RUBYTECH VS-840S

8 Ports VDSL2 Managed IP DSLAM with 2 Giga Ethernet

USER'S MANUAL

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions before using the device.

- **DO NOT** open the device or unit. Opening or removing the cover may expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- **Use ONLY** the dedicated power supply for your device. Connect the power to the right supply voltage (110V AC used for North America and 230V AC used for Europe).
- **Place** connecting cables carefully so that no one will step on them or stumble over them. DO NOT allow anything to rest on the power cord and do NOT locate the product where anyone can work on the power cord.
- **DO NOT** install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- **DO NOT** expose your device to dampness, dust or corrosive liquids.
- **DO NOT** use this product near water, for example, in a wet basement or near a swimming pool.
- **Connect ONLY** suitable accessories to the device.
- **Make sure** to connect the cables to the correct ports.
- **DO NOT** obstruct the device ventilation slots, as insufficient air flow may harm your device.
- **DO NOT** place items on the device.
- **DO NOT** use the device for outdoor applications directly, and make sure all the connections are indoors or have waterproof protection place.
- **Be careful** when unplugging the power, because it may produce sparks.
- **Keep** the device and all its parts and accessories out of the reach of children.
- **Clean** the device using a soft and dry cloth rather than liquid or atomizers. Power off the equipment before cleaning it.
- This product is **recyclable**. Dispose of it properly.

Attention:

Be sure to read this manual carefully before using this product. Especially Safety Warnings.

Caution:

The VDSL2 IP DSLAM are for **indoor** applications only. This product does not have waterproof protection.

VDSL2 Brief

VDSL2 (Very-High-Bit-Rate Digital Subscriber Line 2, ITU-T G.993.2 Standard) is an access technology that exploits the existing infrastructure of copper wires that were originally deployed for POTS services. It can be deployed from central offices, from fibre-fed cabinets located near the customer premises, or within buildings.

ITU-T G.993.2 VDSL2 is the newest and most advanced standard of DSL broadband wireline communications. Designed to support the wide deployment of Triple Play services such as voice, video, data, high definition television (HDTV) and interactive gaming, VDSL2 enables operators and carriers to gradually, flexibly, and cost efficiently upgrade existing xDSL-infrastructure.

ITU-T G.993.2 (VDSL2) is an enhancement to G.993.1 VDSL that permits the transmission of asymmetric and symmetric (Full-Duplex) aggregate data rates up to 200 Mbit/s on twisted pairs using a bandwidth up to 30 MHz.

VDSL2 deteriorates quickly from a theoretical maximum of 200 Mbit/s at 'source' to symmetric 100 Mbit/s at 0.3 km and 50 Mbit/s at 1 km, but degrades at a much slower rate from there, and still outperforms VDSL. Starting from 1,6 km its performance is equal to ADSL2+.

ADSL-like long reach (LR) performance: ADSL-like long reach performance is one of the key advantages of VDSL2. LR-VDSL2 enabled systems are capable of supporting speeds of around 1-4 Mbit/s (downstream) over distances of 2.5 km, gradually increasing the bit rate up to symmetric 100Mbit/s as loop-length shortens. This means that VDSL2-based systems, unlike VDSL1 systems, are not limited to short loops or MTU/MDUs only, but can also be used for medium range applications.

VDSL2 IP DSLAM

The VDSL2 IP DSLAM utilize Lantiq(Infineon) Vinax VDSL2 Chipset, which is a VDSL2 IP DSLAM that aggregates 8 ports into Giga Ethernet uplinks for high-speed data/Internet services.

Based on DMT VDSL2 technologies, VDSL2 IP DSLAM extends data service with line rate of solution for services such as remote lecturing, telemedicine, video conferencing, Video-on-Demand (VoD), IP-TV, Internet access and other various high-speed data applications.

When the number of subscribers increases, the second uplink Giga Ethernet interface can be used to daisy chain to another VDSL2 IP DSLAM. Alternatively, multiple VDSL2 IP DSLAM can be connected to another LAN switch to from a two-tier configuration, thus supporting a lot more subscribers. The VDSL2 IP DSLAM is an ideal solution for delivering cost-effective, high-performance broadband/multimedia services to Multi-Tenant Units (MTUs) or Multi-Dwelling Units (MDUs) such as hotels, campus, hospitals and telecom.

The VDSL2 IP DSLAM provides the important features necessary for robust networks

Key features and benefits :

- **Jumbo packet up to 9k byte:** In computer networking, jumbo frames are Ethernet frames with more than 1500 bytes of payload. Conventionally, jumbo frames can carry up to 9000 bytes of payload, but variations exist and some care must be taken when using the term.

  The original 1500-byte payload size for Ethernet frames was used because of the high error rates and low speed of communications. Thus, if one receives a corrupted packet, only 1500 bytes (plus 18 bytes for the frame header and other overhead) must be re-sent to correct the error. However, each frame requires that the network hardware and software process it. If the frame size is increased, the same amount of data can be transferred with less effort. This reduces CPU utilization (mostly due to interrupt reduction) and increases throughput by allowing the system to concentrate on the data in the frames.

- **IEEE 802.1q Q-in-Q VLAN for performance & security:** The VLAN feature in the switch offers the benefits of both security and performance. VLAN is used to isolate traffic between different users and thus provides better security. Limiting the broadcast traffic to within the same VLAN broadcast domain also enhances performance. VLAN support enabling advanced techniques such as 802.1Q-in-1Q to be deployed.
  And support GVRP up to 4k V-Lan groups.

- **IEEE 802.1x:** port base network access control, this function for wireless users connecting Authentication.
- **Spanning tree:** Support IEEE 802.1d STP/IEEE 802.1w RSTP/IEEE-802.1s MSTP. For mission critical environments with multiple switches supporting STP, you can configure the switches with a redundant backup bridge path, so transmission and reception of packets can be guaranteed in event of any fail-over switch on the network.

- **IEEEE 802.1p QoS(COS) with Four Priority Queues:**
  The QoS(Quality Of Service) feature provides four internal queues to support four different classifications of traffic. High priority packet streams experience less delay inside the switch, which supports lower latency for certain delay-sensitive traffic. The VDSL2 IP DSLAM can classify the packet as one of the 8-level priority to 4 –level queue mapping. I.e. Highest, SecHigh, Lowest, SecLow.

- **Differentiated Services or DiffServ:** is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing Quality of Service (QoS) on modern IP networks. DiffServ can, for example, be used to provide low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic or file transfers.

DiffServ uses the 6-bit **Differentiated Services Code Point** (**DSCP**) field in the IP header for packet classification purposes. DSCP replaces the outdated Type of Service field.

- **IGMP Snooping :** Snooping by 256 IP multicast table for VOD (Video on demand) and Video conference and Internet games application.

- **HTTPS (SSL) Web Access:** Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL protocol to provide encrypted communication and secure identification of a network web server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems.

- **SNMP MIB Support:** SNMP v1/v2c/v3 management and trap function
  Support MIB tables: MIB-II (RFC 1213), Bridge MIBs (RFC 1493), Ethernet-like MIB (RFC 1643 & RFC 2665), private-MIB, USM-MIB (RFC 2574), VACM-MIB (RFC 2575) and RMON-MIB 1, 2, 3, 9 groups (RFC 1757& RFC 2819).

- **Broadcast/Multicast/Unknown-unicast Storm Control:** To limit too many broadcast/multicast/unknown-unicast flooding in the network, broadcast/multicast storm control is used to restrict excess traffic. Threshold values are available to control the rate limit for each port. Packets are discarded if the count exceeds the configured upper threshold.

- **Port Mirroring:** This function could be mirroring and duplicated client side action, but Need to be with mirroring AP as

Session wall or other.

- **ACL(Access Control List):** On some types of proprietary computer hardware, an **Access Control List** refers to rules that are applied to port numbers or network daemon names that are available on a host or other layer 3, each with a list of hosts and/or networks permitted to use the service. Both individual servers as well as routers can have network ACLs. Access control lists can generally be configured to control both inbound and outbound traffic, and in this context they are similar to firewalls. Like Firewalls, ACLs are subject to security regulations and standards.

- **Link Layer Discovery Protocol (LLDP):** is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document **IEEE 802.1AB.**

- **Speed Rate Control(Traffic shaping):** Supports speed rate control function from 128k to 100Mbps.

  Note:

  Regarding our VDSL2 IP DSLAM' principle of bandwidth control, which must rely on flow control to limit bandwidth over hardware, as long as client side doesn't support flow control, the upstream bandwidth control is invalid, so for this case, client side must support flow control function.

- **In band Management:** Provides a console(RS232) port for setup IP or other function
- **Out Of Band Management:** Supports remote control by Web-based Management easy-to-use configuration and ongoing monitoring. This software is embedded in the switch and delivers remote, intuitive management of the switch and connected NIC devices through a single IP address. The VDSL2 IP DSLAM are easy-to-configured and deployed, and offering a

compelling option in terms of cost, performance, scalability and services compared to traditional repeater HUB solutions.

- **2 Dual Media for Flexible Fiber Connection:**Dual media port 9 and 10 are provided for flexible fiber/copper auto link connection. You can select to install optional transceiver modules in these slots for short, medium or long distance fiber backbone attachment. Use of the SFP will auto disable their corresponding built-in 10/100/1000Base-T connections.

- **DHCP Client:** Dynamic Host Configuration Protocol (DHCP) for auto configuration management IP.

- **TFTP Protocol:** Trivial File Transfer Protocol(TFTP) for new version firmware remote upgraded

- **Firmware upgrade support :** HTTP / TFTP protocol.

- **Scalability:** Up to **100** Mbps symmetric performance over single-pair wiring for VDSL2 Channel.

- **Interleave delay time:** To prevent the transmission against burst errors. Please note that enable interleave delay function will reduce a few vdsl2 bandwidth.

- **Noise Margin(SNRM):** In electrical engineering, **noise margin** is the amount by which a signal exceeds the minimum amount for proper operation. VDSL2 IP DSLAM default value is 6db for telecom standard.

- **Upstream Power Back-Off (UPBO):** helps to run services over loops with different length co-located in the same cable binder ("mixed length" deployments), especially in FEXT-dominated noise environment.
  Strong FEXT generated by short loops can significantly degrade the performance of long loops if UPBO is not applied.

On the other hand, UPBO reduces the transmit power of short loops and thus degrades their performance as well. The UPBO technique should take in account both issues.

- **Downstream Power Back-Off (DPBO):** The development of Triple Play services requires higher bandwidth. Higher bandwidth and substantial performance gain can be reached by deploying DSLAM-s in a remote side cabinet near to the customer premises. There is no problem at clean networks where all the customers are connected to the same local cabinet.

- **Trellis coding :** The name *trellis* was coined because a state diagram of the technique, when drawn on paper closely resembles the trellis lattice used in rose gardens. The scheme is basically a convolutional code of rates (r,r+1). Ungerboeck's unique contribution is to apply the parity check on a per symbol basis instead of the older technique of applying it to the bit stream then modulating the bits. The key idea he termed Mapping by Set Partitions. This idea was to group the symbols in a tree like fashion then separate them into two limbs of equal size. At each limb of the tree, the symbols were further apart. Although in multi-dimensions, it is hard to visualize, a simple one dimension example illustrates the basic procedure. Suppose the symbols are located at [1, 2, 3, 4, ...]. Then take all odd symbols and place them in one group, and the even symbols in the second group. This is not quite accurate because Ungerboeck was looking at the two dimensional problem, but the principle is the same, take every other one for each group and repeat the procedure for each tree limb. He next described a method of assigning the encoded bit stream onto the symbols in a very systematic procedure. Once this procedure was fully described, his next step was to program the algorithms into a computer and let the computer search for the best codes. The results were astonishing. Even the most simple code (4 state) produced error rates nearly 1,000 times lower than an equivalent uncoded system. For two years Ungerboeck kept these results private and only conveyed them to close colleagues. Finally, in 1982, Ungerboeck published a paper describing the principles of trellis modulation.

A flurry of research activity ensued, and by 1990 the International Telecommunication Union had published modem standards for the first trellis-modulated modem at 14.4 kbit/s (2,400 baud and 6 bits per symbol). Over the next several years further advances in encoding, plus a corresponding symbol rate increase from 2,400 to 3,429 baud, allowed modems to achieve rates up to 34.3 kbit/s (limited by maximum power regulations to 33.8 kbit/s). Today, the most common trellis-modulated V.34 modems use a 4-dimensional set partition which is achieved by treating two 2-dimensional symbols as a single lattice. This set uses 8, 16, or 32 state convolutional codes to squeeze the equivalent of 6 to 10 bits into each symbol sent by the modem (for example, 2,400 baud × 8 bits/symbol = 19,200 bit/s).

Once manufacturers introduced modems with trellis modulation, transmission rates increased to the point where interactive transfer of multimedia over the telephone became feasible (a 200 kilobyte image and a 5 megabyte song could be downloaded in less than 1 minute and 30 minutes, respectively). Sharing a floppy disk via a BBS could be done in just a few minutes, instead of an hour. Thus Ungerboeck's

- **Echo cancellation :** The term **echo cancellation** is used in telephony to describe the process of removing echo from a voice communication in order to improve voice quality on a telephone call. In addition to improving subjective quality, this process increases the capacity achieved through silence suppression by preventing echo from traveling across a network.

  Two sources of echo have primary relevance in telephony: **acoustic echo** and **hybrid echo**.

  Echo cancellation involves first recognizing the originally transmitted signal that re-appears, with some delay, in the transmitted or received signal. Once the echo is recognized, it can be removed by 'subtracting' it from the transmitted or received signal. This technique is generally implemented using a digital signal processor (DSP), but can also be implemented in software. Echo cancellation is done using either echo suppressors or echo cancellers, or in some cases both.

- **INP(Impulse Noise Protection):** Impulse noise in multicarrier communication systems behaves effectively as a modulating signal that controls the first moment of the background Gaussian noise. The composite noise, which is the aggregate of the Gaussian noise and impulse noise, has a probability density function that is conditionally Gaussian with non-zero average, hence referred to as biased-Gaussian. The BER-equivalent power of the composite noise source is defined as the power of a pure Gaussian noise source that yields the same bit-error rate (BER). The BER-equivalent noise for a biased-Gaussian noise is simply the amplified version of the underlying Gaussian noise source. The amplification factor is derived from the characteristics of the impulse interference. Any bit-loading algorithm designed for Gaussian noise sources is also applicable to biased-Gaussian noise sources provided that the BER-equivalent SNR is used in place of the measured SNR.

- **Syslog :** is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices which would otherwise be unable to communicate a means to notify administrators of problems or performance.

Syslog can be used for computer system management and security auditing as well as generalized informational, analysis, and debugging messages. It is supported by a wide variety of devices (like printers and routers) and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

Table of Contents

Chapter 1. Unpacking Information

1.1 Check list

Carefully unpack the package and check its contents against the checklist.

1.2 Package Contents

1. VDSL2 IP DSLAM Managed VDSL2 IP DSLAM

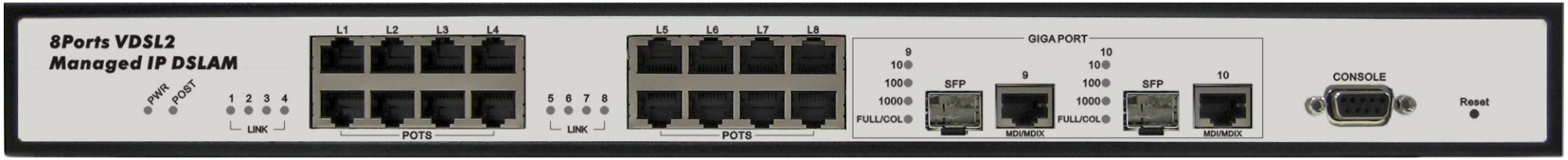
8x VDSL2 Ports(RJ45)，2x 1000Mbps auto link RJ-45/SFP Port

2. 1x AC Power Cord
3. A package contains two Rack Mounting Brackets and four screws
4. 4x Plastic feet(Pre-installed on the bottom)

Notes:

1. Please inform your dealer immediately for any missing or damaged parts. If possible, retain the carton including the original packing materials. Use them to repack the unit in case there is a need to return for repair.
2. If the product has any issue, please contact your local distributor.
3. Please look for the QR code on the bottom of the product, the user can launch the QR code scanning program to scan and download the user's manual electronic format file.

1.3 Product Guide



Product Name：2 ports 10/100/1000 Mbps Ethernet plus 8 ports 100 Mbps VDSL2 With SNMP Management IP DSALM

1.4 Features & Specifications

- Compliant with ITU-T G993.2 VDSL2, G993.1 VDSL, G997.1, G994.1 G.hs standard
- Compliant with IEEE-802.3, 802.3u, 802.3ab, 802.3z Ethernet Standard.
- Support 8a, 8b, 8c, 8d, 12a, 12b, 17a and 30a band profiles.
- Support 997 and 998 band plans.
- Supports Jumbo packet up to 9k byte.
- Supports interleave delay for noise resistant and data loss.
- Supports Virtual Noise.
- Supports SELT(Single-Ended Loop Testing).
- Supports Trellis coding for against noise.
- Supports Echo cancellation for against noise.
- Supports INP(Impulse Noise Protection) for multicarrier communication systems.
- Support UPBO(Upstream PBO) and DPBO(Downstream PBO).
- Supports high bandwidth up to symmetric 100Mbps within 0.3km (984 feet) for VDSL2 ports.
- Supports ADSL LIKE long reach mode up to 2.2 km.

- Supports bandwidth management (rate control) from 128k to 100Mbps.
- Supports IEEE 802.1q tagging VLAN with Q-in-Q.
- Supports quality of phone wiring detected with SNR(Signal to Noise Ratio) indicators.
- Supports TOS IEEE-802.1p with 4 priority queues with DSCP.
- Supports HTTPS (SSL) web management.
- Supports Multicast IP table/IGMP v2 with 512 groups.
- Support IEEE 802.1d STP / IEEE 802.1w RSTP & IEEE-802.1s MSTP.
- Support port mirroring (sniffer) and broadcast storm filtering.
- Supports port security with MAC address filtering.
- Supports remote syslog.
- Supports traffic storm control.
- Support web based for remote management.
- Support SNMP v1/v2/v3 RFC-1493 bridge MIBs, RFC-1643 Ethernet MIB, RFC-1213 MIBII.
- Support RMON groups 1(Statistics), 2(Alarm), 3(Event), 9(History).
- Support HTTP/TFTP for firmware upgrade.
- Support In-Band/Out-of-Band management.
- Support L2/L3/4 access control list(ACL).
- Support DHCP client and Relay & Option 82.
- Supports LLDP(Link Layer Discovery Protocol) protocol.
- Supports surge protection and splitter on board.
- Internal switching power adapter Input: AC 85-265 volts/50-60Hz/1A .
- Rack mount size 19"/1U
- EMI by FCC/CE Class A

- Power Consumption: Max : 37W
- Weight : about 3.2kg

Notes:

1. Features and specifications in this manual are subject to change without prior notice.
2. *(*) Firmware upgradeable for future enhancement.*

1.5 Product Specification

Standard:	IEEE802.3/802.3u/802.3ab/802.3z standards ITU-T G993.2, G993.1,G994.1, G997.1 standards
Interface:	2 * RJ-45 Gigabit TP / SFP combo port 8 * RJ-45 connector for VDSL2 connection 8 * RJ-45 connector for POTS/ISDN connection 1 * console port
Flow control:	Full-duplex: IEEE 802.3x Half-duplex: Back pressure
MAC address table:	8K Entries
VDSL2 Spectrum:	138kHz ~ 30MHz
LED indication:	1 x Power LED 1 x POST LED 2 x Link/Active/Speed/Duplex/Collision Status for Gigabit ports 8 x VDSL Link/Sync. for VDSL2 ports
POTS/ISDN pass filter Spectrum:	0 ~ 120kHz
Operating Temperature:	0°C ~ 50°C (32°F ~ 122°F)
Storage Temperature:	-20°C ~ 70°C (-4°F ~ 158°F)
Humidity:	10 to 90% (non-condensing)
Dimensions:	435mm x 255mm x 44mm (17.13" x 10.04" x 1.73")
Chipsets:	Lantiq(Infineon)

Chapter 2. General Description

2.1 Hardware Description

This section describes the important parts of the IP DSLAM. It features the front and rear panel drawings LEDs, connectors, and IP DSLAM.

2.2 Front Panel

The following figure shows the front panel.

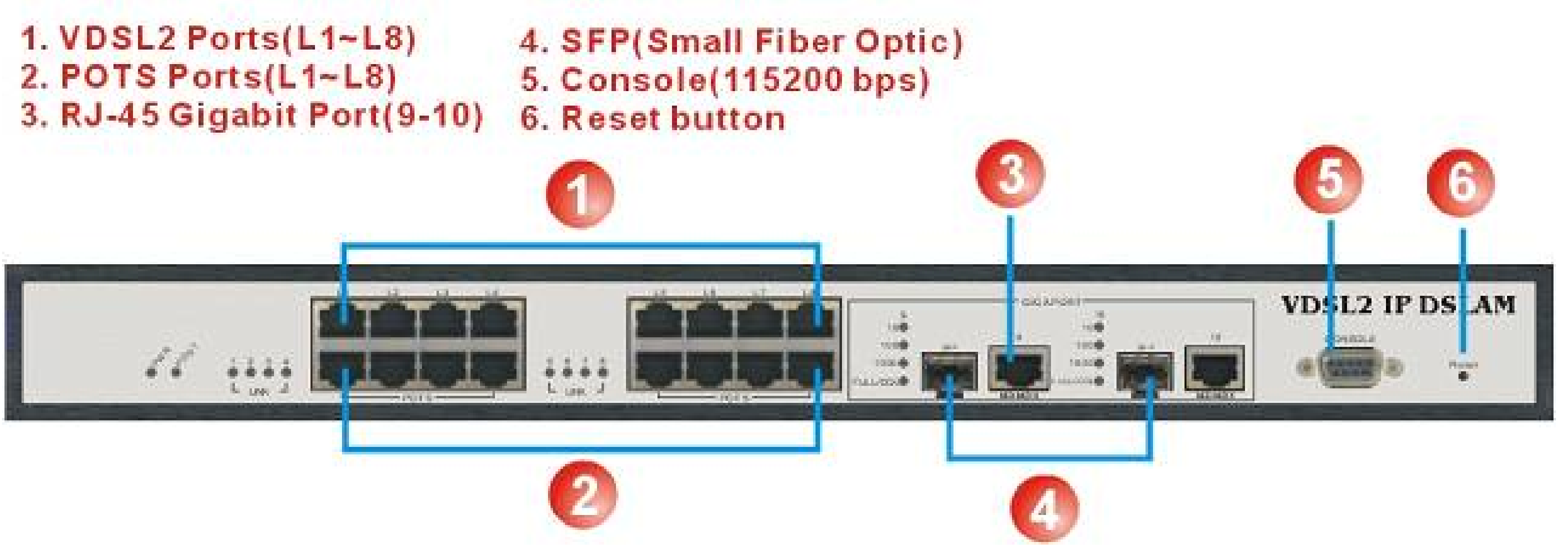


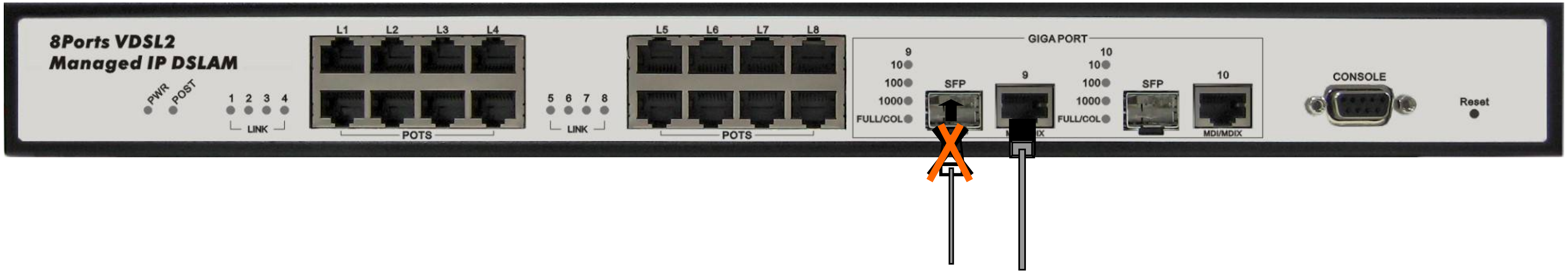
Figure 2.1 Front Panel description

Several LED indicators for monitoring the device itself, and the network status. At a quick glance of the front panel, the user would be knew if the product is receiving power; if it is monitoring another IP DSLAM or other devices; or if a problem exists on the network.

Provides two 1000Mbps auto-sensing RJ-45 Ethernet ports and two GIGA Port.

GIGA Port supports RJ-45 or SFP Interface auto link function. **You can use RJ-45 interface or SFP**

Interface.Figure 2.2



Note:

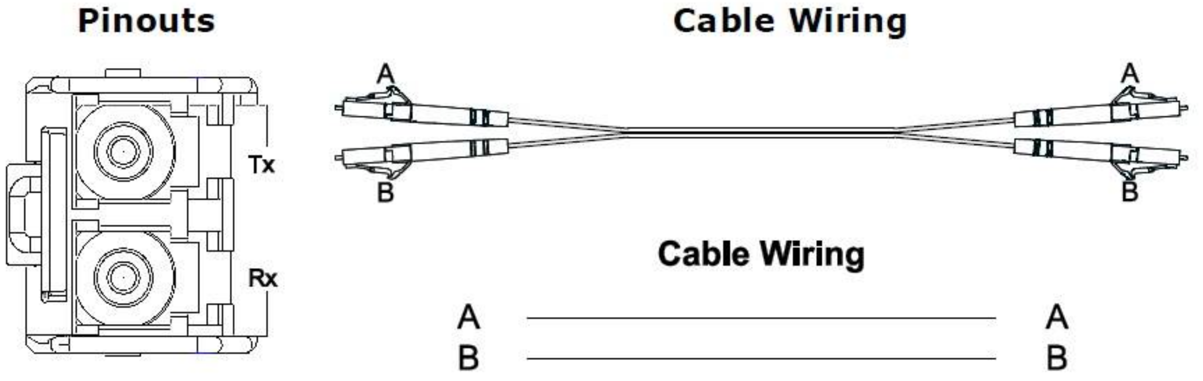
VDSL2 IP DSLAM supports two gigabit TP/SFP combo interfaces, one is copper interface and the other is small fiber optic interface. 9 and 10 port is RJ45 interface, SFP port is SFP interface. GIGA port supports Hot Swappable function; user can plug or unplug Giga port when the switch is operating. Please note that do not use the GIGA port RJ-45 interface and SFP interface in the same time, otherwise it will link in Copper mode (default).

2.3 SFP Fiber Optics

A gigabit interface converter (SFP) is a transceiver that converts electric currents (digital highs and lows) to optical signals, and optical signals to digital electric currents. The SFP is typically employed in fiber optic and Ethernet systems as an interface for high-speed networking. The data transfer rate is 1.25 gigabit per second.

SFP modules allow technicians to easily configure and upgrade electro-optical communications networks. The typical SFP transceiver is a plug-in module that supports hot-plugging (it can be removed and replaced without turning off the system). The devices are economical, because they eliminate the necessity for replacing entire boards at the system level. Upgrading can be done with any number of units at a time, from an individual module to all the modules in a system. SFP (Small Form Pluggable Transceivers), meet the Gigabit Interface Converter specification Rev. 5.4 (MOD_DEF4) industry standard.

	Mode	Wave length	Bit Rate	Voltage	Power Margin
1	LX-Single Mode	10km	1.25Gbps	3.3V	10.5db(10KM or above)
2	SX- Multi Mode	550m	1.25Gbps	3.3V	8.5db(550m)



2.4 LED Indications

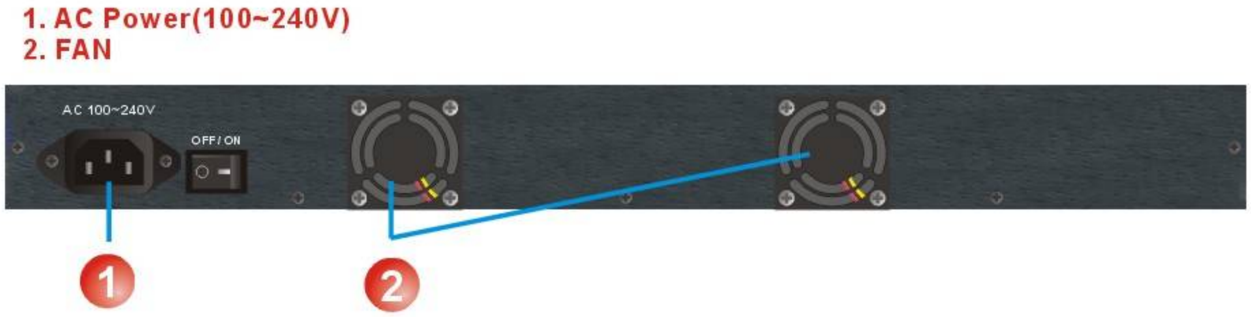
The followings describe the function of each LED indicator:

LEDs	Status	Descriptions
PWR **(Power LED)**	Steady Green	This LED light is located at the left side on the front panel. It will light up (ON) to show that the product is receiving power. Conversely, no light (OFF) means the product is not receiving power.
POST	Steady Green	POST(Power On Self Testing) POST Led will light to show system is booting now. When system is ready the LED will light off.
Speed10/Link **Speed100/Link** **Speed1000/Link** **ACT(Active LEDs)**	Steady Green	Giga port indicates that communications have been set 10/100/1000 Mbps. Each port on the IP DSLAM is assigned an LED light for 100 or 1000 Base-TX connecting
	Blinking	Blinking to show data on Traffic status. Fiber mode only support.
FULL/Col **(Full-Duplex LEDs)**	Steady Green	Indicates that communications have been set to full-duplex operation for the indicated port, The indicator lights up working in Full Duplex, and light down working in Half Duplex
(Collision LEDs)	Blinking	Blinking to show collision status.
VDSL2 Link LEDs	Steady Green	LED light up Steady to show VDSL2 Link is established LED light off Steady to show VDSL2 Link is not established

2.5 Rear Panel

The following figure shows the rear panel of the IP DSLAM.

Figure 2.3 Rear Panel



2.6 AC Power Socket

The power cord should be plug into this socket. The AC Socket accepts AC power 100 to 240 voltage.

Chapter 3. Installation

3.1 Hardware Installation

This chapter describes how to install the IP DSLAM and establish network connections. You may install this IP DSLAM on any level surface (table, shelf, 19 inch rack or wall mounting). However, please take note of the following minimum site requirements before you begin.

◆ 4 plastic feet on the bottom has been pre-installed.

3.2 Pre-Installation Requirements

Before you start actual hardware installation, make sure you can provide the right operating environment, including power requirements, sufficient physical space, and proximity to other network devices that are to be connected. Verify the following installation requirement:

- Power requirements: AC 100V to 240 V at 50 to 60 Hz.
  The IP DSLAM power supply automatically adjusts to the input voltage level.
- The IP DSLAM should be located in a cool dry place, with at least 10cm/4in of space at the front and back for well ventilation.
- Place the IP DSLAM out of direct sunlight, and away from heat sources or areas with a high amount of electromagnetic interference.
- Check if network cables and connectors needed for installation are available.
- Please note the VDSL2 IP DSLAM internal splitter, can pass through voice spectrum is 0KHz ~ 120KHz.

3.3 General Rules

Before making any connections to the IP DSLAM, note the following rules:

- **Ethernet Port (RJ-45)**

  All network connections to the bridge Ethernet port must be made using Category 5 UTP/STP or above for 100Mbps, Category 3, 4 UTP for 10Mbps.

  No more than 100 meters of cabling may be use between the MUX or HUB and an end node.

- **VDSL2 Port (RJ-11)**

  All network connections to the RJ-11port must use **24~26** gauge with **twisted pair** phone wiring.

  We **do not recommend** the use of the telephone line 28 gauge or above.

  The RJ-11 connectors have six positions, two of which are wired. The router uses the center two pins. The pin out assignment for these connectors is presented below.

  Please note that the line port is no polarity, therefore user can reverse the two wires of the phone cable when installed.

RJ-11 Pin out Assignments

Pin#	**MNEMONIC**	**FUNCTION**
1	NC	Unused
2	NC	Unused
3	**DSL**	**Used**
4	**DSL**	**Used**
5	NC	Unused
6	NC	Unused_

3.4 Connection Configuration

The IP DSLAM has 8 x 100 Mbps VDSL2 ports. And 2 Giga Ethernet ports which support connection to 10/100/1000 Ethernet. Support full or half-duplex operation and Auto MDI/MDIX. The transmission mode is using auto-negotiation. Therefore, the devices attached to these ports must support auto-negotiation unless they will always operate at half duplex. If transmissions must run at full duplex, but the attached device does not support auto-negotiation, then you should upgrade this device to a newer version that supports auto-negotiation.

Use any of the 9~10 ports to connect to devices such as a workstation, server, bridge or router. You can also cascade to another compatible IP DSLAM or hub by connecting an MDI or MDIX port.

1. User can connect an (9~10) station port on the IP DSLAM to any device that uses a standard network interface such as a optical fiber converter, workstation or server, or also to a network interconnection device such as a bridge or router (depending on the port type implemented).

2. Prepare the network devices you wish to network. Make sure you have installed VDSL2 CPE Bridge making a connection to any of the IP DSLAM (1~8) station ports. You also need to prepare **24~26 gauge** with twisted pair phone wire with RJ11 plugs at both ends.

3.Connect one end of the cable to the RJ-45 port of the network interface card, and the other end to any available (9~10) station port on the IP DSLAM. Every port support either 10 /100/1000 Mbps connections. When inserting an RJ-45 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Notes:

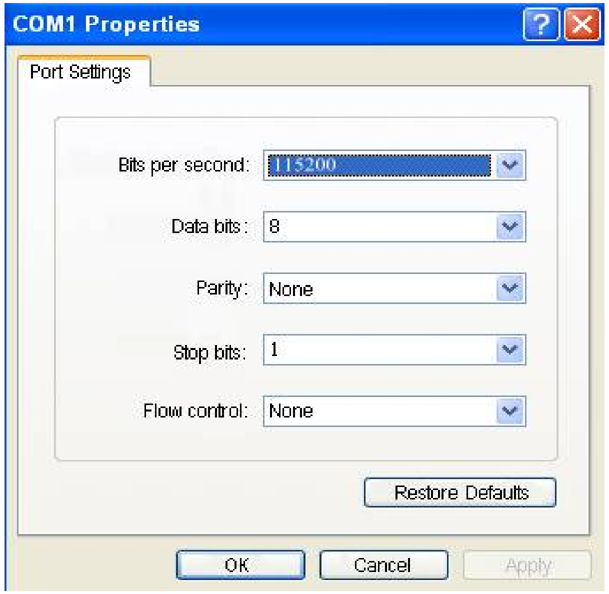
1. Be sure each twisted-pair cable (RJ-45) do not exceed by 100 meters (328 feet).
2. We advise using Category 5 cable for Cable Modem or router connections or to attach to any high bandwidth device to avoid any confusion or inconvenience.

Chapter 4. Management Configuration

4.0 In-Band Management

Console port (RS-232) Configuration

You can configure the product with the local serial console port, If one of the Ethernet port is not in use, you can disable it, that procedure is to connect a notebook computer to the RS-232 port, then boot operating systems, such as using the Windows operating system, and run “Hyper-terminal” program into terminal window, and setup step are as follow.



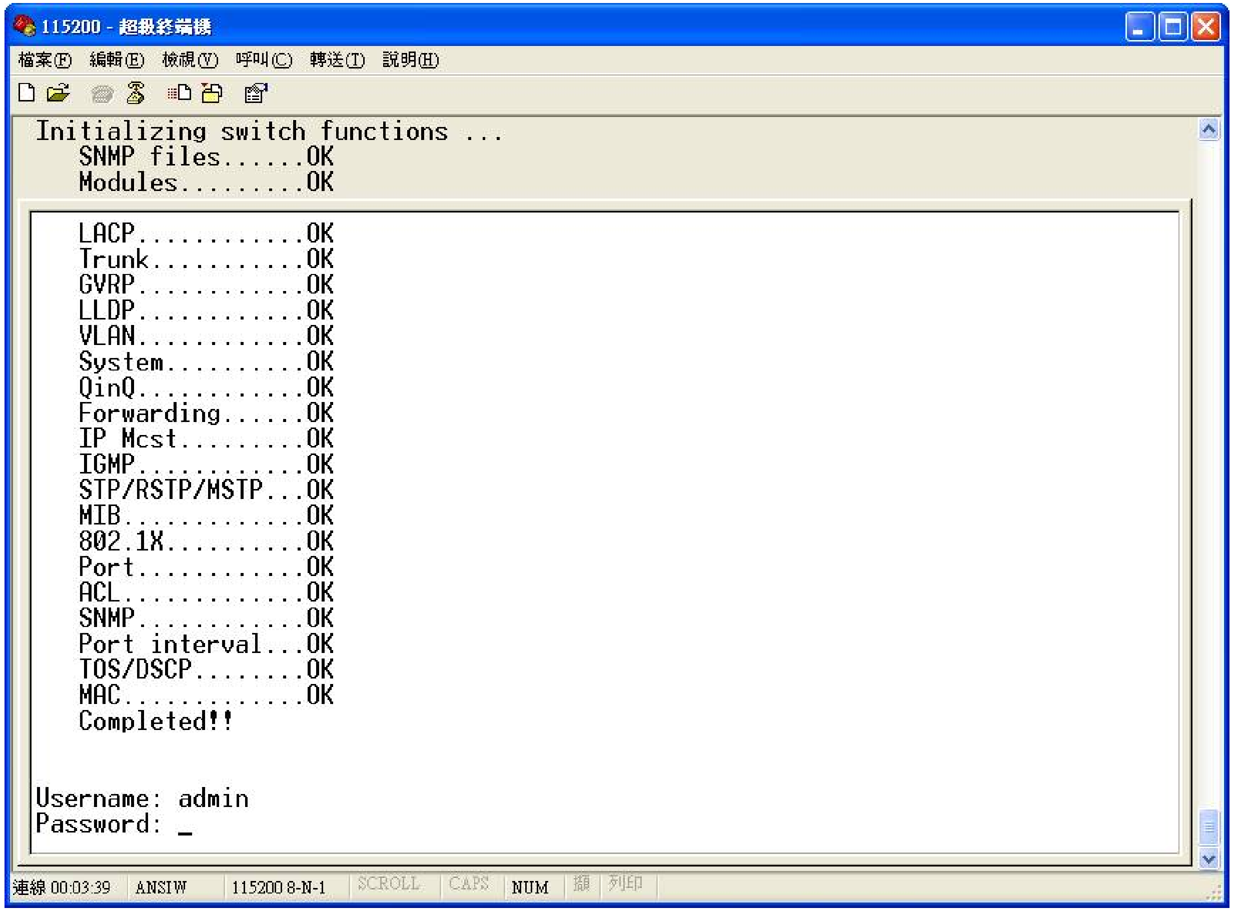
Bits per second: 115200
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

1. Set “Bits per second” at 115200 to the content window.

2. Set “Flow control” at None

3. Connects PC with the IP DSLAM, you will find login manual window on the screen then enter

Login name : ”**admin**” ; password : ”**123**”



```
Initializing switch functions ...
   SNMP files......OK
   Modules.........OK
   LACP............OK
   Trunk...........OK
   GVRP............OK
   LLDP............OK
   VLAN............OK
   System..........OK
   QinQ............OK
   Forwarding......OK
   IP Mcst.........OK
   IGMP............OK
   STP/RSTP/MSTP...OK
   MIB.............OK
   802.1X..........OK
   Port............OK
   ACL.............OK
   SNMP............OK
   Port interval...OK
   TOS/DSCP........OK
   MAC.............OK
   Completed!!


Username: admin
Password: _
```

4. Setting IP Address by Console Port

When you are going to login a IP DSLAM through the web page, you have to configure the IP address first. The default IP address / netmask / default gateway of a switch is **192.168.16.249 / 255.255.255.0 / 192.168.16.1**, without making any configuration changes in advance, you can login a IP DSLAM with default IP address as long as the default IP address can function properly in your network environment. Otherwise, you have to re-configure the IP address, subnet mask and default gateway. The following show how to configure the IP address of a IP DSLAM.

First, login with the console port.

```
Username: admin
Password: 123
```

Second, you will now enter the “IP Address ”, then, setup the IP address, subnet mask and gateway.

```
Switch# configure
Switch(config)# ip address 192.168.1.1 255.255.255.0
Switch(config)# ip default-gateway 192.168.1.254
```

Note:

As you may identify from the commands above Industrial VDSL2 Router is a Linux based device.

Many of the common Linux commands can be used here. However, please consider that you purchased a VDSL2 router device, not a PC. And always keep in mind that provider gives you support for configuring a standard VDSL2 router. If you try to use the VDSL2 router as a Linux hardware platform and modify its internal software structure, there is no support or warranty on the unit.

4.0.1 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) #
```

4.0.1.0 Command Line Editing

The following generic function keys provide functions in all of the menus:

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 line.
<Ctrl>-F; →	Moves the cursor forward one character.
<Ctrl>-K	Deletes from the cursor to the end of the command line.
<Ctrl>-N; ↓	Enters the next command line in the command history.
<Ctrl>-P; ↑	Enters the previous command line in the command history.
<Ctrl>-U	Deletes from the cursor to the beginning of the command line.
<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 word.
<Esc> F	Moves the cursor forward one word.
<Backspace>	Delete the character before the cursor.
<Del>	Delete the character at the cursor.

4.0.1.1 Command Help

You may enter “**?**” at any command mode, and the CLI will return possible commands at that point, along with some description of the keywords:

```
Switch (config) # copy tftp?
running-config Running configurations
flash Flash configurations
firmware Download firmware
```

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. The following example shows you how to enter the **show running-config** command:

```
Switch (config) # sh ru
```

4.0.1.2 Upgrade firmware via console command line

Please run Hyper terminal into terminal window and setup steps are as bellow:

1. Please connects VDSL2 IP DSLAM console port to PC or laptop PC series port.
2. Launch "Hyper Terminal" into terminal window on your PC.

3. Set “Bits per second” at " 115200 " on the content window.
4. Set "Data bits" at " 8 " on the content window.
5. Set "Parity" at " none " on the content window.
6. Set "Stop bits" at " 1 " on the content window.
7. Set “Flow control” at “ none ” on the content window.
8. Power on VDSL2 IP DSLAM and wait some time until the login menu appears.
9. Please enter login name ・” admin ” ; password・” 123 ” to access configuration menu.
10. You will see a symbol as "Switch#", and ready to management VDSL2 IP DSLAM via console.

Note: A TFTP server program is required to be installed in the PC for specified route for following steps.

11. At the CLI command, type the command " conf " and enter to the configuration mode.
12. At the CLI command, type the command "copy tftp firmware <ip-addr> <remote-file>" to upgrade the firmware.
 <ip-addr> specifies the IP address of the TFTP server.
 <remote-file> specifies the file name to download from the TFTP server.
13. Repeat step 9-11 to enter the configuration mode, and type the command " show info ” to show the firmware version, it means that the firmware is updated successfully.

4.0.1.3 Reset system to default via console command line

1. At the CLI command, type the command " erase startup-config " to reset system to default.
2. At the CLI command, type the command " boot " to reboot the VDSL2 IP DSLAM.
3. Follow the section 4.0.1.2 step 9-11 to enter the configuration mode, and type the command " show ip " to find the default ip address.

Note: Default ip it shows must be 192.168.16.249.

4.0.2 System Commands

show running-config

Display the running configuration of the IP DSLAM.

copy running-config startup-config

Backup the switch configurations.

erase startup-config

Reset to default factory settings at next boot time.

clear arp [<*ip-addr*>] Clear entries in the ARP cache.

Parameters:

[<*ip-addr*>] specifies the IP address to be cleared. If no IP address is entered, the entire ARP cache is cleared.

show arp

Show the IP ARP translation table.

ping *ip-addr* [<1..999>] Send ICMP ECHO_REQUEST to network hosts.

Parameters:

[<1..999>] specifies the number of repetitions. If not entered, it will continue to ping until you press <Ctrl>-C to stop.

[**no**] **per-vlan-flooding-portmask** Enable or disable per VLAN default flooding portmask.

per-vlan-flooding-portmask <**unicast** | **multicast**> <*vlan-id*> <*port-list*> Set unicast or multicast per VLAN default flooding portmask.

show per-vlan-flooding-portmask

Display unicast and multicast per VLAN default flooding portmask table.

4.0.3 Switch Static Configuration

4.0.3.0 Port Configuration and Status

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

Turn the port state on or off.

Parameters:

<*port-list*> specifies the ports to be turn on or off. If not entered, all ports are turn on or off.

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

Set port negotiation.

Parameters:

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

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

Set port speed (in mbps) and duplex.

Parameters:

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

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

Enable or disable port flow control.

Parameters:

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.

Parameters:

<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.

Parameters:

<*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.

Parameters:

<*port-list*> specifies the group member ports.

port protected <*port-list*>

Set protected port list.

Parameters:

<*port-list*> specifies the protected port list.

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

Set port priority.

Parameters:

<*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

Parameters:

<*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,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.

Parameters:

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

show port protection

Show protected port information.

4.0.3.1 VLAN

4.0.3.1.0 Virtual LANs

A Virtual LAN (VLAN) is a logical network group that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN within a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically. A station can belong to more than one VLAN group. VLAN prevents users from accessing network resources of another on the same LAN, thus the users can not see the hard disks and printers of another user in the same building. VLAN can also increase the network performance by reducing the broadcast traffic and enhance the security of the network by isolating groups.

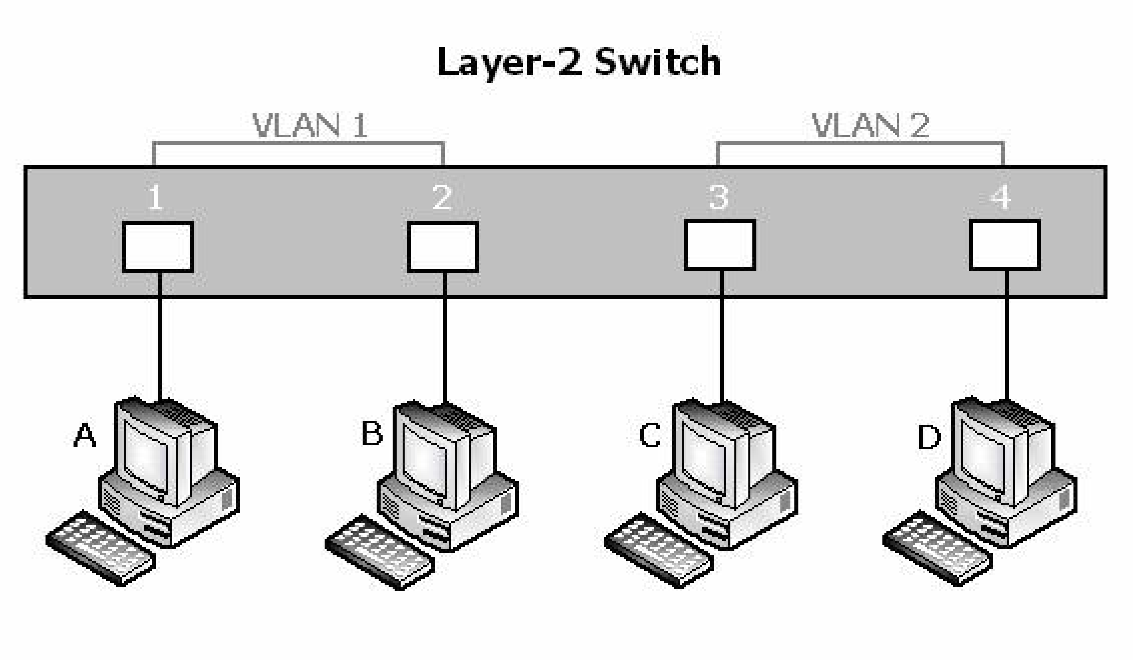
This Switch supports two types of VLANs:

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

Note:

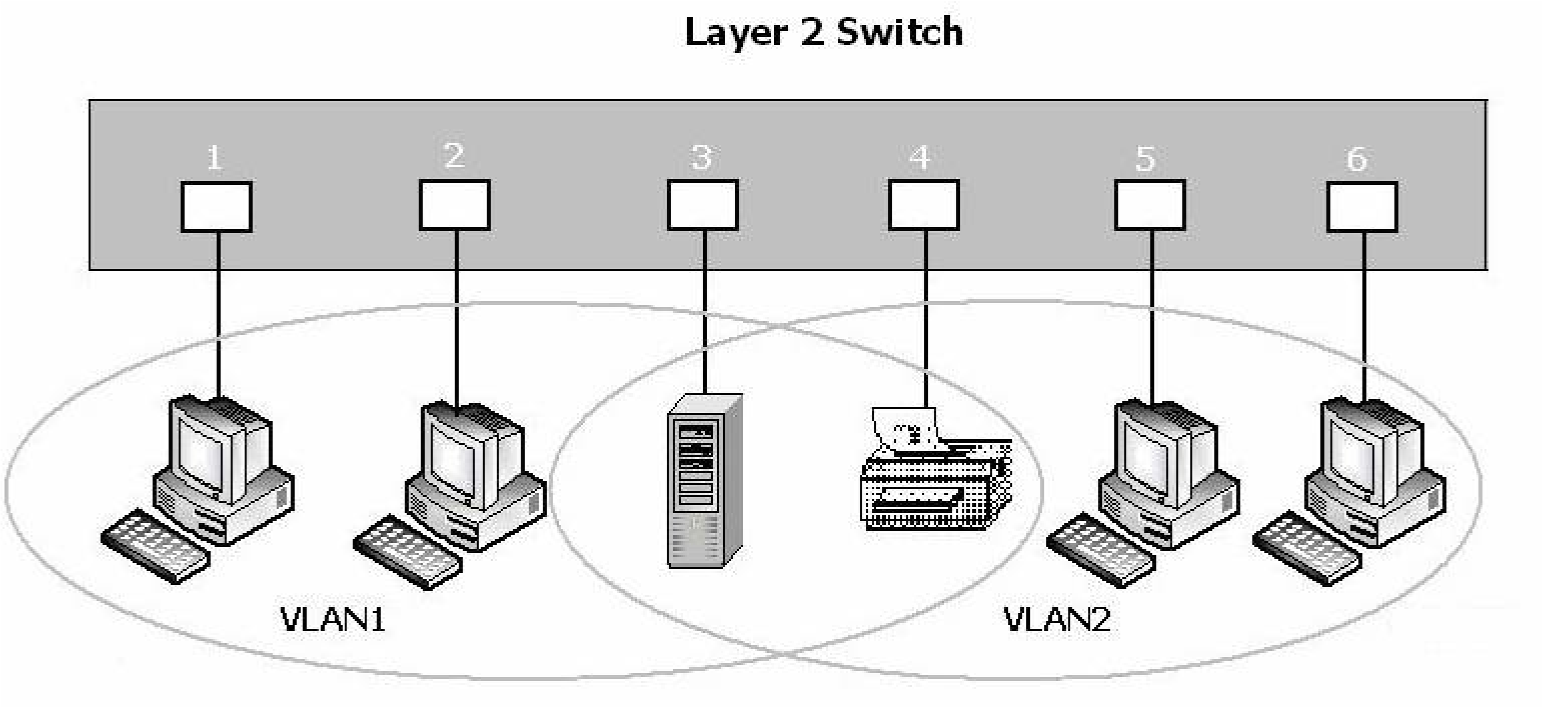
1. Only one of the two VLAN types can be enabled at one time.
2. Example of VLAN setting on "Appendix B".

Port-based VLANs are VLANs where the packet forwarding decision is made based on the destination MAC address and its associated port. You must define the outgoing ports allowed for each port when you use port-based VLANs. In port-based VLANs, the packets received from one port can only be sent to the ports which are configured to the same VLAN. As shown in the following figure, the switch administrator configured port 1~2 as VLAN 1 and port 3~4 as VLAN 2. The packets received from port 1 can only be forwarded to port 2. The packets received from port 2 can only be forwarded to port 1. That means the computer A can send packets to computer B, and vice versa. The same situation also occurred in VLAN 2. The computer C and D can communicate with each other. However, the computers in VLAN 1 can not see the computers in VLAN 2 since they belonged to different VLANs.

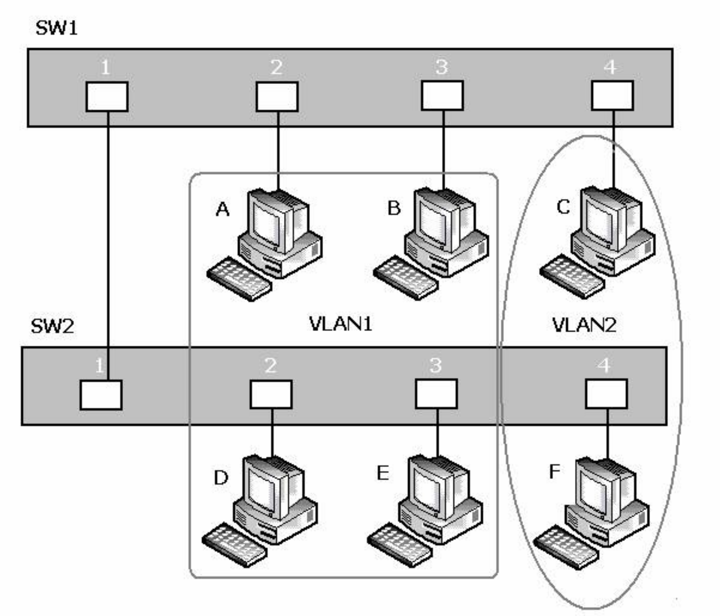


IEEE 802.1Q (tag) -based VLANs enable the Ethernet functionality to propagate tagged packets across the bridges and provides a uniform way for creating VLAN within a network then span across the network. For egress packet, you can choose to tag it or not with the associated VLAN ID of this port. For ingress packet, you can forward this packet to a specific port as long as it is also in the same VLAN group.

The 802.1Q VLAN works by using a tag added to the Ethernet packets. The tag contains a VLAN Identifier (VID) which belongs to a specific VLAN group. And ports can belong to more than one VLAN.



The difference between a port-based VLAN and a tag-based VLAN is that the tag-based VLAN truly divided the network into several logically connected LANs. Packets rambling around the switches can be forwarded more intelligently. In the figure shown below, by identifying the tag, broadcast packets coming from computer A in VLAN1 at sw1 can be forwarded directly to VLAN1. However, the switch could not be so smart in the port-based VLAN mechanism. Broadcast packets will also be forwarded to port 4 of sw2. It means the port-based VLAN can not operate a logical VLAN group among switches.



The VDSL2 IP DSLAM supports both port-based VLAN and tag-based (802.1Q) VLAN modes. The default configuration is tag-based
(802.1Q) VLAN. In the 802.1Q VLAN, initially, all ports on the switch belong to default VLAN, VID is 1.

Note:

You cannot delete the default VLAN group in 802.1Q VLAN mode.

4.0.3.1.1 VLAN Mode

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.

show vlan mode

Display the current VLAN mode.

vlan mode (disabled|port-based|dot1q)

Change VLAN mode.

Parameters:

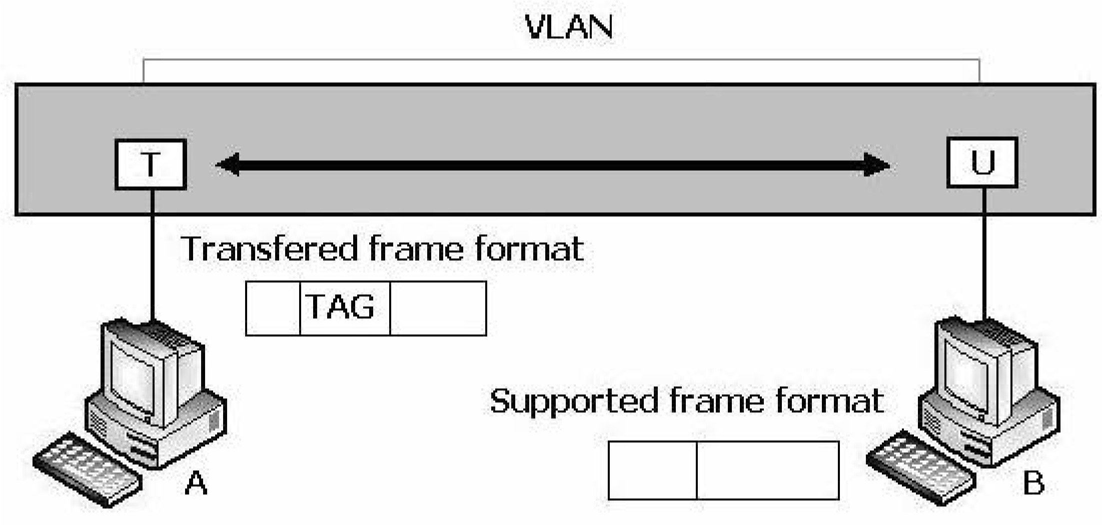
(disabled|port-based|dot1q) specifies the VLAN mode.

Note:

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

VLAN Mode: 802.1Q

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. In the following figure, two different types of devices want to communicate with each other. Since computer A support 802.1Q VLAN and computer B do not, you have to configure two ports both beneath the same VLAN group, and set left port to “Tagged”, right port to “Untagged”. Therefore, two devices will receive packet type as they desired.



4.0.3.1.2 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.

VLAN Commands

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.

Note:

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.

Parameters:

<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.

Parameters:

[<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.

Parameters:

<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.

Parameters:

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 list (eg. 3, 6-8)

show vlan filter [<LIST>]
Show VLAN filter setting.
Parameters:
[<LIST>] specifies the ports to be showed. If not entered, all ports' filter rules will be showed.

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.
Parameters:
<LIST> specifies the port list to be set

show port gvrp

Show GVRP status by port.

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

Set GARP timer.

Parameters:

<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.

Parameters:
<LIST> specifies the port list to be set

show gvrp statistics <LIST>
Show GVRP statistics by port.
Parameters:
<LIST> specifies the port list to be set

[**no**] **gvrp debug** [<**sys** | **err** | **pdu** | **db** | **gen** | **garp** | **gvrp** | **vlan**>]
Enable/disable GVRP debugging output.

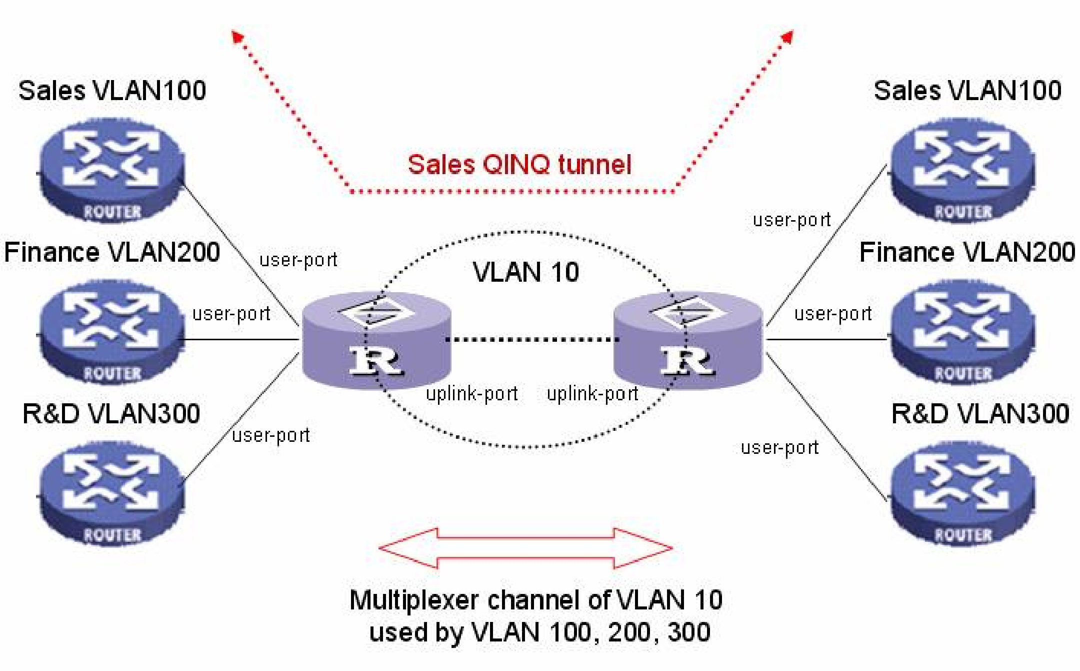
4.0.3.1.3 QinQ VLAN Setting

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification. Using the QinQ feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using QinQ expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets.

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks. QinQ is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer

2 protocol configurations of each customer without impacting the traffic of other customers.

The following figure is an example of QinQ VLAN application.



QinQ Commands

qinq enable

Enable QinQ.

[no] qinq

Disable QinQ.

qinq tpid <TPIDVAL>

Set QinQ tpid.

Parameters:

<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 userport 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 <1-25> <1-4094> <LIST>

Add QINQ tunnel.

Parameters:

<1-25> specifies the tunnel ID

<1-4094> specifies the VLAN ID

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

qinq tunnel delete <1-25>

Delete QinQ tunnel.

Parameters:

<1-25> specifies the tunnel ID

show qinq configuration

Show QinQ global and portal configuration

show qinq tunnel

Show QinQ tunnel information

For example, refer to the figure of QinQ application in previous page, a QinQ tunnel using VLAN10 wants to be created for Sales VLAN100 across the public network. Port1 on left-side VDLS2 IP DSLAM connects to Sales VLAN100 client. Port16 of switch connects to the public network. The following commands needs to be set:

```
qinq enable
qinq tpid 8100
qinq userport enable 1
qinq uplinkport enable 16
qinq tunnel add 1 10 1,16
```

4.0.3.2 Misc Configuration

[no] mac-age-time

Enable or disable MAC address age-out.

mac-age-time <6..1572858> Set MAC address age-out time.

Parameters:

<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 | 1/12>

Set broadcast storm filter mode to off, 1/2, 1/4, 1/8, 1/12

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.

4.0.3.3 Administration

4.0.3.3.0 Change Username/Password

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.

4.0.3.3.1 IP Configuration

User can configure the IP setting and fill in the new value.

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 IP DSLAM as dhcp client, it can get ip from dhcp server

Note:

If this command is set, the IP DSLAM will reboot.

show dhcp

show dhcp enable/disable

4.0.3.4 Port Mirroring

Port monitoring is a feature to redirect the traffic occurred on every port to a designated monitoring port on the IP DSLAM . With this feature, the network administrator can monitor and analyze the traffic on the entire LAN segment. In VDSL2 IP DSLAM, 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.

Note:

1. The default Port Monitoring setting is disabled.

2. The analysis port is dedicated as mirroring port with duplicated traffic flow from mirrored port. The ordinary network traffic is not available for the analysis port.

3. Any member port is not available for this function

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

Parameters:

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

4.0.3.5 Quality of Service

There are four transmission queues with different priorities in VDSL2 IP DSLAM: Highest, SecHigh, SecLow and Lowest. The switch will take packets from the four queues according to its QoS mode setting. If the QoS mode was set to “Disable”, the switch will not perform QoS on its switched network. If the QoS mode was set to “High Empty Then Low”, the switch will never exhaust packets from a queue until the queues with higher priorities are empty. If the QoS mode was set to “weight ratio”, the switch will exhaust packets from the queues according to the ratio. The default value of QoS mode is “weight 8:4:2:1.” That means the switch will first exhaust 8 packets from the queue with highest priority, and then exhaust 4 packets from the queue with second high priority, and so on.

When the switch received a packet, the switch has to decide which queue to put the received packet into. In VDSL2 IP DSLAM, the switch will put received packets into queues according to the settings of “802.1p Priority” and “Static Port Ingress Priority.” When the received packet is an 802.1p tagged packet, the switch will put the packet into a queue according to the 802.1p Priority setting. Otherwise, the switch will put the packet into a queue according the setting of Static Port Ingress Priority.

802.1p Priority: the 802.1p packet has a priority tag in its packet header. The range of the priority is 7~0. The VDSL2 IP DSLAM can specify the mapping between 802.1p priority and the four transmission queues. In the default setting, the packets with 802.1p priority 0~1 are put into the queue with lowest priority, the packets with 802.1p priority 2~3 are put into queue with second low priority, and so on.

Static Port Ingress Priority: each port is assigned with one priority 7~0. The priority of the packet received from one port is set to the same priority of the receiving port. When the priority of the received packet was determined, the packet is treated as an 802.1p packet with that priority and will be put into a queue according to the 802.1p Priority setting.

4.0.3.5.0 QoS Configuration

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.

Commands:

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

Set 802.1p 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.

Parameters:

<*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
```

4.0.3.5.1 Per Port Priority

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

Set port priority.

Parameters:

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

```
e.g. port priority disable 1-5
```

4.0.3.6 MAC Address Table

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 matches 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.

4.0.3.7 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.

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.

4.0.4 Protocol Related Configuration

4.0.4.0 STP/RSTP

[no] spanning-tree

Enable or disable spanning-tree.

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

Set spanning tree forward delay used, in seconds.

Parameters:

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

Note: 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.

Parameters:

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

Note: 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.

Parameters:

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

Note: 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.

Parameters:

<*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.

Parameters:

<*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.

Parameters:

<*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.

Parameters:

[<*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:

[no] spanning-tree debug

Enable or disable spanning tree debugging information.

spanning-tree protocol-version <stp | rstp>

Change spanning tree protocol version.

Parameters:

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.

Parameters:

[<*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.

Parameters:

[<*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.

Parameters:

[<*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.

Parameters:

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.

4.0.4.1 MSTP

[no] spanning-tree

Enable or disable multiple spanning tree.

[no] spanning-tree debug

Enable or disable multiple spanning tree debugging information.

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

Set spanning tree forward delay of CIST, in seconds.

Parameters:

<*4-3*0> specifies the forward delay, in seconds. Default value is 15.

Note: 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.

Parameters:

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

Note: 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.

Parameters:

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

Note: 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.

Parameters:

<*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.

Parameters:

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.

Parameters:

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

spanning-tree name [<*name-string*>]

Set spanning tree bridge name of CIST.

Parameters:

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

spanning-tree revision <*1-65535*>

Set spanning tree bridge revision of CIST.

Parameters:

<*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.

Parameters:

<*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.

Parameters:

<*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.

Parameters:

[<*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.

Parameters:

[<*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.

Parameters:

[<*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.

Parameters:

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.

Parameters:

<*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.

Parameters:

<*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.

Parameters:

<*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.

Parameters:

<*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.

Parameters:

<*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.

Parameters:

[<*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.

Parameters:

<*0-15*> specifies the MSTI instance ID.

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

Show specific port information of MST instance.

Parameters:
<*0-15*> specifies the MSTI instance ID.
<*1-26*> specifies port number.

show vlan spanning-tree

Show per VLAN per port spanning tree status.

4.0.4.2 SNMP

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

4.0.4.2.0 System Options

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.

Parameters:

<name-str> specifies the system name string.

e.g. snmp system-name SWITCH

snmp system-location <location-str>

Set agent location string.

Parameters:

<location-str> specifies the location string.

e.g. snmp system-location office

snmp system-contact <contact-str>

Set agent system contact string.

Parameters:

<contact-str> specifies the contact string.

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

show snmp system

Show SNMP system information.

4.0.4.2.1 Community Strings

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

Set SNMP community string.

Parameters:

<community-str> specifies the community string.

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

no snmp community <community-str>

Delete SNMP community string.

Parameters:

<community-str> specifies the community string.

e.g. no snmp community public

show snmp community

Show SNMP community strings.

4.0.4.2.2 Trap Managers

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

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

Parameters:

<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.

Parameters:

<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.

4.0.4.2.3 SNMP V3 VACM (optional)

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

Join a group.

Parameters:

<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.

Parameters:

<**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.

Parameters:

<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.

Parameters:

<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.

Parameters:

<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.

Parameters:

<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.

4.0.4.2.4 SNMP V3 USM (optional)

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

Setup SNMPv3 engine ID.

Parameters:

<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.

Parameters:

<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.

Parameters:

<user-name> specifies the user name.

e.g. no snmp usm-user testuser

show snmp usm-user

Show all SNMPv3 USM users.

4.0.4.3 IGMP

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (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

[**no**] **igmp debug** Enable/disable IGMP snooping debugging output.

show igmp <**status | router | groups | table**>
Show IGMP snooping information.
Parameters:
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.

4.0.4.4 802.1x

This IP DSLAM 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 IP DSLAM .

[**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.

Parameters:

<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.

Parameters:

<key-str> specifies shared key string.

radius-server nas <id-str>

Set 802.1x NAS identifier.

Parameters:

<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).

Parameters:

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

dot1x timeout tx-period <0..65535>

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

Parameters:

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

dot1x timeout supplicant <1..300>

Set 802.1x supplicant timeout (default: 30 seconds)

Parameters:

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

dot1x timeout radius-server <1..300>

Set radius server timeout (default: 30 seconds).

Parameters:

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

dot1x max-req <1..10>

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

Parameters:

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

dot1x timeout re-authperiod <30..65535>

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

Parameters:

<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.

Parameters:

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

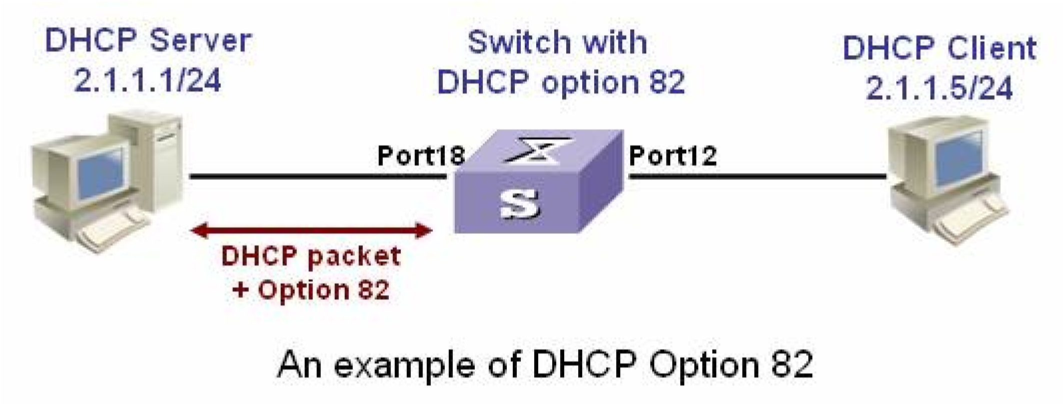
Show 802.1x per port information.

4.0.4.5 DHCP Relay & Option 82

DHCP is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts.

When the **DHCP Option 82** feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified. Option82 Information is inserted by the switch enabled option-82 feature when forwarding client-originated DHCP packets to a DHCP server (RFC 3046). Servers may use this information to implement IP address or other parameter assignment policies. This will significantly enhance the security of DHCP and effectively prevent the attack of DHCP flood.

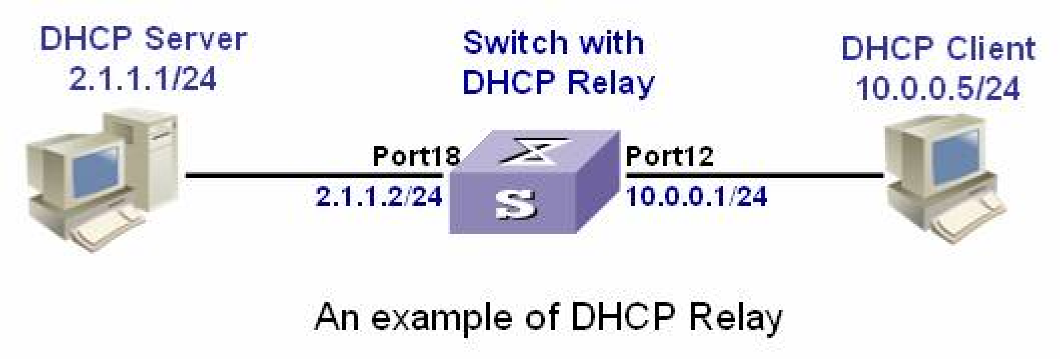
The following figure is an example of DHCP Option 82:



An example of DHCP Option 82

If the **DHCP relay** feature is enabled on the switch, it forwards requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on output interfaces. So DHCP server can provide IP addresses to clients spanning multiple subnets instead of deploying a DHCP server on every subnet.

The following figure is an example of DHCP relay:



An example of DHCP Relay

The following commands are provided for DHCP option82 / relay configuration:

[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

For example, refer to the figure of DHCP option 82 in the previous page, use the following commands to achieve:

```
dhcp-option82
dhcp router 18
dhcp-option82 enable 12
```

Refer to the example figure of DHCP relay application, use the following commands to achieve:

```
dhcp-relay
dhcp router 18
dhcp-relay enable 10.0.0.1 12
```

4.0.4.6 LLDP

Link Layer Discovery Protocol (LLDP) operates on data link layer. It stores and maintains the information about the local device and the devices directly connected to it for network administrators to manage networks through NMS (network management systems). In LLDP, device information is encapsulated in LLDP PDUs in the form of TLV (meaning type, length, and value) triplets and is exchanged between directly connected devices. Information in LLDP PDUs received is restored in its MIB.

Note:

Currently the LLDP neighbor(s) can be seen through the console only. SNMP browser will be supported in the future.

LLDP Operation Mode

LLDP can operate in one of the following modes.

LLDP Mode	Description
TxRx mode	A port in this mode sends and receives LLDP PDUs
Tx mode	A port in this mode only sends LLDP PDUs
Rx mode	A port in this mode only receives LLDP PDUs
Disable mode	A port in this mode does not send or receive LLDP PDUs

LLDP is initialized when an LLDP-enabled port changes to operate in another LLDP operating mode. To prevent LLDP from being initialized too frequently, LLDP undergoes a period before being initialized on an LLDP-enabled port when the port changes to operate in another LLDP operating mode. The period is known as initialization delay, which is determined by the re-initialization delay timer.

Sending LLDP PDUs

A LLDP-enabled device operating in the TxRx mode or Tx mode sends LLDP PDUs to its directly connected devices periodically. It also sends LLDP PDUs when the local configuration changes to inform the neighboring devices of the change timely. In any of the two cases, an interval exists between two successive operations of sending LLDP PDUs. This prevents the network from being overwhelmed by LLDP PDUs even if the LLDP operating mode changes frequently.

To enable the neighboring devices to be informed of the existence of a device or an LLDP operating mode change (from the disable mode to TxRx mode, or from the Rx mode to Tx mode) timely, a device can invoke the fast sending mechanism. In this case, the interval to send LLDP PDUs changes to one second. After the device sends specific number of LLDP PDUs, the interval restores to the normal. (A neighbor is discovered when a device receives an LLDPDU and no information about the sender is locally available.)

Receiving LLDP PDUs

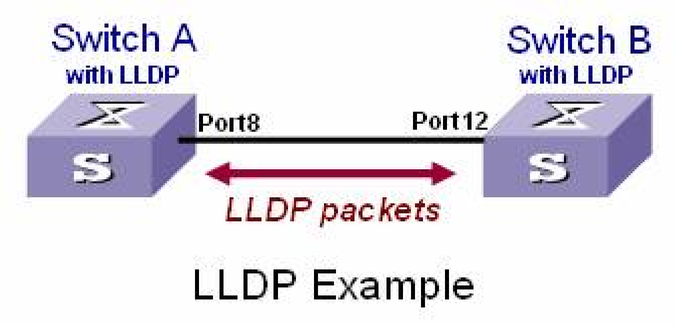
An LLDP-enabled device operating in the TxRx mode or Rx mode validates the TLVs carried in the LLDP PDUs which receive and store the valid neighboring information. An LLDP PDU also carries a TTL (time to live) setting with it. The information about a neighboring device maintained locally ages out when the corresponding TTL expires.

The TTL of the information about a neighboring device is determined by the following expression:

TTL = LLDP hold time × LLDP PDU sending interval (hello-time)

You can set the TTL by configuring the LLDP hold-time and hello-time. Note that the TTL can be up to 65535 seconds. TTL longer than it will be rounded off to 65535 seconds.

The following figure is an example of LLDP connection:



LLDP Commands

[no] lldp

Enable/Disable LLDP global option

lldp hello-time <5-32768>

Set LLDP hello time which is the time interval between the transmission LLDP info packets. The range is from 5 to 32768 seconds. Default is 30 seconds.

lldp hod-time <2-10>

Set LLDP hold time. The range is from 2 to 10. Default is 4.

lldp port <rx|tx|both> [<PORT-LIST>]

Set LLDP port-based receive and transmit packet mode.

Parameters:

<rx|tx|both> **rx:** the port only receive LLDP packets; **tx:** the port only transmit LLDP packets;

both: the port can receive and transmit LLDP packets.

[<PORT-LIST>] specifies the ports to be set. If not specified, all ports are set.

no lldp port [<PORT-LIST>]

Disable LLDP port-based receive and transmit packet mode.

Parameters:

[<PORT-LIST>] specifies the ports to be set. If not specified, all ports are set.

show lldp

Show the LLDP global option, all the ports configuration and the neighbor’s information.

show lldp port [<PORT-LIST>]

show LLDP port configuration and the neighbor’s information..

Parameters:

[<PORT-LIST>] specifies the ports to be set. If not specified, all ports are set.

An LLDP example refer to the figure in previous page, the following commands will be used:

lldp (for switch A & B)

lldp port both 8 (for switch A)

lldp port both 12 (for switch B)

show lldp port 8 (for switch A to see the switch B’s LLDP info learned by Switch A)

```
Port8 Information
State : RX and TX
Pkt Tx : 3868
Pkt Rx : 46409
Neighbor Count : 1
Neighbor 1 information
TTL Time : 5879
Class ID : 56:78:17:45:25:00
Port ID : port(12)
System Name :
System Description : Switch v2.16
Port Description : Port 12
Port SetSpeed : Auto
Port ActualSpeed : FULL-100
```

4.0.5 Syslog

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

Setting the syslog server and loging level.

Parameters:

<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

4.0.6 Reboot switch

4.0.6.0 Reset to Default

erase startup-config

Reset configurations to default factory settings at next boot time.

4.0.6.1 Restart

boot

Reboot (warm-start) the switch.

4.0.7 TFTP Function

4.0.7.0 TFTP Firmware Update

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

Download firmware from TFTP server.

Parameters:

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

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

4.0.7.1 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**.

Parameters:

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

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

4.0.7.2 Backup Configure 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**.

Parameters:

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

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

4.0.8 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.

Note:

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

4.0.8.0 IPv4 ACL commands

no acl <group id>

Delete ACL group.

Parameters:

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

e.g. no acl 1

no acl count <group id>

Reset the ACL group count

Parameters:

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

Enable/Disable acl <group id>

Reset the ACL group count

Parameters:

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

show acl [<group id>]

Show all or ACL group information by group id

Parameters:

<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.

Parameters:

(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.

Parameters:

(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

4.0.8.1 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.

Parameters:

(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

4.0.8.2 SIP/SMAC Binding

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.

Parameters:

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

e.g. no bind 1

show bind [<group id >]

Show Binding group information.

Parameters:

<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.

Parameters:

< 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.

4.1 Remote Network Management

IP Setting

You must setup the “IP Address” with the local serial console port (RS-232 Port), and then you can use this IP address to control this Ethernet Switch by **WEB.** Or you can change your computer’s IP domain same with Ethernet Switch. Then use the default IP address to control this Switch

Network control by “WEB”

1.It provide a WEB browser to manage and monitor the switch, that default values are as followings ：

If you need change IP address in first time，you can use console mode to modify it.

Default IP Address：192.168.16.249

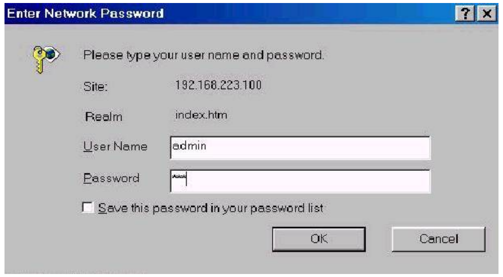
Subnet Mask： 255.255.255.0

Default Gateway：192.168.16.1

User Name：admin

Password： 123

2. Please access **http://192.168.16.249** via web ui to browser the management page, please enter user name and password as above.



Enter Network Password

Please type your user name and password.

Site: 192.168.223.100

Realm index.htm

User Name admin

Password ***

□ Save this password in your password list

This is the ***Web Management Home Overview***

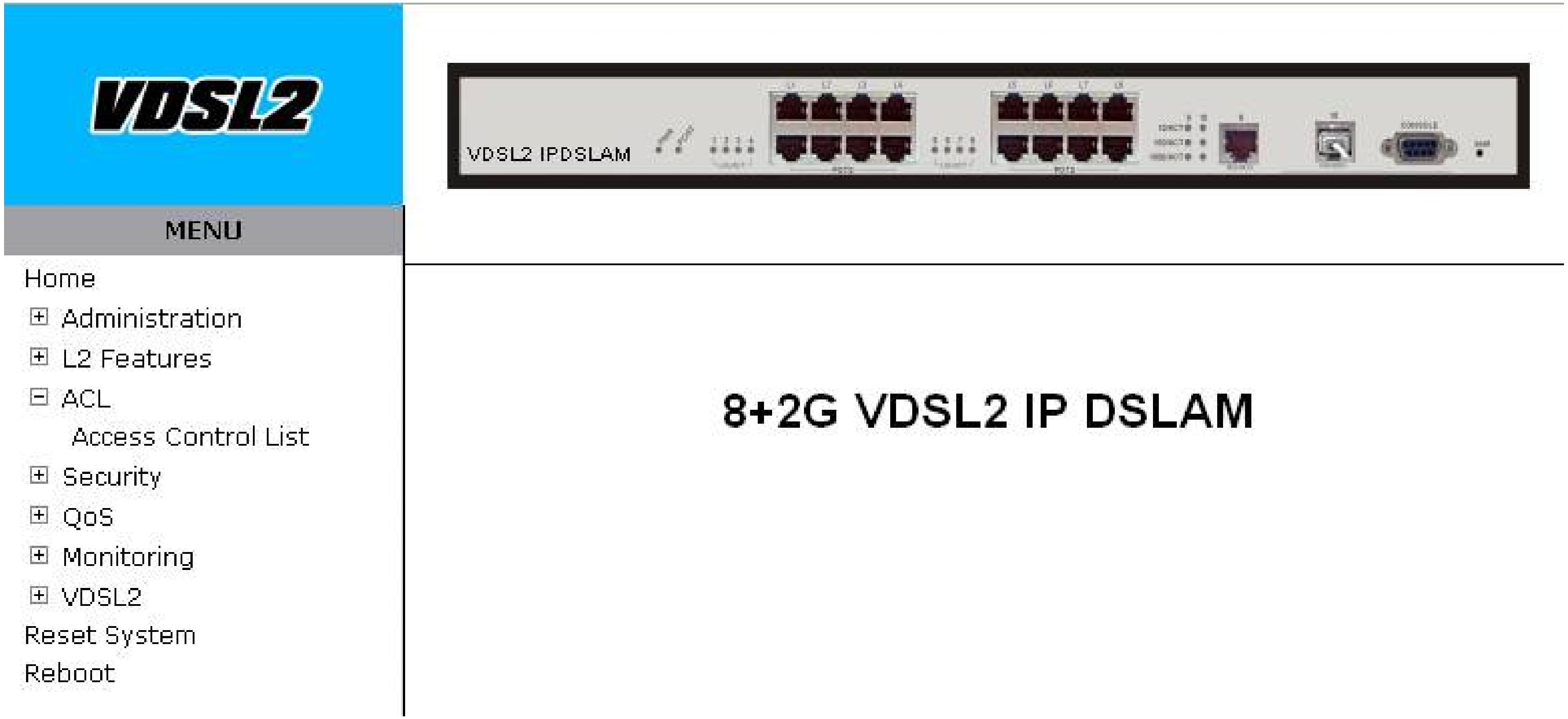


Fig. 4.1 Web Management Home Overview

4.2 Administration

There are many management functions can be set or performed if you expand the submenus of **Administrator** in MENU area. These functions are:

- **IP address Setting (See section 4.2.0)**
- **Switch Settings (See section 4.2.1)**
- **Console Port information(See section 4.2.2)**
- **Port Configuration (See section 4.2.3)**
- **SNMP Configuration (See section 4.2.4)**
- **Syslog Setting (See section 4.2.5)**
- **Firmware Update (See section 4.2.6)**
- **Configuration Backup (See section 4.2.7)**

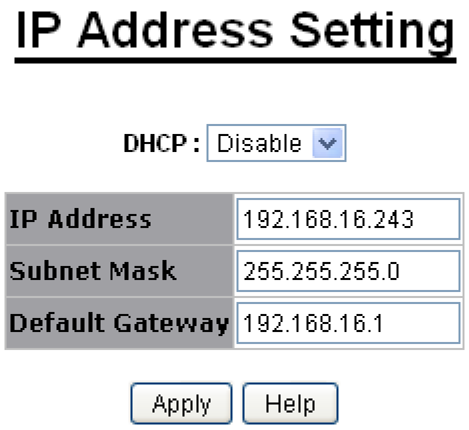
4.2.0 IP Address Setting

User can see and modify the IP address, subnet mask and default gateway in this page, then clicks "Apply" button to confirm (save) the settings, then the switch **reboot** must be done to activate the updates. The IP address can be statically set or dynamically be assigned by enabling DHCP option.

Notes:

1.If any of the value is changed in this field, reboot is necessary.

2.The “DHCP” is dhcp client function, you can choose disable or enable.



IP Address Setting

DHCP : Disable

IP Address	192.168.16.243
Subnet Mask	255.255.255.0
Default Gateway	192.168.16.1

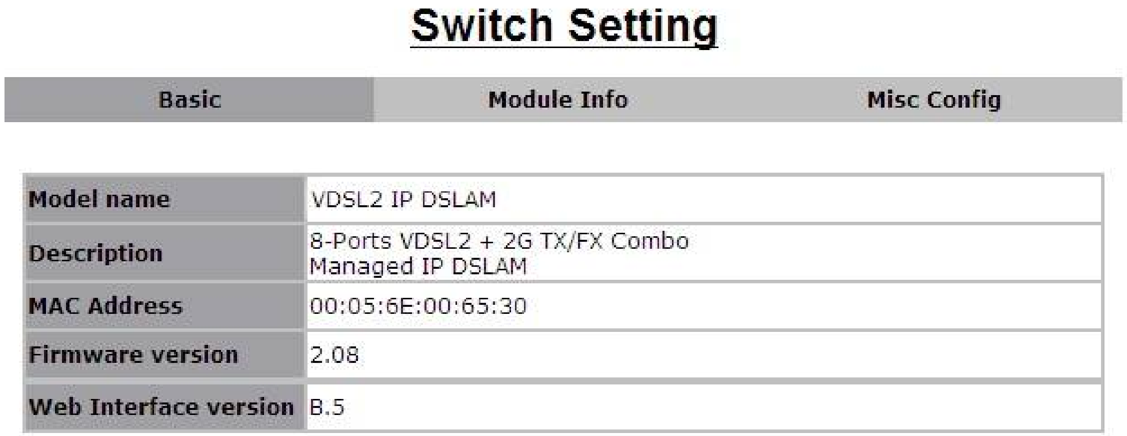
Fig. 4.2.0 IP Address Setting

4.2.1 Switch Setting

4.2.1.0 Basic

All information in **Basic** page is all read only, user can't modify the contents.

Model name: Display the switch's model name.
Description: Display the name of device type.
MAC Address: The unique hardware address assigned by manufacturer (default)
Firmware version: Display the IP DSLAM's driver firmware version.
Web Interface version: Display the switch's web interface firmware version.



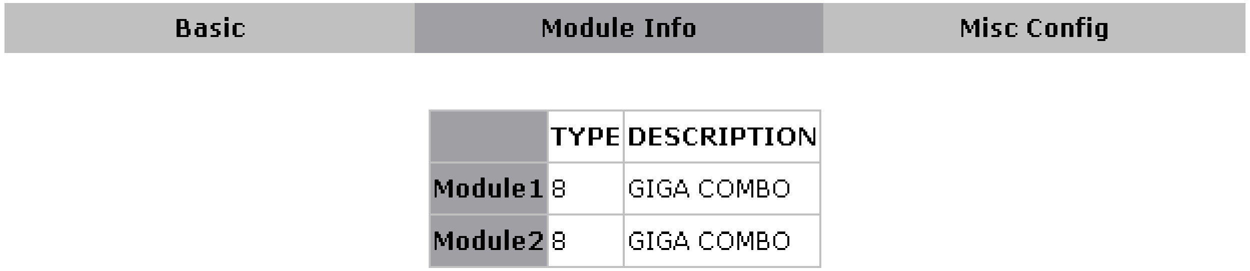
Switch Setting

Model name	VDSL2 IP DSLAM
Description	8-Ports VDSL2 + 2G TX/FX Combo Managed IP DSLAM
MAC Address	00:05:6E:00:65:30
Firmware version	2.08
Web Interface version	B.5

Fig. 4.2.1.0 Switch Setting

4.2.1.1 Module Info

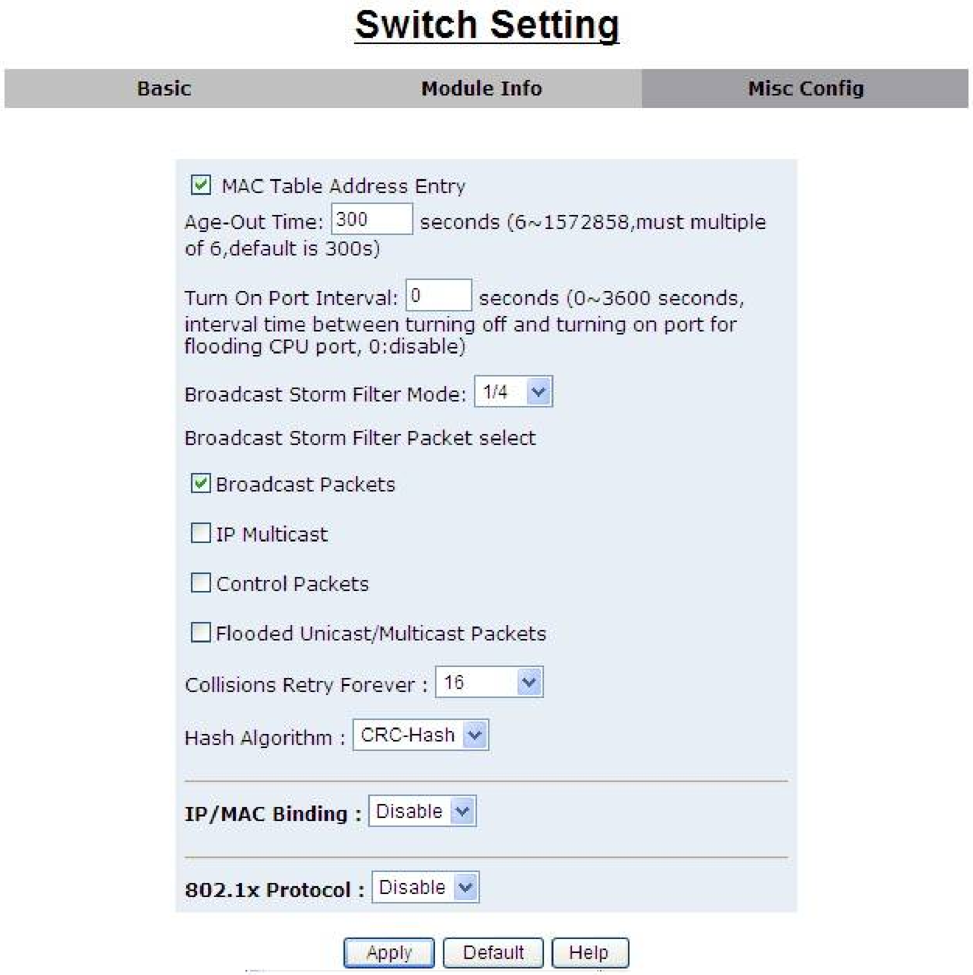
All information in this field is read only, user can't modify its contents. It is only to display the module port information.



	TYPE	DESCRIPTION
Module1	8	GIGA COMBO
Module2	8	GIGA COMBO

Fig. 4.2.1.1 Module Info

4.2.1.2 MISC CONFIG



Switch Setting

☑ 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: 1/4

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

Fig. 4.2.1.2 MISC CONFIG

MAC Address Age-out Time: Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 6~1572858 seconds. **Default is 300 seconds.** The value is a multiple of 6.

Turn on Port Interval: 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.

Broadcast Storm Filter Mode: To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's ingress bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold value are 1/2, 1/4, 1/8, 1/12, and off. **Default is 1/4. If 1/4 can not solve broadcast storm, please config higher value to 1/8 or 1/12.**

Broadcast Storm Filter Packets Select: To select broadcast storm Filter Packets type. If no packets type by selected, mean can not filter any packets .The Broadcast Storm Filter Mode will show OFF. Collisions Retry Forever: In half duplex, collision-retry maximum is 16, 32, or 48 times and packet will be dropped if collisions still happen. In default (Disable), system will retry forever if collisions happen. **Broadcast strom filter packet of default value was selected.**

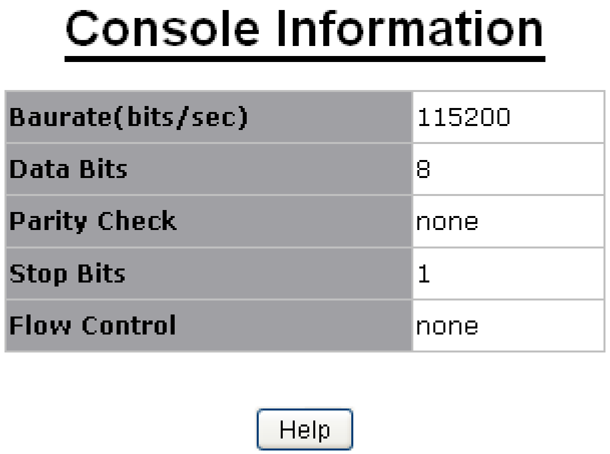
Collision Retry Forever: Default value is 16.
Hash Algorithm: Select Hash Algorithm.
IP/MAC Bing: Enable or disable SMAC and SIP binding.
802.1x Protocol: Enable or disable 802.1x protocol.

4.2.2 Console Port Information

Console is a standard UART (RS-232) interface to communicate with Serial Port.

User can use windows HyperTerminal program to link the switch. Connect To -> Configure:

Bits per seconds: **115200**
Data bits: **8**
Parity: **none**
Stop Bits: **1**
Flow control: **none**



Console Information

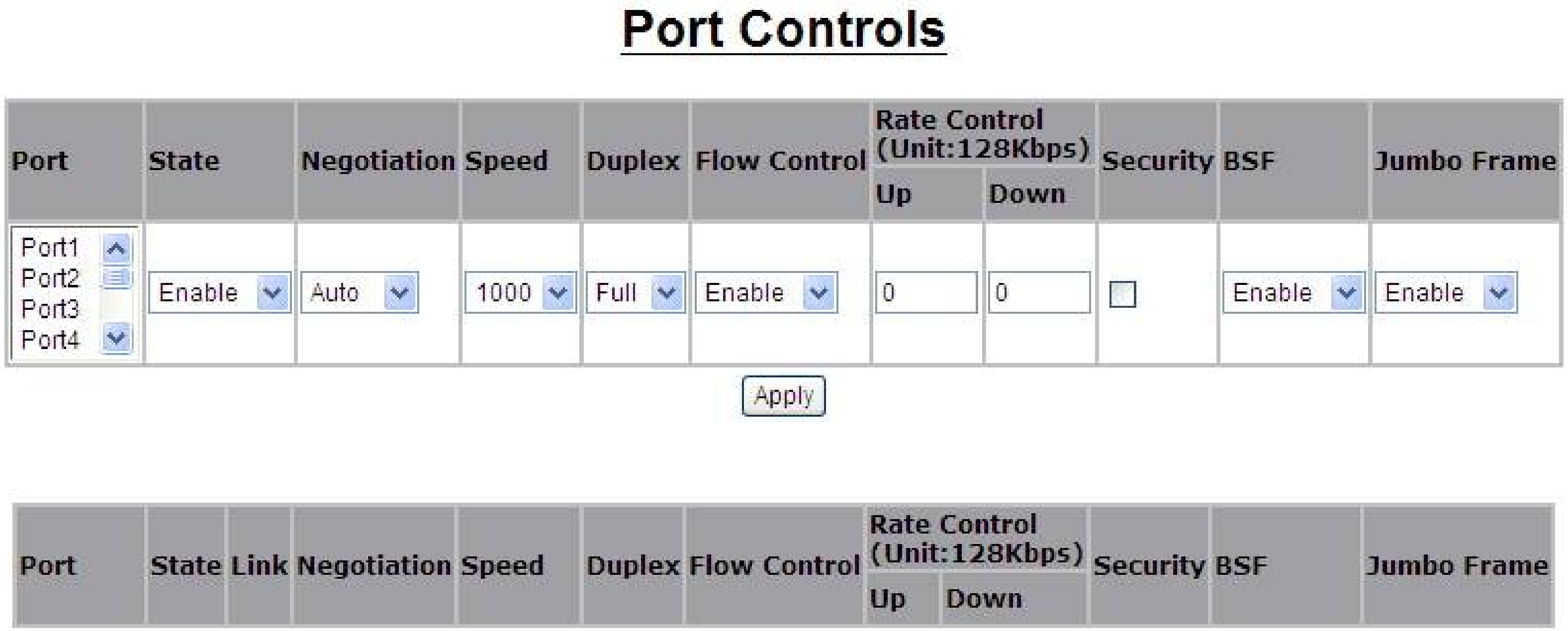
Baurate(bits/sec)	115200
Data Bits	8
Parity Check	none
Stop Bits	1
Flow Control	none

Fig. 4.2.2 Console Information

4.2.3 Port Configuration

4.2.3.0 Port Controls

The following webpage is to provide the display and modification for the port settings. Use the dropdown in Port field to select one or multiple ports in the upper control area. The lower display area will show the port settings for the selected port(s). Use the other control fields in the upper area to modify the port settings for the selected port(s). Press Apply to save and activate the port settings.



Port Controls

Port	State	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit:128Kbps)		Security	BSF	Jumbo Frame
						Up	Down			
Port1 Port2 Port3 Port4	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
							Up	Down			

Fig. 4.2.3.0 Port Controls

- **State:** User can disable or enable this port.

- **Negotiation:** User can set auto negotiation mode is Auto, Nway (specify the speed/duplex on this port and enable auto-negotiation), Force of per port.

- **Speed:** User can set 1000Mbps, 100Mbps or 10Mbps speed on Port9~Port10 (depend on module card mode).

- **Duplex:** User can set full-duplex or half-duplex mode of per port.

- **Flows control:**

Full: User can set flow control function is enable or disable in full mode.
Half: User can set backpressure is enable or disable in half mode.

- **Rate Control(Traffic shaping):** port1 ~ port 8, supports by-port Up(ingress) and Down(egress) rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate at 1Mbps and ingress rate at 500Kbps. Device will perform flow control or backpressure to confine the ingress rate to meet the specified rate.

- **Up(Ingress):** Type the port effective ingress rate. The valid range is 0 ~ 8000. The unit is 128Kbps.

0: disable rate control.
1 ~ 8000: valid rate value

- **Down(Egress):** Type the port effective egress rate. The valid range is 0 ~ 8000. The unit is 128Kbps.

0: disable rate control.

1 ~8000: valid rate value.

- **Port Security:** A port in security mode will be "locked" without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings, and then click Apply to change on this page.

- **BSF:** User can disable/Enable port broadcast storm filtering option by port. The filter mode and filter packets type can be select in Switch Setting > Misc Config page.

- **Jumbo Frame:** User can disable/Enable port jumbo frame option by port. When port jumbo frame is enable, the port forward jumbo frame packet

Note2:

Rate control(Traffic shaping) configuration example. The valid range is 0 ~ 8000. The unit is 128Kbps.

Rate	256k	512K	1M	2M	4M	8M	10M	20M	30M	40M	50M	60M	70M	80M	90M
Up(Ingress)	2	4	8	16	32	64	80	160	240	320	400	480	560	640	720
Down(Egress)	2	4	8	16	32	64	80	160	240	320	400	480	560	640	720

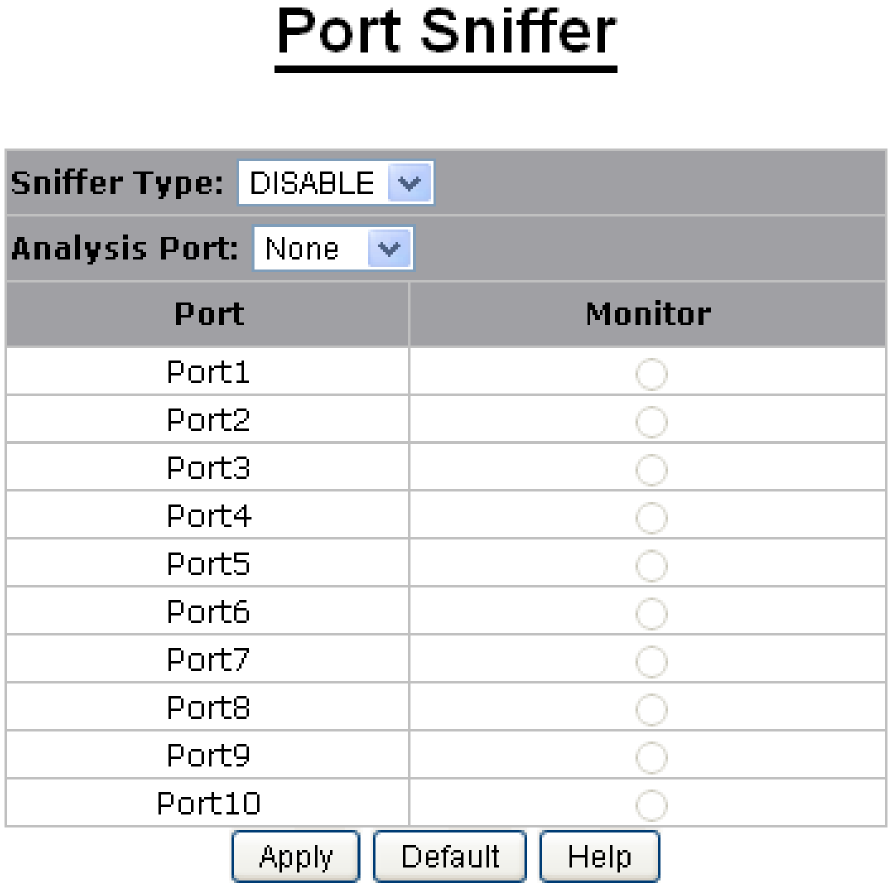
4.2.3.1 Port Sniffer

The Port Sniffer (mirroring) is a method for monitor traffic in switched networks. Traffic through a port can be monitored by one specific port. That is, traffic goes in or out a monitored port will be duplicated into sniffer port.

Sniffer Type: Select a sniffer mode: Disable / Rx / Tx / Both.
Analysis (Monitoring) Port: It' means Analysis port can be used to see the traffic on another port you want to monitor. You can connect Analysis port to LAN analyzer.
Monitored Port: The port you want to monitor. The monitor port traffic will be copied to Analysis port. You can select one monitor ports in the IP DSLAM. User can choose which port that they want to monitor in only one sniffer type.

Notes:

1. The Analysis port is dedicated for monitoring usage. That is the ordinary port function will be unavailable.
2. If you want to disable this function, you must select monitor port to none.



Port Sniffer

Sniffer Type: DISABLE

Analysis Port: None

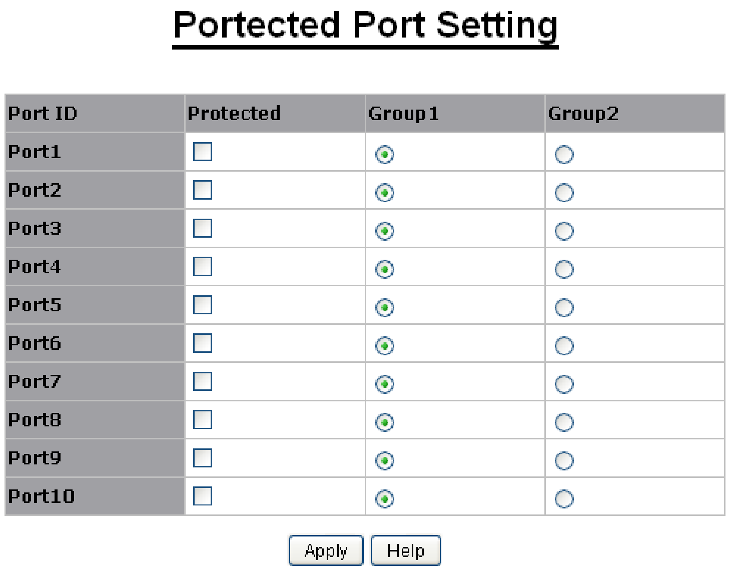
Port	Monitor
Port1	○
Port2	○
Port3	○
Port4	○
Port5	○
Port6	○
Port7	○
Port8	○
Port9	○
Port10	○

Fig. 4.2.3.1 Port Sniffer

4.2.3.2 Protected Port

There are two protected port groups. Ports in different groups can't communicate each other.

In the same group, protected ports can't communicate each other, but can communicate with unprotected ports. Unprotected ports can communicate with any ports, including protected ports. In default, all ports are in Group1 and not protected.



Portected Port Setting

Port ID	Protected	Group1	Group2
Port1	□	●	○
Port2	□	●	○
Port3	□	●	○
Port4	□	●	○
Port5	□	●	○
Port6	□	●	○
Port7	□	●	○
Port8	□	●	○
Port9	□	●	○
Port10	□	●	○

Fig. 4.2.3.2 Protected Port Setting

For example, in the above configuration page for protected port, Port4 in Group2, other ports in Group1, and both Port1& Port2 are protected. These settings provide Port4 can't communicate with other ports in Group1. Port1 & Port2 can't communicate each other but can communicate with other ports in Group1.

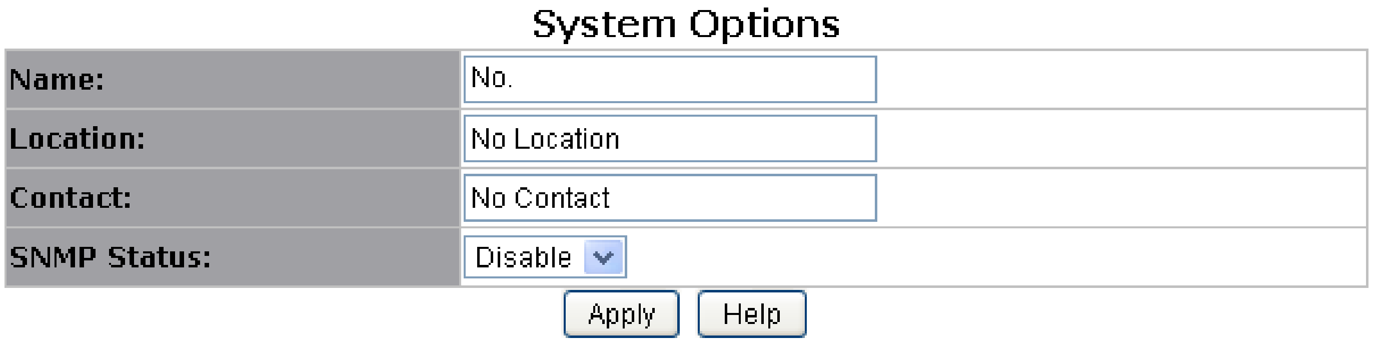
4.2.4 SNMP Configuration

Any Network Management platform running the simple Network Management Protocol (SNMP) can manage the switch, provided the Management Information Base (MIB) is installed correctly on the management station. The SNMP is a Protocol that governs the transfer of information between management station and agent.

4.2.4.0 System Options

Use this page to define management stations as trap managers and to enter SNMP community strings. User can also define a name, location, and contact person for the switch. Fill in the system options data, and then click Apply to update the changes on this page.

Name: Enter a name to be used for the switch.
Location: Enter the location of the switch.
Contact: Enter the name of a person or organization.
SNMP Status: Enable/Disable SNMP Function



System Options

Name:	No.
Location:	No Location
Contact:	No Contact
SNMP Status:	Disable

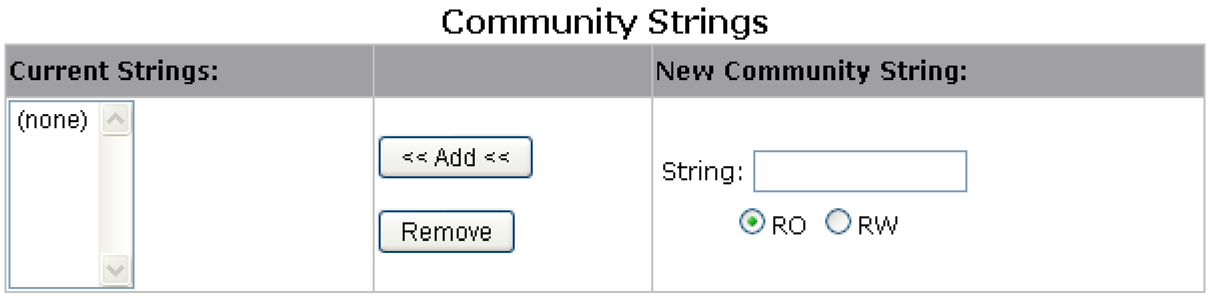
Fig. 4.2.4.0 System Options

4.2.4.1 Community strings

Serve as passwords and can be entered as one of the following:

RO: Read only. Enables requests accompanied by this string to display MIB-object information.

RW: Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.



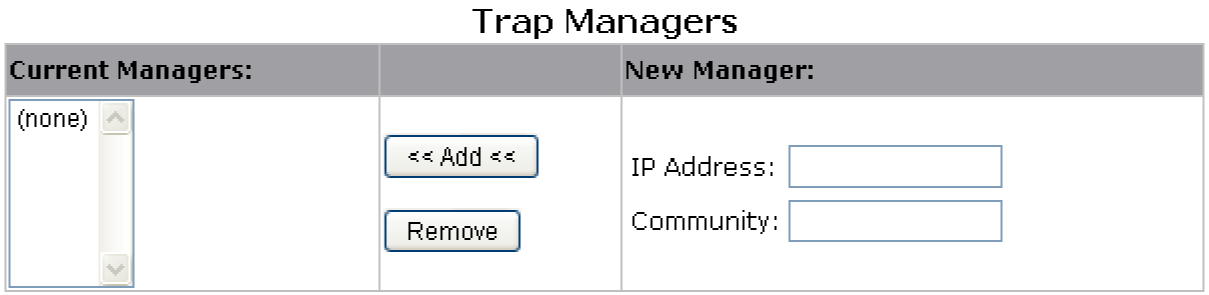
Community Strings

Current Strings:		New Community String:
(none)		String: ____ ● RO ○ RW

Fig. 4.2.4.1 Community strings

4.2.4.2 Trap Manager

Trap Manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string.



Trap Managers

Current Managers:		New Manager:
(none)	<< Add << Remove	IP Address: Community:

Fig. 4.2.4.2 Trap Manager

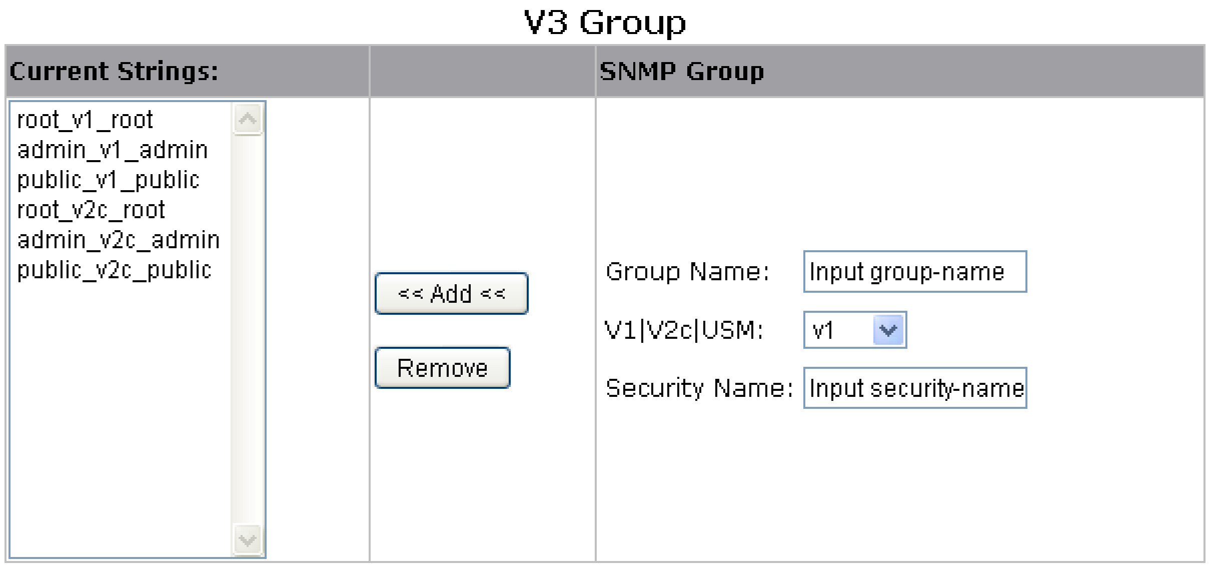
4.2.4.3 SNMPv3 Group

Maintain SNMPv3 group.

Group Name: specifies the group name.

v1 | v2c | USM: specifies the security model.

Security Name: specifies the security name.



Current Strings:
root_v1_root
admin_v1_admin
public_v1_public
root_v2c_root
admin_v2c_admin
public_v2c_public

Group Name: Input group-name

V1|V2c|USM: v1

Security Name: Input security-name

Fig. 4.2.4.3 SNMPv3 Group

4.2.4.4 SNMPv3 View

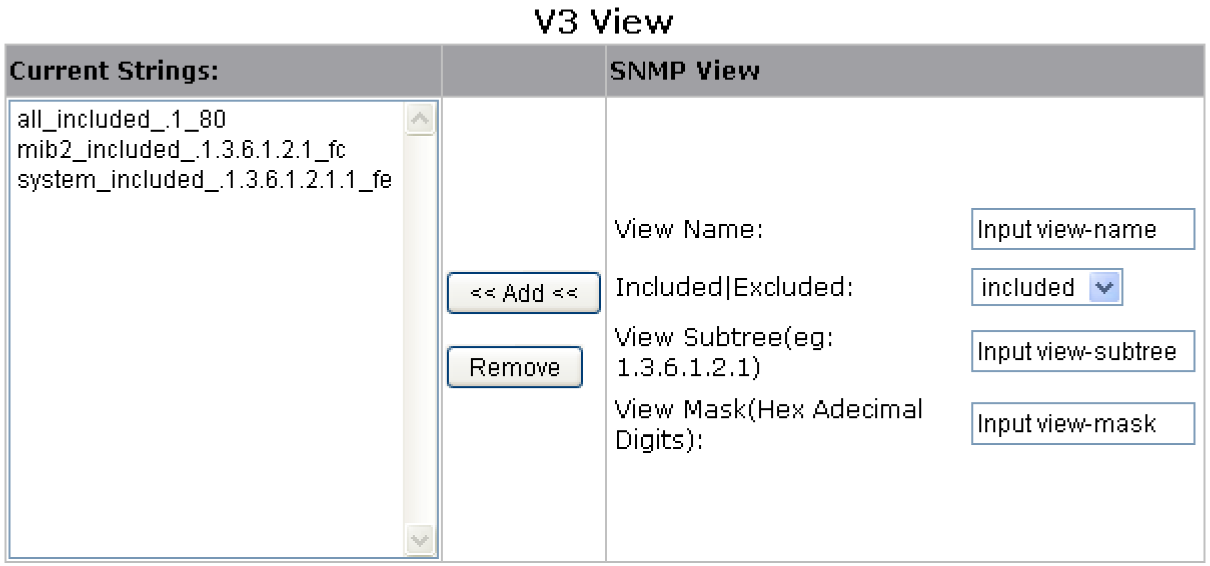
Maintain SNMPv3 view.

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.



V3 View

Current Strings:		SNMP View	
all_included_.1_80 mib2_included_.1.3.6.1.2.1_fc system_included_.1.3.6.1.2.1.1_fe		View Name:	Input view-name
	<< Add <<	Included|Excluded:	included
	Remove	View Subtree(eg: 1.3.6.1.2.1)	Input view-subtree
		View Mask(Hex Adecimal Digits):	Input view-mask

Fig. 4.2.4.4 SNMPv3 View

4.2.4.5 SNMPV3 ACCESS

Group Name: specifies the group name.

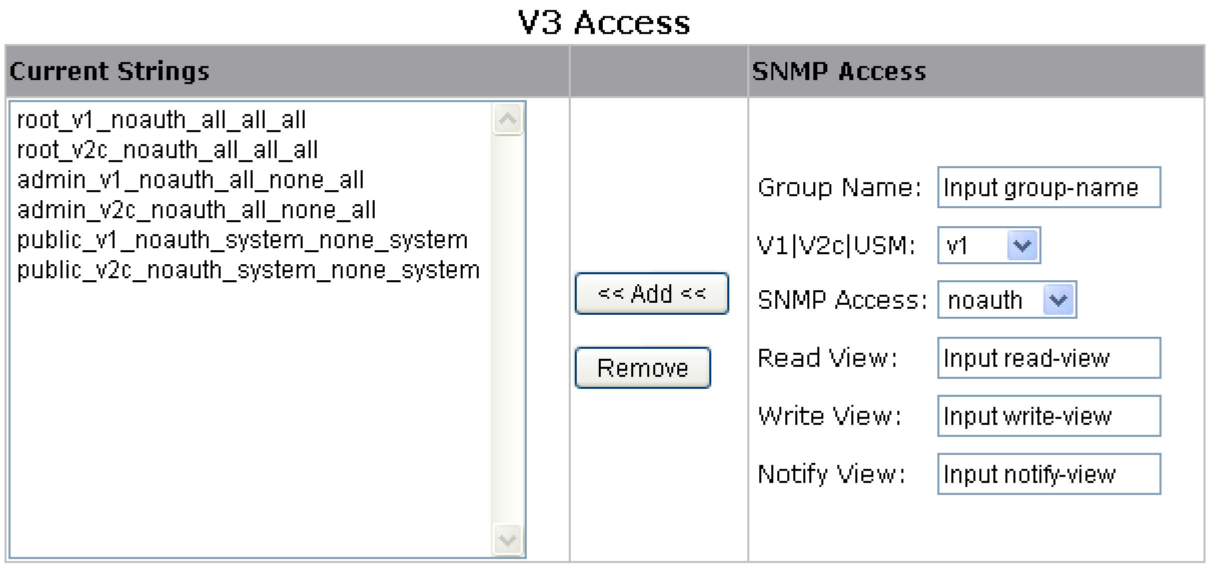
v1 | v2c | USM: specifies the security model.

SNMP Access: specifies the security level (**noauth | auth | authpriv**)

Read View: specifies the access read view name.

Write Name: specifies the access write view name.

Notify Name: specifies the access notify view name.



root_v1_noauth_all_all_all
root_v2c_noauth_all_all_all
admin_v1_noauth_all_none_all
admin_v2c_noauth_all_none_all
public_v1_noauth_system_none_system
public_v2c_noauth_system_none_system

Group Name:	Input group-name
V1|V2c|USM:	v1
SNMP Access:	noauth
Read View:	Input read-view
Write View:	Input write-view
Notify View:	Input notify-view

Fig. 4.2.4.5 SNMPV3 ACCESS

4.2.4.6 SNMPv3 USM-User

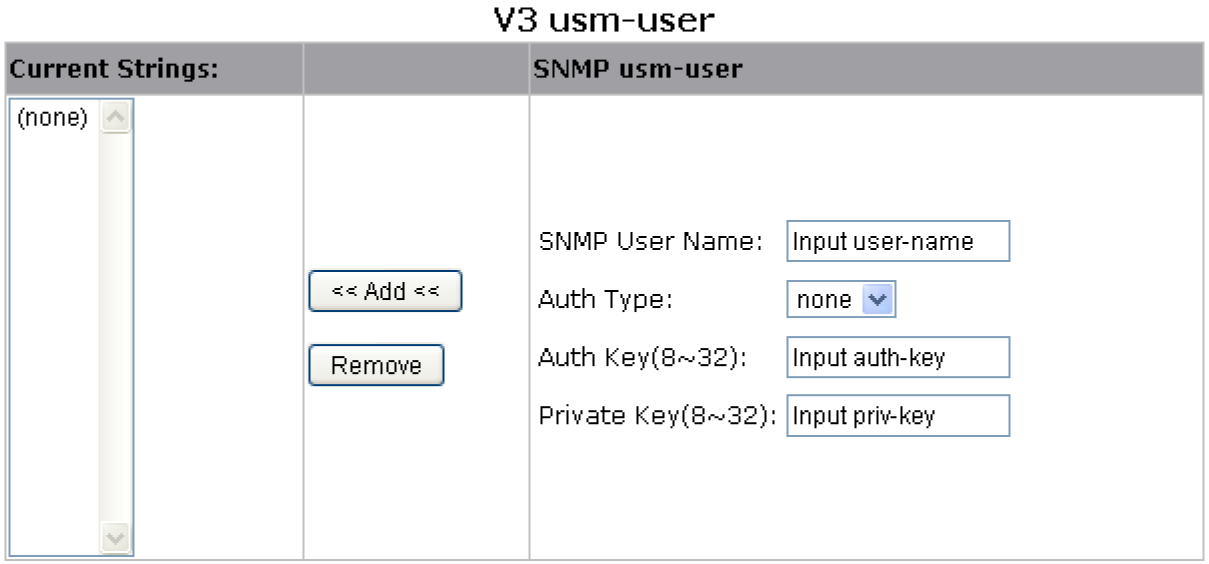
Maintain SNMPv3 USM-user.

User Name: Specifies the user name (should be the security name defined in group)

Auth Type: Specifies the authorization type (**md5 / none**)

Auth-Key: Specifies the authorization key (8~32 chars)

Private Key: Specifies the encrypt key (8~32 chars)



V3 usm-user

Current Strings:		SNMP usm-user
(none)	<< Add << Remove	SNMP User Name: Input user-name Auth Type: none Auth Key(8~32): Input auth-key Private Key(8~32): Input priv-key

Fig. 4.2.4.6 SNMPv3 USM-User

4.2.5 Syslog

This system supports syslog sent to a remote syslog server. Currently system will do syslog for 3 events: **cold start, warm start and link change.** In this page, user needs to setup the following parameters to activate the syslog:

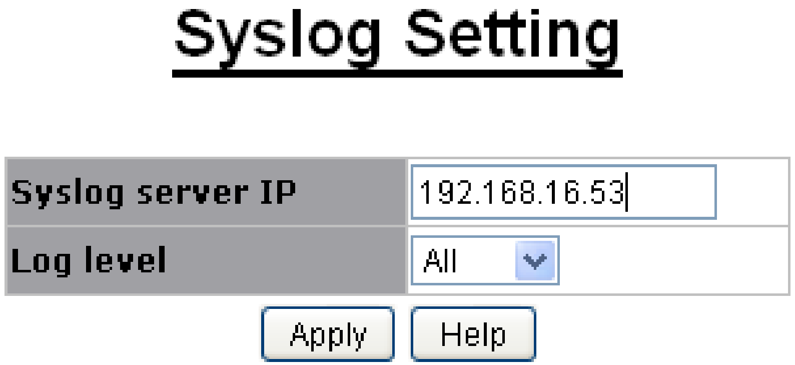
Syslog server IP: The IP address of remote syslog server
Log level: None / Major / All

None : never send syslog message to syslog serverme, and Max Age parameters of the root bridge, regardless of how it is configured.

Major : only send major syslog to syslog server, eg: link up/down, system warm/cold start

All : send all syslog message to syslog server.

Then click Apply button to activate the syslog function.

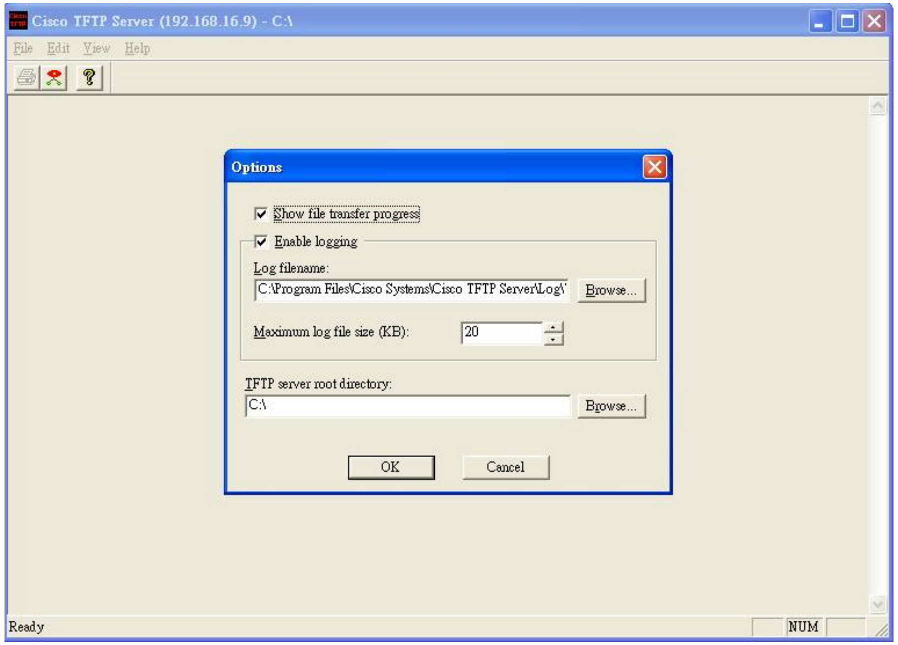


Syslog Setting

Syslog server IP	192.168.16.53
Log level	All

Fig.4.2.5 Syslog

The following example figure shows the syslog server application (e.g. Tftpd32.exe) got the messages from switch which link status is changed on port 9.



☑ Show file transfer progress

☑ Enable logging

Log filename: C:\Program Files\Cisco Systems\Cisco TFTP Server\Log\

Maximum log file size (KB): 20

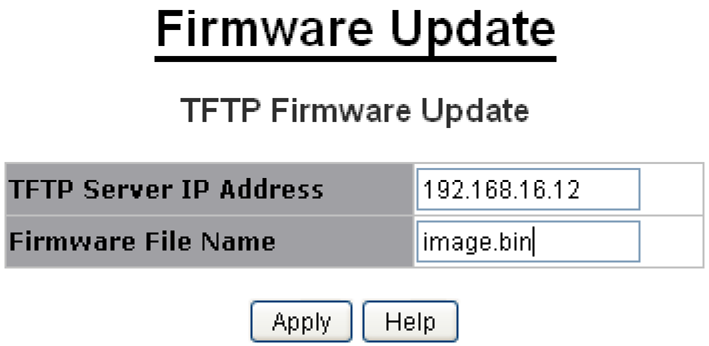
TFTP server root directory: C:\

4.2.6 Firmware Update

This system supports firmware update through two different ways: TFTP and HTTP.

4.2.6.0 TFTP Update

Use this page to assign a TFTP server IP address and an existing firmware image file. Then press Apply button to start the firmware update process.



Firmware Update

TFTP Firmware Update

TFTP Server IP Address	192.168.16.12
Firmware File Name	image.bin

Fig.4.2.6.0 TFTP Update

The firmware image will first update to the RAM area in system. Hit the Update Firmware button to confirm to write to the system's flash memory.

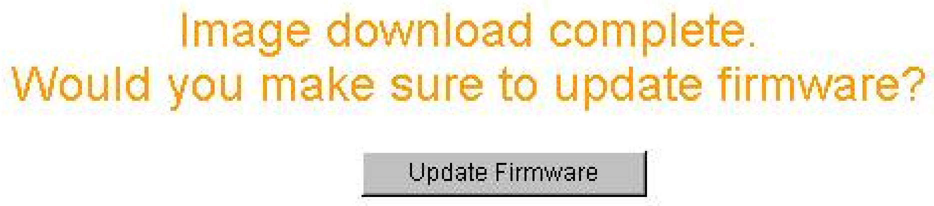
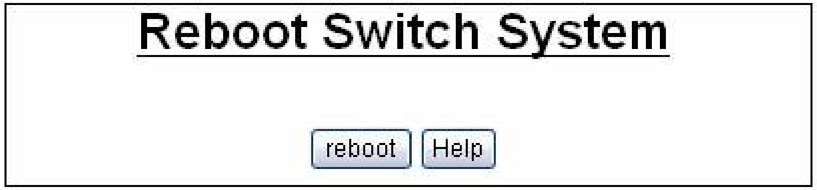


Image download complete.
Would you make sure to update firmware?

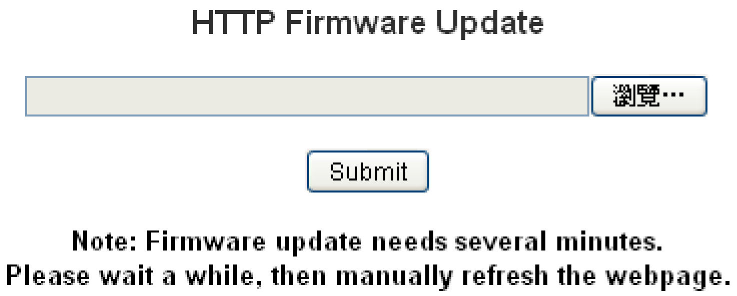
When the whole process is completed, system needs to be rebooted by pressing the reboot button to activate the new firmware.



Reboot Switch System

4.2.6.1 HTTP Update

An alternative for firmware updating is using HTTP transfer. Just like the file copy in Windows, select the valid firmware image file to be uploaded to the switch and hit Submit to start the updating process. This is easier than ordinary TFTP file transfer.


HTTP Firmware Update

Note: Firmware update needs several minutes.
Please wait a while, then manually refresh the webpage.

Fig.4.2.6.1 HTTP Update

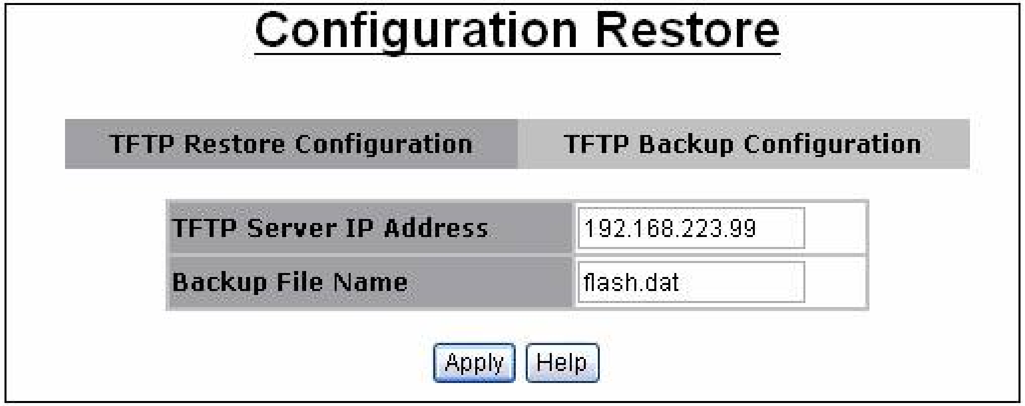
When the firmware image is completely uploaded, system will automatically be rebooted.

4.2.7 Configuration Backup

Just like the firmware update, this system also supports configuration backup/restore through either TFTP or HTTP transfer.

4.2.7.0 TFTP Restore Configuration

Use this page to assign a TFTP server IP address and an existing configuration filename to be restored. Then press Apply button to start the restore process.

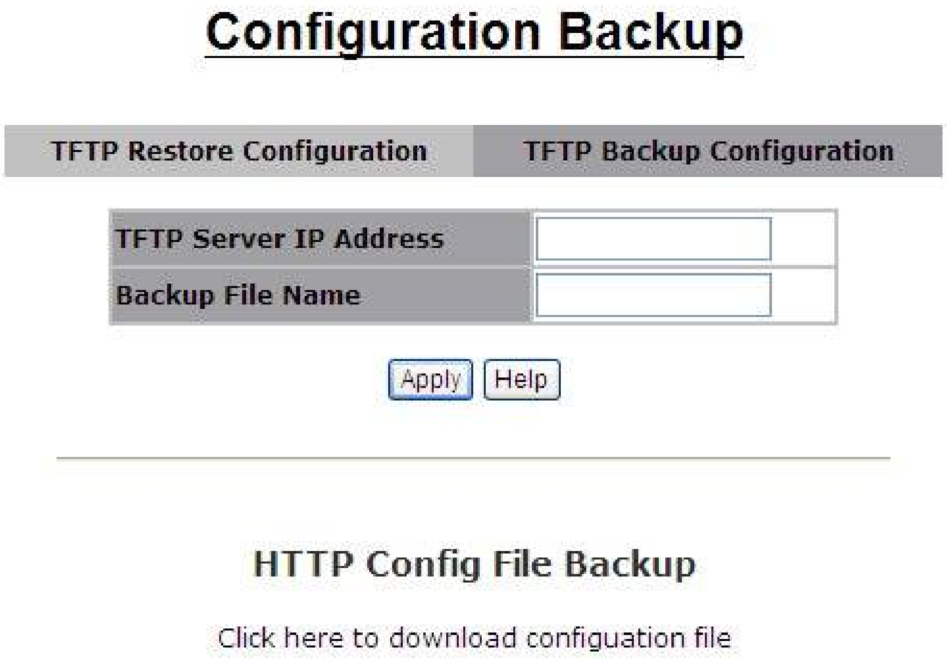

Configuration Restore

TFTP Server IP Address	192.168.223.99
Backup File Name	flash.dat

Fig.4.2.7.0 HTTP Update

4.2.7.1 TFTP Backup Configuration

Use this page to assign a TFTP server IP address and a filename to be stored. Then press Apply button to start the backup process.



Configuration Backup

TFTP Restore Configuration	TFTP Backup Configuration

TFTP Server IP Address	
Backup File Name	

HTTP Config File Backup

Click here to download configuation file

Fig.4.2.7.1 TFTP Backup Configuration

4.3 L2 Features

This switch provides the following L2 features:

- **VLAN Configuration (See section 4.3.0)**
- **Forwarding & Filtering (See section 4.3.1)**
- **IGMP Snooping (See section 4.3.2)**
- **Spanning Tree (STP) (See section 4.3.3)**
- **DHCP Relay & Option 82 (See section 4.3.4)**
- **LLDP (optional) (See section 4.3.5)**

4.3.0 VLAN Configuration

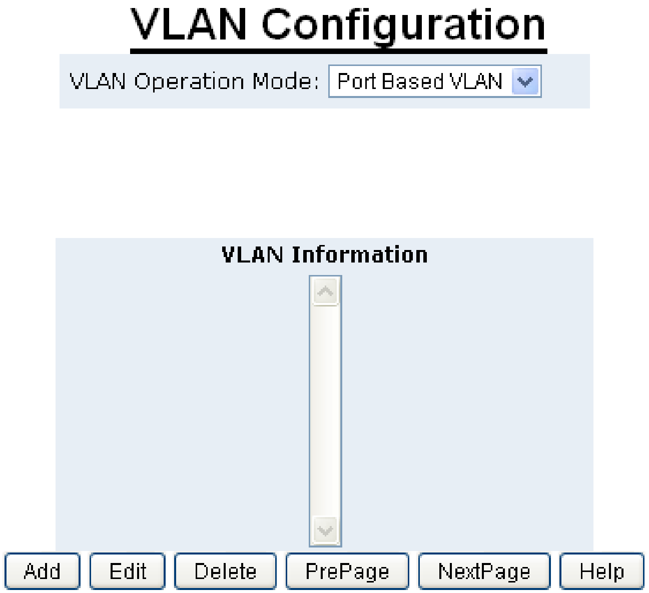
A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

This switch supports port-based, 802.1Q (tagged-based) or no VLAN in web management page. In default, 802.1Q VLAN is enabled for common and advanced operations.

- Static VLAN (See section 4.3.0.0)
- GVRP VLAN (See section 4.3.0.1)
- QinQ VLAN (See section 4.3.0.2)

4.3.0.0 Static VLAN

4.3.0.0.0 Port Based VLAN


VLAN Configuration

VLAN Operation Mode: Port Based VLAN

VLAN Information

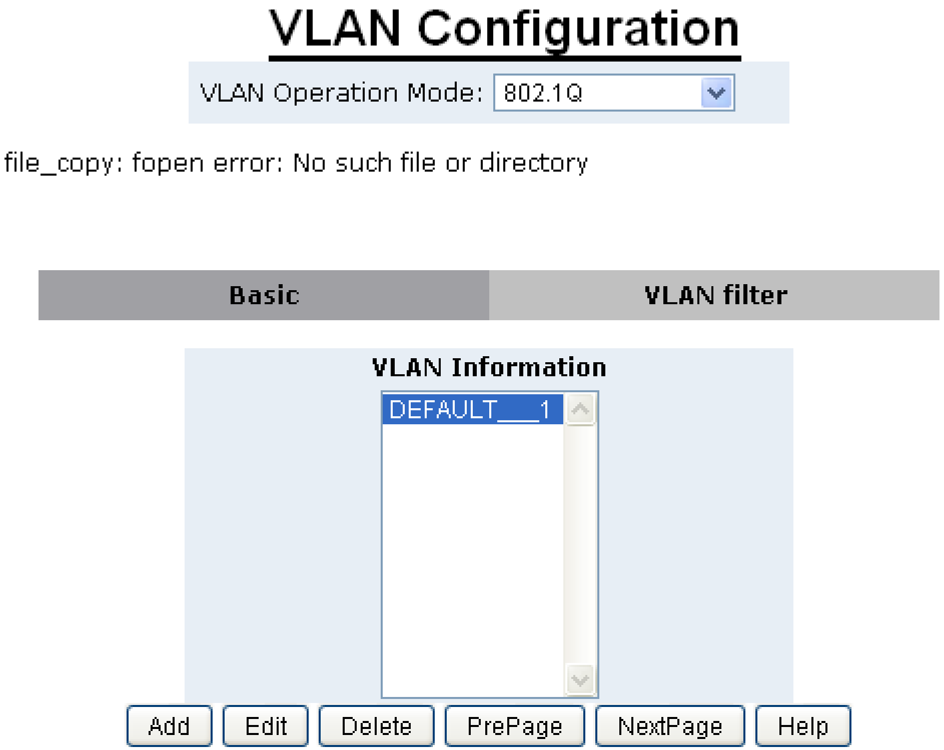
Fig. 4.3.0.0.0 Port Based VLAN

First select Port-based VLAN in VLAN Operation Mode. Then click Add to create a new VLAN group.
Enter the VLAN name, group ID and select the members for the new VLAN. Then click Apply to activate the setting.
If there are many groups that over the limit of one page, you can click the Next Page to view other VLAN groups.

4.3.0.0.1 802.1Q VLAN

In this page, user can create 802.1Q (tag-based) VLAN.

There are up to 512 VLAN groups to provide configuration. While VLAN Operation Mode is changed to 802.1Q VLAN, all ports on the switch belong to default VLAN group which VID is 1. The default VLAN group can't be deleted.

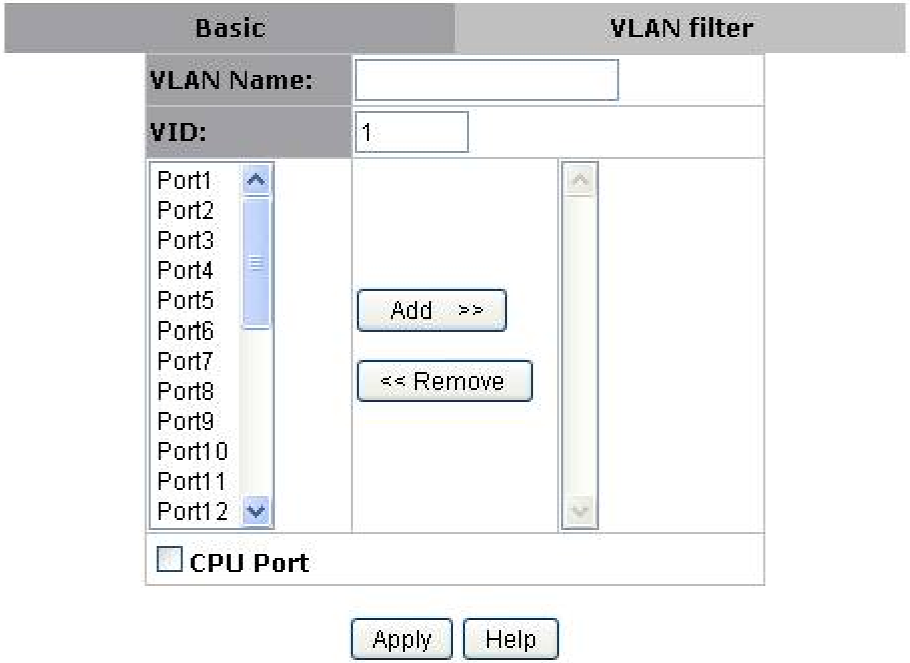


VLAN Configuration

VLAN Operation Mode: 802.1Q

file_copy: fopen error: No such file or directory

Fig. 4.3.0.0.1 802.1Q VLAN



Basic	VLAN filter
VLAN Name:	
VID:	1

Port1
Port2
Port3
Port4
Port5
Port6
Port7
Port8
Port9
Port10
Port11
Port12

□ CPU Port

Fig. 4.3.0.0.2 802.1Q VLAN Add

Basic

Create a VLAN and add tagged member ports to it.

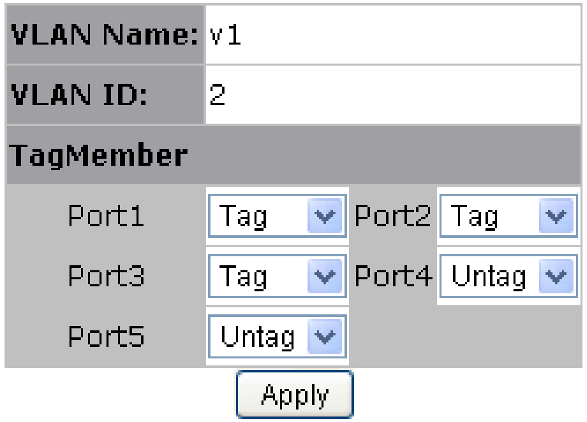
1. From the main menu, click Administrator VLAN configuration, click Add then you will see the page as follow.

2. Type a name for the new VLAN.

3. Type a VID (1~4094). The default is 1.

4. From the Available ports box, select ports to add to the switch and click “Add >>”.

5. Click Next. Then you can view the page as follow：



VLAN Name:	v1		
VLAN ID:	2		
TagMember			
Port1	Tag	Port2	Tag
Port3	Tag	Port4	Untag
Port5	Untag		

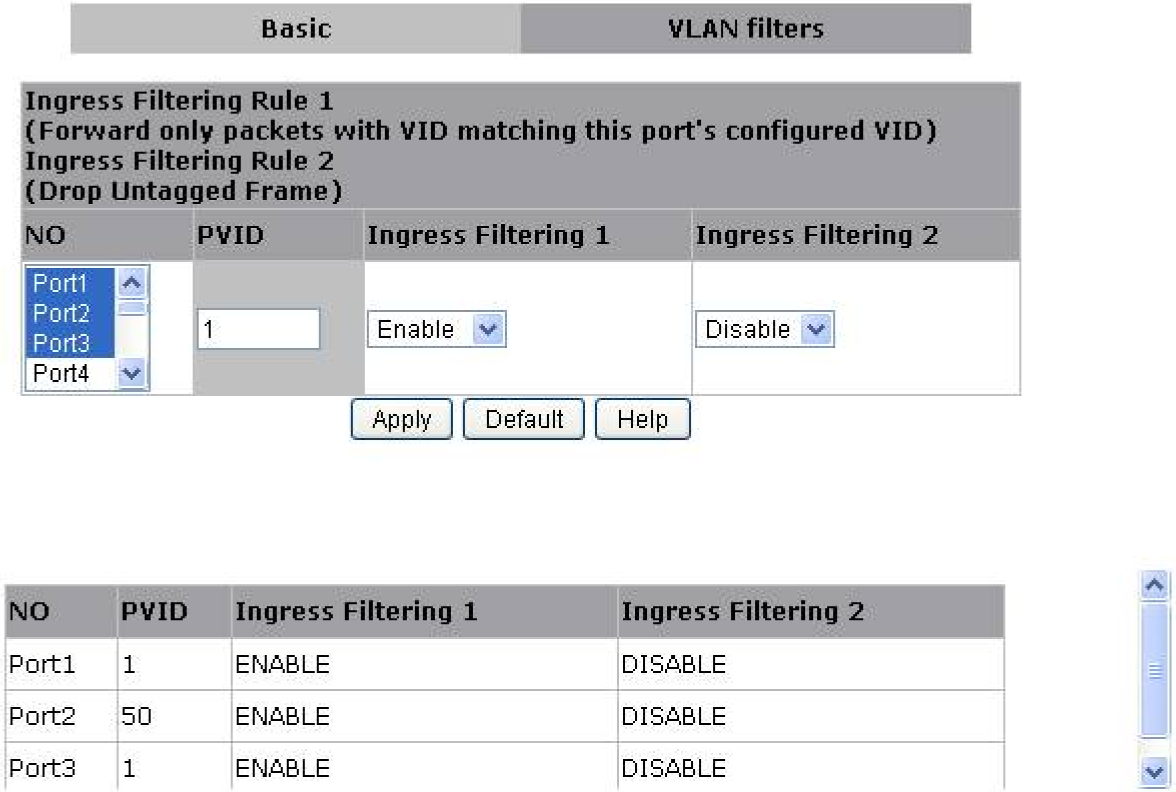
Fig. 4.3.0.0.3 802.1Q VLAN Add

6. Uses this page to set the outgoing frames are VLAN-Tagged frames or no. Then click Apply.

Tag: outgoing frames with VLAN-Tagged.

Untag: outgoing frames without VLAN-Tagged.

VLAN Filters



Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)
Ingress Filtering Rule 2
(Drop Untagged Frame)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port1 Port2 Port3 Port4	1	Enable	Disable

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port1	1	ENABLE	DISABLE
Port2	50	ENABLE	DISABLE
Port3	1	ENABLE	DISABLE

Fig. 4.3.0.0.4 VLAN Filters

Port NO.

Port number(s) to be assigned to see or configure the settings.

Port VID (PVID)

Port VLAN ID will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but that don’t support tagging. This switch allows user to set one PVID for each port, the range is 1~4094, default PVID is 1. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.

Ingress Filtering

Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN. This switch has two ingress filtering rule as follows:

Ingress Filtering Rule 1: A forward only packet with VID matching this port’s configured VID.

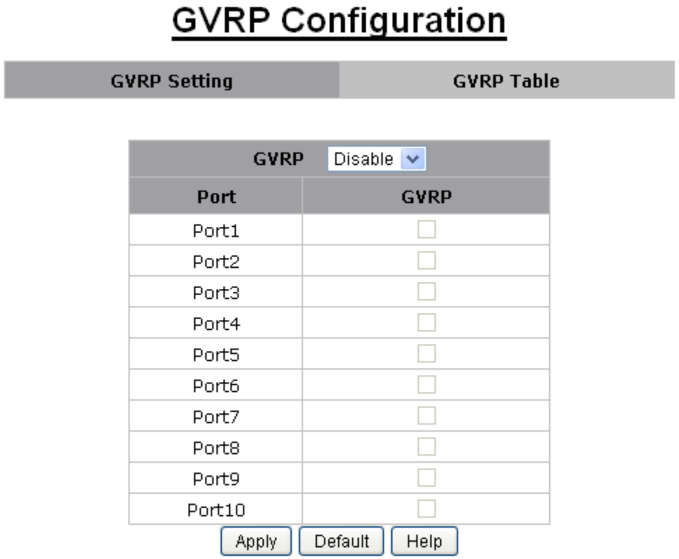
Ingress Filtering Rule 2: Drop Untagged Frame.

4.3.0.1 GVRP VLAN

4.3.0.1.0 GVRP Setting

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch, the switch will automatically add that device to the existing VLAN

GVRP can be enabled per port basis. To enable GVRP function for a port, both global GVRP and special port GVRP are required to configure.



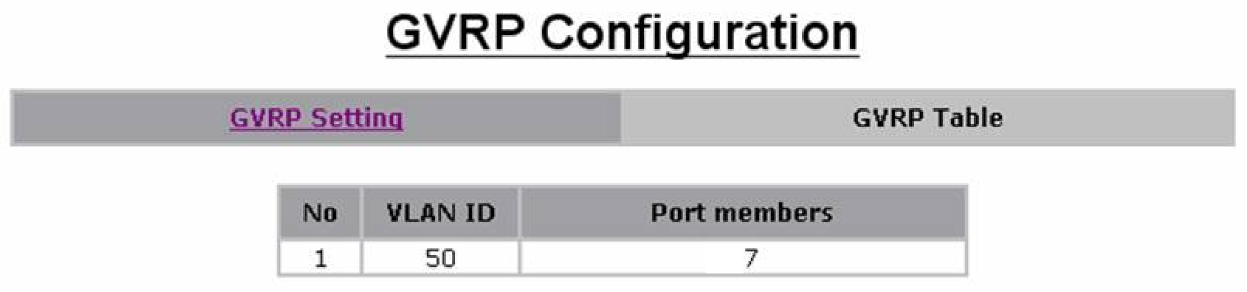
GVRP Configuration

GVRP: Disable

Port	GVRP
Port1	□
Port2	□
Port3	□
Port4	□
Port5	□
Port6	□
Port7	□
Port8	□
Port9	□
Port10	□

Fig.4.3.0.1.0 GVRP VLAN

4.3.0.1.1 GVRP Table



GVRP Configuration

No	VLAN ID	Port members
1	50	7

Fig. 4.3.0.1.1 GVRP Table

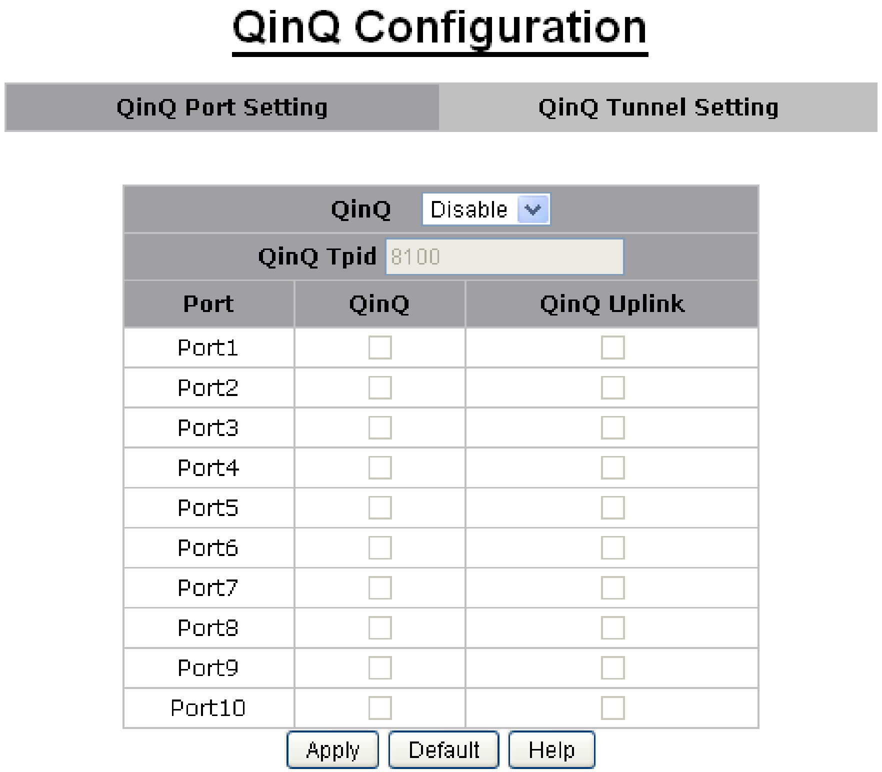
In this page, the VLAN group(s) dynamically created by GVRP can be displayed with VID and port member(s).

4.3.0.2 QinQ VLAN

4.3.0.2.0 QinQ Port Setting

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification. Using the QinQ feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using QinQ expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support QinQ is called a QinQ user-port. A port configured to support QinQ Uplink is called a QinQ uplink-port.

To enable QinQ function, the global **QinQ** option, QinQ **Tpid** and specified port-based QinQ **User** or **Uplink** port option need to be configured.



QinQ Configuration

QinQ Port Setting | QinQ Tunnel Setting

QinQ: Disable

QinQ Tpid: 8100

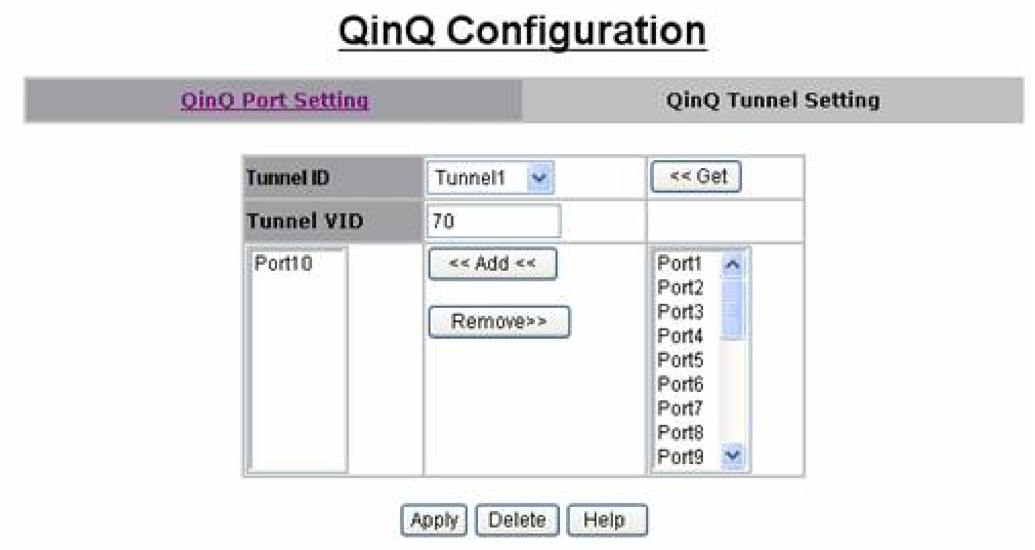
Port	QinQ	QinQ Uplink
Port1	□	□
Port2	□	□
Port3	□	□
Port4	□	□
Port5	□	□
Port6	□	□
Port7	□	□
Port8	□	□
Port9	□	□
Port10	□	□

Fig 4.3.0.2 QinQ VLAN

4.3.0.2.1 QinQ Tunnel Setting

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks. QinQ tunnel is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. When you configure QinQ tunnel, you assign the QinQ user-port and uplink-port to a VLAN ID that is dedicated to QinQ tunnel.

To add QinQ tunnel, you first select QinQ Tunnel ID, then fill VLAN ID QinQ dedicated to QinQ tunnel, and select user-port and uplink-port to be added to QinQ tunnel.



QinQ Configuration

QinQ Port Setting | QinQ Tunnel Setting

Tunnel ID	Tunnel1	<< Get
Tunnel VID	70	
Port10	<< Add << Remove>>	Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8 Port9

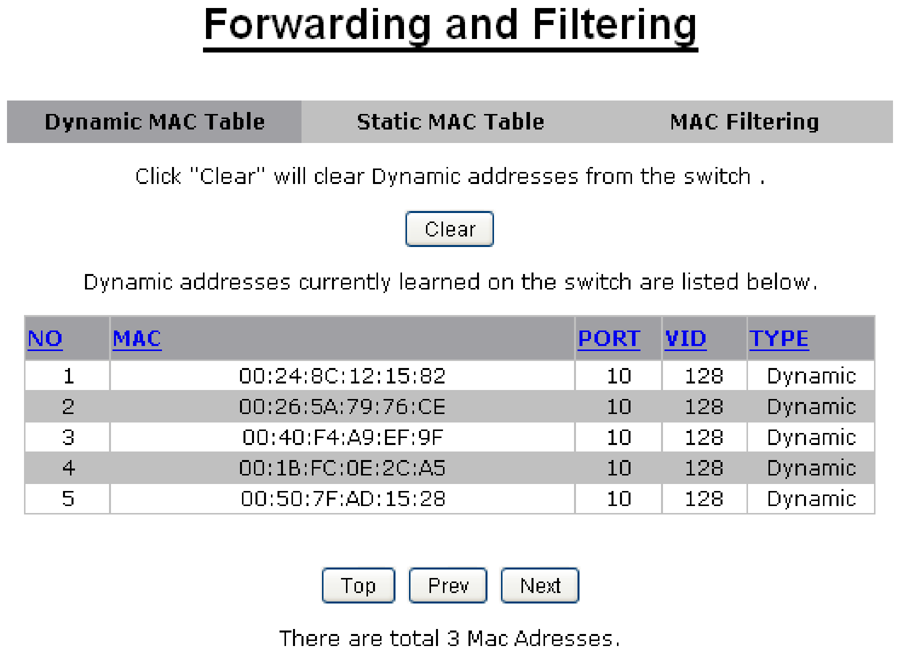
4.3.1 Forwarding and Filtering

In this submenu, the following functions related to forwarding and filtering are provided:

- Dynamic MAC Table (See section 4.3.1.0)
- Static MAC Table (See section 4.3.1.1)
- MAC Filtering (See section 4.3.1.2)

4.3.1.0 Dynamic MAC Address

The switch will dynamically learn the device's MAC address when it corresponding with the switch. MAC address will be stored in MAC address table. Dynamic MAC Table shows the MAC addresses learned by the switch. The table will be shown by pages if larger than 500 MAC Addresses.



Click "Clear" will clear Dynamic addresses from the switch .

Dynamic addresses currently learned on the switch are listed below.

NO	MAC	PORT	VID	TYPE
1	00:24:8C:12:15:82	10	128	Dynamic
2	00:26:5A:79:76:CE	10	128	Dynamic
3	00:40:F4:A9:EF:9F	10	128	Dynamic
4	00:1B:FC:0E:2C:A5	10	128	Dynamic
5	00:50:7F:AD:15:28	10	128	Dynamic

There are total 3 Mac Adresses.

Fig .4.3.1.0 Dynamic MAC Address

Click Clear to clear Dynamic MAC address table.

Click Top to show the first page of MAC address table.

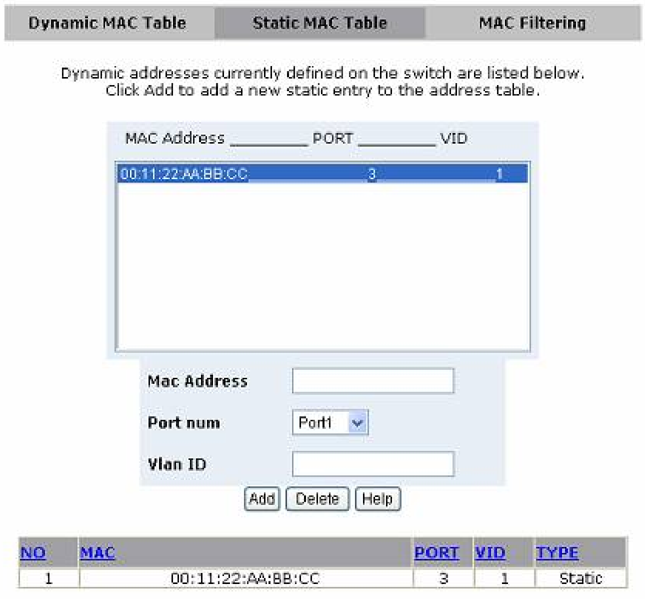
Click Prev to show the previous page of MAC address table. If there is nothing to shown or NO is 1, it is the first page.

Click Next to show the next page of MAC address table. If there is nothing to shown, it is the end page.

4.3.1.1 Static MAC Table

When you add a static MAC address, it permanently remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again.

This table can associate with the **Security** field in **Port Controls** configuration to achieve the access control by source MAC / port / VID binding. That is only ingress traffic with matched lookup (with specified MAC address, port number and VID) in this table can be allowed to access to the switch.



Dynamic addresses currently defined on the switch are listed below.
Click Add to add a new static entry to the address table.

MAC Address _________ PORT _________ VID
00:11:22:AA:BB:CC 3 1

Mac Address
Port num: Port1
Vlan ID

NO	MAC	PORT	VID	TYPE
1	00:11:22:AA:BB:CC	3	1	Static

Fig. 4.3.1.1 Static MAC Table

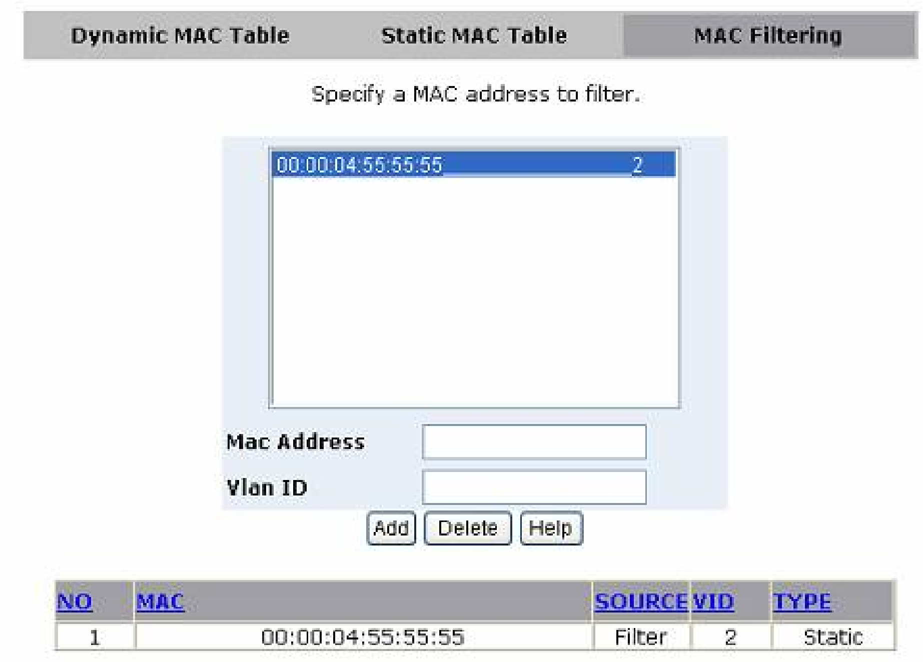
The following parameters can be associated to setup the Static MAC table:
MAC Address: Static MAC address in a MAC entry
Port number: Switch port number to associate with the MAC address in a MAC entry
Vlan ID: If tag-based (IEEE 802.1Q) VLANs are enabled, static MAC address can be associated with individual VLANs. Type the VID in this field to associate with the MAC address.

Click Add to add a new entry. Click Delete to remove a specified entry.

The MAC entries in this table can be sorted by clicking the column NO / MAC / PORT / VID / TYPE.

4.3.1.2 MAC Filtering

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination MAC addresses.



Specify a MAC address to filter.

00:00:04:55:55:55 2

NO	MAC	SOURCE	VID	TYPE
1	00:00:04:55:55:55	Filter	2	Static

Fig. 4.3.1.2 MAC Filtering

MAC Address: MAC address that wants to be filtered.

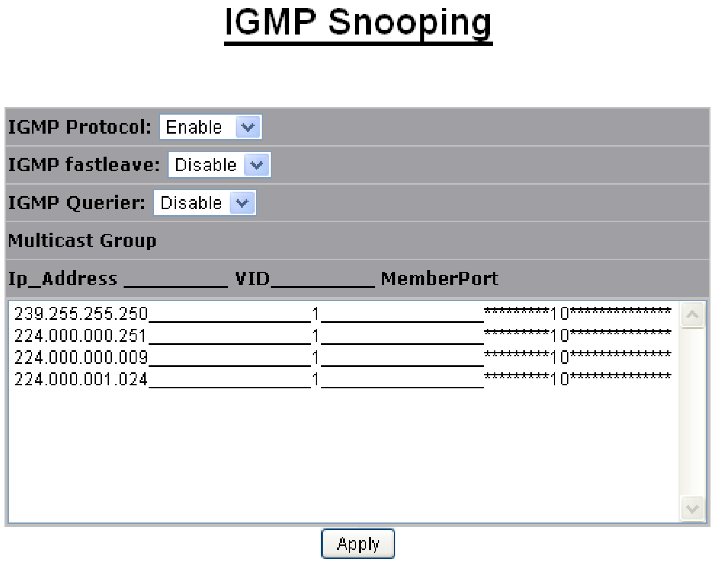
Vlan ID: If tag-based (802.1Q) VLAN are enabled, type the VID in this field to associate with the MAC address.

Click Add to add a new entry. Click Delete to remove a specified entry.

The MAC entries in this table can be sorted by clicking the column NO / MAC / PORT / VID / TYPE.

4.3.2 IGMP Snooping

This switch supports multicast IP, one can enable IGMP protocol on web management's switch setting advanced page, then display the IGMP snooping information in this page, you can view difference multicast group, VID and member port in here, IP multicast addresses range from 224.0.0.0 through 239.255.255.255.



IGMP Snooping

IGMP Protocol: Enable

IGMP fastleave: Disable

IGMP Querier: Disable

Multicast Group

```
Ip_Address __________ VID__________ MemberPort
239.255.255.250_________________1_________________*********10**************
224.000.000.251_________________1_________________*********10**************
224.000.000.009_________________1_________________*********10**************
224.000.001.024_________________1_________________*********10**************
```

Fig. 4.3.2 IGMP Snooping

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite.
IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP have three fundamental types of message as follows:

Message	Description
Query	A message sent from the queries (IGMP router or switch) asking for a response from each host belonging multicast group.
Report	A message sent by a host to the queries to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the queries to indicate that the host has quit being a member of a specific multicast group.

IGMP protocol: Enable/disable IGMP snooping.
IGMP fast leave: Enable/disable IGMP snooping fast leave. If enable, switch will fast delete member who send leave report, else wait one second.
IGMP Querier: Enable/disable IGMP snooping querier. If select disable, the switch can’t send query report.

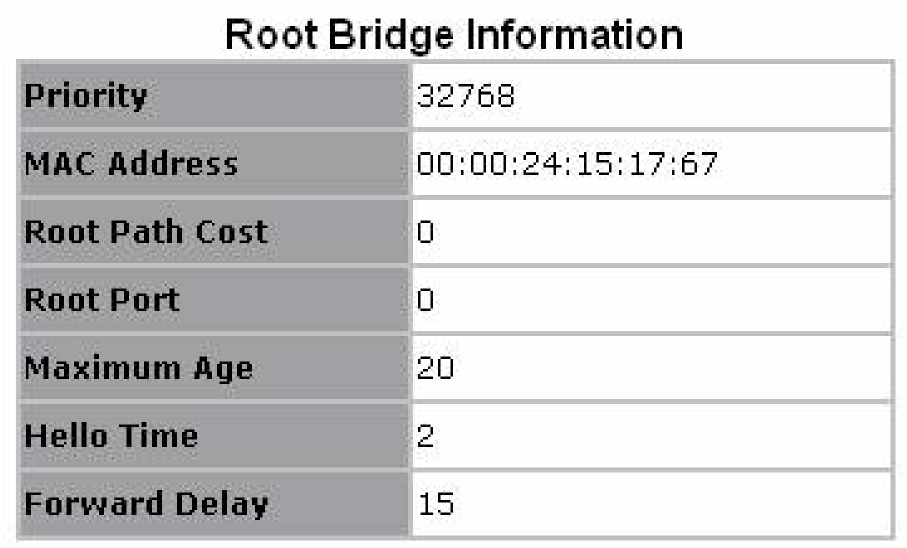
Note:

Do Not use Port based VLAN and IGMP snooping at the same time.

4.3.3 Spanning Tree

4.3.3.0 STP system

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1d) for avoiding loops in switching networks. Enable STP to ensure that only one path at a time is active between any two nodes on the network. You can enable STP on web management's switch setting advanced item, select enable STP. We are recommended that you enable STP on all switches ensures a single active path on the network. You can view STP information about the Root Bridge. Such as following screen.

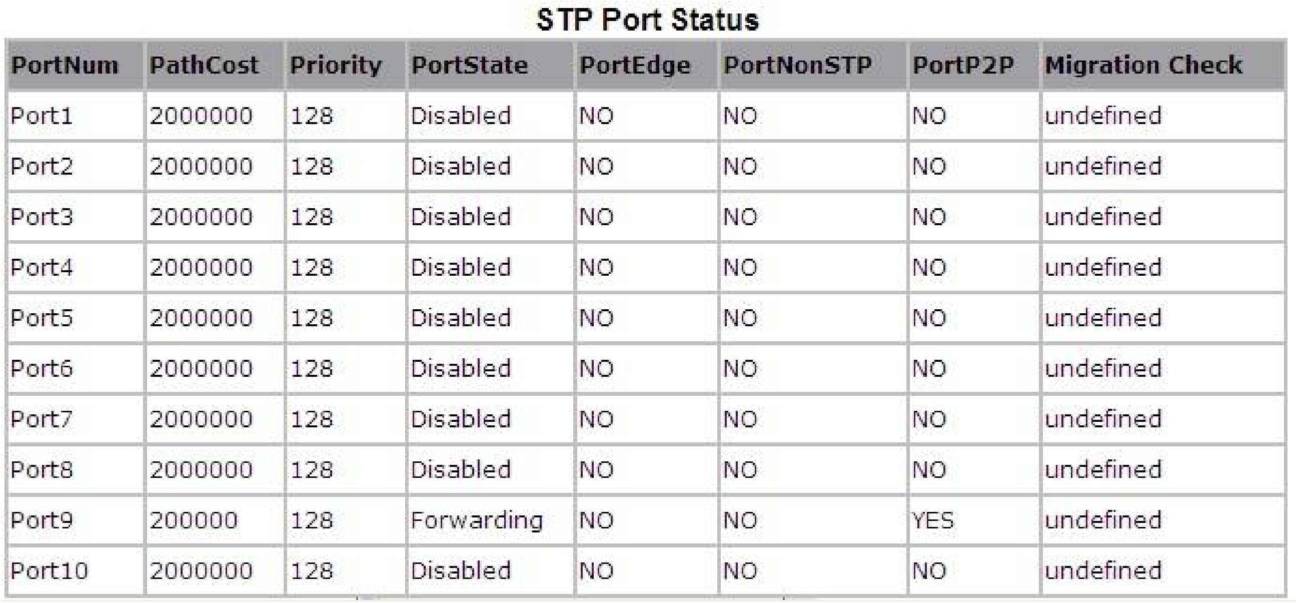


Root Bridge Information

Priority	32768
MAC Address	00:00:24:15:17:67
Root Path Cost	0
Root Port	0
Maximum Age	20
Hello Time	2
Forward Delay	15

Fig. 4.3.3.0a STP system

You can view STP port status about the switch. Such as following screen.

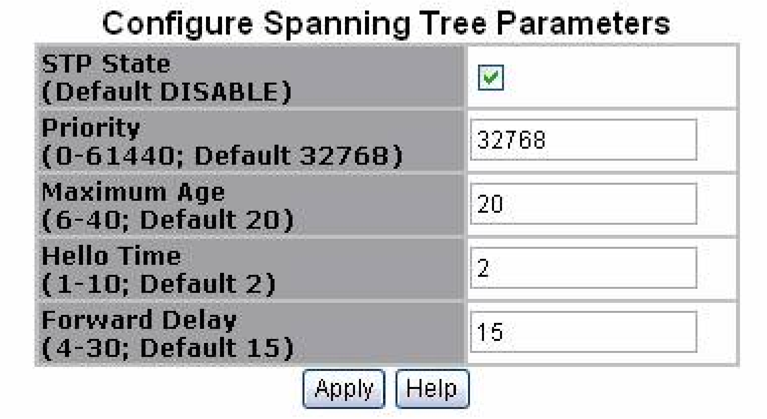


STP Port Status

PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P	Migration Check
Port1	2000000	128	Disabled	NO	NO	NO	undefined
Port2	2000000	128	Disabled	NO	NO	NO	undefined
Port3	2000000	128	Disabled	NO	NO	NO	undefined
Port4	2000000	128	Disabled	NO	NO	NO	undefined
Port5	2000000	128	Disabled	NO	NO	NO	undefined
Port6	2000000	128	Disabled	NO	NO	NO	undefined
Port7	2000000	128	Disabled	NO	NO	NO	undefined
Port8	2000000	128	Disabled	NO	NO	NO	undefined
Port9	200000	128	Forwarding	NO	NO	YES	undefined
Port10	2000000	128	Disabled	NO	NO	NO	undefined

Fig. 4.3.3.0b STP system

You can configure STP parameters, then click Apply button to set the values. Such as following screen.



Configure Spanning Tree Parameters

STP State (Default DISABLE)	☑
Priority (0-61440; Default 32768)	32768
Maximum Age (6-40; Default 20)	20
Hello Time (1-10; Default 2)	2
Forward Delay (4-30; Default 15)	15

Fig. 4.3.3.0c STP system

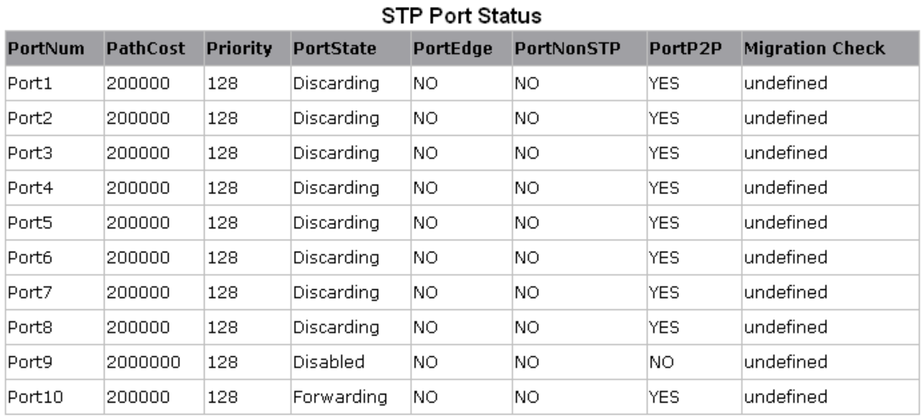
You can select STP state item to enable STP. If you want to disable STP, please cancel the item. Default value of STP sate is disabled.

Parameter	Description
Priority	You can change priority value, A value used to identify the root bridge. The bridge with lowest value has the highest priority and is selected as the root. Value range <0-61440>, the value must be in steps of 4096. Default value is 32768.
Max Age	You can change Max Age value. The maximum age of received protocol information before it is discarded. Value range <6-40>. Default value is 20.
Hello Time	You can change Hello time value. The time interval between the transmission of Configuration BPDUs by a Bridge that is attempting to become the Root or

	is the Root. Value range <1-10>. Default value is 2.
Forward Delay time	You can change forward delay time. The time spent by a Port in the Listening State and the Learning State before moving to the Learning or Forwarding State, respectively. It is also the value used for the ageing time of dynamic entries in the Filtering Database, while received BPDU indicate a topology change. Value range <4-30>. Default value is 15.

NOTE: The above parameters must enforce the following relationships:
2*(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)

The following parameters can be configured on each port, click Apply button to set the values.



STP Port Status

PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P	Migration Check
Port1	200000	128	Discarding	NO	NO	YES	undefined
Port2	200000	128	Discarding	NO	NO	YES	undefined
Port3	200000	128	Discarding	NO	NO	YES	undefined
Port4	200000	128	Discarding	NO	NO	YES	undefined
Port5	200000	128	Discarding	NO	NO	YES	undefined
Port6	200000	128	Discarding	NO	NO	YES	undefined
Port7	200000	128	Discarding	NO	NO	YES	undefined
Port8	200000	128	Discarding	NO	NO	YES	undefined
Port9	2000000	128	Disabled	NO	NO	NO	undefined
Port10	200000	128	Forwarding	NO	NO	YES	undefined

Fig. 4.3.3.0d STP system

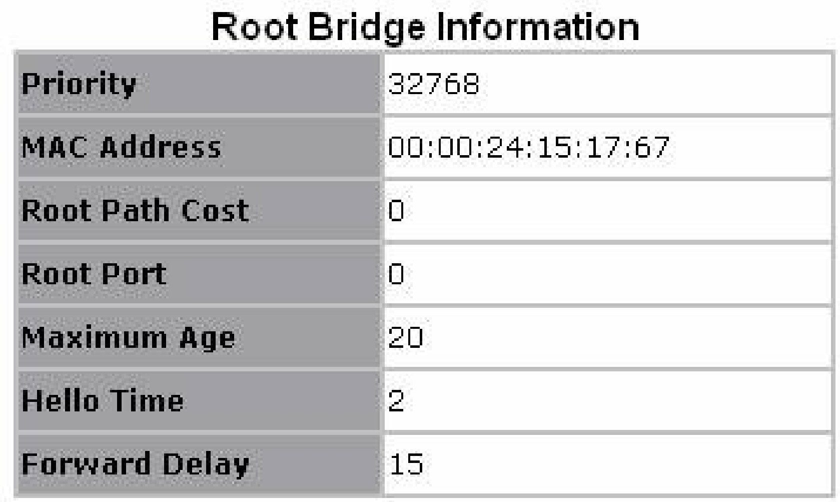
You can select one port in the Port Number item to configure the parameters of the port.

Parameter	Description
Path Cost	The contribution of the path through this port, when the port is the root port, to the total cost of the path to the root for this bridge. Value range <1-65535>.
Port Priority	You can make it more or less likely to become the root port, the lowest number has the highest priority. Value range <0-240>, the value must be in steps of 16. Default value is128.

4.3.3.1 MSTP system

The Multiple Spanning Tree Protocol (MSTP) is a standardized method (IEEE 802.1S) for providing simple and full connectivity for frames assigned to any given VLAN throughout a Bridged Local Area Network comprising arbitrarily interconnected Bridges, each operating MSTP, STP , or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MST Bridges. These Regions and the other Bridges and LANs are connected into a single Common Spanning Tree (CST). You can enable MSTP on web management's switch setting advanced item, select enable MSTP. We are recommended that you enable MSTP on all switches ensures a single active path on the network.

You can view MSTP information about the CIST Root Bridge. Such as following screen.

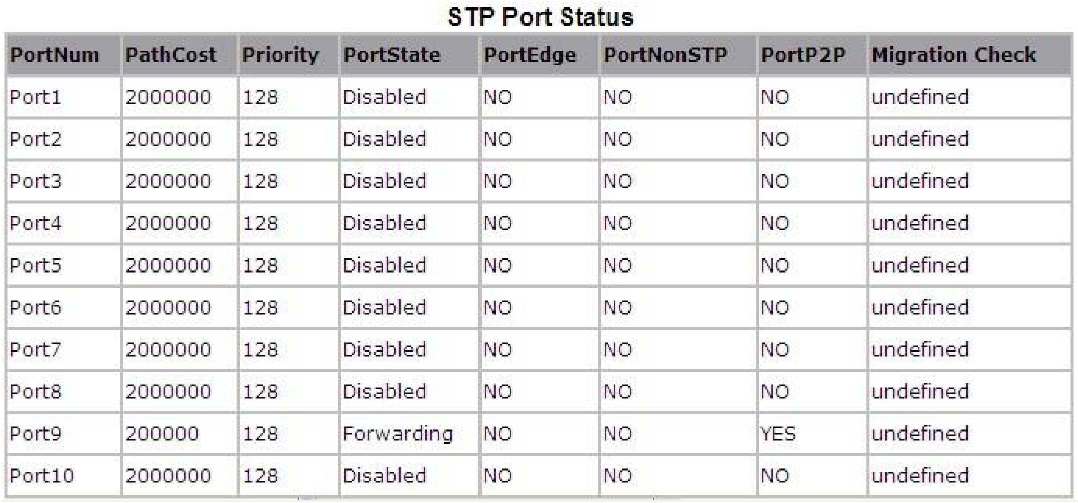


Root Bridge Information

Priority	32768
MAC Address	00:00:24:15:17:67
Root Path Cost	0
Root Port	0
Maximum Age	20
Hello Time	2
Forward Delay	15

Fig. 4.3.3.1a MSTP system

You can view MSTP CIST port status about the switch. Such as following screen

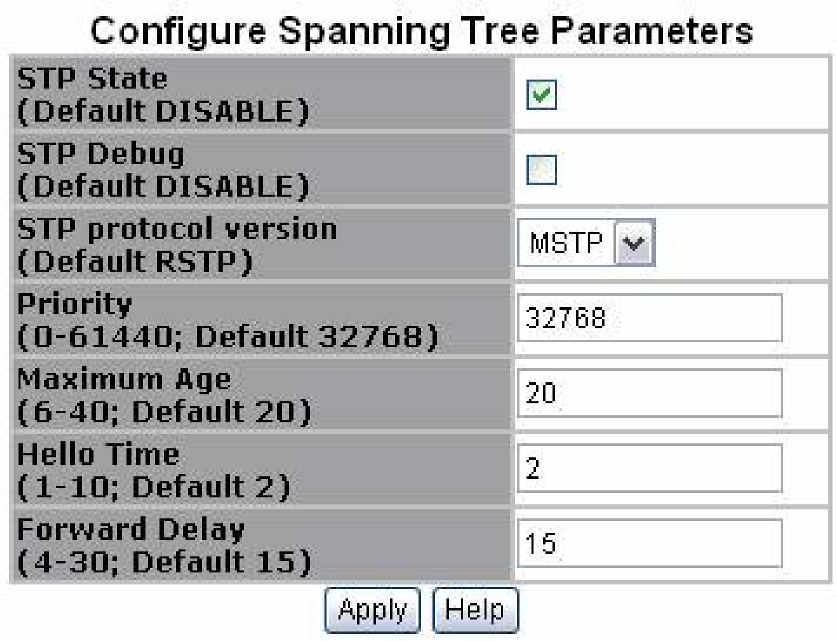


STP Port Status

PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P	Migration Check
Port1	2000000	128	Disabled	NO	NO	NO	undefined
Port2	2000000	128	Disabled	NO	NO	NO	undefined
Port3	2000000	128	Disabled	NO	NO	NO	undefined
Port4	2000000	128	Disabled	NO	NO	NO	undefined
Port5	2000000	128	Disabled	NO	NO	NO	undefined
Port6	2000000	128	Disabled	NO	NO	NO	undefined
Port7	2000000	128	Disabled	NO	NO	NO	undefined
Port8	2000000	128	Disabled	NO	NO	NO	undefined
Port9	200000	128	Forwarding	NO	NO	YES	undefined
Port10	2000000	128	Disabled	NO	NO	NO	undefined

Fig. 4.3.3.1b MSTP system

You can configure MSTP parameters, then click Apply button to set the values. Such as following screen.



Configure Spanning Tree Parameters

STP State (Default DISABLE)	☑
STP Debug (Default DISABLE)	□
STP protocol version (Default RSTP)	MSTP
Priority (0-61440; Default 32768)	32768
Maximum Age (6-40; Default 20)	20
Hello Time (1-10; Default 2)	2
Forward Delay (4-30; Default 15)	15

Fig. 4.3.3.1c MSTP system

You can select STP state item to enable MSTP. If you want to disable MSTP, please cancel the item. Default value of STP sate is disabled.

You can select STP Debug item to output MSTP debug information. If you want to disable the debug, please cancel the item. Default value of STP Debug is disabled.

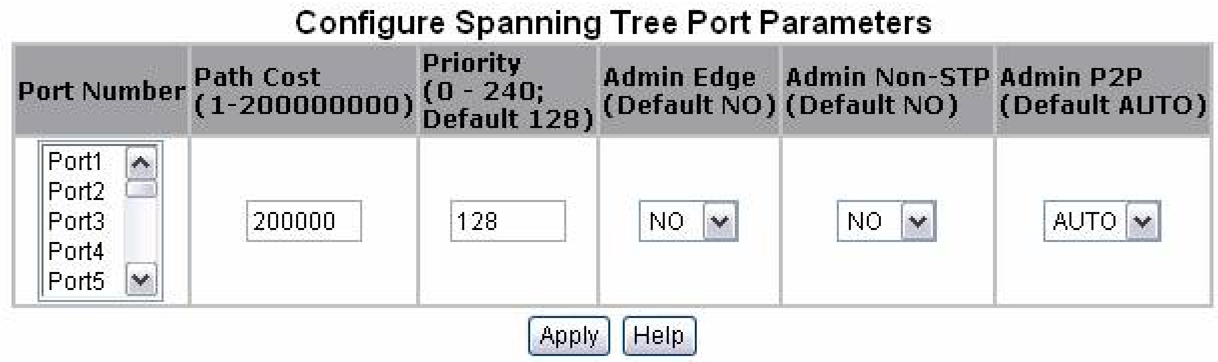
STP protocol version item has two values for you to choose. If you want the protocol version to be STP, you can choose STP. If you want the protocol version to be MSTP, you can choose MSTP. Default value of STP protocol version is MSTP.

Parameter	Description
Priority	You can change priority value, A value used to identify the root bridge. The bridge with lowest value has the highest priority and is selected as the root. Value range <0-61440>, the value must be in steps of 4096. Default value is 32768.
Max Age	You can change Max Age value. The maximum age of received protocol information before it is discarded. Value range <6-40>. Default value is 20.
Hello Time	You can change Hello time value. The time interval between the transmission of Configuration BPDUs by a Bridge that is attempting to become the Root or is the Root. Value range <1-10>. Default value is 2.
Forward Delay time	You can change forward delay time. The time spent by a Port in the Listening State and the Learning State before moving to the Learning or Forwarding State, respectively. It is also the value used for the ageing time of dynamic entries in the Filtering Database, while received BPDU indicate a topology change. Value range <4-30>. Default value is 15.

Note:

The above parameters must enforce the following relationships:
2*(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)

The following parameters can be configured on each CIST port, click Apply button to set the values.



Configure Spanning Tree Port Parameters

Port Number	Path Cost (1-200000000)	Priority (0 - 240; Default 128)	Admin Edge (Default NO)	Admin Non-STP (Default NO)	Admin P2P (Default AUTO)
Port1 Port2 Port3 Port4 Port5	200000	128	NO	NO	AUTO

Fig. 4.3.3.1d MSTP system

You can select one port in the Port Number item to configure the parameters of the CIST port.

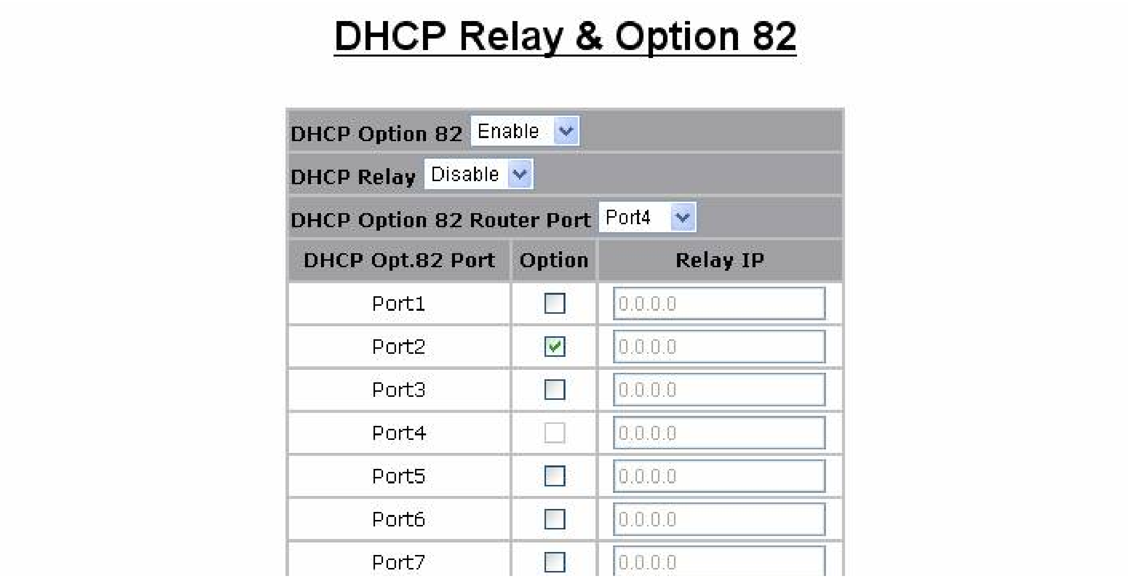
Parameter	Description
Path Cost	The contribution of the path through this port, when the port is the root port, to the totalcost of the path to the root for this bridge. Value range <1-200000000>.
Port Priority	You can make it more or less likely to become the root port, the lowest number has thehighest priority. Value range <0-240>, the value must be in steps of 16. Default value is 28.
Admin Edge	You can choose the value of YES if you want the port to be edge port. If the port is edgeport, when the port becomes a Designated Port it can rapidly transition to the Forwarding Port State. Value range <NO | YES>. Default value is NO.
Admin Non -STP	If you want to disable spanning tree protocol on the port, you can choose the value of YES to this port. Value range <NO | YES>. Default value is NO.
Admin P2P	If you want point-to-point link auto detection on the port, you can choose the value of AUTO to this port. If you want point-to-point link of the port always be true, you can choose the value of YES to this port. If you want point-to-point link of the port always be false, you can choose the value of NO to this port. Value range <AUTO | NO | YES>.Default value is AUTO.

4.3.4 DHCP Relay and Option 82

The Relay Agent Information option (Option82) is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server (RFC 3046). Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies. The DHCP Relay can forward the DHCP broadcast packets to a DHCP server in a different subnet (RFC 1542). So DHCP server can provide IP addresses to clients spanning multiple subnets instead of deploying a DHCP server on every subnet.

4.3.4.0DHCP Option82

To enable DHCP option82 function, need to enable global option82 and special port option82. Then select DHCP router port.



DHCP Relay & Option 82

DHCP Option 82: Enable

DHCP Relay: Disable

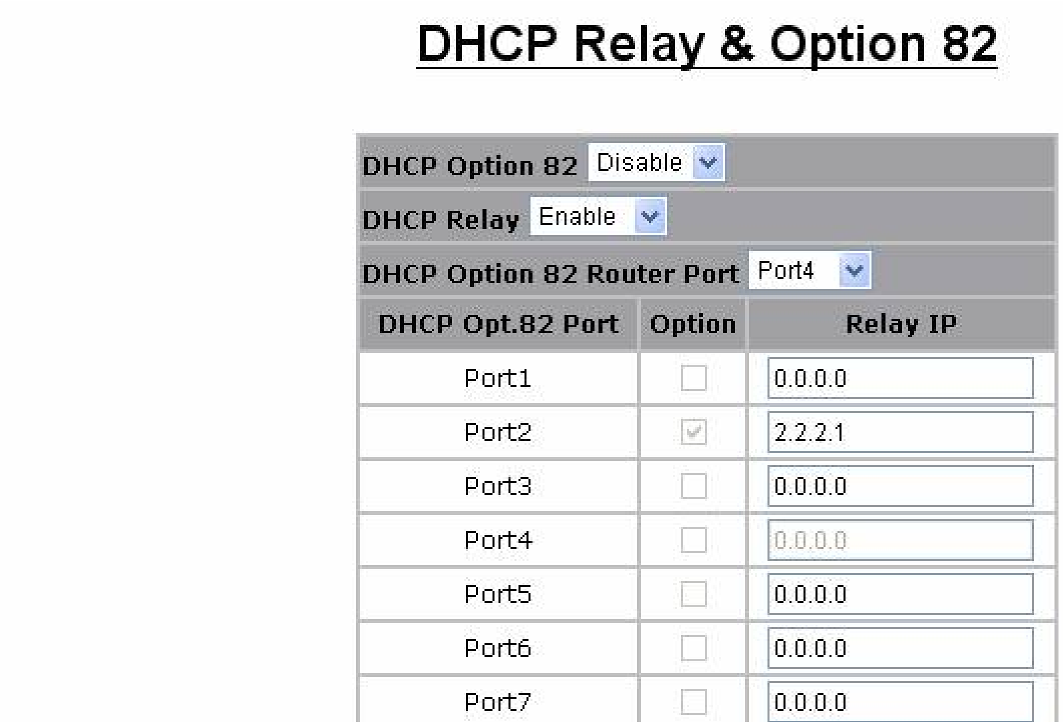
DHCP Option 82 Router Port: Port4

DHCP Opt.82 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

Fig. 4.3.4.0DHCP Option82

4.3.4.1 DHCP Relay

To enable DHCP relay function, need to enable global dhcp-relay and special port dhcp-relay. Then select DHCP router port.



DHCP Relay & Option 82

DHCP Option 82: Disable

DHCP Relay: Enable

DHCP Option 82 Router Port: Port4

DHCP Opt.82 Port	Option	Relay IP
Port1	□	0.0.0.0
Port2	☑	2.2.2.1
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

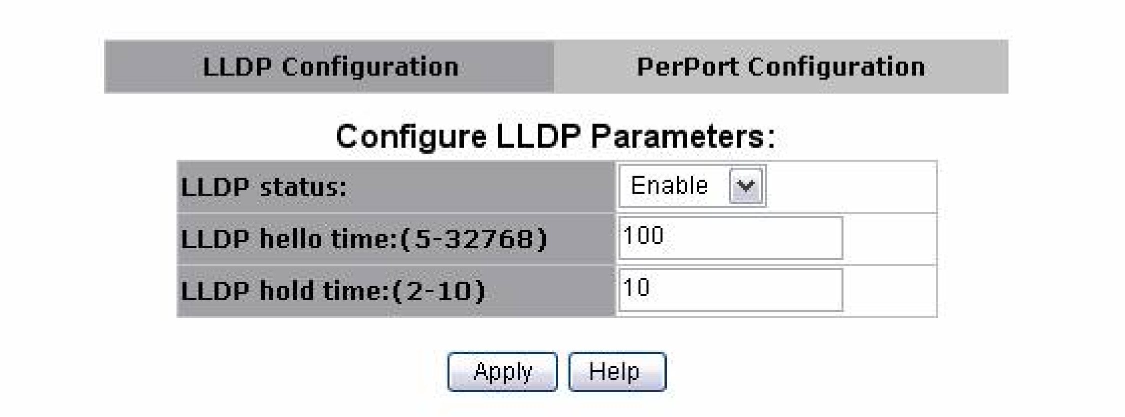
Fig. 4.3.4.1 DHCP Relay

4.3.5 LLDP

This switch supports LLDP (Link Layer Discovery Protocol) function. Please refer to the section 4.3.7 which has descriptions about the LLDP function and operation in console. Here is the web UI to configure this function.

4.3.5.0 LLDP Configuration

This page is to provide the global parameters for LLDP for configuration.



Configure LLDP Parameters:

LLDP status:	Enable
LLDP hello time:(5-32768)	100
LLDP hold time:(2-10)	10

Fig. 4.3.4.0 LLDP Configuration

LLDP Status: Enable/Disable LLDP.

LLDP hello time: LLDP hello time value which is time interval between the transmission LLDP info packets. Value range is from 5 to 32768. Default value is 30.

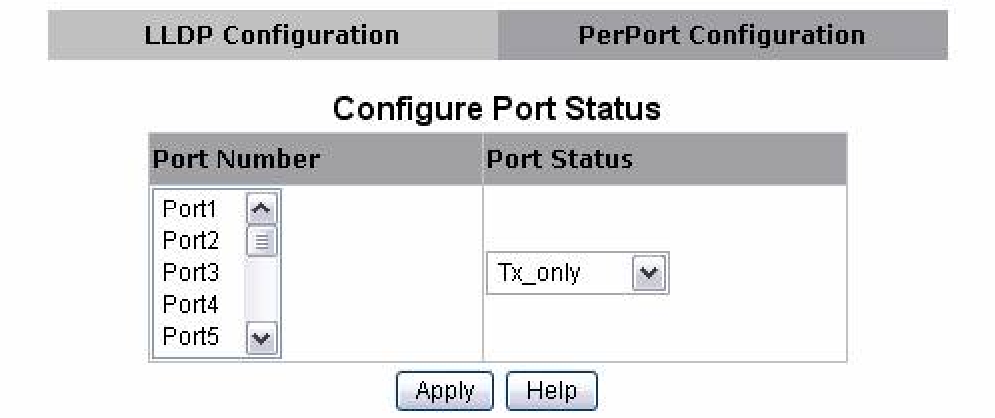
LLDP hold time: LLDP hold time value. Value range is from 2 to 10. Default value is 4.

TTL (time to live) is a period of time for keeping the information about a neighboring device. The information will be aged out when the corresponding TTL expires. TTL can be calculated by configuring LLDP hello time and hold time according to the following expression:

TTL = LLDP hello time × LLDP hold time

4.3.5.1 PerPort Configuration

PerPort LLDP configuration is in this page:



LLDP Configuration | PerPort Configuration

Configure Port Status

Port Number	Port Status
Port1 Port2 Port3 Port4 Port5	Tx_only

Fig. 4.3.5.1a PerPort Configuration

Port Number: specify the port(s) to be configured in the switch.

Port Status: specify one of four port mode to operate LLDP for specified port(s)

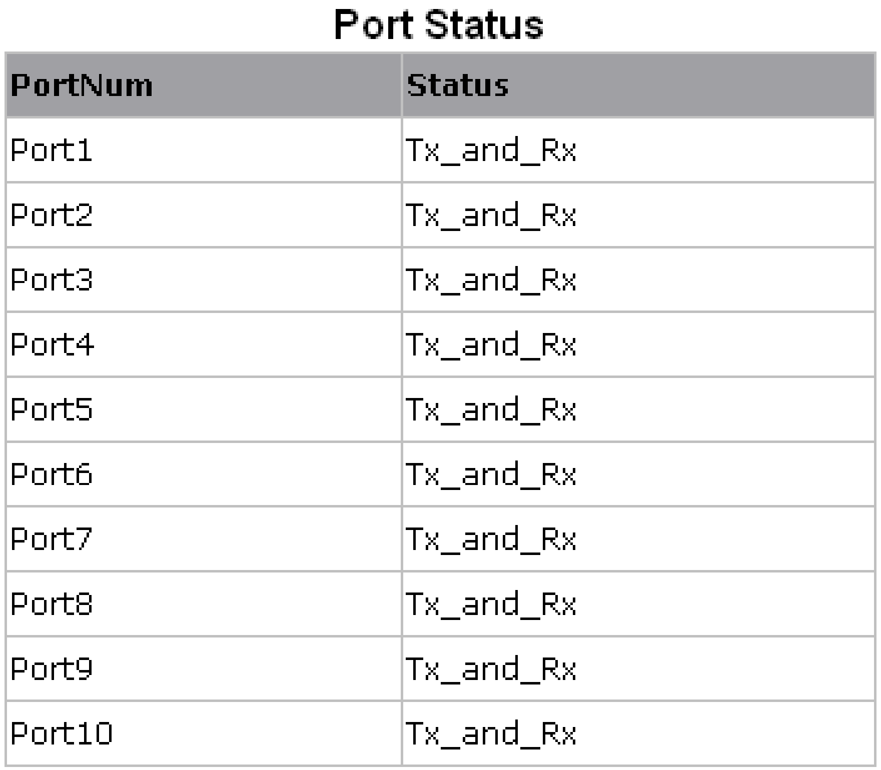
Tx_only: LLDP transmit the packet of the port only

Rx_only: LLDP receive the packet of the port only.

Tx_and_Rx: LLDP transmit and receive the packets of the port.

Disable: LLDP do not transmit and receive the packets of the port.

PerPort LLDP configuration status can be shown in the lower area of this page like the following example:



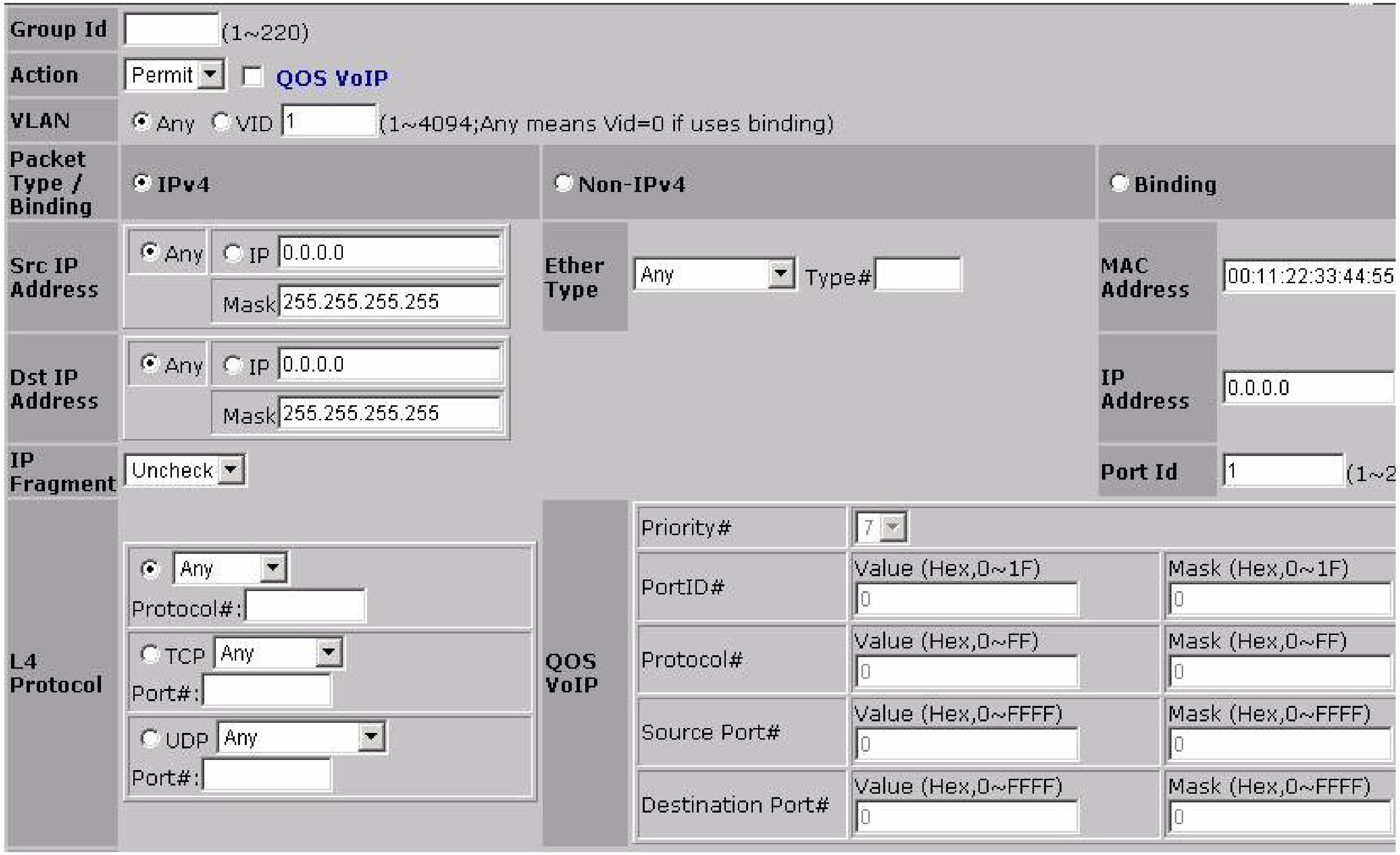
Port Status

PortNum	Status
Port1	Tx_and_Rx
Port2	Tx_and_Rx
Port3	Tx_and_Rx
Port4	Tx_and_Rx
Port5	Tx_and_Rx
Port6	Tx_and_Rx
Port7	Tx_and_Rx
Port8	Tx_and_Rx
Port9	Tx_and_Rx
Port10	Tx_and_Rx

Fig. 4.3.5.1b PerPort Configuration

4.4 Access Control List

Packets can be forwarded or dropped by ACL rules include IPv4 or non-Ipv4. VDSL2 IP DSLAM can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.



Group Id (1~220)

Action Permit ▾ □ QOS VoIP

VLAN ● Any ○ VID 1 (1~4094;Any means Vid=0 if uses binding)

Packet Type / Binding: ● IPv4 ○ Non-IPv4 ○ 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: Uncheck ▾

L4 Protocol: ● Any ▾ Protocol#: ; ○ TCP Any ▾ Port#: ; ○ UDP Any ▾ Port#:

Ether Type: Any ▾ Type#

MAC Address: 00:11:22:33:44:55

IP Address: 0.0.0.0

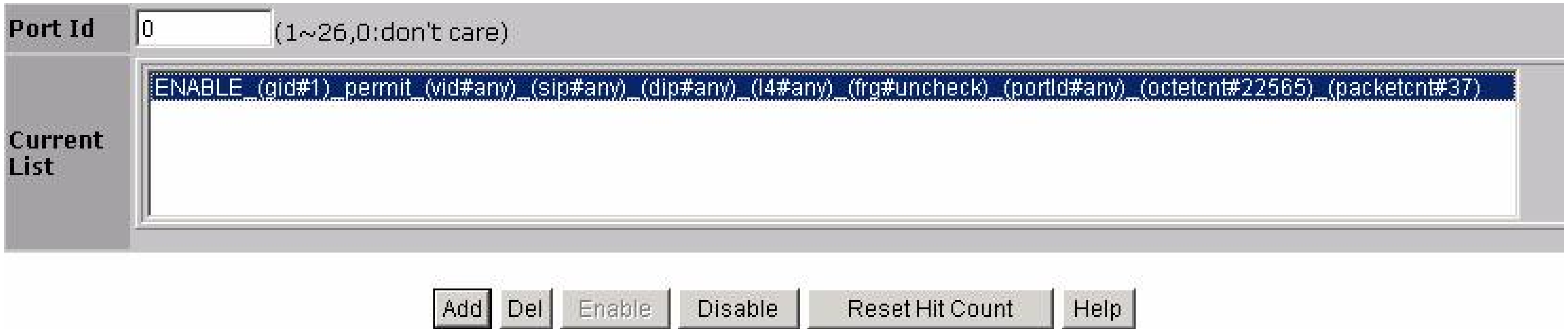
Port Id: 1 (1~2

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

Fig. 4.4a Access Control List

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



Port Id	0 (1~26,0:don't care)
Current List	ENABLE_(gid#1)_permit_(vid#any)_(sip#any)_(dip#any)_(l4#any)_(frg#uncheck)_(portId#any)_(octetcnt#22565)_(packetcnt#37)

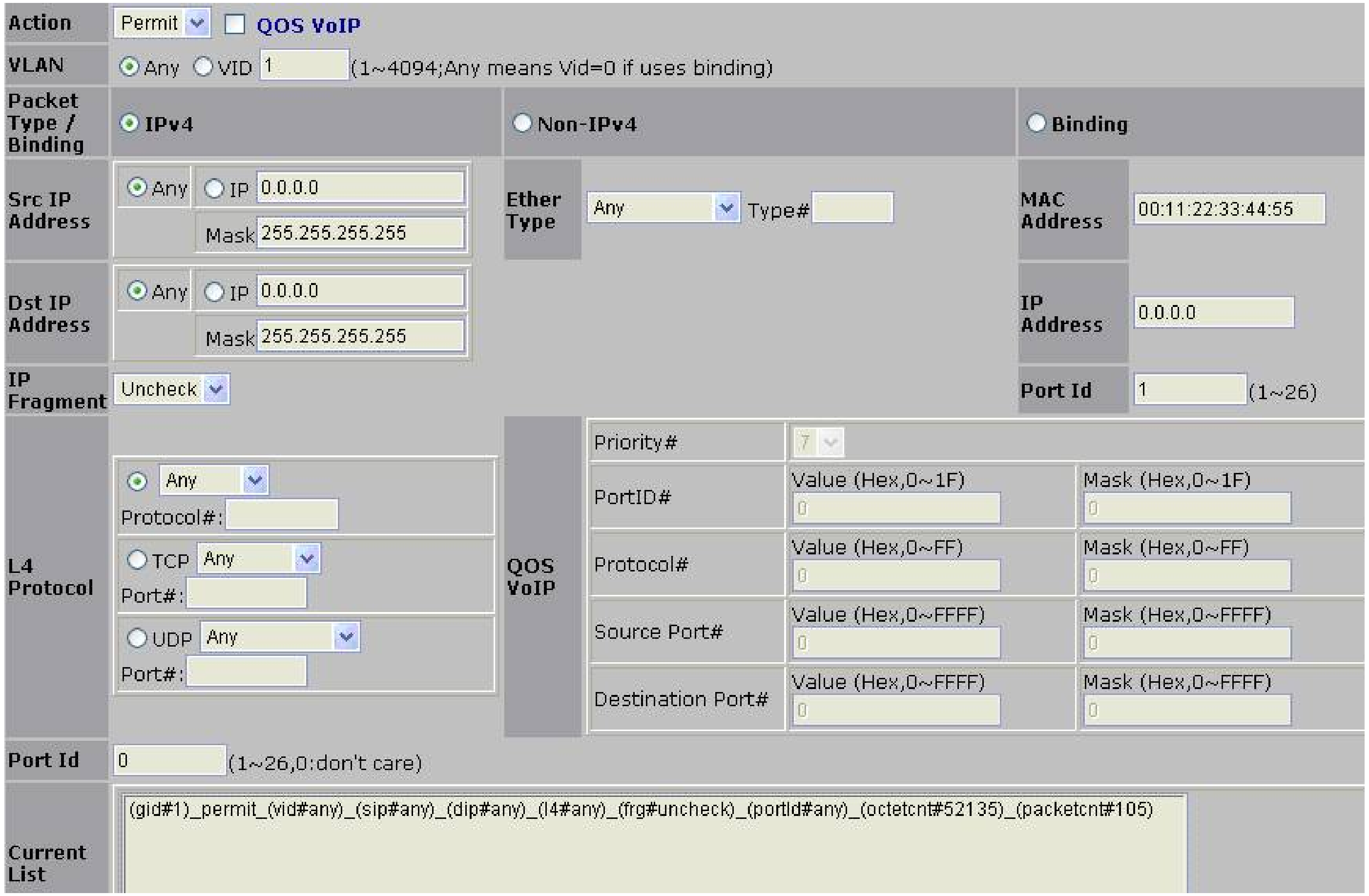
Fig. 4.4b Access Control List

Enable/Disable ACL rule: Select an ACL entry which you want to enable/disable in the Current List. Then click Enable / Disable to execute.

Reset ACL count: Select an ACL entry which you want to reset its counts (**octetcnt** and **packetcnt** fields) in the Current List. Then click Reset Hit Count to do the action.

4.4.0 IPv4

In “Packet Type / Binding” box should select “IPv4”.



Action: Permit □ QOS VoIP

VLAN: ● Any ○ VID 1 (1~4094;Any means Vid=0 if uses binding)

Packet Type / Binding: ● IPv4 ○ Non-IPv4 ○ 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: Uncheck

L4 Protocol:
● Any Protocol#:
○ TCP Any Port#:
○ UDP Any Port#:

Ether Type: Any Type#

MAC Address: 00:11:22:33:44:55

IP Address: 0.0.0.0

Port Id: 1 (1~26)

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

Port Id: 0 (1~26,0:don't care)

Current List:

```
(gid#1)_permit_(vid#any)_(sip#any)_(dip#any)_(l4#any)_(frg#uncheck)_(portId#any)_(octetcnt#52135)_(packetcnt#105)
```

Fig. 4.4.0 IPv4

The related parameters are shown in the following table:

Items	Option	Default value
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit / Deny. a. Permit : Permit packet cross switch. b. Deny: Drop packet.	**Permit**
VLAN	Any / VID. a. Any: Any Vlan id. b. VID: 1~4094. A certain vlan id.	**Any**
Packet Type	IPv4 / Non-IPv4 / Binding a. IPv4: Set Ipv4 packet field. b. Non-IPv4: Set non-Ipv4 packet field. c. Binding: Set binding entry.	**IPv4**
Src IP Address	(Set this field if Packet Type is IPv4, else ignore.) Any / IP and Mask a. Any: Any IP address. b. IP :A certain IP address. Mask: ***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255	**Any**

	Notice: This is not subnet mask.	
Dst IP Address	(Set this field if Packet Type is IPv4, else ignore.) Any / IP and Mask a. Any: Any IP address. b. IP :A certain IP address. Mask: ***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255	**Any**
IP Fragment	(Set this field if Packet Type is IPv4, else ignore.) Uncheck / Check a. Uncheck: Not check IP fragment field. b. Check: Check IP fragment field.	**Uncheck**
L4 Protocol	(Set this field if Packet Type is IPv4, else ignore.) Any / ICMP(1) / IGMP(2) / TCP(6) / UDP(17)	**Any**

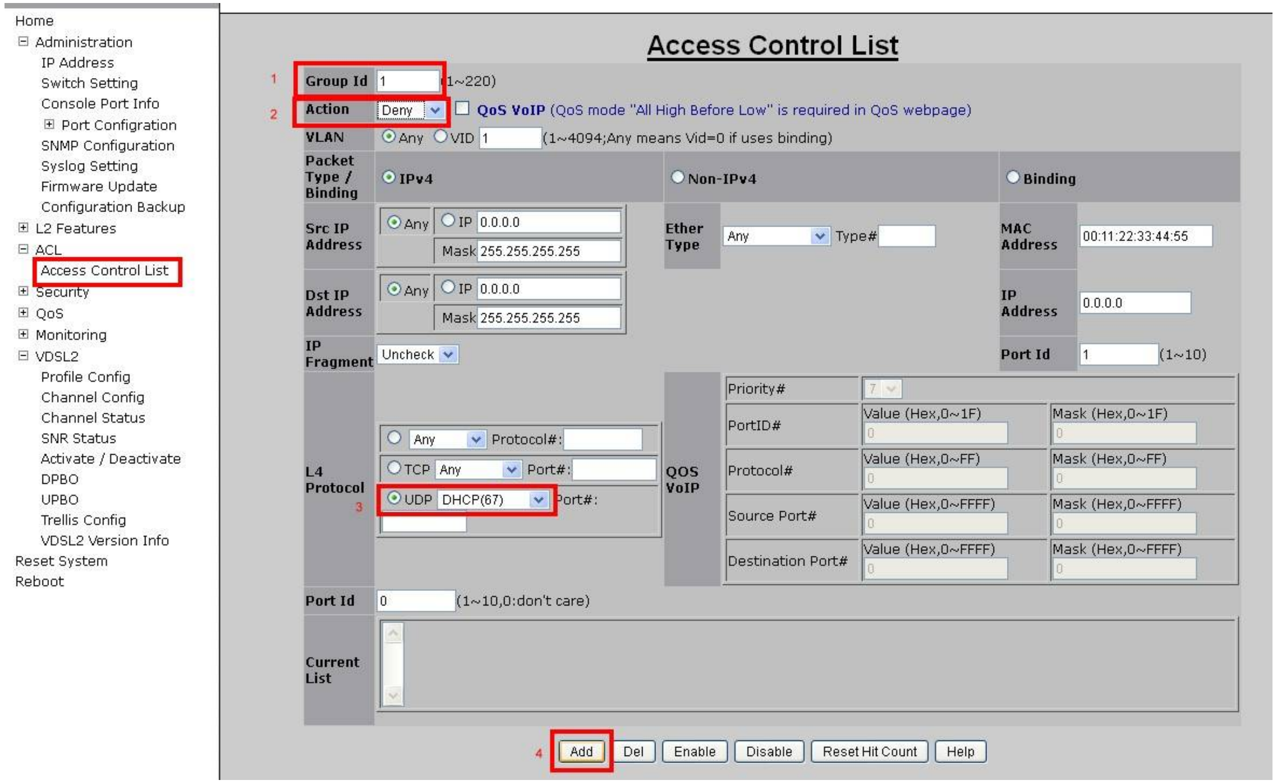
Protocol	(Set this field if Packet Type is IPv4, else ignore.) 0~255. If protocol not find in **L4 Protocol field, you can direct assign number.**	
TCP	(Set this field if Packet Type is IPv4, else ignore.) Any / FTP(21) / HTTP(80)	**Any**

Port	(Set this field if Packet Type is IPv4, else ignore.) 0~65535 If TCP port not find in TCP field, you can direct assign number.	
UDP	(Set this field if Packet Type is IPv4, else ignore.) Any / DHCP(67) / TFTP(69) / NetBios(137)	**Any**
Port	(Set this field if Packet Type is IPv4, else ignore.) 0~65535 If UDP port not find in **UDP field, you can direct assign number.**	
Port Id	Source port id, from 1~10, 0 means don’t care.	**0**
Current List	You create ACL and Binding groups.	

Count	The octetcnt is octet number of the packets hiting the ACL rule. The packetcnt is the packet number Hiting the ACL rule.	**0**

For ACL Example: Blocking DHCP Server, please access “Access Control List” via VDSL2 IP DSLAM web management.

1. Specify a group ID, you can choose number 1~220.
2. Choose Action mode: Deny
3. Choose L4 Protocol: select UDP and choose DHCP(67)
4. Press “Add” button, and you will find the the current List table that shows the settings.



Access Control List

1 Group Id 1 (1~220)

2 Action Deny ☐ QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage)

VLAN ● Any ○ VID 1 (1~4094;Any means Vid=0 if uses binding)

Packet Type / Binding ● IPv4 ○ Non-IPv4 ○ 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 Uncheck

Ether Type Any Type#

MAC Address 00:11:22:33:44:55

IP Address 0.0.0.0

Port Id 1 (1~10)

L4 Protocol
○ Any Protocol#:
○ TCP Any Port#:
3 ● UDP DHCP(67) Port#:

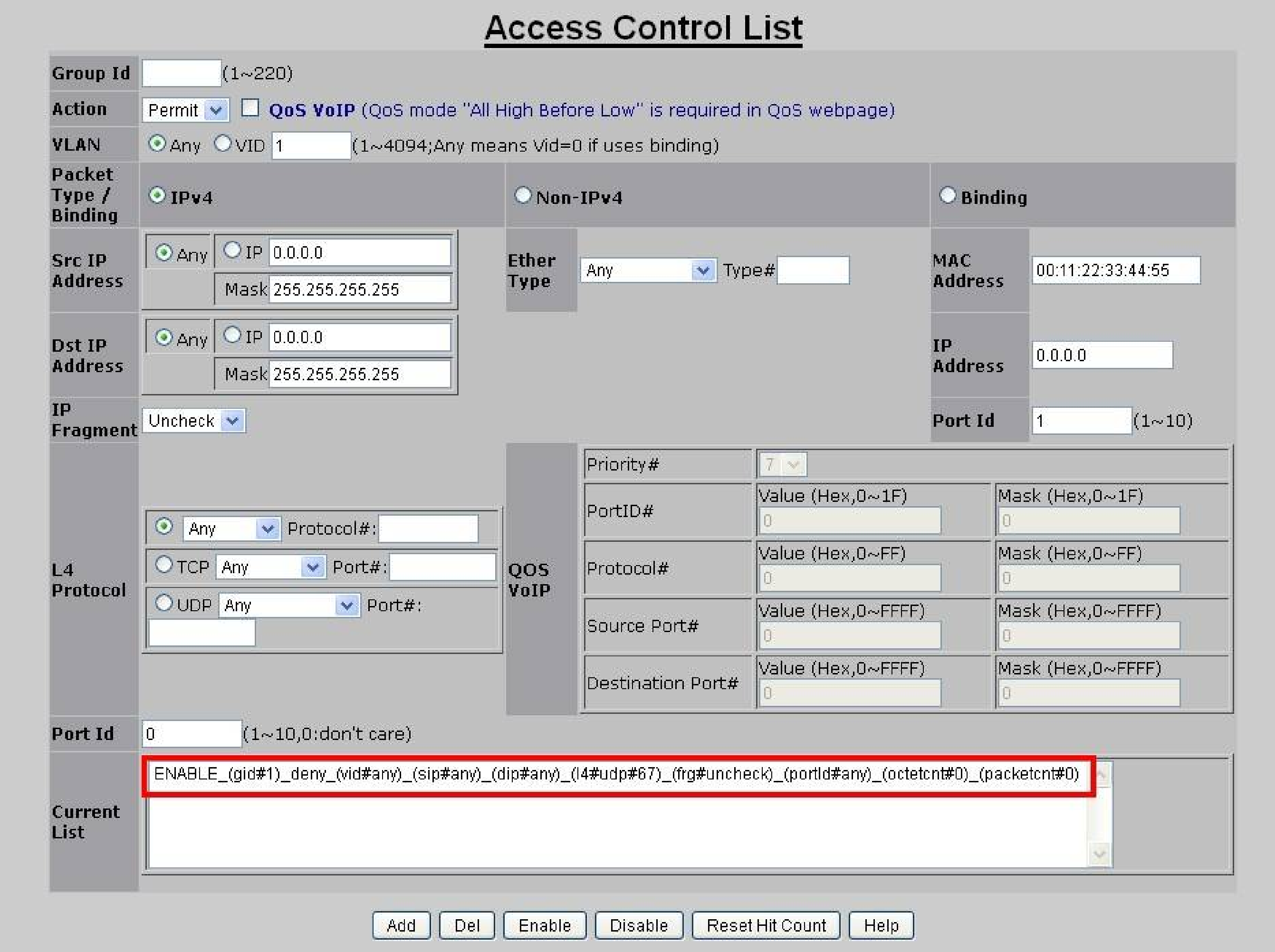
QOS VoIP

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

Port Id 0 (1~10,0:don't care)

Current List

Fig.4.4.0.1 Configure DHCP Block



Access Control List

Group Id: (1~220)

Action: Permit □ QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage)

VLAN: ● Any ○ VID 1 (1~4094;Any means Vid=0 if uses binding)

Packet Type / Binding: ● IPv4 ○ Non-IPv4 ○ 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: Uncheck

L4 Protocol: ● Any Protocol#:
○ TCP Any Port#:
○ UDP Any Port#:

Ether Type: Any Type#:

MAC Address: 00:11:22:33:44:55

IP Address: 0.0.0.0

Port Id: 1 (1~10)

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

Port Id: 0 (1~10,0:don't care)

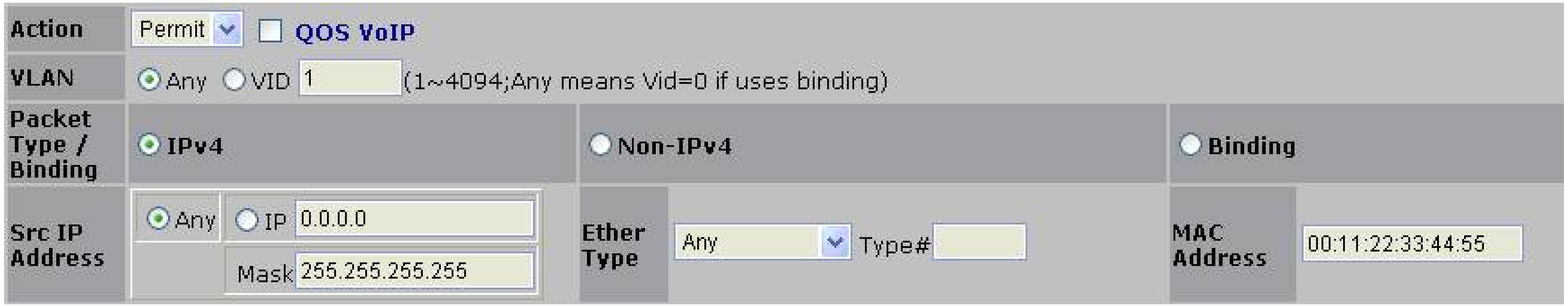
Current List:

```
ENABLE_(gid#1)_deny_(vid#any)_(sip#any)_(dip#any)_(l4#udp#67)_(frg#uncheck)_(portId#any)_(octetcnt#0)_(packetcnt#0)
```

Fig.4.4.0.2 ACL Current List

4.4.1 Non-IPv4

In “Packet Type / Binding” box should select “Non-IPv4”.



Action	Permit ▾ □ QOS VoIP		
VLAN	● Any ○ VID 1 (1~4094;Any means Vid=0 if uses binding)		
Packet Type / Binding	● IPv4	○ Non-IPv4	○ Binding
Src IP Address	● Any ○ IP 0.0.0.0 Mask 255.255.255.255	**Ether Type** Any ▾ Type#	**MAC Address** 00:11:22:33:44:55

Fig. 4.4.1 Non-IPv4

The related parameters are shown in the following table:

Items	Option	Default value
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit / Deny. c. Permit : Permit packet cross switch. d. Deny: Drop packet.	**Permit**
VLAN	Any / VID. a. Any: Any Vlan id.	**Any**

	b. VID: 1~4094. A certain vlan id.	

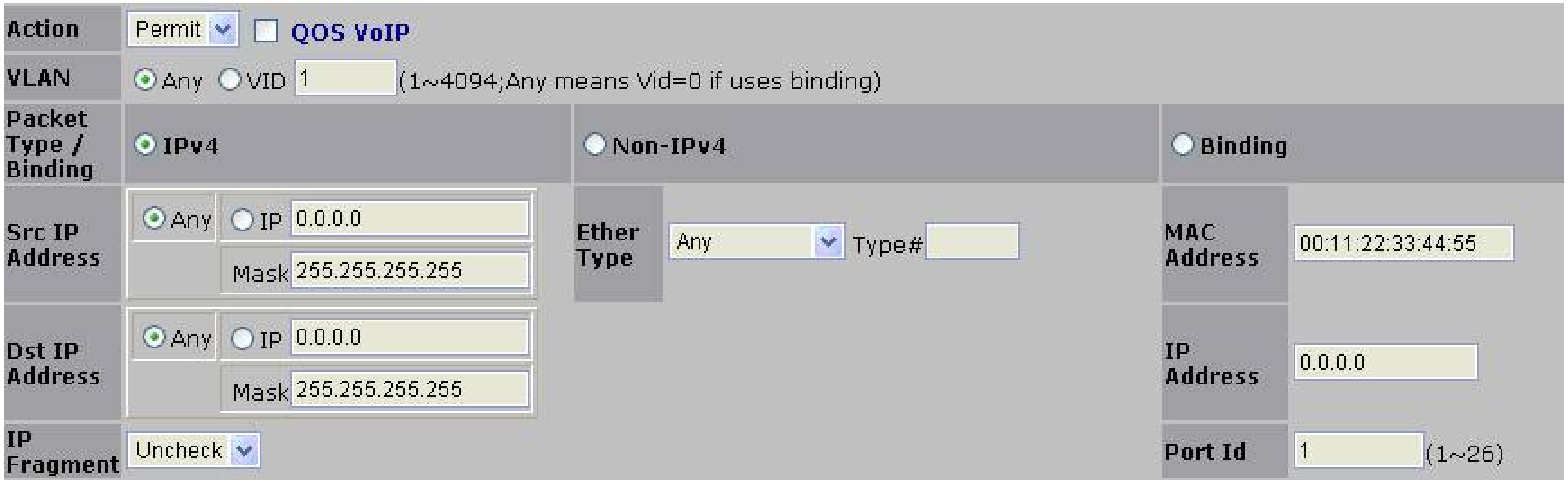
Packet Type	IPv4 / Non-IPv4 / Binding d. IPv4: Set Ipv4 packet field. e. Non-IPv4: Set non-Ipv4 packet field. f. Binding: Set binding function.	**IPv4**
Ether Type	(Set this field if Packet Type is Non-IPv4, else ignore.) Any / ARP(0x0806) / IPX(0x8137)	**Any**
Type	(Set this field if Packet Type is Non-IPv4, else ignore.) 0~0xFFFF If ether type not find in Ether Type field, you can direct assign number.	
Current List	You create ACL and Binding groups.	

4.4.2 Binding

Let device that has specific IP address and MAC address can use network. We can set specific IP address, MAC address, VLAN id and port id to bind, and device can cross switch if all conditions match.

Use binding function; we should enable it first in following page.

In “Packet Type / Binding” box should select “Binding”.



Action	Permit ▾ □ QOS VoIP				
VLAN	● Any ○ VID 1 (1~4094;Any means Vid=0 if uses binding)				
Packet Type / Binding	● IPv4	○ Non-IPv4		○ Binding	
Src IP Address	● Any ○ IP 0.0.0.0 Mask 255.255.255.255	Ether Type	Any ▾ Type#	MAC Address	00:11:22:33:44:55
Dst IP Address	● Any ○ IP 0.0.0.0 Mask 255.255.255.255			IP Address	0.0.0.0
IP Fragment	Uncheck ▾			Port Id	1 (1~26)

Fig. 4.4.2 Binding

The related parameters are shown in the following table:

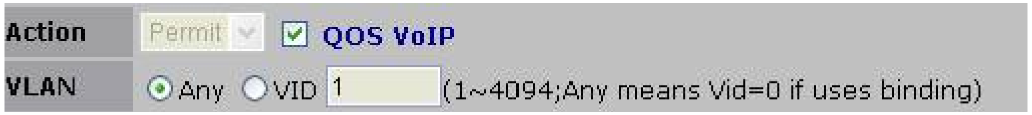
Items	Option	Default value
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit / Deny. e. Permit : Permit packet cross switch.	**Permit**

	f. Deny: Drop packet.	
VLAN	Any / VID. e. Any: Any Vlan id. f. VID: 1~4094. A certain vlan id.	**Any**
Packet Type	IPv4 / Non-IPv4 / Binding g. IPv4: Set Ipv4 packet field. h. Non-IPv4: Set non-Ipv4 packet field. i. Binding: Set binding function.	**IPv4**
Mac address	**:**:**:**:**:** * is represent a digit from 0~9 and A~F, *** is range from 0 to FF.	**00:11:22:33:44:55**
IP address	***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255.	**0.0.0.0**
Port Id	Source port id, from 1~10.	**1**
Current List	You create ACL and Binding groups.	

4.4.3 QoS VoIP

QoS VoIP option in Action field is to provide ingress VoIP packets can be forwarded out with higher priority through the ACL function.

In “Action” box select the “QoS VoIP” checkbox to make QoS VoIP parameter area available to configure.



Action Permit ☑ QOS VoIP

VLAN ● Any ○ VID 1 (1~4094;Any means Vid=0 if uses binding)

Fig. 4.4.3 QoS VoIP

QoS VoIP Parameter	Option	Default value
Priority	0 ~ 7	7
PortID	0~1F	0
PortID Mask	0~1F	0
Protocol	0~FF	0
Protocol Mask	0~FF	0
Source Port	0~FFFF	0
Source Port Mask	0~FFFF	0
Destination Port	0~FFFF	0
Destination Port Mask	0~FFFF	0

All parameters with HEX format provide settings in continuous range.

For example, if we want VoIP packets, with UDP protocol type (17) and source port number is in range of 10000~10015, to be forwarded out with highest priority while network congestion happens, an ACL rule can be created like the following setting:

Parameter	Value

GID	**1**
Action	**QoS VoIP**
VLAN	**Any**
Priority	**7**
PortID	**0**
PortID Mask	**0**
Protocol	**11h**
Protocol Mask	**1FH**
Source Port	**2710h**
Source Port Mask	**FF00h**
Destination Port	**0**
Destination Port Mask	**0**

4.5 Security

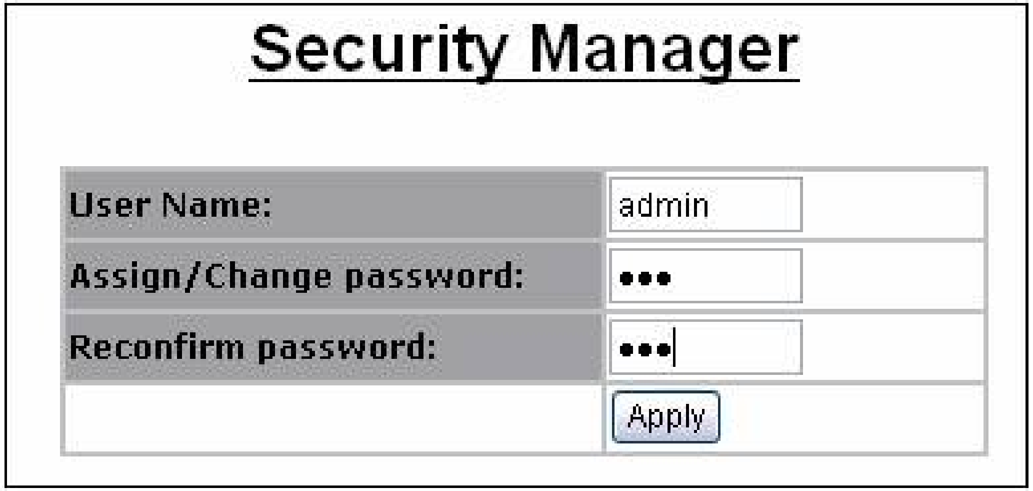
4.5.0 Security Manager

In this page, user can change user name and password with the following parameters.

User Name: Type the new user name.

Assign/Change password: Type the new password.

Reconfirm password: Retype the new password.



Security Manager

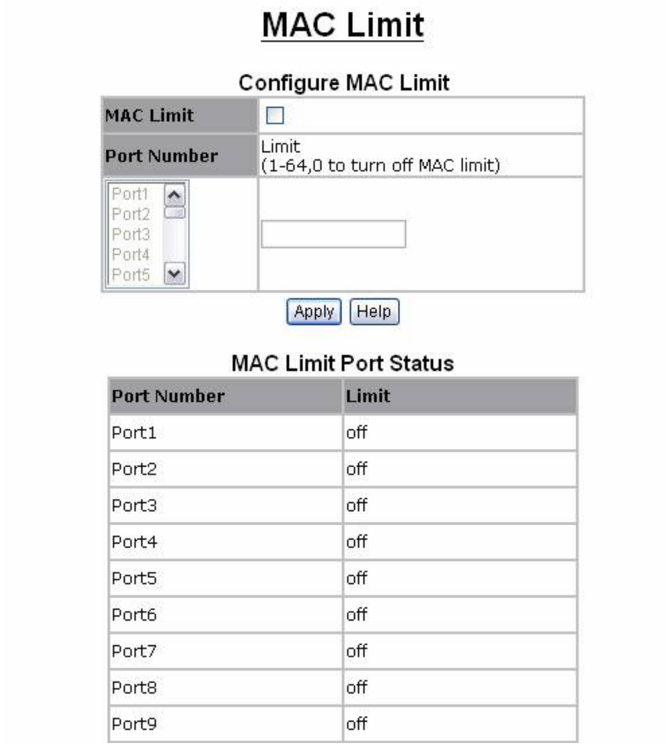
User Name:	admin
Assign/Change password:	•••
Reconfirm password:	•••
	Apply

Fig. 4.5.0 Security Manager

Click Apply to activate the setting.

4.5.1 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.



MAC Limit

Configure MAC Limit

MAC Limit	□
Port Number	Limit (1-64,0 to turn off MAC limit)
Port1 Port2 Port3 Port4 Port5	

MAC Limit Port Status

Port Number	Limit
Port1	off
Port2	off
Port3	off
Port4	off
Port5	off
Port6	off
Port7	off
Port8	off
Port9	off

Fig. 4.5.1 MAC Limit

MAC Limit: enable/disable MAC limit function

Limit: select port number and input Limit value (0~64, 0 to turn off MAC limit)

Click Apply to activate the setting.

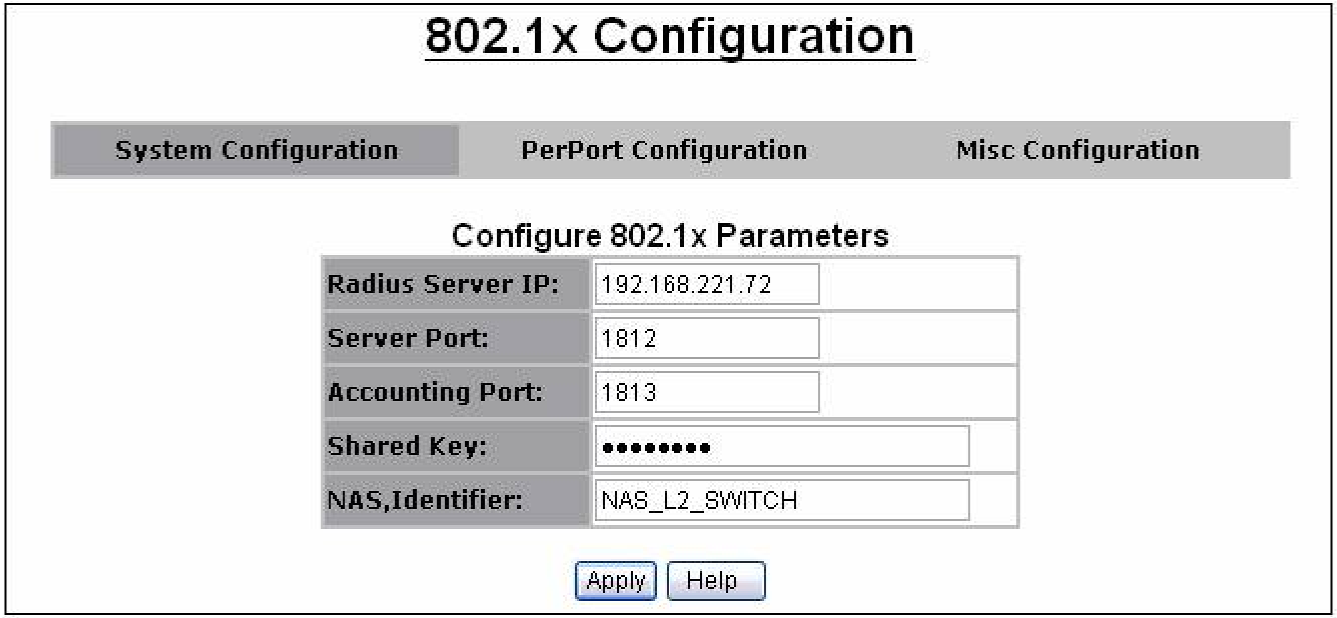
4.5.2 802.1x Configuration

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.

In the beginning, 802.1x configuration page is disabled because 802.1x is disabled in default. To enable 802.1x, go to **Administration** ->**Switch setting** ->**Misc Configs** page to enable the **802.1x protocol** field. After clicked Apply, the 802.1x configuration page will be shown up.

4.5.2.0 System Configuration

In this page, the parameters related to authentication (Radius) server are provided:



802.1x Configuration

System Configuration | PerPort Configuration | Misc Configuration

Configure 802.1x Parameters

Radius Server IP:	192.168.221.72
Server Port:	1812
Accounting Port:	1813
Shared Key:	●●●●●●●●●
NAS,Identifier:	NAS_L2_SWITCH

Fig 4.5.2.0 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).

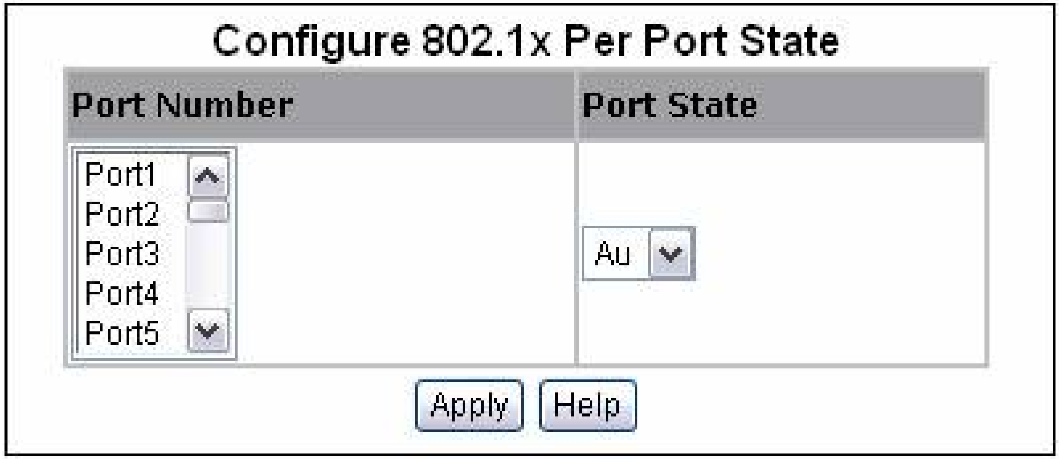
Accounting Port: The UDP port number used by the authentication server to retrieve accounting information (default: 1813).

Shared Key: A key shared between this switch and authentication server.

NAS, Identifier: A string used to identify this switch.

4.5.2.1 Perport Configuration

In this page, you can select the specific port and configure the authorization state. There are 4 kinds of authorization state to provide for each port.



Configure 802.1x Per Port State

Port Number	Port State
Port1 Port2 Port3 Port4 Port5	Au

Fig. 4.5.2.1 Perport Configuration

Fu: Force the specific port to be unauthorized.

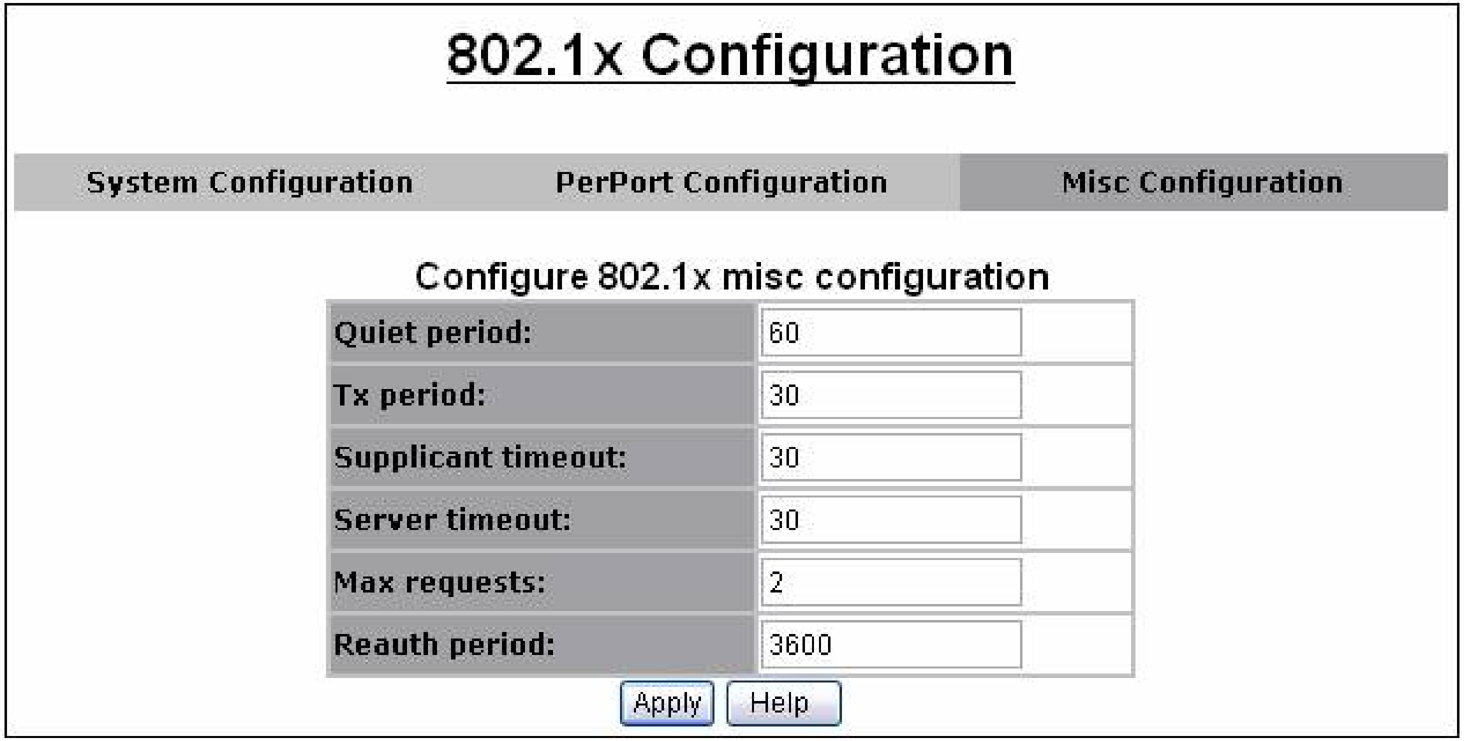
Fa: Force the specific port to be authorized.

Au: The state of the specific port was determined by the outcome of the authentication.

No: The specific port didn't support 802.1x function.

4.5.2.2 Misc Configuration

In this page, you can change the default configuration for the 802.1x standard:



Configure 802.1x misc configuration

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

Fig. 4.5.2.2 Misc Configuration

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).

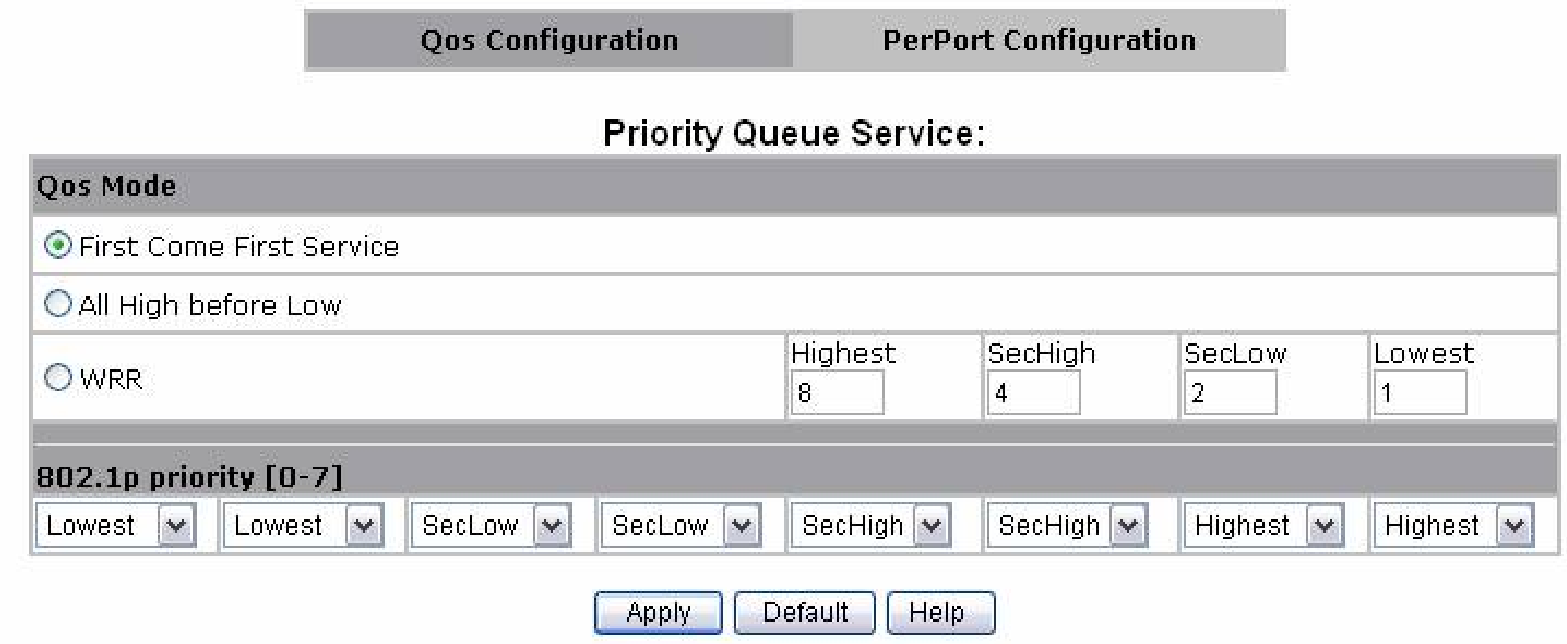
Reauth Period: Used to determine a nonzero number of seconds between periodic re-authentication of the supplications (default value: 3600 seconds).

4.6 QoS

This switch provides quality of service (QoS) to prioritize the packet forwarding when traffic congestion happens. This switch supports port-based (4-level output queue) and 802.1p (8-level priority to 4-level queue mapping) QoS functions. Strict and weight round robin (WRR) QoS mode are supported.

4.6.0 QoS Configuration

This page is mainly to set the QoS mode (First Come First Service, All High before Low, and WRR) and 8-level priority to 4 – level queue mapping.



Priority Queue Service:

Qos Mode

● First Come First Service

○ All High before Low

○ WRR

Highest	SecHigh	SecLow	Lowest
8	4	2	1

802.1p priority [0-7]

Lowest	Lowest	SecLow	SecLow	SecHigh	SecHigh	Highest	Highest

Fig. 4.6.0 QoS Configuration

First Come First Service: The sequence of packets sent is depending on arrive orders. This mode can be regarded as QoS is disabled.

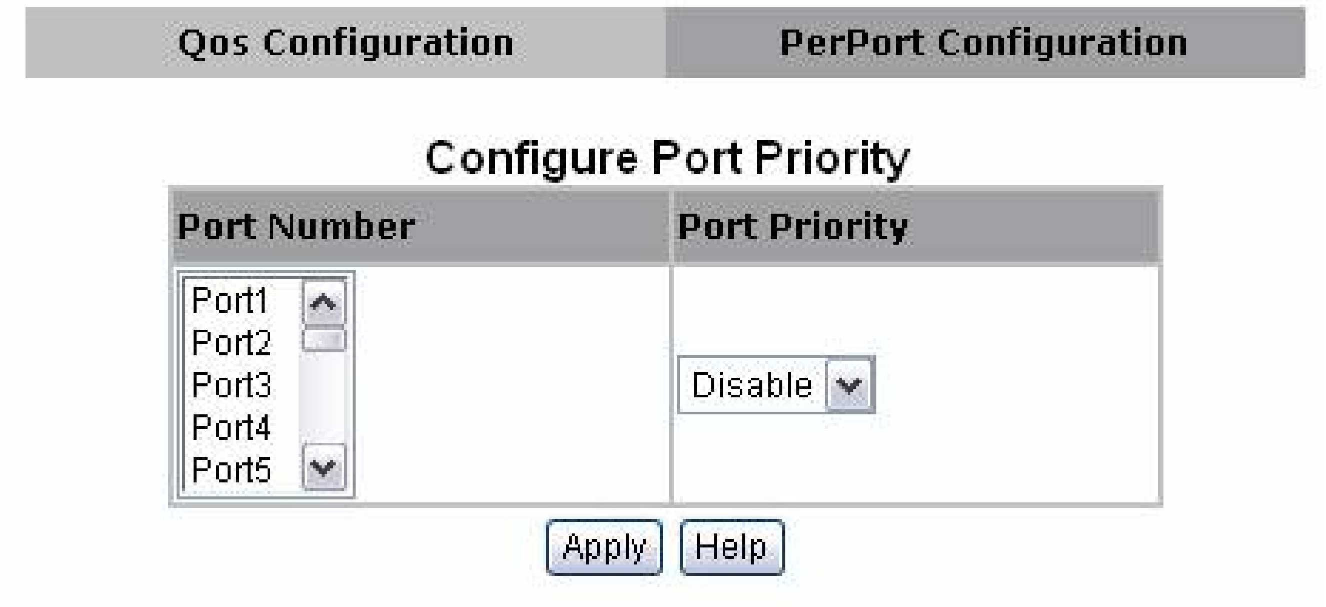
All High before Low: The high priority packets sent before low priority packets.

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.

QoS Priority: 8-level (0~7) priority can be mapped to 4-level (Highest, Second-High, Second-Low, Lowest) queue.

4.6.1 Per-Port Configuration

Per-port priority can be configured and shown in this page.



Configure Port Priority

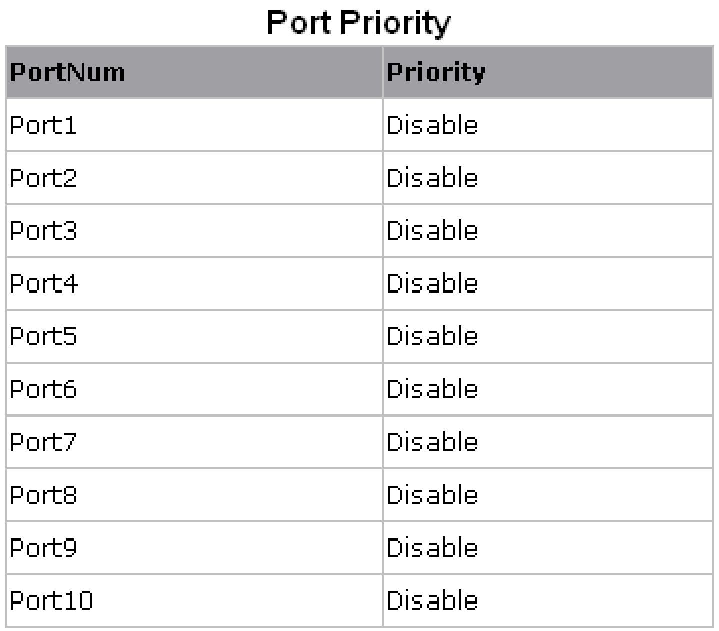
Port Number	Port Priority
Port1 Port2 Port3 Port4 Port5	Disable

Fig. 4.6.1a Per-Port Configuration

Port Number: the ports in the switch.

Port Priority: port priority can be disable or 0-7.

Per-Port priority setting can be displayed like the following figure.



Port Priority

PortNum	Priority
Port1	Disable
Port2	Disable
Port3	Disable
Port4	Disable
Port5	Disable
Port6	Disable
Port7	Disable
Port8	Disable
Port9	Disable
Port10	Disable

Fig. 4.6.1b Per-Port Configuration

4.6.2 ToS/DSCP Configuration

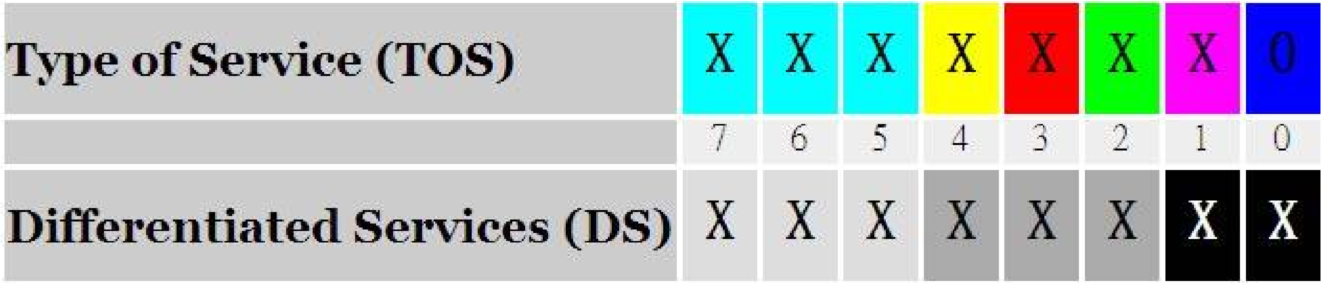
The IP Type of Service Header Field (Reference Only)

The Type of Service field in the IP header was originally defined in RFC 791. It defined a mechanism for assigning a priority to each IP packet as well as a mechanism to request specific treatment such as high throughput, high reliability or low latency.

In practice, only the IP Precedence part of the field was ever used. At its simplest, the higher the value of the IP Precedence field, the higher the priority of the IP packet.

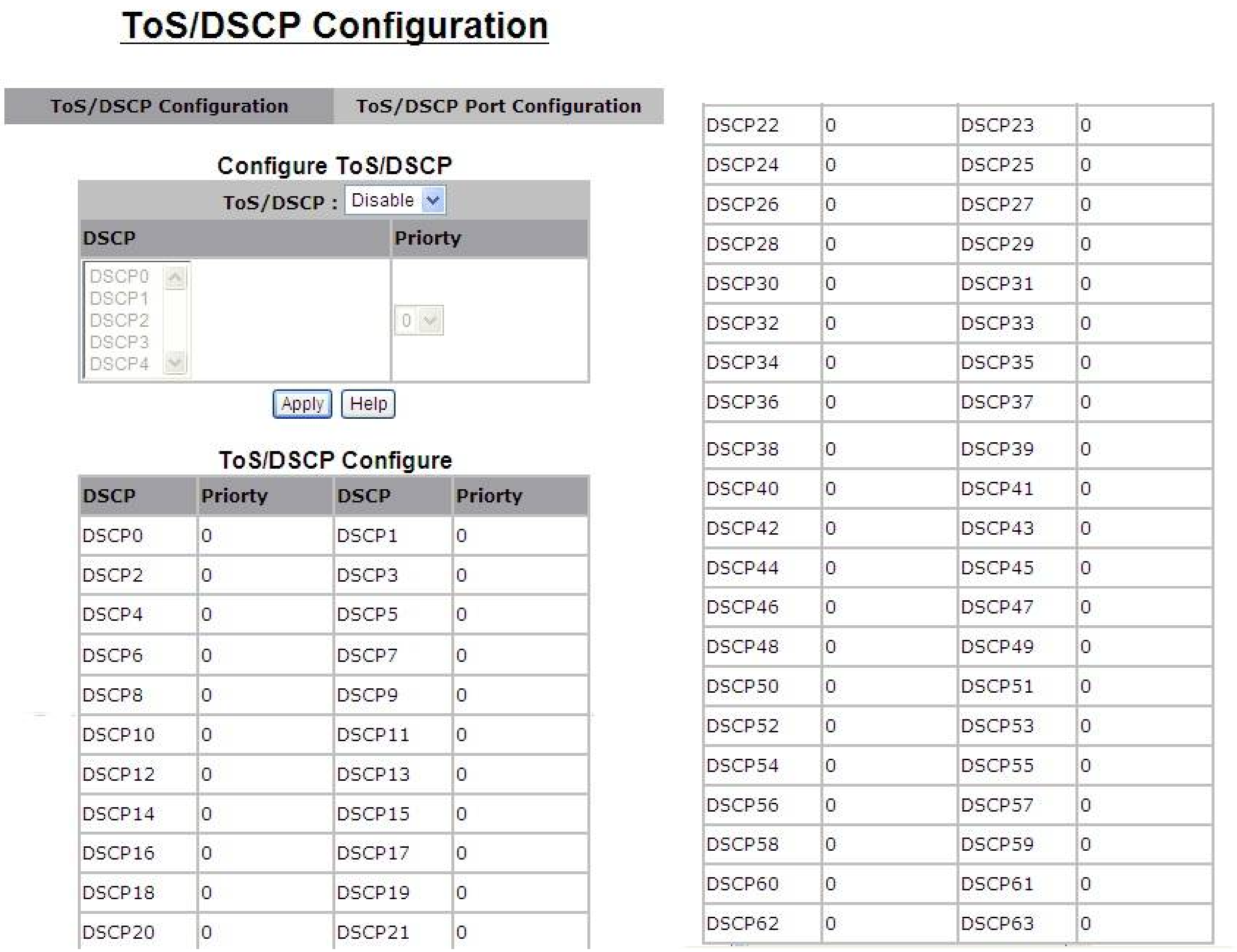
In RFC 2474 the definition of this entire field was changed. It is now called the "DS" (Differentiated Services) field and the upper 6 bits contain a value called the "DSCP" (Differentiated Services Code Point). Since RFC 3168, the remaining two bits (the two least siginficant bits) are used for Explicit Congestion Notification.

The diagram below illustrates the relationship between the bits in the Type of Services/Differeniated Services field in the IP header:



Type of Service (TOS)	X	X	X	X	X	X	X	0
	7	6	5	4	3	2	1	0
Differentiated Services (DS)	X	X	X	X	X	X	X	X

DSCP priority of ToS setting can be displayed like the following figure.



Configure ToS/DSCP

ToS/DSCP : Disable

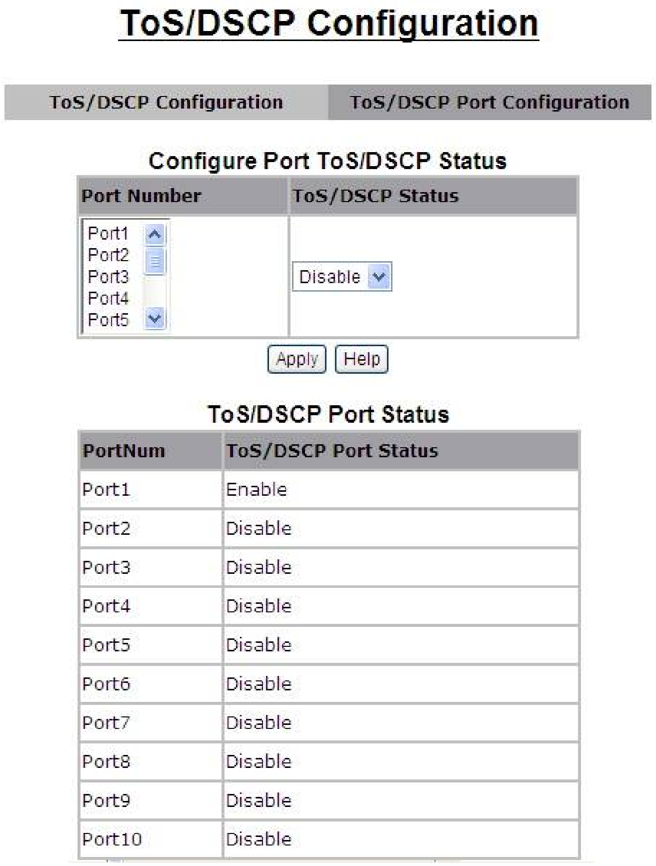
DSCP	Priorty
DSCP0 DSCP1 DSCP2 DSCP3 DSCP4	0

ToS/DSCP Configure

DSCP	Priorty	DSCP	Priorty
DSCP0	0	DSCP1	0
DSCP2	0	DSCP3	0
DSCP4	0	DSCP5	0
DSCP6	0	DSCP7	0
DSCP8	0	DSCP9	0
DSCP10	0	DSCP11	0
DSCP12	0	DSCP13	0
DSCP14	0	DSCP15	0
DSCP16	0	DSCP17	0
DSCP18	0	DSCP19	0
DSCP20	0	DSCP21	0
DSCP22	0	DSCP23	0
DSCP24	0	DSCP25	0
DSCP26	0	DSCP27	0
DSCP28	0	DSCP29	0
DSCP30	0	DSCP31	0
DSCP32	0	DSCP33	0
DSCP34	0	DSCP35	0
DSCP36	0	DSCP37	0
DSCP38	0	DSCP39	0
DSCP40	0	DSCP41	0
DSCP42	0	DSCP43	0
DSCP44	0	DSCP45	0
DSCP46	0	DSCP47	0
DSCP48	0	DSCP49	0
DSCP50	0	DSCP51	0
DSCP52	0	DSCP53	0
DSCP54	0	DSCP55	0
DSCP56	0	DSCP57	0
DSCP58	0	DSCP59	0
DSCP60	0	DSCP61	0
DSCP62	0	DSCP63	0

Fig. 4.6.2a Per-DSCP Configuration

Per-Port status setting can be displayed like the following figure.



ToS/DSCP Configuration

Configure Port ToS/DSCP Status

Port Number	ToS/DSCP Status
Port1 Port2 Port3 Port4 Port5	Disable

ToS/DSCP Port Status

PortNum	ToS/DSCP Port Status
Port1	Enable
Port2	Disable
Port3	Disable
Port4	Disable
Port5	Disable
Port6	Disable
Port7	Disable
Port8	Disable
Port9	Disable
Port10	Disable

Fig. 4.6.2b Per-Port status configuration

DSCP comparison table example(Reference only):

IP Precedence (3 Bits)			DSCP (6bits)						
Name	Value	Bits	Per-Hop Behavior	Drop Precedence	Codepoint Name	Application	DSCP (Binary)	DSCP (Decima)	ToS (Decimal)
Rountine	0	000	Default		Default				
Priotity	1	001	AF	1:Low	AF11	Leased Line	001 010	10(0x0a)	40(0x28)
				2:Medium	AF12	Leased Line	001 100	12(0x0c)	48(0x30)
				3:High	AF13	Leased Line	001 110	14(0x0e)	56(0x38)
Immediate	2	010	AF	1:Low	AF21	IPTV VOD	010 010	18(0x12)	72(0x48)
				2:Medium	AF22	IPTV VOD	010 100	20(0x14)	80(0x50)
				3:High	AF23	IPTV VOD	010 110	22(0x16)	88(0x58)
Flash	3	011	AF	1:Low	AF31	IPTV Broadcast	011 010	26(0x1a)	104(0x68)
				2:Medium	AF32	IPTV Broadcast	011 100	28(0x1c)	112(0x70)
				3:High	AF33	IPTV Broadcast	011 110	30(0x1e)	120(0x78)
Flash Override	4	100	AF	1:Low	AF41	NGN/3G Singaling	100 010	34(0x22)	136(0x88)
				2:Medium	AF42	NGN/3G Singaling	100 100	36(0x24)	144(0x90)
				3:High	AF43	NGN/3G Singaling	100 110	38(0x26)	152(0x98)
Critical	5	101	EF		EF	NGN/3G voice	101 110	46(0x2e)	184(0xb8)
Internetwork Control	6	110	- -		CS6	Protocol	110 100	48(0x30)	192(0xc0)
Network Control	7	111	- -		CS7	Protocol	111 000	56(0x38)	224(0xe0)

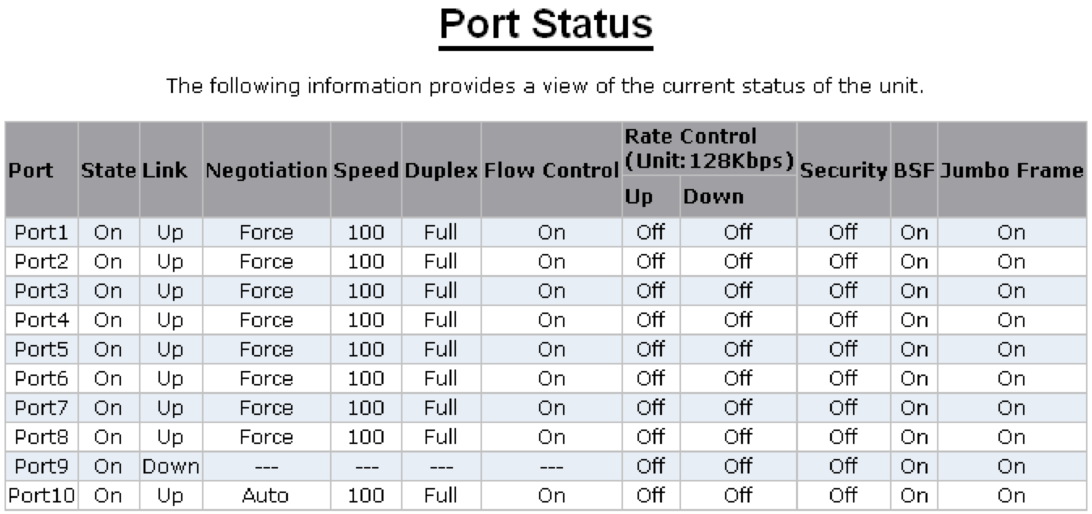
4.7 Monitoring

The following items are provided in Monitoring section:

- Port status
- Port statistics

4.7.0 Port Status

This page provides current status of every port that depends on user's setting and the negotiation result.



Port Status

The following information provides a view of the current status of the unit.

Port	State	Link	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit:128Kbps)		Security	BSF	Jumbo Frame
							Up	Down			
Port1	On	Up	Force	100	Full	On	Off	Off	Off	On	On
Port2	On	Up	Force	100	Full	On	Off	Off	Off	On	On
Port3	On	Up	Force	100	Full	On	Off	Off	Off	On	On
Port4	On	Up	Force	100	Full	On	Off	Off	Off	On	On
Port5	On	Up	Force	100	Full	On	Off	Off	Off	On	On
Port6	On	Up	Force	100	Full	On	Off	Off	Off	On	On
Port7	On	Up	Force	100	Full	On	Off	Off	Off	On	On
Port8	On	Up	Force	100	Full	On	Off	Off	Off	On	On
Port9	On	Down	---	---	---	---	Off	Off	Off	On	On
Port10	On	Up	Auto	100	Full	On	Off	Off	Off	On	On

Fig. 4.7.0 Port Status

State: Display port statuses: **disable or enable**. "Unlink" will be treated as "off".

Link Status: Down means "No Link"; Up means "Link up".

Auto Negotiation: Display the auto negotiation mode: auto/force/nway-force.

Speed status: Display 100Mbps speed, port 1- 8 are 10/100Mbps, Port 9~10 are 10/100/1000Mbps.

Duplex status: Display full-duplex or half-duplex mode.

Flow Control: Display the flow control state

Full: Display the flow control is enabled or disabled in full mode.

Half: Display the backpressure is enabled or disabled in half mode.

Rate Control(Traffic shaping): Display the rate control setting.

Up(Ingress): Display the port effective ingress rate of user setting.

Down(Egress): Display the port effective egress rate of user setting.

Port Security: Display the port security is enabled or disabled.

BSF: Display the port broadcast storm filter control is enable or disable.

Jumbo Frame: Display the jumbo frame is supported or not for the port.

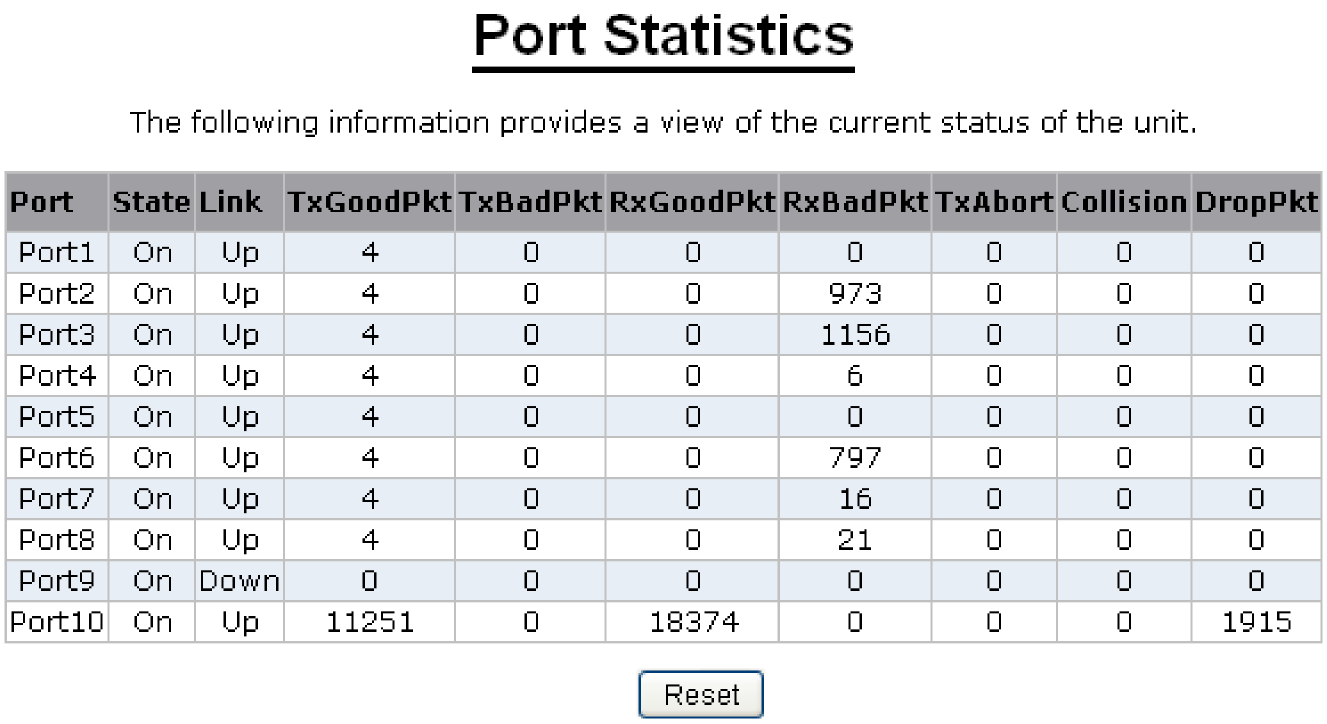
Note:

You can click the Browser’s Refresh button or press <F5> button to obtain the latest status.

4.7.1 Port Statistics

The following information provides a view of the current status of the whole unit.

Press Reset button to clean all count.



Port Statistics

The following information provides a view of the current status of the unit.

Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
Port1	On	Up	4	0	0	0	0	0	0
Port2	On	Up	4	0	0	973	0	0	0
Port3	On	Up	4	0	0	1156	0	0	0
Port4	On	Up	4	0	0	6	0	0	0
Port5	On	Up	4	0	0	0	0	0	0
Port6	On	Up	4	0	0	797	0	0	0
Port7	On	Up	4	0	0	16	0	0	0
Port8	On	Up	4	0	0	21	0	0	0
Port9	On	Down	0	0	0	0	0	0	0
Port10	On	Up	11251	0	18374	0	0	0	1915

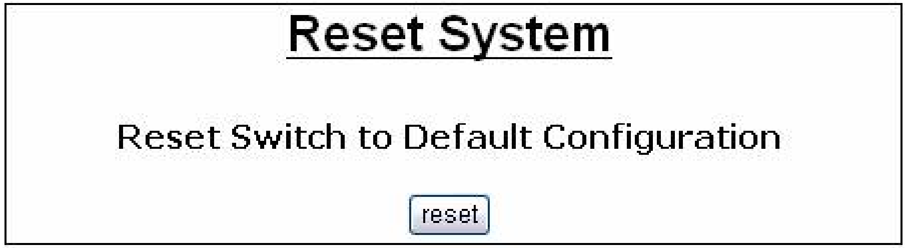
Fig. 4.7.1 Port Statistics

4.8 Reset System

The page to reset the switch to default configuration is shown as below.

Warning:

All configuration settings are restored to factory default setting.



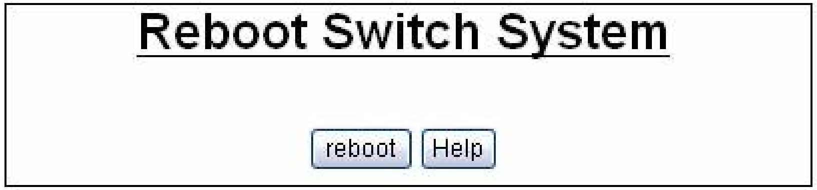
Reset System

Reset Switch to Default Configuration

Fig. 4.8 Reset System

4.9 Reboot

The page to reboot (warm restart) the switch is shown as below.



Reboot Switch System

Fig. 4.9 Reboot

Chapter 5. VDSL2 functions

The page to configure and show VDSL2 functions.

5.1 Profile Config

The page to configure VDSL2 Profile, BandPlan and Tone Mode.

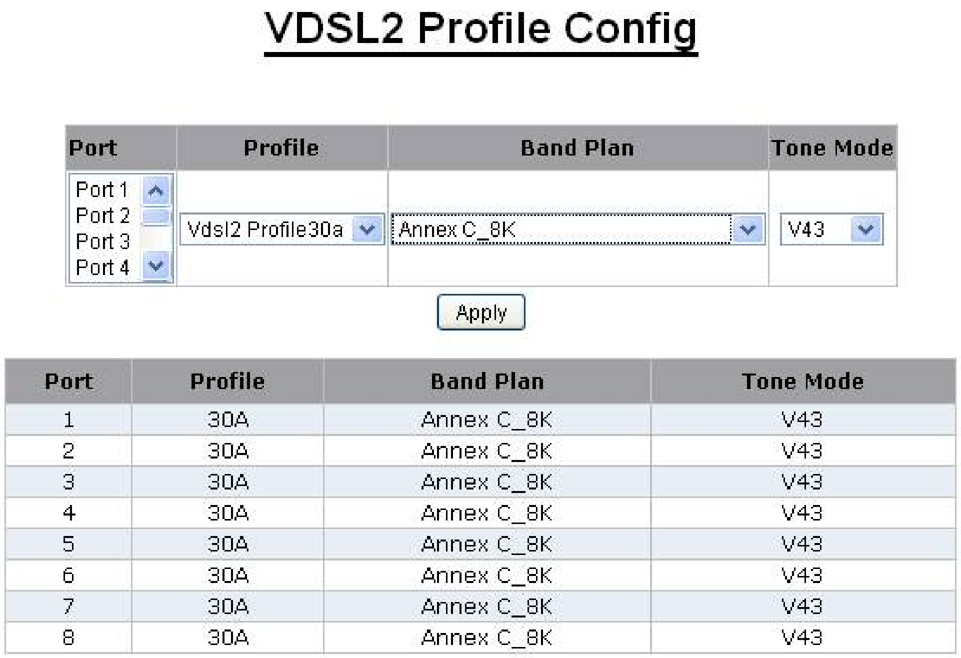
For this function, VDSL2 IP DSLAM provides world wide telecom standard band plan, such as meet European telecom standard band plan 998(17a), USA telecom standard band plan 997(8a, 8b) and APAC Telecom standard band plan (30a) etc.

- **Annex A** specifies bandplans for the North American region and enables VDSL2 IP DSLAM to be deployed with traditional POTS telephony or in an all-digital mode.
- **Annex B** specifies bandplans for Europe and enables VDSL2 IP DSLAM deployment with underlying POTS and ISDN services.
- **Annex C** allows VDSL2 IP DSLAM to coexist with TCM-ISDN services, found primarily in APAC.

VDSL2 IP DSLAM has numerous configuration profiles and bandplans to meet regional service provider requirements. The frequency bandwidth has increased to 30 MHz, with configuration options at 8.5 MHz, 12 MHz, 17.7 MHz and 30 MHz.

Band profile and band plan can only be configured at VDSL2 IP DSLAM as Router will auto-follow up on the settings of VDSL2 IP DSLAM. The only thing that Router must be configured so that the routers will link is the tone mode. However, the default tone mode for VDSL2 IP DSLAM / Router is V43, so at default there’s no need to change the tone mode unless it is required by the telecom companies to use different tone mode. Another important thing is that band profile and band plan setting must be compatible to each other if not access error will show when applied. Please deactivate and activate once the setting has been changed.

Default plan profile and band plan = 30a and C8K

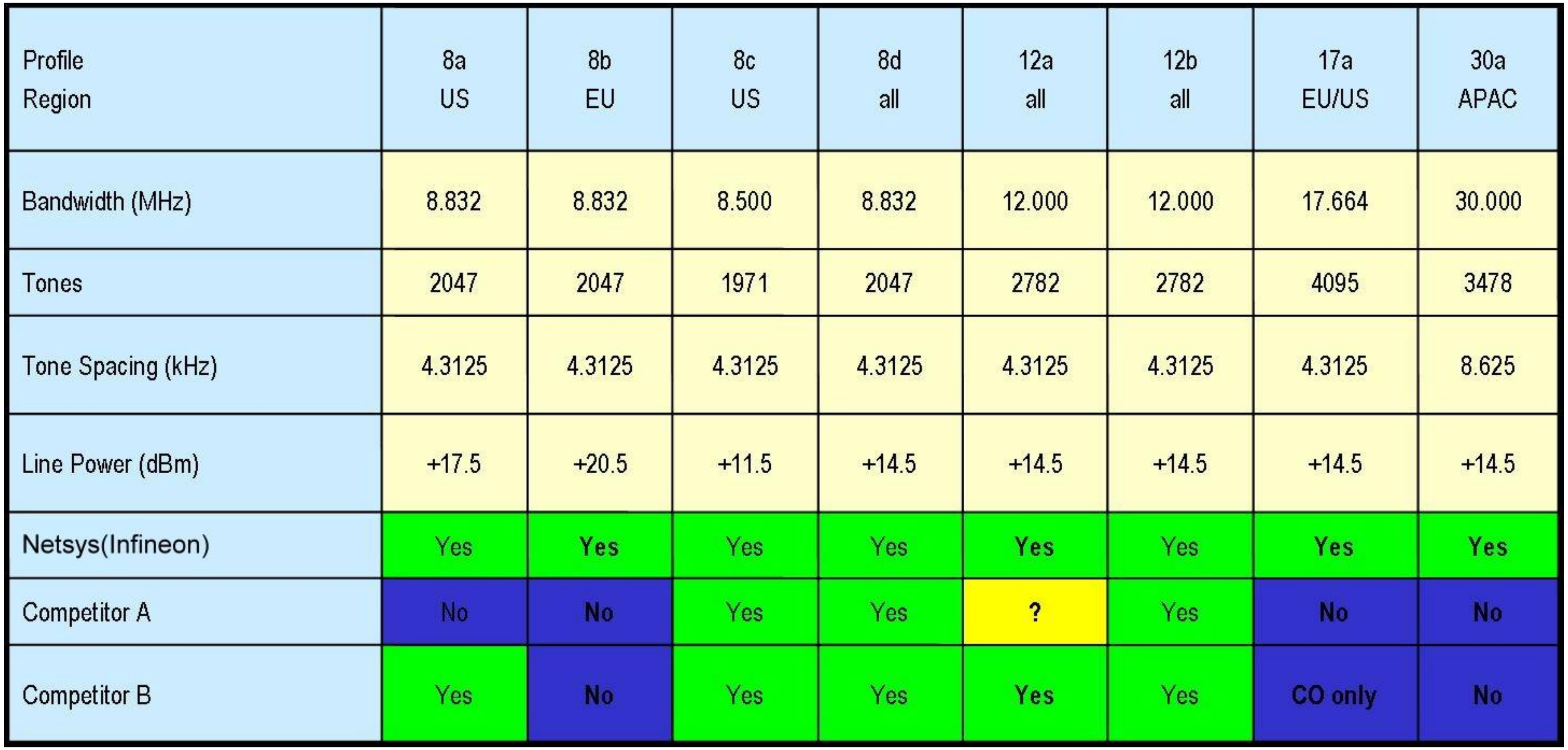


VDSL2 Profile Config

Port	Profile	Band Plan	Tone Mode
Port 1 Port 2 Port 3 Port 4	Vdsl2 Profile30a	Annex C_8K	V43

Port	Profile	Band Plan	Tone Mode
1	30A	Annex C_8K	V43
2	30A	Annex C_8K	V43
3	30A	Annex C_8K	V43
4	30A	Annex C_8K	V43
5	30A	Annex C_8K	V43
6	30A	Annex C_8K	V43
7	30A	Annex C_8K	V43
8	30A	Annex C_8K	V43

Figure 5.1.1 VDSL2 Profile Configuration



Profile Region	8a US	8b EU	8c US	8d all	12a all	12b all	17a EU/US	30a APAC
Bandwidth (MHz)	8.832	8.832	8.500	8.832	12.000	12.000	17.664	30.000
Tones	2047	2047	1971	2047	2782	2782	4095	3478
Tone Spacing (kHz)	4.3125	4.3125	4.3125	4.3125	4.3125	4.3125	4.3125	8.625
Line Power (dBm)	+17.5	+20.5	+11.5	+14.5	+14.5	+14.5	+14.5	+14.5
Netsys(Infineon)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Competitor A	No	No	Yes	Yes	?	Yes	No	No
Competitor B	Yes	No	Yes	Yes	Yes	Yes	CO only	No

Figure 5.1.2 Band Profile Region

The following shows the band profile and band plan compatibility:

	Band Profile List		Band Plan List
0	VDSL2 Profile8a	**0**	Annex A M1_EU32
1	VDSL2 Profile8b	**1**	Annex A M9_EU64
2	VDSL2 Profile8c	**2**	Annex A EU128
3	VDSL2 Profile8d	**3**	Annex B 997-M1c-A-7
4	VDSL2 Profile12a	**4**	Annex B 997-M2x-A
5	VDSL2 Profile12b	**5**	Annex B 997-M2x-M
6	VDSL2 Profile17a	**6**	Annex B 998-M1x-A
7	VDSL2 Profile30a	**7**	Annex B 998-M1x-B
8	VDSL2 Profile17b	**8**	Annex B 998-M2x-A
		9	Annex B 998-M2x-M
		10	Annex B 998-M2x-B
		11	Annex B 998-M2x-NUS0
		12	Annex B 998e17-M2x-NUS0
		13	Annex B 998ADE17-M2x-A

		14	Annex B 998ADE30-M2x-NUS0-A
		15	Annex C_A
		16	Annex C_M
		17	Annex C_8K

The following table shows the band profile and band plan compatibility(VDSL2 IP DSLAM with Router):

Band Profile \ Band Plan	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	O	O	O	X	X	X	X	O	X	X	O	O	X	X	X	X	X	X
1	O	O	O	X	X	X	X	O	X	X	O	O	X	X	X	X	X	X
2	O	O	O	X	X	X	X	O	X	X	O	O	X	X	X	X	X	O
3	O	O	O	X	X	X	X	O	X	X	O	O	X	X	X	X	X	X
4	O	O	O	X	X	X	X	O	X	X	O	X	X	X	X	X	X	X
5	O	O	O	X	O	O	X	O	X	O	X	O	X	X	X	O	O	O
6	O	O	O	X	X	X	X	X	X	X	X	X	O	O	O	O	O	X
7	O	X	O	X	X	X	X	X	X	X	X	X	X	X	O	X	X	O
8	O	O	O	X	X	X	X	X	X	X	X	X	X	O	X	X	X	X

Note: O = Compatible; X = Not Compatible

Table 5.1 VDSL2 IP DSLAM with Router Band Profile / Plan compatibility

The following table shows the band profile and band plan compatibility (VDSL2 IP DSLAM with Bridged)

Band Profile \ Band Plan	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	O	X	O	X	X	X	X	O	X	X	O	O	X	X	X	X	X	X
1	O	O	X	X	X	X	X	O	X	X	O	O	X	X	X	X	X	X
2	O	X	O	X	X	X	X	O	X	X	O	O	X	X	X	X	X	O
3	O	X	O	X	X	X	X	O	X	X	O	O	X	X	X	X	X	X
4	O	O	O	X	X	X	X	X	X	X	O	X	X	X	X	X	X	X
5	O	O	O	X	O	O	X	O	X	O	X	O	X	X	X	O	O	O
6	O	O	O	X	X	X	X	X	X	X	X	X	O	O	X	O	X	X
7	O	X	O	X	X	X	X	X	X	X	X	X	X	X	X	X	X	O
8	O	O	O	X	X	X	X	X	X	X	X	X	X	O	X	X	X	X

Note: O = Compatible; X = Not Compatible

Table 5.2 VDSL2 IP DSLAM with Bridged Band Profile / Plan compatibility

The following table shows the band profile and band plan compatibility (VDSL2 IP DSLAM with Managed CPE Router)

Band Profile \ Band Plan	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	O	O	O	X	X	X	X	O	X	X	O	O	X	X	X	X	X	X
1	O	O	X	X	X	X	X	O	X	X	O	O	X	X	X	X	X	X
2	O	O	O	X	X	X	X	O	X	X	O	O	X	X	X	X	X	O
3	O	O	O	X	X	X	X	O	X	X	O	O	X	X	X	X	X	X
4	O	O	O	X	X	X	X	O	X	X	O	X	X	X	X	X	X	X
5	O	O	O	X	O	O	X	O	X	O	X	O	X	X	X	O	O	O
6	O	O	O	X	X	X	X	X	X	X	X	X	O	O	O	O	O	O
7	O	X	O	X	X	X	X	X	X	X	X	X	X	X	O	X	X	O
8	O	O	O	X	X	X	X	X	X	X	X	X	X	O	X	X	X	X

Note: O = Compatible; X = Not Compatible

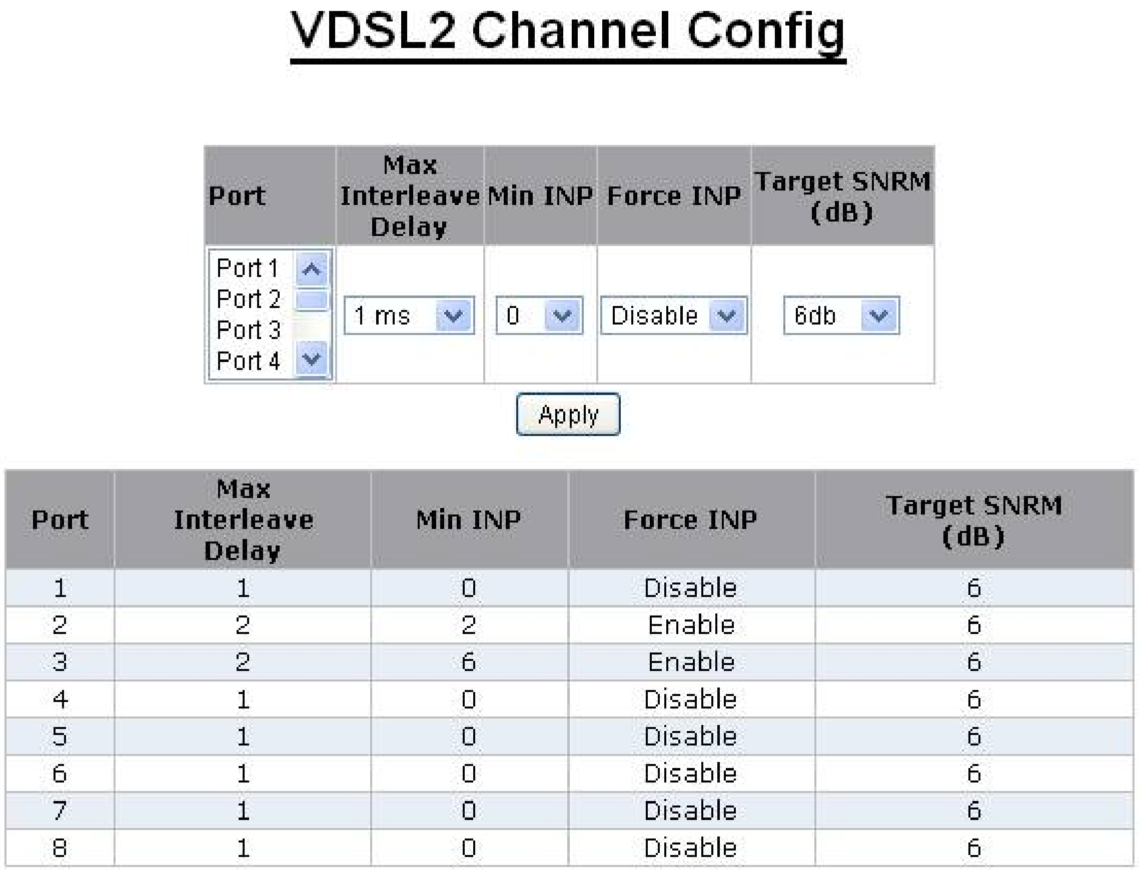
Table 5.3 VDSL2 IP DSLAM with Managed CPE Router Band Profile / Plan compatibility

Note:

Please note that do not configuration multiple different band profile and band plan within 8 VDSL2 ports, this behavior can cause serious crosstalk.

5.2 Channel Config

The page to configure VDSL2 Max Interleave Delay, Min. INP(Impules Noise Protection), Force INP and Target SNRM (Enable Force INP, Max Interleave Delay must be increased also.) The default value of interleave is auto. If you want to get the max throughput, you can set the value of interleave to 1. However, the capability of anti-interference will be reduced.



VDSL2 Channel Config

Port	Max Interleave Delay	Min INP	Force INP	Target SNRM (dB)
Port 1 Port 2 Port 3 Port 4	1 ms	0	Disable	6db

Port	Max Interleave Delay	Min INP	Force INP	Target SNRM (dB)
1	1	0	Disable	6
2	2	2	Enable	6
3	2	6	Enable	6
4	1	0	Disable	6
5	1	0	Disable	6
6	1	0	Disable	6
7	1	0	Disable	6
8	1	0	Disable	6

Figure 5.2.1 Channel Config

Max Interleave Delay: Regarding the interleave delay value time function for anti-noise purpose, due to the noise of each environment are different, therefore you can configure interleave delay value when filed environment has heavy noise.

Min INP (Impulse Noise Protection): Impulse noise in multicarrier communication systems behaves effectively as a modulating signal that controls the first moment of the background Gaussian noise. The composite noise, which is the aggregate of the Gaussian noise and impulse noise, has a probability density function that is conditionally Gaussian with non-zero average, hence referred to as biased-Gaussian. The BER-equivalent power of the composite noise source is defined as the power of a pure Gaussian noise source that yields the same bit-error rate (BER). The BER-equivalent noise for a biased-Gaussian noise is simply the amplified version of the underlying Gaussian noise source. The amplification factor is derived from the characteristics of the impulse interference. Any bit-loading algorithm designed for Gaussian noise sources is also applicable to biased-Gaussian noise sources provided that the BER-equivalent SNR is used in place of the measured SNR.

Froce INP (ITU-T G997.1): This parameter indicates that the framer settings of the bearer shall be selected such that the impulse oise protection computed according to the formula specified in the relevant Recommendation is greater than or equal to the minimal impulse noise protection requirement.
This flag shall have the same value for all the bearers of one line in the same direction.

Target SNRM: Noise Margin is the non-technical term for Signal to Noise Ratio Margin (SNRM). Domestic standard modems and VDSL2 routers often use the terms Noise Margin or SNR when reporting on its value. The Signal to Noise Ratio, as its name implies, is the ratio between the strength of the signal and the level of noise on the line.

That ratio is a major factor in determining the connection speed, as the higher the ratio the higher the possible speed. The SNRM is a margin which by which the noise level can rise before connection is lost.

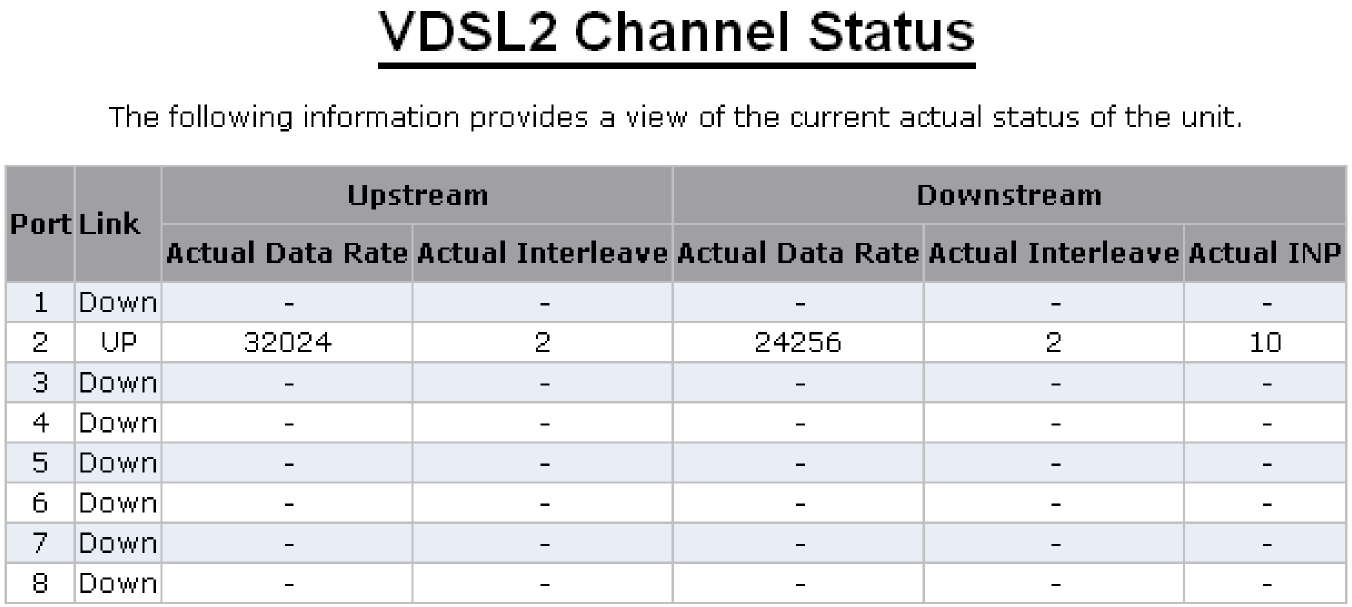
Taking the default (target) value of 6 dB applied is follow up telecom standard. Basically, you don't need configure this value.

Notes:

1. Interleave delay value must greater than or equal to INP value, otherwise VDSL2 will not establish a connection.
2. Please note you must deactivate then activate once on config port when you configure VDSL2 channel config.
3. Please note that increase interleave delay time will reduce few vdsl2 bandwidth and depending on interleave delay time.

5.3 Channel Status

The page to show VDSL2 Upstream / Downstream Actual Data Rate ,Actual Interleave and Actual Impules Noise Protection.



VDSL2 Channel Status

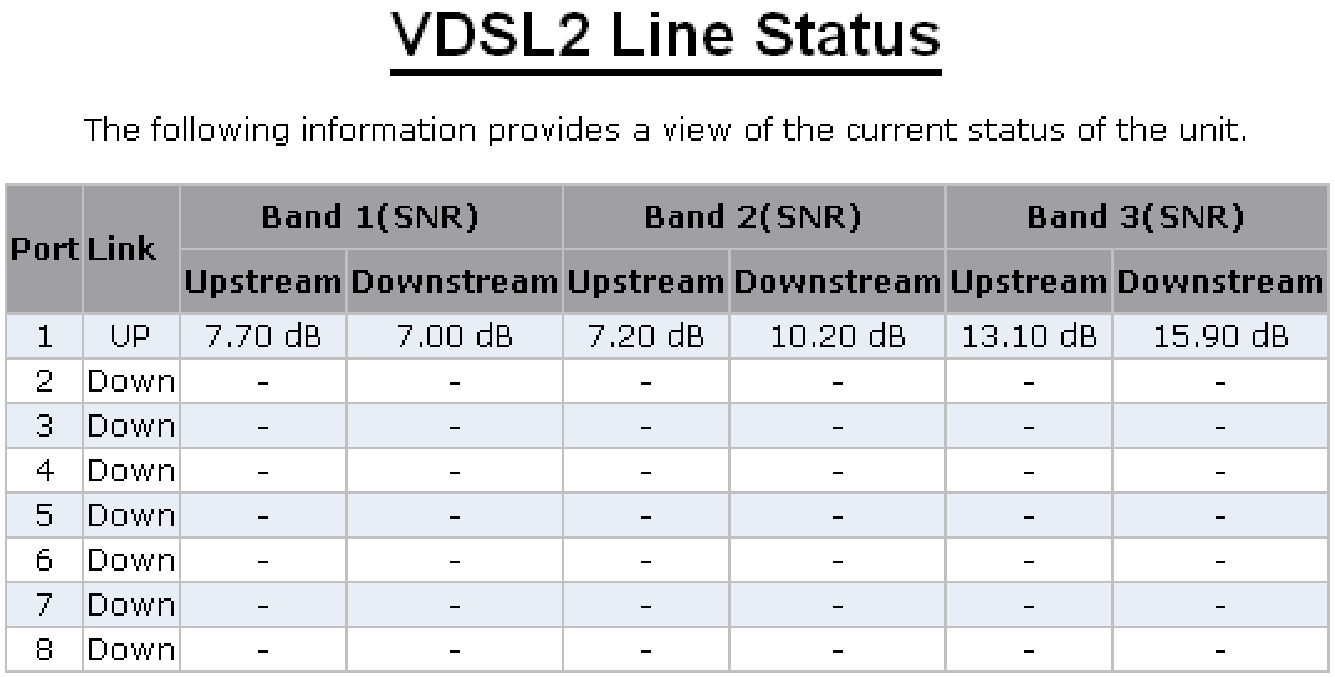
The following information provides a view of the current actual status of the unit.

Port	Link	Upstream		Downstream		
		Actual Data Rate	Actual Interleave	Actual Data Rate	Actual Interleave	Actual INP
1	Down	-	-	-	-	-
2	UP	32024	2	24256	2	10
3	Down	-	-	-	-	-
4	Down	-	-	-	-	-
5	Down	-	-	-	-	-
6	Down	-	-	-	-	-
7	Down	-	-	-	-	-
8	Down	-	-	-	-	-

Figure 5.3.1 Channel Status

5.4 SNR Status

This function provides SNR value for checking phone wiring quality.



VDSL2 Line Status

The following information provides a view of the current status of the unit.

Port	Link	Band 1(SNR)		Band 2(SNR)		Band 3(SNR)	
		Upstream	Downstream	Upstream	Downstream	Upstream	Downstream
1	UP	7.70 dB	7.00 dB	7.20 dB	10.20 dB	13.10 dB	15.90 dB
2	Down	-	-	-	-	-	-
3	Down	-	-	-	-	-	-
4	Down	-	-	-	-	-	-
5	Down	-	-	-	-	-	-
6	Down	-	-	-	-	-	-
7	Down	-	-	-	-	-	-
8	Down	-	-	-	-	-	-

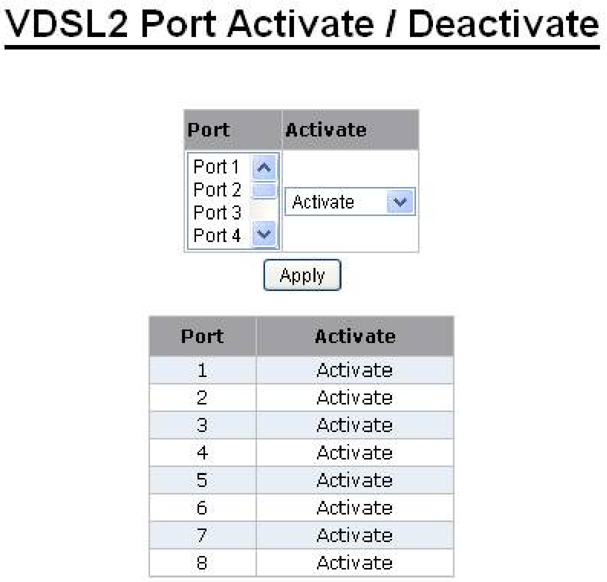
Figure 5.4.1 SNR Status

Note:

Please note that the SNR values is automatically generated. SNR values will vary depending on the quality of the copper wire and environment factors.

5.5 Activate / Deactivate

This function is for Activate / Deactivate VDSL2 port



VDSL2 Port Activate / Deactivate

Port	Activate
Port 1 Port 2 Port 3 Port 4	Activate

Port	Activate
1	Activate
2	Activate
3	Activate
4	Activate
5	Activate
6	Activate
7	Activate
8	Activate

Figure 5.5.1 Port Activate/Deactivate

Note:

1. If VDSL2 port link does not established, please check the tone mode whether is the same, if the same, Deactivate the VDSL2 port of disconnect, and then Activate it.

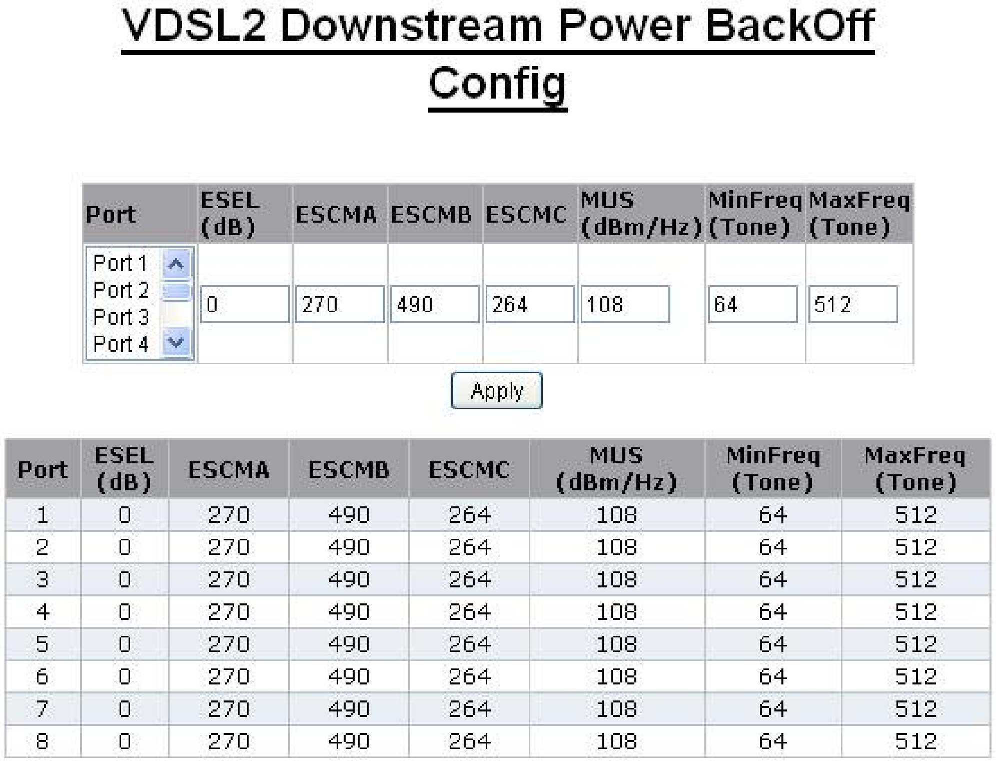
2. If you change the VDSL2 profile configuraiton(profile/band plan/tone mode), please Deactivate the port, and then Activate it.

3. If VDSL2 port link does not established when user has selected the activate and press “apply”button , please press “apply” button again.

4. Please note that each time has only config two ports, please select and press “apply” button.

5.6 DPBO

The page to configure VDSL2 Downstream Power BackOff.



VDSL2 Downstream Power BackOff Config

Port	ESEL (dB)	ESCMA	ESCMB	ESCMC	MUS (dBm/Hz)	MinFreq (Tone)	MaxFreq (Tone)
Port 1 Port 2 Port 3 Port 4	0	270	490	264	108	64	512

Port	ESEL (dB)	ESCMA	ESCMB	ESCMC	MUS (dBm/Hz)	MinFreq (Tone)	MaxFreq (Tone)
1	0	270	490	264	108	64	512
2	0	270	490	264	108	64	512
3	0	270	490	264	108	64	512
4	0	270	490	264	108	64	512
5	0	270	490	264	108	64	512
6	0	270	490	264	108	64	512
7	0	270	490	264	108	64	512
8	0	270	490	264	108	64	512

Figure 5.6.1 DPBO

ESEL:

E-side Electrical Length (DPBOESEL) This configuration parameter defines the assumed electrical length of cables (E-side cables) connecting exchange based DSL services to a remote flexibility point (cabinet), that may also host remotely located DSL that is subject to spectrally shaped downstream power backoff depending on this length. For this parameter the electrical length is defined as the loss (in dB) of an equivalent length of hypothetical cable at a reference frequency defined by the network operator or in spectrum management regulations. DPBOESEL shall be coded as an unsigned integer representing an electrical length from 0 dB to 255 dB. The corresponding values line length to the damping in dB is about 10 dB per 500 m. If DPBOESEL is zero, the DPBO in this is disabled.

ESCMA / ESCMB/ ESCMC:

E-side Cable Model (DPBOESCM) This configuration parameter defines a cable model in terms of three scalars DPBOESCMA, DPBOESCMB and DPBOESCMC that are used to estimate the frequency dependent loss of E-side cables calculated from the DPBOESEL parameter using the formula: ESCM(f) = (DPBOESCMA + DPBOESCMB*sqrt(f) + DPBOESCMC*f)*DPBOESCL Where ESCM is expressed in dB and f is expressed in MHz. DPBOESCMA, DPBOESCMB, DPBOESCMC shall be coded as unsigned integers representing a scalar value from -1 (coded as 0) to 1.5 (coded as 640) in step of 2^-8. All values are valid.

MUS:

Minimum Usable Signal (DPBOMUS) DPBOMUS defines the assumed Minimum Usable receive Signal PSD (in dBm/Hz) for exchange based services, used to modify parameter DPBOFMAX defined below. It shall be coded as an unsigned integer representing a PSD level from 0 dBm/Hz to -127 dBm/Hz. All values are valid.

MinFreq:

Minimum Frequency (DPBOFMIN) DPBOFMIN defines the starting frequency from which the DPBO shall be applied. It shall be coded as a 16 bits unsigned integer representing a start frequency in multiple of 4.3125 KHz. The range of valid values is from 0 to 2048.

MaxFreq:

Maxmum Frequency (DPBOFMAN) DPBOFMAX defines the maximum frequency at which DPBO may be applied. It shall be coded as a 16 bits unsigned integer representing a start frequency in multiple of 4.3125 KHz. The range of valid values is from 32 to 2048.

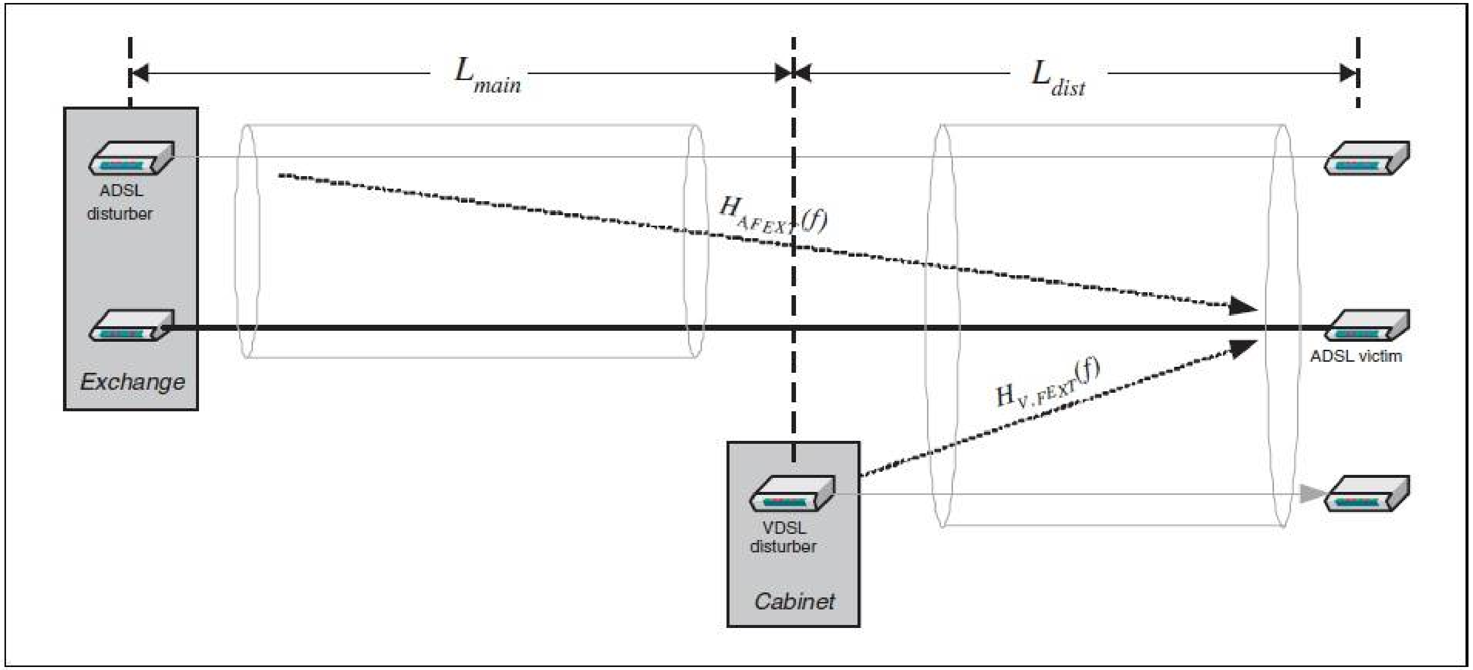


Figure 5.6.2 Basic DPBO Scenario

DPBOESEL is often referred to as E-side electrical length or main-cable electrical length. It is the attenuation in dB at a reference frequency of 1 MHz, of the ADSL cable section between the ADSL CO (exchange) and the VDSL CO (DSLAM). The physical length of this section is denoted **Lmain** in Figure 5.6.2. **DPBOESEL** = 10dB correspond to roughly **Lmain** = 500 m. The correct value of **DPBOESEL** for a particular DSLAM is obtained from a database of the exchange carrier.

The scenario is according to Figure 5.6.2 and Figure 5.6.3. The only 2 parameters which need to be configured are **DPBOESEL** and **DPBOESELMIN**.

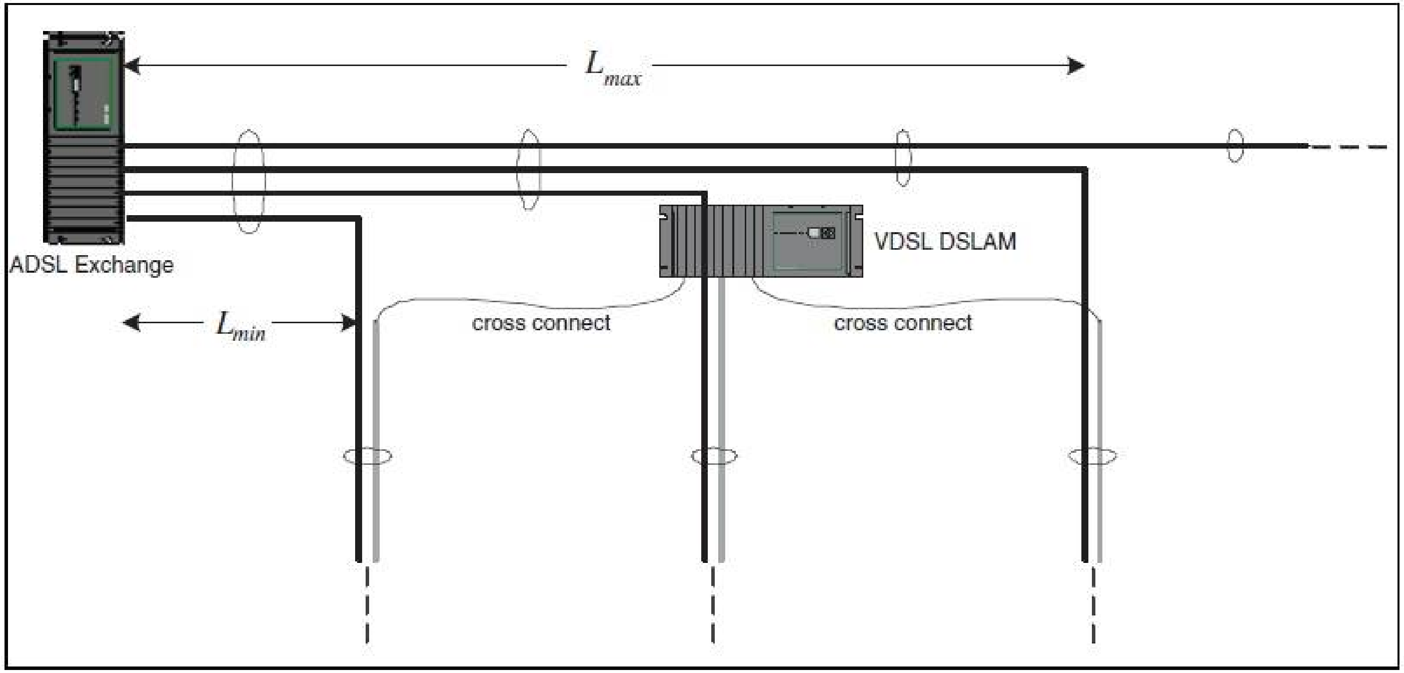


Figure 5.6.3 DPBO Scenario with Cross-connects

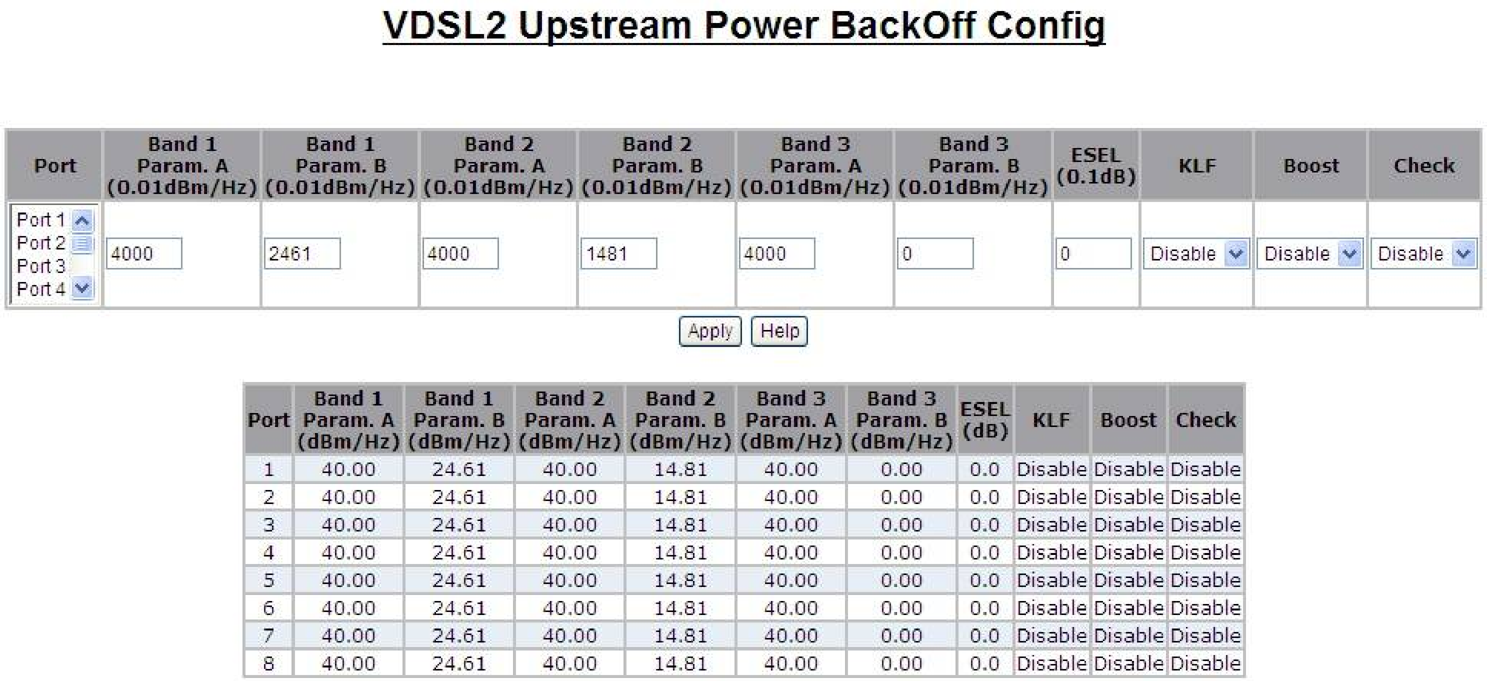
Notes:

1. DPBO is use for ADSL and VDSL mix environment.
2. DPBO explaination: ADSL distance longer length than VDSL2, when the ADSL transmission signal reaches with the same distance with VDSL2, ADSL signal will attenuation, while VDSL2 signal have bigger signal, and it will effect ADSL signal operating. Therefore, please configure DPBO to decrease VDSL2 power to reach reducing the crosstalk purpose.

5.7 UPBO

The page to configure VDSL2 Upstream Power BackOff Config.

This parameter defines the UPBO reference PSD used to compute the upstream power backoff for each upstream band except US0.



VDSL2 Upstream Power BackOff Config

Port	Band 1 Param. A (0.01dBm/Hz)	Band 1 Param. B (0.01dBm/Hz)	Band 2 Param. A (0.01dBm/Hz)	Band 2 Param. B (0.01dBm/Hz)	Band 3 Param. A (0.01dBm/Hz)	Band 3 Param. B (0.01dBm/Hz)	ESEL (0.1dB)	KLF	Boost	Check
Port 1 Port 2 Port 3 Port 4	4000	2461	4000	1481	4000	0	0	Disable	Disable	Disable

Port	Band 1 Param. A (dBm/Hz)	Band 1 Param. B (dBm/Hz)	Band 2 Param. A (dBm/Hz)	Band 2 Param. B (dBm/Hz)	Band 3 Param. A (dBm/Hz)	Band 3 Param. B (dBm/Hz)	ESEL (dB)	KLF	Boost	Check
1	40.00	24.61	40.00	14.81	40.00	0.00	0.0	Disable	Disable	Disable
2	40.00	24.61	40.00	14.81	40.00	0.00	0.0	Disable	Disable	Disable
3	40.00	24.61	40.00	14.81	40.00	0.00	0.0	Disable	Disable	Disable
4	40.00	24.61	40.00	14.81	40.00	0.00	0.0	Disable	Disable	Disable
5	40.00	24.61	40.00	14.81	40.00	0.00	0.0	Disable	Disable	Disable
6	40.00	24.61	40.00	14.81	40.00	0.00	0.0	Disable	Disable	Disable
7	40.00	24.61	40.00	14.81	40.00	0.00	0.0	Disable	Disable	Disable
8	40.00	24.61	40.00	14.81	40.00	0.00	0.0	Disable	Disable	Disable

Figure 5.7.1 UPBO

Param.A/Param.B:

A UPBOPSD defined for each band shall consist of two parameters [a, b]. Parameter A ranges from 40.0 dBm/Hz to 80.95 dBm/Hz in steps of 0.01 dBm/Hz; and parameter B ranges from 0 to 40.95 dBm/Hz in steps of 0.01 dBm/Hz.

ESEL:

This parameter defines the electrical loop length expressed in dB at 1MHz, kl0, configured by the CO-MIB. The value shall be coded as an unsigned 16 bit number in the range 0 (coded as 0) to 128 dB (coded as 1280) in steps of 0.1 dB. The corresponding values line length to the damping in dB is about 10 dB per 500 m.

KLF:

This parameter is a flag that forces the VDSL2 CPE to use the electrical length of the ESEL to compute the UPBO. The value shall be forced if the flag is set to 1. Otherwise, the VDSL2 Units shall determine the electrical length.

Boost:

Enable Boost Mode (not part of G.997.1). If disabled, the UPBO standard mode is used with the LOSS function calculated according to 7.3.1.2.14 of G.997.1 Rev4: LOSS(kl0,f) = kl0*sqrt(f) If enabled, the LOSS function is calculated differently as LOSS(kl0,f) = kl0*sqrt(f) - 10*log10(kl0)

Check:

Enable check for UPBO support of the CPE (not part of G.997.1). Enables/Disables at the VTU_O a verification of the UPBO PSD received from the VTU_R to check if the VTU_R applies UPBO in the correct way. If not, no link is established and a corresponding failure code is reported to the host.

Notes :

1. After any change to VDSL2 settings, must be deactivated then activated once or reboot.
2. UPBO suitable to use for a lot of VDSL2 applications simultaneously occasions.

The scenario is according to **Figure 5.7.2** This text describes the use of the G.997 parameter UPBOPSD-pb, only. This parameter is comprised of the UPBO coefficients A and B defined for each upstream band, separately, which depend on both the cable model and the PSD mask.The other UPBO parameters are usually not configured.

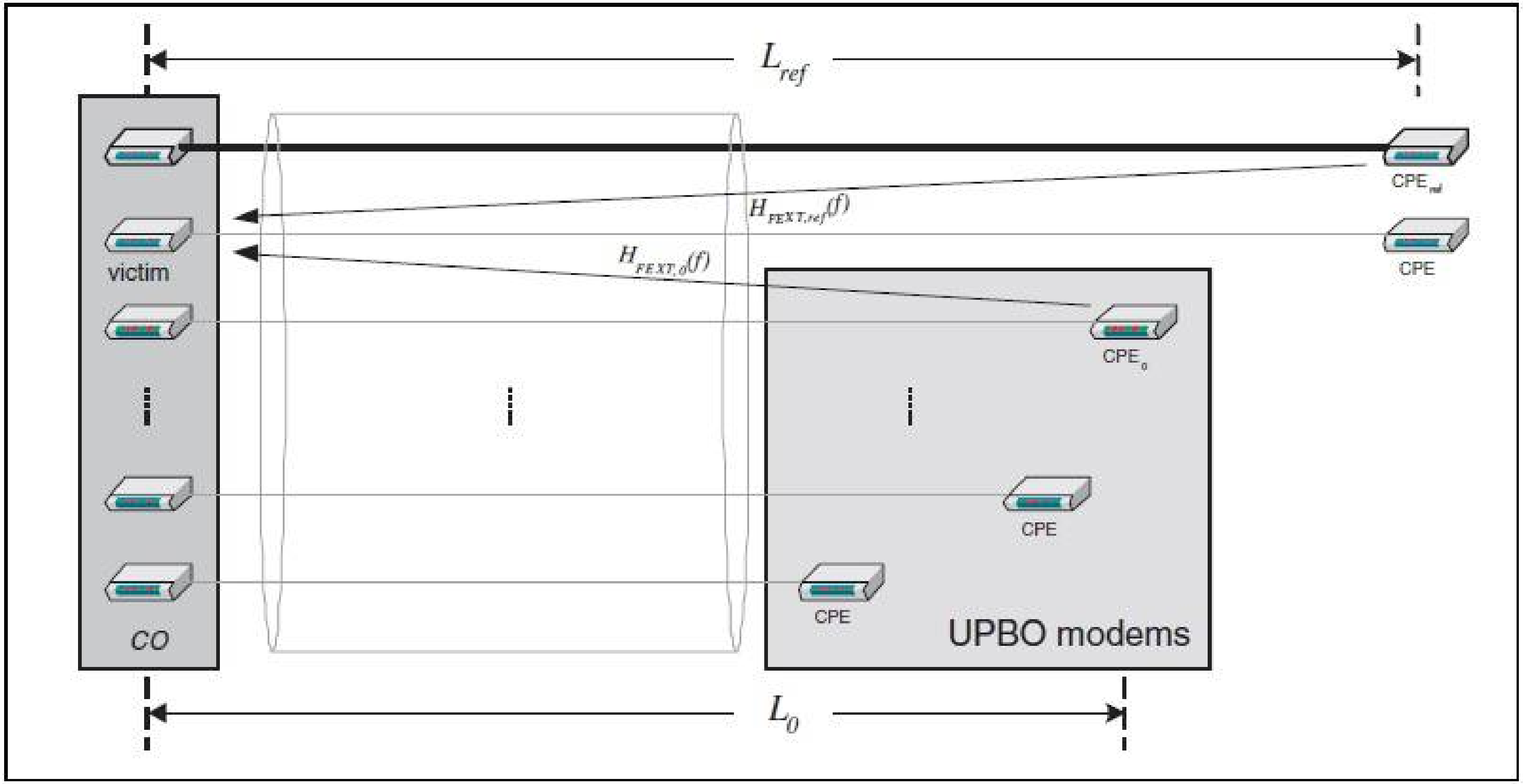
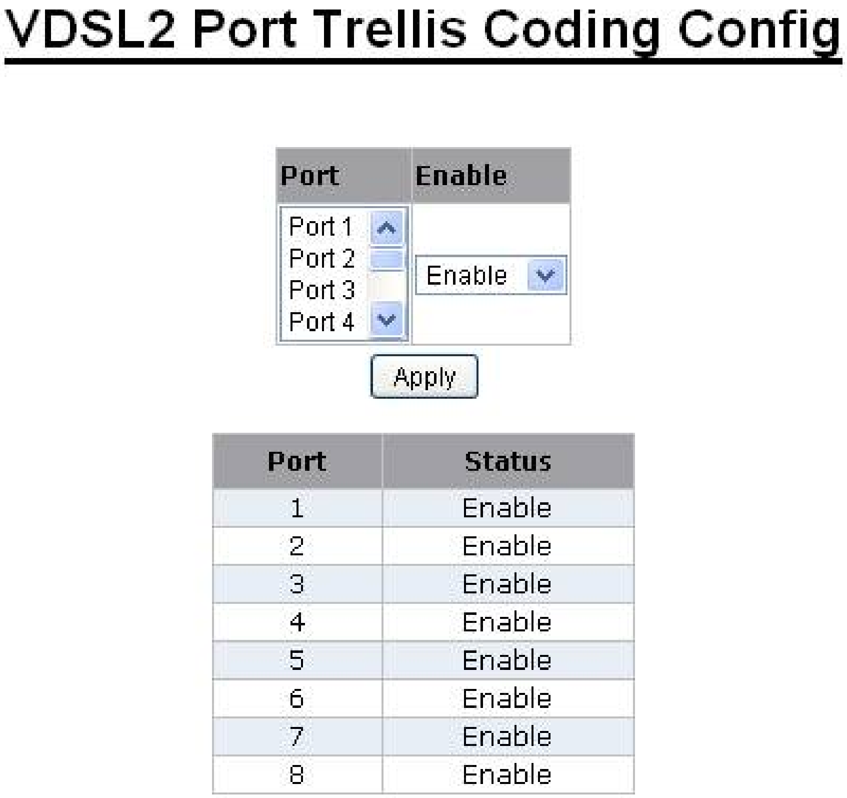


Figure 5.7.2 Basic UPBO Scenario

5.8 Trellis Config

The page to configure VDSL2 Port Trellis Coding Config.



VDSL2 Port Trellis Coding Config

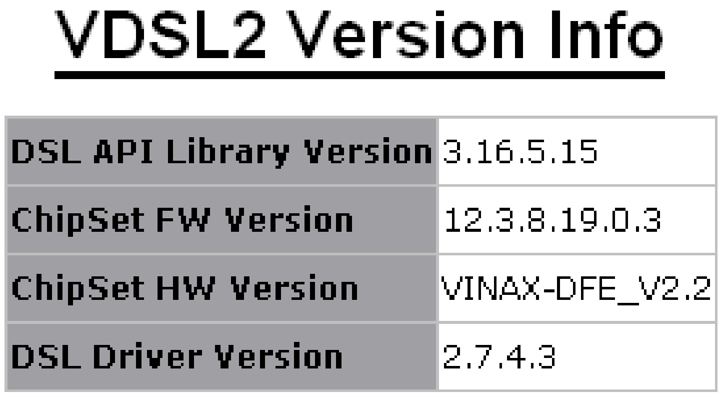
Port	Enable
Port 1 Port 2 Port 3 Port 4	Enable

Port	Status
1	Enable
2	Enable
3	Enable
4	Enable
5	Enable
6	Enable
7	Enable
8	Enable

Figure 5.8 Trellis Config

5.9 VDSL2 Version Info

The page show VDSL2 hardware firmware version.



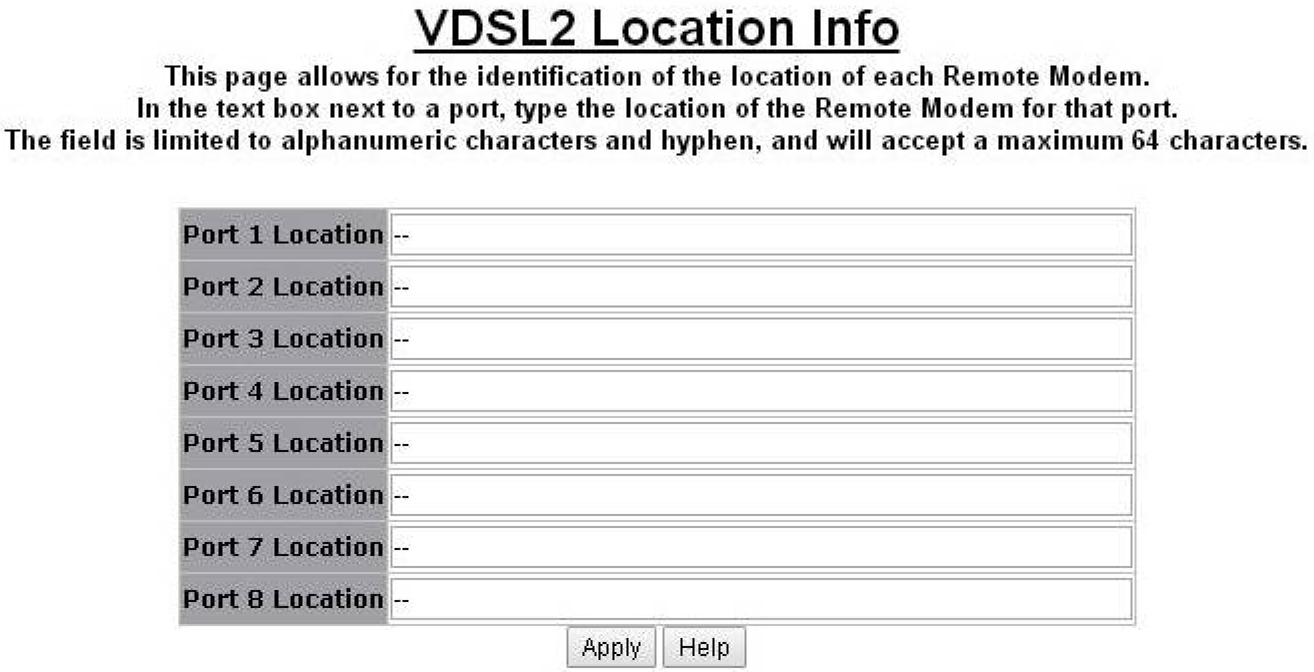
VDSL2 Version Info

DSL API Library Version	3.16.5.15
ChipSet FW Version	12.3.8.19.0.3
ChipSet HW Version	VINAX-DFE_V2.2
DSL Driver Version	2.7.4.3

Figure 5.9.1 Version Info.

5.10 VDSL2 Location Info

The page show VDSL2 port location information.



VDSL2 Location Info

This page allows for the identification of the location of each Remote Modem.
In the text box next to a port, type the location of the Remote Modem for that port.
The field is limited to alphanumeric characters and hyphen, and will accept a maximum 64 characters.

Port 1 Location	--
Port 2 Location	--
Port 3 Location	--
Port 4 Location	--
Port 5 Location	--
Port 6 Location	--
Port 7 Location	--
Port 8 Location	--

Chapter 6. Applications

The Switch provides segmented network architecture. When a port is connected to an end-node, or to a device that breaks up the collision domain (e.g., another switch, bridge or router), the attached device has access to the full bandwidth provided by that port.

Bridging Functions – The Switch provides fully transparent bridging functions which automatically learn node addresses, which are subsequently used to filter and forward all traffic based on the destination address. When traffic passes between devices attached to the same shared collision domain, those packets are filtered from the switch. But when traffic must be passed between unique segments (i.e., different ports on the switch), a temporary link is set up between the switch ports which need to pass this traffic, via the high-speed switching fabric.

Flexible Configuration–This Switch is not only designed to segment your network, but also to provide a wide range of options in setting up network connections. It can be used as a simple stand-alone switch; or can be connected with standard hub, switches, or other network interconnection devices in various configurations. Some of the common applications for the Switch are described in this chapter.

Switch Used as Collapsed Backbone for Starter Network

This Switch is an excellent choice for new Ethernet installations where significant growth is expected in the near future. You can easily build on this basic configuration, adding direct full-duplex connections to workstations or servers (i.e., up to 20 Mbps or even 200 Mbps of dedicated bandwidth per node).Then, when the time comes for further expansion, just daisy-chain any IEEE 802.3 or IEEE 802.3u compliant switch or hub. This Switch can also be easily integrated with upper-level protocol devices you later add into the network.

Last Mile of FTTx Deployment

The VDSL2 IP DSLAM is an ideal solution for FTTx (FTTB / FTTH, etc.) applications. It support high bandwidth over existing telephone wires in the "last mile" from the ISP / Telecom / Service Provider's fiber node to the buildings and customers' houses. The Intelligent VDSL2 IP DSLAM provides a high speed, 100Mbps transmission over phone wiring over a single Internet account to provide simultaneous independent Internet access to multiple users. It is excellent for phone line network built under internet because the whole building could share the internet to the wider area network with minimum cost and get max efficiency.

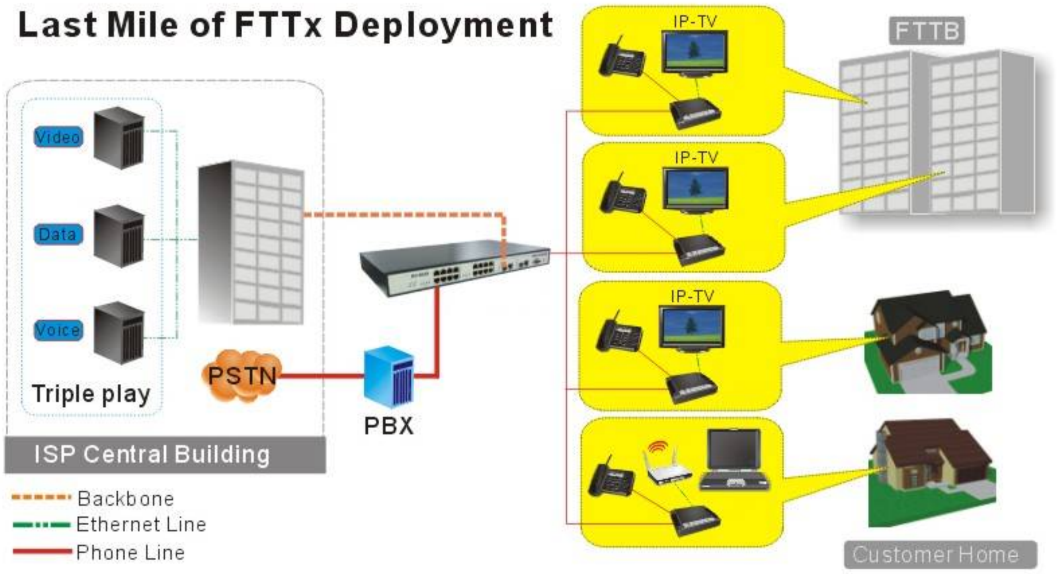


Figure 6.1 VDSL2 application diagram

Application for Sharing a single internet account

If multiple users would like to share a single internet account using the switch, which is to be connected to a IP sharing device, then to a xDSL or Cable Modem.

Note:

For network applications that actually require Router (e.g., Interconnecting dissimilar network types), attaching the SWITCH directly to a router can significantly improve overall home networking performance.

High bandwidth backbone ready

The VDSL2 IP DSLAM provides 10/100/1000Mbps auto sensing for external trunk device (Fiber optics, Wireless Bridge, xDSL & other WAN services).

Appendix A: Troubleshooting

Diagnosing IP DSLAM Indicators

The Switch can be easily monitored through its comprehensive panel indicators. These indicators assist the network manager in identifying problems the Switch may encounter. This section describes common problems you may encounter and possible solutions

1. Symptom:	**POWER indicator does not light up (green) after power on.**
Cause:	Defective power outlet, power cord, internal power supply
Solution:	Cheek the power outlet by plugging in another that is functioning properly. Check the power cord with another device. If these measures fail to resolve the problem, have the unit power supply replaced by an qualified distributor.

2. Symptom:	**Link indicator does not light up (green) after making a connection.**
Cause:	Network interface (e.q., a network adapter card on the attached device), network cable, or switch port is defective.
Solution:	2.1 Verify if both of the switch and attached device are powered on. 2.2 Be sure the cable is plugged into both the switch and corresponding device. 2.3 Verify that the proper cable type is used and its length does not exceed specified limits. 2.4 Check the adapter on the attached device and cable connections for possible defects. 2.5 Replace the defective adapter or cable if necessary.

3. Symptom:	**Upstream bandwidth control failed.**
Cause:	NIC(Networking Interface Card) does not have flow control function.
Solution:	Be sure the NIC(**Networking Interface Card**) supports flow control function.

4. Question:	**The customer reported that bandwidth control did not work in either direction when the port was set to 1 on the ingress and 1 on the Down(egress). One of our new HP laptops should bandwidth control at around 125K on the download, but around 1.7Mbps on the upload. On my laptop, it was around 100K on the download and 225K on the upload. Is there a reason why we are seeing such varied results and has there been any other reported problem with this feature lately?**
Answer:	Regarding our VDSL2 IP DSLAM' principle of bandwidth control, which must rely on flow control to limit bandwidth over hardware, as long as client side doesn't support flow control, the upstream bandwidth control is invalid, so for this case, client side must support flow control function.

5. Question:	**Why VDSL2 configure change invalid ?**
Answer:	After any change to VDSL2 configure. Line must be deactivated then activated once or reboot, then new configure will be valid.

6. Question:	**Is that possible to use ADSL2+ modems with with the VDSL2 IP DSLAM ?**
Answer:	Please Note that it is not possible to use ADSL2+ modems with the VDSL2 IP DSLAM, since ADSL2+ is based on ATM frame and our VDSL2 IP DSLAM is based on EFM frame. Two frames are not compatible.

7. Question:	**Sometimes the CPE lose the connection to DSLAM.**
Cause:	Due to heavy noise of field environment or phone wiring does not meet specifications.
Solution:	1. We strong recommend all VDSL2 ports must use **24** gauge with twisted pair phone wiring. 2. Please replace the head of RJ11 wiring, if it has been oxidized or damaged. 3. Using phone cable must be stretched straight, without using reel phone cable, this will cause heavy crosstalk noise. 4. If port link problem, please change band profile to long reach mode as 12a or 8d AnnexB.

8. Question:	**Sometimes the IP DSLAM unstable.**
Cause:	Due to heavy noise or impulse noise of field environment caused unstable.
Solution:	1. If VDSL2 IP DSLAM hangs up, please enable broadcast strom function, and configure to value 1/4 or higher. please refer to section 4.2.1.2. 2. If CPE happened sync issue, please configure interleave delay time to anti-noise, please refer to section 5.2 3. Enable INP(impulse noise protection) to 8 or above and enable "Force INP" for preventing impulse noise.
Notes:	1. Please note that enable interleave delay function will reduce a few vdsl2 bandwidth. 2. Interleave delay value must greater than or equal to INP value, otherwise VDSL2 will not establish a connection. 3. Please note you must deactivate then activate once on config port when you configure INP and interleave dalay value.

9. Question:	What is an acceptable SNR for VDSL2?
Answer	Higher SNR numbers represent cleaner signals with less noise. In some instances interleaving can help raise the noise margin to an acceptable level. < 6dB: An SNR of less than 6 dB usually will result in line issues. 7dB - 10dB: This is a decent SNR but doesn't leave much room for variances in line conditions. 11dB - 20dB: Most people who live within a short amount of distance from the VRAD (less than 1500 feet) will have an SNR within that range. This will result in little to no sync problems. 20dB - 28dB: Outstanding SNR, you must have the VRAD as your next door neighbor.

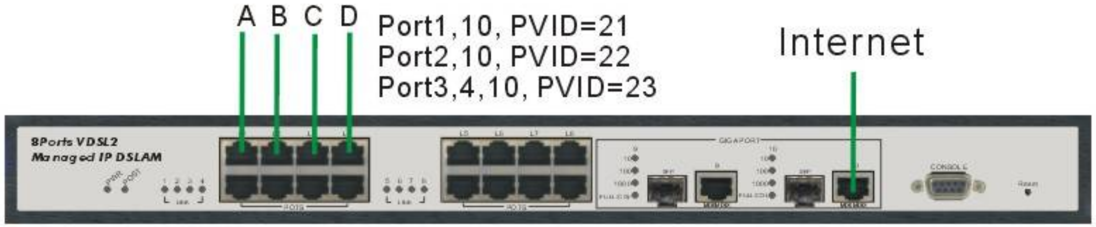
10. Question:	I would like to fully understand the limitations of the low pass filter in the IP DSLAM (0-125Khz). Can you please cover this in more detail as I do not want this to affect these potential projects.
Answer	IP DSLAM working frequency is from 138khz - 30Mhz, and POTS ports build in a low pass splitter(0 -125khz), we found many kinds of PBX spectrum in hotel system, every hotel's PBX working spectrum was different, if hotel PBX spectrum is low than IP DSLAM POTS port, it means hotel's PBX spectrum doesn't conflict with IP DSLAM, but it is impossible. According with our experience that almost of Hotel PBX spectrum is high than POTS splitter, so only one method can do it, you can try parallel connect line port without through POTS port, for this method that PBX spectrum must not overlap IP DSLAM working spectrum, and please note you have to check hotel PBX system in advance when you will install a hotel.

Appendix B: Example of VLAN Setting

Example 1:

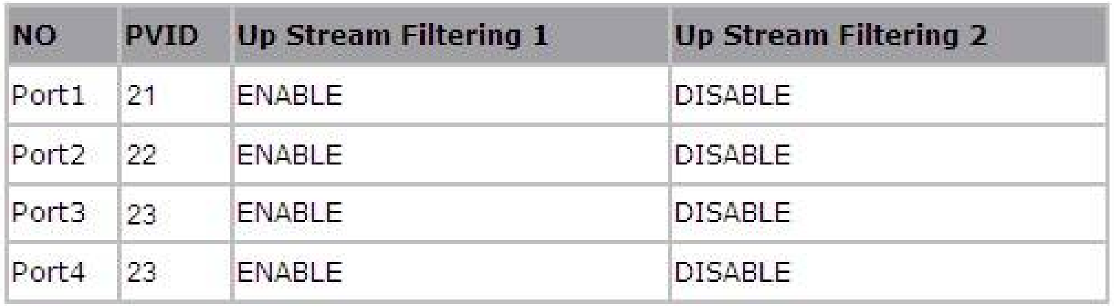
4 users join to Internet by VDSL system like following drawing, and have 7 demands.

1. User A connects to port 1 and join to Internet through port 10.
2. User B connects to port 2 and join to Internet through port 10.
3. User C connects to port 3 and join to Internet through port 10.
4. User D connects to port 4 and join to Internet through port 10.
5. User A isolate with Users B, C and D.
6. User B isolate with Users A, C and D.
7. User C and D in the same Group and isolate with Users A and B.



Setup Procedure:

Setup Port VID: Assign a Port VLAN ID (1~4094) for untagged traffic on each port like following: Port 1 PVID=21, Port 2 PVID=22, Port 3, 4 PVID=23



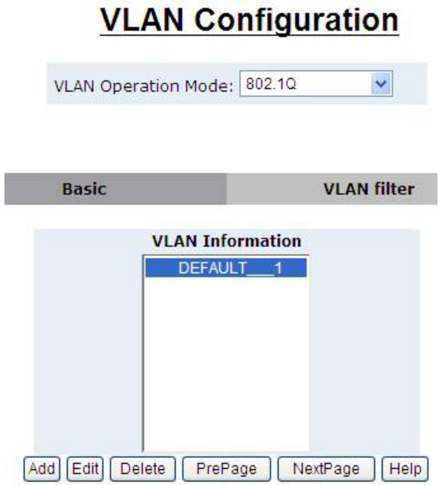
NO	PVID	Up Stream Filtering 1	Up Stream Filtering 2
Port1	21	ENABLE	DISABLE
Port2	22	ENABLE	DISABLE
Port3	23	ENABLE	DISABLE
Port4	23	ENABLE	DISABLE

VLAN Filters

Add VLAN Group:

There are 256 VLAN groups available for configuration. Add a VLAN Group VID=21 member ports = port 1 & port 10

Note: Do not change the default_1 group.



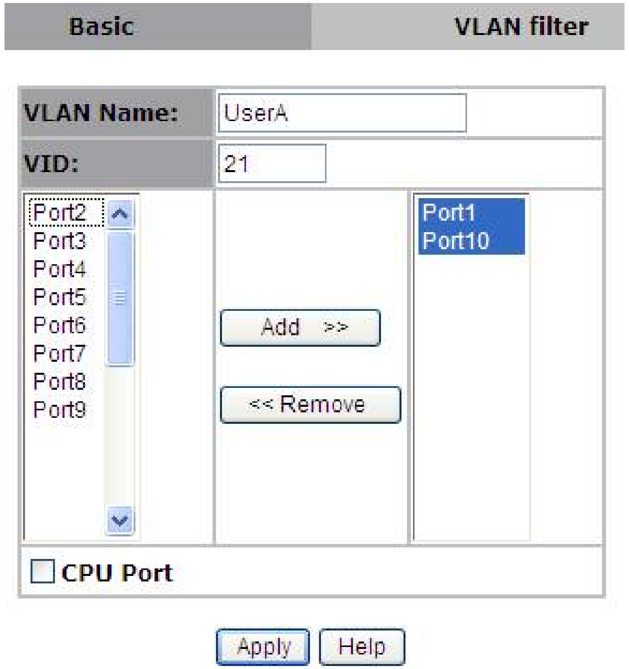
VLAN Configuration

VLAN Operation Mode: 802.1Q

VLAN Information

DEFAULT__1

Setup VLAN Name=UserA, VID=21, select member ports 1 & 10.



VLAN Name: UserA

VID: 21

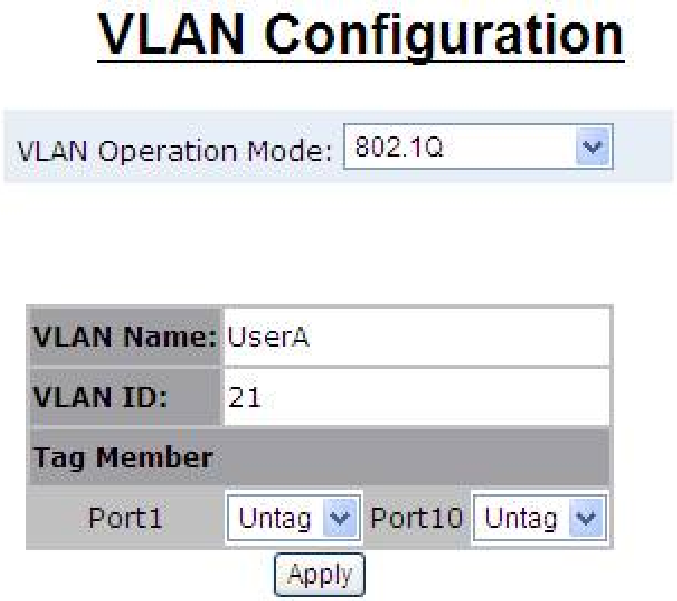
Port1
Port10

□ CPU Port

Note:

If Vlan group include cpu port. The member of this group can management this vdsl2 Ipdslam.

Select Untag or Tag Setup. Unless the device (computer or switch) which connect to port 1 or port 10 can support Tagging VLAN, otherwise select Untag.



VLAN Configuration

VLAN Operation Mode: 802.1Q

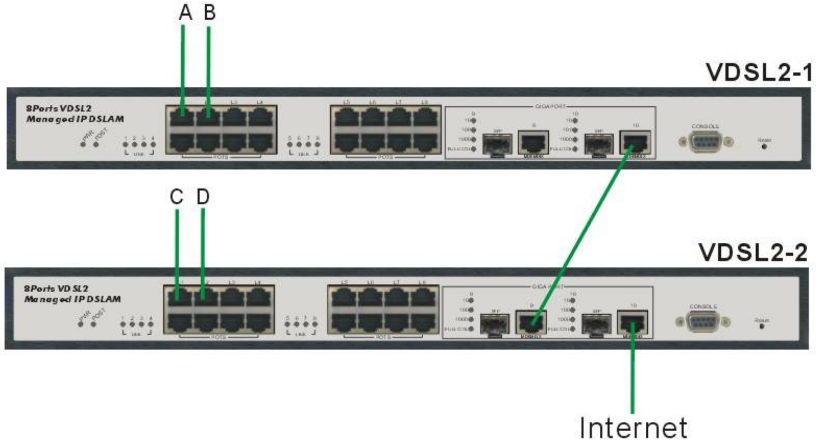
VLAN Name:	UserA
VLAN ID:	21
Tag Member	
Port1	Untag
Port10	Untag

Add a VLAN Group Name=UserB, VID=22, member ports = port 2 & port 10 with Untag.
Add a VLAN Group Name=UserCD, VID=23, member ports = port 3, port 4 & port 10 with Untag.

Example 2:

4 users join to Internet through 2 IP DSLAMs like the following drawing, and have 7 demands.

1. User A connect to port 1 of VDSL2-1 and join to Internet through port 10 of VDSL2-2.
2. User B connect to port 2 of VDSL2-1 and join to Internet through port 10 of VDSL2-2.
3. User C connect to port 1 of VDSL2-2 and join to Internet through port 10 of VDSL2-2.
4. User D connect to port 2 of VDSL2-2 and join to Internet through port 10 of VDSL2-2.
5. User A isolate with Users B, C and D.
6. User C isolate with Users A, B and D.
7. User B and D in the same Group and isolate with Users A and B.



Setup Procedure:

VDSL2-1 Setup:

a. Setup Port VID: Port 1 PVID=11, Port 2 PVID=12

b. Add VLAN Group:

Note: Do not change the default_1 group.

Add a VLAN Group, Group name=UserA VID=11 member ports = port 1 & port 26

Select Untag or Tag Setup for VID=11 group:

Port Number	Untag/Tag Select
1	Untag
10	Tag

Add a VLAN Group, Group name=UserBD VID=12, member ports = port 2 & port 26

Select Untag or Tag Setup for VID=12 group:

Port Number	Untag/Tag Select
2	Untag
10	Tag

VDSL2-2 Setup:

a. Setup Port VID: Port 1 PVID=21, Port 2 PVID=12

b. Add VLAN Group:

Do not change the default_1 group.

Add a VLAN Group, Group name=UserA VID=11 member ports = port 9 & port 10

Select Untag or Tag Setup for VID=11 group:

Port Number	Untag/Tag Select
9	Tag
10	Untag

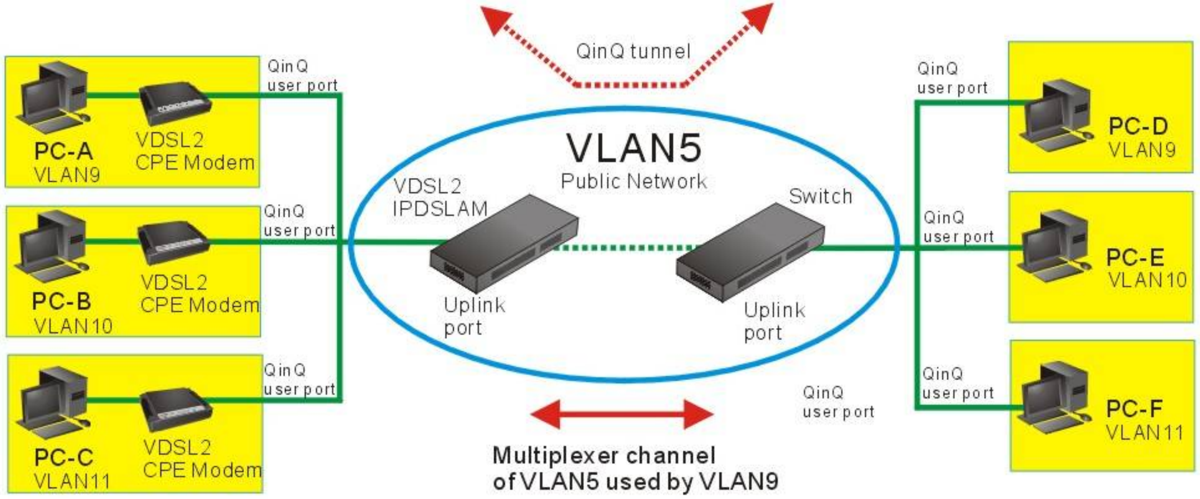
Add a VLAN Group, Group name=UserBD VID=12 member ports = port 2 & port 25 & port 26 Select Untag or Tag Setup for VID=12 group:

Port Number	Untag/Tag Select
1	Untag
2	Untag
9	Tag
10	Untag

Example 3:

6 x PC join to Internet through VDSL2 IP DSLAM like the following drawing, and have 8 demands.

1. PC-A connect to port 1 of VDSL2 and join to Internet through port 9 of VDSL2
2. PC-B connect to port 2 of VDSL2 and join to Internet through port 9 of VDSL2
3. PC-C connect to port 3 of VDSL2 and join to Internet through port 9 of VDSL2
4. PC-D connect to port 1 of Switch and join to Internet through port 25 of Switch.
5. PC-E connect to port 2 of Switch and join to Internet through port 25 of Switch.
6. PC-F connect to port 3 of Switch and join to Internet through port 25 of Switch.
7. VDSL2 and Switch join a vlan group and VID set 5.
8. PC-A, -B, -C and PC-D, -E, -F join a vlan group and VID set 9,10,11, QinQ tunnel using VLAN5 wants to be created for VLAN9,10,11 across the public network.

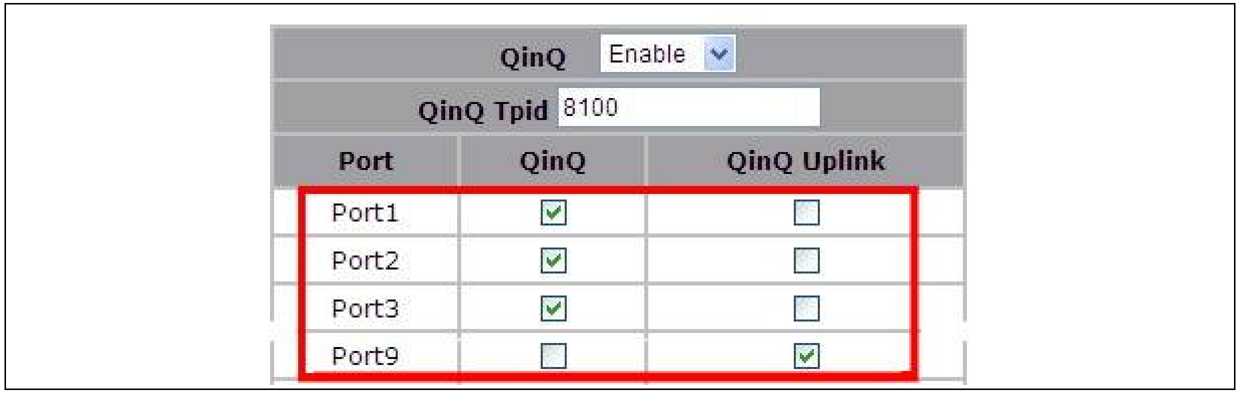


Setup Procedure:

1. Enable 802.1Q VLAN and remove port1,2,3 for 802.1Q VLAN from default group.
2. A QinQ tunnel using VLAN5 wants to be created for VLAN9 across the public network.
3. Port 1,2,3 on left-side of the VDSL2 IP DSLAM connects to VLAN9 client. Port 9 of the VDSL2 IP DSLAM connects to public network.
4. Add six VLAN Groups as follow form.

VDSL2 VLAN Group	Switch VLAN Group	VLAN VID	Untag/Tag Select
1,9	1,25	9	Port1/2/3 Untag Port9/25 Tag
2,9	2,25	10	
3,9	3,25	11	

1. VDSL2 IP DSLAM port9 connects to Switch Port 25.

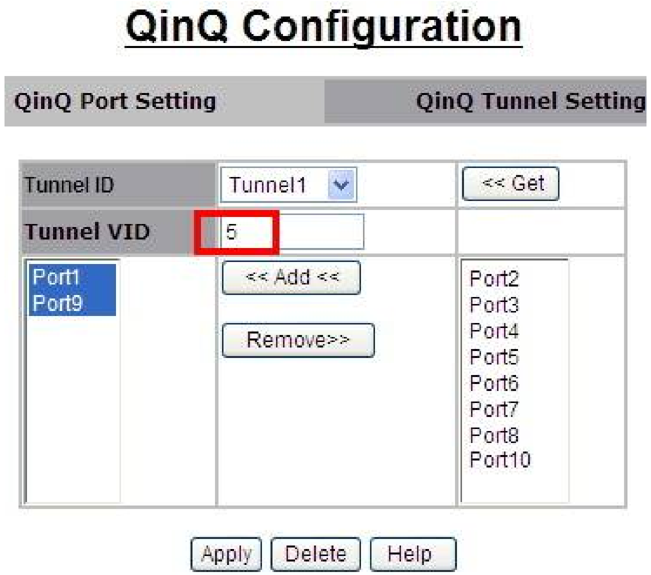


QinQ: Enable

QinQ Tpid: 8100

Port	QinQ	QinQ Uplink
Port1	☑	□
Port2	☑	□
Port3	☑	□
Port9	□	☑

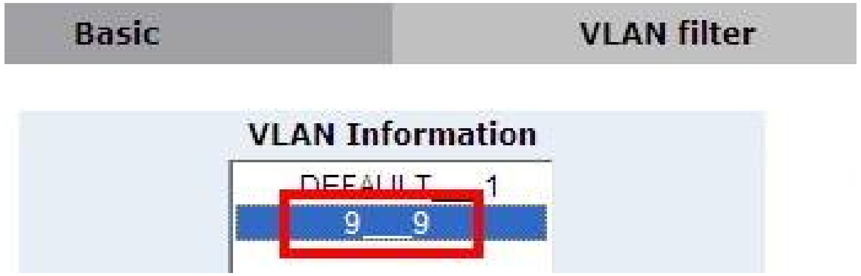
1. QinQ Tpid: 8100(default).
2. VDSL2 QinQ Userport: Port1, 2, 3. QinQ uplink port Port9.
3. Switch QinQ Userport: Port1, 2, 3. QinQ uplink port :Port25.



QinQ Configuration

Tunnel ID	Tunnel1	
Tunnel VID	5	
Port1 Port9		Port2 Port3 Port4 Port5 Port6 Port7 Port8 Port10

1. Set tunnel1 VID5 within port1,9 for VDSL2 and Switch set tunnel1 VID5 within port1,25.
2. Set tunnel2 VID5 within port2,9 for VDSL2 and Switch set tunnel2 VID5 within port2,25.
3. Set tunnel3 VID5 within port3,9 for VDSL2 and Switch set tunnel3 VID5 within port3,25.



1. Set port 1,9 / 2,9 / 3,9 in the group within the VLAN VID9,10,11 for VDSL2.

2. Set port 1,25 / 2,25 / 3,25 in the group within the VLAN VID9,10,11 for Switch.

Appendix C: Cable Requirements

A CAT 3, 4 or 5 UTP (unshielded twisted pair) cable is typically used to connect the Ethernet device to the modem. A 10Base-T cable often consists of four pairs of wires, two of which are used for transmission. The connector at the end of the 10Base-T cable is referred to as an RJ-45 connector and it consists of eight pins. The Ethernet standard uses pins 1, 2, 3 and 6 for data transmission purposes. (Table C-1)

Table C-1 RJ-45 Ethernet Connector Pin Assignments

PIN #	MDI		MDI-X	
	Signal	Media Dependant interface	Signal	Media Dependant interface-cross
1	TX+	Transmit Data +	RX+	Receive Data +
2	TX-	Transmit Data -	RX-	Receive Data -
3	RX+	Receive Data +	TX+	Transmit Data +
4	--	Unused	--	Unused
5	--	Unused	--	Unused
6	RX-	Receive Data -	TX-	Transmit Data -
7	--	Unused	--	Unused
8	--	Unused	--	Unused

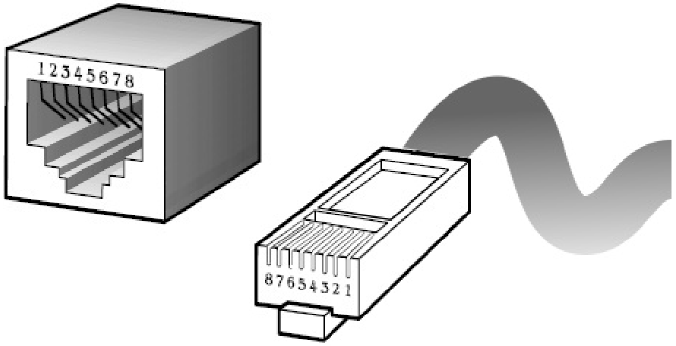


Figure C-1 Standard RJ-45 repectacle/connector

Note:

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

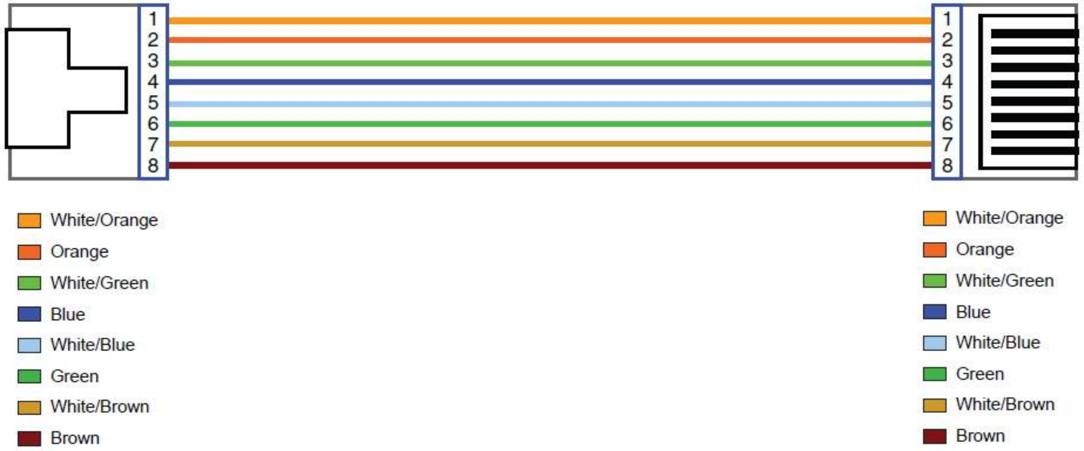


Figure C-2 Pin Assignments and Wiring for an RJ-45 Straight-Through Cable

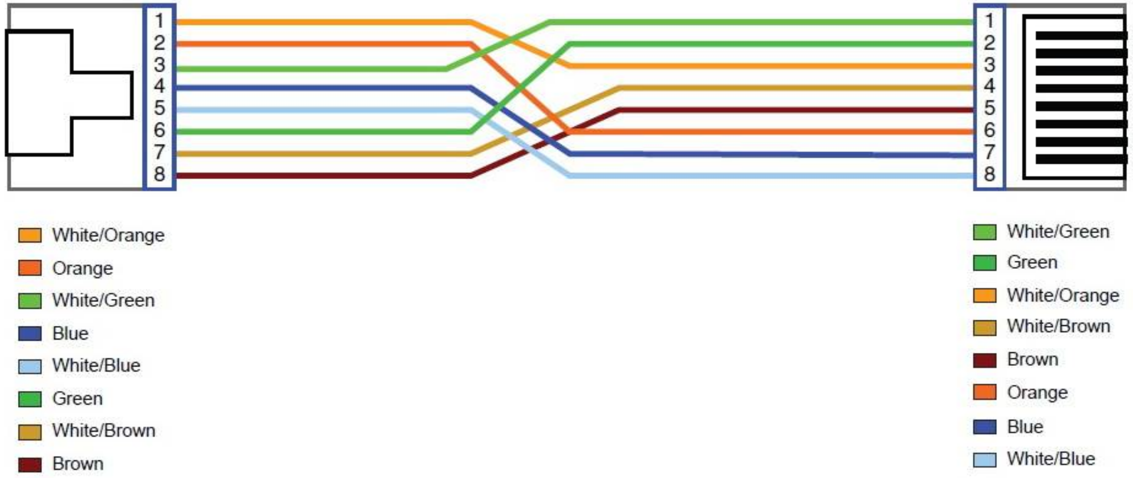


Figure C-3 Pin Assignments and Wiring for an RJ-45 Crossover Cable

Serial Console Interface Connector Pin Assignments

The serial console interface connector is a 9-pin, RS-232 D-type, DTE connector. A null modem cable is required to connect a workstation running the Linux or Windows operating system. Table C-2 lists the pin assignments for the serial console interface connector.

Table C-2 RS-232 Connector Pin Assignments

Description	Pin	I/O	Signal Name
Not used	1	-	-
Receive data; input	2	In	RXD
Transmit data; output	3	Out	TXD
Data terminal ready; output	4	Out	DTR
Interface signal ground	5	-	GND
Data set ready; input	6	In	DSR
Not used	7	-	-
Not used	8	-	-
Not used	9	-	-

The CDEs have one standard serial port connector located on the back of the device. Figure C-4 shows the pin number assignments for the 9-pin, male D-shell serial port connector on the back of the device. These pin number assignments conform to the industry standard for RS-232 communications.

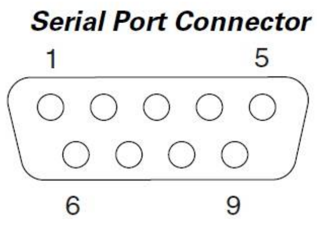


Figure C-4

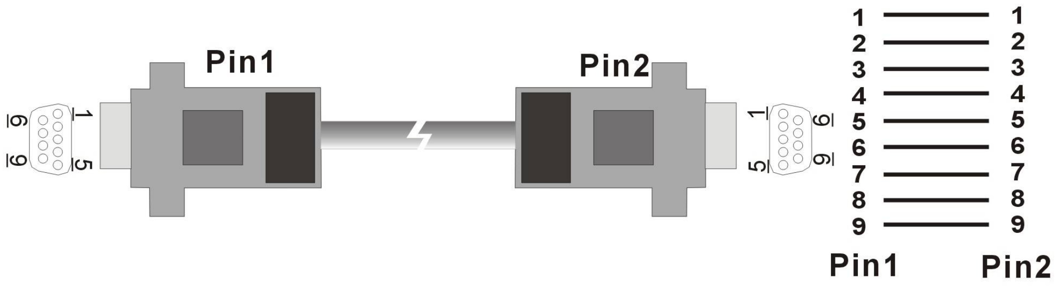


Figure C-5 Pin Assignments and Wiring for an RS-232 Cable

Appendix D: Compliance and Safety Information

System Diagnosis

Power and Cooling Problems

If the POWER indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or internal power supply as explained in the previous section. However, if the unit should turn itself off after running for a while, check for loose power connections, power losses or surges at the power outlet, and verify that the fan on back of the unit is unobstructed and running prior to shutdown. If you still cannot isolate the problem, then the internal power supply may be defective. In this case, contact your supplier for assistance.

Installation

Verify that all system components have been properly installed. If one or more components appear to be malfunctioning (e.g., the power cord or network cabling), test them in an alternate environment where you are sure that all the other components are functioning properly.

Transmission Mode

The default methods of selecting the transmission mode for all RJ-45 ports are auto-negotiation. Therefore, if the Link signal is disrupted (e.g., by unplugging the network cable and plugging it back in again, or by resetting the power), the port will try to reestablish communications with the attached device via auto-negotiation. If auto-negotiation fails, then communications are set to half duplex by default. Based on this type of industry-standard connection policy, if you are using a full-duplex device that does not support auto-negotiation, communications can be easily lost (i.e., reset to the wrong mode) whenever the attached device is reset or experiences a power fluctuation. The best way to resolve this problem is to upgrade these devices to versions which support auto-negotiation.

Cabling

1. Verify that the cable type is correct. Be sure RJ-45 cable connectors are securely seated in the required ports. Use 100Ω straight-through cables for all standard connections. Use Category 5 cable for 100Mbps Fast Ethernet connections, or Category 3, 4 or 5 cables for standard 10Mbps Ethernet connections.
2. Make sure all devices are connected to the network. Equipment any have been unintentionally disconnected from the network.
3. When cascading two devices using RJ-45 station ports at both ends of the cable (i.e., an Auto-MDIX port), if supports a auto-MDIX used, crossover cable is not need.

External Adapters

Make sure the network interface hardware and software drivers for the attached devices are functioning properly. Check the adapter cards and associated drivers used in any attached workstation or server.

Physical Configuration

If problems occur after altering the network configuration, restore the original connections, and try to track the problem down by implementing the new changes, one step at a time. Ensure that cable distances and other physical aspects of the installation do not exceed recommendations

System Integrity

As a last resort verify the switch integrity with a power-on reset. Turn the power to the switch off and then on several times. If the problem still persists and you have completed all the preceding diagnoses, contact your dealer for assistance.

Installation

No need for driver(Plug & Play).

Use a computer (notebook) to do the installation.

Connect with the RS232 port of the switch with the notebook.

Remote Network Control by Web.

FCC Mark Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

This is a CE class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

WEEE Warning

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

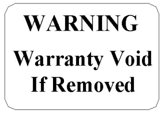
Warranty

The original owner that the product delivered in this package will be free from defects in material and workmanship for one year parts after purchase.

There will be a minimal charge to replace consumable components, such as fuses, power transformers, and mechanical cooling devices. The warranty will not apply to any products which have been subjected to any misuse, neglect or accidental damage, or which contain defects which are in any way attributable to improper installation or to alteration or repairs made or performed by any person not under control of the original owner.

The above warranty is in lieu of any other warranty, whether express, implied, or statutory, including but not limited to any warranty of merchantability, fitness for a particular purpose, or any warranty arising out of any proposal, specification, or sample. Shall not be liable for incidental or consequential damages. We neither assumes nor authorizes any person to assume for it any other liability.

Note: Please do not tear off or remove the warranty sticker as shown, otherwise the warranty will be void.



WARNING
Warranty Void
If Removed