Networking your world

# NV-600A

## ADSL2+/VDSL2 Modem Router

# USER'S MANUAL

Http://www.netsys.com.tw

# Copyright

Copyright © 2012 by National Enhance Technology Corp. All rights reserved.

**Trademarks**

NETSYS is a trademark of National Enhance Technology Corp.
Other brands 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 from 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 users follow in line with the environmental conditions to use this product.

# Foreword: VDSL2 Router solution

**Attention:**

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

Netsys' NV-600A is a management of the VDSL2 CPE router that leverages the extraordinary bandwidth promise of VDSL2 (max. 100Mbps symmetric) technology, the next step in the delivery of new high-speed Internet applications in commercial environments. Quick, easy, economical to install and maintain, the NV-600A works over the existing copper wire infrastructure. NV-600A is a CPE (Customer Premise Equipment) device. And compatible with the NV-802S (8Ports VDSL2 IP DSLAM) and NV-700L (VDSL2 CO Extender).

The NV-600A will allow operators worldwide to compete with cable and satellite operators by offering services such as HDTV, VOD, videoconferencing, high speed Internet access and advanced voice services including VoIP, over a standard copper telephone cable. The NV600A is seen by many operators as an ideal accompaniment to a FTTP rollout, where for instance fiber optic is supplied directly to an apartment block and from there copper cable is used to supply residents with high-speed VDSL2.

**Caution:**

The NV-600A is for **indoor** applications only. This product does not have waterproof protection, please do not use it in outdoor applications.

## Safety Warnings

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

- **DO NOT** open the device or unit. Opening or removing the cover may expose users to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact the user's vendor for further information.
- **Use ONLY** the dedicated power supply for user's device. Connect the power to the right supply voltage (110V AC used for North America and 230V AC used for Europe. NV-600A supports 12 VDC power input).
- **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 user's device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- **DO NOT** expose user's device to dampness, dust or corrosive liquids.
- **DO NOT** use this product near water, for example, in a wet basement or near a swimming pool.
- **Connect ONLY** suitable accessories to the device.
- **Make sure** to connect the cables to the correct ports.
- **DO NOT** obstruct the device ventilation slots, as insufficient air flow may harm user's device.
- **DO NOT** place items on the device.
- **DO NOT** use the device for outdoor applications directly, and make sure all the connections are indoors or have waterproof protection place.
- **Be careful** when unplugging the power, because it may produce sparks.
- **Keep** the device and all its parts and accessories out of the reach of children.
- **Clean** the device using soft and dry cloth rather than liquid or atomizers. Power off the equipment before cleaning it.

◆ This product is **recyclable**. Dispose of it properly.

# Table of Contents


**COPYRIGHT** ..... **1**

**SAFETY WARNINGS** ..... **3**

1.1 CHECK LIST ..... 9

**CHAPTER 2. INSTALLING THE ROUTER** ..... **10**

2.1 HARDWARE INSTALLATION ..... 10

2.2 PRE-INSTALLATION REQUIREMENTS ..... 10

2.3 GENERAL RULES ..... 11

2.4 CONNECTING THE ROUTER ..... 12

2.5 CONNECTING THE RJ-11 / RJ-45 PORTS ..... 13

**2.6 VDSL2 APPLICATION** ..... 14

**CHAPTER 3. HARDWARE DESCRIPTION** ..... **16**

3.1 FRONT PANEL ..... 17

3.2 FRONT INDICATORS ..... 17

**3.3 REAR PANEL** ..... 18

**CHAPTER 4. CONFIGURE THE NV-600A VIA WEB BROWSER** ..... **21**

**4.1 LOGIN** ..... 22

***4.1.1 Home*** ..... *23*

***4.1.2 Quick Setup*** ..... *25*

4.2 SELECT THE MENU LEVEL ..... 31
4.3 SELECT "SYSTEM" ..... 32
*4.3.1 Host Name Config* ..... *33*
*4.3.2 System Time* ..... *34*
*4.3.3 Administrator Settings* ..... *36*
*4.3.4 Web Settings* ..... *38*
*4.3.5 Software/Firmware Upgrade* ..... *39*
*4.3.6 Configuration Settings* ..... *40*
*4.3.7 System Log* ..... *43*
*4.3.8 SSL Certificate* ..... *46*
*4.3.9 Mac Table Aging Time* ..... *47*
*4.3.10 Vlan Tag Pass Through Mode Setting* ..... *48*
*4.3.11 Reset* ..... *50*
4.4 SELECT "STATISTICS" ..... 51
*4.4.1 LAN* ..... *52*
*4.4.2 WAN* ..... *54*
4.5 SELECT "xDSL" ..... 56
*4.5.1 xDSL Status* ..... *57*
*4.5.2 Vectoring Mode selection* ..... *59*
4.6 SELECT "WAN" ..... 61
*4.6.1 WAN Mode Selection* ..... *62*
*4.6.2 Auto Detect Setting* ..... *64*
*4.6.3 WAN Channel Config* ..... *67*
*4.6.4 VLAN Channel config* ..... *71*

*4.6.5 WAN Setting* ..... *74*
*4.6.6 WAN Status* ..... *89*
*4.6.7 DNS* ..... *93*
*4.6.8 DDNS* ..... *95*
*4.6.9 OAM Configuration* ..... *97*
4.7 SELECT "LAN" ..... 101
*4.7.1 LAN ARP List* ..... *102*
*4.7.2 LAN Settings* ..... *103*
*4.7.3 UPnP Devices List* ..... *113*
*4.7.4 LAN Switch Port Setting* ..... *114*
*4.7.5 LAN Port Status* ..... *115*
4.8 SELECT "ROUTE" ..... 116
*4.8.1 Static Routing* ..... *117*
*4.8.2 RIP Support* ..... *120*
*4.8.3 Routing Table List* ..... *123*
4.9 SELECT "FIREWALL" ..... 126
*4.9.1 Firewall Setting* ..... *127*
*4.9.2 IPv6 Firewall Setting* ..... *128*
*4.9.3 Packet Filtering* ..... *130*
*4.9.4 URL Filtering* ..... *144*
*4.9.5 Parental Control* ..... *146*
*4.9.6 Application Server Settings* ..... *148*
*4.9.7 Access Control List (ACL)* ..... *151*
4.10 NAT ..... 153

*4.10.1 NAT Settings* ..... 154
*4.10.2 Virtual Server* ..... 155
*4.10.3 Port Triggering* ..... 159
*4.10.4 DMZ* ..... 錯誤! 尚未定義書籤。
4.11 QoS ..... 165
*4.11.1 QoS Settings* ..... 166
*4.11.2 Queue Config* ..... 168
*4.11.3 Class Config* ..... 172
4.12 MULTICAST ..... 178
*4.12.1 Proxy Settings* ..... 179
*4.12.2 Snooping Settings* ..... 181
*4.12.3 Advanced Settings* ..... 183
4.13 IPSEC ..... 185
*4.13.1 Tunnel Mode* ..... 186
4.14 IPV6 ..... 189
*4.14.1 IPv6 Setting* ..... 190
*4.14.2 6RD Configuration* ..... 192
*4.14.3 DS-Lite Configuration* ..... 194
4.15 DIAGNOSTICS ..... 196
*4.15.1 Diagnostic Test Suite* ..... 197
4.16 SNMP ..... 199
*4.16.1 SNMP Options* ..... 200
*4.16.2 SNMPv3 Settings* ..... 203
*4.16.3 Add v3 user* ..... 204

APPENDIX A: CABLE REQUIREMENTS ..... 206

APPENDIX B: PRODUCT SPECIFICATION ..... 209

APPENDIX C: ROUTER MODE SELECT ..... 212

APPENDIX D: TROUBLESHOOTING ..... 215

APPENDIX F: COMPLIANCE INFORMATION ..... 223

WARRANTY ..... 227

CHINESE SJ/T 11364-2014 ..... 228

# Chapter 1. Unpacking Information

## 1.1 Check List

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

**Package Contents:**

| | | | |
|---|---|---|---|
| | | | |
| 1 x Managed VDSL2 CPE router | 1 x QR code for user's manual hyperlink. | Accessory Kit: 1 x Ehternet Cable, 1 x Phone wire, 1 x DC12V Power Adapter | |

**Notes:**

1. Please inform users dealer at once about any missing or damaged parts. If possible, keep the carton including the original packing materials. Use them to repack the unit in case there is a need to return for repair.
2. If the product has any problem, please contact the user's local vendor.
3. Do not use sub-standard power supply. Before connecting the power supply to the device, be sure to check compliance with the specifications. The NV-600A uses a DC12V/1A power supply.
4. The power supply included in the package is commercial grade. Do not use industrial-grade applications.
5. Please look for the QR code on the bottom of the product, the user can launch the QR code scanning program to scan and download the user's manual electronic format file. Above QR code icon is for reference.

# Chapter 2. Installing the Router

## 2.1 Hardware Installation

This chapter describes how to install the router and establish network connections. The NV-600A may be installed on any level surface (e.g. a table or shelf). However, please take note of the following smallest site requirements before users begin. **The NV-600A has 2 pre-installed rubber feet.**

## 2.2 Pre-installation Requirements

Before users start the actual hardware installation, make sure users 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 requirements:

- Power requirements: **DC 12 V / 1A**
- The router should be located in a cool dry place, with at least **10cm/4in** of space at the front and back for ventilation.
- Place the router away from direct sunlight, heat sources, or areas with a high amount of electromagnetic interference.
- Check if the 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 with radio amplifying stations nearby or transformer stations nearby.

## 2.3 General Rules

Before making any connections to the router, please note the following rules:

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

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

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

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

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

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

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

  Please note that the line port is without polarity, therefore users can reverse the two wires of the phone cable when installed.

RJ-11 Pin out Assignments

| Pin# | MNEMONIC | FUNCTION |
|---|---|---|
| 1 | NC | Unused |
| 2 | NC | Unused |
| **3** | **DSL** | **Used** |
| **4** | **DSL** | **Used** |
| 5 | NC | Unused |

| | | |
|---|---|---|
| 6 | NC | Unused_ |

## 2.4 Connecting the Router

The router has four Ethernet ports which support connection to Ethernet operation. The devices attached to these ports must support auto-negotiation /10Base-T / 100Base-TX / 1000Base-TX unless they always operate at half duplex. Use any of the Ethernet ports to connect devices such as Monitor systems, Servers, Switches, bridges or routers.

**Notes:**

1. The (RJ11/Terminal Block) Line port is used to connect the telephone that is connected to VDSL2 CO and CPE router (Point-to-point solution).
2. The Slave device (CPE) must be connected to the Master device (CO) through the telephone wire. The Slave cannot be connected to another Slave, and the Master cannot be connected to another Master.

## 2.5 Connecting the RJ-11 / RJ-45 Ports

- The Line port has 2 connectors: RJ-11 and terminal block. It is used to connect with NV-700L(CO) using a single pair phone cable to NV-600A(CPE) bridge side (point to point solution). Take note that NV-600A line port cannot be used at the same time. Either RJ-11 port is connected or terminal block is connected using a straight connection (Figure 2.4) or cross-over connection (Figure 2.5)

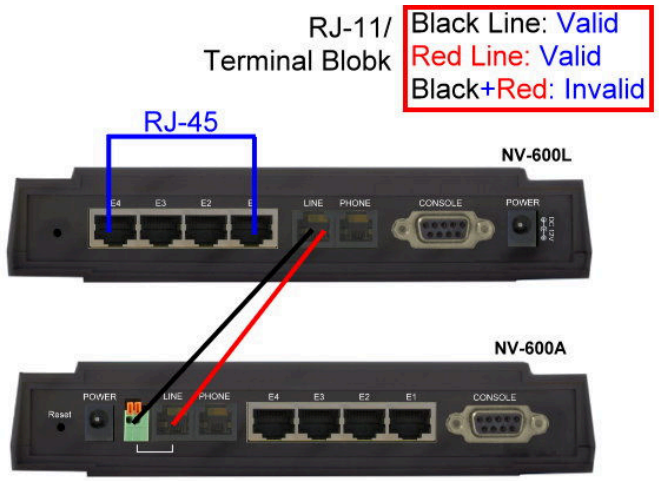



**Figure 2.1 NV-600A line ports straight connection**

- When inserting a RJ-11 plug, make sure the tab on the plug clicks into position to ensure that it is properly seated.
- **Do not** plug an RJ-11 phone jack connector into the Ethernet port (RJ-45 port). This may damage the router. Instead, use only twisted-pair cables with RJ-45 connectors that conform to Ethernet standard.

**Notes:**

1. Be sure each twisted-pair cable (RJ-45 ethernet cable) does not exceed 100 meters (333 feet).
2. We recommend using Category 5~7 UTP/STP cables for Cable bridge or Router connections to avoid any confusion or inconvenience in the future when users are attached to high bandwidth devices.
3. RJ-11 (VDSL2 Line port) uses **24 ~ 26** gauge with twisted pair phone wiring, we do not recommend 28 gauge or above.
4. Be sure phone wire has been installed before the NV-600A boot.

## 2.6 VDSL2 Application

The router's line port supports 100Mbps/0.3km for data service across existing phone wiring. It is easy-to-use which do not require installation of additional wiring. Every modular phone jack in the home can become a port on the LAN. Networking devices can be installed on a single telephone wire that can be installed within suitable distance (depending on speed) (Figure 2.2)

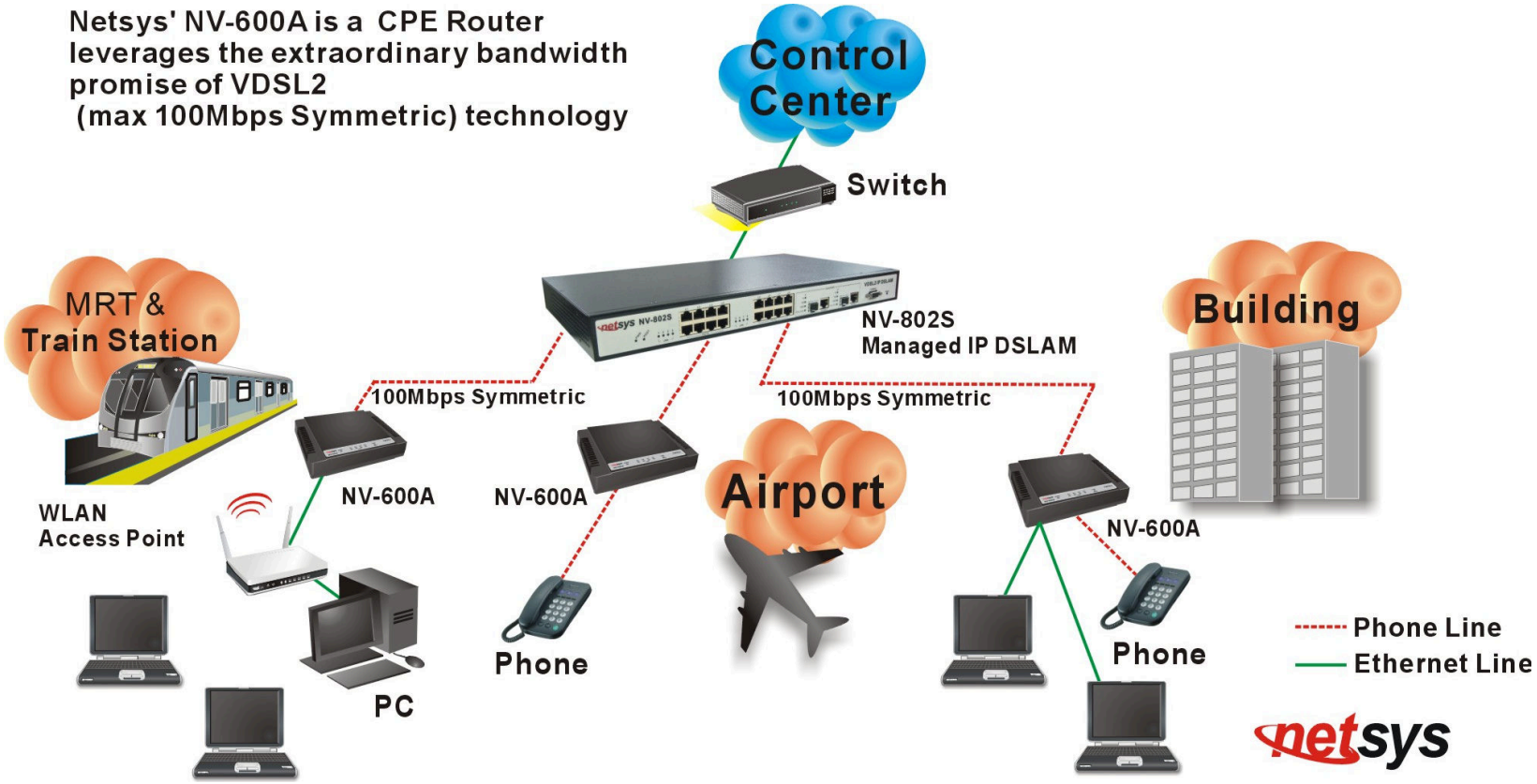



Figure 2.2 NV-600A application

### ◆ 2.6.1 Connect the NV-700L and the NV-600A to the Line

The objective for VDSL2 is to pass high speed data over a twisted pair cable. In the setup, connect NV-700L to NV-600A through phone wire (24~26 AWG) or line simulator or any other hardware representation of a cable network, with or without noise injection and crosstalk simulations.

### ◆ 2.6.2 Connect the NV-700L and the NV-600A to LAN Devices

In the setup, usually an Ethernet tester serves as a representation of the LAN side as well as a representation of the WAN side.

### ◆ 2.6.3 Run Demos and Tests

The Ethernet tester may send data downstream as well as upstream. It also receives the data in order to check the integrity of the data transmission. Different data rates can be tested under different line conditions.

# Chapter 3. Hardware Description

This section describes the important parts of the vdsl2 router. It features the front panel and rear panel.

**NV-600A Outward**

## 3.1 Front Panel

The figure shows the front panel. (Figure 3.1)

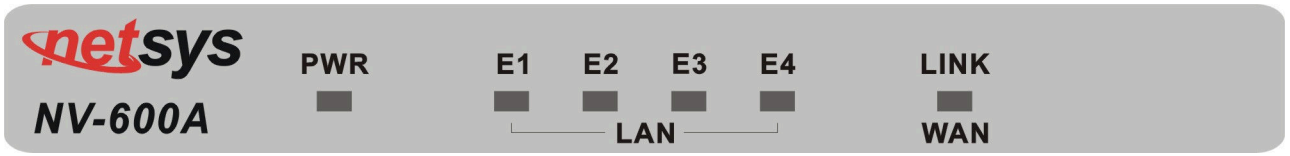



**Figure 3.1 Front Panel (NV-600A)**

## 3.2 Front Indicators

The router has **Six** LED indicators. The following Table shows the description. (Table 3-1)

**Table 3-1** LED Indicators Description and Operation

| LED | Color | Status | Descriptions |
|---|---|---|---|
| PWR (Power LED) | Green | On (Steady) | Lights to indicate that the VDSL2 router had power |
| | | Off | The device is not ready or has malfunctioned. |
| E1 ~ E4 (Ethernet LED) | Green | On (Steady) | The device has a good Ethernet connection. |
| | | Blinking | The device is sending or receiving data. |
| | | Off | The LAN is not connected or has malfunctioned. |
| LINK (VDSL2 LED) | Green | On (Steady) | The Internet or network connection is up. |
| | | Fast Blinking | The device is sending or receiving data. |
| | | Slow Blinking | The Internet or network connection is down. |

**Note:**

It is normal for the connection between two Routers to take up to 3 minutes, due to NV-700L/NV-600A to establish a link mechanism in auto-negotiation, with detects and calculates CO and CPE both PBO and PSD level, noise levels and other arguments for getting a better connection.

## 3.3 Rear Panel

The following figure shows the rear panel. (Figure 3.2)

**Figure 3.2 Rear Panel**

And the table shows the description. (Table 3-2)

**Table 3-2** Description of the router rear connectors

| Connectors | Type | Description |
|---|---|---|
| Reset | Tact switch Button | The reset button allows users to reboot the VDSL2 or load the default settings.<br>**Press and hold for 1-5 seconds: Reboot the VDSL2 Router**<br>**Press over 5 seconds: Load the default settings** |
| Power | DC Power Jack | External Power Adapter: Input: AC 85~240Volts/50~60Hz<br>Output: DC 12V/1A |
| Line | RJ-11/Terminal Block | For connecting to a VDSL2 device. (**Do not** use RJ11 and Terminal Block at the same time.) |
| Phone | RJ-11 | For connecting to the POTS equipment or ISDN router |
| Gigabit Ethernet (E1-E4) | RJ-45 | For connecting to an Ethernet equipped device. |
| Link (WAN) | RJ-11/Terminal Block | For connecting a VDSL2 bridge. (**Do not** use RJ11 and Terminal Block at the same time.) |
| CONSOLE | RS-232 | For connecting a PC with RS-232 serial port over a D-SUB Cable |

**Before user installed power and device, please read and follow these essentials:**

- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.

**Note:**

Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.

- Users can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring sharing similar electrical characteristics can be bundled together.
- Users should separate input wiring from output wiring.
- We recommend that users mark all equipment into the wiring system.

# Chapter 4. Configure the NV-600A Via Web Browser

The NV-600A provides a built-in HTML based management interface that allows users configure the NV-600A via Internet Browser. Best viewed at using Chrome or Firefox.

In order to use the web browser to configure the device, users may need to allow:

- Web browsers pop up windows from user's device. Web pop-up blocking is enabled by defaulting in windows 7 or above.
- Java Scripts. (Enabled by default)
- Java permissions. (Enabled by default)

Launch users web browser and input the IP address 192.168.16.254 (NV-600A) on the Web page.

The following section user can find default username and password.

## 4.1 Login

The default username is "admin"and password is "admin", too. The password is changeable in Administrator Settings.

It is advisable to change the administrator password for the security of the user's network.

Figure 4.1 Login Password

### 4.1.1 Home

After successful login using the username **admin**, the home page of NV-600A is loaded in web browser for NV-600A. User can also click the "Home" on the left navigation bar. The home page displays the information screen as shown in Figure 4.1.1

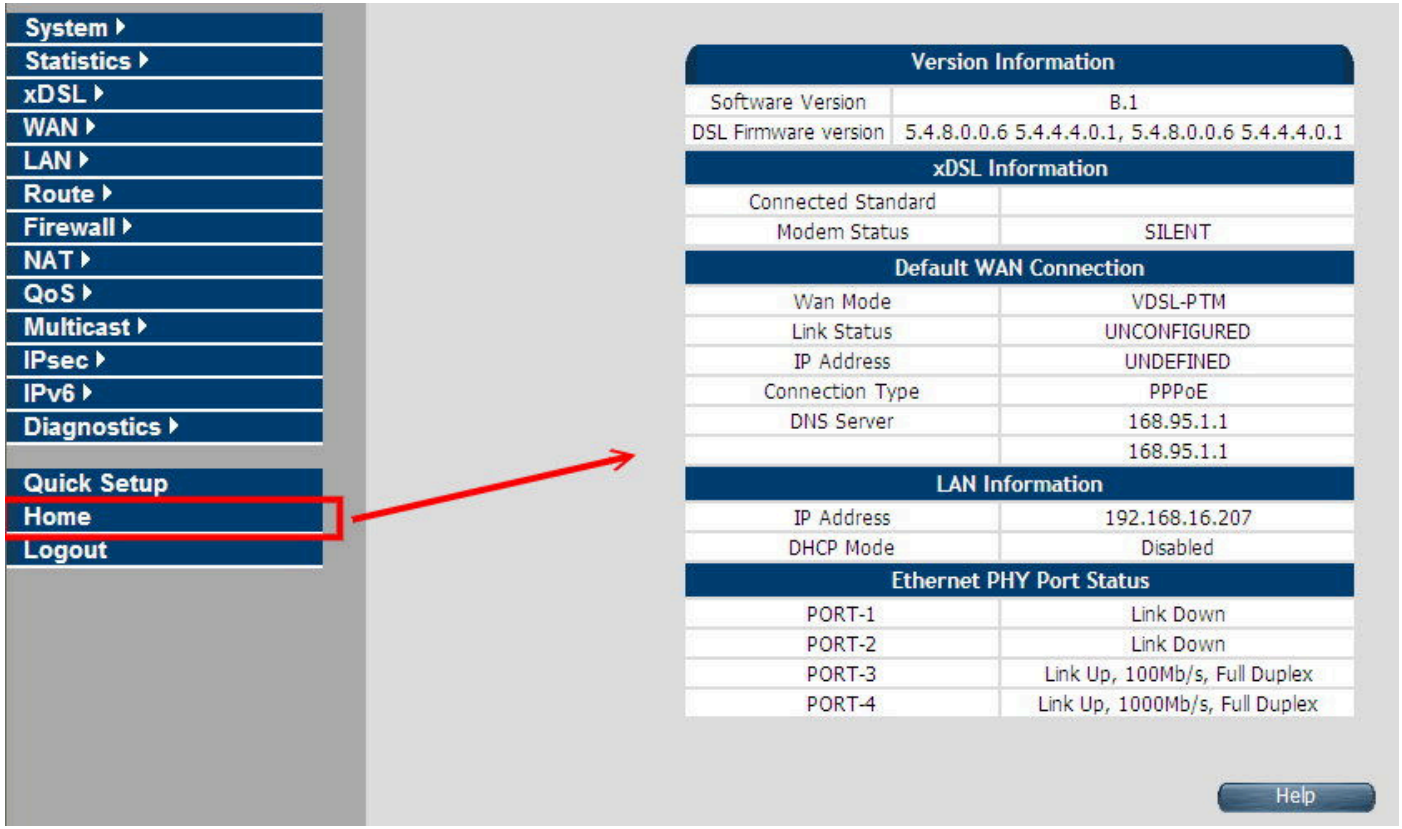



**Figure 4.1.1 Home Information**

The screen contains the following details:

**Fields in Home page**

| Field | Description |
|---|---|
| **Version Information** | |
| Software Version | Shows the current version of NV-600A Software loaded on the device. |
| DSL Firmware version | Shows the current version of xDSL firmware loaded on the device. Applicable only for DSL platforms. |
| **xDSL Information** | |
| Connected Standard | The DSL Standard which is being used currently between DSL CPE and DSLAM. |
| Modem Status | Displays the status of the physical xDSL Line in terms of the modem and mode selected. |
| **Default WAN Connection** | |
| Wan Mode | Current WAN mode being used in CPE. |
| Link Status | Shows the status of default WAN connection. |
| IP Address | Shows the IP address of default WAN connection. |
| Connection Type | Shows the Connection Type information of default WAN connection. |
| DNS Server | Shows the primary and secondary DNS servers configured in default WAN connection. |
| **LAN information** | |
| IP Address | It shows the IP address of LAN interface of CPE. This IP address is to be used for accessing the CPE device from LAN side e.g. Web UI or UPnP sessions. |
| DHCP Mode | Shows the DHCP Mode on LAN interface of CPE device. |
| **Ethernet PHY Port Status** | |
| PORT-1 ~PORT-4 | Shows the status of first to fourth ethernet port of CPE device. |

## 4.1.2 Quick Setup

The **Quick Setup** is located on the left side of the screen. Quick Setup provides a simple and easy step for applying minimal configuration to CPE device, for making it ready to use. The **CPE Quick Setup** window is displayed as shown in Figure 4.1.2. Click on Quick Setup to view and configure the following connections.

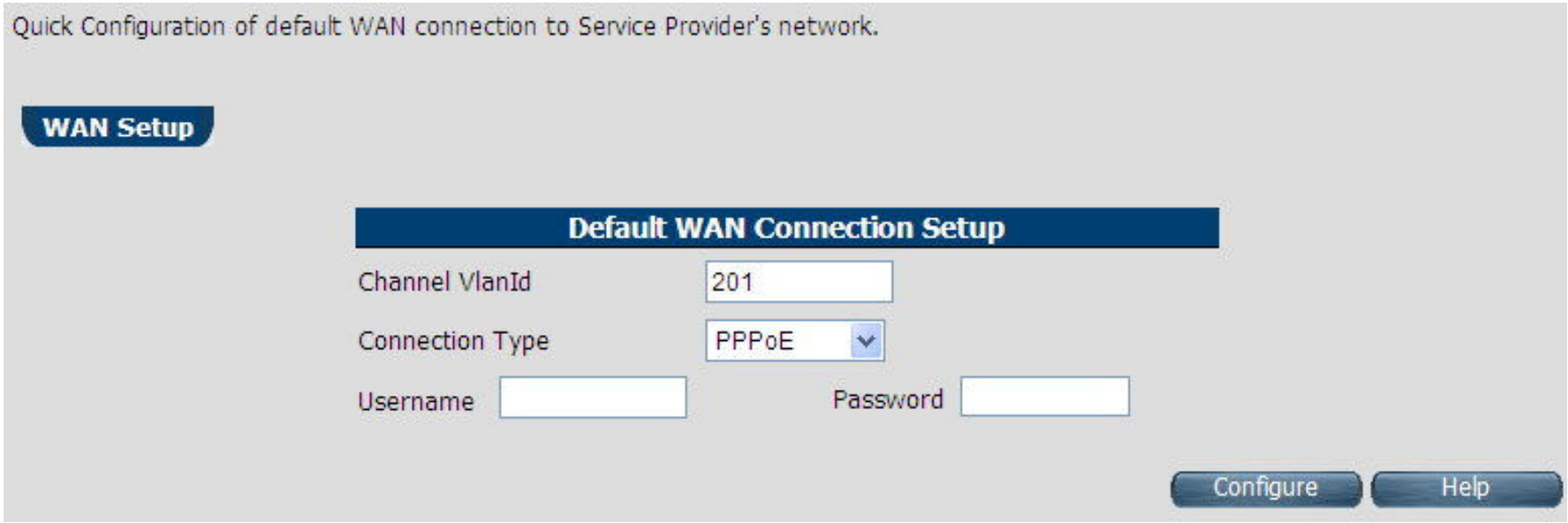



**Figure 4.1.2 Quick Setup**

◆ **WAN Setup**

When the user clicks on Quick Setup, the **WAN Setup** tab is displayed as shown in Figure 4.1.2.1. The **WAN Setup** enables the user to configure the default WAN connection. The user has to supply fields, and the CPE device will take all necessary actions to ensure the default WAN is configured. In case, the WAN connection is already existing in CPE device, the same gets re-created with newly supplied attributes from the user. The default WAN Setup configuration shows the Bridged status.

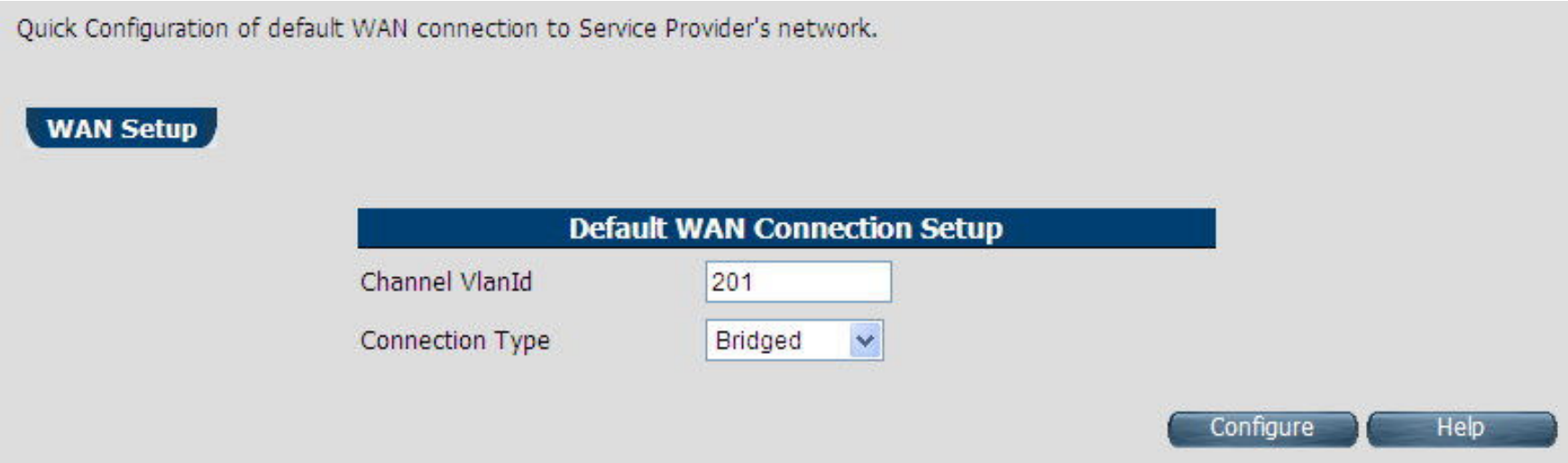



**Figure 4.1.2.1 WAN setup Bridged**

The screen contains the following details:

**Fields in Home page**

| Field | Description |
|---|---|
| Channel VlanId | Specify VLAN Id. Reserved or internally used VLANs that cannot be configured in Quick WAN Setup are listed. |
| Connection Type | Specify the Connection Type from the dropdown. Available options are **Bridged**, **Dynamic** and **Static**. |

◆ Click **Configure** to configure the default WAN connection setup.

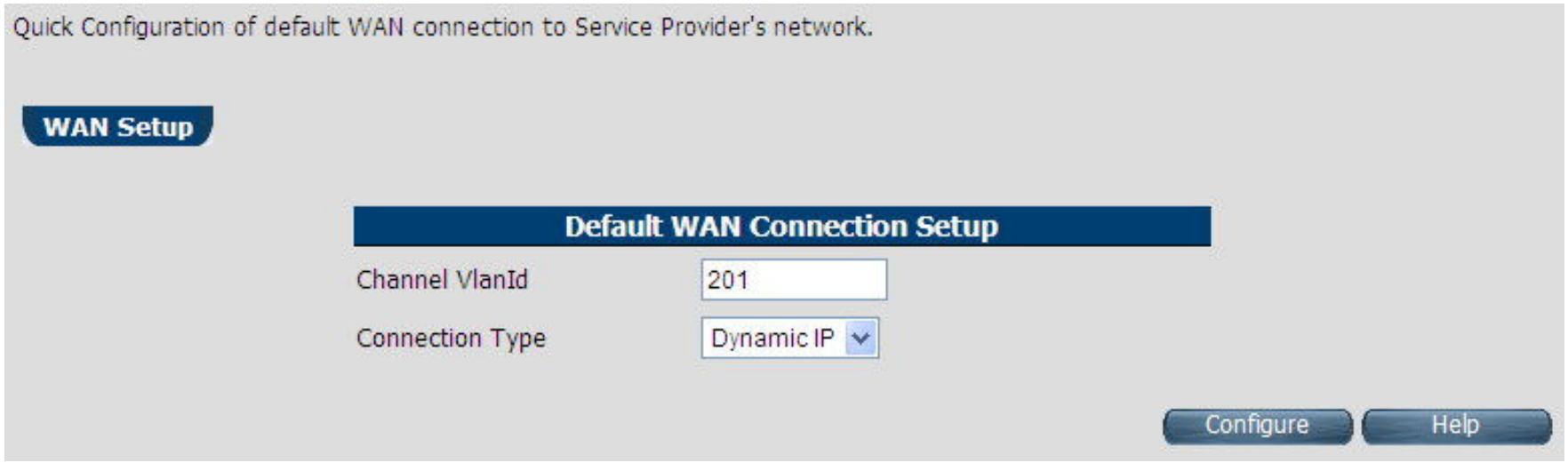



**Figure 4.1.2.2 WAN setup Dynamic IP**

The screen contains the following details:

**Fields in WAN setup Dynamic IP**

| Field | Description |
|---|---|
| Channel VlanId | Specify VLAN ID. |
| Connection Type | Specify the Connection Type from the dropdown. |

◆ Click **Configure** to configure the selected WAN connection setup.

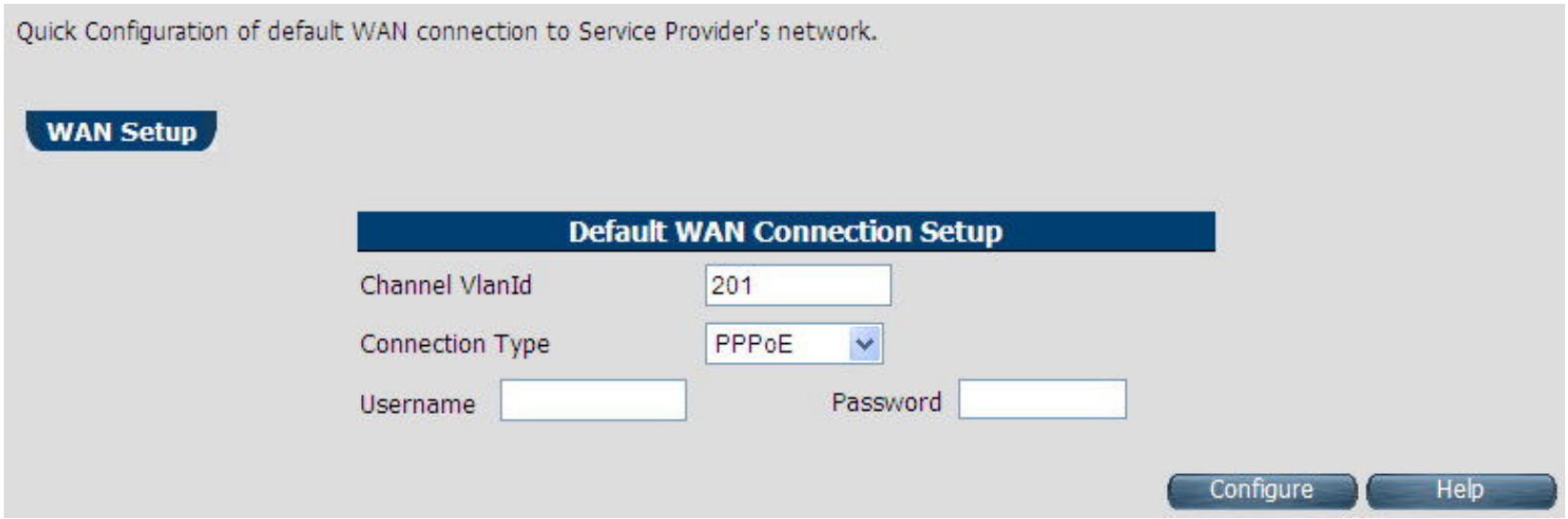



**Figure 4.1.2.3 WAN setup PPPoE**

The screen contains the following details:

**Fields in WAN setup PPPoE**

| Field | Description |
|---|---|
| Channel VlanId | Specify VLAN ID. |
| Connection Type | Specify the Connection Type from the dropdown. |
| Username | Enter a valid Username. |
| Password | Enter a valid Password. |

◆ Click **Configure** to configure the selected WAN connection setup.

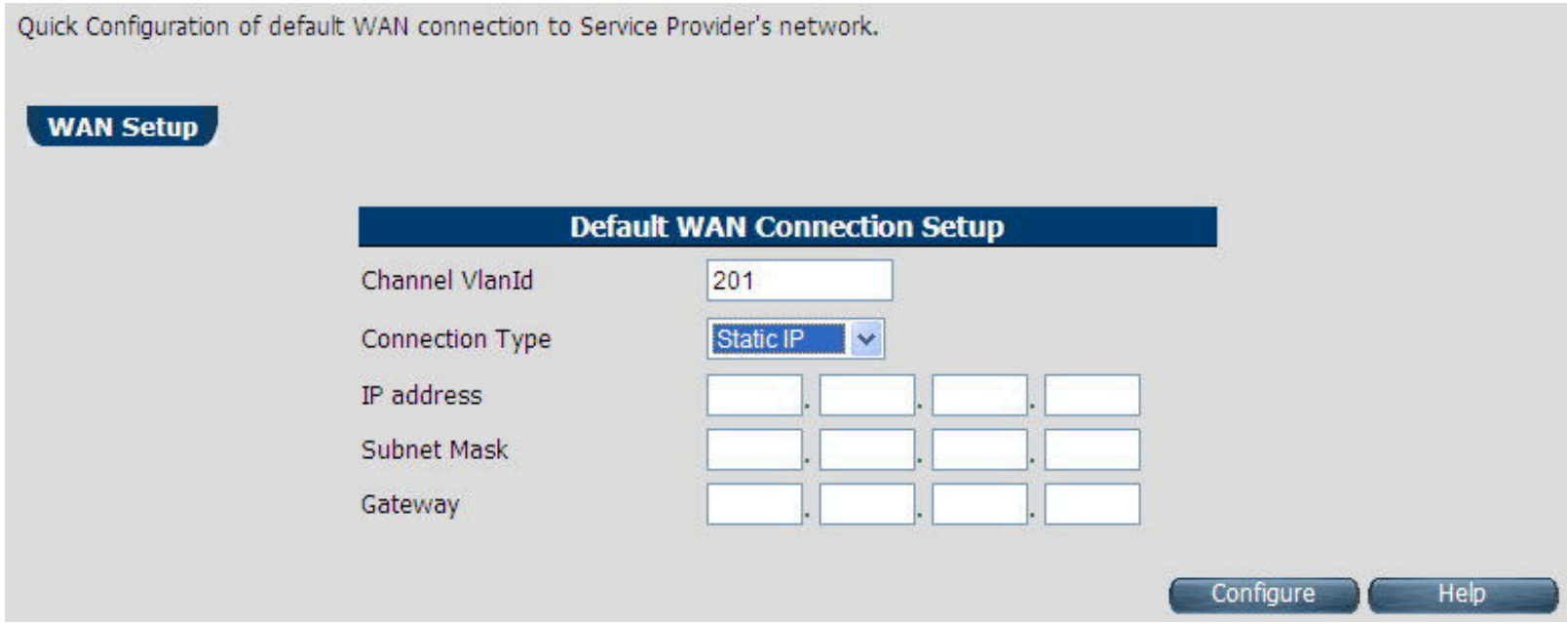



**Figure 4.1.2.4 WAN setup Static IP**

The screen contains the following details:

**Fields in WAN setup Static IP**

| Field | Description |
|---|---|
| Channel VlanId | Specify VLAN ID. |
| Connection Type | Specify the Connection Type from the dropdown. |
| IP Address | Specify the IP Address of NV-600A CPE's WAN link. |
| Subnet Mask | Specify the Subnet Mask of NV-600A CPE's WAN link. |
| Gateway | Specify the Gateway address of the NV-600A CPE's WAN. |

◆ Click **Configure** to configure the selected WAN connection setup.

**Note:**

When WAN mode is other than ATM, the corresponding web pages will be available in WAN setup. Those web pages will not ask users for fields like ATM VCC etc.

## 4.2 Select the Menu Level

There is an easy Setup for end users at the setup of NV-600A with **SYSTEM**, **Statistics**, **xDSL**, **WAN**, **LAN**, **Route**, **FIREWALL**, **NAT**, **QoS** , **Multicast**, **Ipsec** , **IPv6**, **Diagonstics**, **Quick Setup**, **Home**, **Logout** for more detail configurations.

**Figure 4.2 Select the Menu Level (NV-600A)**

## 4.3 Select "SYSTEM"

Select the "SYSTEM". The menu below will be used frequently. It includes the sub-menus of **Host Name Config**、**System Time**、**Administrator Settings**、**Web Settings**、**Software/Firmware Upgrade**、**System Log**、**SSL Certificat**、**Mac Table Aging Time**、**Vlan Tag Pass Through** and **Reset**. A screen is displayed as shown in Figure 4.3

**Figure 4.3 System Setup**

### 4.3.1 Host Name Config

To configure the host name of NV-600A, users have to enter host and domain name. Click the **Host Name Config** link (**System > Host Name Config)** on the left navigation bar. A screen is displayed as shown in Figure 4.3.1.

**Figure 4.3.1 Host Name Config**

**Fields in Host Name Config**

| Field | Description |
|---|---|
| Host Name | Enter the host name of the VDSL2 CPE. This is used to address VDSL2 CPE, by using this name instead of typing the IP address. Maximum Characters: 60. |
| Domain Name | Enter the domain name of the VDSL2 CPE. Maximum Characters: 60. |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

## 4.3.2 System Time

Users can set System Time by connecting to a **Simple Network Time Protocol** (SNTP) server allows the Modem to synchronize the system clock to the global Internet. The synchronized clock in the Modem is used to record the security log and control client filtering. This page provides the time zone selection and NTP (Network Time Protocol) configuration. Click the **System Time** link (**System > System Time)** on the left navigation bar and a screen is displayed as shown in Figure 4.3.2.

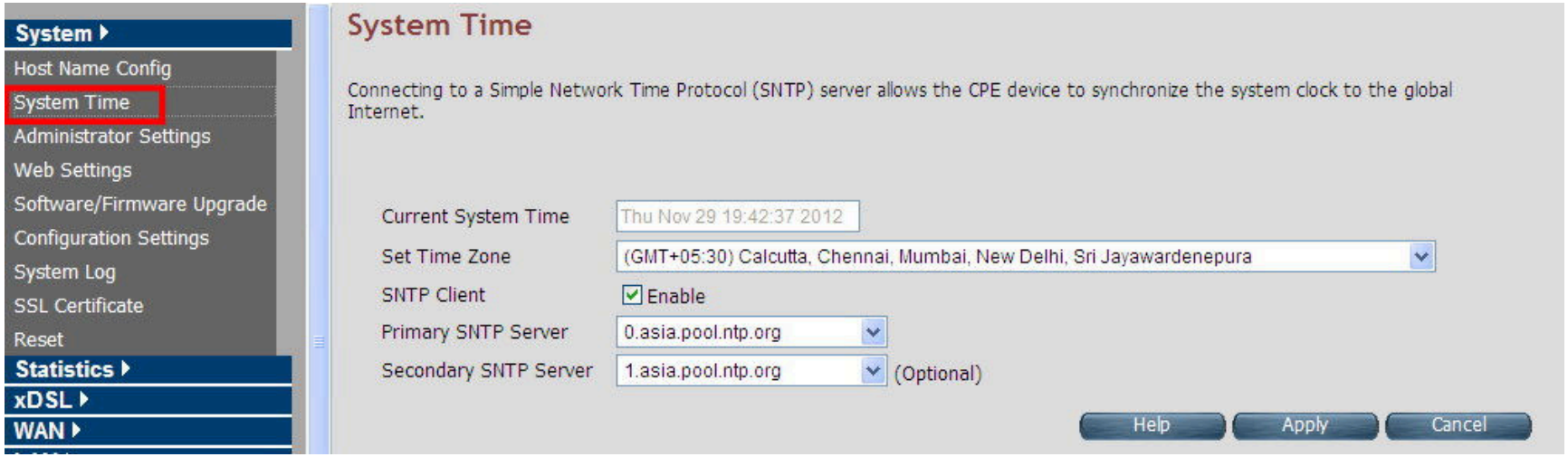



**Figure 4.3.2 System Time Configuration**

**Fields in System Time**

| Field | Description |
|---|---|
| Current System Time | Current Time in System is shown in Day, Date and Time of day. |
| Set Time Zone | Select the time zone from the list of worldwide time zones in pull-down options. |
| SNTP Client | Tick on Check box, if SNTP client has to be enabled. |

**Fields in System Time (Cont'd)**

| Field | Description |
|---|---|
| Primary SNTP Server | Main NTP Server to be selected from dropdown list. |
| Secondary SNTP Server | Backup NTP Server (optional). |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

**Note:**

**Static Routing functionality is used to define the connected Gateway between the LAN and WAN.** For example, if we want to activate the Network Time Protocol (NTP) service, and we have to define the Gateway connected to NTP server in the WAN. Please refer to "static routing" for user's reference.

## 4.3.3 Administrator Settings

To change the password for the administrator, click the **Administrator Settings** link (**System** > **Administrator Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.3.3. This page allows the user to change the login password.

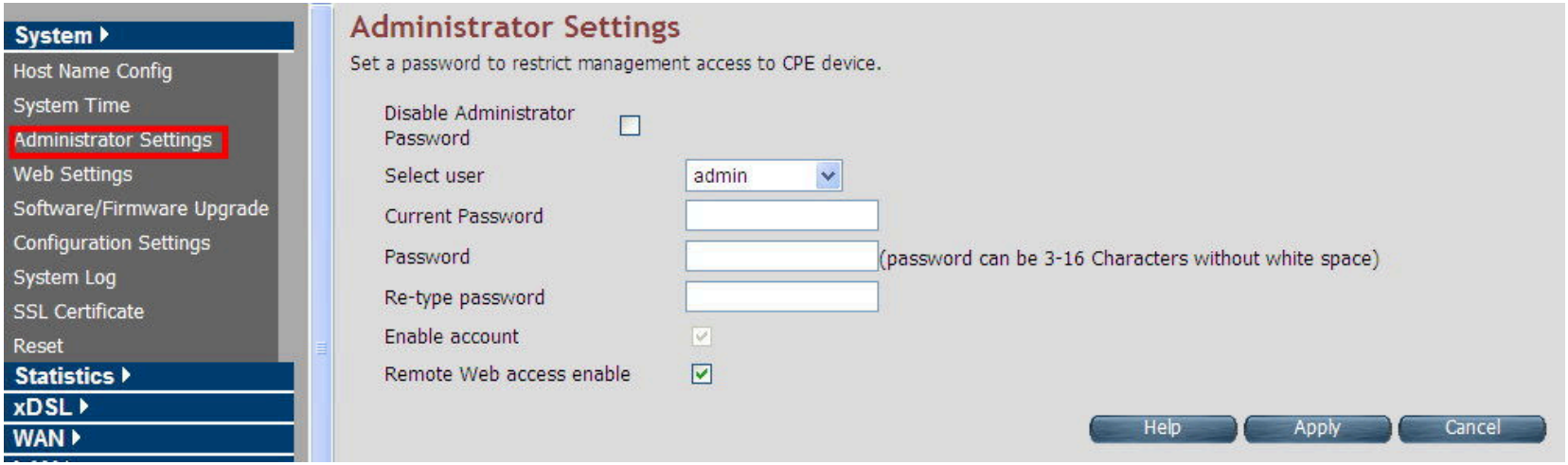



**Figure 4.3.3 Administrator Settings**

**Fields in Administrator Settings**

| Field | Description |
|---|---|
| Disable Administrator Password | Select this to disable the web prompts for user login password. |
| Select User | Select user type. The available options are **Admin** and **support user**. |
| Current Password | The user should specify the current login password. |
| Password | The user should specify the new password desired. The password should be at least 3 characters and not more than 16 characters in length without a white space. |

**Fields in Administrator Settings (Cont'd)**

| Field | Description |
|---|---|
| Re-type Password | The user should re-type the new password entered in previous field. |
| Enable Account | To enable the user account login. |
| Remote Web Access Enable | To enable web access from WAN side. |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

## 4.3.4 Web Settings

This page shows the details of Web login timeout settings for the CPE device in seconds. Click the **Web Settings** link (**System** > **Web Settings**) on the left navigation bar and a screen is displayed as shown in Figure 4.3.4

**Figure 4.3.4 Web Settings**

**Fields in Web Settings**

| Field | Description |
|---|---|
| Auto Logout Duration | This is the logout duration after which the web session is automatically logged out. The unit is in seconds. |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

## 4.3.5 Software/Firmware Upgrade

To update the system firmware, click the **Software/Firmware Upgrade** link (**System > Software/Firmware Upgrade**) on the left navigation bar. A screen displays the current version of NV-600A Software running on the device as shown in Figure 4.3.5

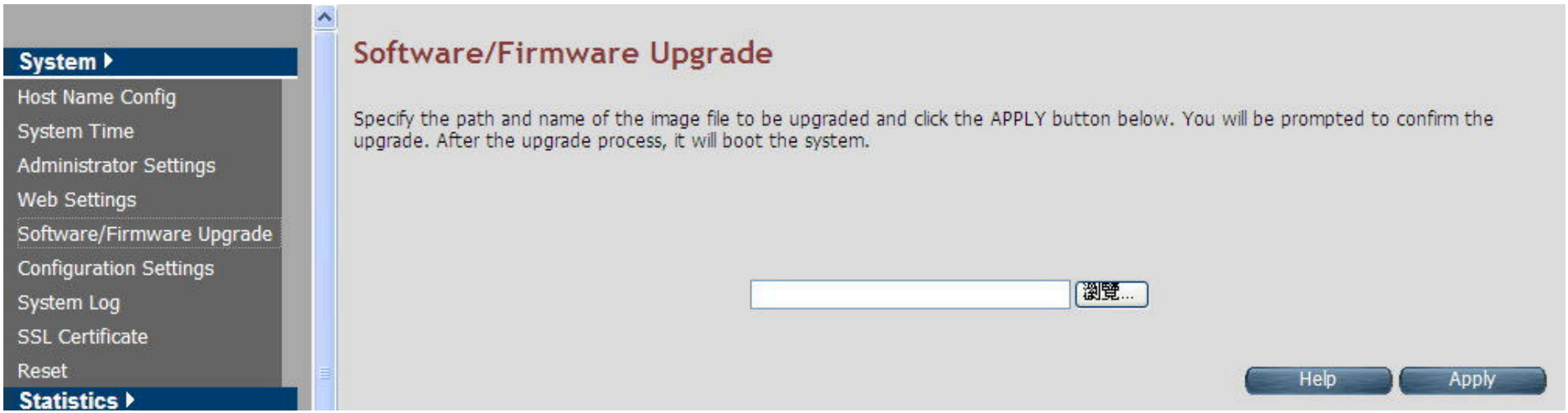



**Figure 4.3.5 Software/Firmware Upgrade**

- Click **Browse** to specify the software image file from host, to be upgraded in system.
- Click **Apply** to start the software upgrade process.

**Note:**

Users can click Home on the left navigation bar to view the current software version.

## 4.3.6 Configuration Settings

To manage the configuration of the system, click the **Configuration Settings** link (**System > Configuration Settings**) on the left navigation bar. This page allows users to backup the current configuration of CPE to host PC or restore the previously backed-up configuration in host PC to CPE as displayed in Figure 4.3.6

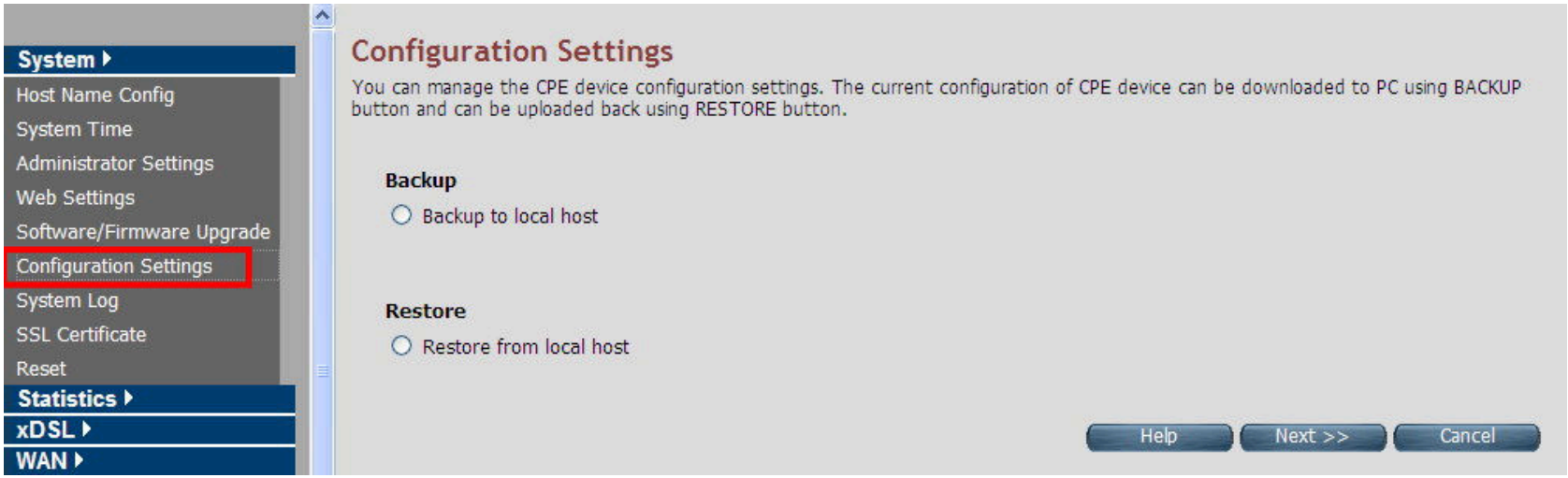



**Figure 4.3.6 Configuration Settings**

**Fields in Configuration Settings**

| Field | Description |
|---|---|
| Backup to local host | This will back up the current active configuration of CPE in Host machine. |
| Restore from local host | This will load the user supplied configuration to CPE from Host machine. |

- Click **Next** to start the firmware upgrade process.
- Click **Cancel** to exit from this page without saving the changes.

## ■ Backup Current Active Configuration

As mentioned before, this option allows users to back up the current active configuration running in router system. This is very helpful when a user wants to backup the current working configuration of router for rollbacks, if needed in future. It is recommended that before any complex nature of configuration is done by the user the current active configuration should be backed up in the host machine. The Local Host Configuration backup is shown in Figure 4.3.6.1

**Figure 4.3.6.1 Configuration Backup**

When users click **the Backup** button as shown in Figure 4.3.6.1, it will back up the config settings of CPE in connected PC from where Web UI is being accessed.

## ■ Restore Previous Backed-up Configuration

As mentioned before, this option allows users to restore the earlier backed up configuration in router system. This operation is handy for restoring the system to last backed-up configuration mode. The Local Host Configuration restore is shown in Figure 4.3.6.2. The system will go for reboot after configuration is restored. When CPE boots up it will be running with newly applied configuration.

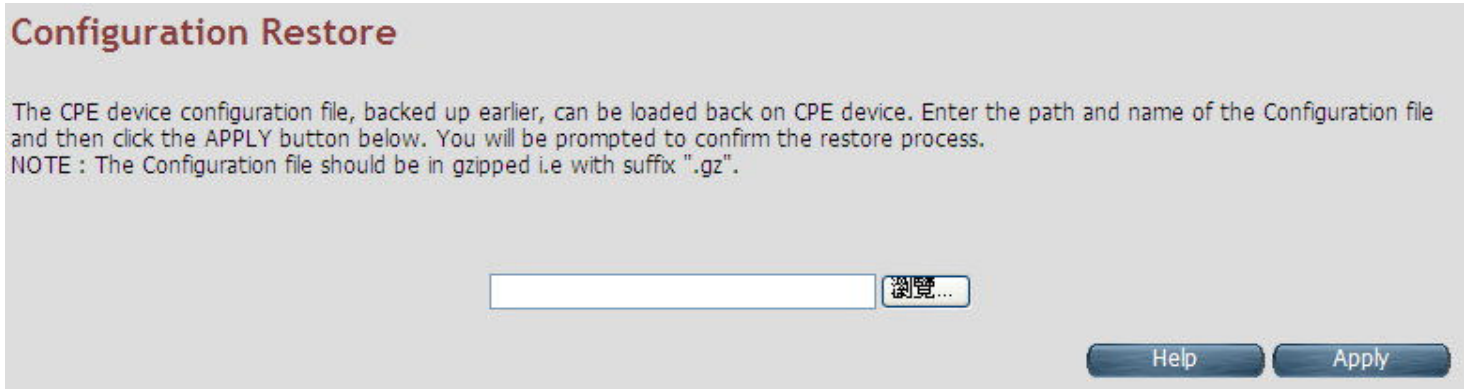



**Figure 4.3.6.2 Configuration Restore**

◆ Click **the Apply** button to restore the config settings.

### 4.3.7 System Log

To view the logs produced in system, click the **System Log** link (**System > System Log**) on the left navigation bar. A screen is displayed as shown in Figure 4.3.7

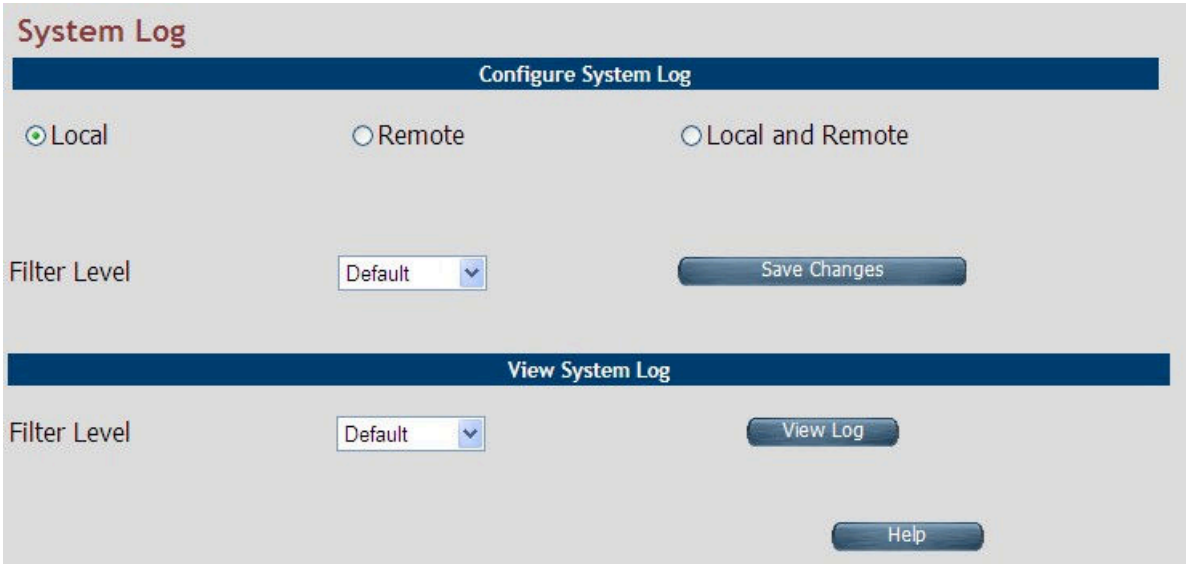



**Figure 4.3.7 System Log**

This page allows users to manage logging options in CPE device.

- If "Local" is selected, the events are logged locally in the system.
- If "Remote" is selected, the messages are logged to a remote server.
- If the "Local and Remote" option is selected, messages are logged locally in the system as well as to the remote server.

The events pertaining to priority equal to or higher to the selected level will be logged. The "Default" level logs all events.

For viewing system log, the events corresponding to the priority level equal to or higher than the selected level will be displayed here.

The screen holds the following details: **Fields in System Log**

| Field | Description |
|---|---|
| Configure System Log | Select the mode of log. The possible options are:<br>◆ **Local Mode:** The log text is displayed in web browser itself.<br>◆ **Remote Mode:** Specify the IP address and UDP port number for log transfer using syslog.<br>◆ **Local and Remote Mode:** This supports both options mentioned above. |
| Filter Level | The user can apply one of the following filters to record logging above the specified level. Click on <SAVE CHANGES> button for applying the log level selection.<br>◆ **Default:** The default pre-selected levels of logs are recorded.<br>◆ **Debug:** Debug and above levels of logs are recorded.<br>◆ **Info:** Informative and above level of logs are recorded.<br>◆ **Notice:** Notice type and above level of logs are recorded.<br>◆ **Warning:** Warning type and above levels of logs are recorded.<br>◆ **Error:** Error type and above levels of logs are recorded.<br>◆ **Critical:** Critical type and above levels of logs are recorded.<br>◆ **Alert:** Alert type and above level of logs are recorded.<br>◆ **Emerg:** Emergency type of log information is recorded. |
| View System Log | The user can apply one of the following filters to view specific logs of certain level:<br>◆ **Default:** The default pre-selected levels of logs are viewed.<br>◆ **Debug:** Debug and above levels of logs are viewed.<br>◆ **Info:** Informative and above-level logs are viewed.<br>◆ **Notice:** Notice type and above level of logs are viewed.<br>◆ **Warning:** Warning type and above levels of logs are viewed.<br>◆ **Error:** Error type and above levels of logs are viewed.<br>◆ **Critical:** Critical type and above levels of logs are viewed.<br>◆ **Alert:** Alert type and above level of logs are viewed.<br>◆ **Emerg:** Emergency type of log information is viewed. |

- Click **Save Changes** to configure the system log settings.
- Click **View Log** to fetch the logs in browser.

When users click **View log** button, a screen is displayed as shown in Figure 4.3.7.1. This screen is an example of system log of default level as shown in the browser.

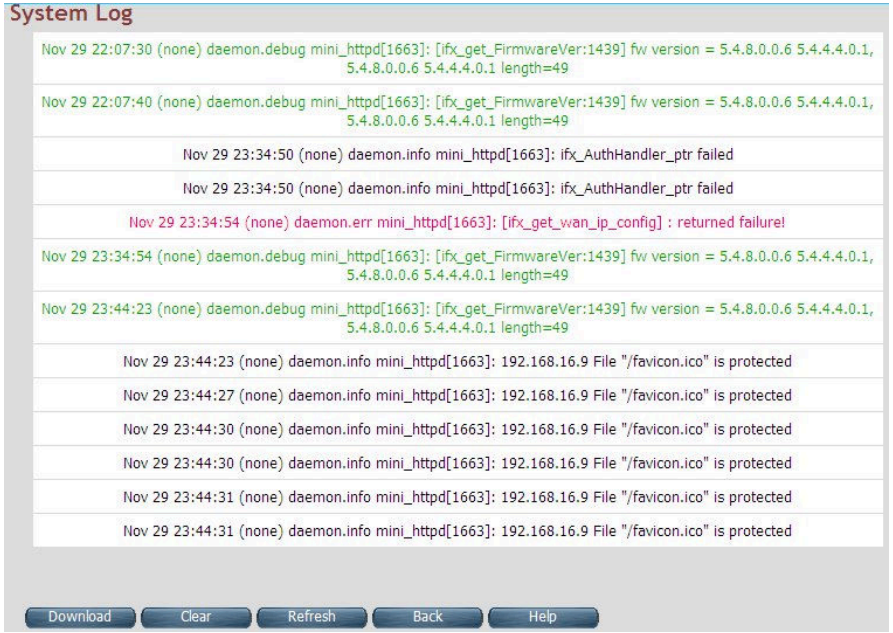



**Figure 4.3.7.1 View System Log**

For the ease of readability, log messages of different levels are using different colors.

**For example:** all the debug messages are shown in green colored text.

- Click **Download** to save the file in Host Computer.
- Click **Clear** to clear the log from the system.
- Click **Refresh** to get the recent log.
- Click **Back** to go back to System Log page.

## 4.3.8 SSL Certificate

To install an SSL Certificate for SSL tunnel, click the **SSL Certificate** link (**System > SSL Certificate**) on the left navigation bar. A screen is displayed as shown in Figure 4.3.8

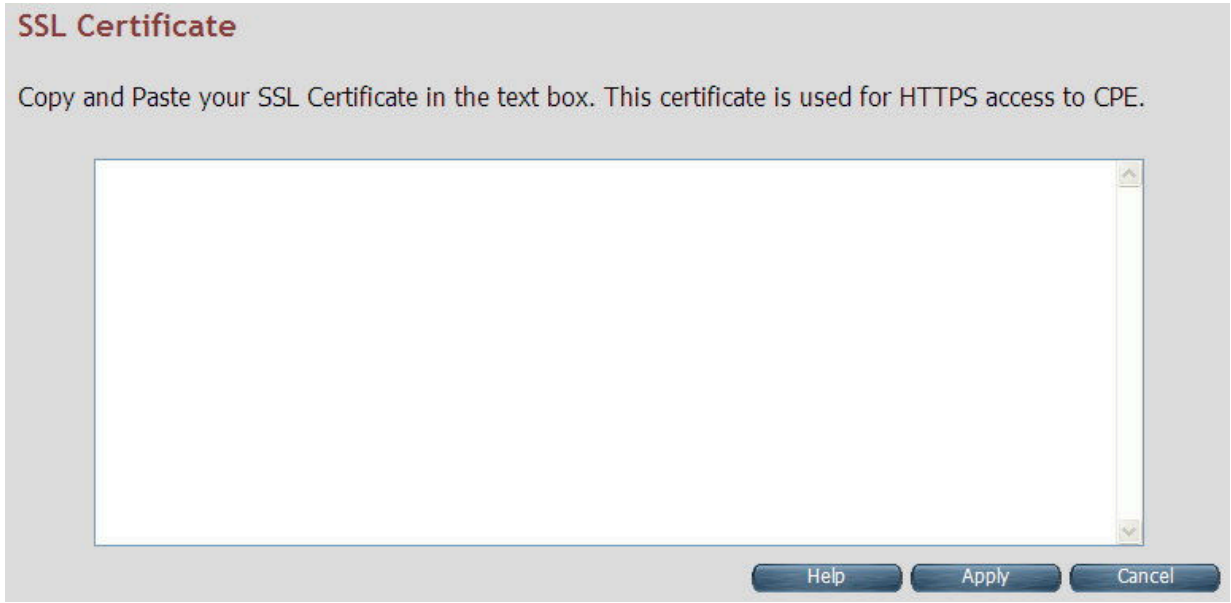



**Figure 4.3.8 SSL Certificate**

- Click **Apply** to install the entered certificate.
- Click **Cancel** to cancel the installation of entered certificate.

### 4.3.9 Mac Table Aging Time

Click the **Mac Table Aging Time** on the left navigation bar. This page allows users to select the Mac Table Aging Time in Figure 4.3.9. The default of Mac Table is 300 seconds.

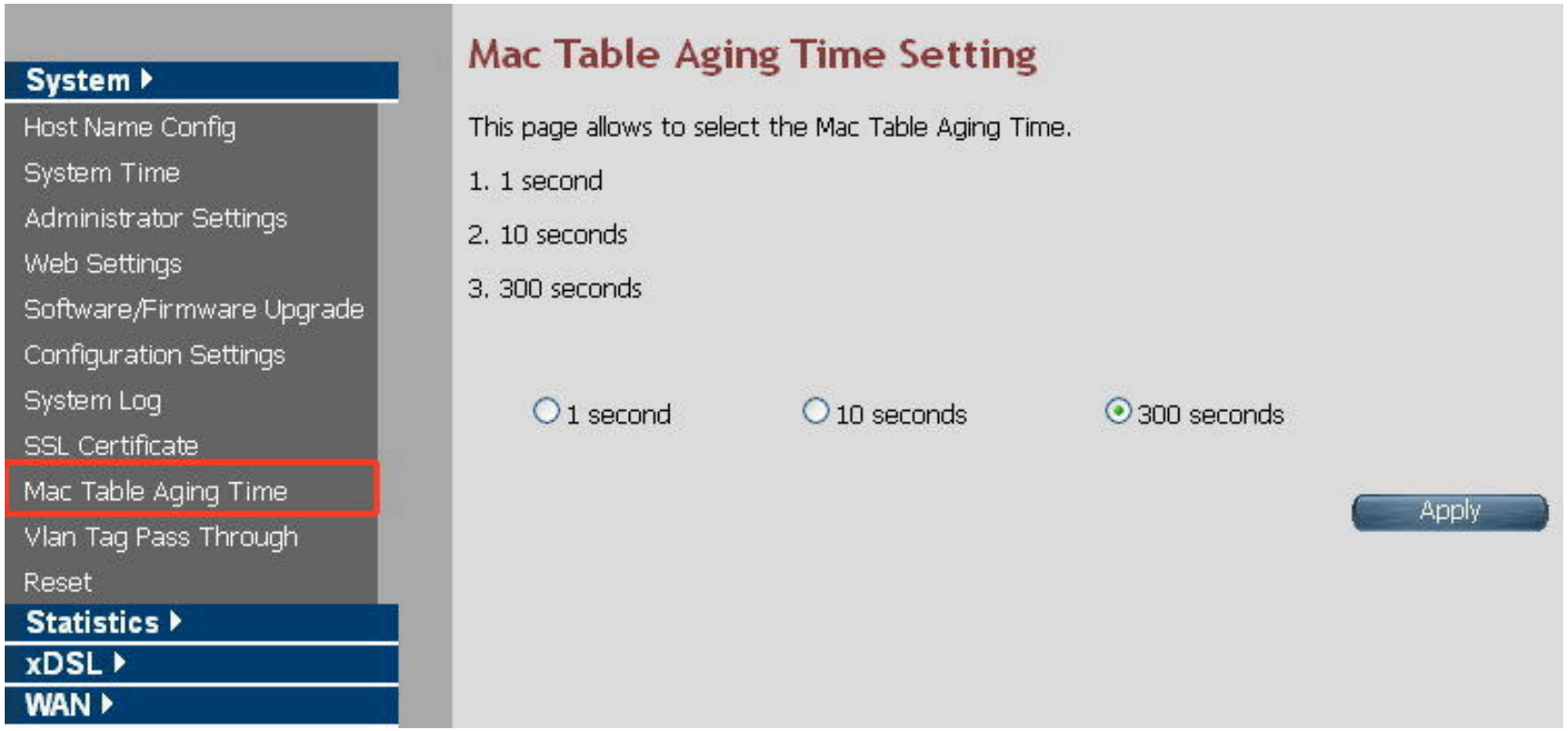



**Figure 4.3.9 Mac Table Aging Time**

- Click **Apply** button to select Mac Table Aging Time setting. Click **Apply** button to select Mac Table Aging Time setting.

## 4.3.10 Vlan Tag Pass Through Mode Setting

Click the **Vlan Tag Pass Through** on the left navigation bar. This page allows users to select the Vlan Tag Pass Through Mode in Figure 4.3.10

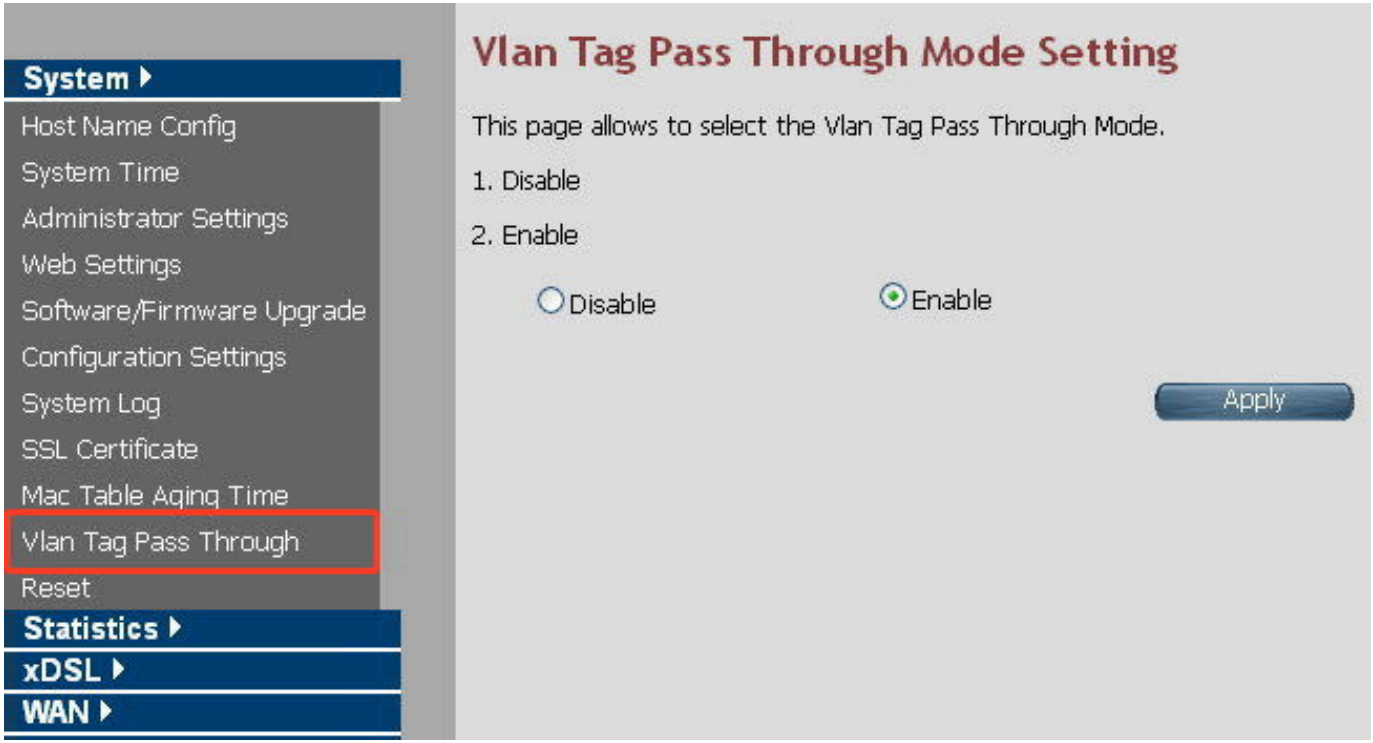



**Figure 4.3.10 Vlan Tag Pass Through Mode**

- Click **Apply** button to select Vlan Tag Pass Through Mode.

## 4.3.11 Reset

To reboot the system, click **Reset** link (**System > Reset**) on the left navigation bar. A screen is displayed as shown in Figure 4.3.11

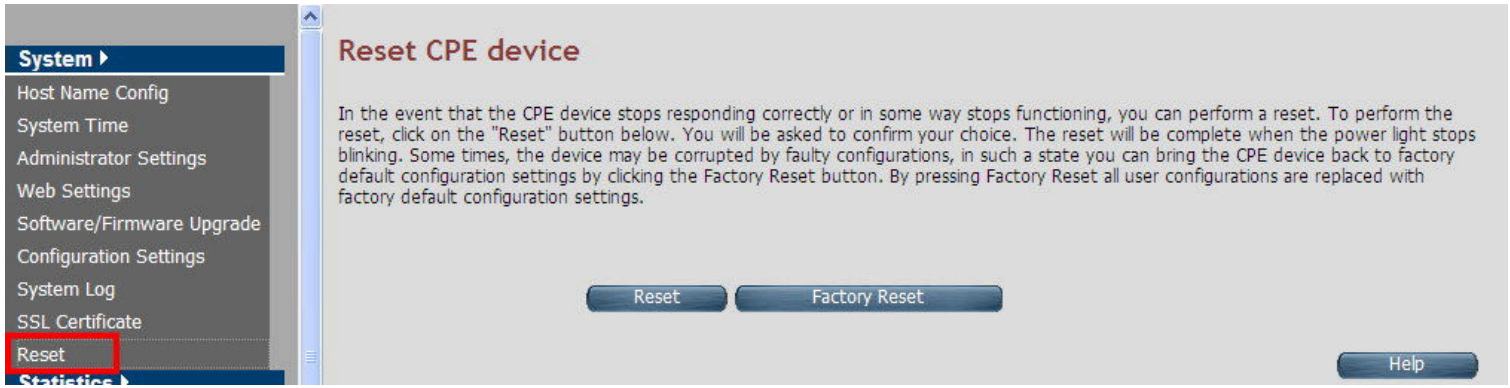



**Figure 4.3.11 Reset**

- Click Reset to reboot the system. This does not change the configurations existing in the system.
- Click Factory Reset to reset the device configuration to factory defaults configuration. This operation will result in saving the current configuration and reverted back to factory shipped configuration.

When **Reset** or **Factory Reset** is clicked, a confirmation message is displayed as shown in Figure 4.3.11.1

**Figure 4.3.11.1 Reset Confirmation Message**

- Click **Ok** to perform the operation on CPE.
- Click **cancel** to exit from this page.

## 4.4 Select "Statistics"

Select the "Statistics" link on left navigation menu. The menu below includes the sub-menus of LAN and WAN. A screen is displayed as shown in Figure 4.4.

**Figure 4.4 Statistics on the left navigator bar**

## 4.4.1 LAN

To get the LAN Statistics, click the **LAN** link (**Statistics > LAN**) on the left navigation bar. A screen is displayed as shown in Figure 4.4.1

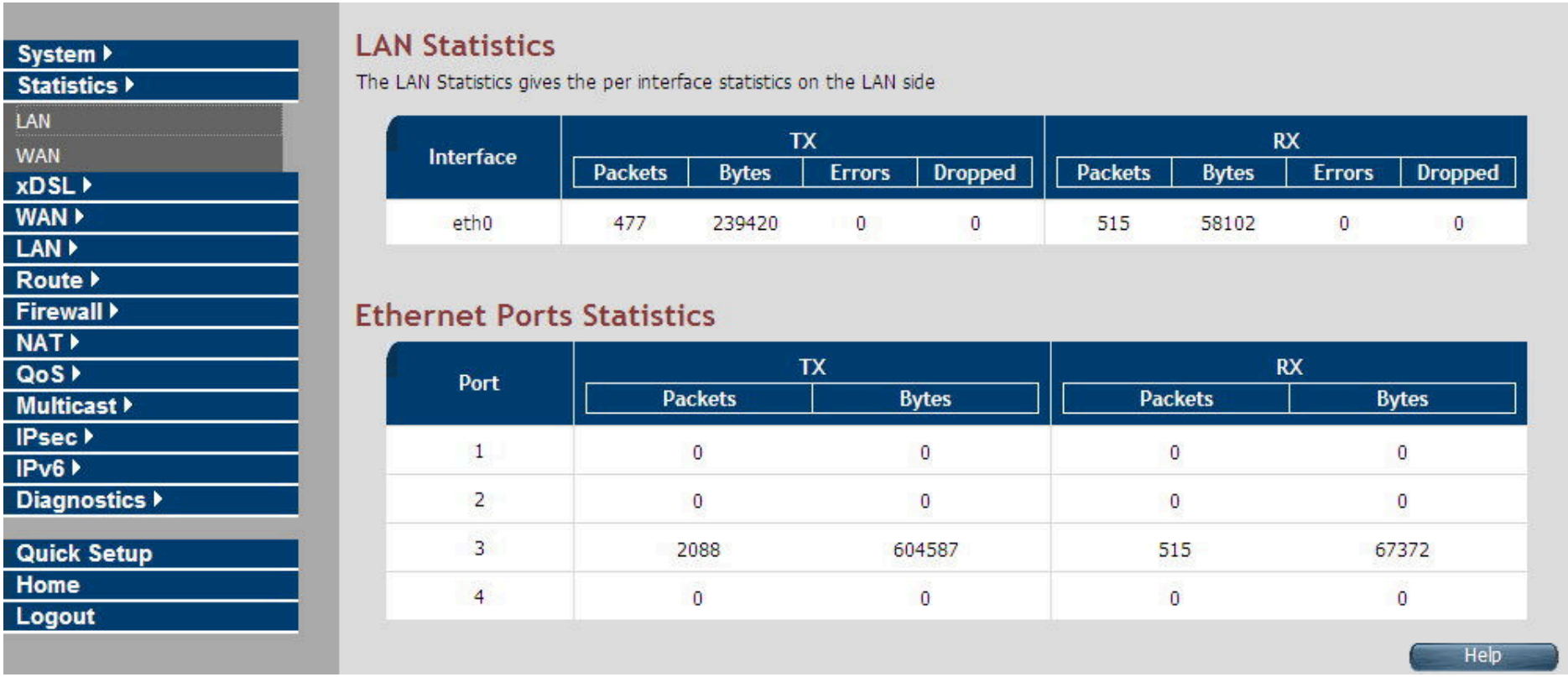



**Figure 4.4.1 LAN Statistics**

The screen contains the following details:

**Fields in LAN Statistics:**

| Field | Description |
|---|---|
| Interface | Name of LAN Interface (e.g. eth0, usb0 etc.) |
| TX | Transmit Counters:<br>◆ Total packets transmitted from this interface.<br>◆ Total bytes transmitted form this interface.<br>◆ Total Error packets on this interface.<br>◆ Total Dropped packets on this interface. |
| RX | Receive Counters:<br>◆ Total packets received from this interface.<br>◆ Total bytes received form this interface.<br>◆ Total Erroneous packets on this interface.<br>◆ Total Dropped packets on this interface. |

## 4.4.2 WAN

To get WAN Statistics, click the **WAN** link (**Statistics > WAN**) on the left navigation bar. A screen is displayed as shown in Figure 4.4.2

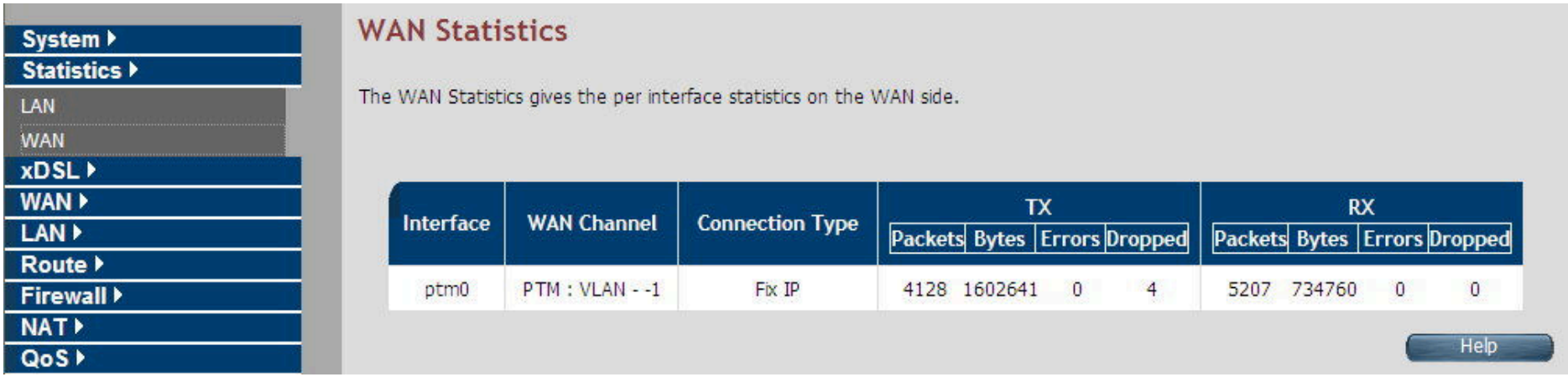



**Figure 4.4.2 WAN Statistics**

The screen contains the following details:

**Fields in WAN Statistics:**

| Field | Description |
|---|---|
| Interface | Name of WAN Interface. |
| WAN Channel | Information about WAN Channel such as VCC or WAN-ethernet channel. |

| | |
|---|---|
| Connection Type | Type of WAN Connection. |

**Fields in WAN Statistics** (cont'd)**:**

| Field | Description |
|---|---|
| TX | Transmit Counters for WAN interface:<br>◆ Total packets transmitted from this interface.<br>◆ Total bytes transmitted form this interface.<br>◆ Total Erroneous packets transmitted on this interface.<br>◆ Total Dropped packets transmitted on this interface. |
| RX | Receive Counters for WAN interface:<br>◆ Total packets received from this interface.<br>◆ Total bytes received form this interface.<br>◆ Total Erroneous packets received on this interface.<br>◆ Total Dropped packets on this interface. |

## 4.5 Select "xDSL"

Users can view the **xDSL** link on the left navigation bar of the CPE Home page. This web page is available only on DSL platforms. Select the "xDSL". The menu below includes the sub-menus of xDSL Status. A screen is displayed as shown in Figure 4.5.

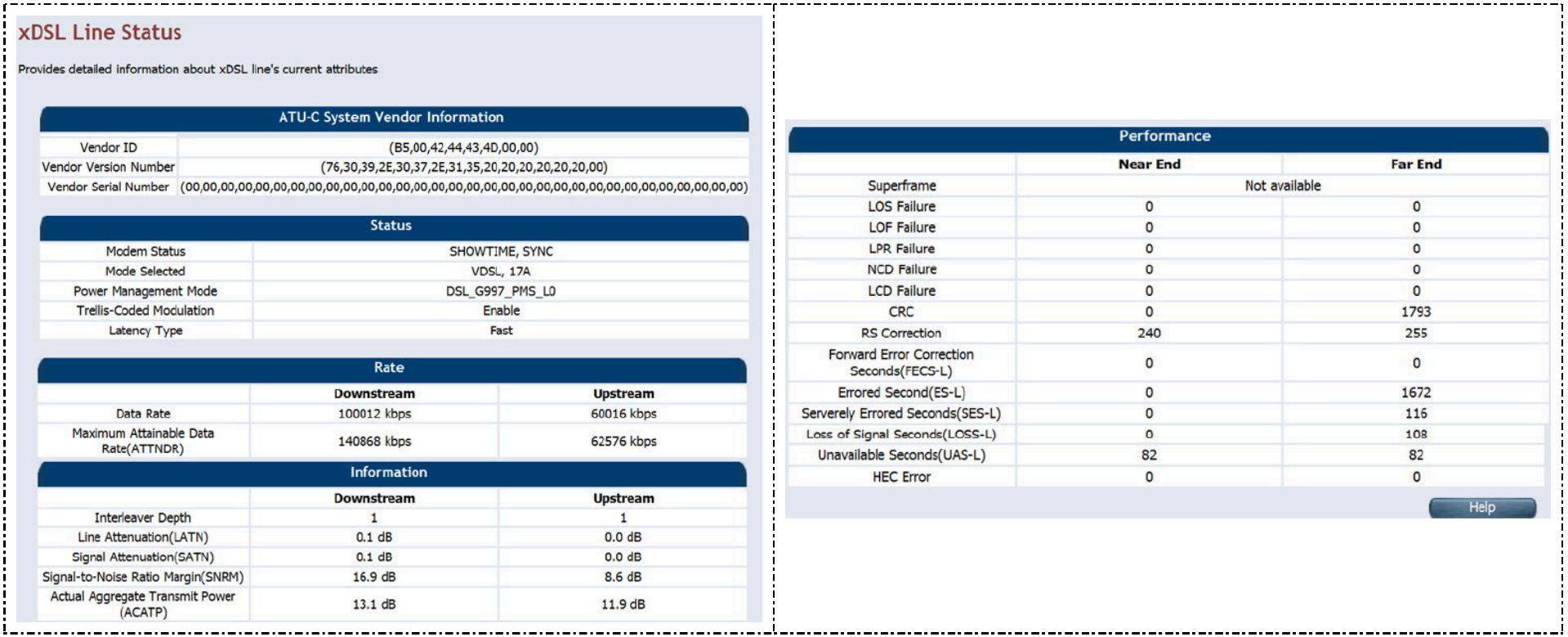
**Figure 4.5 Select xDSL**

**Note:**

These options help to monitor and configure the DSL physical parameters in the device.

## 4.5.1 xDSL Status

To view the xDSL Status, click the **xDSL Status** link (**xDSL > xDSL Status**) on the left navigation bar. A screen is displayed as shown in Figure 4.5.1



xDSL Line Status

Provides detailed information about xDSL line's current attributes

| ATU-C System Vendor Information | |
|---|---|
| Vendor ID | (B5,00,42,44,43,4D,00,00) |
| Vendor Version Number | (76,30,39,2E,30,37,2E,31,35,20,20,20,20,20,20,00) |
| Vendor Serial Number | (00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00) |

| Status | |
|---|---|
| Modem Status | SHOWTIME, SYNC |
| Mode Selected | VDSL, 17A |
| Power Management Mode | DSL_G997_PMS_L0 |
| Trellis-Coded Modulation | Enable |
| Latency Type | Fast |

| Rate | Downstream | Upstream |
|---|---|---|
| Data Rate | 100012 kbps | 60016 kbps |
| Maximum Attainable Data Rate(ATTNDR) | 140868 kbps | 62576 kbps |

| Information | Downstream | Upstream |
|---|---|---|
| Interleaver Depth | 1 | 1 |
| Line Attenuation(LATN) | 0.1 dB | 0.0 dB |
| Signal Attenuation(SATN) | 0.1 dB | 0.0 dB |
| Signal-to-Noise Ratio Margin(SNRM) | 16.9 dB | 8.6 dB |
| Actual Aggregate Transmit Power (ACATP) | 13.1 dB | 11.9 dB |

| Performance | Near End | Far End |
|---|---|---|
| Superframe | Not available | |
| LOS Failure | 0 | 0 |
| LOF Failure | 0 | 0 |
| LPR Failure | 0 | 0 |
| NCD Failure | 0 | 0 |
| LCD Failure | 0 | 0 |
| CRC | 0 | 1793 |
| RS Correction | 240 | 255 |
| Forward Error Correction Seconds(FECS-L) | 0 | 0 |
| Errored Second(ES-L) | 0 | 1672 |
| Serverely Errored Seconds(SES-L) | 0 | 116 |
| Loss of Signal Seconds(LOSS-L) | 0 | 108 |
| Unavailable Seconds(UAS-L) | 82 | 82 |
| HEC Error | 0 | 0 |

Help

**Figure 4.5.1 xDSL Status**

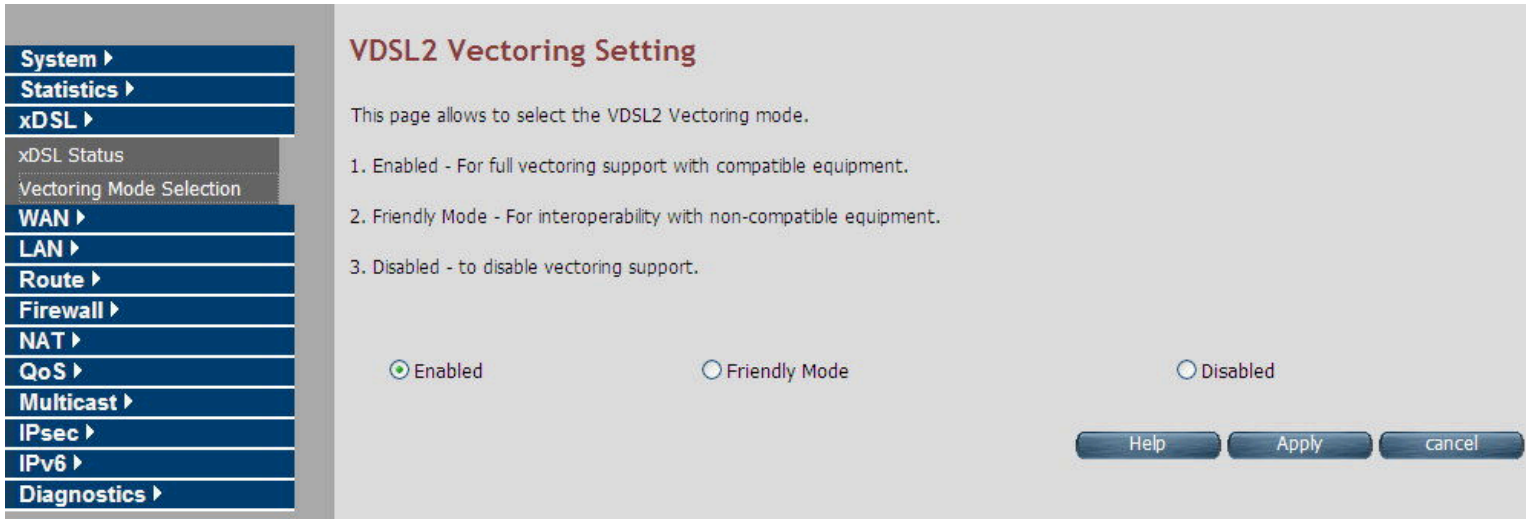
The screen contains the following details:

**Fields in xDSL Status:**

| Field | Description |
|---|---|
| ATU-C System Vendor Information | Displays the Vendor ID, Version Number and the Serial Number of the ATU-C (DSLAM). |
| Status | Displays the status of the physical xDSL Line in terms of the modem, mode selected, Trellis-Coded Modulation and the Latency Type |
| Rate | Displays the data rate and the maximum attainable data rate |
| Information | Displays the information about the xDSL line, in terms of Line Attenuation, Signal Attenuation, Signal to Noise Ratio and other such parameters |
| Performance | Displays the performance figures of the physical xDSL line |

## 4.5.2 Vectoring Mode selection

For viewing the vectoring mode, click the **Vectoring Mode Selection** link (**xDSL > Vectoring Mode Selection**) on the left navigation bar. A screen is displayed as shown in Figure 4.5.2




**Fields in Vectoring Mode Selection**

| Field | Description |
|---|---|
| Enabled | Enable VDSL2 Full Vectoring mode (Default setting), it will auto follow the CO side vectoring configuration. |
| Friendly Mode | Enable VDSL2 Vectoring-Friendly mode, it will auto follow the CO side vectoring configuration. |
| Disabled | Disable VDSL2 Vectoring feature. |

**Notes:**

1. NV-600A vdsl2 vectoring technology default setting is enabled.
2. Vectoring technology is mainly used in intensive line equipment, such as 24-Port VDSL2 IP DSLAM.
3. If users would like to use NV-600A vectoring technology, NV-600A and IP DSLAM both need support vectoring technology features and need both enabled. The NV-600A will auto follow the IP DSLAM vectoring technology configuration.
4. Vectoring technology does not support point to point applications.

**About vectoring function (Reference only):**

Vectoring is a transmission method that employs the coordination of line signals for reduction of crosstalk levels and improvement of performance. It is based on the concept of noise cancellation, much like noise-cancelling headphones. The ITU-T G.993.5 standard, "Self-FEXT cancellation (vectoring) for use with VDSL2 transceivers" (2010), also known as G.vector, describes vectoring for VDSL2. The scope of Recommendation ITU-T G.993.5 is specifically limited to the self-FEXT (far-end crosstalk) cancellation in the downstream and upstream directions. The far end crosstalk (FEXT) generated by a group of near-end transceivers and interfering with the far-end transceivers of that same group is cancelled. This cancellation takes place between VDSL2 transceivers, not necessarily of the same profile.

## 4.6 Select "WAN"

Users can view **the WAN** link on the left navigation bar for WAN related settings. Select the "NAT". The menu below includes the sub-menus of **WAN Mode Selection**, **WAN Channel Config**, **VLAN Channel Config**, **WAN Setting**, **WAN Status**, **DNS**, **DDNS**, **and OAM Configuration**. A screen is displayed as shown in Figure 4.6.

**Figure 4.6 WAN options**

## 4.6.1 WAN Mode Selection

To configure the WAN Mode Setting, click the **WAN Mode Selection** (**WAN > WAN Mode Selection**) on the left navigation bar. A screen is displayed as shown in Figure 4.6.1

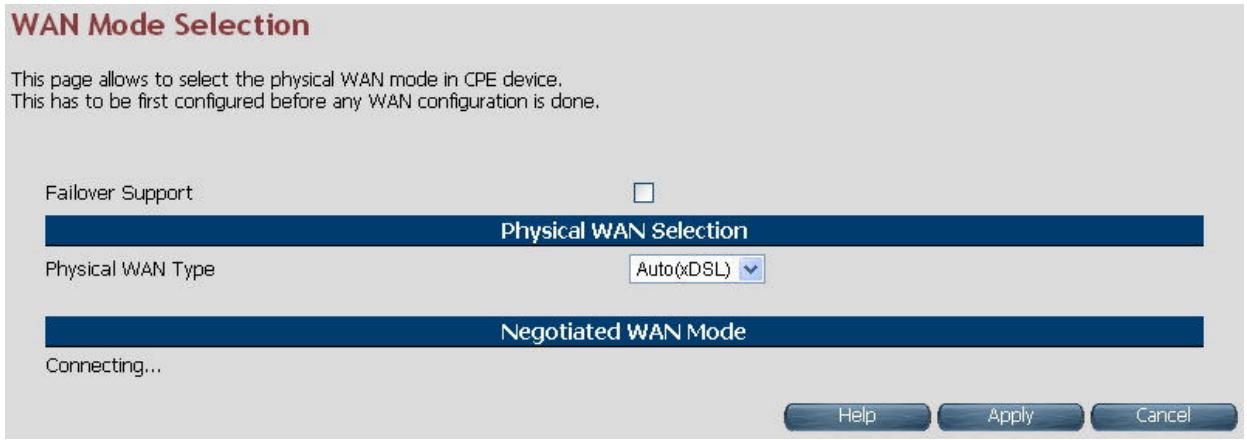



**Figure 4.6.1 WAN Mode Setting (Selected Auto)**

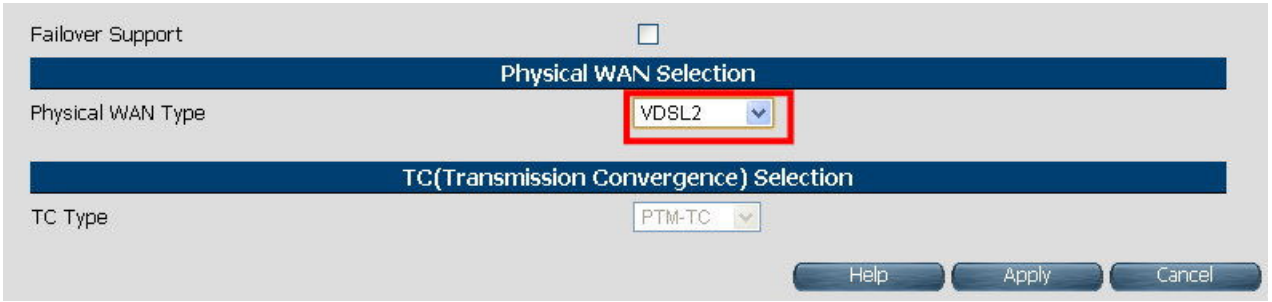



**Figure 4.6.1.1 WAN Mode Setting (Selected ADSL2+ / VDSL2)**

The screen holds the following details:

**Fields in WAN Mode Setting:**

| Field | Description |
|---|---|
| Failover Support | Select this checkbox to enable Dual WAN support. |
| **Primary WAN Selection** | |
| Physical WAN Type | Choose the WAN type from the drop-down list. For multi-WAN mode supported CPE image the dropdown will present following options - ADSL2+, VDSL2, xDSL (Auto), WAN Ethernet over MII-0, WAN Ethernet over MII-1, 3G WAN and LTE WAN. |
| **TC (Transmission Convergence) Selection** | |
| TC Type | Choose the Transmission Convergence from the drop-down list - 1). ATM-TC or 2). PTM-TC or 3). Auto. This field is displayed, only if ADSL2+ or xDSL is chosen as the WAN type. |

- Click Apply at any time during configuration to save the information that users have entered.
- Click Cancel to exit from this page without saving the changes.

Note:

If a user would like to use ADSL to connect NV-600A, please select ADSL item of Physical WAN Type, and confirm the TC type item is ATM-TC.

## 4.6.2 Auto Detect Setting

Auto detect feature is a fully automatic way to find and configure VC channel or VLAN channel for active WAN PHY of the device and WAN protocol for the same (PPPoE/DHCP).

Users have to provide pool of VC channels or VLAN channels which will be probed one by one sequentially and upon successful detection of a channel, WAN protocol probing will be done and configured in the device.

To configure the **Auto Detect Config**, click **Auto Detect Config** (**WAN > Auto Detect Config**) on the left navigation bar. A screen is displayed as shown in Figure 4.6.2

**Figure 4.6.2 Port Mapping Configuration**

The screen contains the following details:

**Fields in Auto detect Config:**

| Field | Description |
|---|---|
| ADSL-PTM VLAN Pool | This displays the current configured VLAN pool for autodetect in ADSL-PTM WAN mode. |
| Add/Delete ADSL-PTM VLAN to Pool | Add or delete VLAN to ADSL-PTM VLAN pool. |
| VDSL-PTM VLAN Pool | This displays the current configured VLAN pool for autodetect in VDSL-PTM WAN mode. |
| Add/Delete VDSL-PTM VLAN to Pool | Add or delete VLAN to VDSL-PTM VLAN pool. |
| MII-1 VLAN Pool | This displays the current configured VLAN pool for autodetect in MII-1 WAN mode. |
| Add/Delete MII-1 VLAN to Pool | Add or delete VLAN to MII-1 VLAN pool. |
| MII-0 VLAN Pool | This displays the current configured VLAN pool for auto-detect in MII-0 WAN mode. |
| Add/Delete MII-0 VLAN to Pool | Add or delete VLAN to MII-0 VLAN pool. |
| VCC Pool | This displays the current configured VCC pool for auto-detect in ADSL-ATM WAN mode. |
| Add/Delete VC to Pool | Add or delete VCC to ADSL-ATM VCC pool. |
| L2 VCC Auto Detect | Select this to enable VCC auto detection from the specified pool for ADSL-ATM WAN mode |
| L2 ADSL - PTM VLAN Auto Detect | Select this to enable VLAN auto detection from the specified pool for ADSL - PTM WAN mode. |
| L2 VDSL - PTM VLAN Auto Detect | Select this to enable VLAN auto detection from the specified pool for VDSL - PTM WAN mode. |

**Fields in Auto detect Config(cont'd):**

| Field | Description |
|---|---|
| L2 MII-1 VLAN Auto Detect | Select this to enable VLAN auto detection from the specified pool for MII-1 WAN mode. |
| L2 MII-0 VLAN Auto Detect | Select this to enable VLAN auto detection from the specified pool for MII-0 WAN mode. |
| L3 VCC Auto Detect | Select this to enable WAN auto detection (in sequence of PPPoE/DHCP) in ADSL-ATM WAN mode. |
| L3 ADSL - PTM VLAN Auto Detect | Select this to enable WAN auto detection (in sequence of PPPoE/DHCP) in ADSL-PTM WAN mode. |
| L3 VDSL - PTM VLAN Auto Detect | Select this to enable WAN auto detection (in sequence of PPPoE/DHCP) in VDSL-PTM WAN mode. |
| L3 MII-1 VLAN Auto Detect | Select this to enable WAN auto detection (in sequence of PPPoE/DHCP) in MII-1 WAN mode. |
| L3 MII-0 VLAN Auto Detect | Select this to enable WAN auto detection (in sequence of PPPoE/DHCP) in MII-0 WAN mode. |

## 4.6.3 WAN Channel Config

To configure the **WAN Channel Config**, click the **WAN Channel Config** (**WAN > WAN Channel Config**) on the left navigation bar. A screen is displayed as shown in Figure 4.6.3.

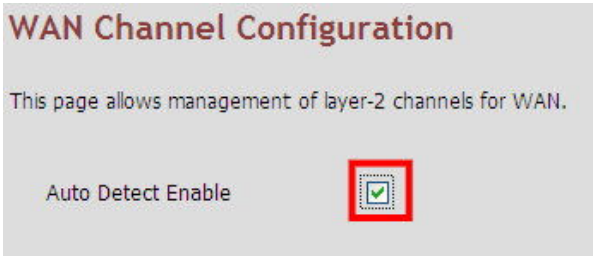



**Figure 4.6.3**

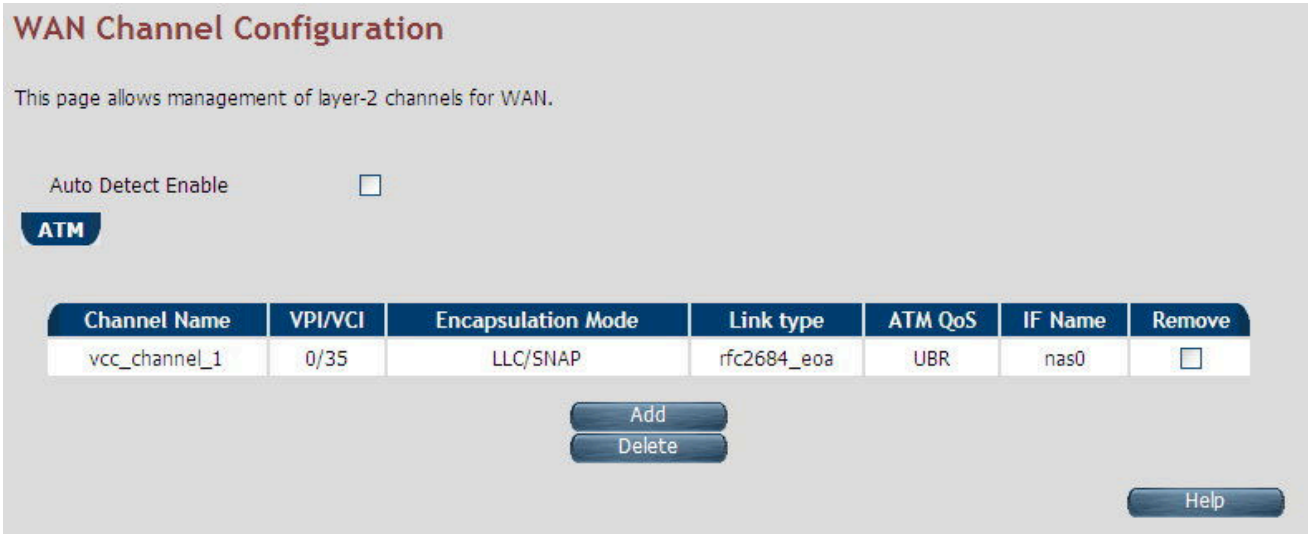



**Figure 4.6.3.1 WAN Channel Config (Auto Detecting does not check the checkbox)**

The screen contains the following details:

**Fields in WAN Channel Config:**

| Field | Description |
|---|---|
| **ATM** | The ATM based WAN channels are configured through the ATM tab. |
| | |
| Auto Detect Enable | To enable Auto Detect. |
| Channel Name | User specified VCC Name. |
| VPI/VCI | Virtual Path Identifier and Virtual Channel Identifier. |
| Encapsulation Mode | Encapsulation Mode for this VCC from dropdown - LLC/SNAP or VCMux mode. |
| Link type | Shows AAL5 Link type for ATM VCC (values such as EoATM, IPoATM, PPPoATM). |
| ATM QoS | Quality of Service for ATM VCC |
| IF Name | ATM Channel interface name in system. |
| Remove | Select this option to delete an ATM channel. |

When users click **Add** inside the WAN Channel-ATM tab, a screen is displayed as shown in Figure 4.6.3.2

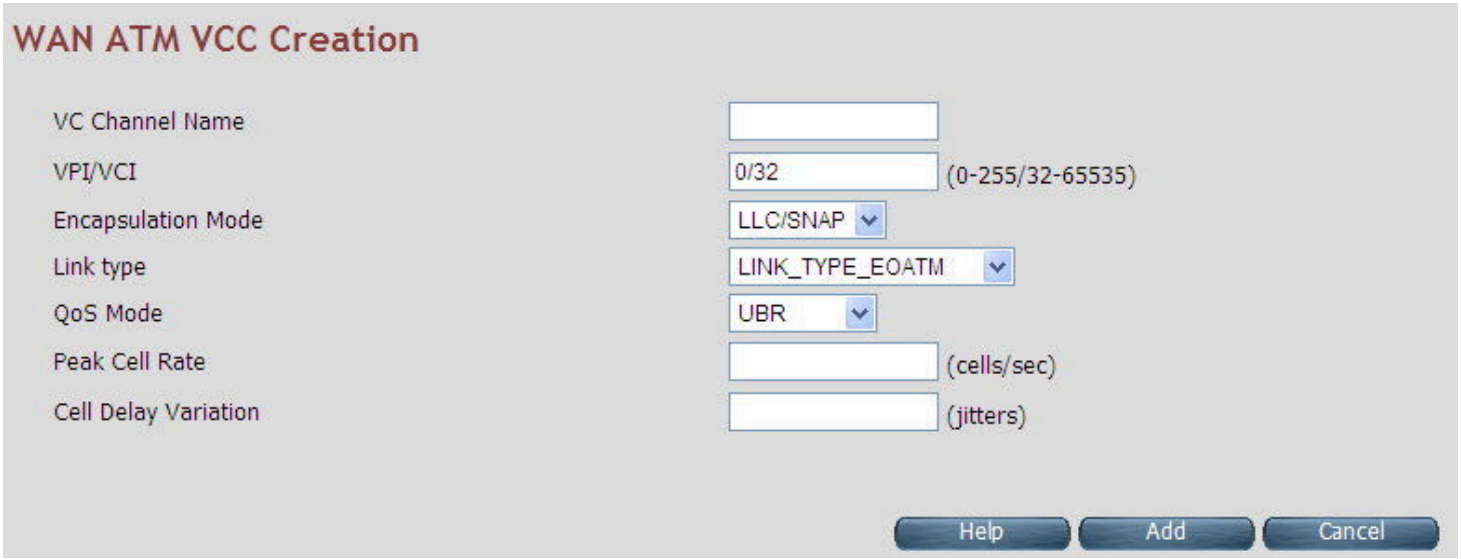



**Figure 4.6.3.2 WAN Channel Config - ATM VCC Creation**

The screen contains the following details:

**Fields in WAN Channel Config:**

| Field | Description |
|---|---|
| VC Channel Name | User specified VCC Name. |
| VCI/VPI | Virtual Path Identifier and Virtual Channel Identifier |
| Encapsulation Mode | Encapsulation Mode for this VCC from dropdown - LLC/SNAP or VCMux mode. |
| Link type | Select AAL5 Link type for ATM VCC (possible values such as EoATM, IPoATM, PPPoATM). |
| QoS Mode | Quality of Service for ATM VCC. Available options are **UBR**, **CBR, rt-VBR**, **nrt-VBR** and **UBR+**. |
| Peak Cell Rate | Peak Cell Rate specified in cells/second. |
| Cell Delay Variation | Cell Delay Variation is specified in terms of jitters. |

- Click **Add** to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

## 4.6.4 VLAN Channel config

To configure the **VLAN Channel Config**, click the **VLAN Channel Config** (**WAN > VLAN Channel Config**) on the left navigation bar. A screen is displayed as shown in Figure 4.6.4.

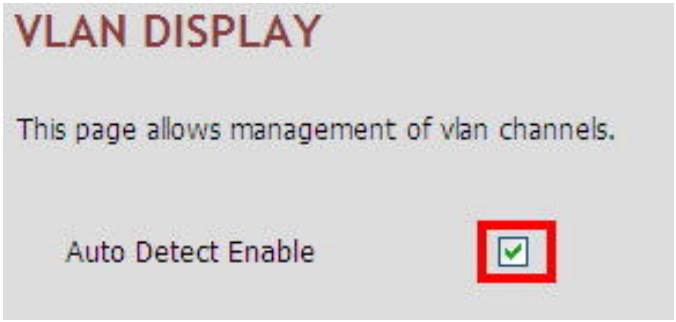



Figure 4.6.4

Figure 4.6.4.1 VLAN Channel Config Display (Auto Detecting does not check the checkbox)

The screen contains the following details:

**Fields in VLAN Display:**

| Field | Description |
|---|---|
| Auto Detect Enable | To enable Auto Detect. |
| VLAN Name | User specified VLAN Channel name. |
| Base WAN Name | Displays the L2 interface names over which VLAN Channel has been configured. |
| VLAN id | VLAN identifier in range of 1- 4095. |
| IF Name | VLAN interface name. |
| MAC Address | MAC address of VLAN interface name. |
| Select | Select this option to delete a specific VLAN channel. |

- Click **Add** to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

When users click **Add** button inside the VLAN Channel Config page, a screen is displayed as shown in Figure 4.6.4.2

**Figure 4.6.4.2 VLAN Channel Config - Add**

The screen contains the following details:

**Fields in VLAN Creation:**

| Field | Description |
|---|---|
| VLAN Channel Name | User specified VLAN Channel name. |
| Mode Name | List of L2 interfaces over which VLAN Channels can be configured. |
| VLAN Id | VLAN identifier in range of (7 - 4095). VLAN Identifiers (1 - 6) are internally used in the system for special purposes and are not available to users for configuration. |
| Override MAC Address | This is an option to configure MAC address by overriding physical MAC address. In the current release, this option is not available to users for configuration. |

- Click **Add** to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

## 4.6.5 WAN Setting

To configure the WAN interface, click the **WAN Setting** link (**WAN > WAN Setting**) on the left navigation bar and a screen is displayed as shown in Figure 4.6.5.

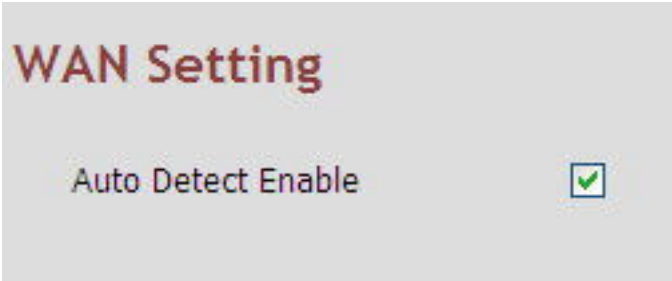



Figure 4.6.5 WAN Setting - Auto Detect Enable

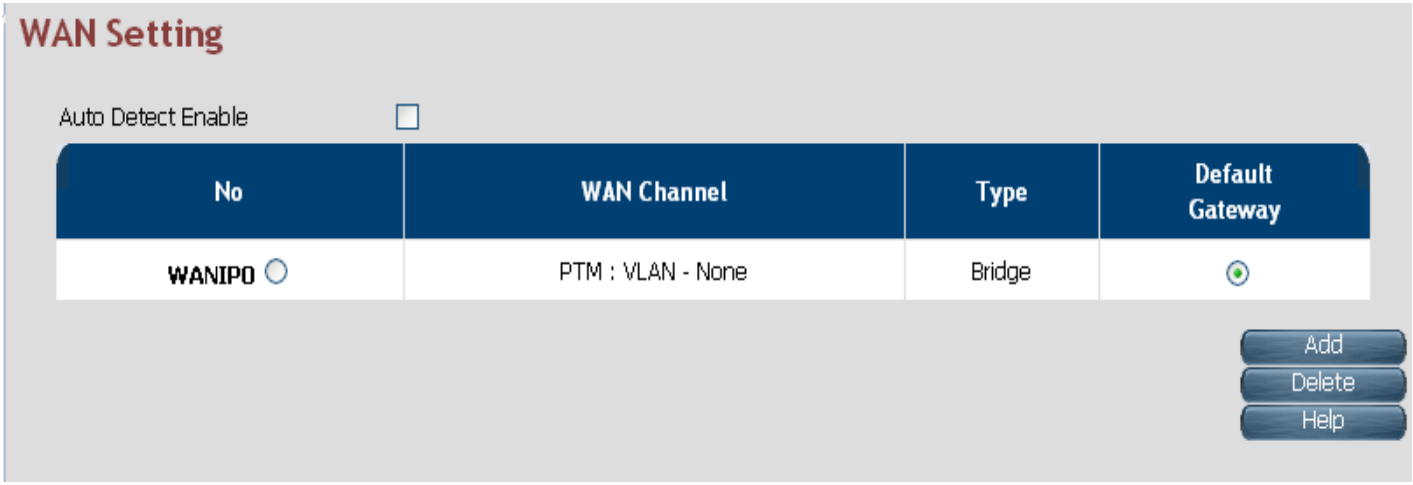



Figure 4.6.5.1 WAN Setting

The NV-600A can support up to maximum 16 WAN connections in system. When a hardware based QoS is enabled in system, it limits the number of VCCs to 8 only for ATM based WAN. For creating a new WAN connection, click **Add** in the WAN setting page. Please follow the rest of the steps for creating the WAN connection.

The last column named DEFAULT GATEWAY allows users to select the WAN for relevant WAN mode setting in WAN setting web page. When the user clicks any of the radio buttons, he will be asked to confirm the same. If the user clicks **Apply**, the default gateway will be configured on the selected WAN connection, otherwise the changes will not be applied.

The screen holds the following details:

**Fields in WAN Settings:**

| Field | Description |
|---|---|
| Auto Detect Enable | To enable Auto Detect. |
| WAN Number | The configured WAN are referred through auto-assigned names in form WANIP<No.> or WANPPP<No.> where <No.> start from 0. |
| WAN Channel | Provides information of layer-2 WAN channel configured. |
| Type | Provides information about types of WAN such as PPPoE or DHCP or Bridged etc. |
| Default VoIP Interface | This option is present in only IAD models, where VoIP is supported. This is the default interface for VoIP packets. |
| Default Gateway | This option allows users to configure default route in system. The chosen WAN will be used for the default route. |

When users click **the Add** button in WAN Settings web page, a screen is displayed as shown in Figure 4.6.5.2

**Figure 4.6.5.2 WAN Settings – Apply – Step1**

The screen contains the following details:

**Fields in WAN Settings – Apply – Step1:**

| Field | Description |
|---|---|
| Attached Channel | Select the WAN Channel (e.g. PVC) from drop-down, being configured as WAN. |
| Dynamic IP Address | To get users IP Address from user's service provider (means NV-600A is DHCP client on WAN) click **Apply**. |
| Static IP Address | To enter the WAN interface IP Address of NV-600A enable this field and click **Apply**. |
| PPPoE | Point-to-Point Protocol over Ethernet used for connecting to the ISP, click **Apply**. |
| PPPoA | Point-to-Point Protocol over ATM used for connecting to the ISP, click **Apply**. This setting is applicable only for ATM WAN mode. |
| Bridge | To configure the WAN of bridged type, select this field and click **Apply**. |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

### 4.6.5.1 Dynamic IP Address

To configure the WAN interface of DHCP IP type, select **Dynamic IP Address** option. A screen is displayed as shown in Figure 4.6.5.3

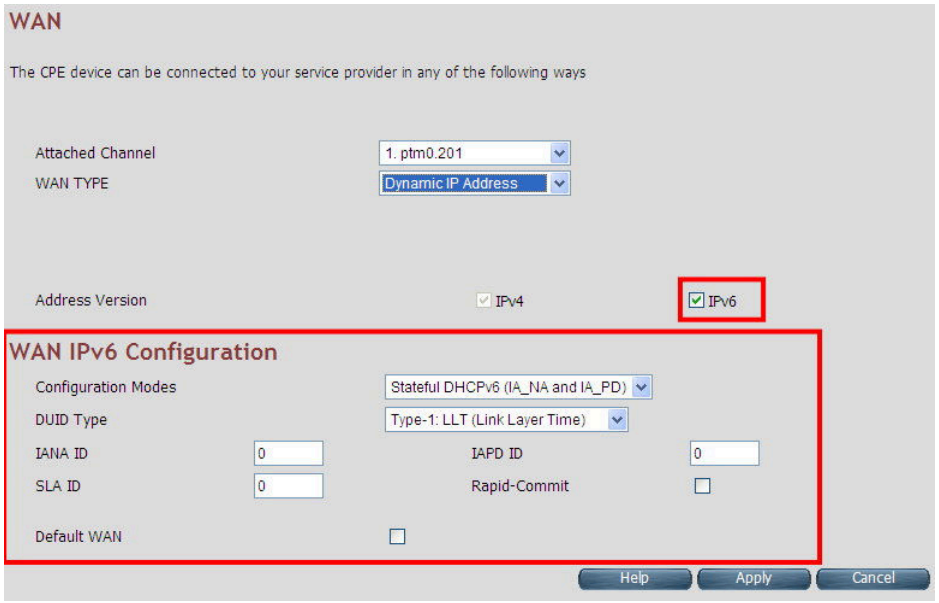



**Figure 4.6.5.3 Dynamic IP Address**

Please Enable IPv6 to set the WAN IPv6 Configuration. Select the IPv6 Setting (**IPv6 > IPv6 setting**) on the left navigation bar.

### 4.6.5.2 Static IP Address

To configure the WAN interface to use a static IP address, select the option **Static IP Address** in the **WAN Settings** screen. A screen is displayed as shown in Figure 4.6.5.4

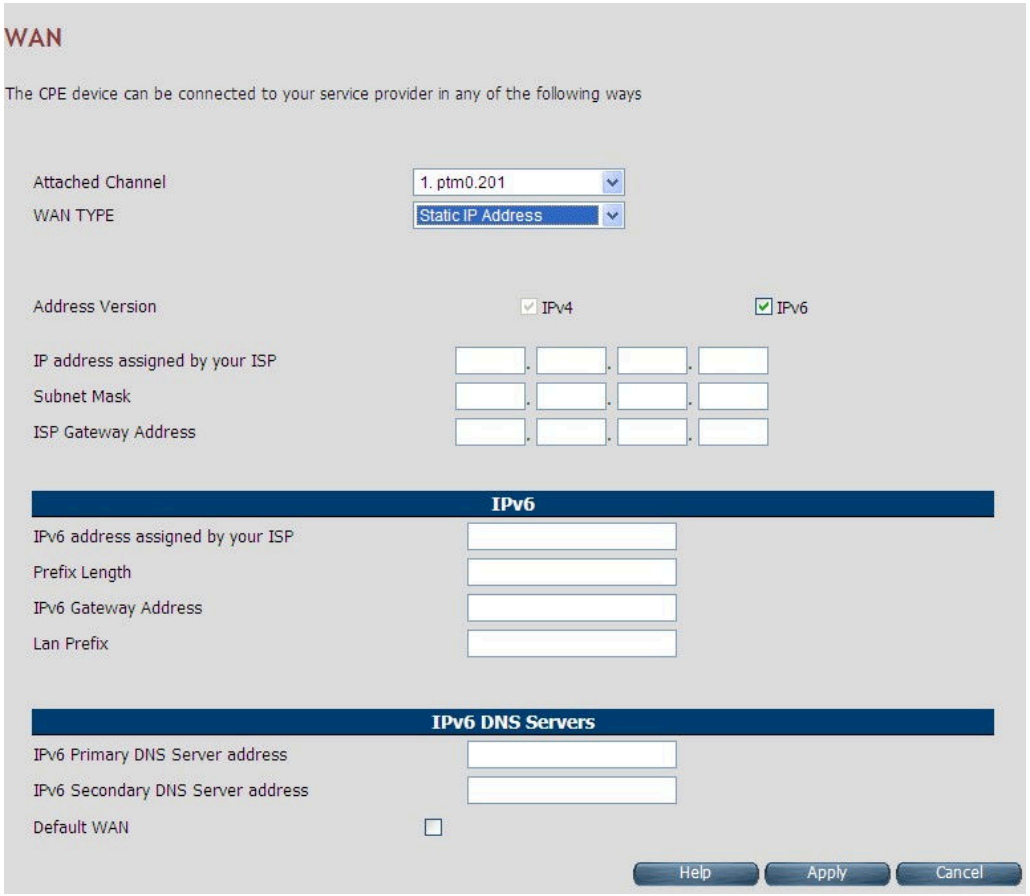



**Figure 4.6.5.4 WAN Static IP**

The screen contains the following details:

**Fields in Static IP:**

| Field | Description |
|---|---|
| **Address Version** | |
| IP address assigned by users ISP | To specify the IP Address of NV-600A CPE's WAN link. |
| Subnet Mask | To specify the Subnet Mask of NV-600A CPE's WAN link. |
| ISP Gateway Address | To specify the Gateway address of the NV-600A CPE's WAN. |
| **IPv6** | |
| IPv6 address assigned by users ISP | This is the static IP address for the WAN interface. |
| Prefix Length | This is the prefix length of the IPv6 address. |
| IPv6 Gateway Address | This is the default gateway. |
| LAN Prefix | This is the prefix used to auto-configure LAN side hosts. |
| **IPv6 DNS Servers** | |
| IPv6 Primary DNS Server Address | This is the primary DNS server. |
| IPv6 Secondary DNS Server Address | This is the secondary DNS server. |
| Default WAN | This option allows users to configure default route for relevant WAN mode of this WAN connection. |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

### 4.6.5.3 PPPoE

To configure the WAN interface to use PPPoE, choose the option **PPPoE**. A screen is displayed as shown in Figure 4.6.5.5

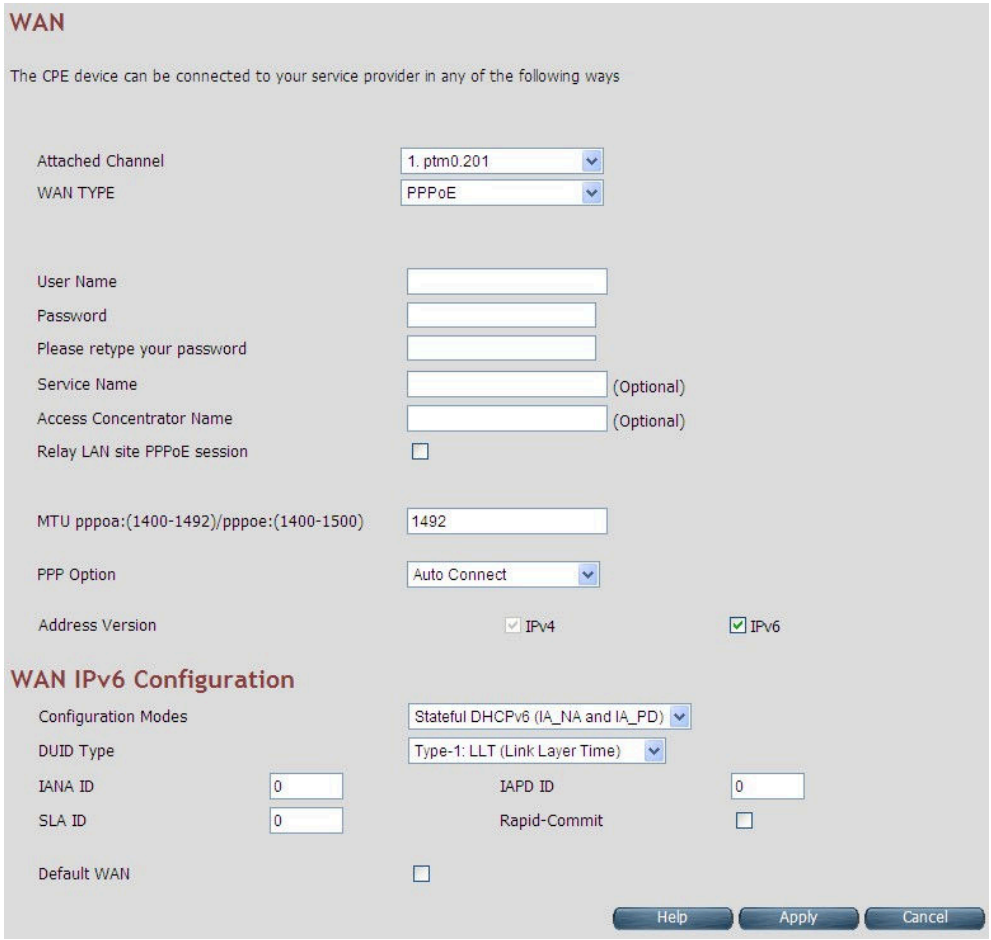



**Figure 4.6.5.5 WAN PPPoE creation**

The screen contains the following details:

**Fields in PPPoE WAN:**

| Field | Description |
|---|---|
| Username | To enter a username for PPPoE session used for authentication in B-RAS. |
| Password | To enter a password for PPPoE session used for authentication in B-RAS. |
| Please retype user's password | To enter the same password again to reconfirm. |
| Service Name | PPP Service Name (optional). |
| Access Concentrator Name | PPP Access concentrator Name (optional). |
| Relay LAN site PPPoE Session | This feature allows to enable/disable a PPPoE relay session. PPPoE relay also called PPPoE Passthrough. |
| PPP Option | Choose the option from the drop-down list. The available options are Auto Connect, Dial-On-Demand and Manual Connect. |
| Address Version | This option allows configurability of IPv4 and/or IPv6 stack on per WAN interface. |

**Fields in PPPoE WAN (WAN IPv6 Configuration):**

| Field | Description |
|---|---|
| Configuration Modes | This option allows users to select the following modes of IPv6 configuration:<br>◆ Stateful DHCPv6(IA_NA and IA_PD)<br>◆ SLAAC (Address Configuration) with DHCPv6 (IA_PD) |
| DUID Type | This option allows users to configure different DUID (DHCP Unique Identifier) types:<br>◆ "Type-1: LLT (Link Layer Time)<br>◆ "Type-2: EN (Enterprise Number)<br>◆ "Type-3: LL (Link Layer) |
| IANA ID | IANA option represents IPv6 address, and parameters related to the same being accepted by DHCPv6 clients. IANA is the Identity Association for Non- Temporary Addresses option. This Identifier is to be configured when Stateful DHCPv6 configuration mode is selected. |
| IAPD ID | IAPD options represent one or more IPv6 prefixes and parameters related to it. IAPD is the Identity Association for Prefix Delegation. This identifier to be configured in both Stateful DHCPv6 or SLAAC+DHCPv6 configuration modes. |
| SLA ID | This parameter is called Site Level Aggregation Identifier. This identifier is used to configure the subnet for DHCPv6 client configuration. |
| Rapid commit | This declaration enables DHCPv6-client to request the DHCPv6-server to perform a Rapid Commit. Handshaking will happen with two DHCPv6 messages. |
| Default WAN | This option allows users to configure default route for relevant WAN mode of this WAN connection. |

◆ Click **Apply** at any time during configuration to save the information that users have entered.

◆ Click **Cancel** to exit from this page without saving the changes.

### 4.6.5.4 PPPoA

The PPP-over-ATM (PPPoA) mode is valid **only for ATM based** WAN. To configure the WAN interface to use PPPoA, select the option **PPPoA** option. A screen is displayed as shown in Figure 4.6.5.6

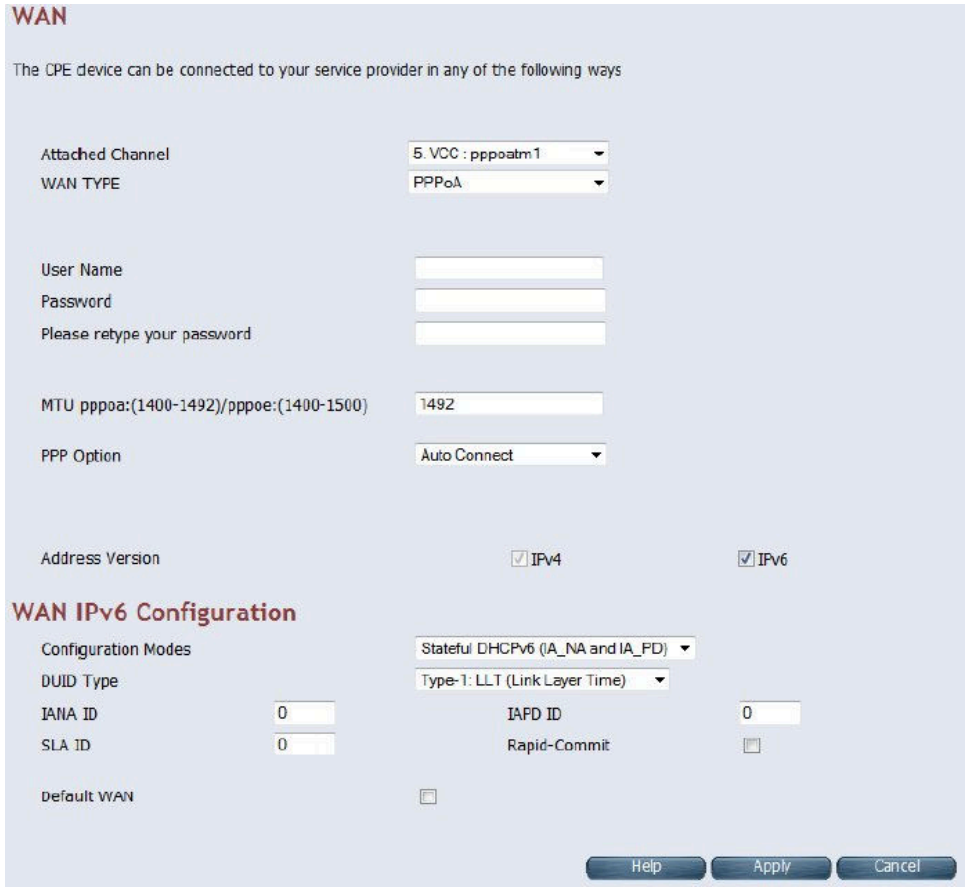


**Figure 4.6.5.6 WAN PPPoA creation**

The screen contains the following details:

**Fields in PPPoA WAN:**

| Field | Description |
|---|---|
| Username | To enter the username to be used in the PPPoA session. |
| Password | To enter the corresponding password for the specified username. |
| Please retype user's password | To enter the password again to reconfirm. |
| Dial on Demand | This feature allows users to automatically re-connect to the service provider once the connection is lost. The checkbox can be enabled or disabled for this feature. |
| Maximum Idle Time | Specifies how long the connection may remain idle before the PPPoA connection gets automatically disconnected. The Idle Timeout is specified in seconds. |
| Address Version | For PPPoA, the only supported IP addressing is IPv4 currently. The IPv6 for PPPoA is not available in this version of NV-600A. |

**Fields in PPPoA WAN IPv6 Configuration:**

| Field | Description |
|---|---|
| Configuration Modes | This option allows users to select the following modes of IPv6 configuration:<br>◆ Stateful DHCPv6(IA_NA and IA_PD)<br>◆ SLAAC (Address Configuration) with DHCPv6 (IA_PD) |
| DUID Type | This option allows users to configure different DUID (DHCP Unique Identifier) types:<br>◆ "Type-1: LLT (Link Layer Time)<br>◆ "Type-2: EN (Enterprise Number)<br>◆ "Type-3: LL (Link Layer) |
| IANA ID | IANA option represents IPv6 address, and parameters related to the same being accepted by DHCPv6 clients. IANA is the Identity Association for Non- Temporary Addresses option. This Identifier is to be configured when Stateful DHCPv6 configuration mode is selected. |
| IAPD ID | IAPD options represent one or more IPv6 prefixes and parameters related to it. IAPD is the Identity Association for Prefix Delegation. This identifier to be configured in both Stateful DHCPv6 or SLAAC+DHCPv6 configuration modes. |
| SLA ID | This parameter is called Site Level Aggregation Identifier. This identifier is used to configure the subnet for DHCPv6 client configuration. |
| Rapid commit | This declaration enables DHCPv6-client to request the DHCPv6-server to perform a Rapid Commit. Handshaking will happen with two DHCPv6 messages. |
| Default WAN | This way allows users to configure default route for relevant WAN mode of this WAN connection. |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

### 4.6.5.5 Bridge

The option **Bridge** enables the bridge mode, which is a common connection method used for xDSL modem. Select this option on WAN Settings page and click Next. A screen is displayed as shown in Figure 4.6.5.7

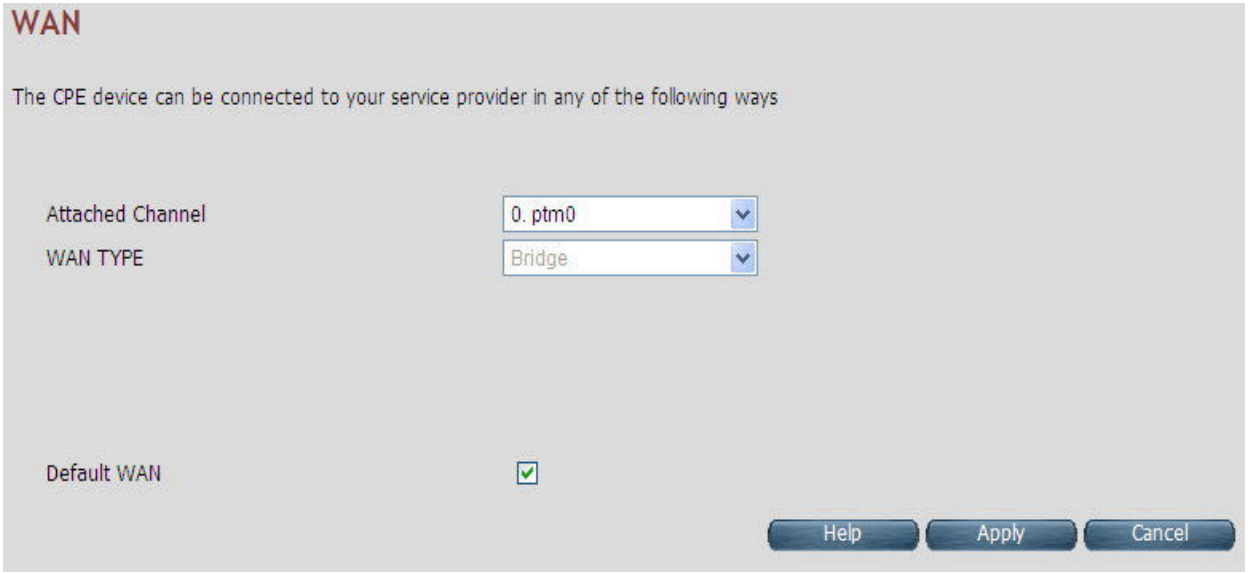



**Figure 4.6.5.7 Bridge WAN Setting**

The screen contains the following details:

**Fields in Bridge Configuration:**

| Field | Description |
|---|---|
| Default WAN | This way allows users to configure default route for relevant WAN mode of this WAN connection. |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

### 4.6.5.6 Delete

This way allows users to delete the selected configured WAN connection. This makes WAN connections free to re-choose the type of protocol and other parameters configuration.

- Click **Cancel** to exit from this page without saving the changes.
- Click **Apply** for deleting the WAN connection.

## 4.6.6 WAN Status

To display the status report of VCCs, click the **WAN Status** link (**WAN > WAN Status**) on the left navigation bar. A screen displayed as shown in Figure 4.6.6

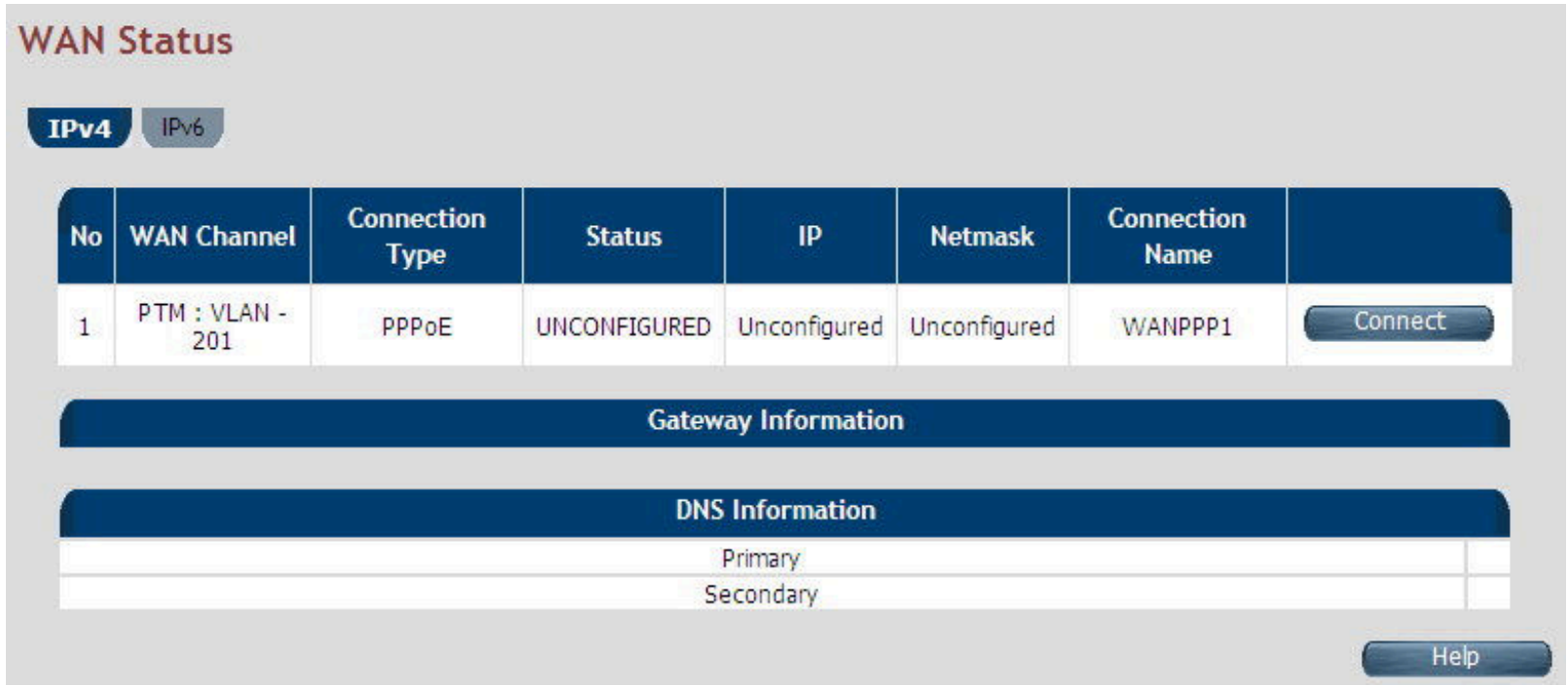



Figure 4.6.6 WAN Status

The screen contains the following details:

**Fields in WAN Status:**

| Field | Description |
|---|---|
| IPv4/IPv6 | Choose the appropriate tab to view the status. |
| WAN Channel | For the currently configured WAN interface, this gives the layer-2 WAN channel information (such as ATM VCC). |
| Connection Type | The type of connection mode in which NV-600A is configured. |
| Status | Displays the connection status of the WAN. |
| IP | Displays the IP address in use. |
| Netmask | Displays the netmask in use. |
| Configured Connection Name | Displays the configured connection name. |
| Gateway Information | Provides information about the gateway. |
| DNS Information | Provides information about the primary and secondary DNS. |

The control buttons shown against a few WAN are explained below.

**Fields in Control Fields displayed in WAN Status Screen:**

| Field | Description |
|---|---|
| Connect | This button appears only for PPPoA and PPPoE type of WAN links. On clicking this button, it tries to set up PPP link. |
| Disconnect | This button too appears only for PPPoA and PPPoE type of WAN links. On clicking this button, it brings down the PPP link. |
| Renew | This button appears only for DHCP type of WAN links. On clicking this button, it tries to establish renewal of the current lease. |
| Release | This button appears only for DHCP type of WAN links. On clicking this button, it tries to release the current lease. |

When users click on the IPv6 tab in the WAN Status page, a screen is displayed as shown in Figure 4.6.6.1

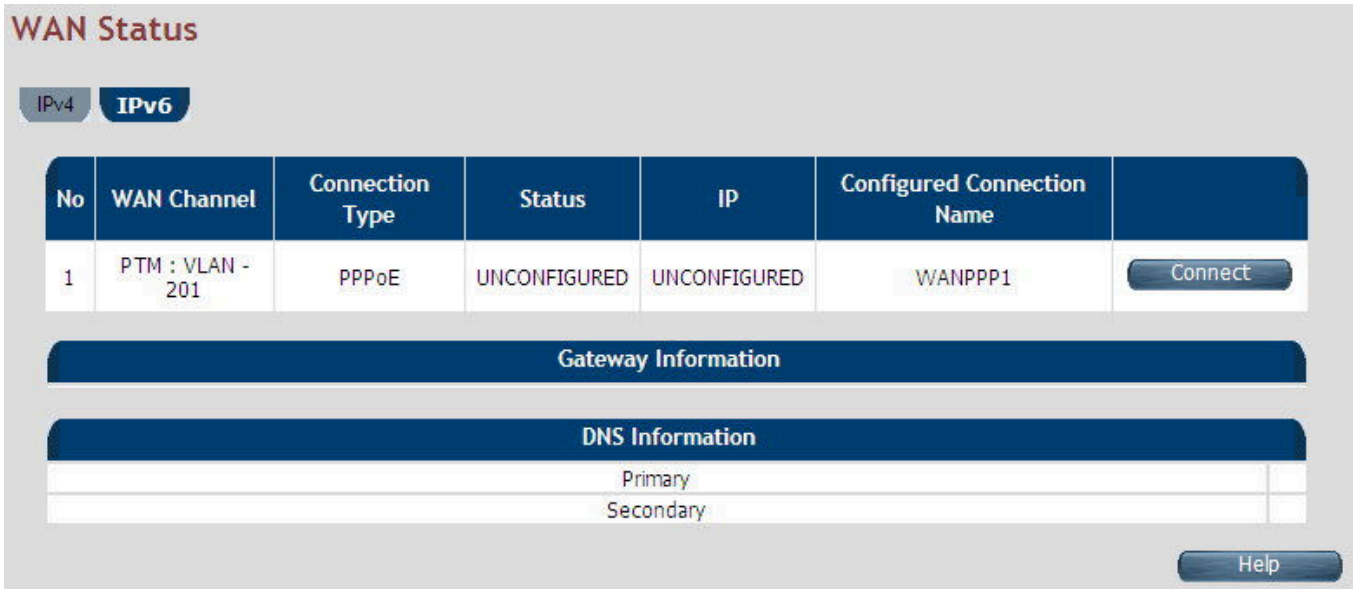



**Figure 4.6.6.1 WAN Status IPv6 Tab**

The screen contains the details as described in table of **"Fields in WAN Status"**.

## 4.6.7 DNS

To configure the Domain Name Server (DNS) address, click the **DNS** link (**WAN > DNS**) on the left navigation bar. A screen is displayed as shown in Figure 4.6.7. For statically configured WAN, it is mandatory to configure DNS addresses through this page.

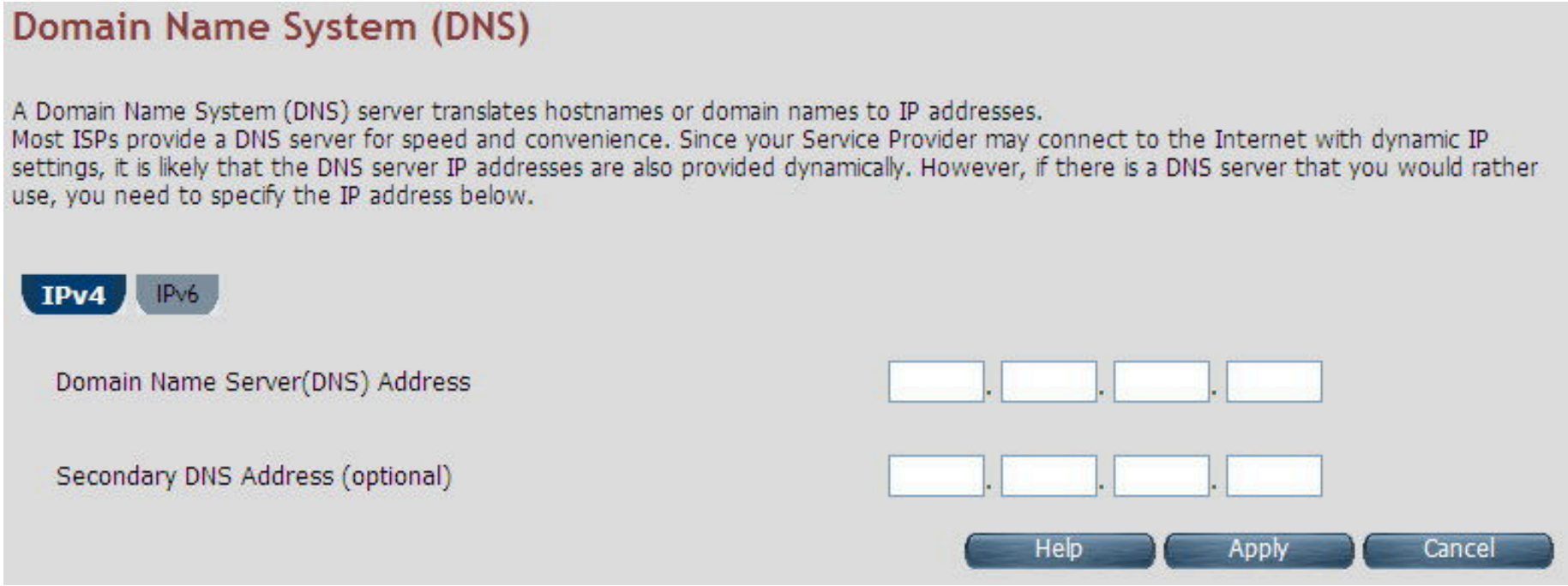



**Figure 4.6.7 DNS Configuration**

The screen contains the following details:

**Fields in DNS:**

| Field | Description |
|---|---|
| IPv4/IPv6 | Select the appropriate tab to configure IPv4 or IPv6. IPv6 support is currently not available for DNS configuration. |
| Domain Name Server (DNS) Address | Enter the DNS address of the primary DNS server. |
| Secondary DNS Address (optional) | Enter the address of the secondary DNS server, if available. It is an optional parameter. |

- Click **Cancel** to exit from this page without saving the changes.
- Click **Apply** for deleting the WAN connection.

## 4.6.8 DDNS

The Dynamic DNS is useful for getting a FQDN URL registered for a dynamic IP address to a DNS service provider. The NV-600A software integrates support for three Dynamic DNS service providers:

• dhs • dyndns • dyns

The user needs to register first with a chosen DNS Service provider. The registered information needs to be configured in DDNS settings web page. To configure thee registers information in DDNS settings page, click the **DDNS** link (**WAN > DDNS**) on the left navigation bar. A screen is displayed as shown in Figure 4.6.8

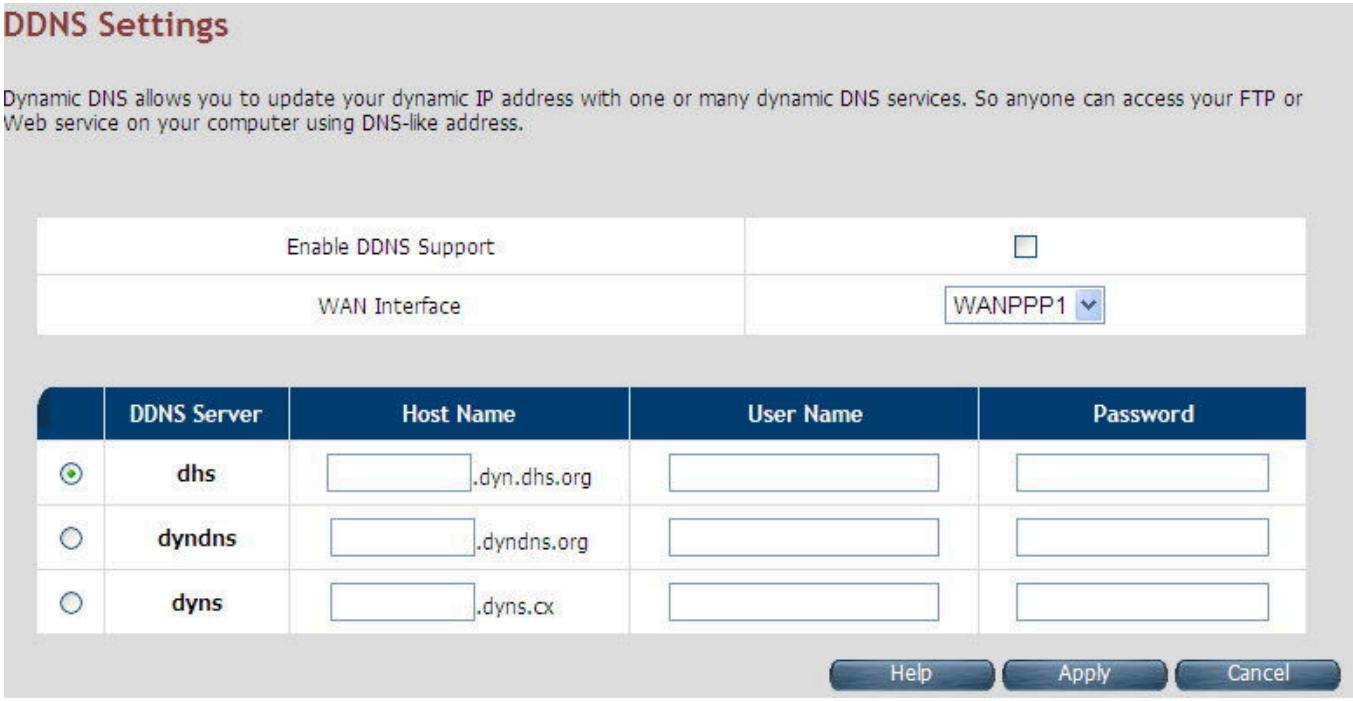



**Figure 4.6.8 DDNS Settings**

The screen contains the following details:

**Fields in DDNS:**

| Field | Description |
|---|---|
| Enable DDNS support | Check box to enable DDNS support in CPE. |
| WAN Interface | WAN Interface name from dropdown for DDNS resolution. The DDNS agent running in CPE keeps track of changes in the IP address of chosen WAN and informs DNS service provider. |
| DDNS Server | Dynamic DNS Server Provider. |
| Host Name | Host name registered with DDNS Service provider. This is part of FQDN used for accessing the host. |
| Username | Registered username with DDNS service provider. |
| Password | Registered password with DDNS service provider. |

- Click **Apply** for applying the DDNS changes into system.
- Click **Cancel** to exit from this page without saving the changes.

## 4.6.9 OAM Configuration

This page provides ATM F5 based OAM test. Hence the settings are valid only for ATM based WAN. To configure the ADSL OAM settings, click the **OAM Configuration** link (**WAN > OAM Configuration**) on the left navigation bar. This release supports only F5 type of OAM tests as shown in Figure 4.6.9

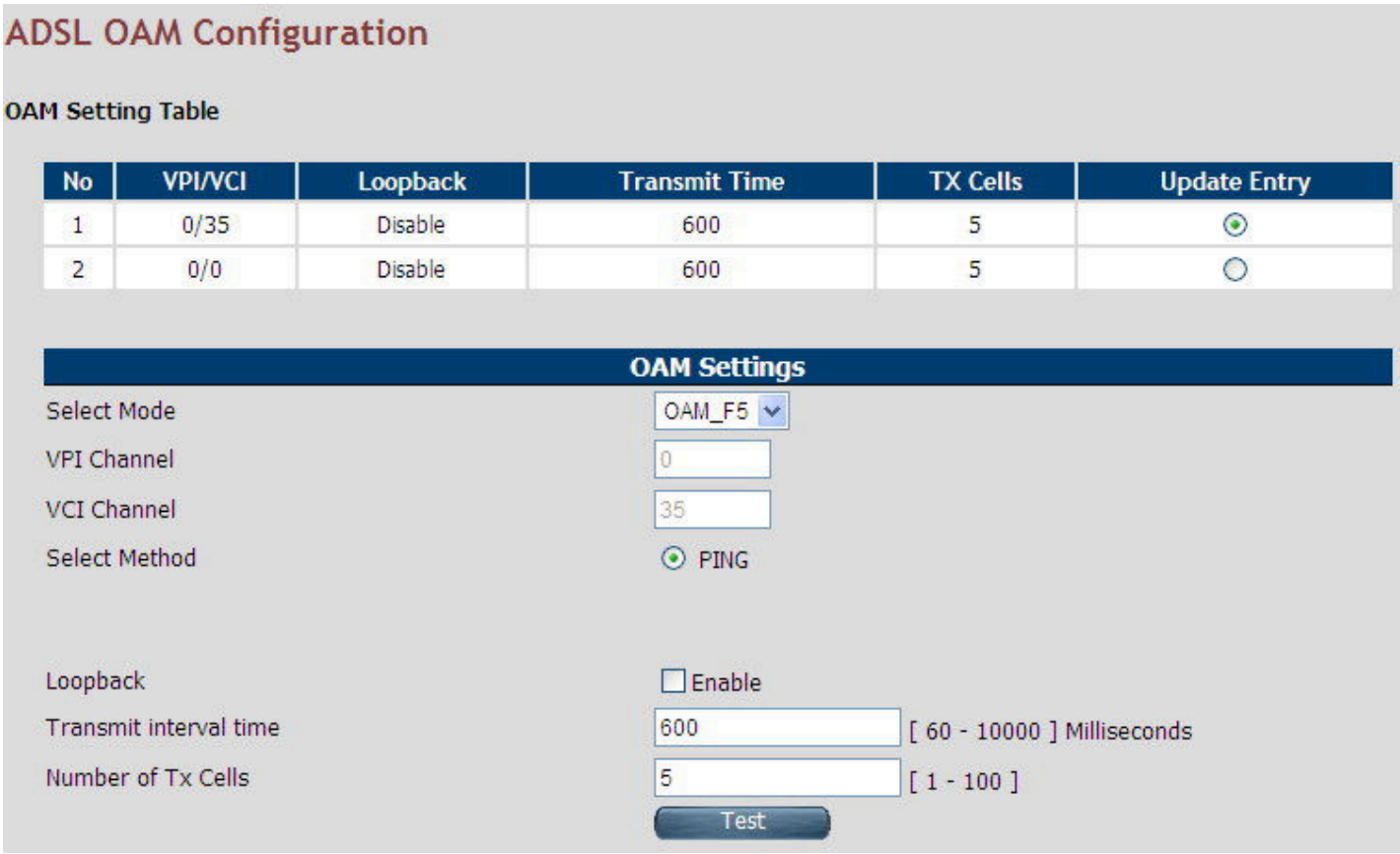



**Figure 4.6.9 ADSL OAM F5 Test**

The screen contains the following details:

**Fields in ADSL OAM F5 Test page:**

| Field | Description |
|---|---|
| OAM F5 Setting Table | This table displays all active connections with the following OAM parameters information:<br>◆ No: Number<br>◆ VPI: Virtual Path Identifier<br>◆ VCI: Virtual Connection Identifier<br>◆ Loopback: Enabled or Disabled<br>◆ Transmit Time: actual value in milliseconds<br>◆ Tx Cells: No of cells to be transmitted<br>◆ Update Entry: |
| **OAM Settings** | |
| Select Mode | OAM_F5 |
| VPI Channel | Displays the selected VPI channel of the OAM F5 Setting Table. |
| VCI Channel | Displays the selected VCI channel of the OAM F5 Setting Table. |
| F5 Loopback | Used to enable/disable F5 Loopback. |
| F5 Transmit Interval time | Configures the time (in ms) for the interval to send F5 loopback cells. |
| Number of Tx cells | Count to total number of transmitted ATM cells. |

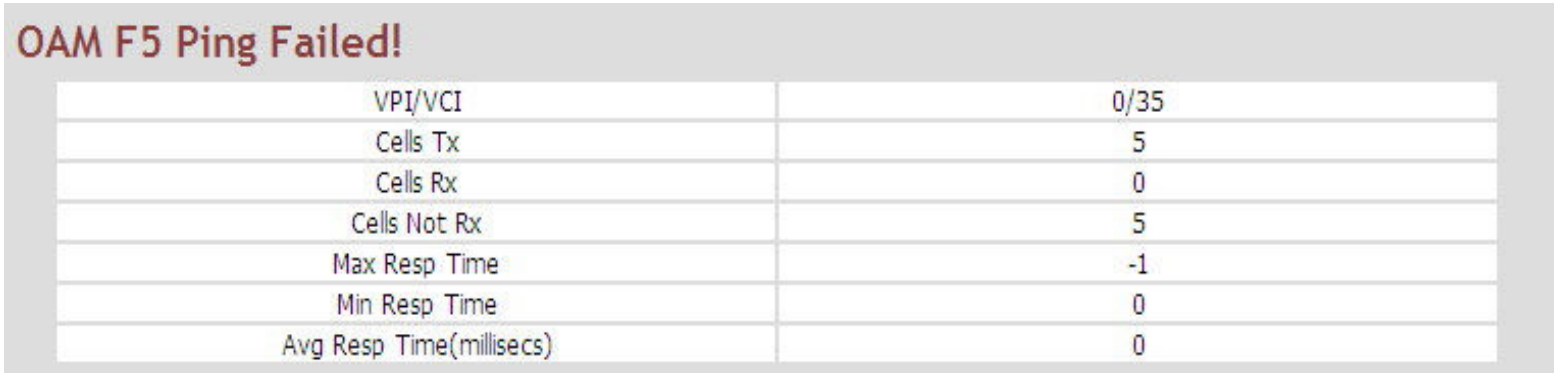
◆ Click **Test** to view the OAM F5 results.

When users test the OAM Configuration, the F5 result is displayed as shown in Figure 4.6.9.1 and this may be a failure or successful OAM F5 result.

OAM F5 Ping Successful!

| | |
|---|---|
| VPI/VCI | 0/35 |
| Cells Tx | 5 |
| Cells Rx | 0 |
| Cells Not Rx | 5 |
| Max Resp Time | -1 |
| Min Resp Time | 0 |
| Avg Resp Time(millisecs) | 0 |

**Figure 4.6.9.1 Tset Successful**



OAM F5 Ping Failed!

| | |
|---|---|
| VPI/VCI | 0/35 |
| Cells Tx | 5 |
| Cells Rx | 0 |
| Cells Not Rx | 5 |
| Max Resp Time | -1 |
| Min Resp Time | 0 |
| Avg Resp Time(millisecs) | 0 |

**Figure 4.6.9.2 Test Failed**

The screen contains the following details:

**Fields in ADSL OAM F5 Test Page:**

| Field | Description |
|---|---|
| VPI/VCI | Displays the selected VPI/VCI channel of the OAM F5 Setting Table. |
| Cells Tx | Count of total number of transmitted ATM cells. |
| Cells Rx | Count of total number of received ATM cells. |
| Cells not Rx | Count of total number of not received ATM cells. |
| Max Resp Time | Displays the maximum response time in milliseconds. |
| Min Resp Time | Displays the minimum response time in milliseconds. |
| Avg Resp Time (milliseconds) | Displays the average response time in milliseconds. |

## 4.7 Select "LAN"

When connecting the NV-600A to a new control PC, one may want to go through the following steps in order to make the IP address previously set by ifconfig in the console or on some later occasion, one may want to change it again without using the console, then the menu below will be helpful. In order to set the IP address, click on "LAN Settings". Users can view **LAN** in the left navigation bar for LAN related settings.

Select the "LAN". The menu below includes the sub-menus of **LAN ARP List**, **LAN Settings**, **UPnP Devices**, **LAN Switch Port Setting**, **LAN Port Status**, A screen is displayed as shown in Figure 4.7.

**Figure 4.7 LAN options**

### 4.7.1 LAN ARP List

To view the ARP entries list that is currently present in CPE, click the **LAN ARP List** link (**LAN > LAN ARP List**) on the left navigation bar. A screen is displayed as shown in Figure 4.7.1

**Figure 4.7.1 ARP List**

The screen contains the following details:

**Fields in LAN ARP List:**

| Field | Description |
|---|---|
| MAC Address | MAC Address of next hop node from ARP entry. |
| IP Address | IP Address of node from ARP entry. |
| HW Type | Hardware Type for ARP entry. 0x1 corresponds to IEEE 802.3 ethernet based interface. |

◆ Click **Perform ARP Scan** to ensure the ARP entries are connected to the CPE.

### 4.7.2 LAN Settings

To configure the LAN interface, click the **LAN Settings** link (**LAN > LAN Settings**) on the left navigation bar. In case the Secondary level subnet Range checkbox is checked, some additional data and options will be on display. A screen is displayed (DHCP Server mode) as shown in Figure 4.7.2.

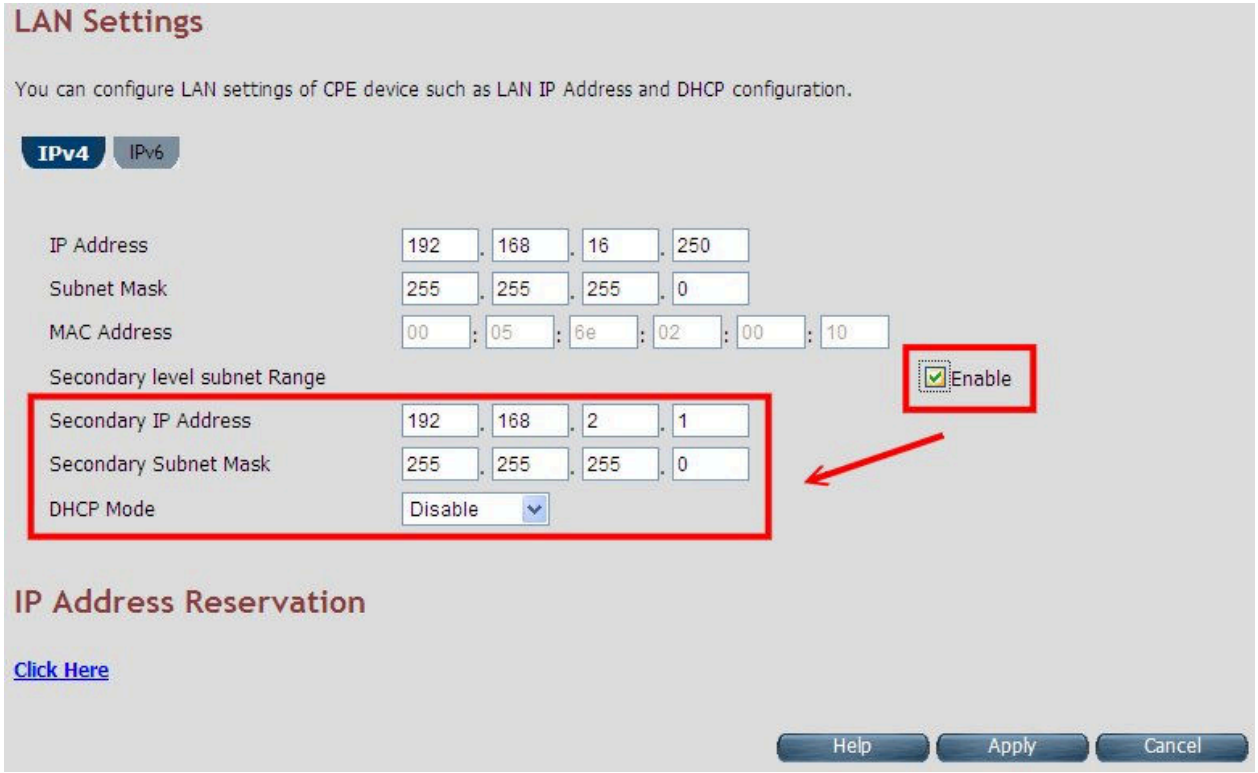



**Figure 4.7.2 LAN Settings – DHCP Server**

The screen contains the following details:

**Fields in LAN Settings:**

| Field | Description |
|---|---|
| IP Address | Used to enter the LAN interface IP Address of CPE device. |
| Subnet Mask | To enter the LAN Subnet Mask of CPE device. |
| MAC Address | MAC Address of LAN bridge device. It can be overridden by specifying the user supplied MAC address here. |
| Enable | To enable the secondary IP address on the LAN interface. |
| Secondary IP Address | This is to enter the secondary IP address. |
| Secondary Subnet Mask | This is to enter the secondary subnet mask. |
| DHCP Mode | To choose the mode of DHCP in NV-600A. The options available are: Disable, Server and Relay Agent. The default value is **Disable**. If DHCP Mode is set to **Server,** there are some additional options available, which are shown in **Figure 4.7.2**. IP Pool Starting Address - To enter the starting IP Address of the DHCP server pool. IP Pool Ending Address - To enter the ending IP Address of the DHCP server pool. Lease Time - To specify the lease period for DHCP allocation. Local Domain Name (optional) - To enter the Domain Name of the DHCP server. DHCP Server IP - IP address of the DHCP server on the interface shown, to which the DHCP requests are relayed. |

| Field | Description |
|---|---|
| **DHCP Server** | |
| IP Pool Starting Address | DHCPv4 pool start IPv4 address. |
| IP Pool Ending Address | DHCPv4 pool and IPv4 address. |
| Lease Time | Lease Time for every DHCP leased entry. Select from dropdown of allowed values. |
| Local Domain Name | Local domain name configured to LAN hosts by DHCPv4 server. |

- Click APPLY at any time during configuration to save the information that users have entered.
- Click CANCEL to exit from this page without saving the changes.

When users click the **Click Here** link under IP Address Reservation in the LAN Settings page, a screen is displayed as shown in Figure 4.7.2.1 This is used for the reservation of IP address of client's MAC address in DHCP server.

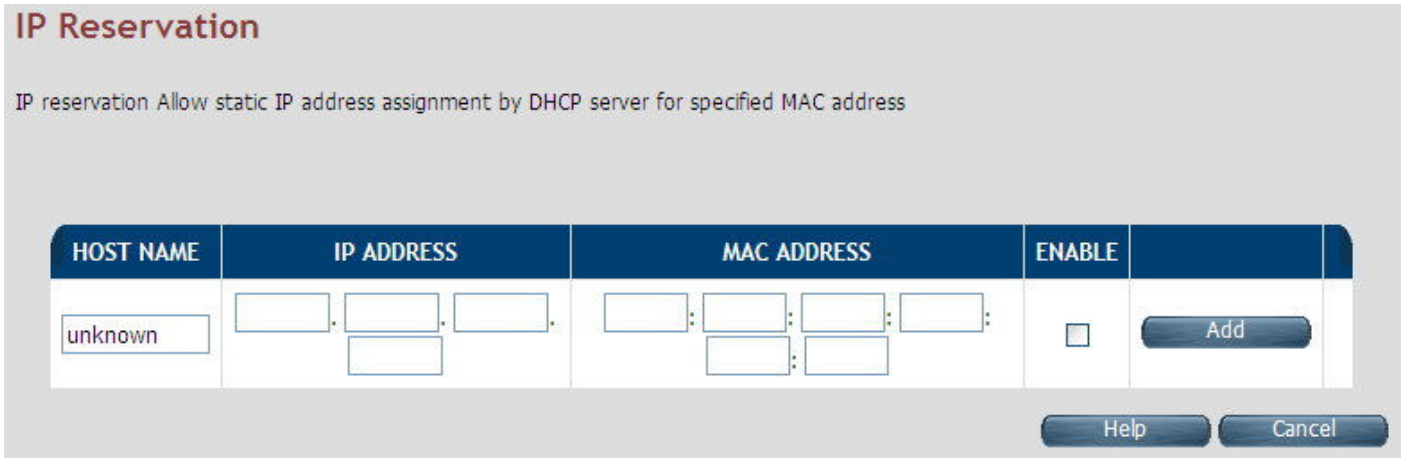



**Figure 4.7.2.1 IP Reservation**

The screen contains the following details:

**Fields in LAN Settings:**

| Field | Description |
|---|---|
| Host Name | Host Computer name. |
| IP Address | IP Address to be statistically reserved for this host identified by MAC address. |
| MAC Address | MAC address of Host computer for which static IP reservation is needed. |
| Enable | To enable this static IP reservation entry. |
| Add | To add this IP reservation entry. |

- Click APPLY to save the changes that users have entered.
- Click CANCEL to exit from this page without saving the changes.

The following pages describe the LAN Settings for IPv6:

### LAN Settings - IPv6 Tab

If IPv6 functionality is enabled through (**Advanced Setup > IPv6**), then LAN Settings web page also presents IPv6 tab. Based on the **Auto Configuration Mode**, the following screens are displayed as shown in Figure 4.7.2.2, Figure 4.7.2.3 and Figure 4.7.2.4.

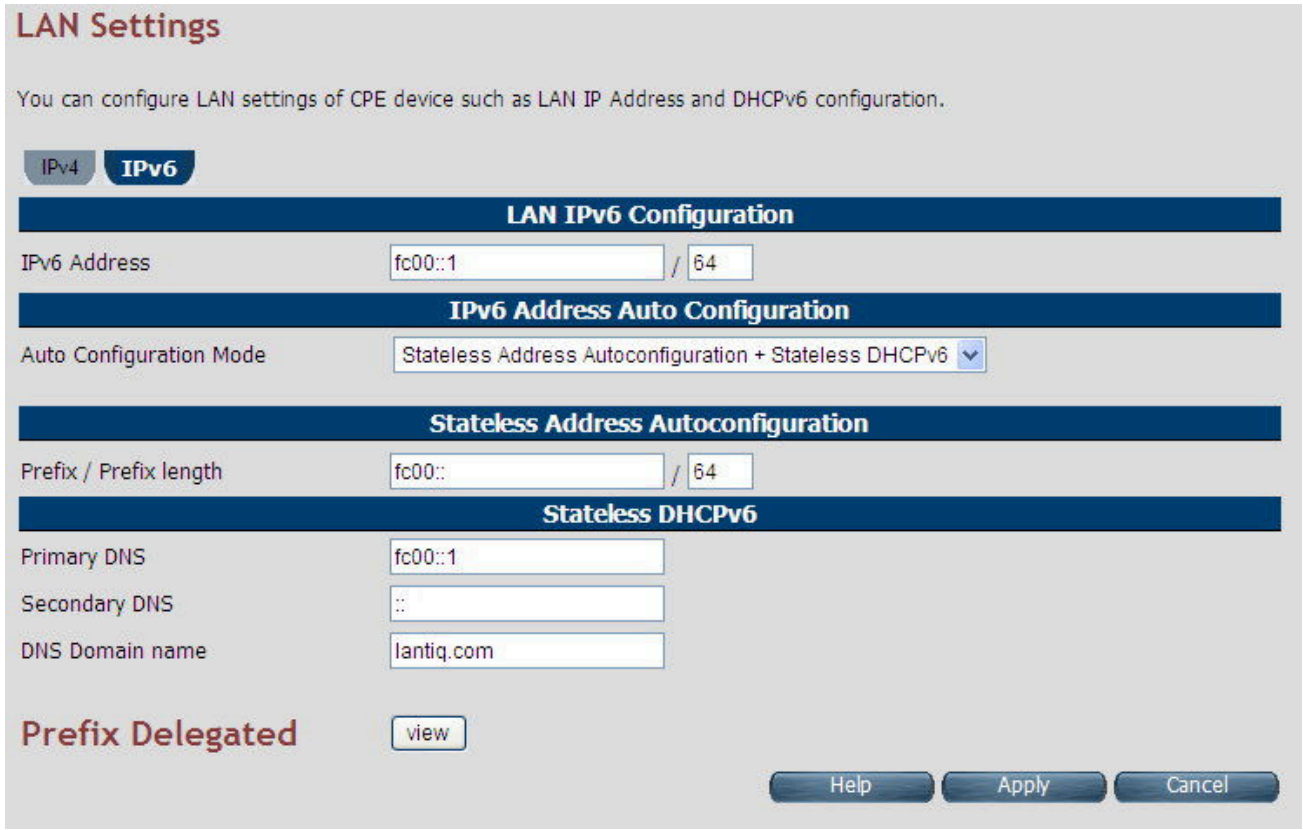


Figure 4.7.2.2 LAN Settings - IPv6 Tab (Option 1: SLAAC + Stateless DHCPv6)

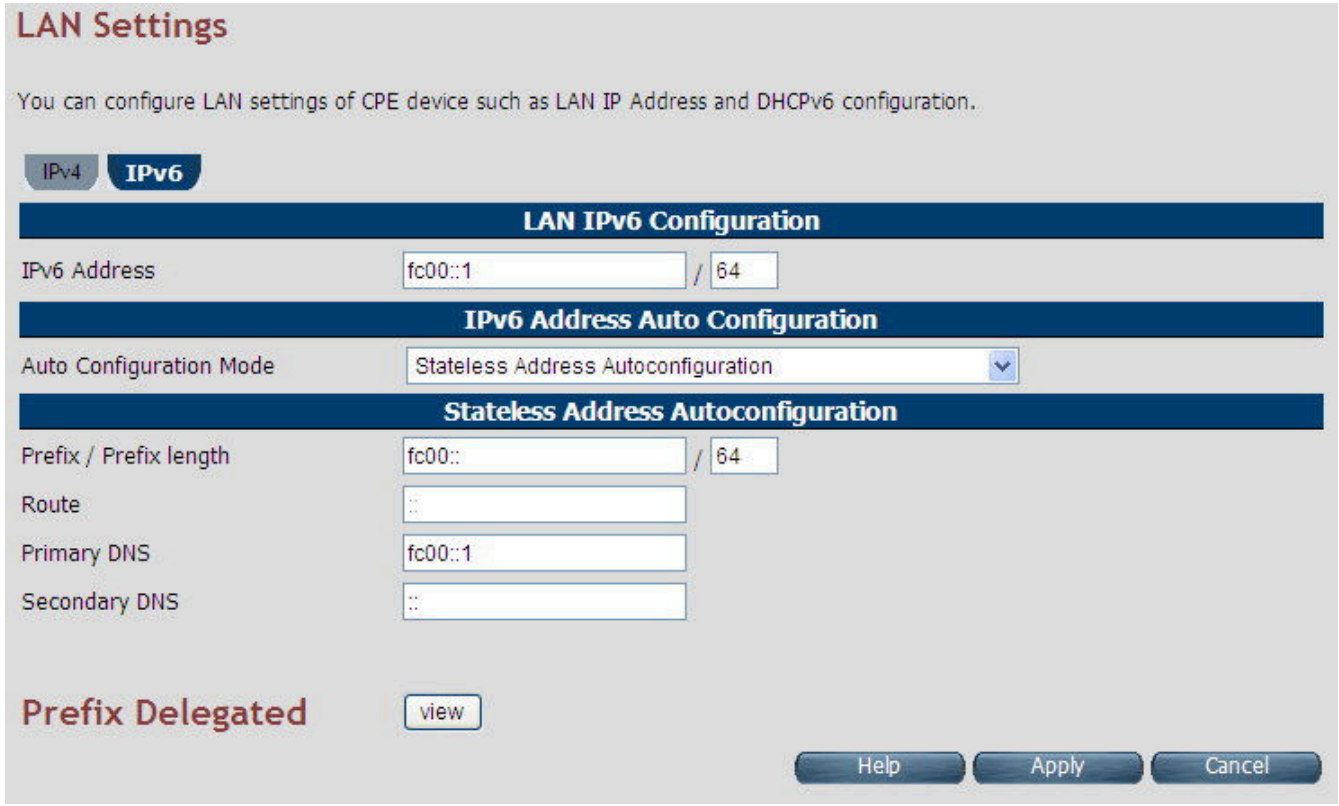



Figure 4.7.2.3 LAN Settings - IPv6 Tab (Option 2: SLAAC)

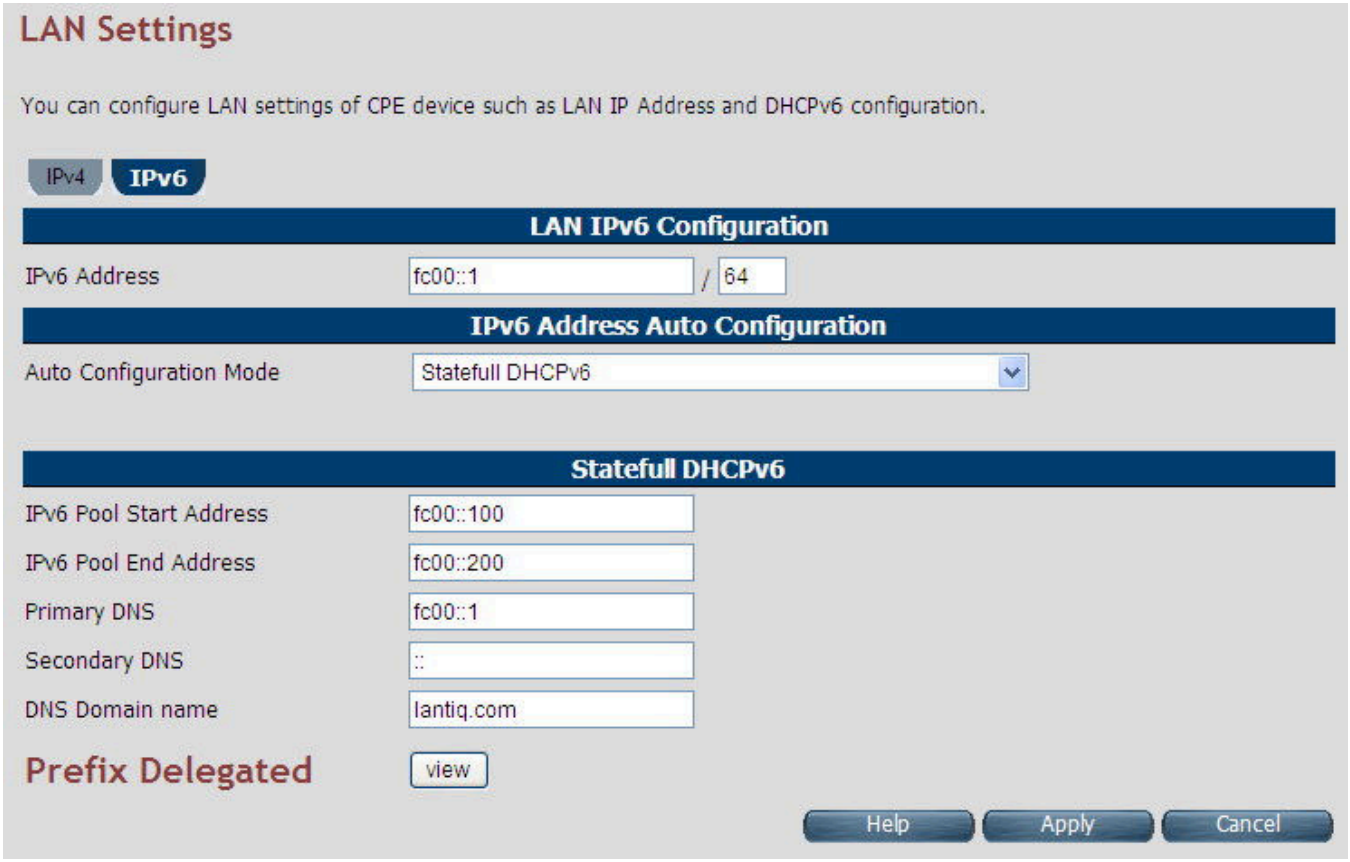



**Figure 4.7.2.4 LAN Settings - IPv6 Tab (Option 3: Stateful DHCPv6 Server)**

For LAN interface, the NV-600A uses SLAAC based prefix assignment to LAN hosts. The IPv6 prefix obtained from DHCPv6 on WAN is automatically passed to LAN hosts for their IPv6 address configuration.

The screen contains the following details:

**Fields in LAN Settings – IPv6:**

| Field | Description |
|---|---|
| **LAN IPv6 Configuration** | |
| IPv6 Address | IPv6 Address of CPE |
| **IPv6 Address Autoconfiguration** | |
| Auto Configuration Mode | Auto Configuration Mode on LAN interface for LAN hosts. • Stateless Auto Config (SLAAC) + Stateful DHCPv6 • Stateless Auto Config (SLAAC) Stateful DHCPv6 **Stateless Address Autoconfiguration** |
| **Stateless Address Autoconfiguration** | |
| Prefix/Prefix Length | IPv6 Prefix and Length Configuration. |
| Route | IPv6 Route for configuration in LAN host. |
| Primary DNS | Primary DNS for IPv6 name resolution. |
| Secondary DNS | Secondary DNS for IPv6 name resolution. |
| **Stateful DHCPv6** | |
| Primary DNS | Primary DNSv6 Address. |
| Secondary DNS | Secondary DNSv6 Address. |
| DNS Domain Name | Domain Name. |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

When users click **Prefix Delegated view** button in the LAN Settings - IPv6 page, a screen is displayed as shown in Figure 4.7.2.5

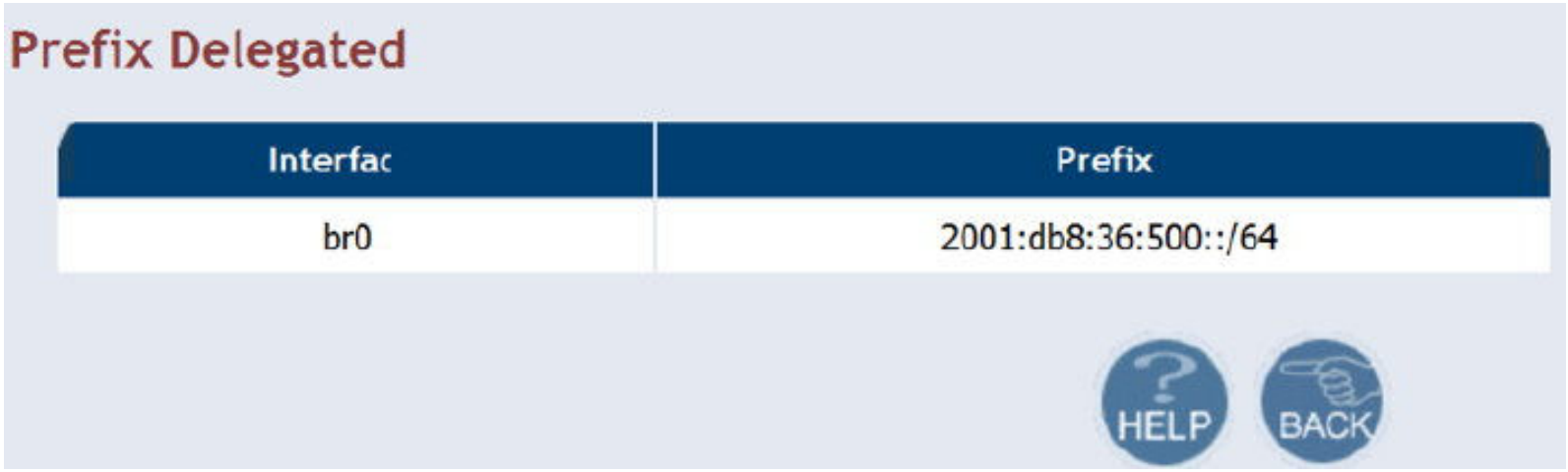



**Figure 4.7.2.5 Prefix Delegated view**

- Click **Back** to exit from this page.

### 4.7.3 UPnP Devices List

To discover the UPnP Devices in LAN network, click the **UPnP Devices** link (**LAN** > **UPnP Devices**) on the left navigation bar. When click UPnP page, please wait a few time to show the UpnP device information. A screen is displayed as shown in Figure 4.7.3

**Figure 4.7.3 UPnP device list**

The screen contains the following details:

**Fields in UPnP Device List:**

| Field | Description |
|---|---|
| UPnP Devices | IP address of the device connected discovered through UPnP protocol. |
| Friendly Name | Name of the device connected. |
| UUID | Universal Unique Identifier. |

◆ Click **Refresh** to view a new UPnP devices list.

### 4.7.4 LAN Switch Port Setting

To discover the All-LAN Port Setting in LAN network, click the **LAN Switch Port Setting** link (**LAN** > **LAN Switch Port Setting**) on the left navigation bar. A screen is displayed as shown in Figure 4.7.4

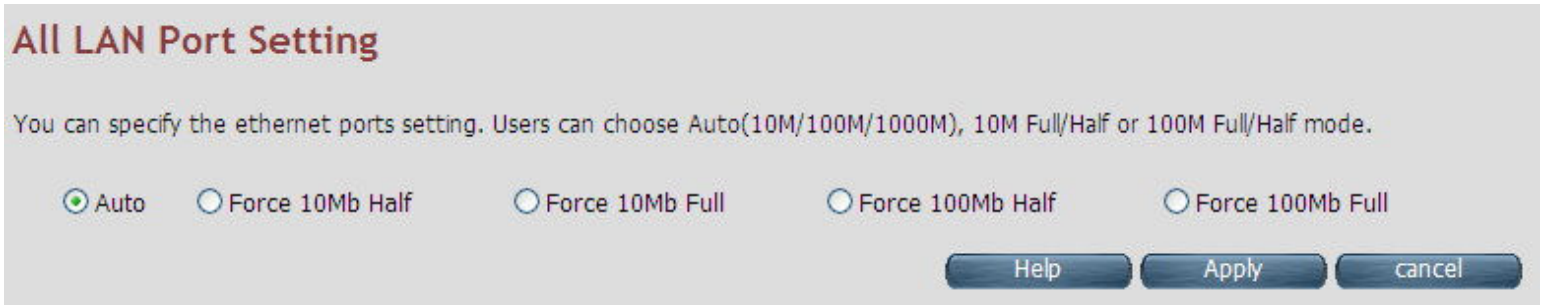



**Figure 4.7.4 All LAN Port Setting**

- Default value is "Auto 10/100 Full/Half".
- Click APPLY to save the information that has been entered.
- Click CANCEL to exit from this page without saving the changes.

### 4.7.5 LAN Port Status

To discover the LAN Port Status in LAN network, click the **LAN Port Status** link (**LAN** > **LAN Port Status**) on the left navigation bar. A screen is displayed as shown in Figure 4.7.5

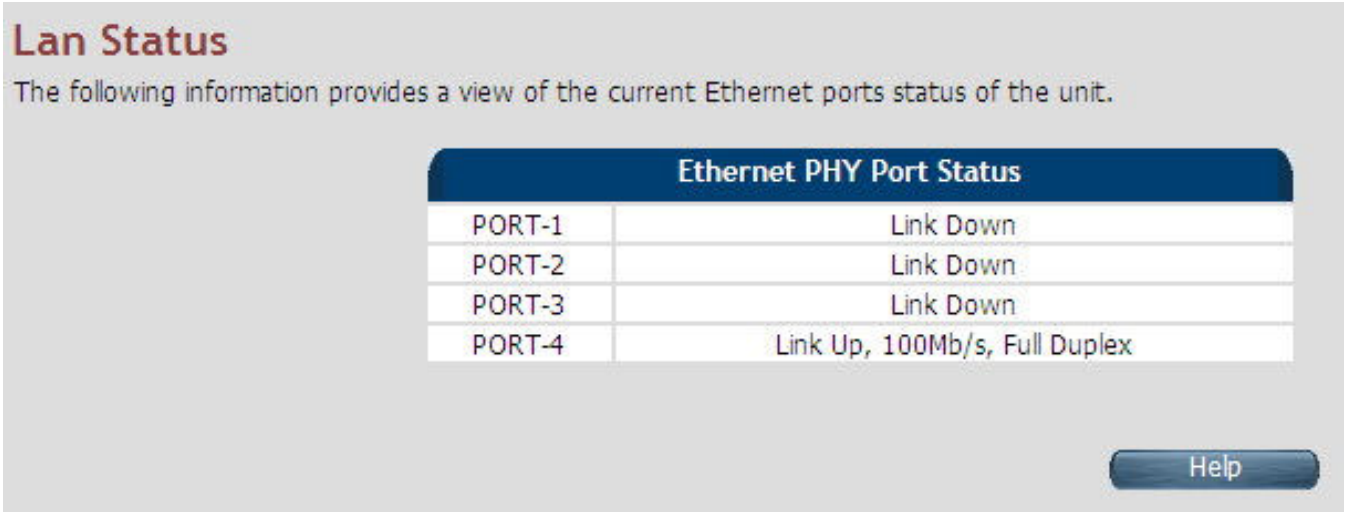



**Figure 4.7.5 LAN Port Status**

**Example Table:**

| Input 1 | Output 1 | Input 2 | Output 2 | Input 3 | Output 3 | Input 4 | Output 4 |
|---|---|---|---|---|---|---|---|
| NWAY 10M Full | 10M Full | Force 10M Full | 10M Half | None | Link Down | NWAY 10M Half | 10M Half |
| Input 5 | Output 5 | Input 6 | Output 6 | Input 7 | Output 7 | Input 8 | Output 8 |
| NWAY 100M Half | 100M Half | Force 100M Full | 100M Half | Auto 100M Full | 100M full | Auto | 100M FULL |

## 4.8 Select "Route"

If there are multiple routers installed on users' network, it is necessary to configure the VDSL2 router unit's routing functions. Select the "Route". The menu below includes the sub-menus of **Static Routing**, **RIP Support** and **Routing Table List**. Following are the options available under **Route** menu as shown in Figure 4.8.

**Figure 4.8 Route Options on the Left Navigator Bar**

### 4.8.1 Static Routing

The static routing function determines the path that data follows over users' network before and after it passes through users' router. Users can use static routing to allow different IP domain users to access the Internet through this VDSL2 Router device.

To set up Static Routing, click the **Static Routing** link (**Route > Static Routing**) on the left navigation bar. A screen is displayed as shown in Figure 4.8.1.

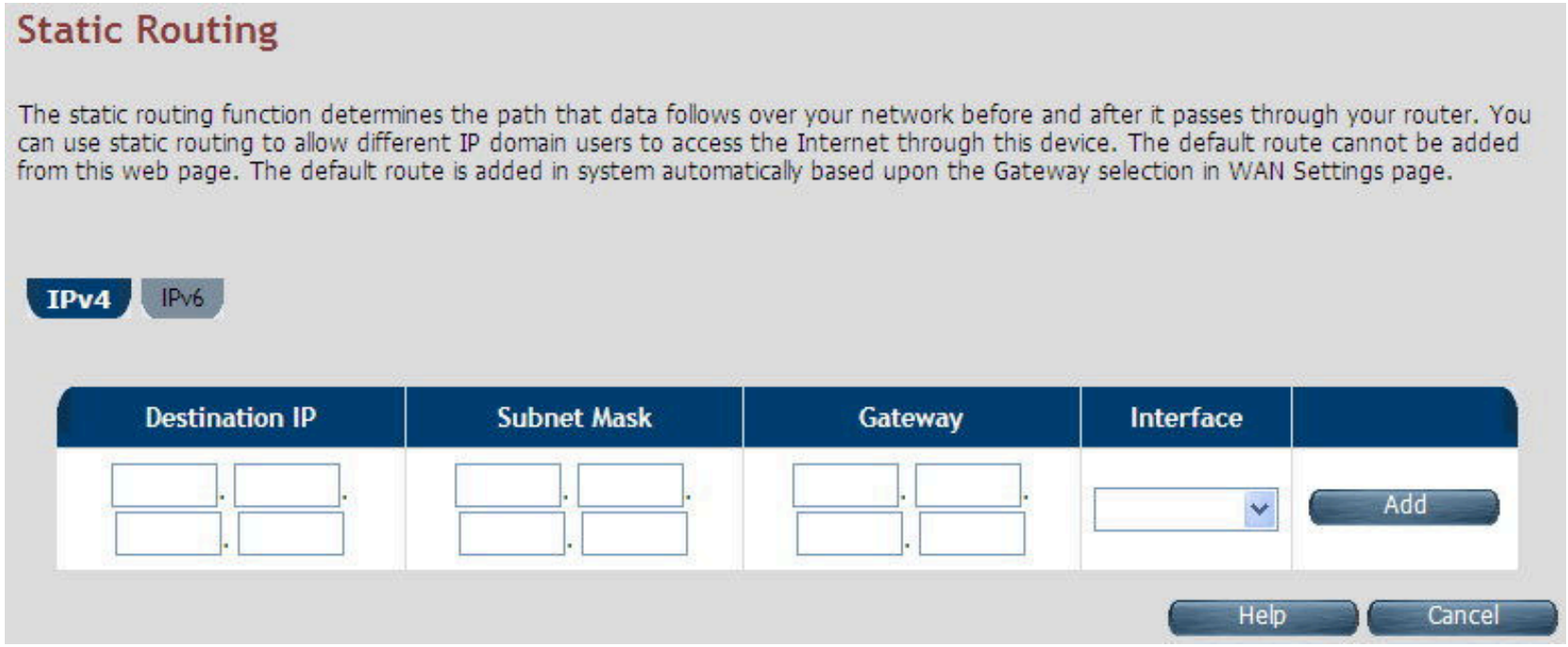



**Figure 4.8.1 Static Routing Configuration**

The screen contains the following details:

**Fields in Static Routing:**

| Field | Description |
|---|---|
| Destination LAN IP | To enter the destination IP Address of routing entry. Enter the IP Address **0-0-0-0** of routing entry. |
| Subnet Mask | To enter the Subnet Mask of routing entry. Enter the Subnet Mask **0-0-0-0** of routing entry. |
| Gateway | To enter the Gateway address of routing entry. Enter the Gateway address of routing entry. |
| Interface | To enter the outgoing interface name for this route. It can be selected from dropdown. |

- Click Add to create a new static route of specified destination IP, Netmask and Gateway values.
- Click **Cancel** to exit from this page without saving the changes.

**Notes:**

**1. Static Routing functionality is used to define the connected Gateway between the LAN and WAN.** For example, if we want to activate the Network Time Protocol (NTP) service, and we have to define the Gateway connected to NTP server in the WAN.

2. The gateway for static routing is just used for switch (Bridged) mode.

3. The gateway IP domain should be the same LAN, e.g. if the LAN IP is 192.168.1.1, the gateway IP should be 192.168.X. (where X is a number, range is 2-255)

When users click the **IPV6** tab on the Static Routing page, a screen is displayed as shown in Figure 4.8.1.1 The addition and deletion of static IPv6 routes is not supported currently.

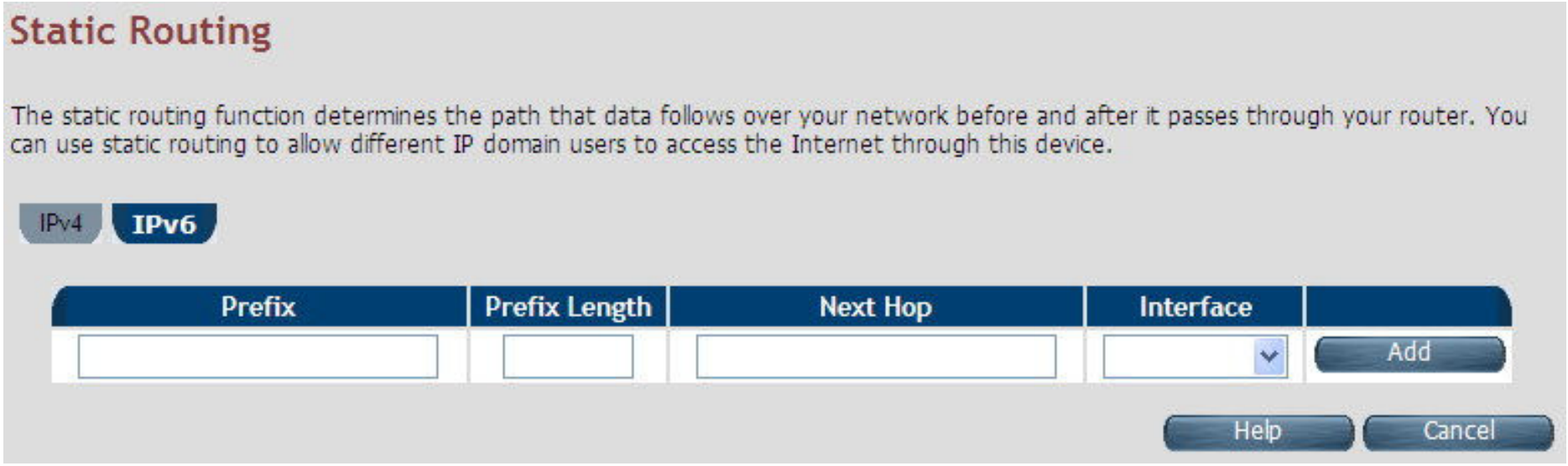



**Figure 4.8.1.1 Static Routing IPv6**

**Tip:**

Please note that default route should not be added from this web page. To configure default route, specify default Gateway on selected WAN in **WAN Setting** page.

### 4.8.2 RIP Support

The RIP support for enabling dynamic routes in CPE may be present in some pre-built packages. To enable the RIP support, click the **RIP Support** link (**Route > RIP Support**) on the left navigation bar. A screen is displayed as shown in Figure 4.8.2.

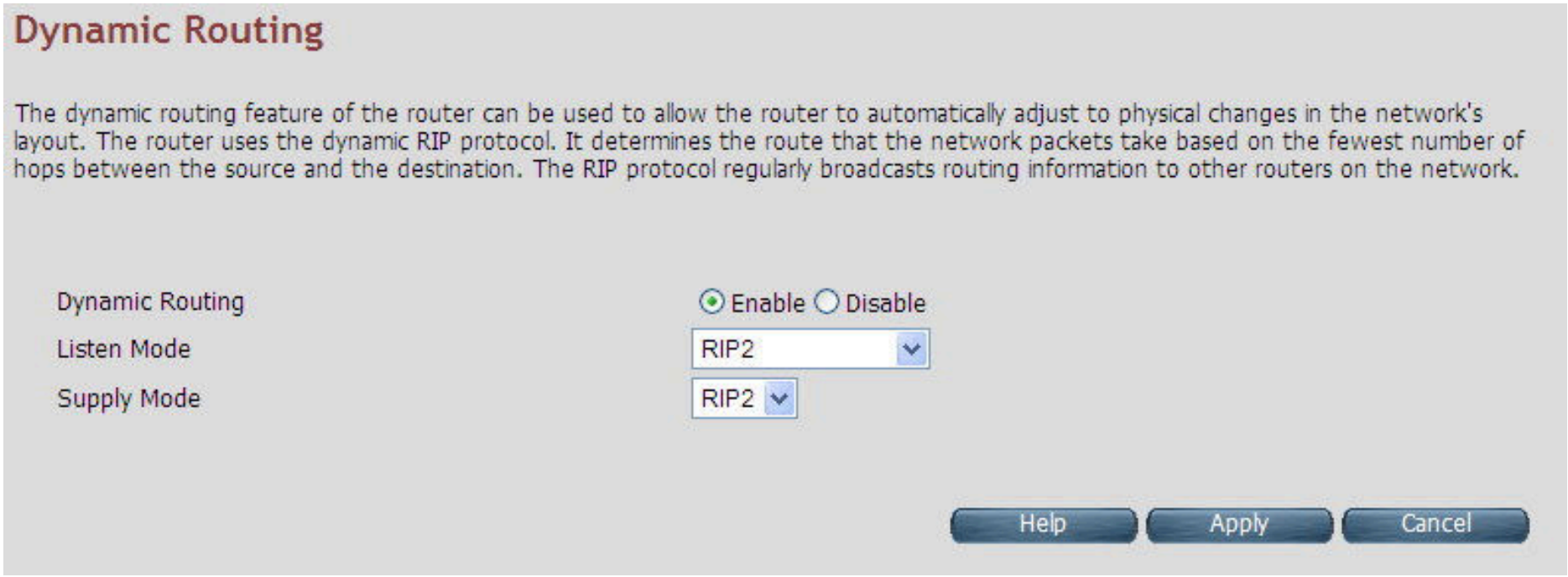



**Figure 4.8.2 Dynamic Routing**

The screen contains the following details:

**Fields in Dynamic Routing:**

| Field | Description |
|---|---|
| Dynamic Routing | To enable or disable the Dynamic Routing (RIP) in CPE. |
| Listen Mode | To configure the listen mode of RIP to:<br>◆ Disabled<br>◆ RIP1<br>◆ RIP2<br>◆ Both (RIP1 + RIP2) |
| Supply Mode | To configure the supply mode of RIP to:<br>◆ Disabled<br>◆ RIP1<br>◆ RIP2 |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

**Note (Reference Only):**

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed on a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance, in other words the route is considered unreachable.

RIP implements the split horizon, route poisoning and hold down mechanisms to prevent incorrect routing information from being

propagated. These are some of the stability features of RIP. It is also possible to use the Routing Information Protocol with Metric-Based Topology (RMTI) algorithm to cope with the count-to-infinity problem. With RMTI, it is possible to detect every possible loop with a very small computation effort.

RIP uses the User Datagram Protocol (UDP) as its transport protocol and is assigned the reserved port number 520.

**RIP version 1**: The original specification of RIP, defined in RFC 1058, was published in 1988 and uses classful routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). This limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must be the same size. There is also no support for router authentication, making RIP vulnerable to various attacks.

**RIP version 2**: Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed in 1993 and last standardized in 1998. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier specification if all Must Be Zero protocol fields in the RIPv1 messages are properly specified. In addition, compatibility switch features allow fine-grained interoperability adjustments.

### 4.8.3 Routing Table List

The Routing table allows users to see how many routings routing on users VDSL2 router routes table and interface information. To view the Routing entry table list of NV-600A, click on the "Routing Table List" link in the left navigation bar. A screen is displayed as shown in Figure 4.8.3.

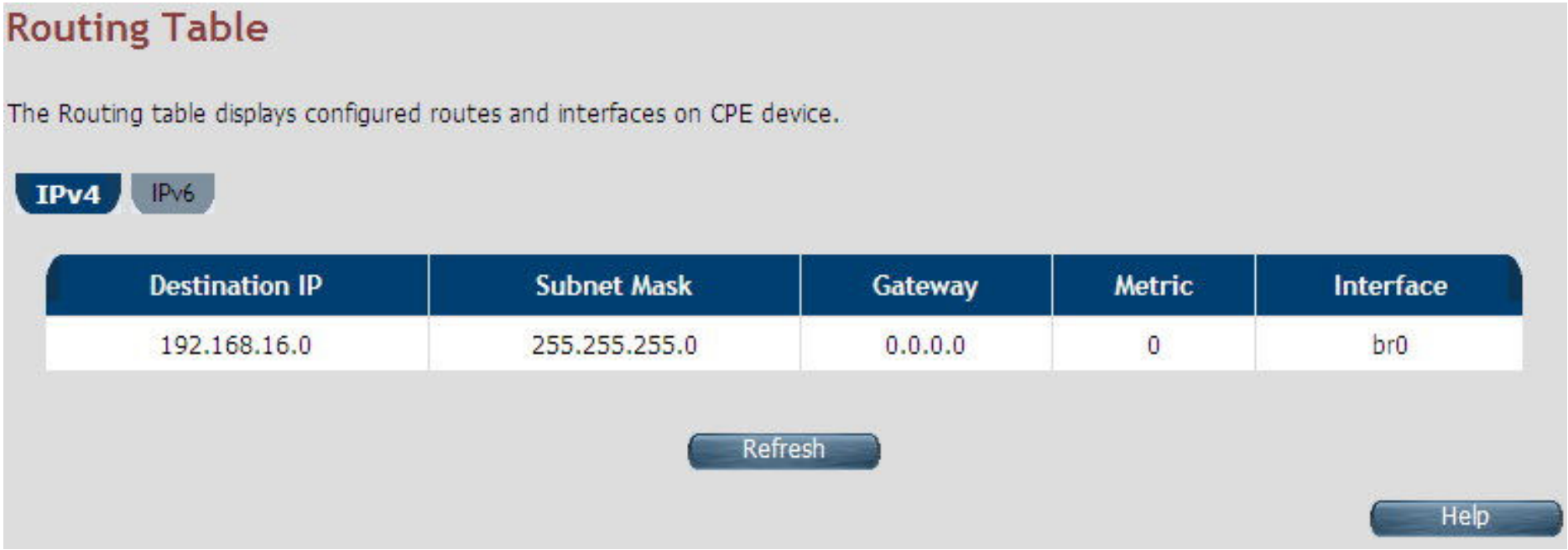



Figure 4.8.3 Routing Table List

The screen contains the following details:

**Fields in Static Routing:**

| Field | Description |
|---|---|
| Destination IP | Destination IPv4 address for route. |
| Subnet Mask | Destination IPv4 subnet mask for route. |
| Gateway | IPv4 gateway address for this route. |
| Metric | Routing metric is a number used by the routing protocol. Higher metrics have the effect of making a route less favorable by Router. |
| Interface | This depends on the interfaces currently configured in the system. Possible values are: br0 - Bridge interface • eth0 - First ethernet interface • eth1 - Second ethernet interface (maybe connected to an external switch) nas<i> - e.g. nas0. Ethernet over ATM interface (Applicable only to ATM WAN). • ppp<i> - e.g. ppp0. PPPoE or PPPoA interface |
| Refresh | When users click **Refresh** button, it will refresh the table of IPv4 routes by gathering fresh list of routes from system. |

**Routing Table List - IPv6 Tab**

If IPv6 functionality is enabled through (**Quick Setup > IPv6**), then the Routing Table List web page also lists all IPv6 routes in system under IPv6 tab as shown in Figure 4.8.3.1

**Figure 4.8.3.1 Routing List – IPv6 Tab**

## 4.9 Select "Firewall"

Users can view **Firewall** link on the left navigation bar of the NV-600A CPE homepage. The menu below includes the sub-menus of **Firewall Setting**, **IPv6 Firewall Setting**, **Packet Filtering**, **URL Filtering**, **Parental Control**, **Application Server Settings** and **ACL**. The following are the options available under **Firewall** as shown in Figure 4.8

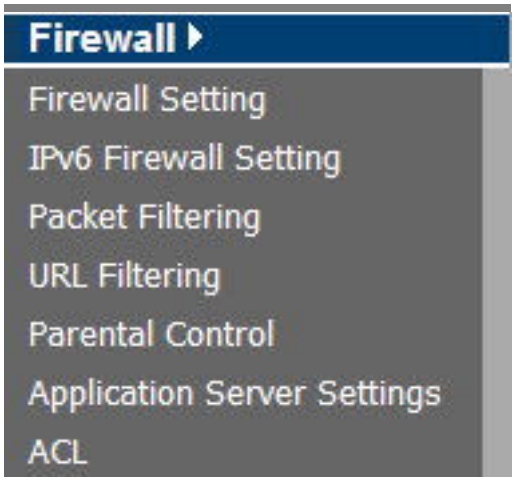



**Figure 4.9 Firewall Options**

### 4.9.1 Firewall Setting

To enable or disable the firewall, click the **Firewall Setting** link (**Firewall > Firewall Setting**) on the left navigation bar. A screen is displayed as shown in Figure 4.8.1

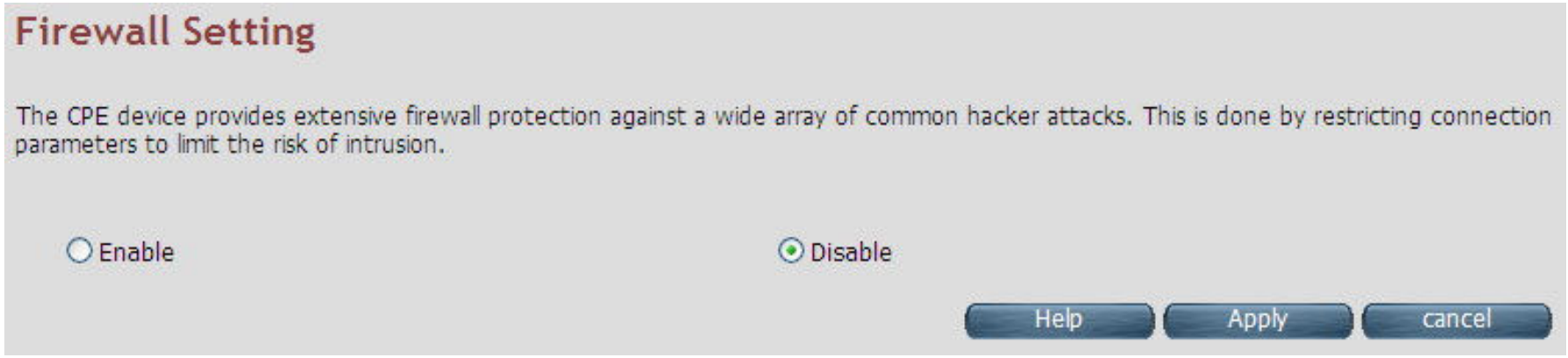



**Figure 4.9.1 Firewall Setting**

The screen contains the following details:

**Fields in Firewall Setting:**

| Field | Description |
|---|---|
| Firewall Setting | It allows to ENABLE or DISABLE the firewall in UGW. |

- Click APPLY at any time during configuration to save the information that users have entered.
- Click CANCEL to exit from this page without saving the changes.

### 4.9.2 IPv6 Firewall Setting

To enable or disable the firewall, click the **IPV6 Firewall Setting** link (**Firewall > IPv6 Firewall Setting**) on the left navigation bar. A screen is displayed as shown in Figure 4.8.2

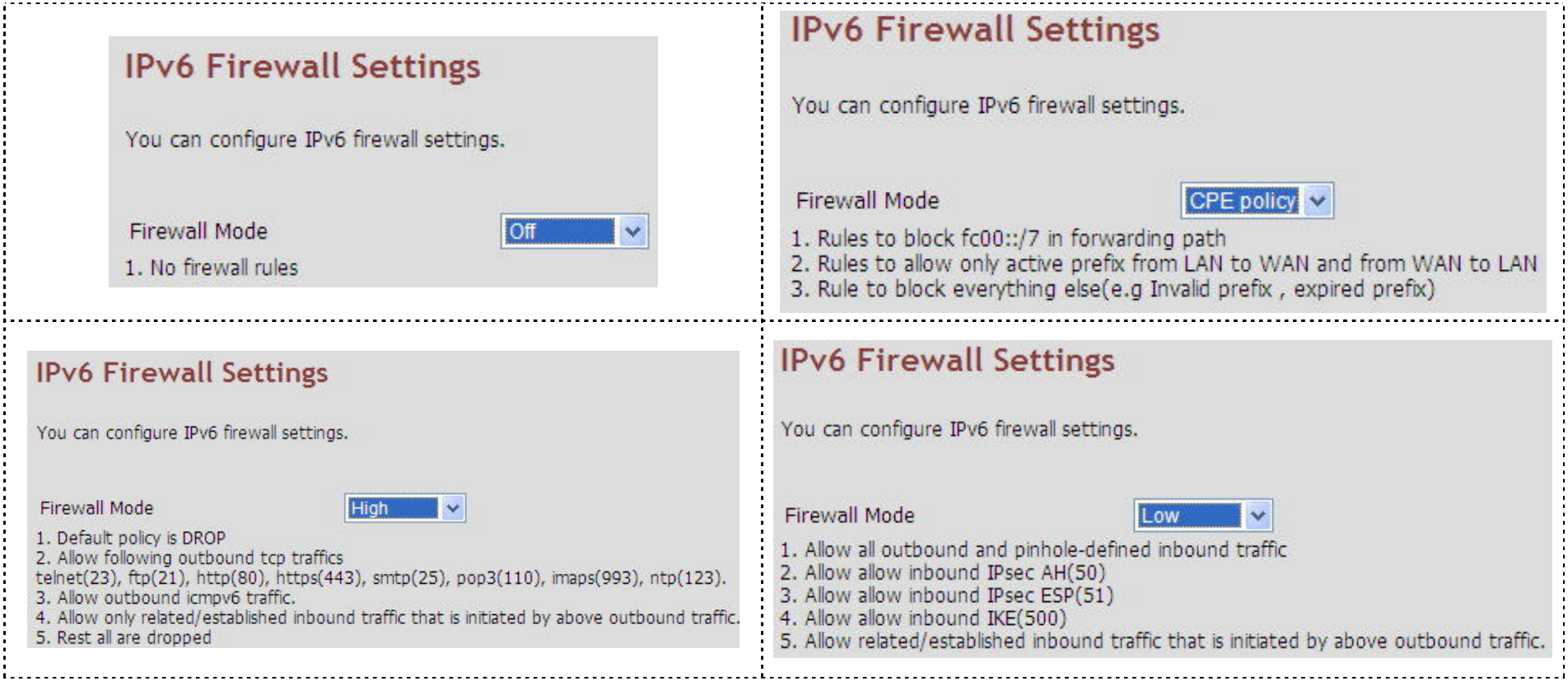



**Figure 4.9.2 IPv6 Firewall Setting**

The screen contains the following details:

**Fields in UPnP Settings:**

| Field | Description |
|---|---|
| Firewall Mode | The available options are **Off**, **CPE policy**, **High** and **Low**. |

- Click APPLY for committing the desired action.
- Click CANCEL to exit from this page without saving the changes.

### 4.9.3 Packet Filtering

To enable Packet Filtering, click the **Packet Filtering** link (**Firewall > Packet Filtering**) on the left navigation bar. A screen is displayed as shown in Figure 4.8.3

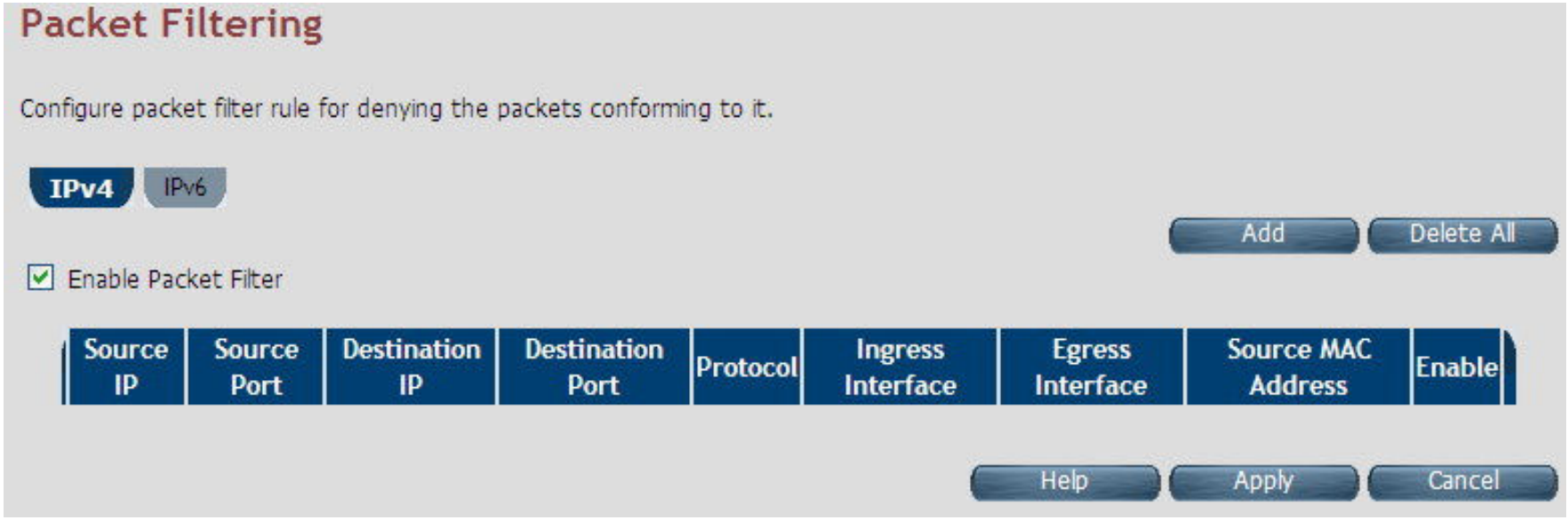



**Figure 4.9.3 Packet Filtering**

The screen contains the following details:

**Fields in Packet Filtering:**

| Field | Description |
|---|---|
| IPV4/IPv6 | Choose the appropriate tab to configure. |
| Enable Packet Filter | To enable or disable the Packet Filter feature of NV-600A CPE. To enable, select the check box. |
| Source IP | Filter IP Address range of the local machine under NV-600A CPE. |
| Source Port | Filter Port number range of the local machine under NV-600A CPE. |
| Destination IP | IP address of the destination. |
| Destination Port | Port address of the destination. |
| Protocol | Filter protocol. (TCP or UDP). |
| Ingress Interface | Input interface of the packet. |
| Egress Interface | Output interface of the packet. |
| Source MAC Address | Source MAC Address of packet originating host. |
| Enable | To provide more IP Addresses of the WAN interface. |
| Add | On pressing Add button, the screen shown in Figure 4.8.3.1 is displayed for adding a new packet filtering rule in system. |
| Delete All | To delete all the packet filtering rules configured in system. |

- Click Apply at any time during configuration to save the information that users have entered.
- Click CANCEL to exit from this page without saving the changes.

When users have chosen IPv4 tab, and click Add button in the Packet Filtering page, a screen is displayed as shown in Figure 104. If. users choose IPv6 tab and click on Add button, a screen is displayed as shown in Figure 4.8.3.2.

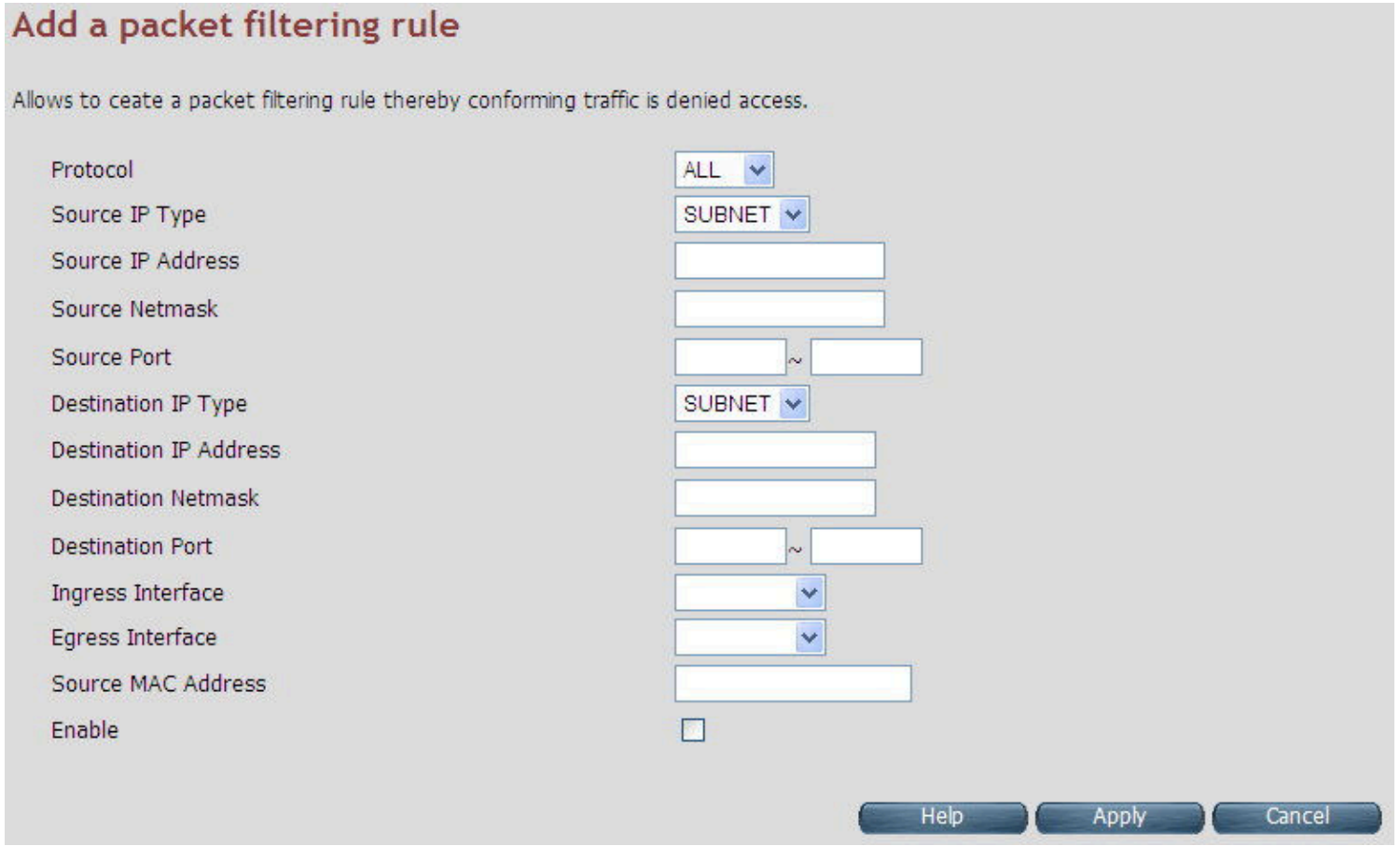



**Figure 4.9.3.1 Add a Packet Filtering Rule for Firewall - IPv4**

The screen contains the following details:

**Fields in "Add a Packet Filtering Rule" page:**

| Field | Description |
|---|---|
| Protocol | To select the protocol. The options available are ALL, TCP, UDP, ICMP, AH and ESP. |
| Source IP | The source IP can be a SINGLE address or a SUBNET, involving a range of IP addresses. |
| IP Address | To specify the source IP address. |
| Netmask | To specify the netmask for the source address. |
| Source Port | To specify the range of the source port. Valid for protocols TCP or UDP only. |
| Destination IP Type | The destination IP can be a SINGLE address or a SUBNET or All involving a range of IP addresses. |
| IP Address | To specify the destination IP address. |
| Netmask | To specify a netmask for the destination IP address. |
| Destination Port | To specify the range of the destination port. Valid for protocols TCP or UDP only. |
| Ingress Interface | To specify the input interface of the packet from dropdown options. (e.g. WAN1). |
| Egress Interface | To specify the output interface of the packet from dropdown options. (e.g. WAN2). |
| Source MAC Address | This is the source host's MAC address. |
| Enable | To enable/disable the particular packet filtering rule. |

- Click Apply at any time during configuration to for adding the packet filtering rule.
- Click CANCEL to exit from this page without saving the changes.

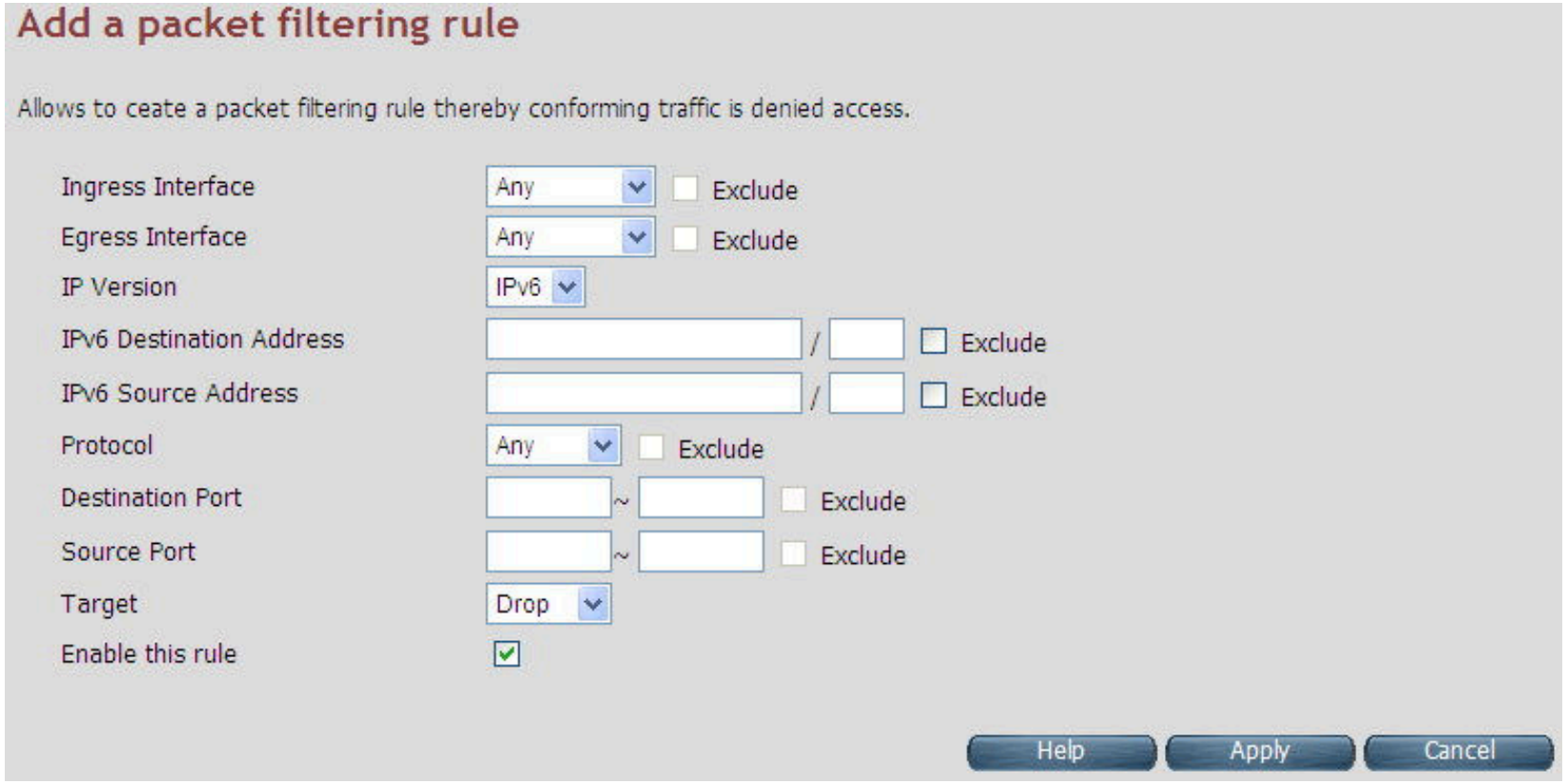



**Figure 4.9.3.2 Add a Packet Filtering Rule for Firewall - IPv6**

The screen contains the following details:

**Fields in "Add a Packet Filtering Rule - IPv6" page:**

| Field | Description |
|---|---|
| Ingress Interface | To specify the input interface of the packet from dropdown options. (e.g. WAN1). |
| Egress Interface | To specify the output interface of the packet from dropdown options. (e.g. WAN2). |
| Exclude | To exclude the selected option. |
| IP Version | Displays the IP version. |
| IP Source Address | To specify the source IP address. |
| Protocol | To select the protocol. The options available are ALL, TCP, UDP, ICMP, AH and ESP. |
| Source Port | To specify the range of the source port. Valid for protocols TCP or UDP only. |
| Destination Port | To specify the range of the destination port. Valid for protocols TCP or UDP only. |
| Destination IP Type | The destination IP can be a SINGLE address or a SUBNET or All involving a range of IP addresses. |
| Exclude | To exclude the selected option. |
| Target | The available options are Drop, Reject and Accept. |
| Enable this rule | Enable/disable this rule. |

- Click Apply at any time during configuration to for adding the packet filtering rule.
- Click CANCEL to exit from this page without saving the changes.

## ◆ Packet Filtering configuration example:

### 1. Packet Filter configuration procedures:

(1). All devices must be connected and turned on.

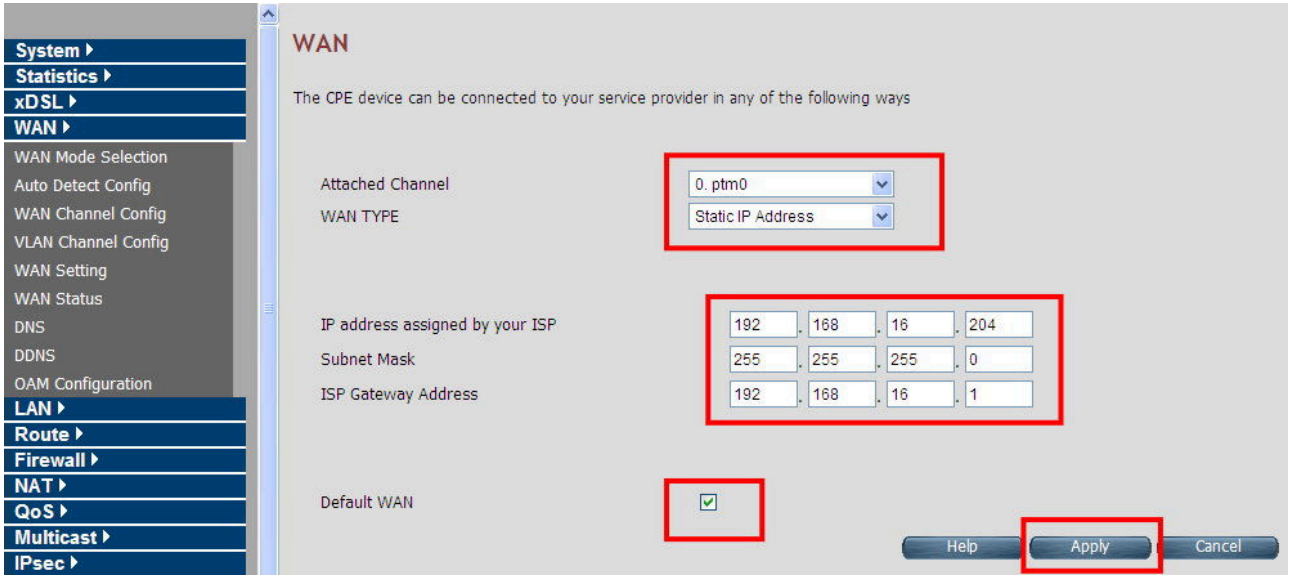
(2). Confirm that the NV-600A is in router mode (default mode).

(3). If there is no router mode, please refer to the following configuration diagram to configure the router mode and packet filter.

(4). All the configuration arguments are for reference only.

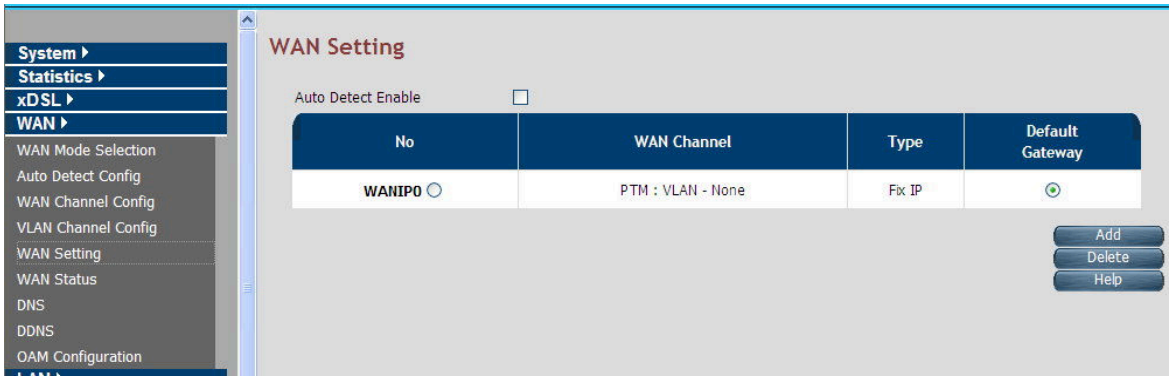
### 2. Router mode configuration:

◆ WAN setting



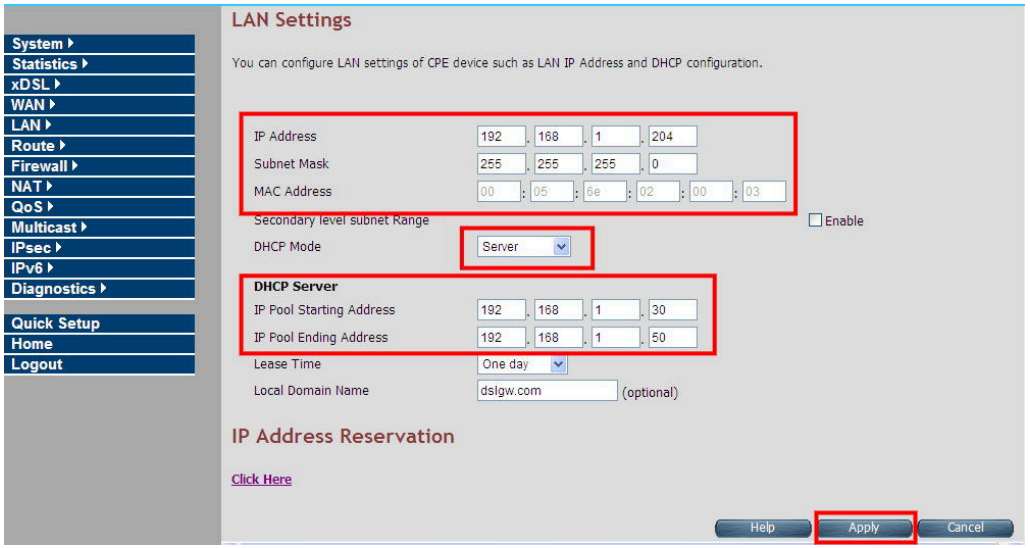
**Configure example: WAN→WAN Setting**

| Items | Setting argument / Action |
|---|---|
| Attached Channel | Default |
| WAN TYPE | Static IP Address |
| IP address assigned by tour ISP | WAN IP: 192.168.16.204 (Example) |
| Subnet Mask | 255.255.255.0 (Example) |
| ISP Gateway Address | 192.168.16.1(Example) |
| Default WAN | Please check box |
| Apply Button | Click it |




**WAN setting complete**

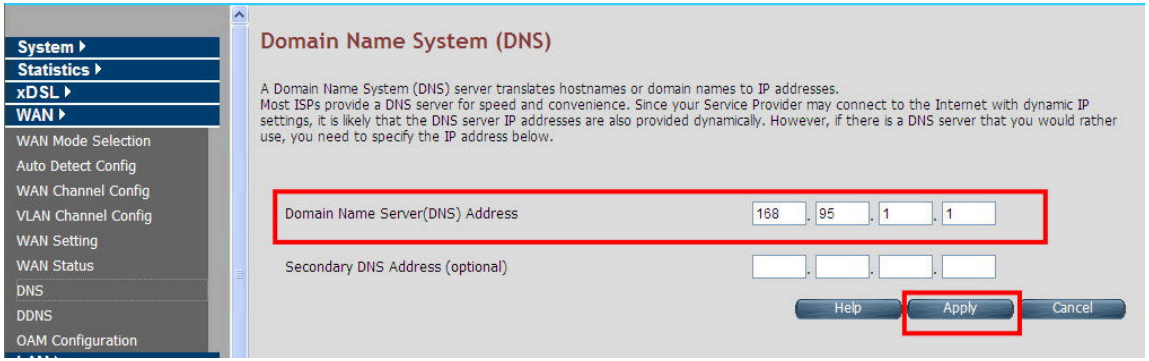
◆ **LAN Setting**




**Configure example: LAN→LAN Settings**

| Items | Setting argument / Action |
|---|---|
| IP Address | LAN IP: 192.168.1.204 (Example) |
| Subnet Mask | 255.255.255.0(Example) |
| MAC Address | NV-600A mac address (Auto detect) |
| DHCP Server | Server |
| IP Pool Starting Address | 192.168.1.30 (DHCP IP pool example) |
| IP Pool Ending Address | 192.168.1.50 (DHCP IP pool example) |
| Apply Button | Click it |

◆ **DNS Setting**

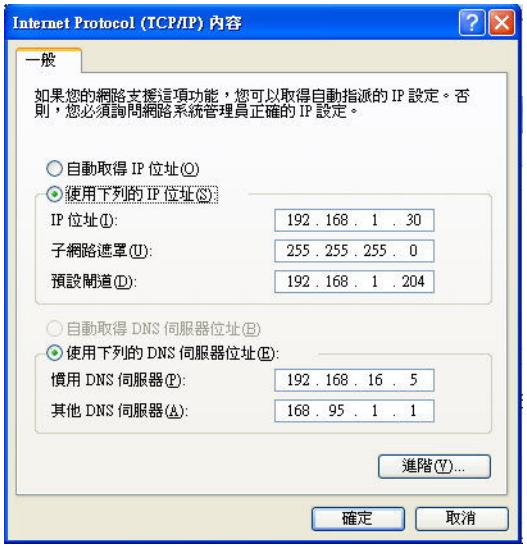



**Configure example: WAN→DNS**

| Items | Setting argument / Action |
|---|---|
| DNS Address | DNS IP: 168.95.1.1 (Example) |
| Apply Button | Click it |

**Note:** When configuration is completed with the above arguments, please reboot the NV-600A.

◆ **PC NIC card setting**

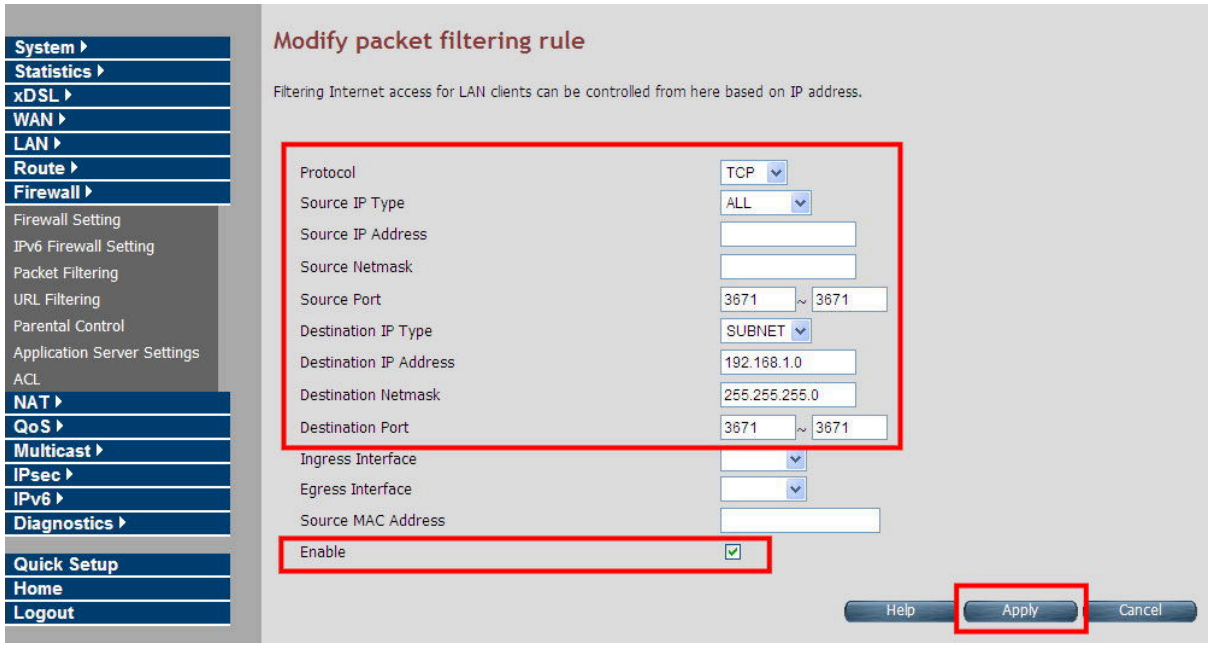



**Configure example:**

| Items | Setting argument / Action |
|---|---|
| IP Address | PC LAN IP: 192.168.1.30 (Example) |
| Subnet Mask | 255.255.255.0 (Example) |
| Gateway | 192.168.1.204 (Example) |
| DNS | 192.168.16.5 (Example) |

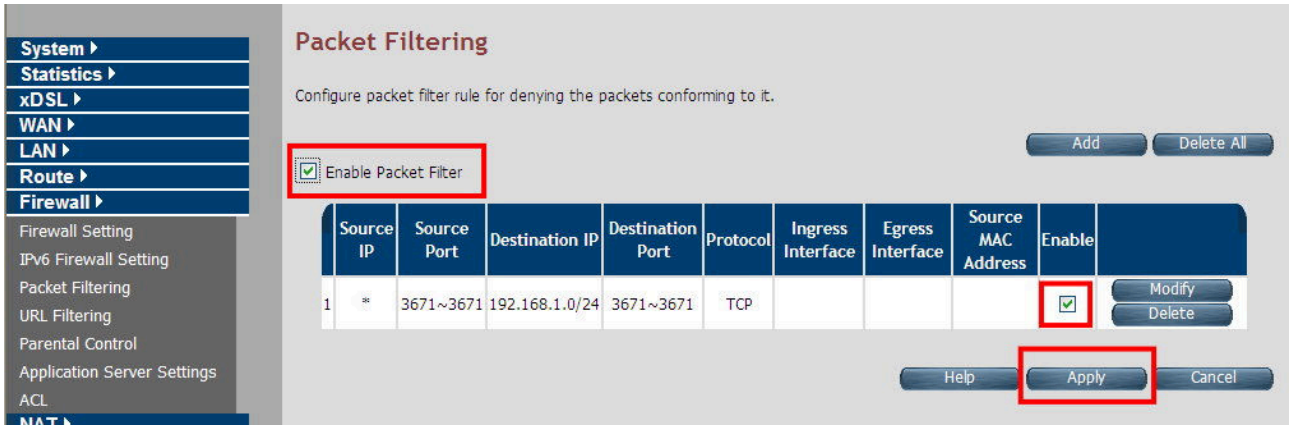
**3. Packet Filtering configuration:**

## ◆ NV-600A Packet Filtering



**Configure example: Firewall Packet Filtering**

| Items | Setting argument / Action |
|---|---|
| Protocol | TCP (Example) |
| Source IP Type | ALL (All source IP Address) |
| Source port | 3671~3671 |
| Destination IP Type | Subnet |
| Destination IP Address | 192.168.1.0<br>(Example, it means 192.168.1.0~192.168.16.255) |
| Destination Netmask | 255.255.255.0 (Example) |
| Destination port | 3671~3671 |
| Enable | Please check box |
| Apply Button | Click it |




**Packet filtering complete**

◆ **Enable Firewall function:**

The firewall has to be enabled in order to start the packet filter.

**Note:**

All the setting arguments above are examples; please follow the on-site environment to set.

## 4.9.4 URL Filtering

Using URL Filtering, the user can block the access to specific URLs to the web users by adding them to the list in the URL Blocking web page. To configure the URL Filtering, click the **URL Filtering** link (**Firewall > URL Filtering**) on the left navigation bar. A screen is displayed as shown in Figure 4.8.4

**Figure 4.9.4 URL Blocking**

The screen holds the following details:

**Fields in URL Blocking:**

| Field | Description |
|---|---|
| Domain Name | URL of the domain that needs to be blocked. For example: www.google.com.tw |
| Select | Selecting this option to remove the URL entry from the blocked list. |

- Click Add for adding a new URL filtering entry.
- Click Delete for deleting the existing URL filtering entry.

### 4.9.5 Parental Control

To configure the Parental Control, click the **Parental Control** link (**Firewall > Parental Control**) on the left navigation bar. A screen is displayed as shown in Figure 4.8.5

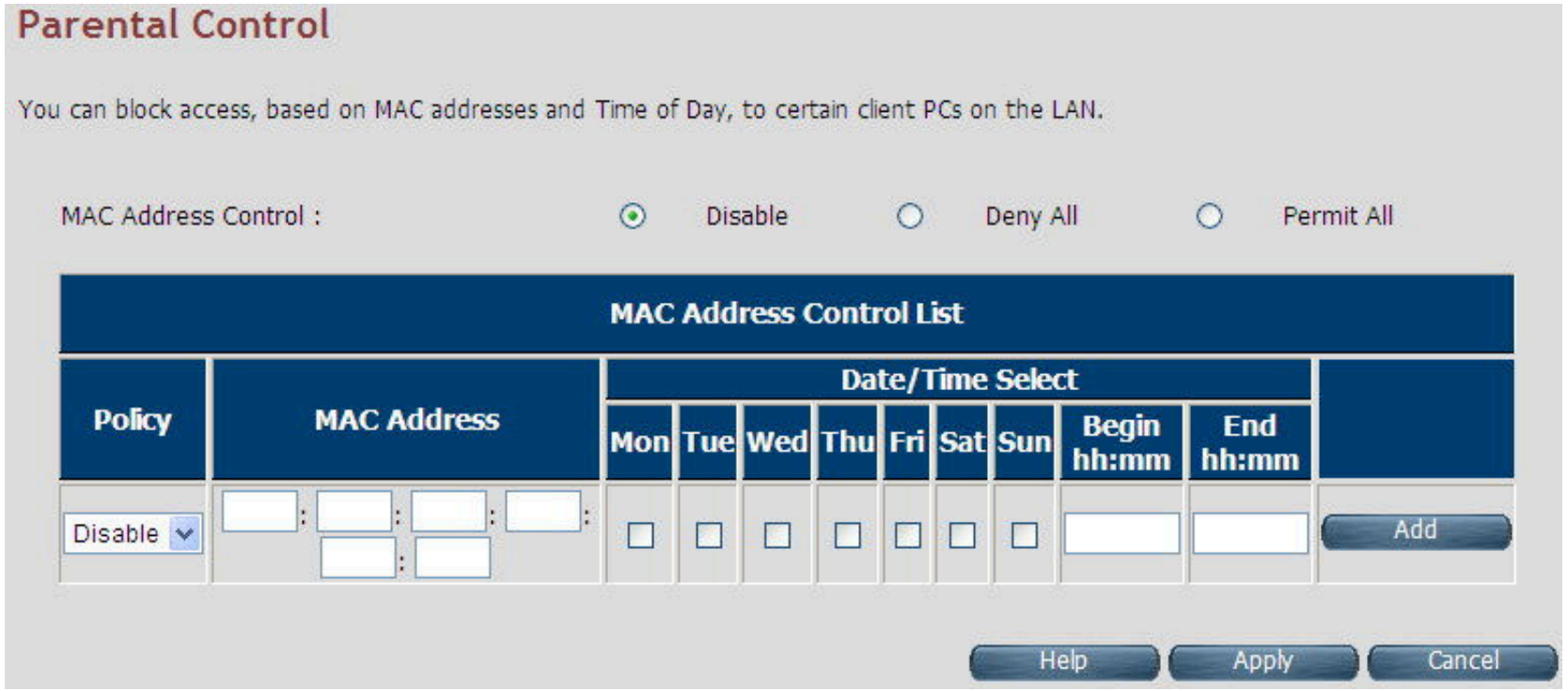



**Figure 4.9.5 Parental Control Configuration**

The screen contains the following details:

**Fields in Parental Control:**

| Field | Description |
|---|---|
| MAC Address Control | To disable/" deny all"/" permit all" - MAC address control feature. |
| MAC Address Control List | |
| Policy | To specify whether the particular MAC address is disabled, denied or permitted. |
| MAC Address | To assign the controlled MAC address for local machine. |
| Date/Time Select | To select the day(s) and time slot when the policy has to be applied on the MAC address provided. The Begin time entered should not be later than the End time and should be in the 24-hour format (hh:mm). |

- Click Add at any time during configuration to add the specified MAC address entry in the table.
- Click Apply at any time during configuration to save the information that users have entered.
- Click Cancel to exit from this page without saving the changes.

### 4.9.6 Application Server Settings

To configure the Application Server Settings, click the **Application Server** Settings link (**Firewall** > **Application Server Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.8.6

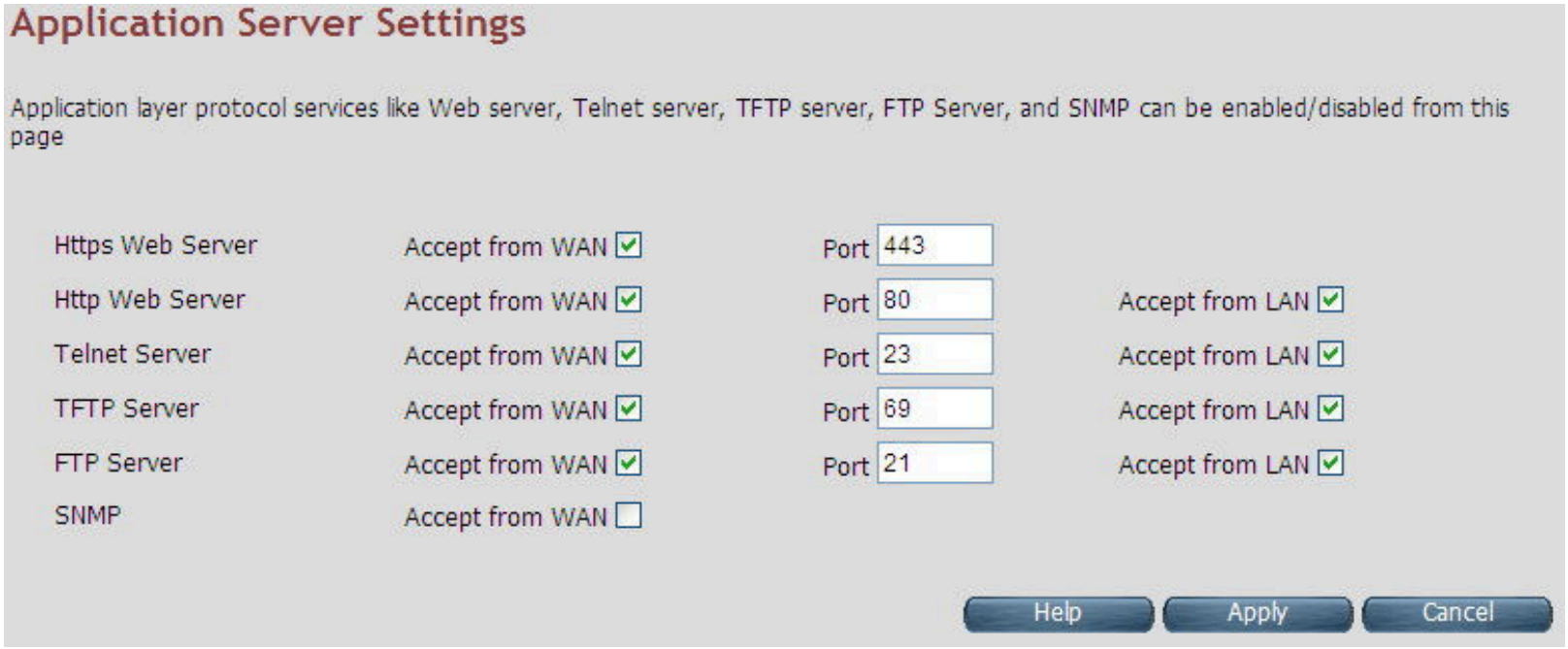



**Figure 4.9.6 Application Server Settings**

The screen contains the following details:

**Fields in Application Servers Settings:**

| Field | Description |
|---|---|
| Web Server | Web Server settings:<br>◆ The acceptance from WAN<br>◆ The Port Number<br>◆ The acceptance from LAN |
| Telnet Server | Telnet Server settings:<br>◆ The acceptance from WAN<br>◆ The Port number<br>◆ The acceptance from LAN |
| TFTP Server | TFTP Server Settings:<br>◆ The acceptance from WAN<br>◆ The Port number<br>◆ The acceptance from LAN |
| FTP Server | FTP Server Settings:<br>◆ The acceptance from WAN<br>◆ The Port number<br>◆ The acceptance from LAN |
| FTP Server | FTP Server Settings:<br>◆ The acceptance from WAN<br>◆ The Port number<br>◆ The acceptance from LAN |
| SNMP | SNMP Server Settings:<br>◆ Acceptance from WAN |

- Click Apply for committing the App Server settings.
- Click Cancel to exit from this page without saving the changes.

### 4.9.7 Access Control List (ACL)

To configure the access control list, click the **ACL** link (**Firewall > ACL**) on the left navigation bar. This can be used for allowing specified IP addresses to access the NV-600A CPE from WAN. The system allows up to 16 ACL entries to be configured in the CPE device. A screen is displayed as shown in Figure 4.8.7.

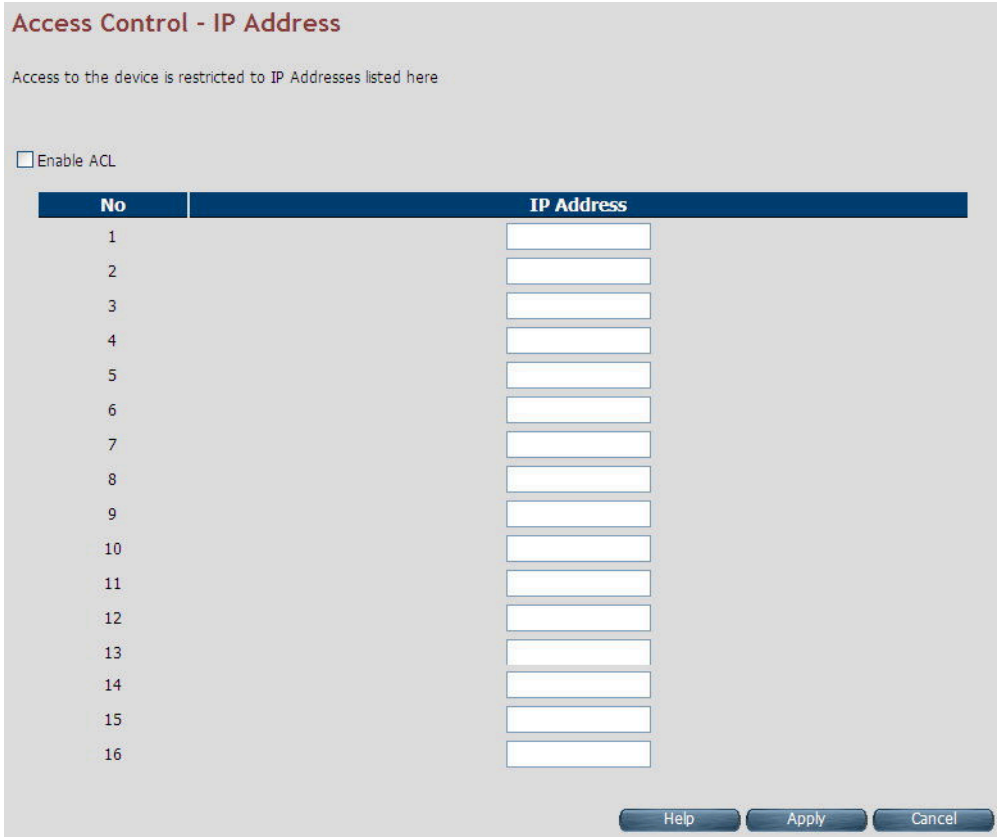



**Figure 4.9.7 Application Server Settings**

The screen contains the following details:

**Fields in ACL Setting:**

| Field | Description |
|---|---|
| Enable ACL | To enable/disable ACL settings. |
| IP Address | If ACL is enabled, the IP addresses specified here are allowed to access device. |

- Click Apply after filling in the IP address for adding the entry to ACL list.
- Click Cancel to exit from this page without saving the changes.

## 4.10 NAT

Users can view the NAT on the left navigation bar of the NV-600A CPE homepage. The menu below includes the sub-menus of **NAT Settings**, **Virtual Server**, **PortTriggering** and **DMZ**. The following are the options available under NAT as shown in Figure 4.10

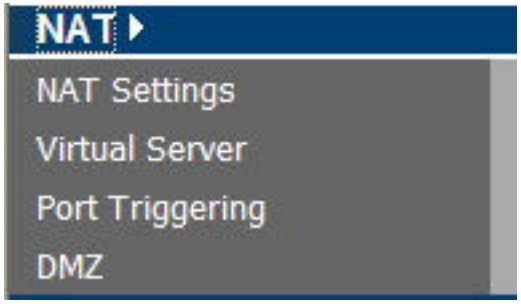



**Figure 4.10 NAT Options**

## 4.10.1 NAT Settings

To configure Network Address Translation (NAT), click the **NAT Settings** link (**NAT > NAT Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.9.1

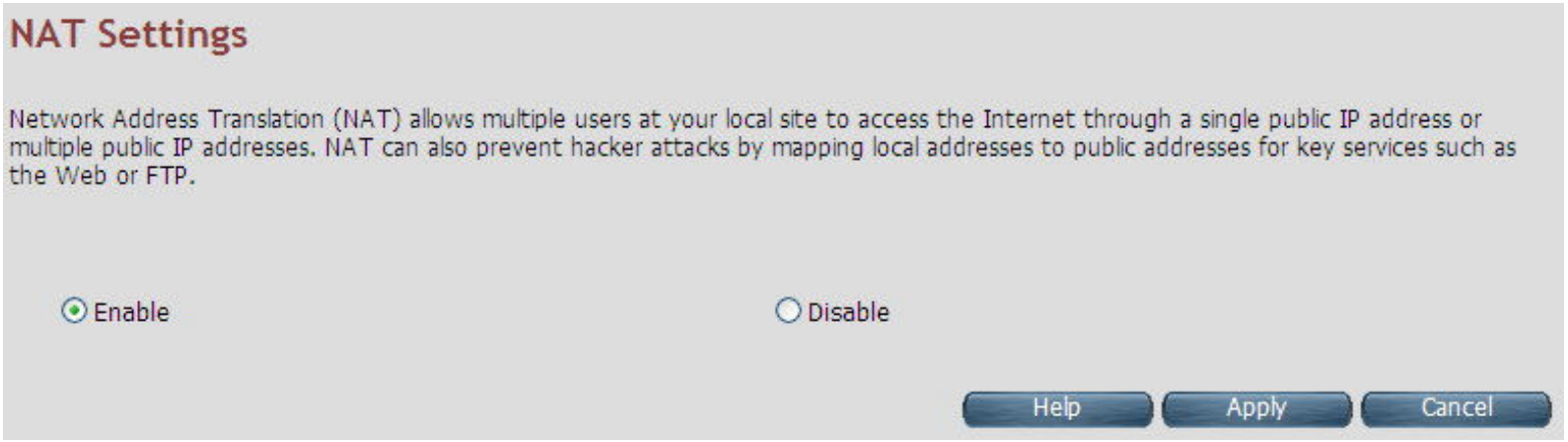



**Figure 4.10.1 Network Address Translation (NAT) Settings**

The screen contains the following details:

**Fields in Network Address Translation:**

| Field | Description |
|---|---|
| NAT Settings | Used to Enable or Disable the Network Address Translation feature. |

- Click Apply for activating or deactivating the NAT feature.
- Click CANCEL to exit from this page without saving the changes.

### 4.10.2 Virtual Server

To configure the virtual server, click the **Virtual Server** link (**NAT > Virtual Server**) on the left navigation bar. A screen is displayed as shown in Figure 4.9.2

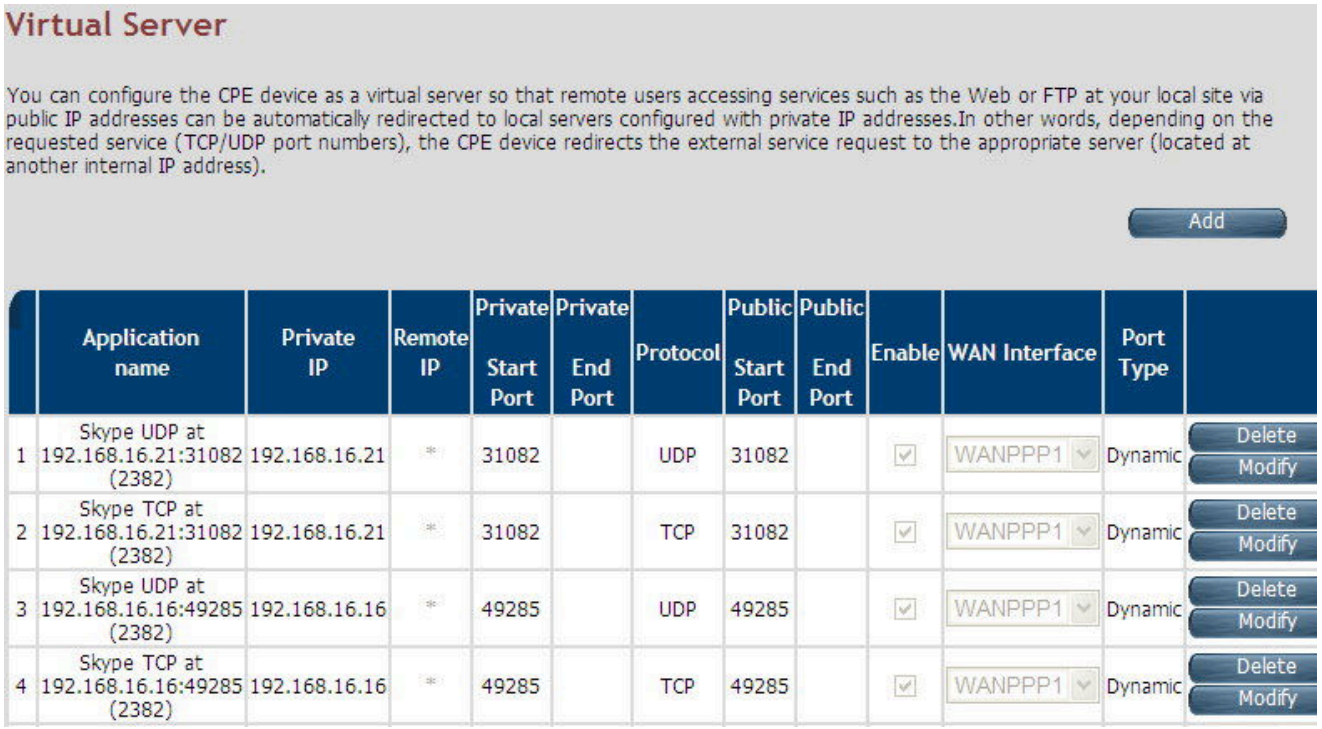



**Figure 4.10.2 Virtual Server**

The screen contains the following details:

**Fields in Virtual Server Page:**

| Field | Description |
|---|---|
| Application Name | Configured Application Name for Virtual Server rule. |
| Private IP | Private IP address of Virtual Server rule. |
| Remote IP | Remote IP address of Virtual Server rule. |
| Private Start Port | Private Port starting range. |
| Private End Port | Private Port ending range. for single port the start and end both are same |
| Protocol | Virtual Server protocol - TCP or UDP or Both i.e. TCP/UDP. |
| Public Start Port | Public Port starting range. |
| Public End Port | Public Port ending range. for single port the start and end both are same |
| Enabled | To enable the specified entry of the virtual server. |
| WAN Interface | WAN interface on which the Virtual Server rule is configured. |

- Click Add to add a Virtual Server entry.

When users click the Add button in the Virtual Server page, a screen opens with a new web page as shown in Figure 4.9.2.1

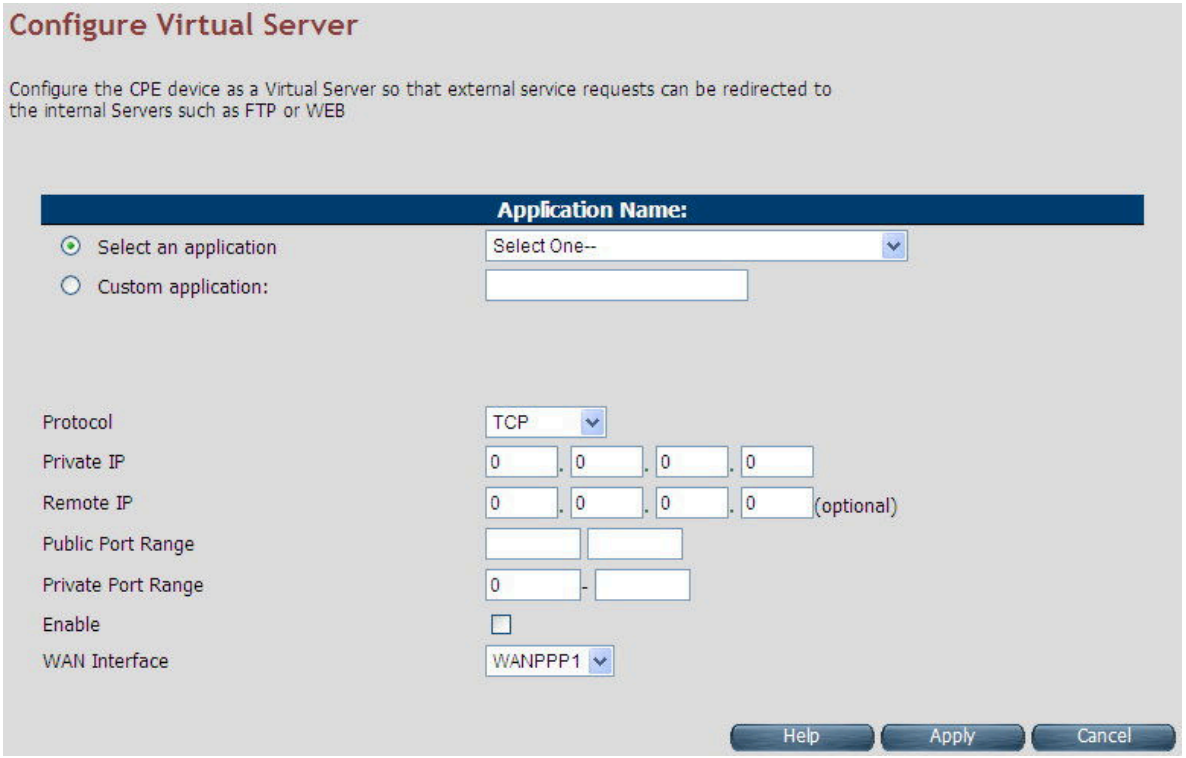



**Figure 4.10.2.1 Virtual Server Add**

The screen contains the following details:

**Fields in Virtual Server - Add:**

| Field | Description |
|---|---|
| Application Name | Specify Application name from dropdown or custom name for Virtual Server rule. |
| Protocol | Specify Virtual Server protocol - TCP or UDP or Both i.e. TCP/UDP. |
| Private IP | Specify Private IP address of Virtual Server rule. |
| Remote IP | Specify Remote IP address of Virtual Server rule. |
| Public Port Range | Specify Public Port range. |
| Private Port Range | Specify Private Port range. For single port, the start and end both are same. |
| Enabled | To enable the specified entry of the virtual server, tick on check box. |
| WAN Interface | Specify WAN interface on which the Virtual Server rule is configured. |

- Click Apply at any time during configuration to save the information that users have entered.
- Click CANCEL to exit from this page without saving the changes.

**Note:**

1. NV-600A can be set up to support up to 48 virtual servers.

### 4.10.3 Port Triggering

To configure Port Triggering, click the **Port Triggering** link (**NAT > Port Triggering**) on the left navigation bar. A screen is displayed as shown in Figure 4.9.3

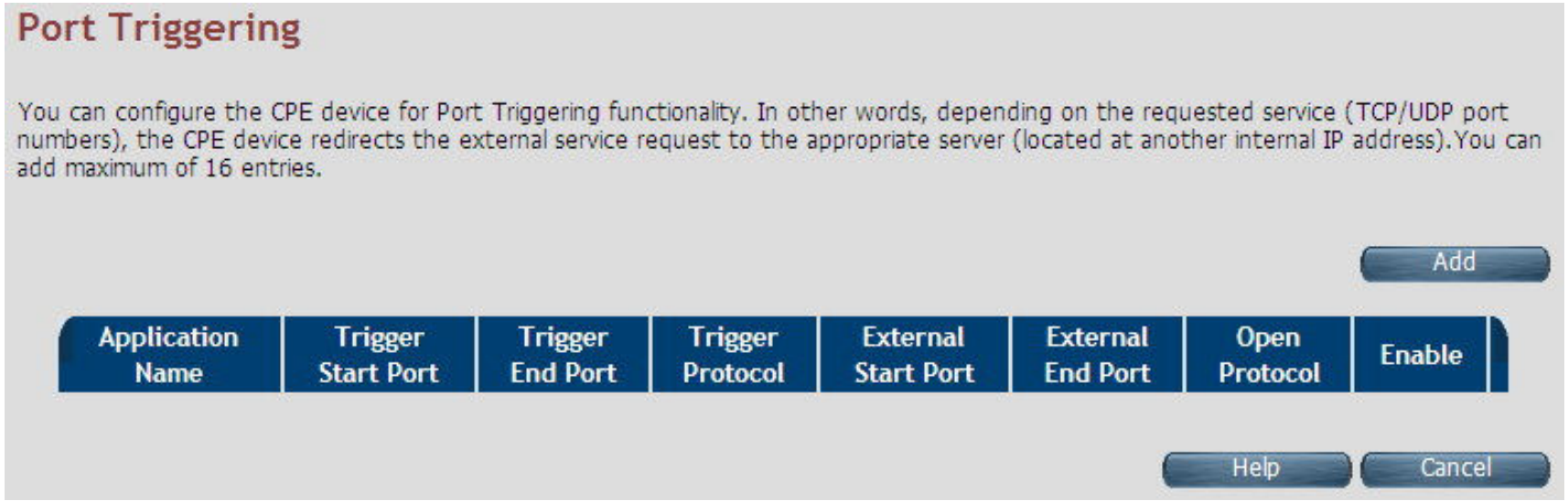



**Figure 4.10.3 Port Triggering**

The screen contains the following details:

**Fields in Port Triggering:**

| Field | Description |
|---|---|
| Application Name | Port Triggering Application Name |
| Trigger Start Port | Trigger Port start range. |
| Trigger End Port | Trigger Port End Range. In the case of one port, the end and start both are same. |
| Trigger Protocol | Trigger Protocol - TCP, UDP or TCP/UDP. |
| External Start Port | External Port Start range. |
| External End Port | External Port End Range. |
| Open Protocol | Protocol to be opened from external input - TCP, UDP or TCP/UDP. |
| Enable | Enable or Disable of Port Triggering Rule. |
| Add | Add a Port Triggering entry. |

- Click Cancel to exit from this page without saving the changes.

When users click Add button in the Port Triggering page, a screen is displayed as shown in Figure 4.9.3.1.

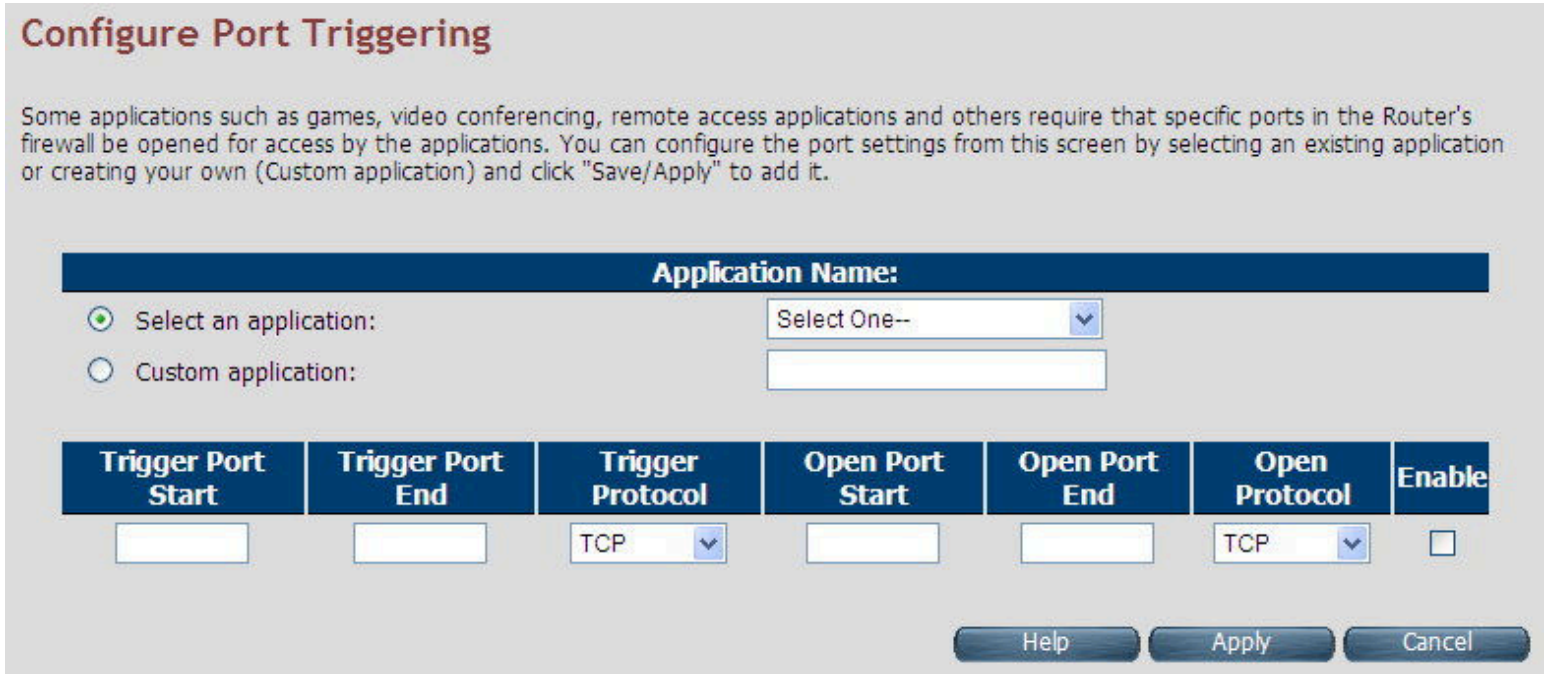



**Figure 4.10.3.1 Port Triggering Add**

The screen contains the following details:

**Fields in Port Triggering:**

| Field | Description |
|---|---|
| Application Name | Port Triggering Application Name. |
| Trigger Port Start | Trigger Port start range. |
| Trigger Port End | Trigger Port End Range. In the case of one port, the end and start both are same. |
| Trigger Protocol | Trigger Protocol - TCP, UDP or TCP/UDP. |
| Open Port Start | Open Port Start range. |
| Open Port End | Open Port End range. |
| Open Protocol | Protocol to be opened from external input - TCP, UDP or TCP/UDP. |
| Enable | Enable or Disable the Port Triggering Rule. |

- Click Apply at any time during configuration to save the information that users have entered.
- Click CANCEL to exit from this page without saving the changes.

### 4.10.4 DMZ

To configure the DMZ (Demilitarized Zone), click the **DMZ** link (**NAT > DMZ**) on the left navigation bar. Upon configuration of DMZ all traffic sent towards RG would be unconditionally forwarded to DMZ Lan Host. A screen is displayed as shown in Figure 4.9.4.

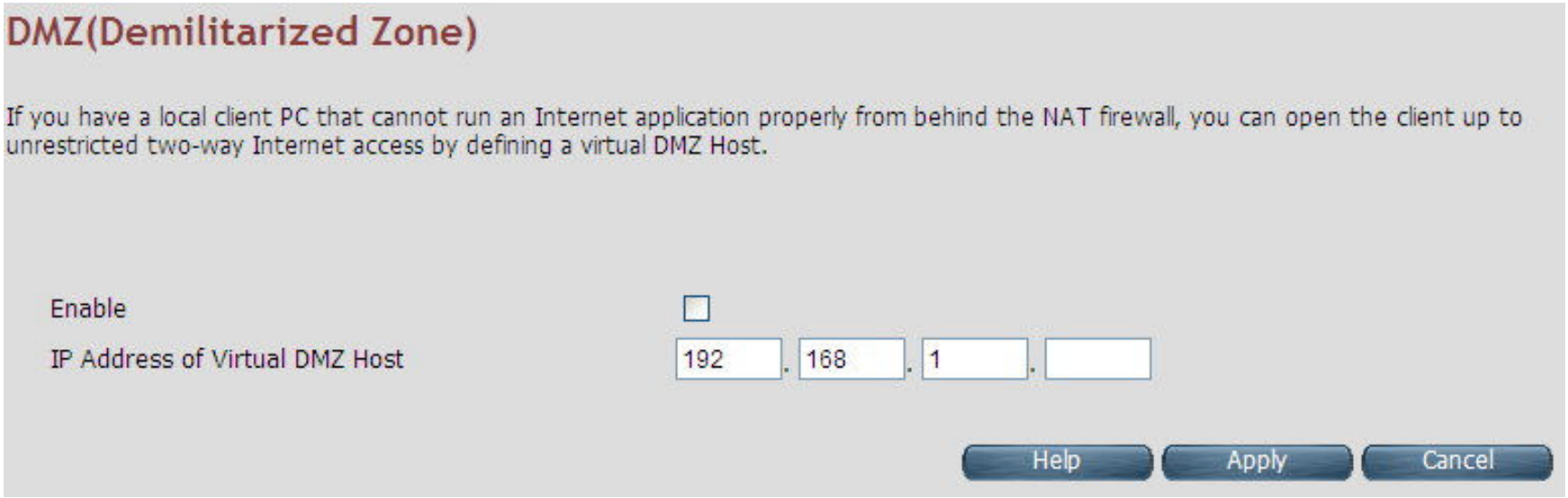



**Figure 4.10.4 DMZ (Demilitarized Zone)**

The screen contains the following details:

**Fields in DMZ:**

| Field | Description |
|---|---|
| Enable | To enable or disable the DMZ setting of NV-600A CPE. Select the check box to enable. |
| IP Address of Virtual DMZ Host | To enter the IP Address of the DMZ host. |

- Click Apply for applying the configured DMZ.
- Click Cancel to exit from this page without saving the changes.

## 4.11 QoS

Users can view QoS on the left navigation bar of the NV-600A CPE homepage. The menu below includes the sub-menus of QoS Settings, Queue Config and Class Config. The following are the options available under QoS as shown in Figure 4.11

Figure 4.11 QoS Options

### 4.11.1 QoS Settings

To configure the Quality of Service (QoS) Settings, click the **QoS Settings** link (**QoS > QoS Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.11.1

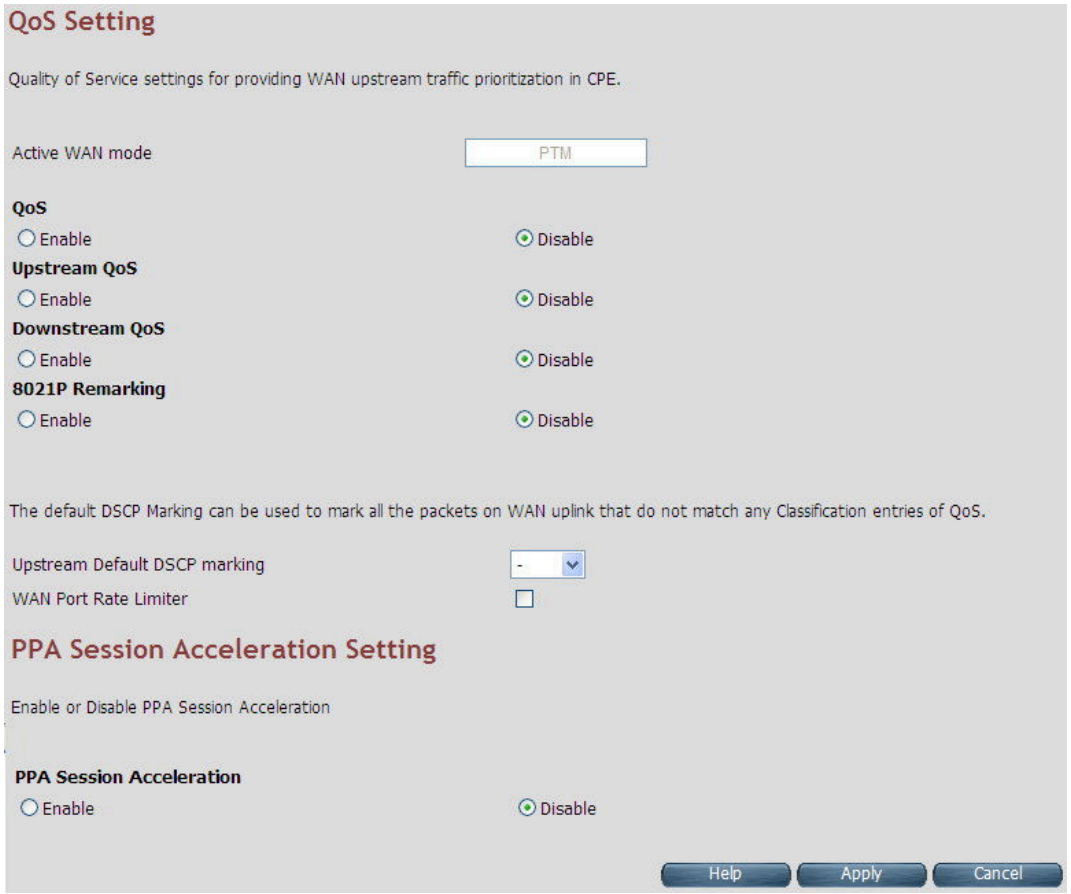


**Figure 4.11.1 QoS Settings**

The screen contains the following details:

**Fields in QoS Settings:**

| Field | Description |
|---|---|
| Active WAN mode | Informative Parameter to show current WAN mode being used in CPE. |
| QoS | |
| Enable | This option will enable the QoS feature in NV-600A system. |
| Disable | This option will disable the QoS feature in NV-600A system. |
| Upstream QoS | |
| Enable | This option will enable the upstream QoS. |
| Disable | This option will disable the upstream QoS. |
| Downstream QoS | |
| Enable | This option will enable downstream QoS. |
| Disable | This option will disable the downstream QoS. |
| 8021P Remarking | |
| Enable/Disable | This will enable/disable global 8021P Remarking. |
| Upstream Default DSCP Marking | Default DSCP Marking for non-classified packets. By default, it is "No Change" for these non-classified (default) traffic flows. |
| WAN Port Rate Limiter | Checkbox for limiting physical port rate limit on WAN upstream link. |
| PPA Session Acceleration Setting | |
| PPA Session Acceleration | To enable/disable the session acceleration feature. |

- Click Apply for applying the QoS setting changes into system.
- Click CANCEL to exit from this page without saving the changes.

## 4.11.2 Queue Config

To configure the Queue Config, click the **Queue Config** link (**QoS > Queue Config**) on the left navigation bar. A screen is displayed as shown in Figure 4.11.2

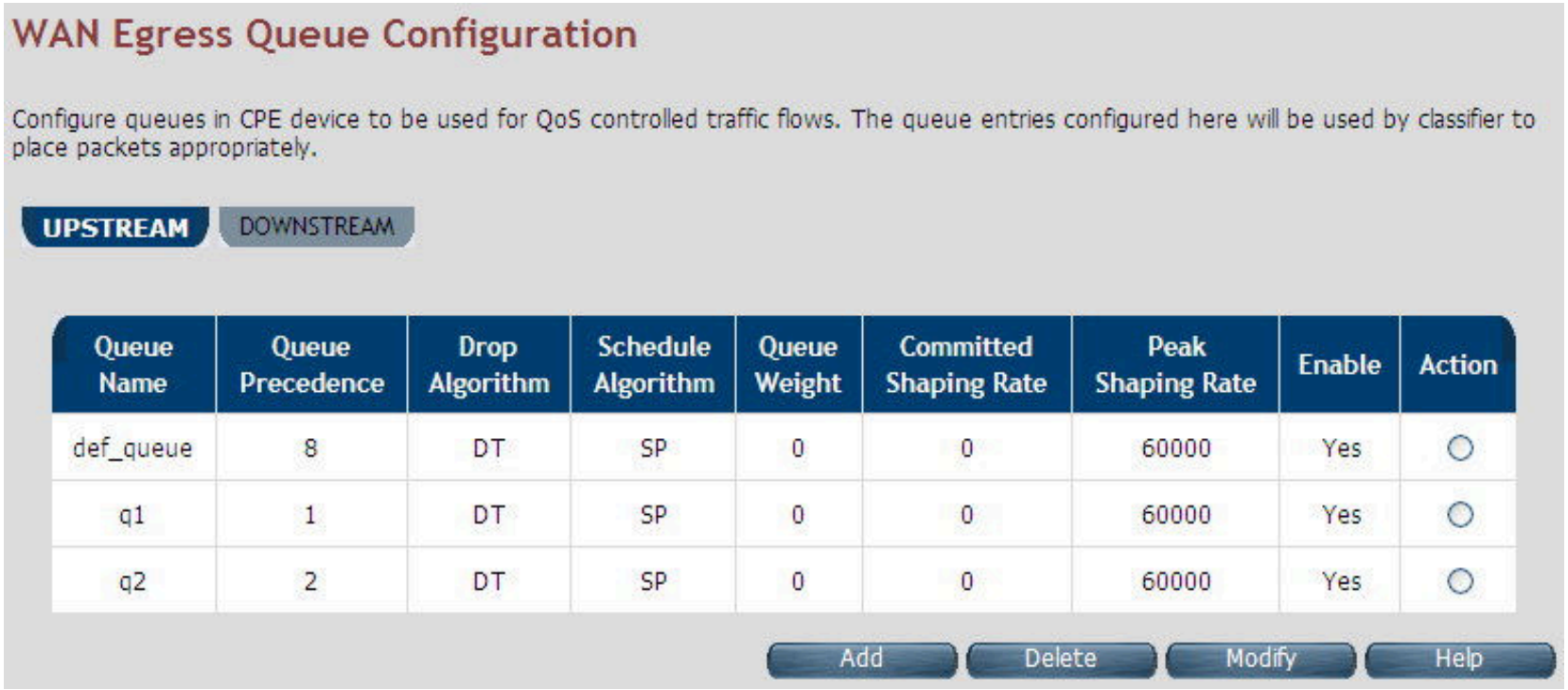



**Figure 4.11.2 Queue Config**

The screen contains the following details:

**Fields in Queue Config - Upstream:**

| Field | Description |
|---|---|
| Upstream/Downstream | Selection tab for upstream/downstream Queue configuration. |
| Queue Name | This is the name of the queue configured in system. |
| Queue Precedence | Precedence of Queue. (Lower values denote higher priority). |
| Drop Algorithm | This specifies the nature of drop in case of congestion. The supported drop algorithms are DT (Drop Tail) or RED (Random Early Discard). |
| Scheduler Algorithm | This is the queue scheduling algorithm used for the queue. The support queue Scheduling algorithms are SP (Strict Priority) or WFQ (Weighted Fair Queuing). |
| Queue Weight | Valid for Weighted Queuing mode of scheduled queues. |
| Committed Shaping Rate | Committed or Guaranteed Shaping Rate in Kbps or Percentage. |
| Peak Shaping Rate | Peak or Maximum shaping rate (ceiling) in Kbps or Percentage. |
| Enable | This provides the status of queue entry. (Enabled or disabled). |
| Action | Selection button for applying Modify or Delete action on selected queue. |
| Add | This button is used to add a new queue. |
| Delete | This button is used to delete the selected queue entry. |
| Modify | This button is used to modify the selected queue entry. |

When users click Add button in the Port Triggering page, a screen is displayed as shown in Figure 4.10.2.1.

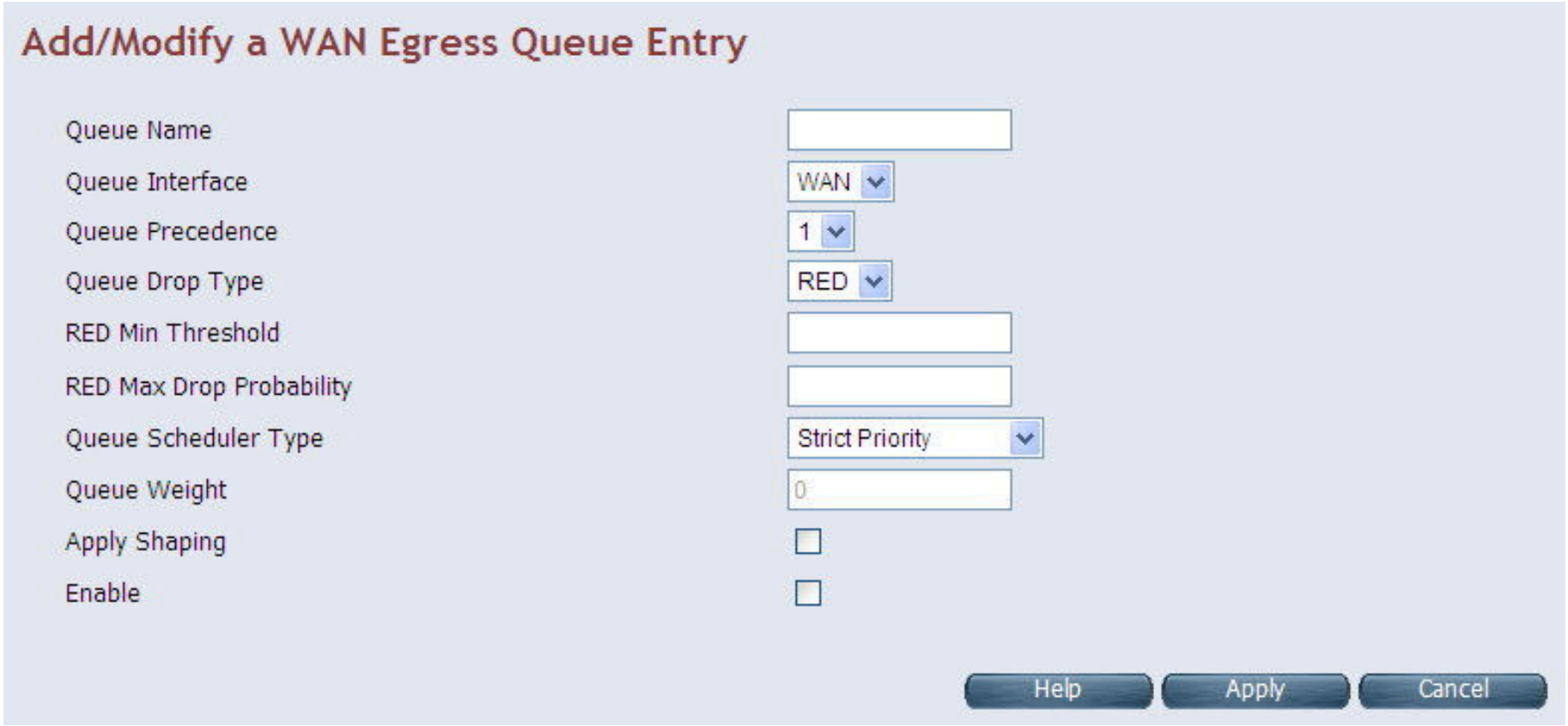



**Figure 4.11.2.1 Add/Modify a Queue Entry**

The screen contains the following details:

**Fields in Add/Modify a Queue Entry:**

| Field | Description |
|---|---|
| Queue Name | Name or Identifier of Queue. |
| Queue Interface | This is the Egress interface to which the queue is attached. For xRX200 platform the dropdown for LAN egress would also appear. This indicates downstream QoS (WAN to Ethernet LAN) is supported by xRX200 platforms. |
| Queue Precedence | Precedence of Queue. (Lower values denote higher priority). |
| Queue Drop Type | Drop Algorithm of Queue (DT [Drop Tail] or RED [Random Early Discard]). |
| RED Min Threshold | RED Threshold Value, applicable for RED Drop algo. |
| RED Max Drop Probability | RED Maximum Drop Probability in Percentage (drop_p). Value should be <100. |
| Queue Scheduler Type | Queue scheduling Algorithm. (SP or WFQ) |
| Queue Weight | Valid for Weighted Queuing mode of scheduled queues. |
| Apply Shaping | To apply shaping on queue. |
| Enable | Enable or Disable of Queue. |

- Click Apply for applying the changes.
- Click CANCEL to exit from this page without saving the changes.

### 4.11.3 Class Config

To classify the upstream traffic. Click the **Class Config** link (**QoS > Class Config**) on the left navigation bar. A screen is displayed as shown in Figure 4.11.3

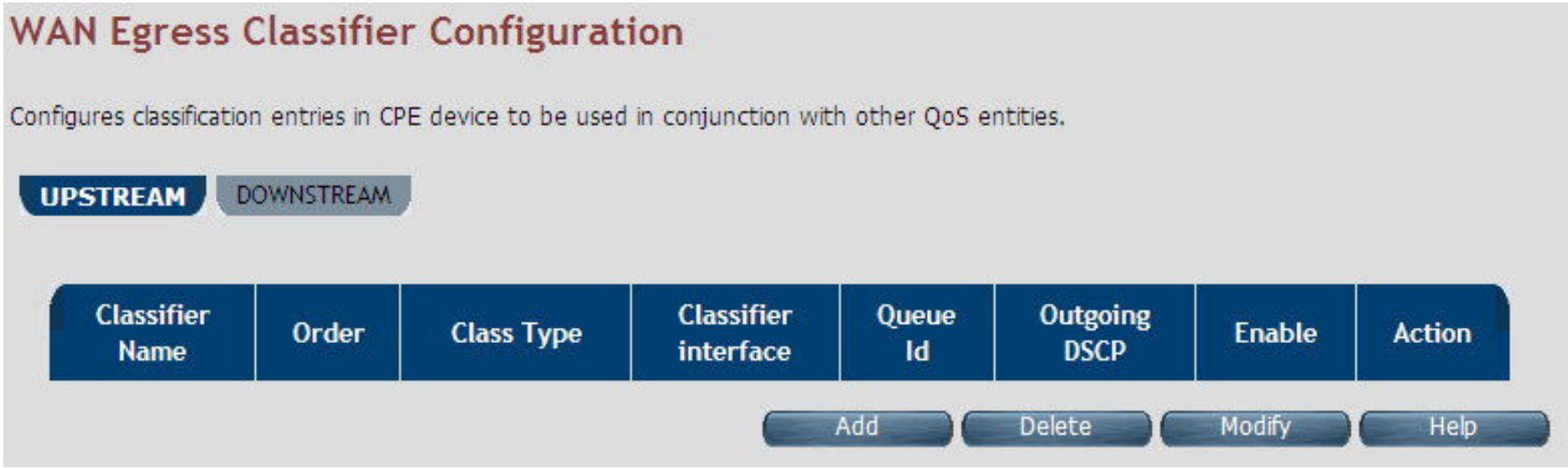



**Figure 4.11.3 Class Config**

The screen contains the following details:

**Fields in Class Config:**

| Field | Description |
|---|---|
| Upstream/Downstream | Selection tab for upstream/downstream Classifier configuration. |
| Classifier Name | This is the name or identifier of the classifier entry. |
| Order | This shows the order of the classification entry. |
| Class Type | Type of Classifier - Multi Field Classifier (MFC) or DSCP or 802.1p based. |
| Classifier Interface | This is a Packet Input Source for classified flow. |
| Queue Id | Queue Id for classified flow. |
| Outgoing DSCP | This is the DSCP mark for next hop. |
| Enable | Status of Classification entry. |
| Action | Selection option for deleting or modifying action on chosen classifier. |
| Add | This is the button used to add a classification entry to categorize traffic flow. |
| Delete | Delete button for deleting selected queue. |
| Modify | Modify button for modifying chosen queue. |

When users click Add or Modify in the Classifier Config page, a screen is displayed as shown in Figure 4.10.3.1

**Figure 4.11.3.1 Add/Modify a Classifier Rule (DSCP Based)**

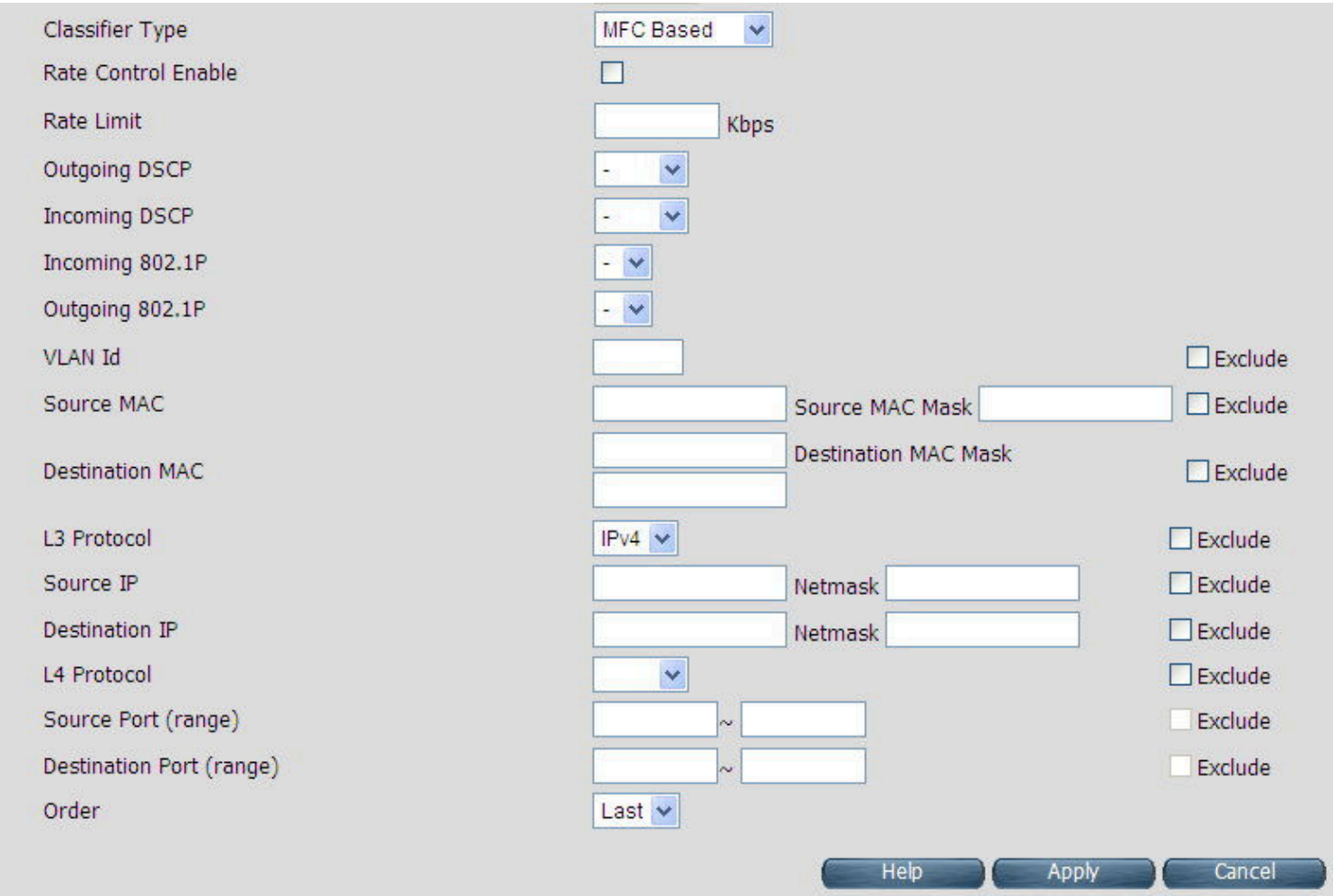



**Figure 4.11.3.1 Add/Modify a Classifier Rule (MFC Based)**

The screen contains the following details:

**Fields in Add/Modify a Classifier Rule:**

| Field | Description |
|---|---|
| Classifier Name | This is the name of Classifier. This is a Unique identifier for an instance of classifier rule. |
| Enable | This is used to enable or disable the QoS Classifier entry. |
| Classifier Interface | This is used to select upstream/downstream classifier. |
| Disable acceleration | This is used to disable acceleration for this classifier. |
| Queue Name | This is the Queue Identifier to be associated with this classifier rule. This is presented in dropdown for associating with this classifier entry. |
| Ingress Interface | Packet Input Source for classified flow. |
| Classifier Type | Type of Classifier - Multi Field Classifier (MFC) or DSCP or 802.1p based. |
| Rate Control Enable | Configuration of classifier-based rate control. |
| Rate Limit | Rate limit per classifier. |
| Outgoing DSCP | Outgoing DSCP Marking - if any to be done on this classifier rule. |
| Incoming DSCP | Incoming DSCP for identifying the flow. |
| Incoming 802.1P | Incoming 802.1P for identifying the flow. |
| Outgoing 802.1P | Outgoing 802.1P Marking - if any to be done on this classifier rule. |
| VLAN Id | Incoming VLAN id. |
| Source MAC | Source MAC classification. |
| Source MAC Mask | Mask bits for Source MAC. |

| | |
|---|---|
| Destination MAC | Destination MAC classification. |
| Destination MAC Mask | Mask bits for Destination MAC. |
| L3 Protocol | Drop down to select IPv4/IPv6. |
| Source IP | Source IPv4/IPv6 classification. |
| Netmask | Mask bits for Source IP. |
| Destination IP | Destination IPv4/IPv6 classification. |
| Netmask | Mask bits for Source IP. |
| L4 Protocol | Dropdown to select L4 protocol like UDP/TCP/ICMP etc. |
| Source Port Range | Start and end source port range. |
| Destination Port Range | Start and end destination port range. |
| Order | Classification order. |

- Click Apply for applying the changes.
- Click CANCEL to exit from this page without saving the changes.

## 4.12 Multicast

Users can view Multicast on the left navigation bar of the NV-600A CPE homepage. The menu below includes the sub-menus of **Proxy Settings**, **Snooping Settings** and **Advanced Settings**. The following are the options available under Multicast as shown in Figure 4.12

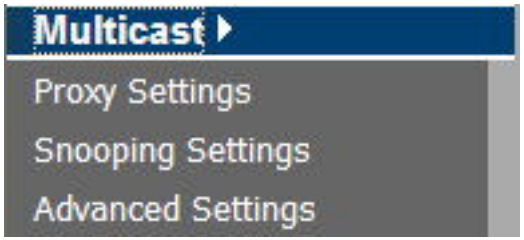



**Figure 4.12 Multicast Options**

### 4.12.1 Proxy Settings

To configure the Multicast proxy settings in CPE, click the **Proxy Settings** link (**Multicast > Proxy Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.12.1

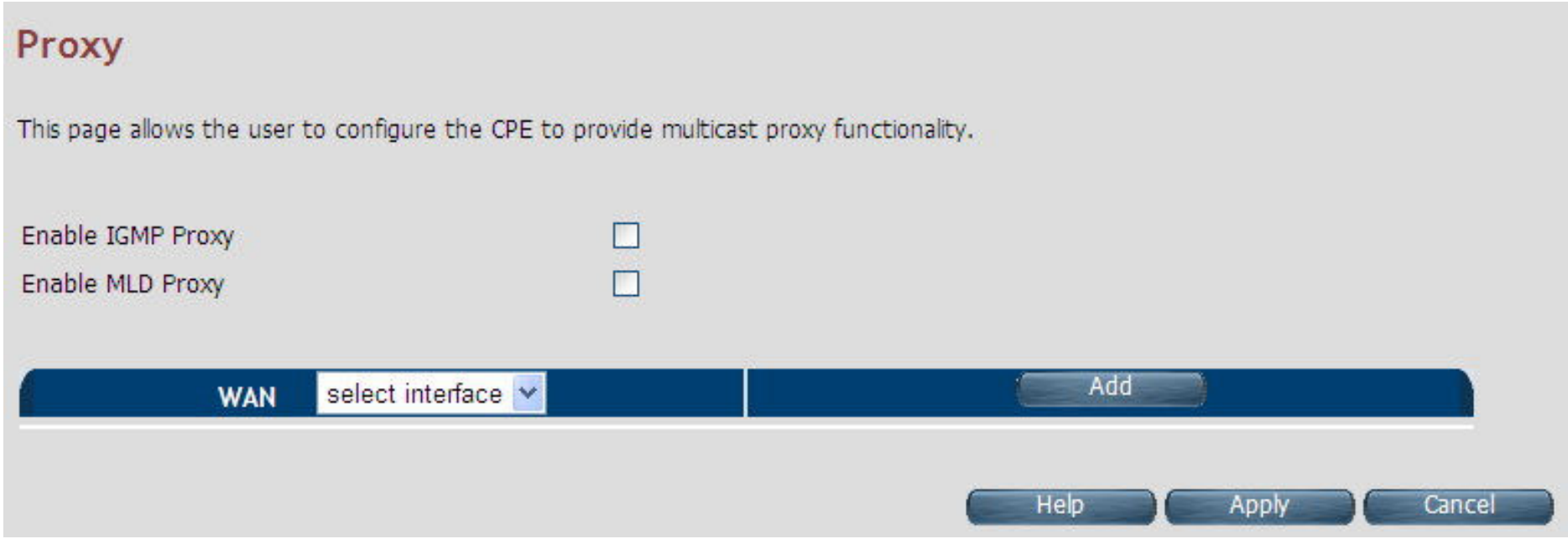



**Figure 4.12.1 IGMP Proxy**

The screen contains the following details:

**Fields in IGMP Proxy:**

| Field | Description |
|---|---|
| Enable IGMP Proxy | Enable or disable the IGMPv3/IGMPv2 Proxy functionality. |
| Enable MLD Proxy | Enable or disable the MLDv2 (IPv6) Proxy functionality. |
| WAN | Select one of the WAN interfaces from the drop-down menu on which Multicast Proxy functionality to be enabled. |
| Add | Add an IGMP proxy configuration. |

- Click Apply at any time during configuration to save the information that users have entered.
- Click CANCEL to exit from this page without saving the changes.

### 4.12.2 Snooping Settings

To configure the Multicast Snooping settings, click the **Snooping Settings** link (**Multicast > Snooping Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.11.2

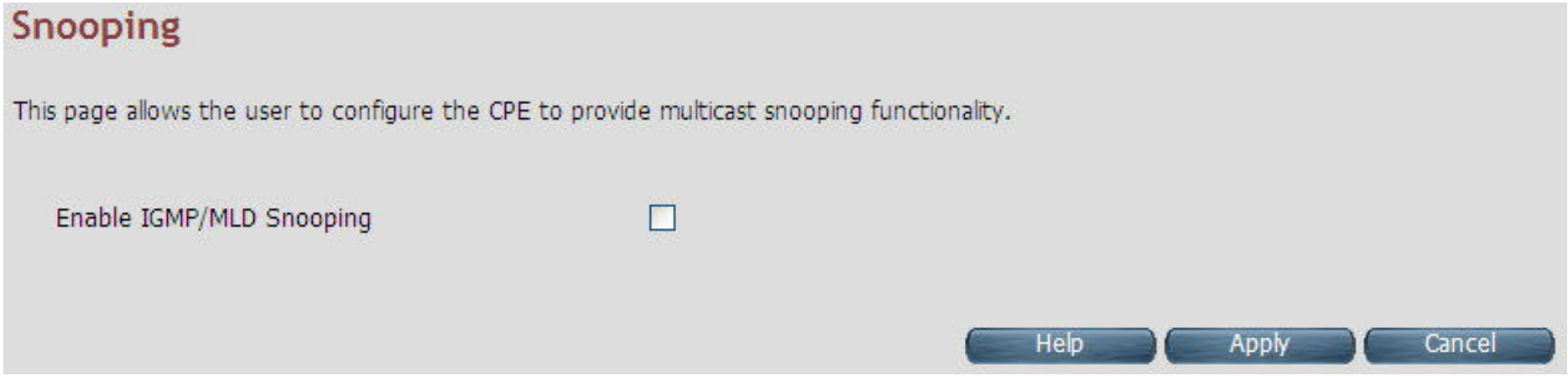



**Figure 4.12.2 IGMP Snooping**

The screen contains the following details:

**Fields in Fields in Snooping:**

| Field | Description |
|---|---|
| Enable IGMP Snooping | Enable or Disable the IGMPv3/IGMPv2 Snooping functionality. |
| Enable MLD Snooping | Enable or Disable the MLDv2 (IPv6) Snooping functionality. |

- Click Apply at any time during configuration to save the information that users have entered.
- Click CANCEL to exit from this page without saving the changes.

### 4.12.3 Advanced Settings

To configure the advanced settings on Multicast features, click the **Advanced Settings** link (**Multicast > Advanced Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.11.3

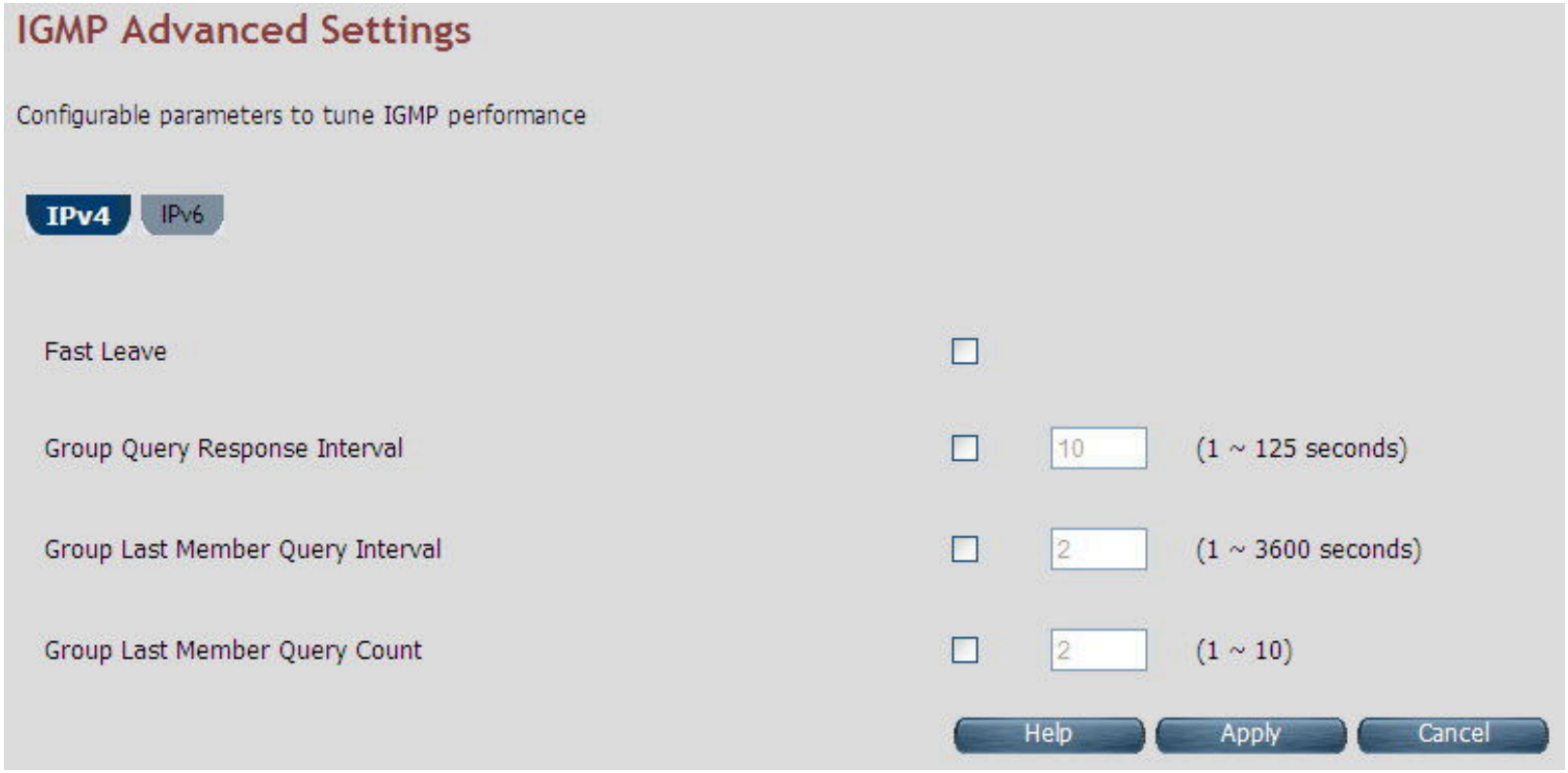



**Figure 4.12.3 Multicast Advanced Settings**

The screen contains the following details:

**Fields in Multicast Advanced Settings:**

| Field | Description |
|---|---|
| IPv4/IPv6 | Choose the proper tab to configure either for IPv4 or IPv6. |
| Fast Leave | To enable or disable Fast-Leave support in IGMPv3/IGMPv2. The fast leave is not to wait till group membership timers on multicast routers have expired, but quickly send a group-specific query and if not, reports were received, remove the group entry. |
| Group Query Interval | Specify Group Query Interval in range of 1-3600 seconds. |
| Group Query Response Interval | Specify Group Query Response Interval in range of 1-3600 seconds. |
| Group Last Member Query Interval | Group Last Member Query Interval in range of 1-3600 seconds. |
| Group Last Member Query Count | Group Last Member Query Count in range of 1 to 10. |

**Tip:**

**Similar settings are available for MLDv2 under IPv6 tab.**

## 4.13 IPsec

When users click IPsec on the left navigation bar of the NV-600A CPE homepage. The menu below includes the sub-menus of Tunnel Mode. The following option Tunnel Mode is available under IPsec as shown in Figure 4.13

Figure 4.13 IPsec Option

### 4.13.1 Tunnel Mode

When users click the **Tunnel Mode** link (**IPsec > Tunnel Mode**) on the left navigation bar, a screen is displayed as shown in Figure 4.13.1

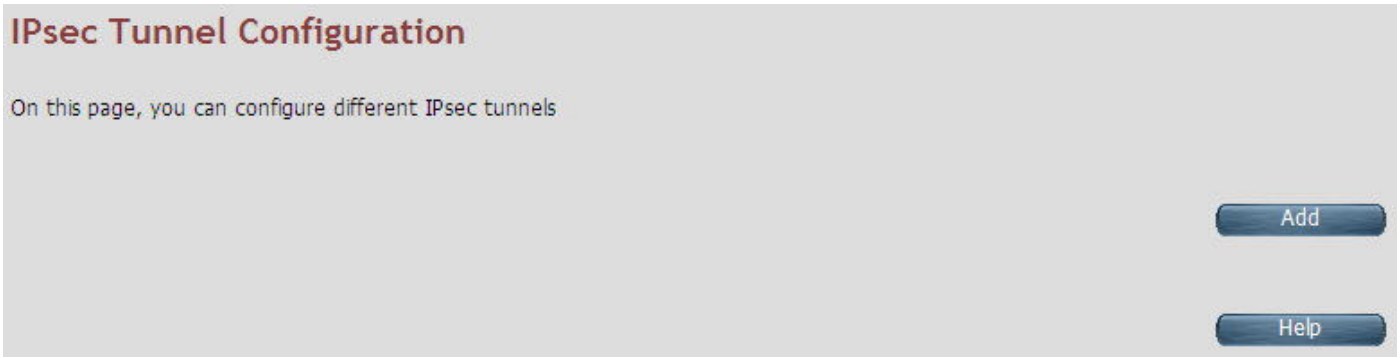



**Figure 4.13.1 IPsec Tunnel Configuration**

When users click Add button in the IPsec Tunnel Configuration page, a screen is displayed as shown in Figure 4.12.1.1

**Figure 4.13.1.1 Add IPSec Tunnel Mode Configuration**

The screen contains the following details:

**Fields in Add IPSec Add Configuration:**

| Field | Description |
|---|---|
| Tunnel Name | IPsec Tunnel name |
| AUTH_METHOD | This is the authentication method. |
| PSK Secret | Shared secret string used for tunnel authentication. |
| IKE Mode | IKE v1 or v2 algorithm |
| WAN Interface | WAN on which tunnel to be created., |
| My Subnet | LAN host connected to CPE. |
| Peer Address | Remote tunnel end point address. |
| Peer Subnet | Remote host IP address. |
| Enable | Enable or disable of tunnel. |
| IKE Cipher | Cipher algorithm to be selected from dropdown. |
| IKE Hash | Hash algorithm to be selected from dropdown. |
| IKE DH Group | DH group algorithm to be selected from dropdown. |
| IKE PRF | PRF algorithm to be selected from dropdown. |
| ESP Cipher | ESP Cipher algorithm to be selected from dropdown. |
| ESP Hash | ESP Hash algorithm to be selected from dropdown. |
| Key Lifetime | Key Lifetime in seconds. |
| Retry | Number of retries in case key exchange fails. |

- Click Apply for applying the configured IPsec tunnel.
- Click CANCEL to exit from this page without saving the changes

## 4.14 IPv6

When users click the IPv6 link on the left navigation bar of the NV-600A CPE homepage. The menu below includes the sub-menus of **IPv6 Setting**, **6RD Configuration** and **DS-Lite Configuration**. The following options are available as shown in Figure 4.13

**Figure 4.14 IPV6 Options**

### 4.14.1 IPv6 Setting

To enable or disable IPv6 functionality in CPE, click the **IPv6 Setting** link on the left navigation bar. A screen is displayed as shown in Figure 4.14.1. By default, IPv6 is not enabled.

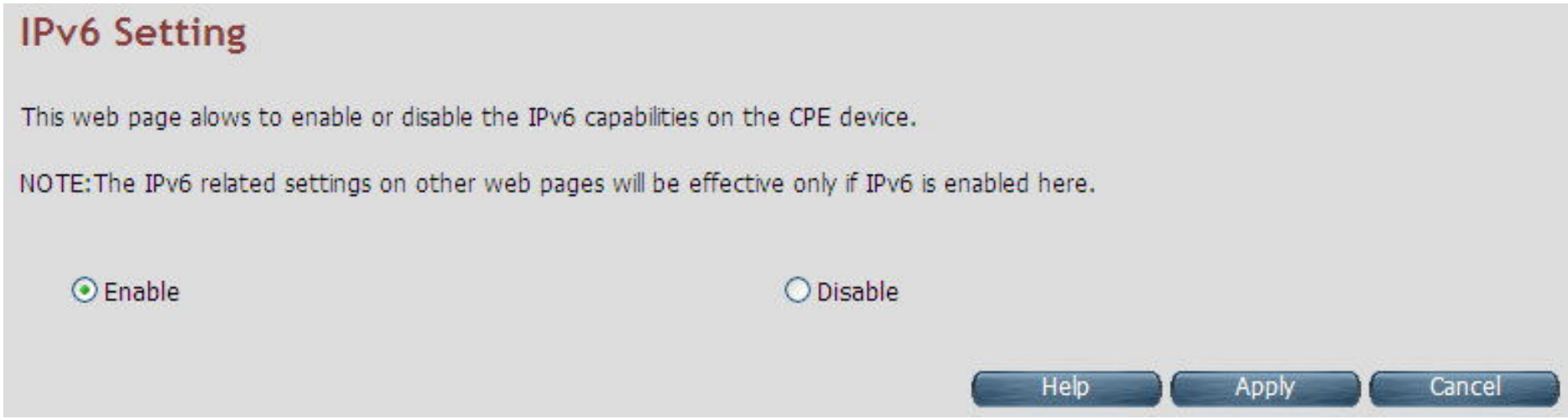



**Figure 4.14.1 IPv6 Setting**

The system wide IPv6 feature can be enabled or disabled through this web page. Select appropriate control and click Apply button for making the change effective in CPE. All other IPv6 features in CPE would be in effect, only when this global IPv6 is enabled in CPE.

**Fields in IPv6 Setting:**

| IPv6 Setting | |
|---|---|
| Enable | Enable IPv6 functionality in CPE. |
| Disable | Disable IPv6 functionality in CPE. |

- Click Apply at any time during configuration to save the information that users have entered.
- Click CANCEL to exit from this page without saving the changes.

### 4.14.2 6RD Configuration

The NV-600A supports IPv6 transition mechanism defined in 6RD (RFC 5569). To configure the 6RD configuration, click the **6RD configuration** link (**IPv6 > 6RD Configuration**) on the left navigation bar. A screen is displayed as shown in Figure 4.13.2

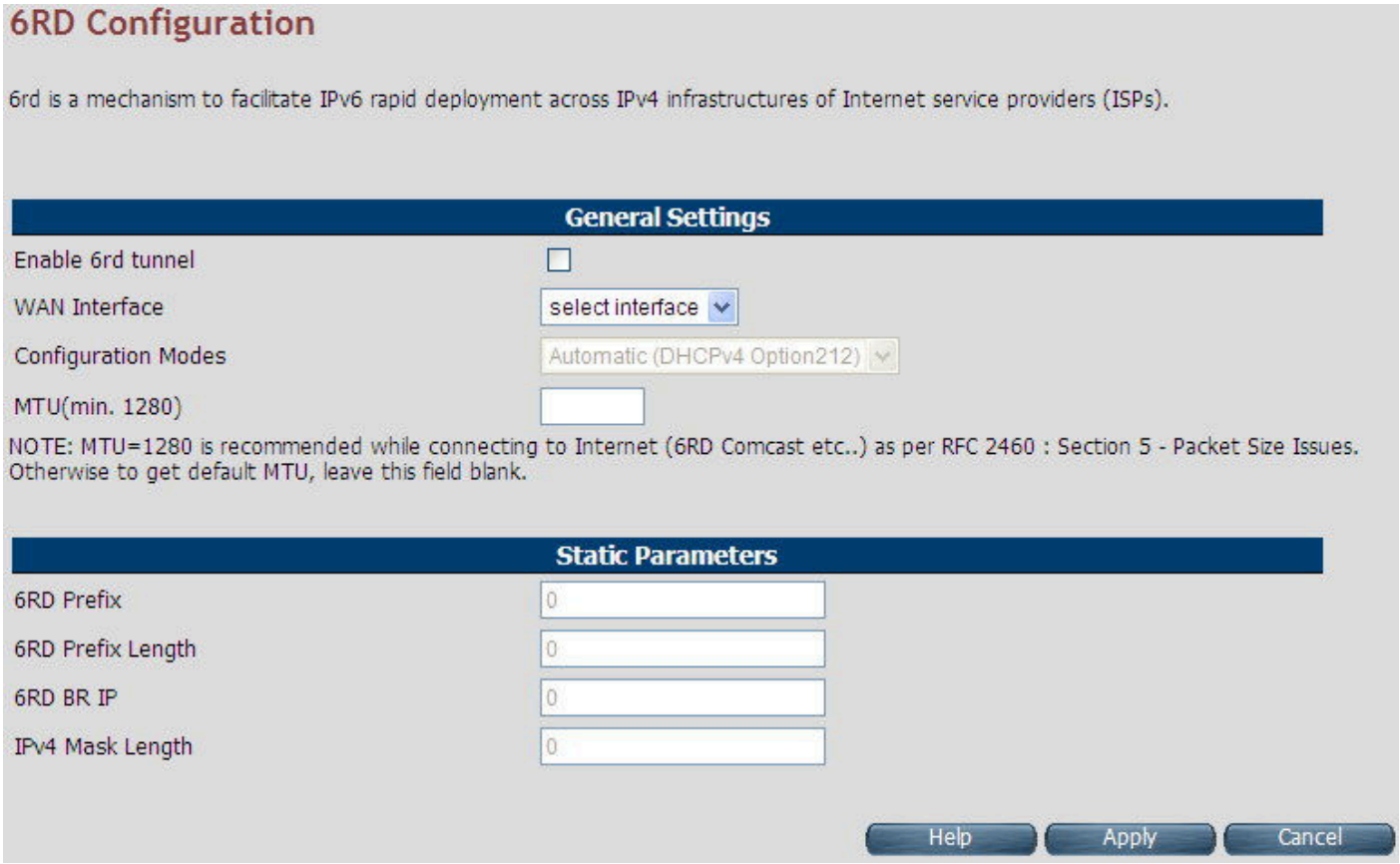



**Figure 4.14.2 6RD Configuration**

The screen contains the following details:

**Fields in 6RD Configuration:**

| Field | Description |
|---|---|
| General Settings | |
| Enable 6RD tunnel | To enable or disable 6RD functionality in CPE. |
| WAN Interface | Select WAN interface form dropdown on which 6RD tunnel to be created. |
| Configuration Modes | Select dynamic 6RD tunnel through DHCP option or static tunnel configuration. |
| MTU (min. 1280) | Optionally, users can specify Maximum Transfer Unit size for 6RD tunnel. |
| Static Parameters | |
| 6RD Prefix | 6RD Prefix string. |
| 6RD Prefix Length | 6RD Prefix Length. |
| 6RD BR IP | 6RD Broder Relay's IPv4 address. |
| IPV4 Mask Length | IPv4 address Mask Length. |

- Click Apply at any time during configuration to save the information that users have entered.
- Click CANCEL to exit from this page without saving the changes.

### 4.14.3 DS-Lite Configuration

The NV-600A supports DS-Lite configuration mechanism. To configure the Ds-Lite configuration, click the **DS-Lite** configuration link (**IPv6 > DS-Lite Configuration**) on the left navigation bar. A screen is displayed as shown in Figure 4.13.3

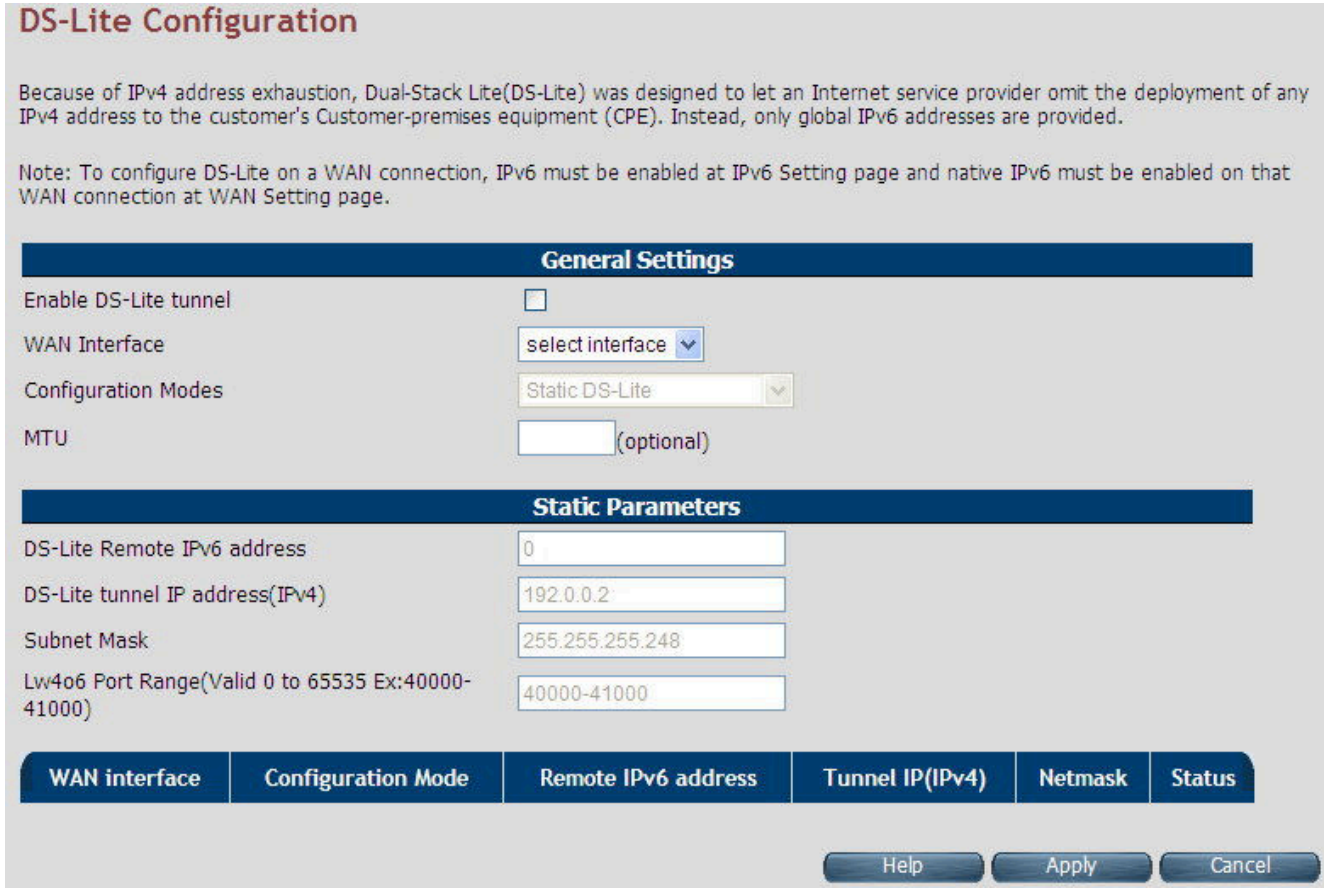


**Figure 4.14.3 DS-Lite Configuration**

The screen contains the following details:

**Fields in DS-Lite Configuration:**

| Field | Description |
|---|---|
| General Settings | |
| Enable DS-Lite tunnel | To enable/disable DS-Lite functionality in CPE. |
| WAN Interface | Select WAN interface from dropdown on which DS-Lite tunnel has to be created. |
| Configuration Modes | Modes to configure DS-Lite tunnel on a WAN interface. Currently, Static, Dynamic (DHCPv6 option-64) and Lw4o6 DS-Lite modes are supported. |
| MTU | Optionally, it is used to specify Maximum Transfer Unit size for DS-Lite tunnel. |
| Static Parameters | |
| DS-Lite Remote IPv6 address | IPv6 address of the remote tunnel endpoint. (When users select Dynamic mode, this field is disabled.) |
| DS-Lite tunnel IP address (IPv4) | IPv4 address of the remote tunnel endpoint. |
| Subnet Mask | IPv4 Address subnet mask. |
| Lw4o6 Port Range | This is the port range for Source NAT. Applicable only for Lw4o6 type. |

- Click Apply at any time during configuration to save the information that users have entered.

- Click CANCEL to exit from this page without saving the changes.

## 4.15 Diagnostics

When users click Diagnostics link on the left navigation bar of the NV-600A CPE homepage. The menu below includes the sub-menus of Diagnostic Test Suite. The following options are available under Diagnostics as shown in Figure 4.15

**Figure 4.15 Diagnostics Options**

### 4.15.1 Diagnostic Test Suite

To configure the Diagnostic Test Suite settings, click the **Diagnostic Test Suite** link (**Diagnostics > Diagnostic Test Suite**) on the left navigation bar. A screen is displayed as shown in Figure 4.15.1

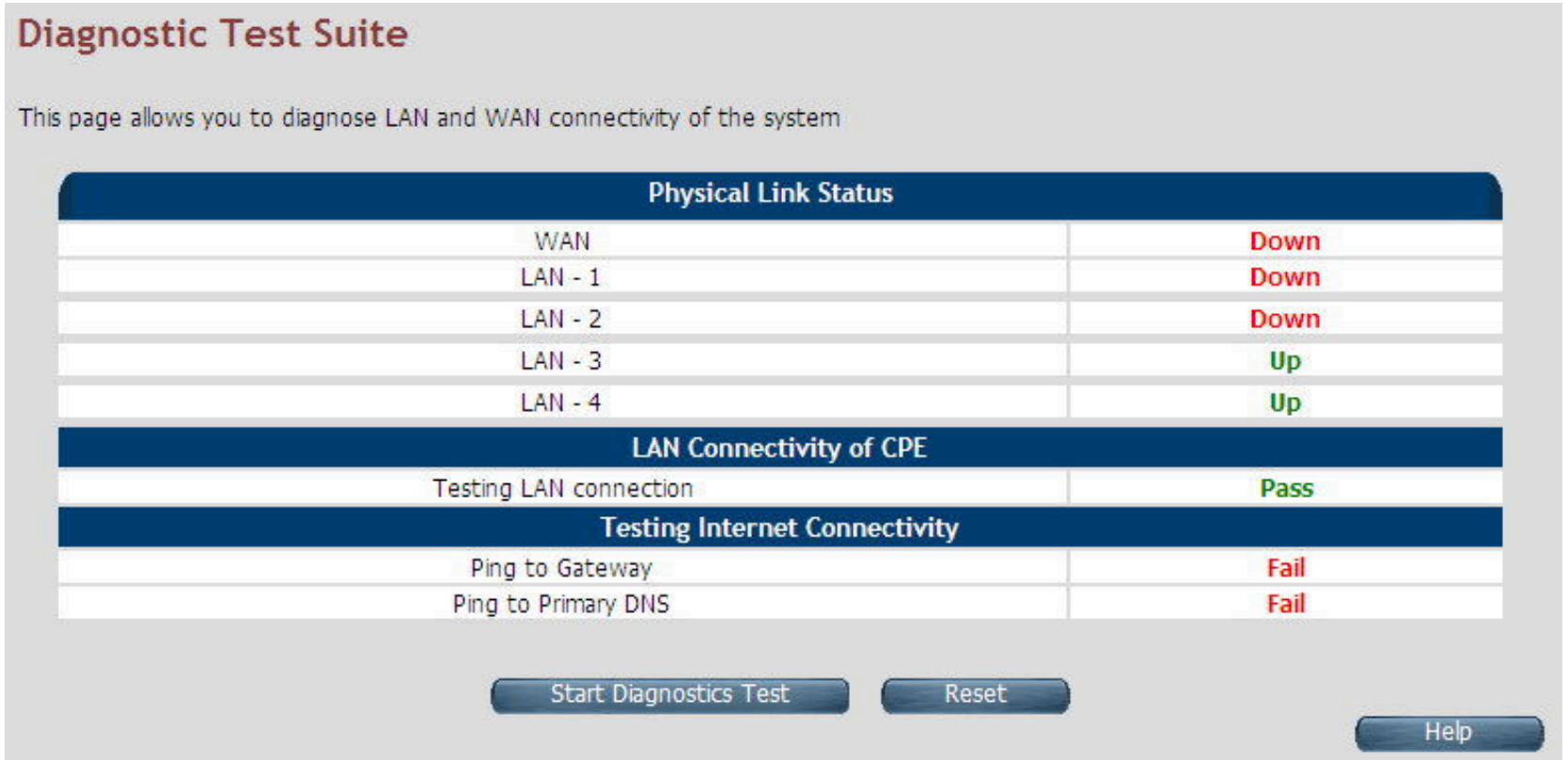



Figure 4.15.1 Diagnostic Test Suite

The screen contains the following details:

**Fields in Diagnostic Test Suite:**

| Field | Description |
|---|---|
| Connection Status | |
| WAN | DSL WAN State |
| Wireless | Wireless State |
| ENET LAN-0 | Ethernet LAN Port-0 state. |
| ENET LAN-1 | Ethernet LAN Port-1 state |
| ENET LAN-2 | Ethernet LAN Port-2 state |
| ENET LAN-3 | Ethernet LAN Port-3 state |
| LAN Connectivity of CPE | |
| Testing LAN Connection | Status of LAN connection Diagnostics |
| Testing xDSL Connection | |
| Testing xDSL Synchronization | xDSL Synchronization Test. |
| Testing ATM Connection on default WAN ATM PVC | |
| Testing ATM OAM F5 End to End Ping | F5 end to end ping test. |
| Testing Internet Connectivity | |
| Ping to Gateway | Ping to Gateway IP address. |
| Ping to Primary DNS | Ping to Primary DNS IP address. |
| Start Diagnostics Test | Initiates the Diagnostics test. |
| Reset | Resets the diagnostics output. |

**Note: Please wait a few seconds to show the test result.**

## 4.16 SNMP

Users can view SNMP on the left navigation bar of the NV-600A CPE homepage. The menu below includes the sub-menus of **SNMP Settings** and **SNMPv3 Settings**. The following options are available under Diagnostics as shown in Figure 4.16

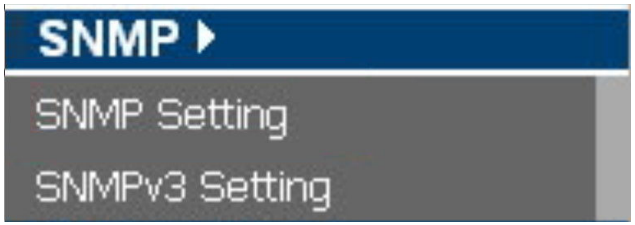



**Figure 4.16**

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

## 4.16.1 SNMP Options

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

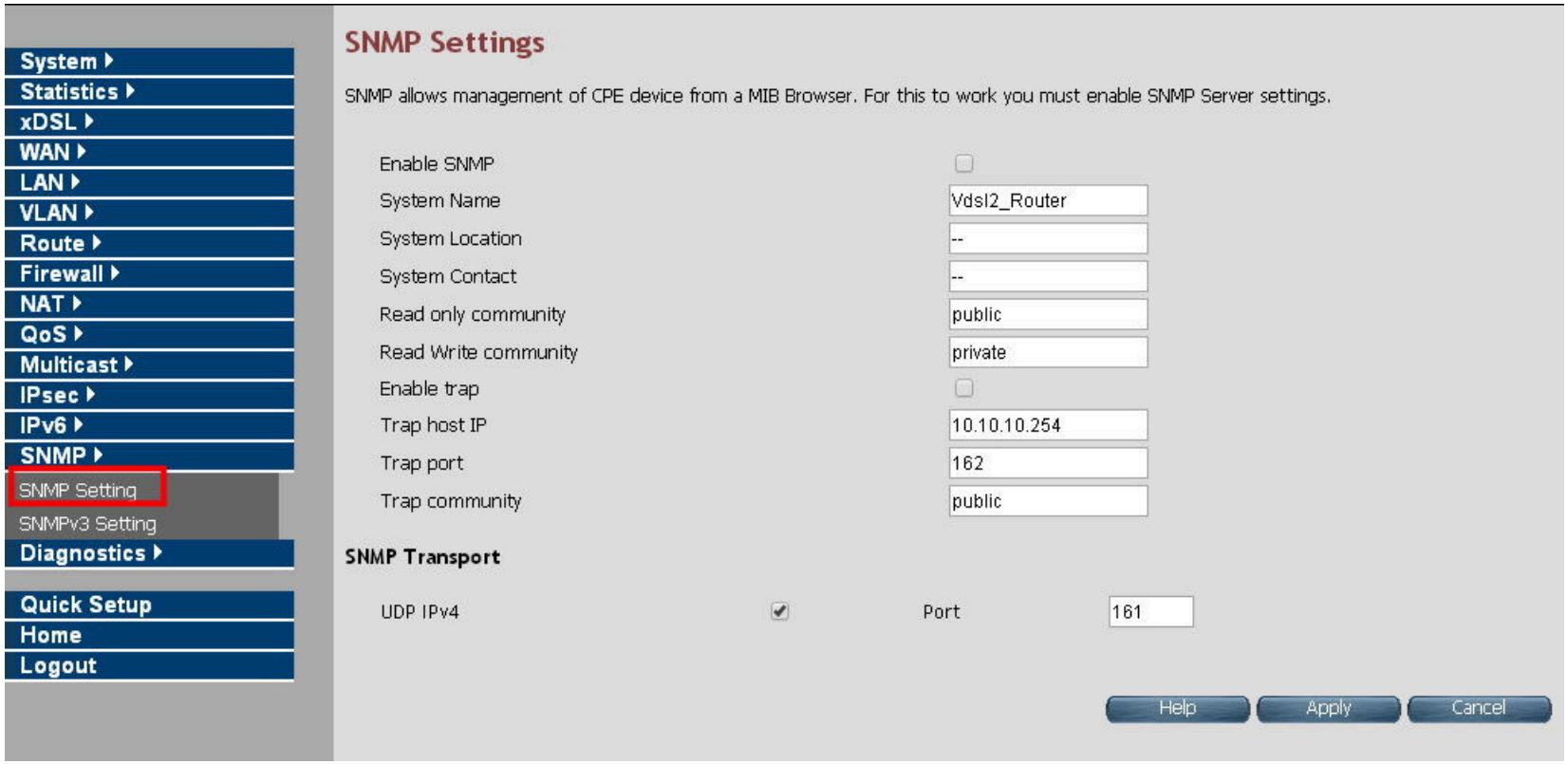



Fig. 4.16.1 SNMP Settings

The screen contains the following details:

**Fields in SNMP Setting:**

| IPv6 Setting | |
|---|---|
| **Enable SNMP** | Enable/Disable SNMP Function |
| **System Name** | Enter a name to be used for the router |
| **System Location** | Enter the location of the router |
| **System Contact** | Enter the name of a person or organization |
| **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. |
| **Enable Trap** | To enable or disable Trap Setting. Select the check box to Enable or Disable the Trap function of NV-600A. |
| **Trap Host IP** | Create a trap manager by entering the IP address. |
| **Trap port** | Specifies the trap port. Default trap port is "162". |
| **Trap community** | Create a trap manager by entering a community string. |
| **SNMP Transport** | Specifies the trap port. Default trap port is "161". |

- Click **Apply** at any time during configuration to save the information that users have entered.
- Click **Cancel** to exit from this page without saving the changes.

## 4.16.2 SNMPv3 Settings

The CPE decive provides Security to SNMP access in SNMPv3. Users can configure the users to have Authorized access to SNMP data. When users click **Add** inside the **SNMPv3 Settings,** a screen is displayed as shown in Figure 4.16.2

**Fig. 4.16.2 SNMPv3 Settings**

## 4.16.3 Add v3 user

Fig. 4.16.3 SNMP Setting

The screen contains the following details:

**Fields in Add a V3 user Setting:**

| IPv6 Setting | |
|---|---|
| **User Access** | specify the user Access. |
| **User Name** | specify the username. |
| **Security Level** | specify the Security level. |
| **Authorization Protocol** | specify the authorization type. (MD5/DES) |
| **Auth Password** | specify the authorization key. (8~15 chars) |
| **Privacy Protocol** | specify the privacy type. (MD5/DES) |
| **Privacy Password** | specify the encrypt key. (8~15 chars) |

- Click Apply at any time during configuration to save the information that users have entered.
- Click CANCEL to exit from this page without saving the changes.

# Appendix A: Cable Requirements

## A.1 Ethernet Cable

A CAT 3~7 UTP (unshielded twisted pair) cable is typically used to connect the Ethernet device to the router. A 10Base-T cable often consists of four pairs of wires, two of which are used for transmission. The connector at the end of the 10Base-T cable is referred to as an RJ-45 connector and it consists of eight pins. The Ethernet standard uses pins 1, 2, 3 and 6 for data transmission purposes. (Table A-1)

**Table A-1** RJ-45 Ethernet Connector Pin Assignments

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

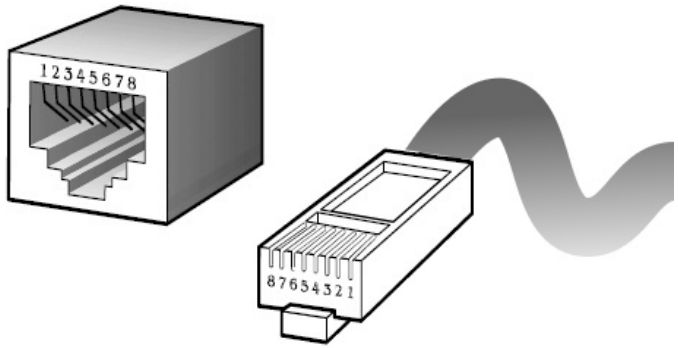



**Figure A-1 Standard RJ-45 receptacle/connector**

**Note:**

Please make sure users connected cables have the same pin assignment as the table above before deploying the cables into the users' network.

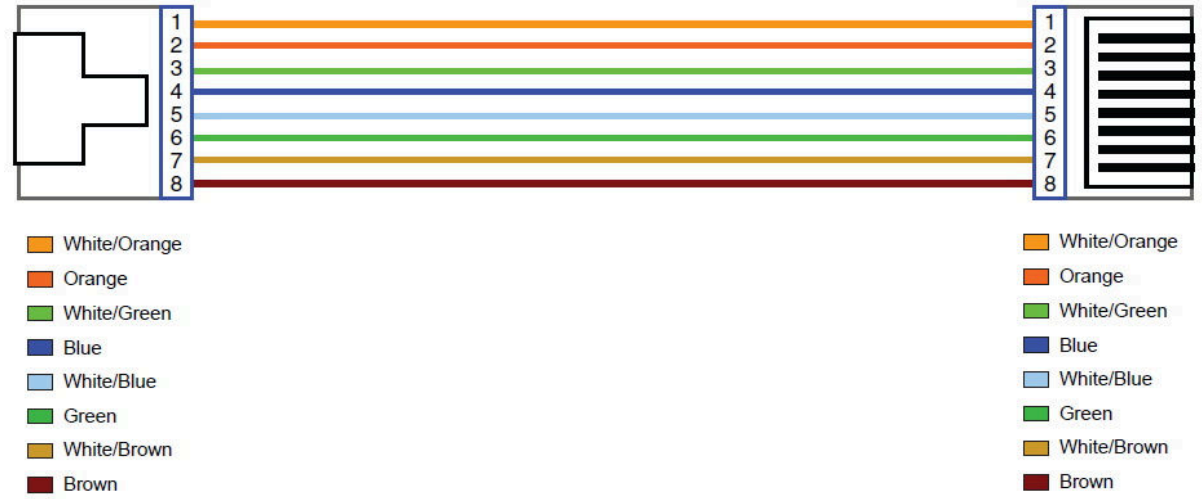



**Figure A-2 Pin Assignments and Wiring for an RJ-45 Straight-Through Cable**

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

## A.2 Telephone wire

Standard telephone wire of any gauge or type-flat, twisted or quad is used to connect the Modem to the telephone network. A telephone cable typically consists of three pairs of wires, one of which is used for transmission. The connector at the end of the telephone cable is called an RJ-11 connector and it consists of six pins. POTS (plain old telephone services) use pins 3 and 4 for voice transmission. A telephone cable is shown below. (Figure A-4)

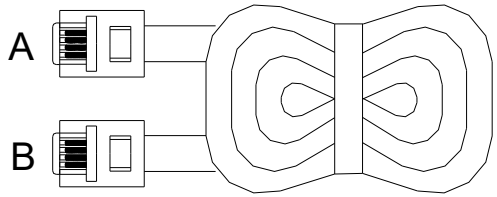



**Figure A-4 Telephone cable**

The A and B connectors on the rear of the Modem are RJ-11 connectors. These connectors are wired identically. The RJ-11 connectors have six positions, two of which are wired. The Modem uses the center two pins. The pin out assignment for these connectors is presented below. (Table A-2)

**Table A-2** RJ-11 Pin out Assignments

| Pin# | MNEMONIC | FUNCTION |
|---|---|---|
| 1 | NC | Unused |
| 2 | NC | Unused |
| **3** | **TIP** | **POTS** |
| **4** | **RING** | **POTS** |
| 5 | NC | Unused |
| 6 | NC | Unused_ |

# Appendix B: Product Specification

## Key Features & Benefits

- Supports ITU-T G.993.5 Vectoring
- Support ATM and PTM transmission mode auto detection (ADSL Annex B backward compatible)
- Supports high bandwidth up to 100Mbps symmetric over line ports
- Support 8a, 8b, 8c, 8d, 12a, 12b, 17a, 17b, and 30a band profile
- Support 997, 998 band plan
- Support ATM-TC, ATM and AAL5 (ATM Flow Throughout / OAM Cell Filter and Forwarding / AAL5 SAR: PVC / ATM Traffic Class / ATM PVC Shaping / ATM PVC Scheduling)
- Supports ATM Total Upstream Priority Queues
- Support uPnP/PPPoE/PPPoATM/IPv4/IPv6/NAT/NAPT
- Support static routing for IPv4 and IPv6 forwarding
- Support Firewall functions contain Packet filtering, DMZ, Mac Address based filtering, Parental Control, Application based filtering
- Support DHCP Server/DHCP Relay/DHCP Client/DHCPv6 Client/DHCPv6 Server/DNS/DNS Proxy or Relay/DNSv6 Proxy or Relay/NTP Client/HTTP1.1 server
- Support Multicast IP table/IGMP v3 Proxy and Snooping
- Support IEEE 802.1p VLAN Priority and mapping to DSCP
- Supports 802.1q VLAN tagging
- Supports HTTP/HTTPS(SSL) web management
- Support remote management and monitor

- Support configuration backup and restore
- Provides surge protection for Line port
- Supports jumbo frame up to 1680 bytes
- Supports IEEE 802.1w RSTP (*)
- Support Router & Switch (Bridged) mode selection
- Supports 8 queue MFC/DSCP both type QoS.
- Supports Dual Firmware Image Backup
- Supports Dying Gasp
- Supports SNMP v1 / v2c / v3

**Note:**

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

## Product Specification

| | |
|---|---|
| **Standard:** | IEEE802.3/802.3u/802.3ab standards<br>ITU-T G992.1/G992.3/G992.5/G993.1/G997.1/G993.2 standards |
| **Physical Interface:** | 4 x RJ-45 10/100/1000Mbps Ethernet port<br>1 x RJ-11/Terminal Block connector for VDSL2 line port<br>1 x RJ-11 connector for POTS/ISDN device<br>1 x console port (RS232C/115200bps) |
| **Flow control:** | Full duplex: IEEE 802.3x |

| | |
|---|---|
| | Half duplex: Back pressure |
| **LED Indicators:** | 1 x Power LED<br>4 x Link/Active Status for Ethernet port<br>1 x Link LED for VDSL2 port |
| **Switch method:** | Store and forward |
| **Typical Power Consumption:** | 6.7 W |
| **Power Input:** | Input Voltage: 12 VDC (Commercial-grade power adapter) |
| **EMC:** | EMI Compliant: FCC Class B<br>EMS Compliant: CE mark Class B |
| **Operating Temperature:** | 0°C ~ 50°C (32°F ~ 122°F)<br>Fanless, free air cooling |
| **Storage Temperature:** | -20°C ~ 70°C (-4°F ~158°F) |
| **Humidity:** | 10% to 90% (non-condensing) |
| **Weight:** | About 0.4 kgs |
| **Dimensions:** | 184 x 146 x 40 mm (7.2" x 5.74" x 1.57") |
| **Chipsets:** | Lantiq VRX |

# Appendix C: Router Mode select

This appendix describes how to select the router mode, The NV-600A default mode is switch (bridged mode), please refer to the following steps to select the router mode or switch mode.

## ◆ Select the Router mode:

1. To configure the router mode settings, click the **LAN Settings** link (**LAN > LAN Settings**) on the left navigation bar. Then select the "Server" at the DHCP Mode and click Apply at any time during configuration to save the information that users have entered. A screen is displayed as shown in Figure C.1

**Figure C-1 DHCP Mode – Server**

**Note:**

Please refer to section 4.7.2 to configure the DHCP Server settings.

2. Click the **WAN Setting** link (**WAN Setting > WAN**) on the left navigation bar to specify the WAN setting. Please cancel the check of the Auto Detect Enable and Add to config the wan type.

**Figure C-2 WAN Setting**

3. Please refer to section **4.5.6** to configure the wan type, the user can set up the Dynamic IP Address, Static IP Address, PPPoE mode.

**Figure C-3 Config WAN Type**

- Click Apply for applying the changes.
- Click CANCEL to exit from this page without saving the changes.

# Appendix D: Troubleshooting

## Diagnosing the Router's Indicators

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

| | |
|---|---|
| **1. Symptom:** | POWER indicator does not light up (green) after power on. |
| **Cause:** | Defective External power supply |
| **Solution:** | Check the power plug by plugging in another that is functioning properly. Check the power cord with another device. Check the terminal block and make sure to fasten the power cord. If these measures fail to resolve the problem, have the unit power supply replaced by a qualified distributor. |
| **Note:** | Please refer to the power status table to check power input status. Section 3.3 |

| | |
|---|---|
| **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:** | 2.1 Power off and re-power on the VDSL2 router.<br>2.2 Verify that the switch and attached device are power on.<br>2.3 Be sure the cable is plugged into both the switch and corresponding device.<br>2.4 Verify that the proper cable type is used, and its length does not exceed specified limits.<br>2.5 Check the router on the attached device and cable connections for possible defects.<br>2.6 Make sure that the phone wire must be connecting NV-600A first, when powered on.<br>2.7 Replace the defective router or cable if necessary. |

| 3. Symptom: | VDSL Link cannot be established. |
|---|---|
| Cause: | VDSL setting failure or phone cable length is over the specification limit. |
| Solution: | 3.1 Please make sure that the phone wire must be connected between NV-700L(CO) and NV-600A (CPE) when both are power on. NV-700L (CO) will do link speed function depending on phone wire length, therefore if NV-700L (CO) can't detect NV-600A (CPE) over phone wire while both powers are on, this will cause the link to fail.<br>3.2 Please check phone wire, we recommend using 24-26 gauge with twisted pair and without rust.<br>3.3 Please reinsert power when changing cable length or link time over 3 minutes. |
| Note: | Phone wire must meet CAT 3 standard or above and **without clustering**, otherwise will cause more cross talk issues to reduce DSL power driver. |

| 4. Question: | What is VDSL2? (Only reference) |
|---|---|
| Answer: | Very-high-speed digital subscriber line 2 (VDSL2) is an access technology that exploits the existing infrastructure of copper wires that were originally deployed for traditional telephone service. It can be deployed from central offices, from fiber-optic connected cabinets located near the customer premises, or within buildings. It was defined in standard ITU-T G.993.2 finalized in 2005.<br>VDSL2 was the newest and most advanced standard of digital subscriber line (DSL) broadband wireline communications. Designed to support the wide deployment of triple play services such as voice, video, data, high-definition television (HDTV) and interactive gaming, VDSL2 was intended to enable operators and carriers to gradually, flexibly, and cost-efficiently upgrade existing xDSL infrastructure. |

| | |
|---|---|
| | The protocol was standardized in the International Telecommunication Union telecommunications sector (ITU-T) as Recommendation G.993.2. It was announced as finalized on 27 May 2005,[1] and first published on 17 February 2006. Several corrections and amendments were published in 2007 through 2011.<br><br>VDSL2 is an enhancement to very-high-bitrate digital subscriber line (VDSL), Recommendation G.993.1. It permits the transmission of asymmetric and symmetric aggregate data rates up to 200 Mbit/s downstream and upstream on twisted pairs using a bandwidth up to 30 MHz<br><br>VDSL2 deteriorates quickly from a theoretical maximum of 250 Mbit/s at source to 100 Mbit/s at 0.5 km (1,600 ft) and 50 Mbit/s at 1 km (3,300 ft), but degrades at a much slower rate from there, and still outperforms VDSL. Starting from 1.6 km (1 mi) its performance is equal to ADSL2+.<br><br>ADSL-like long reach performance is one of the key advantages of VDSL2. LR-VDSL2 enabled systems are capable of supporting speeds of around 1–4 Mbit/s (downstream) over distances of 4–5 km (2.5–3 miles), gradually increasing the bit rate up to symmetric 100 Mbit/s as loop-length shortens. This means that VDSL2-based systems, unlike VDSL1 systems, are not limited to short local loops or MTU/MDUs only but can also be used for medium range applications. |

| 5. Question: | What is SNR(Signal-to-Noise)? (Only reference) |
|---|---|
| Answer: | Signal-to-noise ratio (often abbreviated SNR or S/N) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to noise power. A ratio higher than 1:1 indicates more signal than noise. While SNR is commonly quoted for electrical signals, it can be applied to any form of signal (such as isotope levels in an ice core or biochemical signaling between cells). The ratio is usually measured in decibels(dB)<br>The signal-to-noise ratio, the bandwidth, and the channel capacity of a communication channel are connected by the Shannon–Hartley theorem.<br>In digital communications, the SNR will probably cause a reduction in data speed because of frequent errors that require the source (transmitting) computer or terminal to resend some packets of data. SNR measures the quality of a transmission channel over a network channel. The greater the ratio, the easier it is to identify and subsequently isolate and eliminate the source of noise. |

| 6. Symptom: | Connected the CO Router with CPE Router within 300 meters RJ-11 phone cable got only less than 10 Mbit/s. |
|---|---|
| Cause: | Some testing programs which are based on TCP/IP protocol such as FTP, Iperf, NetIQ, the bandwidth of testing outcome will be limited by TCP window size. |
| Solution: | We recommend testing VDSL2 bandwidth best by Smartbit equipment, if users don't have Smartbit, we recommend test that by IPERF program, and TCP window size must be settled max. 64k, the parameter as iperf –c server IP address –i 1 –t 50 –w 65535 for client side. |

| | |
|---|---|
| **7. Question:** | I just bought a Netsys' NV-600A to replace my Quest DSL modem for my home. I was told any VDSL2 modem would replace and give me higher communication speeds. It doesn't get users on the internet when hooked up. All lights come on but no Link light. Is this the completely wrong application for this unit? |
| **Answer:** | Re: Please note NV-600A is a remote side (CPE side), it must be connected to the CO side to work. Tone mode, Band profile and band plan setting must be compatible with each other if no access error will show when applied. Please deactivate and activate once the setting has been changed. |

| | |
|---|---|
| **8. Question:** | We need to set up a default gateway on a NV-600 pair which are in Bridge mode, as they want to manage the units from a different network. |
| **Answer:** | When the application is used within the LAN, the switch(bridged) mode is not necessary to set up a gateway .However, if the application crosses various network segments (LAN to WAN or WAN to LAN), users must set up a gateway to connect different network segment.<br>Regarding how to configure a default gateway at switch(bridged) mode for crossing various network segments, please refer to the section 4.8.1 for user's reference.<br>Configuration gateway example from static routing:<br>Destination LAN IP: 0-0-0-0<br>Subnet Mask: 0-0-0<br>Gateway: 255-255-255-0<br>**Note:** Static Routing functionality is used to define the connected Gateway between the LAN and WAN. |

| 9. Question: | Is it possible to use the ADSL2 IP DSLAM with the NV-600A? |
|---|---|
| Answer: | NV-600A supports the ADSL backward compatible, therefore the NV-600A can connect to ADSL2 IP DSLAM (Annex B). |

| 10. Question: | What can I do if I forgot my password. |
|---|---|
| Answer: | If users forgot user's password, users must reset user's router. Unfortunately, this process will change all users' settings back to the factory defaults. To reset the router, locate the reset on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for over 5 seconds. Release the button and the router will go through its reboot process. The default ip is 192.168.16.254. When logging in, the default username and password both are "admin". |

| 11. Question: | What is the maximum Ethernet frame MTU for these routers? |
|---|---|
| Answer: | NV-600A maximum Ethernet frame MTU is 1680 bytes (Jumbo Frame). |

# System Diagnostics

## Power and Cooling Problems

If the POWER indicator does not turn on when the power cord is plugged in, users 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. If users still cannot isolate the problem, then the internal power supply may be defective. In this case, please contact the user's 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 users are sure that all the other components are functioning properly.

## Transmission Mode

The default method of selecting the transmission mode for RJ-45 ports is 10/100 Mbps ETHERNET, for RJ-11 port are auto-negotiation VDSL. Therefore, if the Link signal is disrupted (e.g. by unplugging the network cable and plugging it back in again, or by resetting the power), the port will try to reestablish communications with the attached device via auto-negotiation. If auto-negotiation fails, then communications are set to half duplex by default. Based on this type of commercial-standard connection policy, if users 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 a version that supports Ethernet and VDSL.

### 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 users have completed all the preceding diagnoses, then contact the user's dealer.

# Appendix F: Compliance 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 the 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 prevent the user's authority to operate the equipment.

If this telephone equipment causes harm to the telephone network, the telephone company will notify users 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, users will be advised of the users' right to file a complaint with the FCC if users believe it is necessary.

The telephone company may make changes to its facilities, equipment, operations or procedures that could affect the proper functioning of the user's equipment. If they do, users will be notified in advance in order for users to make necessary modifications to maintain uninterrupted service.

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

## FCC Warning

This equipment has been tested to comply with the limits for a **Class B** 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.

## RoHS Mark Warning

RoHS stands for Restriction of Hazardous Substances and impacts the entire electronics industry and many electrical products as well. The original RoHS, also known as Directive 2002/95/EC, originated in the European Union in 2002 and restricts the use of six hazardous materials found in electrical and electronic products. All applicable products in the EU market from July 1, 2006, must pass RoHS compliance. Directive 2011/65/EU was published in 2011 by the EU, which is known as RoHS-Recast or RoHS 2. RoHS 2 includes a **CE-marking directive**, with RoHS compliance now being required for CE marking of products. RoHS 2 also added Categories 8 and 9 and has additional compliance recordkeeping requirements. Directive 2015/863 was published in 2015 by the EU, which is known as RoHS 3. RoHS 3 adds four additional restricted substances (phthalates) to the list of six.

## 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 cross-out wheeled bin symbol. Do not dispose of WEEE is unsorted municipal waste and has to collect such WEEE separately.

## Warranty

The original product that the owner 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 the 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:**

**1.DO NOT TEAR OFF OR REMOVE THE WARRANTY STICKER AS SHOWN, OR THE WARRANTY IS VOID.**

**2.WARRANTY VOID IF USE COMMERCIAL-GRADE POWER ADAPTER IS USED AT HARSH ENVIRONMENTS.**

## Chinese SJ/T 11364-2014

| 部件名称 | 有毒有害物质或元素 | | | | | |
|---|---|---|---|---|---|---|
| | 铅(Pb) | 汞(Hg) | 镉(Cd) | 六价铬[Cr(VI)] | 多溴联苯(PBB) | 多溴二苯醚(PBDE) |
| 结构壳体 | ○ | ○ | ○ | ○ | ○ | ○ |
| 电路组 | ○ | ○ | ○ | ○ | ○ | ○ |
| 包装及配件 | ○ | ○ | ○ | ○ | ○ | ○ |

○：表示该有毒物质在该部件所有均质材料中的含量均在 GB/T 26572 标准规定的限量要求以下。

╳：表示该有毒物质至少在该部件的某依均质材料中的含量超出 GB/T 26572 标准规定的限量要求。

上述规范仅适用於中国法律