netsys

Networking your world

NVF-2400S

4 Band VDSL 24 Ports Managed IP DSLAM with 2 Giga Ethernet

USER'S MANUAL

Http://www.netsys.com.tw

Copyright

Trademarks

NETSYS is a trademark of National Enhance Technology Corp.
Other brand and product names are registered trademarks or trademarks of their respective holders.

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, National Enhance Technology Corp. hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETSYS reserves the right to make changes to the products described in this document without notice. NETSYS does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Maximum signal rate derived form IEEE Standard specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate. Netsys does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Make sure you follow in line with the environmental conditions to use this product.

Foreword:VDSL Solution

The VDSL networking solution delivers Cost-effective, high-performance broadband access to multi-unit buildings (hotels, apartments, and multi-tenant unit office buildings) and enterprise campus environments such as manufactories, educational campuses, and medical facilities. VDSL technology dramatically extends Ethernet over existing Category 1/2/3 wiring at data speed of 5/15/25 Mbps (full duplex) and distances up to 1700/1100/600 meters. The VDSL technology delivers broadband service on the same lines as Plain Old Telephone Service (POTS), digital telephone, and ISDN system. In addition, VDSL supports modes compatible with symmetric digital subscriber line, allowing service providers to provision VDSL to buildings where broadband services already exist.

The VDSL solution includes (NVF-2400S), and VDSL Bridge for Customer Premise Equipment (CPE) device.

The VDSL solution delivers everything needed to quickly deploy an Ethernet-based network with the performance required to deliver high-speed Internet access at much greater distances and drive services like IP telephony and audio/video streaming. With this technology, a broad range of customers can benefit from lower operating Costs and rapid deployment. The VDSL solution provides multicast, Layer 2 Quality of Service (QoS), Link Aggregation (LACP) dynamic trunking groups, security, GVRP, IGMP for VOD (Video on demand) and SNMP RMON management and Web-based Switch network management.

The NVF-2400S is a bridge between external Internet backbone through a router for IP sharing and the building 110D telephone rack mount or telephone box. It utilizes the available telephone wire to enable high-speed Internet access to building's residents.

The NVF-2400S uses the phone line networking technology endorsed by the VDSL (Very High Data Rate DSL), and the NVF-2400S utilizes the already existing telephone wire to deliver 5/15/25 Mbps Internet access on each RJ-21 port.

This gives users a low-Cost, end-to-end solution and eliminates the need to train installation teams on multiple systems.

24 Ports VDSL + 2 Giga Ethernet

The NVF-2400S provide 1 x RJ-21 (24 x POTS Ports) with splitter on board, 1 x RJ-21 (24 x VDSL Ports) and 2 x 10/100/1000Mbps auto-sensing RJ-45. The NVF-2400S is a rack-unit (1.5RU) high, 299 mm deep. It is a standard 19" Rack mounted size. The NVF-2400S delivers dedicated bandwidth per port at rates up to 25 Mbps. VDSL transmissions coexist with POTS and ISDN, and can be compatible with ADSL/HomePNA traffic in the same building. This VDSL IP DSLAM can be configured on a per-switch basis to support the following modes:

5/10/15 Mbps symmetrical rate (up to 1700 / 1100 / 600 meters) and speed rate control from 100kbps up to 25Mbps. The NVF-2400S and VDSL Bridge provide fast and easy connectivity into building patch panels with RJ-21 connector. The 10/100/1000 Ethernet ports can be used to connect servers, Ethernet switches. These connectivity options provide multiple price/performance options to meet building and budget requirements.

Attention:

Be sure to read this manual carefully before using this product. Especially Legal Disclaimer, Statement of Conditions and Safty Warnings.

Caution:

The NVF-2400S are for **indoor** applications only. This product does not have waterproof protection.

The NVF-2400S provides the important features necessary for robust networks:

Quality of Service:	Supports 802.1p QoS. Provides high-and low-priority queuing on a per-port basis.
Supports IGMP:	Snooping by 256 IP multicast table for VOD (Video on Demand) and Video Conference and Internet games application.
Scalability:	Supports bandwidth control from 100k to **5/15/25** Mbps symmetric performance over single-pair wiring. Fast Ethernet Channel port aggregation.
Security:	**802.1Q Tag base** and **port-based** virtual local-area network (VLAN) support. Private VLAN access, assuring port security without requiring a VLAN per port, and also **Supports MAC filtering to Lock MAC address and 802.1V Protocol VLAN.**
In-Band Management:	NVF-2400S provides a console port for setup IP or other function.
Out of Band Management:	NVF-2400S support remote control by Telnet and Web-based Management easy-to-use configuration and ongoing monitoring. This software is embedded in the NVF-2400S and delivers remote, intuitive management of NVF-2400S and connected VDSL CPE devices through a single IP address. The NVF-2400S is easy-to-configured and deployed, and offering a compelling option in terms of cost, performance, scalability and services compared to traditional ATM-based xDSL solutions.
Speed Rate Control:	NVF-2400S supports speed rate control function, from 100kbps to 5/15/25Mbps.
IEEE-802.1x:	port base network access control, this function for wireless users connecting Authentication.
Spanning tree:	Supports IEEE802.1d for MAC bridge and link redundant.
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.
SNR indication:	Signal to Noise Ratio (SNR) for check phone wiring quality and cross talk for offering wiring information to engineer.
FAN & Temperature Monitor:	This is a monitoring function for the cooler FAN speed and inner temperature status, if the FAN stops or the temperature is over 70°C, the alarm trap will be sent via SNMP.

SNMP MIB Supports:	RFC-1213 MIBII, RFC-1493 Bridge MIB, RFC-1643 Ether like MIB, RFC-1757 RMON MIB / groups 1,2,3,9, Enterprise MIB.
Supports Interleave Setup:	To prevent the transmission against noise and data error.
Giga port auto link supports:	This function can be auto sensing client interface media with Copper or fiber optic and link one and supports hot swap.
Alarm:	In order to make sure the system is working normally, the NVF-2400S provides Fan and Temperature monitor and management, you can see through WEB or Telnet which shows the internal temperature and fan speed, if the temperature exceeds 70°C or the fan stops working, the VDSL IP DSLAM will send a SNMP trap to inform the Trap management server.
Hacker prevention:	To avoid hacker to enter management system through client side (CPE), the NVF-2400S will filter system IP from client side.
Supports multiple web browsers:	IE, Mozilla & Netscape under Windows O/S Mozilla & Netscape under Linux O/S

Safety Warnings

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

- **DO NOT** open the device or unit. Opening or removing covers can 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 cord or power adapter to the right supply voltage (110V AC in North America or 230V AC in Europe).
- **DO NOT** use the device if the power supply is damaged as it might cause electrocution. If the power supply is damaged, remove it from the power outlet. DO NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- **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 airflow may harm your device.
- **DO NOT** store things on the device.
- **DO NOT** use the device for outdoor applications, and make sure all the connections are indoors. There may be a remote risk of electric shock from lightning.
- **Be careful** when unplugging the power, because the transformer may be very hot.
- **Keep** the device and all its parts and accessories out of children's reach.
- **Clean** the device using a soft and dry cloth rather than liquid or atomizers. Power off the equipment before cleansing it.
- This product is **recyclable**. Dispose of it properly.

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 x NVF-2400S VDSL IP DSLAM
- 1 x User's Manual CD
- 1 x AC Power cord
- 2 x Rack Mounting Brackets
- 8 x Screws for Brackets
- 4 x Plastic feet(Pre-installed on the bottom)
- 2 x 1.5m RJ-21 male-to-male Telco connector wire (Option Parts)

Note:

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.

Chapter 2. General Description

2.1 Hardware Description

This section describes the important parts of the NVF-2400S. It features the front indicators and rear connectors.

NVF-2400S Outlook

2.2 Front Panel

The following figure shows the front panel. (Figure 2.1)

1. RJ-21 POTS/ ISDN Port
2. Status Indicators
3. RJ-21 VDSL line Port
4. RJ-45 Gigabit Port
5. Console(Baud rate: 9600 bps)
6. Reset button

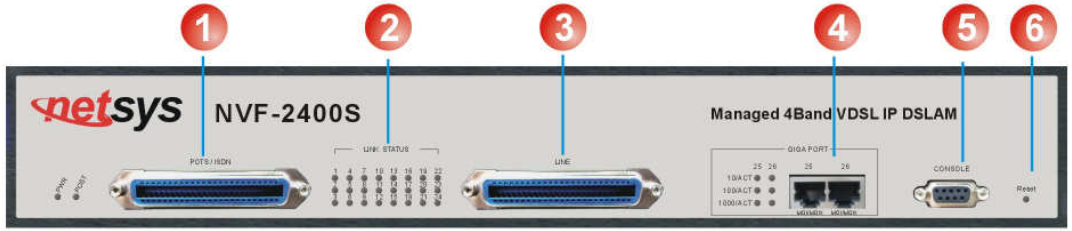


Figure 2.1 Front Panel description

Tip:

The NVF-2400S has **Splitter embedded** between each VDSL and POTS. It permits delivery of broadband service on the same lines as Plain Old Telephone Service (POTS), ISDN traffic and VDSL Signal.

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

The 24-port VDSL IP DSLAM provides one 10/100/1000Mbps auto-sensing RJ-45 Ethernet port as Ethernet expansion port and one 10/100/1000 RJ-45 trunk port with auto link function.

2.3 Front Indicators

The following describes the function of each LED indicator. (Table 2-1)

Table 2-1 LED Indicators Description and Operation

LEDs	Color	Status	Descriptions
PWR (Power LED)	Green	Steady	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 (LED OFF) means the product is not receiving power.
POST	Green	Steady	POST(Power On Self Testing)POST Led will light to show system is booting now. When system is ready the led will light off.
LINK STATUS	Green	Steady	Each station port on the VDSL is assigned an LED light for "Good Linkage". Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage.
10 LINK/ACT	Green	Steady Blinking	Each RJ45 station port on the Ethernet is assigned an LED light for "10M Good Linkage". Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage. And Flashing to show data transmission.
100 LINK/ACT	Green	Steady Blinking	Each RJ45 station port on the Ethernet is assigned an LED light for "100M Good Linkage". Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage. And Flashing to show data transmission.
1000 LINK/ACT	Green	Steady Blinking	Each RJ45 station port on the Ethernet is assigned an LED light for "1000M Good Linkage". Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage. And Flashing to show data transmission.

2.4 Rear Panel

The following figure shows the rear connectors. (Figure 2.2)

Figure 2.2 Rear Panel description

Note:

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

Chapter 3. Complete Installation

3.1 Hardware Installation

This chapter describes how to install the NVF-2400S to establish network connection. You may install the 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.

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:

Verify the following installation requirements:

- Power requirements: AC 100V to 240 V at 50 to 60 Hz.

  Tip:

  The Switching 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 ventilation
- Place the NVF-2400S away from **direct sunlight**, **heat sources**, or areas with a high amount of electromagnetic interference.
- Check if network cables and connectors needed for installation are available
- **Do Not** install phone lines strapped together with AC power lines, or telephone office line with voice signal.
- **Avoid** installing this device radio amplifying station nearby or transformer station nearby.
- Please note NVF-2400S internal splitter, can pass through voice spectrum is 0KHz ~ 630KHz.

3.3 General Rules

Before making any connections to the NVF-2400S, note the following rules:

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

  All network connections to the NVF-2400S Ethernet port must be made using Category 5 UTP for 100Mbps and Category 3, 4 UTP for 10Mbps. No more than 100 meters (about 333 feet) of cabling may be use between NVF-2400S or with HUB or an end node.

- **VDSL Port (RJ-21)**

  All home networks connected to VDSL.

  1 X RJ-21 Cable (Male to Male) Using **Pin 1 ~ 24, 26 ~ 49.**

  RJ-21 Pins 25 & 50 are not used.

- We **do not** recommend **using 28 Gauge** or above phone line.

3.4 NVF-2400S Connections

The 24-port VDSL IP DSLAM has 2 x GIGA Ethernet supporting full or half-duplex operation. 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 "**25**" port connects to devices such as server, bridge or router. You can also cascade to another compatible MUX or hub by connecting the 26 port to the other device.

3.5 Ethernet Ports Connections

Ethernet Port "25" and "26" support auto MDI/MDIX.

You can connect the "25 or 26" port on the IP DSLAM to any device that uses a standard network interface such as a Cable modem, ADSL modem, Ethernet Switch, workstation or server, or also to a network interconnection device such as a bridge or router (depending on the port type implemented).

Prepare straight through (or cross over) shielded or unshielded twisted-pair cables with RJ-45 plugs on both ends. Use 100Ω Category 5 cable for connections. Connect one end of the cable to "25" port of the IP DSLAM, and the other end to a standard RJ-45 station port on cable modem, ADSL router, wireless bridge, etc. When inserting an RJ-45 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Note:

Make sure the length of twisted-pair cable is not over **100** meters (328 feet).

3.6 VDSL Ports Connections

1. Prepare the network devices you wish to connect. Make sure you have installed suitable VDSL Bridge before making a connection to any of the IP DSLAM (1-24) station ports. You also need to prepare one **18 ~ 26** gauge twisted pair phone wiring with RJ-21 plugs at both ends.

2. Connect one end of the cable to the RJ-21 port of the Home Access network adapter, and the other end to any available (1~24) station port on the VDSL. Every port supports 5/15/25 Mbps connections. When inserting an RJ-21 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

   - Instead, use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Note:

We advise using Category 5 cable for Cable Modem or Router connections to avoid any confusion or inconvenience in the future when you upgrade attached to high bandwidth devices.

3.7 Basic Configuration

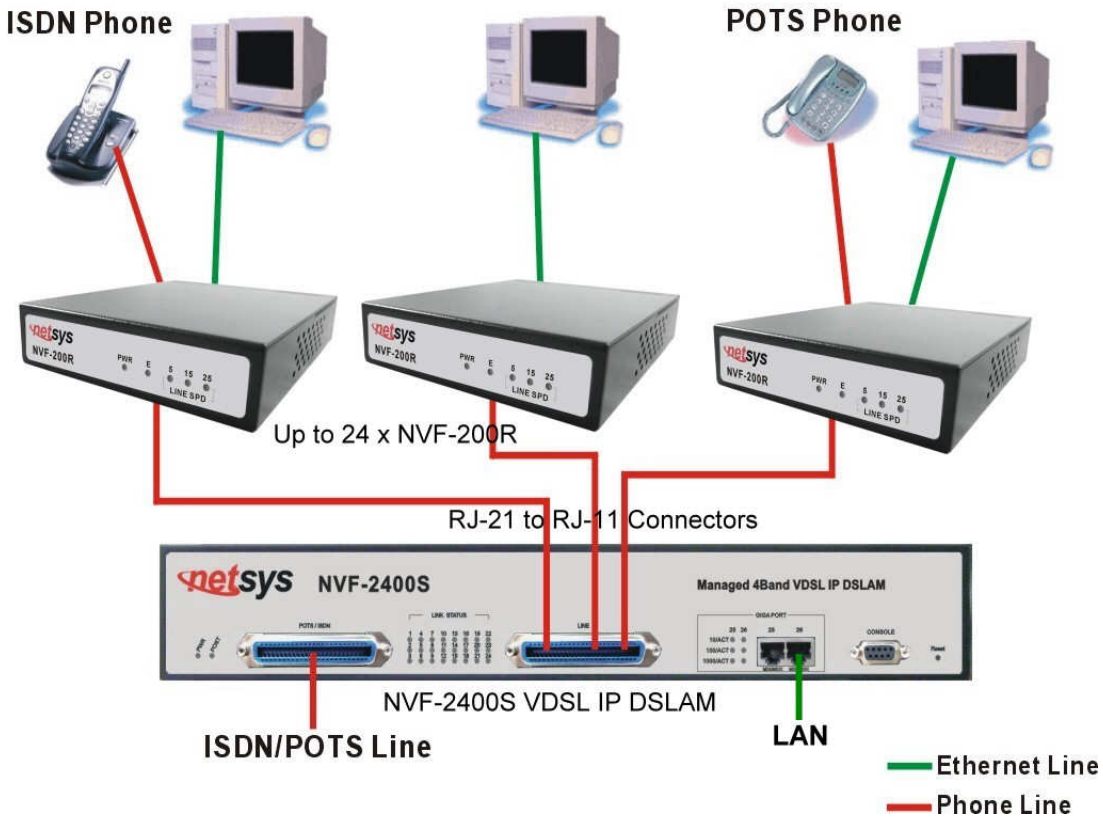


Figure 3.1 NVF-2400S Basic Application Diagram

Chapter 4. Management Configuration

4.1 In-Band Management

Console Port (RS-232) Configuration (Change IP Address via Hyperterminal)

1. Connect IP DSLAM with PC/Laptop's RS-232 port, launch "Hypert erminal" in the Windows™ system. (Figure 4.1)

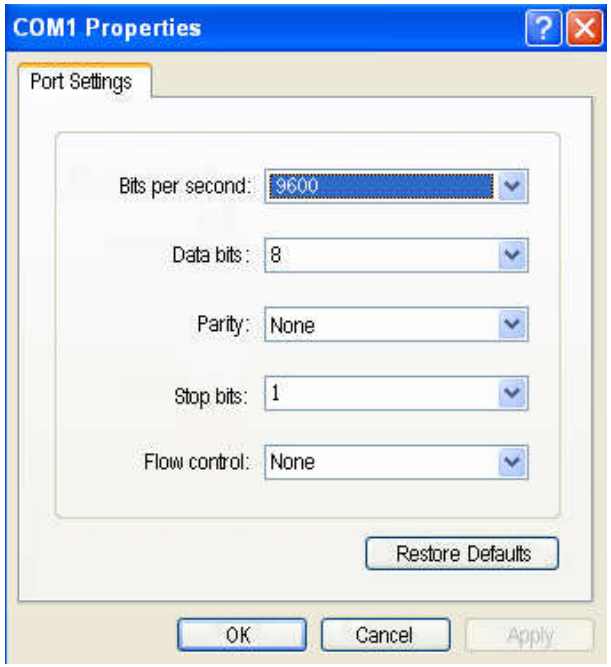


Figure 4.1 COM1 Properties

2. Set "**Bits per second**" at **9600** to the content window.
3. Set "**Flow control**" at **None**

4. After login window show on the screen, it will ask for Login Name and Password.

   Login Name: **admin**, Password: **123**

   Main Manual window will show on the screen as the following: (Figure 4.2)

Figure 4.2 Main Menu

Operation Button:

Tab=Next Item;

Backspace=Previous Item;

Enter = Select Item

5. Change the IP Configuration, enter the IP configuration page and follow these steps:

(1) Select "**Switch Static Configuration"** to enter the Switch Configuration page.

(2) Select "**Administration Configuration"** to enter the Device Configuration page. (Figure 4.3)

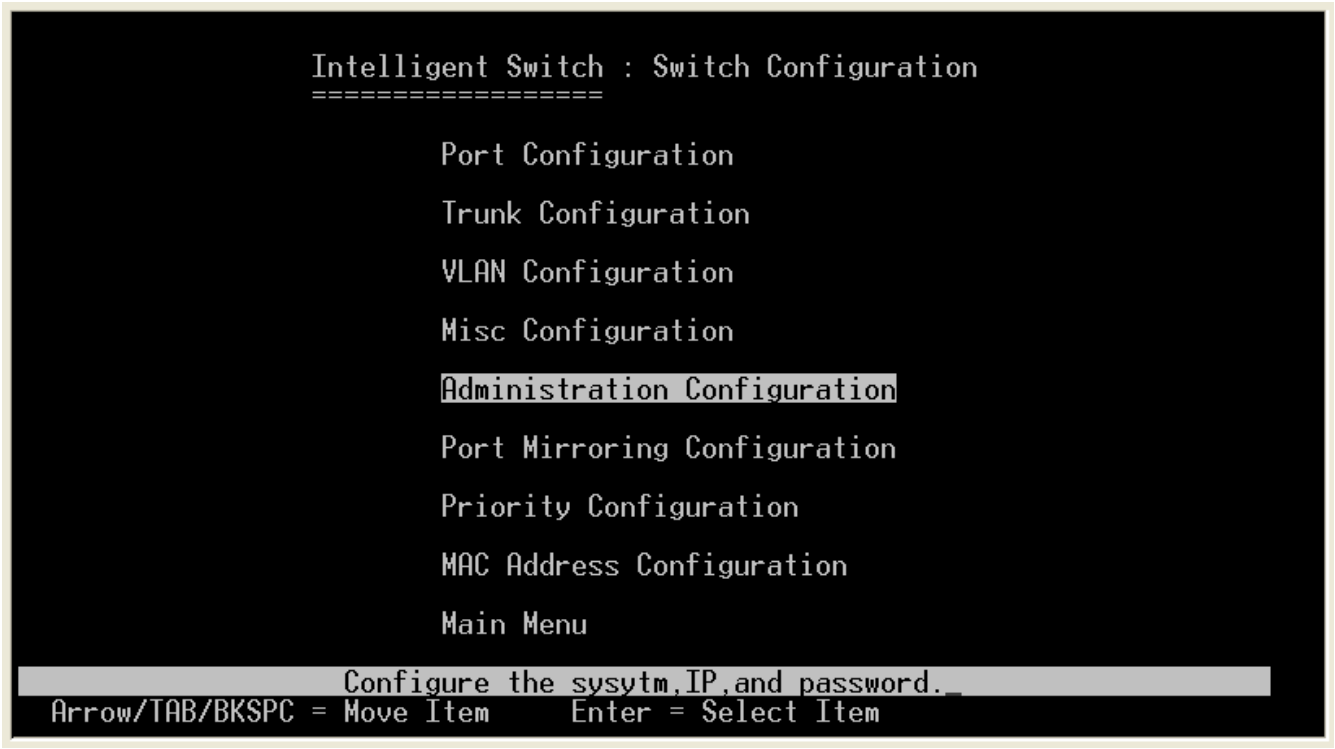


Figure 4.3 IP Configuraiton-1

(3) Select **"IP Configuration"** to enter the IP configuration page. (Figure 4.4)

Figure 4.4 IP Configuraiton-2

(4) In the **"IP Configuration"**, it allows user to setup the DHCP, IP Address, Subnet Mask and Gateway. (Figure 4.5)

Figure 4.5 IP Configuraiton-3

a. Select **<Edit>** to Change IP address, Subnet Mask and Gateway
b. Select **<Save>** to save the configuration and go back to System Configuration page
c. Select **<Quit>** to go back to the previous menu
d. Press **CTRL+A** to go back to the last action

4.1.1 Main Menu

There is an easy Setup for end users at the setup of NVF-2400S with **Switch Static Configuration**, **Protocol Related Configuration**, **Status and Counters**, **Temperature & Fan Monitor**, **Reboot Switch**, **TFTP Update firmware**, **Logout** for more detail configurations. (Figure 4.6)

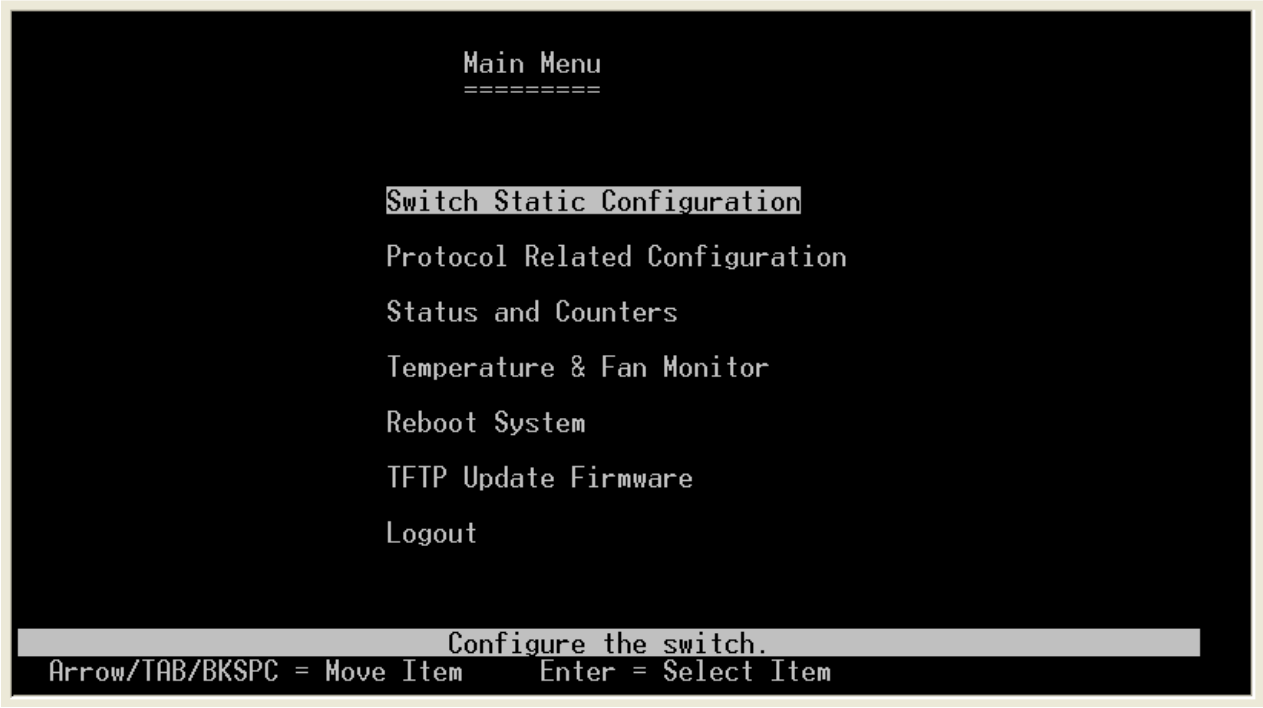


Figure 4.6 Main Menu introduction

4.1.1.1 Static Switch Configuration

Select the "Switch Static Configuration". The menu below includes the sub-menus of **Port**, **Trunk**, **VLAN**, **Misc**, **Administration**, **Port Mirroring**, **Priority**, **Mac Address** and **Main Menu**. (Figure 4.7)

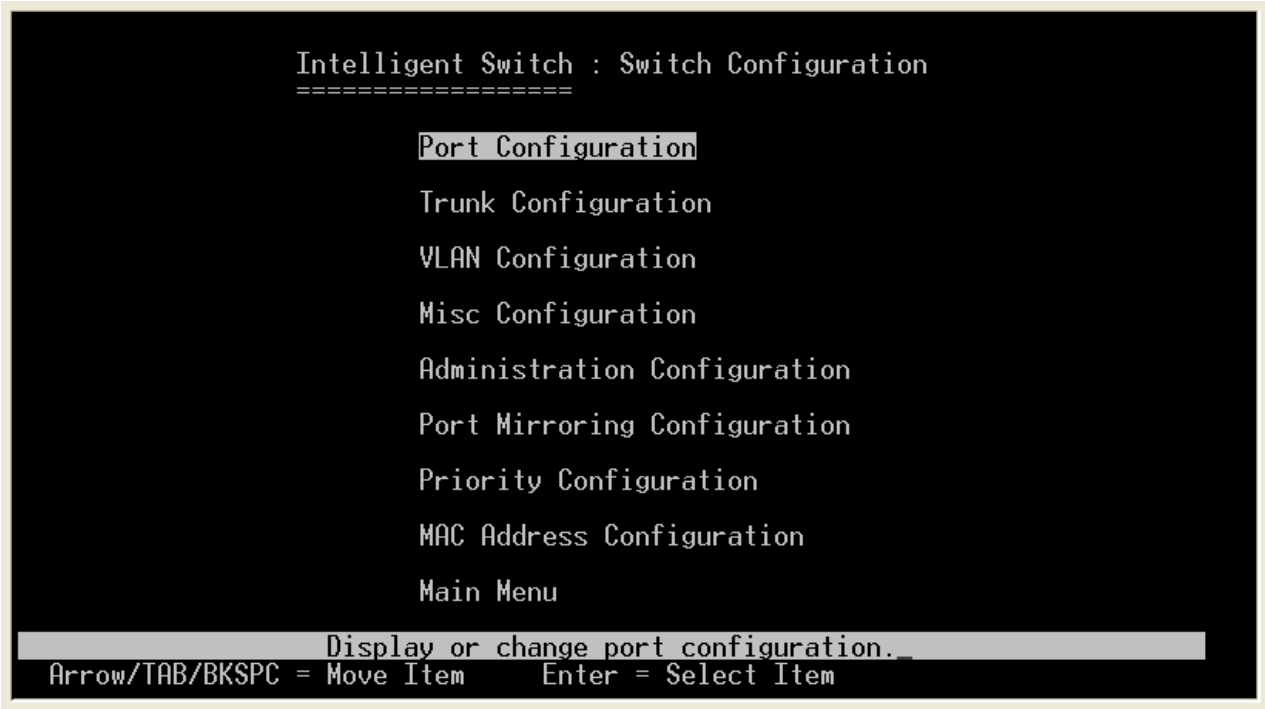


Figure 4.7 Switch Static Configuration

4.1.1.1.1 Port Configuration

Display or change port configuration. (Figure 4.8)

Item	Description
Port:	Shows the port number of NVF-2400S from ports **1 to 24**.
Type:	Shows the media type of the port's device.
InRate & OutRate:	Shows and configure the ingress and egress rate at 100K step size. Valid Range is from 0 to 1000. **(e.g. 250 x 100K = 25Mbps)**
Enabled:	Shows and configure if the port is enabled or not.
Speed/Duplex Config:	Shows and configure the speed of each port if it is Auto/5M/15M/25Mbps.
Flow Control:	Shows and configure if the port is enabled or not at half-duplex or full-duplex.

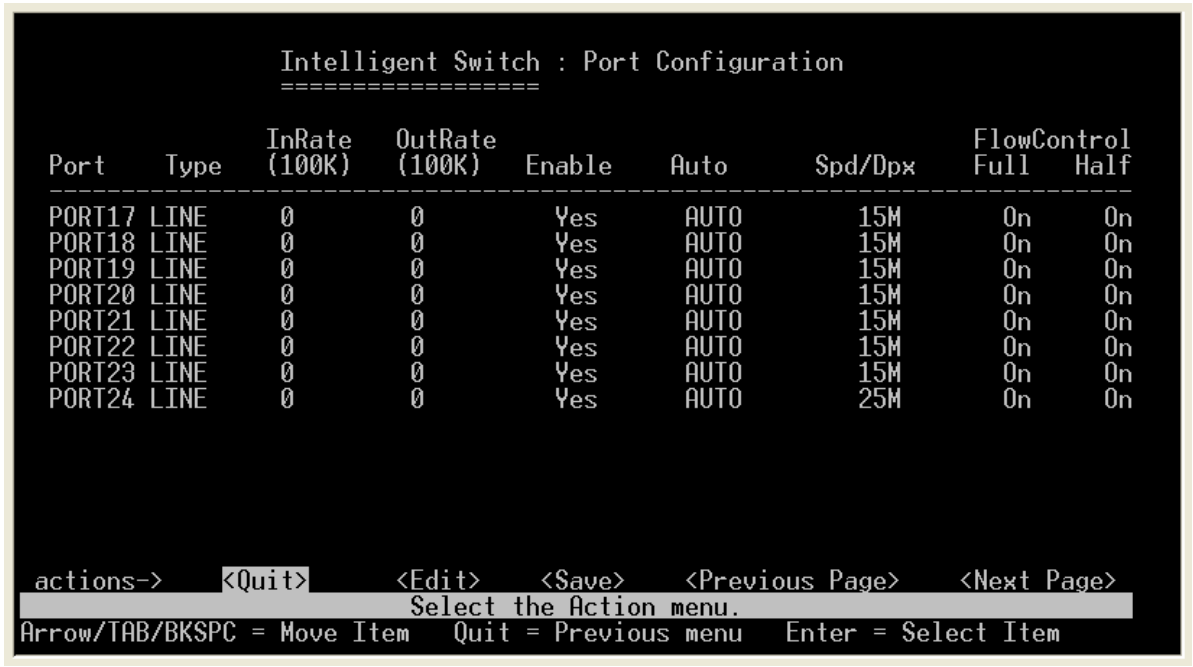


Figure 4.8 Port Configuration

4.1.1.1.2 Trunk Configuration

Display or change trunk configuration. (Figure 4.9)

Item	Description
TRK1 to TRK7:	Shows if TRK1 to TRK7 trunk configuration is disabled, static or LACP.

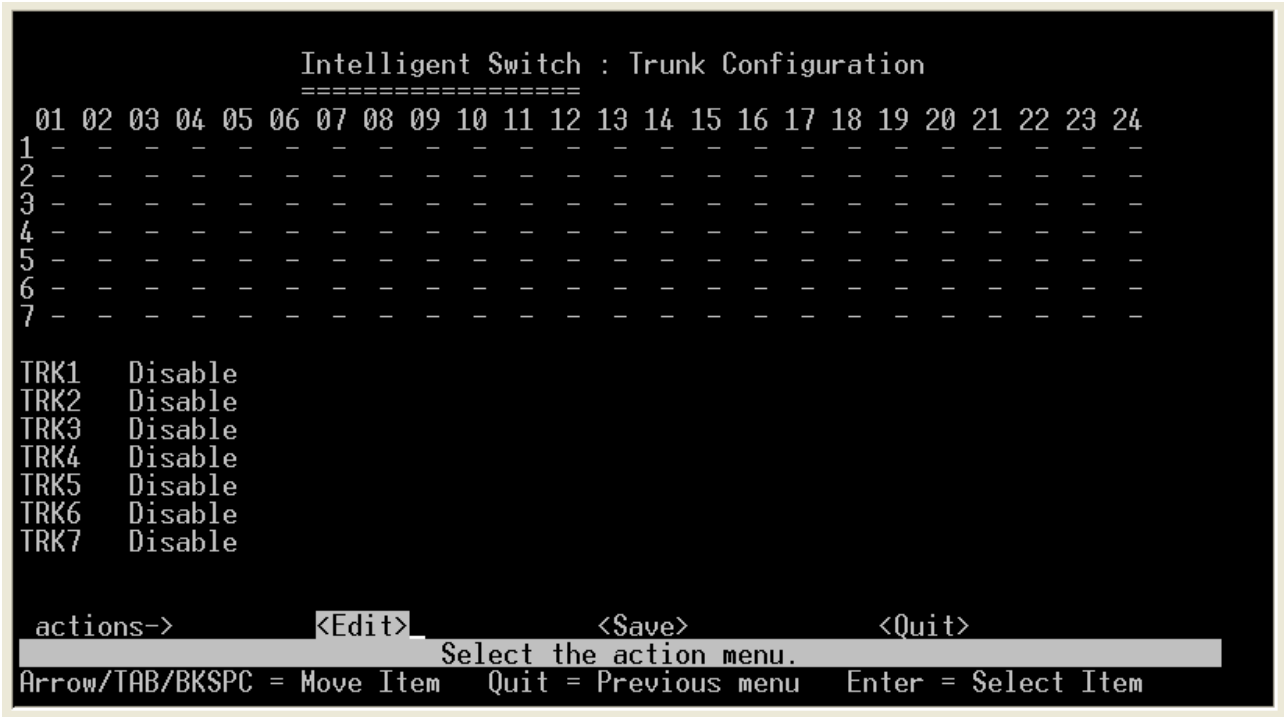


Figure 4.9 Trunk Configuration

4.1.1.1.3 VLAN Configuration

Select the "VLAN Configuration". The menu below includes the sub-menus of **VLAN Configure**, **Create a VLAN Group**, **Edit/Delete a VLAN Group**, **Group Sorted Mode**. Display or change VLAN (Virtual Local Area Network) configuration. (Figure 4.10)

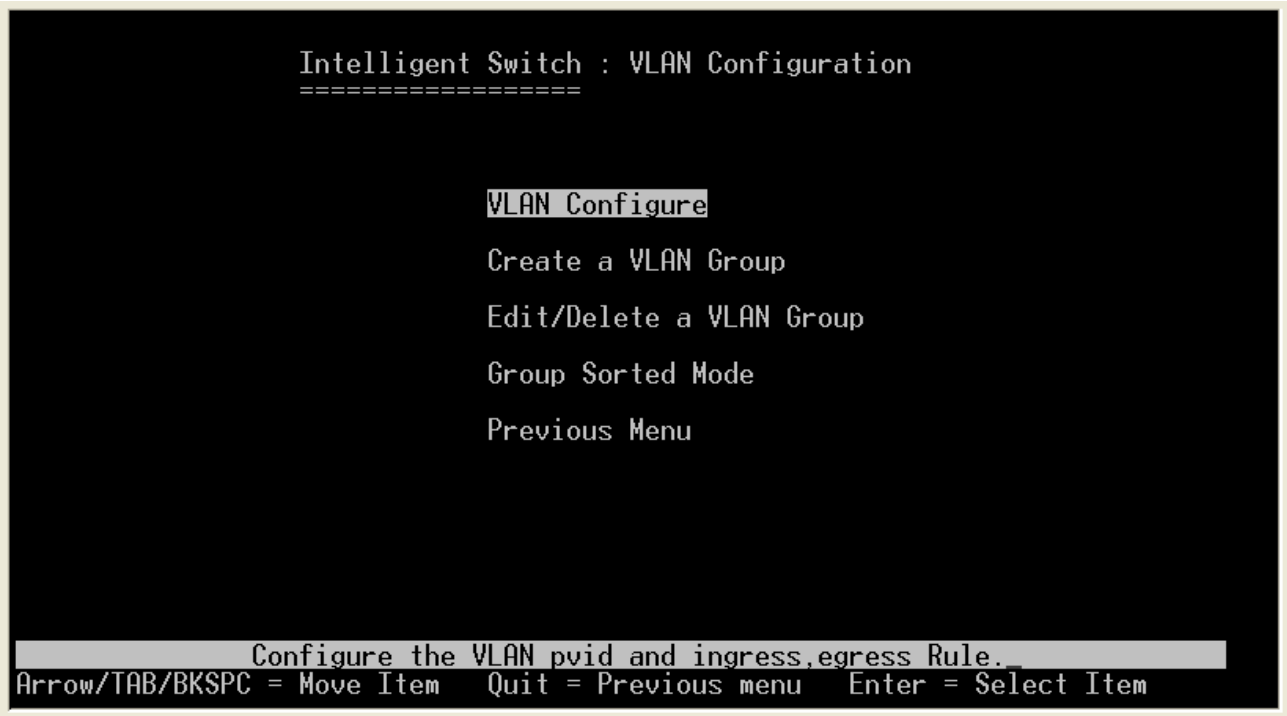


Figure 4.10 VLAN Configure

4.1.1.1.3.1 VLAN Configure

Configure the VLAN PVID and Ingress/Egress Rule.

Item	Description
VLAN Mode:	User can choose from 4 VLAN modes, respectively, 802.1Q, Port Based and Disable. Default VLAN mode is disabled.

VLAN Mode: **Disabled** (Figure 4.11)

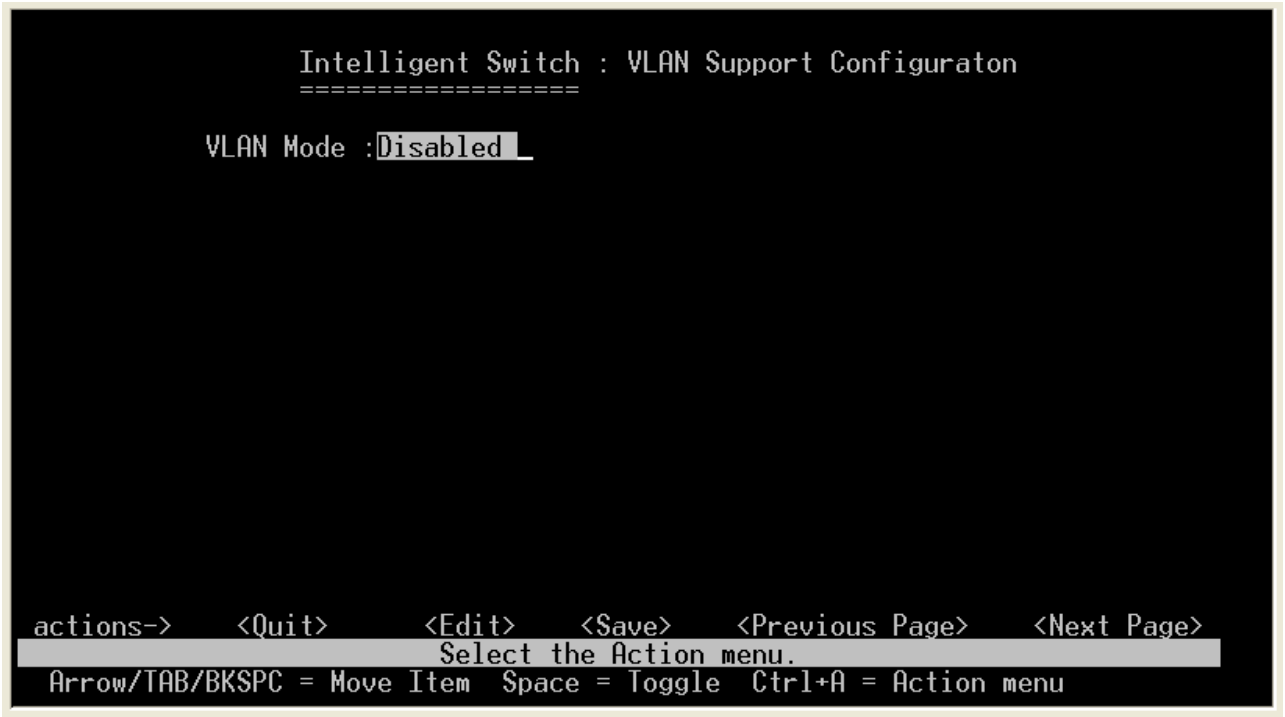


Figure 4.11 VLAN Mode: Disable

VLAN Mode: **PortBased**(Figure 4.12)

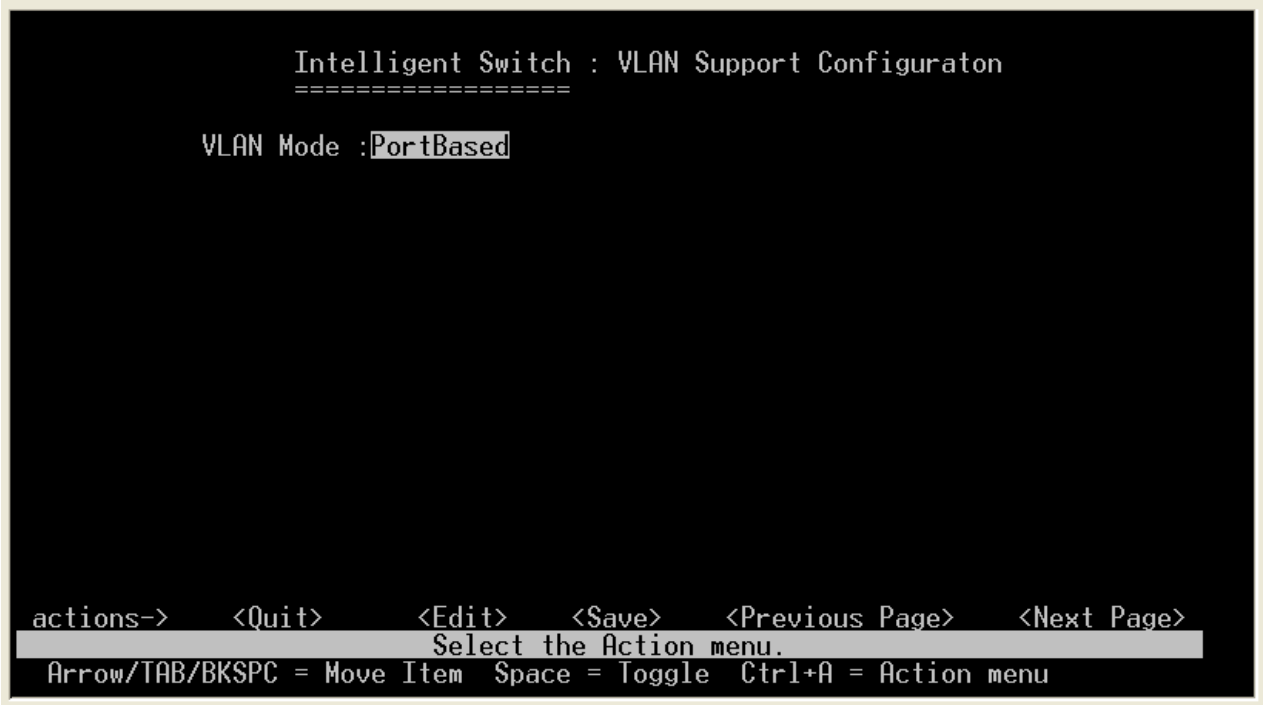


Figure 4.12 VLAN Mode: Port Based

VLAN Mode: **802.1Q**(Figure 4.13)

Item	Description
Port:	Shows the port of NVF-2400S VDSL IP DSLAM.
PVID:	Shows the PVID value. Valid range is from 1 to 4094.
IngressFilter1 NonMember Pkt:	Shows the packet being dropped or forwarded.
IngressFilter2 Untagged Pkt:	Shows the packet being dropped or forwarded.

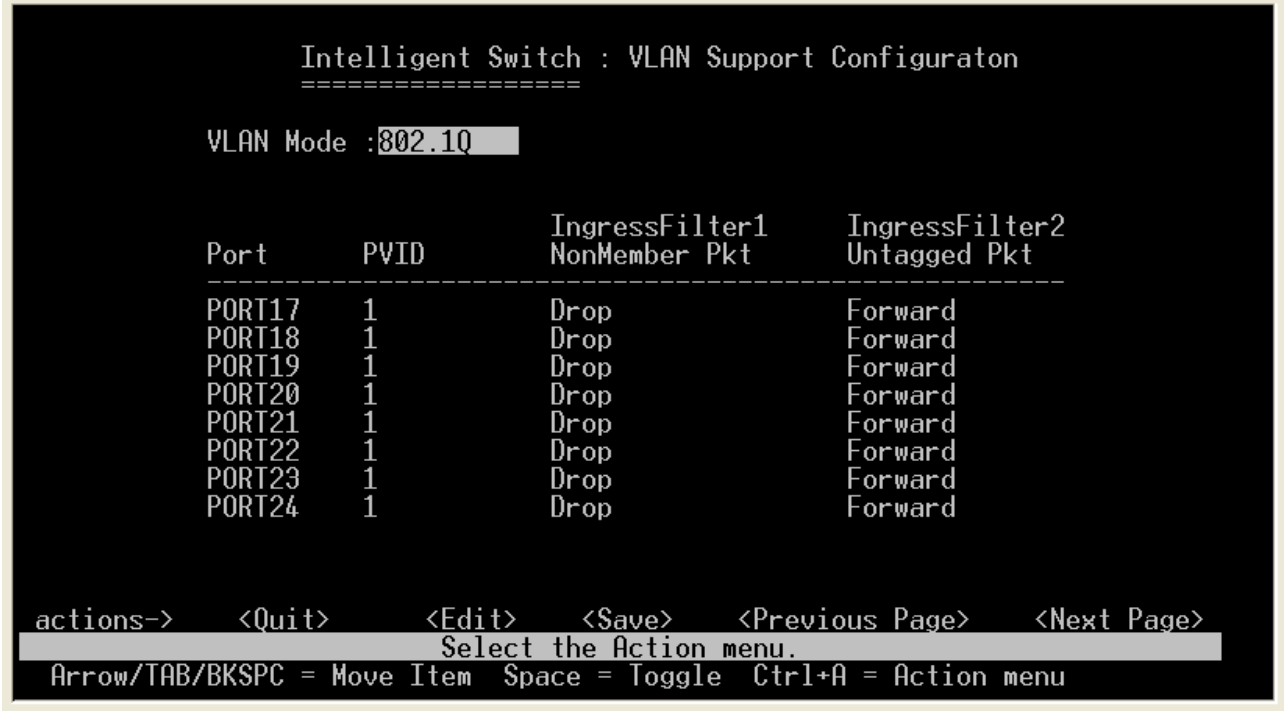


Figure 4.13 VLAN Mode: 802.1Q

4.1.1.1.3.2 Create a VLAN Group

Create a VLAN Group. (Figure 4.14)

Item	Description
VLAN Name:	Input VLAN name valid up to 16 characters.
Grp ID:	Input VLAN ID, valid range is from 1 to 4094.
Port:	Shows the port number of NVF-2400S VDSL IP DSLAM.
Member:	Shows if the port is a member of the VLAN group or not.

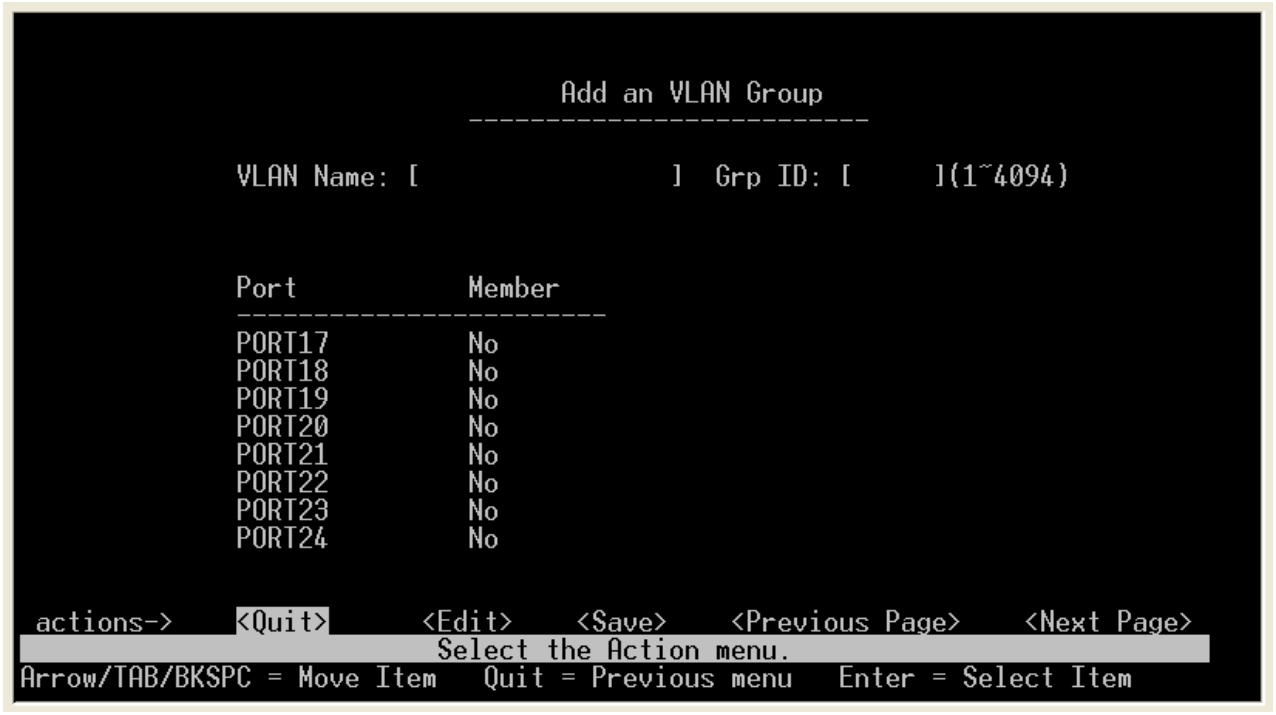


Figure 4.14 Create a VLAN Group

4.1.1.1.3.3 Edit/Delete a VLAN Group

Edit/Delete a VLAN Group. (Figure 4.15)

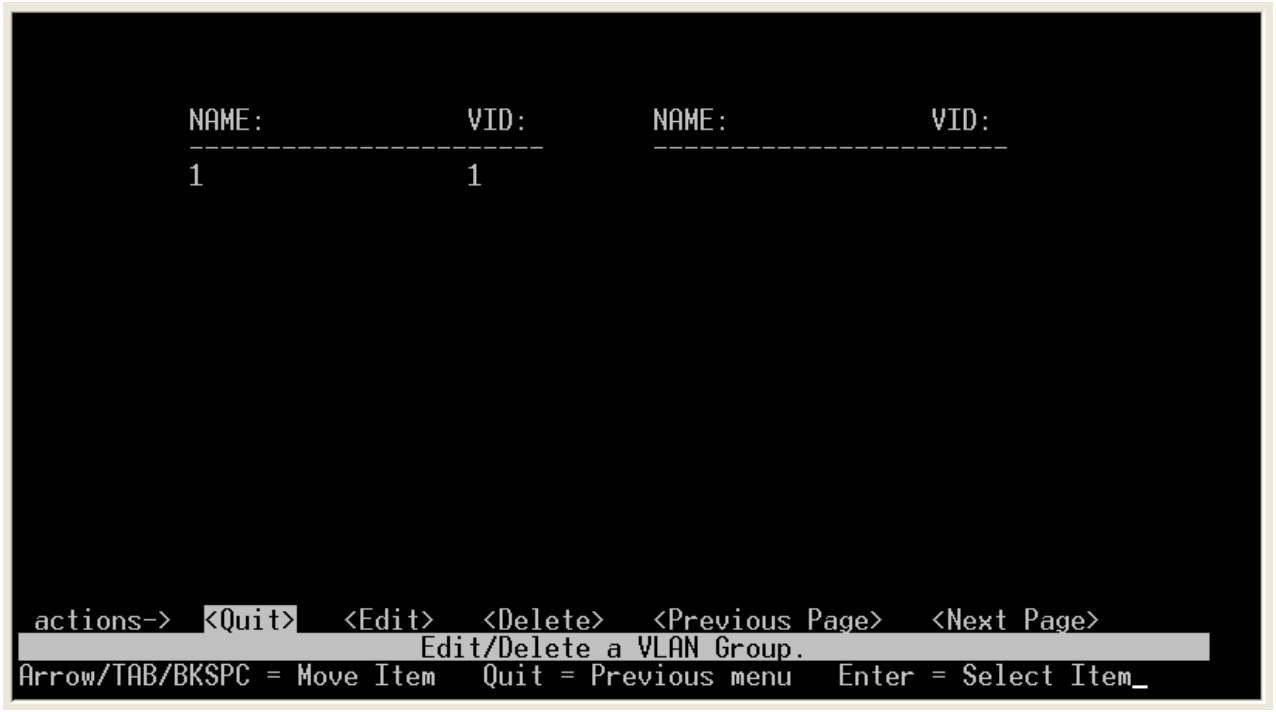


Figure 4.15 Edit or Delete a VLAN Group

4.1.1.1.3.4 Group Sorted Mode

Select a group sorted mode. (Figure 4.16)

Item	Description
Group Sorted:	Group sorted can either be sorted by name or by VID.

Figure 4.16 Group Sorted Mode

4.1.1.1.4 Misc Configuration

Select the "Misc Configuration". The menu below includes the sub-menus of **Mac Age interval**, **Broadcast Storm Filtering**, **Max bridge transmit delay bound**, **Collisions Retry Forever** and **Hash Algorithm**. Please configure the miscellaneous items as follows. (Figure 4.17)

Figure 4.17 Misc Configuration

4.1.1.1.4.1 MAC Age Interval

Configure the MAC aging time. (Figure 4.18)

Item	Description
MAC Age Interval:	MAC aging interval is from 120 to765 seconds; disabled is 0.

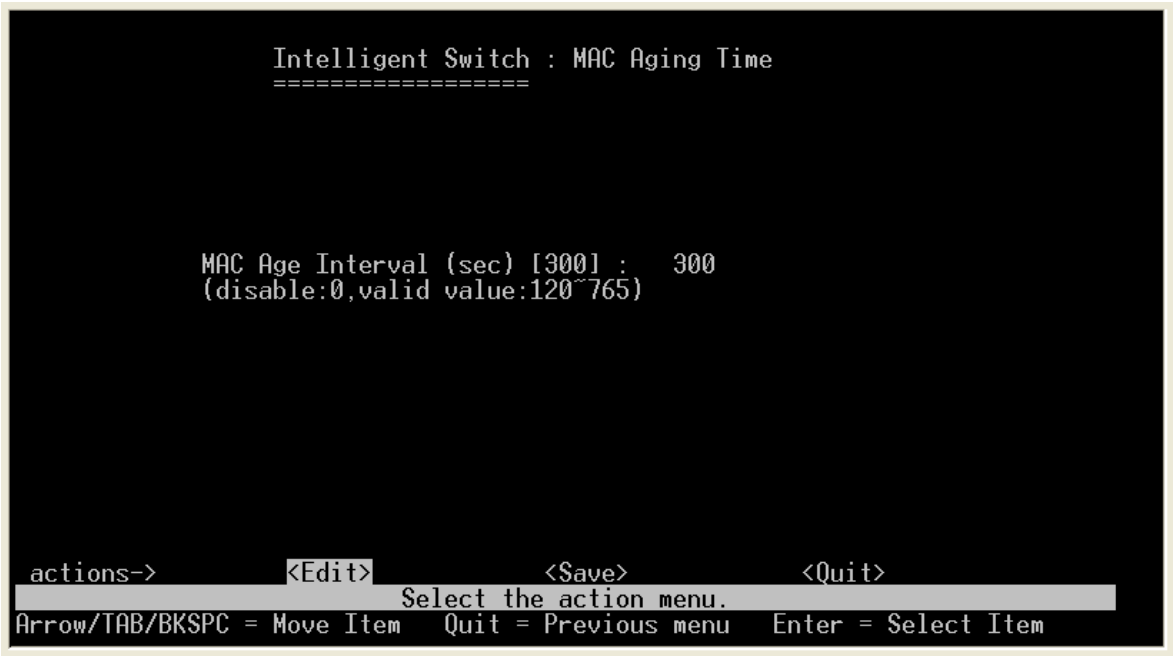


Figure 4.18 Mac Aging Time

Note:

If not set the aging-time, ip address and mac address mapping will be always there, even for a computer using the same ip to access does not automatically update the mac table. After setting the aging-time, every time of Aging time interval will arrive to relearn the MAC address table. In fact, this time does not need special setting, default MAC age interval is **300** seconds.

4.1.1.1.4.2 Broadcast Storm Filtering

To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. (Figure 4.19)

Item	Description
Broadcast Storm Filter Mode:	Broadcast storm filter mode can either be 5%, 10%, 15%, 20%, 25% or NO. Default broadcast storm filter is at 5%.

Figure 4.19 Broadcast Storm Filter mode

4.1.1.1.4.3 Max Bridge Transmit Delay Bound

Configure the maximum bridge transmit delay bound. Default maximum bridge transmit delay bound is OFF, low queue delay bound is disabled, and low queue max delay time is 255ms. (Figure 4.20)

Item	Description
Max bridge transmit delay bound:	Limit the packets queuing time in switch. If enable, the packets queued exceed will be drop. This valid value are 1sec, 2 sec,3sec, 4 sec and off.
Low Queue Delay Bound:	Low queue delay bound can either be Enable or Disable.
Low Queue Max Delay Time:	Low queue max delay time is from 1 to 255ms. (2ms/unit)

Figure 4.20 Configure the maximum bridge transmit delay bound.

4.1.1.1.4.4 Collisions Retry Forever

Default is enabled. (Figure 4.21)

Item	Description
Collisions Retry Forever:	Collisions retry forever can either be enabled or disabled. ◆ Disable: If happen collision will retry 48 times and then drop frame. ◆ Enable: If happen collision will retry forever.

Figure 4.21 Collisions Retry Forever

4.1.1.1.4.5 Hash Algorithm

Provide CRC or Direct Map. This Hash Algorithm is for hardware maintain on MAC table calculation. (Figure 4.22)

Item	Description
Hash Algorithm:	Hash algorithm mode can either be CRC-Hash or DirectMap. Default is at CRC-Hash.

Figure 4.22 Hash Algorithm

4.1.1.1.5 Administration Configuration

Select the "Administration Configuration". The menu below includes the sub-menus of **Change Username**, **Change Password**, **Device Information** and **IP configuration.** Please configure the Administration items as follows. (Figure 4.23)

Figure 4.23 Administration Configuration

4.1.1.1.5.1 Change Username

Item	Description
Username:	Shows and configure the current username.

(Figure 4.24)

Figure 4.24 User Name Configuration

4.1.1.1.5.2 Change Password

Configure the password, type the numbers will be masked. (Figure 4.25)

Item	Description
Old Password:	Type the old password.
New Password:	Type the new password.
Enter again:	Type the new password again.

Figure 4.25 Password Configuration

4.1.1.1.5.3 Device Information

Configure the device information, you can edit and create your own name. (Figure 4.26)

Item	Description
Device Name:	Shows the whole device name.
Device Description:	Shows the description of the device.
Device Location:	Shows the location of the device.
Device Content:	Shows the content of the device.

Figure 4.26 Device Information

4.1.1.1.5.4 IP Configuration

Configure the IP(Internet Protocol) information. (Figure 4.27)

Item	Description
DHCP:	Shows DHCP can either be enabled or disabled. (Default DHCP is disabled)
IP Address:	Shows the IP address of the device.
Subnet Mask:	Shows the subnet mask of the device.
Gateway:	Shows the gateway of the device.

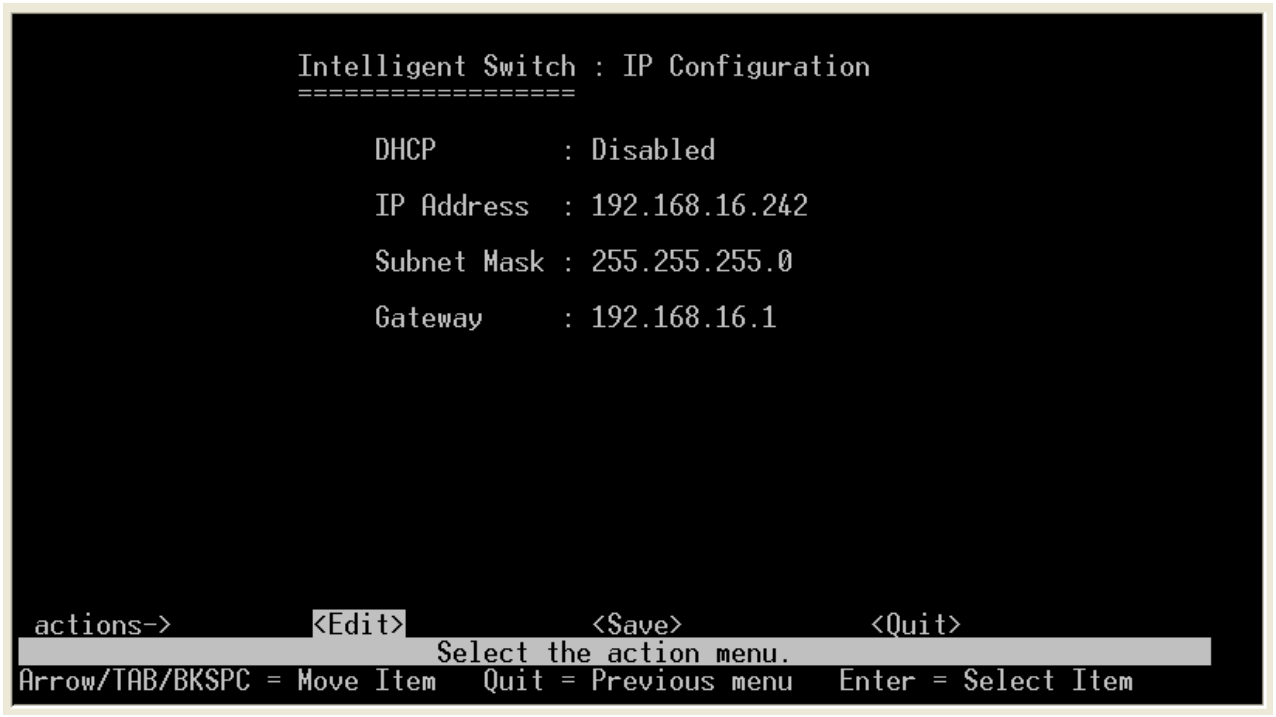


Figure 4.27 IP Configuration

4.1.1.1.6 Port Mirroring Configuration

Display or change port mirror configuration. (Figure 4.28)

Item	Description
Sniffer mode:	Disable (Default Sniffer mode is disabled).

Figure 4.28 Sniffer Mode: Disable

Tip:

This function can special monitor client side as duplicate mail, Http…..etc, but need to be used with the application software (i.e. sniffer software).

Sniffer Mode: **Rx** (Figure 4.29)

Item	Description
Monitoring Port:	Can be selected from Port1 to Port26 as the monitoring port.
Monitored Port:	Port1 to port26 can be monitored by the monitoring port if it is check as a member.

Figure 4.29 Sniffer Mode: Rx (Rx packet only)

Sniffer Mode: **Tx** (Figure 4.30)

Item	Description
Monitoring Port:	Can be selected from Port1 to Port26 as the monitoring port.
Monitored Port:	Port1 to port26 can be monitored by the monitoring port if it is check as a member.

Figure 4.30 Sniffer Mode: Tx (Tx packet only)

Sniffer Mode: **Both** (Figure 4.31)

Item	Description
Monitoring Port:	Can be selected from Port1 to Port26 as the monitoring port.
Monitored Port:	Port1 to port26 can be monitored by the monitoring port if it is check as a member.

Figure 4.31 Sniffer Mode: Both (Rx and Tx packet)

4.1.1.1.7 Priority Configuration

Display or change port priority configuration. (Figure 4.32)

Figure 4.32 Priority Configuration

4.1.1.1.7.1 Port Static Priority

Configure port static priority. (Figure 4.33)

Item	Description
Port Static Priority:	Port static priorities can either be disabled, low or high, default static priority is disabled.

Figure 4.33 Port Priority

4.1.1.1.7.2 802.1p Priority

Configure 802.1p priority. (Figure 4.34)

Item	Description
Qos Mode:	◆ First Come First Serve. ◆ All High Before Low. ◆ High/Low Queue Service Ratio H:[1] L:[1]. Default QoS Mode is First Come First Serve (FCFS).

Figure 4.34 QoS(Quality of Service) Priority Configuration

4.1.1.1.8 MAC Address Configuration

Select the "Mac Address Configuration". The menu below includes the sub-menus of **Filtering Mac Address**. (Figure 4.35)

Figure 4.35 Mac address configuration

4.1.1.1.8.1 Filtering MAC Address

Filtering the MAC address configuration. (Figure 4.36)

Figure 4.36 Filter Mac Address

Tip:

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. For example, if your network is congested because of high utilization from one MAC address, you can filter all traffic transmitted from that MAC address, restoring network flow while you troubleshoot the problem.

Add filter MAC Address. (Figure 4.37)

Item	Description
Mac Address:	Input the MAC address of certain device to be filtered out.

Figure 4.37 Add filter Mac Address

4.1.1.2 Protocol Related Configuration

Select the "Protocol Related Configuration". The menu below includes the sub-menus of STP, SNMP, GVRP, IGMP, LACP and 802.1X. Please configure the protocol items as follows. (Figure 4.38)

Figure 4.38 Configure the Protocol Related

4.1.1.2.1 STP

Select the "STP". The menu below includes the sub-menus of **STP Enable**, **System Configuration** and **Perport Configuration**. Please configure the STP items as follows. (Figure 4.39)

Figure 4.39 Spanning Tree Protocol

4.1.1.2.1.1 STP Enable

The Spanning-Tree Protocol (STP) is a standardized method (IEEE 802.1d) for used to prevent forwarding loops on a LAN. When STP enabled, to ensure that only one path at a time is active between any two nodes on the network. (Figure 4.40)

We are recommended that you **enable STP** on all switches ensures a single active path on the network.

Item	Description
STP:	Spanning Tree Protocol can either be enabled or disabled. Default is enabled.

Figure 4.40 STP Enable / Disable

4.1.1.2.1.2 System Configuration

Configure the STP system information. (Figure 4.41)

Item	Description
Priority:	A priority value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. Valid input priority range is from 0 to 65535. Default priority is **32768**.
Max Age:	The number of seconds a bridge waits without receiving . Spanning-Tree Protocol configuration messages before attempting a reconfiguration.Valid input max age range is from 6 to 40. Default max age is **20**.
Hello Time:	The number of seconds between the transmission of Spanning-Tree Protocol configuration messages.Valid input hello time range is from 1 to 10. Default hello time is **2**.
Forward Delay Time:	The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state.Valid input forward delay time range is from 4 to 30. Default forward delay time is **15**.

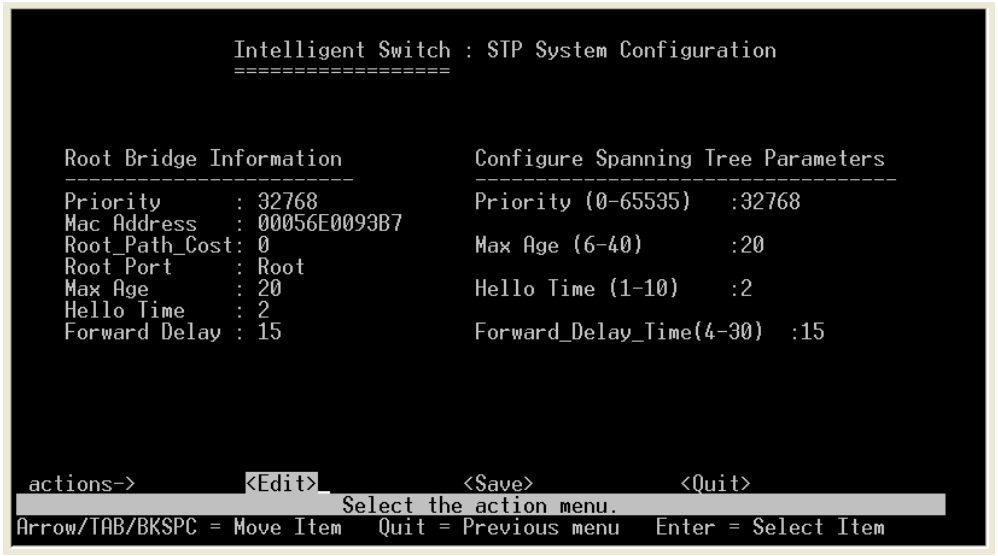


Figure 4.41 STP System Configuration

4.1.1.2.1.3 Perport Configuration

Configure the STP per port configuration. Default pathcost is 10 and priority is 128. (Figure 4.42)

Item	Description
Port:	Shows the port number of NVF-2400S VDSL IP DSLAM.
PortState:	Shows the condition of the port if it is enabled or disabled.
PathCost:	Specifies the path cost of the port that switch uses to determine which port are the forwarding ports the lowest number is forwarding ports, the rage is 1-65535 and default value base on IEEE802.1D 10Mb/s = 50-600 100Mb/s = 10-60 1000Mb/s = 3-10
Priority:	You can make it more or less likely to become the root port, the range is from 0 to 255,default setting is 128, the lowest number has the highest priority.

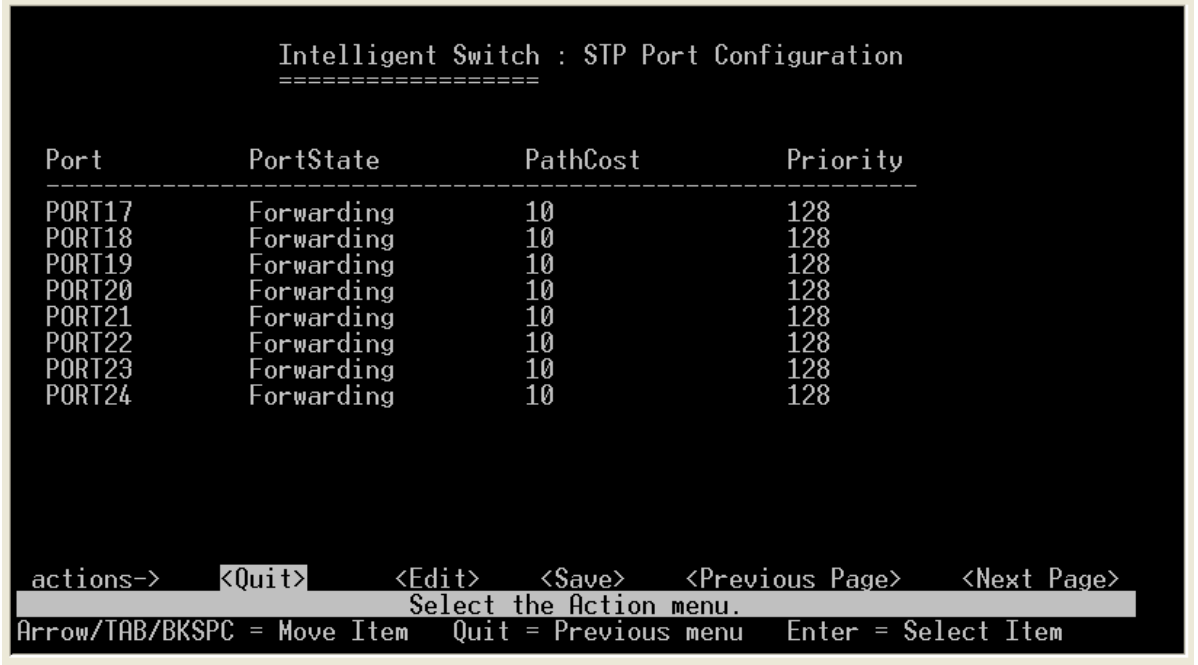


Figure 4.42 STP Port Configuration

4.1.1.2.2 SNMP

Select the "SNMP". The menu below includes the sub-menus of **System Options**, **Community Strings** and **Trap Mangers**. SNMP means Simple Network Manager Protocol. Please configure the SNMP items as follows. (Figure 4.43)

Figure 4.43 SNMP Configuration

4.1.1.2.2.1 System Options

Configure the system options. (Figure 4.44)

Item	Description
System Name:	Configuration to your own system name up to 32 characters.
System Contact:	Configuration to your own system contact up to 32 characters. (i.e. a person or organization)
System Location:	Configuration to your own system location up to 32 characters.

Figure 4.44 system options

4.1.1.2.2.2 Community Strings

Configure the community. (Figure 4.45)

For example,community name set to "public", Write access set to "Restricted", means enable requests accompanied by this string to display MIB-object information. And another community name set to "private", Write access set to "Unrestricted", means enable requests accompanied by this string to display MIB-object information and to set MIB objects.

Figure 4.45 SNMP Community Configuration

Add SNMP Community(Figure 4.46)

Item	Description
Community Name:	Input valid community name up to 32 characters to be included in the SNMP community.
Write Access:	Write access can either be restricted or unrestricted.

Figure 4.46 Add SNMP Community

4.1.1.2.2.3 Trap Managers

A trap manager is a management station that receives traps, the system alerts generated by the IP DSLAM. 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. (Figure 4.47)

Figure 4.47 Trap Managers Confiruration

Add SNMP Trap manager. (Figure 4.48)

Item	Description
IP:	Input IP address to be included in the SNMP trap manager.
Community Name:	Input valid community name up to 32 characters to be included in the SNMP trap manager.

Figure 4.48 Add SNMP Trap Manager

4.1.1.2.3 GVRP

Configure the GVRP protocol. Default GVRP is disabled. (Figure 4.49)

Item	Description
GVRP:	GARP VLAN Registration Protocol can either be enabled or disabled.

Figure 4.49 GVRP Configuration Enable / Disable

4.1.1.2.4 IGMP

Configure the IGMP protocol. Default IGMP is disabled. (Figure 4.50)

Item	Description
IGMP:	Internet Group Management Protocol can either be enabled or disabled.

Figure 4.50 IGMP Configuration

4.1.1.2.5 LACP

Select the "LACP ". The menu below includes the sub-menus of **Working Ports Setting**, **State Activity** and **LACP Status**. The LACP(Link Aggregation Control Protocol) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. In conclusion, Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode**, more detail information refers to IEEE802.3ad. (Figure 4.51)

Figure 4.51 LACP Configuration

4.1.1.2.5.1 Working Ports Setting

Configure LACP group. (Figure 4.52)

Figure 4.52 LACP Group Configuration

4.1.1.2.5.2 State Activity

Configure the LACP port state activity. (Figure 4.53)

Item	Description
Port:	Shows the port number of NVF-2400S VDSL IP DSLAM.
State Activity:	State Activity for LACP can either be active or passive.

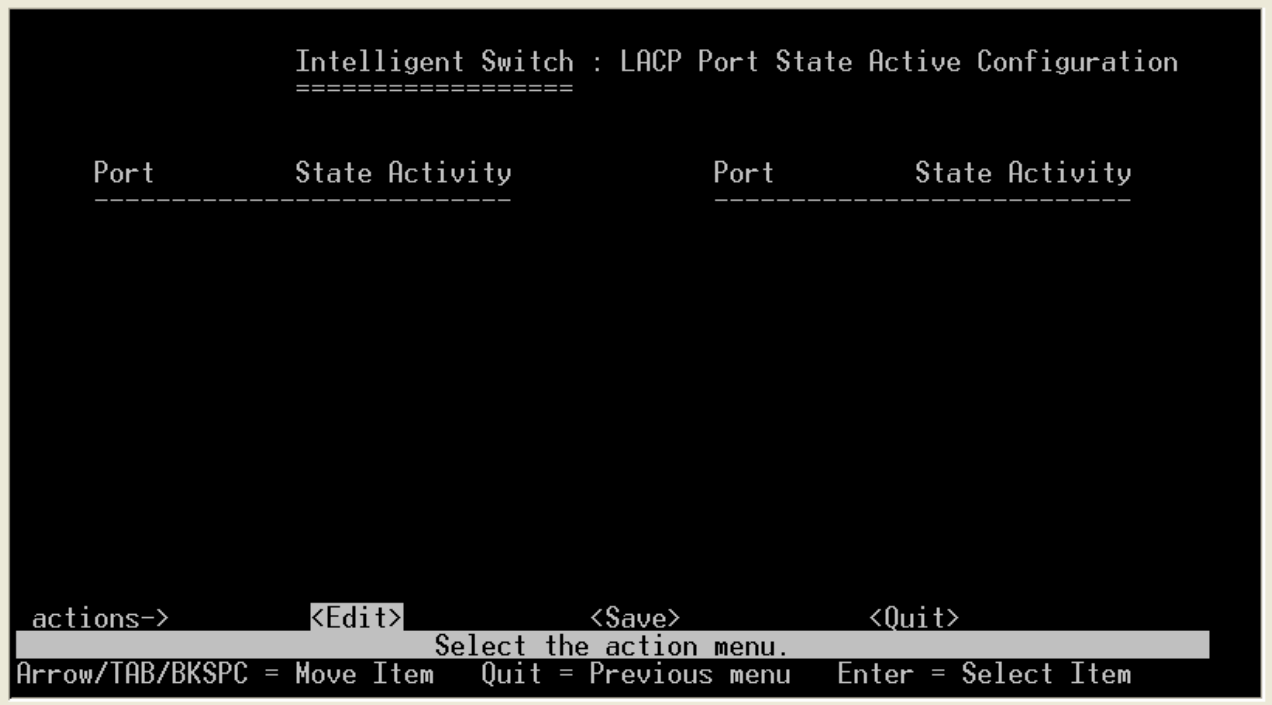


Figure 4.53 LACP Port State Active Configuration

4.1.1.2.5.3 LACP Status

Show the LACP group status. This page is no group active. LACP don't working. (Figure 4.54)

Figure 4.54 LACP Group Status

4.1.1.2.6 802.1X

Select the "802.1x protocol". The menu below includes the sub-menus of **System**, **PerPort** and **Misc**. Please configure the 802.1x(port access control protocol) items as follows. (Figure 4.55)

Figure 4.55 802.1x protocols

4.1.1.2.6.1 802.1x Enable/Disable

Default 802.1x is disabled. (Figure 4.56)

Item	Description
802.1x:	802.1x protocol can either be enabled or disabled.

Figure 4.56 802.1x Enable/Disable

4.1.1.2.6.2 System Configuration

Configure 802.1x system information. (Figure 4.57)

Item	Description
Radius Server IP:	Shows and configure the IP of your radius server.
Shared Key:	Shows and configure the values of your shared key.
NAS.Identifier:	Shows and configure the values of your NAS(Network Attached Storage) ID.
Server Port:	Shows and configure the values of your server port. Default port is 1812.
Accounting Port:	Shows and configure the values of your accounting port. Default port is 1813.

Figure 4.57 802.1x System Configuration

4.1.1.2.6.3 PerPort Configuration

Configure the per port information. Default port status is **No**. (Figure 4.58)

Item	Description
Port Status:	Port status can be either Force Unauth=Fu, Force Auth=Fa, Auto=Au, and None=No.

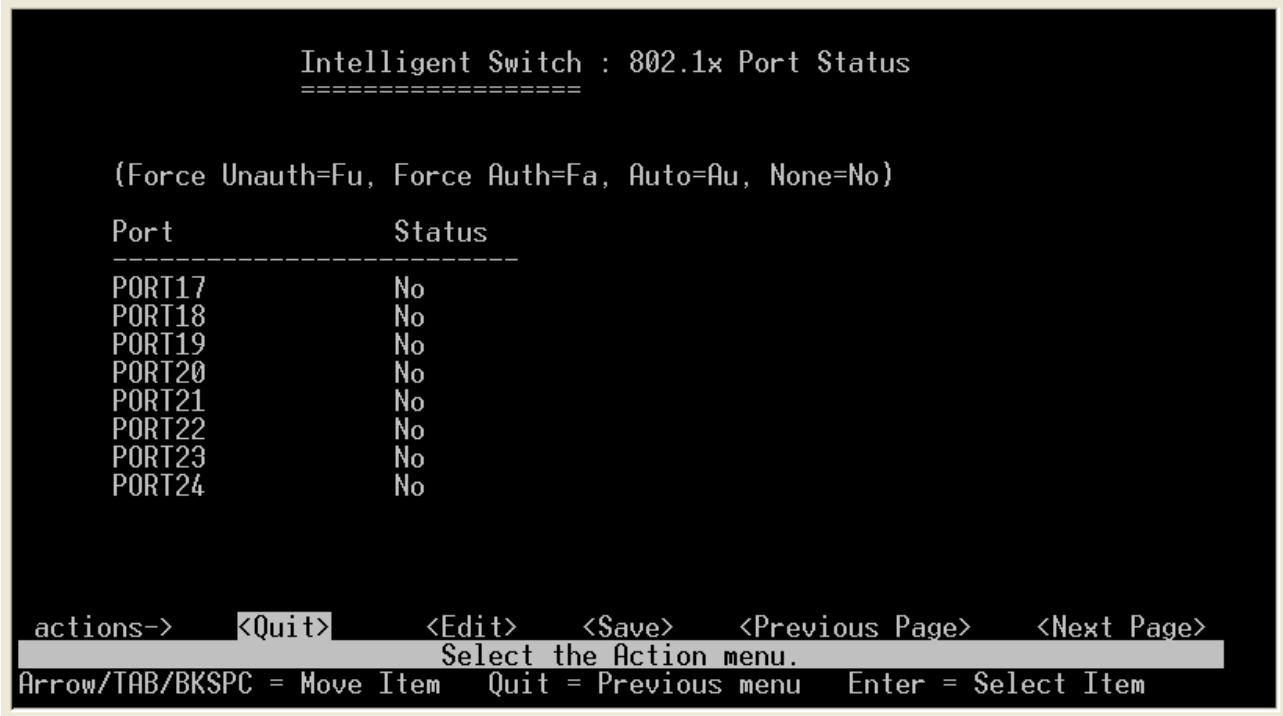


Figure 4.58 Port Configuration

4.1.1.2.6.4 Misc Configuration

Configure the 802.1x miscellaneous information. (Figure 4.59)

Item	Description
Quiet-period:	Quiet period is from 0 to 65535. Default value is **60**.
Tx-period:	Transmit period is from 0 to 65535. Default value is **30**.
Suppliant-timeout:	Suppliant timeout valid range is from 1 to 300. Default value is **30**.
Server-timeout:	Server timeout valid range is from 1 to 300. Default value is **30**.
ReAuthMax:	Reauthorization maximum valid range is from 1 to 10. Default value is **2**.
Reauth-period:	Reauthorization period is from 1 to 9999999. Default value is **3600**.

Figure 4.59 802.1x Misc Configuration

4.1.1.3 Status and Counters

Select the "Status and Counters". The menu below includes the sub-menus of **Port Status**, **Port Counters**, **System Information** and **Main Menu**. (Figure 4.60)

Figure 4.60 Status and Counters

4.1.1.3.1 Port Status

Display current status of all the switch ports. (Figure 4.61)

Item	Description
Port:	Shows the port number of NVF-2400S VDSL IP DSLAM.
Link Status:	Shows the status of the link.
InRate & OutRate:	Shows the ingress and egress rate at 100K step size. (e.g. 250 x 100K = 25Mbps)
Enable:	Shows if the port is active or not.
SNR:	Shows the SNR (Signal to Noise Ratio) of the port
Spd/Dpx:	Shows at what mode is the port set. It can be Auto, 5M, 15M and 25Mbps.

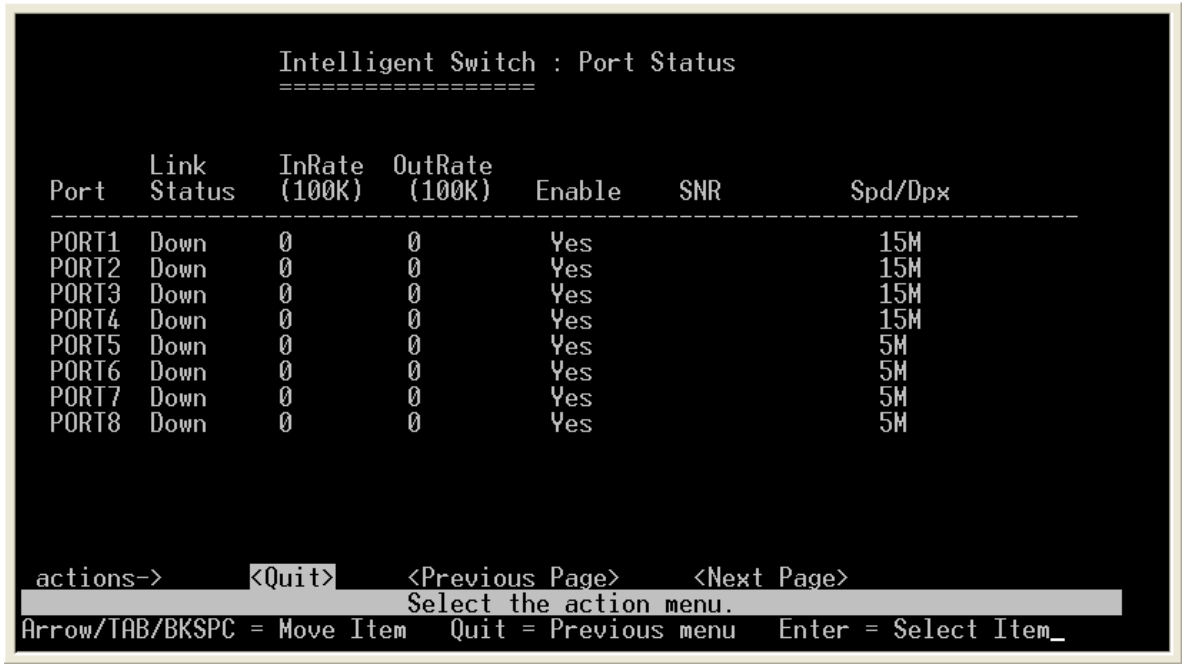


Figure 4.61 Port Stauts

4.1.1.3.2 Port Counters

Display a summary of network activity. (Figure 4.62)

Item	Description
Port:	Shows the port number of NVF-2400S VDSL IP DSLAM.
TxGoodPkt and RxGoodPkt:	Shows the values of good packets transmitted and received.
TxBadPkt and RxBadPkt:	Shows the values of bad packets transmitted and received.
TxAbort:	Shows the values of the aborted packets being transmitted.
Collision:	Shows the values of the collided packets.
DropPkt:	Shows the values of packet being drop.

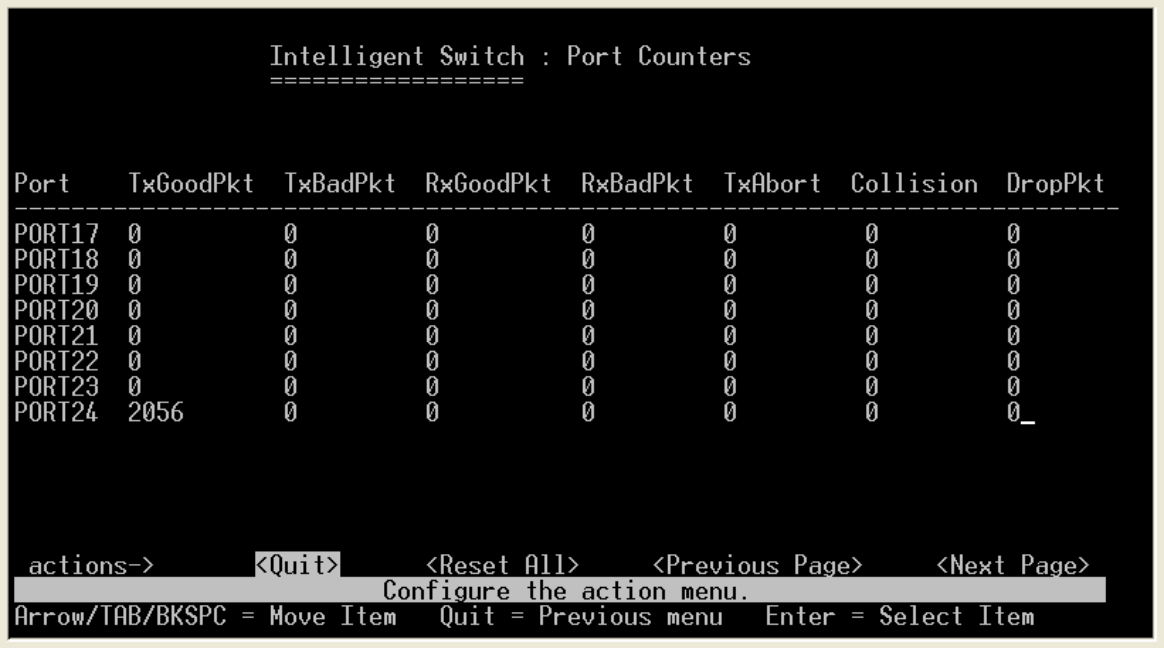


Figure 4.62 Port Counters

4.1.1.3.3 System Information

Display the switch system. (Figure 4.63)

Item	Description
MAC Address:	Shows the unique MAC address of the device.
Firmware version:	Shows the firmware version being used by the device.
PCBA version:	Shows the PCBA version being used by the device.
Default configuration value version:	Shows the version of the default configuration being used.

Figure 4.63 System Information

4.1.1.4 Temperature & Fan Monitor

Display temperature is degrees Celsius(℃) and fan monitor in RPM. (Figure 4.64)

Figure 4.64 Temperature & FAN Monitor

4.1.1.5 Reboot System

Select the "Restart ". The menu below includes the sub-menus of **Default** and **Restart**. (Figure 4.65)

Figure 4.65 Restart Configuration

4.1.1.5.1 Default

Recovering to default. (Figure 4.66)

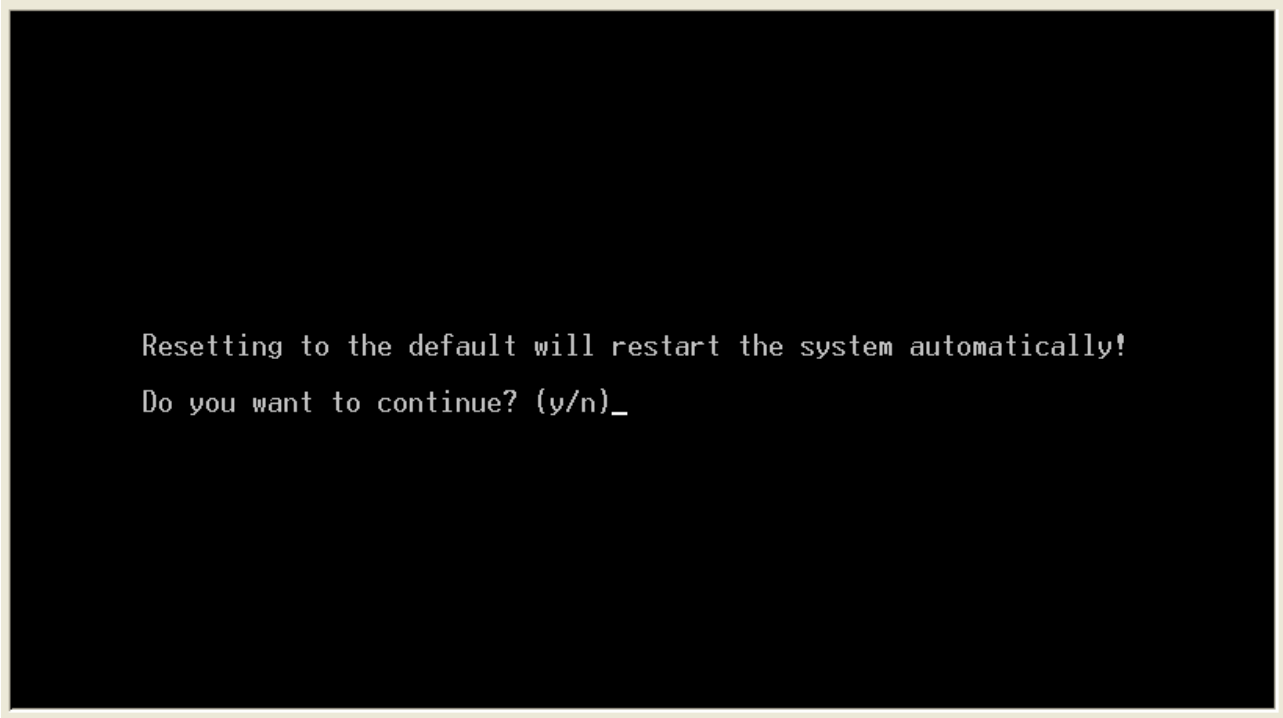


Figure 4.66 Resetting to the default system

Caution:

1. All settings will return to factory defaults.
2. After set to default system, please reboot the system.

Choose "**Yes**"

Reset the system to default automatically. (Figure 4.67)

If you choose "No", it will go back to previous menu.

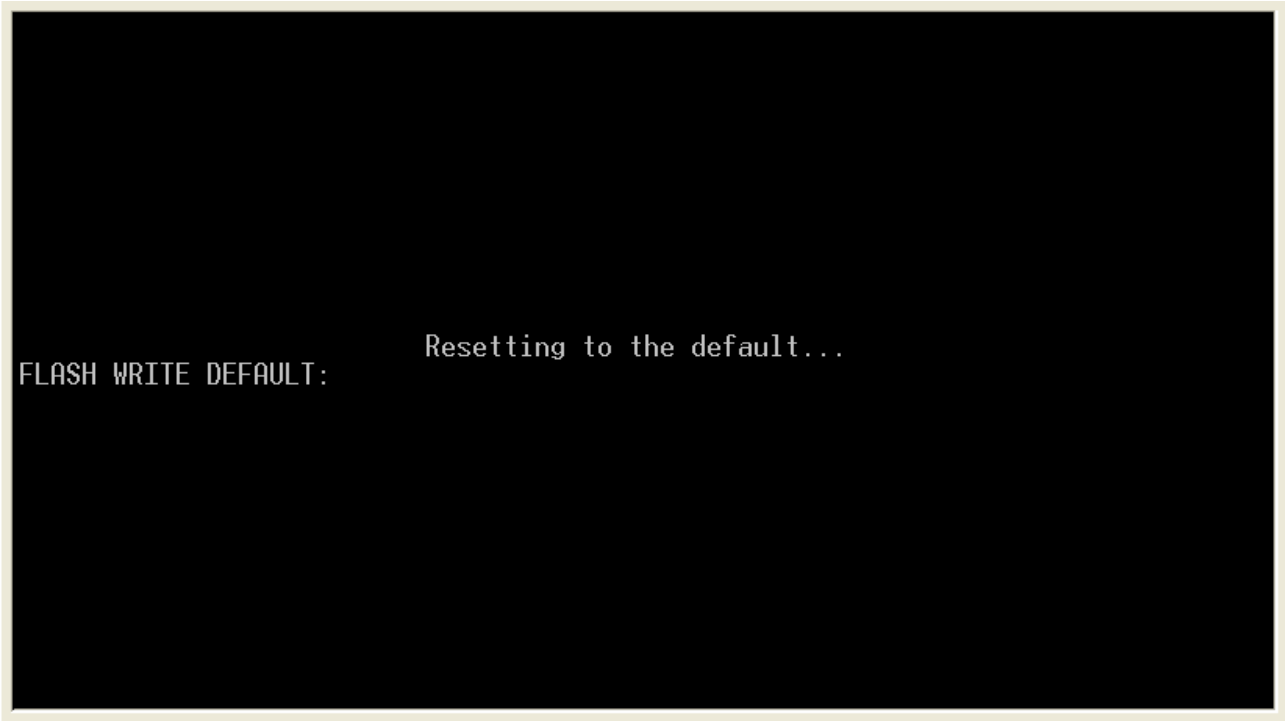


Figure 4.67 Resetting to the default

4.1.1.5.2 Restart

Restart the system. (Figure 4.68)

Figure 4.68 Restart the system

4.1.1.6 TFTP Update Firmware

Select the "TFTP Update firmware Configuration ". The menu below includes the sub-menus of **TFTP Update Firmware**, **TFTP Restore** and **TFTP Backup**. (Figure 4.69)

Figure 4.69 TFTP Update firmware Configuration

4.1.1.6.1 TFTP Update Firmware

Use TFTP to update firmware. (Figure 4.70)

Item	Description
TFTP Server:	Input the IP address of the TFTP server, it is usually the IP address of the PC with TFTP server installed.
Remote File Name:	Input the file name of the firmware.

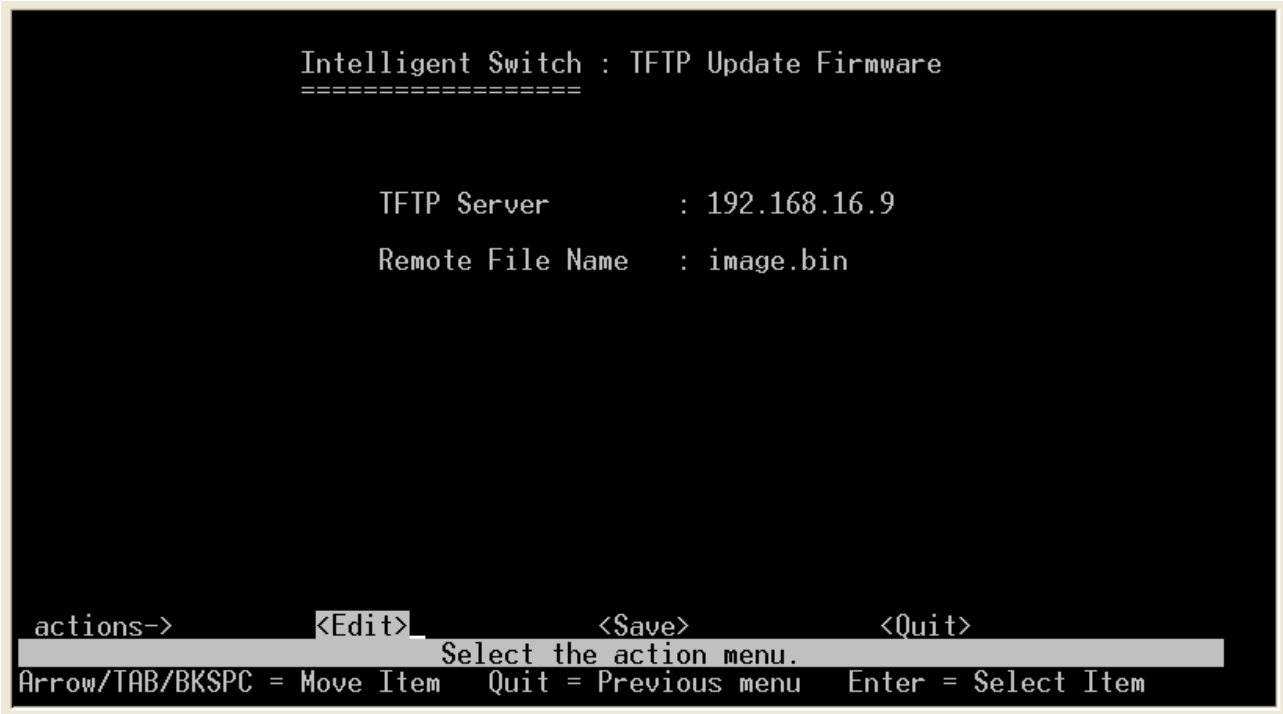


Figure 4.70 TFTP Update Firmware

4.1.1.6.2 TFTP Restore Configuration

Use TFTP to update new configuration file to NVF-2400S. (Figure 4.71)

Item	Description
TFTP Server:	Input the IP address of the TFTP server, it is usually the IP address of the PC with TFTP server installed.
Remote File Name:	Input the file name of the configuration file.

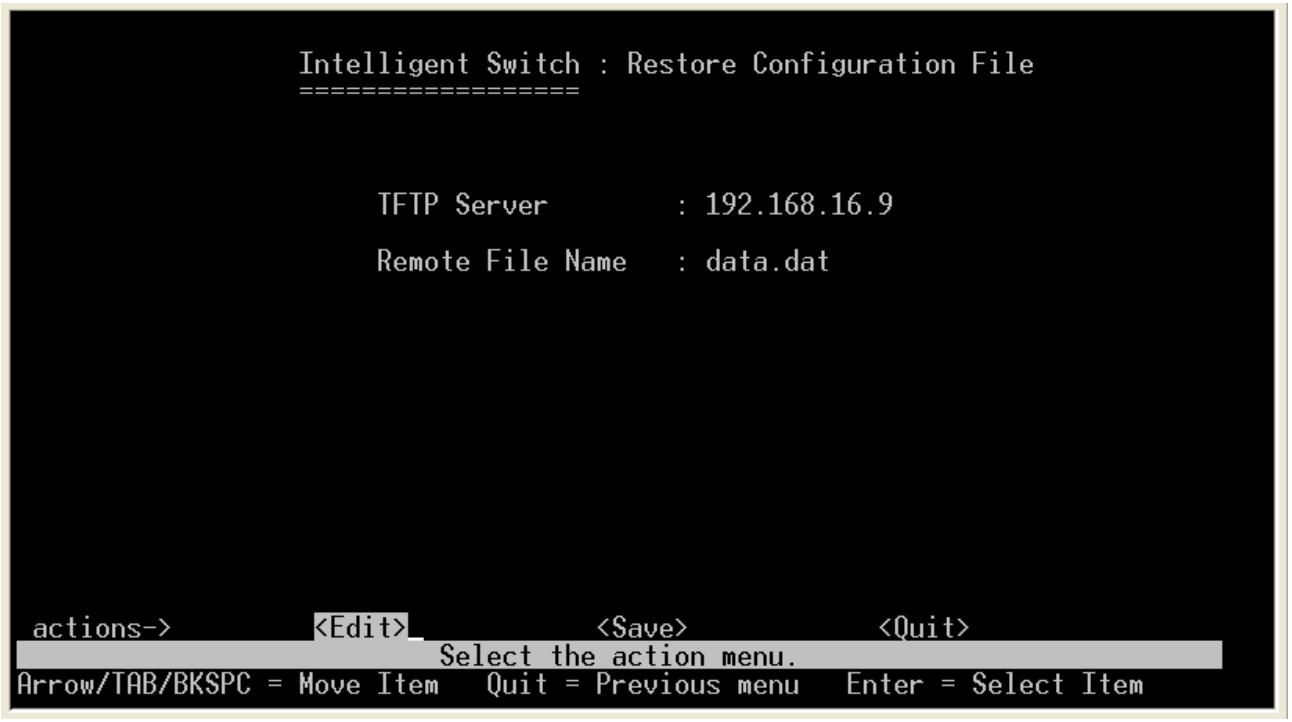


Figure 4.71 Restore Configuration

4.1.1.6.3 TFTP Backup Configuration

Use TFTP to backup the configuration of NVF-2400S into a configuration file. (Figure 4.72)

Item	Description
TFTP Server:	Input the IP address of the TFTP server, it is usually the IP address of the PC with TFTP server installed.
Remote File Name:	Input the file name of the configuration file.

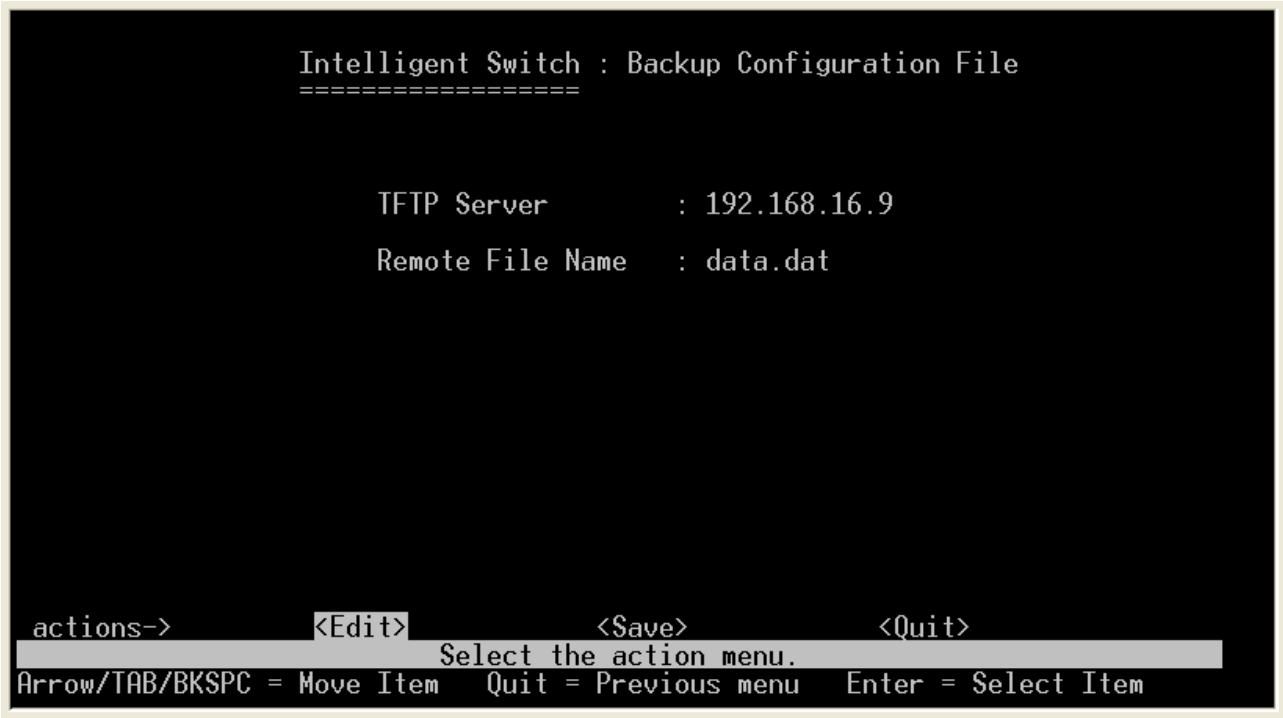


Figure 4.72 TFTP Backup Configuration

4.1.1.7 Logout

Exit this user interface program. (Figure 4.73)

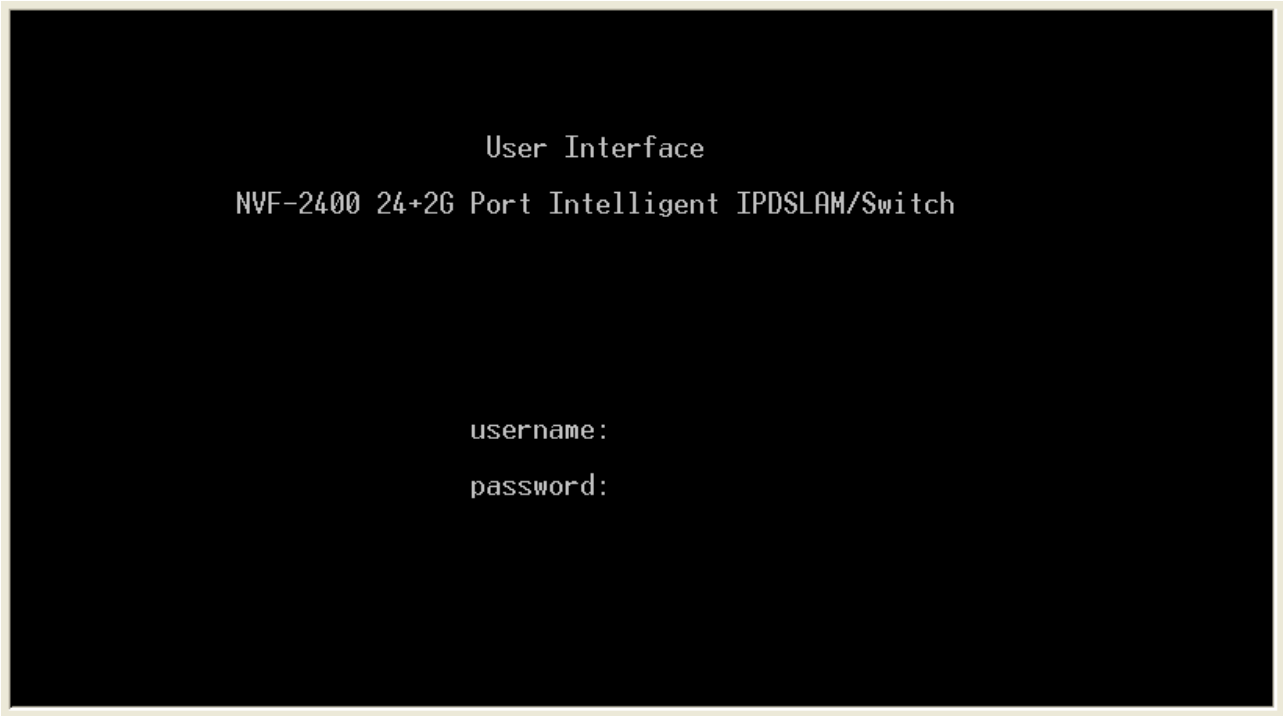


Figure 4.73 Logout

4.2 Remote Network Management

4.2.1 IP Setting

It must assign an IP for NVF-2400S via the console port (RS-232 Port) before users configure NVF-2400S via **Telnet** and **Web.** Or users can modify the PC/Laptop's IP domain same as the VDSL IP DSLAM and use the manufacturer default IP to configure NVF-2400S.

1. Remote control by "Telnet"

To enter Telnet, type the IP address of the VDSL switch to connect management system. And type user name and password.

Default User Name: **admin**
Default Password: **123**

Note:

1. For the security reason, the device limits the numbers of user login via Telnet and Console port. User can't login the device via Telnet and Console port at the same time.
User must log-out to leave after finish configures the device via Consol port, or the user can't login via Telnet.

2. WEB management doesn't limit the numbers of user login.

2. Network control by "WEB"

The NVF-2400S provides WEB UI to manage the device. The default configurations are as follows:

Default IP Address: **192.168.16.250**
Subnet Mask: **255.255.255.0**
Default Gateway: **192.168.16.1**
User Name: **admin**
Password: **123**

User can modify the IP Configuration instead of the manufacturer default settings via Console port before login the IP DSLAM via WEB UI. User can use the Default IP Address or User's defining IP Address get into the Web UI, and it will ask for user name and password as above. (Figure 4.74)

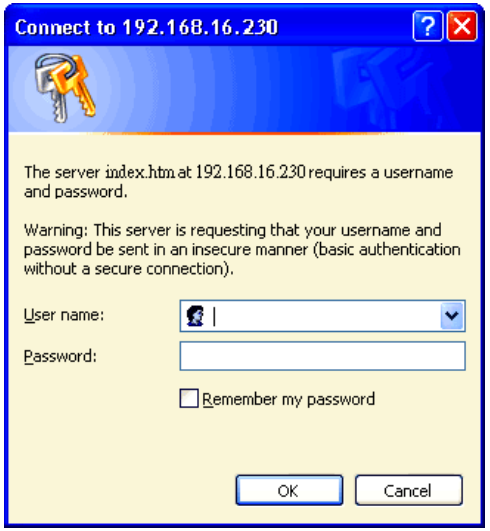


Figure 4.74 Username and Password

4.3 Web Basic Management

4.3.1 Port Status

This page can see every port status that depended on user setting and the negotiation result. (Figure 4.75)

Item	Description
State:	Display port status disable or enable. "Unlink" will be treated as "off".
Link:	Down is "No Link", UP is "Link".
SNR:	The SNR(Signal to Noise Ratio) can use as an indication of the quality of the Link. If SNR Value>25, it means connection in Good Link status.
Speed:	Ports 1-24 are 5/15/25Mbps VDSL, Ports 25-26 are 10/100/1000Mbps.
Duplex:	Display full-duplex or half-duplex mode.
Flow Control:	**Full:** Display the flow control status is "enable" or "disable" in full mode. **Half:** Display the backpressure is "enable" or "disable" in half mode
Rate Control:	Display the rate control setting. **Ingr:** Display the Port effective ingress rate of user setting. **Egr:** Display the Port effective egress rate of user setting.

Port Status

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

Port		State		Link	SNR(db)	Speed		Duplex		Flow Control			Rate Control(100K)		Priority	Security
										Config		State	State			
Id	Location	Config	State			Config	State	Config	State	Full	Half		Ingr	Egr		
1	0	On	On	Down	NoLink	25M	5M	Full	Full	On	On	On	Off	Off	Disable	Off
2	0	On	On	Down	NoLink	25M	5M	Full	Full	On	On	On	Off	Off	Disable	Off
3	0	On	On	Down	NoLink	25M	5M	Full	Full	On	On	On	Off	Off	Disable	Off

Figure 4.75 Port Status

4.3.2 Port Statistics

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

Press "Reset" button to clean all counts. (Figure 4.76)

Port Statistics

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

Port	Location	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
1	0	On	Down	0	0	0	0	0	0	0
2	0	On	Down	0	0	0	0	0	0	0
3	0	On	Down	0	0	0	0	0	0	0
4	0	On	Down	0	0	0	0	0	0	0
5	0	On	Up	14487	0	0	0	0	0	0
6	0	On	Down	0	0	0	0	0	0	0
7	0	On	Up	14481	0	0	0	0	0	0
8	0	On	Up	14485	0	0	0	0	0	0
9	0	On	Up	14317	0	0	0	0	0	0
10	0	On	Down	0	0	0	0	0	0	0
11	0	On	Up	14478	0	0	0	0	0	0
12	0	On	Up	14483	0	0	0	0	0	0
13	0	On	Down	0	0	0	0	0	0	0
14	0	On	Down	0	0	0	0	0	0	0
15	0	On	Down	0	0	0	0	0	0	0
16	0	On	Down	0	0	0	0	0	0	0
17	0	On	Down	0	0	0	0	0	0	0

Reset

Figure 4.76 Port Statistics

4.3.3 TFTP Update

The following menu functions allow user update the firmware and remote boot device: (Figure 4.77)

1. Install TFTP Server and execute afterwards.
2. Copy firmware update version image.bin to TFTP Server directory.
3. In web management select administrator—TFTP update firmware.
4. Download new image.bin file then in web management press <update firmware>.
5. After update finished, press <reboot> to restart switch.

Figure 4.77 TFTP Update

4.3.4 TFTP Backup

TFTP Restore Configuration

Use this function to set TFTP server address. User can restore EEPROM value from here, but before the IP DSLAM restore the flash image file, the image file must store in TFTP server. (Figure 4.78)

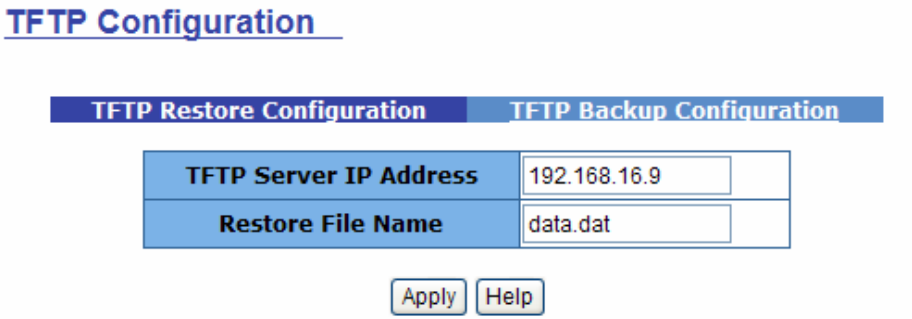


Figure 4.78 TFTP Restore Configuration

TFTP Backup Configuration

Use this function to set TFTP server IP address. User can save current EEPROM value from here, then go to the TFTP restore configuration page to restore the EEPROM value. (Figure 4.79)

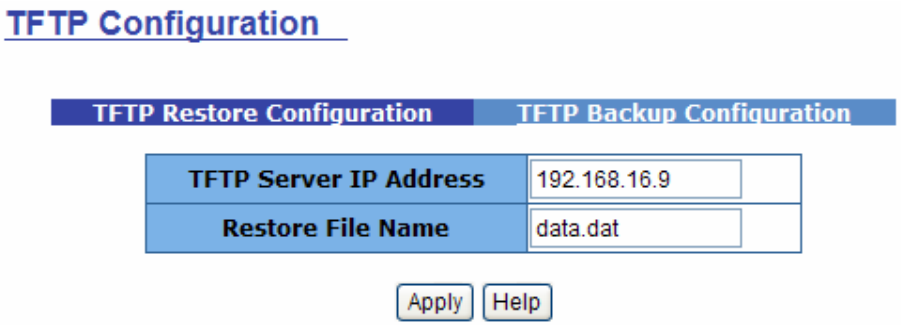


Figure 4.79 TFTP Backup Configuration

4.4 Web Administrator Management

4.4.1 IP Address

1. User can configure the IP Settings and fill the new values in here. (Figure 4.80)

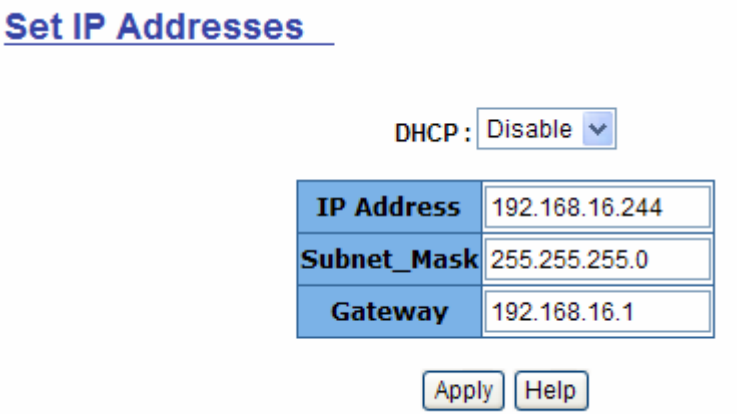


Figure 4.80 IP Address

4.4.2 Switch Settings

Basic: (Figure 4.81)

Item	Description
Description:	Display the name of device type.
MAC Address:	The unique hardware address assigned by manufacturer (default)
Firmware Version:	Display the device's Firmware version.
Hardware version:	Display the device's Hardware version.
Default config value version:	Display write to default EEPROM value table version.

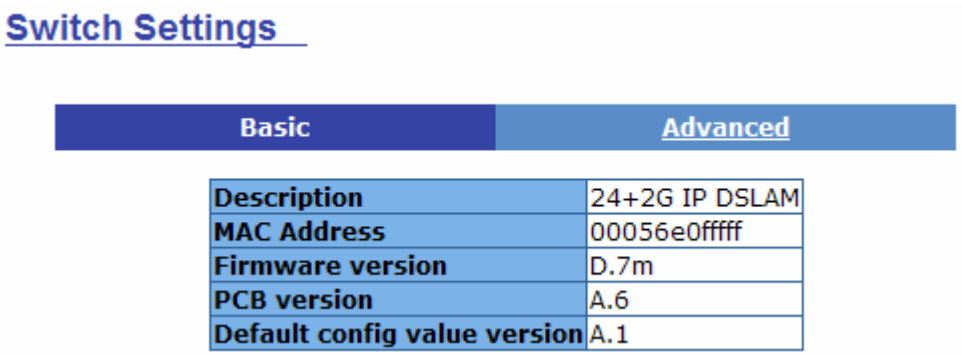


Figure 4.81 Switch Settings - Basic

Advanced(Miscellaneous Settings): (Figure 4.82)

Item	Description
Mac Address Age-out Time:	Setting the time for inactive MAC address remains in the Switch's address table.
Max bridge transit delay bound control:	Limit the packets queuing time in IP DSLAM. If this function is enable, the packets queued exceed will be dropped.
Broadcast Storm Filter:	To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active.

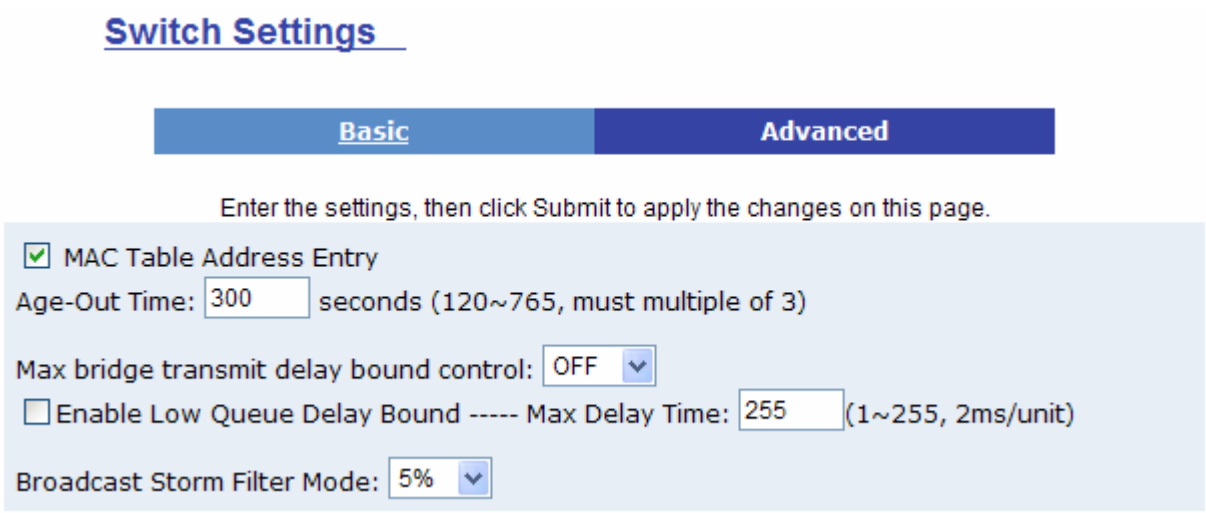


Figure 4.82 Switch Settings - Advanced

Priority Queue Service settings(Figure 4.83)

Item	Description
First Come First Service:	The sequence of packets sent is depend on arrive order.
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 high priority packets sent before one low priority packet is sent. For example, 5 High: 2 Low means that the switch sends 5 high priority packets before sending 2 low priority packets.
QoS Policy: High Priority Levels:	0~7 priority level can map to high or low queue.
Collisions Retry Forever:	Enable or Disable Collisions Retry Forever.
Hash Algorithm:	Select in CRC-Hash mode or Direct Map mode
802.1x Protocol:	Enable or disable 802.1x Protocol.

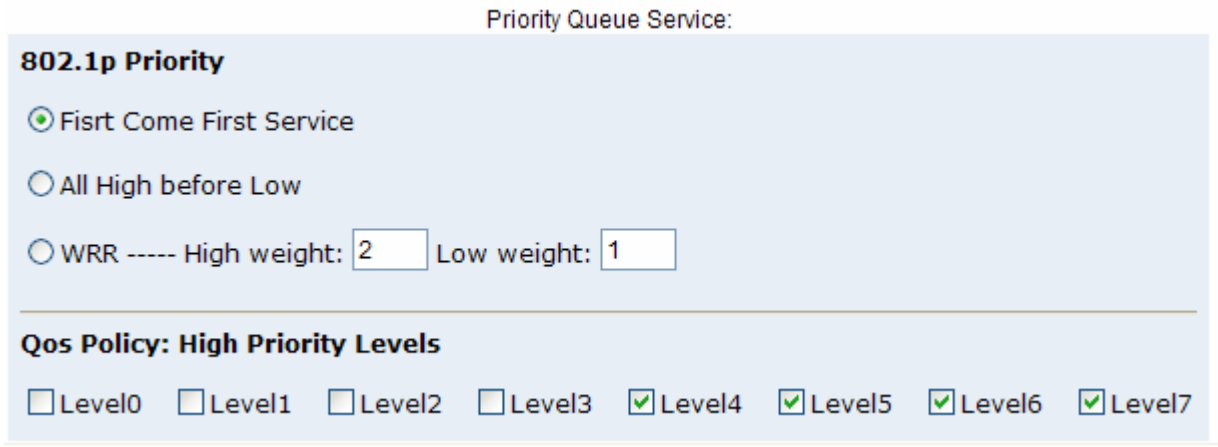


Figure 4.83 Priority Queue Service settings

4.4.3 Port Controls

This section shows you how to change every port status and speed mode. (Figure 4.84)

Item	Description
State:	User can disable or enable this port control.
Negotiation:	User can set auto negotiation mode is Auto, Force of per port, Nway (specify the speed/duplex on this port and enable auto-negotiation).
Speed:	User can set 5Mbps / 15Mbps / 25Mbps for port 1 ~ 24. 1000Mbps, 100Mbps or 10Mbps speed for Port25 ~ Port26.
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:	NVF-2400S, port 1 ~ port 24, supports by-port ingress and egress rate control. For example, assume Port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. IP DSLAM will be performed flow control or backpressure to confine the ingress rate to meet the specified rate.
	Ingress: The valid range is 0 ~ 100 (100 = 10Mbps). The unit is 100K. 0: disable rate control.
	Egress: The valid range is 0 ~ 100 (100 = 10Mbps). The unit is 100K. 0: disable rate control.

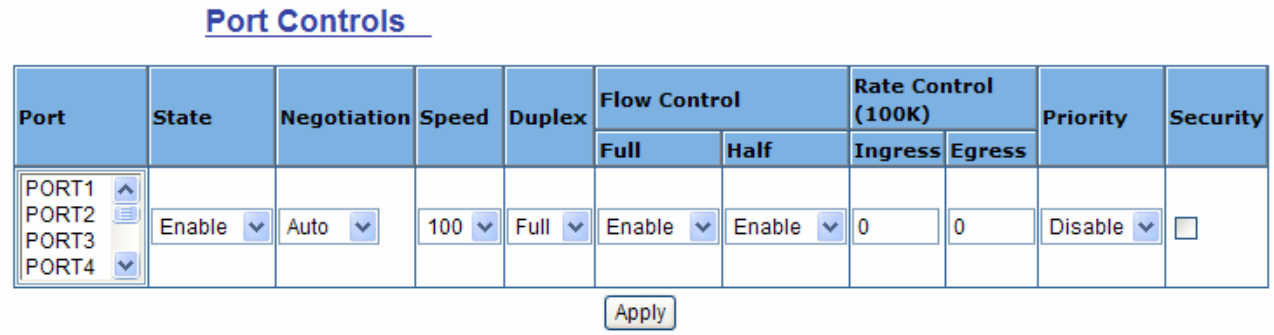


Figure 4.84 Port Controls

4.4.4 Trunking

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. In conclusion, Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refers to IEEE802.3ad. (Figure 4.85)

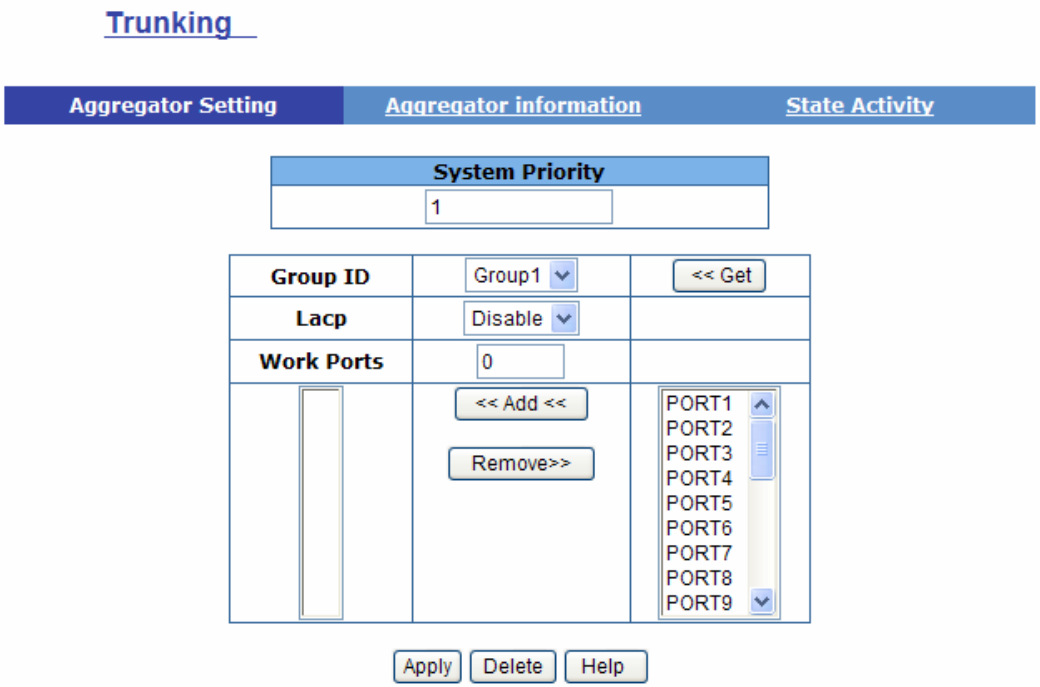


Figure 4.85 Trunking

AGGREGATOR SETTING

System Priority: A value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.

1. **Group ID:** There are seven trunk groups to provide configure. Choose the "group id" and click "Get".
2. **LACP:** If enable, the group is LACP static trunking group. If disable, the group is local static trunking group. All ports support LACP dynamic trunking group. If connecting to the device that also supports LACP, the LACP dynamic trunking group will be created automatically.
3. **Work ports:** Allow max four ports can be aggregated at the same time. If LACP static trunking group, the exceed ports is standby and able to aggregate if work ports fail. If local static trunking group, the number must be as same as the group member ports.
4. Select the ports to join the trunking group. Allow max four ports can be aggregated at the same time.
5. If LACP enable, you can configure LACP Active/Passive status in each ports on State Activity page.
6. Click Apply.

AGGREGATOR INFORMATION

When you are setting LACP aggregator, you can see relation information in here. (Figure 4.86)

1. This page is no group active. LACP don't working.

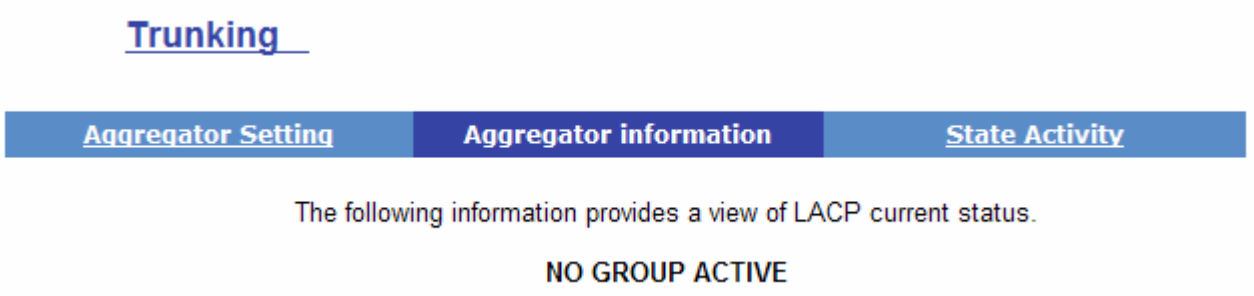


Figure 4.86 Aggregator Information

2. This page is Static Trunking group. (Figure 4.87)

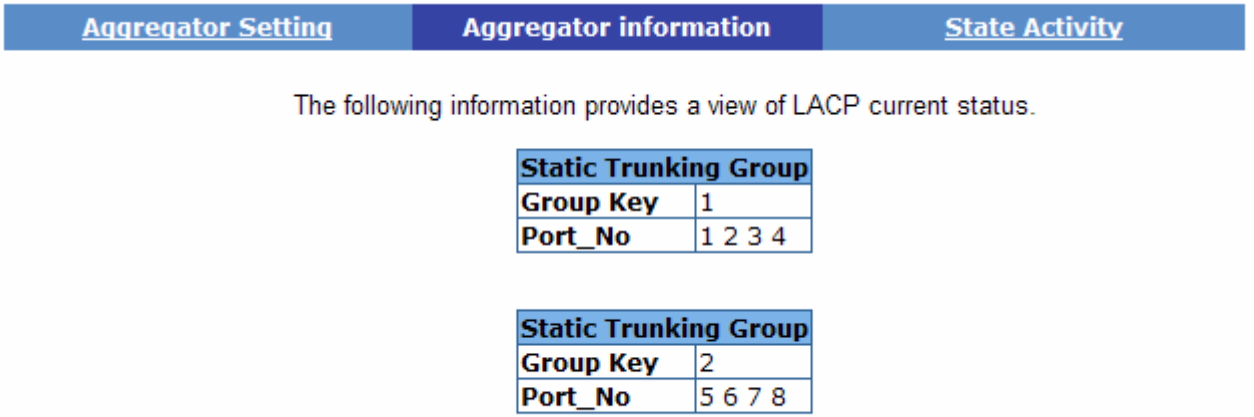


Figure 4.87 Static Trunking group

State Activity(Figure 4.88)

Active (select): The port automatically sends LACP protocol packets.

Passive (no select): The port does not automatically sends LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

1. A link having either two active LACP ports or one active port can perform dynamic LACP trunking. A link has two passive LACP ports will not perform dynamic LACP trunking because both ports are waiting for and LACP protocol packet from the opposite device.
2. If you are active LACP's actor, when you are select trunking port, the active status will be created automatically.

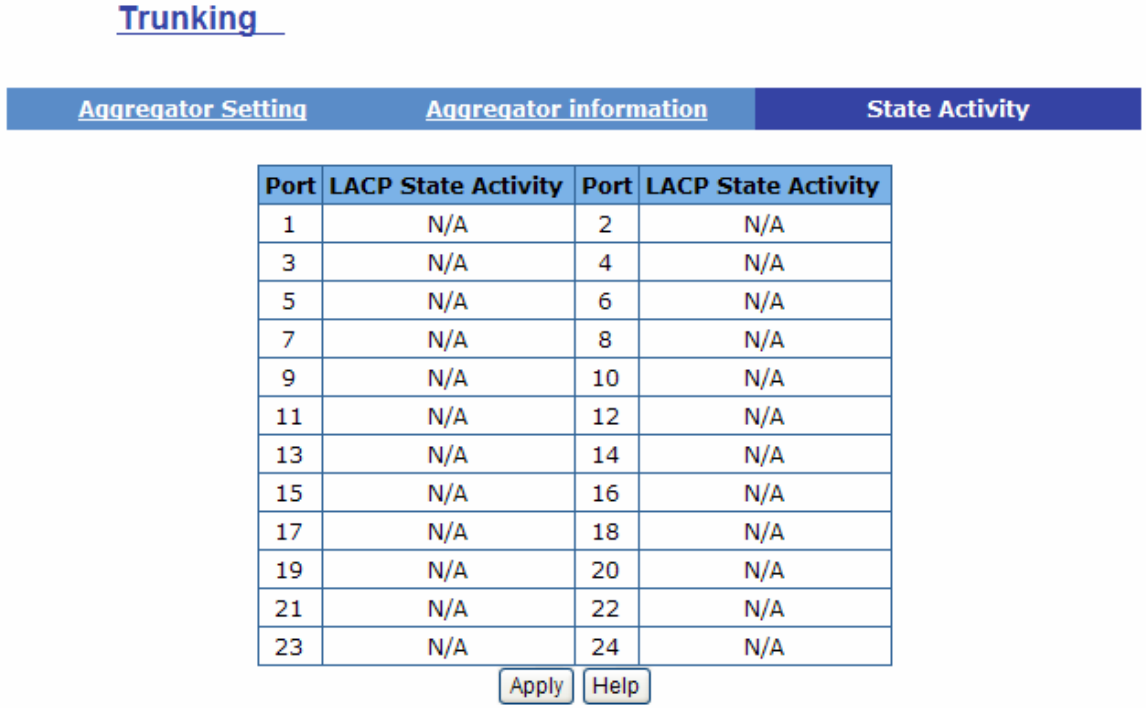


Figure 4.88 State Activity

4.4.5 Filter Database

IGMP Snooping(Figure 4.89)

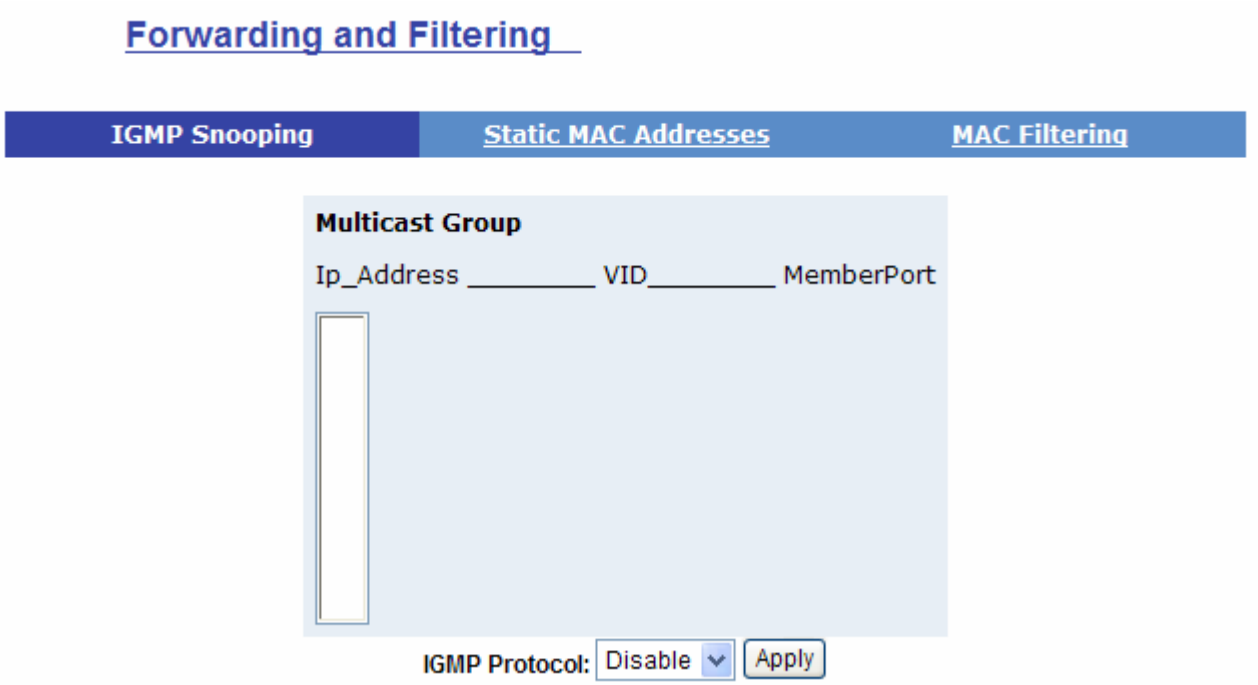


Figure 4.89 IGMP Snooping

The NVF-2400S supports IP multicast, you 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.

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 carrier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the carrier 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 carrier to indicate that the host has quit being a member of a specific multicast group.

Static MAC Addresses

New entry of static address can be added and list can be defined to the address table. (Figure 4.90)

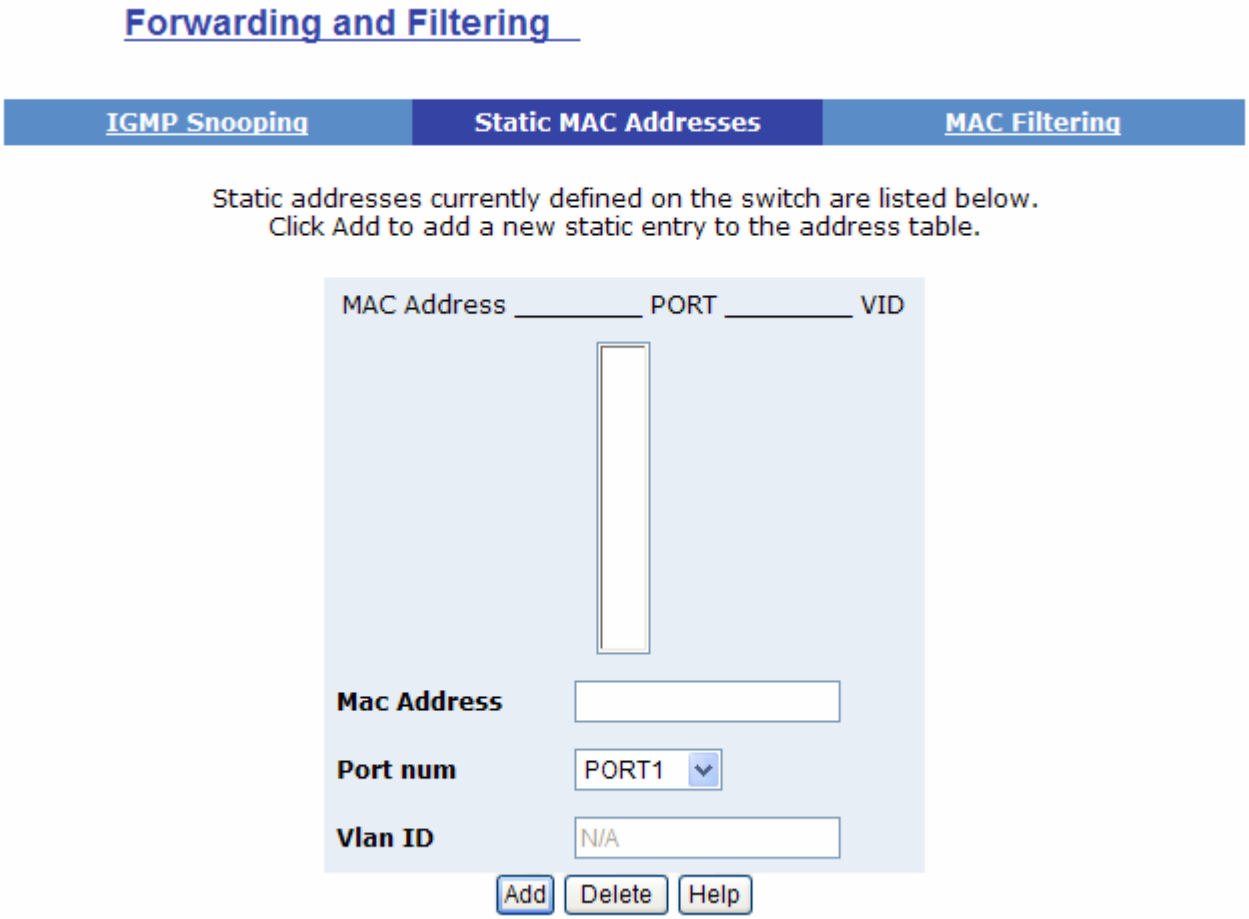


Figure 4.90 Static MAC Addresses

MAC filtering

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. (Figure 4.91)

Figure 4.91 MAC filtering

1. In the MAC Address box, enter the MAC address that wants to filter.
2. If tag-based (802.1Q) VLAN are set up on the switch, in the VLAN ID box, type the VID to associate with the MAC address.
3. Click the Add.
4. Choose the MAC address that you want to delete and then click the Delete.

4.4.6 VLAN Config

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. (Figure 4.92)

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.

The VDSL IP DSLAM support port-based VLAN and 802.1Q (tagged-based) VLAN in web management page.

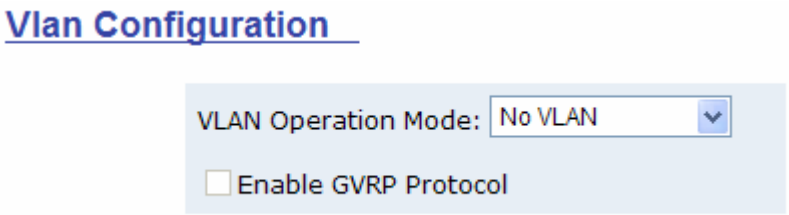


Figure 4.92 VLAN Config

NOTE:

The device may need 50 seconds for changing VLAN Operation Mode from No VLAN to 802.1Q.
It is necessary to reboot the IP DSLAM for valid value after the VLAN mode changed every time.

Port-based VLAN

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. (Figure 4.93)

Figure 4.93 VLAN connection diagram

Create a new VLAN group:

1. Click Add to create a new VLAN group. (Figure 4.94)
2. Enter the VLAN name, group ID and select the members for the new VLAN, then click Apply.
3. If the VLAN groups over the page's limitation, user can use "Next Page" to view other VLAN groups.

Note:

If the trunk groups exist, it (ex: TRK1, TRK2…) will show in select menu of ports, and user can set it in the member of the VLAN or not.

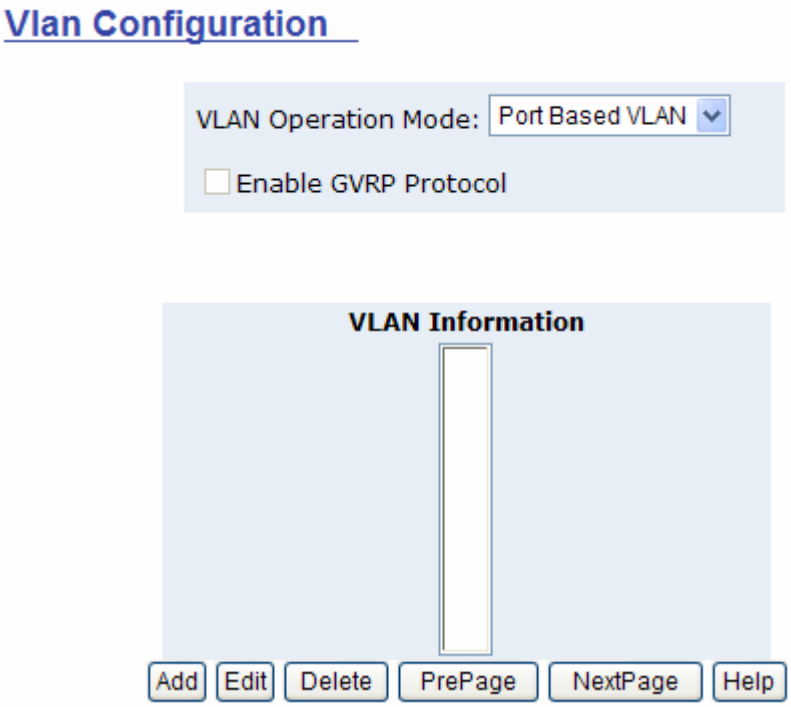


Figure 4.94 VLAN Configuration

Tag-based VLAN (IEEE 802.1Q VLAN) (Figure 4.95)

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

In order to an end station to send packets to different VLANs, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

Figure 4.95 VLAN connection diagram

802.1Q VLAN(Figure 4.96)

This page, user can create Tag-based VLAN, and enable or disable GVRP protocol.

There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. **The default VLAN can't be deleted.**

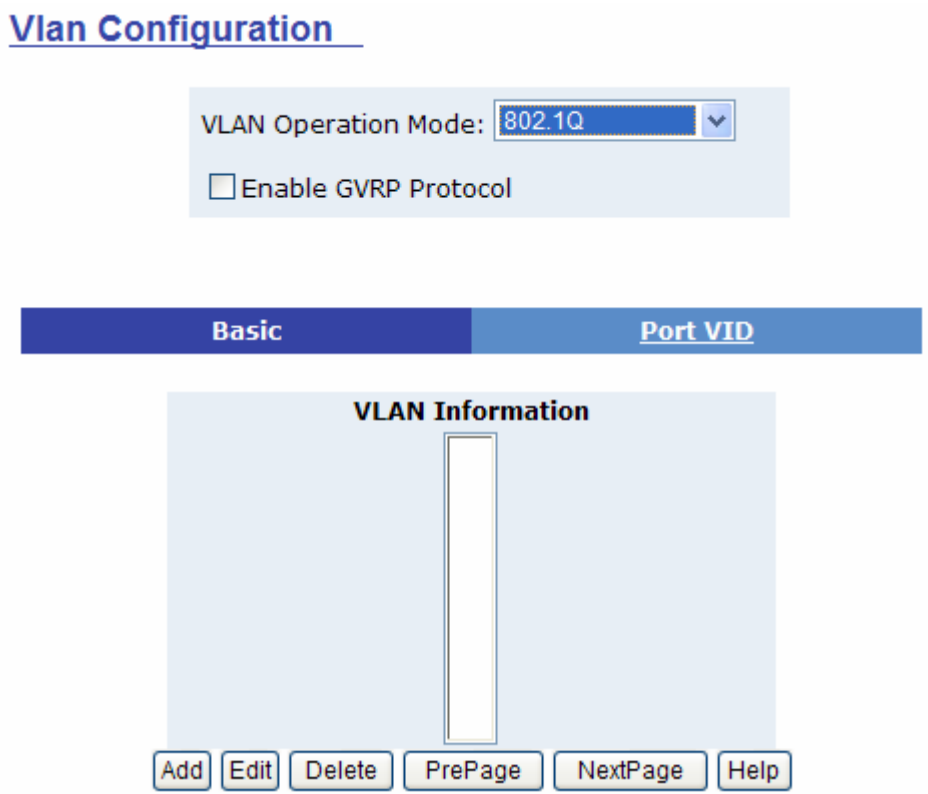


Figure 4.96 802.1Q VLAN Mode

GVRP (GARP [Generic Attribute Registration Protocol] VLAN Registration Protocol)

GVRP allows automatic VLAN configuration between the switch and nodes. If the NVF-2400S is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the NVF-2400S, the NVF-2400S will automatically add that device to the existing VLAN.

Port VID (PVID)

Set the port VLAN ID that 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. VDSL SWITCH each port allows user to set one PVID, 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. (Figure 4.97)

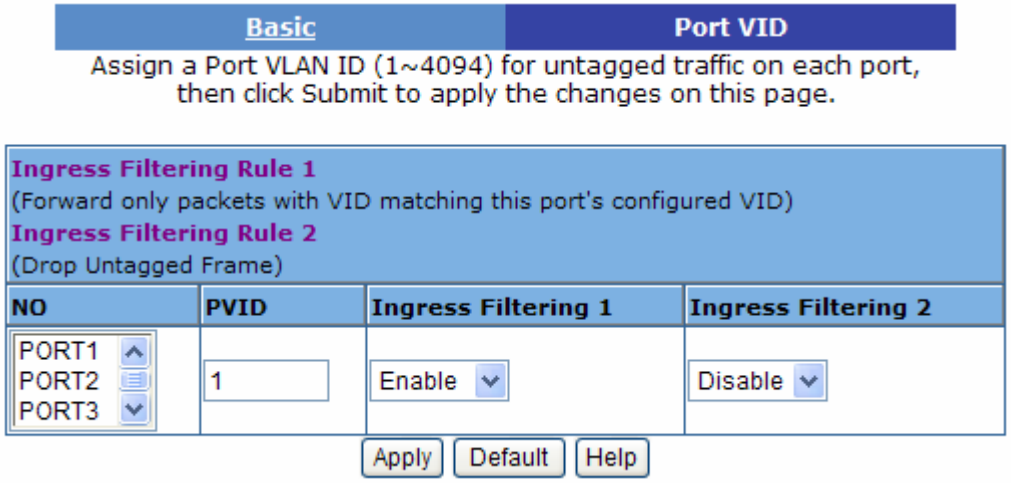


Figure 4.97 Port VID

The 24-ports VDSL IP DSLAM has 16 PVID ranges. PVID of Port 1 ~ Port 26 must be in the same range.

Num.	PVID Range	Num.	PVID Range	Num.	PVID Range	Num.	PVID Range
1	1~255	5	1024~1279	9	2048~2303	13	3072~3327
2	256~511	6	1280~1535	10	2304~2559	14	3328~3583
3	512~767	7	1536~1791	11	2560~2815	15	3584~3839
4	768~1023	8	1792~2047	12	2816~3071	16	3840~4094

Ingress Filtering

Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN.

VDSL IP DSLAM has two ingress filtering rule as follows:

Item	Description
Ingress Filtering Rule 1:	Forward only packets with VID matching this port's configured VID.
Ingress Filtering Rule 2:	Drop Untagged Frame.

4.4.7 Spanning Tree

The Spanning-Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP enabled, to ensure that only one path at a time is active between any two nodes on the network.

You can enable Spanning-Tree Protocol on web management's switch setting advanced item, select enable Spanning-Tree protocol. We are recommended that you enable STP on all NVF-2400S to ensure a single active path on the network. (Figure 4.98)

You can view spanning tree information about the Root Bridge.

Root Bridge Information

Priority	32768
Mac Address	00056e002557
Root_Path_Cost	14
Root Port	PORT25
Max Age	20
Hello Time	2
Forward Delay	15

Figure 4.98 Root Bridge Information

You can view spanning tree status about the switch as the following screen. (Figure 4.99)

STP Port Status

PortNum	PathCost	Priority	PortState
PORT1	10	128	FORWARDING
PORT2	10	128	FORWARDING
PORT3	10	128	FORWARDING
PORT4	10	128	FORWARDING
PORT5	10	128	FORWARDING

Figure 4.99 STP Port status

You can set new value for STP parameter(Figure 4.100)

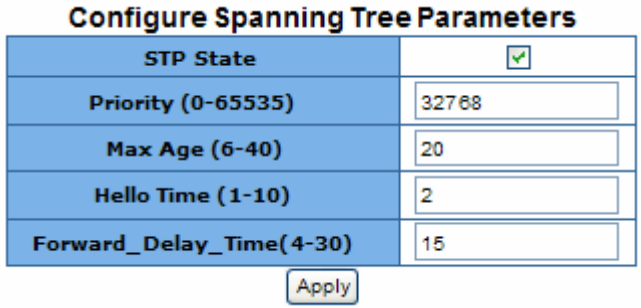


Figure 4.100 Configure STP parameters

Parameter	Description
Priority	You can change priority value, A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. Enter a number 1 through 65535.
Max Age	You can change Max Age value, The number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting a reconfiguration. Enter a number 6 through 40.
Hello Time	You can change Hello time value, the number of seconds between the transmissions of Spanning-Tree Protocol configuration messages. Enter a number 1 through 10.
Forward Delay time	You can change forward delay time, The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a number 4 through 30.

The following parameter can be configured on each port(Figure 4.101)

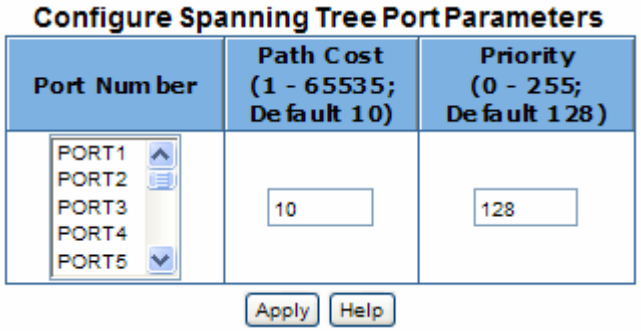


Figure 4.101 Configure STP port parameters

Parameter	Description
Port Priority	Define the priority of each port, the rage is from 0 to 255, the lower number has the higher priority. Default Value is 128.
Path Cost	Specifies the Path Cost of the port that switch uses to determine which port are the forwarding ports the lowest number is forwarding ports, the rage is from 1 to 65535 and default value base on IEEE802.1D 10Mb/s = 50-600 100Mb/s = 10-60 1000Mb/s = 3-10

4.4.8 Port Sniffer

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

Item	Description
Sniffer Mode:	Press Space key to set sniffer mode: Disable\Rx\Tx\Both.
Monitoring Port:	It means sniffer port can be used to see all monitor port traffic. You can connect sniffer port to LAN analyzer or netxray.
Monitored Port:	The ports you want to monitor. All monitor port traffic will be copied to sniffer port. You can select max 25 monitoring ports in the switch. User can choose which port wants to monitored in only one sniffer mode.

If you want to disable the function, you must select monitor port to none. (Figure 4.102)

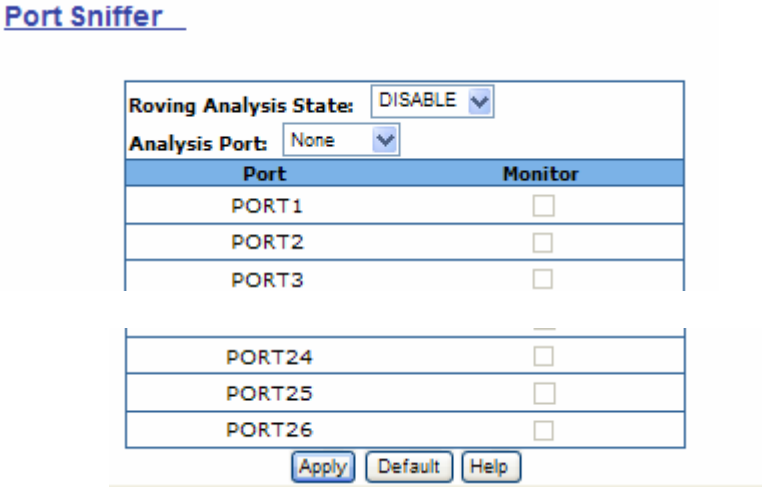


Figure 4.102 Port Sniffer

4.4.9 SNMP

Any Network Management 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 and agent.

1. 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. (Figure 4.103)

Item	Description
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.

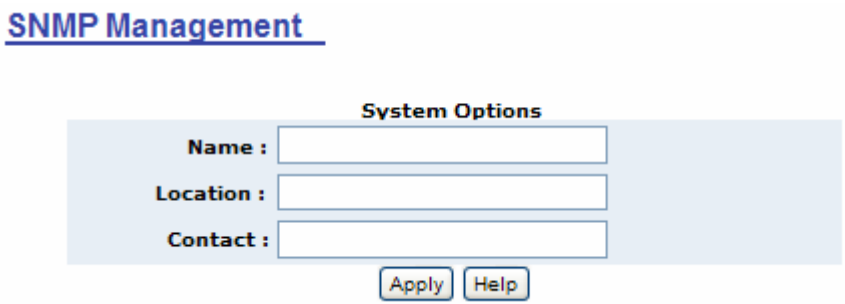


Figure 4.103 system options

2. Community strings serve as passwords and can be entered as one of the following:

Item	Description
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.

3. Trap Manager

A 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. (Figure 4.104)

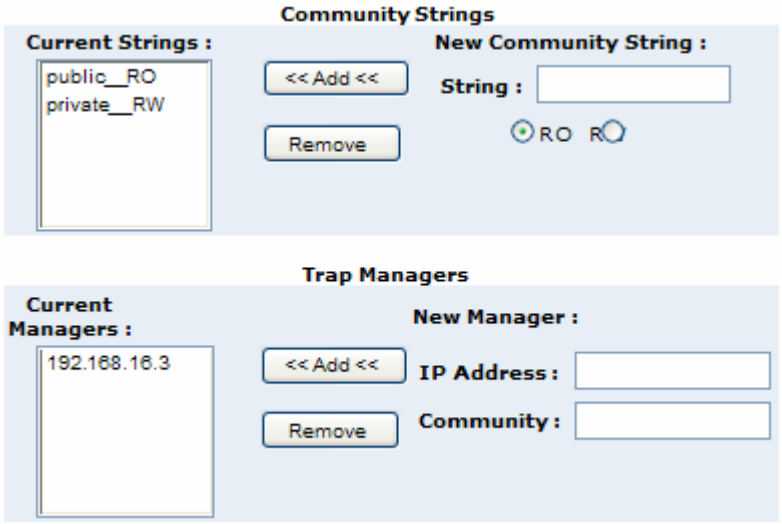


Figure 4.104 Community Strings and Trap Mangers

4.4.10 Security Manager

Using this page, user can change web management user name and password. (Figure 4.105)

Item	Description
User name:	Type the new user name.
Password:	Type the new password.
Reconfirm password:	Retype the new password.

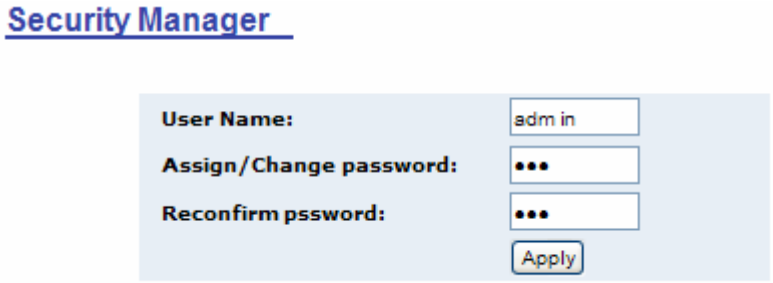


Figure 4.105 Security Manager

4.4.11 802.1X Config

System Configuration

802.1x makes using of the physical access characteristics of IEEE802 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.

To enable 802.1x, you still to fill in the authentication server information:

Item	Description
Radius Server IP Address:	The IP address of the authentication server.
Server Port:	The UDP port number used by the authentication server to authenticate.
Accounting Port:	The UDP port number used by the authentication server to retrieve accounting information.
Shared Key:	A key shared between this switch and authentication server.
NAS Identifier:	A string used to identify this switch.

Per port Configuration

In this page, you can select the specific port and configure the authorization state.

Each port can select four kinds of authorization state:

Item	Description
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.

Misc Configuration

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

Item	Description
Quiet Period:	used to define periods of time during which it will not attempt to acquire a supplicant (Default time is 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 is 30 seconds).
Server Timeout:	used to determine timeout conditions in the exchanges between the authenticator and authentication server (Default value is 30 seconds).
ReAuthMax:	used to determine the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (Default value is 2 times).
ReAuth Period:	used to determine a nonzero number of seconds between periodic re-authentication of the supplications (Default value is 3600 seconds).

4.4.12 Bridge Location

This function allows for the identification of the location of each Remote Bridge. In the text box to a port, type the location of the Remote Bridge for that port. The field is limited to alphanumeric characters and hyphen, and will accept a maximum 10 characters. (Figure 4.106)

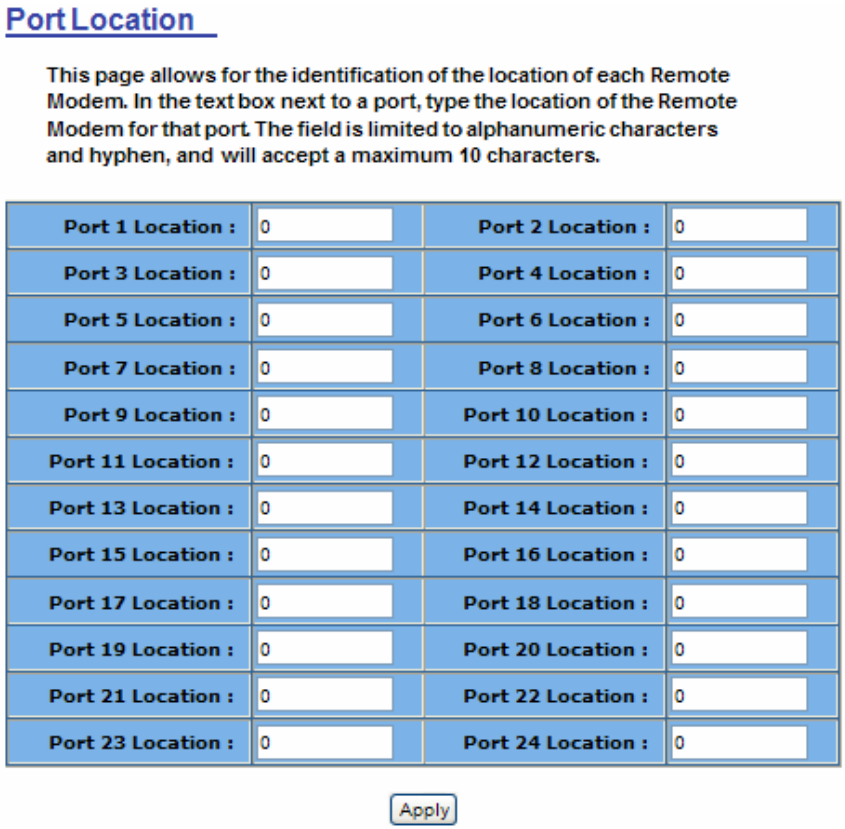


Figure 4.106 Port Location

4.4.13 Interleave

This function is used in digital data transmission technology to protect the transmission against noise issue and data error.

If during transit more than a certain amount of data has been lost then the data cannot be correctly decoded. Short bursts of noise on the line can cause these data packets to become corrupt and the bridge has to re-request data which in turn can slow down the overall rate at which data is transmitted.

Interleaving is a method of taking data packets, chopping them up into smaller bits and then rearranging them so that once contiguous data is now spaced further apart into a non continuous stream. Data packets are re-assembled by your bridge.

The diagram below is an example of how interleaved traffic is transmitted. (Figure 4.107)

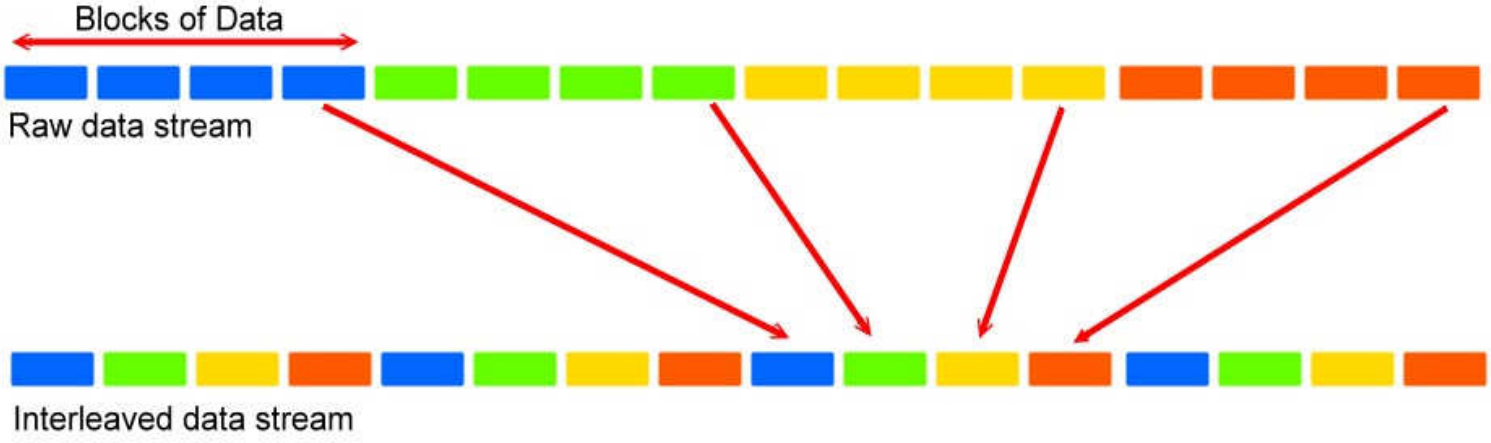


Figure 4.108 Interleave diagram

If your line is particularly susceptible to bursts of noise then interleaving should improve your vdsl experience simply because if you lose a whole batch of data then this could cause your bridge to loose sync with the exchange.

Using Interleaving, the bridge is able to re-assemble the data or if necessary just re-request the part of the data that it is unable to recover. By increasing the interleave depth of each ports that are susceptible to noise, this will improve error performance and stability of marginal lines.

Interleave Depth is defines as the number of bits (or bytes) in each block of data.
VDSL supports a various levels of interleaving, the depth of which can range from 0 (no interleaving) to 64.

Interleave Delay is defines as the mapping (relative spacing) between subsequent input bytes at the interleave input and their placement in the bit stream at the interleave output.

Maximum Interleave Delay is the configurable attribute on some DSLAMs/routers as the maximum time for the Interleave Delay. The higher the Interleave Delay the greater the Interleaving Depth.

Note:

Interleaving Depth & Interleaving Delay do not appear to be the same thing as the additional amount of latency you will see when interleaving is switched on nor is latency affected by speed (e.g. it does not decrease when you go from 1Mb to 5Mb).

The following ports can modify the desired interleave depth. (Figure 4.108)

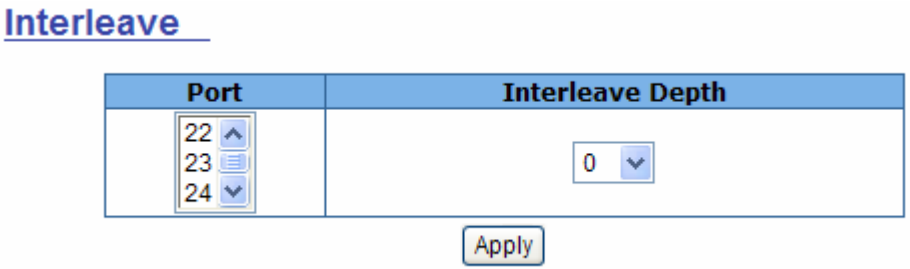


Figure 4.108 Interleave Depth

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

Interleave depth value will show in the state only if the port is connected. (Figure 4.109)

Port	Interleave		Port	Interleave	
	Config	State		Config	State
1	8	0	13	8	0
2	8	0	14	8	0
3	8	0	15	8	0
4	8	0	16	8	0
5	8	8	17	8	0
6	8	0	18	8	0
7	8	8	19	8	0
8	8	8	20	8	0
9	8	8	21	8	0
10	8	0	22	8	0
11	8	8	23	8	0
12	8	8	24	8	8

Figure 4.109 Interleave status

4.4.14 Reset System

Reset NVF-2400S to default configuration. (Figure 4.110)

Figure 4.110 Reset System

4.4.15 Reboot

Reboot the NVF-2400S in software reset. (Figure 4.111)

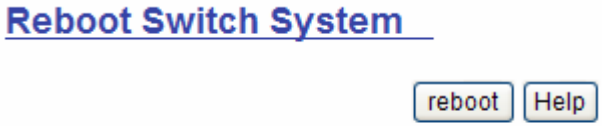


Figure 4.111 Reboot System

Chapter 5. Applications

The VDSL provides home network architecture. Transforming an apartment into a Multiple-Family Home network area, sharing a single internet account for multiple users with Router & Cable Modem, it can provide unlimited access time in the internet at a reasonable low price.

Bridging Functions

The NVF-2400S provides full transparent bridging function. It automatically connects node addresses, that are later used to filter and forward all traffic based on the destination address. When traffic passes between devices attached to the shared collision domain, those packets are filtered from the IP DSLAM. But when traffic must be passed between unique segments (e.g. different ports of the IP DSLAM), a temporary link is set up between the IP DSLAM ports in order to pass this traffic, NVF-2400S (the high-speed VDSL fabric).

Transceiver function

The NVF-2400S supports Ethernet to VDSL convert and it can transmit or receive packet from Ethernet port to the RJ21 port or VDSL port to Ethernet port.

Flexible Configuration

The NVF-2400S is not only designed to segment your network, but also to provide a wide range of options in the configuration of Home network connections. It can be used as a simple stand-alone IP DSLAM; or can be connected with another IP DSLAM, Cable modem, Router, XDSL, ISDN, gateway or other network interconnection devices in various configurations. Some of the common applications of the IP DSLAM are described in this chapter.

Used as Apartment for Internet Access

The NVF-2400S provides a high speed, 5/15/25Mbps transmission over existing home telephone wiring over a single Internet account to provide simultaneous independent Internet access to multiple users.

No mater ISDN Telephone system or POTS Telephone system you are. VDSL Technology let you can use telephone system and VDSL network system in the same time.

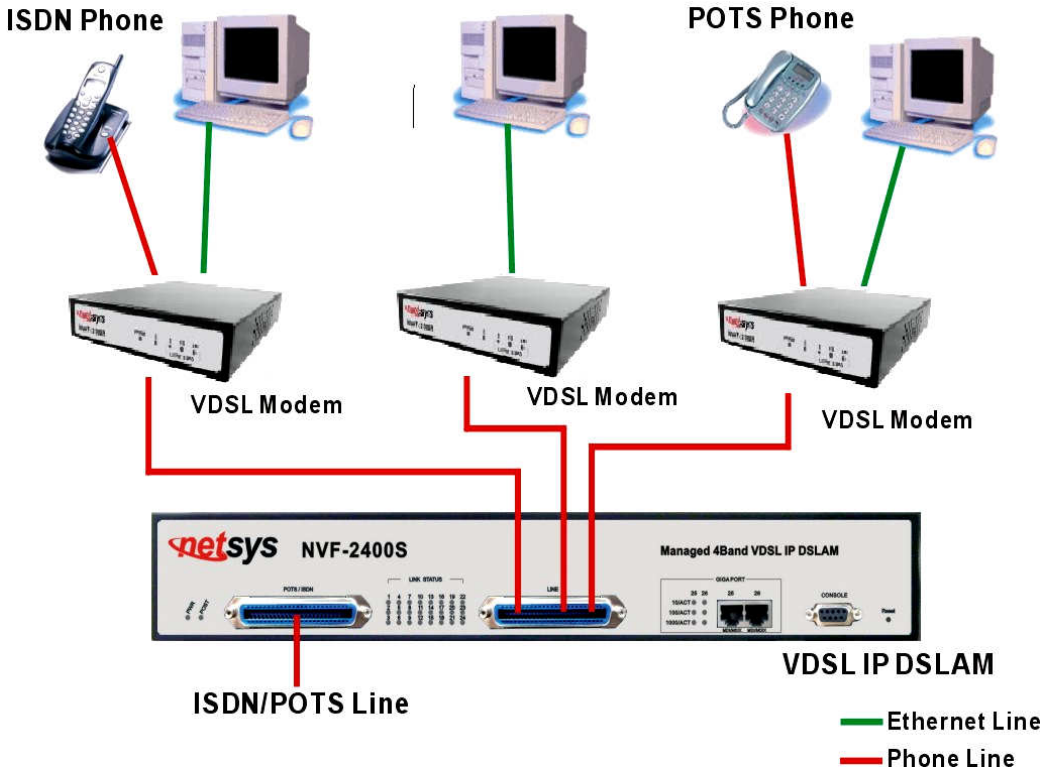


Figure 5.1 NVF-2400S Application Diagram

Application for sharing a single internet account

If multiple users would like to share a single internet account using the NVF-2400S, which is to be connected to IP sharing device then to xDSL or Cable Modem.

Note:

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

Appendix A: RJ-21 Telco ports distribution

A.1 RJ-21 Pin and VDSL port contrast list

Table A-1

VDSL 50 Pin RJ-21 Cable Connector List Cable Characteristic = 24 AWG twist wire	
1	24 & 49
2	23 & 48
3	22 & 47
4	21 & 46
5	20 & 45
6	19 & 44
7	18 & 43
8	17 & 42
9	16 & 41
10	15 & 40
11	14 & 39
12	13 & 38
13	12 & 37
14	11 & 36
15	10 & 35
16	9 & 34
17	8 & 33
18	7 & 32
19	6 & 31
20	5 & 30
21	4 & 29
22	3 & 28
23	2 & 27
24	1 & 26

Note: RJ-21 Pin25 & 50 are not used

RJ-21 Cable Drawing (150 cm Male to Male, 24AWG)

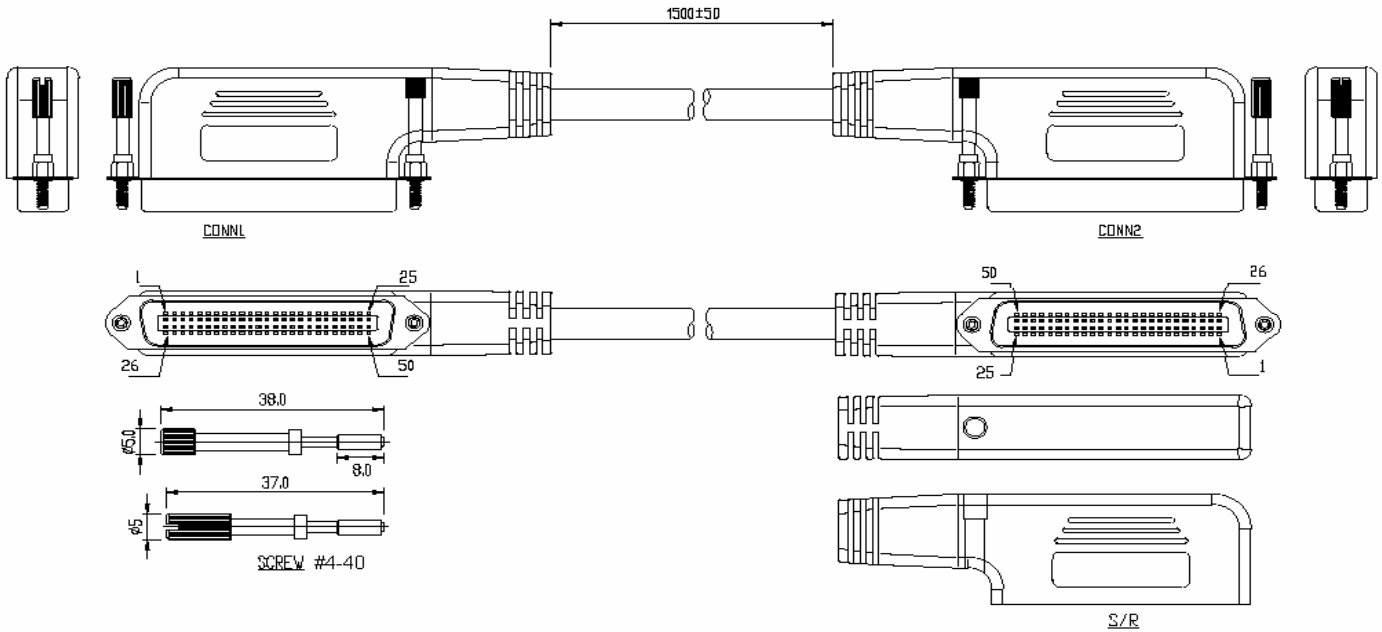


Figure A-1

A.2 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 A-2 lists the pin assignments for the serial console interface connector.

Table A-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 A-2 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.

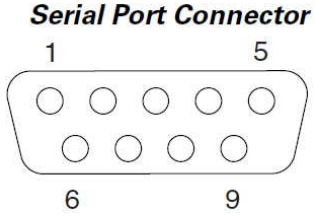


Figure A-2

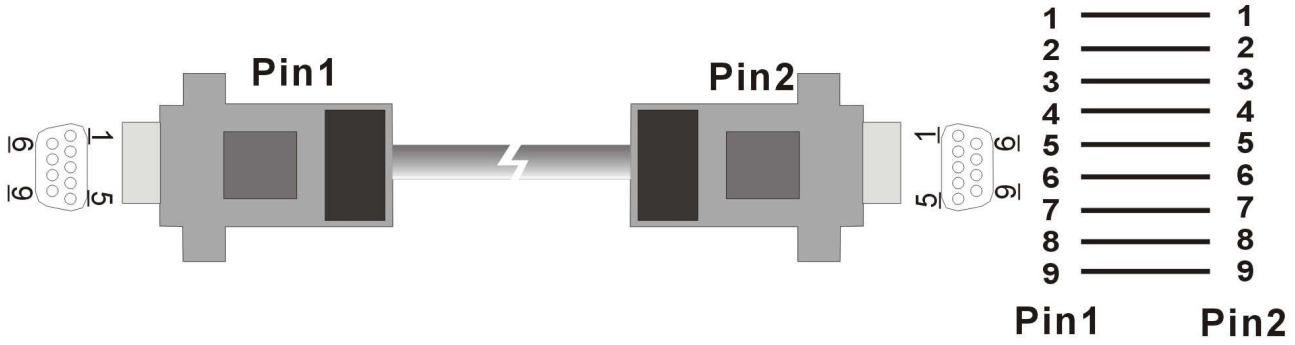
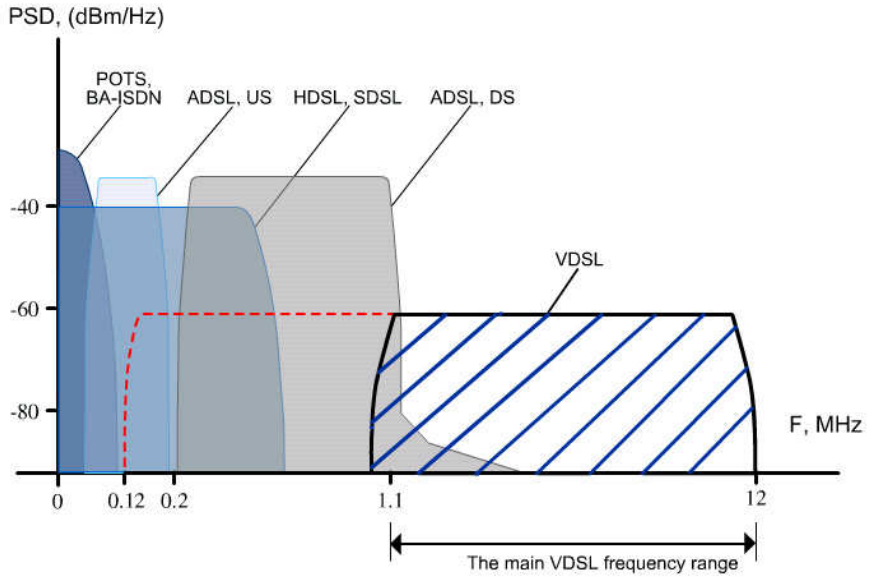


Figure A-3 Pin Assignments and Wiring for an RS-232 Cable

Appendix B: VDSL Spectrum

VDSL Technology – Requirements & Definitions
Spectral Allocation



- Co-exists with legacy Voice and ISDN services
- Co-exists with other xDSL technologies
- Programmable notch filter to avoid Radio Frequency Interference

Slide 5

Figure B.1 VDSL Spectral Allocation

Appendix C: Product Specification

Key Features & Benefits

- Supports bandwidth management (speed rate control) 5M/15M/25Mbps for VDSL port with long driver capable up to 1.7/1.1/0.6km (5666/3666/1999 feet)
- Supports GARP/GVRP IEEE-802.1p/q tagging VLAN, IEEE 802.1v protocol VLAN, port base VLAN
- Supports quality of phone wiring detected with SNR (Signal to Noise Ratio) indications
- Supports QOS IEEE-802.1p
- Supports IGMP V2 Snooping
- Supports BOOTP/DHCP Client
- Supports Bandwidth Control
- Supports LACP IEEE-802.3ad Port Trunking
- Supports IEEE 802.1d Spanning Trees
- Supports Port Mirroring (Sniffer)
- Supports Broadcast Storm filtering
- Supports 802.1x Port Based Network Access Control
- Supports Web Base and Telnet for remote management
- Supports SNMP v1 RFC-1493 Bridge MIBs, RFC-1643 Ethernet MIB, RFC-1213 MIB II, Enterprise MIB
- Supports RMON groups 1, 2, 3, 9 (RFC-1757 RMON MIB)
- Supports TFTP/XMODEM for firmware upgrade
- Supports In-Band/Out-of-Band Management
- Supports Interleave Setup
- Supports RS-232 console port for functions setup (DB-9Pin Female / 9600bps)
- Spectral compatibility with XDSL, ISDN (2B1Q/4B3T), HomePNA
- EMI certified by CE, FCC
- Safety by EN60950-1

Product Specification

Standard:	IEEE802.3 standard IEEE802.3u standard IEEE802.3ab standard Compliant with ETSI, ITU, ANSI standards
Interface:	2 * RJ-45 10/100/1000Mbps Ethernet port 24 * RJ-21 connector for VDSL connection 24 * RJ-21 connector for POTS/ISDN connection
Flow control:	Full duplex: IEEE 802.3x Half duplex: Back pressure
MAC address table:	6K Entries
LED indication:	Power and POST Link/Active/Speed/Duplex Status for Ethernet port Link for VDSL port
VDSL Frequency Spectrum:	Transmitter: 900 kHz ~ 3.9MHz Receiver: 4MHz & 7.9MHz
POTS/ISDN pass filter Spectrum:	0 ~ 630kHz
Power Consumption:	38.5W
Operating Temperature:	0℃ ~ 50℃ (32℉ ~ 122℉)
Storage Temperature:	-20℃ ~ 70℃ (-4℉ ~ 158℉)
Humidity:	10 to 90% (non-condensing)
Weight:	About 6kg
Dimensions:	434 x 299 x 66 mm

Appendix D: 4 Band VDSL Electrical Characteristics

Parameter		Min.	Typ.	Max.	Unit
Spectrum	Transmit	0.9		3.9	MHz
	Receive	4		7.9	MHz
PSD Level	Transmit	-70		-61.5	dBm/Hz
	Receive	-70		-60	dBm/Hz
Noise Margin			6		dB
5Mbps Link Margin	Transmit	27	31	35	dB
	Receive	27	31	35	dB
15Mbps Link Margin	Transmit	36	38	40	dB
	Receive	36	38	40	dB
25Mbps Link Margin	Transmit	41	43	45	dB
	Receive	41	43	45	dB

Appendix E: Example of VLAN Setting

Example 1:

4 users join to Internet by VDSL system like following drawing, and have 7 demands. (Figure E-1)

User A connects to port 1 and join to Internet through port 26

User B connects to port 2 and join to Internet through port 26

User C connects to port 3 and join to Internet through port 26

User D connects to port 4 and join to Internet through port 26

User A isolate with Users B, C and D

User B isolate with Users A, C and D

User C and D in the same Group and isolate with Users A and B

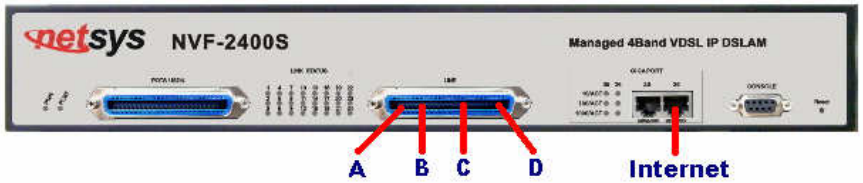


Figure E.1 VLAN example diagram

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 (Figure E-2)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
PORT1	1	ENABLE	DISABLE
PORT2	1	ENABLE	DISABLE
PORT3	1	ENABLE	DISABLE
PORT4	1	ENABLE	DISABLE

Figure E.2 Setup Port VID

Add VLAN Group: (Figure E-3)

There are 256 VLAN groups available for configuration. Add a VLAN Group VID=21 member ports = port 1 & port 26

Note:

Do not change the default_1 group.

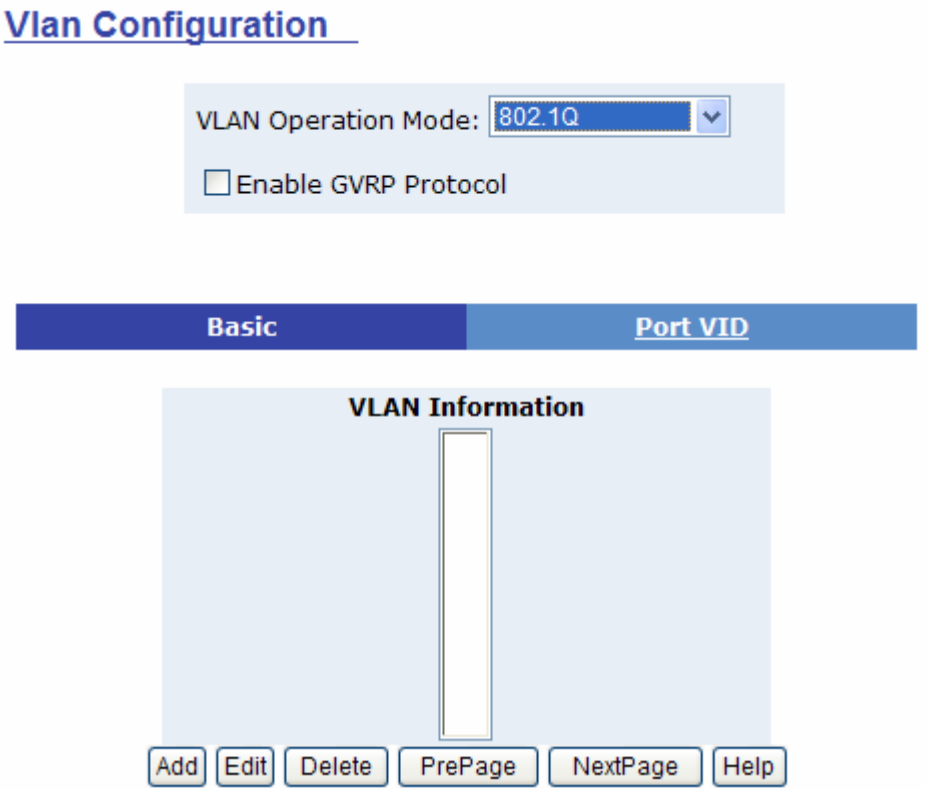


Figure E.3 Add VLAN Group

Setup VLAN Name=UserA, VID=21, select member ports 1 & 26 (Figure E-4)

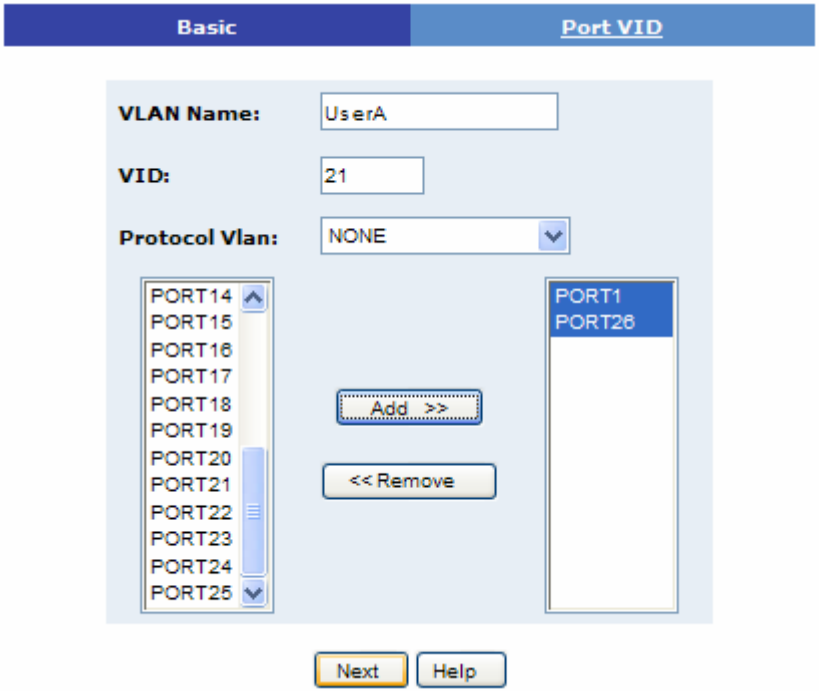


Figure E.4 Select and add VLAN member ports

Select Untag or Tag Setup. Unless the device (computer or switch) which connect to port 1 or port 26 can support Tagging VLAN, otherwise select Untag. (Figure E-5)

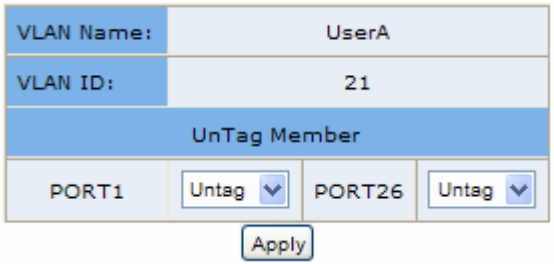


Figure E.5 Select Tag / Untag

Add a VLAN Group Name=UserB, VID=22 member ports = port 2 & port 26

Add a VLAN Group Name=UserCD, VID=23 member ports = port 3, port 4 & port 26

Example 2:

4 users join to Internet through 2 IP DSLAMs like the following drawing, and have 7 demands. (Figure E-6)

User A connect to port 1 of VDSL-1 and join to Internet through port 26 of VDSL-2

User B connect to port 2 of VDSL-1 and join to Internet through port 26 of VDSL-2

User C connect to port 1 of VDSL-2 and join to Internet through port 26 of VDSL-2

User D connect to port 2 of VDSL-2 and join to Internet through port 26 of VDSL-2

User A isolate with Users B, C and D

User C isolate with Users A, B and D

User B and D in the same Group and isolate with Users A and B

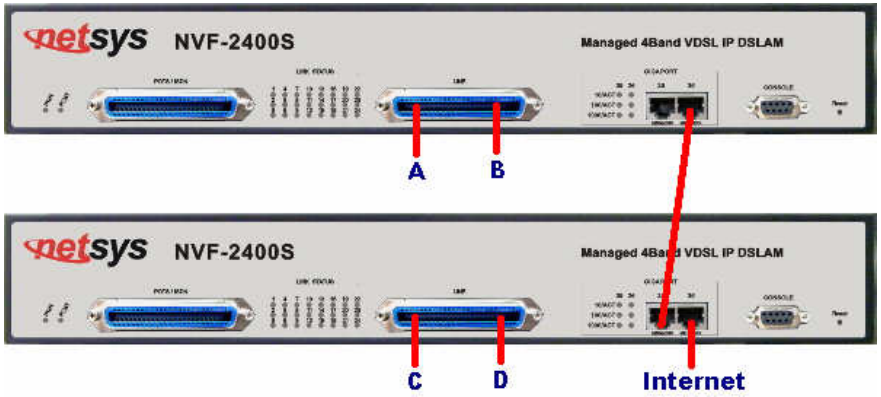


Figure E.6 VLAN example dirgram

Setup Procedure:

VDSL-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
26	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
26	Tag

VDSL-2 SETUP:

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

b. Add VLAN Group:

Caution:

Do not change the default_1 group.

Add a VLAN Group, Group name=UserA VID=11 member ports = port 25 & port 26

Select Untag or Tag Setup for VID=11 group:

Port Number	Untag/Tag Select
25	Tag
26	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
2	Untag
25	Tag
26	Untag

Add a VLAN Group, Group name=UserC VID=21 member ports = port 1 & port 26

Select Untag or Tag Setup for VID=21 group:

Port Number	Untag/Tag Select
1	Untag
26	Untag

Appendix F: Troubleshooting

Diagnosing VDSL Indicators

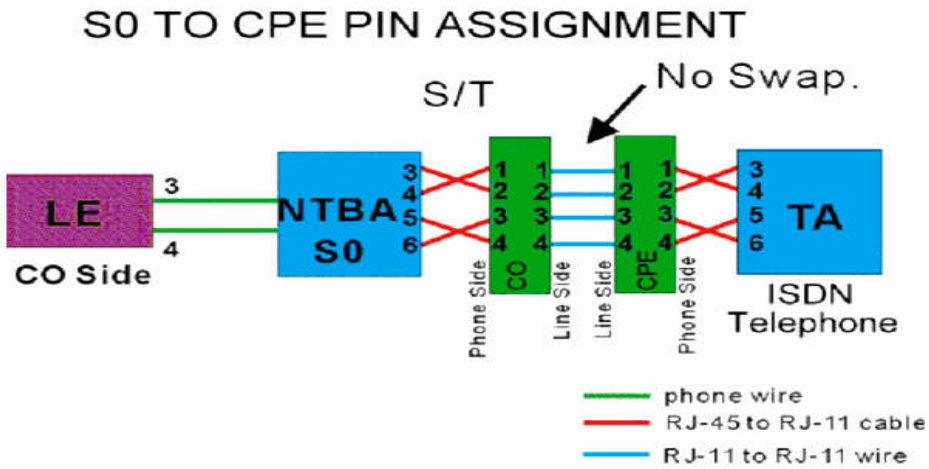
The VDSL can be easily monitored through its comprehensive panel indicators. These indicators assist the network manager in identifying problems of the IP DSLAM may encounter. This section describes common problems you may encounter and possible solutions.

1. Symptom:	POWER indicator does not light up (green) after power on.
Cause:	Defective Power outlet, Power cord, Internal power supply
Solution:	Check 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 a qualified distributor.

2. Symptom:	Link indicator does not light up (green) after making a connection.
Cause:	Network interface (ex. a network adapter card on the attached device), network cable, or switch port is defective.
Solution:	◆ Power off and re- power on the IP DSLAM. ◆ Verify that the switch and attached device are powered on. ◆ Be sure the cable is plugged into both the switch and corresponding device. ◆ Verify that the proper cable type is used and its length does not exceed specified limits. ◆ Check the adapter on the attached device and cable connections for possible defects. ◆ Replace the defective adapter or cable if necessary.

3. Symptom:	VDSL Link cannot be established.
Cause:	VDSL speed mode setting failure or phone cable length is over the specification limit of the speed mode.
Solution:	◆ Please make sure that the phone wire must be connected between NVF-2400S and NVF-200R when both are power on. NVF-2400S will do link speed function depending on speed mode setting and phone wire length, therefore if NVF-2400S can't detect NVF-200R over phone wire while both power on, this will cause the link to fail. ◆ Please check phone cable must be 24 gauge with twisted pair and without rust, and the length is not over 1.9km.
Note:	Phone cable must meet CAT 3 standard or above and without clustering, otherwise will cause more cross talk issue to reduce DSL power driver.

4. Symptom:	VDSL line is at link margin.
Cause:	When the VDSL line is linking between 2 speeds at 5/15Mbps or 15/25Mbps.
Solution:	Fixed the speed to 5Mbps when it is linking between 5/15Mbps or fixed the speed to 15Mbps when it is linking between 15/25Mbps.

5. Symptom:	We tested with a regular S0 bus from an NTBA - data works, but ISDN telephone does not.
Solution:	You must connect according to the following chart if you want to connect CO and CPE with NTBA. 

6. Symptom:	VDSL flickers at 25Mbps when multicast streams.
Cause:	Power level is too high and noise immunity is weak.
Solution:	Fixed the speed to 15Mbps, since 15Mbps is ideal for multicast streaming while 25Mbps is for transferring large data file at high speed.

System Diagnostics

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 power is 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, please contact your local dealer.

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 selections of the transmission mode for the RJ-45 ports are auto-negotiation using the default method. 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 re-establish communications with the attached device (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 version that will 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 100/1000Mbps Fast Ethernet connections, or Category 3, 4 or 5 cables for standard 10Mbps Ethernet connections. Be sure RJ21 phone wiring, use **18~26 gauge**.
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 (NVF-2400S) supports auto MDIX), without crossover cable can be used.

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, then contact your dealer for assistance.

Appendix G: Compliance and Safety Information

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a computing device, pursuant to Part 15 of 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 instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. The equipment and the receiver should be connected to outlets on separate circuits.
4. Consult the dealer or an experienced radio/television technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

If this telephone equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the

proper functioning of your equipment. If they do, you will be notified in advance in order for you to make necessary modifications to maintain uninterrupted service.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

Important Safety Instructions

Caution1:

The direct plug-in wall transformer serves as the main disconnect for the product. The socket outlet shall be installed near the product and be readily accessible.

Caution2:

Do not use this equipment near water, for example in a wet basement. Avoid using a telephone during an electrical storm. There may be a remote risk of electrical shock from lightning.

Caution3:

Do not use the telephone to report a gas leak in the vicinity of the leak.
If trouble is experienced with this unit, please contact customer service of your dealer immediately.

Caution4:

Do not disassemble this equipment. It does not contain any user serviceable components.

FCC Warning

This equipment has been tested 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 can generate, use, and 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 owner's expense.

CE Mark Warning

This is a class B 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. We shall not be liable for incidental or consequential damages. We neither assume nor authorize any person to assume for it any other liability.

WARNING:
DO NOT TEAR OFF OR REMOVE THE WARRANTY STICKER AS SHOWN, OR THE WARRANTY IS VOID.