

VDSM2-1524 VDSL2 IP DSLAM

User Manual



Version 1.00

Copyright by CTC Union Communications Inc., all right reserved

The information in this document has been checked carefully and is believed to be correct as of the date of publication. CTC Union Communications Inc. reserves the right to make changes in the product of specification, or both, presented in this publication at any time without notice. CTC Union Communications assumes no responsibility or liability arising from the specification listed herein. CTC Union Communications make no representations that the use of its products in the manner described in this publication will not infringe on existing or future patents, trademark, copyright, or rights of third parties. Implication or other under any patent or patent rights of CTC Union Communications Ins. Grants no license.

All other trademarks and registered trademarks are the property of their respective holders.

Tables of Contents

COPYRIGHT BY CTC UNION COMMUNICATIONS INC., ALL RIGHT RESERVED	2
TABLES OF CONTENTS	3
CHAPTER 1 INTRODUCTION.....	5
1.1 FEATURES.....	6
1.2 SPECIFICATION	8
CHAPTER 2 HARDWARE INSTALLATION	1
2.1 FRONT PANEL.....	1
2.1.1 Connectors	1
2.1.2 LED Indicators	2
2.1.3 Reset Button.....	2
2.2 PIN ASSIGNMENT OF RJ21 CABLE.....	3
CHAPTER 3 WEB CONFIGURATION.....	4
3.1 ADMINISTRATION.....	8
3.1.1 IP Address.....	9
3.1.2 Switch Setting.....	10
3.1.3 Console Port Information	13
3.1.4 Port Configuration.....	13
3.1.5 SNMP Configuration.....	17
3.1.6 Syslog Setting	23
3.1.7 Alarm Configuration.....	23
3.1.8 Temperatures & Fan Status	24
3.1.9 Firmware Update	24
3.1.10 Configuration Backup.....	25
3.1.11 SNTP Setting	26
3.2 L2 FEATURES	27
3.2.1 VLAN Configuration	27
3.2.1.1 Static VLAN.....	28
3.2.1.2 GVRP VLAN.....	32
3.2.1.3 QinQ VLAN	34
3.2.2 Trunking	36
3.2.3 Forwarding & Filtering.....	38
3.2.4 IGMP Snooping	41
3.2.5 Spanning Tree.....	42

3.2.5.1	System Configuration	43
3.2.5.2	PerPort Configuration	44
3.2.5.3	Instance.....	44
3.2.5.4	Interface.....	45
3.2.6	DHCP Relay & Opt.82.....	46
3.2.6.1	DHCP Option 82	47
3.2.6.2	DHCP Relay.....	47
3.2.6.3	DHCP Option 82 Router Port	47
3.2.6.4	DHCP Opt. 82 Port Table	48
3.3	ACL	49
3.3.1	IPv4.....	50
3.3.2	Non-IPv4.....	51
3.3.3	Binding	51
3.4	SECURITY.....	53
3.4.1	Security Manager.....	53
3.4.2	MAC Limit	54
3.4.3	802.1x Configuration	55
3.5	QoS.....	58
3.5.1	QoS Configuration	58
3.5.2	ToS/DSCP	60
3.6	MONITORING.....	61
3.6.1	Port Status.....	61
3.6.2	Port Statistics.....	62
3.7	VDSL	63
3.7.1	Configuration.....	63
3.7.2	Profile Table.....	65
3.8	RESET SYSTEM.....	66
3.9	REBOOT	66
CHAPTER 4	CONFIGURATION VIA CONSOLE	67
APPENDIX	68

Chapter 1 Introduction

CTC Union VDSM2-1524 VDSL2 IP DSLAM 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 VDSM2-1524 VDSL2 IP DSLAM 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:

- VDSM2-1524 VDSL2 IP DSLAM 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 and SSH

Operating Requirements:

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

* CTC Union 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

VDSM2-1524 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**
VDSM2-1524 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 VDSM2-1524 locally with CONSOLE port. Via CONSOLE, users are able to configure VDSM2-1524 with menu-driven interface with any terminal emulation program, such as, Hyperterminal and Teraterm. (115200, 8, None, 1, None)
- **GE1 & GE2**
For connecting Gigabit Ethernet, VDSM2-1524 provides Gigabit Ethernet combo interfaces, TP and SFP.
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			

註解 [u1]: Need to confirm LED status

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

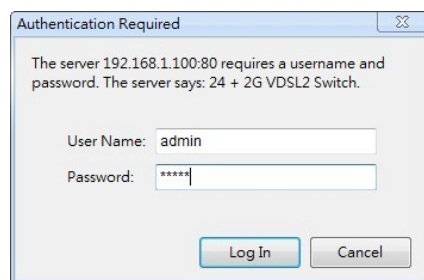
The VDSL2 IP DSLAM allows users to manage and change its configurations with web browsers. Users are able to login the web management system with any standard web browser, such as, Internet Explorer, Firefox, etc.

Default IP Address	192.168.0.100
Default User Name	admin
Default Password	admin

TABLE 1 DEFAULT LOGIN INFORMATION

Note: 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.

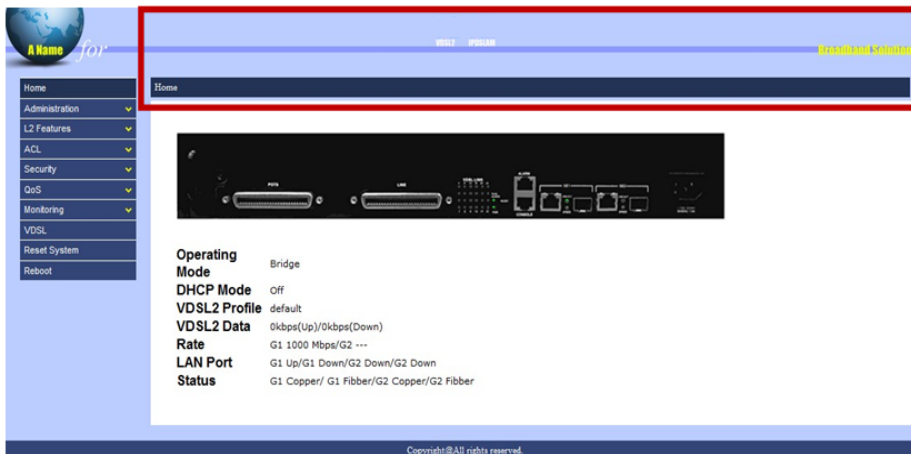


Please key in the correct login information and the main page of the management will be showed as the following image.



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.

Note: 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)

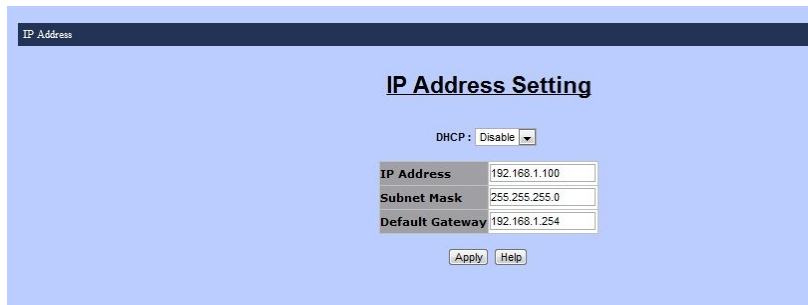
3.1 Administration



“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



The screenshot shows a web interface titled "IP Address Setting". At the top left, there is a tab labeled "IP Address". The main content area has a light blue background. In the center, there is a form with the following fields:

- DHCP:
- IP Address:
- Subnet Mask:
- Default Gateway:

At the bottom of the form, there are two buttons: "Apply" and "Help".

“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

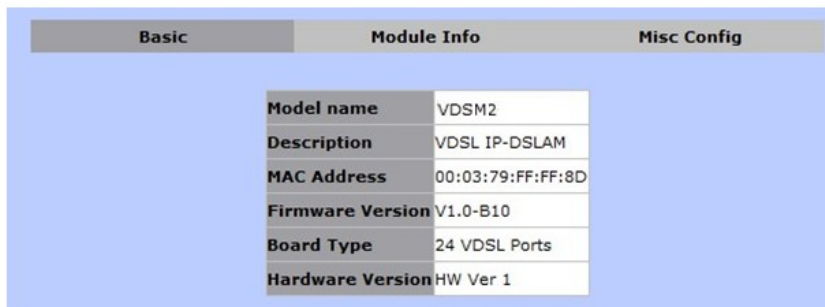


“Switch Setting” presents information of the switch in the following sub-functions. Note: only “Misc Config” section allows users to change the settings of the switch.

- 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

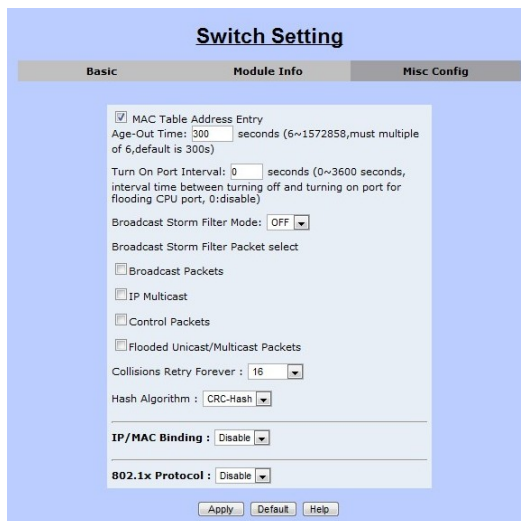


	TYPE	DESCRIPTION
Module1	8	GIGA COMBO
Module2	8	GIGA COMBO

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

Note: in the following contents, these two uplinks will be called Mod1 and Mod2.

- Misc Config



MAC Table Address Entry
Age-Out Time: 300 seconds (6~1572858, must multiple of 6, default is 300s)

Turn On Port Interval: 0 seconds (0~3600 seconds, interval time between turning off and turning on port for flooding CPU port, 0:disable)

Broadcast Storm Filter Mode: OFF

Broadcast Storm Filter Packet select

Broadcast Packets

IP Multicast

Control Packets

Flooded Unicast/Multicast Packets

Collisions Retry Forever: 16

Hash Algorithm: CRC-Hash

IP/MAC Binding: Disable

802.1x Protocol: Disable

Apply Default Help

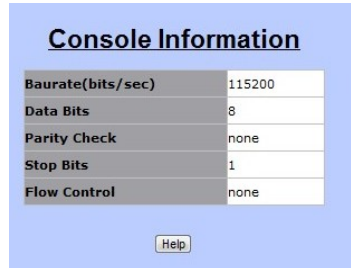
Users are allowed to modify the following details of the switch.

- 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. Note: 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 (Note: 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
 - Note: 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	State	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit: 128Kbps)	Security BSF	Jumbo Frame
						Ingress Egress		
Mod2 Trk1	Enable	Auto	1000	Full	Enable	0 0	Enable	Enable

Port	State	Link	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit: 128Kbps)	Security BSF	Jumbo Frame
							Ingress Egress		
Mod1	On	Up	Auto	1000	Full	On	Off Off	Off	On

“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
 - Note: “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
 - Note: 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.

- Note: 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.

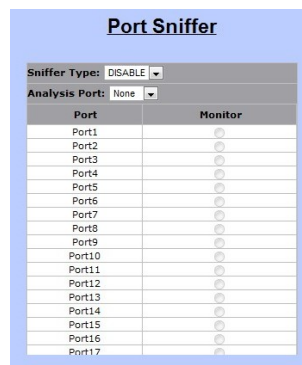
- BSF

- 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 Setting			
Port ID	Protected	Group1	Group2
Port1	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port2	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port3	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port4	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port5	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port6	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port7	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port8	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port9	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>

“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:K_LdB)	SNR Margin(DS) (Unit:K_LdB)	Firmware Version	Detail	
Port1	30le	0	0	NA	NA	NA	[Advance]	
Port2	30le	0	0	NA	NA	NA	[Advance]	
Port3	30le	0	0	NA	NA	NA	[Advance]	
Port4	30le	0	0	NA	NA	NA	[Advance]	
Port5	30le	0	0	NA	NA	NA	[Advance]	
Port6	30le	0	0	NA	NA	NA	[Advance]	
Port7	30le	0	0	NA	NA	NA	[Advance]	
Port8	30le	0	0	NA	NA	NA	[Advance]	
Port9	30le	0	0	NA	NA	NA	[Advance]	
Port10	30le	0	0	NA	NA	NA	[Advance]	
Port11	30le	0	0	NA	NA	NA	[Advance]	
Port12	30le	0	0	NA	NA	NA	[Advance]	
Port13	30le	0	0	NA	NA	NA	[Advance]	
Port14	30le	130966	130966	97	236	0	[Advance]	
Port15	30le	0	0	NA	NA	NA	[Advance]	
Port16	30le	0	0	NA	NA	NA	[Advance]	
Port17	30le	0	0	NA	NA	NA	[Advance]	
Port18	30le	0	0	NA	NA	NA	[Advance]	
Port19	30le	0	0	NA	NA	NA	[Advance]	
Port20	30le	0	0	NA	NA	NA	[Advance]	
Port21	30le	0	0	NA	NA	NA	[Advance]	
Port22	30le	0	0	NA	NA	NA	[Advance]	
Port23	30le	0	0	NA	NA	NA	[Advance]	
Port24	30le	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	(ms) ms
DNP	0 0.1 symbols	DNP	(ms) 0.1 symbols
CRC 15M	NA	CRC 15M	(ms)
CRC 1Delay	151400	CRC 1Delay	(ms)
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
sdh21LineStatusPerDataRate	0 Kbps	sdh21LineStatusPerDataRate	0 Kbps
sdh21LineStatusAttainableRate	0 Kbps	sdh21LineStatusAttainableRate	0 Kbps
sdh21LineStatusElectricalLength	0 0.1 dB	sdh21LineStatusElectricalLength	0 0.1 dB
sdh21LineStatusSNRMargin	0 (US0) 0.1dB	sdh21LineStatusSNRMargin	0 (<=) 0.1dB
sdh21LineStatusSNRMargin	0 (US1) 0.1dB	sdh21LineStatusSNRMargin	0 (DS1)
sdh21LineStatusSNRMargin	0.1dB	sdh21LineStatusSNRMargin	0.1dB
sdh21LineStatusSNRMargin	108836 (US2) 0.1dB	sdh21LineStatusSNRMargin	164356 (DS2)
sdh21LineStatusSNRMargin	0.1dB	sdh21LineStatusSNRMargin	0.1dB
sdh21LineStatusSNRMargin	12 (US3) 0.1dB	sdh21LineStatusSNRMargin	12 (DS3)
sdh21LineStatusSNRMargin	0.1dB	sdh21LineStatusSNRMargin	0.1dB
sdh21LineStatusSNRMargin	NA (US4) 0.1dB	sdh21LineStatusSNRMargin	-(DS4)
sdh21LineStatusSNRMargin	100 secs	sdh21LineStatusSNRMargin	237 secs
sdh21LineStatusSNRMargin	96	sdh21LineStatusSNRMargin	236
sdh21LineStatusSNRMargin	96	sdh21LineStatusSNRMargin	236
sdh21LineStatusSNRMargin	NA	sdh21LineStatusSNRMargin	NA
sdh21LineStatusSNRMargin	NA	sdh21LineStatusSNRMargin	NA
sdh21LineStatusSNRMargin	0	sdh21LineStatusSNRMargin	0
sdh21LineStatusSNRMargin	sdh21LineStatusSNRMargin	sdh21LineStatusSNRMargin	sdh21LineStatusSNRMargin
sdh21LineStatusSNRMargin	0	sdh21LineStatusSNRMargin	0
sdh21LineStatusSNRMargin	NA	sdh21LineStatusSNRMargin	NA
sdh21LineStatusSNRMargin	NA	sdh21LineStatusSNRMargin	NA
sdh21LineStatusSNRMargin	0	sdh21LineStatusSNRMargin	0

3.1.5 SNMP Configuration

The screenshot shows the 'SNMP Configuration' page. The 'System Options' section includes fields for Name (Layer 2 Switch), Location (No Location), Contact (No Contact), and SNMP Status (Disable). Below this is the 'Community Strings' section, which has a 'Current Strings' list (currently empty) and a 'New Community String' section with an 'Add' button and a 'String' input field.

“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

This screenshot shows the 'System Options' section of the SNMP Configuration page. It contains the following fields: Name (Layer 2 Switch), Location (No Location), Contact (No Contact), and SNMP Status (Disable). There are 'Apply' and 'Help' buttons at the bottom of this section.

- 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.

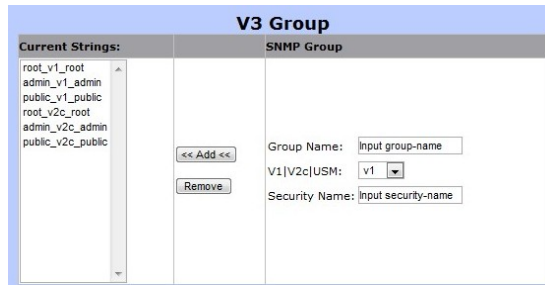
● Trap Manager



- 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.

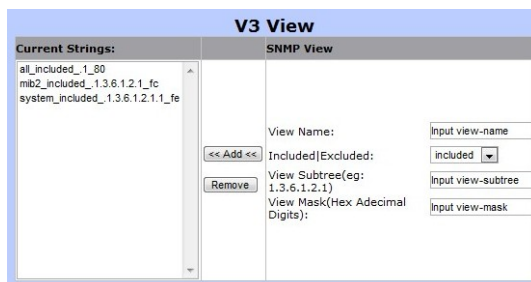
● SNMPv3 Group



- 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.

註解 [u2]: Check whether it is maintain or not

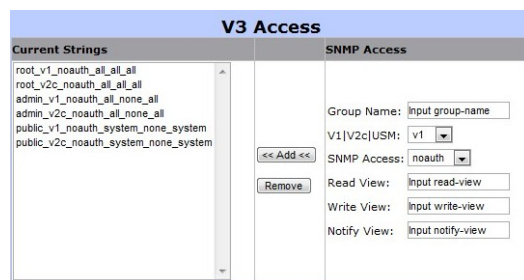
● SNMPv3 View



“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

註解 [u3]: Re-phase

- 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

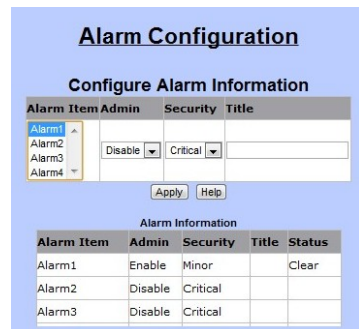


“Syslog” function is supported in this VDSL2 IP DSLAM system. The system will send logs to a remote log system. In this system, three events will be reported to the remote log system: cold start, warm start and link change. The followings are necessary for connecting the remote syslog server.

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

註解 [u4]: Need to know what's the difference between major and all

3.1.7 Alarm Configuration



Alarm Item	Admin	Security	Title
Alarm1	Enable	Minor	
Alarm2	Disable	Critical	
Alarm3	Disable	Critical	
Alarm4			

Alarm Item	Admin	Security	Title	Status
Alarm1	Enable	Minor		Clear
Alarm2	Disable	Critical		
Alarm3	Disable	Critical		

“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

Temperature and Fan Information	
Temperature Local	54 C
Temperature Remote 1	61 C
Temperature Remote 2	59 C
Fan1 Status	Medium Speed
Fan2 Status	Medium Speed
Fan3 Status	Medium Speed

“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

TFTP Firmware Update

TFTP Server IP Address

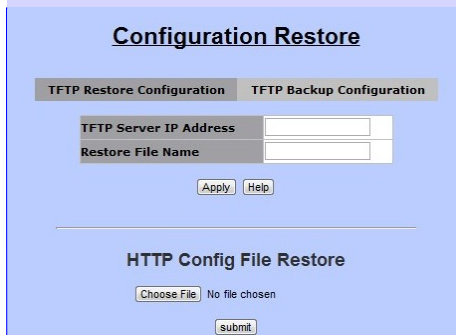
Firmware File Name

HTTP Firmware Update

No file chosen

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

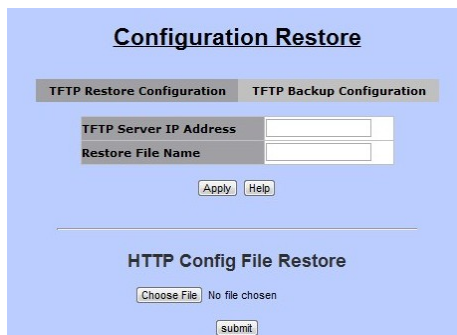
3.1.10 Configuration Backup



註解 [u5]: The user interface is not making any sense.

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 Setting	
SNTP	Disable
SNTP server IP	
UTC Type	Before-UTC
Time Range(0~24)	0
Time	
Apply Help	

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.

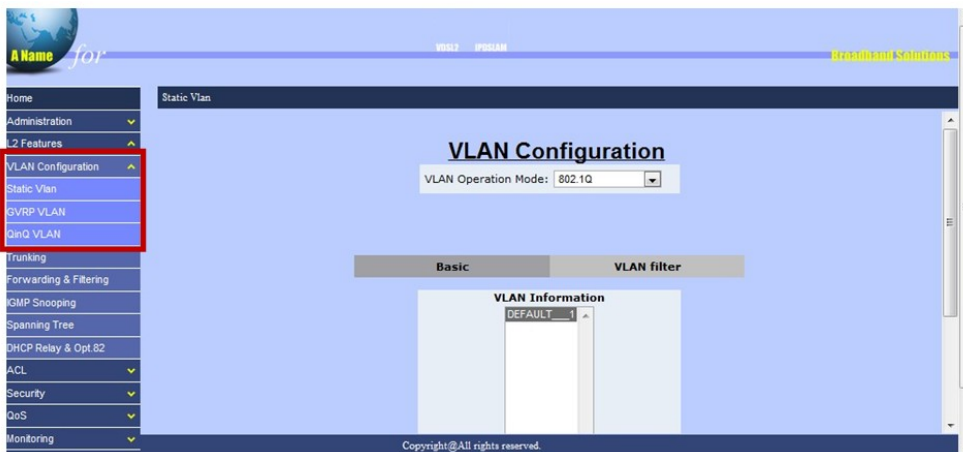
3.2 L2 Features

VDSL2 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

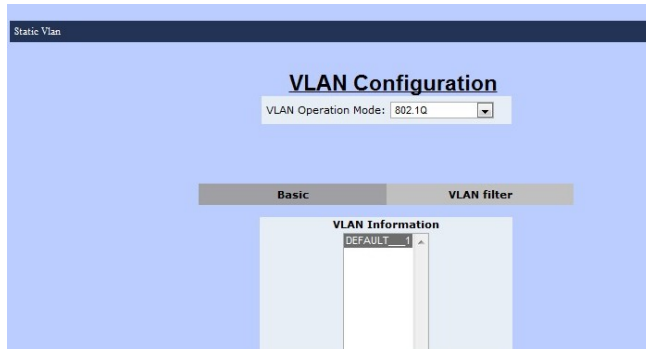
“VLAN” stands for “Virtual Local Area Network” or “virtual LAN”. It is a concept of separating and grouping LAN segments by a common set of requirements. VLAN presents couple benefits, such as, simplifying network design, enhancing bandwidth performance and improving, etc.



The VDSL2 IP DSLAM supports three kinds of VLAN algorithms:

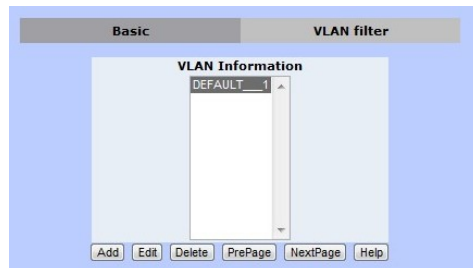
- Static VLAN
- GVRP VLAN
- QinQ VLAN

3.2.1.1 Static VLAN



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

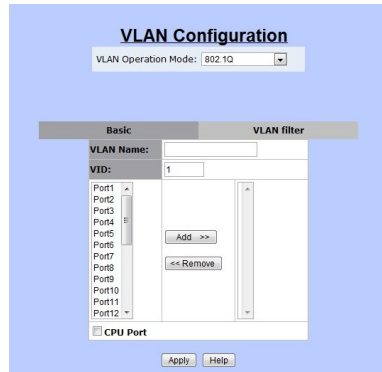
- VLAN Operation Mode
 - No VLAN
 - To disable VLAN mode.
 - Port-Based VLAN
 - To setup VLAN groups by ports.
 - 802.1Q VLAN
 - To setup VLAN groups by 802.1Q VLAN tags.
- Basic



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

Note: The VLAN mode of VLAN operation mode is the global setting of “Basic” and “VLAN Filter”.

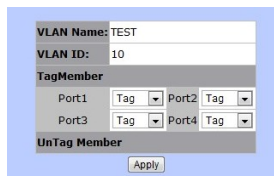
- Add



- To create a new VLAN group.

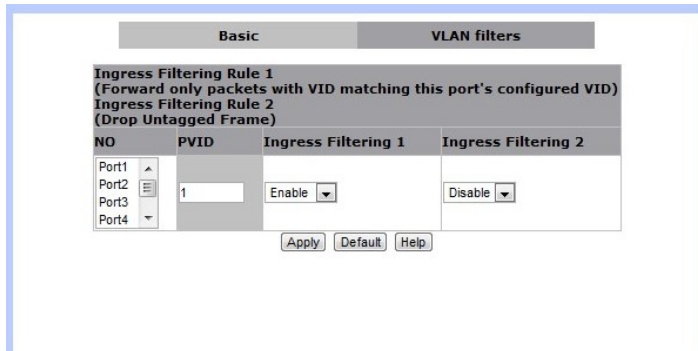
Name	Description
VLAN Name	The name of this VLAN group
VID	VLAN ID
VLAN Members	There are three columns in this section. <ul style="list-style-type: none"> ➢ Ports (left-hand side): Port1 ~ Port24, Mod1, Mod2 ➢ Add or Remove (middle): for adding or removing a port ➢ Selected Ports (right-hand side): 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



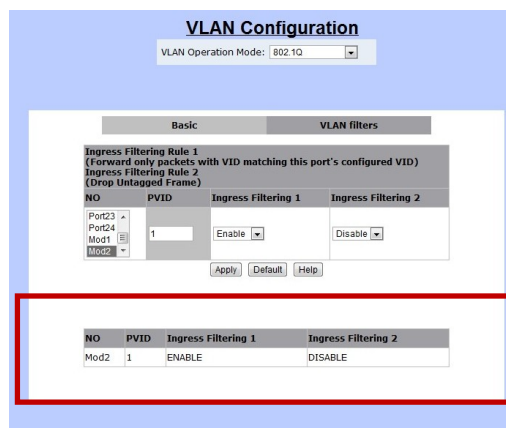
VLAN filter function is for setting the filtering rules for all ports (Port1 ~ Port24, Mod1 and Mod2).

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.

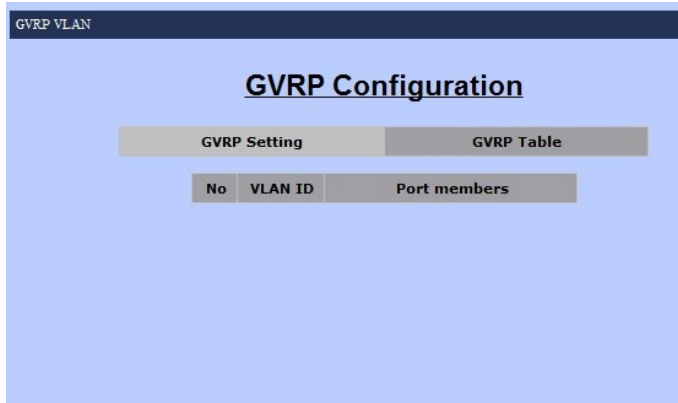


- PVID
 - The VLAN ID of ingress packets.

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

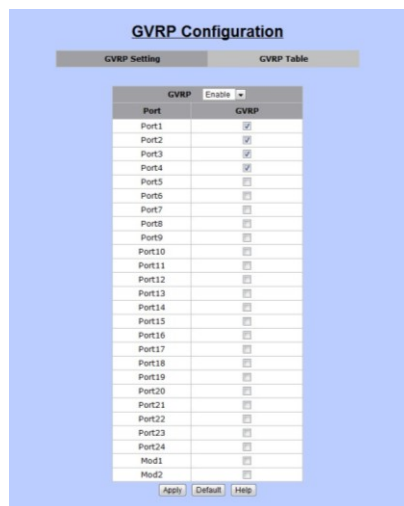
- Ingress Filtering 1
 - Only these ingress packets with the assigned VLAN ID are able to pass through this port.
 - Options: Enable or Disable (disable filtering function)
- Ingress Filtering 2
 - Enabling this rule will drop all untagged packets.
 - Options: Enable (only packets with the assigned VLAN 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

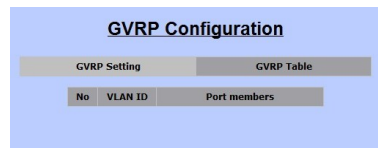


- ◆ GVRP
 - Options: Enable or Disable
- ◆ Port & GVRP
 - Port1 ~ Port24, Mod1, Mod2 & corresponding checkbox.

- 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.

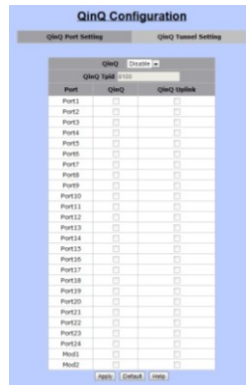


The screenshot shows a web interface titled "GVRP Configuration". It has two tabs: "GVRP Setting" and "GVRP Table", with "GVRP Table" being the active tab. Below the tabs is a table with the following header:

No	VLAN ID	Port members
----	---------	--------------

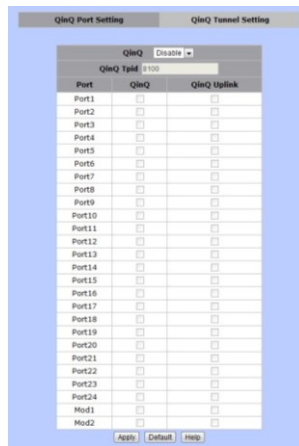
- GVRP will learn VLAN ID and its group member automatically. This table will show this information.

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



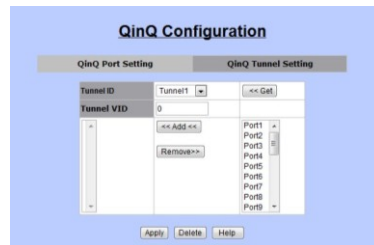
- This section is for setting up QinQ mode, TPID, and group members.
- The followings are the details that are required to be filled in for setting QinQ function.
 - ◆ QinQ: Disable or Enable
 - ◆ QinQ TPID:
 - TPID stands for “Tag Protocol Identifier”.

- 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.



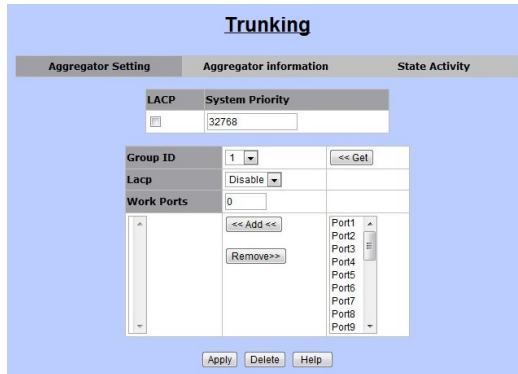
- QinQ Tunnel Setting

註解 [u6]: ???



- Tunnel ID
- Tunnel VID
-

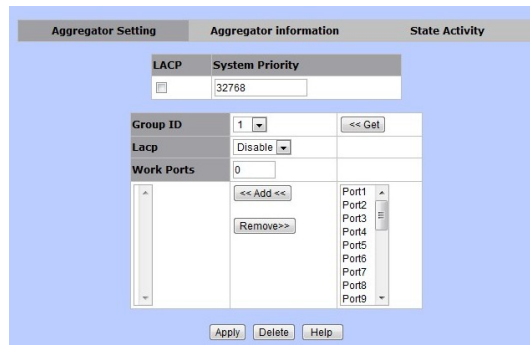
3.2.2 Trunking



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:

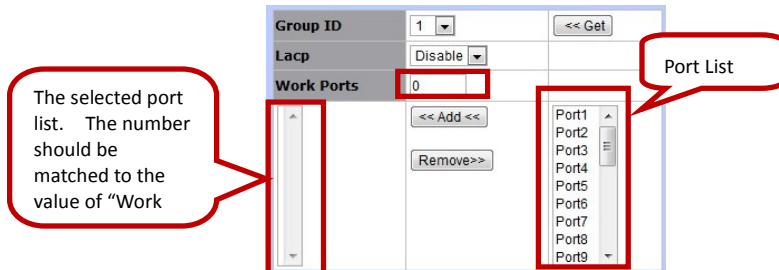
- Static Trunk
- LACP

- 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. (Note: 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)

註解 [u7]: Need image

- Static Activity

Port LACP State Activity		Port LACP State Activity	
1	N/A	2	N/A
3	<input checked="" type="checkbox"/> Active	4	<input checked="" type="checkbox"/> Active
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A
11	N/A	12	N/A
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	N/A
19	N/A	20	N/A
21	N/A	22	N/A
23	N/A	24	N/A
25	N/A	26	N/A

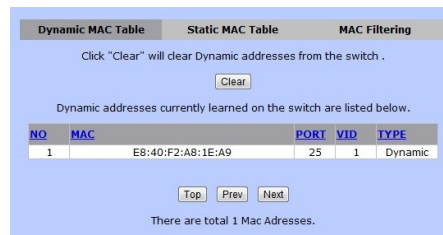
- This area is for setting up LACP mode (active or passive)
 - ◆ Active: the active port will send LACP packets automatically.
 - ◆ Passive: the passive port will not send LACP packets but it will respond if and only if it receives LACP packets from the other end.

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.

Dynamic addresses currently learned on the switch are listed below.

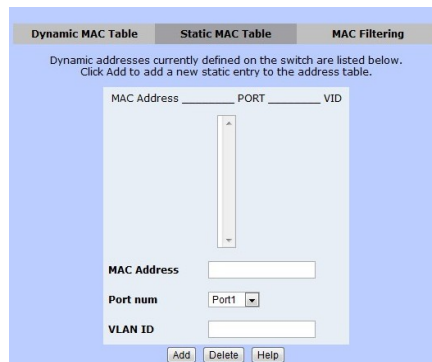
NO	MAC	PORT	VID	TYPE
1	E8:40:F2:A8:1E:A9	25	1	Dynamic

There are total 1 Mac Addresses.

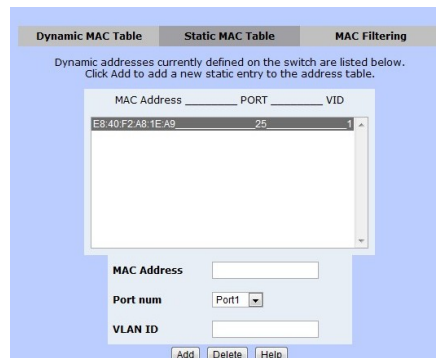
- Clear: to clear the dynamic MAC address table.

- 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. (Note: if there is nothing showed, it means this is the end page.)

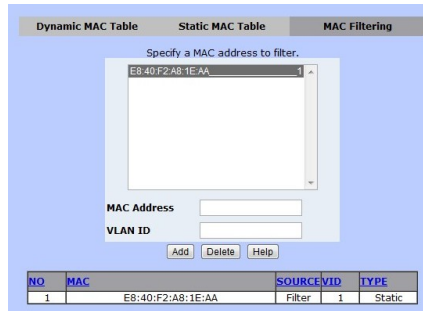
- Static MAC Table



- 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

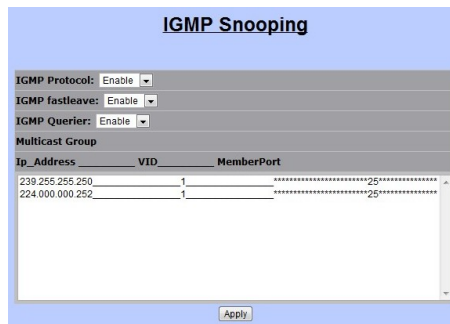


- Users are able to define and drop unwanted traffic in “MAC Filtering” function.

3.2.4 IGMP Snooping



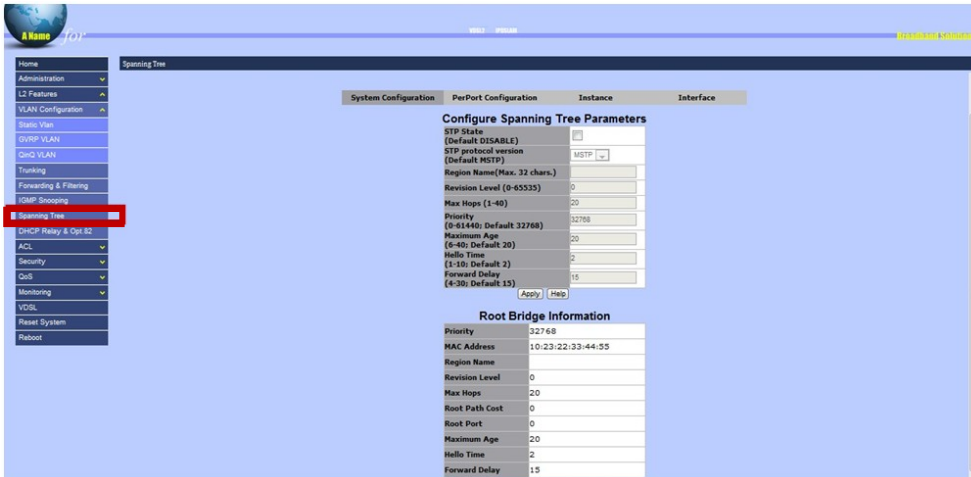
“IGMP” stands for “Internet Group Management Protocol”. IGMP allows hosts and routers to build multicast group memberships. IGMP snooping presents the process of IGMP network traffic listening. With this feature, VDSL2 IP DSLAM is able to listen to IGMP conversation between hosts and routers. The switch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



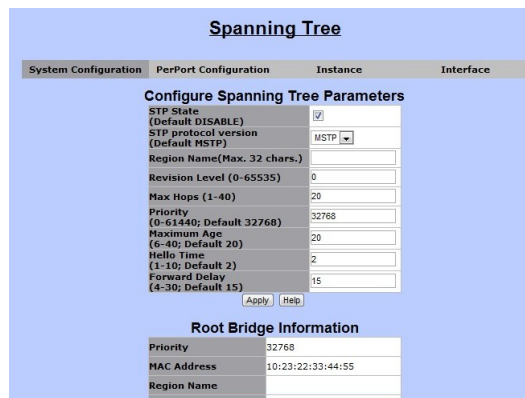
The following settings are needed in order to allow IGMP snooping work properly.

- 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

Root Bridge Information	
Priority	32768
MAC Address	10:23:22:33:44:55
Region Name	

“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.
 - ◆ Note: 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

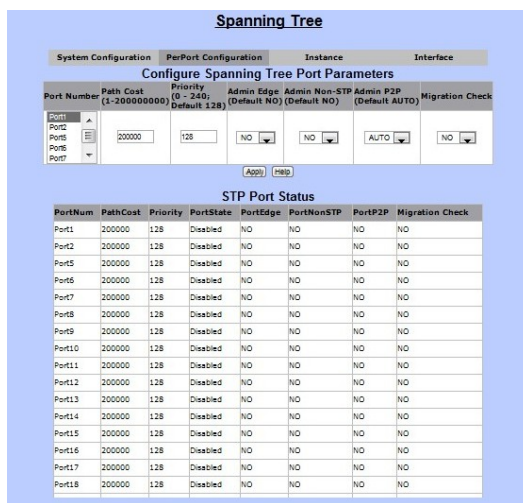
註解 [u8]: ??

註解 [u9]: ????

- Revision Level
- Max Hops
- Root Path Cost
- **Maximum Age**
- Hello Time
- Forward Delay

註解 [u10]: ??

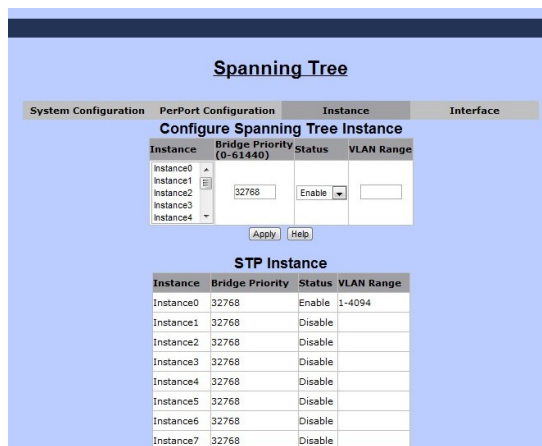
3.2.5.2 PerPort Configuration



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

3.2.5.3 Instance

註解 [u11]: For what?



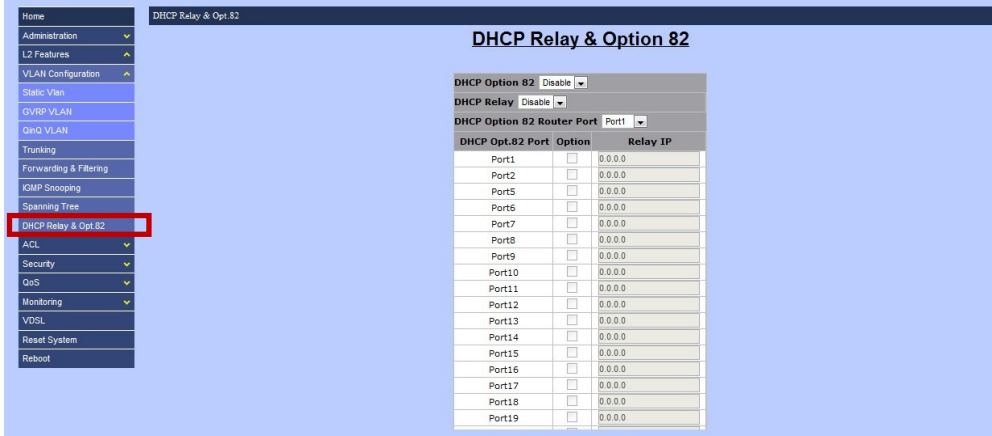
3.2.5.4 Interface

Spanning Tree

System Configuration	PerPort Configuration	Instance	Interface
MSTP Port Priority and Path Cost Settings			
Instance		0	
Port Number		Port1	
Port Priority(0~240)		128	
Path Cost(1~200000000)		0	
Save Setting Help			
Instance		0	

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.

Port Option	Relay IP
Port1	0.0.0.0
Port2	0.0.0.0
Port3	0.0.0.0
Port4	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
Port20	0.0.0.0
Port21	0.0.0.0
Port22	0.0.0.0
Port23	0.0.0.0
Port24	0.0.0.0
Mod1	0.0.0.0
Mod2	0.0.0.0
Tot1	0.0.0.0

3.2.6.1 DHCP Option 82

DHCP Option 82 Disable

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 Disable

DHCP Relay is for enabling or disabling DHCP Relay function.

3.2.6.3 DHCP Option 82 Router Port

DHCP Option 82 Router Port Port1

“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.

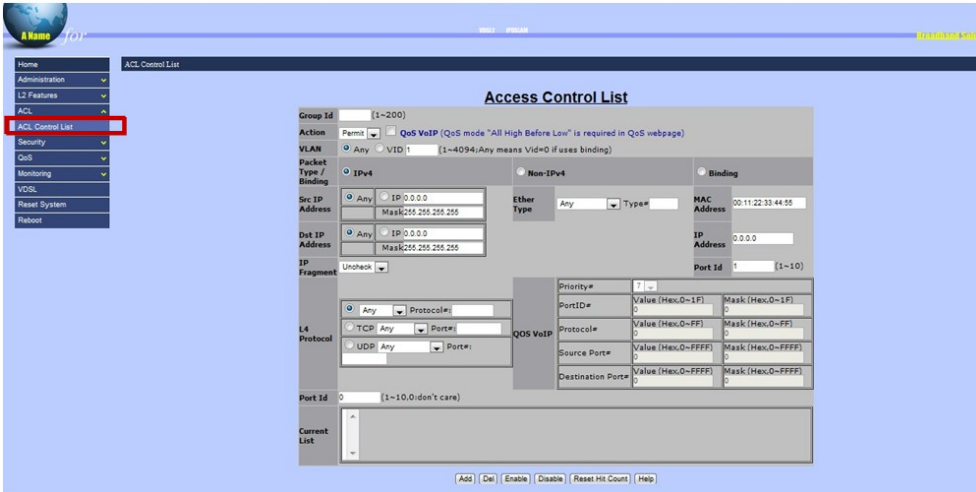
3.2.6.4 DHCP Opt. 82 Port Table

DHCP Opt.82 Port	Option	Relay IP
Port1	<input type="checkbox"/>	0.0.0.0
Port2	<input type="checkbox"/>	0.0.0.0
Port5	<input type="checkbox"/>	0.0.0.0
Port6	<input type="checkbox"/>	0.0.0.0
Port7	<input type="checkbox"/>	0.0.0.0
Port8	<input type="checkbox"/>	0.0.0.0
Port9	<input type="checkbox"/>	0.0.0.0
Port10	<input type="checkbox"/>	0.0.0.0
Port11	<input type="checkbox"/>	0.0.0.0
Port12	<input type="checkbox"/>	0.0.0.0
Port13	<input type="checkbox"/>	0.0.0.0
Port14	<input type="checkbox"/>	0.0.0.0
Port15	<input type="checkbox"/>	0.0.0.0
Port16	<input type="checkbox"/>	0.0.0.0
Port17	<input type="checkbox"/>	0.0.0.0
Port18	<input type="checkbox"/>	0.0.0.0
Port19	<input type="checkbox"/>	0.0.0.0

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

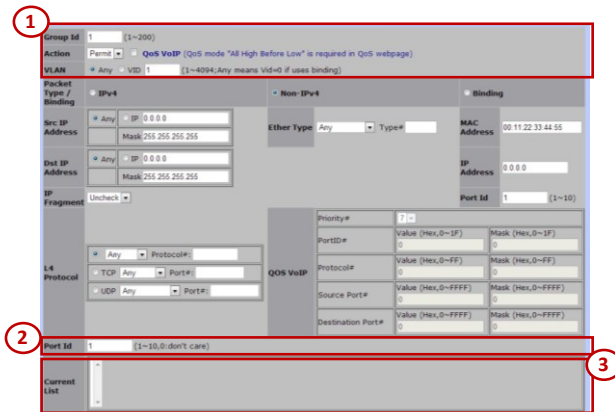
- Option: the checkbox for enabling or disabling DHCP Relay Information Option 82 function.
- Relay IP: for assign the IP address of the port.

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)

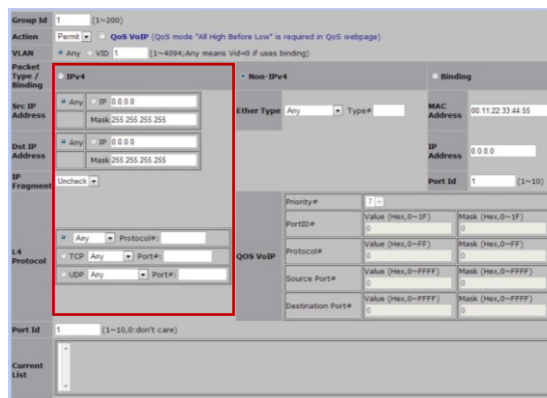
Section 2:

- 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

The screenshot shows the configuration page for a Non-IPv4 rule. The 'Ether Type' field is highlighted with a red box. The configuration includes the following fields and values:

- Group Id: 1 (range 1~200)
- Action: Permit (QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage))
- VLAN: Any (VID: 1 (range 1~4094, Any means Vid=0 if uses binding))
- Packet Type / Binding: Non-IPv4
- Src IP Address: Any (IP: 0.0.0.0, Mask: 255.255.255.255)
- Dst IP Address: Any (IP: 0.0.0.0, Mask: 255.255.255.255)
- IP Fragment: Unchecked
- L4 Protocol: Any (TCP/UDP)
- QoS VoIP: Priority# 7, PortID# 0, Protocol# 0, Source Port# 0, Destination Port# 0
- Port ID: 1 (range 1~10, don't care)
- Current List: Empty

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

3.3.3 Binding

The screenshot shows the configuration page for a Binding rule. The 'Binding' section is highlighted with a red box. The configuration includes the following fields and values:

- Group Id: 1 (range 1~200)
- Action: Permit (QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage))
- VLAN: Any (VID: 1 (range 1~4094, Any means Vid=0 if uses binding))
- Packet Type / Binding: Binding
- Src IP Address: Any (IP: 0.0.0.0, Mask: 255.255.255.255)
- Dst IP Address: Any (IP: 0.0.0.0, Mask: 255.255.255.255)
- IP Fragment: Unchecked
- L4 Protocol: Any (TCP/UDP)
- QoS VoIP: Priority# 7, PortID# 0, Protocol# 0, Source Port# 0, Destination Port# 0
- Port ID: 1 (range 1~10, don't care)
- Current List: Empty

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

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

QoS VoIP:

QoS VoIP	Priority#	7	
	PortID#	Value (Hex,0~1F) 0	Mask (Hex,0~1F) 0
	Protocol#	Value (Hex,0~FF) 0	Mask (Hex,0~FF) 0
	Source Port#	Value (Hex,0~FFFF) 0	Mask (Hex,0~FFFF) 0
	Destination Port#	Value (Hex,0~FFFF) 0	Mask (Hex,0~FFFF) 0

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

Note: 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



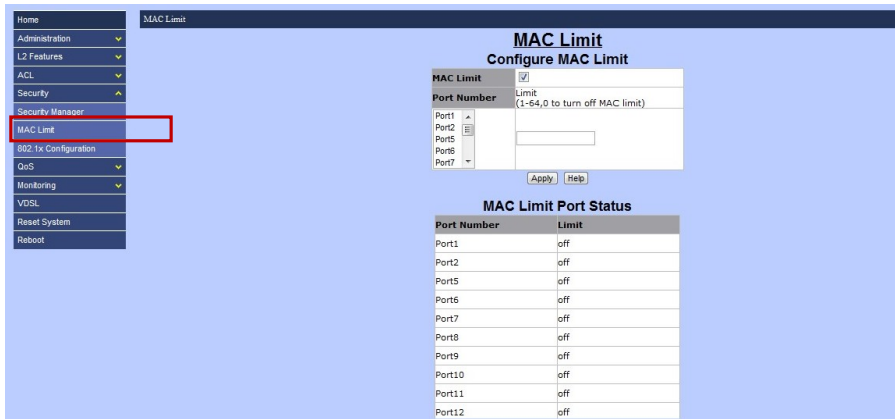
“Security Manager” allows users to change the user name and password for login purpose.

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

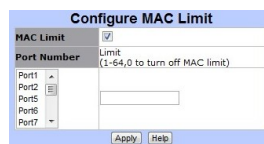
Note: the default user name and password are “admin” and “admin”.

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:

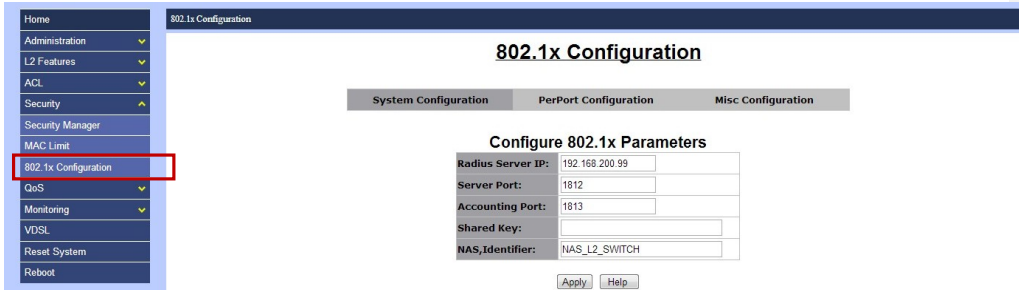
- MAC Limit: enable or disable MAC limit function.
- Limit: the maximum number of MAC addresses should be blocked.

- MAC Limit Port Status

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

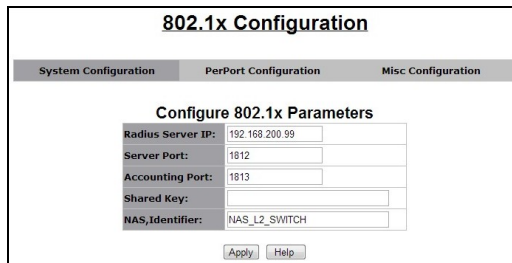


802.1x makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication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

Note: 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

Port Number	Port State
Port1	Au
Port2	No
Port3	No
Port4	No
Port5	No

PortNum	State
Port1	No
Port2	No
Port3	No
Port4	No
Port5	No
Port6	No
Port7	No
Port8	No
Port9	No
Port10	No
Port11	No
Port12	No
Port13	No

“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

Quiet period:	60
Tx period:	15
Supplicant timeout:	30
Server timeout:	30
Max requests:	2
Reauth period:	3600

“Misc Configuration” 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:

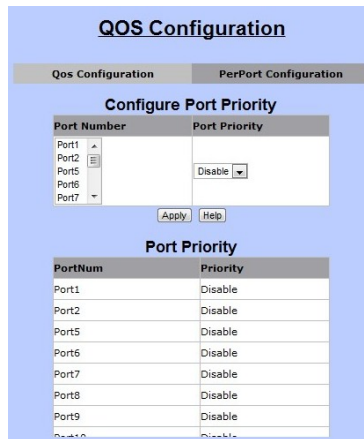
- First Come First Service
 - The sequence of packets sent is depending on arrive orders. This mode can be regarded as QoS is disabled.
- All High before Low
 - The high priority packets sent before low priority packets.

- 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

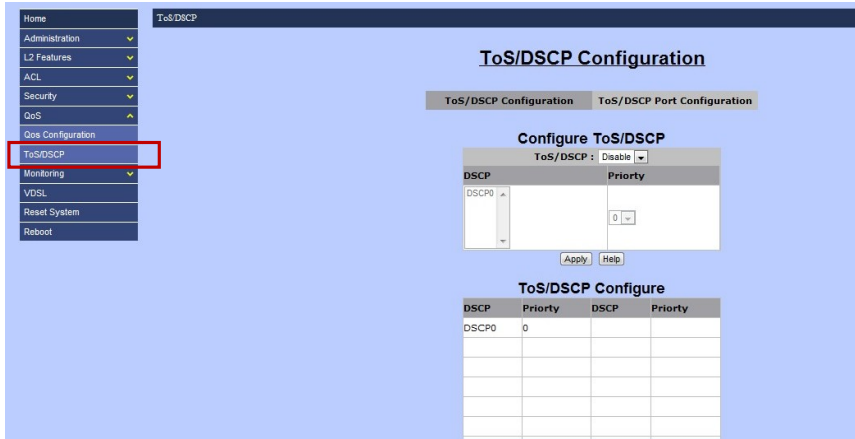


"PerPort Configuration" section allows users to setup the priority level for each port. Users are able to setup QoS algorithm with Port-Based algorithm in this page.

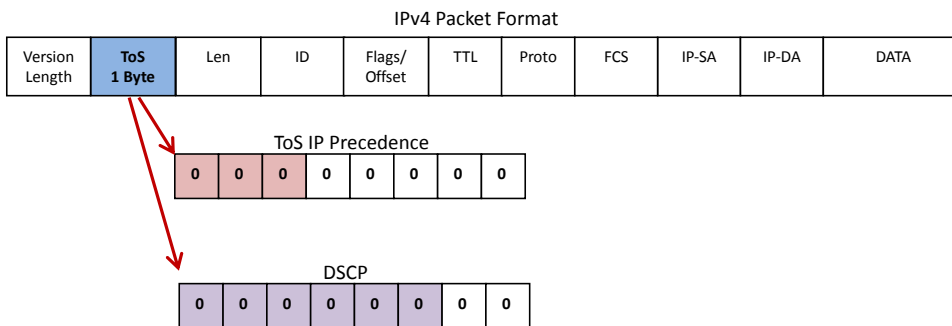
- Port Priority:
 - Options: Disable, 0 ~ 7.

3.5.2 ToS/DSCP

註解 [u12]: Not ready???



“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.

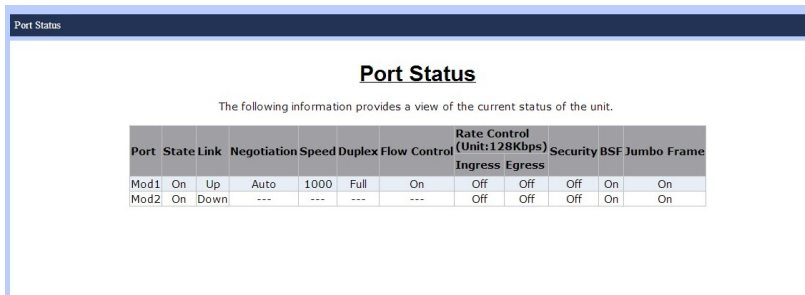


3.6 Monitoring

Home
Administration
L2 Features
ACL
Security
QoS
Monitoring
Port Status
Port Statistics
VDSL
Reset System
Reboot

“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	State	Link	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit: 128Kbps)		Security	BSF	Jumbo Frame
							Ingress	Egress			
Mod1	On	Up	Auto	1000	Full	On	Off	Off	Off	On	On
Mod2	On	Down	---	---	---	---	Off	Off	Off	On	On

“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

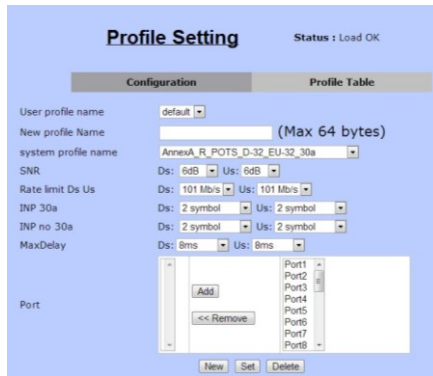
3.7 VDSL



“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

註解 [u13]: How to count bytes?

	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 Setting													Status : Load OK
Configuration											Profile Table		
User Name	System Name	SNR(0.1 Rate DB)		Rate Limit(kbps)		INP 30a(symbol)		INP Other(symbol)		Max Delay(ms)		Port	
		Ds	Us	Ds	Us	Ds	Us	Ds	Us	Ds	Us		
default	AnnexA_R_POTS_D-32_EU-32_30a	60	60	101000	101000	2	2	2	2	8	8	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24	

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

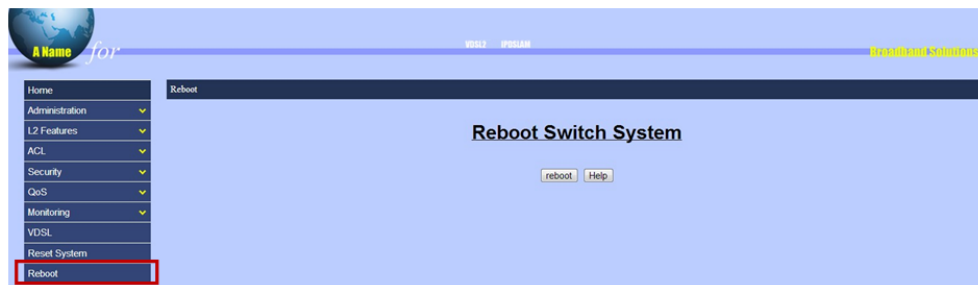
User Name	The profile name
System Name	VDSL2 Band profile
SNR (Ds / Us)	SNR value
Rate Limit (Ds / Us)	The data rate
INP 30a (Ds / Us)	INP level for VDSL2 profile 30a
INP Other (Ds / Us)	INP level for the other VDSL2 profiles
Max Delay	Maximum delay
Port	The port members of this profile

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.

Appendix