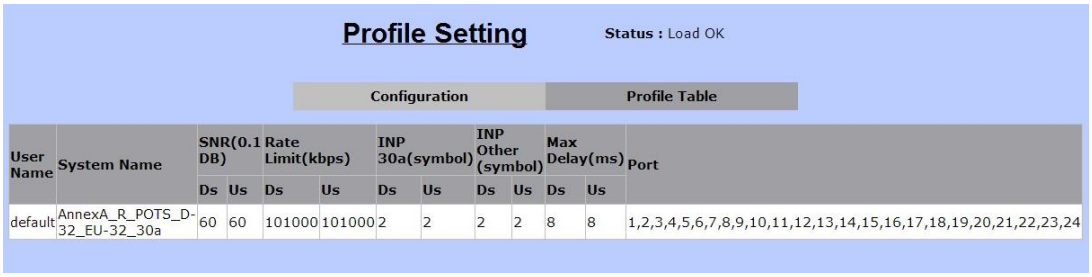


"Configuration" is where users set up VDSL profiles and store these profiles into the system. The followings are the details of each VDSL profile users can set up.

Item	Description
User Profile Name	The name of user-defined profile. Note: There are 21 pre-defined profiles. These names are not changeable. Users are allowed to save new profiles with "New" button.
New Profile Name	New profile name (up to 64 bytes)
System Profile Name	This option is for setting up VDSL band profile. Different profile results in different connection status of data rate and distance. 1. AnnexA_R_POTS_D-64_EU-64_30a 2. AnnexA_R_POTS_D-32_EU-32_17a 3. AnnexA_R_POTS_D-32_EU-32_12b 4. AnnexA_R_POTS_D-32_EU-32_12a 5. AnnexA_R_POTS_D-32_EU-32_8a 6. AnnexA_R_POTS_D-32_EU-32_8b 7. AnnexA_R_POTS_D-32_EU-32_8c 8. AnnexA_R_POTS_D-32_EU-32_8d 9. AnnexA_R_POTS_D-32_EU-64_30a_NUS0 10. AnnexA_R_POTS_D-32_EU-64_17a 11. AnnexB_B7-1_997-M1c-A-7 12. AnnexB_B7-2_997-M1x-M-8 13. AnnexB_B7-3_997-M1x-M 14. AnnexB_B7-4_997-M2x-M-8 15. AnnexB_B7-5_997-M2x-A 16. AnnexB_B7-6_997-M2x-M 17. AnnexB_B7-9_997E17-M2x-A 18. AnnexB_B7-10_997E30-M2x-NUS0 19. AnnexB_B8-1_998-M1x-A

	20. AnnexB_B8-1_998-M1x-B 21. AnnexB_B8-4_998-M2x-A 22. AnnexB_B8-5_998-M2x-M 23. AnnexB_B8-6_998-M2x-B 24. AnnexB_B8-8_998E17-M2x-NUS0 25. AnnexB_B8-9_998E17-M2x-NUS0-M 26. AnnexB_B8-10_998ADE17-M2x-NUS0-M 27. AnnexB_B8-11_998ADE17-M2x-A 28. AnnexB_B8-12_998ADE17-M2x-B 29. AnnexB_B8-13_998E30-M2x-NUS0 30. AnnexB_B8-14_998E30-M2x-NUS0-M 31. AnnexB_B8-15-998ADE30-M2x-NUS0-M 32. AnnexB_B8-16-998ADE30-M2x-NUS0-A 33. AnnexC_POTS_25-138_b 34. AnnexC_POTS_25-276_b 35. AnnexC_TCM_ISDN
SNR	SNR values for both downstream and upstream (6dB ~ 24dB)
Rate Limit Ds Us	The data rates for both downstream and upstream
INP 30a	INP levels for VDSL2 profile 30a for both downstream and upstream
INP no 30a	INP levels for other VDSL2 profiles (8a, 8b, 8c, 8d, 12a, 12b, and 17a) for both downstream and upstream
Max Delay	The maximum delay time for both downstream and upstream Options: No limit, No delay, 1ms ~ 63ms
Port	For assigning which ports should be applied the profile to.

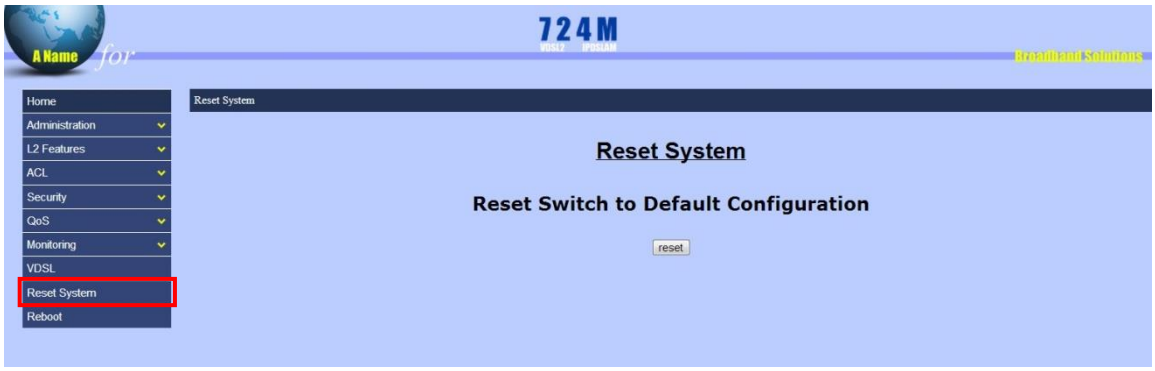
3.7.2 PROFILE TABLE



"Profile Table" is for users to review the details of existing profiles in the following details.

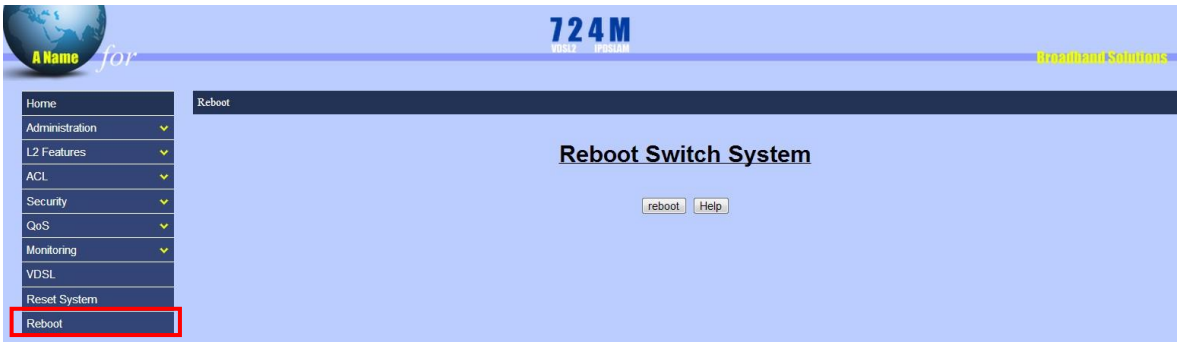
User Name	The profile name
System Name	VDSL2 Band profile
SNR (Ds / Us)	SNR value
Rate Limit (Ds / Us)	The data rate
INP 30a (Ds / Us)	INP level for VDSL2 profile 30a
INP Other (Ds / Us)	INP level for the other VDSL2 profiles
Max Delay	Maximum delay
Port	The port members of this profile

3.8 RESET SYSTEM



"Reset System" is for restoring all configurations back to the default factory configurations. All the settings will be changed back to the original state.

3.9 REBOOT



"Reboot" allows users to reboot the switch without turning off the power.

CHAPTER 4 CONFIGURATION VIA CONSOLE

The VDSL2 IP DSLAM support Command Line Interface for users to access the switch without opening any web browser. It is easily accessible for users with any terminal emulation program, such as, Hyperterminal, or teraterm, etc.

CHAPTER 5 COMMAND LINE INTERFACE

5.1 OPERATION NOTICE

To enter the "configuration" mode, you need to be in the privileged mode, and then type the command configure

Switch# configure

Switch (config) #

The followings are the available configurations of the switch.

exit	Exit current mode and change to the previous mode
logout	Log out the system
help	Show the description of a command
history	Set the number of history commands
no	Negate a command or set its defaults
show	Show running system information
hostname	Set up the switch's network name
disable	Turn off privileged mode (disable configuration mode)
password	Password information
timeout	Set up the timeout for the current CLI
syslog-server	Set up the information of syslog server
broadcast	Set up Broadcast storm filter mode
collision-retry	Set up the settings of collision-retry function
mac-age-time	Enable MAC address age-out function
mac-hash	Set up MAC hash algorithm
mirror-port	Port monitoring information
qos	QoS information
tosport	ToS/DSCP port status information
tosdscp	ToS/DSCP information
clear	Clear values in destination protocol
mac-address-table	MAC address table information
smac-address-table	MAC address table information
filter	Filter destination MAC address information

mac-limit	MAC limit
port	Port information
boot	Reboot the switch
copy	Copy configurations
dhcp	DHCP information
erase	Erase configuration
ip	IP information
ping	Send ICMP ECHO_REQUEST to network hosts
dhcp-option82	Enable DHCP option 82 feature
dhcp-relay	Enable DHCP relay feature
qinq	QinQ information
trunk	Trunking information
vlan	VLAN information
dot1x	802.1x information
radius-server	Radius server information
garp	GARP information
gvrp	GVRP information
igmp	IGMP information
lacp	LACP information
snmp	SNMP information
sntp	Start SNTP service
spanning-tree	Spanning Tree Protocol
acl	ACL information
enable	Enable privileged command mode
bind	Enable SIP/SMAC binding
dslcli	Run DSL CLI
interface	Commands for interfaces
profiles	Commands for profiles
util	Commands for VDSL utility

5.1.1 COMMAND LINE EDITING

Keys Function

Keys	Function
<Ctrl>-B; ←	Moves the cursor back one character.
<Ctrl>-D	Deletes the character at the cursor.
<Ctrl>-E	Jumps to the end of the current command
<Ctrl>-F; →	Moves the cursor forward one character.
<Ctrl>-K	Deletes from the cursor to the end of the
<Ctrl>-N; ↓	Enters the next command line in the
<Ctrl>-P; ↑	Enters the previous command line in the
<Ctrl>-U	Deletes from the cursor to the beginning of
<Ctrl>-W	Deletes the last word typed.
<Esc> B	Moves the cursor backward one word.
<Esc> D	Deletes from the cursor to the end of the
<Esc> F	Moves the cursor forward one word.
<Backspace>	Delete the character before the cursor.
<Del>	Delete the character at the cursor.

5.1.2 COMMAND HELP

You may enter ? at any command mode, and the CLI will return possible commands at that point

You may use the <Tab> key to do keyword auto completion:

Switch (config) # copy tftp r<Tab>

Switch (config) # copy tftp running-config

You do not need to type in the entire commands; you only need to type in enough characters for the CLI to recognize the command as unique.

5.2 SYSTEM COMMANDS

show running-config

Show the running configuration of the switch.

copy running-config startup-config

Backup the configurations of the switch.

erase startup-config

Reset to default factory configurations at the following boot time.

clear arp [ip-address]

Clear entries in the ARP cache in the selected IP address.

show arp

Show IP ARP translation table.

ping ip-addr [<1…999>]

Send ICMP ECHO_REQUEST to the selected IP address.

<1…999>: the number of repetitions. If there is no value in this area, it will continuously ping until users press <Ctrl>+C to stop.

no per-vlan-flooding-portmask

Enable or disable per VLAN default flooding port mask.

per-vlan-flooding-portmask <unicast | multicast> <vlan-id> <port-list>

Set unicast or multicast per VLAN default flooding port mask.

show per-vlan-flooding-portmask

Display unicast and multicast per VLAN default flooding port mask table.

5.3 SWITCH STATIC CONFIGURATION

port state <on | off> [<port-list>]

Turn on or turn off the port state.

<port-list>: specifies the ports to be turn on or off. If no <port-list> value, all ports will be turn on or turn off.

port nego <force | auto > [<port-list>]

Set port negotiation mode.

<port-list>: specifies the ports to be set. If no value, all port will be set.

port speed <10 | 100 | 1000> <full | half> [<port-list>]

Set port speed (mbps) and duplex.

<port-list>: specifies the ports to be set. If no value, all port will be set.

port flow <enable | disable> <enable | disable> [<port-list>]

Enable or disable port flow control.

1st <enable | disable>: enables or disables flow control in full duplex mode.

2nd <enable | disable>: enables or disables flow control in half duplex mode.

<port-list>: specifies the ports to be set. If not entered, all ports are set.

port rate <ingress | egress> <0..8000> [<port-list>]

Set port effective ingress or egress rate.

<0...8000>: specifies the ingress or egress rate. (0…8000)

<port-list>: specifies the ports to be set. If not entered, all ports are set.

port security <on | off> [<port-list>]

Set port priority. When port security is on, the port will stop MAC address learning, and forward only packets with MAC address in the static MAC address table.

<port-list> specifies the ports to be set. If not entered, all ports are set.

port protected group <1-2> <port-list>

Set protected port group member.

<port-list> specifies the group member ports.

port protected <port-list>

Set protected port list.

<port-list> specifies the protected port list.

port priority <disable | low | high> [<port-list>]

Set port priority.

<port-list> specifies the ports to be set. If not entered, all ports are set.

port jumboframe <enable | disable> [<port-list>]

Set port jumbo frame. When port jumbo frame is enable, the port forward jumbo frame packet

<port-list> specifies the ports to be set. If not entered, all ports are set.

port interval <0-3600>:

While flooding CPU port at the speed of 4MB/s or larger, system will close relative port. And system will open this port using this interval value.0 represents system will never enable this after close it for flooding CPU.

show port status

Show port status, including port State, Link, Trunking,VLAN,Negotiation,Speed,Duplex,Flow control, Rate control ,Priority,Security,BSF control.

show port statistics <port-id>

Show port statistics, including TxGoodPkt, TxBadPkt, RxGoodPkt, RxBadPkt,TxAbort, Collision, and DropPkt.

<port-id> specifies the port to be shown.

show port protection

Show protected port information.

5.4 TRUNK CONFIGURATION

Trunk allows the switch to combine ports. It can be used to increase the bandwidth to some devices to provide a high-speed link. Trunk can also provide a redundant link for fault tolerance. If one link in the trunk failed, the switch can balance the traffic among the remaining links.

5.4.1 TRUNKING COMMANDS

show trunk

Show trunking information.

trunk add <trunk-id> <lacp | no-lacp> <port-list> <active-port-list>

Add a new trunk group.

<trunk-id> specifies the trunk group to be added.

<lacp> specifies the added trunk group to be LACP enabled.

<no-lacp> specifies the added trunk group to be LACP disabled.

<port-list> specifies the ports to be set.

<active-port-list> specifies the ports to be set to LACP active.

no trunk <trunk-id>

Delete an existing trunk group.

<trunk-id> specifies the trunk group to be deleted.

5.4.2 LACP COMMANDS

[no] lacp

Enable/disable LACP.

lacp system-priority <1..65535>

Set LACP system priority.

Parameters:

<1..65535> specifies the LACP system priority.

no lacp system-priority

Set LACP system priority to the default value 32768.

show lacp status

Show LACP enable/disable status and system priority.

show lacp

Show LACP information.

show lacp agg <trunk-id>

Show LACP aggregator information.

<trunk-id> specifies the trunk group to be shown.

show lacp port <port-id>

Show LACP information by port.

<port-id> specifies the port to be shown.

If VLAN group exist, all of the members of static trunk group must be in same VLAN group.

5.5 VLAN CONFIGURATION

5.5.1 VIRTUAL LANS

A Virtual Local Area Network is a group of devices that function as a single Local Area Network segment (broadcast domain). The devices that make up a particular VLAN may be widely separated, both by geography and location in the network.

The creation of VLANs allows users located in separate areas or connected to separate ports to belong to a single VLAN group. Users that are assigned to such a group will send and receive broadcast and multicast traffic as though they were all connected to a single network segment.

VLAN aware switches isolate broadcast and multicast traffic received from VLAN groups, keeping broadcasts from stations in a VLAN confined to that VLAN.

When stations are assigned to a VLAN, the performance of their network connection is not changed. Stations connected to switched ports do not sacrifice the performance of the dedicated switched link to participate in the VLAN. As a VLAN is not a physical location, but a membership, the network switches determine VLAN membership by associating a VLAN with a particular port.

Higher-end switches allow the functionality and implementation of VLANs. The purpose of implementing a VLAN is to improve the performance of a network or apply appropriate security features.

The switch supports two types of the VLANS, only one of two VLAN types can be enable at one time

- Port-based VLAN
- IEEE 802.1Q (tag)-based

- VLAN Mode: Port based

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

- VLAN Mode: 802.1Q

If a trunk group exists, you can see it (e.g. TRUNK1, TRUNK2…) after port 8. And, you can configure it to be a member of the VLAN group. In the setting, port was set to Untagged if devices underneath this port do not support VLAN-tagging. Thus the switch can send untagged frames to this port. Consequently, device that do not support VLAN-tagging or do not enable VLAN tagging could successfully fetch the incoming frames and could communicate with device that transfers tagged frames, and vice versa.

- Advanced 802.1Q VLAN Setting

Ingress filters configuration when a packet was received on a port, you can govern the switch to drop it or not if it is an untagged packet. Furthermore, if the received packet is tagged but not belonging to the same VALN group of the receiving port, you can also control the switch to forward or drop the packet. The example below configures the switch to drop the packets not belonging to the same VLAN group and forward the packets not containing VLAN tags.

You can delete the default VLAN group in 802.1Q VLAN mode

show vlan mode

Display the current VLAN mode.

vlan mode (disabled|port-based|dot1q)

Change VLAN mode.

(disabled|port-based|dot1q) specifies the VLAN mode.

Change the VLAN mode for every time, user have to restart the switch for valid value.

show vlan mode

Display the current VLAN mode.

vlan mode (disabled|port-based|dot1q)

Change VLAN mode.

Parameters:

(disabled|port-based|dot1q) specifies the VLAN mode.

Change the VLAN mode for every time, user have to restart the switch for valid value.

vlan add <1-4094> <NAME> <cpu-port|no-cpu-port> <LIST> [<LIST>]

Add or edit VLAN entry.

<1-4094> specifies the VLAN id or Group id (if port based VLAN mode)

<NAME> specifies the VLAN group name.

<cpu-port|no-cpu-port> specifies the CPU port belong this VLAN group.

1st <LIST> specifies the ports to be set to VLAN members.

2nd [<LIST>] specifies the ports to be set to tagged members. If not entered, all members set to untagged.

e.g. vlan add 1 vlan1 cpu-port 1-4 . This VLAN entry has four members (from port1 to port4) and all members are untagged.

no vlan <1-4094>

Delete VLAN entry.

Parameters:

<1-4094> specifies the VLAN id or group id (if port based VLAN). e.g. no vlan 1

show vlan [<1-4094>]

Show VLAN entry information.

[<1-4094>] specifies the VLAN id, null means all valid entries. e.g. show vlan 1

show vlan static

Show static VLAN entry information.

vlan pvid <LIST> <1-4094>

Set port default VLAN id.

<LIST> specifies the ports to be set.

<1-4094> specifies the port VLAN id.

show vlan pvid [<LIST>]

Show port default VLAN id.

Parameters:

[<LIST>] specifies the ports to be showed. If not entered, all port's PVID will be showed.

vlan filter <enable|disable> <enable|disable> <LIST>

Set ingress filter rules.

1st <enable|disable> specifies the non-members packet will be forwarded or not. If set enable, forward only packets with VID matching this port's configured VID.

2nd <enable|disable> specifies the untagged frame will be dropped or not. If set enable, drop untagged frame.

<LIST> specifies the port or trunk list (eg. 3, 6-8, Trk2)

show vlan filter [<LIST>]

Show VLAN filter setting.

[<LIST>] specifies the ports to be showed. If not entered, all ports' filter rules will be showed.

5.6 GVRP COMMANDS

[no] gvrp

Enable or disable GVRP.

show gvrp status

Show GVRP enable or disable status.

[no] port gvrp <LIST>

Enable or disable GVRP by port.

<LIST> specifies the port or trunk list to be set.

show port gvrp

Show GVRP status by port.

garp timer <join | leave | leave-all> <0..65535>

Set GARP timer.

<join | leave | leave-all> specifies a timer (Join, Leave, or Leave-All) to be set

<0..65535> specifies the timer in seconds.

show garp timer

Show GARP timer.

show gvrp db

Show GVRP DB.

show gvrp gip

Show GVRP GIP.

show gvrp machine

Show GVRP machine.

clear gvrp statistics <LIST>

Clear GVRP statistics by port.

<LIST> specifies the port or trunk list to be set

show gvrp statistics <LIST>

Show GVRP statistics by port.

<LIST> specifies the port or trunk list to be set

5.7 QINQ COMMANDS

qinq enable

Enable QinQ.

[no] qinq

Disable QinQ.

qinq tpid <TPIDVAL>

Set QinQ tpid.

<TPIDVAL> specifies QinQ tpid value (Hex, 1~FFFF)

qinq userport <enable|disable> <LIST>

A port configured to support client end of QinQ tunnel is called a QinQ user-port. Use this command to enable/disable QinQ user port to specified port(s).

qinq uplinkport <enable|disable> <LIST>

A port configured to support network end of QinQ tunnel is called a QinQ uplink-port. Use this command to enable/disabel QinQ uplinkport to specified port(s).

qinq tunnel add <1-9> <1-4094> <LIST>

Add QINQ tunnel.

<1-9> specifies the tunnel ID

<1-4094> specifies the VLAN ID

<LIST> specifies the ports to be set to QINQ tunnel.

qinq tunnel delete <1-9>

Delete QinQ tunnel.

<1-9> specifies the tunnel ID

show qinq configuration

Show QinQ global and portal configuration

show qinq tunnel

Show QinQ tunnel information

5.8 MISC CONFIGURATION

[no] mac-age-time

Enable or disable MAC address age-out.

mac-age-time <6..1572858>

Set MAC address age-out time.

<6..1572858> specifies the MAC address age-out time. The value must be divisible by 6. Type the number of seconds that an inactive MAC address remains in the switch's address table

show mac-age-time

Show MAC address age-out time

broadcast mode <off | 1/2 | 1/4 | 1/8 | 1/16>

Set broadcast storm filter mode to off, 1/2, 1/4, 1/8, 1/16

broadcast select <unicast/multicast | control packet | ip multicast | broadcast>

Select the Broadcast storm filter packet type:

- Unicast/Multicast: Flood unicast/multicast filter
- Control Packets: Control packets filter
- IP multicast: Ip multicast packets filter
- Broadcast Packets: Broadcast Packets filter
-

Collision-Retry <off | 16 | 32 | 48>

Parameters:

<off|16|32|48> In half duplex, collision-retry maximum is 16, 32 or 48 times and packet will be dropped if collisions still happen. In default (off), if collision happens, it will retry forever.

Hash <crc-hash | direct-map>

Set hash algorithm to CRC-Hash or DirectMap.

5.9 ADMINISTRATION CONFIGURATION

hostname <name-str>

Set switch name.

<name-str> specifies the switch name. If you would like to have spaces within the name, use quotes (“”) around the name.

no hostname: Reset the switch name to factory default setting.

[no] password <manager | operator | all>

Set or remove username and password for manager or operator. The manager username and password is also used by the web UI.

ip address <ip-addr> <ip-mask>

Set IP address and subnet mask.

ip default-gateway <ip-addr>

Set the default gateway IP address.

show ip

Show IP address, subnet mask, and the default gateway.

show info

Show basic information, including system info, MAC address, and firmware version.

dhcp

Set switch as dhcp client, it can get ip from dhcp server

If this command is set, the switch will reboot.

show dhcp

show dhcp enable/disable

5.10 PORT MIRRORING CONFIGURATION

Port monitoring is a feature to redirect the traffic occurred on every port to a designated monitoring port on the switch. With this feature, the network administrator can monitor and analyze the traffic on the entire LAN segment. In the switch, you can specify one port to be the monitoring port and any single port to be the monitored port. You also can specify the direction of the traffic that you want to monitor. After properly configured, packets with the specified direction from the monitored ports are forwarded to the monitoring port.

mirror-port <rx | tx | both> <port-id> <port-list> Set port monitoring information. (RX only|TX only|both RX and TX)

rx specifies monitoring rx only.

tx specifies monitoring tx only.

both specifies monitoring both rx and tx.

<port-id> specifies the analysis port ID. This port receives traffic from all monitored ports.

<port-list> specifies the monitored port list.

show mirror-port

Show port monitoring information

5.11 QUALITY OF SERVICE

QoS (Quality of Service) refers to a broad collection of networking technologies and techniques. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results. Elements of network performance within the scope of QoS often include availability (uptime), bandwidth (throughput), latency (delay), and error rate.

QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications. A network monitoring system must typically be deployed as part of QoS, to insure that networks are performing at the desired level.

- **QoS Mode:**

- **First Come First Service**: The sequence of packets sent is depending on arrive orders.

- **All High before Low**: The high priority packets sent before low priority packets.

- **WRR**: Weighted Round Robin. Select the preference given to packets in the switch's high-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest：4 second-high means that the switch sends 8 highest-priority packets before sending 4 second high priority packets.

-

- **Qos Level**: 0~7 priority level can map to highest, second-high, second-low, lowest queue.

qos priority <first-come-first-service | all-high-before-low |weighted-round-robin> [<highest-weight>][<sechighweight>][<sec low -weight>] [<lowest-weight>]

Set 802.1q priority.

e.g. qos priority weighted-round-robin 8,4,2,1

qos level < highest | second-high | second-low | lowest > <level-list>

Set priority levels to highest, second-high, second-low and lowest.

<level-list> specifies the priority levels to be high or low. Level must be between 1 and 7.

e.g. qos level highest 7

e.g. qos level lowest 4

show qos

Show QoS configurations, including 802.1p priority, priority level.

e.g. show qos

QoS configurations:

QoS mode: first come first service

Highest weight: 8

Second High weight: 4

Second Low weight: 2

Lowest weight: 1

802.1p priority [0-7]:

Lowest Lowest SecLow SecLow SecHigh SecHigh Highest Highest

- **Per Port Priority**

port priority <disable | [0-7]> [<port-list>]

Set port priority.

[<port-list>] specifies the ports to be set. If not entered, all ports are set.

e.g. port priority disable 1-5

5.12 MAC ADDRESS CONFIGURATION

5.12.1 COMMANDS FOR MAC

clear mac-address-table

Clear all dynamic MAC address table entries.

mac-address-table static <mac-addr> <vlan-id> <port-id | port-list>

Set static unicast or multicast MAC address. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be port-list. Otherwise, it must be port-id.

no mac-address-table static <mac-addr> <vlan-id>

Delete static unicast or multicast MAC address table entries.

show mac-address-table

Display MAC address table entries.

show mac-address table static

Display static MAC address table entries.

show mac-address-table multicast

Display multicast related MAC address table.

smac-address-table static <mac-addr> <vlan-id> <port-id | port-list>

Set static unicast or multicast MAC address in secondary MAC address table. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be port-list. Otherwise, it must be port-id.

show smac-address-table

Display secondary MAC address table entries.

show smac-address-table multicast

Display multicast related secondary MAC address table.

[no] filter <mac-addr> <vlan-id>

Set MAC address filter. The packets will be filtered if both of the destination MAC address and the VLAN tag match the filter entry. If the packet does not have a VLAN tag, then it matches an entry with VLAN ID 1.

show filter

Display filter MAC address table.

5.12.2 MAC LIMITS

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an "opening" is available, the switch stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked. User can configure the MAC limit setting and fill in the new value.

mac-limit

Enable MAC limit.

no mac-limit

Disable MAC limit.

Mac-limit <port-list> <1-64>

Set port MAC limit value, 0 to turn off MAC limit of port.

show mac-limit

Show MAC limit information, including MAC limit enable/disable, per-port MAC limit setting.

5.13 PROTOCOL RELATED COMMENDS

5.13.1 STP/RSTP

[no] spanning-tree

Enable or disable spanning-tree.

spanning-tree forward-delay <*4-30*>

Set spanning tree forward delay used, in seconds.

<*4-30*> specifies the forward delay, in seconds. Default value is 15.

The parameters must enforce the following relationships:

2(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)*

spanning-tree hello-time <*1-10*>

Set spanning tree hello time, in seconds.

<*1-10*> specifies the hello time, in seconds. Default value is 2.

The parameters must enforce the following relationships:

2(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)*

spanning-tree maximum-age <*6-40*>

Set spanning tree maximum age, in seconds.

<*6-40*> specifies the maximum age, in seconds. Default value is 20.

The parameters must enforce the following relationships:

2(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)*

spanning-tree priority *<0-61440>*

Set spanning tree bridge priority.

<0-61440> specifies the bridge priority. The value must be in steps of 4096.

spanning-tree port path-cost *<1-200000000>* [*<port-list>*]

Set spanning tree port path cost.

<1-200000000> specifies port path cost.

[*<port-list>*] specifies the ports to be set. Null means all ports.

spanning-tree port priority *<0-240>* [*<port-list>*]

Set spanning tree port priority.

<0-240> specifies the port priority. The value must be in steps of 16.

[*<port-list>*] specifies the ports to be set. Null means all ports.

show spanning-tree

Show spanning-tree information.

show spanning-tree port [*<port-list>*]

Show spanning tree per port information.

[*<port-list>*] specifies the port to be shown. Null means all ports.

The remaining commands in this section are only for system with RSTP (rapid spanning tree, 802.1w) capability:

spanning-tree protocol-version <stp | rstp>

Change spanning tree protocol version.

stp specifies the original spanning tree protocol (STP,802.1d).

rstp specifies rapid spanning tree protocol (RSTP,802.1w).

[no] spanning-tree port mcheck [<port-list>]

Force the port to transmit RST BPDUs. No format means not force the port to transmit RST BPDUs.

[<port-list>] specifies the ports to be set. Null means all ports.

[no] spanning-tree port edge-port [<port-list>]

Set the port to be edge connection. No format means set the port to be non-edge connection.

[<port-list>] specifies the ports to be set. Null means all ports.

[no] spanning-tree port non-stp [<port-list>]

Disable or enable spanning tree protocol on this port.

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree port point-to-point-mac <auto | true | false> [<port-list>]

Set the port to be point to point connection.

auto specifies point to point link auto connection.

true specifies point to point link true.

false specifies point to point link false.

[<port-list>] specifies the ports to be set. Null means all ports.

5.13.2 MSTP

[no] spanning-tree

Enable or disable multiple spanning tree.

spanning-tree forward-delay <4-30>

Set spanning tree forward delay of CIST, in seconds.

<4-30> specifies the forward delay, in seconds. Default value is 15.

The parameters must enforce the following relationships:

2(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)*

spanning-tree hello-time <1-10>

Set spanning tree hello time of CIST, in seconds.

<1-10> specifies the hello time, in seconds. Default value is 2.

The parameters must enforce the following relationships:

2(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)*

spanning-tree maximum-age <6-40>

Set spanning tree maximum age of CIST, in seconds.

<6-40> specifies the maximum age, in seconds. Default value is 20.

The parameters must enforce the following relationships:

2(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)*

spanning-tree priority <0-61440>

Set spanning tree bridge priority of CIST and all MSTIs.

<0-61440> specifies the bridge priority. The value must be in steps of 4096. Default value is 32768.

spanning-tree protocol-version { stp | mstp }

Set spanning tree protocol version of CIST.

stp specifies the original spanning tree protocol (STP,802.1d).

mstp specifies the multiple spanning tree protocol (MSTP,802.1s).

spanning-tree max-hops <1-40>

Set spanning tree bridge maximum hops of CIST and all MSTIs.

<1-40> specifies the bridge maximum hops. Default value is 20.

spanning-tree name [<name-string>]

Set spanning tree bridge name of CIST.

[<name-string>] specifies the bridge name. Default name is null.

spanning-tree revision <1-65535>

Set spanning tree bridge revision of CIST.

<1-65535> specifies the bridge revision. Default value is 0.

spanning-tree port path-cost <1-200000000> [<port-list>]

Set spanning tree port path cost of CIST.

<1-200000000> specifies port path cost.

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree port priority <0-240> [<port-list>]

Set spanning tree port priority of CIST.

<0-240> specifies the port priority. The value must be in steps of 16.

[<port-list>] specifies the ports to be set. Null means all ports.

[no] spanning-tree port mcheck [<port-list>]

Force the port of CIST to transmit MST BPDUs. No format means not force the port of CIST to transmit MST BPDUs.

[<port-list>] specifies the ports to be set. Null means all ports.

[no] spanning-tree port edge-port [<port-list>]

Set the port of CIST to be edge connection. No format means set the port of CIST to be non-edge connection.

[<port-list>] specifies the ports to be set. Null means all ports.

[no] spanning-tree port non-stp [<port-list>]

Disable or enable spanning tree protocol on the CIST port.

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree port point-to-point-mac <auto | true | false> [<port-list>]

Set the port of CIST to be point to point connection.

auto specifies point to point link auto connection.

true specifies point to point link true.

false specifies point to point link false.

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree mst <0-15> priority <0-61440>

Set spanning tree bridge priority of MSTI.

<0-15> specifies the MSTI instance ID.

<0-61440> specifies the MSTI bridge priority. The value must be in steps of 4096. Default value is 32768.

spanning-tree mst <0-15> vlan [<vlan-list>]

Set MSTI to map VLAN list.

<0-15> specifies the MSTI instance ID.

[<vlan-list>] specifies the mapped VLAN list. Null means all VLANs.

spanning-tree mst <0-15> port path-cost <1-200000000> [<port-list>]

Set spanning tree port path cost of MSTI.

<1-200000000> specifies port path cost.

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree mst <0-15> port priority <0-240> [<port-list>]

Set spanning tree port priority of MSTI.

<0-240> specifies the port priority. The value must be in steps of 16.

[<port-list>] specifies the ports to be set. Null means all ports.

no spanning-tree mst <0-15>

Delete the specific MSTI.

<0-15> specifies the MSTI instance ID.

show spanning-tree

Show spanning-tree information of CIST.

show spanning-tree port [<port-list>]

Show spanning tree port information of CIST.

[<port-list>] specifies the port to be shown. Null means all ports.

show spanning-tree mst configuration

Show MST instance map.

show spanning-tree mst <0-15>

Show MST instance information.

<0-15> specifies the MSTI instance ID.

show spanning-tree mst <0-15> port <1-26>

Show specific port information of MST instance.

<0-15> specifies the MSTI instance ID.

<1-26> specifies port number.

show vlan spanning-tree

Show per VLAN per port spanning tree status.

5.14 SNMP

Any Network Management running the simple Network Management Protocol (SNMP) can be management the switch.

snmp /no snmp

Enable or disable SNMP.

show snmp status

Show enable or disable status of SNMP.

snmp system-name <name-str>

Set agent system name string.

<name-str> specifies the system name string.

e.g. snmp system-name SWITCH

snmp system-location <location-str>

Set agent location string.

<location-str> specifies the location string.

e.g. snmp system-location office

snmp system-contact <contact-str>

Set agent system contact string.

<contact-str> specifies the contact string.

e.g. snmp system-contact abc@sina.com

show snmp system

Show SNMP system information.

snmp community <read-sysinfo-only | read-all-only | read-write-all> <community-str>

Set SNMP community string.

<community-str> specifies the community string.

e.g. snmp community read-all-only public

no snmp community <community-str>

Delete SNMP community string.

<community-str> specifies the community string.

e.g. no snmp community public

show snmp community

Show SNMP community strings.

snmp trap <ip-addr> [<community-str>] [<1...65535>]

Set SNMP trap receiver IP address, community string, and port number.

<ip-addr> specifies the IP address.

<community-str> specifies the community string.

<1...65535> specifies the trap receiver port number.

e.g. snmp trap 192.168.200.1 public

no snmp trap <ip-addr> [<1…65535>]

Remove trap receiver IP address and port number.

<ip-addr> specifies the IP address.

<1…65535> specifies the trap receiver port number.

e.g. no snmp trap 192.168.200.1

show snmp trap

Show all trap receivers.

snmp group <group-name> <v1 | v2c | usm> <security-name>

Join a group.

<group-name> specifies the group name.

<v1 | v2c | usm> specifies the security model.

<security-name> specifies the security name.

e.g. snmp group test usm testuser

no snmp group <v1 | v2c | usm> <security-name>

Leave a group.

<v1 | v2c | usm> specifies the security model.

<security-name> specifies the security name.

e.g. no snmp group usm testuser

show snmp group

Show group list.

snmp view <view-name> <included | excluded> <view-subtree> <view-mask>

Add a view.

<view-name> specifies the view name.

<included | excluded> specifies the view type.

<view-subtree> specifies the view subtree (e.g. .1.3.6.1.2.1).

<view-mask> specifies the view mask, in hexadecimal digits.

e.g. snmp view testview included 1.3.6.1.2.1 0xff

no snmp view <view-name>

Delete a view.

<view-name> specifies the view name.

e.g. no snmp view system

show snmp view

Show view list.

snmp access <group-name> <v1 | v2c | usm> <noauth | auth | authpriv> <read-name> <write-name> <notify-name>

Add an access control.

<group-name> specifies the group name.

<v1 | v2c | usm> specifies the security model.

<noauth | auth | authpriv> specifies the security level.

<read-name> specifies the access read view name.

<write-name> specifies the access write view name.

<notify-name> specifies the access notify view name.

e.g. snmp access test usm testauth all all all

no snmp access <group-name> <v1 | v2c | usm> <noauth | auth | authpriv>

Delete an access control.

<group-name> specifies the group name.

<v1 | v2c | usm> specifies the security model.

<noauth | auth | authpriv> specifies the security level.

e.g. no snmp access test usm auth

show snmp access

Show access list.

snmp engine-id <enterprise-id> <engine-id>

Setup SNMPv3 engine ID.

<engine-id> specifies the engine ID, in the format of text string.

e.g. snmp engine-id 123456789123456789123456

show snmp engine-id

Show SNMPv3 engine ID.

snmp usm-user <user-name> [<md5 | none>]

Add SNMPv3 USM user.

<user-name> specifies the user name.

<md5 | none> specifies the authentication type.

e.g. Create a user name is testuser and password is 12345678, use auth md5 then enter CLI command:

snmp usm-user testuser md5 <cr>

New password for authentication (8<=length<=32):

12345678<cr>

Retype new password:

12345678<cr>

no snmp usm-user <user-name>

Delete SNMPv3 USM user.

<user-name> specifies the user name.

e.g. no snmp usm-user testuser

show snmp usm-user

Show all SNMPv3 USM users.

5.15 IGMP

The internet Group Management Protocol (IGMP) is an internal protocol of the IP suite

[no] igmp

Enable/disable IGMP snooping.

[no] igmp fastleave

Enable/disable IGMP snooping fast leave. If enable, switch will fast delete member who send leave report, else wait one second.

[no] igmp querier

Enable/disable IGMP snooping querier.

[no] igmp CrossVLAN

Enable/disable IGMP snooping CrossVLAN

show igmp <status | router | groups | table>

Show IGMP snooping information.

status specifies IGMP snooping status and statistics information.

router specifies IGMP snooping router's IP address.

groups specifies IGMP snooping multicast group list.

table specifies IGMP snooping IP multicast table entries.

igmp clear_statistics

Clear IGMP snooping statistics counters.

5.16 802.1X PROTOCOL

This switch supports IEEE 802.1x standard which provides port-based access control by validating end user's authorization through authentication (RADIUS) server. EAP-MD5/TLS/PEAP authentication types are supported for this switch.

[no] dot1x

Enable or disable 802.1x.

radius-server host <ip-addr> <1024..65535> <1024..65535>

Set radius server IP, port number, and accounting port number.

<ip-addr> specifies server's IP address.

1st <1024..65535> specifies the server port number.

2nd <1024..65535> specifies the accounting port number.

radius-server key <key-str>

Set 802.1x shared key.

<key-str> specifies shared key string.

radius-server nas <id-str>

Set 802.1x NAS identifier.

<id-str> specifies NAS identifier string.

show radius-server

Show radius server information, including radius server IP, port number, accounting port number, shared key, NAS identifier

dot1x timeout quiet-period <0..65535>

Set 802.1x quiet period. (default: 60 seconds).

<0..65535> specifies the quiet period, in seconds.

dot1x timeout tx-period <0..65535>

Set 802.1x Tx period. (default: 15 seconds).

<0..65535> specifies the Tx period, in seconds.

dot1x timeout supplicant <1..300>

Set 802.1x supplicant timeout (default: 30 seconds)

<1..300> specifies the supplicant timeout, in seconds.

dot1x timeout radius-server <1..300>

Set radius server timeout (default: 30 seconds).

<1..300> specifies the radius server timeout, in seconds.

dot1x max-req <1..10>

Set 802.1x maximum request retries (default: 2 times).

<1..10> specifies the maximum request retries.

dot1x timeout re-authperiod <30..65535>

Set 802.1x re-auth period (default: 3600 seconds).

<30..65535> specifies the re-auth period, in seconds.

show dot1x

Show 802.1x information, quiet period, Tx period, supplicant timeout, server timeout, maximum requests, and re-auth period.

dot1x port <fu | fa | au | no> <port-list>

Set 802.1x per port information.

fu specifies forced unauthorized.

fa specifies forced authorized.

au specifies authorization.

no specifies disable authorization.

<port-list> specifies the ports to be set.

show dot1x port

Show 802.1x per port information.

5.17 DHCP RELAY & OPTION 82

[no] dhcp-option82

Enable/disable DHCP option82 function.

[no] dhcp-relay

Enable/disable DHCP relay function.

dhcp-option82 <enable | disable> <LIST>

Enable/disable port-based option82 function.

dhcp-relay <enable | disable> <LIST> <IP address>

Enable/disable port-based DHCP relay function.

dhcp router <LIST>

Set DHCP router port

show dhcp configuration

Show DHCP configuration information

5.18 SYSLOG

syslog-server <server-ip> <logging-level>

Setting the syslog server and loging level.

<server-ip> specifies the syslog server IP

<logging-level> specifies the logging level (0: none; 1: major; 2: all)

show syslog-server

Display the syslog server IP and logging level

5.19 REBOOT SWITCH

- **Reset to Default**

erase startup-config

Reset configurations to default factory settings at next boot time.

- **Restart**

boot

Reboot (warm-start) the switch.

5.20 TFTP FUNCTION

- **TFTP Firmware Update**

copy tftp firmware <ip-addr> <remote-file>

Download firmware from TFTP server.

<ip-addr> specifies the IP address of the TFTP server.

<remote-file> specifies the file to be downloaded from the TFTP server.

- **Restore Configure File**

copy tftp <running-config | flash> <ip-addr> <remote-file>

Retrieve configuration from the TFTP server. If the remote file is the text file of CLI commands, use the keyword running-config. If the remote file is the configuration flash image of the switch instead, use the keyword flash.

<ip-addr> specifies the IP address of the TFTP server.

<remote-file> specifies the file to be downloaded from the TFTP server.

- **Backup Configure File**

copy <running-config | flash> tftp <ip-addr> <remote-file>

Send configuration to the TFTP server. If you want to save the configuration in a text file of CLI commands, use the keyword running-config. If you want to save the configuration flash image instead, use the keyword flash.

<ip-addr> specifies the IP address of the TFTP server.

<remote-file> specifies the file to be backed up to the TFTP server.

5.21 ACCESS CONTROL LIST

Packets can be forwarded or dropped by ACL rules include IPv4 or non-IPv4 packets. This switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

This function is available only in the 802.1q VLAN enabled environment.

- **IPv4 ACL commands**

no acl <group id>

Delete ACL group.

<group id> specifies the group id (1~220).

e.g. no acl 1

no acl count <group id>

Reset the ACL group count

<group id> specifies the group id (1~220).

Enable/Disable acl <group id>

Reset the ACL group count

<group id> specifies the group id (1~220)

Enable/Disable acl <group id>

Reset the ACL group count

<group id> specifies the group id (1~220)

show acl [<group id>]

Show all or ACL group information by group id

<group id> specifies the group id, null means all valid groups.

e.g. show acl 1

Group Id : 1

Action : Permit

Rules:

Vlan ID : Any

IP Fragement : Uncheck

Src IP Address : Any

Dst IP Address : Any

L4 Protocol : Any

Port ID : Any

Hit Octet Count : 165074

Hit Packet count : 472

acl (add|edit) <group id> (permit|deny) <0-4094> ipv4 <0-255> A.B.C.D A.B.C.D A.B.C.D A.B.C.D (check|unCheck) <0- 65535> <0-26>

Add or edit ACL group for IPv4 packets.

(add|edit) specifies the operation.

<group id> specifies the group id (1~220).

(permit|deny) specifies the action. permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN id. 0 means don't care.

<0-255> specifies the IP protocol. 0 means don't care.

1st A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

2nd A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

3rd A.B.C.D specifies the Destination IP Address. 0.0.0.0 means don't care.

4th A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

(check|unCheck) specifies the IP Fragment. check: Check IP fragment field; unCheck: Not check IP fragment field.

<0-65535> specifies the Destination port number if TCP or UDP. 0 means don't care.

<0-26> specifies the Port id. 0 means don't care.

e.g. acl add 1 deny 1 ipv4 0 192.168.1.1 255.255.255.255 0.0.0.0 0.0.0.0 unCheck 0 0

This ACL rule will drop all packet from IP is 192.168.1.1 with VLAN id=1 and IPv4.

acl (add|edit) <group id> (qosvoip) <0-4094> <0-7> <0-1F> <0-1F> <0-FF> <0-FF> <0-FFFF> <0-FFFF> <0-FFFF> <0-FFFF>

Add or edit ACL group for Ipv4.

(add|edit) specifies the operation.

<group id>specifies the group id (1~220).

(qosvoip) specifies the action, do qos voip packet adjustment.

<0-4094> specifies the VLAN id. 0 means don't care.

<0-1F> specifies the port ID value.

<0-1F> specifies the port ID mask.

<0-FF> specifies the protocol value.

<0-FF> specifies the protocol mask.

<0-FFFF> specifies the source port value.

<0-FFFF> specifies the source port mask.

<0-FFFF> specifies the destination port value.

<0-FFFF> specifies the destination mask.

e.g. acl add 1 qosvoip 1 7 1 1 0 0 0 0 0 0

- **Non-IPv4 ACL commands**

no acl <group id> and **show acl** [**<group id>**] commands are the same as in Ipv4 ACL commands.

acl (add|edit) <1-220> (permit|deny) <0-4094> nonipv4 <0-65535>

Add or edit ACL group for non-Ipv4.

(add|edit) specifies the operation.

<group id> specifies the group id (1~220).

(permit|deny) specifies the action. permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN id. 0 means don't care.

<0-65535> specifies the Ether Type. 0 means don't care.

e.g. acl add 1 deny 0 nonipv4 2054

This ACL rule will drop all packets for ether type is 0x0806 and non-IPv4

5.22 BINDING

5.22.1 SIP/SMAC BINDING COMMANDS

Source IP (SIP) / Source MAC (SMAC) address binding is another type of ACL rule to provide secured access to the switch. Only the traffic which matches all criteria of specified source IP address, source MAC address, VLAN ID and port number can be allowed to access to the switch. This function is also called IP-MAC lock.

bind

Enable binding function.

no bind

Disable binding function.

no bind <group id>

Delete Binding group.

<group id> specifies the group id (1~220).

e.g. no bind 1

show bind [<group id >]

Show Binding group information.

<group id> specifies the group id (1~220), null means all valid groups.

e.g. show bind 1

bind add < group id > A:B:C:D:E:F <0-4094> A.B.C.D <1-26>

Add Binding group.

< group id > specifies the group id (1~220).

1st A.B.C.D specifies the MAC address.

<0-4094> specifies the VLAN id. 0 means don't care.

2nd A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

3rd A.B.C.D specifies the IP Address.

<1-26> specifies the Port id.

e.g. bind add 1 00:11:22:33:44:55 0 192.168.1.1 1. This Binding rule will permit all packet cross switch from device’s IP is

192.168.1.1 and MAC is 00:11:22:33:44:55 and this device connect to switch port id=1.

5.23 VDSL2 COMMANDS

5.23.1 VDSL2 INTERFACE COMMANDS

interface xdsl [show l set]

Command for xdsl interfaces

interface xdsl show oid <portid> <oid>

show vdsl logic MIB entry

<1-8> or <1-24> port id

interface xdsl show roid <portid> <oid>

show vdsl real MIB entry

<1-8> or <1-24> port id

interface xdsl status <portid>

show line status

<1-8> or <1-24> port id

interface xdsl show invent <portid>

show inventory of xdsl lines

<1-8> or <1-24> port id

interface xdsl show threshold <portid>

show threshold of xdsl lines

<1-8> or <1-24> port id

interface xdsl show table

show mib tables of xdsl lines

<1-8> or <1-24> port id

profile xdsl-line save

Save all profile configurations

profile xdsl-line init

Initialize profile from save profile

profile xdsl-line set

Set commands for xdsl profile

profile xdsl-line set dsl-bandplan <profile_name> <value>

To enable a predefined set of PSD- mask, PSD level and sub carrier mask dependent on profile and bandplan selection for a VDSL config profile

profile xdsl-line set fix-rate <profile_name> <value>

Specify the profile to use fix rate in bit/s

profile xdsl-line set margin-target-snr-ds <profile_name> <value-dec>

Signal noise ration margin target downstream settings

<0-310>

profile xdsl-line set margin-target-snr-us <profile_name> <value-dec>

Signal noise ration margin target upstream settings

<0-310>

profile xdsl-line set margin-max-snr-ds <profile_name> <value-dec>

Signal noise ration margin max downstream settings

<0-310>

profile xdsl-line set margin-max-snr-us <profile_name> <value-dec>

Signal noise ration margin max upstream settings

<0-310>

profile xdsl-line set margin-min-snr-ds <profile_name> <value-dec>

Signal noise ration margin min downstream settings

<0-310>

profile xdsl-line set margin-min-snr-us <profile_name> <value-dec>

Signal noise ration margin min upstream settings

<0-310>

profile xdsl-line set rate-limit-max-ds-ch1 <profile_name> <value-dec>

Ch1 max data rate on downstream direction settings

<0-200000>kbps

profile xdsl-line set rate-limit-max-us-ch1 <profile_name> <value-dec>

Ch1 max data rate on upstream direction settings

<0-200000>kbps

profile xdsl-line set rate-limit-max-ds-ch2 <profile_name> <value-dec>

Ch2 max data rate on downstream direction settings

<0-200000>kbps

profile xdsl-line set rate-limit-max-us-ch2 <profile_name> <value-dec>

Ch2 max data rate on upstream direction settings

<0-200000>kbps

profile xdsl-line set rate-limit-min-ds-ch1 <profile_name> <value-dec>

Ch1 min data rate on downstream direction settings

<0-200000>kbps

profile xdsl-line set rate-limit-min-us-ch1 <profile_name> <value-dec>

Ch1 min data rate on upstream direction settings

<0-200000>kbps

profile xdsl-line set rate-limit-min-ds-ch2 <profile_name> <value-dec>

Ch2 min data rate on downstream direction settings

<0-200000>kbps

profile xdsl-line set rate-limit-min-us-ch2 <profile_name> <value-dec>

Ch2 min data rate on upstream direction settings

<0-200000>kbps

profile xdsl-line set max-delay-ds-ch1<profile_name> <value-dec>

Ch1 max interleave delay on downstream direction settings

<0-63>ms

profile xdsl-line set max-delay-us-ch1<profile_name> <value-dec>

Ch1 max interleave delay on upstream direction settings

<0-63>ms

profile xdsl-line set inp-min-prot-ds-ch1<profile_name> <value-dec>

Ch1 downstream min impulse noise protection in 4.3125kHz (symbol) settings

<1-18>

profile xdsl-line set inp-min-prot-us-ch1<profile_name> <value-dec>

Ch1 upstream min impulse noise protection in 4.3125kHz (symbol) settings

<1-18>

profile xdsl-line set inp-min-prot-ds-ch1<profile_name> <value-dec>

Ch1 downstream min impulse noise protection in 8.625kHz (symbol) settings

<1-17>

profile xdsl-line set inp-min-prot-us-ch1<profile_name> <value-dec>

Ch1 upstream min impulse noise protection in 8.625kHz (symbol) settings

<1-17>

profile xdsl-line set max-delay-ds-ch2<profile_name> <value-dec>

Ch2 max interleave delay on downstream direction settings

<0-63>ms

profile xdsl-line set max-delay-us-ch2<profile_name> <value-dec>

Ch2 max interleave delay on upstream direction settings

<0-63>ms

profile xdsl-line set inp-min-prot-ds-ch2<profile_name> <value-dec>

Ch2 downstream min impulse noise protection in 4.3125kHz (symbol) settings

<1-18>

profile xdsl-line set inp-min-prot-us-ch2<profile_name> <value-dec>

Ch2 upstream min impulse noise protection in 4.3125kHz (symbol) settings

<1-18>

profile xdsl-line set inp-min-prot-ds-ch2<profile_name> <value-dec>

Ch2 downstream min impulse noise protection in 8.625kHz (symbol) settings

<1-17>

profile xdsl-line set inp-min-prot-us-ch2<profile_name> <value-dec>

Ch2 upstream min impulse noise protection in 8.625kHz (symbol)

<1-17>

APPENDIX