netsys

Networking your world

NV-600W

Managed Wireless VDSL2 Router

USER'S MANUAL

Http://www.netsys.com.tw

Copyright

Trademarks

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

Legal Disclaimer

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

Statement of Conditions

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

Maximum signal rate derived 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 you 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-600W is a managed wireless VDSL2 router that leverages the extraordinary bandwidth promise of VDSL2 technology and compliant with the IEEE 802.11n standard. It can enhance wireless speeds up to 300 Mbps* and extend the coverage. NV-600W also supports one-touch Wi-Fi Protected Setup (WPS) with the push button that only takes a few seconds to setup a secured wireless network.

In recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. Anyone can bring a built-in WLAN client smartphone, tablet or notebook into a meeting room for a conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access. The NV-600W is equipped with a wireless LAN interface compliant with the standard IEEE 802.11n protocol. To boost its performance even further, the NV-600W is also loaded with an advanced wireless technology to lift up the data rate up to 300 Mbps*. You can finally smoothly enjoy a wide range of apps on your smart phone, tablet or smart TV.

(*). The maximum wireless data transfer rate is derived from IEEE Standard 802.11 specifications. Actual data transfer rate will vary from network environment including: distance, network traffic, building site materials/construction, interference from other wireless devices, and other adverse conditions.

Caution:

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

Safety Warnings

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

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

TABLE OF CONTENTS

COPYRIGHT 1

FOREWORD: VDSL2 ROUTER SOLUTION 2

SAFETY WARNINGS 3

1.1 Check List 10

CHAPTER 2. INSTALLING THE ROUTER 11

2.1 Hardware Installation 11

2.2 Pre-installation Requirements 11

2.3 General Rules 12

2.4 Connecting the Router 13

2.5 Connecting the RJ-11 / RJ-45 Ports 14

2.6 VDSL2 Application 15

CHAPTER 3. HARDWARE DESCRIPTION 19

3.1 Front Panel 20

3.2 Front Indicators 20

3.3 Rear Panel 22

CHAPTER 4. CONFIGURING THE NV-600W VIA WEB BROWSER 25

4.1 Login 26
4.1.1 Home 28
4.1.2 Quick Setup 30

4.2 Select the Menu Level 38

4.3 Select "SYSTEM" 39
4.3.1 Host Name Configuration 40
4.3.2 System Time 41
4.3.3 Administrator Settings (User Account Management) 43
4.3.4 Web Settings 45
4.3.5 Software/Firmware Upgrade 46
4.3.6 Configuration Settings 47
4.3.7 System Log 50
4.3.8 SSL Certificate 53
4.3.9 Reset 54

4.4 Select "Statistics" 55

4.4.1 LAN....56
4.4.2 WAN....58

4.5 Select "xDSL"....60
4.5.1 xDSL Status....61
4.5.2 Vectoring Mode selection....63

4.6 Select "WAN"....65
4.6.1 WAN Mode Selection....66
4.6.2 Auto Detect Setting....68
4.6.3 WAN Channel Configuration....71
4.6.4 VLAN Channel Configuration....75
4.6.5 WAN Setting....78
4.6.6 WAN Status....92
4.6.7 DNS....96
4.6.8 DDNS....98
4.6.9 OAM Configuration....100

4.7 Select "LAN"....104
4.7.1 LAN ARP List....105
4.7.2 LAN Settings....106
4.7.3 UPnP Devices List....116
4.7.4 LAN Switch Port Setting....117
4.7.5 LAN Port Status....118
4.7.6 VLAN Settings....119

4.8 Select "Route" 121
4.8.1 Static Routing 122
4.8.2 RIP Support 125
4.8.3 Routing Table List 128

4.9 Select "Wireless" 131
4.9.1 Radio Settings 132
4.9.2 Security Settings 134
4.9.3 WMM Settings 140
4.9.4 WPS Settings 142
4.9.5 Station List 144

4.10 Select "Firewall" 145
4.10.1 Firewall Setting 146
4.10.2 IPv6 Firewall Setting 147
4.10.3 Packet Filtering 149
4.10.4 URL Filtering 163
4.10.5 Parental Control 165
4.10.6 Application Server Settings 167
4.10.7 Access Control List (ACL) 169

4.11 NAT 171
4.11.1 NAT Settings 172
4.11.2 Virtual Server 173
4.11.3 Port Triggering 177

4.11.4 DMZ 181

4.11 QoS 183
4.11.1 QoS Settings 184
4.11.2 Queue Configuration. 187
4.11.3 Class Configuration 191

4.12 Multicast 197
4.12.1 Proxy Settings 198
4.12.2 Snooping Settings 200
4.12.3 Advanced Settings 202

4.13 IPsec 204
4.13.1 Tunnel Mode 205

4.14 IPv6 208
4.14.1 IPv6 Setting 209
4.14.2 6RD Configuration 211
4.14.3 DS-Lite Configuration 213

4.15 Diagnostics 215
4.15.1 Diagnostic Test Suite 216

APPENDIX A: CABLE REQUIREMENTS 218

APPENDIX B: PRODUCT SPECIFICATION 221

APPENDIX C: ROUTER/BRIDGED MODE SELECT 224

APPENDIX D: NV-600L & NV-600A/W COMPATIBILITY TABLE 229

APPENDIX E: TROUBLESHOOTING 231

APPENDIX F: COMPLIANCE INFORMATION 240

WARRANTY 243

CHINESE SJ/T 11364-2014 244

Chapter 1. Unpacking Information

1.1 Check List

Thank you for choosing Netsys NV-600W. Before installing the router, please verify the contents inside the package.

Package Contents:

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

Notes:

1. Please inform your dealer immediately for any missing or damaged parts. If possible, retain the carton including the original packing materials. Use them to repack the unit in case there is a need to return for repair.
2. If the product has any issue, please contact your local 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-600W uses a DC12V/1A power supply.
4. The power supply included in the package is commercial-grade. Do not use in 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 the network connections. The NV-600W may be installed on any level surface (e.g. a table or shelf). However, please take note of the following minimum site requirements before you begin. **The NV-600W has pre-installed two rubber feet and two 2dBi (or 5dBi) Antennas (2.4 GHz).**

2.2 Pre-installation Requirements

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

Verify the following installation 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.
- Please note that the voice spectrum allowed by the NV-600W internal splitter is 0 KHz ~ 120 KHz.

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 ports must be made using Category 5 UTP 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 two pins. The pin out assignment for these connectors is presented below.

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

RJ-11 Pin out Assignments

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

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 will 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-600L (CO) using a single pair phone cable to NV-600W (CPE) bridge side (point to point solution). Take note that NV-600W line port RJ-11 and terminal block cannot be used at the same time. Either RJ-11 port is connected or terminal block is connected using straight connection. (Figure 2.1).

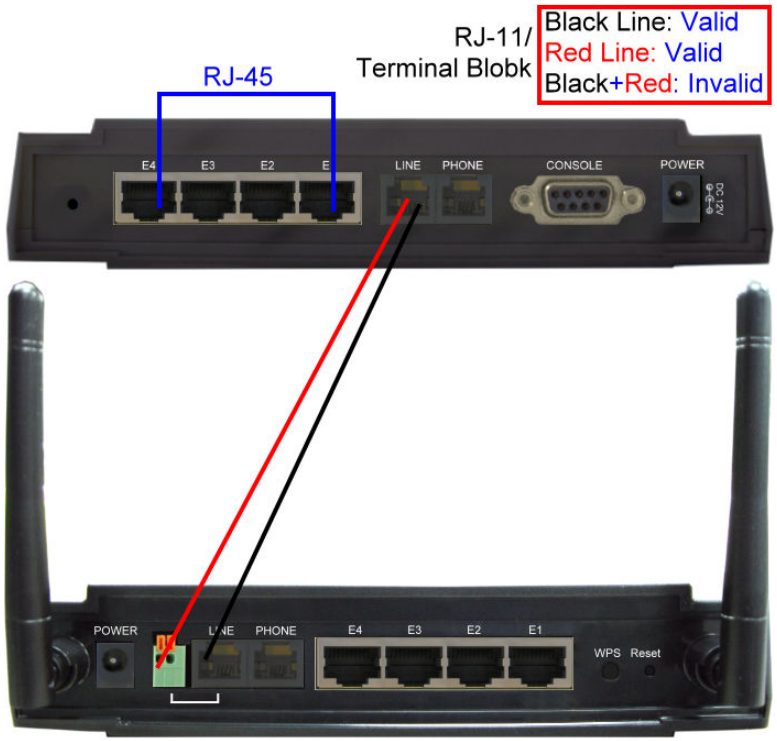


Figure 2.1 NV-600W line ports straight connection

- 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 a 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 advise using Category 5~7 UTP/STP cables for making Bridge or Router connections to avoid any confusion or inconvenience in the future when you attach high bandwidth devices.
3. Use **24 ~ 26** gauge twisted pair phone wiring, we do not recommend 28 gauge or above.
4. Be sure phone wire has been installed before the NV-600W 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 and do not requires 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 a suitable distance. (Figure 2.2)

Figure 2.2 NV-600W applications

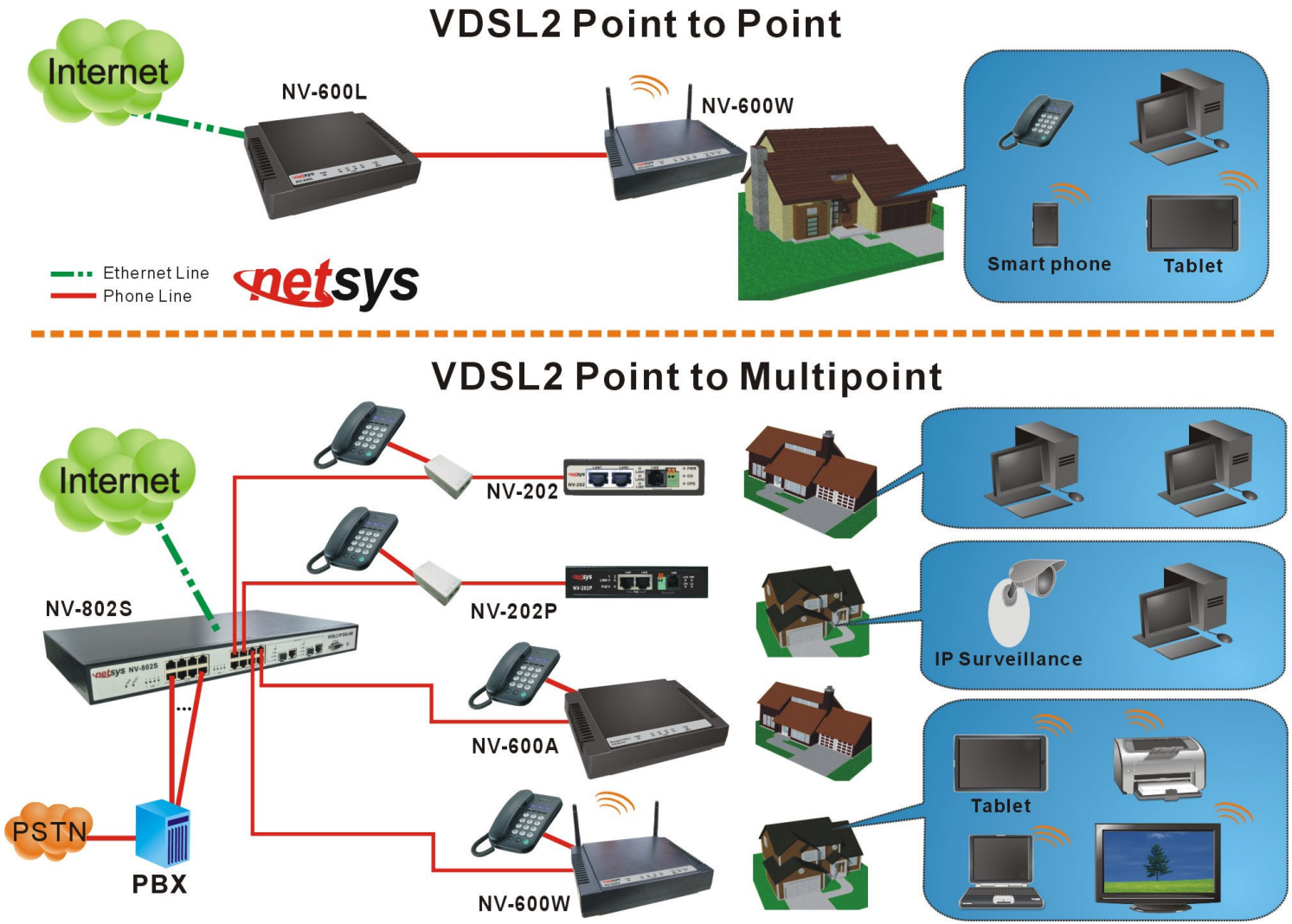


Figure 2.2.1 VDSL2 applications

◆ 2.6.1 Connect the NV-600L and the NV-600W to the Line

The objective for VDSL2 is to pass high speed data over a twisted pair cable. In the setup, connect NV-600L to NV-600W 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-600L and the NV-600W 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.

◆ 2.6.4 Wireless Basics

In recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. Anyone can bring a built-in WLAN client Smartphone, tablet or notebook into a meeting room for a conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access. The NV-600W is equipped with a wireless LAN interface compliant with the standard IEEE 802.11n protocol. To boost its performance even further, the NV-600W is also loaded with an advanced wireless technology to lift up the data rate up to 300 Mbps. You can finally smoothly enjoy a wide range of apps on your smart phone, tablet or smart TV.

- **What is WEP?**

Wired Equivalent Privacy (WEP) is an easily broken security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, was at one time widely in use and was often the first security choice presented to users by router configuration tools.

- **What is WPA?**

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy).

WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

A flaw in a feature added to Wi-Fi, called Wi-Fi Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. WPA and WPA2 security implemented without using the Wi-Fi Protected Setup feature are unaffected by the security vulnerability.

Chapter 3. Hardware Description

This section describes the important parts of the wireless VDSL2 router. It features the front and rear panel.

Wireless Router Outward

3.1 Front Panel

The front panel provides a simple interface monitoring of the router. (Figure 3.1) shows the front panel of the NV-600W

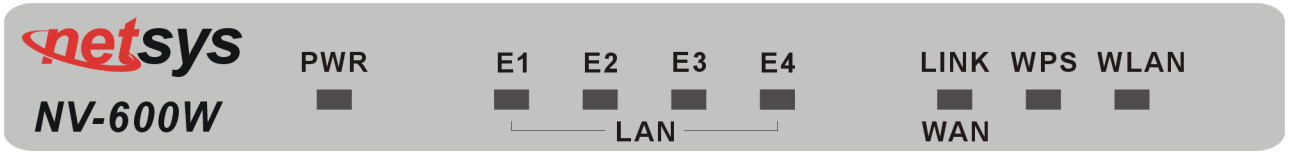


Figure 3.1 NV-600W Front Panel

3.2 Front Indicators

The wireless router has **Eight** 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)	When the router is powered on, and in ready state.
		Off	When the router is powered off
E1 ~ E4 (Ethernet LED)	Green	On(Steady)	The device has a good Ethernet connection.
		Blinking	The device is sending or receiving data via the corresponding LAN port.
		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.

LED	Color	Status	Descriptions
WPS	Green	On(Steady)	The WPS connection is ready.
		Off	The WPS is not available, or WPS is not enabled or initialized
WLAN (Wireless LED)	Green	On(Steady)	Wireless access point is ready.
		Blinking	Data is being transmitted through WLAN
		Off	Wireless access point is off or has malfunctioned.

Notes:

1. It is normal for the connection between two Routers to take up to 3 minutes, due to NV-600L/W to establish a link mechanism in auto-negotiation, that detects and calculates CO and CPE both PBO and PSD level, noise levels and other arguments for getting a better connection.
2. Every time the user presses the WPS button, there will be two minutes of time to detect the available equipment. If the WPS function does not detect the device, the WPS light will turn off.

3.3 Rear Panel

The rear panel provides the physical connectors connected to the power adapter and any other network device. (Figure 3.2) shows the rear panel of the NV-600W.

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	Reset Button	The reset button allows users to reboot the VDSL2 or load the default settings. **Press and hold for 1-5 seconds: Reboot the VDSL2 Router** **Press over 5 seconds: Load the default settings**
Power	DC Power Jack	External Power Adapter: Input: AC 85~240Volts/50~60Hz 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 an Ethernet equipped device.
Link (WAN)	RJ-11/Terminal Block	Allows data communication between the router and the VDSL2 network. (**Do not** use RJ11 and Terminal Block at the same time.)
WPS	WPS Button	Press this button to make a network connection through WPS (WPS function is only supported on windows 7 or above operating systems). Every time the user presses the WPS button, there will be two minutes of time to detect the available equipment.

Before installing power and device, please read and follow these essentials:

- Use separate paths to route wiring for power and devices. If power 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.

- You 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.
- You should separate input wiring from output wiring.
- We recommend that you mark all equipment in the wiring system.
- The maximum wireless data transfer rate is derived from IEEE Standard 802.11 specifications. Actual data transfer rate will vary from network environment including: distance, network traffic, building site materials/construction, interference from other wireless devices, and other adverse conditions.

Chapter 4. Configuring the NV-600W via Web Browser

The NV-600W provides a built-in HTML based management interface that allows configuration of the NV-600W via Internet Browser. Best viewed using Chrome or Firefox browsers.

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

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in windows XP SP2 or above.
- Java Scripts. (Enabled by default)
- Java permissions. (Enabled by default)

Launch your web browser and input the IP address 192.168.1.1 (NV-600W) in the Web page.
Following section user can find default username and password.

4.1 Login

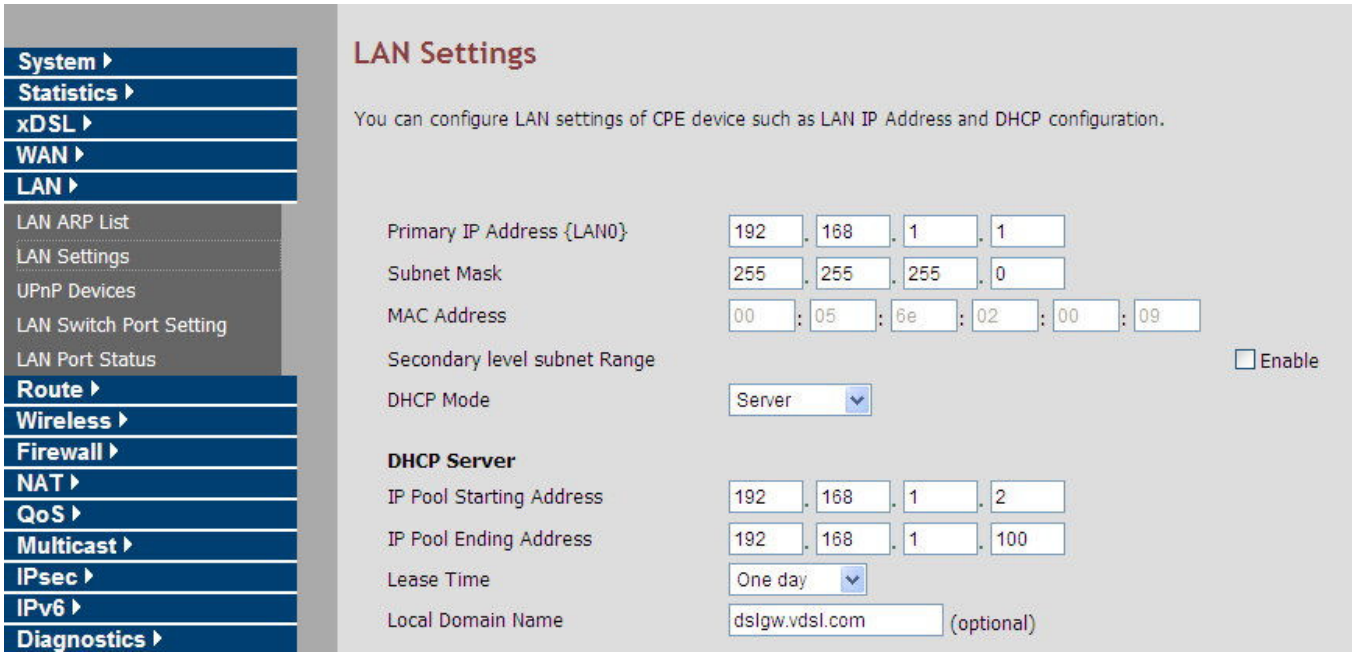
The default username is "admin" and password is "admin", too. The password is changeable in Administrator Settings. It is advisable to change the administrator password for the security of your network.

Figure 4.1 Login Password

◆ **About Wifi mode:**

Default wifi mode is enabled, default security setting is WPA2-AES, and the shared key (password) is "**12345678**". User can find information on wifi and login information sticker; it is located at the bottom of the product.

- The NV-600W default mode is **Router mode**. Following screenshot is for default LAN settings and WAN settings.



4.1.1 Home

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

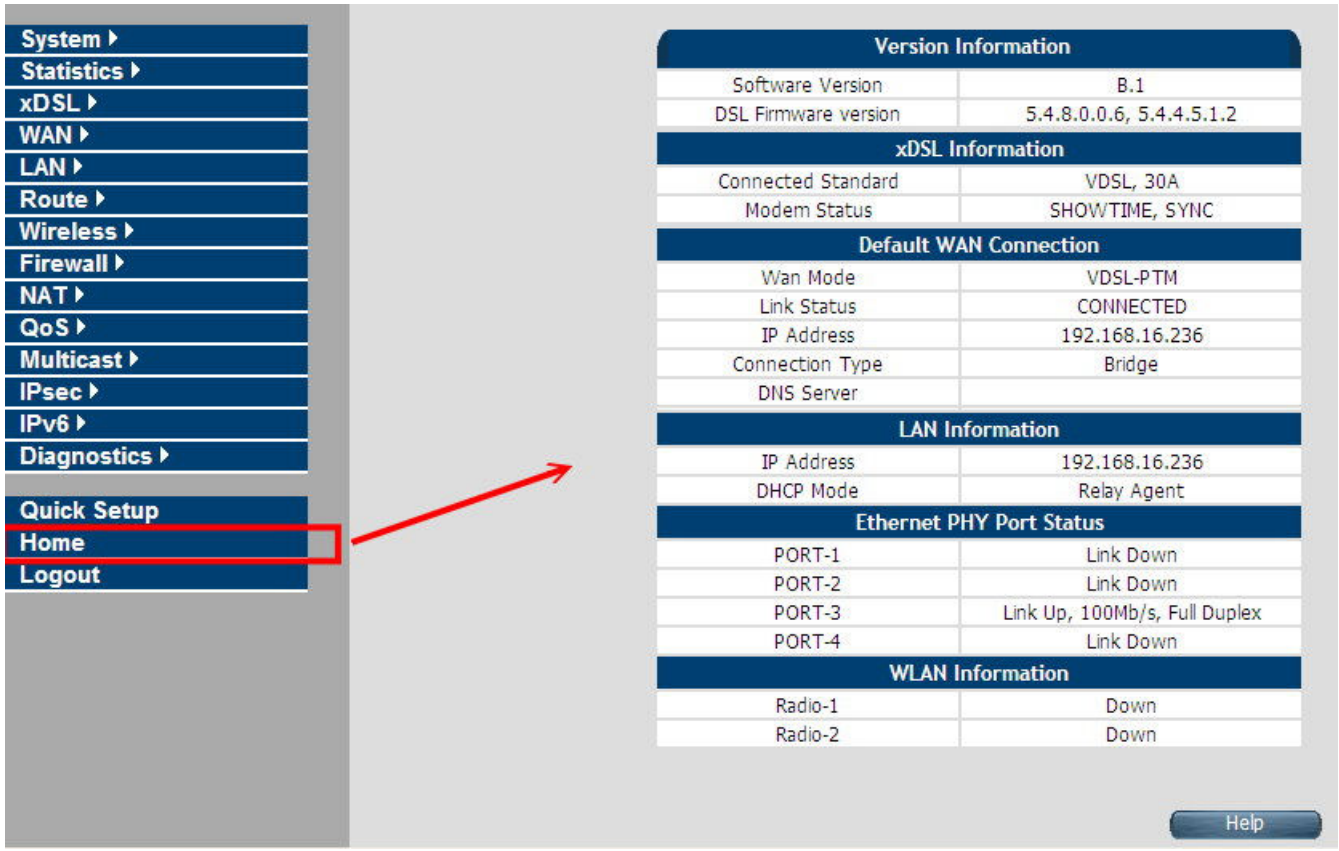


Figure 4.1.1 Home Information

The screen contains the following details:

Fields in Home page

Field	Description
Version Information	
Software Version	Shows the current version of the 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	Shows the IP address of LAN interface of CPE. This IP address 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.
WLAN Information	
Radio-1	Shows the status of WLAN Radio-1.
Radio-2	Shows the status of WLAN Radio-2. (Available only in concurrent dual band WLAN platforms).

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.

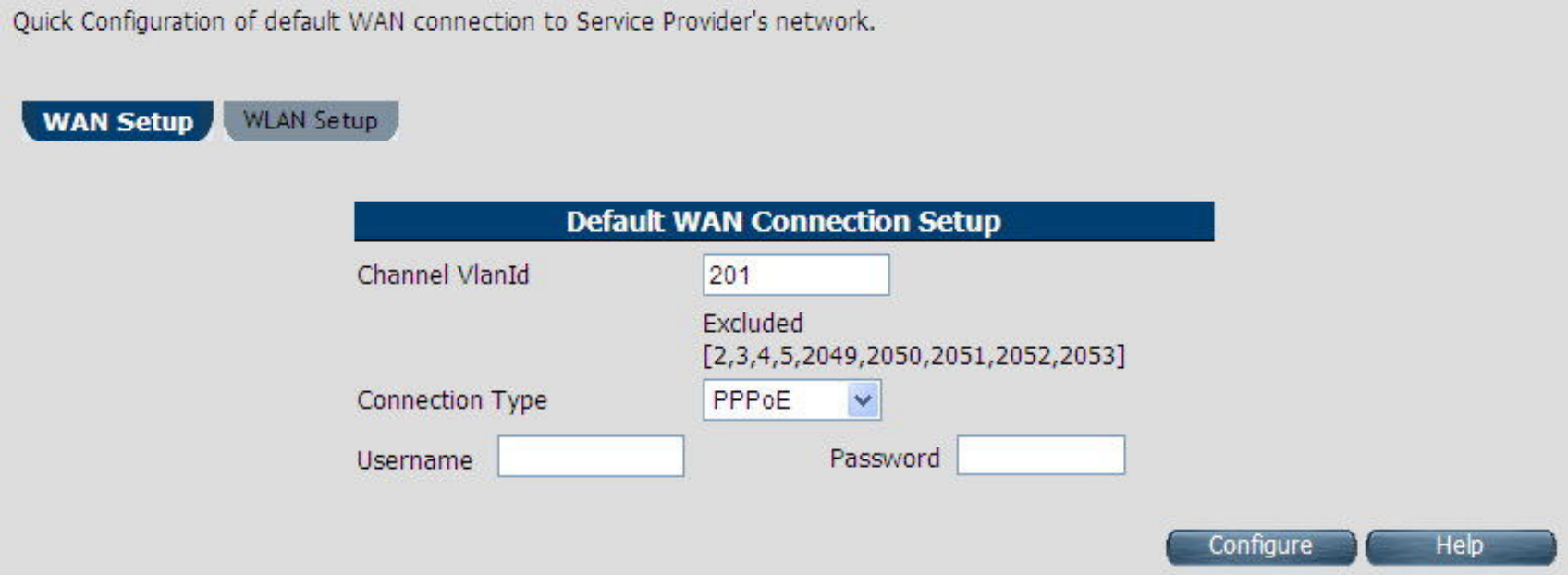


Figure 4.1.2 Quick Setup

◆ **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 already exists in CPE device, the same gets re-created with newly supplied attributes from the user. The default WAN Setup configuration shows the Bridged status.

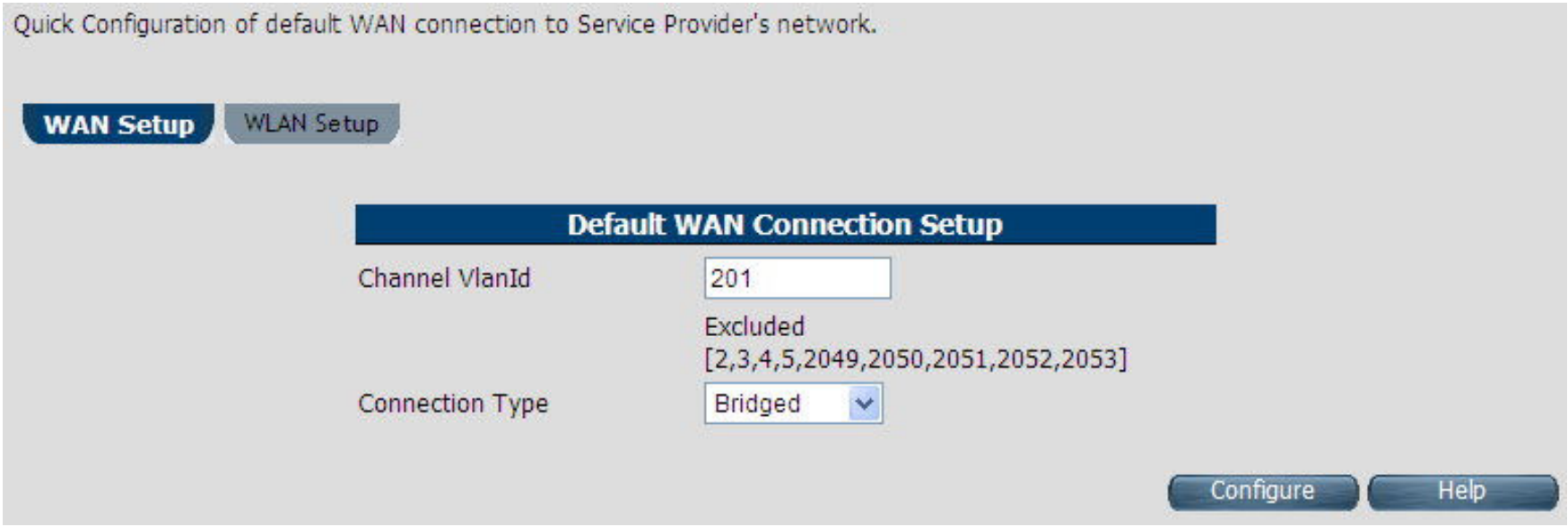


Figure 4.1.2.1 WAN setup Bridged

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.

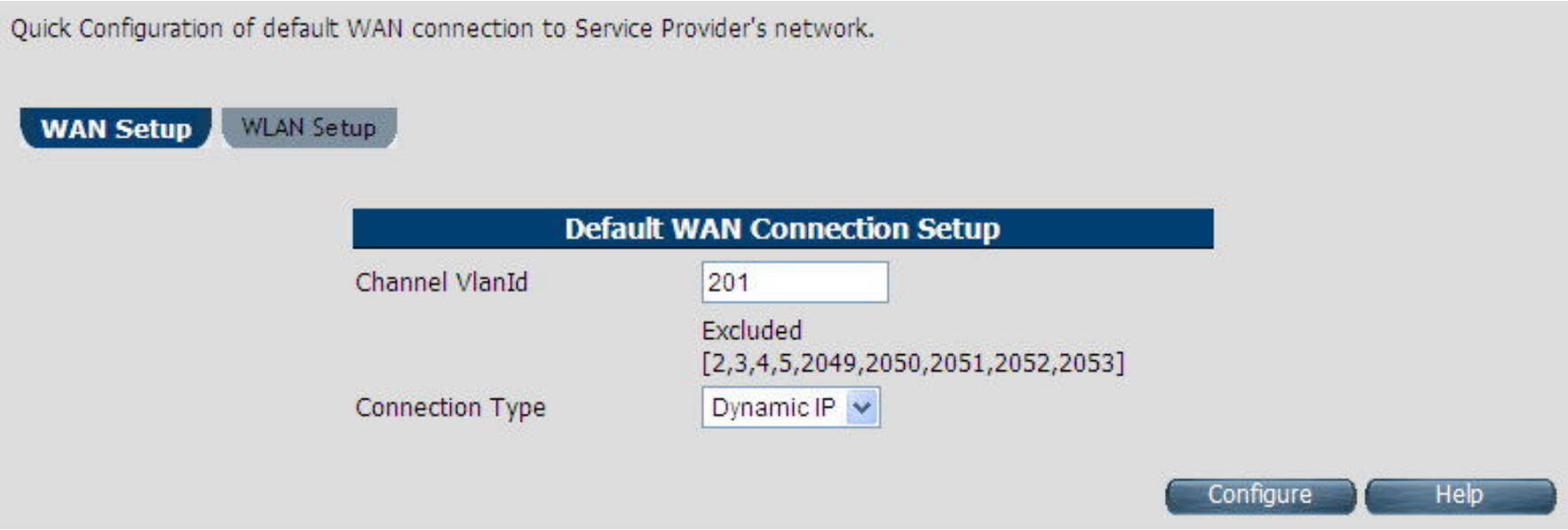


Figure 4.1.2.2 WAN setup Dynamic IP

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.

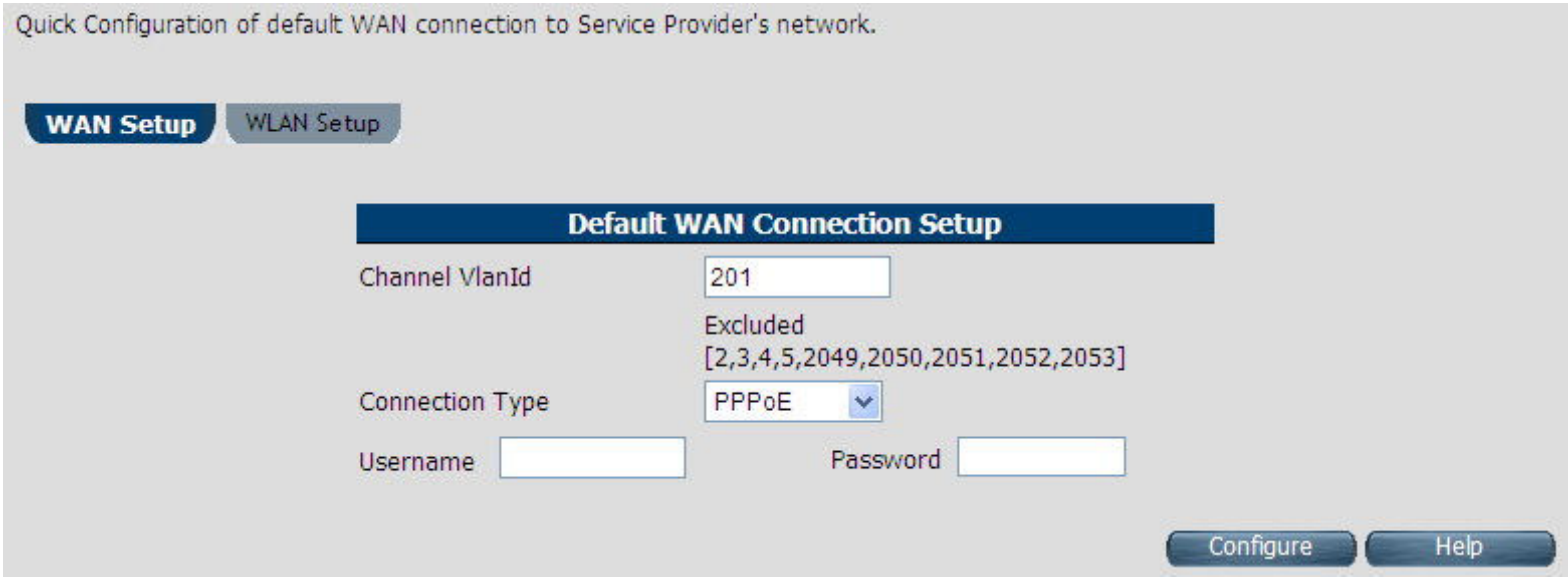


Figure 4.1.2.3 WAN setup PPPoE

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.

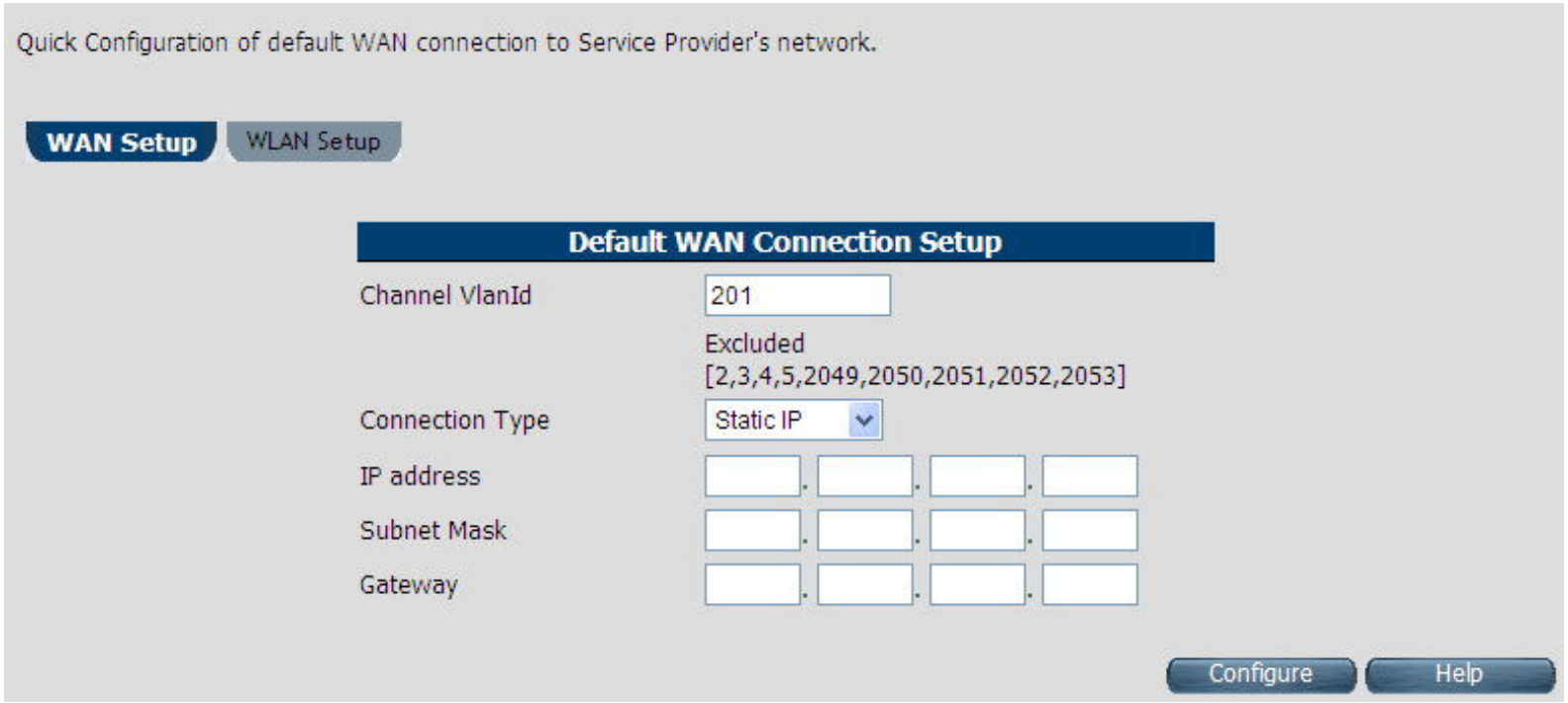


Figure 4.1.2.4 WAN setup Static IP

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-600W CPE's WAN link.
Subnet Mask	Specify the Subnet Mask of NV-600W CPE's WAN link.
Gateway	Specify the Gateway address of the NV-600W 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 user for fields like ATM VCC etc.

◆ **WLAN Setup**

When the user clicks on Quick Setup, the **WLAN Setup** tab is displayed as shown in **Figure 4.1.2.5**. The WLAN tab allows the user to configure the Wireless LAN in CPE Router.

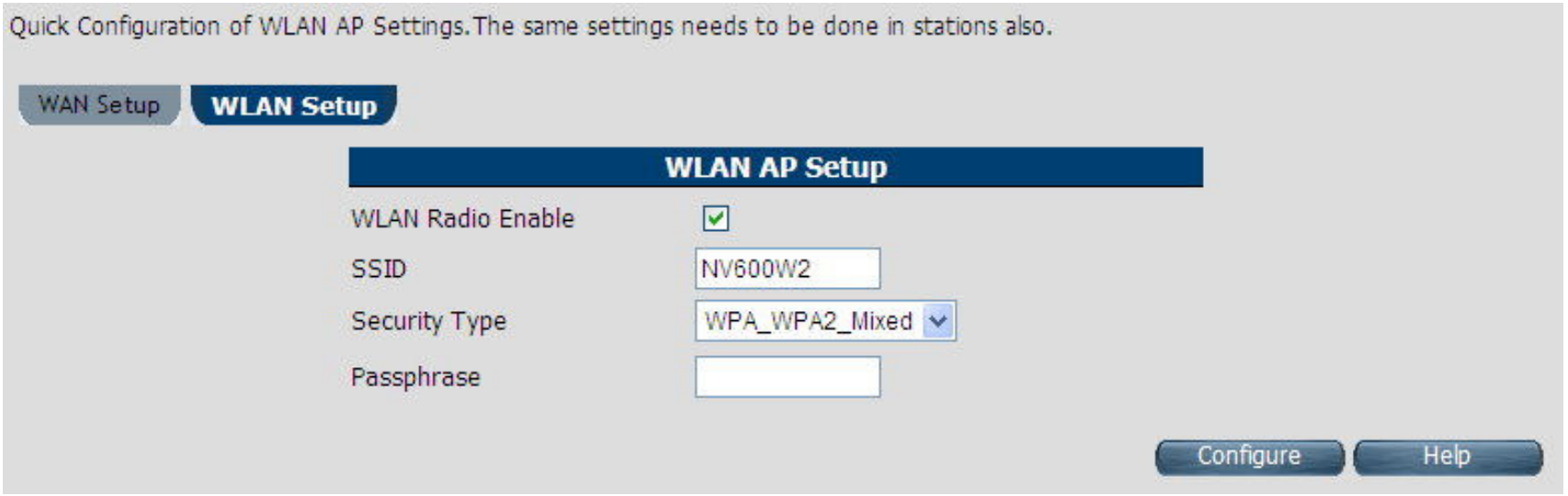


Figure 4.1.2.5 WLAN Setup

The screen contains the following details:

Fields in WAN setup Static IP

Field	Description
WLAN AP Setup	
WLAN Radio Enable	To Enable or Disable WLAN feature in CPE.
SSID	SSID Name.
Security Type	Security Type for AP are: ■ Basic (non-11n mode) ■ WPA (non-11n mode)
Passphrase	Secret String, from where the dynamic keys are generated. It is applicable only in case of WPA2 or WPA-WPA2 Mixed mode in Security Type.

◆ Click **Configure** to configure the Wireless LAN AP in CPE device.

4.2 Select the Menu Level

There is an easy Setup for end users at the setup of NV-600W with **SYSTEM**, **Statistics**, **xDSL**, **WAN**, **LAN**, **Route**, **Wireless**, **FIREWALL**, **NAT**, **QoS** , **Multicast**, **IPsec** , **IPv6**, **Diagnostics**, **Quick Setup**, **Home**, **Logout** for more detailed configurations.

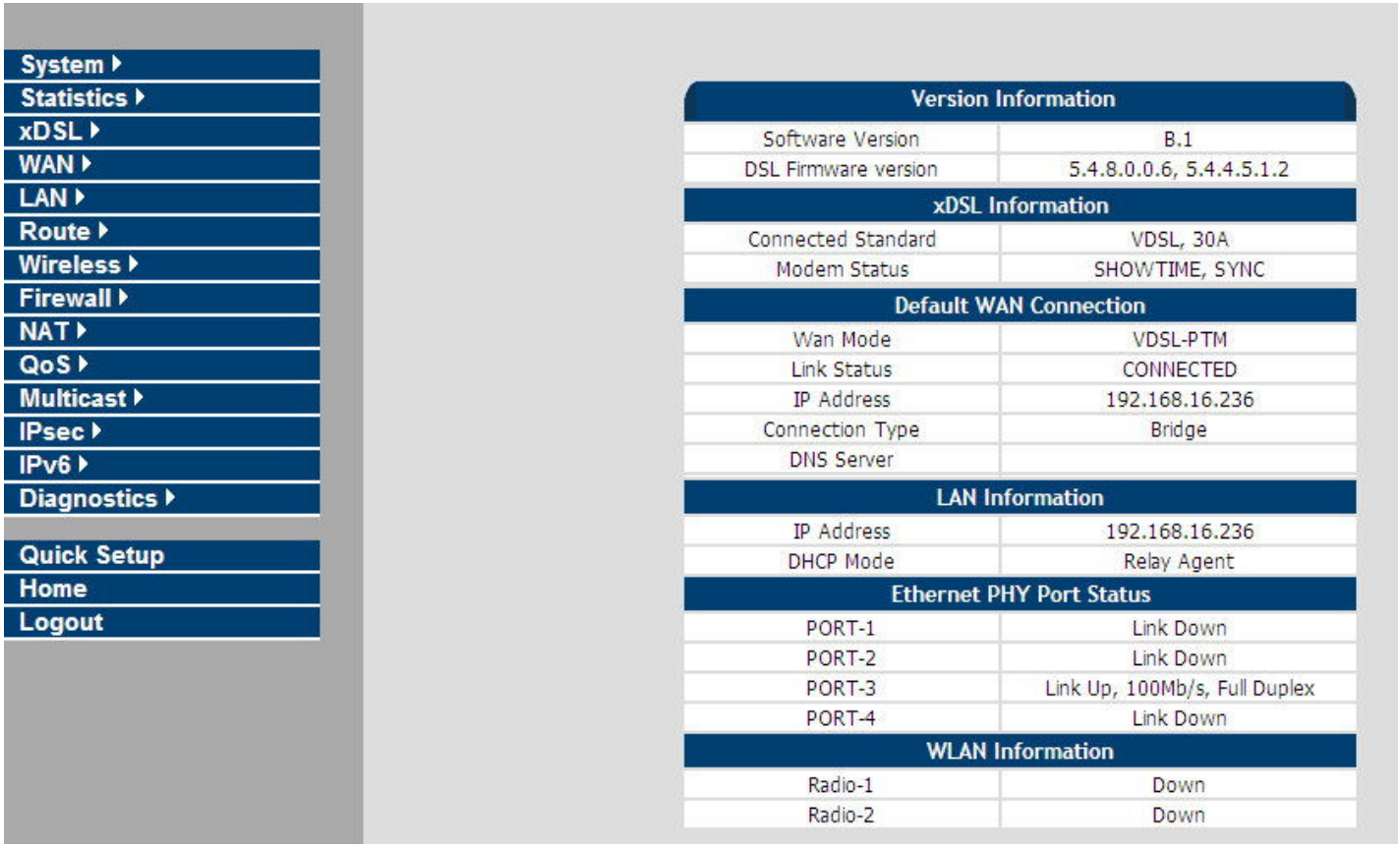


Figure 4.2 Select the Menu Level (NV-600W)

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 Certificate** and **Reset**. A screen is displayed as shown in Figure 4.3

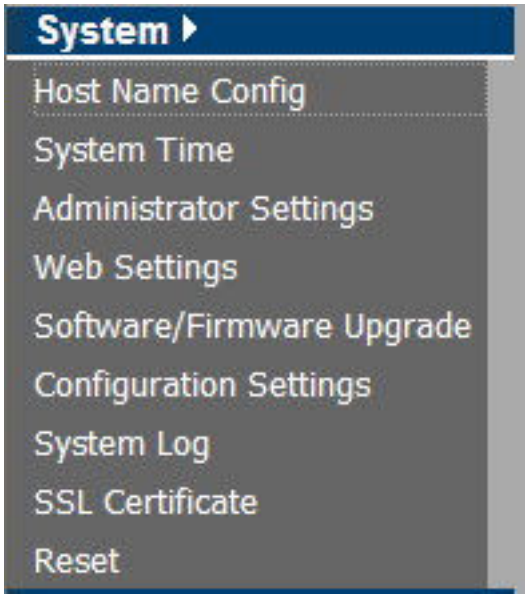


Figure 4.3 System Setup

4.3.1 Host Name Configuration

To configure the host name of NV-600W, you 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.

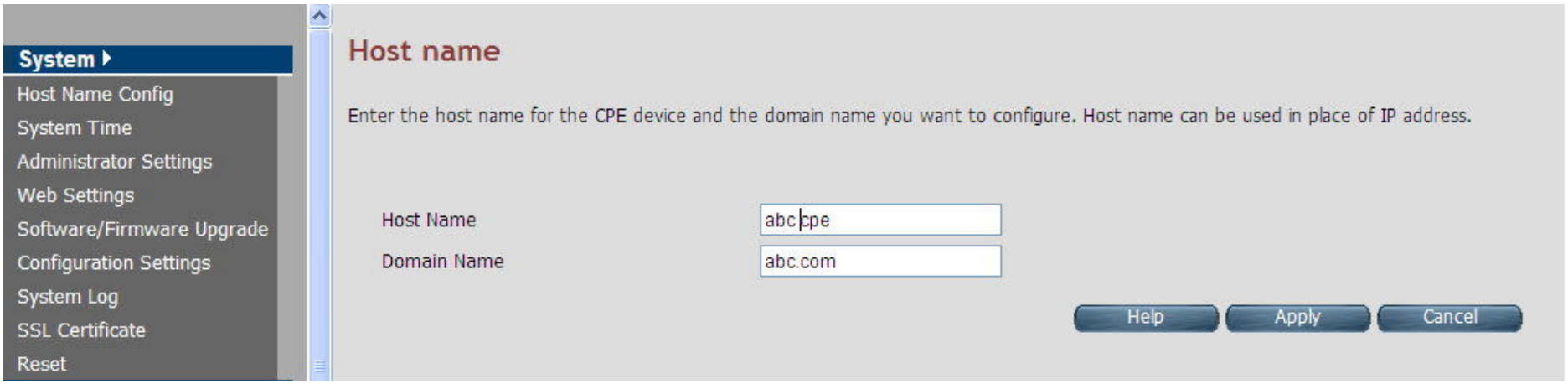


Figure 4.3.1 Host Name Configuration

Fields in Host Name Configuration

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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

4.3.2 System Time

You 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.

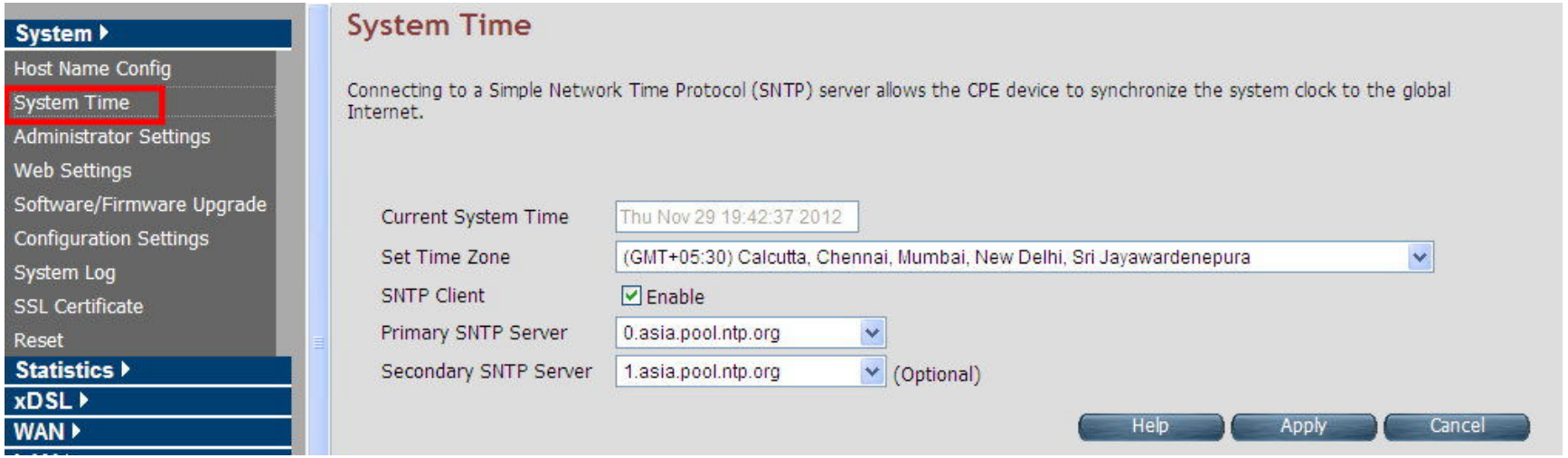


Figure 4.3.2 System Time Configuration

Fields in System Time

Field	Description
Current System Time	Current Time in System shown in Day, Date and Time of day.
Set Time Zone	Select the time zone form 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 form dropdown list.
Secondary SNTP Server	Backup NTP Server (optional).

- Click **Apply** at any time during configuration to save the information that you 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, we have to define the Gateway connected to NTP server in the WAN. Please refer to "static routing" for your reference.

4.3.3 Administrator Settings (User Account Management)

If you want to change the password for the administrator, click the **Administrator Settings** link (**System** > **Administrator Settings**) in 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
Password-less Login	Select this to enable login without prompting for Login page.
Select User	Select user type. The available options are admin and support_user.
Account Option	Edit option to modify User settings or Enable checkbox to Enable/Disable User.

Fields in Resource Access

Field	Description
Web Access	Web UI access permission - Local, Remote or both.
File Share Access	File share Access Permission - FTP, Samba or both.
Telnet Access	Telnet console access for user.

Fields in Account Option (Selected Edit boxes)

Field	Description
User Name	Type a new user name of account.
Current Password	The user should specify the current login password.
New 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.
Re-type Password	The user should re-type the new password entered in previous field.

Figure 4.3.3-1

- Click **Apply** at any time during configuration to save the information that you 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 logout duration after which the web session is automatically log-out. The unit is in seconds.

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

4.3.5 Software/Firmware Upgrade

For updating 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-600W Software running on the device as shown in Figure 4.3.5

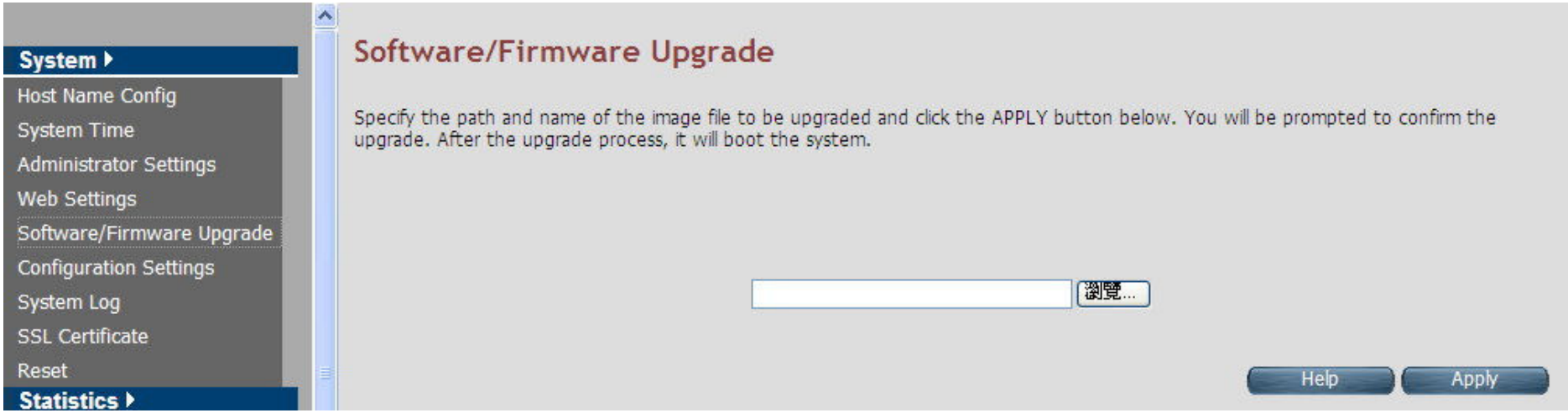


Figure 4.3.5 Software/Firmware Upgrade

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

Note:

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

4.3.6 Configuration Settings

For managing 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

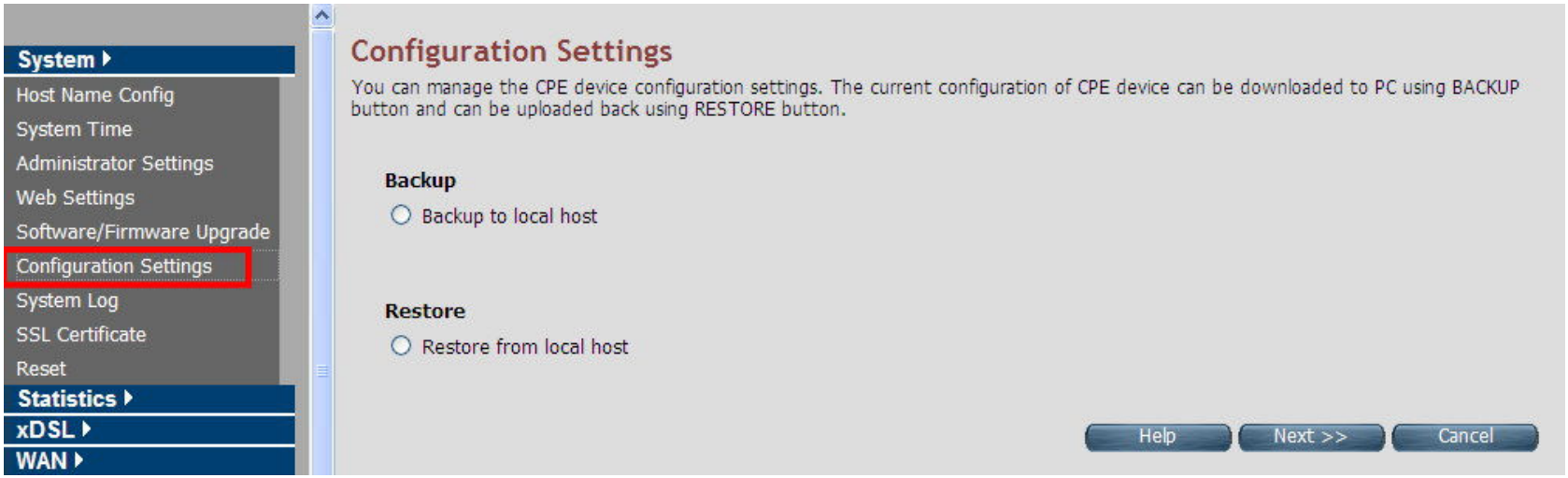


Figure 4.3.6 Configuration Settings

Fields in Configuration Settings

Field	Description
Backup to local host	This will backup 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 backup the current active configuration running in the router system. This is very helpful, when a user wants to backup the current working configuration of the router for rollbacks, if required in future. It is recommended that before any complex nature of configuration is done by user the current active configuration should be backed up in host machine. The Local Host Configuration backup is shown in Figure 4.3.6.1

Figure 4.3.6.1 Configuration Backup

When you click the **Backup** button as shown in Figure 4.3.6.1, it will backup the configuration settings of CPE in connected PC from where Web UI is being accessed.

■ Restore Previous Backed-up Configuration

As mentioned before this option allows the user 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 reboot after the configuration is restored. When the CPE boots up, it will be running with the newly applied configuration.

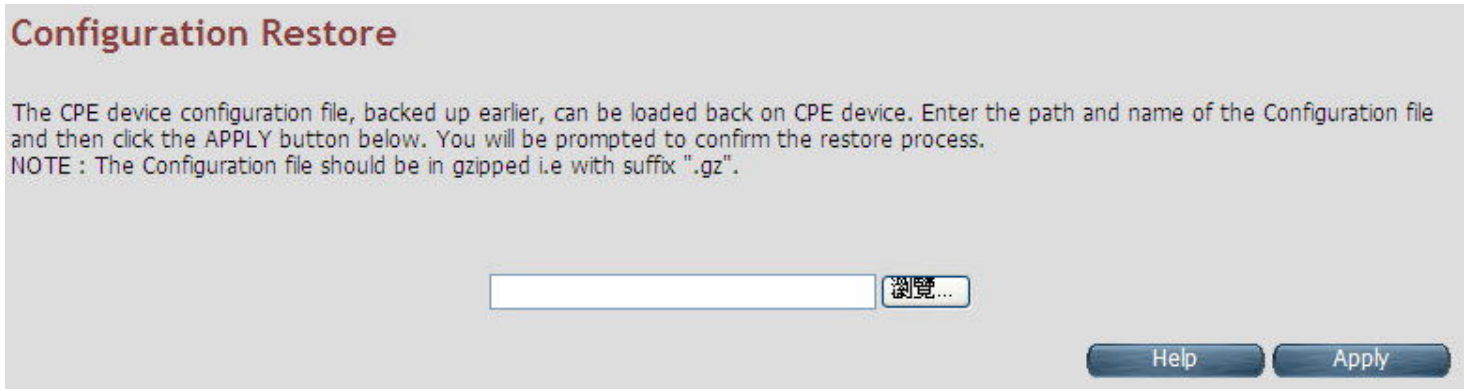


Figure 4.3.6.2 Configuration Restore

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

4.3.7 System Log

For viewing the logs produced in the 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

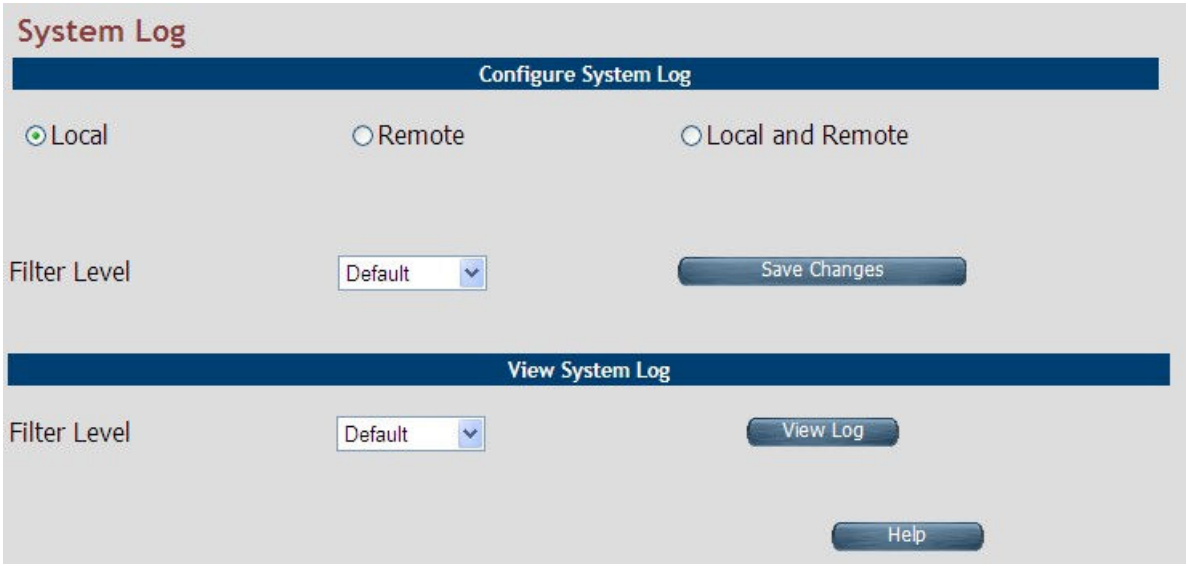


Figure 4.3.7 System Log

This page allows managing 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 "Local and Remote" option is selected, messages are logged locally in the system as well as to the remote server.

The events pertaining to the priority equal or higher to the selected level will be logged. "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 contains the following details: **Fields in System Log**

Field	Description
Configure System Log	Select the mode of log. The possible options are: ◆ **Local Mode:** The log text is displayed in web browser itself. ◆ **Remote Mode:** Specify the IP address and UDP port number for log transfer using syslog. ◆ **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. ◆ **Default:** The default pre-selected levels of logs are recorded. ◆ **Debug:** Debug and above levels of logs are recorded. ◆ **Info:** Informative and above level of logs are recorded. ◆ **Notice:** Notice type and above level of logs are recorded. ◆ **Warning:** Warning type and above levels of logs are recorded. ◆ **Error:** Error type and above levels of logs are recorded. ◆ **Critical:** Critical type and above levels of logs are recorded. ◆ **Alert:** Alert type and above level of logs are recorded. ◆ **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: ◆ **Default:** The default pre-selected levels of logs are viewed. ◆ **Debug:** Debug and above levels of logs are viewed. ◆ **Info:** Informative and above level of logs are viewed. ◆ **Notice:** Notice type and above level of logs are viewed. ◆ **Warning:** Warning type and above levels of logs are viewed. ◆ **Error:** Error type and above levels of logs are viewed. ◆ **Critical:** Critical type and above levels of logs are viewed. ◆ **Alert:** Alert type and above level of logs are viewed. ◆ **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 you 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.

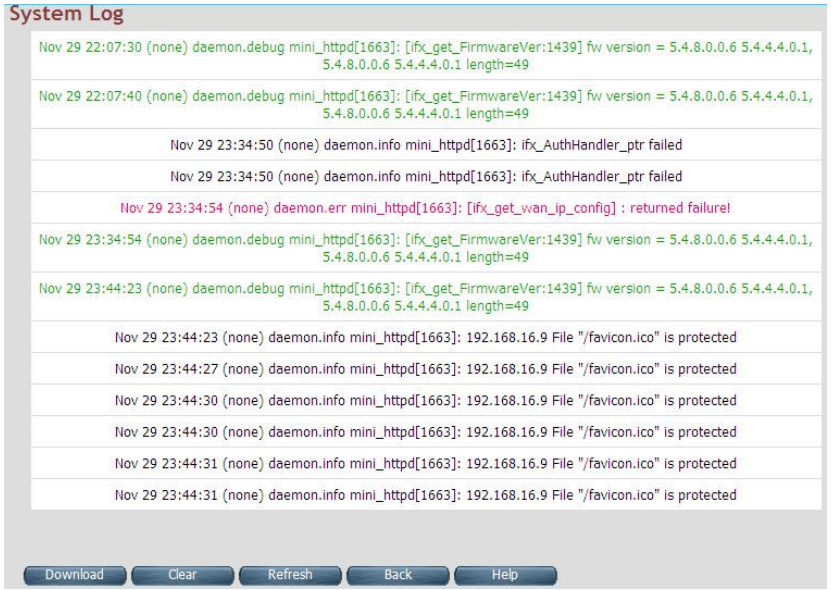


Figure 4.3.7.1 View System Log

For the ease of readability, the 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

For installing a 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

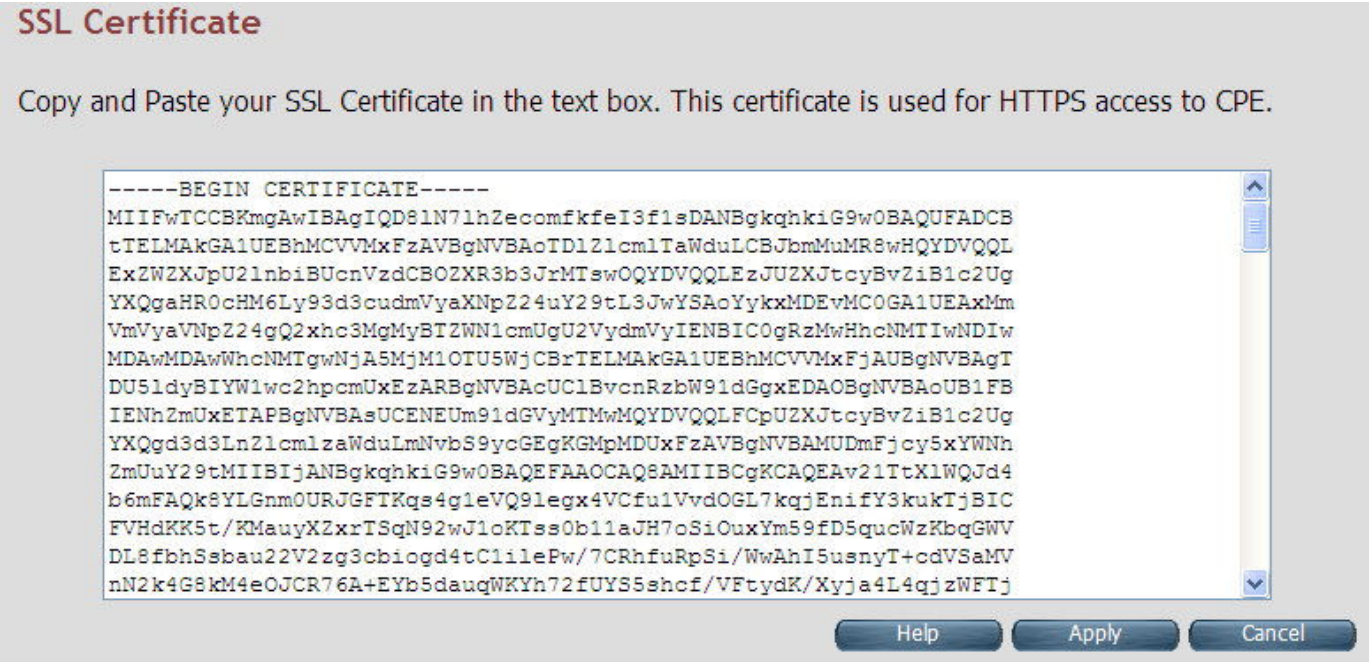


Figure 4.3.8 SSL Certificate

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

4.3.9 Reset

To reboot the system, click **Reset** link (**System > Reset**) on the left navigation bar. A screen is displayed as shown in Figure 4.3.9

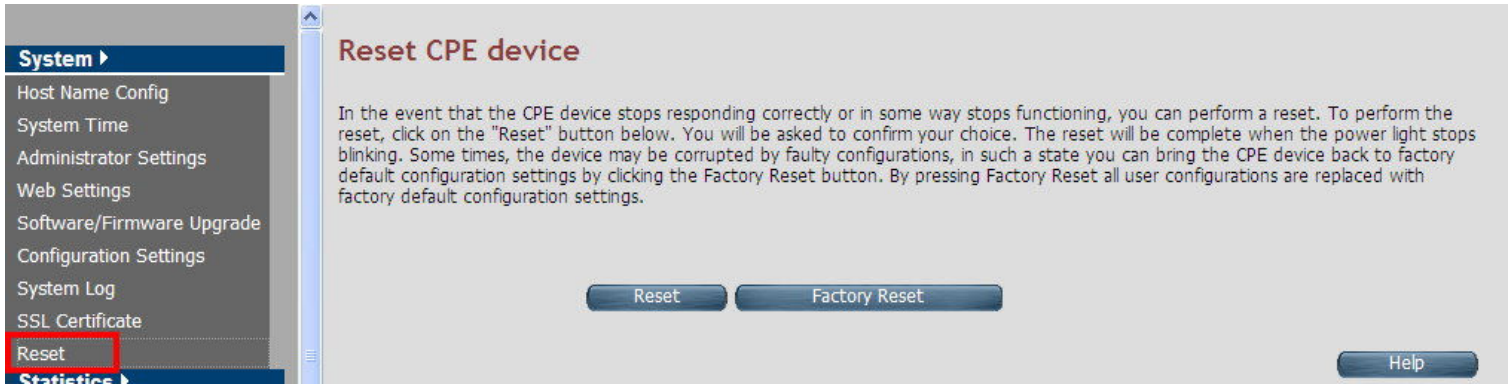


Figure 4.3.9 Reset

- Click Reset to reboot the system. This does not change the configurations existing in 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 4.3.9.1

Figure 4.3.9.1 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 in the left navigator bar

4.4.1 LAN

For viewing 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

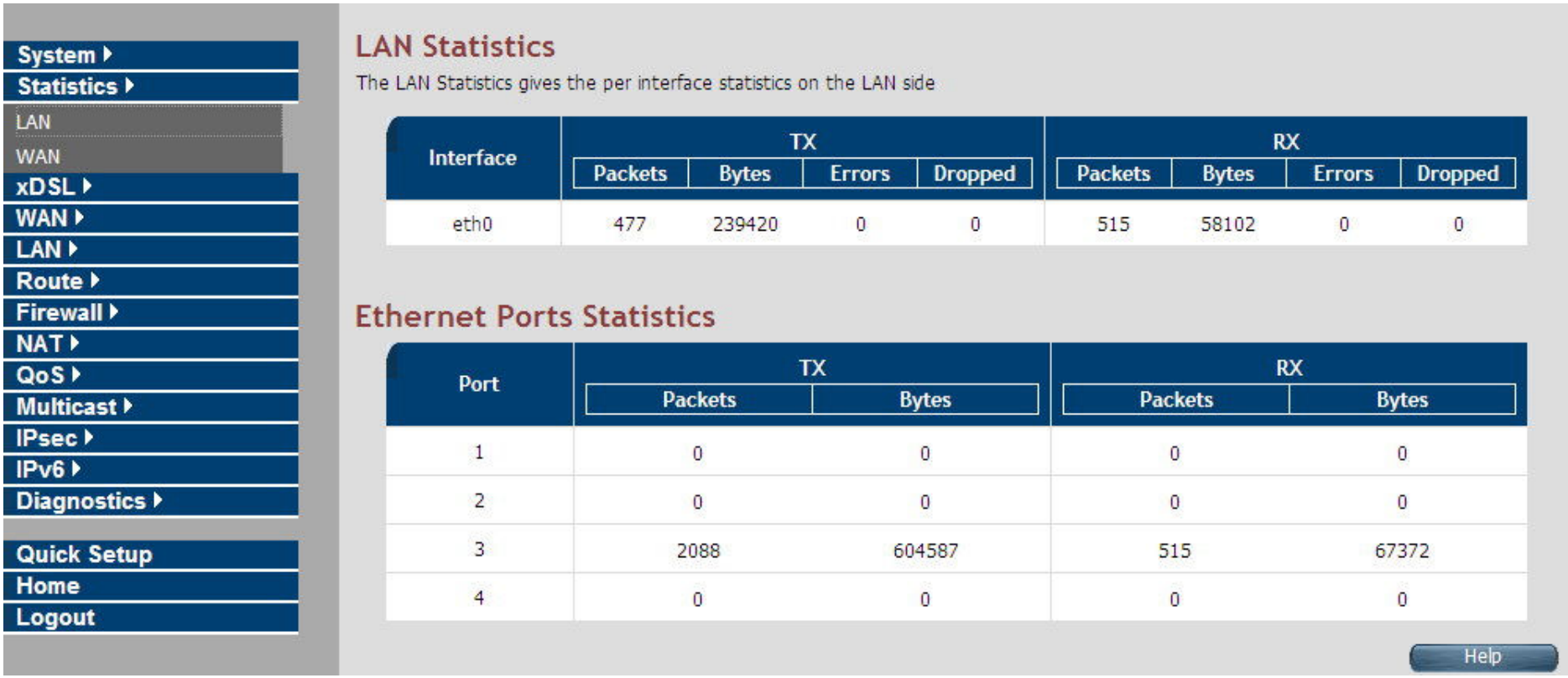


Figure 4.4.1 LAN Statistics

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: ◆ Total packets transmitted from this interface. ◆ Total bytes transmitted form this interface. ◆ Total Error packets on this interface. ◆ Total Dropped packets on this interface.
RX	Receive Counters: ◆ Total packets received from this interface. ◆ Total bytes received form this interface. ◆ Total Erroneous packets on this interface. ◆ Total Dropped packets on this interface.

4.4.2 WAN

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

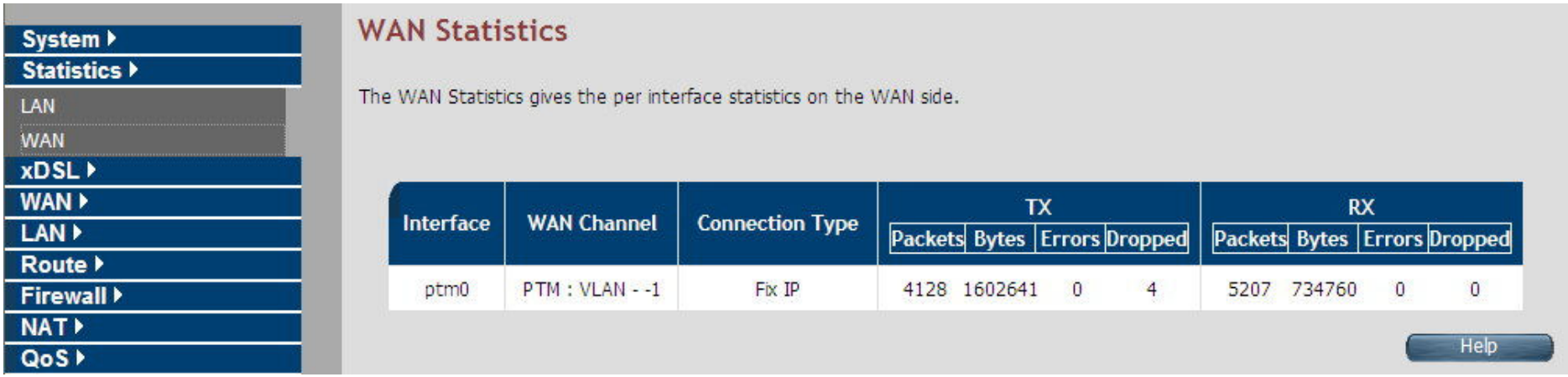


Figure 4.4.2 WAN Statistics

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: ◆ Total packets transmitted from this interface. ◆ Total bytes transmitted form this interface. ◆ Total Erroneous packets transmitted on this interface. ◆ Total Dropped packets transmitted on this interface.
RX	Receive Counters for WAN interface: ◆ Total packets received from this interface. ◆ Total bytes received form this interface. ◆ Total Erroneous packets received on this interface. ◆ Total Dropped packets on this interface.

4.5 Select "xDSL"

You 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.

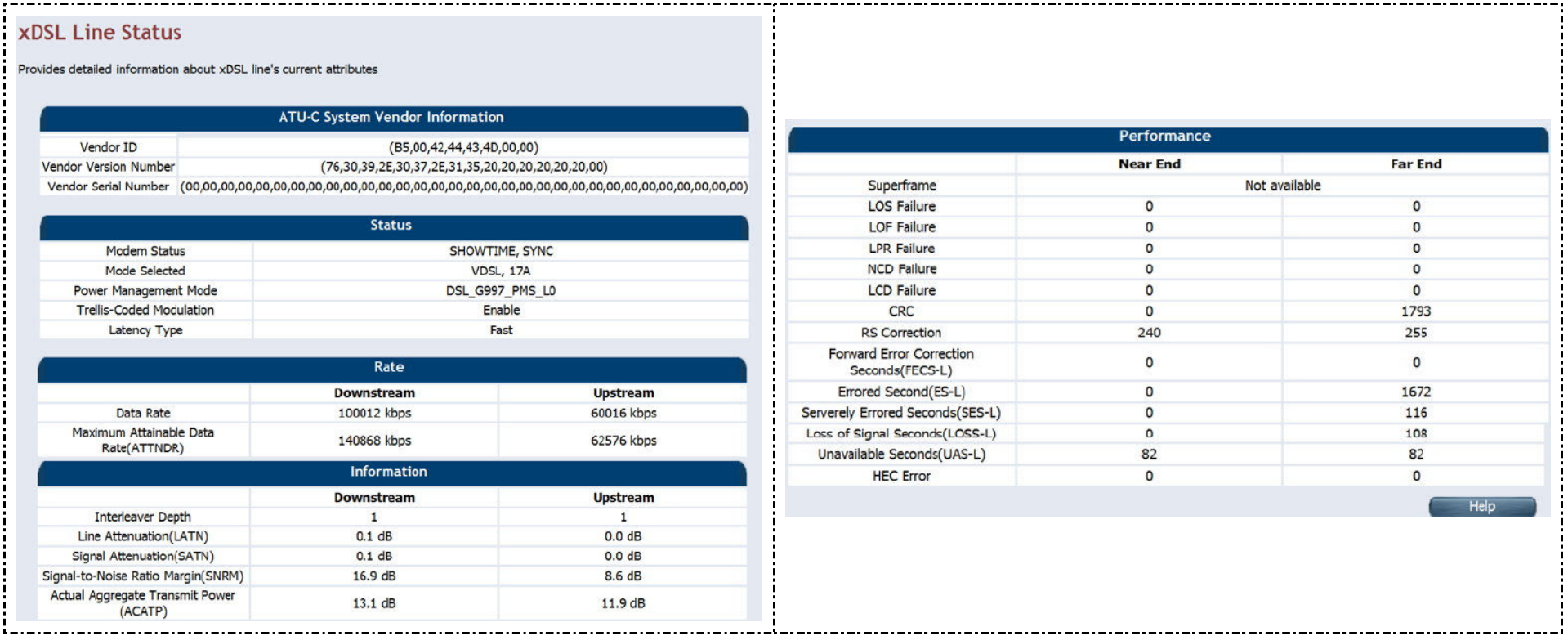
Figure 4.5 Select xDSL

Note:

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

4.5.1 xDSL Status

For viewing 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
Severely 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

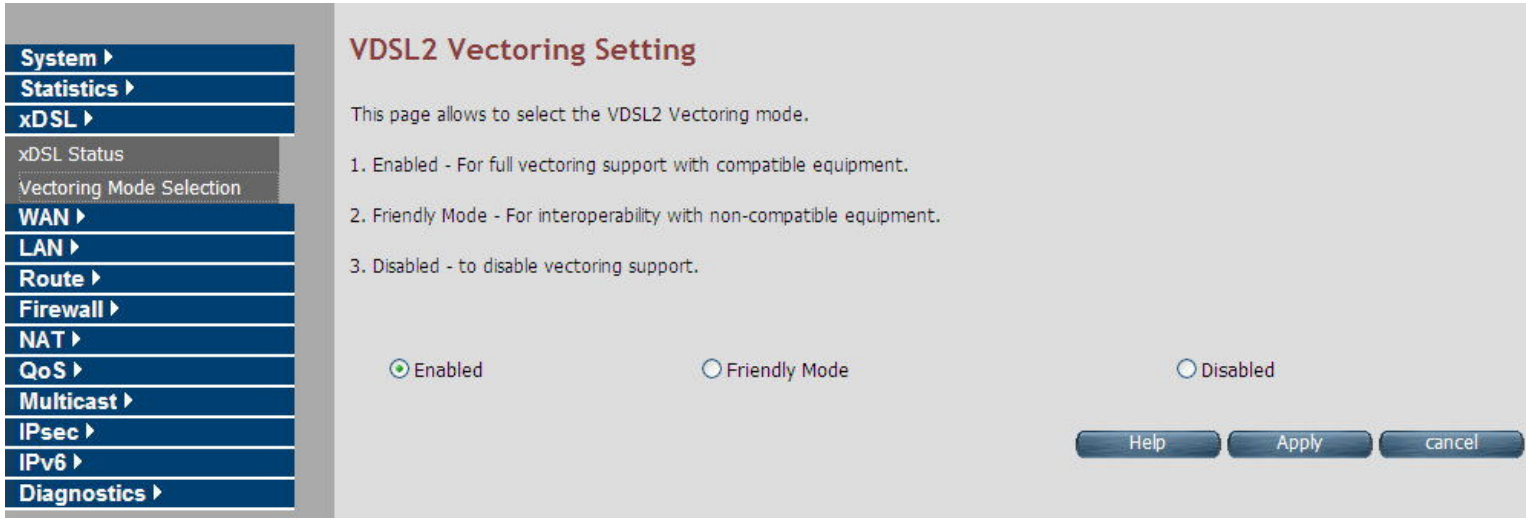
The screen contains the following details:

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-600W vdsl2 vectoring technology default setting is enabled.
2. If user would like to use vectoring technology, NV-600W and IP DSLAM both need support vectoring technology and need both enabled. NV-600W will auto follow the IP DSLAM vectoring technology to configure.
3. Vectoring technology does not support point to point applications.

About vectoring technology (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-cancellation 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"

You can view **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

For configuring 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

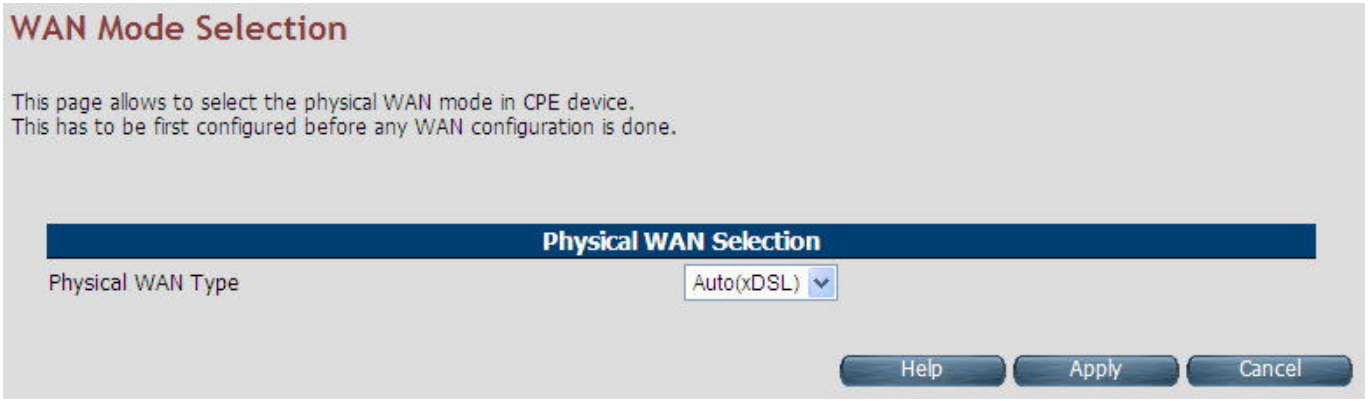


Figure 4.6.1 WAN Mode Setting (Selected Auto)

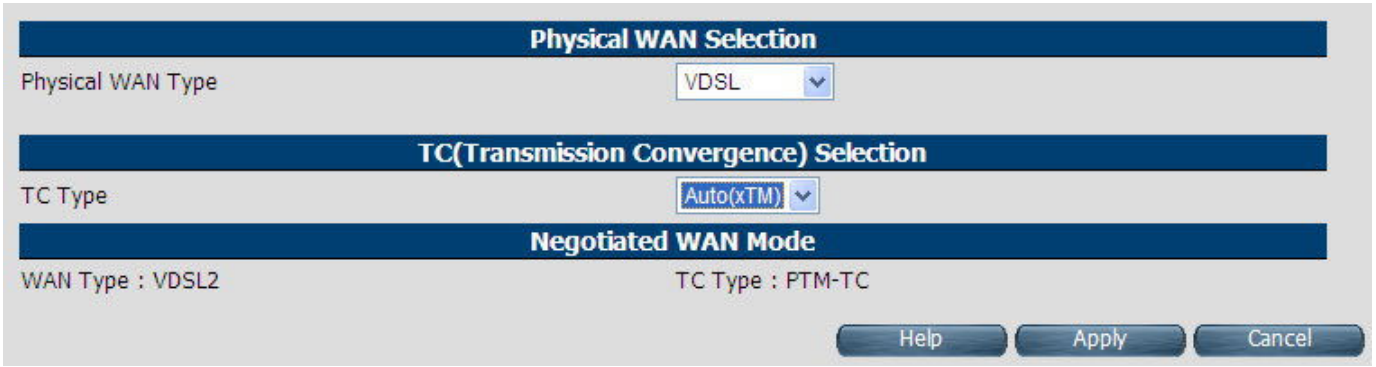


Figure 4.6.1.1 WAN Mode Setting (Selected ADSL2+ / VDSL2)

The screen contains 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.
Negotiated WAN Mode	
WAN Type	Show WAN type status
TC Type	Show TC type status

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

4.6.2 Auto Detect Setting

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

User has 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.

For configuring 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

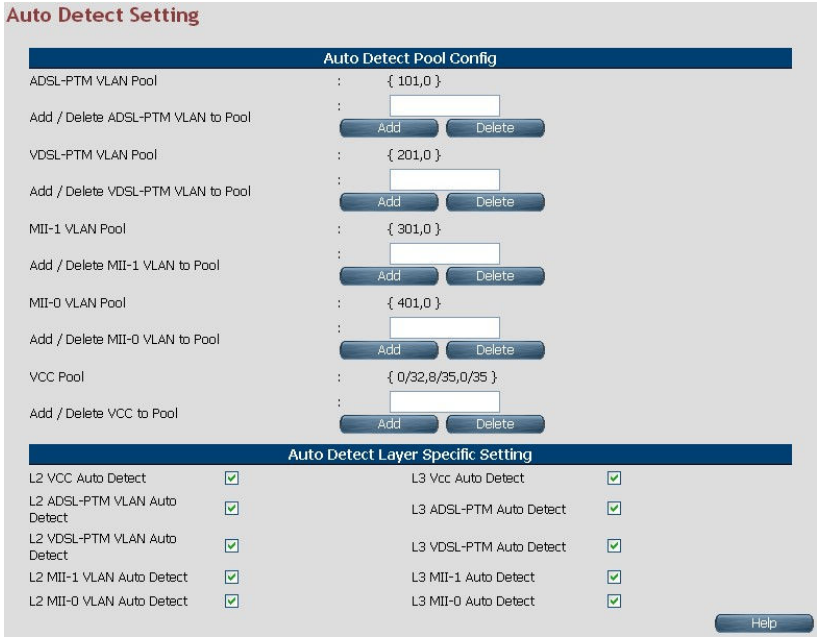


Figure 4.6.2 Port Mapping Configuration

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 auto-detect 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 auto-detect 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 Configuration

For configuring the **WAN Channel Configuration**, 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.

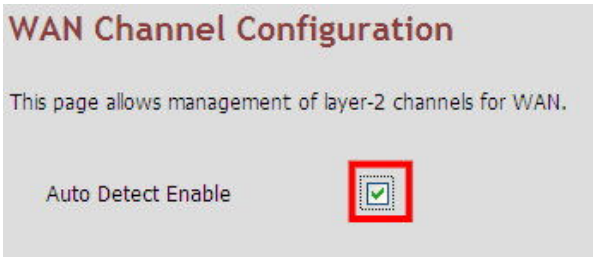


Figure 4.6.3

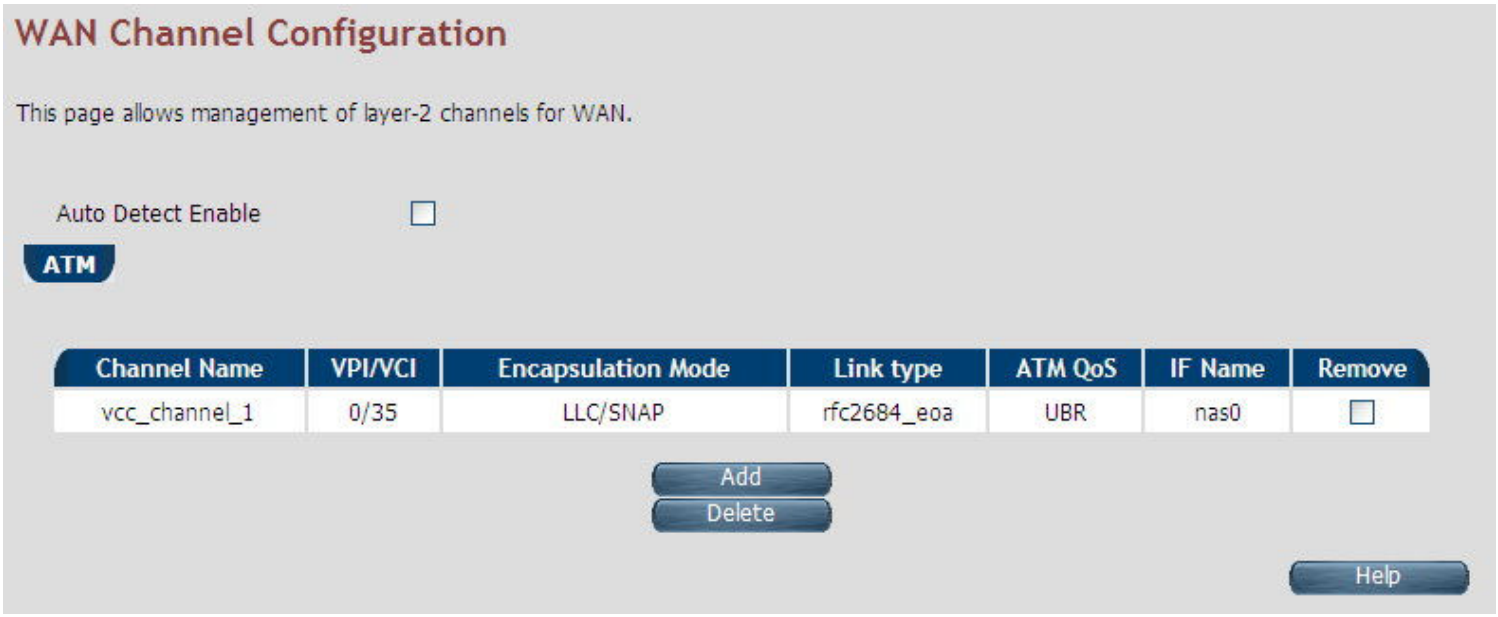


Figure 4.6.3.1 WAN Channel Configuration (Auto Detecting does not check the checkbox)

The screen contains the following details:

Fields in WAN Channel Configuration:

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

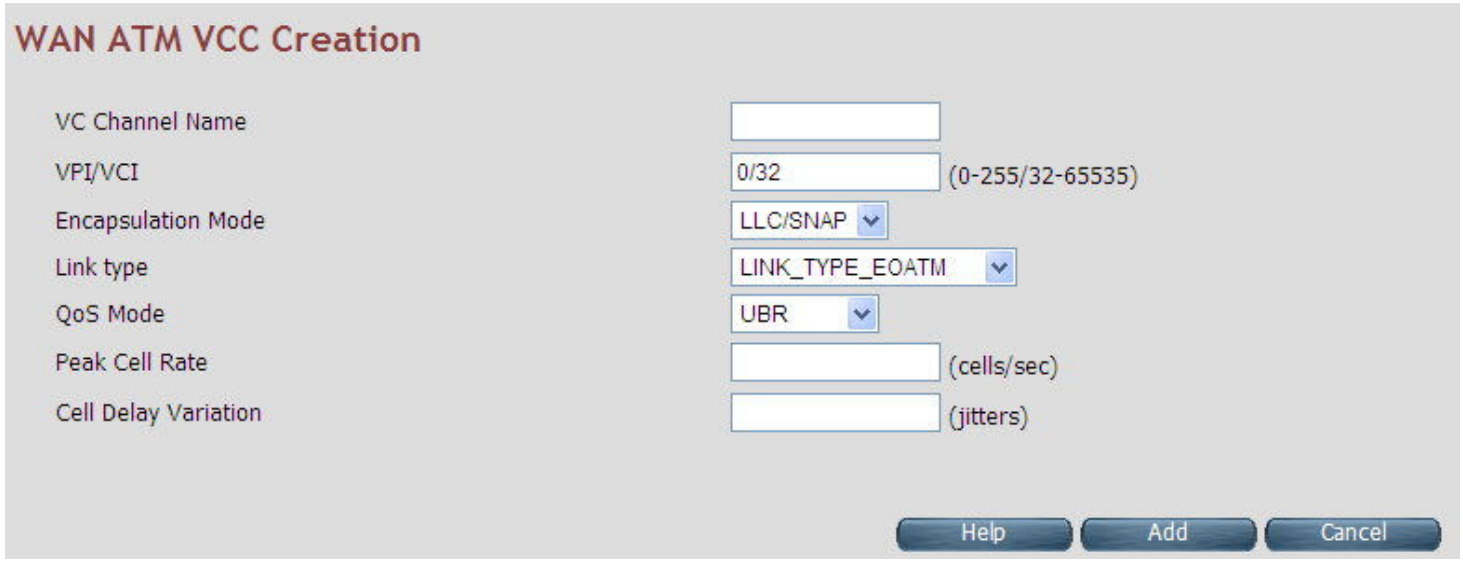


Figure 4.6.3.2 WAN Channel Configuration - ATM VCC Creation

The screen contains the following details:

Fields in WAN Channel Configuration:

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 specified in terms of jitters.

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

4.6.4 VLAN Channel Configuration

For configuring the **VLAN Channel Configuration**, 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

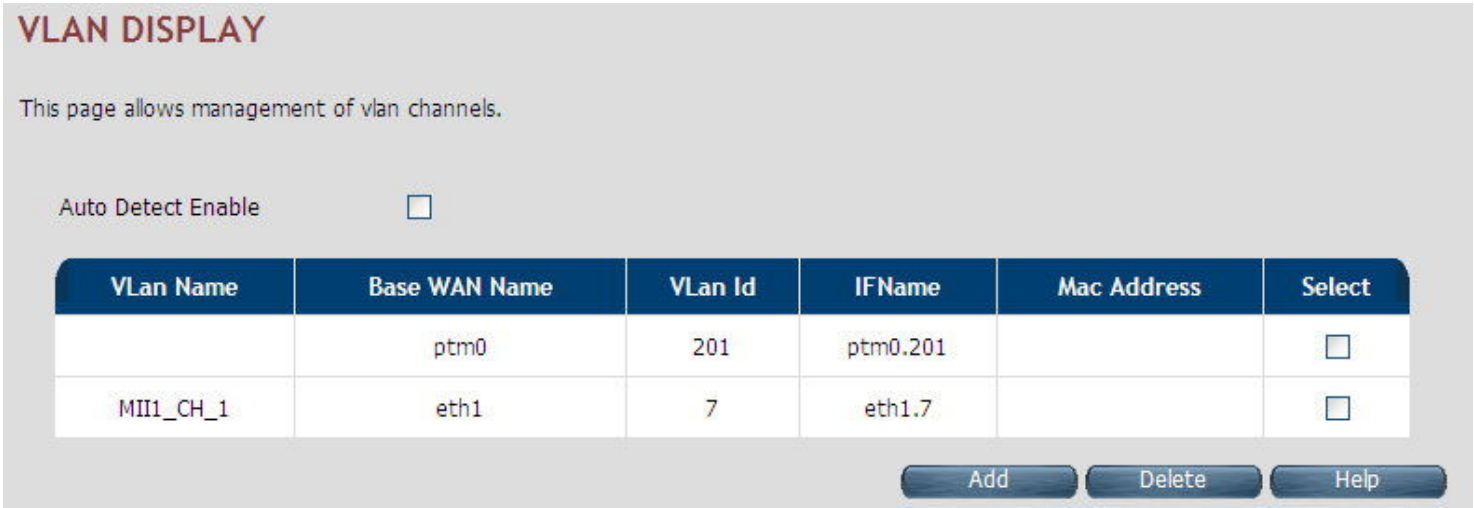


Figure 4.6.4.1 VLAN Channel Configuration Display (Auto Detecting does not check the checkbox)

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 7- 4095. VLAN Identifiers (1 - 6) are internally used in system for special purpose and are not available to user for configuration.
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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

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

Figure 4.6.4.2 VLAN Channel Configuration - 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 system for special purpose and are not available to user 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 user for configuration.

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

4.6.5 WAN Setting

For configuring 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.

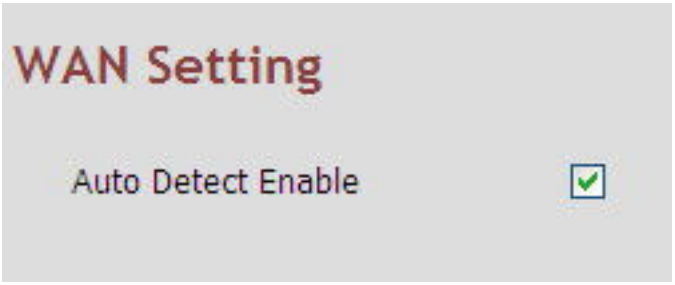


Figure 4.6.5 WAN Setting - Auto Detect Enable

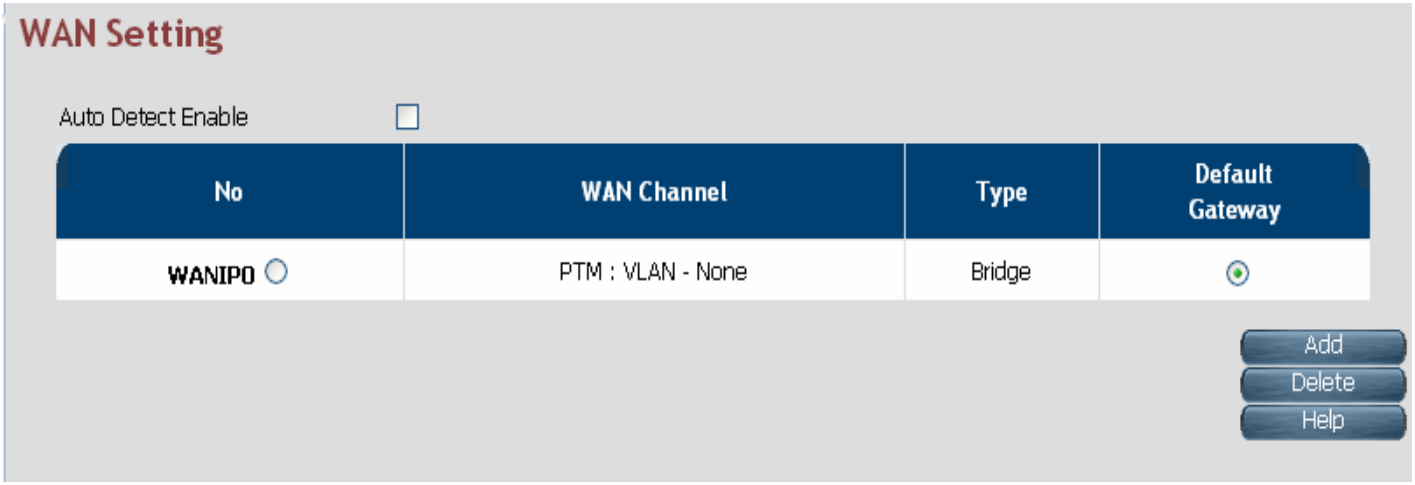


Figure 4.6.5.1 WAN Setting

The NV-600W can support up to a maximum of 16 WAN connections in system. When 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 selecting 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 contains 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 type of WAN such as PPPoE or DHCP or Bridged etc.
Default VoIP Interface	This option is present only in IAD models, where VoIP is supported. This is the default interface for VoIP packets.
Default Gateway	This option allows configuring default route in system. The chosen WAN will be used for default route.

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

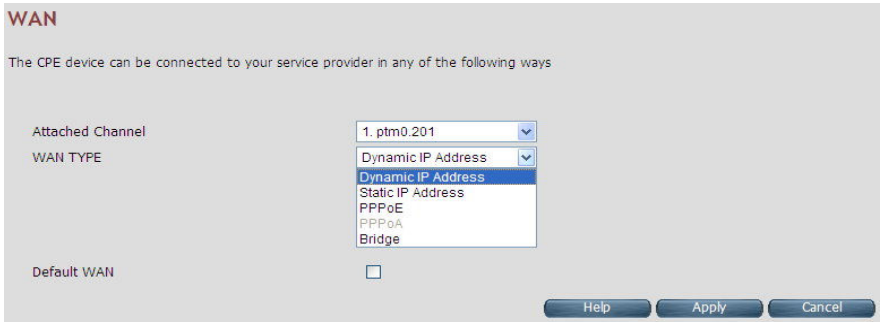


Figure 4.6.5.2 WAN Settings – Apply – Step1

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 your IP Address from your service provider (means NV-600W is DHCP client on WAN) click **Apply**.
Static IP Address	To enter the WAN interface IP Address of NV-600W 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 you 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

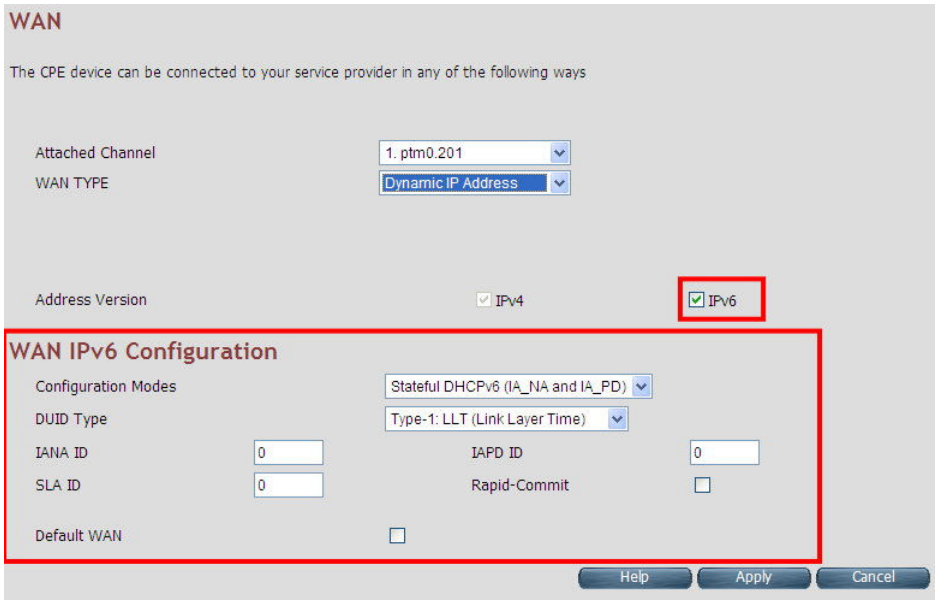


Figure 4.6.5.3 Dynamic IP Address

Please Enable IPv6 to set the WAN IPv6 Configuration. Select 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

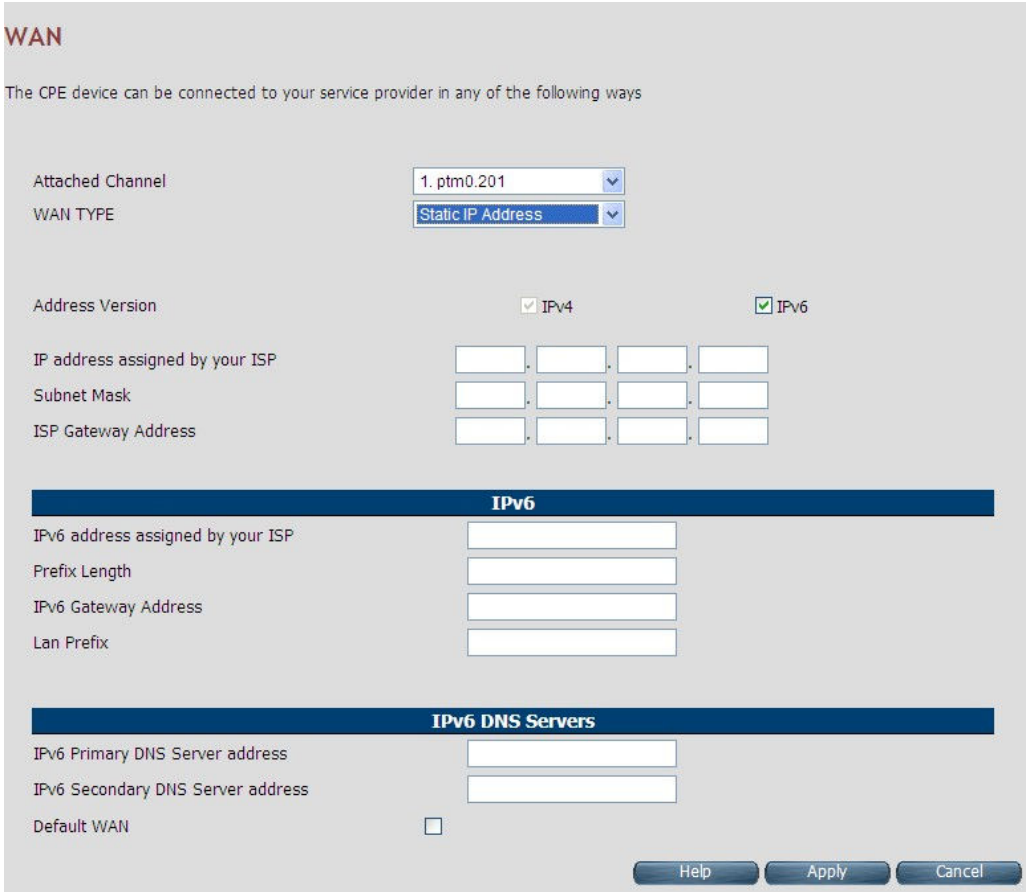


Figure 4.6.5.4 WAN Static IP

The screen contains the following details:

Fields in Static IP:

Field	Description
Address Version	
IP address assigned by your ISP	To specify the IP Address of NV-600W CPE's WAN link.
Subnet Mask	To specify the Subnet Mask of NV-600W CPE's WAN link.
ISP Gateway Address	To specify the Gateway address of the NV-600W CPE's WAN.
IPv6	
IPv6 address assigned by your 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 configuring default route for relevant WAN mode of this WAN connection.

- Click **Apply** at any time during configuration to save the information that you 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

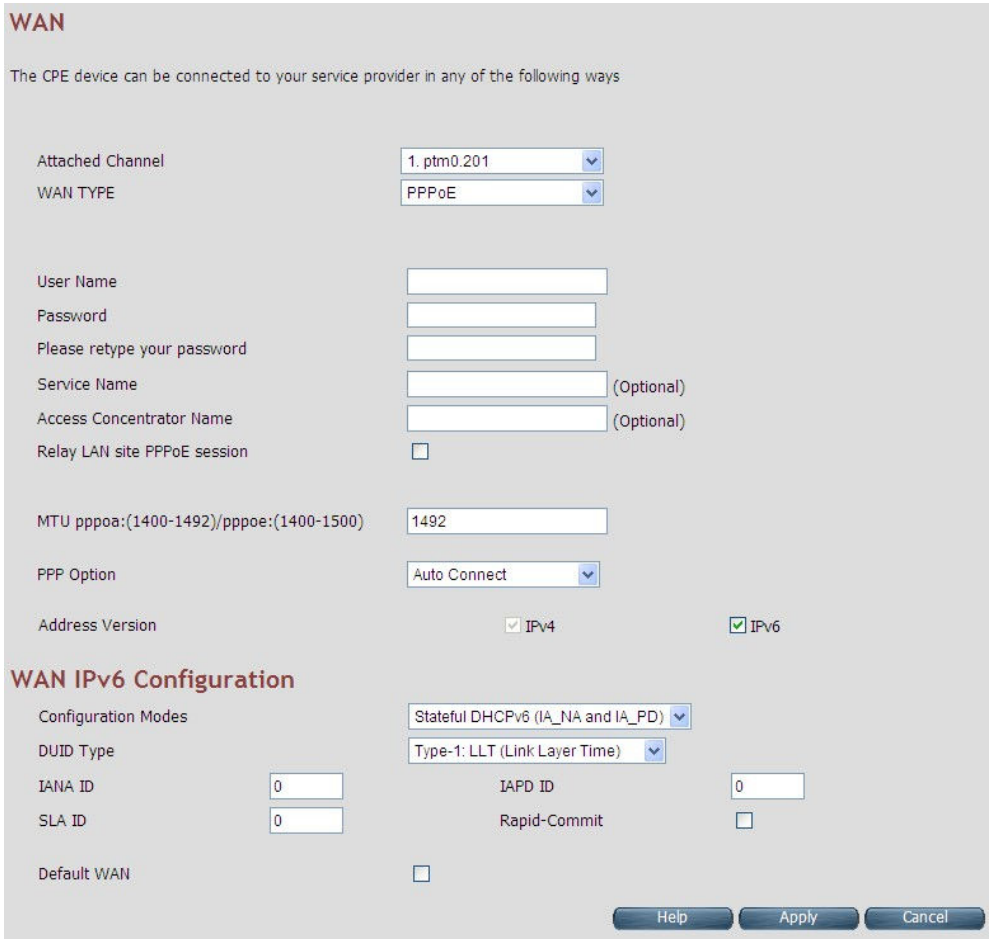


Figure 4.6.5.5 WAN PPPoE creation

The screen contains the following details:

Fields in PPPoE WAN:

Field	Description
User Name	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 your 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 enable/disable a PPPoE relay session. PPPoE relay also called PPPoE Passthrough.
PPP Option	Choose the option form 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 to select following modes of IPv6 configuration: ◆ Stateful DHCPv6(IA_NA and IA_PD) ◆ SLAAC (Address Configuration) with DHCPv6 (IA_PD)
DUID Type	This option allows to configure different DUID (DHCP Unique Identifier) types: ◆ "Type-1: LLT (Link Layer Time) ◆ "Type-2: EN (Enterprise Number) ◆ "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 has to be configured when Stateful DHCPv6 configuration mode is selected.
IAPD ID	IAPD options represent one or more IPv6 prefix and parameters related to it. IAPD is the Identity Association for Prefix Delegation. This identifier needs to be configured in both Stateful DHCPv6 and 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 DHCPv-server to perform a Rapid Commit. Handshaking will happen with two DHCPv6 messages.
Default WAN	This option allows configuring default route for relevant WAN mode of this WAN connection.

- Click **Apply** at any time during configuration to save the information that you 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
User Name	To enter the username to be used in the PPPoA session.
Password	To enter the corresponding password for the specified username.
Please retype your password	To enter the password again to reconfirm.
Dial on Demand	This feature allows the device to automatically re-connect to the service provider if 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-600W.

Fields in PPPoA WAN IPv6 Configuration:

Field	Description
Configuration Modes	This option allows to select following modes of IPv6 configuration: ◆ Stateful DHCPv6(IA_NA and IA_PD) ◆ SLAAC (Address Configuration) with DHCPv6 (IA_PD)
DUID Type	This option allows to configure different DUID (DHCP Unique Identifier) types: ◆ "Type-1: LLT (Link Layer Time) ◆ "Type-2: EN (Enterprise Number) ◆ "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 has to be configured when Stateful DHCPv6 configuration mode is selected.
IAPD ID	IAPD options represent one or more IPv6 prefix 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 DHCPv-server to perform a Rapid Commit. Handshaking will happen with two DHCPv6 messages.
Default WAN	This option allows configuring default route for relevant WAN mode of this WAN connection.

◆ Click **Apply** at any time during configuration to save the information that you 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 **Apply**. A screen is displayed as shown in Figure 4.6.5.7

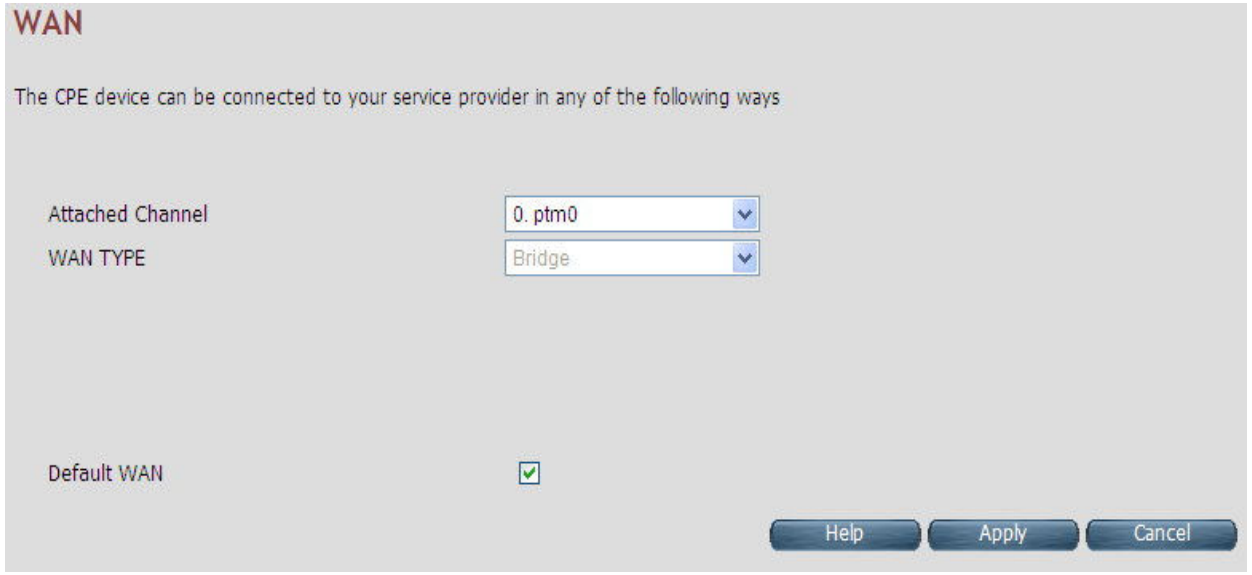


Figure 4.6.5.7 Bridge WAN Setting

The screen contains the following details:

Fields in Bridge Configuration:

Field	Description
Default WAN	This option allows configuring default route for relevant WAN mode of this WAN connection.

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

4.6.5.6 Delete

This option allows deleting 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

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

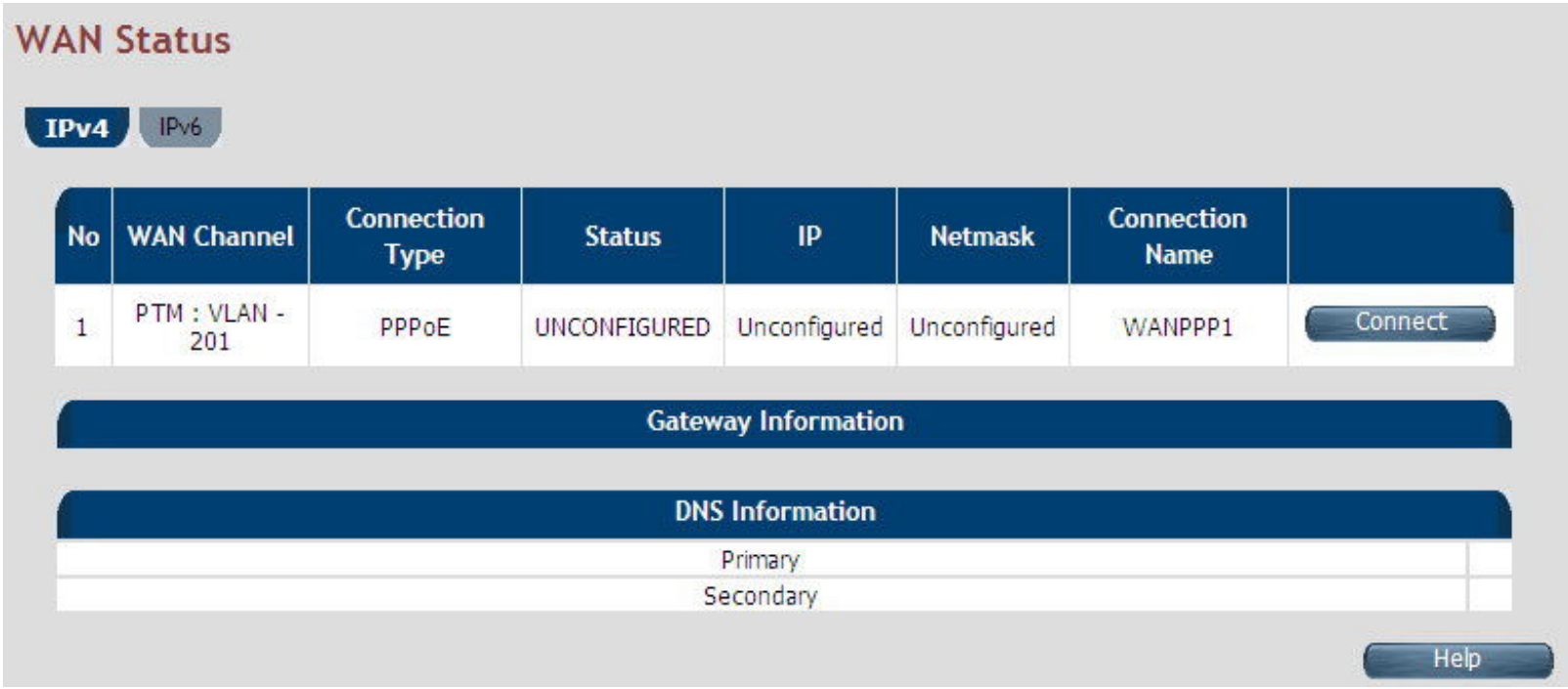


Figure 4.6.6 WAN Status

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 the connection mode in which NV-600W 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 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 establish PPP link.
Disconnect	This button 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 renew 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 you click on the IPv6 tab in the WAN Status page, a screen is displayed as shown in Figure 4.6.6.1

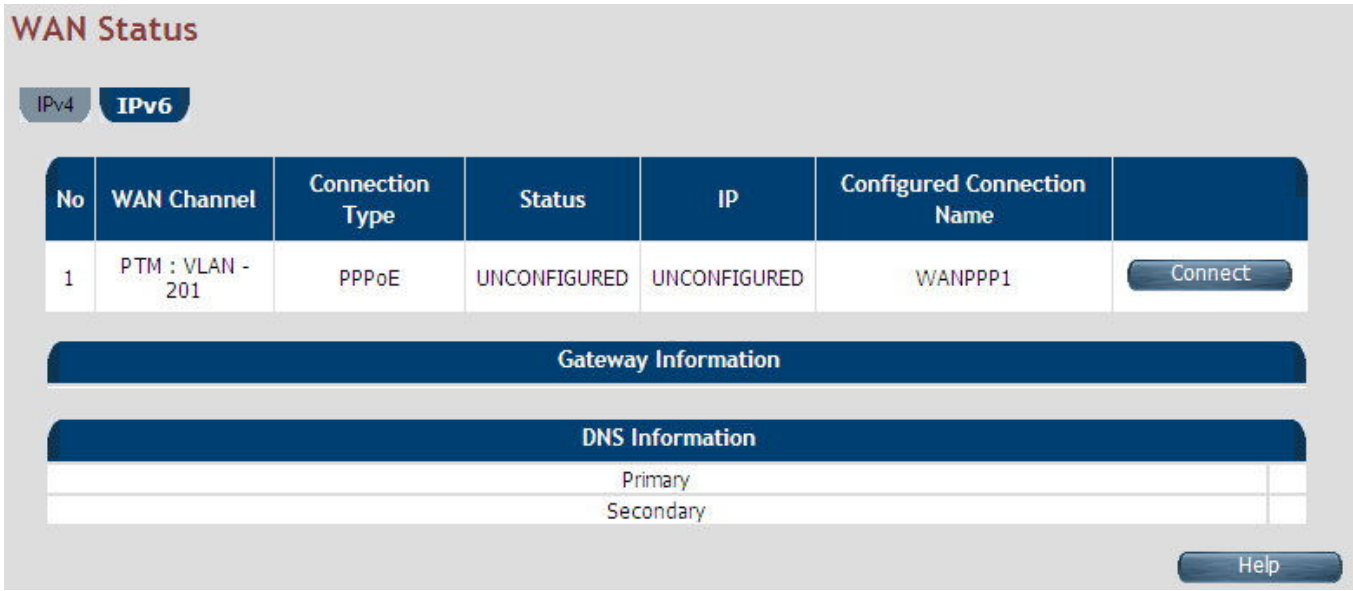


Figure 4.6.6.1 WAN Status IPv6 Tab

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

- For enabling IPv6 function, click the **IPv6 setting** link (**IPv6 > IPv6 setting**) on the left navigation bar.

4.6.7 DNS

For configuring 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.

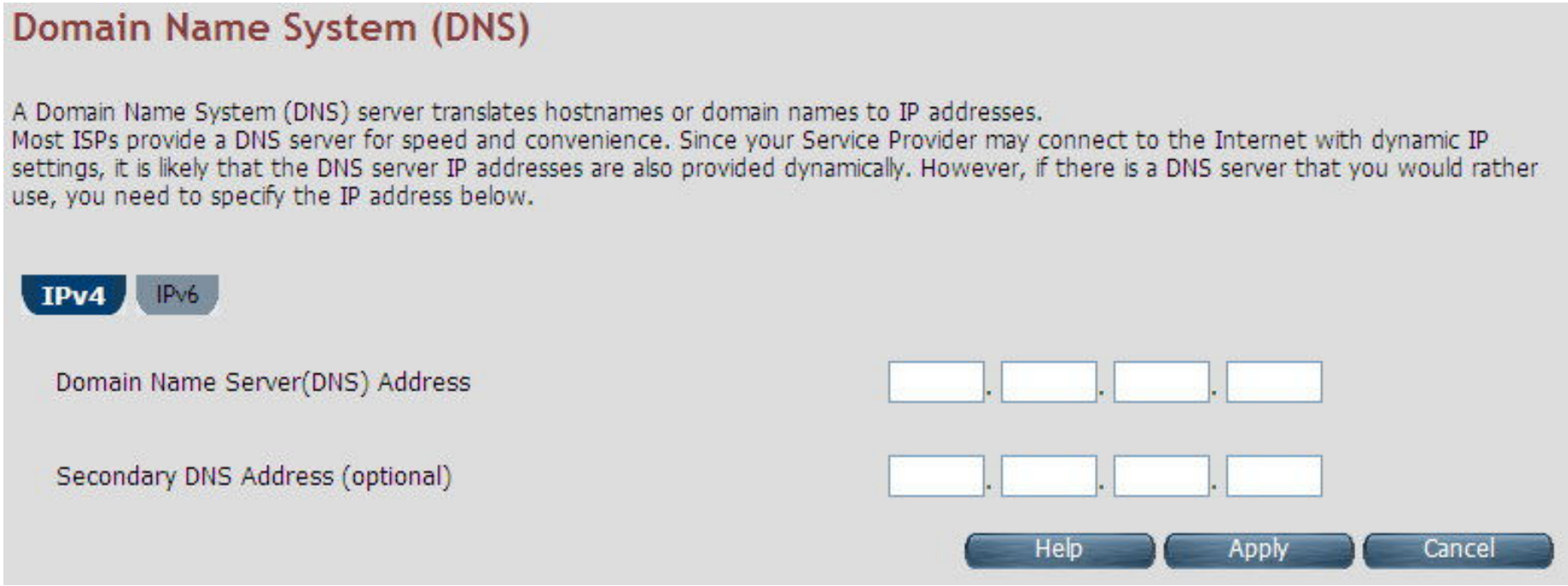


Figure 4.6.7 DNS Configuration

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.
- For enabling IPv6 function, click the **IPv6 setting** link (**IPv6 > IPv6 setting**) on the left navigation bar.

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-600W 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 registered 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

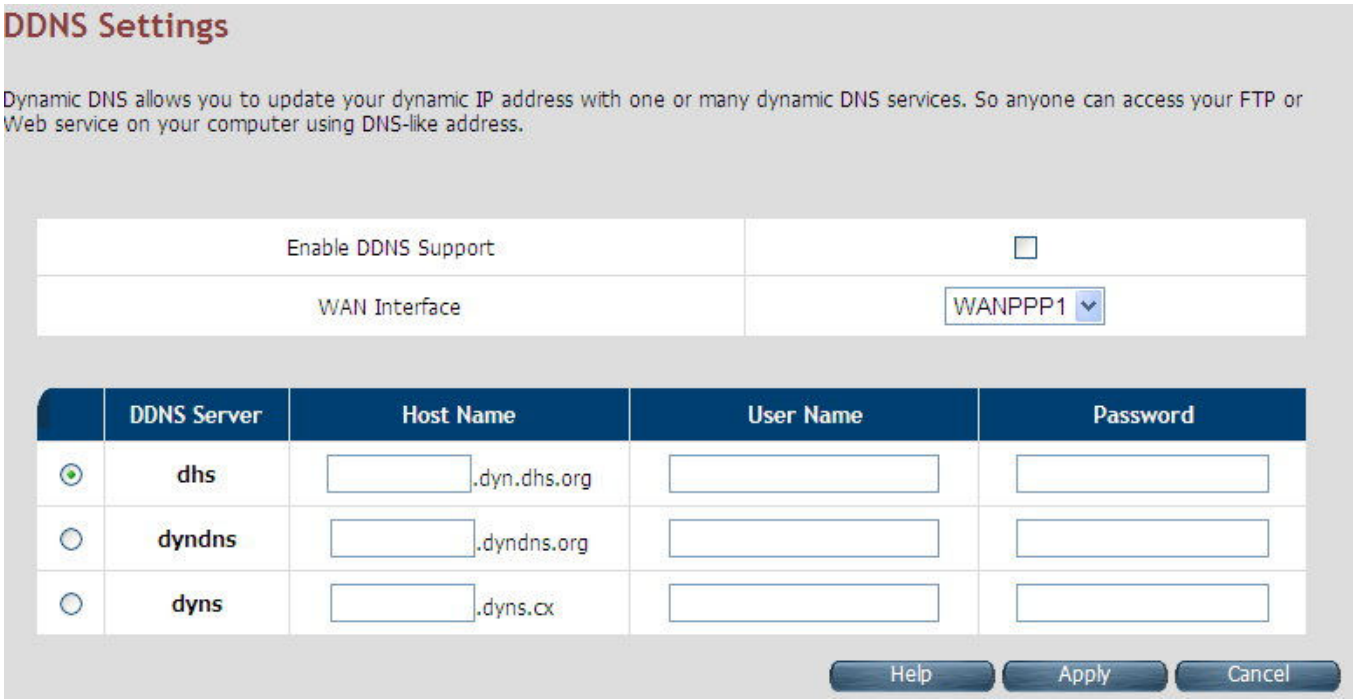


Figure 4.6.8 DDNS Settings

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 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.
User Name	Registered user name 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. For configuring 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

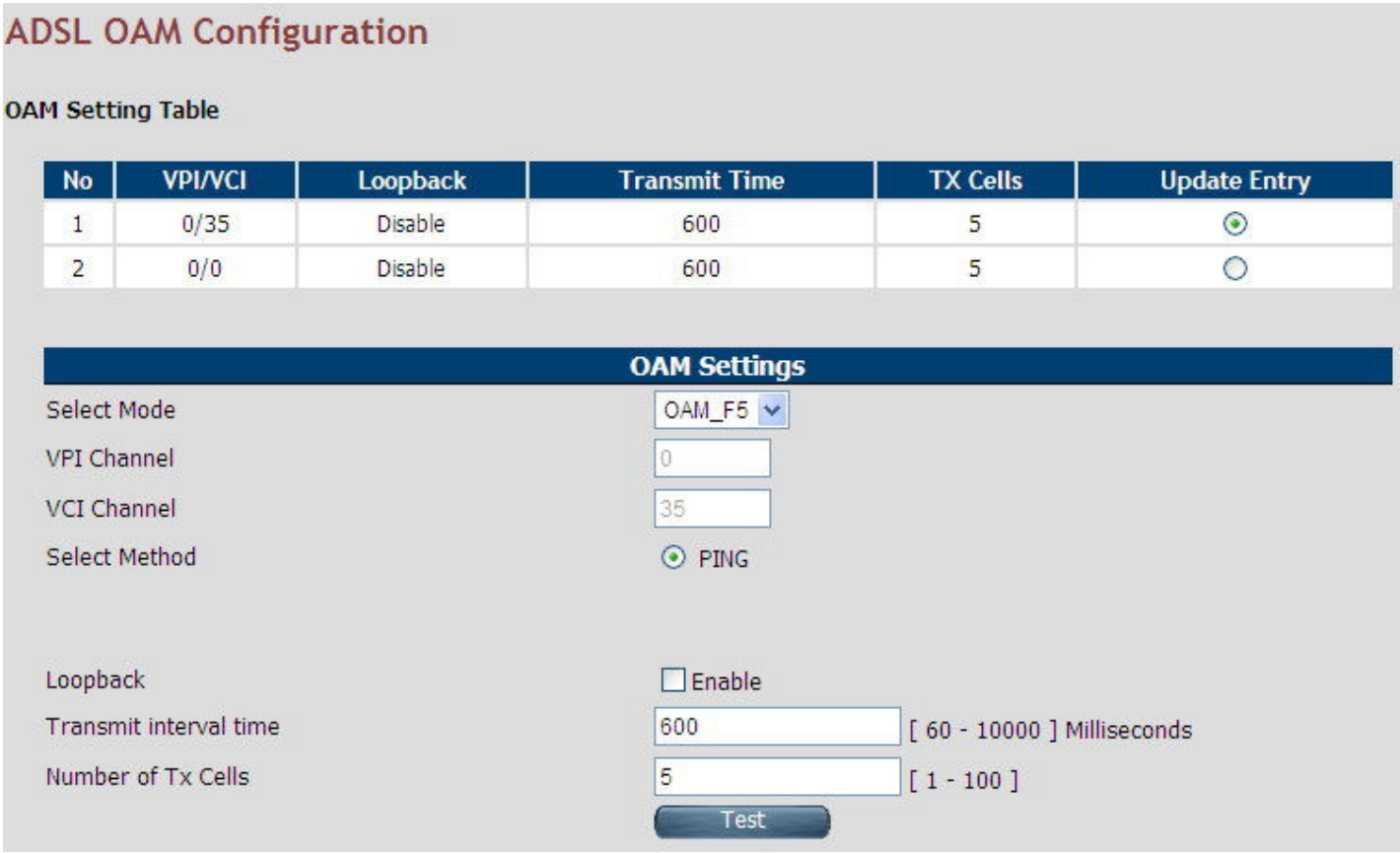


Figure 4.6.9 ADSL OAM F5 Test

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 following OAM parameters information: ◆ No: Number ◆ VPI: Virtual Path Identifier ◆ VCI: Virtual Connection Identifier ◆ Loopback: Enabled or Disabled ◆ Transmit Time: actual value in milliseconds ◆ Tx Cells: No of cells to be transmitted ◆ 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 you 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.

Figure 4.6.9.1 Test Successful

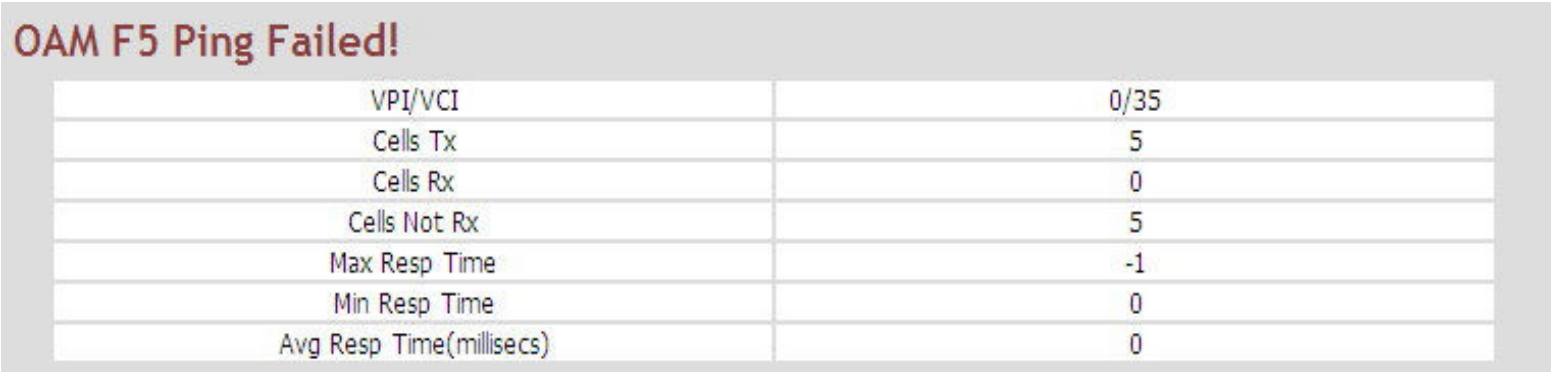


Figure 4.6.9.2 Test Failed

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 (millisecs)	Displays the average response time in milliseconds.

4.7 Select "LAN"

For setting the IP address, connect the NV-600W to a new control PC and access the web user interface, click on "LAN Settings". You 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** and **LAN Port Status**. A screen is displayed as shown in Figure 4.7.

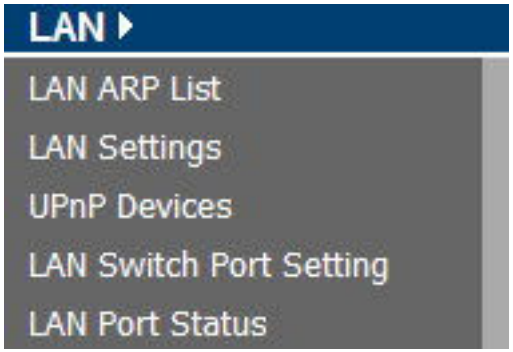


Figure 4.7 LAN options

4.7.1 LAN ARP List

For viewing the ARP entry 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 connected to the CPE.

4.7.2 LAN Settings

For configuring 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.

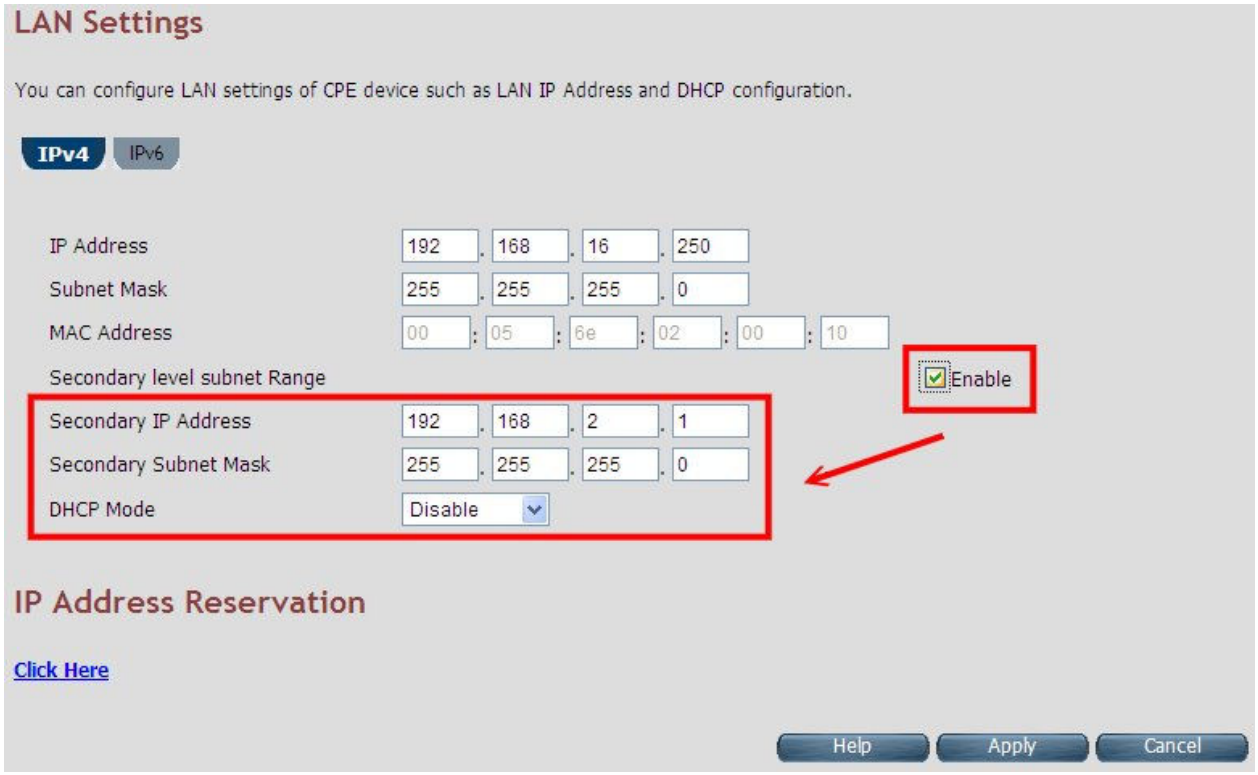


Figure 4.7.2 LAN Settings – DHCP Server

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-600W. 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 is shown, to which the DHCP requests are relayed.

Field	Description
DHCP Server	
IP Pool Starting Address	DHCPv4 pool starting IPv4 address.
IP Pool Ending Address	DHCPv4 pool end 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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

When you 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.

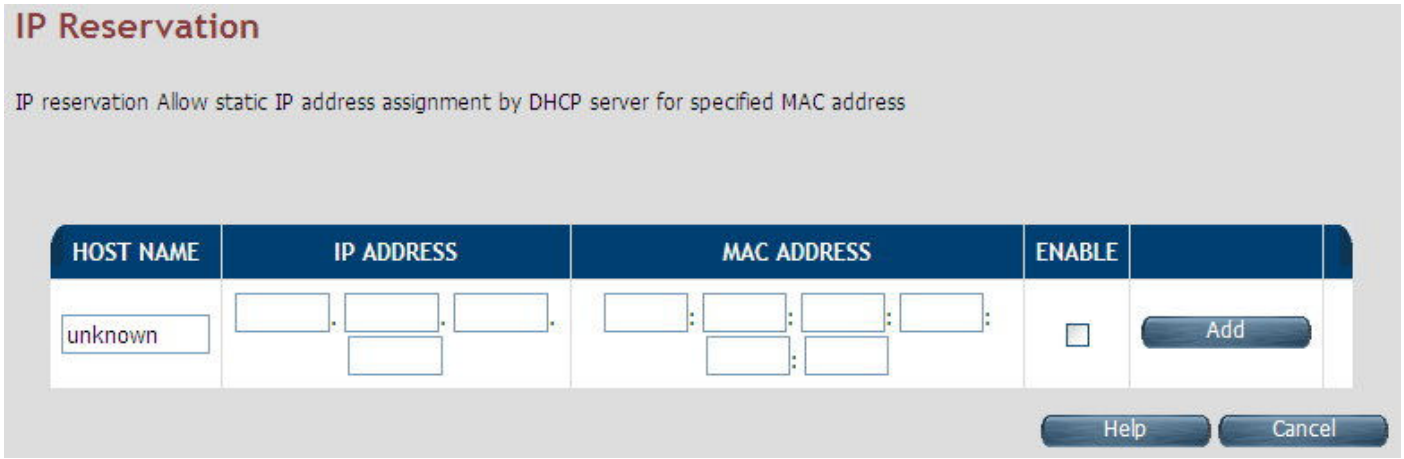


Figure 4.7.2.1 IP Reservation

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 you 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.

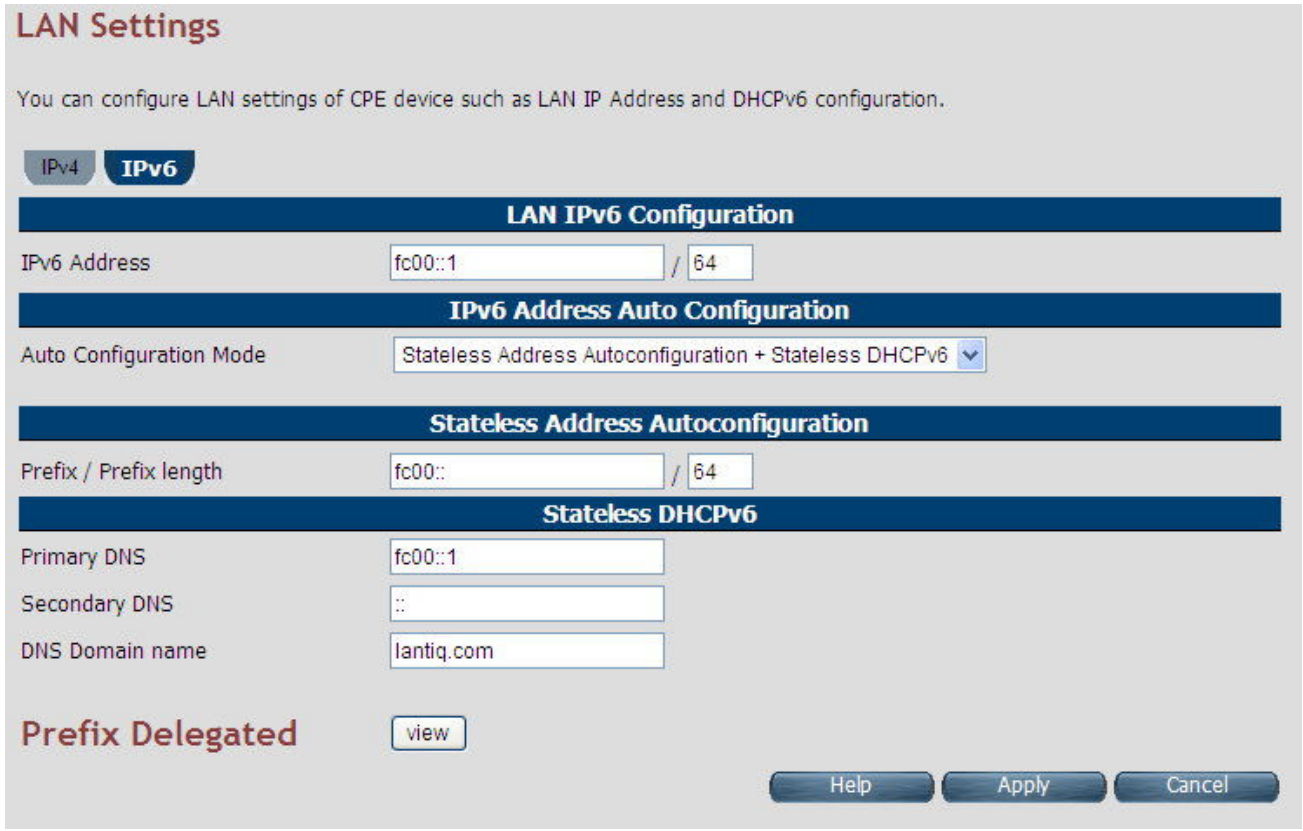


Figure 4.7.2.2 LAN Settings - IPv6 Tab (Option 1: SLAAC + Stateless DHCPv6)

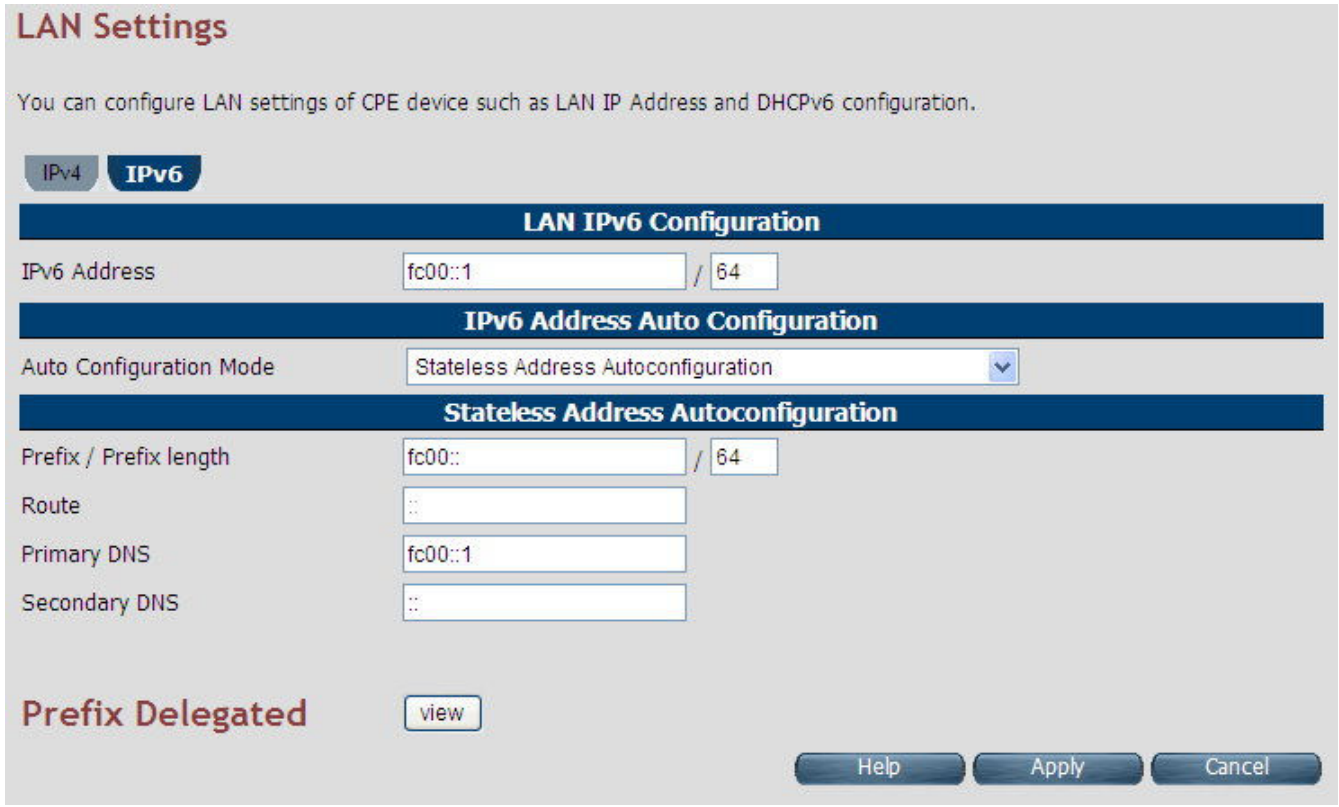


Figure 4.7.2.3 LAN Settings - IPv6 Tab (Option 2: SLAAC)

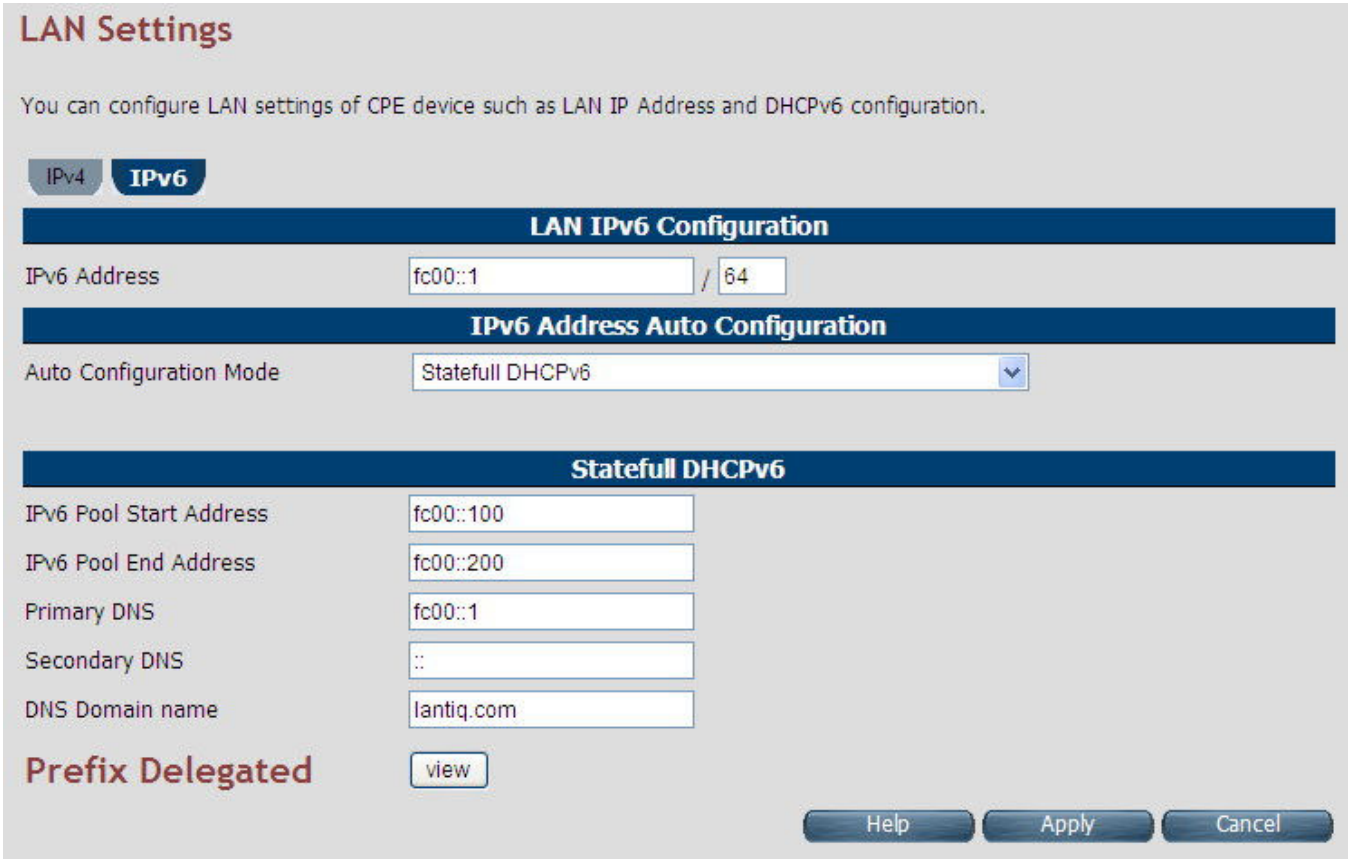


Figure 4.7.2.4 LAN Settings - IPv6 Tab (Option 3: Statefull DHCPv6 Server)

For LAN interface, the NV-600W 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 Auto configuration	
Auto Configuration Mode	Auto Configuration Mode on LAN interface for LAN hosts. • Stateless Auto Config (SLAAC) + Statefull DHCPv6 • Stateless Auto Config (SLAAC) • Statefull DHCPv6 **Stateless Address Auto configuration**
Stateless Address Auto configuration	
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.
Statefull 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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

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

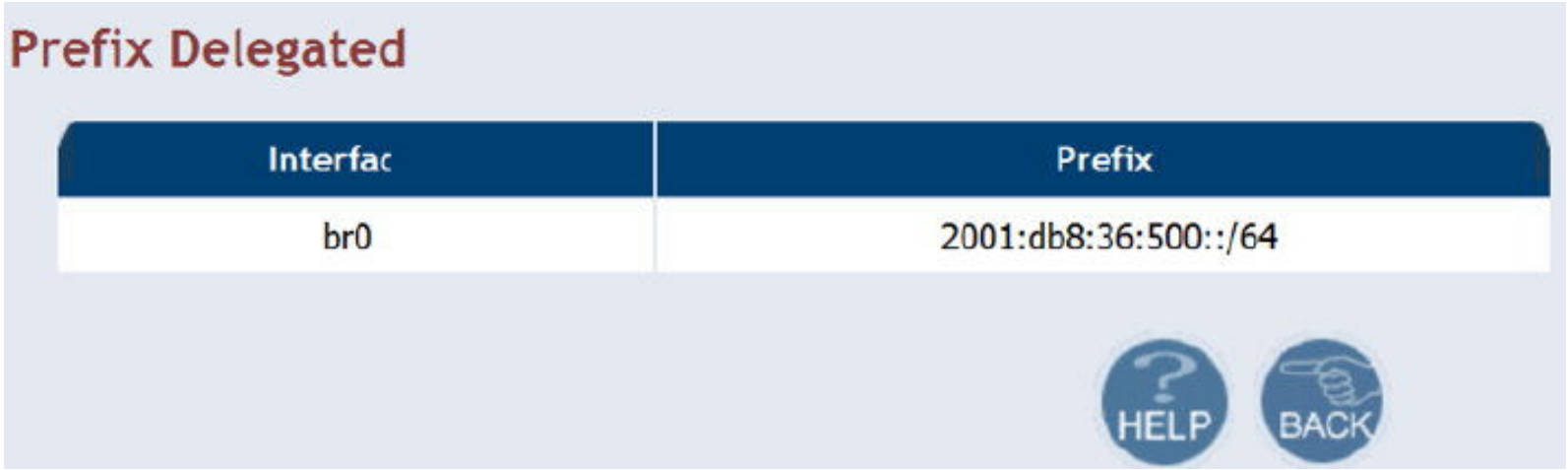


Figure 4.7.2.5 Prefix Delegated view

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

4.7.3 UPnP Devices List

For discovering the UPnP Devices in LAN network, click the **UPnP Devices** link (**LAN** > **UPnP Devices**) on the left navigation bar. 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

For discovering 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

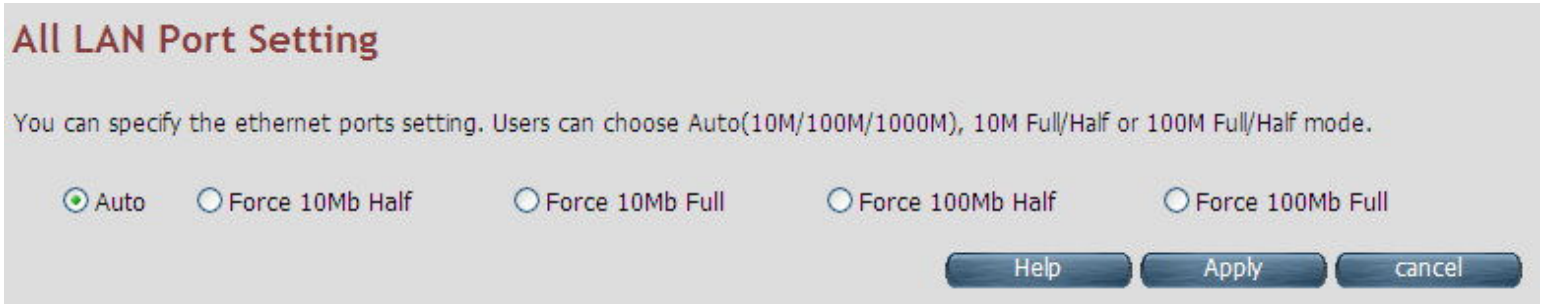


Figure 4.7.4 All LAN Port Setting

- 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

For viewing 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

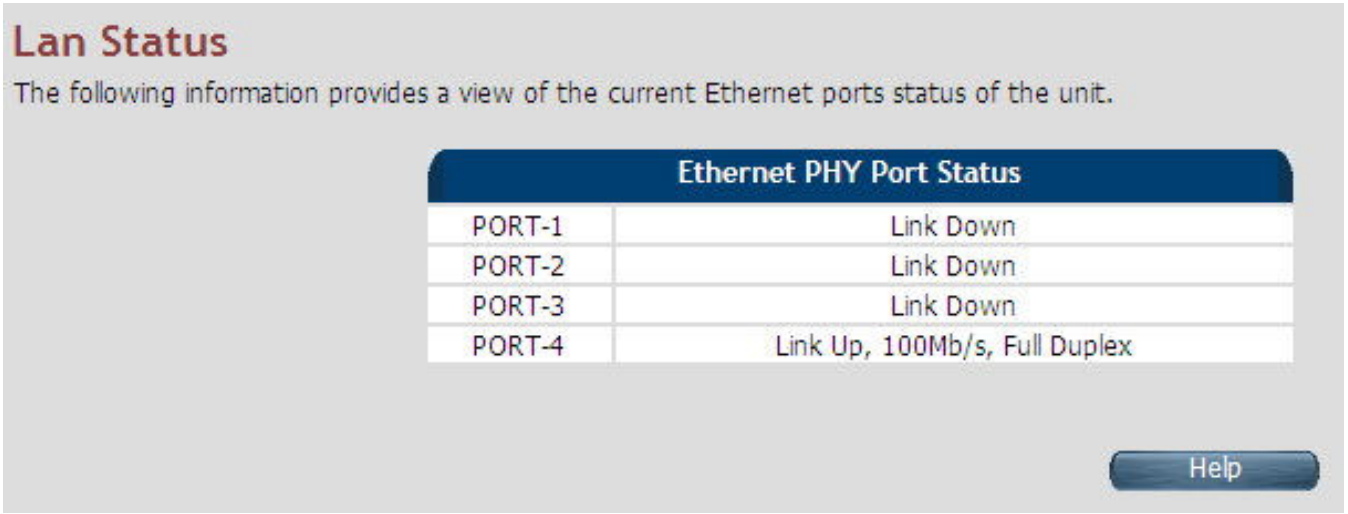


Figure 4.7.4 LAN Port Status

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 Full	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

4.7.6 VLAN Settings

To discover the Port-based VLAN Settings in LAN network, click the **VLAN Settings** link (**LAN** > **VLAN Settings**) on the left navigation bar. The Port Base Vlan settings default value is independent of each port. A screen is displayed as shown in Figure 4.7.6

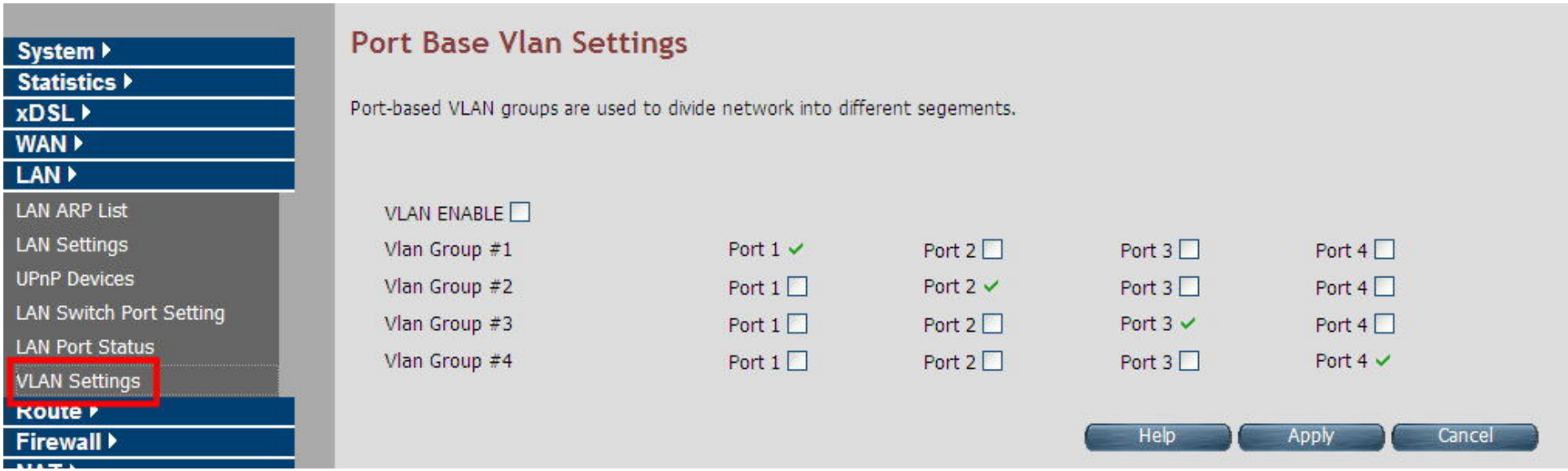
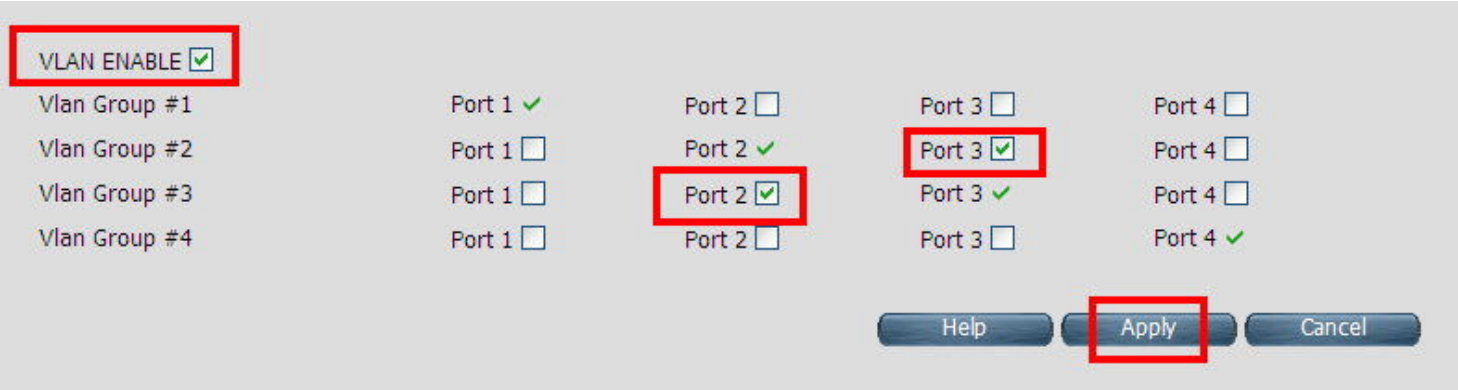


Figure 4.7.6 LAN Port Status

- Check the "VLAN ENABLE" checkbox to enable the Port-based VLAN.
- Click APPLY to save the VLAN settings that has been checked.
- Click CANCEL to exit from this page without saving the changes.

The following table is to configure VLAN settings Example:

When enable VLAN, all ports does not communicate. Please refer to the following example to configure the intercommunication status of each port.

Status	Examples
Port 1 & Port 4 intercommunicate	
Port 2 & Port3 intercommunicate	

4.8 Select "Route"

If there are multiple routers installed on your 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 your network before and after it passes through your router. You can use static routing to allow different IP domain users to access the Internet through this VDSL2 Router device.

For setting 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.

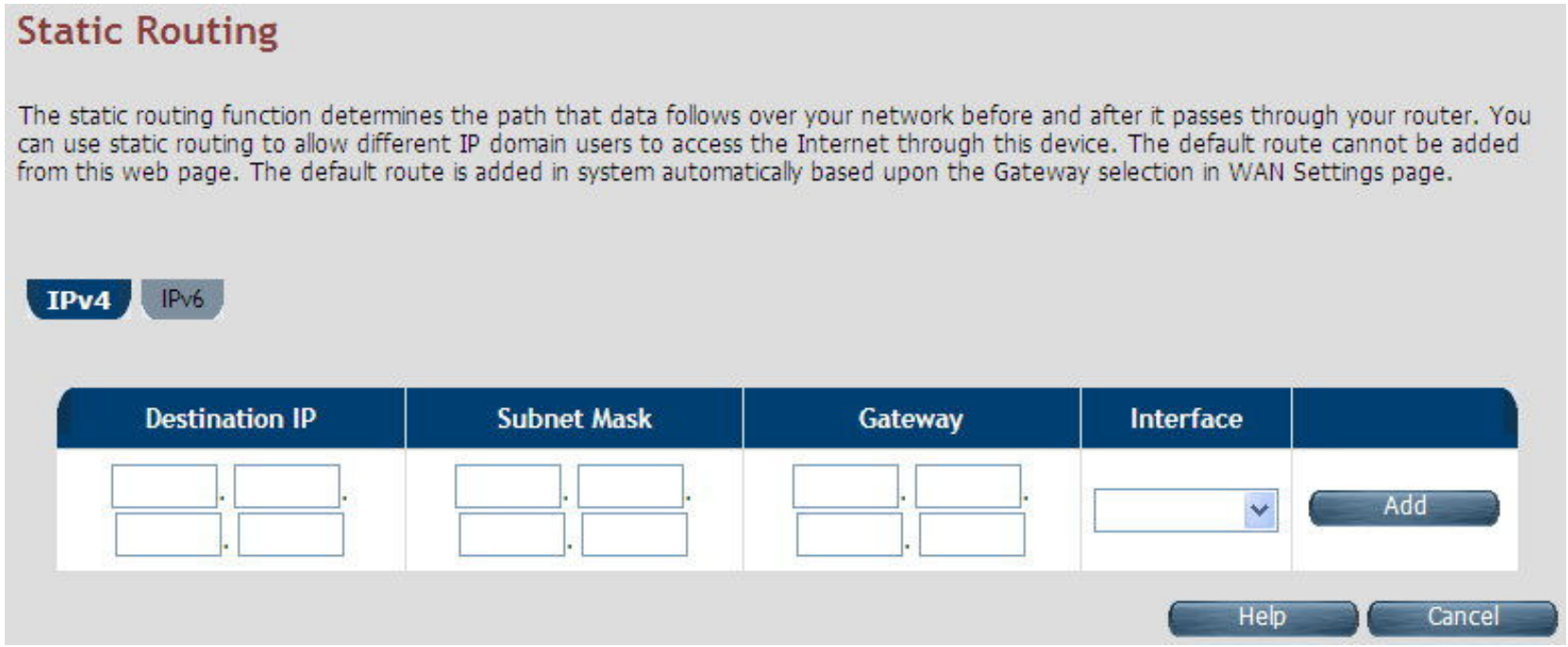


Figure 4.8.1 Static Routing Configuration

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 user would like to activate the Network Time Protocol (NTP) service, user have to define the Gateway connected to NTP server in the WAN.
2. The gateway of 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 192.168.1.X. (where X represents a number, range is 2-255)

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

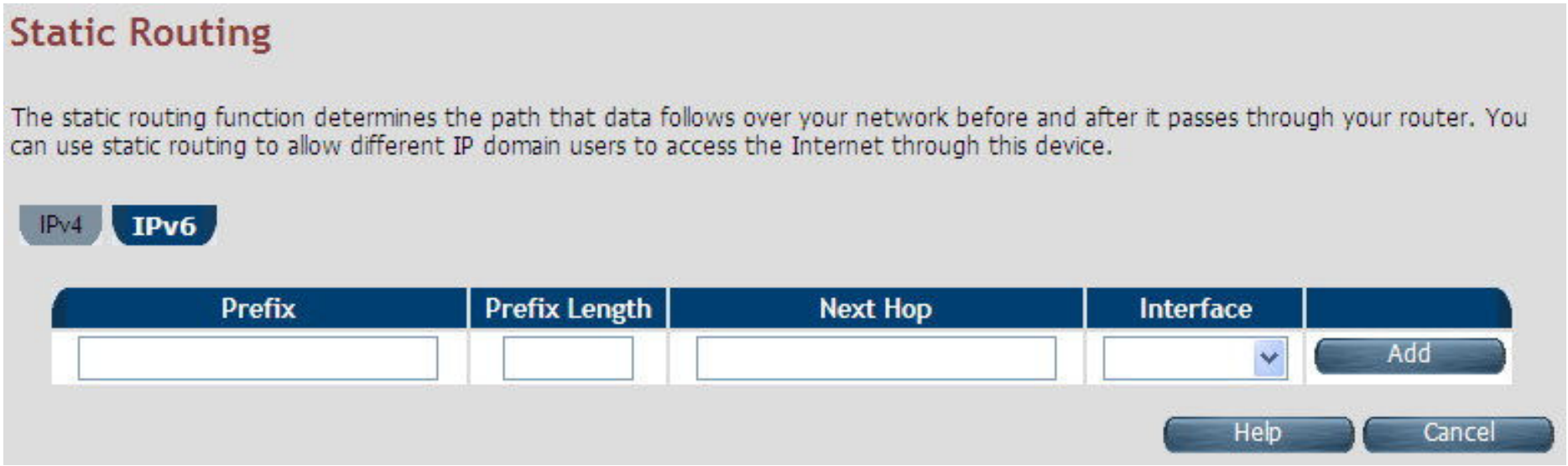


Figure 4.8.1.1 Static Routing IPv6

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 of pre-built packages. For enabling 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.

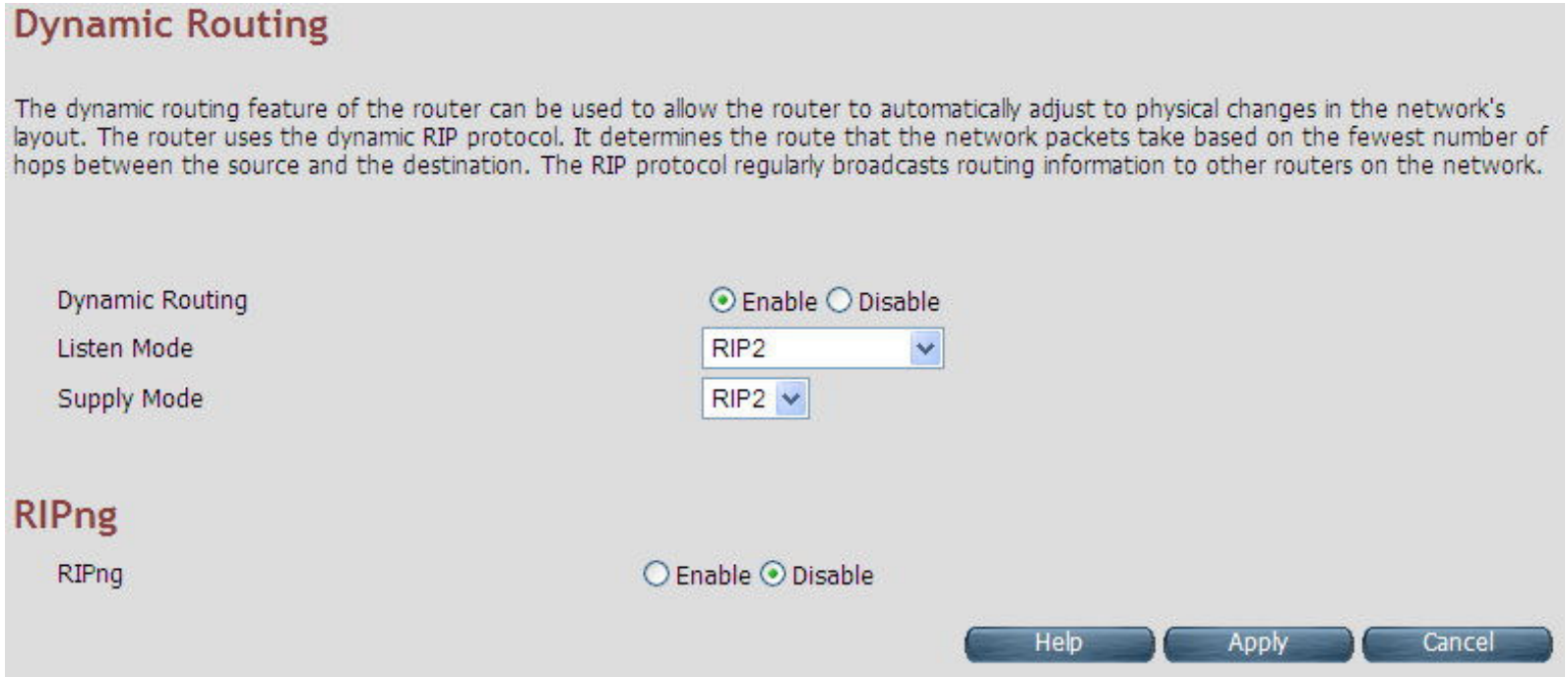


Figure 4.8.2 Dynamic Routing

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: ◆ Disabled ◆ RIP1 ◆ RIP2 ◆ Both (RIP1 + RIP2)
Supply Mode	To configure the supply mode of RIP to: ◆ Disabled ◆ RIP1 ◆ RIP2
RIPng	To enable or disable RIPng.

- Click **Apply** at any time during configuration to save the information that you 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 in 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 holddown 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 have 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, a compatibility switch feature allows fine-grained interoperability adjustments.

4.8.3 Routing Table List

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

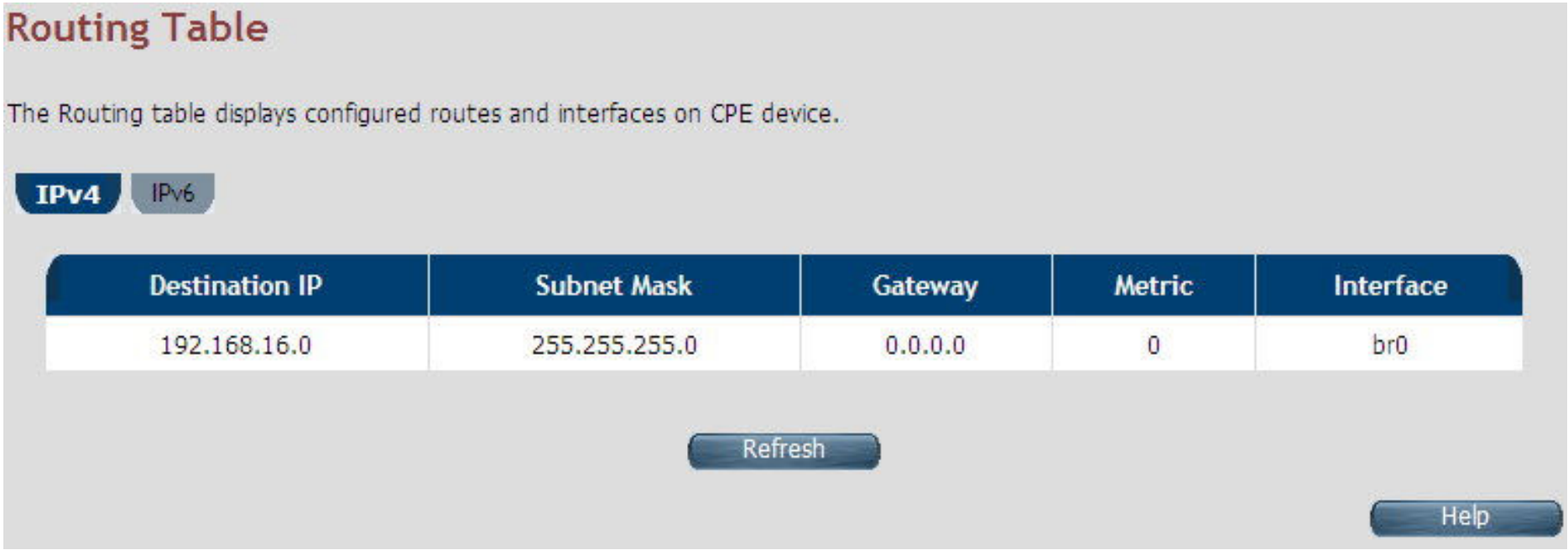


Figure 4.8.3 Routing Table List

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 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 you click **Refresh** button, it will refresh the table of IPv4 routes by gathering fresh list of routes from system.

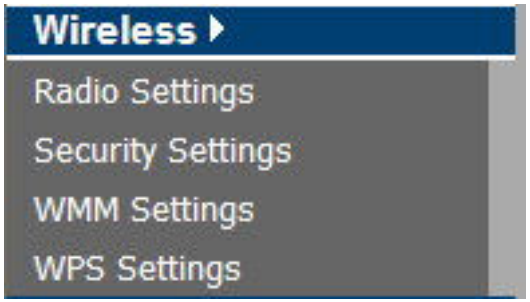
Routing Table List - IPv6 Tab

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 "Wireless"

This section describes Wireless LAN configuration options in CPE web page. This section applies only to those CPE systems, which support Wireless LAN functionality. You can view the **Wireless** link on the left navigation bar of the NV-600W CPE homepage. The menu below includes the sub-menus of Radio Settings, Security Settings, WMM Settings and WPS Settings. Following are the options available under **Firewall** as shown in Figure 4.9



4.9.1 Radio Settings

For viewing the radio settings, click Radio Settings link (Wireless > Radio Settings) on the left navigation bar. A screen is displayed as shown in Figure 4.9.1 this screen will show two tabs - Radio-1 and Radio-2 for Concurrent Dual Band WLAN platforms.

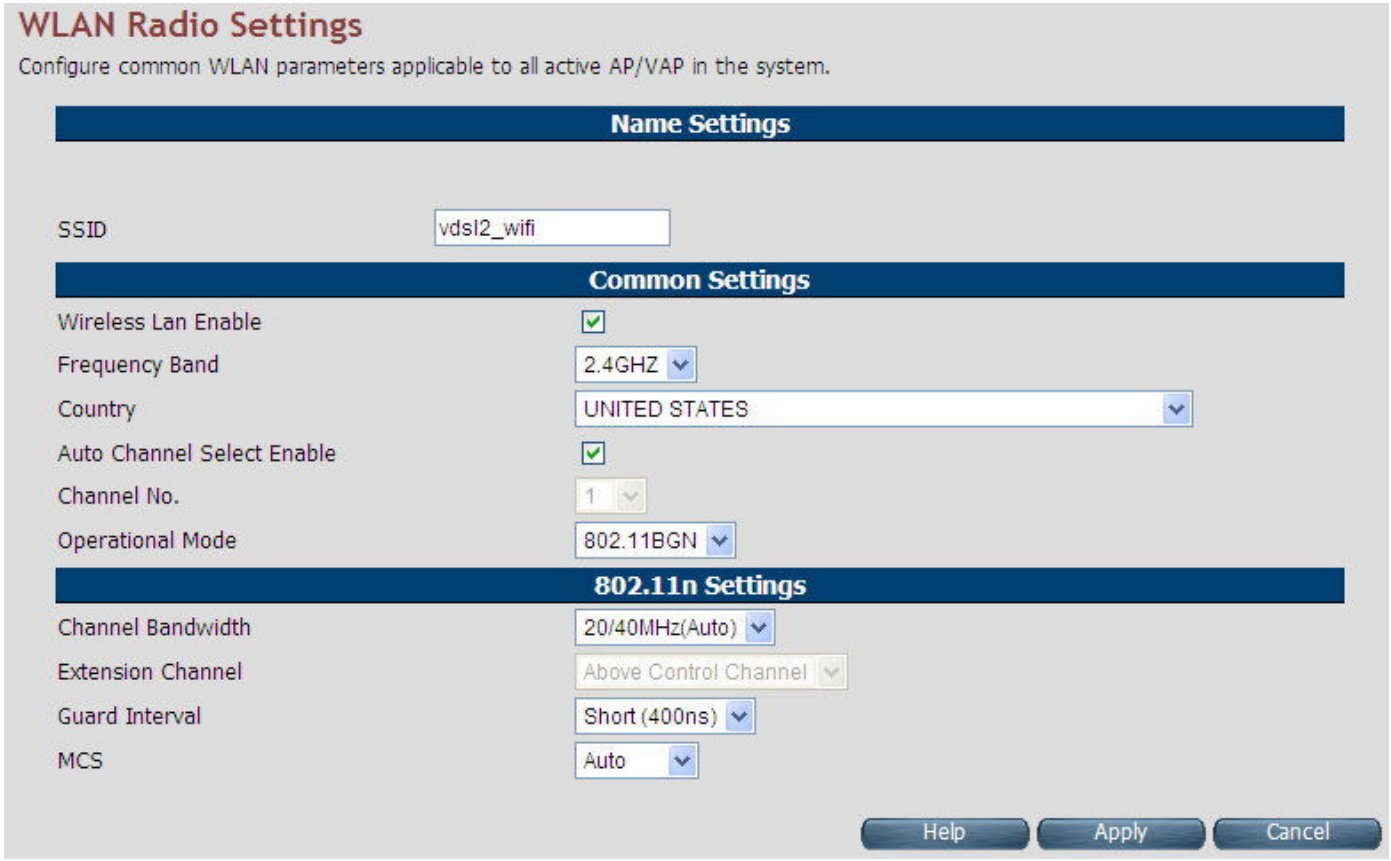


Figure 4.9.1 Radio Settings

The screen contains the following details:

Fields in Radio Setting:

Field	Description
Name Settings	
SSID	Service Set Identifier - public name of WLAN Network.
Common Settings	
Wireless LAN Enable	Enable / Disable the WLAN Radio of the device.
Frequency Band	Frequency Band for WLAN (2.4 GHz). After setting, need reboot.
Country	Country - where WLAN CPE is operating. After setting, need reboot.
Auto Channel Select Enable	To enable automatic channel selection support.
Channel no	Channel No. to be used in WLAN AP. When Auto Channel Select is enabled, this option cannot be used.
Operational Mode	Operational Mode of WLAN (e.g. 802.11BG, 802.11G 802.11N etc.)
802.11n Settings	
Channel Bandwidth	Channel Bandwidth - 20 or 20/40 MHz.
Extension Channel	Extension channel position - Above Control Channel or Below Control Channel.
Guard Interval	Guard interval between channels.
MCS	Modulation and Coding Scheme

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

4.9.2 Security Settings

The Security Settings page presents Wireless Security related settings. For viewing the wireless security related settings, click the **Security Settings** link (**Wireless** > **Security Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.9.2

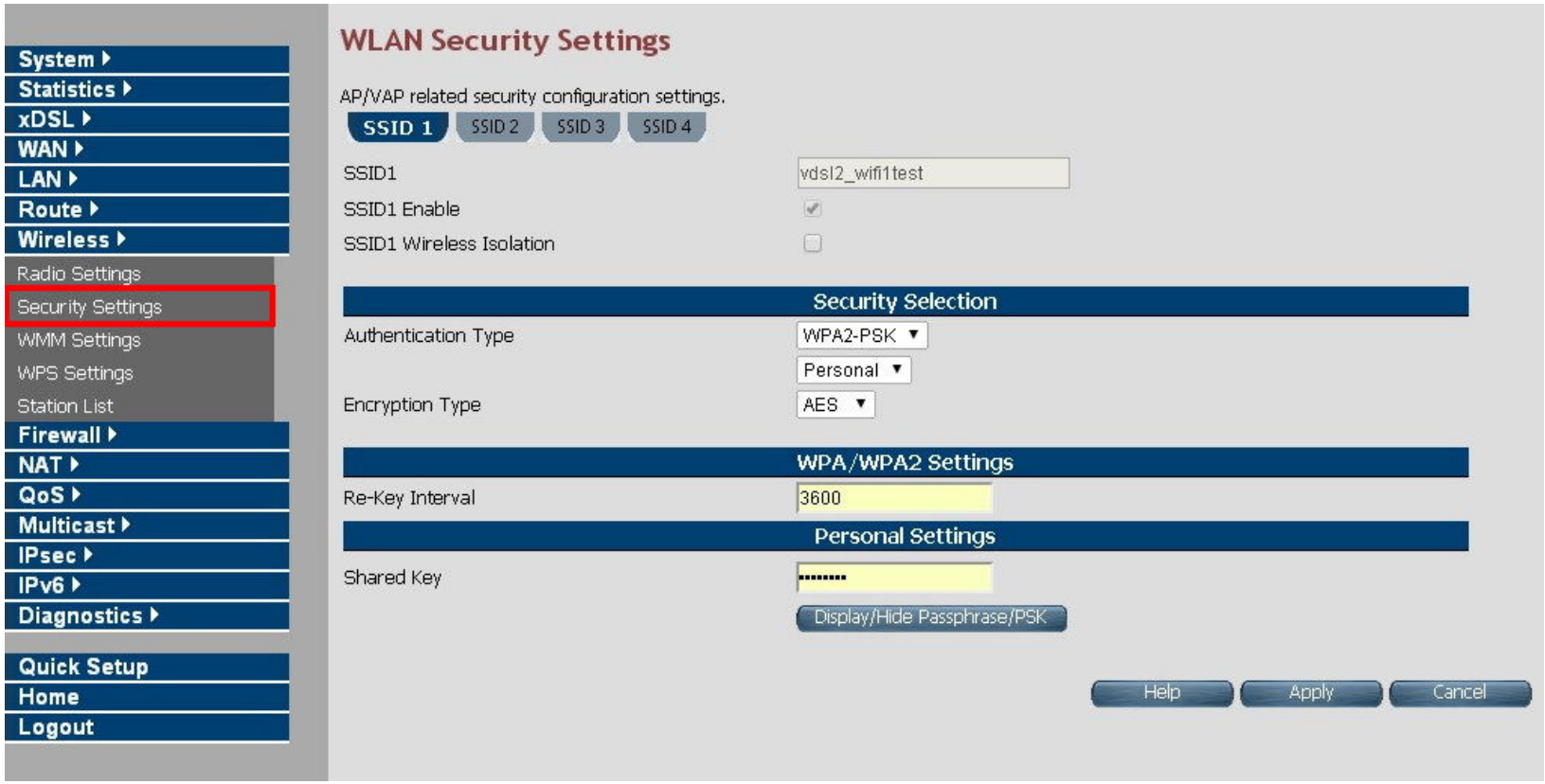


Figure 4.9.2 WLAN Security Settings

The screen contains the following details:

Fields in Security Setting:

Field	Description
SSID1~SSID4	Presents configured SSID1, SSID2, SSID3, and SSID4.
SSID1~SSID4 Enable	Enable SSID1, SSID2, SSID3, and SSID4.
SSID1~SSID4 Wireless Isolation	Enable / Disenable the network connection to LAN ports and another wirelessly connected device.
Security Selection	
Algorithm Type	Select Algorithm Type for the chosen Encryption type.
Encryption Type	Select Encryption Type for the chosen beacon type. Each encryption mode will bring out different web page and ask you to offer additional configuration.

◆ SSID1~4 Wireless Isolation

When you enable the wireless isolation, it prevents SSID from connecting to LAN ports. This is used to confine and restrict clients connected to the Wi-Fi network. They can't interact with devices connected to the more secure wired network, nor can they communicate with each other, in essence isolating it on the wireless network. They can only access the Internet.

- Encryption Type: Basic, Algorithm Type: None (Wireless open)

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

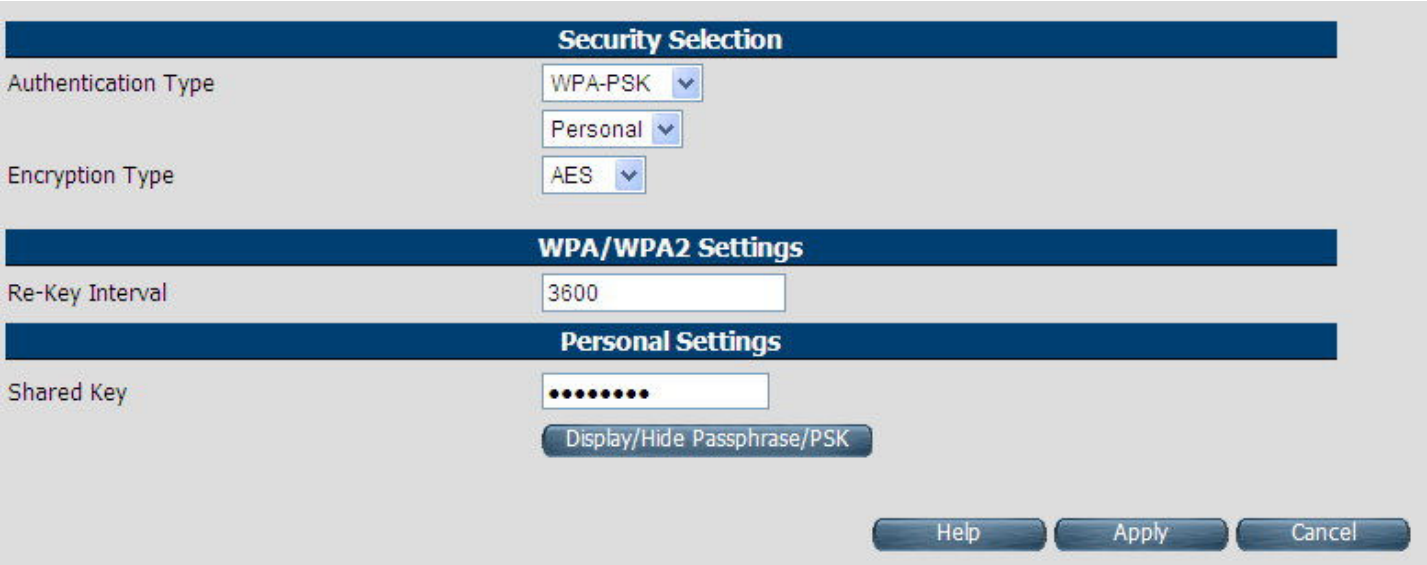
- Encryption Type: Basic, Algorithm Type: WEP

If you choose WEP as the security configuration, you have to specify encryption key (WEP Key 1 ~ WEP Key 4). All wireless devices must support the same WEP encryption bit size and have the same key.

Four keys can be entered here, but only one key index can be selected at a time. The keys can be entered in ASCII and HEX key. Choose the key you wish to use by using the Default Key drop down list.

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

- Encryption Type: WPA-PSK/WPA2-PSK. If you choose WPA-PSK/WPA2-PSK as the security configuration, you have to specify WPA mode, algorithm and pre-shared key.



Fields in WPA-PSK/WPA2-PSK Setting:

Field	Description
Security Selection	
Encryption Type (WPA-PSK/WPA2-PSK)	The WPA/WPA2 encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA or WPA2 as WPA mode.

Fields in WPA-PSK/WPA2-PSK Settings (Cont'd):

Field	Description
Authentication Type	■ **Personal:** Specify the Pre-shared key. ■ **Radius:** Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users. The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management. 
Algorithm Type	Select Algorithm Type for the chosen Encryption type. Choose the WPA algorithm, TKIP or AES.
Pre-shared Key	The keys can be entered in ASCII. Type the key you wish to use.

4.9.3 WMM Settings

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE, AC_BK, AC_VI and AC_VO for WMM. APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. When you click WMM Settings link Wireless > WMM Settings) on the left navigation bar, a screen is displayed as shown in Figure 4.9.3

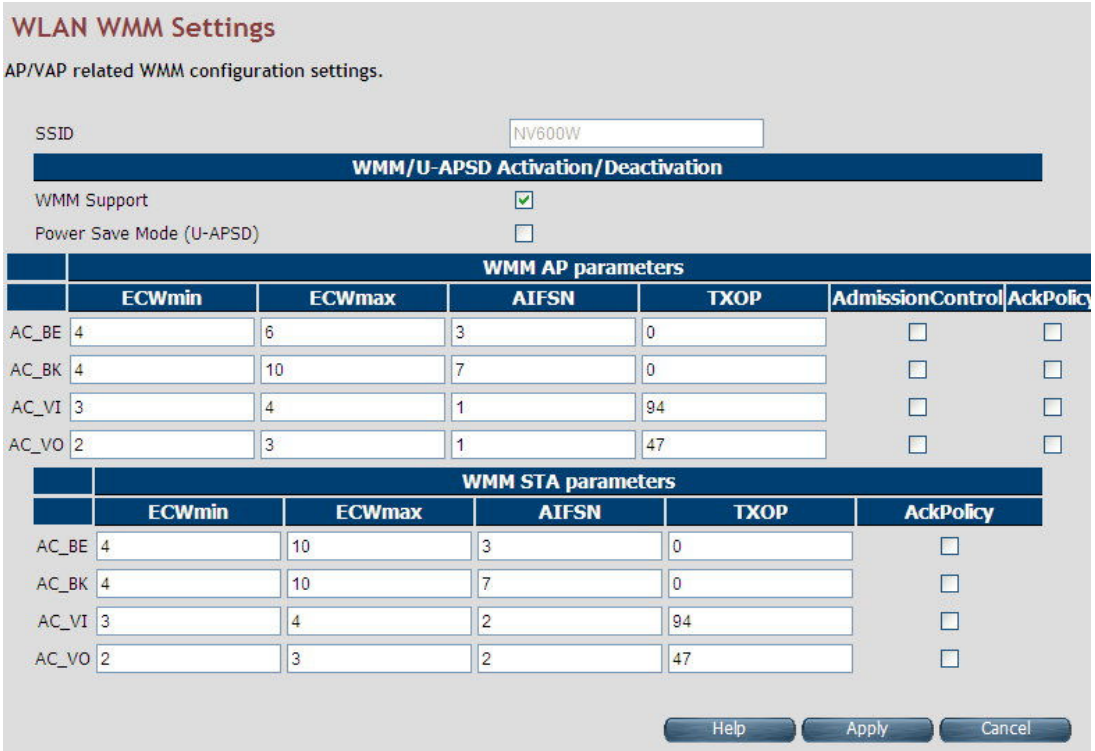


Figure 4.9.3 WLAN WMM Settings

The screen contains the following details:

Fields in WMM Setting:

Field	Description
SSID	SSID information presented in R-O format for AP/VAP selected.
WMM/U-APSD Activation/Deactivation	
WMM Support	Enable or Disable of WMM.
Power Save Mode (U-APSD)	Power Saving variant of WMM Enable or Disable. This feature is not available for XWAY™ WAVE300 WLAN.
WMM AP Parameters	
ECWmin	Exponential of Contention Window minimum Parameter.
ECWmax	Exponential of Contention Window maximum Parameter.
AIFSN	Arbitrary Inter Frame Spacing Number.
TXOP	Transmit Opportunity.
Admission Control	Enable / Disable WLAN Flow admission control.
AckPolicy	Acknowledgement Policy.
WMM STA Parameters	
ECWmin	Exponential of Contention Window minimum Parameter.
ECWmax	Exponential of Contention Window maximum Parameter.
AIFSN	Arbitrary Inter Frame Spacing Number.
TXOP	Transmit Opportunity.
AckPolicy	Acknowledgement Policy.

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

4.9.4 WPS Settings

WPS (Wi-Fi Protected Setup) provides an easy procedure to make a network connection between wireless stations and wireless access points with the encryption of WPA and WPA2. If you choose WPS as the security configuration, you can press Start WPS PIN and Start WPS PBC to complete the wireless connection. When you click WPS Settings link (Wireless > WPS Settings) on the left navigation bar, a screen is displayed as shown in Figure 4.9.4

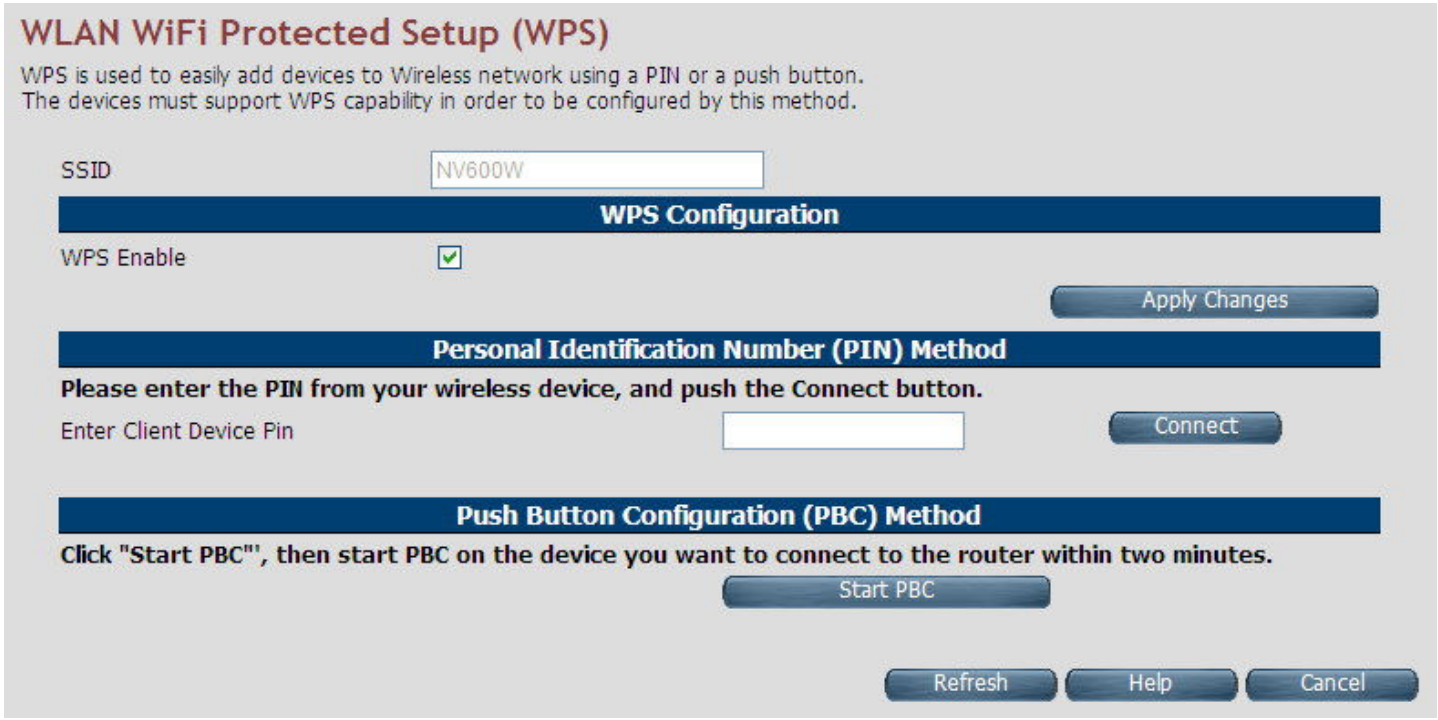


Figure 4.9.4 WPS Settings

The screen contains the following details:

Fields in WPS Setting:

Field	Description
SSID	SSID as shown in Read Only info.
WPS Configuration	
WPS Enable	Enable WPS.
Personal Identification Number (PIN) Number	
Enter Client Device PIN	You need to enter the PIN number in the field.
Current Router PIN	Current WLAN PIN for System.
Push Button Configuration (PBC) Method	
Start PBC	Click the virtual button in this page to start Push button Configuration pairing.

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

Note:

WPS Function is only supported by windows 7 or above, or any operating system that supports WPS function.

4.9.5 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code.Please click Station List link (Wireless > Station List) on the left navigation bar, a screen is displayed as shown in Figure 4.9.4

Figure 4.9.5 WPS Settings

Fields in Station List:

Field	Description
MAC Address	Display the MAC Address for the connected station.
IP Address	Display the WAN IP address for the connected station.
Auth	Display the authentication of the connected station.
Encrypt	Display the encryption type adapted by the connected station.

4.10 Select "Firewall"

You can view **Firewall** link on the left navigation bar of the NV-600W 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**. Following are the options available under **Firewall** as shown in Figure 4.10

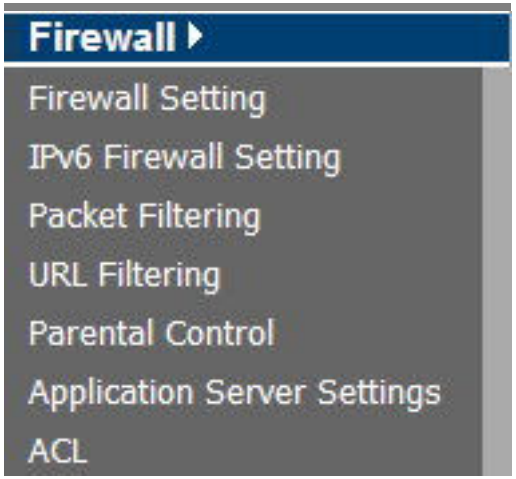


Figure 4.10 Firewall Options

4.10.1 Firewall Setting

For enabling or disabling the firewall, click the **Firewall Setting** link (**Firewall > Firewall Setting**) on the left navigation bar. A screen is displayed as shown in Figure 4.10.1

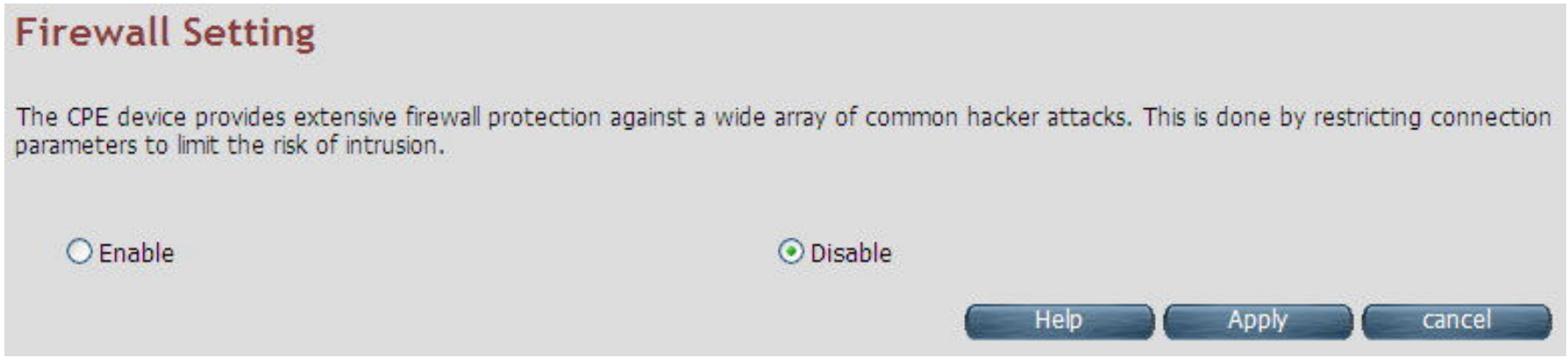


Figure 4.10.1 Firewall Setting

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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

4.10.2 IPv6 Firewall Setting

For enabling or disabling the IPv6 firewall, click the **IPV6 Firewall Setting** link (**Firewall > IPv6 Firewall Setting**) on the left navigation bar. A screen is displayed as shown in Figure 4.10.2

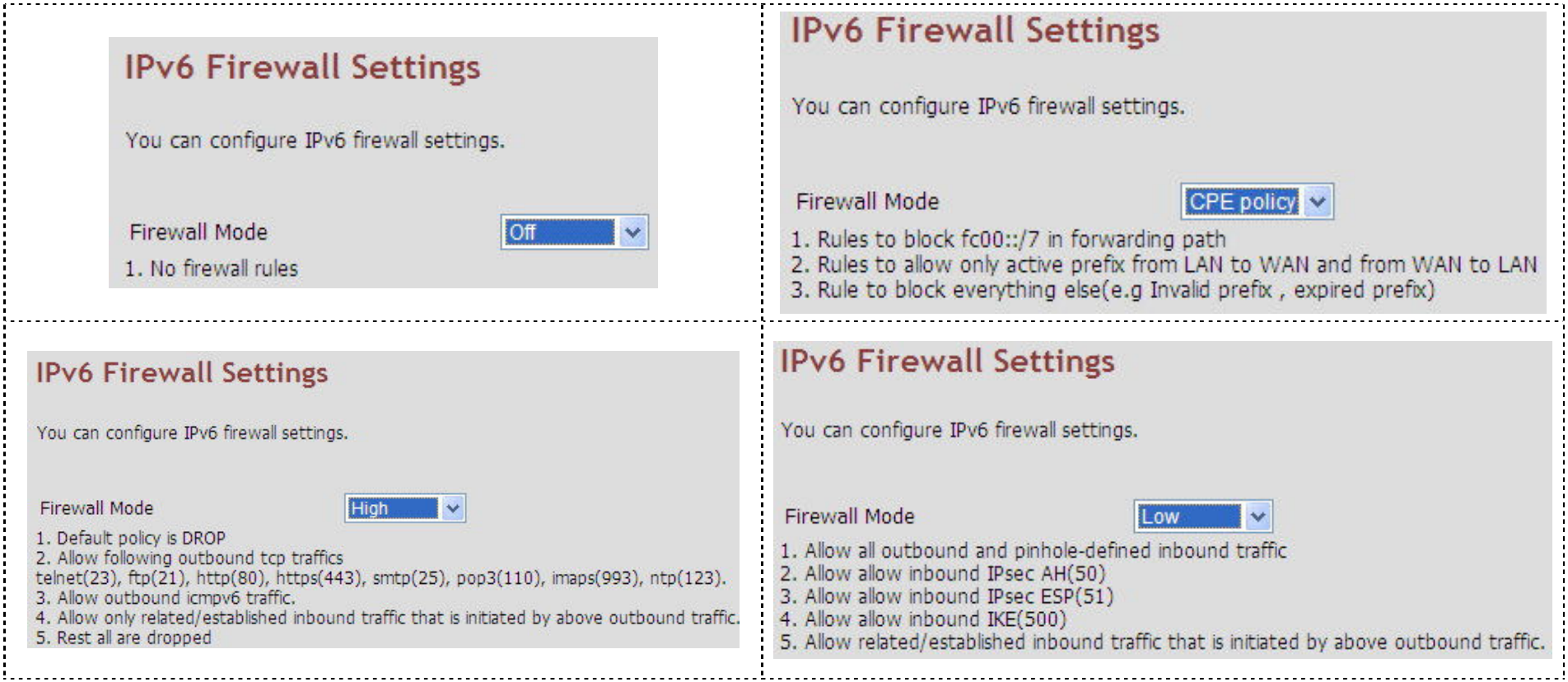


Figure 4.10.2 IPv6 Firewall Setting

The screen contains the following details:

Fields in UPnP Settings:

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

- Please note that the user must enable IPv6 settings before configuring the IPv6 firewall.
- Click **Apply** for committing the desired action.
- Click **Cancel** to exit from this page without saving the changes.

4.10.3 Packet Filtering

For enabling Packet Filtering, click the **Packet Filtering** link (**Firewall > Packet Filtering**) on the left navigation bar. A screen is displayed as shown in Figure 4.10.3

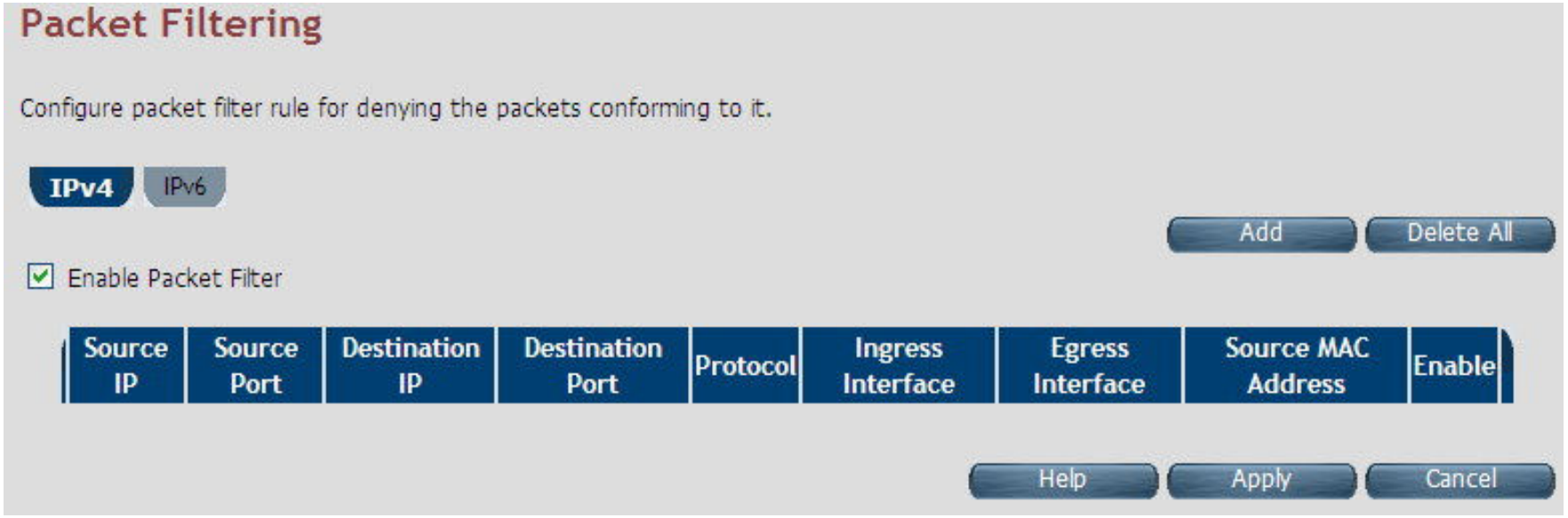


Figure 4.10.3 Packet Filtering

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 the Packet Filter feature of NV-600W CPE, select the check box.
Source IP	Filter IP Address range of the local machine under NV-600W CPE.
Source Port	Filter Port number range of the local machine under NV-600W 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	The screen shown in Figure 4.9.3.1 is displayed when 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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

When you have chosen IPv4 tab, and click Add button in the Packet Filtering page, a screen is displayed as shown in Figure 4.10.3.1. If you choose IPv6 tab and click on Add button, a screen is displayed as shown in Figure 4.10.3.2.

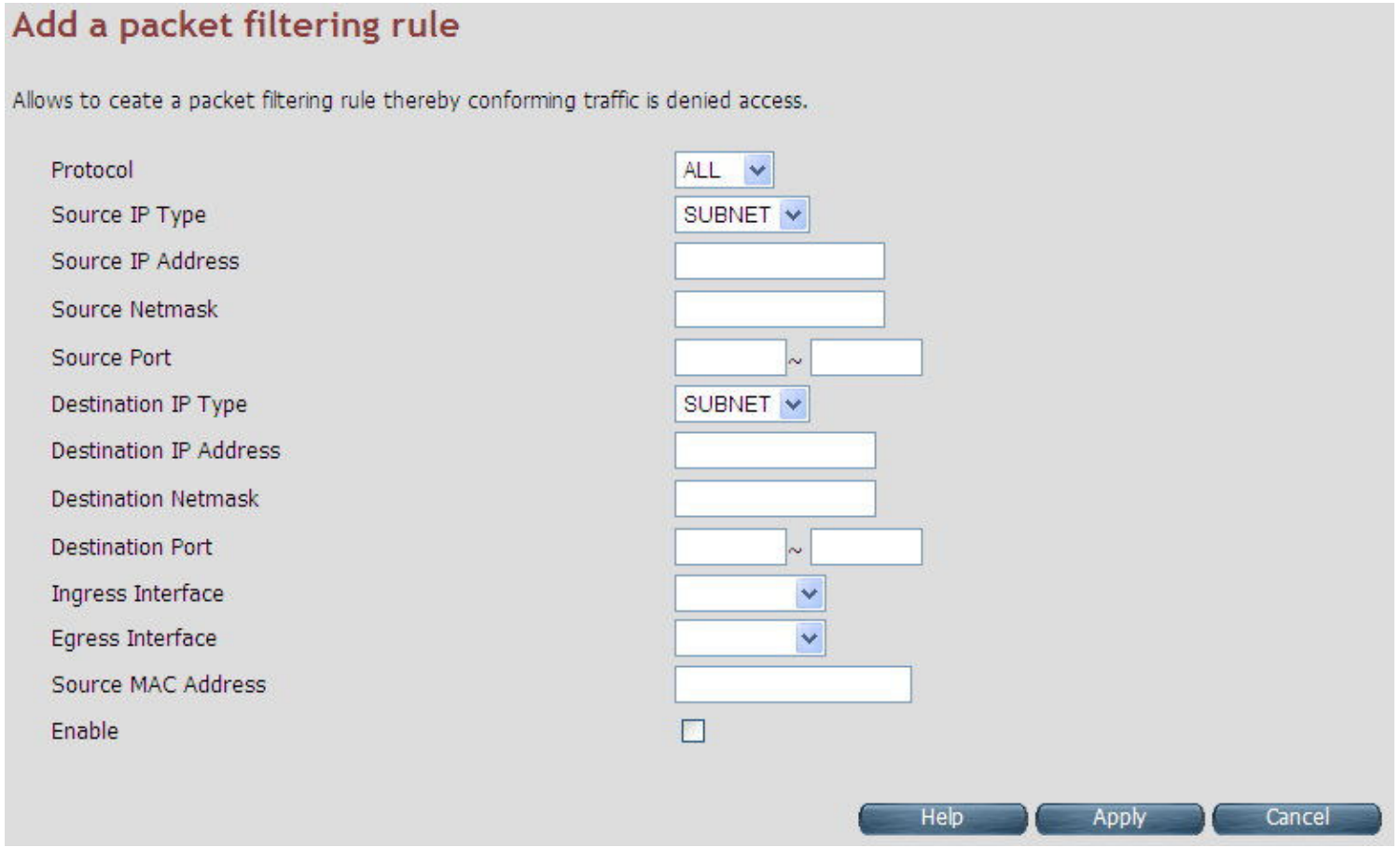


Figure 4.10.3.1 Add a Packet Filtering Rule for Firewall - IPv4

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.

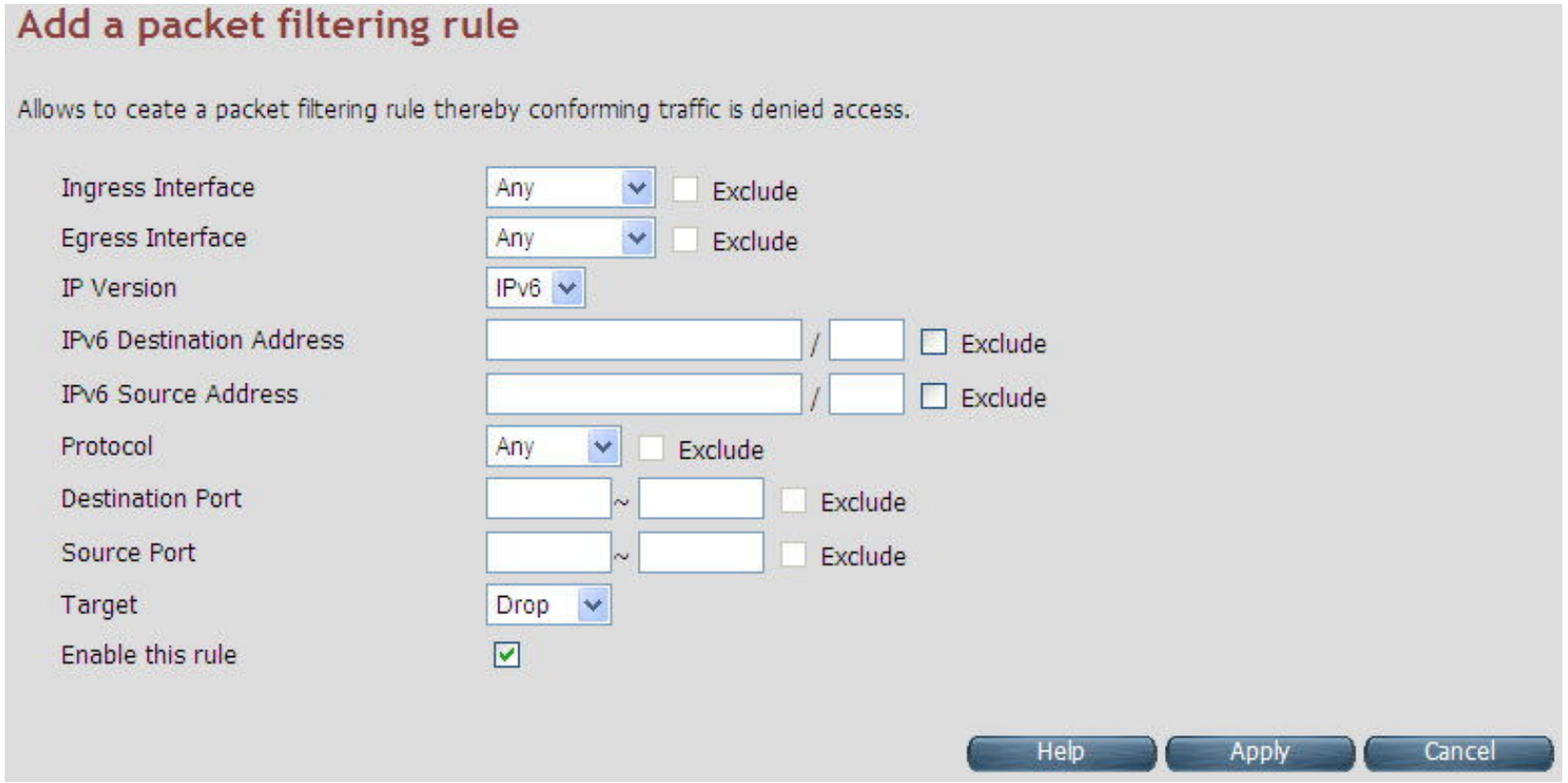


Figure 4.10.3.2 Add a Packet Filtering Rule for Firewall - IPv6

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.

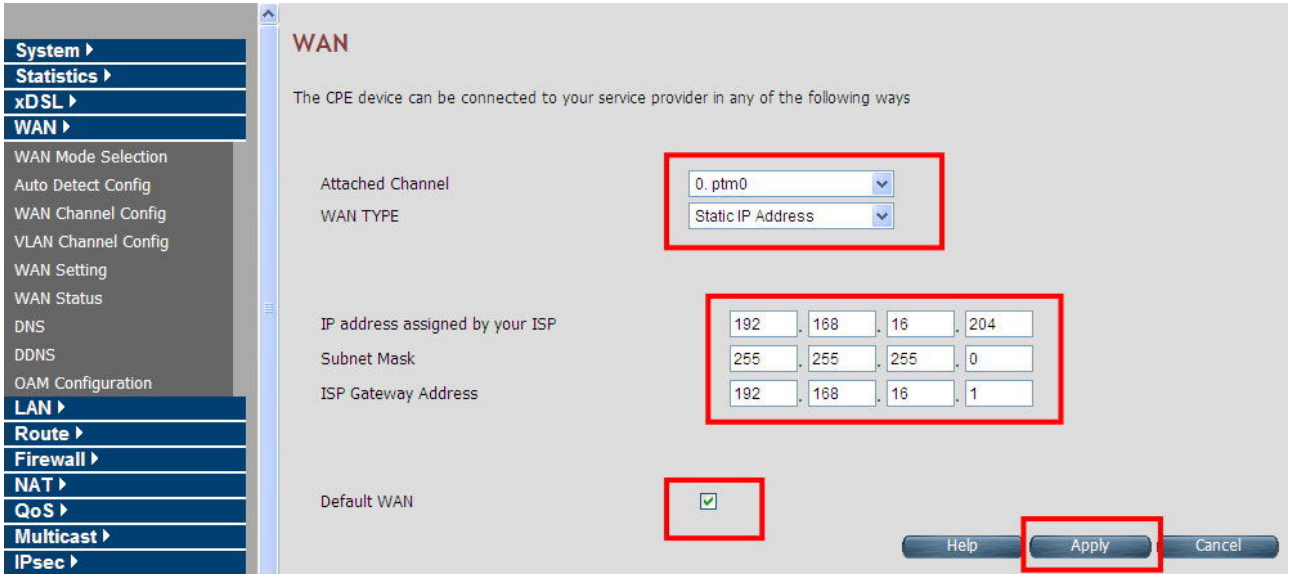
(2). Confirm that the NV-600W is in router mode (default mode).

(3). If there is not 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.

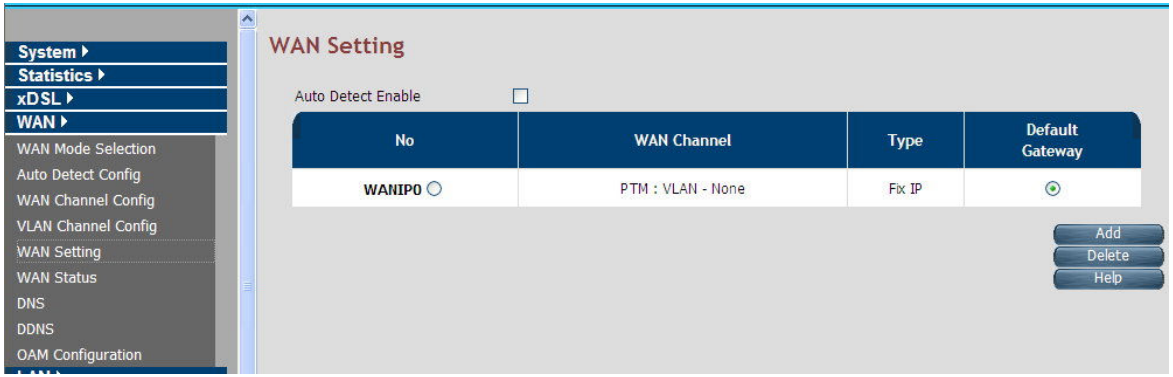
3. Router mode configuration:

◆ WAN setting



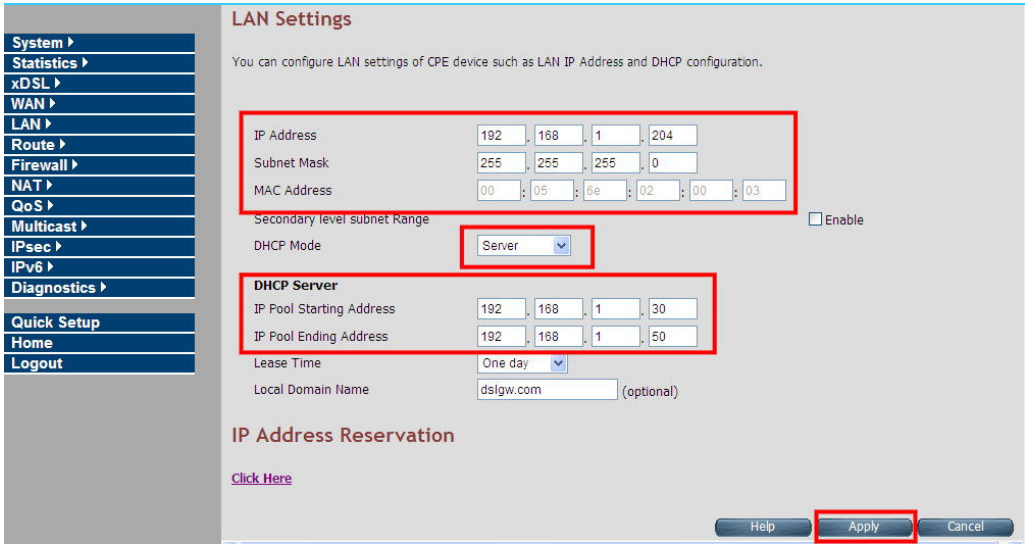
Configure example: WAN→WAN Setting

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

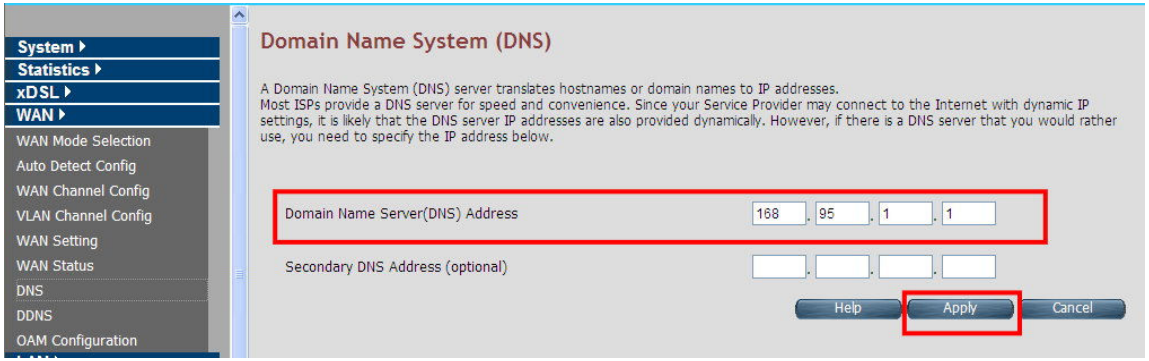
◆ LAN Setting



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-600W 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**

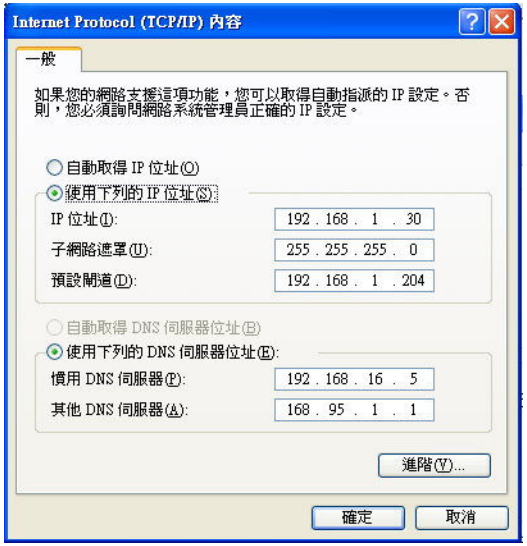


Configure example: WAN→DNS

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-600W.

◆ **PC NIC card setting**

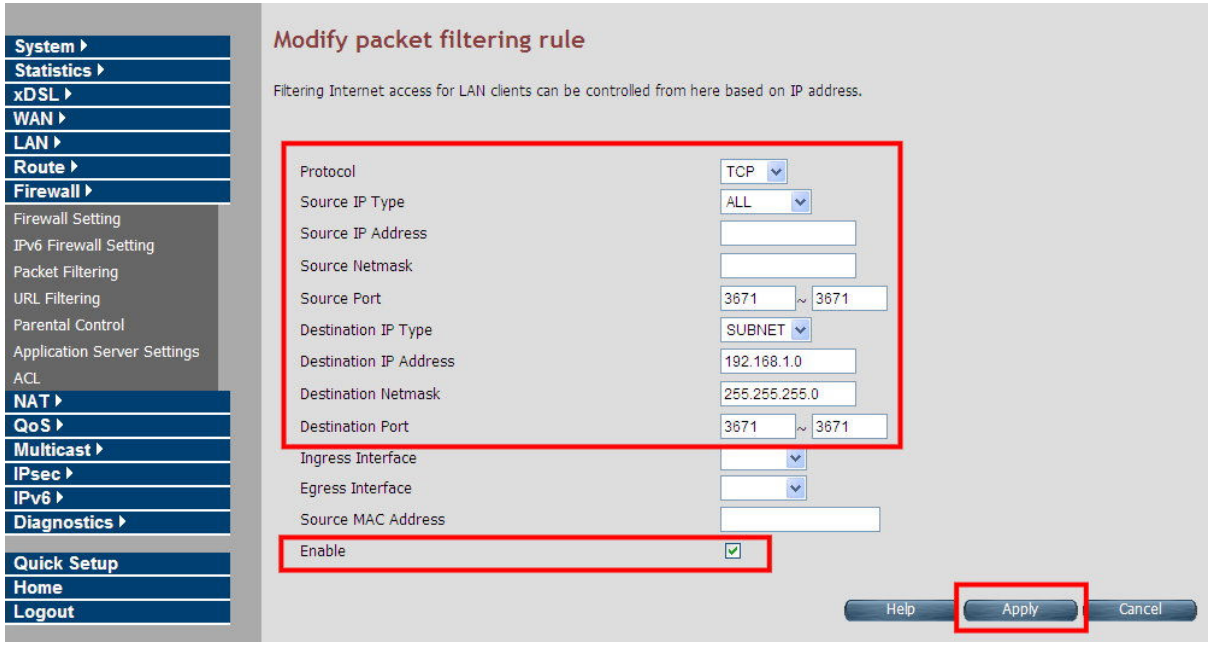


Configure example:

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)

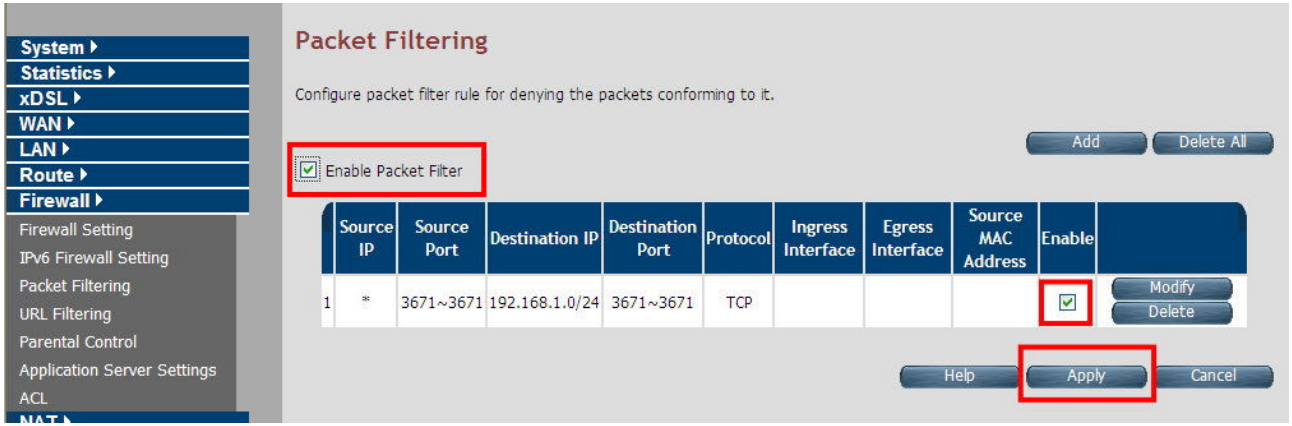
3. Packet Filtering configuration:

- **NV-600W 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 (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.

4.10.4 URL Filtering

URL Filtering is used to block the access to specific URLs to the web users by adding them to the list in the URL Blocking web page. For configuring the URL Filtering, click the **URL Filtering** link (**Firewall > URL Filtering**) on the left navigation bar. A screen is displayed as shown in Figure 4.10.4

Figure 4.10.4 URL Blocking

The screen contains 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	Select this option to remove the URL entry from blocked list.

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

4.10.5 Parental Control

For configuring the Parental Control, click the **Parental Control** link (**Firewall > Parental Control**) on the left navigation bar. A screen is displayed as shown in Figure 4.10.5

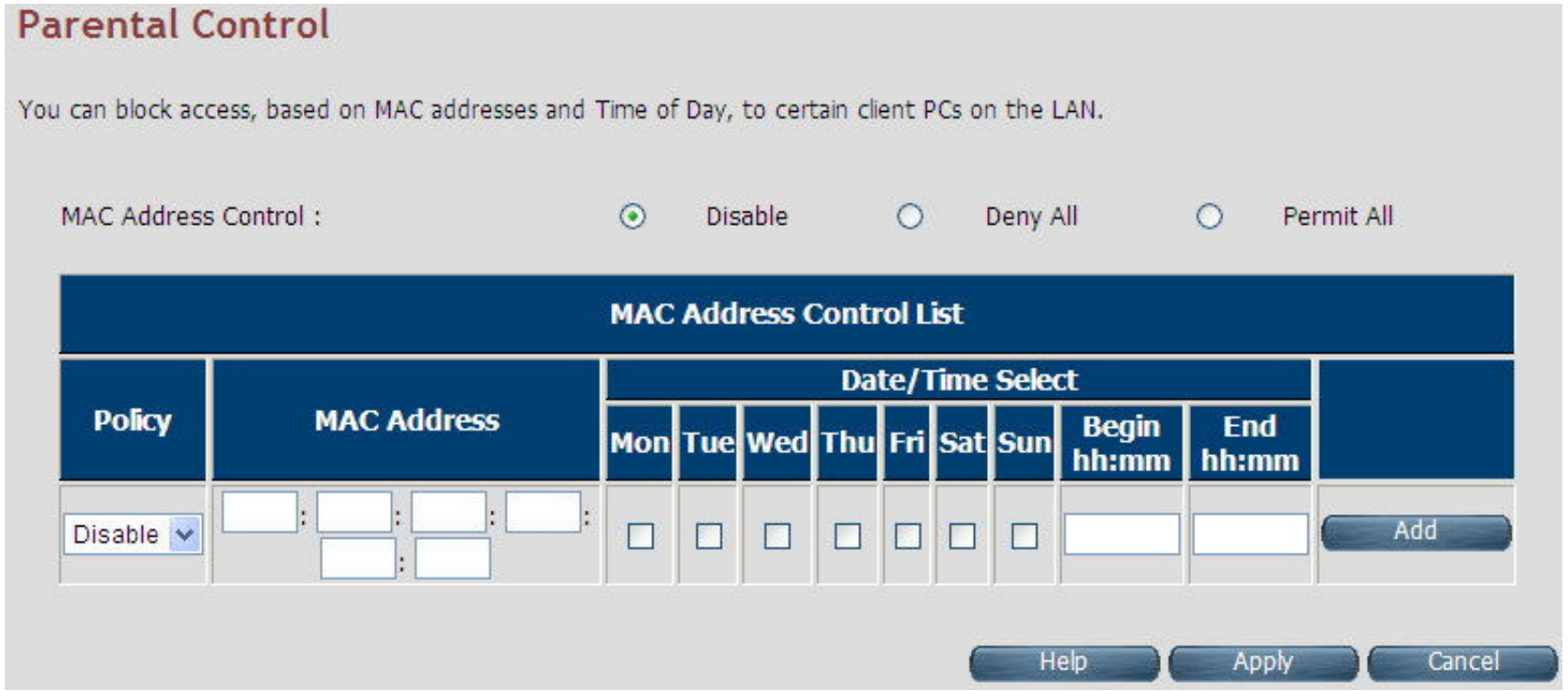


Figure 4.10.5 Parental Control Configuration

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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

4.10.6 Application Server Settings

For configuring 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 4.10.6

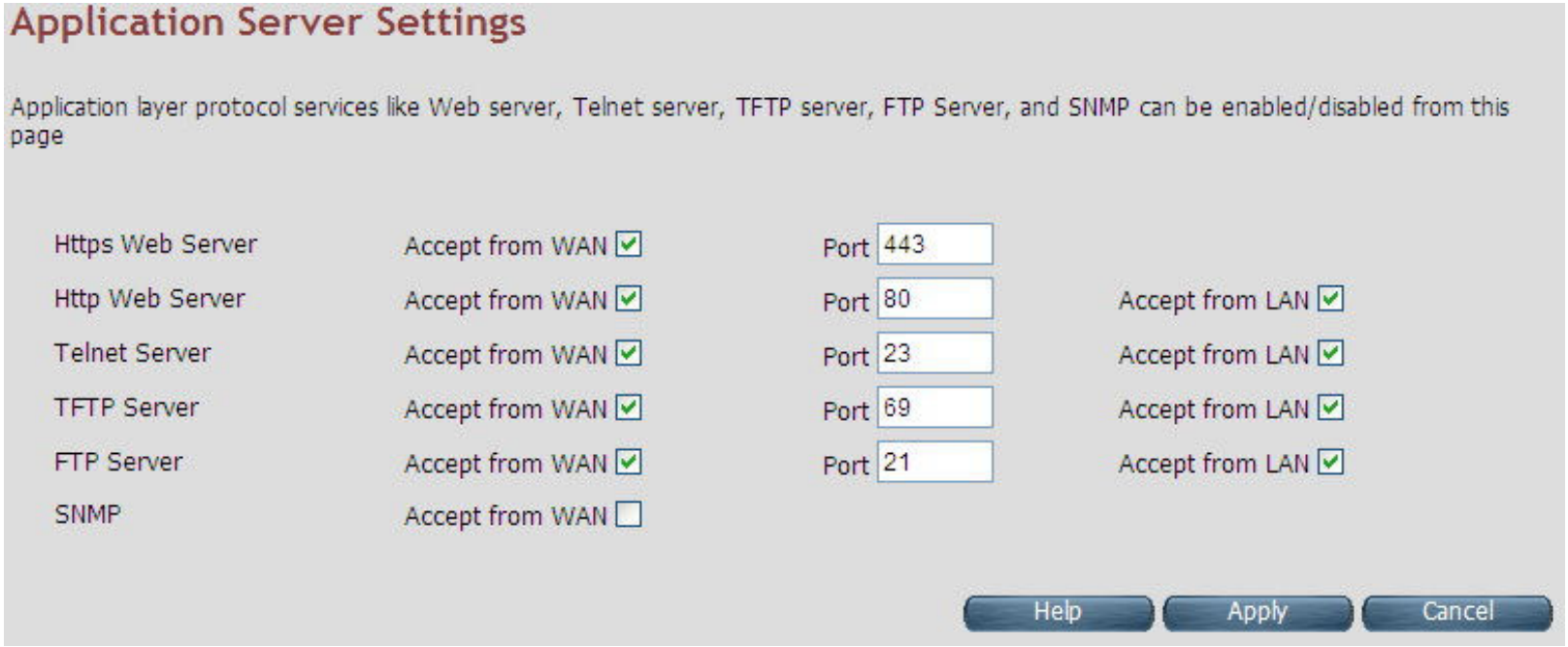


Figure 4.10.6 Application Server Settings

The screen contains the following details:

Fields in Application Servers Settings:

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

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

4.10.7 Access Control List (ACL)

For configuring 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-600W 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 4.10.7.

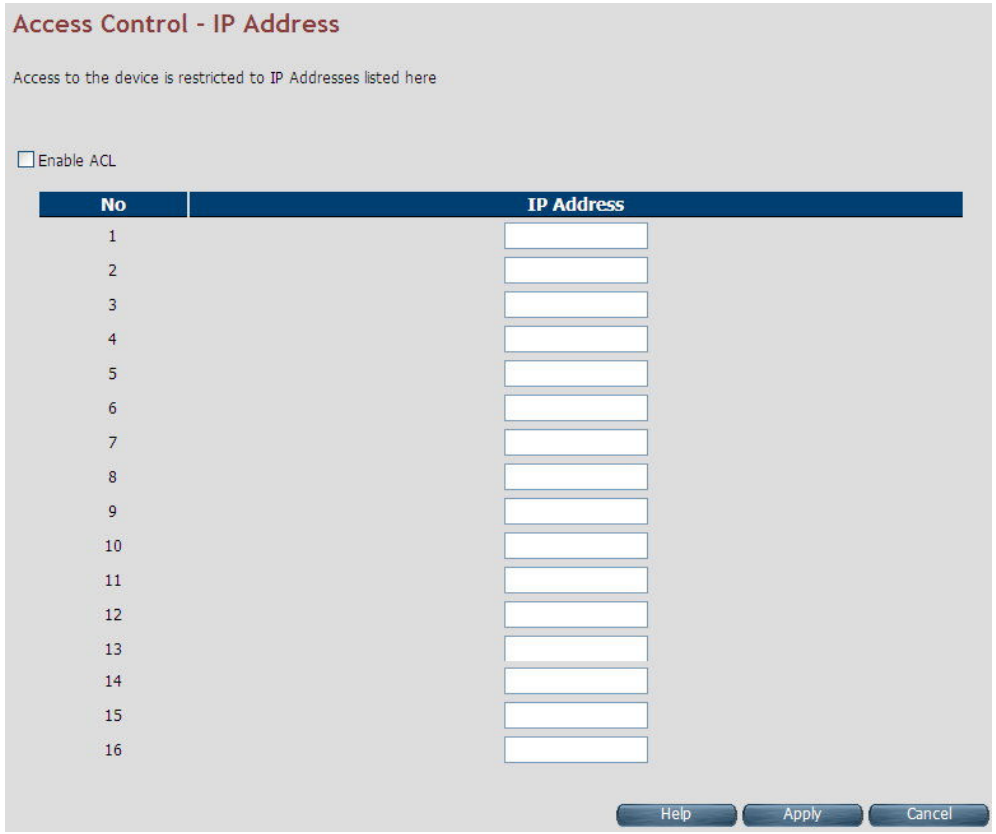


Figure 4.10.7 Application Server Settings

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

4.11 NAT

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

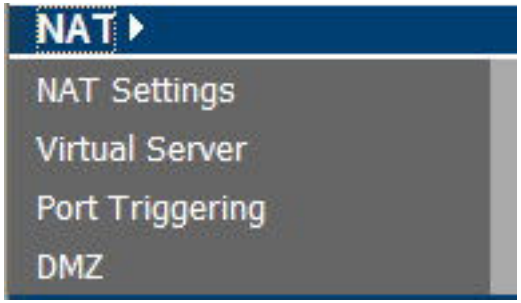


Figure 4.11 NAT Options

4.11.1 NAT Settings

For configuring 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 4.11.1

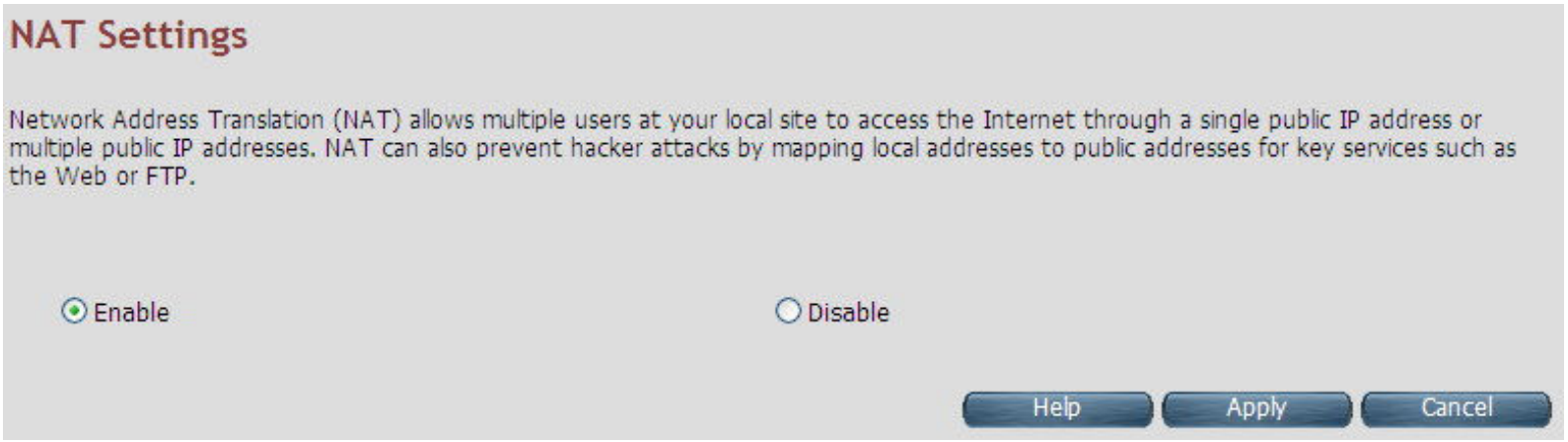


Figure 4.11.1 Network Address Translation (NAT) Settings

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.

4.11.2 Virtual Server

For configuring the virtual server, click the **Virtual Server** link (**NAT > Virtual Server**) on the left navigation bar. A screen is displayed as shown in Figure 4.11.2

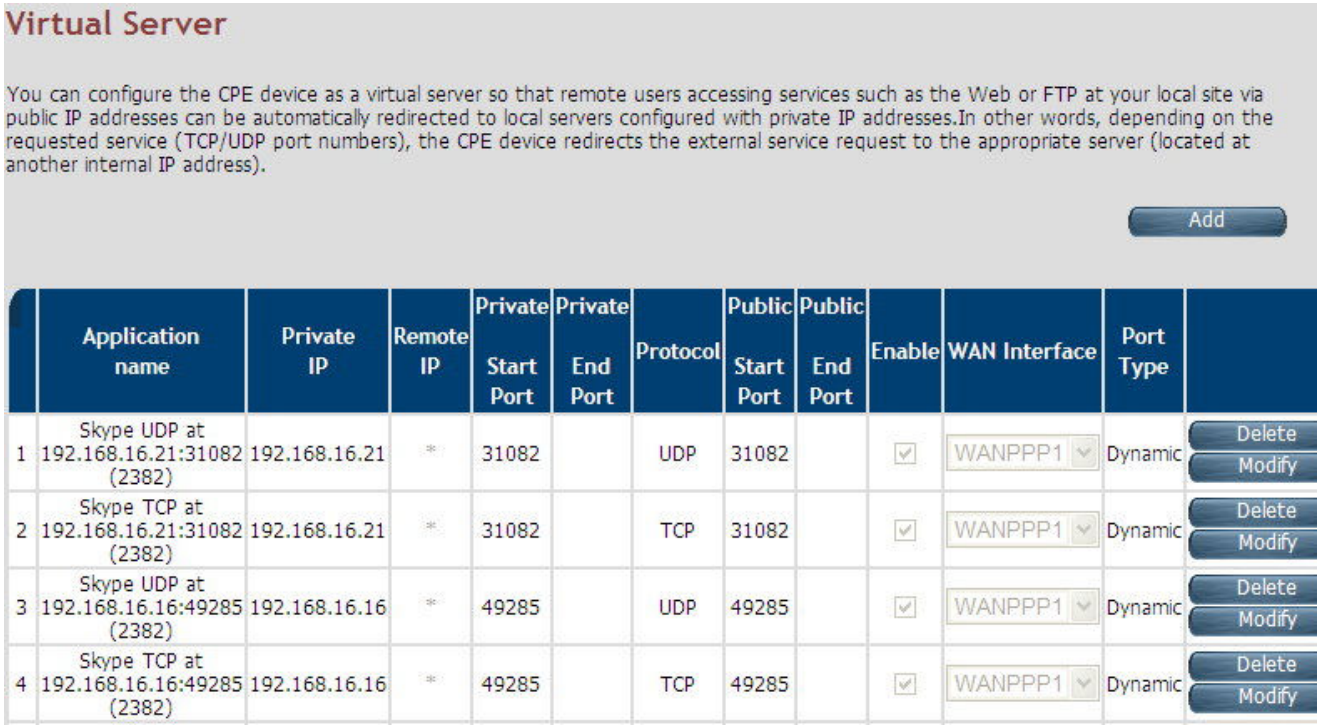


Figure 4.11.2 Virtual Server

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 you click the **Add** button in the Virtual Server page, a screen opens with a new web page as shown in Figure 4.10.2.1

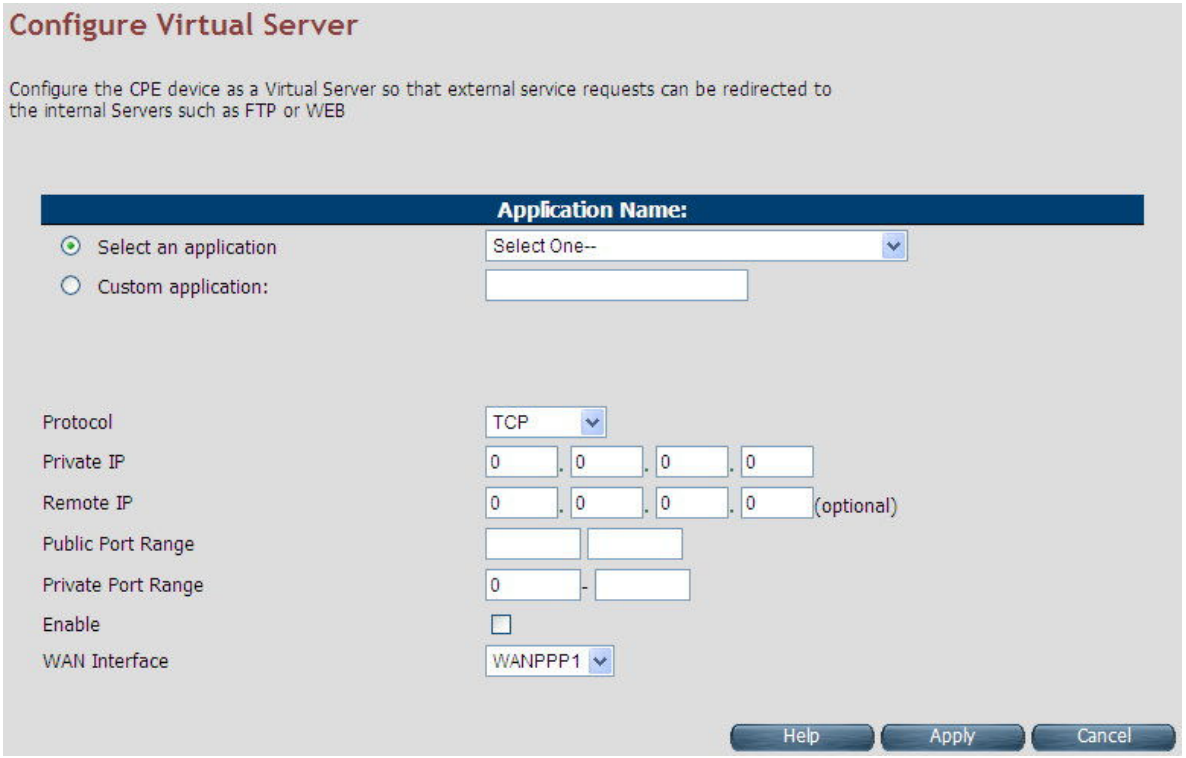


Figure 4.11.2.1 Virtual Server Add

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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

Note:

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

4.11.3 Port Triggering

For configuring Port Triggering, click the **Port Triggering** link (**NAT > Port Triggering**) on the left navigation bar. A screen is displayed as shown in Figure 4.10.3

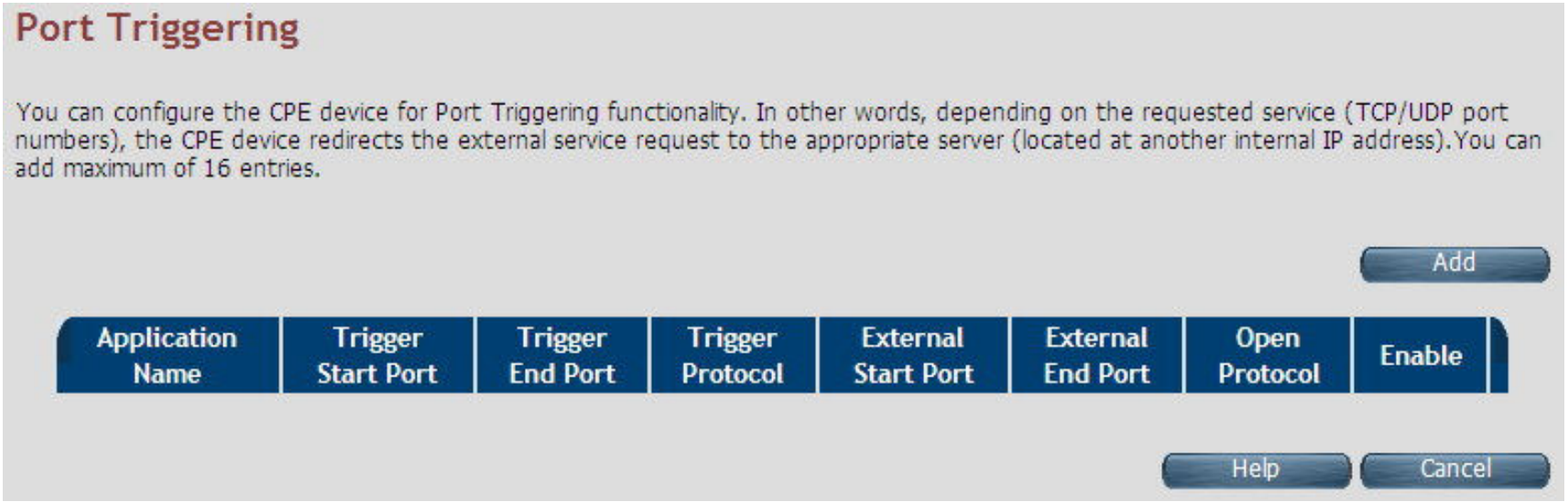


Figure 4.11.3 Port Triggering

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 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 you click the **Add** button in the Port Triggering page, a screen is displayed as shown in Figure 4.11.3.1.

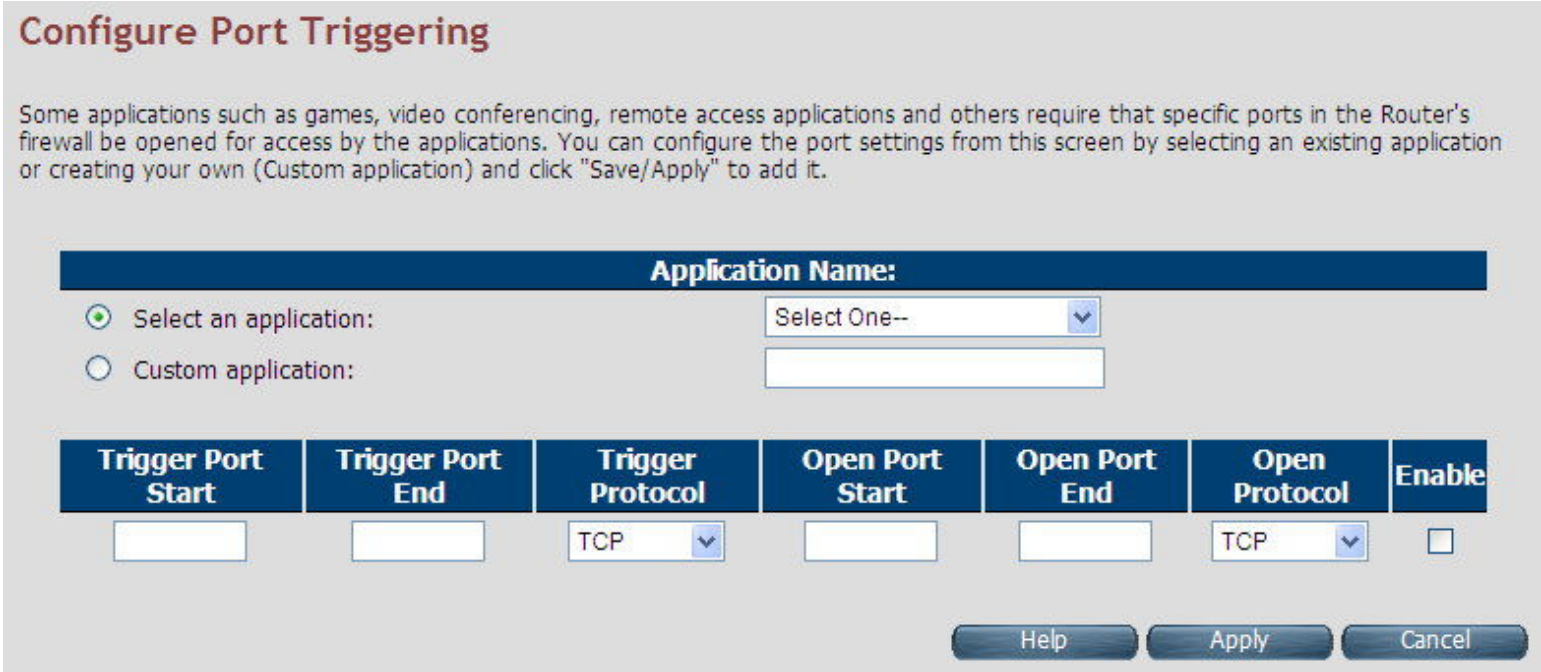


Figure 4.11.3.1 Port Triggering Add

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 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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

4.11.4 DMZ

For configuring 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 4.10.4.

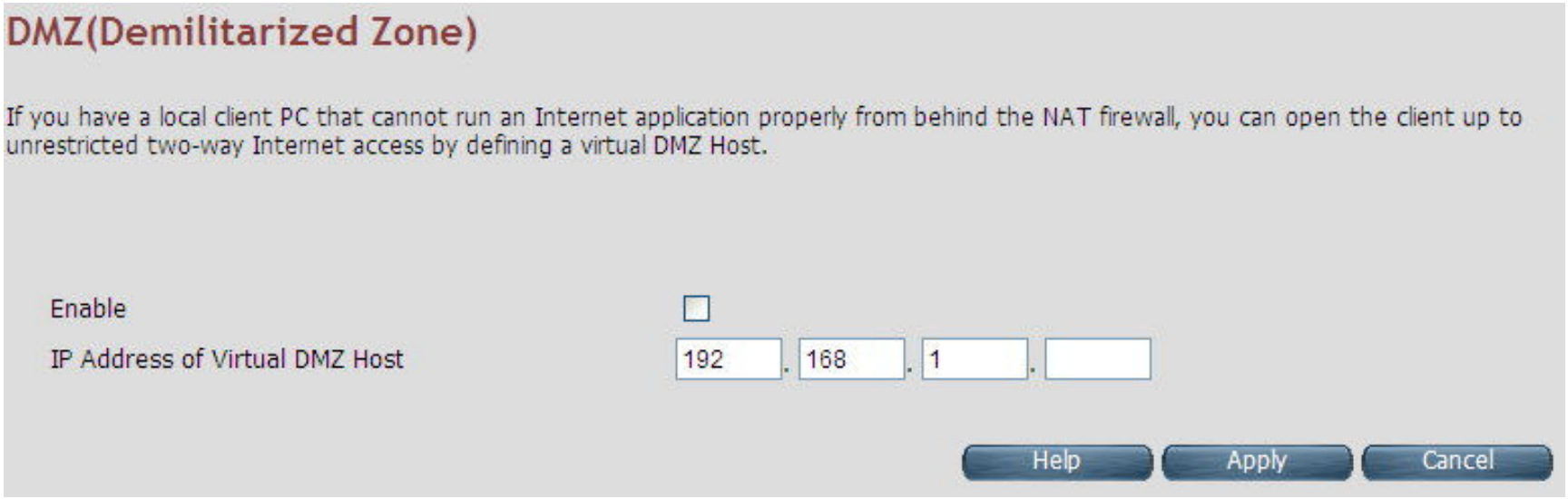


Figure 4.11.4 DMZ (Demilitarized Zone)

The screen contains the following details:

Fields in DMZ:

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

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

Figure 4.11 QoS Options

4.11.1 QoS Settings

For configuring 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

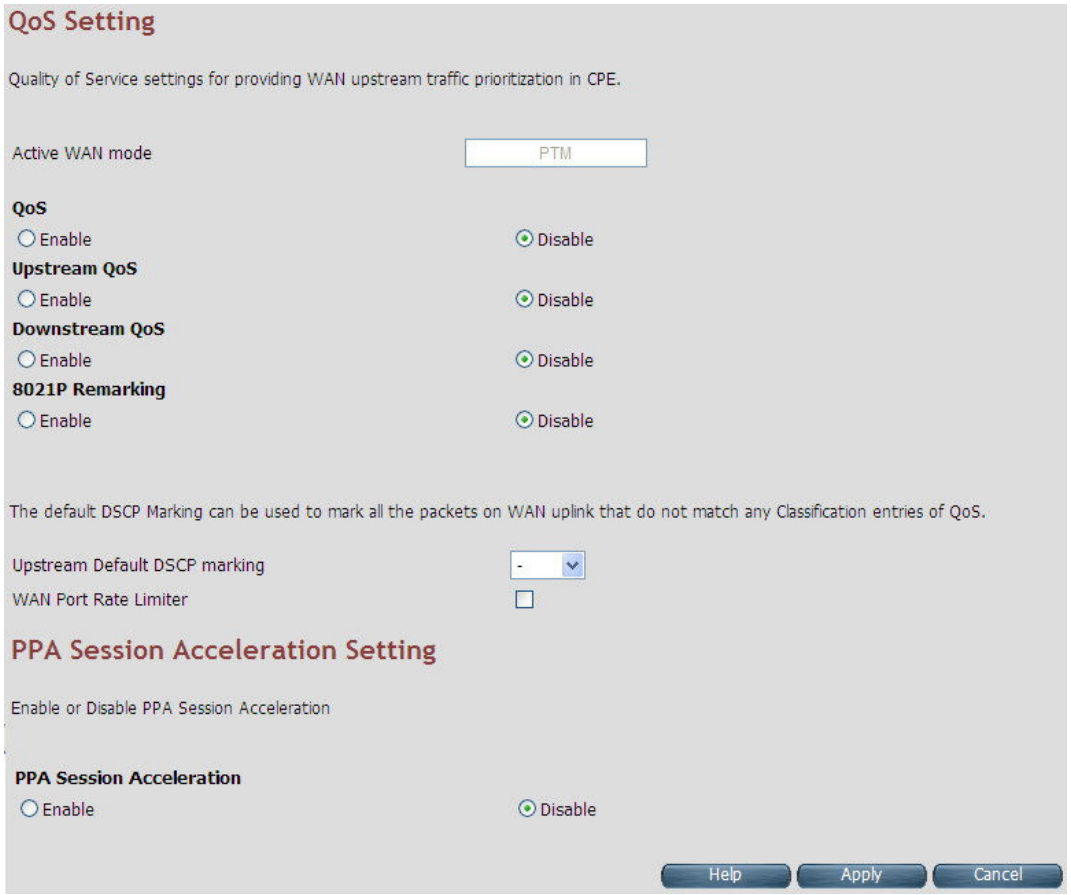


Figure 4.11.1 QoS Settings

The screen contains the following details:

Fields in QoS Settings:

Field	Description
Active WAN mode	Informative Parameter to show current WAN mode being used.
QoS	
Enable	This selection will enable the QoS feature.
Disable	This selection will disable the QoS feature.
Upstream QoS	
Enable	This selection will enable the upstream QoS.
Disable	This selection will disable the upstream QoS.
Downstream QoS	
Enable	This selection will enable the downstream QoS.
Disable	This selection 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	Check-box for limiting physical port rate limit on WAN upstream link.
PPA Session Acceleration Setting	
PPA Session Acceleration	Hardware Acceleration based on Protocol Processing Engine (PPE) of Lantiq. 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.

DSCP comparison table example (Reference only):

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

4.11.2 Queue Configuration.

For configuring the Queue Configuration, 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 Configuration

The screen contains the following details:

Fields in Queue Configuration - Upstream:

Field	Description
Upstream/Downstream	Selection tab for upstream/downstream Queue configuration.
Queue Name	This is the name of the queue configured in the 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 supported 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 you click the **Add** button in the Port Triggering page, a screen is displayed as shown in Figure 4.11.2.1.

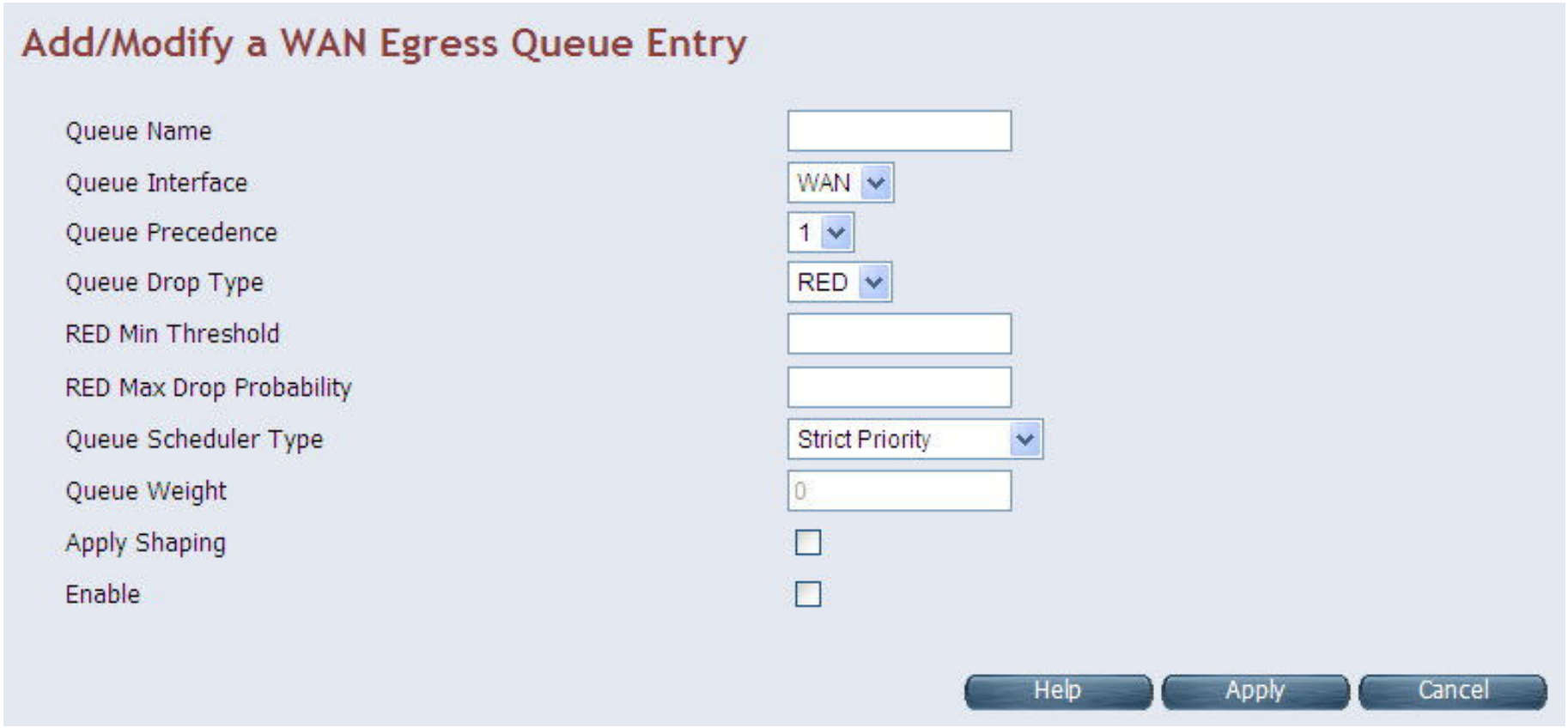


Figure 4.11.2.1 Add/Modify a Queue Entry

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 on 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 algorithm.
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 Configuration

For classifying 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

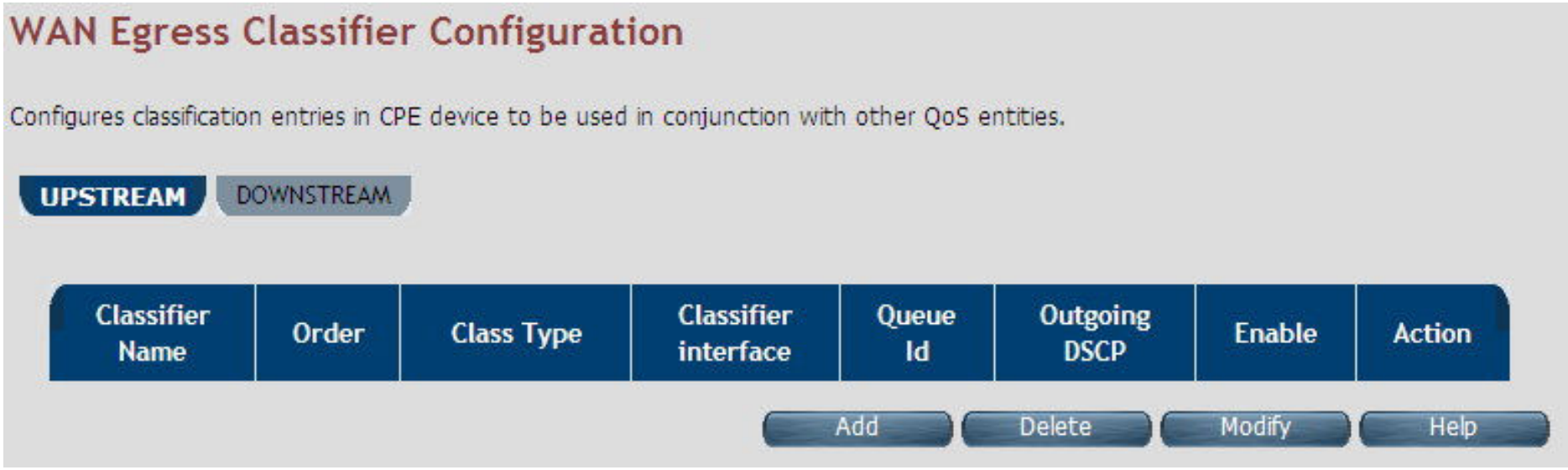


Figure 4.11.3 Class Configuration

The screen contains the following details:

Fields in Class Configuration:

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 a traffic flow.
Delete	Delete button for deleting selected queue.
Modify	Modify button for modifying chosen queue.

When you click Add or Modify in the Classifier Configuration page, a screen is displayed as shown in Figure 4.11.3.1

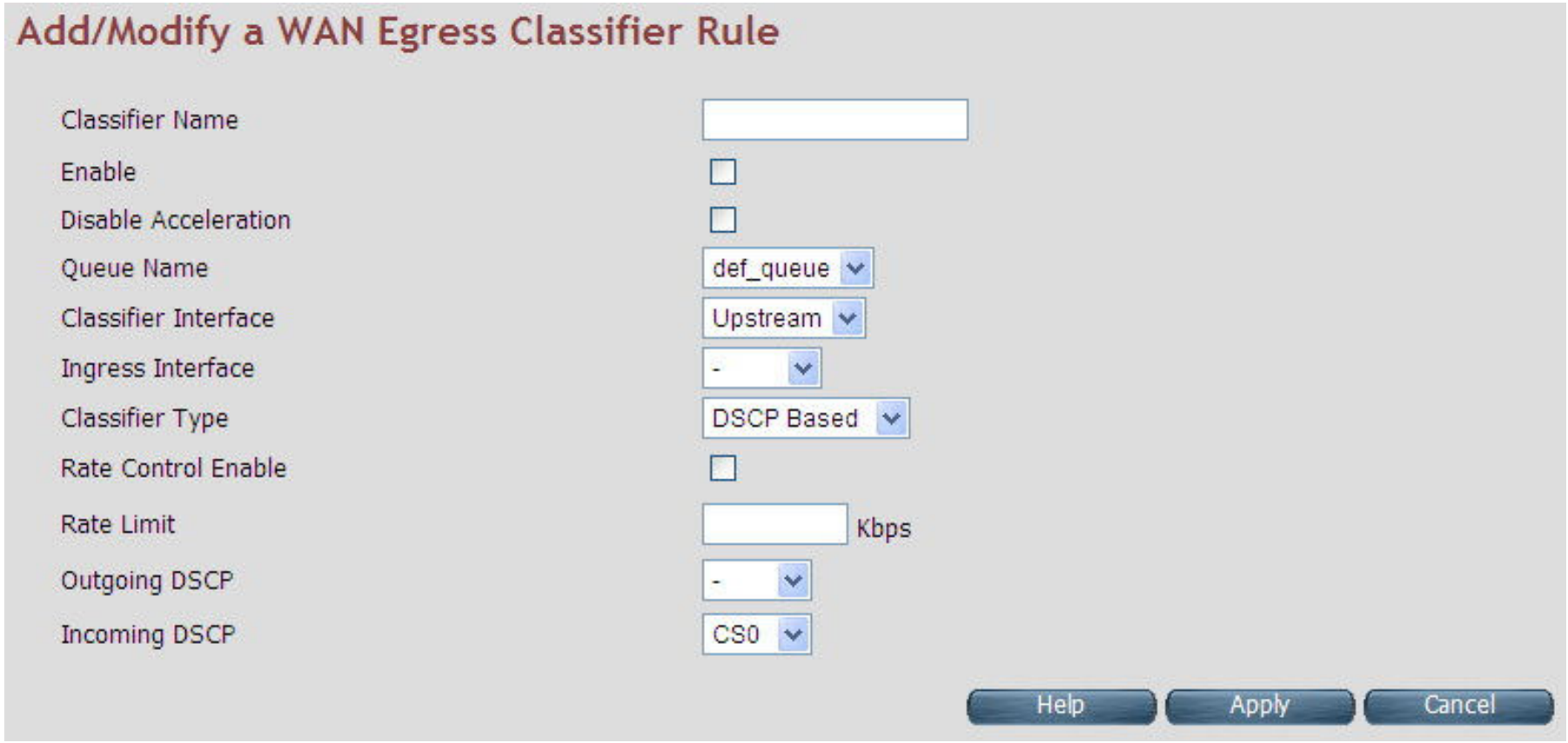


Figure 4.11.3.1 Add/Modify a Classifier Rule (DSCP Based)

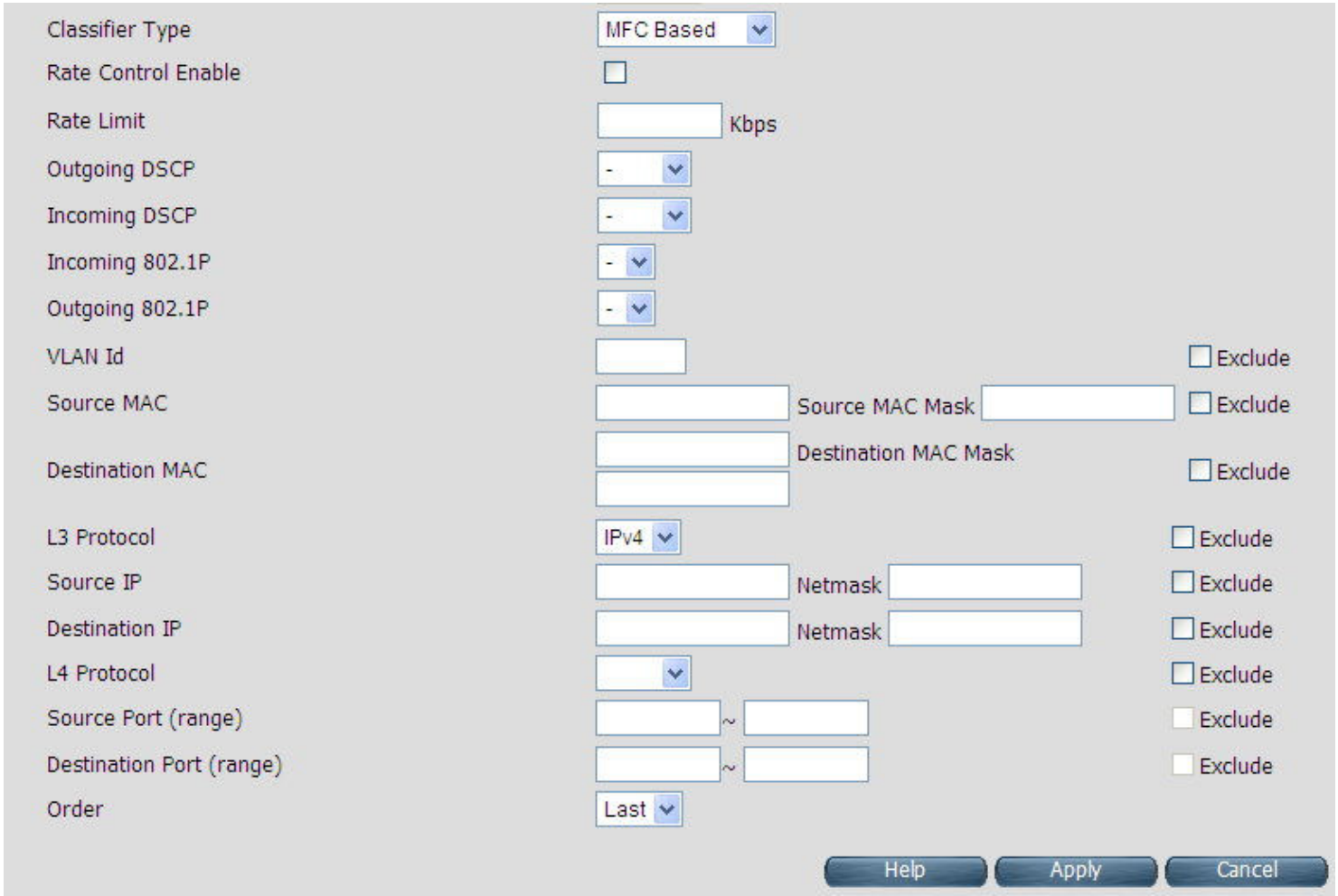


Figure 4.11.3.1 Add/Modify a Classifier Rule (MFC Based)

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	Dropdown 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

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

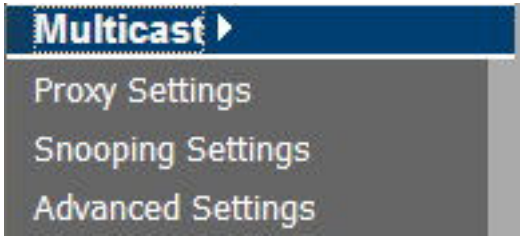


Figure 4.12 Multicast Options

4.12.1 Proxy Settings

For configuring 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

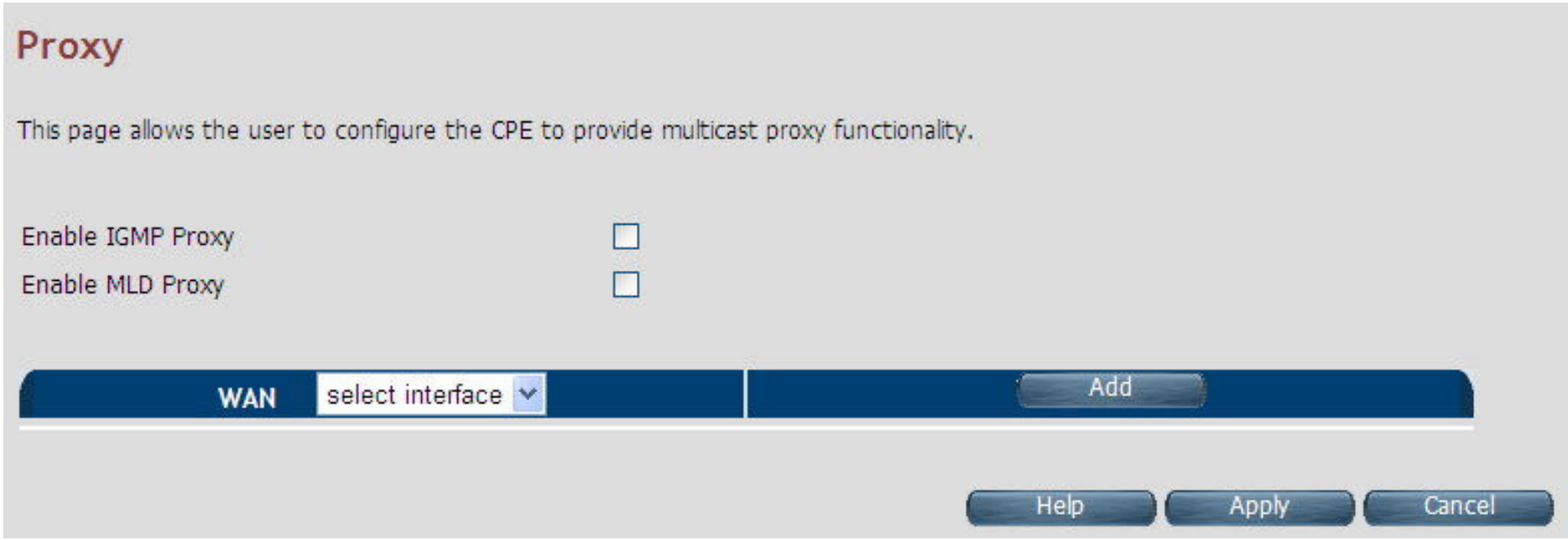


Figure 4.12.1 IGMP Proxy

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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

4.12.2 Snooping Settings

For configuring 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 4.12.2

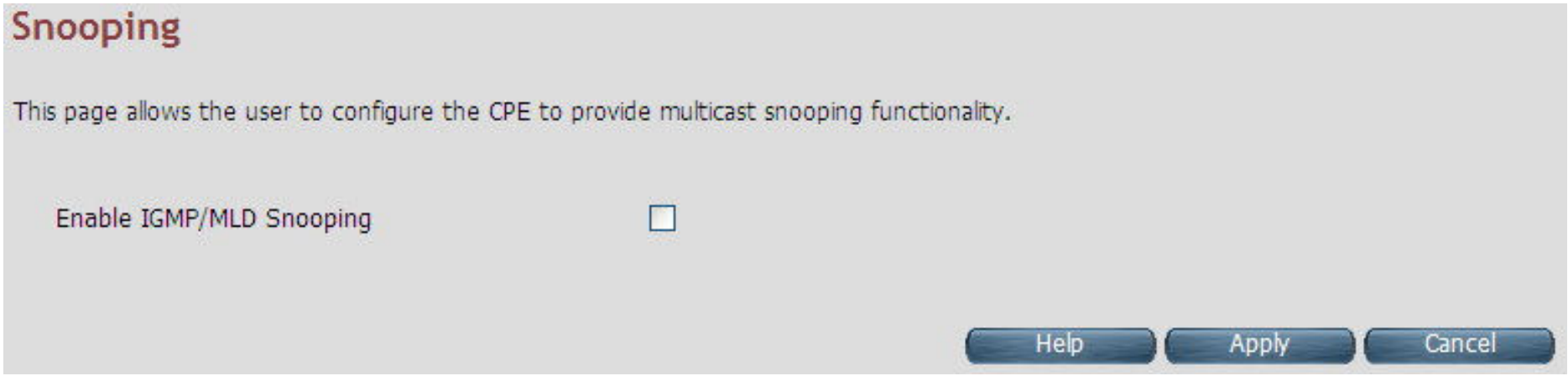


Figure 4.12.2 IGMP Snooping

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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

4.12.3 Advanced Settings

For configuring 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 4.12.3

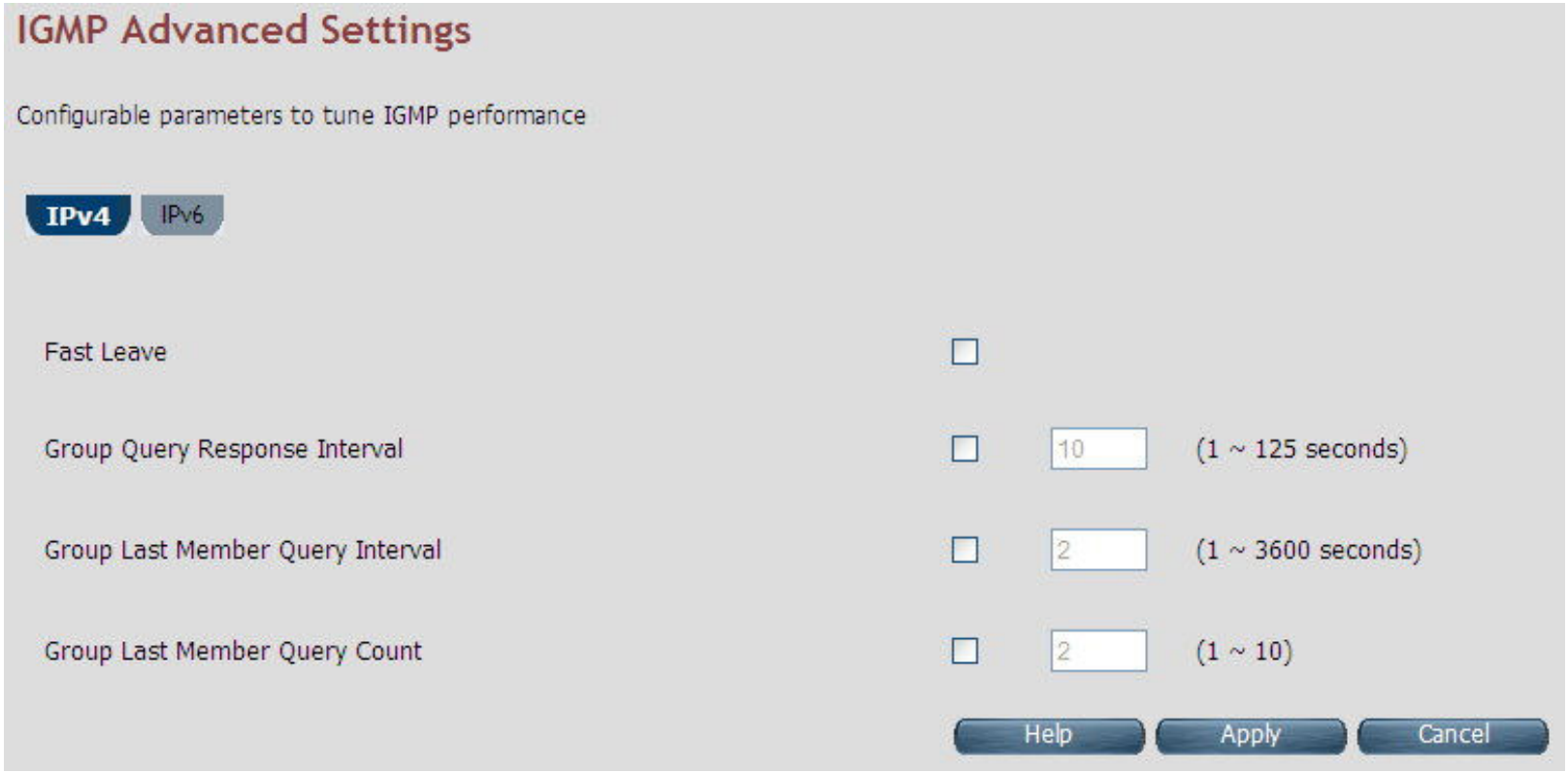


Figure 4.12.3 Multicast Advanced Settings

The screen contains the following details:

Fields in Multicast Advanced Settings:

Field	Description
IPv4/IPv6	Choose the appropriate tab to configure either for IPv4 or IPv6.
Fast Leave	To enable or disable Fast-Leave support in IGMPv3/IGMPv2. The fast-leave will not to wait until group membership timers on multicast routers have expired, but quickly send a group-specific query and if not report 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 the IPv6 tab.

4.13 IPsec

When clicking the IPsec on the left navigation bar of the NV-600W CPE homepage. The menu below includes the sub-menu **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 you click the **Tunnel Mode** link (**IPsec > Tunnel Mode**) on the left navigation bar, a screen is displayed as shown in Figure 4.13.1

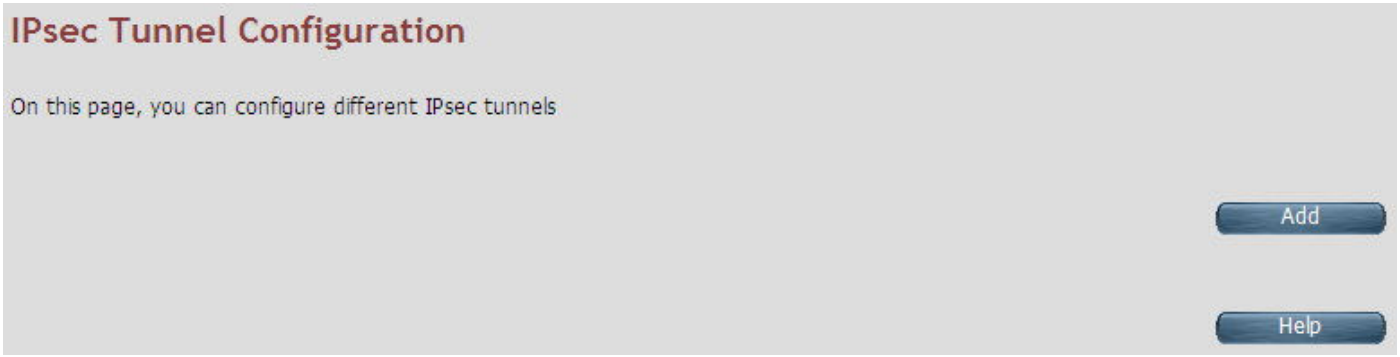


Figure 4.13.1 IPsec Tunnel Configuration

When you click Add button in the IPsec Tunnel Configuration page, a screen is displayed as shown in Figure 4.13.1.1

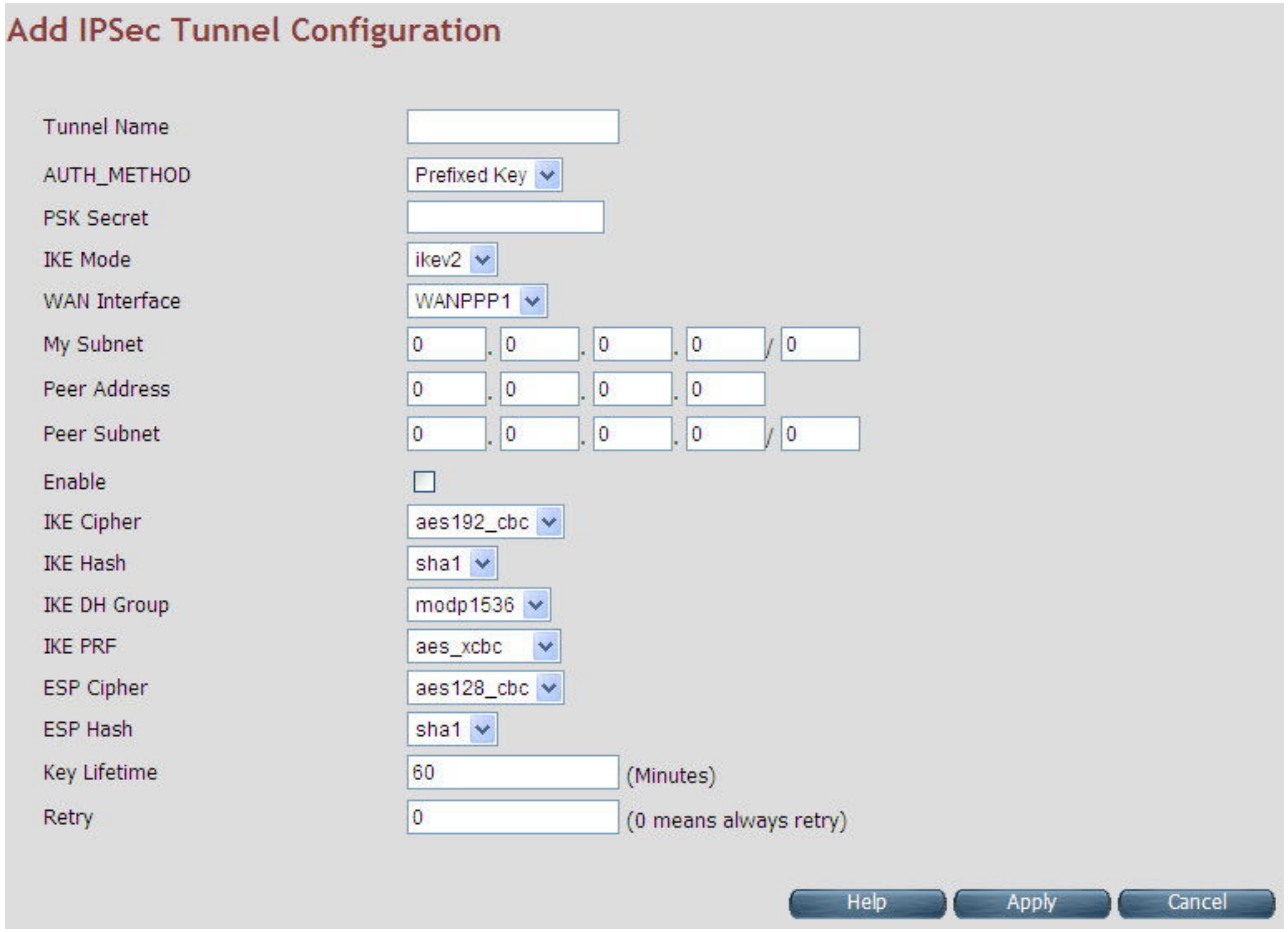


Figure 4.13.1.1 Add IPSec Tunnel Mode Configuration

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 the tunnel will 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 clicking on the IPv6 link on the left navigation bar of the NV-600W 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 4.14

Figure 4.14 IPv6 Options

4.14.1 IPv6 Setting

To enable or disable IPv6 functionality in CPE, click on 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.

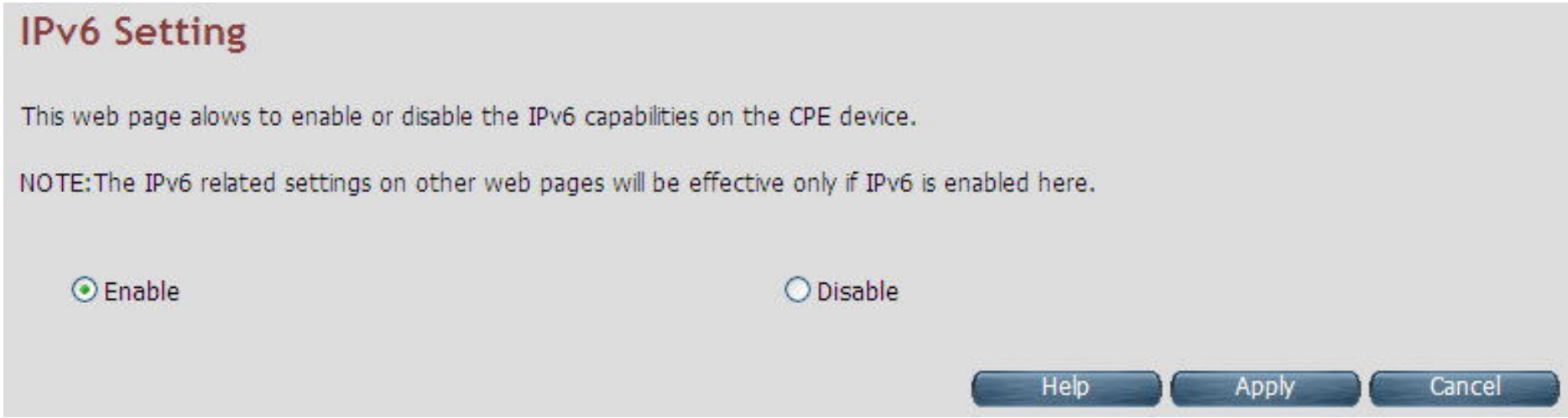


Figure 4.14.1 IPv6 Setting

The system wide IPv6 feature can be enabled or disabled through this web page. Select the appropriate control and click the **Apply** button for making the change effective in CPE. All other IPv6 features in CPE will 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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

4.14.2 6RD Configuration

The NV-600W supports IPv6 transition mechanism defined in 6RD (RFC 5569). For configuring the 6RD configuration, click on the **6RD configuration** link (**IPv6 > 6RD Configuration**) on the left navigation bar. A screen is displayed as shown in Figure 4.14.2

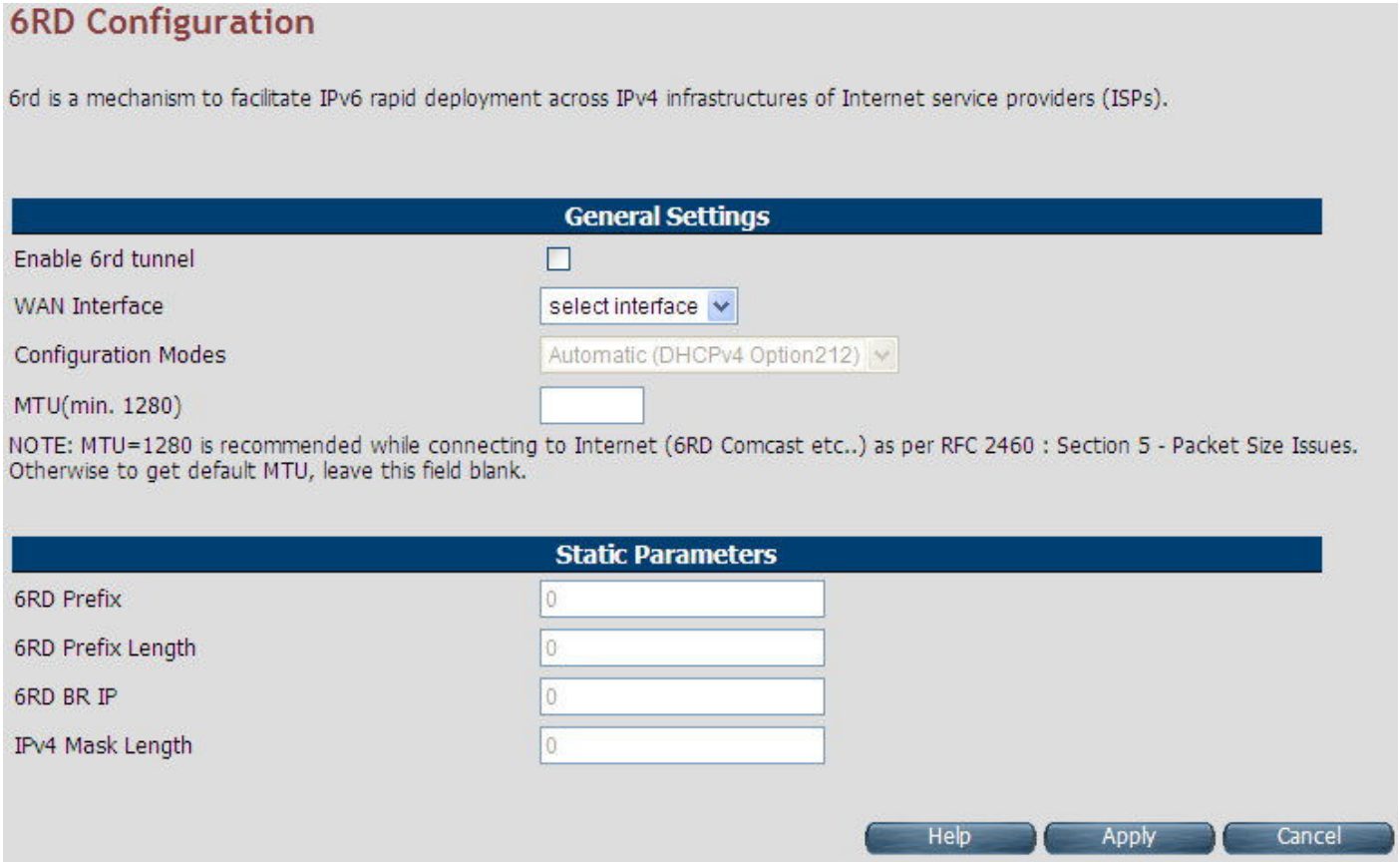


Figure 4.14.2 6RD Configuration

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, you 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 Border Relay's IPv4 address.
IPV4 Mask Length	IPv4 address Mask Length.

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

4.14.3 DS-Lite Configuration

The NV-600W supports DS-Lite configuration mechanism. For configuring 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 4.14.3

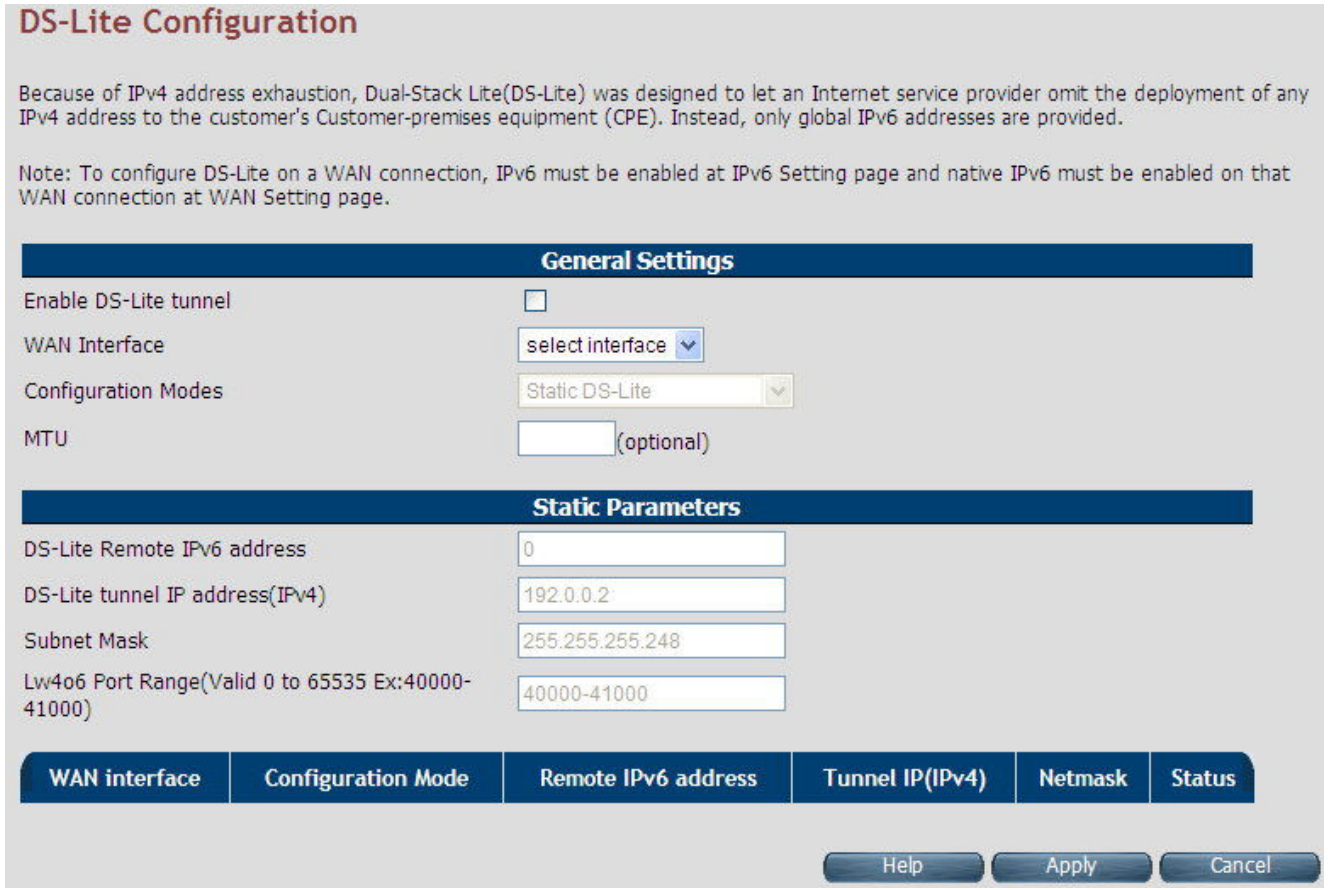


Figure 4.14.3 DS-Lite Configuration

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	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 you 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 you have entered.
- Click **Cancel** to exit from this page without saving the changes.

4.15 Diagnostics

When clicking on the **Diagnostics link** on the left navigation bar of the NV-600W 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

For configuring 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

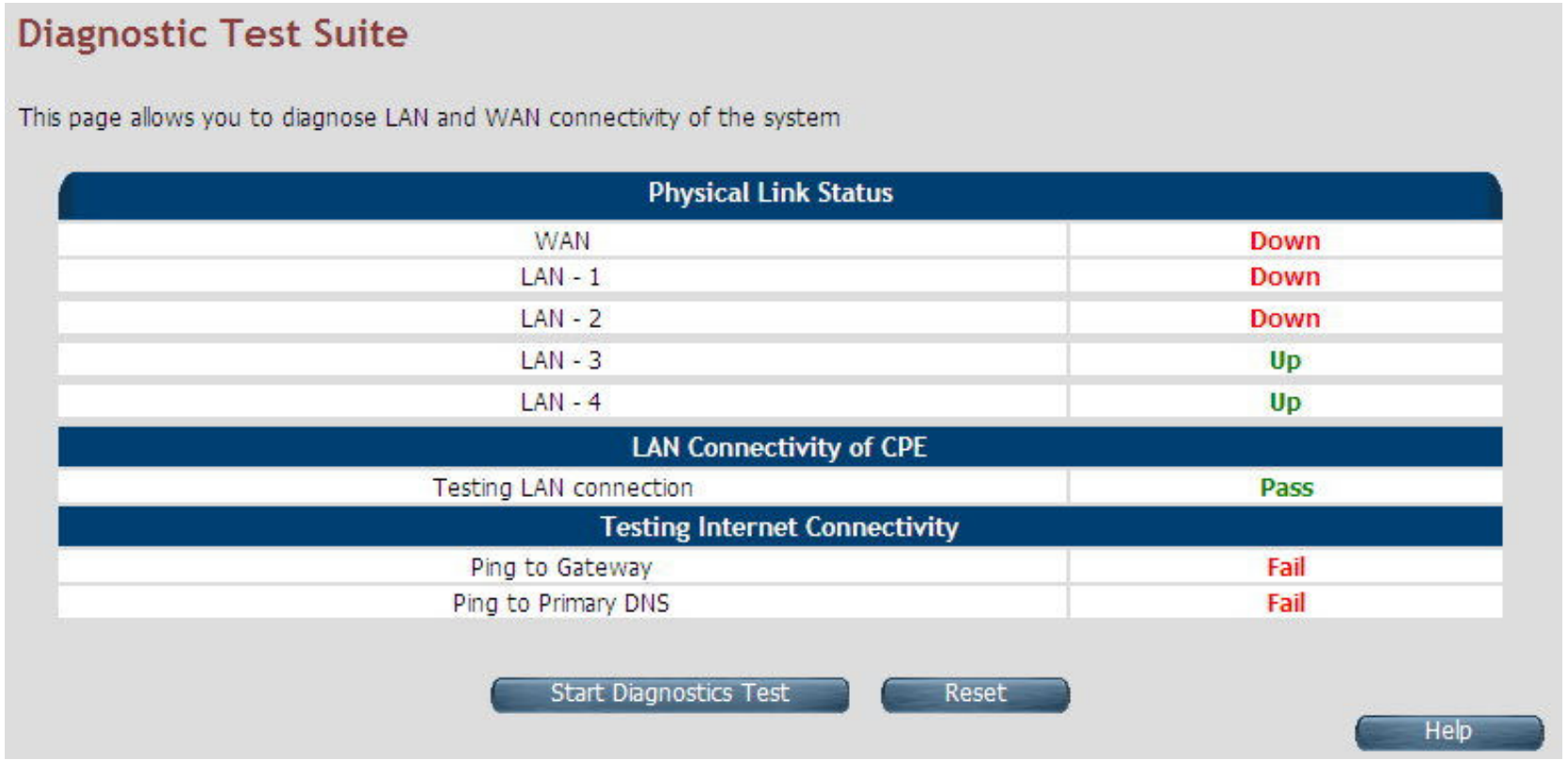


Figure 4.15.1 Diagnostic Test Suite

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.

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 Dependent interface	**Signal**	Media Dependent 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

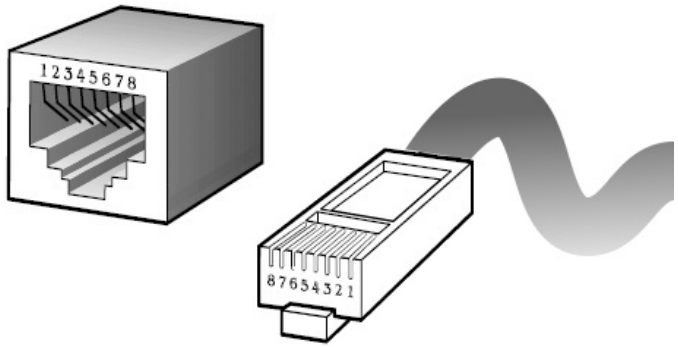


Figure A-1 Standard RJ-45 receptacle/connector

Note:

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

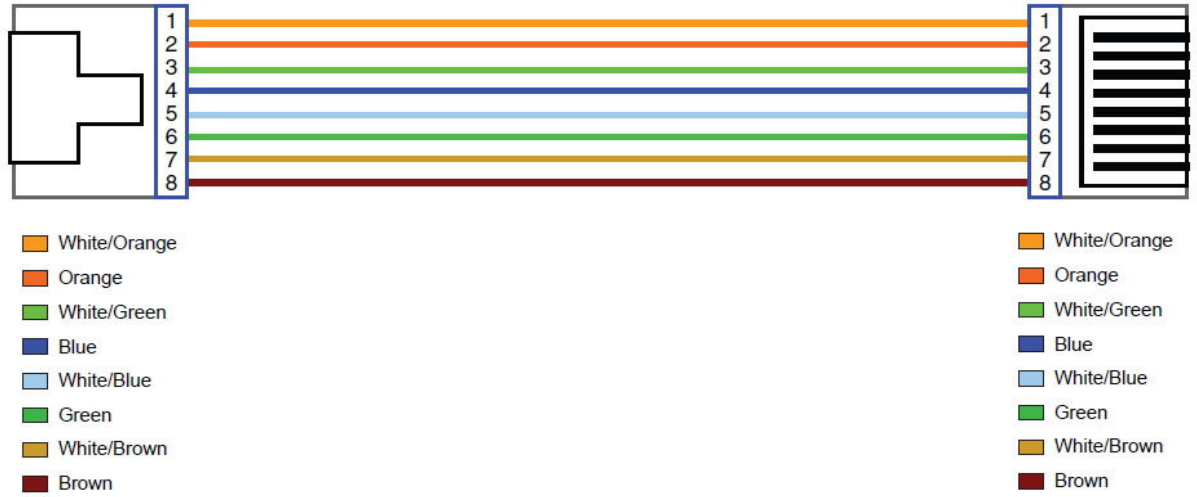


Figure A-2 Pin Assignments and Wiring for an RJ-45 Straight-Through Cable

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-6)

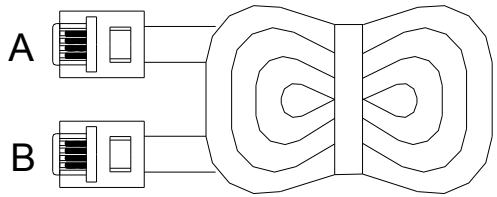


Figure A-4 Telephone cable

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-3)

Table A-3 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

- Compliant with IEEE 802.11b/g/n wireless standard with 2T2R (Up to 300 Mbps)
- Supports WPS, PIN, PBC
- Supports WEP,WPA,WPA2,TKIP,AES
- Supports QoS-WMM,WMM-PS
- Low power with Advanced Power Management
- Supports ATM and PTM transmission mode auto detection (ADSL backward compatible)
- Supports high bandwidth up to 100Mbps symmetric over line ports
- Supports 8a, 8b, 8c, 8d, 12a, 12b, 17a, 17b, and 30a band profile
- Supports 997, 998 band plan
- Supports ATM-TC,ATM and AAL5 (ATM Flow Throughput / OAM Cell Filter and Forwarding / AAL5 SAR:PVC / ATM Traffic Class / ATM PVC Shaping / ATM PVC Scheduling)
- Supports ATM Total Upstream Priority Queues
- Supports uPnP/PPPoE/PPPoATM/IPv4/IPv6/NAT/NAPT
- Supports static routing for IPv4 and IPv6 forwarding
- Supports Firewall functions contains Packet filtering, DMZ, Mac Address based filtering, Parental Control, Application based filtering
- Supports DHCP Server/ DHCP Relay/ DHCP Client/ DHCPv6 Client/ DHCPv6 Server/ DNS/ DNS Proxy or Relay/ DNSv6 Proxy or Relay/ NTP Client/HTTP1.1 server
- Supports Multicast IP table/IGMP v3 Proxy and Snooping
- Supports IEEE 802.1p VLAN Priority and mapping to DSCP

- Supports 802.1q Tag Vlan/Port base Vlan
- Supports HTTP/HTTPS(SSL) web management
- Supports remote management and monitor
- Supports configuration backup and restore
- Provides surge protection for Line port
- Supports Router & Switch(Bridged) mode selection
- Supports 8 queue MFC/DSCP both type QoS.
- Supports Dual Firmware Image Backup
- Supports Dying Gasp

Notes:

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

Product Specification

Standard:	IEEE802.3/802.3u/802.3z/802.11b/802.11g/802.11n standards ITU-T G992.1/G992.3/G992.5/G993.1/G997.1/G993.2 standards
Wireless Frequency Range	2.4GHz
Physical Interface:	4 x RJ-45 10/100/1000Mbps Ethernet port 1 x RJ-11/Terminal Block connector for VDSL2 line port 1 x RJ-11 connector for POTS/ISDN device 2 x 2dBi Antennas. (5dBi antennas optional) 1 x WPS Button

	1 x Reset Button for resetting to factory default MTU: 1680 bytes
Flow control:	Full duplex: IEEE 802.3x Half duplex: Back pressure
LED Indicators:	1 x Power LED 4 x Link/Active Status for Ethernet port 1 x Link LED for VDSL2 port 1 x WPS LED 1 x WLAN LED
Switch method:	Store and forward
Typical Power Consumption:	7.92 W
Power Input:	Input Voltage: 12 VDC (Commercial-grade power adapter)
EMC:	EMI Compliant: FCC EMS Compliant: CE mark
Operating Temperature:	0°C ~ 50°C (32°F ~ 122°F) Fan-less, free air cooling
Storage Temperature:	-20°C ~ 70°C (-4°F ~158°F)
Humidity:	10% to 90% (non-condensing)
Weight:	About 0.44 Kg.
Dimensions:	184 x 158 x 104 mm (7.2" x 6.22" x 4.1") with 2dBi Antenna
Chipsets:	Lantiq VRX

Appendix C: Router/Bridged Mode select

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

◆ Selecting the Router mode:

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

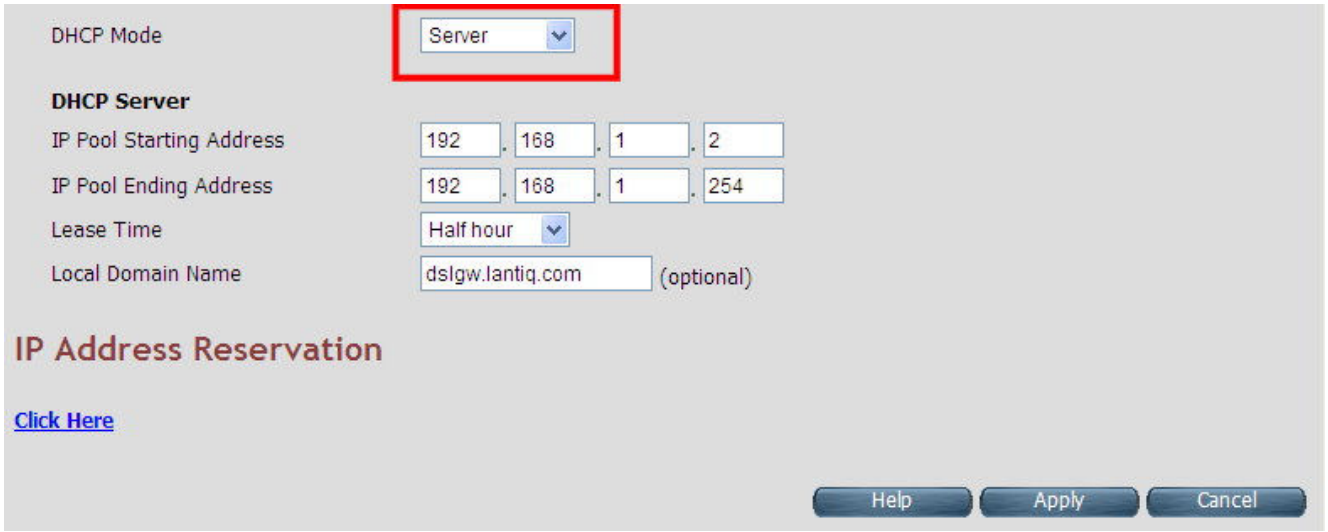


Figure C-1 DHCP Mode – Server

Note:

Please refer to the section 4.7.2 for configuring the DHCP Server settings.

2. Click the **WAN Setting** link (**WAN Setting > WAN**) on the left navigation bar to specify the WAN settings. Please uncheck the Auto Detect Enable option, and click **Add** to configure the WAN type.

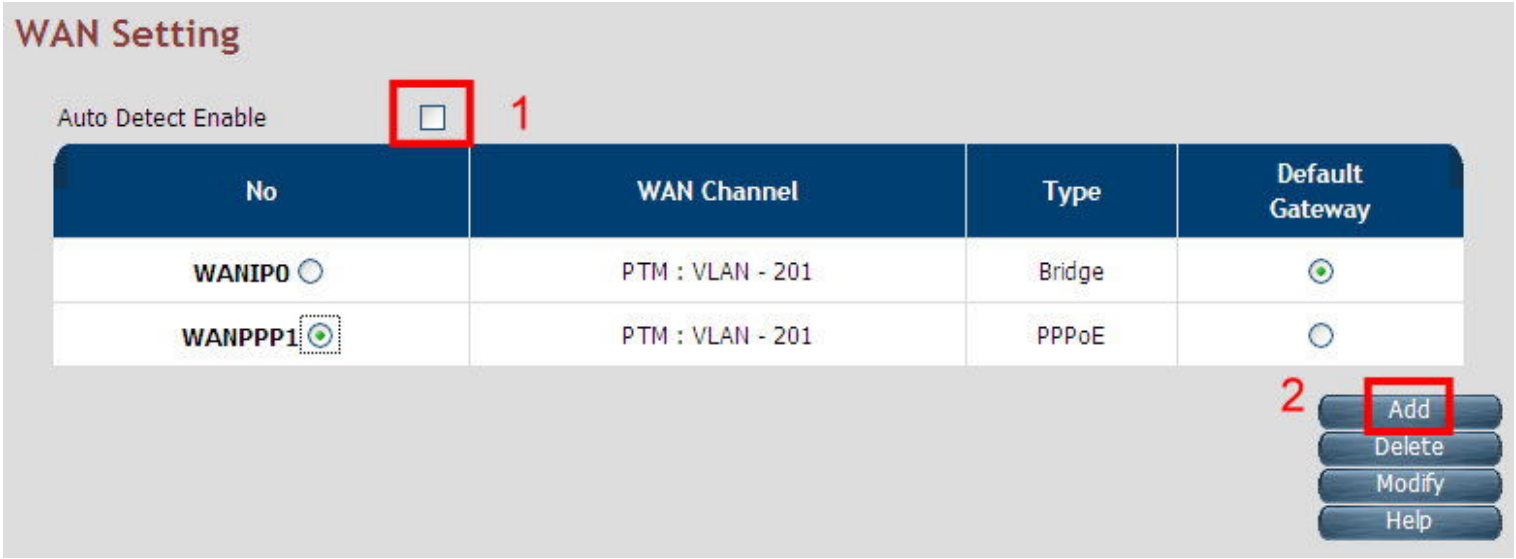


Figure C-2 WAN Setting

3. Please refer to the **section 4.5.6** for configuring the WAN type; the user can configure the Dynamic IP Address, Static IP Address, PPPoE mode.

Figure C-3 Configuring WAN Type

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

◆ Select the Bridged mode:

1. To configure the bridged mode settings, click the **LAN Settings** link (**LAN > LAN Settings**) on the left navigation bar. Then select the "Disable" at the DHCP Mode, and click Apply at any time during configuration to save the information that you have entered. A screen is displayed as shown in Figure C.4

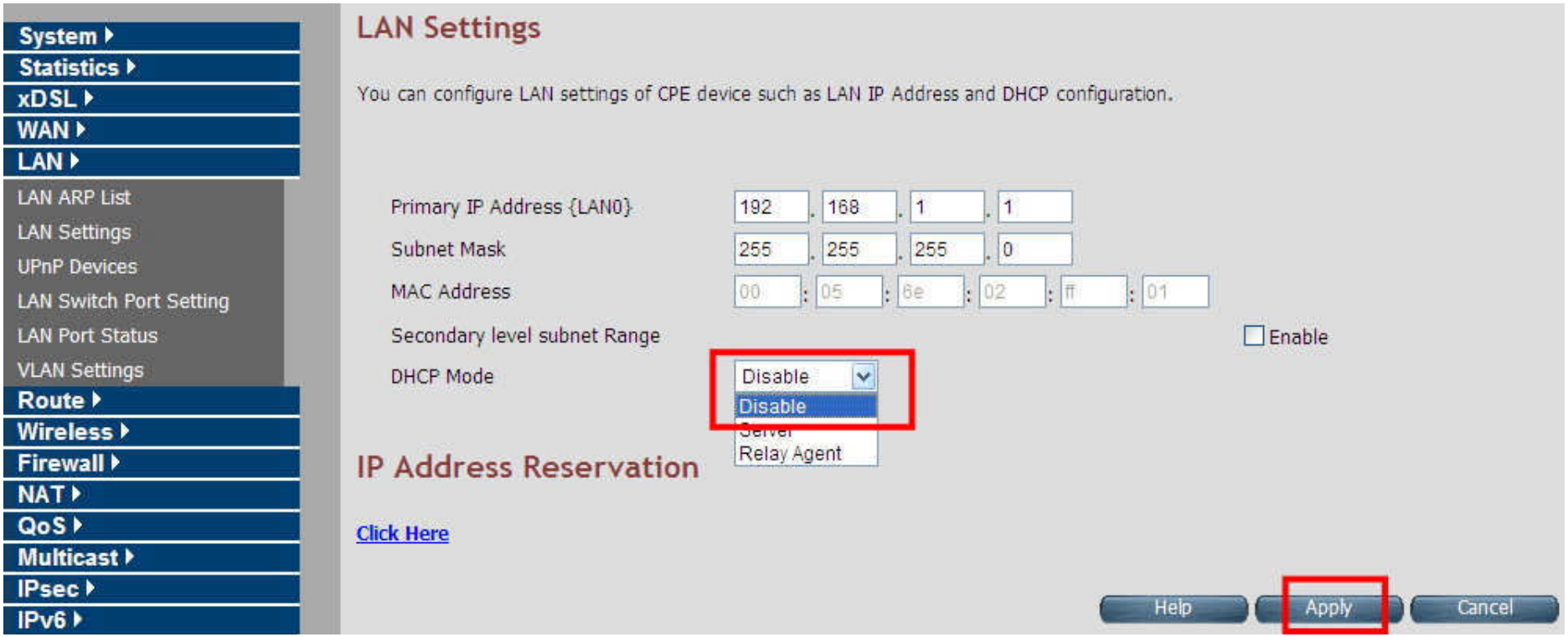


Figure C-4 DHCP Mode – Disable

2. Click the **WAN Setting** link (**WAN Setting > WAN**) on the left navigation bar to specify the WAN setting. Please modify WAN settings to Bridge. A screen is displayed as shown in Figure C.5

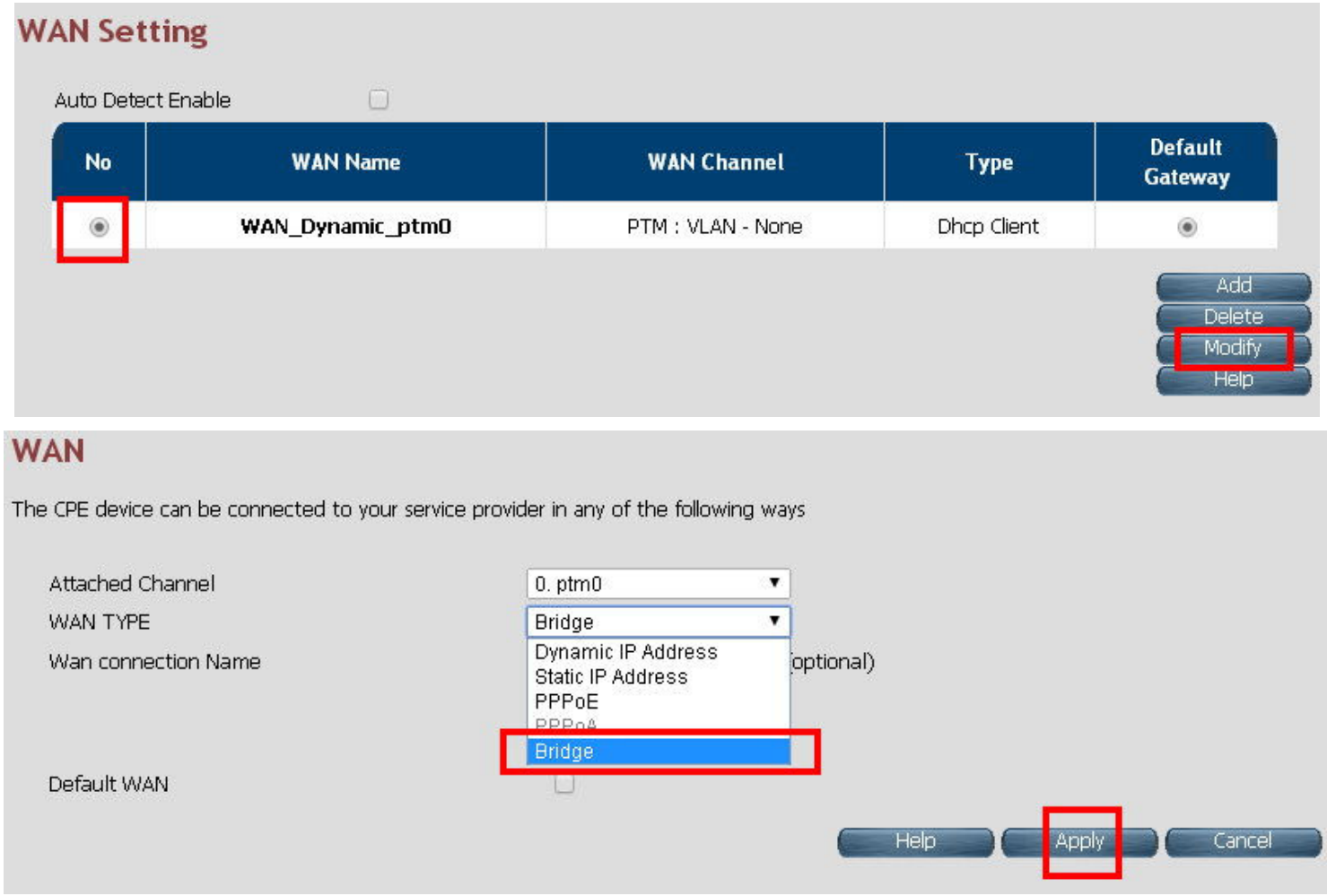


Figure C-5 WAN Setting

Appendix D: NV-600L & NV-600A/W Compatibility Table

The following shows the band profile and band plan compatibility table:

	Band Profile List		Band Plan List
0	VDSL2 Profile8a	0	Annex A M1_EU32
1	VDSL2 Profile8b	1	Annex A M9_EU64
2	VDSL2 Profile8c	8	Annex B 997-M2x-A (B05)
3	VDSL2 Profile8d	9	Annex B 997-M2x-M (B06)
4	VDSL2 Profile12a	10	Annex B 997-M1c-A-7 (B07)
5	VDSL2 Profile12b	11	Annex B 998-M1x-B (B08)
6	VDSL2 Profile17a	13	Annex B 998-M2x-A (B10)
7	VDSL2 Profile30a	14	Annex B 998-M2x-M (B11)
8	VDSL2 Profile17b	16	Annex B 998-M2x-B (B12)
		18	Annex B 998-M2x-NUS0 (B13)
		20	Annex C
		21	Annex C_8K
		22	Annex B 997-M2x-NUS0
		23	Annex C 1M1
		24	Annex C_8K 1M1
		25	Annex B 998E17-M2x-A
		26	Annex B 998E17-M2x-NUS0

Band Profile \ Band Plan	0	1	8	9	10	11	13	14	16	18	20	21	22	23	24	25	26
0 (8a)	X	X	X	O	X	X	X	X	X	X	X	X	X	X	X	X	X
1 (8b)	X	X	O	O	X	X	X	X	X	X	X	X	X	X	X	X	X
2 (8c)	X	X	X	X	X	X	X	O	X	X	X	X	X	X	X	X	X
3 (8d)	X	X	O	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4 (12a)	X	O	X	X	X	O	X	O	O	X	X	X	X	X	X	X	X
5 (12b)	O	O	X	X	O	O	O	O	O	O	X	X	X	X	X	X	X
6 (17a)	O	X	X	X	O	O	O	O	O	X	O	X	X	O	X	X	X
7 (30a)	O	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
8 (17b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Appendix E: 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 you 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 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. 2.2 Verify that the switch and attached device are power on. 2.3 Be sure the cable is plugged into both the switch and corresponding device. 2.4 Verify that the proper cable type is used and its length does not exceed specified limits. 2.5 Check the router on the attached device and cable connections for possible defects. 2.6 Make sure that the phone wire must be connecting NV-600W first, when powered on. 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-600L (CO) and NV-600W (CPE) when both are power on. NV-600L (CO) will do link speed function depending on phone wire length, therefore if NV-600L (CO) can't detect NV-600W (CPE) over phone wire while both power on, this will cause the link to fail. 3.2 Please check the phone wire, we recommend using 24-26 gauge twisted pair cables without rust. 3.3 Please reinsert power when changing the cable length or link time over 3 minutes.
Note:	The phone wire must meet CAT 3 standard or above and **without clustering**, otherwise it will cause more cross talk, reducing the 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. VDSL2 was the newest and most advanced standard of digital subscriber line (DSL) broadband wire line 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. VDSL2 is an enhancement to very-high-bit rate 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. 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+. 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 the 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) The signal-to-noise ratio, the bandwidth, and the channel capacity of a communication channel are connected by the Shannon–Hartley theorem. 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 protocols such as FTP, Iperf, NetIQ, the testing bandwidth outcome will be limited by TCP window size.
Solution:	We recommend testing VDSL2 bandwidth using Smartbits® equipment or IPERF program. The TCP window size must be set to 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-600W to replace my Quest DSL modem for my home. I was told any VDSL2 modem would work and give me higher communication speeds. It doesn't get me internet when hooked up. All lights come on but no Link light. Is this the complete wrong application for this unit?
Answer:	Please note NV-600W is a remote side (CPE side), it must be connected to the CO side to work.

	Tone mode, Band profile and band plan settings must be compatible with each other, if not; access error will show when applied. Please deactivate and activate once the settings have been changed.

8. Question:	We need to set up a default gateway on a NV-600 pair which is 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), you must set up a gateway to connect a different network segment. Regarding on how to configure a default gateway at switch (bridged) mode for crossing various network segments, please refer to the section 4.8.1 for your reference. Example for configuring the gateway from static routing: Destination LAN IP: 0-0-0-0 Subnet Mask: 0-0-0-0 Gateway: 255-255-255-0 **Note:** Static Routing functionality is used to define the connected Gateway between the LAN and WAN.

9. Question:	What can I do if I forgot my password?
Answer:	If you forgot your password, you must reset your router. This process will change all your settings back to the factory default. To reset the router, locate the reset button 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 192.168.1.1. When logging in, the default username and password are both "**admin**".

10. Question:	Is it possible to use ADSL2 IP DSLAM with the NV-600W?
Answer:	NV-600W support the ADSL Annex B backward compatible, therefore the NV-600W can connect to ADSL2 IP DSLAM.

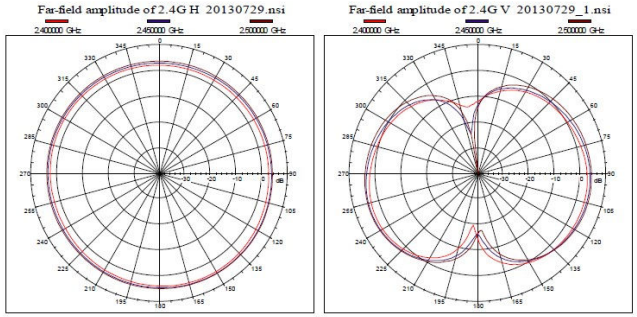
11. Question:	I have purchased a kit of NV600L and NV600W to extend the property WiFi network. They will sit in the property LAN which is served by a modem router and off an ADSL telecom connection. Each NV unit will have a fixed IP LAN address. All WiFi user addresses are provided by the gateway modem router. The reason for purchase is to extend the LAN service via phone lines to the WiFi access point. I would appreciate a simple configure set up for each unit. e.g. should the 600L be configured as a switch or router?. Do I need to configure a VDSL2 WAN between the 600L and 600W?
Answer:	Basically, use default settings that the network can be established. NV-600L should configure to switch mode (default mode), and NV-600W configure to router mode (default mode).

12. Question:	What is the maximum Ethernet frame MTU for these routers?
Answer:	NV-600W maximum Ethernet frame MTU is 1680 bytes.

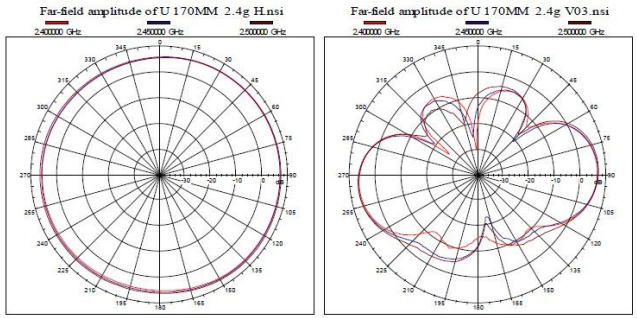
13. Question:	We have a customer who previously had the NV-600W (regular antenna) and we sent them a NV-600W with the 5db antenna (high power output) to replace the original unit when it failed, but the new unit with 5db antenna has less coverage than the original unit. Can you please send me the NV-600W wireless configuration settings to optimize the range of the high output antenna? If they are the same, why is the NV-600W with the 5db antenna, providing less coverage? Please advise.

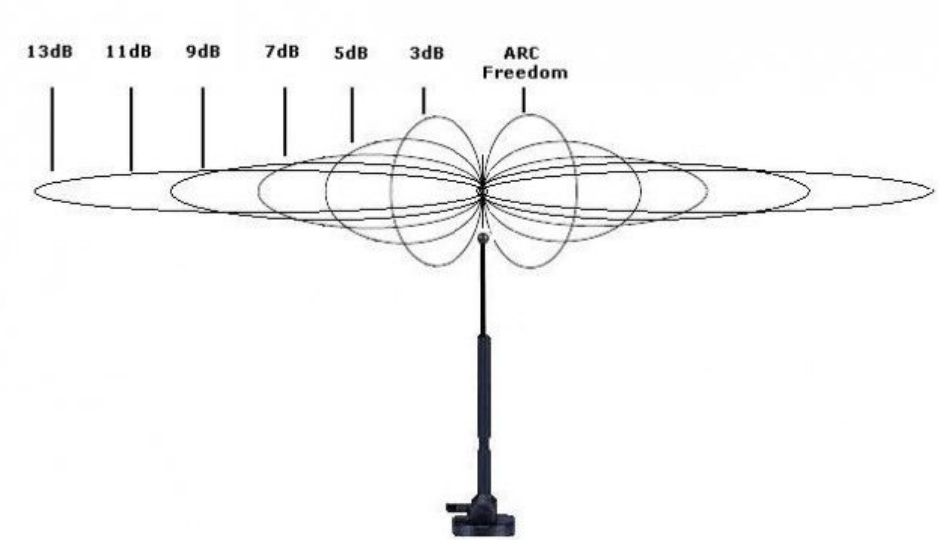
Answer:	Please note that the two antennas have almost the same coverage range, the difference between the two antennas is the Gain pattern shape (the 5dBi Gain pattern shape is butterfly and the 2dBi Gain pattern shape is chubbier), and also the 5dBi antenna has higher penetrating power (ex. Through walls). So regarding this issue, we don't think that the 5dBi is providing less coverage, we think is because of the Gain pattern shape. Furthermore, the actual performance will vary depending on the environment factors.

Gain Pattern 2dBi Antenna



Gain Pattern 5dBi Antenna





System Diagnostics

Power and Cooling

If the POWER indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or internal power supply as explained in the previous section. However, if the unit power is off after running for a while, check for loose power connections, power losses or surges at the power outlet. If you still cannot isolate the problem, then the internal power supply may be defective. In this case, please contact your local dealer.

Installation

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

Transmission Mode

The transmission mode for RJ45 ports is Giga Ethernet, for RJ-11 port is auto-negotiation VDSL2. 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 you are using a full-duplex device that does not support auto-negotiation, communications can be easily lost (i.e. reset to the wrong mode) whenever the attached device is reset or experiences a power fluctuation, the best way to resolve this problem is to upgrade these devices to a version that support 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 you have completed all the preceding diagnoses, then contact your 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 radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

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

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

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

FCC Warning

This equipment has been tested, 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

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

WEEE Warning

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

Warranty

The original 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 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 SJ/T 11364/2014 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 SJ/T 11364-2014 标准规定的限量要求。						

上述规范仅适用於中国法律