ALL126AS3

VDSL2 100 Mbit Slave/Bridge Vectoring

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.

ALLNET' ALL126AS3 is a management of the VDSL2 CPE router that leverages the extraordinary bandwidth promise of VDSL2 (max. 100Mbps symmetric) technology, the next step in the delivery of new high-speed Internet applications in commercial environments. Quick, easy, economical to install and maintain, the ALL126AS3 works over existing copper wire infrastructure. ALL126AS3 is a CPE
(Customer Premise Equipment) device. And compitable with the NV-802S(8Ports VDSL2 IP DSLAM) and NV-600L (VDSL2 CO Router).
ALLNET ALL126AS3 will allow operators worldwide to compete with cable andsatellite operators by offering services such as HDTV, VOD, videoconferencing, high speed Internet access and advanced voice services including VoIP, over a standard copper telephone cable.ALLNET NV600A is seen by many operators as an ideal accompaniment to a FTTP rollout, where for instance fiber optic is supplied direct to an apartment block and from there copper cable is used to supply residents with high-speed VDSL2.

Caution:

The ALL126AS3 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. ALL126AS3 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

Chapter 1. Unpacking Information

1.1 Check List

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

Package Contents:

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

Notes:

1. Please inform 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 ALL126AS3 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 ALL126AS3 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 ALL126AS3 has 2 pre-installed rubber feet.**

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 ALL126AS3 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 port must be made using Category 5 UTP/STP or above for 100 Mbps, Category 3, 4 UTP for 10Mbps.

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

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

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

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

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

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

RJ-11 Pin out Assignments

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

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 ALL126AS3(CPE) bridge side (point to point solution). Take note that ALL126AS3 line port cannot be used at the same time. Either RJ-11 port is connected or terminal block is connected using a straight connection (Figure 2.4) or cross-over connection(Figure 2.5)

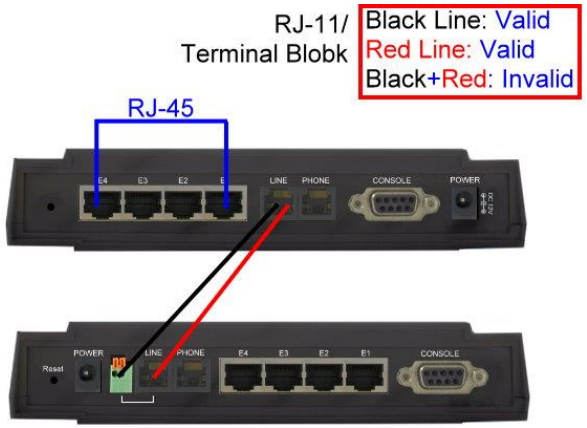


Figure 2.1 ALL126AS3 line ports straight connection

- 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 Cable bridge or Router connections to avoid any confusion or inconvenience in the future when you attached to high bandwidth devices.
3. RJ-11 (VDSL2 Line port) use **24 ~ 26** gauge with twisted pair phone wiring, we do not recommend 28 gauge or above.
4. Be sure phone wire has been installed before the ALL126AS3 boot.

2.6 VDSL2 Application

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

2.6.1 Connect the NV-600L and the ALL126AS3 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 ALL126AS3 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 ALL126AS3 to LAN Devices

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

2.6.3 Run Demos and Tests

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

Chapter 3. Hardware Description

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

ALL126AS3 Outward

3.1 Front Panel

The figure shows the front panel. (Figure 3.1)

Figure 3.1 Front Panel(ALL126AS3)

3.2 Front Indicators

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

Table 3-1 LED Indicators Description and Operation

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

Note:

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

3.3 Rear Panel

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

Figure 3.2 Rear Panel

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

Table 3-2 Description of the router rear connectors

Connectors	Type	Description
Reset	Tact switch Button	The reset buttons 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 to an Ethernet equipped device.
Link (WAN)	RJ-11/Terminal Block	For connecting a VDSL2 bridge. (**Do not** use RJ11 and Terminal Block at the same time.)
CONSOLE	RS-232	For connecting a PC with RS-232 serial port over a D-SUB Cable

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

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

Note:

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

- 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.

Chapter 4. Configure the ALL126AS3 Via Web Browser

The ALL126AS3 provides a built-in HTML based management interface that allow user configure the ALL126AS3 via Internet Browser. Best viewed at using the Chrome or Firefox.

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 192.168.16.254 (ALL126AS3) 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

4.1.1 Home

After successful login using the username **admin**, the home page of ALL126AS3 is loaded in web browser for ALL126AS3. Uesr can aslo click the "Home" on the left navigation bar. The home page displays the information screen as shown in Figure 4.1.1

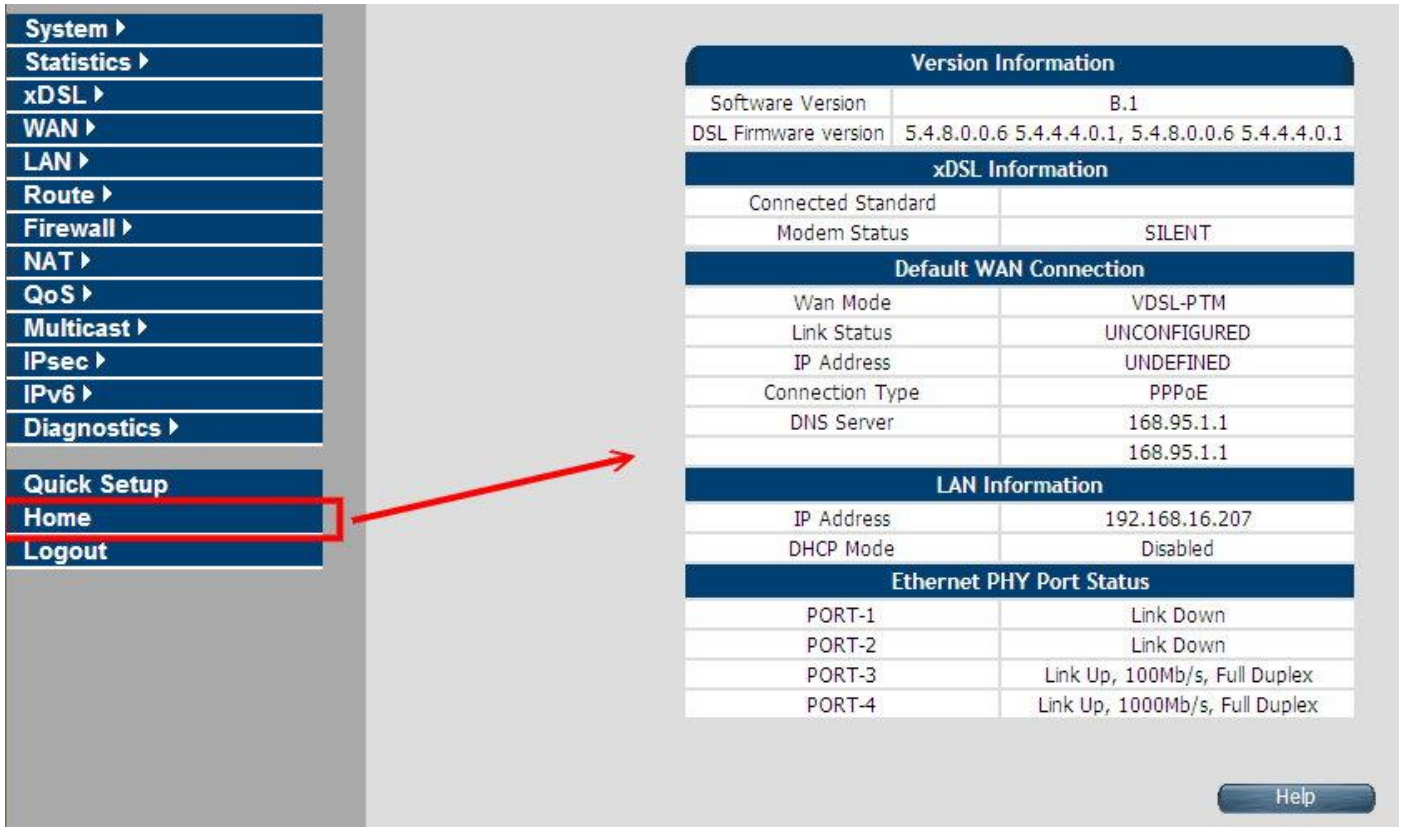


Figure 4.1.1 Home Information

The screen contains the following details:

Fields in Home page

Field	Description
Version Information	
Software Version	Shows the current version of ALL126AS3 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, TELNET or UPnP sessions.
DHCP Mode	Shows the DHCP Mode on LAN interface of CPE device.
Ethernet PHY Port Status	

PORT-1 ~PORT-4	Shows the status of first to fourth ethernet port of CPE device.

4.1.2 Quick Setup

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

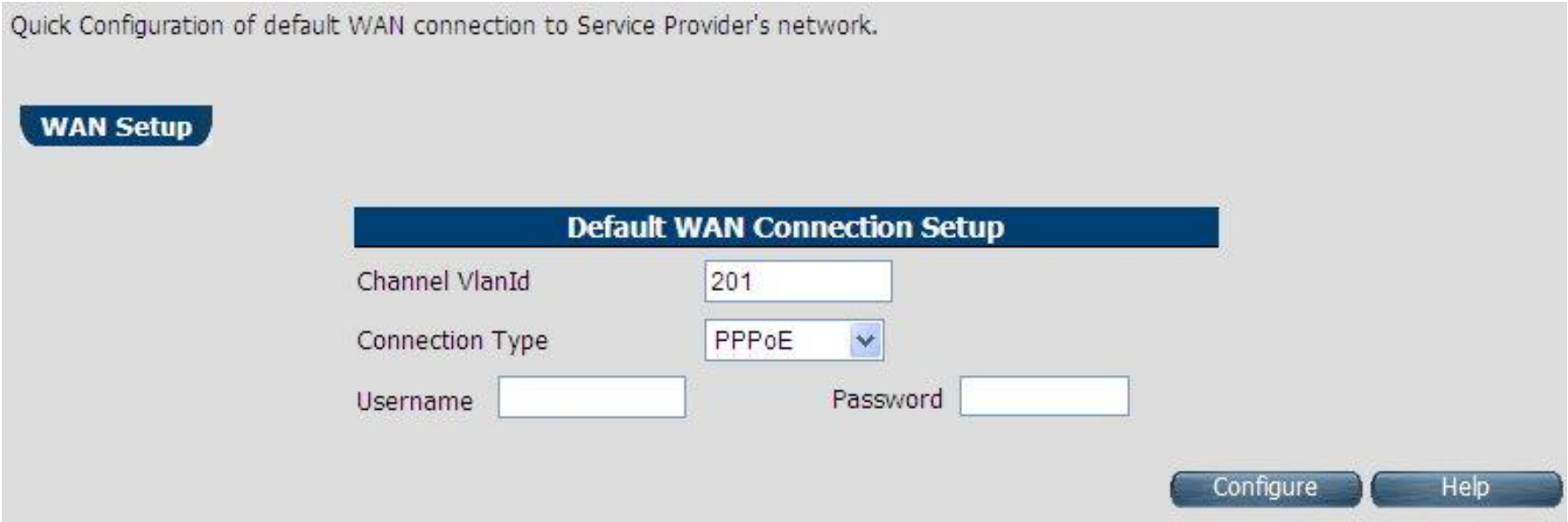


Figure 4.1.2 Quick Setup

◆ **WAN Setup**

When the user clicks on Quick Setup, the **WAN Setup** tab is displayed as shown in Figure 4.1.2.1. The **WAN Setup**enables the user

to configure the default WAN connection. The user has to supply fields and the CPE device will take all necessary actions to ensure the default WAN is configured. In case, the WAN connection is already existing in CPE device, the same gets re-created with newly supplied attributes from the user. The default WAN Setup configuration shows the Bridged status.

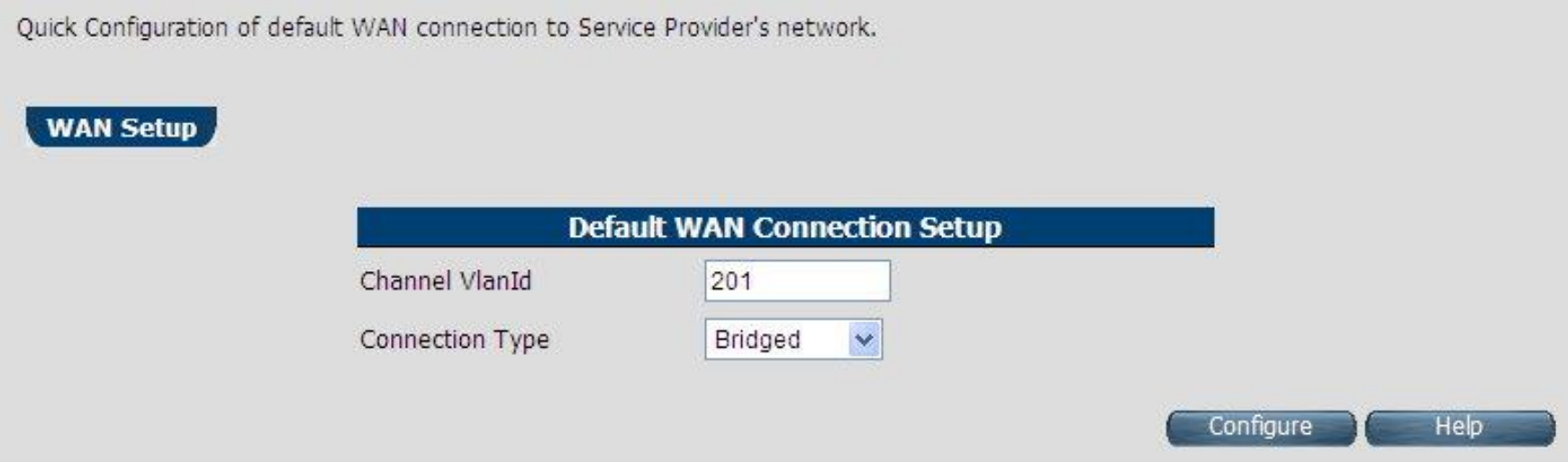


Figure 4.1.2.1 WAN setup Bridged

The screen contains the following details:

Fields in Home page

Field	Description
Channel VlanId	Specify VLAN Id. Reserved or internally used VLANs that can not 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.

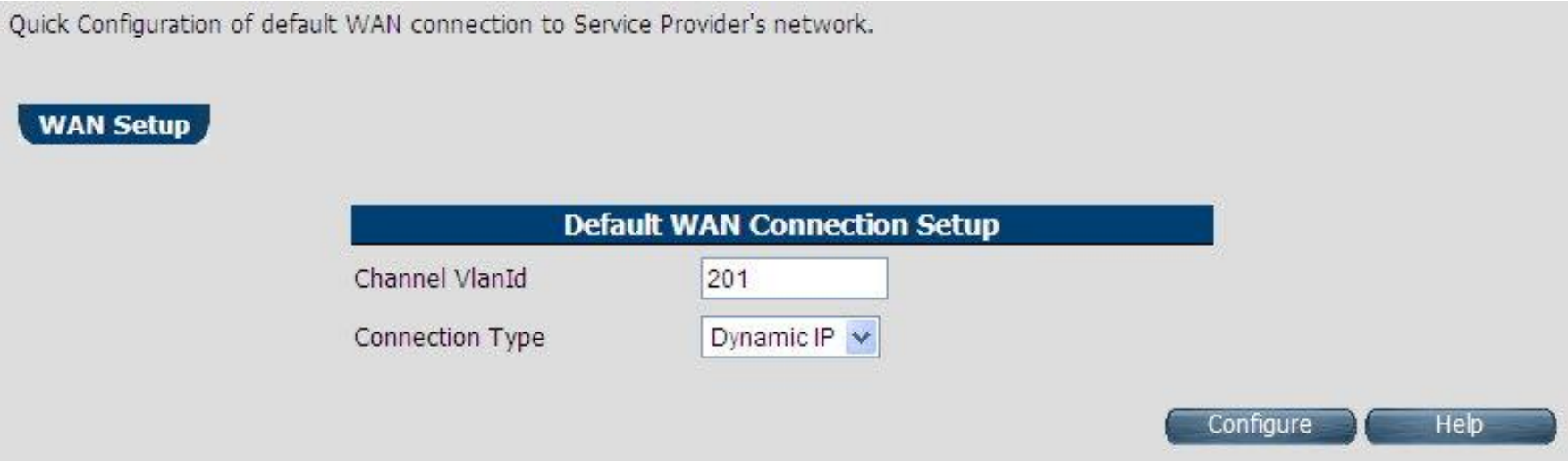


Figure 4.1.2.2 WAN setup Dynamic IP

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.

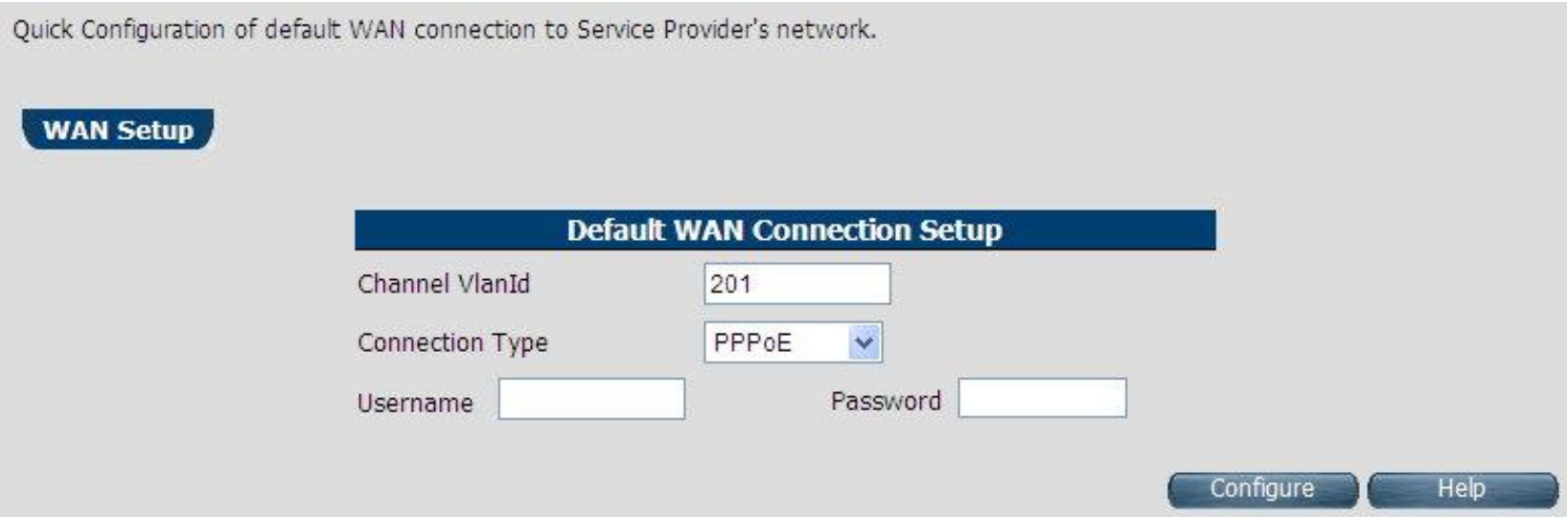


Figure 4.1.2.3 WAN setup PPPoE

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.

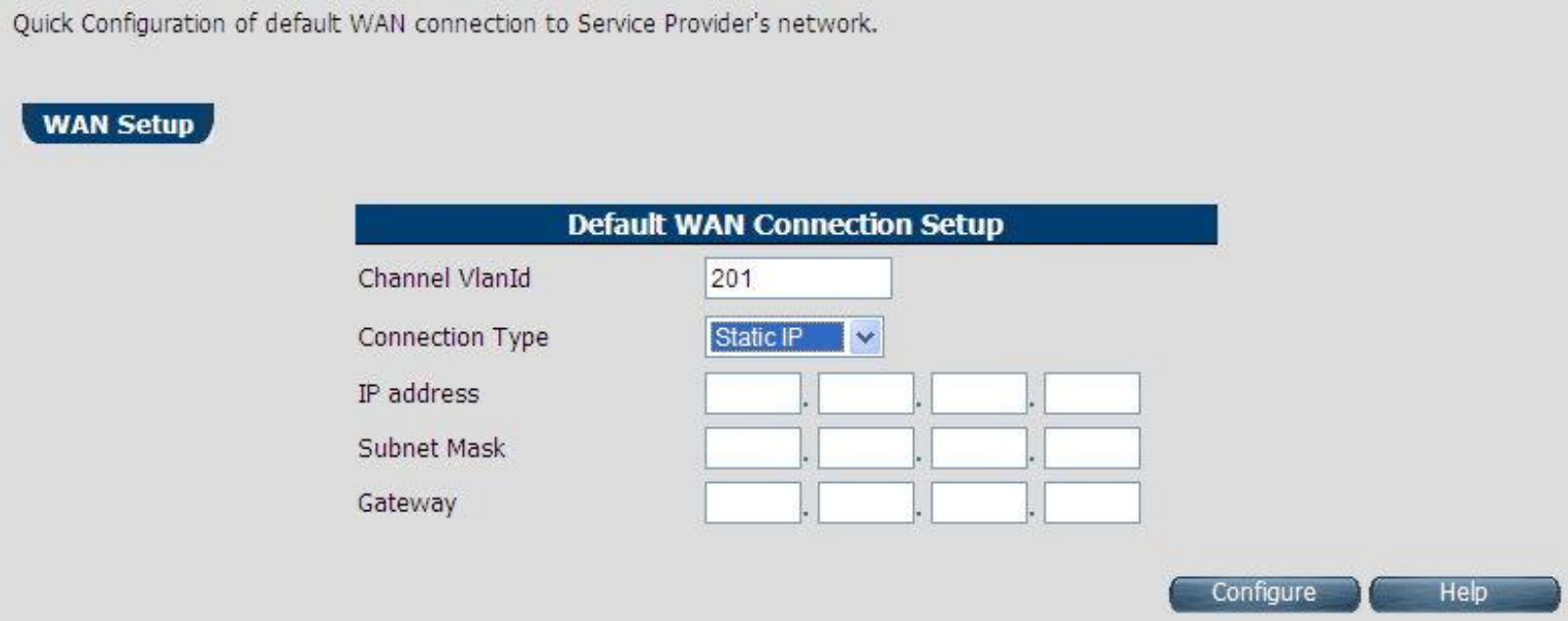


Figure 4.1.2.4 WAN setup Static IP

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 ALL126AS3 CPE's WAN link.
Subnet Mask	Specify the Subnet Mask of ALL126AS3 CPE's WAN link.
Gateway	Specify the Gateway address of the ALL126AS3 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.

4.2 Select the Menu Level

There is an easy Setup for end users at the setup of ALL126AS3 with **SYSTEM**, **Statistics**, **xDSL**, **WAN**, **LAN**, **Route**, **FIREWALL**, **NAT**, **QoS** , **Multicast**, **Ipsec** , **IPv6**, **Diagonstics**, **Quick Setup**, **Home**, **Logout** for more detail configurations.

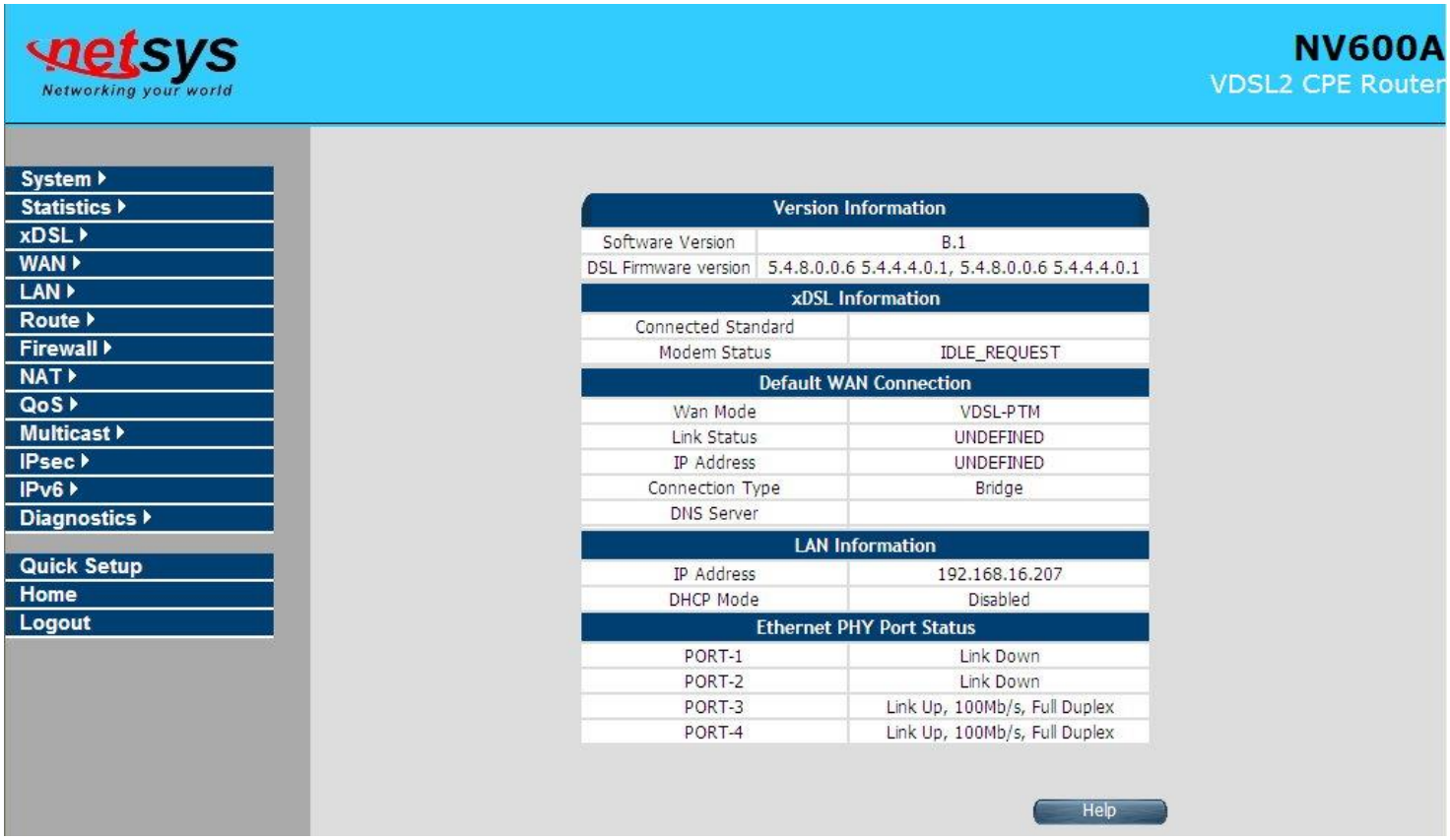


Figure 4.2 Select the Menu Level (ALL126AS3)

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 Config

To configure the host name of ALL126AS3, 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 Config

Fields in Host Name Config

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

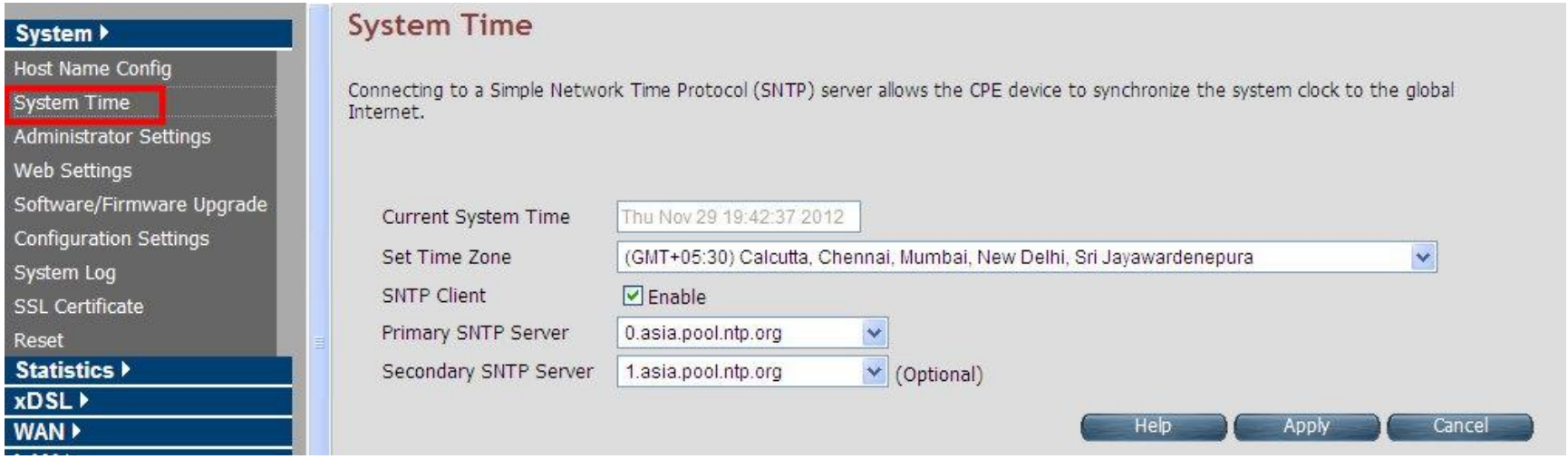


Figure 4.3.2 System Time Configuration

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, and 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

To change the password for the administrator, click the **Administrator Settings** link (**System** > **AdministratorSettings**) 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 AdministratorSettings

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

Fields in AdministratorSettings (Cont'd)

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

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

To update the system firmware, click the **Software/Firmware Upgrade** link (**System > Software/Firmware Upgrade**) on the left navigation bar. A screen displays the current version of ALL126AS3 Software running on the device as shown in Figure 4.3.5

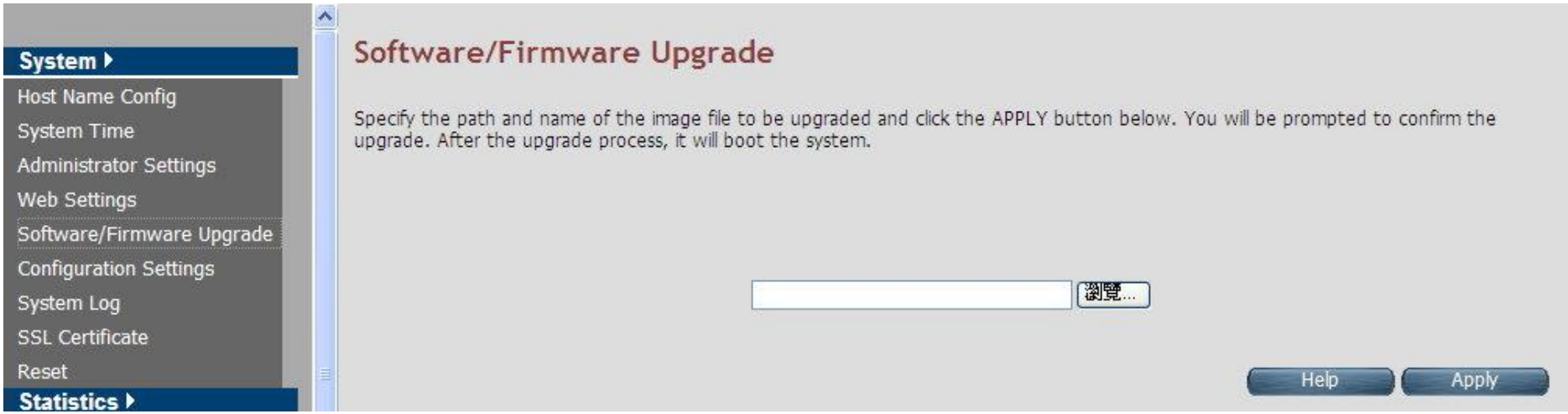


Figure 4.3.5 Software/Firmware Upgrade

- 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

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

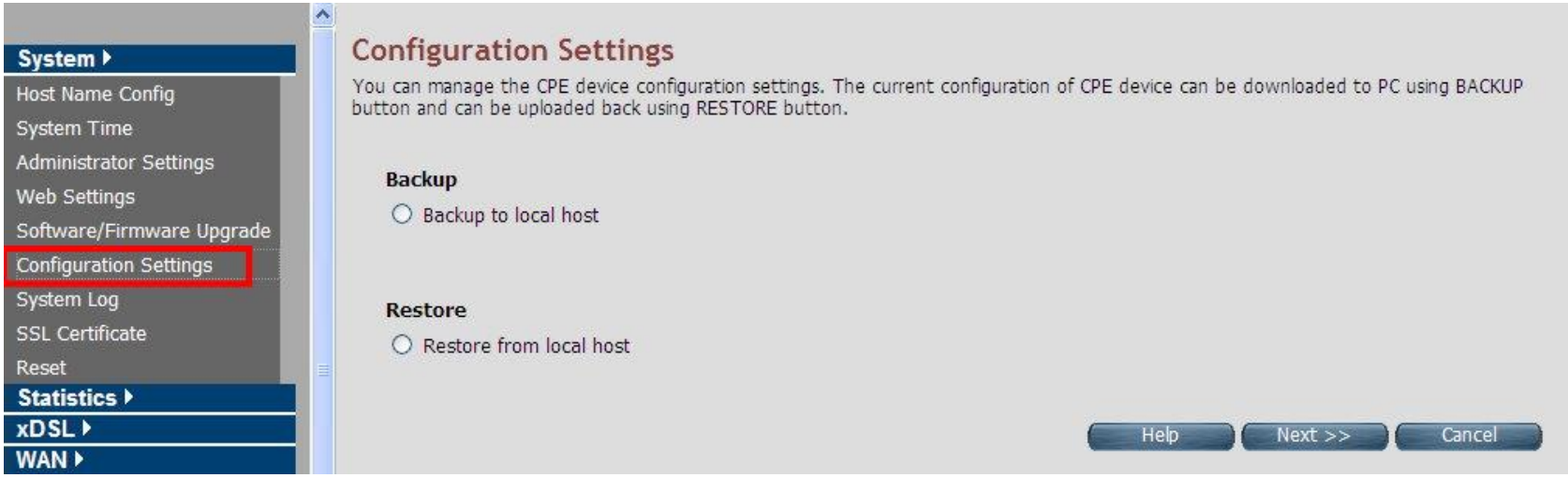


Figure 4.3.6 Configuration Settings

Fields in Configuration Settings

Field	Description
Backup to local host	This will 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 user to backup the current active configuration running in router system. This is very helpful, when a user wants to backup the current working configuration of router for rollbacks, if 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 are shown in Figure 4.3.6.1

Figure 4.3.6.1 Configuration Backup

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

■ Restore Previous Backed-up Configuration

As mentioned before this option allows 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 are shown in Figure 4.3.6.2. The system will go for reboot after configuration is restored. When CPE boots up it will be running with newly applied configuration.

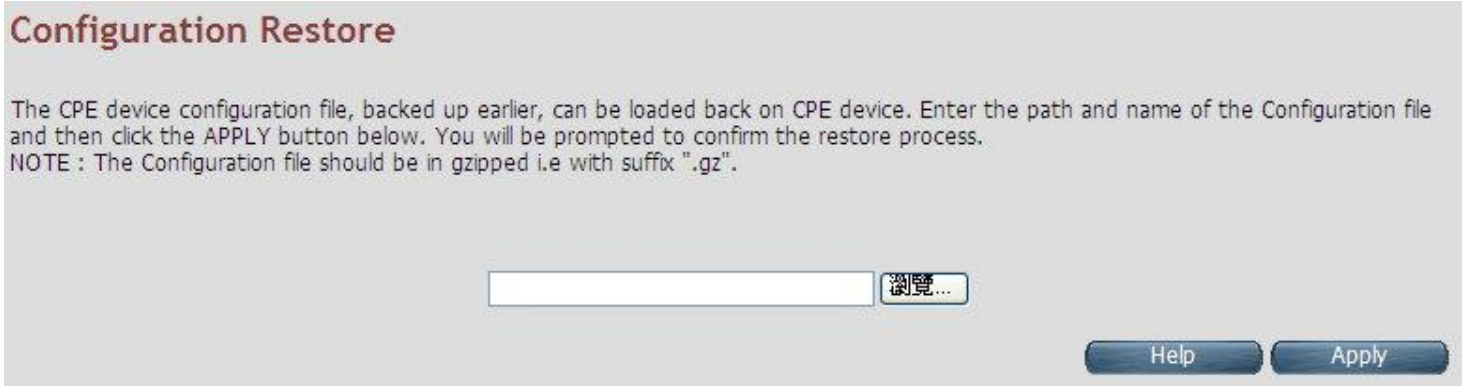


Figure 4.3.6.2 Configuration Restore

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

4.3.7 System Log

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

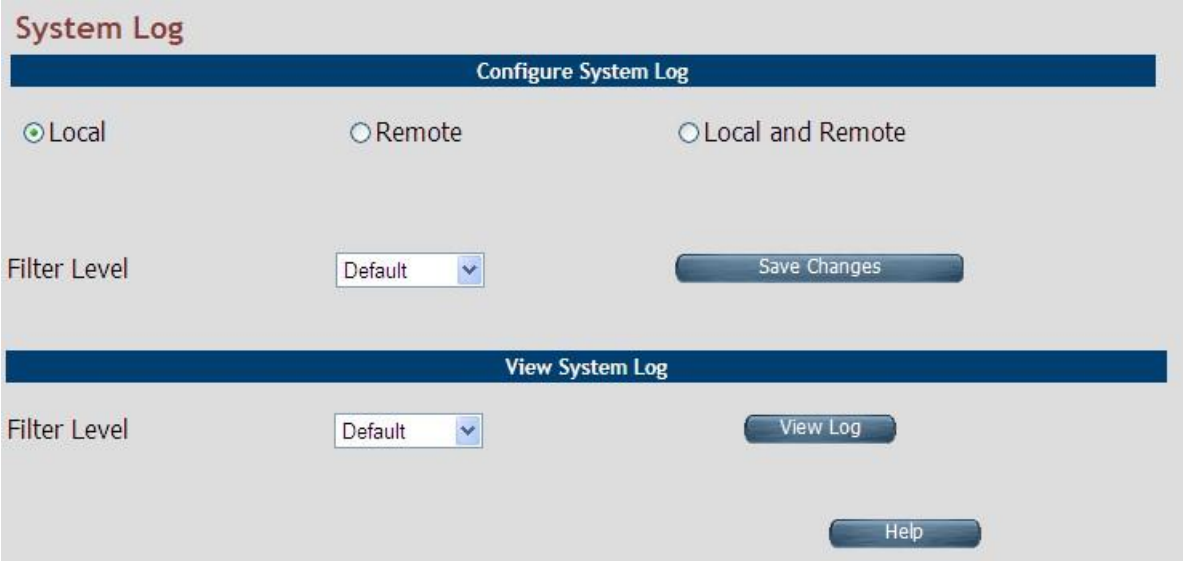


Figure 4.3.7 System Log

This page allows to manage logging options in CPE device.

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

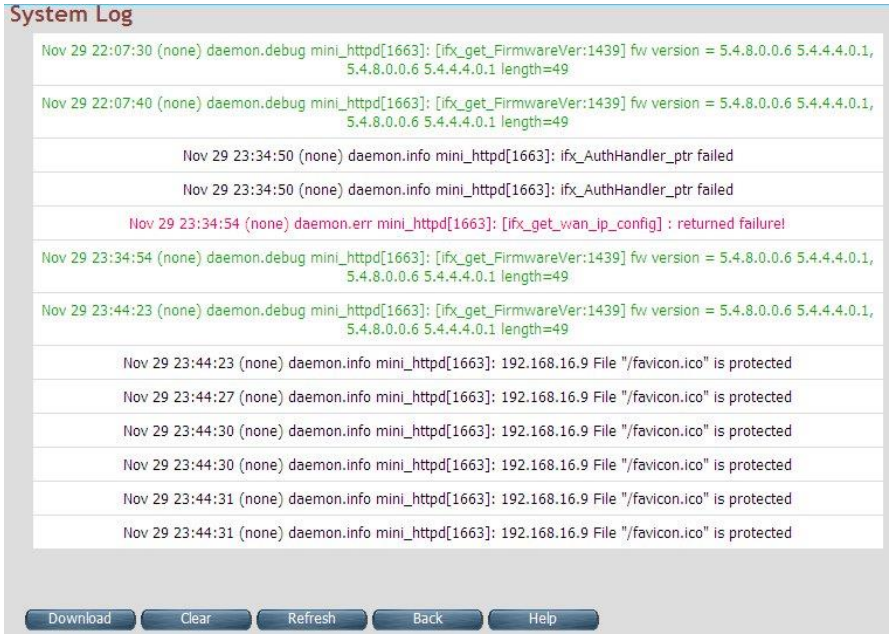


Figure 4.3.7.1 View System Log

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

To install 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

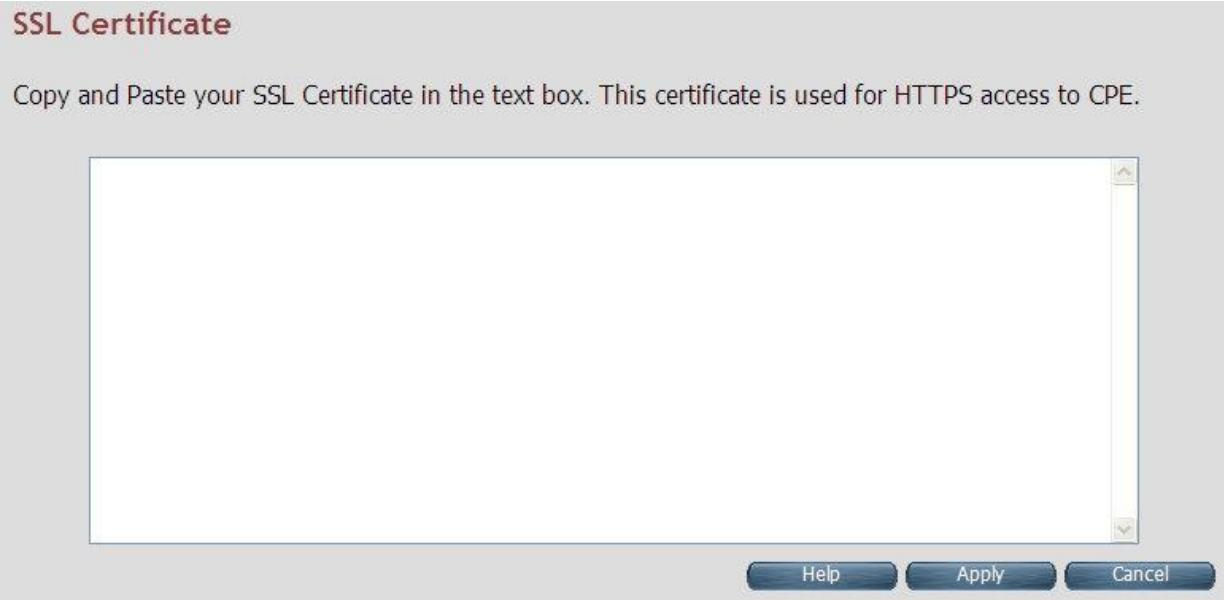


Figure 4.3.8 SSL Certificate

- Click **Apply** to install the entered certificate.
- Click **Cancel** for 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

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

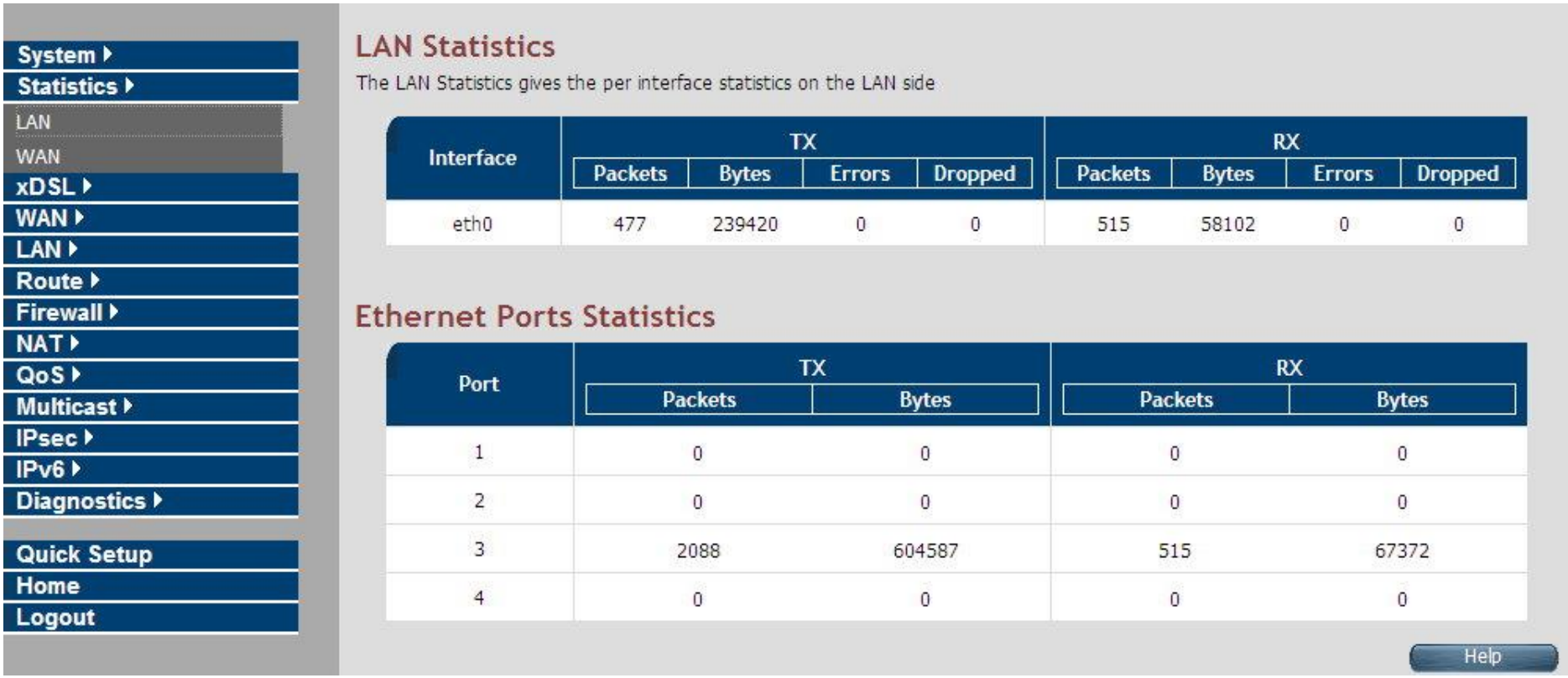


Figure 4.4.1 LAN Statistics

The screen contains the following details:

Fields in LAN Statistics:

Field	Description
Interface	Name of LAN Interface (e.g. eth0, usb0 etc.)
TX	Transmit Counters: ◆ 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 Errorneous packets on this interface. ◆ Total Dropped packets on this interface.

4.4.2 WAN

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

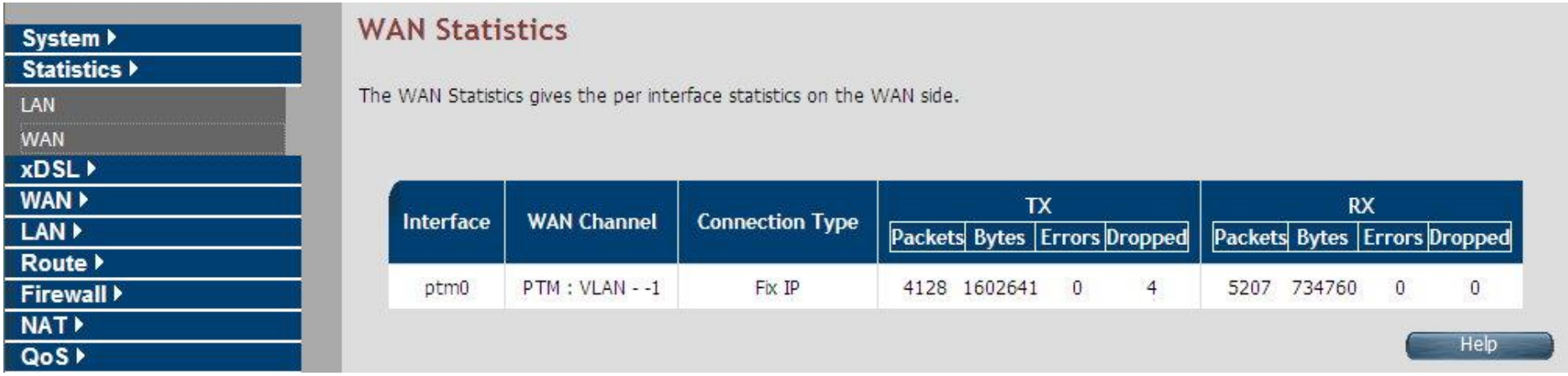


Figure 4.4.2 WAN Statistics

The screen contains the following details:

Fields in WAN Statistics:

Field	Description
Interface	Name of WAN Interface.

WAN Channel	Information about WAN Channel such as VCC or WAN-ethernet channel.
Connection Type	Type of WAN Connection.

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

Field	Description
TX	Transmit Counters for WAN interface: ◆ Total packets transmitted from this interface. ◆ Total bytes transmitted form this interface. ◆ Total Errorneous 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 Errorneous 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

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

xDSL Line Status

Provides detailed information about xDSL line's current attributes

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

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

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

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

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

Help

Figure 4.5.1 xDSL Status

The screen contains the following details:

Fields in xDSL Status:

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

4.5.2 Vectoring Mode selection

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

Fields in Vectoring Mode Selection

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

Notes:

1. ALL126AS3 vdsl2 vectoring technology default setting is enabled.
2. Vectoring technology is mainly used in intensive line equipment, such as 24-Port VDSL2 IP DSLAM.
3. If user would like to use ALL126AS3 vectoring technology, ALL126AS3 and IP DSLAM both need support vectoring technology features and need both enabled. The ALL126AS3 will auto follow the IP DSLAM vectoring technology configuration.
4. Vectoring technology does not support point to point applications.

About vectoring function(Reference only):

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

4.6 Select "WAN"

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

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

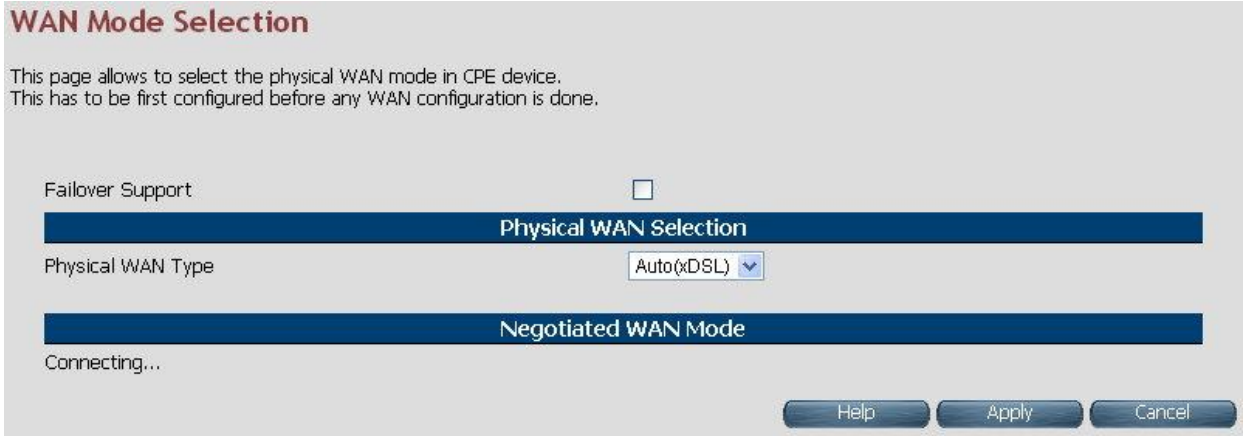


Figure 4.6.1 WAN Mode Setting(Seleted Auto)

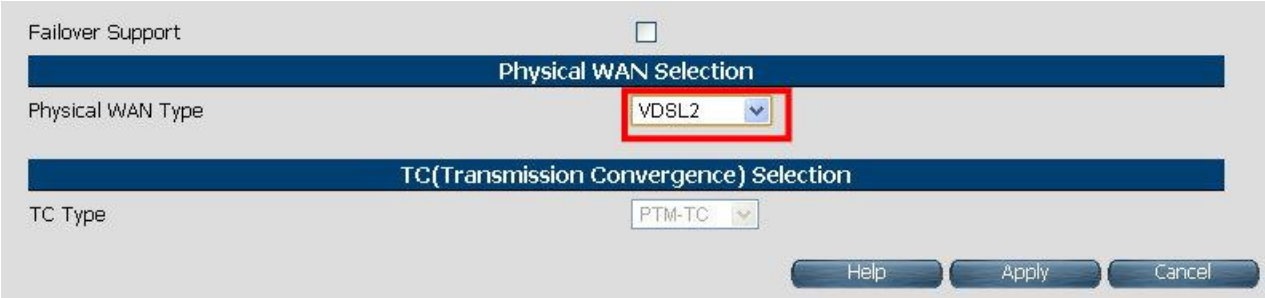


Figure 4.6.1.1 WAN Mode Setting(Seleted ADSL2+ / VDSL2)

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.

- 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:

If user would like to use ADSL to connect ALL126AS3, please select ADSL item of Physical WAN Type, and confirm the TC type itme is ATM-TC.

4.6.2 Auto Detect Setting

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

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

Figure 4.6.2 Port Mapping Configuration

The screen contains the following details:

Fields in Auto detect Config:

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

Fields in Auto detect Config(cont'd):

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

4.6.3 WAN Channel Config

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

Figure 4.6.3

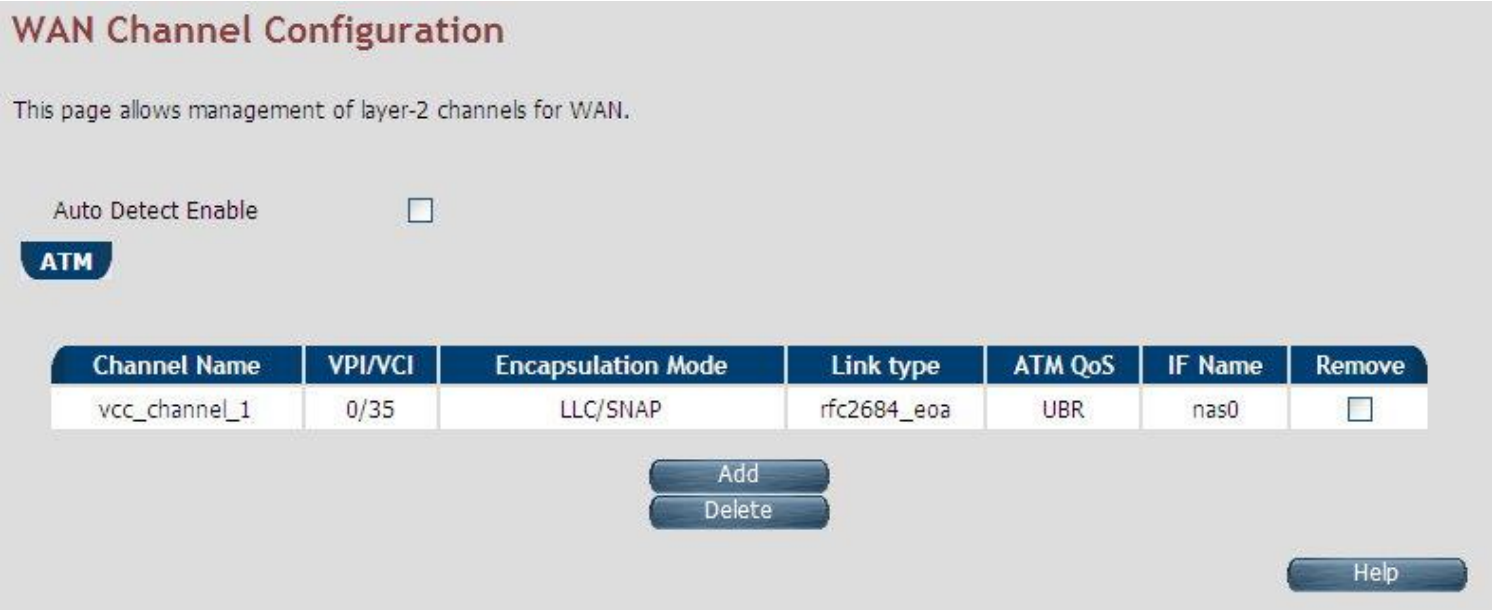


Figure 4.6.3.1 WAN Channel Config (Auto Detecting does not check the checkbox)

The screen contains the following details:

Fields in WAN Channel Config:

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

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

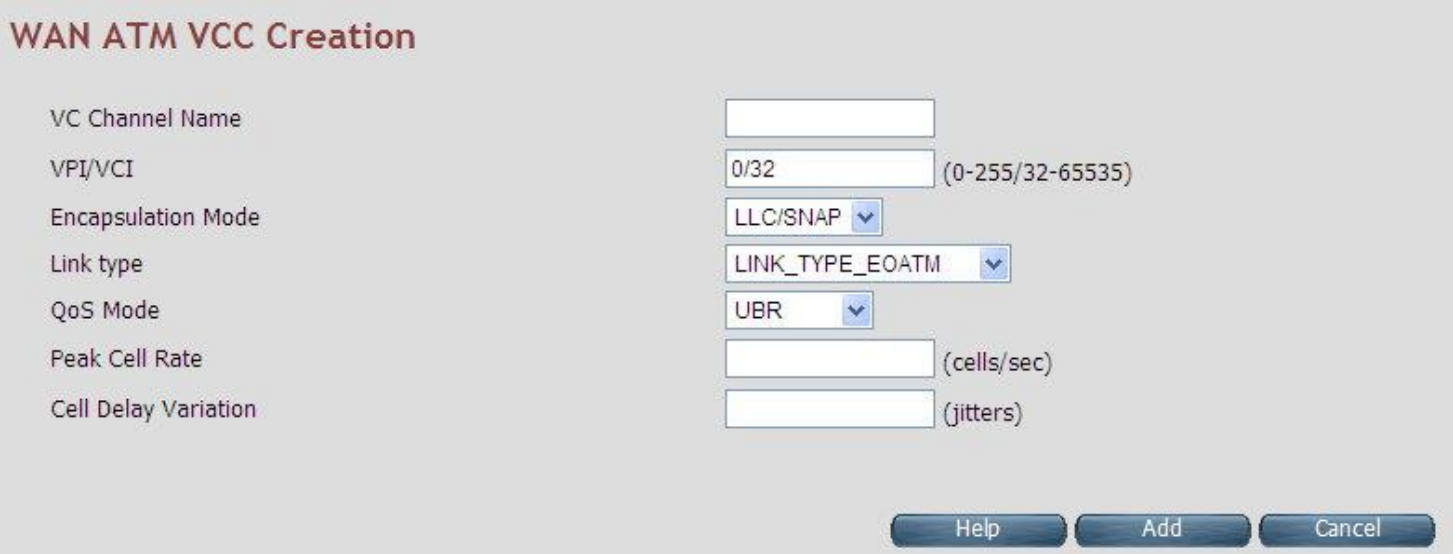


Figure 4.6.3.2 WAN Channel Config - ATM VCC Creation

The screen contains the following details:

Fields in WAN Channel Config:

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

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

Figure 4.6.4

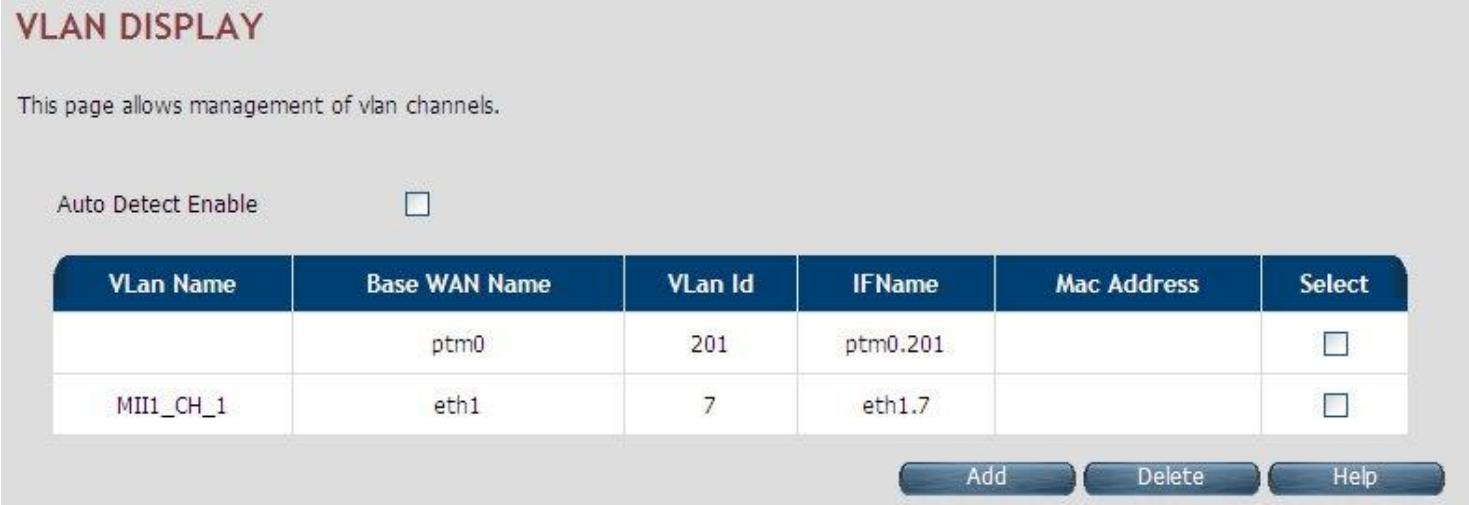


Figure 4.6.4.1 VLAN Channel Config Display(Auto Detecting does not check the checkbox)

The screen contains the following details:

Fields in VLAN Display:

Field	Description
Auto Detect Enable	To enable Auto Detect.
VLAN Name	User specified VLAN Channel name.
Base WAN Name	Displays the L2 interface names over which VLAN Channel has been configured.
VLAN id	VLAN identifier in range of 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 Config page, a screen is displayed as shown in Figure 4.6.4.2

Figure 4.6.4.2 VLAN Channel Config - Add

The screen contains the following details:

Fields in VLAN Creation:

Field	Description
VLAN Channel Name	User specified VLAN Channel name.
Mode Name	List of L2 interfaces over which VLAN Channels can be configured.
VLAN Id	VLAN identifier in range of (7 - 4095). VLAN Identifiers(1 - 6) are internally used in 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

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

Figure 4.6.5 WAN Setting - Auto Detect Enable

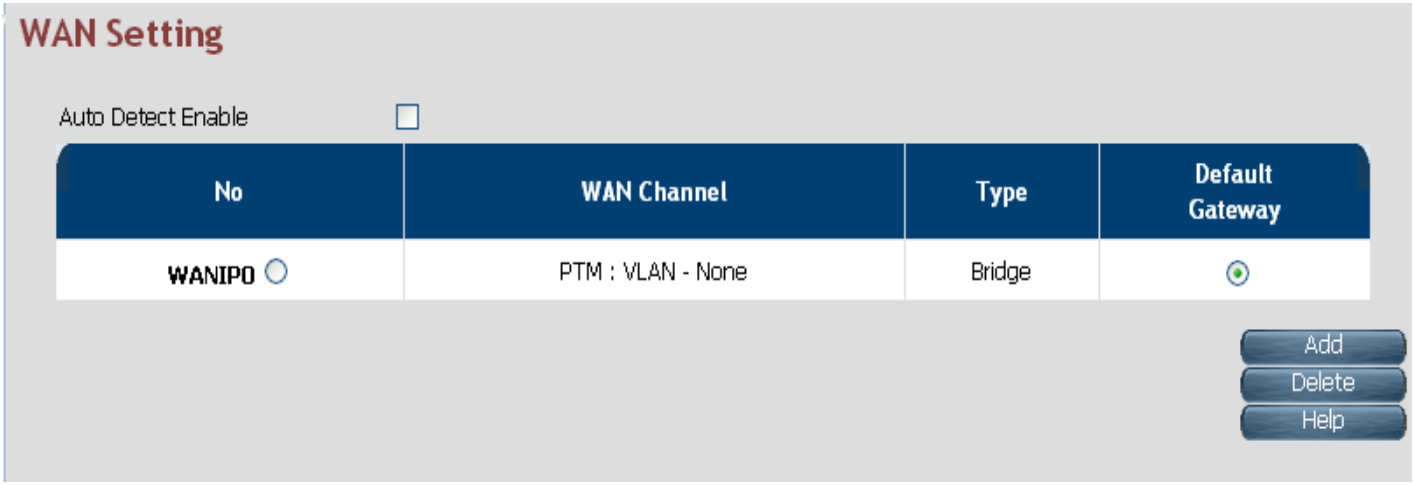


Figure 4.6.5.1 WAN Setting

The ALL126AS3 can support up to maximum 16 WAN connections in system. When a hardware based QoS is enabled in system, it limits the number of VCCs to 8 only for ATM based WAN. For creating a new WAN connection, click **Add** in the WAN setting page. Please follow the rest of the steps for creating the WAN connection.

The last column named DEFAULT GATEWAY allows to select the WAN for relevant WAN mode setting in WAN setting web page. When the user clicks any of the radio button, 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 in only IAD models, where VoIP is supported. this is default interface for VoIP packets.
Default Gateway	This option allows to configure 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 ALL126AS3 is DHCP client on WAN) click **Apply**.
Static IP Address	To enter the WAN interface IP Address of ALL126AS3 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

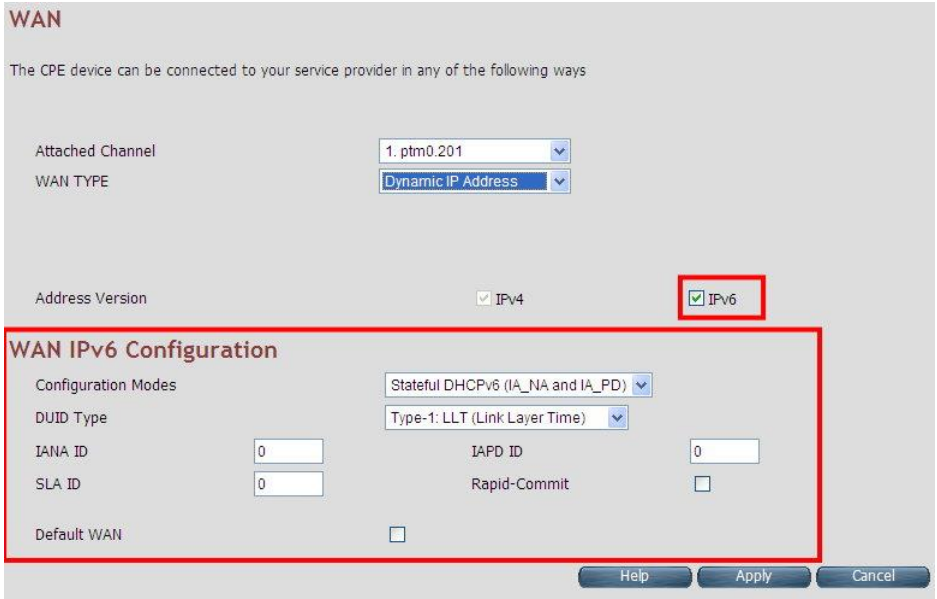


Figure 4.6.5.3 Dynamic IP Address

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

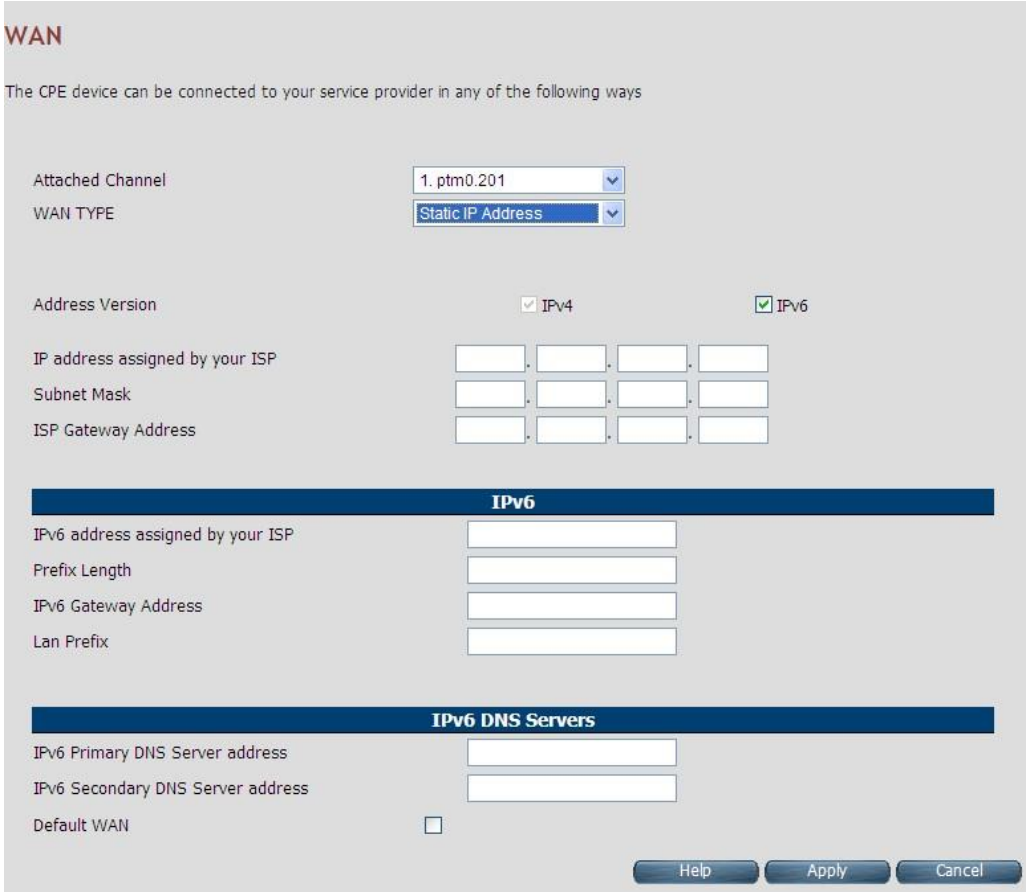


Figure 4.6.5.4 WAN Static IP

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 ALL126AS3 CPE's WAN link.
Subnet Mask	To specify the Subnet Mask of ALL126AS3 CPE's WAN link.
ISP Gateway Address	To specify the Gateway address of the ALL126AS3 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 to configure 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

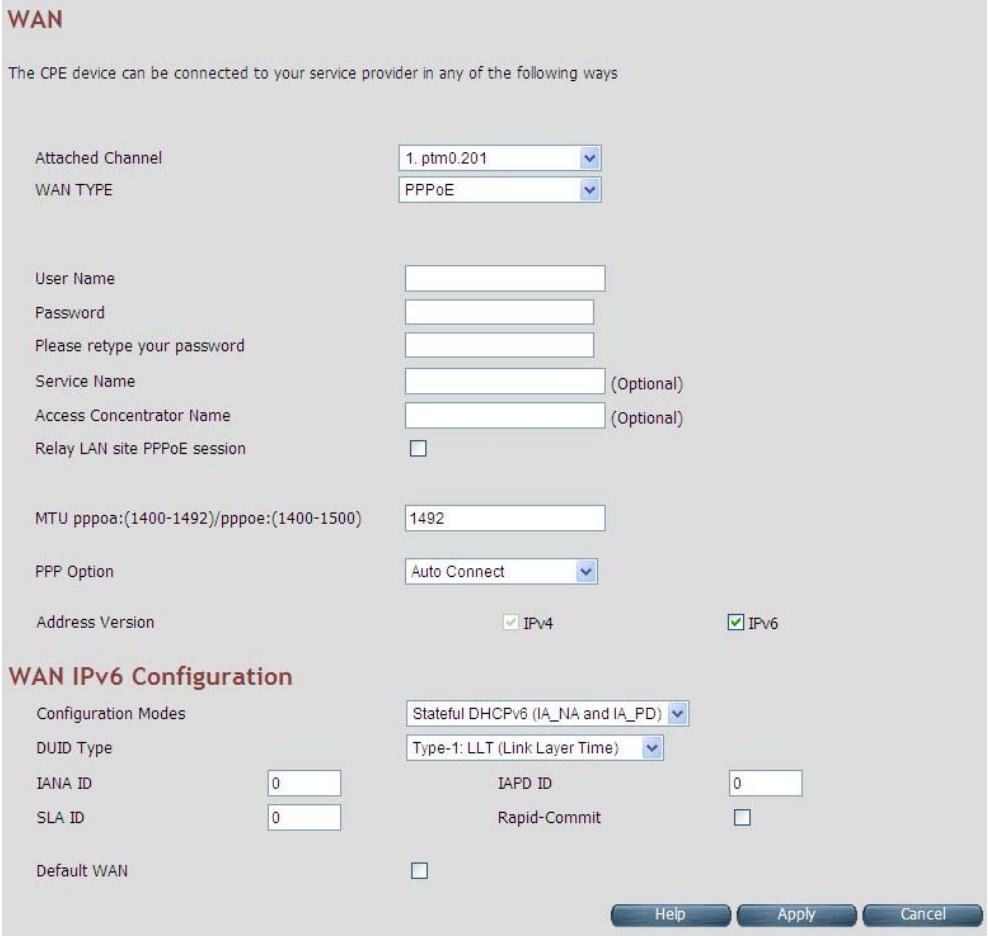


Figure 4.6.5.5 WAN PPPoE creation

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 to 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 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 to configure 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 to automatically re-connect to the service provider once the connection was 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 ALL126AS3.

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 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 to configure 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 Next. A screen is displayed as shown in Figure 4.6.5.7

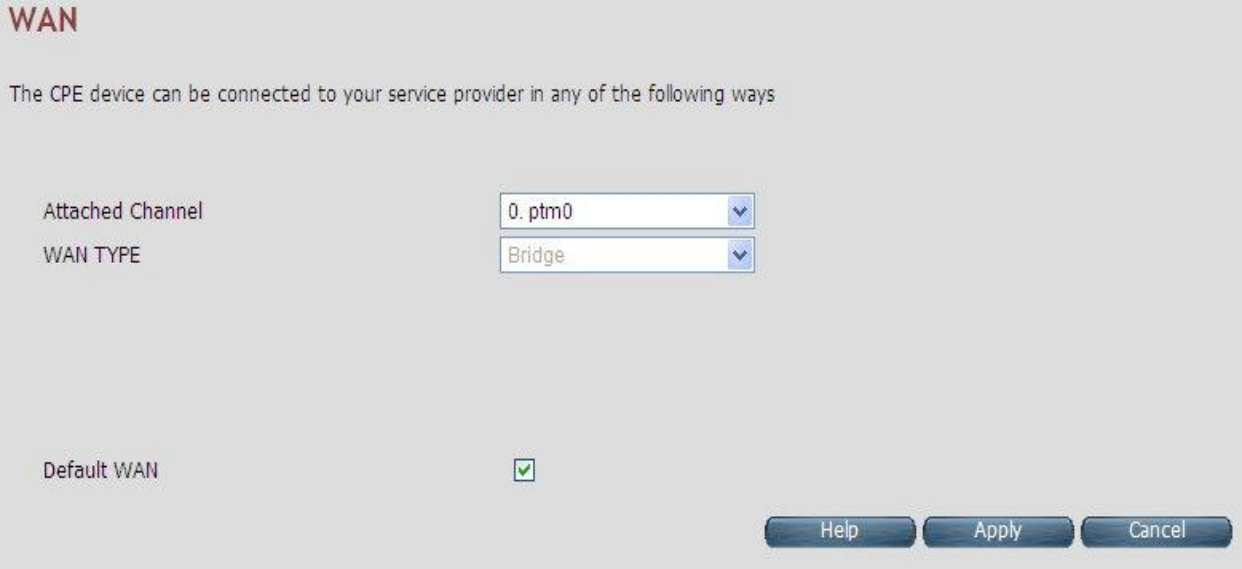


Figure 4.6.5.7 Bridge WAN Setting

The screen contains the following details:

Fields in Bridge Configuration:

Field	Description
Default WAN	This option allows to configure 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 to delete the selected configured WAN connection. This makes WAN connections free to re-choose the type of protocol and other parameters configuration.

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

4.6.6 WAN Status

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

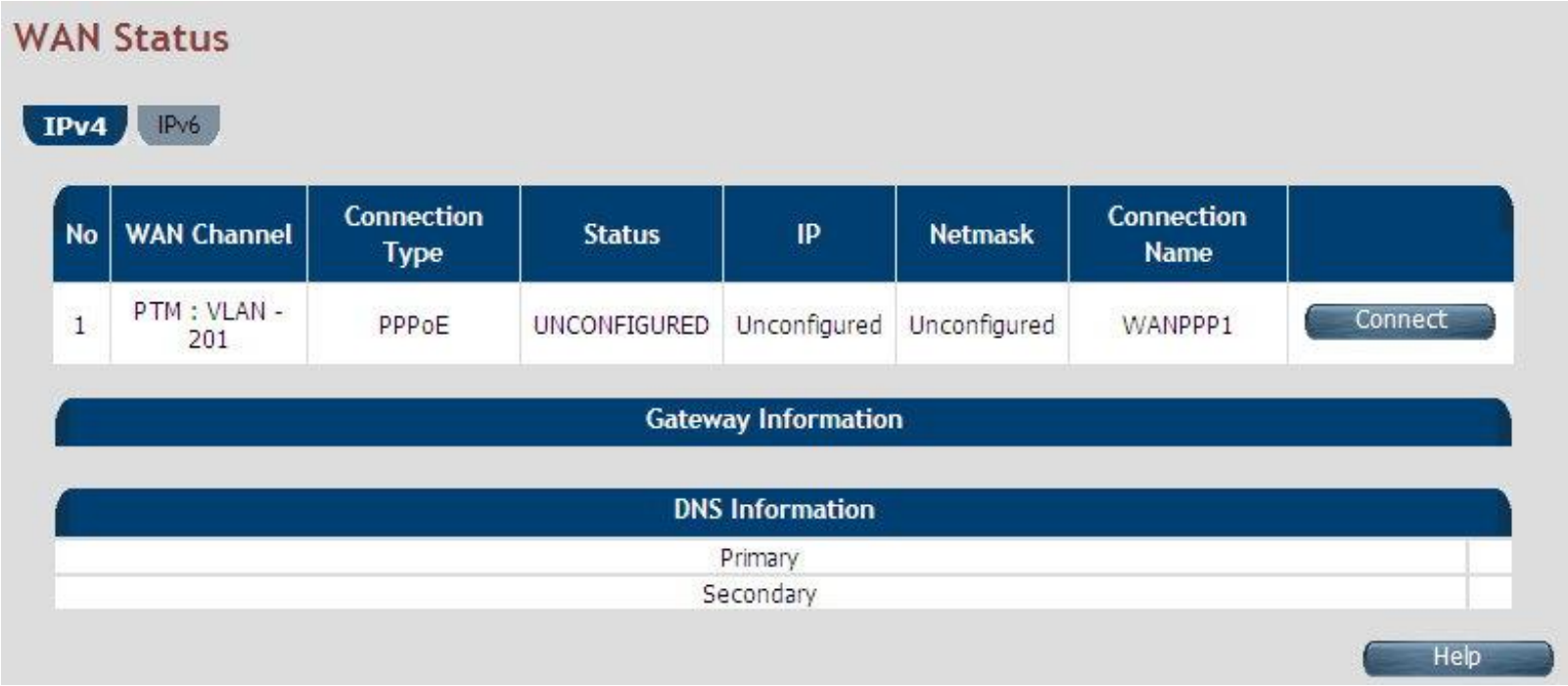


Figure 4.6.6 WAN Status

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 ALL126AS3 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 too appears only for PPPoA and PPPoE type of WAN links. On clicking this button, it brings down the PPP link.
Renew	This button appears only for DHCP type of WAN links. On clicking this button, it tries to establish 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

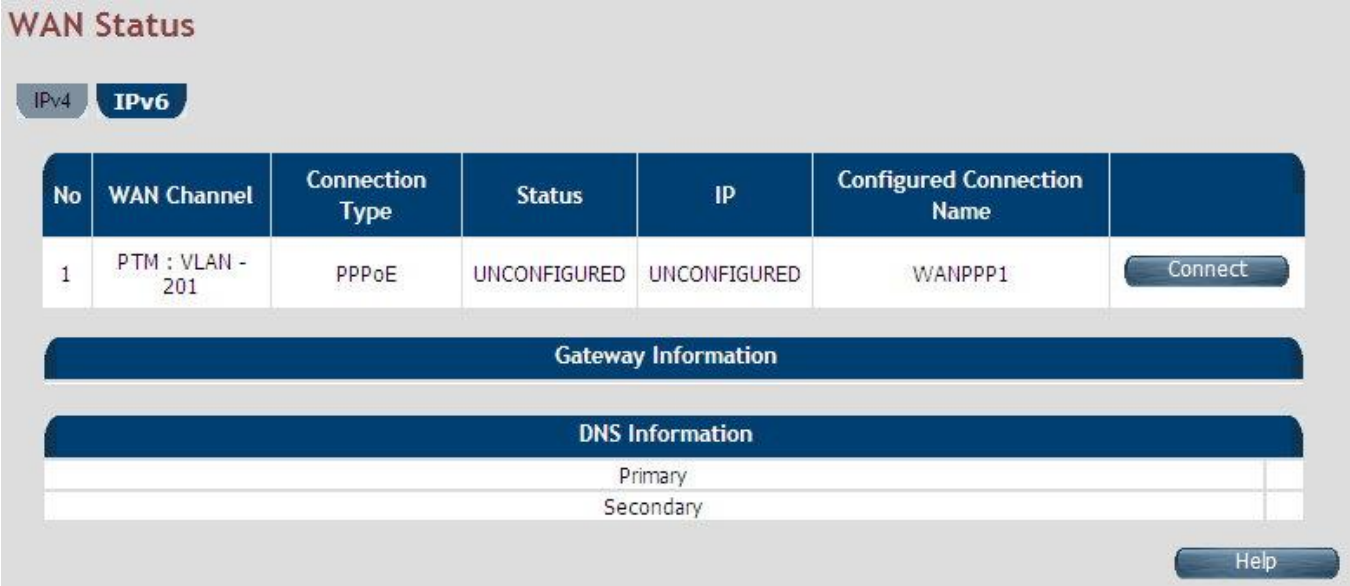


Figure 4.6.6.1 WAN Status IPv6 Tab

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

4.6.7 DNS

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

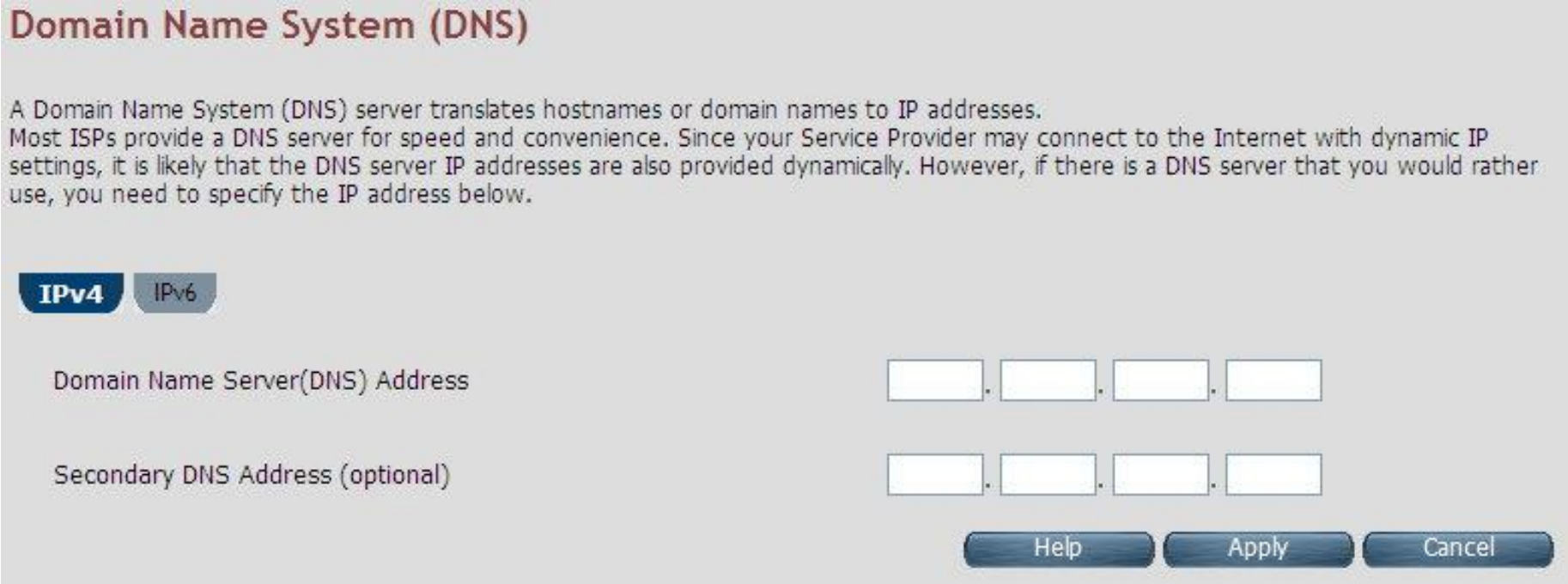


Figure 4.6.7 DNS Configuration

The screen contains the following details:

Fields in DNS:

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

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

4.6.8 DDNS

The Dynamic DNS is useful for getting a FQDN URL registered for a dynamic IP address to a DNS service provider. The ALL126AS3 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

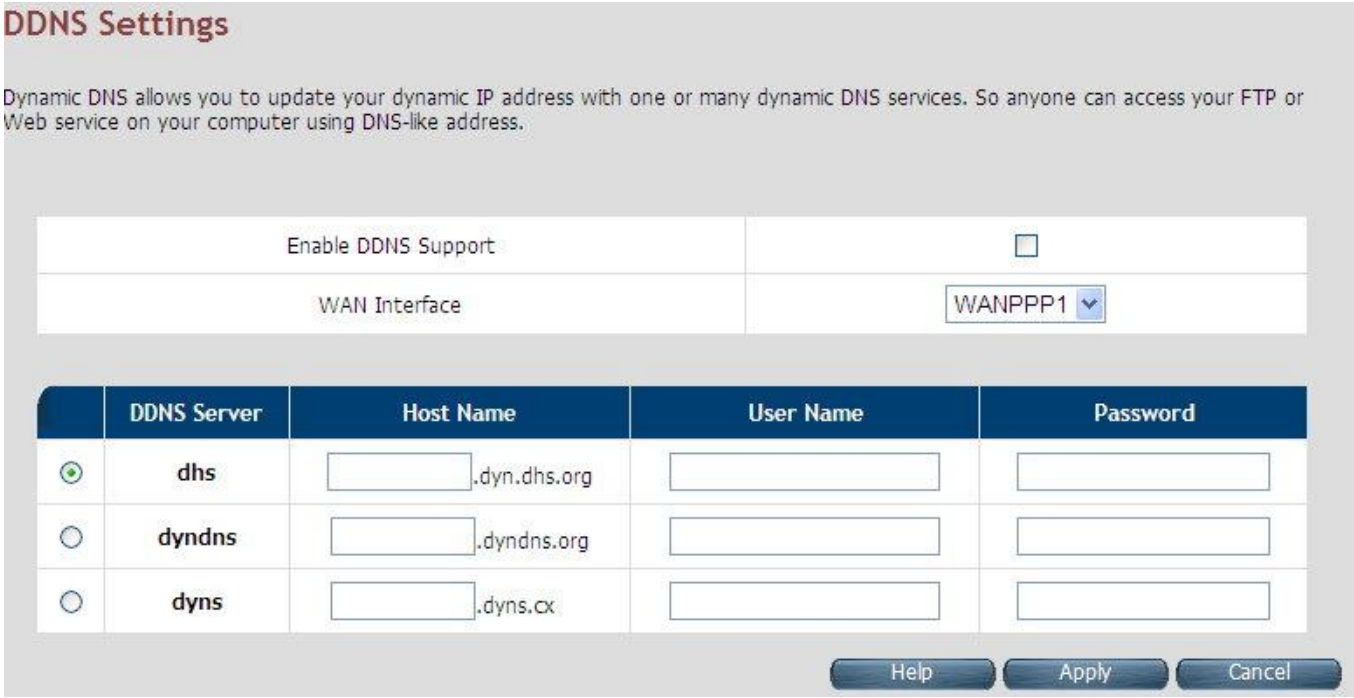


Figure 4.6.8 DDNS Settings

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. To configure the ADSL OAM settings, click the **OAM Configuration** link (**WAN > OAM Configuration**) on the left navigation bar. This release supports only F5 type of OAM tests as shown in Figure 4.6.9

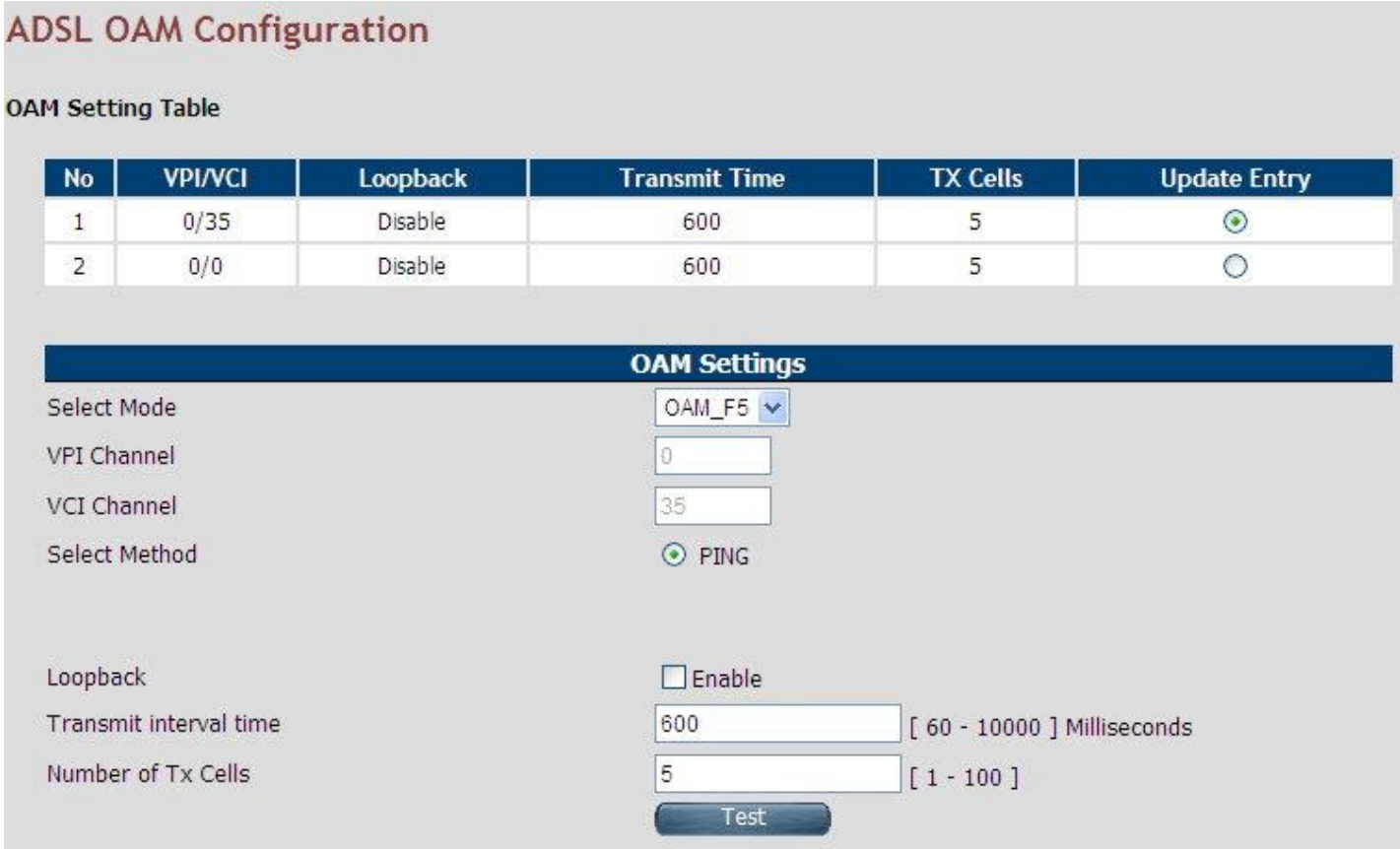


Figure 4.6.9 ADSL OAM F5 Test

The screen contains the following details:

Fields in ADSL OAM F5 Test page:

Field	Description
OAM F5 Setting Table	This table displays all active connections with 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.

OAM F5 Ping Successful!

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

Figure 4.6.9.1 Tset Successful

OAM F5 Ping Failed!

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

Figure 4.6.9.2 Test Failed

The screen contains the following details:

Fields in ADSL OAM F5 Test Page:

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

4.7 Select "LAN"

When connecting the ALL126AS3 to a new control PC, one may want to go through the following steps in order to make the IP address previously set by ifconfig in the console or on some later occasion, one may want to change it again without using the console, then the menu below will be helpful. In order to set the IP address, click on "LAN Settings". 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**, **LAN Port Status**, **VLAN Settings**. A screen is displayed as shown in Figure 4.7.

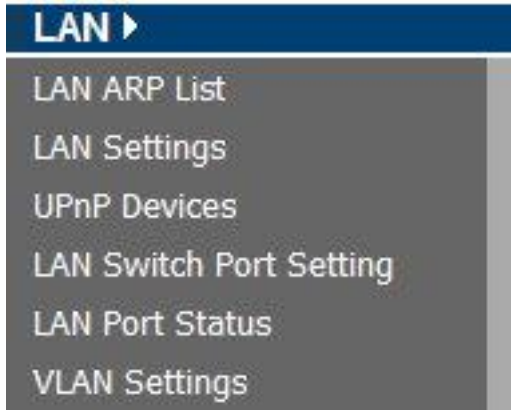


Figure 4.7 LAN options

4.7.1 LAN ARP List

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

Figure 4.7.1 ARP List

The screen contains the following details:

Fields in LAN ARP List:

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

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

4.7.2 LAN Settings

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

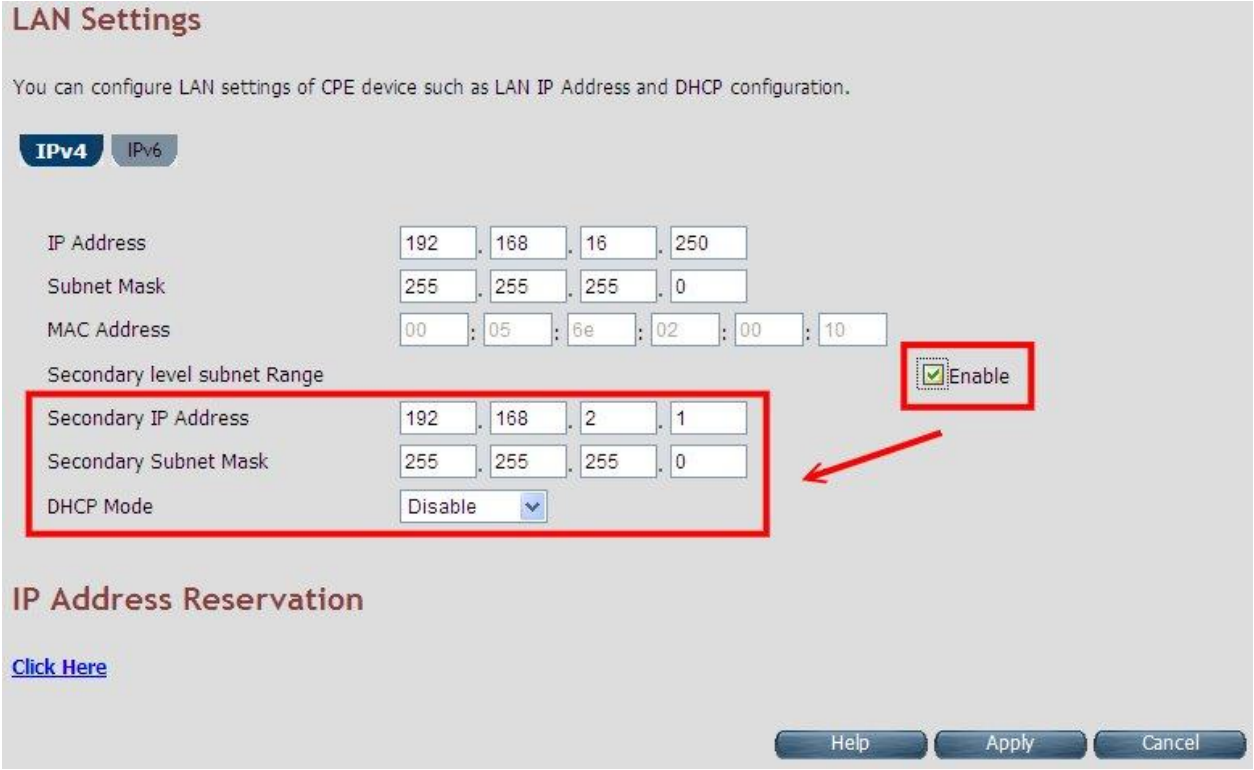


Figure 4.7.2 LAN Settings – DHCP Server

The screen contains the following details:

Fields in LAN Settings:

Field	Description
IP Address	Used to enter the LAN interface IP Address of CPE device.
Subnet Mask	To enter the LAN Subnet Mask of CPE device.
MAC Address	MAC Address of LAN bridge device. It can be overridden by specifying the user supplied MAC address here.
Enable	To enable the secondary IP address on the LAN interface.
Secondary IP Address	This is to enter the secondary IP address.
Secondary Subnet Mask	This is to enter the secondary subnet mask.
DHCP Mode	To choose the mode of DHCP in ALL126AS3. The options available are: Disable, Server and Relay Agent. The default value is **Disable**. If DHCP Mode is set to **Server,** there are some additional options available, which are shown in **Figure 4.7.2**. IP Pool Starting Address - To enter the starting IP Address of the DHCP server pool. IP Pool Ending Address - To enter the ending IP Address of the DHCP server pool. Lease Time - To specify the lease period for DHCP allocation. Local Domain Name (optional) - To enter the Domain Name of the DHCP server. DHCP Server IP - IP address of the DHCP server on the interface shown, to which the DHCP requests are relayed.

Field	Description
DHCP Server	DHCP Mode: Server **DHCP Server** IP Pool Starting Address: 192 . 168 . 1 . 2 IP Pool Ending Address: 192 . 168 . 1 . 254 Lease Time: Half hour Local Domain Name: dslgw.lantiq.com (optional)
IP Pool Starting Address	DHCPv4 pool start 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.

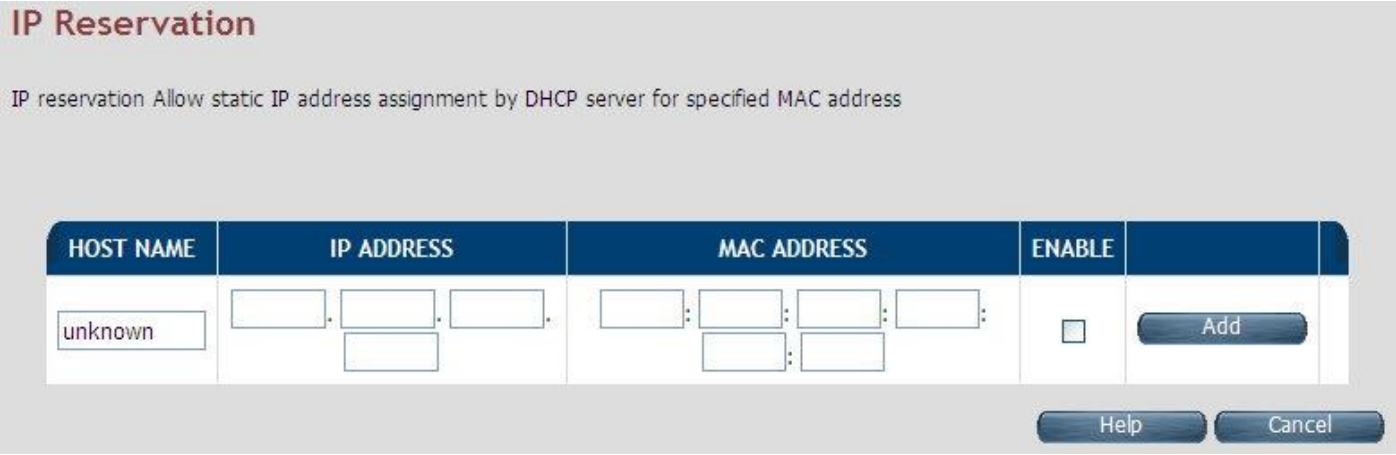


Figure 4.7.2.1 IP Reservation

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 is as shown in Figure 4.7.2.2, Figure 4.7.2.3 and Figure 4.7.2.4.

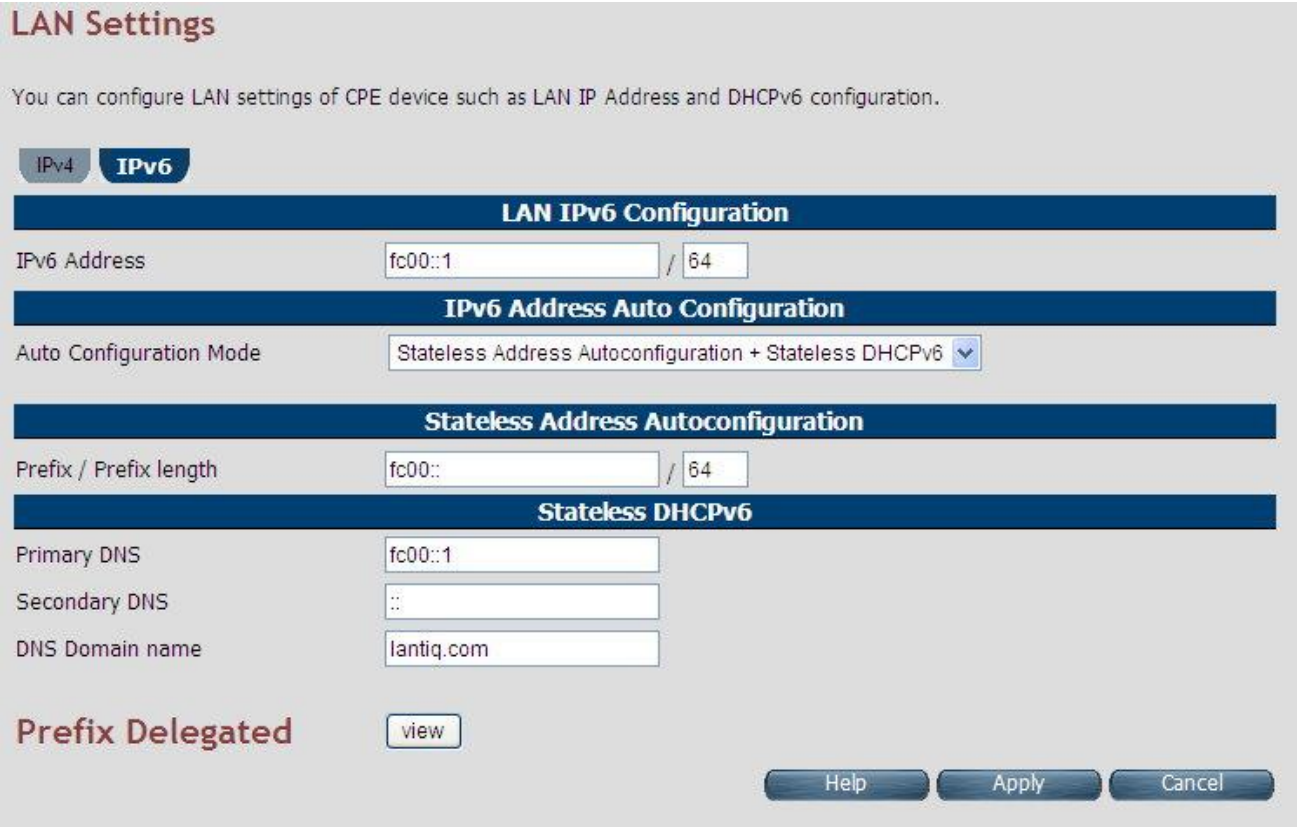


Figure 4.7.2.2 LAN Settings - IPv6 Tab (Option 1: SLAAC + Stateless DHCPv6)

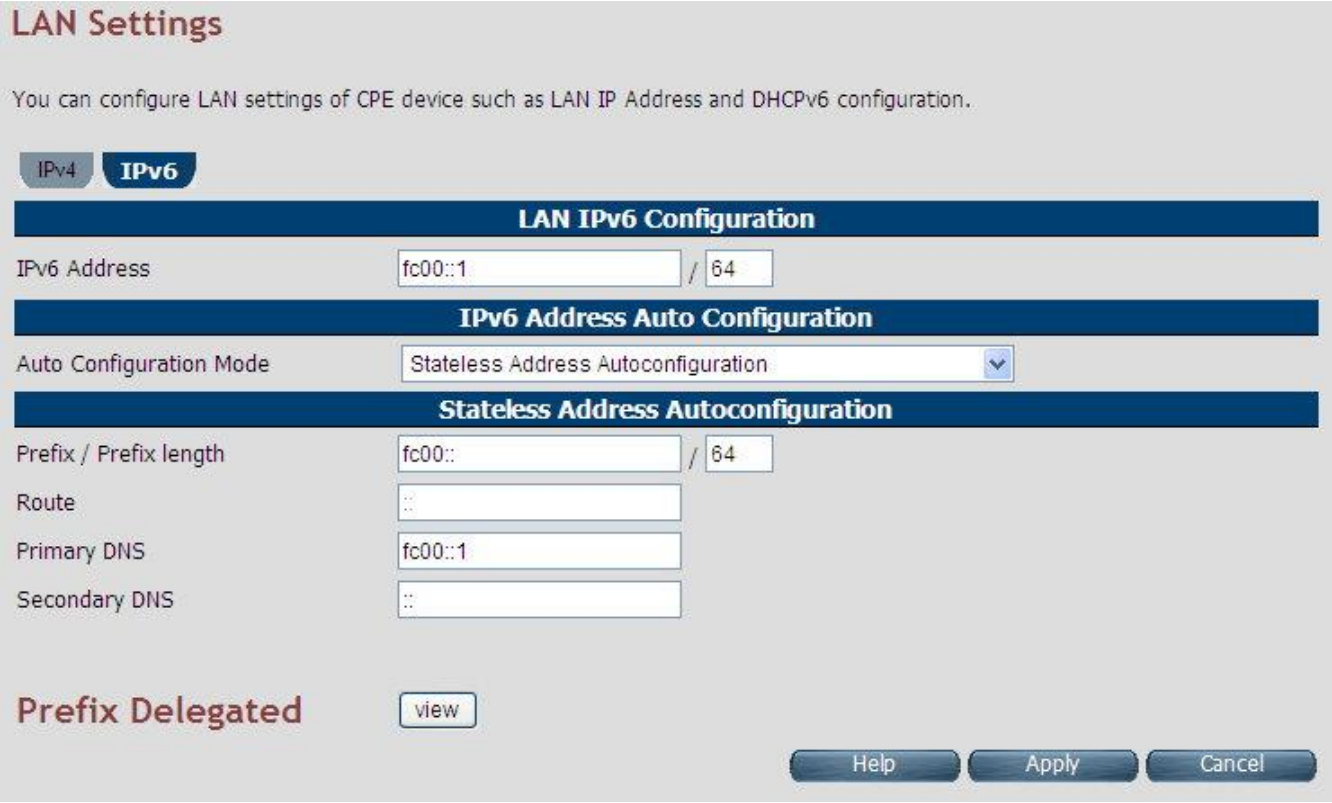


Figure 4.7.2.3 LAN Settings - IPv6 Tab (Option 2: SLAAC)

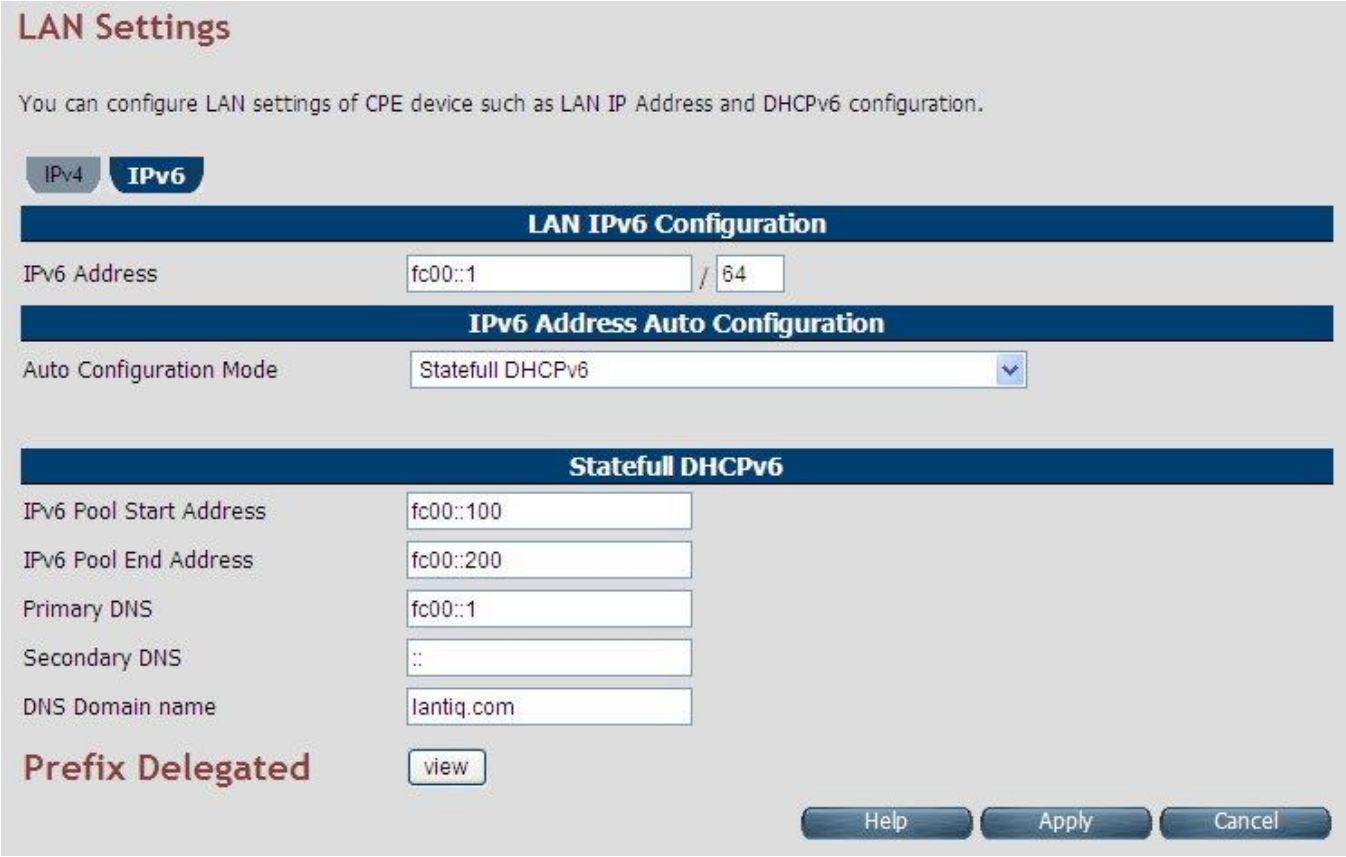


Figure 4.7.2.4 LAN Settings - IPv6 Tab (Option 3: Statefull DHCPv6 Server)

For LAN interface, the ALL126AS3 uses SLAAC based prefix assignment to LAN hosts. The IPv6 prefix obtained from DHCPv6 on WAN is automatically passed to LAN hosts for their IPv6 address configuration.

The screen contains the following details:

Fields in LAN Settings – IPv6:

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

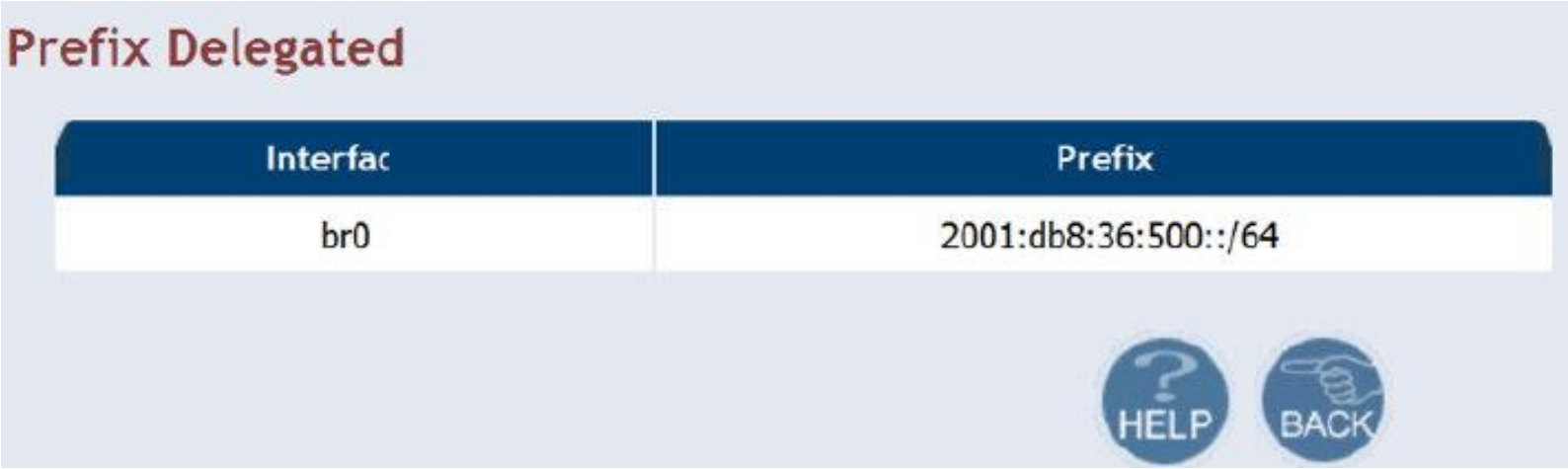


Figure 4.7.2.5 Prefix Delegated view

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

4.7.3 UPnP Devices List

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

Figure 4.7.3 UPnP device list

The screen contains the following details:

Fields in UPnP Device List:

Field	Description
UPnP Devices	IP address of the device connected discovered through UPnP protocol.
Friendly Name	Name of the device connected.

UUID	Universal Unique Identifier.

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

4.7.4 LAN Switch Port Setting

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

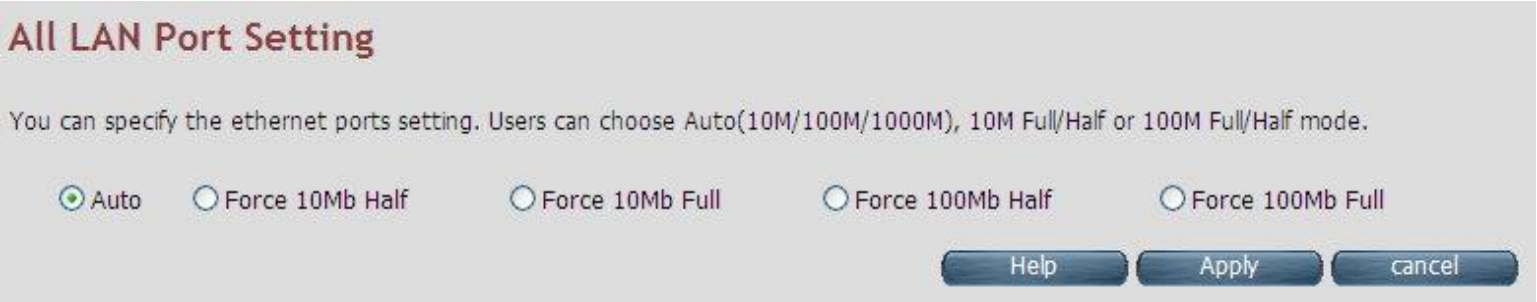


Figure 4.7.4 All LAN Port Setting

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

4.7.5 LAN Port Status

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

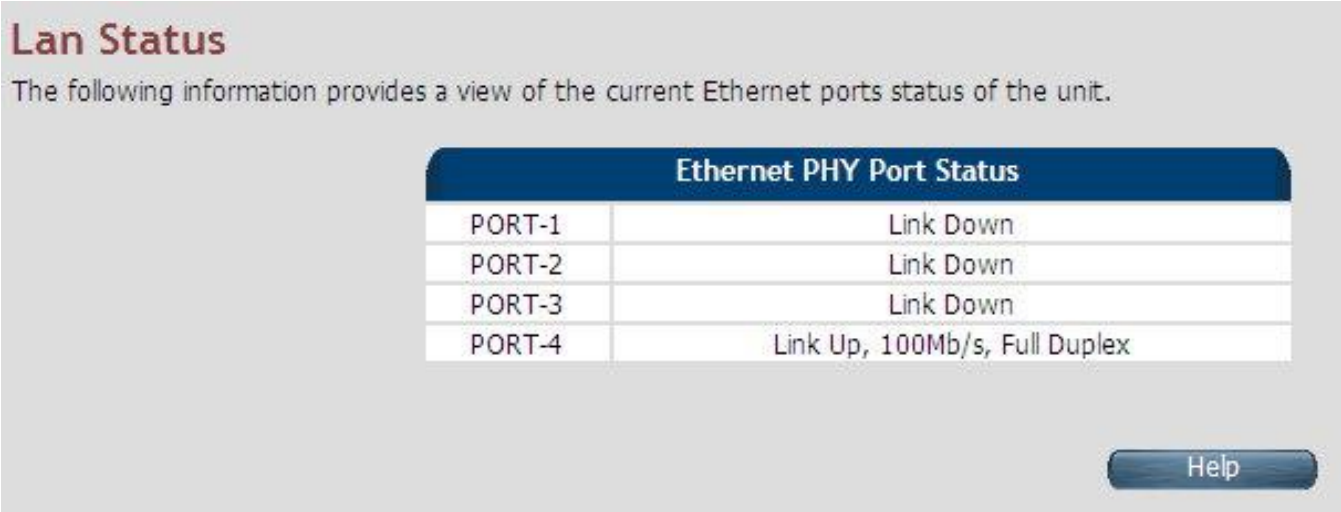


Figure 4.7.5 LAN Port Status

Example Table:

Input 1	Output 1	Input 2	Output 2	Input 3	Output 3	Input 4	Output 4

NWAY 10M Full	10M Full	Force 10M Full	10M Half	None	Link Down	NWAY 10M Half	10M Half
Input 5	Output 5	Input 6	Output 6	Input 7	Output 7	Input 8	Output 8
NWAY 100M Half	100M Half	Force 100M Full	100M Half	Auto 100M Full	100M full	Auto	100M FULL

4.7.6 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

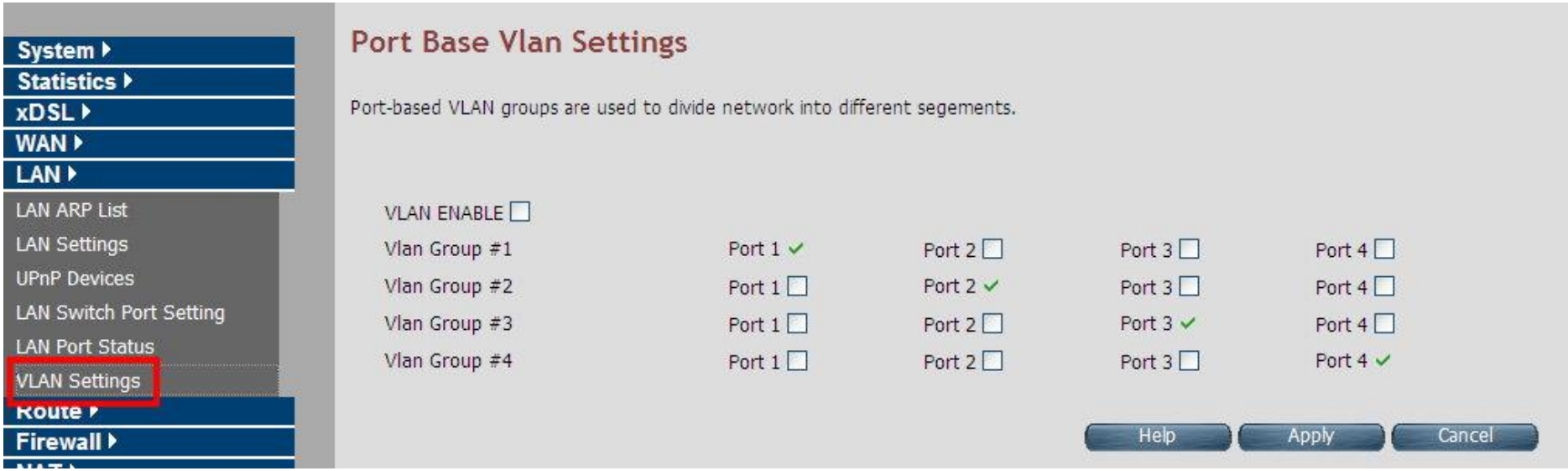


Figure 4.7.6 LAN Port Status

◆ 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.

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

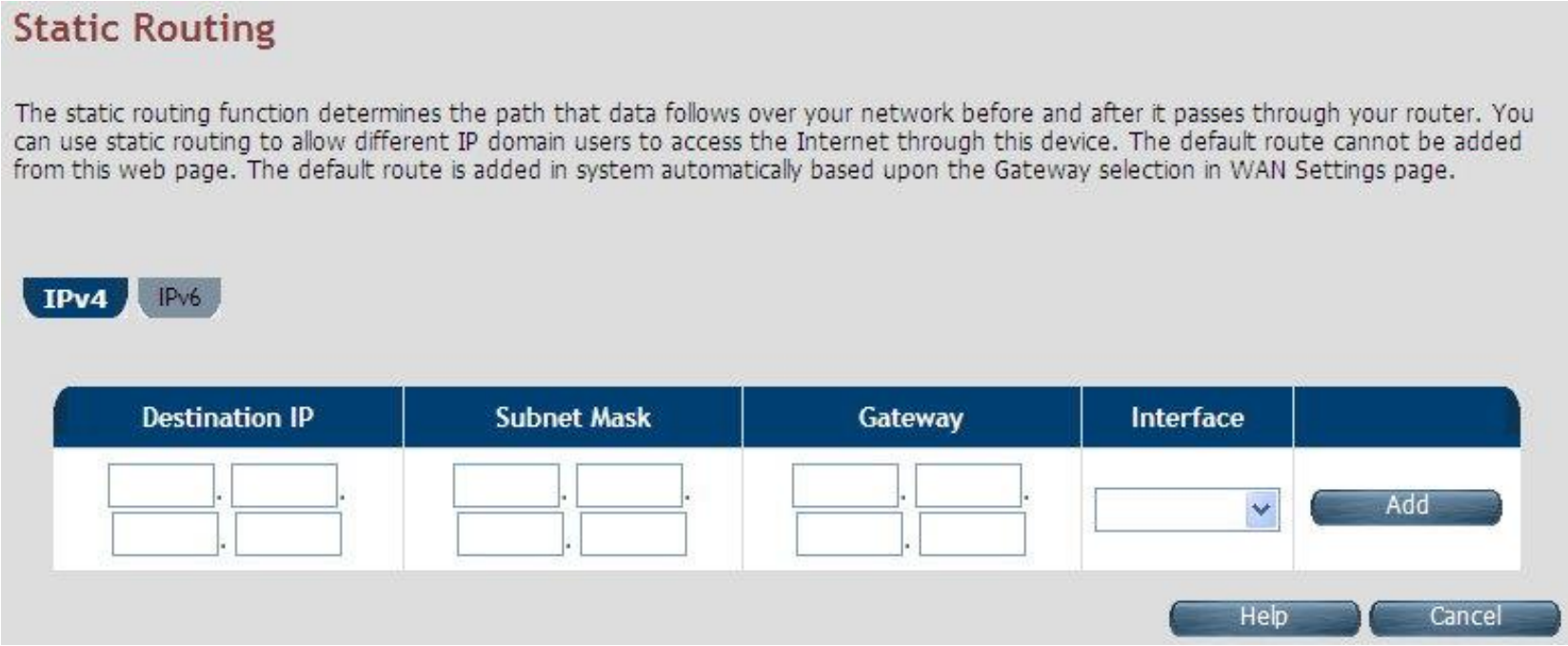


Figure 4.8.1 Static Routing Configuration

The screen contains the following details:

Fields in Static Routing:

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

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

Notes:

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

2. The gateway of static routing 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 is not supported currently.

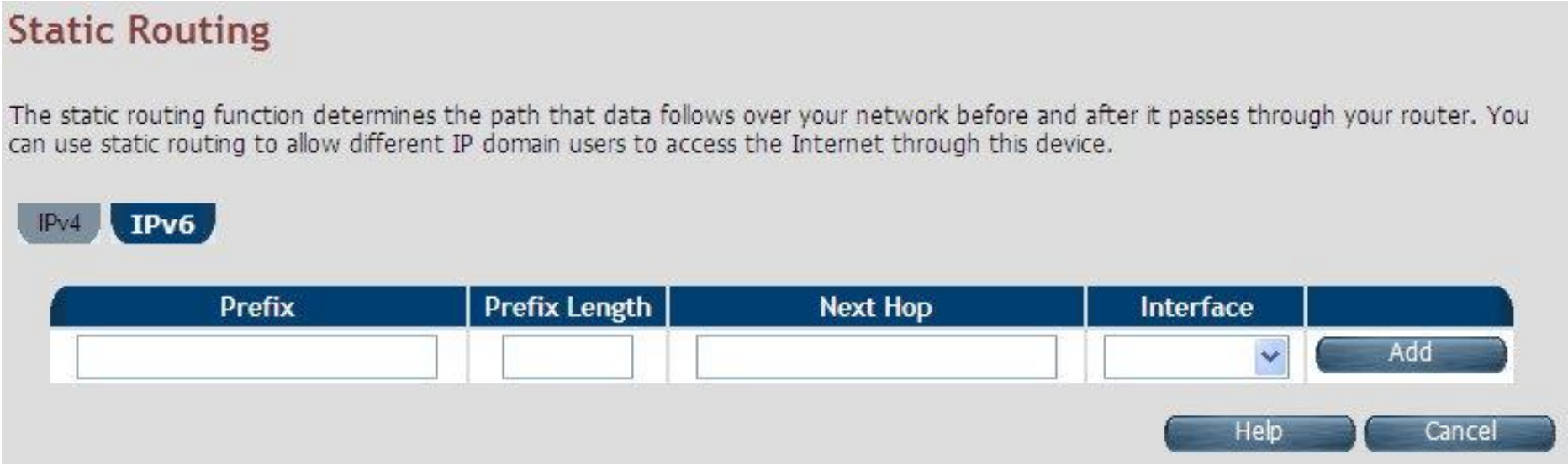


Figure 4.8.1.1 Static Routing IPv6

Tip:

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

4.8.2 RIP Support

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

Figure 4.8.2 Dynamic Routing

The screen contains the following details:

Fields in Dynamic Routing:

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

- 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.
To view the Routing entry table list of ALL126AS3, click on the "Routing Table List" link in the left navigation bar. A screen is displayed as shown in Figure 4.8.3.

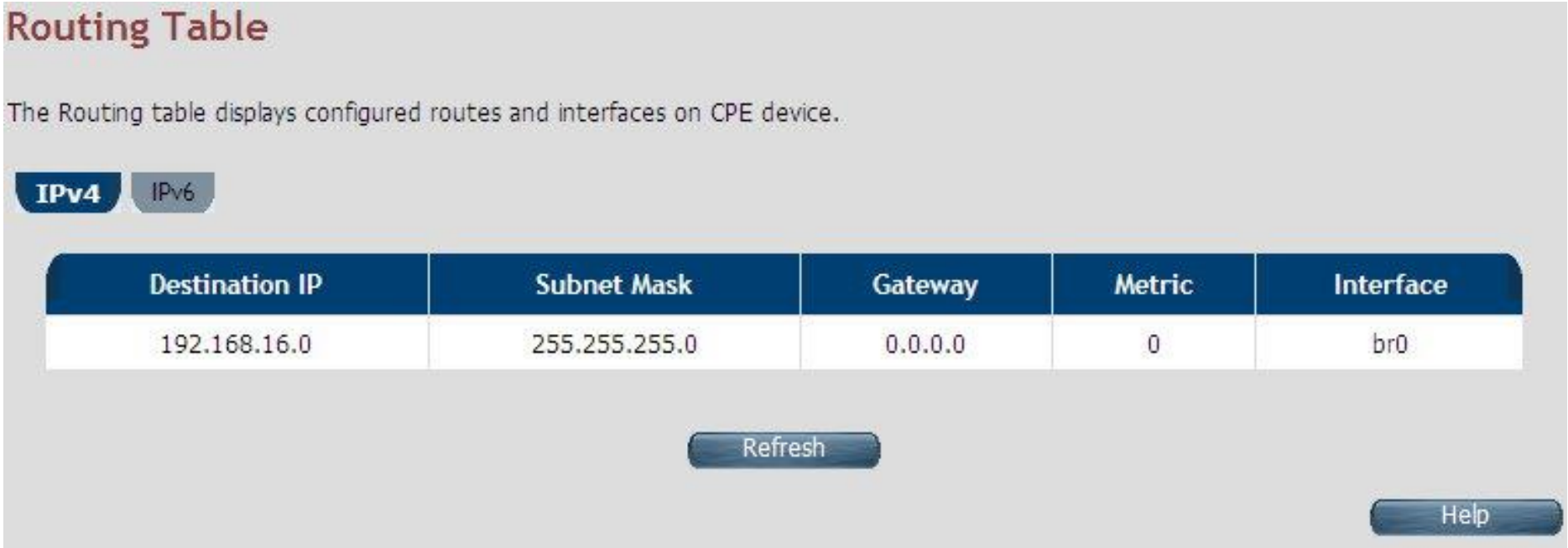


Figure 4.8.3 Routing Table List

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

Destination	Next Hop	Metric	Interface
fc00::/64	::	256	br0
fe80::/64	::	256	br0
fe80::/64	::	256	eth0
ff02::1/128	ff02::1	0	br0
ff00::/8	::	256	br0
ff00::/8	::	256	eth0
ff00::/8	::	256	ptm0
ff00::/8	::	256	ptm0.201

Figure 4.8.3.1 Routing List – IPv6 Tab

4.9 Select "Firewall"

You can view **Firewall** link on the left navigation bar of the ALL126AS3 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 4.9

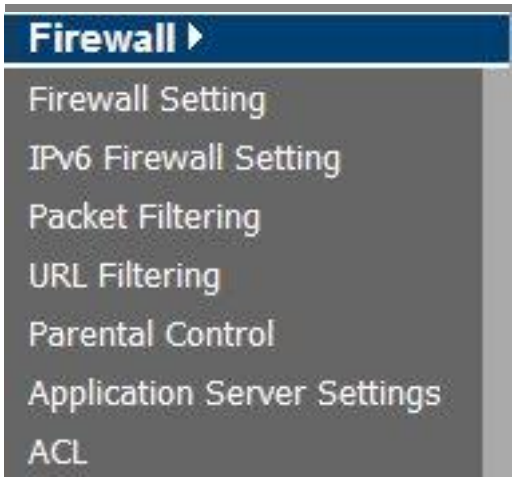


Figure 4.9 Firewall Options

4.9.1 Firewall Setting

To enable or disable the firewall, click the **Firewall Setting** link (**Firewall > Firewall Setting**) on the left navigation bar. A screen is displayed as shown in Figure 4.9.1

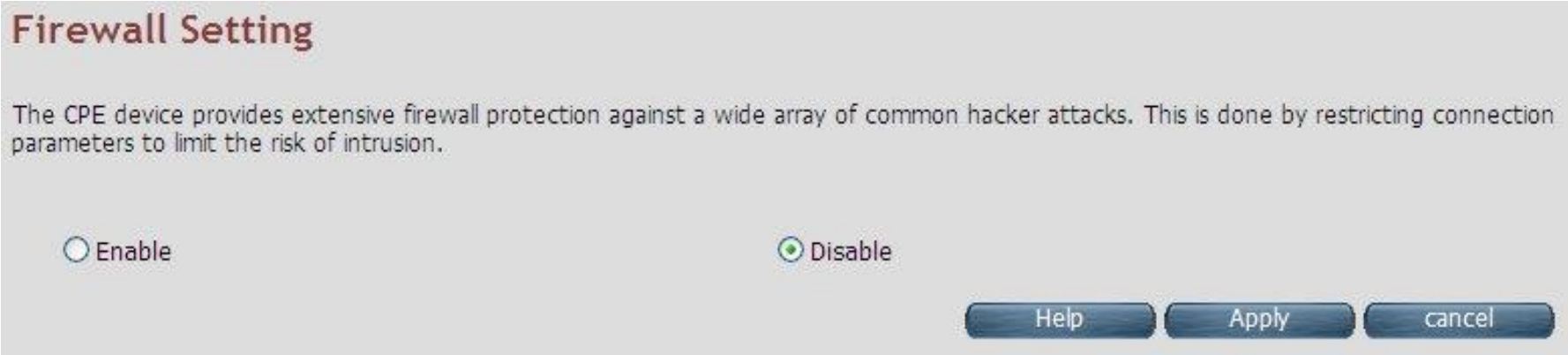


Figure 4.9.1 Firewall Setting

The screen contains the following details:

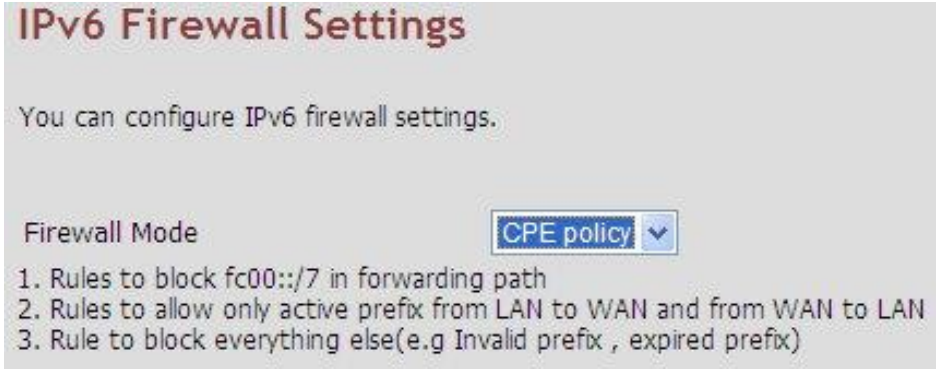
Fields in Firewall Setting:

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

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

4.9.2 IPv6 Firewall Setting

To enable or disable the firewall, click the **IPV6 Firewall Setting** link (**Firewall > IPv6 Firewall Setting**) on the left navigation bar. A screen is displayed as shown in Figure 4.9.2



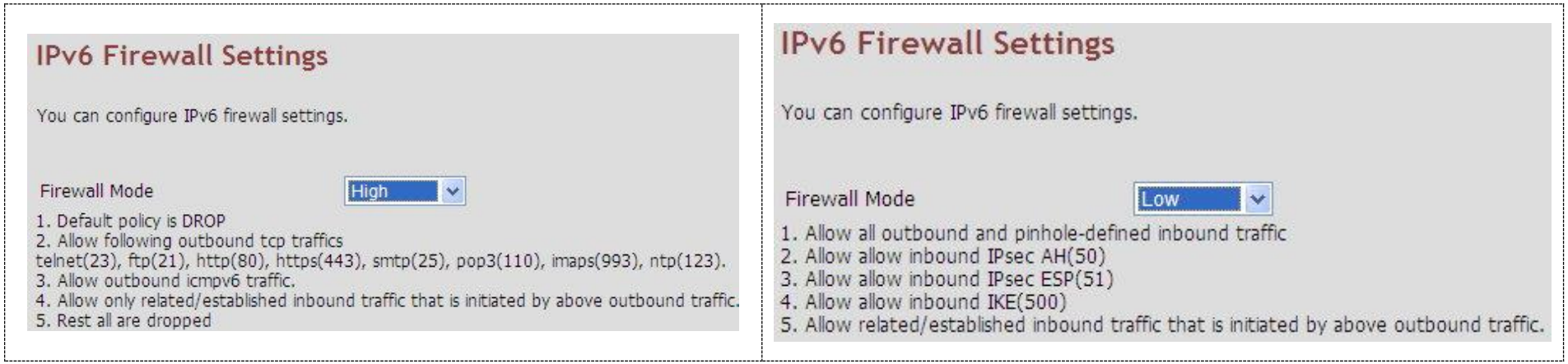


Figure 4.9.2 IPv6 Firewall Setting

The screen contains the following details:

Fields in UPnP Settings:

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

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

4.9.3 Packet Filtering

To enable Packet Filtering, click the **Packet Filtering** link (**Firewall > Packet Filtering**) on the left navigation bar. A screen is displayed as shown in Figure 4.9.3

Figure 4.9.3 Packet Filtering

The screen contains the following details:

Fields in Packet Filtering:

Field	Description
IPV4/IPv6	Choose the appropriate tab to configure.
Enable Packet Filter	To enable or disable the Packet Filter feature of ALL126AS3 CPE. To enable, select the check box.
Source IP	Filter IP Address range of the local machine under ALL126AS3 CPE.
Source Port	Filter Port number range of the local machine under ALL126AS3 CPE.
Destination IP	IP address of the destination.
Destination Port	Port address of the destination.
Protocol	Filter protocol. (TCP or UDP).
Ingress Interface	Input interface of the packet.
Egress Interface	Output interface of the packet.
Source MAC Address	Source MAC Address of packet originating host.
Enable	To provide more IP Addresses of the WAN interface.
Add	On pressing Add button, the screen shown in Figure 4.9.3.1 is displayed for adding a new packet filtering rule in system.
Delete All	To delete all the packet filtering rules configured in system.

- Click Apply at any time during configuration to save the information that 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 104. If. you choose IPv6 tab and click on Add button, a screen is displayed as shown in Figure 4.9.3.2.

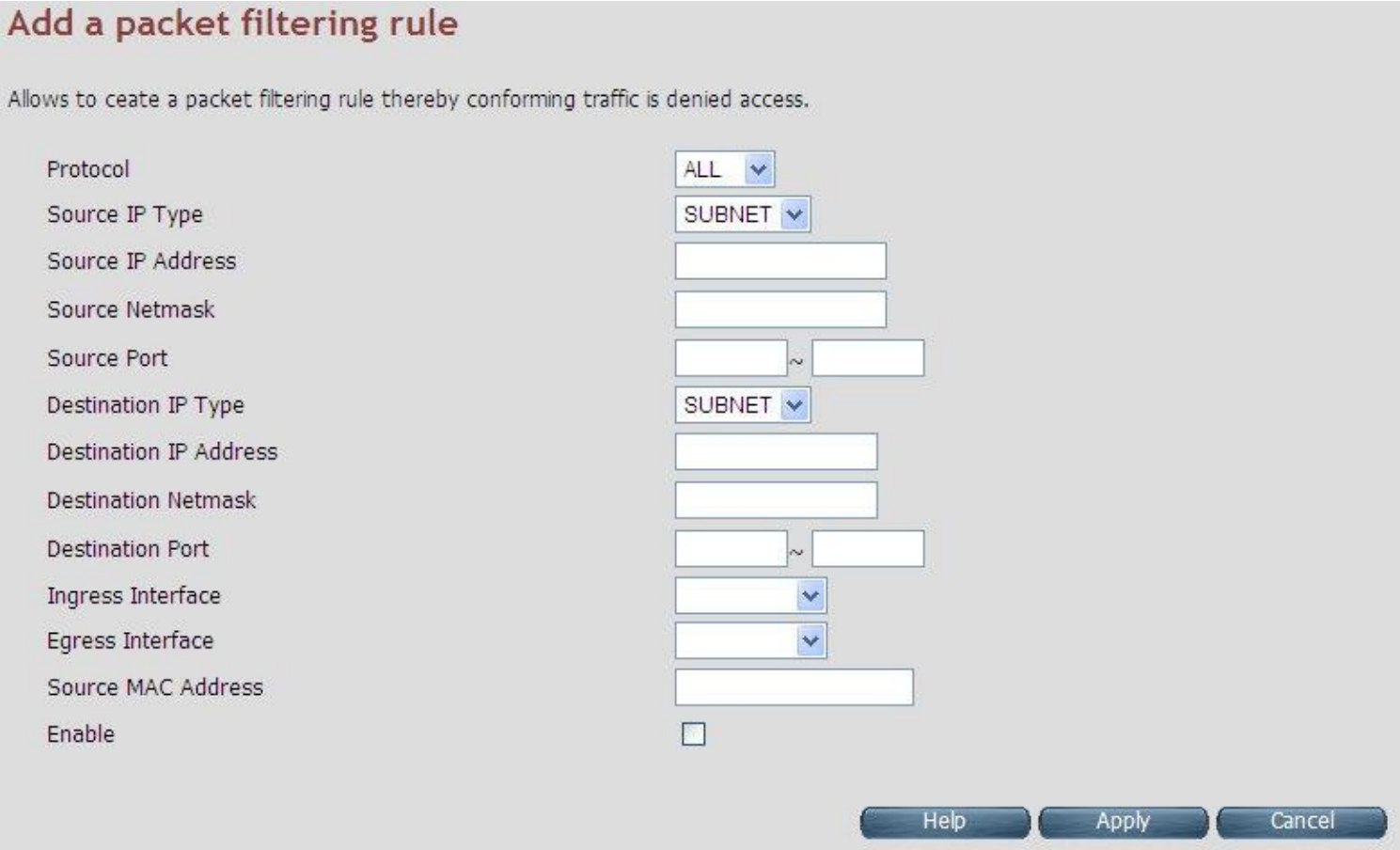


Figure 4.9.3.1 Add a Packet Filtering Rule for Firewall - IPv4

The screen contains the following details:

Fields in"Add a Packet Filtering Rule" page:

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

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

Figure 4.9.3.2 Add a Packet Filtering Rule for Firewall - IPv6

The screen contains the following details:

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

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

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

◆ Packet Filtering configuration example:

1. Packet Filter configuration procedures:

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

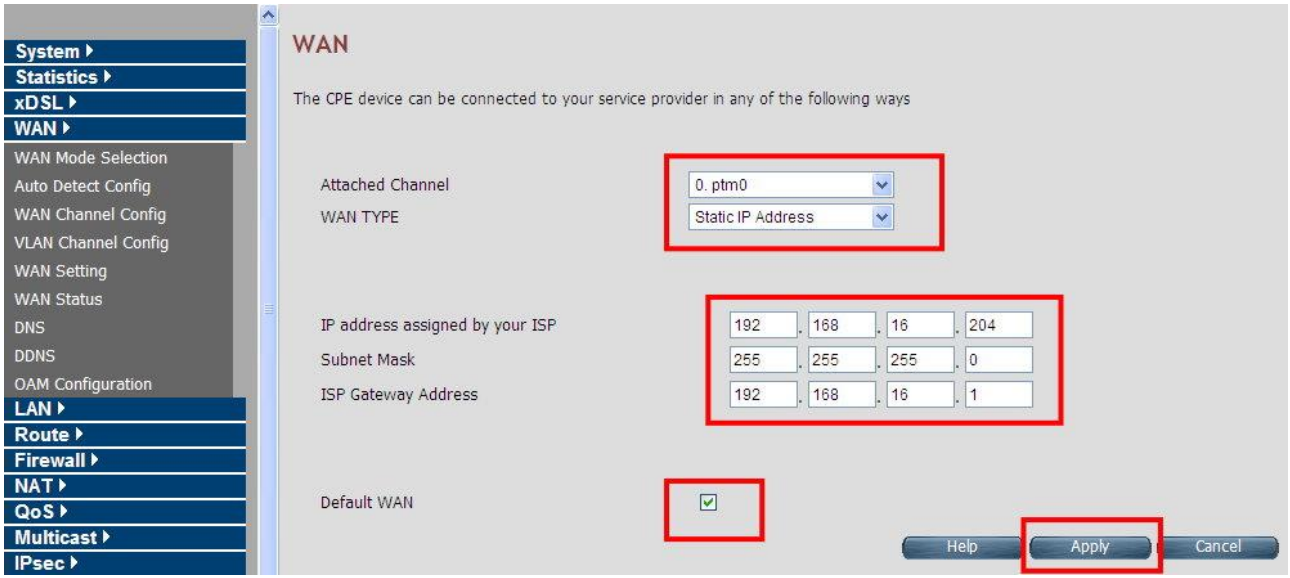
(2). Confirm that the ALL126AS3 is in router mode (default mode).

(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.

2. Router mode configuration:

◆ WAN setting

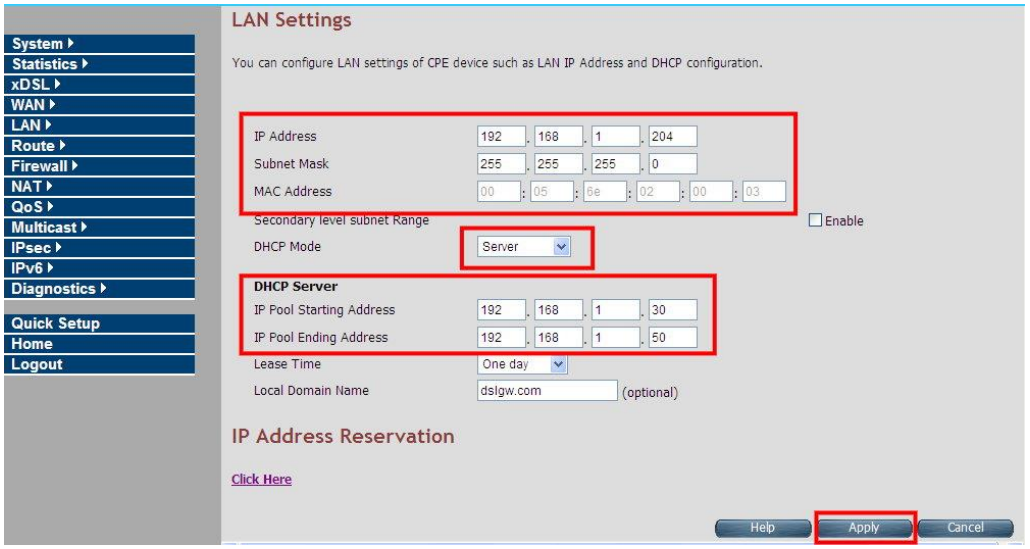


Configure example: WAN→WAN Setting

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

WAN setting complete

◆ LAN Setting

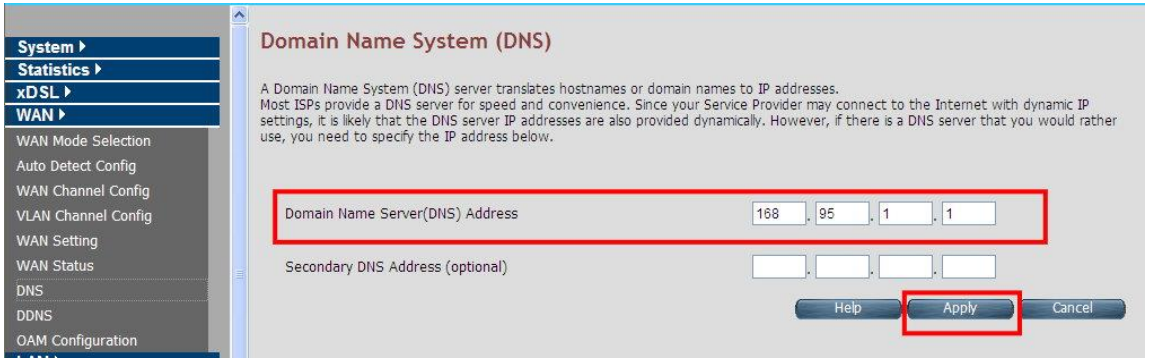


Configure example: LAN→LAN Settings

Items	Setting argument / Action
IP Address	LAN IP: 192.168.1.204 (Example)
Subnet Mask	255.255.255.0(Example)
MAC Address	ALL126AS3 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**

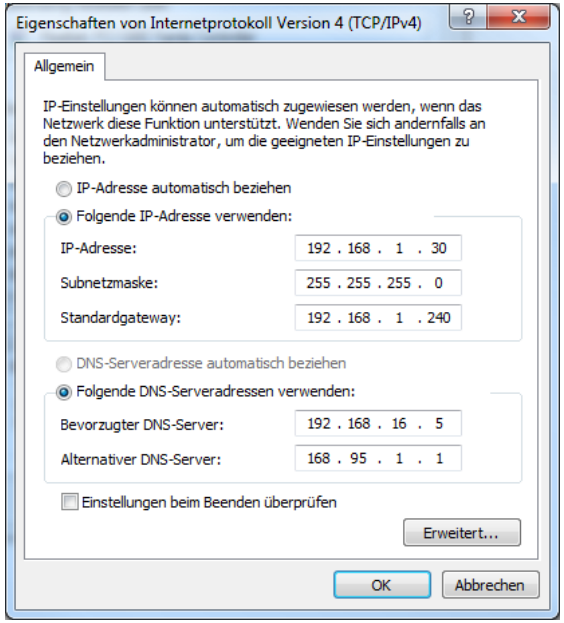


Configure example: WAN→DNS

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 ALL126AS3.

◆ **PC NIC card setting**

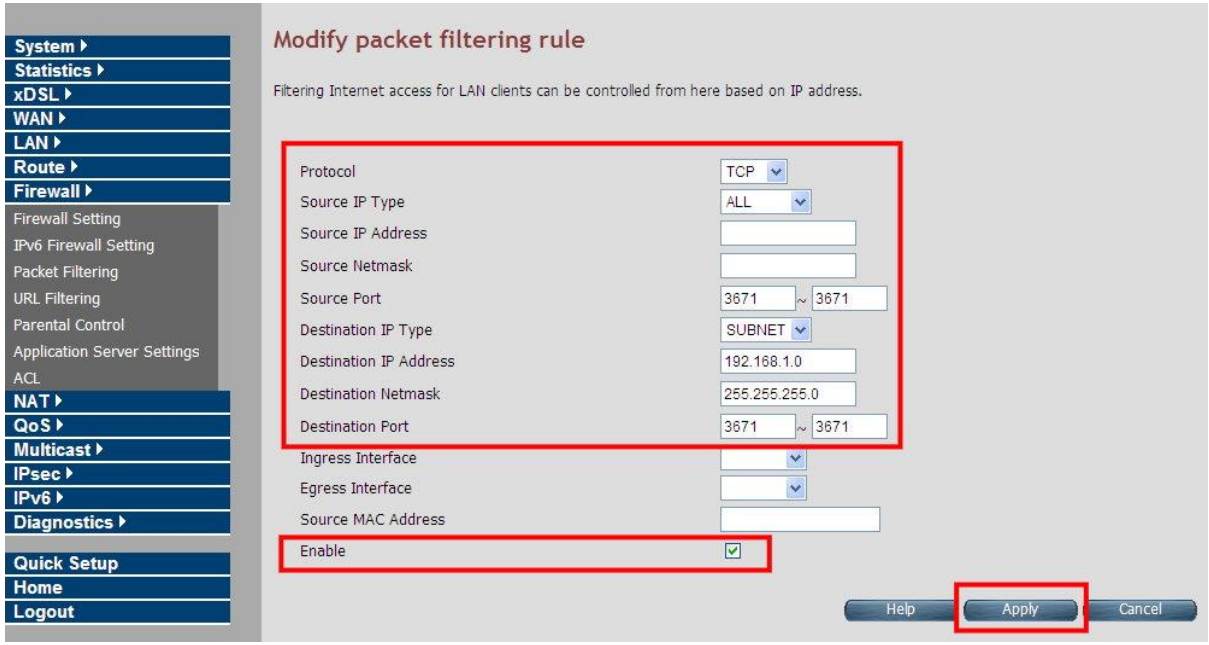


Configure example:

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)

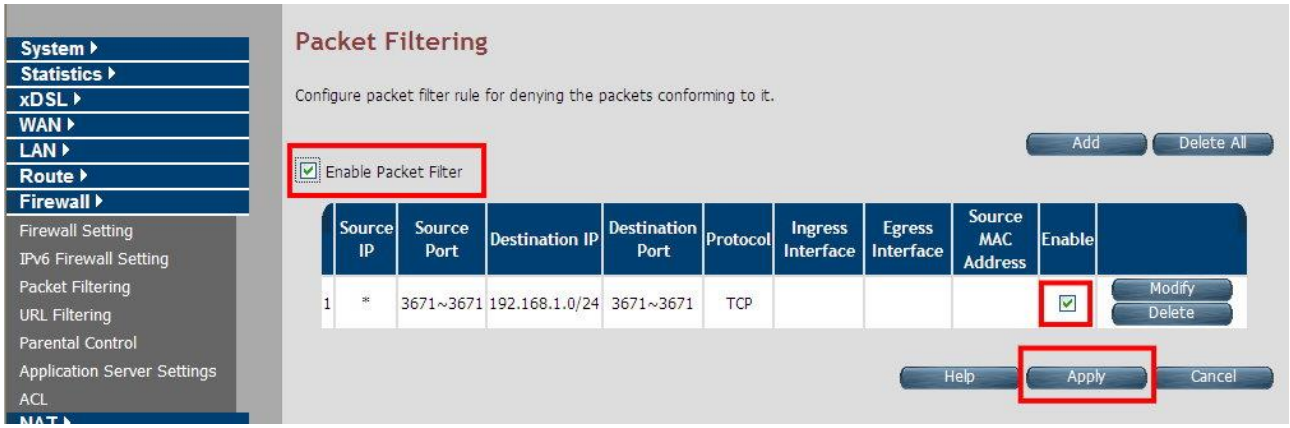
3. Packet Filtering configuration:

- **ALL126AS3 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.

4.9.4 URL Filtering

Using URL Filtering, the user can block the access to specific URLs to the web users by adding them to the list in the URL Blocking web page. To configure the URL Filtering, click the **URL Filtering** link (**Firewall > URL Filtering**) on the left navigation bar. A screen is displayed as shown in Figure 4.9.4

Figure 4.9.4 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.

4.9.5 Parental Control

To configure the Parental Control, click the **Parental Control** link (**Firewall > Parental Control**) on the left navigation bar. A screen is displayed as shown in Figure 4.9.5

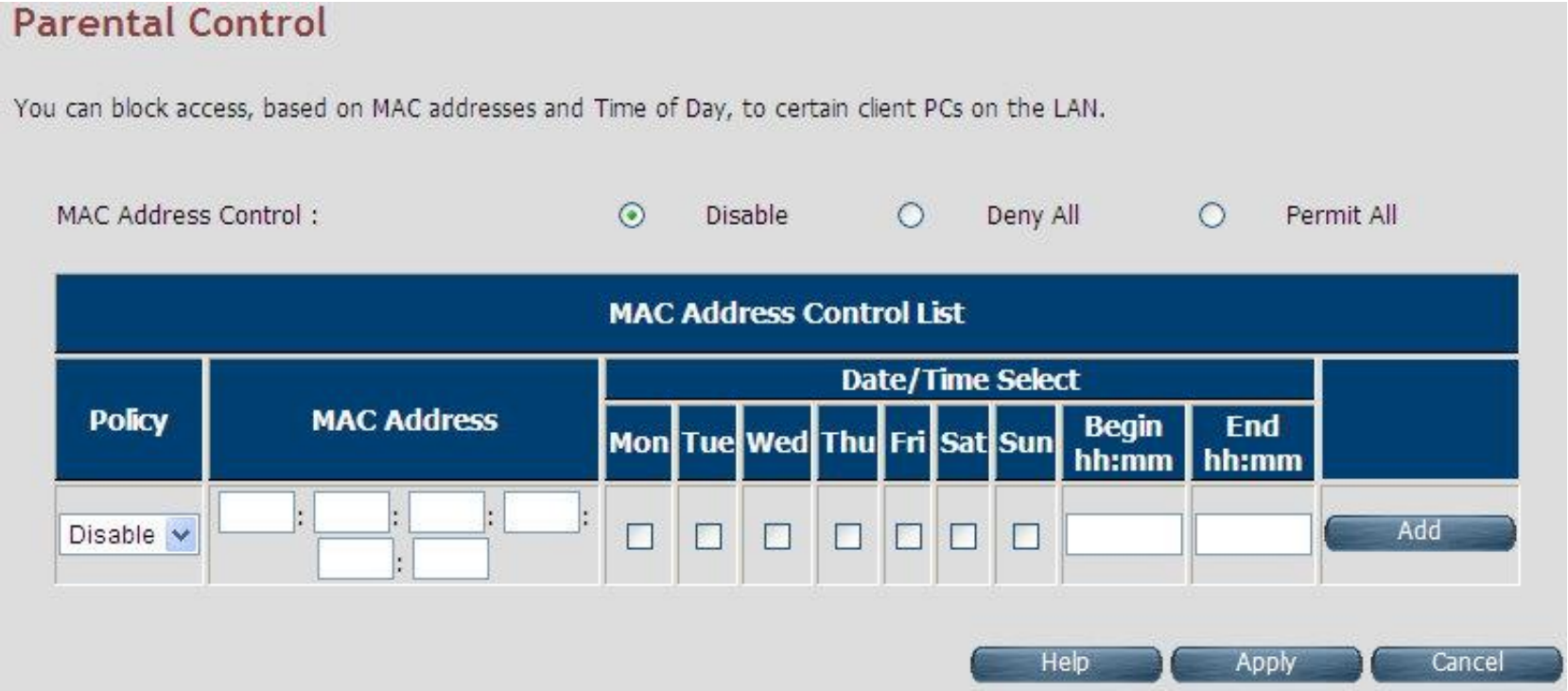


Figure 4.9.5 Parental Control Configuration

The screen contains the following details:

Fields in Parental Control:

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

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

4.9.6 Application Server Settings

To configure the Application Server Settings, click the **Application Server** Settings link (**Firewall** > **Application Server Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.9.6

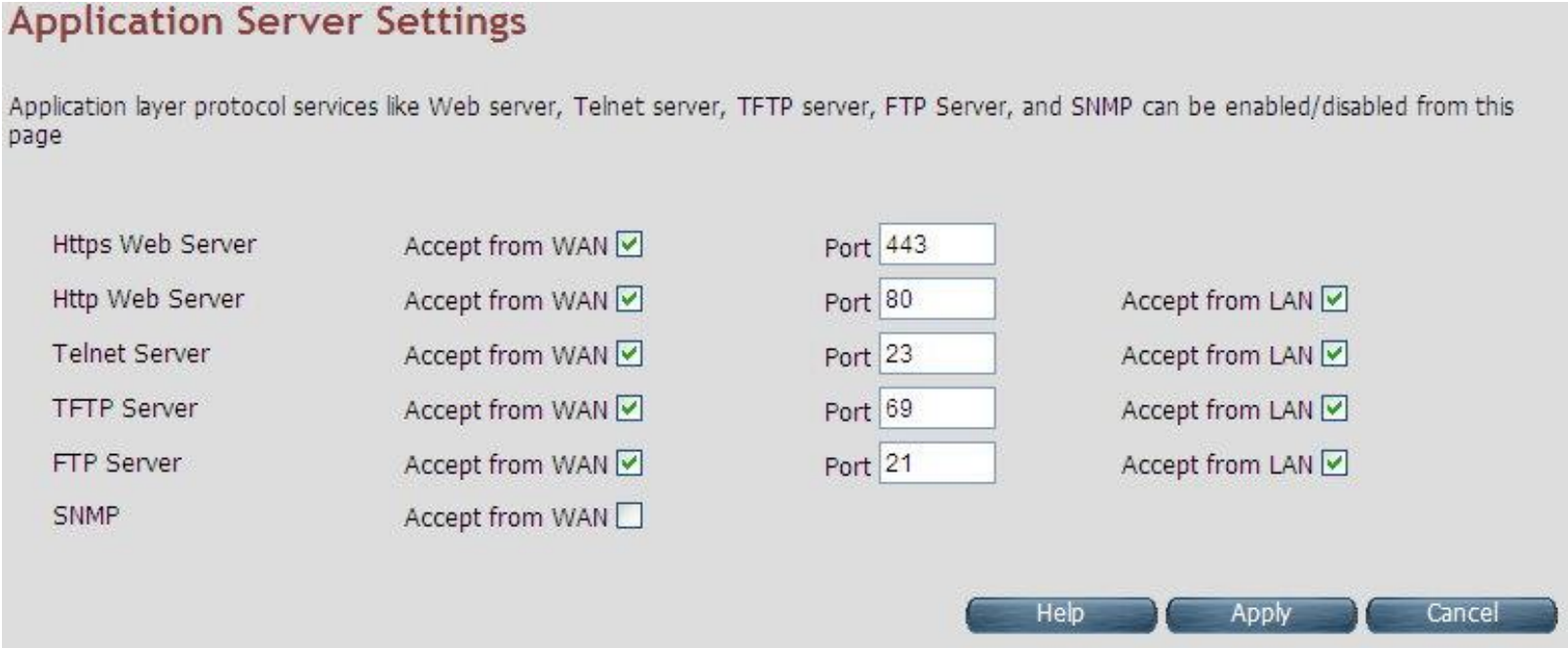


Figure 4.9.6 Application Server Settings

The screen contains the following details:

Fields in Application Servers Settings:

Field	Description
Web Server	Web Server settings: ◆ 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.

4.9.7 Access Control List (ACL)

To configure the access control list, click the **ACL** link (**Firewall > ACL**) on the left navigation bar. This can be used for allowing specified IP addresses to access the ALL126AS3 CPE from WAN. The system allows upto 16 ACL entries to be configured in the CPE device.A screen is displayed as shown in Figure 4.9.7.

Figure 4.9.7 Application Server Settings

The screen contains the following details:

Fields in ACL Setting:

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

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

4.10 NAT

You can view the NAT on the left navigation bar of the ALL126AS3 CPE homepage. The menu below includes the sub-menus

of NAT Settings, Virtual Server, PortTriggering and DMZ. Following are the options available under NAT as shown in Figure 4.10

Figure 4.10 NAT Options

4.10.1 NAT Settings

To configure Network Address Translation (NAT), click the **NAT Settings** link (**NAT > NAT Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.10.1

Figure 4.10.1 Network Address Translation (NAT) Settings

The screen contains the following details:

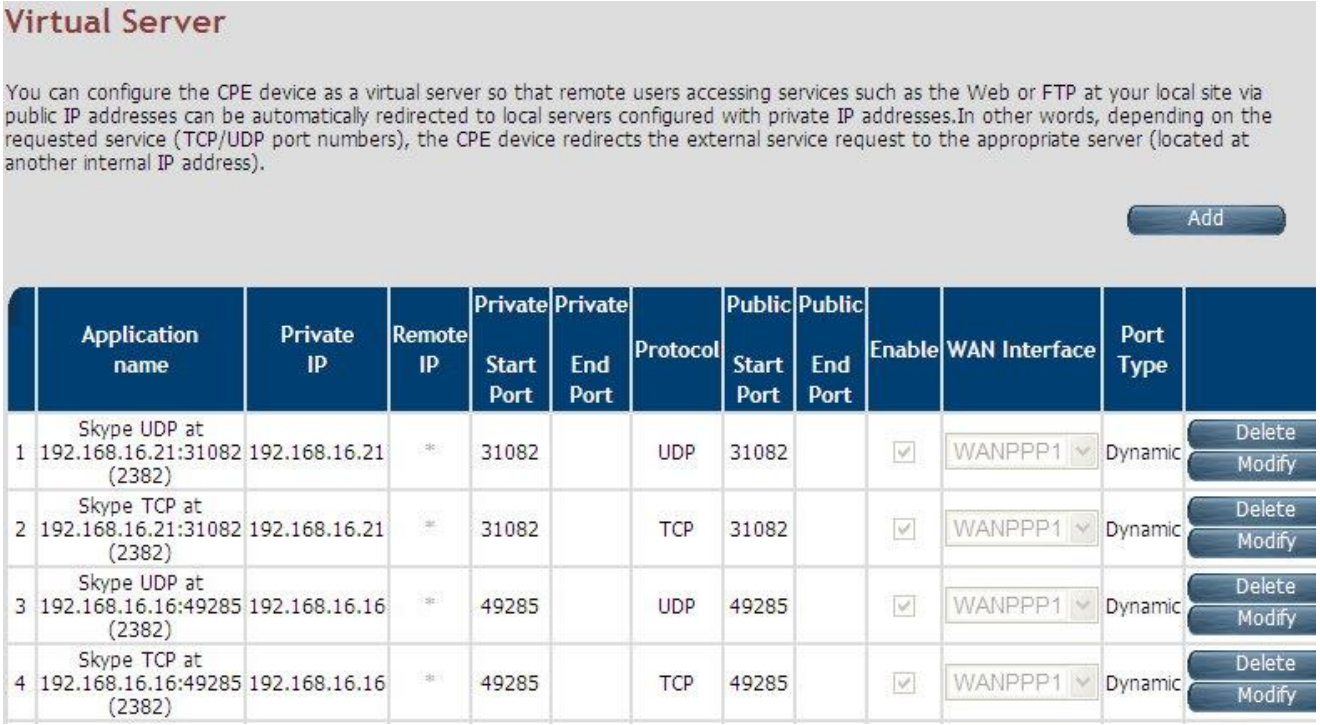
Fields in Network Address Translation:

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

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

4.10.2 Virtual Server

To configure the virtual server, click the **Virtual Server** link (**NAT > Virtual Server**) on the left navigation bar. A screen is displayed as shown in Figure 4.10.2



Virtual Server

You can configure the CPE device as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses.In other words, depending on the requested service (TCP/UDP port numbers), the CPE device redirects the external service request to the appropriate server (located at another internal IP address).

Add

	Application name	Private IP	Remote IP	Private Start Port	Private End Port	Protocol	Public Start Port	Public End Port	Enable	WAN Interface	Port Type	
1	Skype UDP at 192.168.16.21:31082 (2382)	192.168.16.21	*	31082		UDP	31082		☑	WANPPP1	Dynamic	Delete Modify
2	Skype TCP at 192.168.16.21:31082 (2382)	192.168.16.21	*	31082		TCP	31082		☑	WANPPP1	Dynamic	Delete Modify
3	Skype UDP at 192.168.16.16:49285 (2382)	192.168.16.16	*	49285		UDP	49285		☑	WANPPP1	Dynamic	Delete Modify
4	Skype TCP at 192.168.16.16:49285 (2382)	192.168.16.16	*	49285		TCP	49285		☑	WANPPP1	Dynamic	Delete Modify

Figure 4.10.2 Virtual Server

The screen contains the following details:

Fields in Virtual Server Page:

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

- Click Add to add a Virtual Server entry.

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

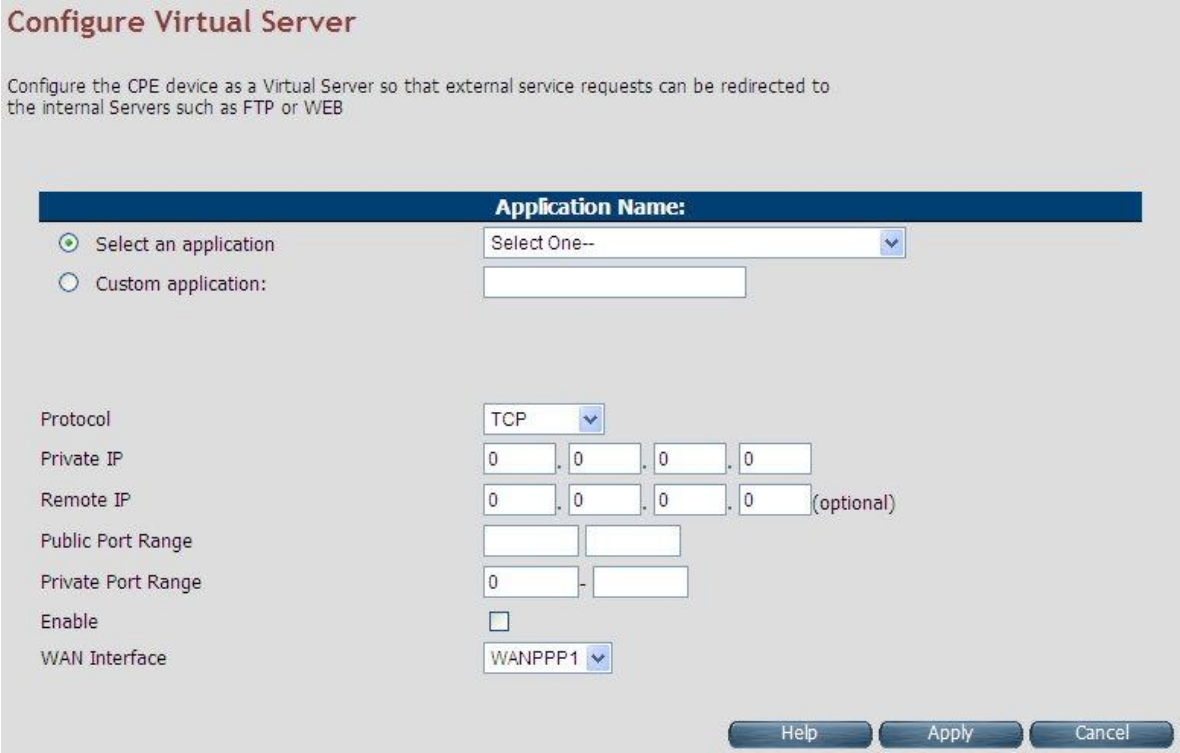


Figure 4.10.2.1 Virtual Server Add

The screen contains the following details:

Fields in Virtual Server - Add:

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

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

4.10.3 Port Triggering

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

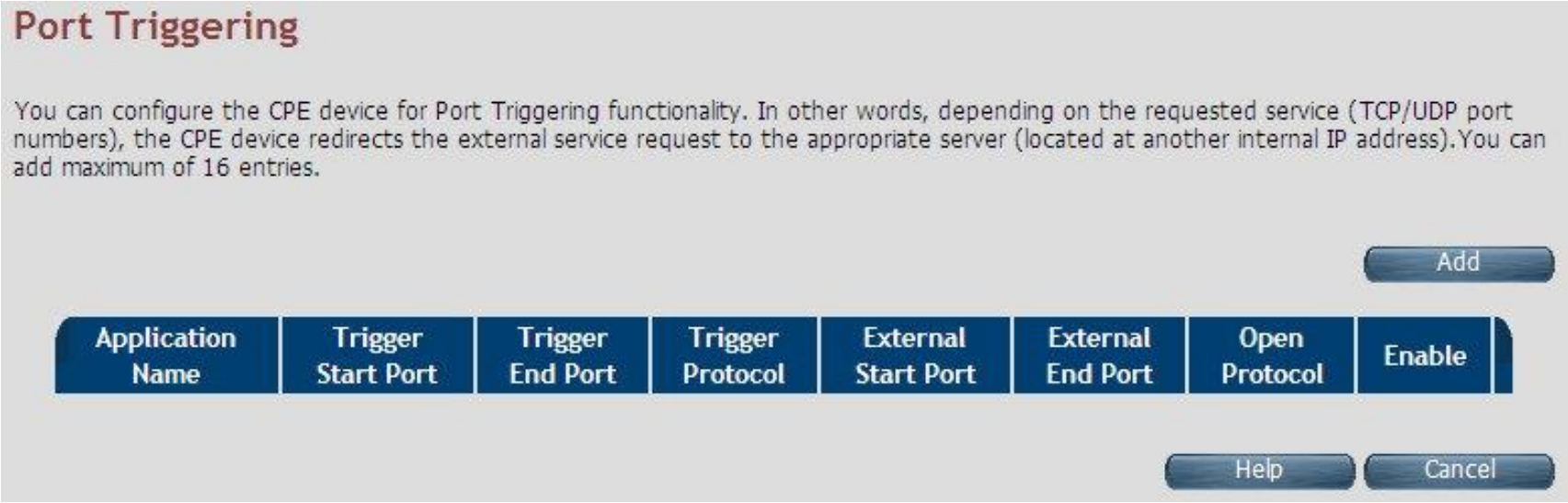


Figure 4.10.3 Port Triggering

The screen contains the following details:

Fields in Port Triggering:

Field	Description
Application Name	Port Triggering Application Name
Trigger Start Port	Trigger Port start range.
Trigger End Port	Trigger Port End Range. In 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 Add button in the Port Triggering page, a screen is displayed as shown in Figure 4.10.3.1.

Figure 4.10.3.1 Port Triggering Add

The screen contains the following details:

Fields in Port Triggering:

Field	Description
Application Name	Port Triggering Application Name.
Trigger Port Start	Trigger Port start range.
Trigger Port End	Trigger Port End Range. In 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.

4.10.4 DMZ

To configure the DMZ (Demilitarized Zone), click the **DMZ** link (**NAT > DMZ**) on the left navigation bar. Upon configuration of DMZ all traffic sent towards RG would be unconditionally forwarded to DMZ Lan Host. A screen is displayed as shown in Figure 4.10.4.

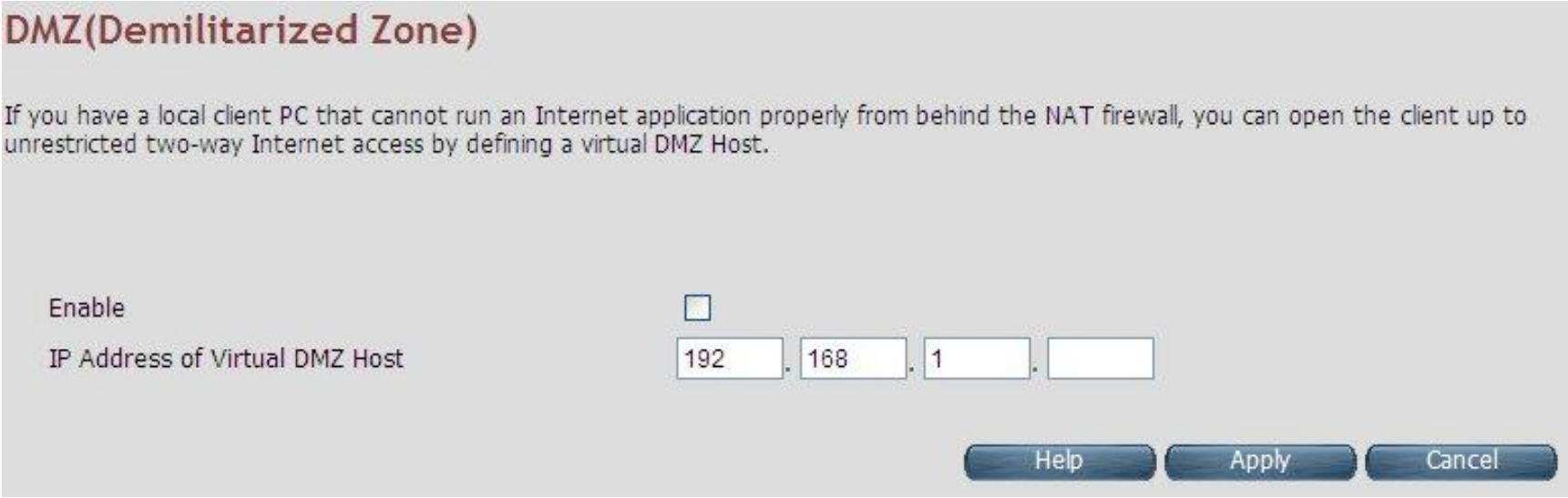


Figure 4.10.4 DMZ (Demilitarized Zone)

The screen contains the following details:

Fields in DMZ:

Field	Description
Enable	To enable or disable the DMZ setting of ALL126AS3 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 ALL126AS3 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

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

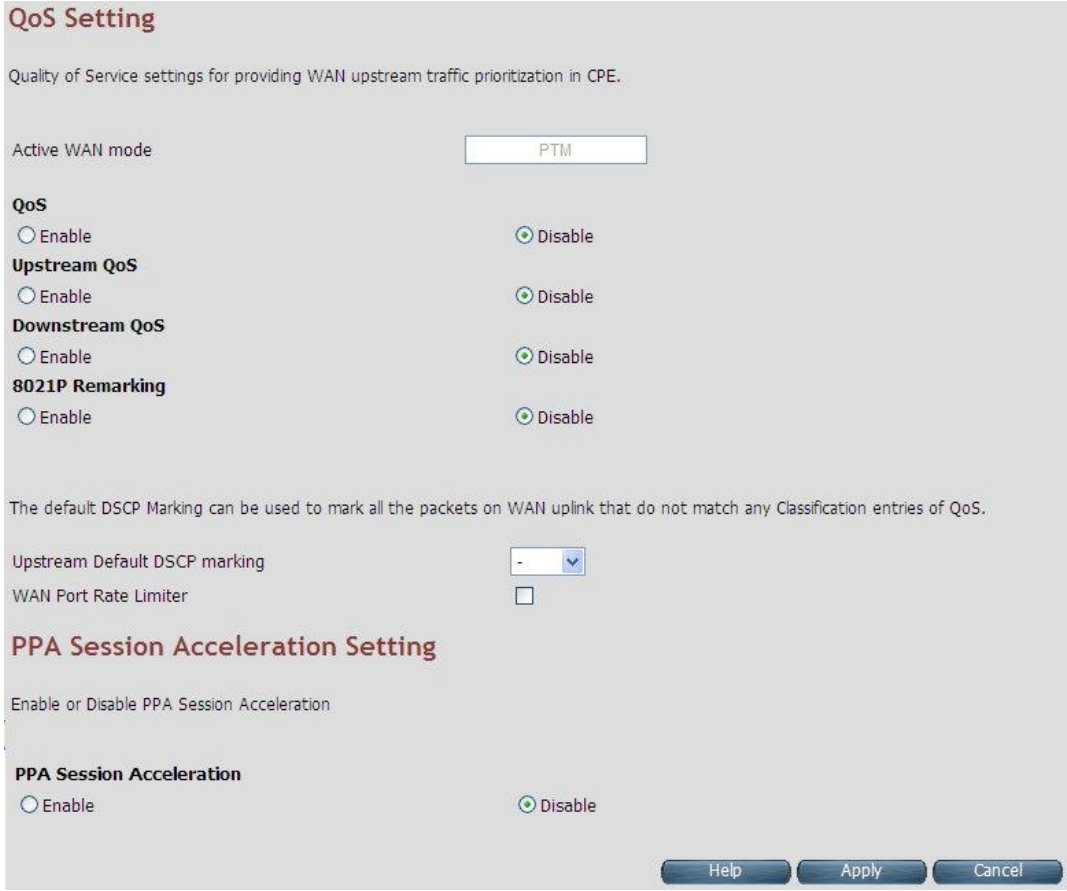


Figure 4.11.1 QoS Settings

The screen contains the following details:

Fields in QoS Settings:

Field	Description
Active WAN mode	Informative Parameter to show current WAN mode being used in CPE.
QoS	
Enable	This selection will enable the QoS feature in ALL126AS3 system.
Disable	This selection will disable the QoS feature in ALL126AS3 system.
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	To enable/disable the session acceleration feature.

- Click Apply for applying the QoS setting changes into system.

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

4.11.2 Queue Config

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

Queue Name	Queue Precedence	Drop Algorithm	Schedule Algorithm	Queue Weight	Committed Shaping Rate	Peak Shaping Rate	Enable	Action
def_queue	8	DT	SP	0	0	60000	Yes	
q1	1	DT	SP	0	0	60000	Yes	
q2	2	DT	SP	0	0	60000	Yes	

Figure 4.11.2 Queue Config

The screen contains the following details:

Fields in Queue Config - Upstream:

Field	Description
Upstream/Downstream	Selection tab for upstream/downstream Queue configuration.
Queue Name	This is the name of the queue configured in system.
Queue Precedence	Precedence of Queue. (Lower values denote higher priority).
Drop Algorithm	This specifies the nature of drop in case of congestion. The supported drop algorithms are DT (Drop Tail) or RED (Random Early Discard).
Scheduler Algorithm	This is the queue scheduling algorithm used for the queue. The 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 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 algo.
RED Max Drop Probability	RED Maximum Drop Probability in Percentage (drop_p). Value should be <100.
Queue Scheduler Type	Queue scheduling Algorithm. (SP or WFQ)
Queue Weight	Valid for Weighted Queuing mode of scheduled queues.
Apply Shaping	To apply shaping on queue.
Enable	Enable or Disable of Queue.

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

4.11.3 Class Config

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

Figure 4.11.3 Class Config

The screen contains the following details:

Fields in Class Config:

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

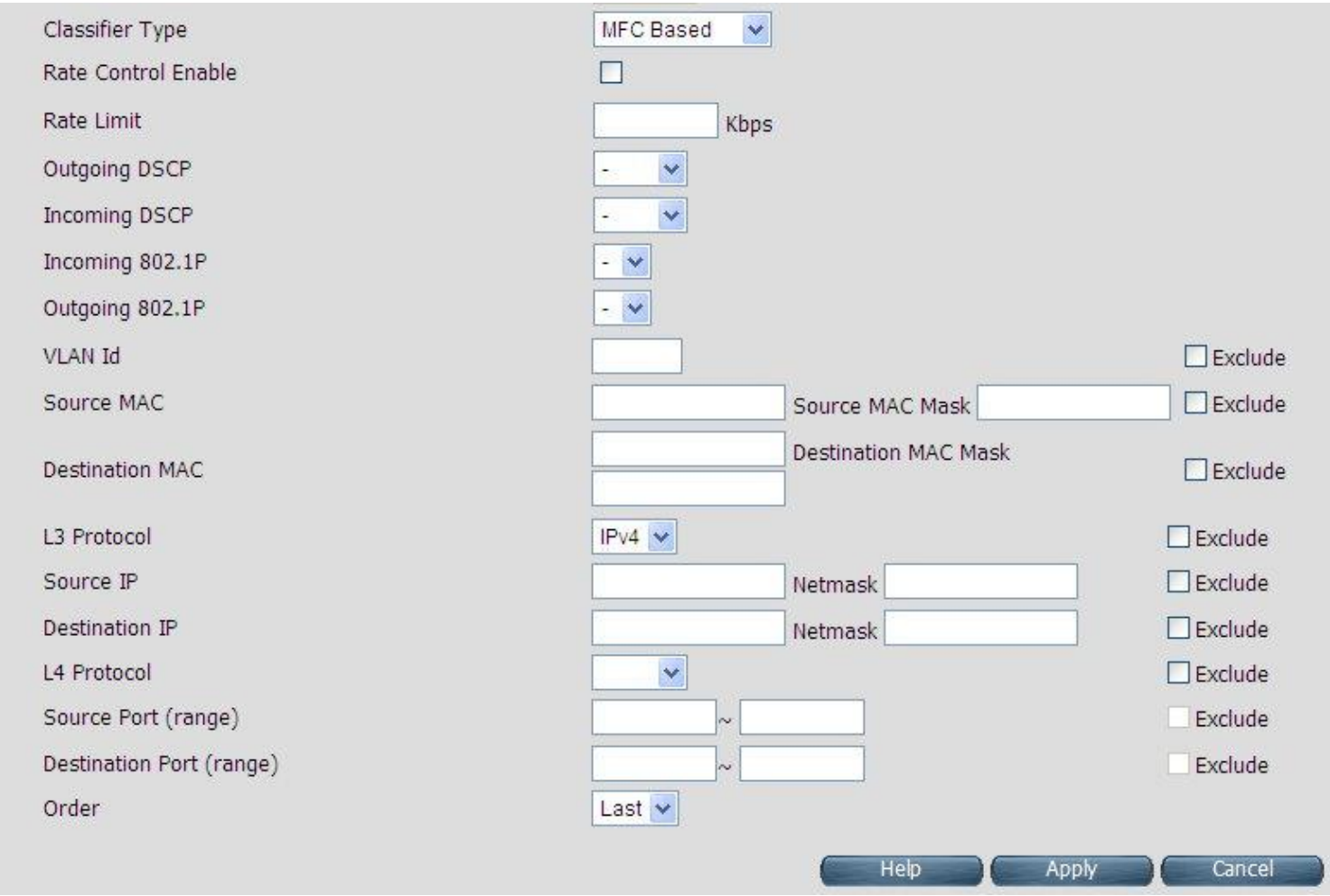


Figure 4.11.3.1 Add/Modify a Classifier Rule(MFC Based)

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 an 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 ALL126AS3 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

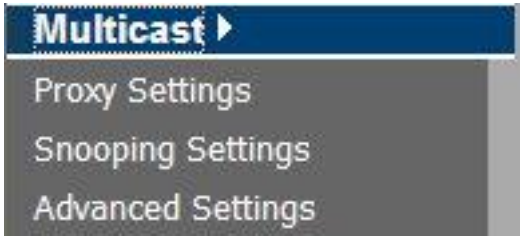


Figure 4.12 Multicast Options

4.12.1 Proxy Settings

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

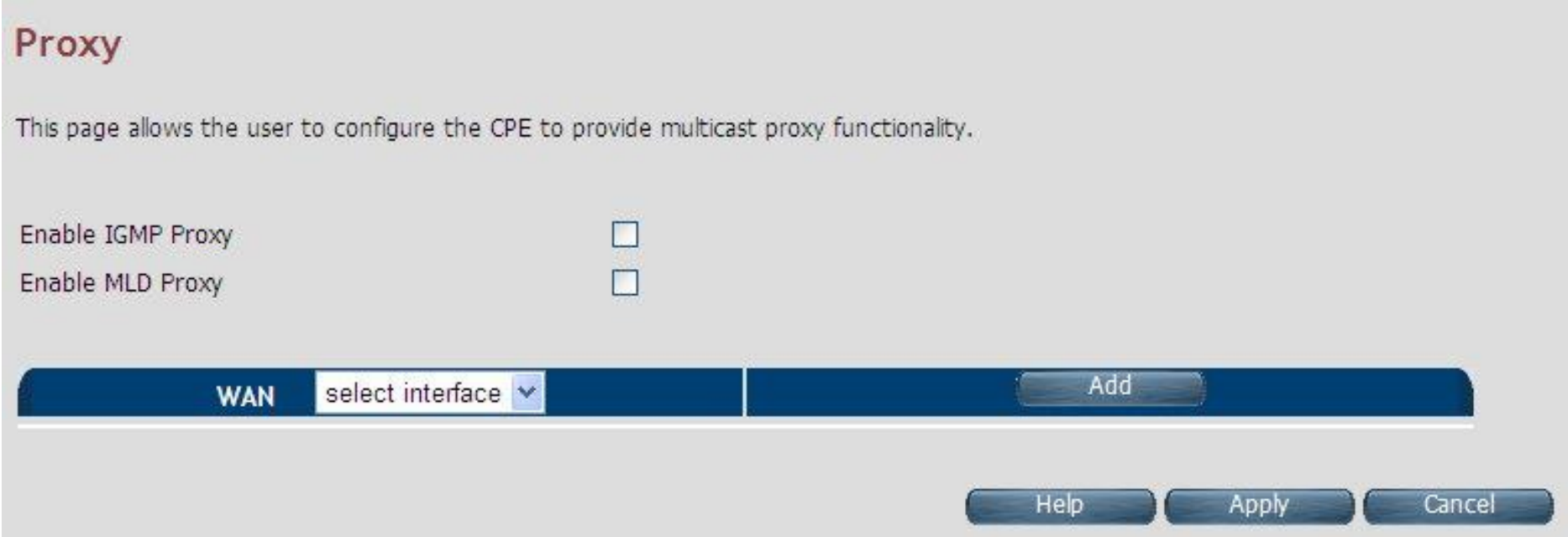


Figure 4.12.1 IGMP Proxy

The screen contains the following details:

Fields in IGMP Proxy:

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

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

4.12.2 Snooping Settings

To configure the Multicast Snooping settings, click the **Snooping Settings** link (**Multicast > Snooping Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.12.2

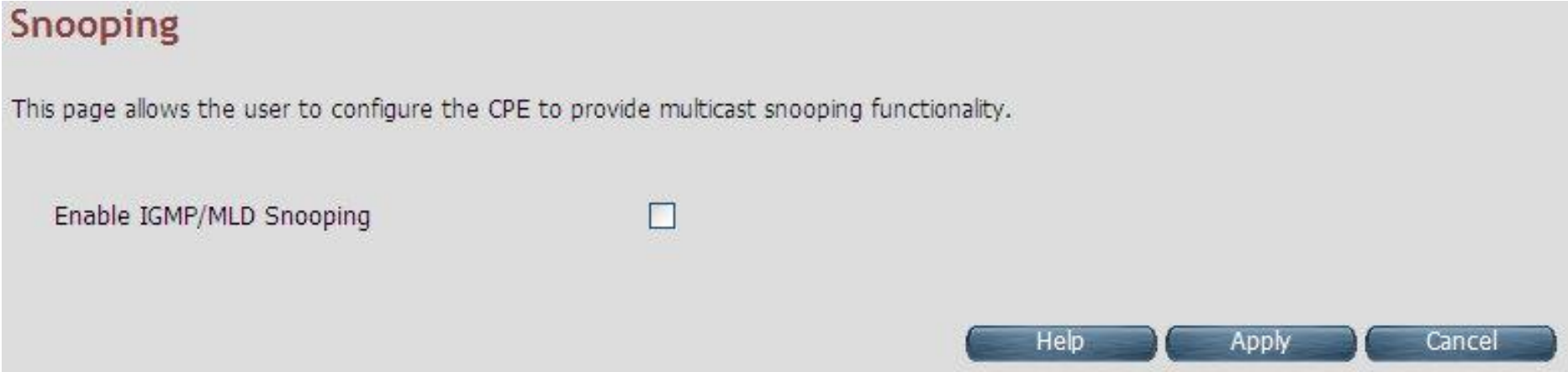


Figure 4.12.2 IGMP Snooping

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

To configure the advanced settings on Multicast features, click the **Advanced Settings** link (**Multicast > Advanced Settings**) on the left navigation bar. A screen is displayed as shown in Figure 4.12.3

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 is not to wait till 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 IPv6 tab.

4.13 IPsec

When you click IPsec on the left navigation bar of the ALL126AS3 CPE homepage. The menu below includes the sub-menus of Tunnel Mode. The following option Tunnel Mode is available under IPsec as shown in Figure 4.13

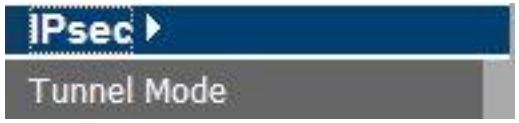


Figure 4.13 IPsec Option

4.13.1 Tunnel Mode

When 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

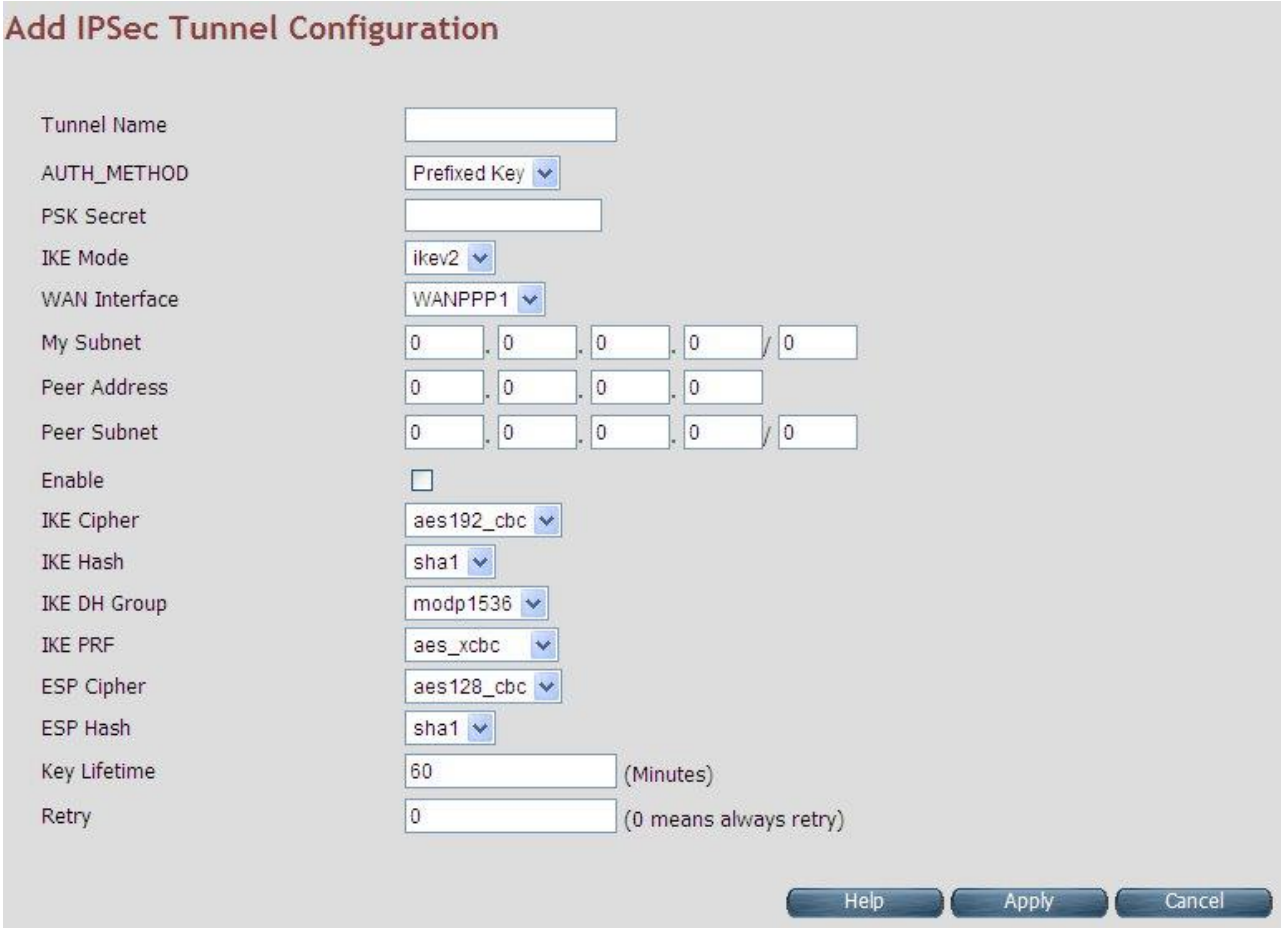


Figure 4.13.1.1 Add IPSec Tunnel Mode Configuration

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 tunnel to be created.,
My Subnet	LAN host connected to CPE.
Peer Address	Remote tunnel end point address.
Peer Subnet	Remote host IP address.
Enable	Enable or Disable of tunnel.
IKE Cipher	Cipher algorithm to be selected from dropdown.
IKE Hash	Hash algorithm to be selected from dropdown.
IKE DH Group	DH group algorithm to be selected from dropdown.
IKE PRF	PRF algorithm to be selected from dropdown.
ESP Cipher	ESP Cipher algorithm to be selected from dropdown.
ESP Hash	ESP Hash algorithm to be selected from dropdown.
Key Lifetime	Key Lifetime in seconds.
Retry	Number of retries in case key exchange fails.

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

4.14 IPv6

When you click IPv6 link on the left navigation bar of the ALL126AS3 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 the **IPv6 Setting** link on the left navigation bar. A screen is displayed as shown in Figure 4.14.1. By default IPv6 is not enabled.

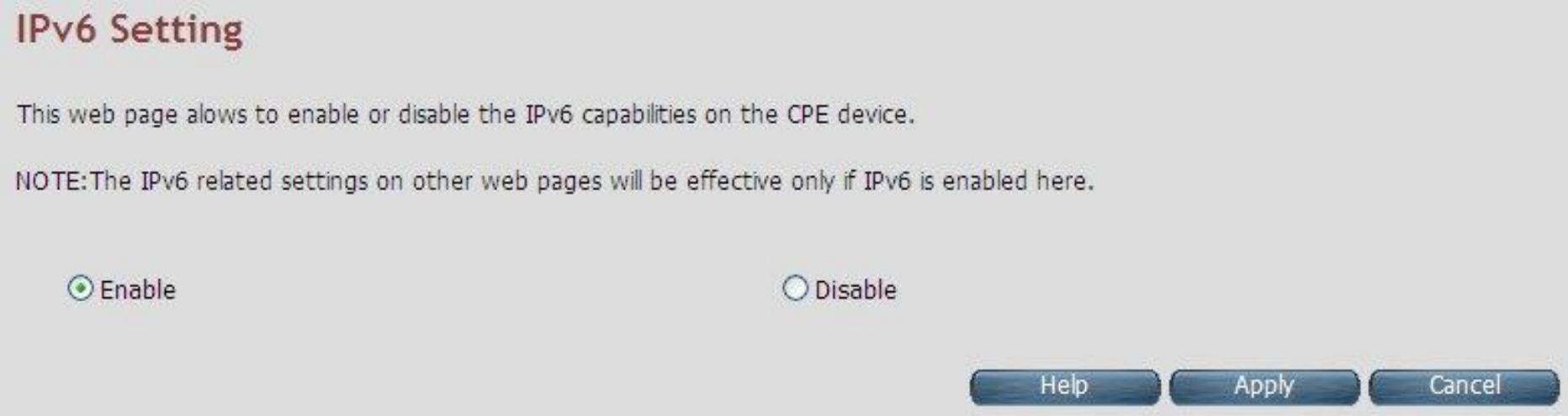


Figure 4.14.1 IPv6 Setting

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

Fields in IPv6 Setting:

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

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

4.14.2 6RD Configuration

The ALL126AS3 supports IPv6 transition mechanism defined in 6rd (RFC 5569). To configure the 6RD configuration, click the **6RD configuration** link (**IPv6 > 6RD Configuration**) on the left navigation bar. A screen is displayed as shown in Figure 4.14.2

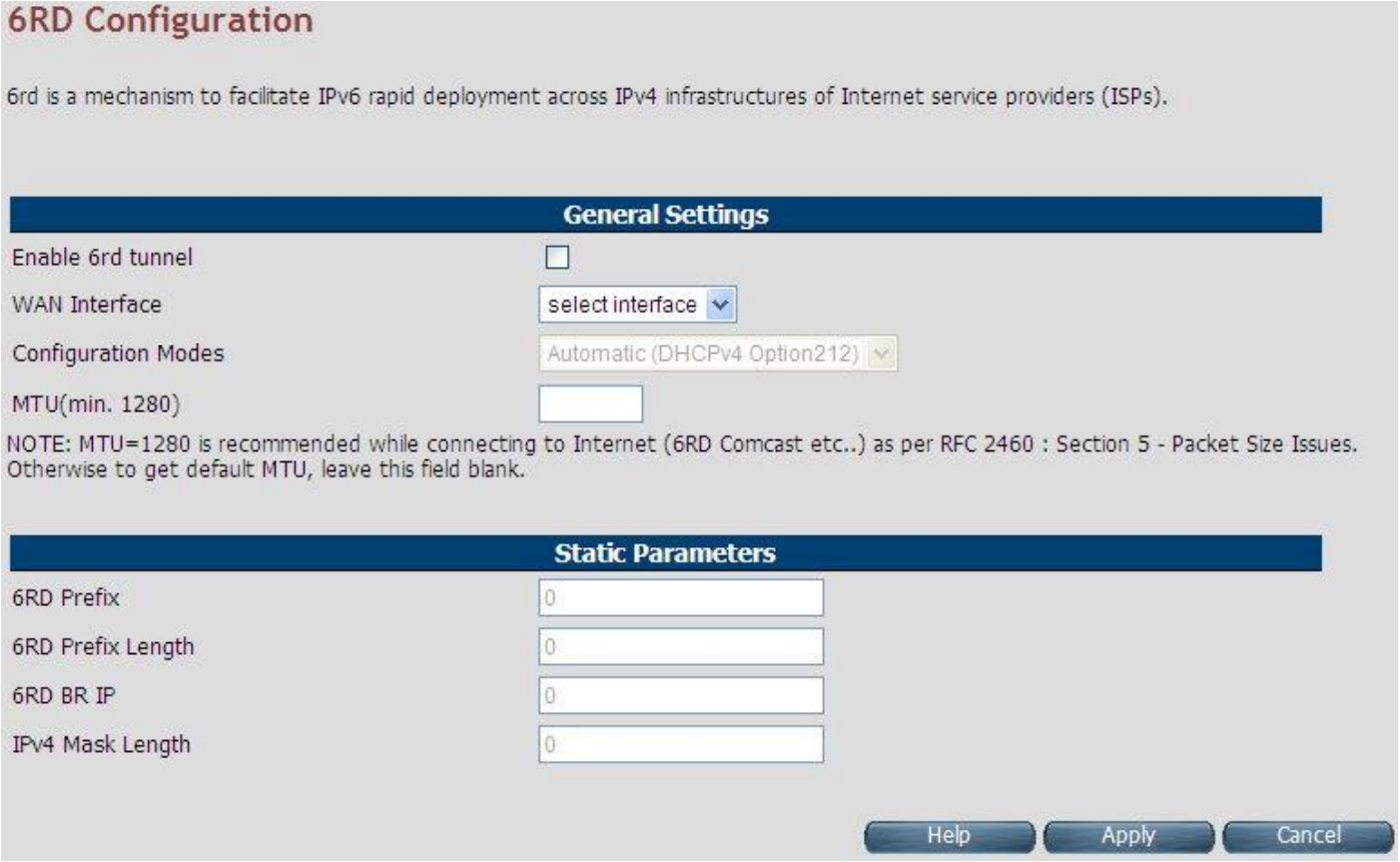


Figure 4.14.2 6RD Configuration

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 Broder 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 ALL126AS3 supports DS-Lite configuration mechanism. To configure the Ds-Lite configuration, click the **DS-Lite** configuration link (**IPv6 > DS-Lite Configuration**) on the left navigation bar. A screen is displayed as shown in Figure 4.14.3

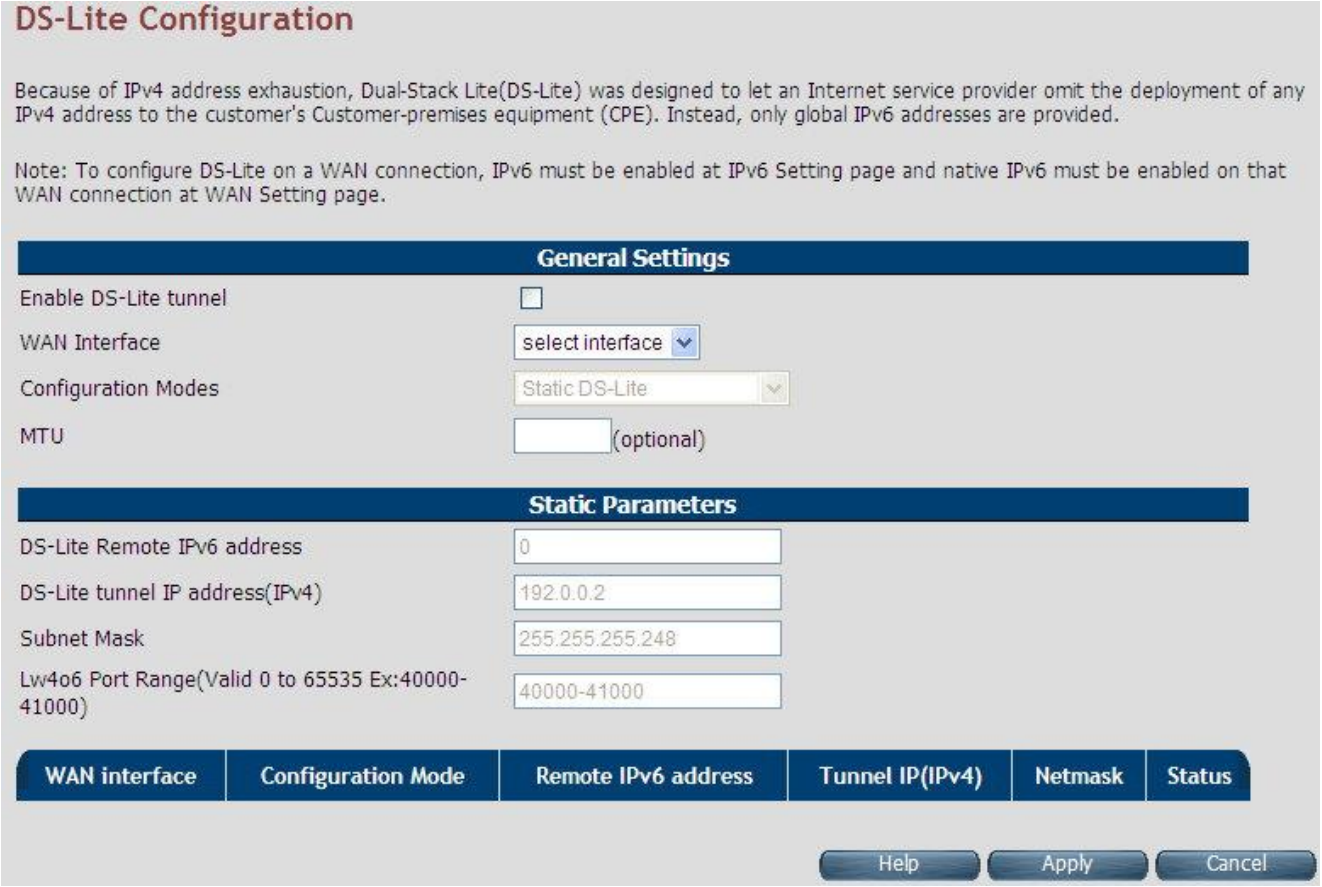


Figure 4.14.3 DS-Lite Configuration

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	Optionally, it is used to specify Maximum Transfer Unit size for DS-Lite tunnel.
Static Parameters	
DS-Lite Remote IPv6 address	IPv6 address of the remote tunnel endpoint. (When 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 you click Diagnostics link on the left navigation bar of the ALL126AS3 CPE homepage. The menu below includes the sub-menus of **Diagnostic Test Suite**. The following options are available under Diagnostics as shown in Figure 4.15

Figure 4.15 Diagnostics Options

4.15.1 Diagnostic Test Suite

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

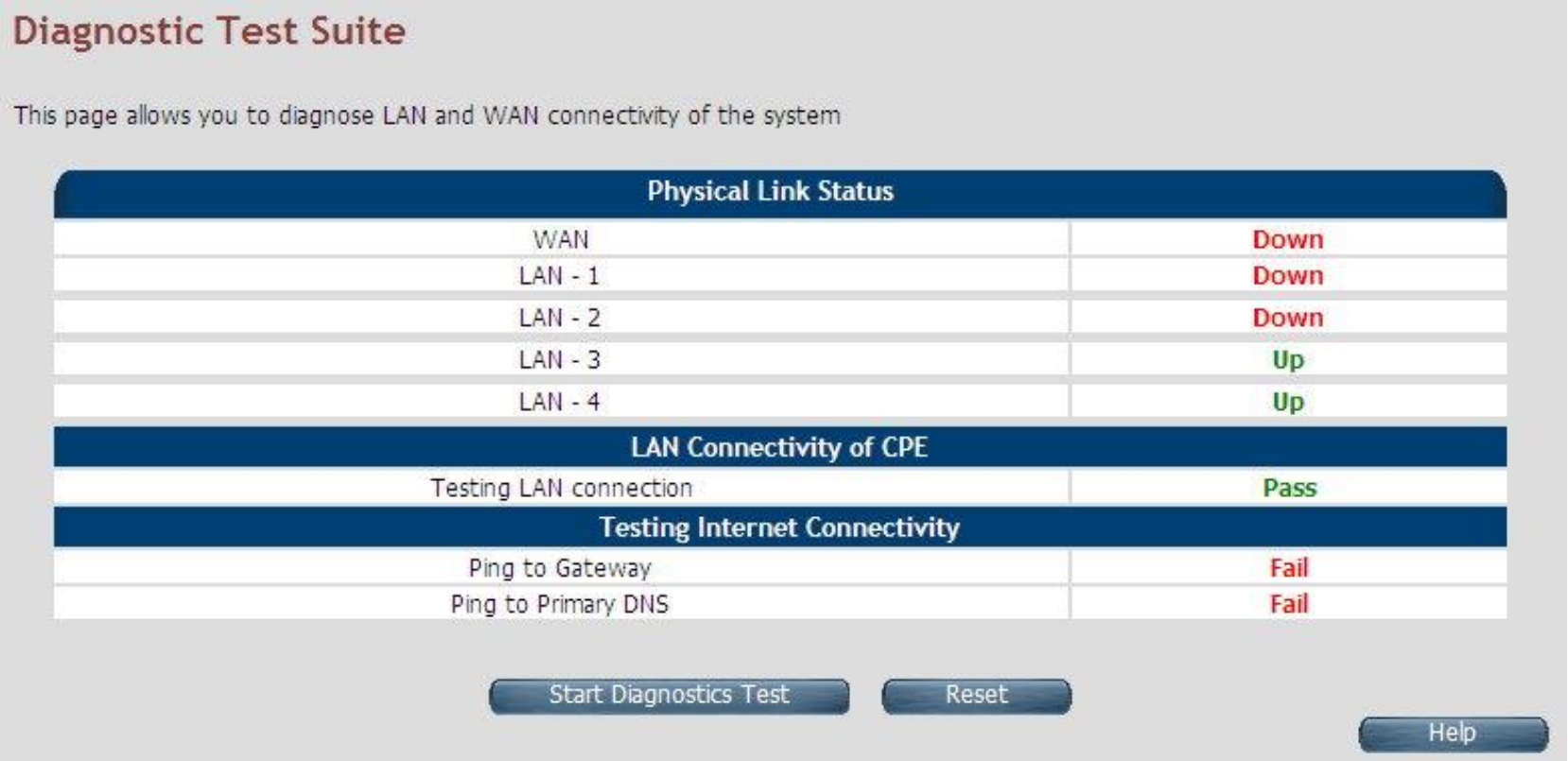


Figure 4.15.1 Diagnostic Test Suite

The screen contains the following details:

Fields in Diagnostic Test Suite:

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

Reset	Resets the diagnostics output.

Note: Please wait 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 Dependant interface	**Signal**	Media Dependant interface-cross
1	TX+	Transmit Data +	RX+	Receive Data +
2	TX-	Transmit Data -	RX-	Receive Data -
3	RX+	Receive Data +	TX+	Transmit Data +
4	--	Unused	--	Unused
5	--	Unused	--	Unused
6	RX-	Receive Data -	TX-	Transmit Data -
7	--	Unused	--	Unused
8	--	Unused	--	Unused

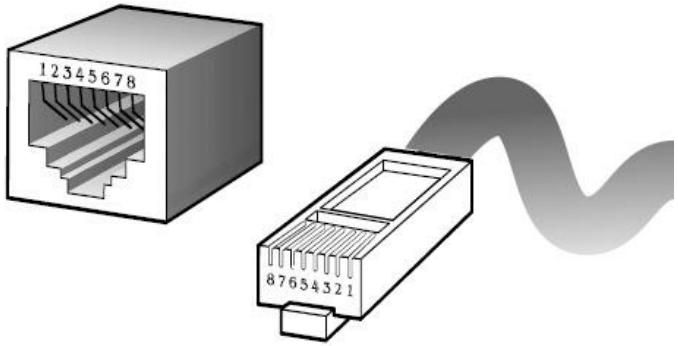


Figure A-1 Standard RJ-45 repectacle/connector

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-4)

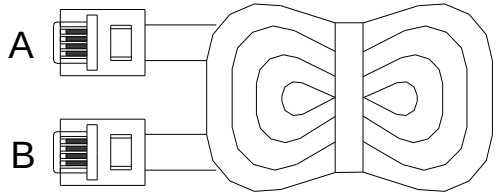


Figure A-4 Telephone cable

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

Table A-2 RJ-11 Pin out Assignments

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

Appendix B: Product Specification

Key Features & Benefits

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

- Support remote management and monitor
- Support configuration backup and restore
- Provides surge protection for Line port
- Supports jumbo frame up to 1680 bytes
- Supports IEEE 802.1w RSTP(*)
- Support Router & Switch(Bridged) mode selection
- Supports 8 queue MFC/DSCP both type QoS.

Note:

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 standards ITU-T G992.1/G992.3/G992.5/G993.1/G997.1/G993.2 standards
Physical Interface:	4 x RJ-45 10/100/1000Mbps Ethernet port 1 x RJ-11/Terminal Block connector for VDSL2 line port 1 x RJ-11 connector for POTS/ISDN device 1 x console port(RS232C/115200bps)

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
Switch method:	Store and forward
Typical Power Consumption:	6.7 W
Power Input:	Input Voltage: 12 VDC (Commerical-grade power adapter)
EMC:	EMI Compliant: FCC Class B EMS Compliant: CE mark Class B
Operating Temperature:	0°C ~ 50°C (32°F ~ 122°F) Fanless, free air cooling
Storage Temperature:	-20°C ~ 70°C (-4°F ~158°F)
Humidity:	10% to 90% (non-condensing)
Weight:	About 0.4 kgs
Dimensions:	184 x 146 x 40 mm (7.2" x 5.74" x 1.57")
Chipsets:	Lantiq VRX

Appendix C: Router Mode select

This appendix describes how to select the router mode, The ALL126AS3 default mode is switch(bridged mode), please refer to the following steps to select the router mode or switch mode.

◆ Select the Router mode:

1. To configure the router mode settings, click the **LAN Settings** link (**LAN > LAN Settings**) on the left navigation bar. Then select the "Server" at the DHCP Mode, and click Apply at any time during configuration to save the information that 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 to configure the DHCP Server settings.

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

Figure C-2 WAN Setting

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

Figure C-3 Config WAN Type

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

Appendix D: NV-600L & ALL126AS3/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 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 ALL126AS3 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 ALL126AS3 (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 ALL126AS3 (CPE) over phone wire while both power on, this will cause the link to fail. 3.2 Please check phone wire, we recommend use 24-26 gauge with twisted pair and without rust. 3.3 Please reinsert power when change cable length or link time over 3 minutes.
Note:	Phone wire must meet CAT 3 standard or above and **without clustering**, otherwise will cause more cross talk issue to reduce DSL power driver.

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

	infrastructure. The protocol was standardized in the International Telecommunication Union telecommunications sector (ITU-T) as Recommendation G.993.2. It was announced as finalized on 27 May 2005,[1] and first published on 17 February 2006. Several corrections and amendments were published in 2007 through 2011. VDSL2 is an enhancement to very-high-bitrate digital subscriber line (VDSL), Recommendation G.993.1. It permits the transmission of asymmetric and symmetric aggregate data rates up to 200 Mbit/s downstream and upstream on twisted pairs using a bandwidth up to 30 MHz. 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 program which is base on TCP/IP protocol such as FTP, Iperf, NetIQ, the bandwidth of testing outcome will be limited by TCP window size.
Solution:	We recommend to test VDSL2 bandwidth best by Smartbit equipment, if you don't have Smartbit, we recommend test that by IPERF program, and TCP window size must be settled max. 64k, the parameter as iperf –c server IP address –i 1 –t 50 –w 65535 for client side.

7. Question:	I just bought a ALLNET ALL126AS3 to replace my Quest DSL modem for my home. I was told any VDSL2 modem would replace and give me higher communication speeds. It doesn't get me internet when hooked up. All lights come on but no Link light. Is this the complete wrong application for this

	unit?
Answer:	Re: Please note ALL126AS3 is a remote side(CPE side), it must be connected to the CO side to work. Tone mode, Band profile and band plan setting must be compatible to each other if not access error will show when applied. Please deactivate and activate once the setting has been changed.

8. Question:	We need to set up a default gateway on a NV-600 pair which are in Bridge mode, as they want to manage the units from a different network.
Answer:	When the application is used within the LAN, the switch(bridged) mode is not necessary to set up a gateway .However, if the application crosses various network segments (LAN to WAN or WAN to LAN), you must set up a gateway to connect different network segment. Regarding how to configure a default gateway at switch(bridged) mode for crossing various network segments , please refer to the section 4.8.1 for your reference. Configuration gateway example 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:	Is it possible to use ADSL2 IP DSLAM with the ALL126AS3?
Answer:	ALL126AS3 support the ADSL backward compatible, therefore the ALL126AS3 can connect to ADSL2 IP DSLAM(Annex B).

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

11. Question:	What is the maximum Ethernet frame MTU for these routers?
Answer:	ALL126AS3 maximum Ethernet frame MTU is 1680 bytes(Jumbo Frame).

System Diagnostics

Power and Cooling Problems

If the POWER indicator does not turn on when the power cord is plugged in, 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 default method of selecting the transmission mode for RJ-45 ports is 10/100 Mbps ETHERNET, for RJ-11 port are auto-negotiation VDSL. Therefore, if the Link signal is disrupted (e.g. by unplugging the network cable and plugging it back in again, or by resetting the power), the port will try to reestablish communications with the attached device via auto-negotiation. If auto-negotiation fails, then communications are set to half duplex by default. Based on this type of commercial-standard connection policy, if 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.

CE-Declaration of Conformity

For the following equipment: Germering, 3rd of January, 2015

VDSL2 Slave Modem

ALL126AS3

The safety advice in the documentation accompanying the products shall be obeyed. The conformity to the above directive is indicated by the CE sign on the device.

The Allnet ALL126AS3 conforms to the Council Directives of 2004/108/EC.

This equipment meets the following conformance standards:

EN55022:2010,
EN61000:3-2:2006+A1:2009+A2:2009
EN61000-3-3:2008
IEC61000-4-4:2004+A1:2010
IEC61000-4-5:2005
IEC61000-4-6:2008
IEC61000-4-8:2009
IEC61000-4-11:2004

EN55024:2010
IEC61000-4-2:2008
IEC61000-4-3:2006+A1:2007+A2:2010

This equipment is intended to be operated in all countries.

This declaration is made by
ALLNET Computersysteme GmbH
Maistraße 2
82110 Germering
Germany

Germering, 03.01.2015

Wolfgang Marcus Bauer
CEO

DISCLAIMER_OF_WARRANTY

This Program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2 of the License.

This Program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this Program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

The full text of the GNU General Public License version 2 is included with the software distribution in the file LICENSE.GPLv2

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES

PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Written Offer for Source Code

For binaries that you receive from ALLNET GmbH Computersysteme on physical media or within the download of the offered firmware that are licensed under any version of the GNU General Public License (GPL) or the GNU LGPL, you can receive a complete machine-readable copy of the source code by sending a written request to:

ALLNET GmbH Computersysteme

Maistrasse 2
82110 Germering

Your request should include: (i) the name of the covered binary, (ii) the version number of the ALLNET product containing the covered binary, (iii) your name, (iv) your company name (if applicable) and (v) your return mailing and email address (if available). We may charge you a nominal fee to cover the cost of the media and distribution. Your request must be sent within three (3) years of the date you received the GPL or LGPL covered code. For your convenience, some or all of the source code may also be found at:

http://www.allnet.de/gpl.html

LICENSE.GPLv2

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other

Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the

operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and

all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License

may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals

of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE

POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be

mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

LICENSE.LGPLv2.1

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use,

not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using

a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or

other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not

covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public

License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy

from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work

during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is

interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute

the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made

generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library

specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting

redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software

Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!