COMTREND CORPORATION

CT-535
Wireless ADSL Router
User's Manual

Version A1.3, November 20, 2003

261035-017

Revision History

Modified the following sections:

- ADSL Mode
- DHCP
- NAT
- Configure

Preface

This manual provides information to network administrators. It covers the installation, operation and applications of the Wireless ADSL Router

Warning

Before servicing or disassembling this equipment, always disconnect all power and telephone lines from the wall outlet.

Use an appropriate power supply and a UL Listed telephone line cord. Specification of the power supply is stated in Appendix A - Specifications.

TABLE OF CONTENTS

Chapter 1 Introduction

1.1 Overview

The wireless ADSL router combines cutting-edge wireless technology with routing/bridge functions. It enables multiple users to share a high speed ADSL connection, without connecting any wires. To ensure the security of your valuable data the router employs state-of-the-art security features such as WEP data encryption, L2TP, and IpSec pass through. To provide maximum immunity from broadband interference the router incorporates the latest wireless modulation technology (DSSS). The router is designed for residential and business users who need wireless access through an ADSL router.

In addition to wireless connectivity, the wireless ADSL router has four 10/100 Base-T Ethernet ports for LAN connection. It can access the Internet, Corporate LAN, or Video on Demand over one ordinary telephone line, and establish up to 8 concurrent virtual-connections to multiple destinations.

1.2 Features

The Wireless ADSL Router has the following features:

- Wireless built-in ADSL router
- IEEE 802.11b compliance
- 11Mbps/5.5Mbps/2Mbps/1Mbps data rates with auto-fallback support
- WEP data encryption
- Four 10/100 Base-T Ethernet ports for LAN connection
- Bridge/Router
- AAL5 for ATM over ADSL
- UBR/CBR/VBR ATM services
- VC-based and LLC multiplexing
- Up to 8 VCs
- Embedded SNMP agent and RFC MIB II
- Web-based management
- OAM F4 and F5
- Static route/RIP/RIP v2 routing
- Dynamic IP assignment and Network Address Translation

1.3 Application

The following diagram shows a typical application of the router, which can be used for G.lite and G.DMT applications.

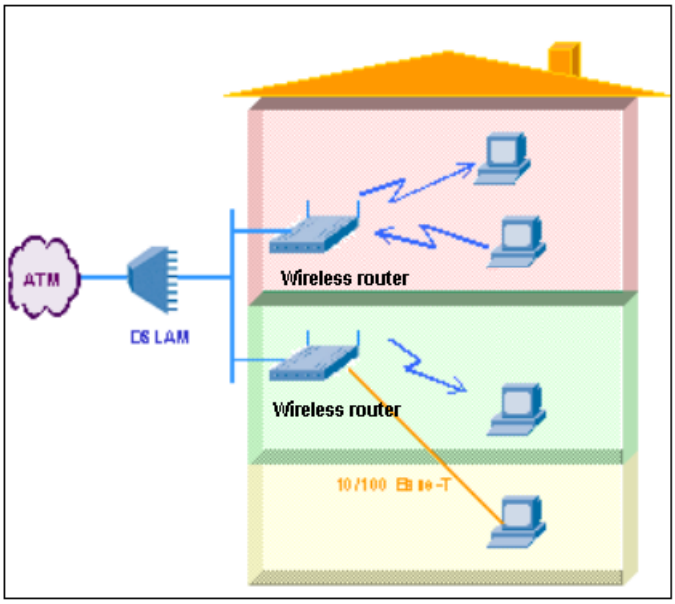
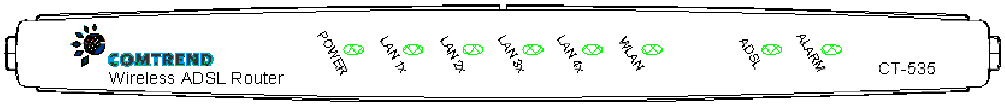


Figure 1-1 Application

1.4 Front Panel LED Indicators

The front panel LEDs are shown in the picture below, followed by an explanation in the table below.



LED	Color	Mode	Function
Power	Green	On Off	The router is powered up The router is powered down.
LAN 1x~4x	Green	On Blink Off	Ethernet connection is established. Data transmitting or receiving Ethernet connection is not established.
WLAN	Green	Blink Off On	Data transmitting or receiving over WLAN The wireless is not installed. The wireless module is ready and idle.
ADSL	Green	On Off	The ADSL connection is established. ADSL connection is not established.
ALARM	Red	On	The ADSL link is terminated.
		Off	Normal operating status

Chapter 2 Installation

2.1 Preparing for Hardware Installation

The following equipment may be necessary to install the router:

- **A VT-100 compatible terminal**
  This terminal is essential to perform the initial configuration of the router. Normally this is a terminal with a VT-100 emulation program, such as Telix.

- **An RJ45-to-DB9 cable to connect to the Console Port**
  An RS232, RJ45-to-DB9 straight-through cable is required to connect the terminal to the device.

- **AC power adapter**
  A suitable power adapter is shipped with the router. It is used to provide the necessary power for the router's operation.

- **LAN connection cable**
  To connect to a hub or PC, use an RJ45 cable.

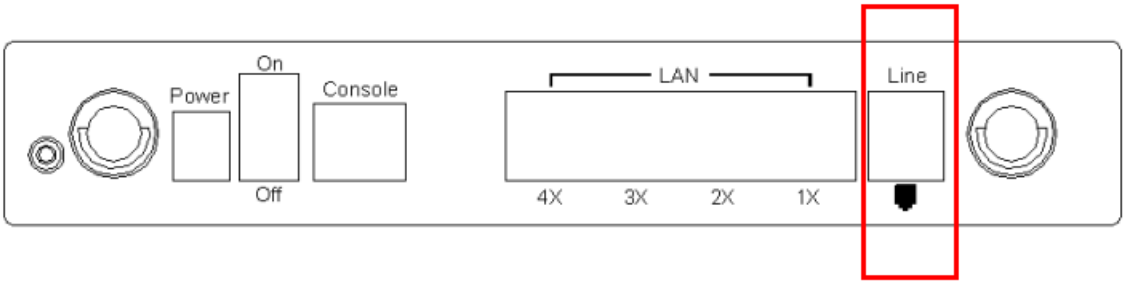
- **RJ11 cable**
  An RJ11 cable is needed to connect to the LINE port.

- **Optional micro filter and POTS splitter**
  If you wish to connect both the router and a telephone, you will need the optional micro filter or POTS splitter.

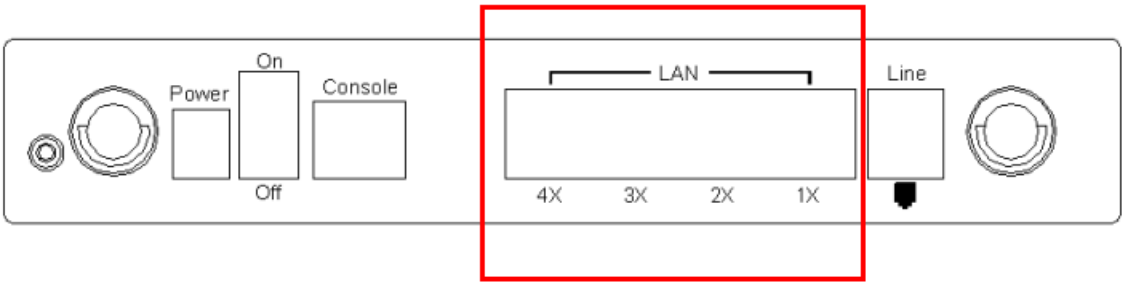
2.2 Hardware Installation

Follow the instructions below to complete the hardware connections.

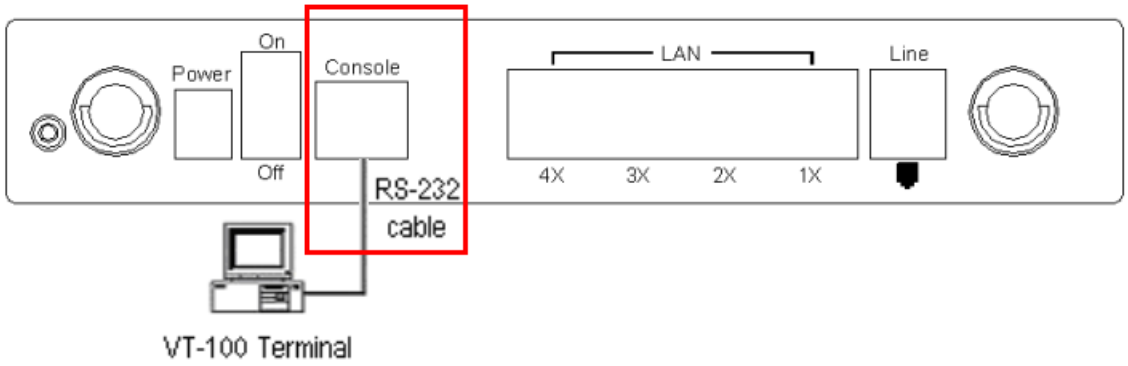
Step 1 Connect the **Line** port to a telephone-line using the supplied RJ-11 cable; or if you wish to connect both the router and a telephone, connect the ADSL port to a micro filter or POTS splitter with a RJ11 connection cable.



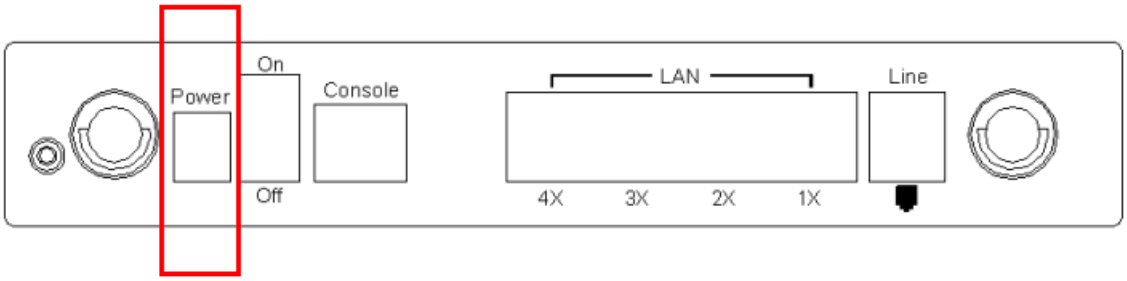
Step 2 To connect to a hub or PC, use a RJ45 cable. You can connect the router to four LAN devices. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.



Step 3 (Optional) In order to manage your device through the console port you will need to use a straight-through cable with an **RJ-45 connector** to attach to the modem, and a **female RS-232 connector** to connect to the serial port on a PC. The PC must be equipped with a VT-100 emulation program, such as HyperTerminal 5 or Telix.

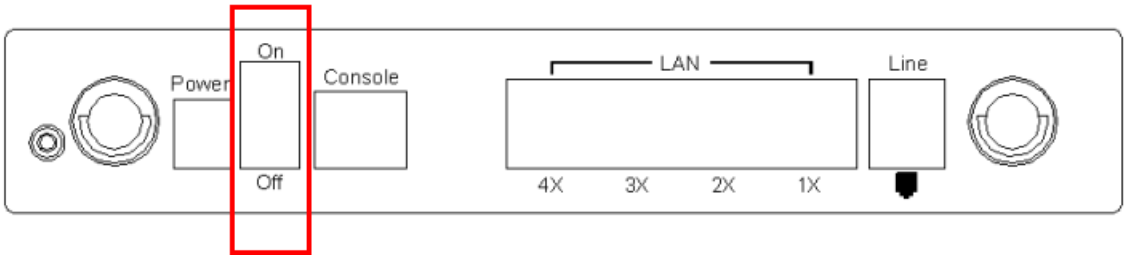


Step 4 Connect the **Power** jack to the shipped power cord.



Step 5 Attach the power adapter to the wall outlet or other AC source.

Step 6 After all connections have been made, turn the power-switch to the on position. After power on, the router performs a self-test. Wait for a few seconds until the test is finished, then the router will be ready to operate.



Caution 1: If the router fails to power up, or it malfunctions, first verify that the power supply is connected correctly. Then power it on again. If the problem persists, contact our technical support engineers.

Caution 2: Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from the wall outlet.

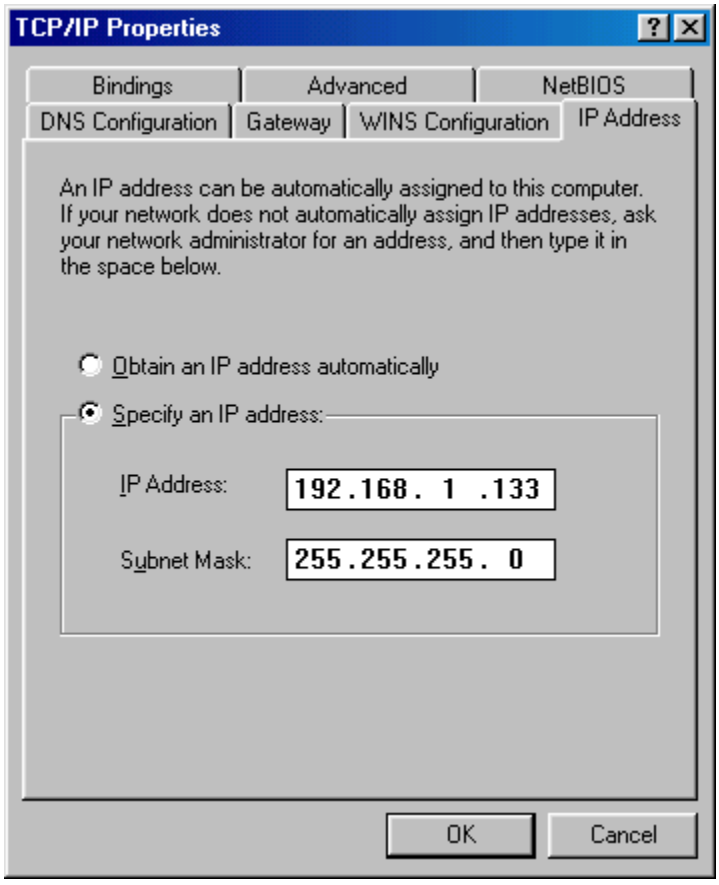
Chapter 3 Login via the Web Browser

This section describes how to manage the router via a Web browser from the remote end. You can use a web browser such as Microsoft Internet Explorer, or Netscape Navigator. It is best to set your display resolution to 1024 x 768. To change the resolution you can go to the Microsoft Windows control panel and click on the **Display** icon, and change the display settings. You will find the display settings there. A unique default user account is assigned with user name **root** and password **12345**. The user can change the default password later when logged in to the device.

3.1 IP Address

To log on to the device using a web browser, your workstation and the device should both be on the same network segment.

STEP 1: Enter the TCP/IP screen and change the IP address to the domain of 192.168.1.x/24. You should choose an IP address from 192.168.1.132-192.168.1.254 to avoid conflict with IP addresses reserved for the DHCP pool (192.168.1.3 to 192.168.1.131).



STEP 2: Click OK to submit the settings.

STEP 3: Start your Internet browser with the default IP address 192.168.1.1.

3.2 Login Procedure

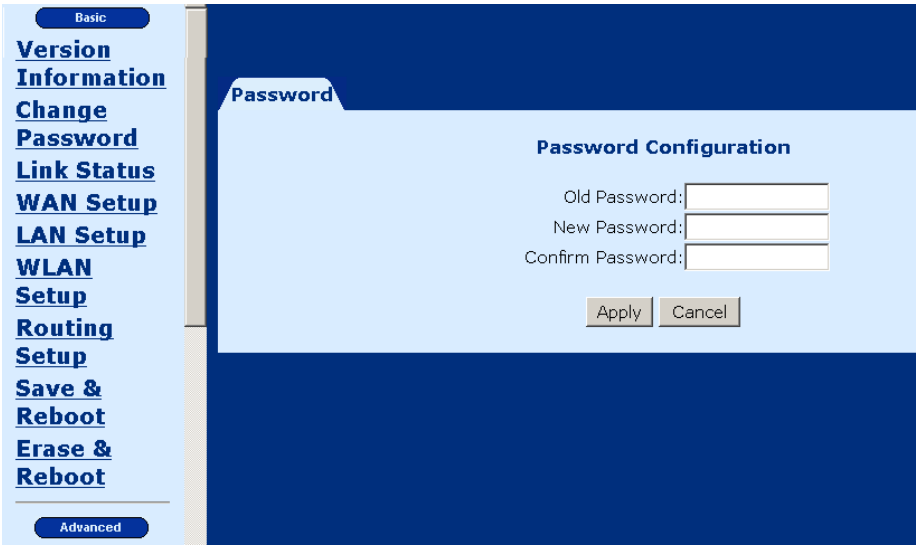
To log on to the system from the Web browser, follow the steps below:

STEP 1: Start your Internet browser.

STEP 2: Type the IP address for the router in the Web address field. For example, if the IP address is 192.168.1.1, type **http://192.168.1.1**

STEP 3: You will be prompted to enter your user name and password. Enter the user name and password; the user name is **root** and the default password is **12345**. The password is case-sensitive.

STEP 4: After successfully logging in, you will reach the main menu.

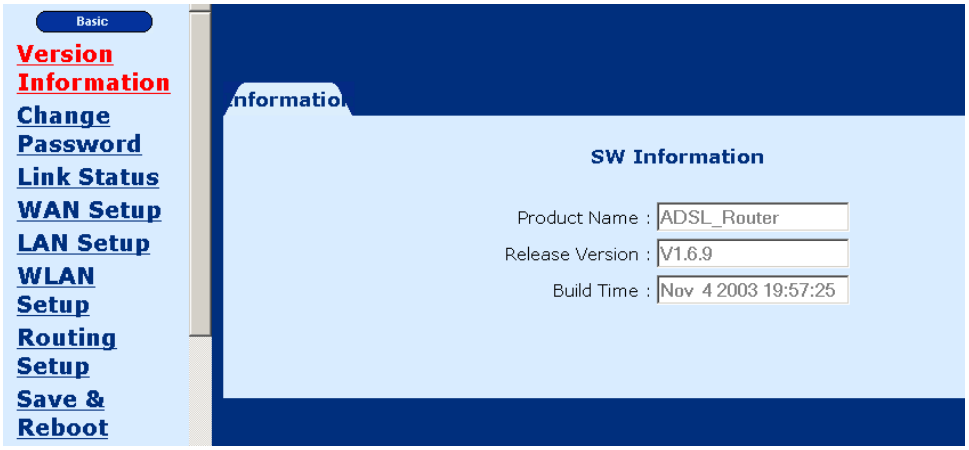


Chapter 4 Web Basic Configuration

From the **Basic** menu bar, you can verify the software version, change passwords, configure the WAN/LAN interfaces, set-up routing, save settings, reboot the device, and retrieve the factory default settings.

4.1 Version Information

To verify the software version of your router, from the **Basic** Menu bar, click on **Version Information**. The information will display as in the screenshot below.



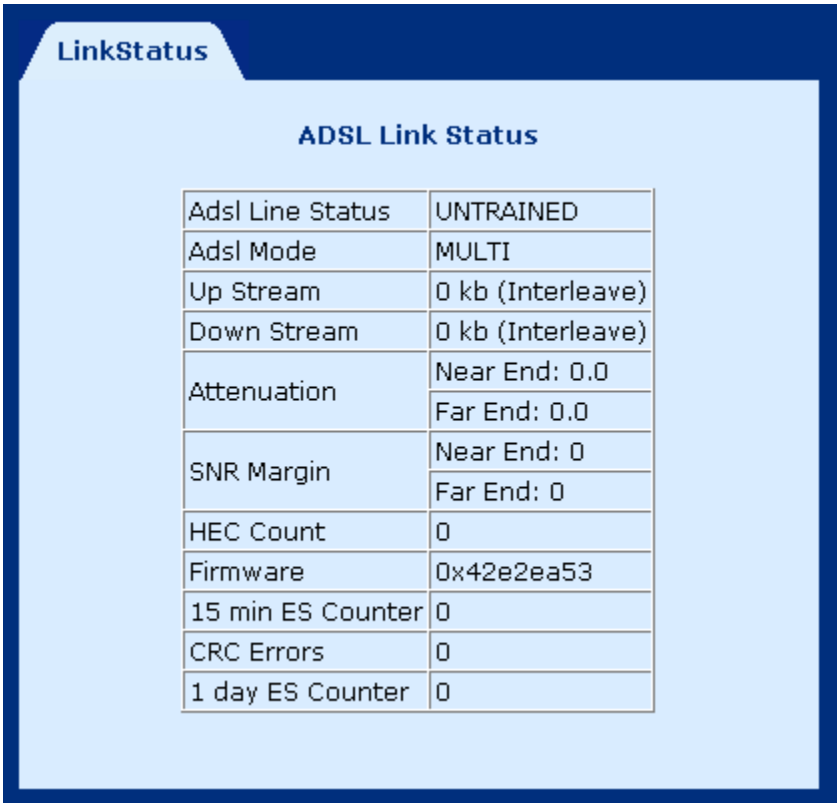
4.2 Change the Password

To modify the password, click **Change Password** from the menu bar. Type the old password and type the new password twice. Click **Apply** to submit the settings.

If you change the password, make sure you keep a record of it in a safe place, as you will require it next time you log-on.

4.3 ADSL Link Status

To view the ADSL link status, click **Link Status** from the tool bar. The page includes the following information:

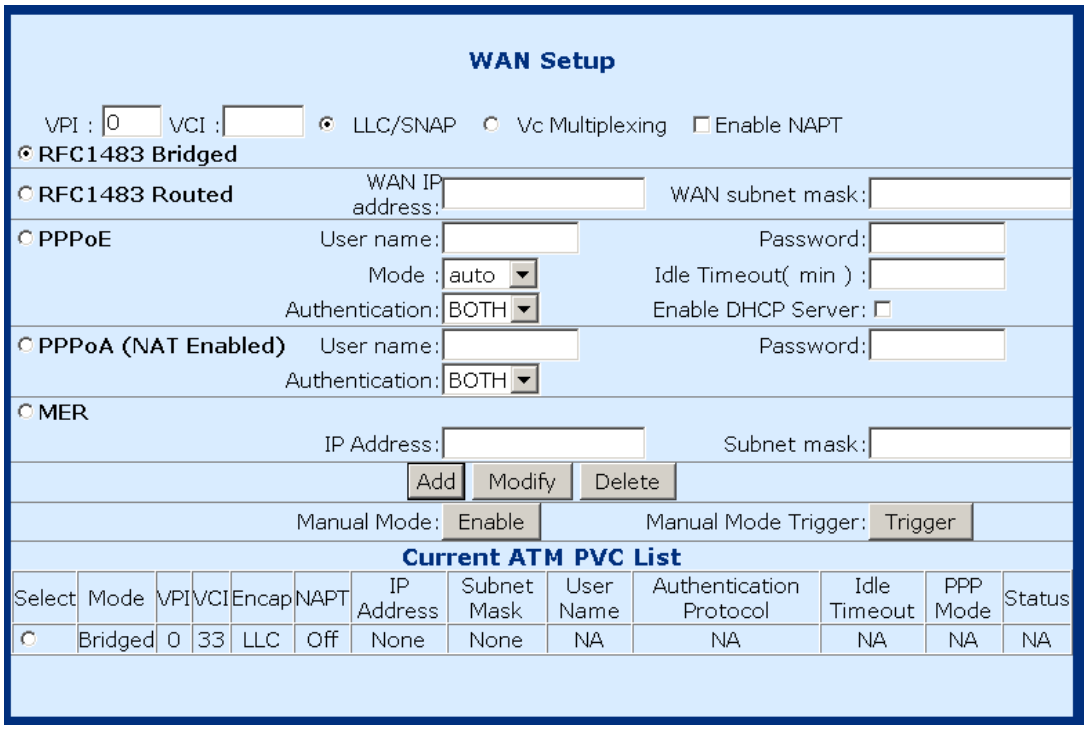


ADSL Line Status	Shows the current status of the ADSL line
ADSL Mode	Shows the ADSL standard that is currently configured. The standards are: ANSI, G.DMT, G.LITE, MULTI.
Upstream	Upstream data rate negotiated by DSL link (Kbit/s)
Downstream	Downstream data rate negotiated by DSL link (Kbit/s)
Attenuation	Current attenuation (dB) of both near end and far end.
SNR Margin	Current SNR margin (dB)
HEC	Number of ATM cells received with errors, since start of link.
Firmware	The version number of the firmware
15 min ES counter	Number of errored seconds for the current 15 minute period
CRC errors	Number of errors per second since training
1 day ES counter	Number of errored seconds for the current day

4.4 WAN Setup

Click WAN Setup from the tool bar and configure the WAN interface for these services: RFC1483 Bridged, RFC1483 Routed, PPPoE, PPPoA, and MER. The following are the common settings to set up these services.

- VPI and VCI
- LLC Encapsulation: With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
- VC Multiplexing: With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol.
- Enable NAPT: NAPT or Network Address Port Translation, enables the translation of private and public addresses. This feature is available for RFC 1483 Routed, PPPoE, PPPoA, and MER. It is enabled for PPPoE.



4.4.1 RFC 1483 Bridged

When using RFC 1483 style bridging, Ethernet frames are "bridged" over ATM Virtual Circuits. The Ethernet frames are encapsulated using either LLC Encapsulation or VC Multiplexing. With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit. With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol. Since the Ethernet packets are bridged, the router's only responsibility is to pass the Ethernet packets to and from the Internet Service Provider and the local network. The IP addresses of the local network are assigned by the ISP either statically or dynamically.

ADD AN ENTRY

To set up the RFC 1483 Bridged, configure the common fields on the top of the page and click the Add button to add the entry.

MODIFY AN ENTRY

To modify an entry, complete the following steps:

STEP 1: Select the entry from the **Current ATM PVC List,** at the bottom of the WAN Setup page. The current values of the selected entry will display in the upper section of the page.

STEP 2: Change the parameters.

STEP 3: Click **Modify**.

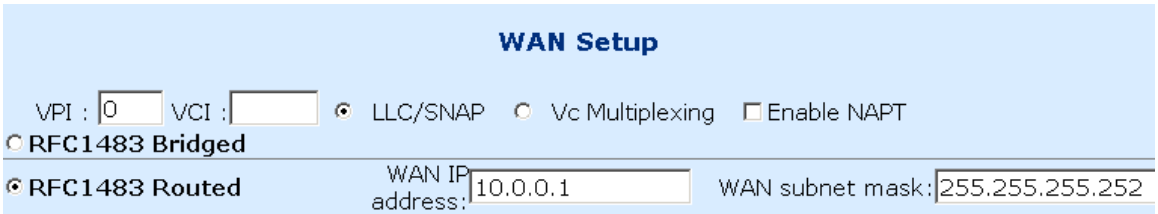
DELETE AN ENTRY

To delete an entry, Select it from the **Current ATM PVC List,** at the bottom of the WAN Setup page, and click the **Delete** button.

4.4.2 RFC 1483 Routed

ADD AN ENTRY

To set up the RFC 1483 Routed, configure the common settings on the top of the page, click RFC 1483 Routed and configure the specific settings (WAN IP address and WAN subnet mask). Click the Add button to add the entry.



MODIFY AN ENTRY

To modify an entry, complete the following steps:

STEP 1: Select the entry from the **Current ATM PVC List,** at the bottom of the WAN Setup page. The current values of the selected entry will display in the upper section of the page.

STEP 2: Change the parameters.

STEP 3: Click **Modify**.

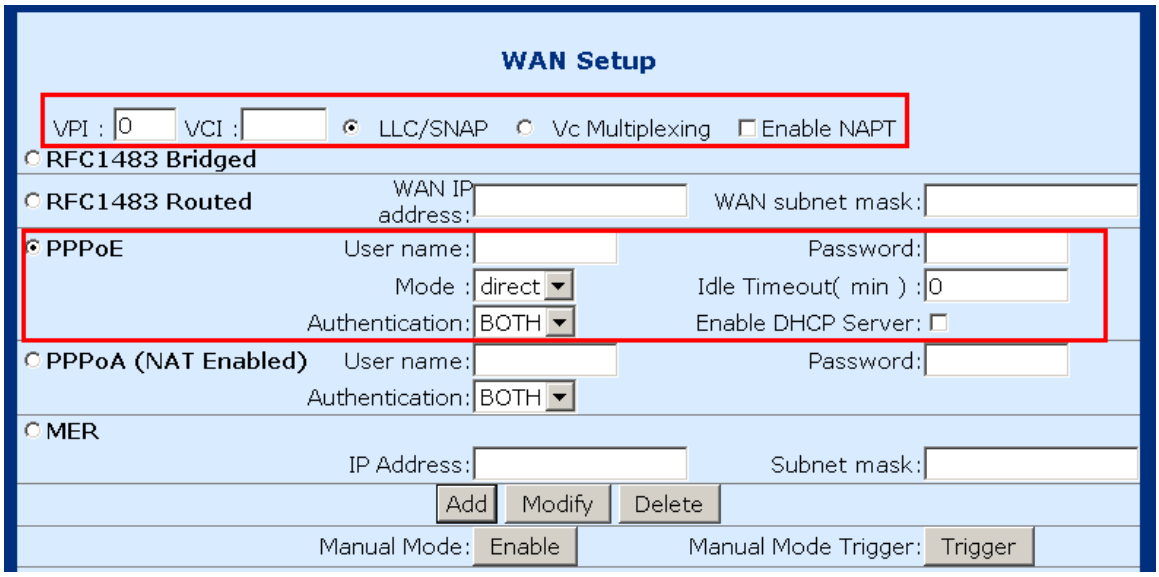
DELETE AN ENTRY

To delete an entry, Select it from the **Current ATM PVC List,** at the bottom of the WAN Setup page, and click the **Delete** button.

4.4.3 PPPoE

PPPoE provides service providers similar billing and access control as present in dial-up services. In addition, with direct support to Ethernet it provides a low cost solution to supporting multiple hosts at the customer premises. PPPoE provides session authentication using Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). Session accounting is possible and conservation of bandwidth can be done by closing down unused sessions. By utilizing PPP, link and network parameters are easily negotiated between the IAD/Router and the ISP.

When using PPPoE, the system is assigned an IP address from the Internet Service Provider as part of establishing the network connection. The system can be configured as a DHCP server for its LAN and NAT can be used to translate private addresses to public addresses. In this way, computers in the LAN do not have to have their own public IP addresses.



ADD AN ENTRY

To set up PPPoE, click PPPoE, configure the common fields on the top of the page, as well as the following fields. At the bottom of the screen, click the **Add** button to add the entry. In addition, If the PPPoE mode is set to **auto,** clicking the MANUAL MODE **Enable** button will effectively disable auto mode, and require the user to reconnect a terminated PPPoE session by clicking the MANUAL MODE **Trigger** button. Subsequently, to return to Auto-mode, click on the MANUAL MODE **Disable** button, which will appear in place of the MANUAL MODE **Enable** button.

- **User name/Password:** used for the remote customers to login during dialup.
- **Mode:** Direct and Auto. If the mode is set to AUTO, the PPPoE negotiation automatically starts when the system identifies any traffic required to be transferred on the link. When DIRECT is selected the PPPoE negotiation is started manually using the "pppoestart" command. The default is DIRECT.

- **Idle Timeout:** defines the period of idle time (minutes) after which the PPPoE link will be terminated.
- **Authentication:** Defines the authentication code: PAP, CHAP or BOTH. If the authentication code is set to BOTH, the router will follow the authentication settings (PAP, CHAP) of the remote DSLAM.
- **Enable DHCP Server:** enables the DHCP server. This field is automatically checked when PPPoE is selected. Deselect the field to disable the DHCP server. The DHCP server dynamically allocates network addresses and delivers configuration parameters to hosts.

MODIFY AN ENTRY

To modify an entry, complete the following steps:

STEP 1: Select the entry from the **Current ATM PVC List,** at the bottom of the WAN Setup page. The current values of the selected entry will display in the upper section of the page.

STEP 2: Change the parameters.

STEP 3: Click **Modify**.

DELETE AN ENTRY

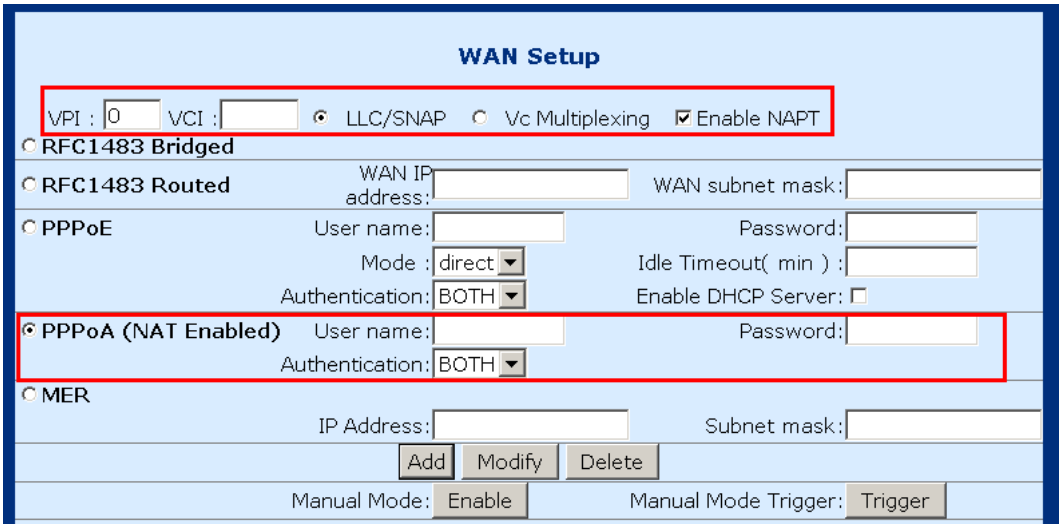
To delete an entry, Select it from the **Current ATM PVC List,** at the bottom of the WAN Setup page, and click the **Delete** button.

4.4.4 PPPoA

ADD AN ENTRY

To set up PPPoA, click PPPoA, configure the common fields and the following fields. Click the Add button to add the entry.

- **User name** and **Password:** used for remote customers to login upon dialup. PPPoA is manually activated by entering startup commands from the page: Advanced>Configure PPPoA.
- **Authentication:** Defines the authentication code: PAP, CHAP or BOTH. If the authentication code is set to BOTH, the router will follow the authentication settings (PAP, CHAP) of the remote DSLAM.



MODIFY AN ENTRY

To modify an entry, complete the following steps:

STEP 1: Select the entry from the **Current ATM PVC List,** at the bottom of the WAN Setup page. The current values of the selected entry will display in the upper section of the page.

STEP 2: Change the parameters.

STEP 3: Click **Modify**.

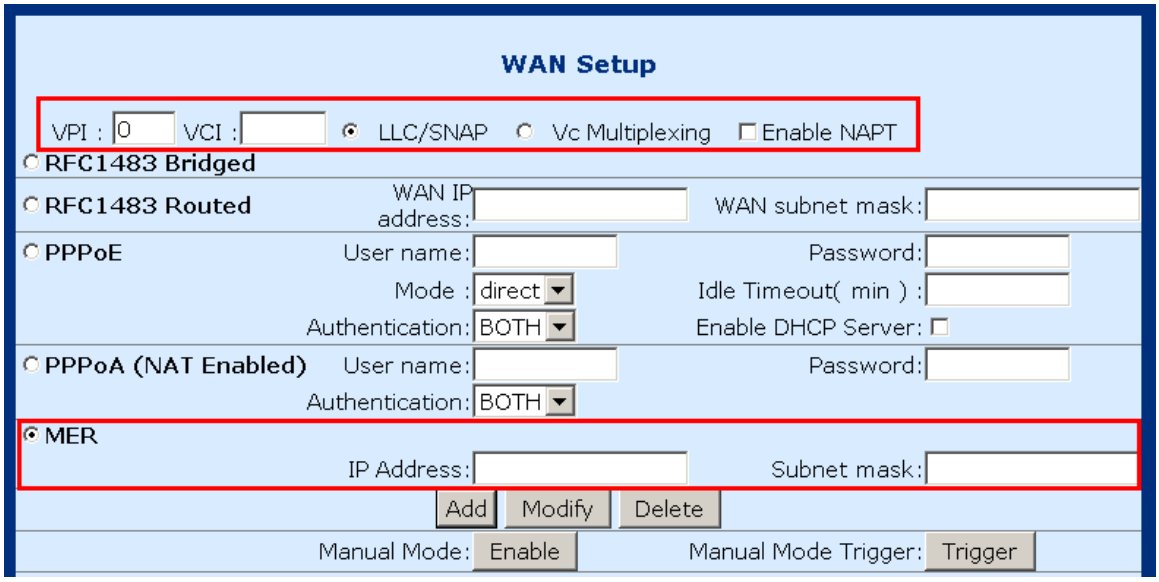
DELETE AN ENTRY

To delete an entry, Select it from the **Current ATM PVC List,** at the bottom of the WAN Setup page, and click the **Delete** button.

4.4.5 MER

MAC Encapsulation Routing (MER) enables the ATU-R to route IP addresses on the RFC1483 bridged link. NAPT function is supported to allow multiple private IP addresses on the LAN to share a public IP address.

To set up the MER service, configure the common fields, and then enter the IP Address and Subnet Mask under the MER section of the screen. Click the Add button to add the entry.



To modify an entry, complete the following steps:

STEP 1: Select the entry from the **Current ATM PVC List,** at the bottom of the WAN Setup page. The current values of the selected entry will display in the upper section of the page.

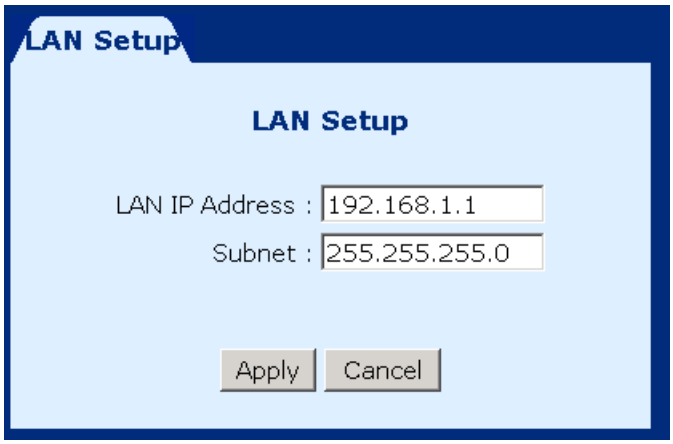
STEP 2: Change the parameters.

STEP 3: Click **Modify**.

To delete an entry, Select it from the **Current ATM PVC List,** at the bottom of the WAN Setup page, and click the **Delete** button.

4.5 LAN IP Address

The default LAN IP address is 192.168.1.1. Click **LAN Setup** from the menu bar to configure the LAN IP address. Type the **IP address** and **subnet mask**. Click **Apply** to submit the settings. When the new IP address is applied, the Web configuration will be interrupted. Use the new IP address to login.



4.6 WLAN Configuration

Parameters that specifically deal with the wireless functions of your router can be accessed from **WLAN Setup** on the Basic menu bar. The menu is subdivided into several menus: WLAN Basic, WLAN Advanced, WLAN WEP, WLAN Filter, and WLAN Radio. Each of these menus will be covered below.

To enable the WLAN radio wave function, click the **Radio** tab. Tick **ON** in the Radio Status field, and click the Apply button to submit the setting. To disable it, tick **OFF** and click the **Apply** button.

4.6.1 WLAN Basic Parameters

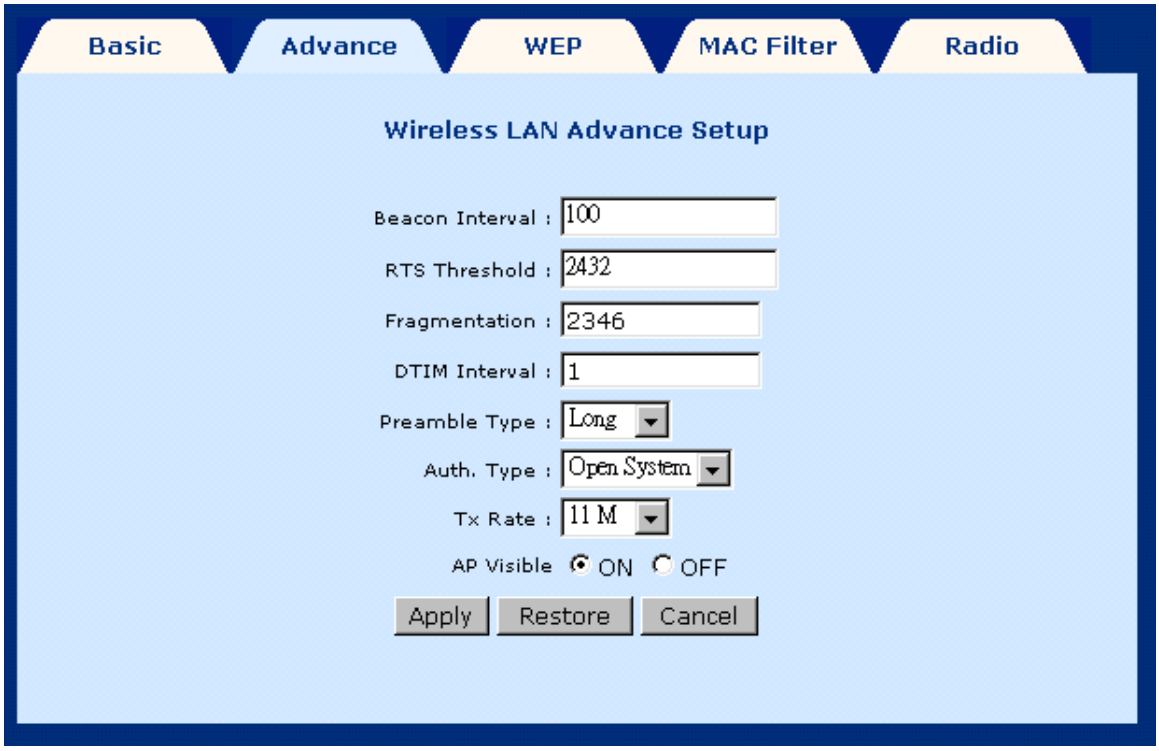
To access the WLAN Basic parameters click on the **WLAN Basic** tab on the **WLAN Settings** screen. The WLAN Basic Parameters menu includes the parameters listed below. After changing any parameters, click on the **Apply** button to update the parameters, or click on the **Restore** button to retain the original settings.

IP Address	Enter the **IP address** for the WLAN interface
Subnet Mask	Enter a **subnet mask** for the WLAN interface
SSID	The SSID should match with your client adapters. The SSID (Service Set ID) allows you to uniquely identify your Access Point in the radio environment.
Channel	The channel should match with client adapters. The Direct Sequence Spread Spectrum (DSSS) channel number is an identifier for the frequency on which your WLAN connectivity is enabled in the WLAN network. Although the configurable DSSS channel number range is from 1 up to 14, restrictions apply depending on the country where the Wireless ADSL Router is used- **FCC**: channels 1 to 11; **ETSI**: channels 1 to 13.

4.6.2 WLAN Advanced Functions

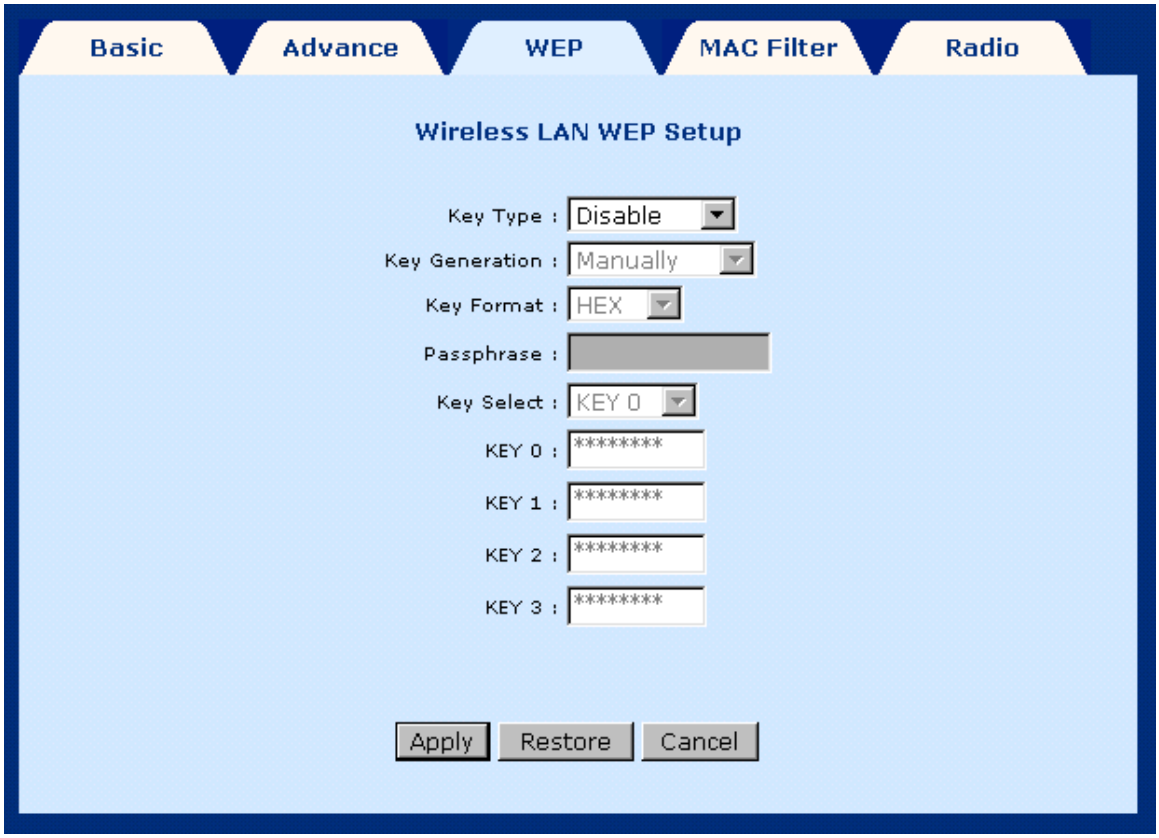
To access the WLAN Advanced parameters click on the **WLAN Advance** tab on the **WLAN Settings** screen. The WLAN Advanced Parameters menu includes the parameters listed below. After changing any parameters, click on the **Apply** button to update the parameters, or click on the **Restore** button to retain the original settings.

Beacon Interval	Specify the Beacon Interval value. Enter a value between 1 and 1000. The value represents the time in nano-seconds that Beacon packets are sent by an Access Point to synchronize a wireless network.
RTS Threshold	This value should normally remain at its default setting of 2,432. Should you encounter inconsistent data flow, only minor modifications are recommended. The value must match with remote clients.
Fragmentation	This field is used to specify the fragmentation threshold. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should normally remain at its default setting of 2,346. This value must match client adapters.
DTIM Interval	Enter a value between 1 and 65535. This number represents the time between sending delivery traffic identification messages (DTIMs) used for power saving and multicast/broadcast delivery. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages.
Preamble Type	**long**, **short** . Should match client adapters. Short enables faster throughput, but it can only be used when all network elements comply with the IEEE 802.11b standard.
Auth. Type	**Open System** [no security during authentication process], **Shared Key** [using WEP encryption during authentication process].
Tx Rates	The transfer rate of the router should be equal to or greater than the clients, the options are: 1-2-5-11 (Mbps).
AP Visible	When this is **ON** the AP can be detected by wireless clients, when it is set to **Off,** the AP can not be detected by wireless clients.


Basic
Advance
WEP
MAC Filter
Radio
Wireless LAN Advance Setup
Beacon Interval : 100
RTS Threshold : 2432
Fragmentation : 2346
DTIM Interval : 1
Preamble Type : Long
Auth. Type : Open System
Tx Rate : 11 M
AP Visible ON OFF
Apply
Restore
Cancel

4.6.3 WLAN WEP Parameters:

To access the WLAN WEP parameters click on the **WLAN WEP** tab on the **WLAN Settings** screen. This screen is used to set-up WEP security. WEP security uses an encryption keyword on all transmitted and received data. The parameters are described below. After changing any parameters, click on the **Apply** button to update the parameters, or click on the **Restore** button to retain the original settings.



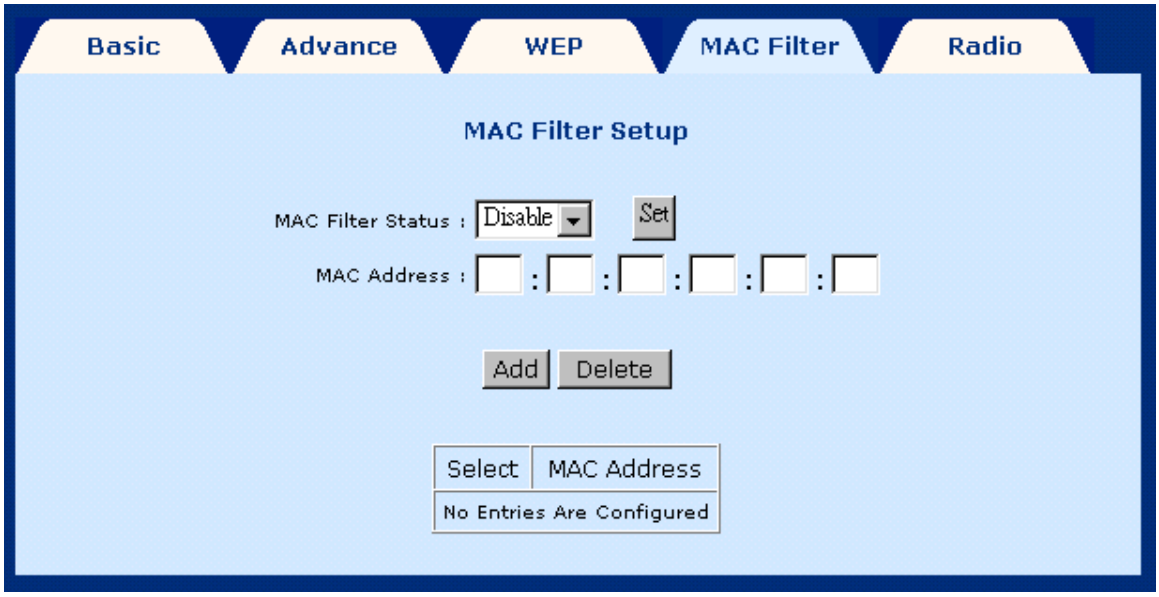
Key Type	**Disabled, 64 bits, 128 bits**. This parameter determines the level of security. Disabled means no security, 128 bits provides the highest security. This parameter must match with the remote-clients.
Key Generation	Select **Passphrase** to enable automatic key generation, or **Manually** to manually enter each key. The manual key generation provides two forms, Hex decimal and ASCII string. If Manually is chosen, also configure the fields below.
Passphrase	Enter a Passphrase if you wish clients to require a Passphrase to connect with the access point.
Key Format	There are two key formats, Hex decimal, and ASCII string. Choose one of the formats for manual key generation. When the key type is 64 bits, the key space in Hex format is 10 bytes, and in ASCII string is 5 bytes. When the key type is 128 bits, the key space in Hex format is 26 bytes, and in ASCII string is 13 bytes.
Key Select	If you are using a manual key generation, select a Key number from 0~3, and type the access password in the chosen field.
Key 0~3	The access password could be hexadecimal format or ASCII string code, which depends on the above Key Format you have chosen. You can configure all the four key passwords (0-3), but only the chosen key will take effect. The password will be required to be set on any wireless client that you wish to connect with your access point.

4.6.4 Mac Filter

This screen allows wireless access to be restricted or enabled based on a MAC address. Enter the following parameters.

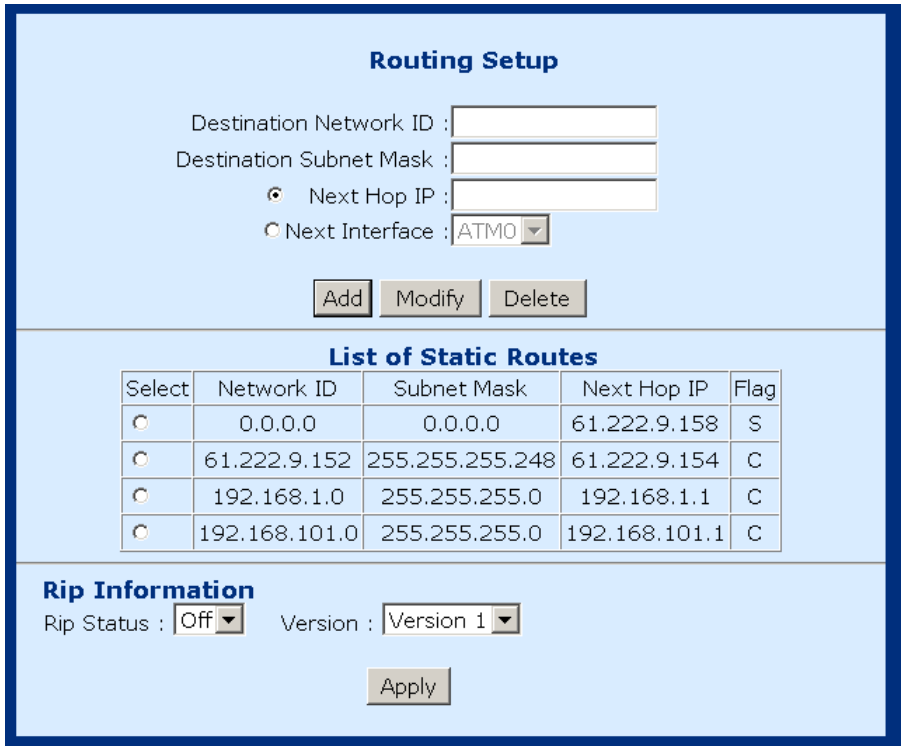
- MAC filter status: **Disable** - de-activates MAC filtering, **allow** – permits access for the specified MAC address, **deny –**reject access of the specified MAC address. Click the **SET** button to submit the setting. (the status will impact all MAC Addresses that have been entered as filters)
- MAC address: Enter the MAC address of the access point, and then click the **Add** button.

To **delete an entry** select the entry at the bottom of the screen and then click the **Delete** button, located in the middle of the screen.



4.7 Routing

Click **Routing Setup** from the menu bar to configure the routing functions. Routing functions includes RIP and static routing.



4.7.1 Enable RIP

To enable RIP, complete the following steps:

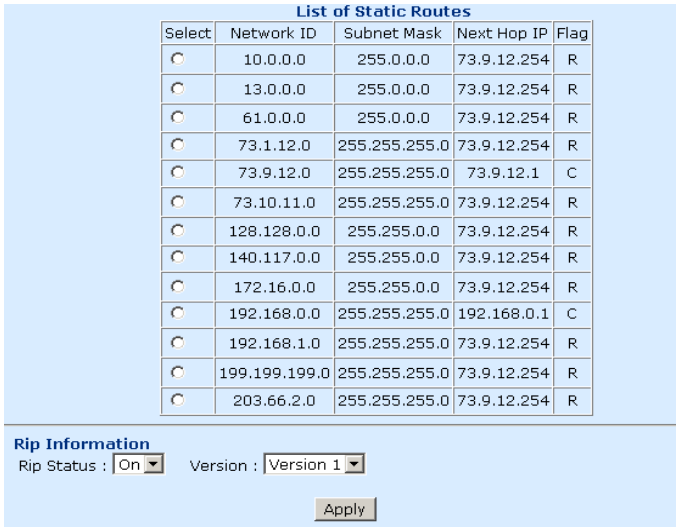
STEP 1: Click **Routing Setup** from the menu bar.

STEP 2: Select **On** in the Rip Status field.

STEP 3: Select a RIP Version (Version 1 or Version 2) from the Version field.

STEP 4: Click **Apply** to submit the settings.

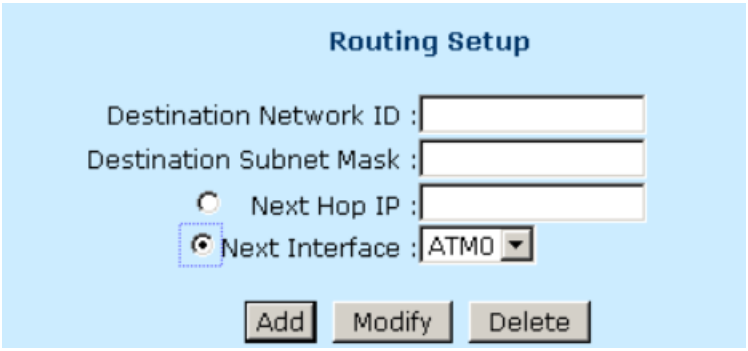
STEP 5: After submitting the new Rip settings, the List of Static Routes will be updated to reflect this change. A screen similar to the following will be displayed:



Flag: R = RIP Route, S = Static Route, C = Connect Route

4.7.2 Static route configuration

The Routes Configuration field allows you to add, modify, and delete a static route. Type the Destination Network ID, subnet mask, and next hop IP and click a button below to perform the requested function.



Add:
To add a static route complete the following steps:

STEP 1: Click **Routing Setup** from the menu bar.

STEP 2: Enter parameters for **Destination Network ID**, **Subnet Mask**, **Next Hop IP,** and **Next Interface** (note you must select between entering a Next Hop IP or Next interface).

STEP 3: Click the **ADD** button.

Modify:
To modify a static route complete the following steps:

STEP 1: Select the entry you wish to modify from the List of Static Routes.

STEP 2: Change the parameters.

STEP 3: Click the **Modify** button.

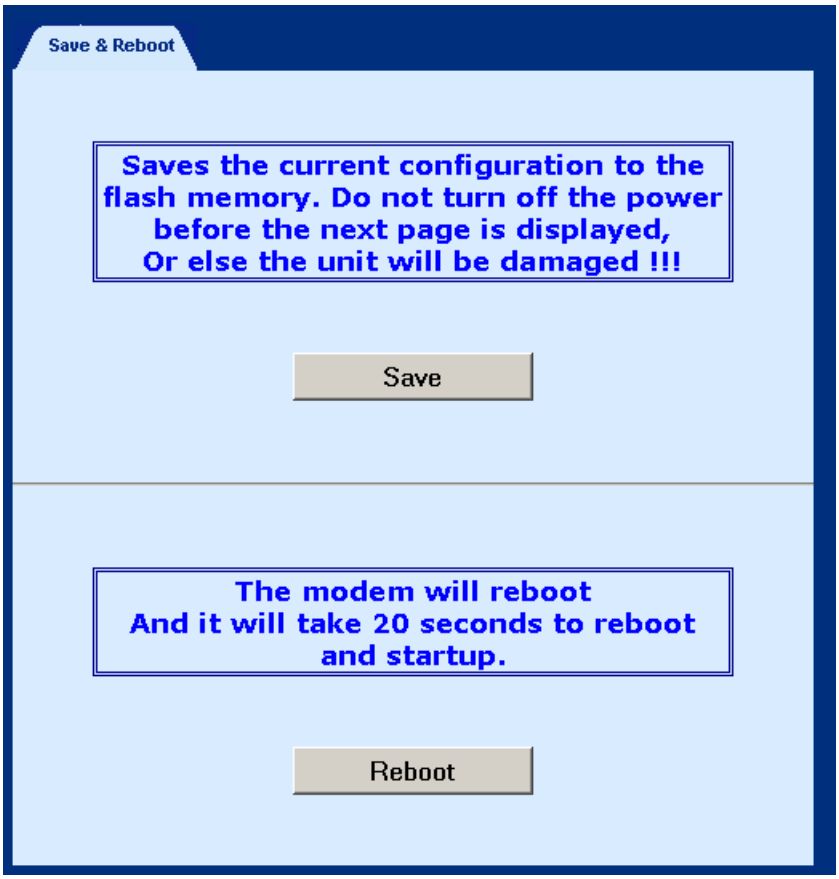
Delete:
STEP 1: Select the entry you wish to **delete** from the List of Static Routes

STEP 2: Change the parameters.

STEP 3: Click the **Delete** button.

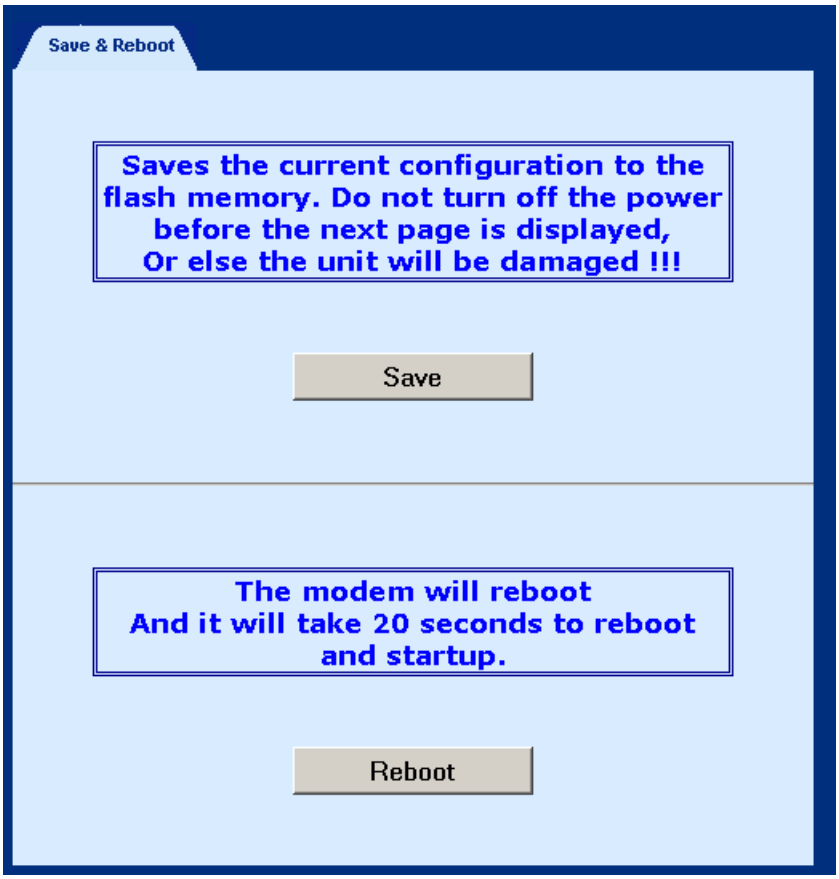
4.8 Save

To save the settings to Flash, click **Save & Reboot** from the menu bar. In the main pane, click **Save**.



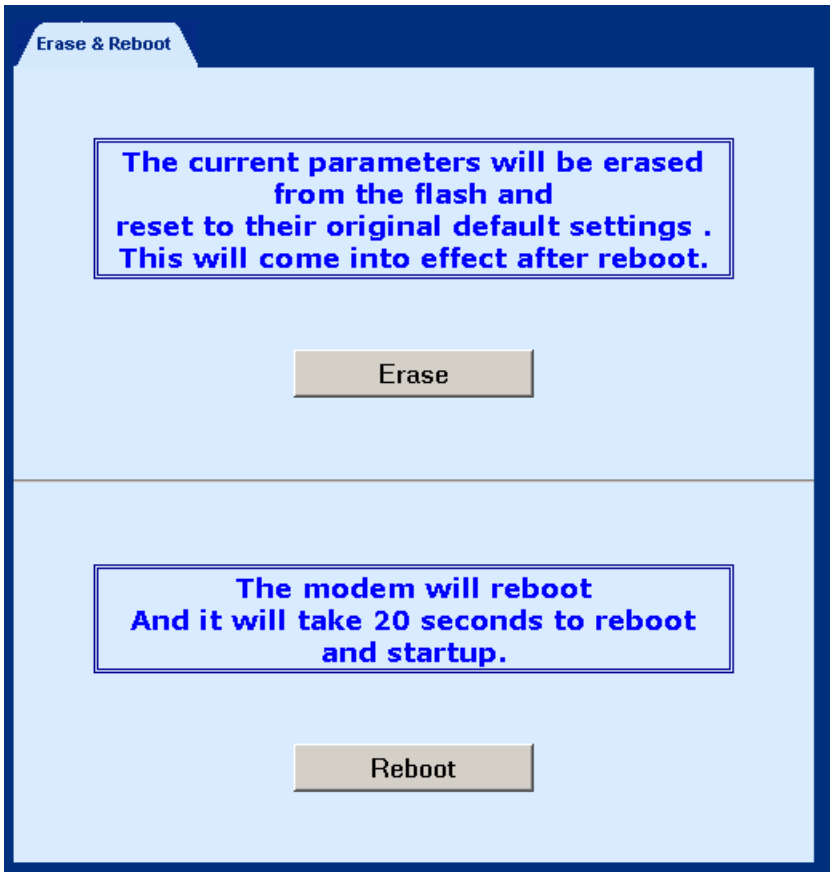
4.9 Reboot

To reboot the router, click **Save & Reboot** from the menu bar. In the main pane, click on **Reboot**.



4.10 Retrieve default settings

To retrieve the default settings, click **Erase & Reboot** from the menu bar. In the main pane, click **Erase**.



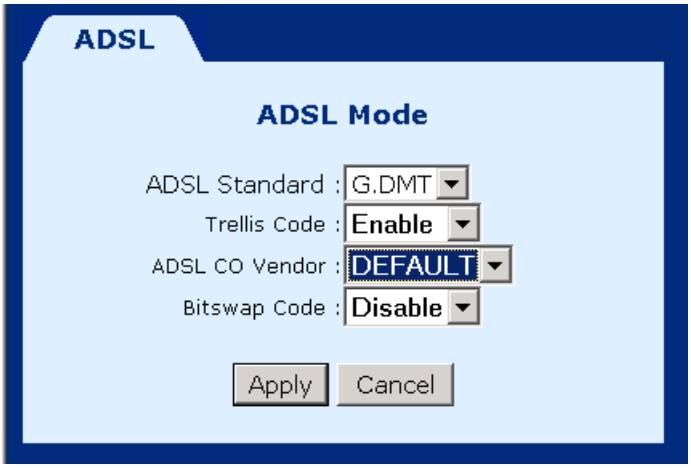
Chapter 5 WEB Advanced Configuration

5.1 ADSL Mode

Click the **ADSL Mode** button from the Advanced menu bar.

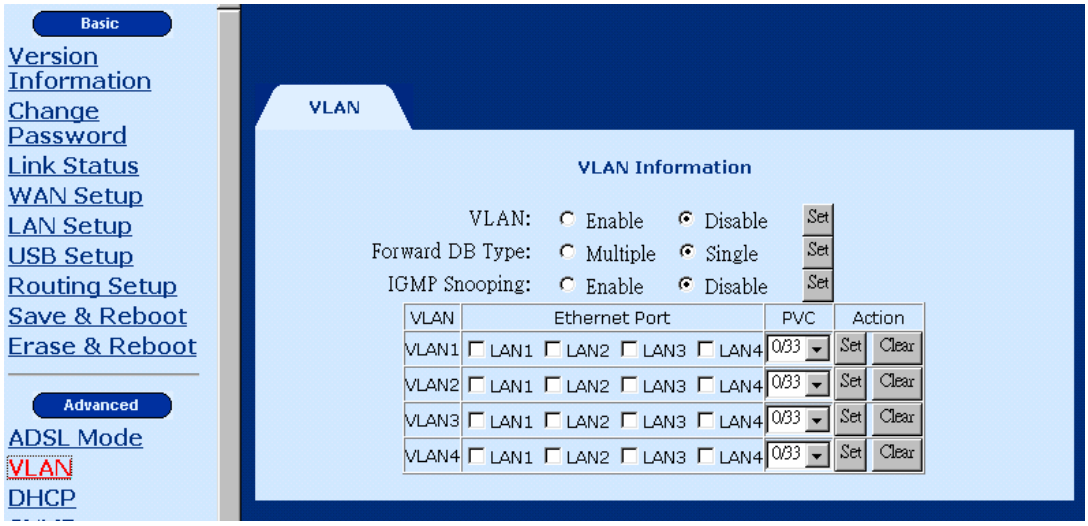
- There are four ADSL modes: ANSI, G.DMT, G.LITE, MULTI. The default ADSL mode is MULTI. MULTI mode enables the device to auto-adjust its mode to match the remote CO DSLAM. You can specify an ADSL mode on this page, and click the Apply button to submit the settings.
- Trellis Code: Enable, Disable
- ADSL CO Vendor: Default, Broadcom, GsV, Infineon and TI.
- This field selects the CO chipset vendor. Choose the applicable CO chipset vendor for the CO DSLAM chipset; if the vendor is not Broadcom, GsV, Infineon or TI, select the Default option.
- Bitswap Code: Enable, Disable

After changing the parameters, click the **Apply** button to submit the settings.



5.2 VLAN

To configure the VLAN function, click **VLAN** from the Advanced menu bar. The following parameters are displayed:



Parameters:

VLAN: Select **enable** or **disable** to activate/deactivate the VLAN function.

Forward DB Type: Used to configure the forwarding database learning type. There are two types of learning for the FDB: Multi and Single.

Multiple: the learned entries will be distributed to five databases, (VLAN 1~4 and non-VLAN)

Single: the learned entries will be collected into a single database.

IGMP Snooping: Select **enable** or **disable** to activate/deactivate IGMP snooping.

VLAN: Check the VLAN interface to enable it or uncheck it to disable it.

Ethernet Port: Select the LAN interfaces you wish to attach to each VLAN. **Note that each LAN interface can only be attached to one VLAN.**

PVC: Select the VCI/VPI value for the VLAN, you can only select from values that have been configured as Bridge mode on the WAN interface (refer to section 4.4, WAN Setup).

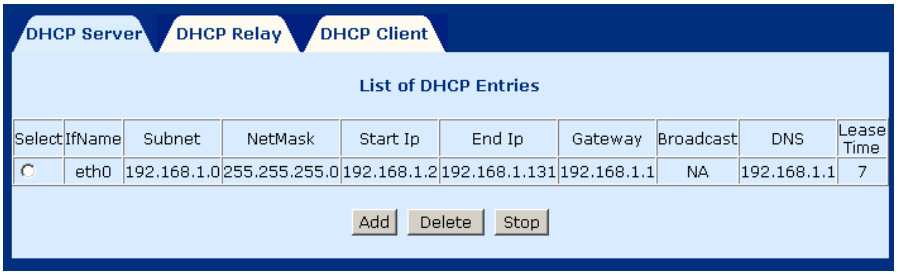
Action: Click the **Set** button to apply the settings, or click the **Clear** button to delete a VLAN group.

5.3 DHCP

The Dynamic Host Configuration Protocol (DHCP) provides a centralized approach to allocating IP addresses. It allows IP addresses to be dynamically assigned on an as needed basis, from a pool of addresses. The DHCP server is enabled by factory default with the default IP address of the eth0 to be 192.168.1.1/24.

5.3.1 Enable DHCP Server

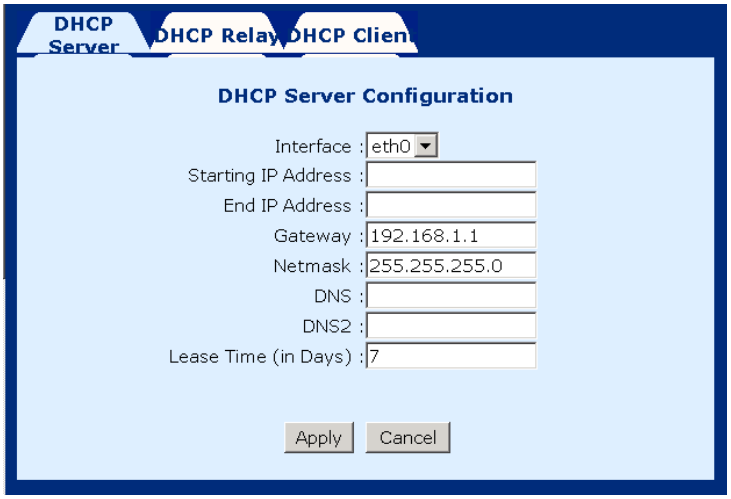
STEP 1: Click **DHCP** from the menu bar. There is a default DHCP entry on the screen. The default settings are as follows.



STEP 2: To enable the DHCP entry, chose the entry and click the Start button. A Stop button will display on the screen as follows.

5.3.2 Add DHCP Server

To add an entry, click the Add button, and fill out the following parameters. Click **Apply** to submit the settings.



- **Interface: eth0/wlan0.** This configures the interface that will provide the DHCP function. By factory default, the entry for interface **eth0** is defined with the gateway address 192.168.1.1, and subnet mask 255.255.255.0. The default entry for interface **wlan0** is defined with the gateway address 192.168.101.1, and subnet mask 255.255.255.0.
- **Starting IP Address:** The first IP address of the address pool in the DHCP server. Note the IP address should be in the same subnet as the router's LAN IP address.
- **End IP Address:** The last IP address of the address pool in the DHCP server. Note the IP address should be in the same subnet as the router's LAN IP address.
- **Gateway:** The gateway IP address
- **Netmask:** The subnet mask of the IP network
- **DNS:** The IP address of the Domain Name Server
- **DNS2:** The second IP address of the Domain Name Server
- **Lease Time (in Days):** Upon login, the remote workstation will obtain an IP address. This field defines the period of time that the workstation can use this IP address to access the Internet.

5.3.3 Disable DHCP Server

To **stop** a DHCP Server, complete the following steps:

STEP 1: Click **DHCP** from the menu bar.

STEP 2: Choose a DHCP entry, and click **Stop**.

5.3.4 Delete DHCP Server

To **delete** a DHCP Server, complete the following steps:

STEP 1: Click **DHCP** from the menu bar.

STEP 2: Choose a DHCP entry, and click **Delete**.

5.4 DHCP Relay

The DHCP packet format is based on a BootP packet. As a result, DHCP uses the BootP relay agent to forward DHCP packets. This scheme provides interoperability between existing BootP clients and DHCP servers. The BootP relay agent uses the same criteria and methods for forwarding both DHCP and BootP packets. The DHCP Relay is disabled by default.

5.4.1 Enable the DHCP Relay

To enable the BOOTP/DHCP Relay complete the following steps:

STEP 1: Access the BOOTP/DHCP Relay screen by clicking on **DHCP** on the Advanced Menu, and then click the **DHCP Relay** tab.

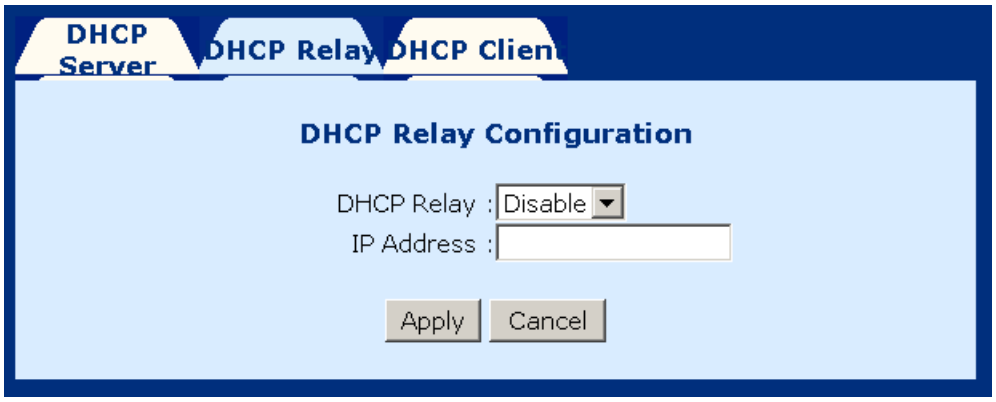
STEP 2: In the DHCP Relay field, select **Enable**, and enter the IP Address you want to receive BOOT REQUEST or DHCP packets from clients.

STEP 3: Click on the **Apply** button.

5.4.2 Disable the BOOTP/DHCP Relay

To disable the BOOTP/DHCP Relay complete the following steps:

STEP 1: Access the BOOTP/DHCP Relay screen by clicking on **DHCP** on the Advanced Menu, and then click the **BOOTP/DHCP Relay** tab.



STEP 2: In the DHCP Relay field, select **Disable**, and enter the IP Address you want to receive BOOT REQUEST or DHCP packets from clients.

STEP 3: Click on the Apply button.

5.5 DHCP Client

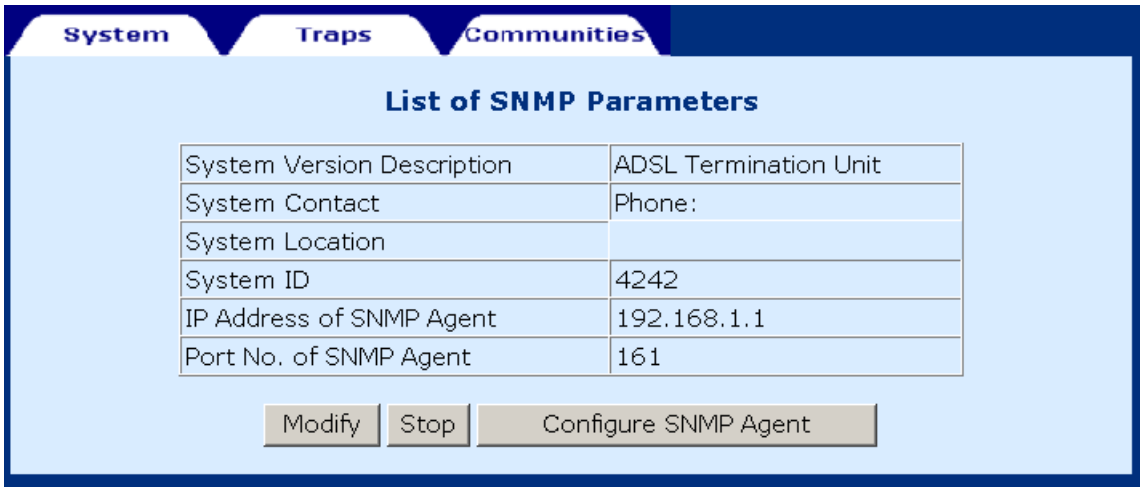
Note: Before starting the DHCP Client function, the user needs to make sure that the DHCP Server is reachable; if the ADSL Router fails to get the IP Address from DHCP Server, the ADSL Router needs to be rebooted.

The router can also be configured as a DHCP client. In this case, the router can broadcast a request to the DHCP Host, for an IP address, subnet mask, and domain name, to be assigned. To set the router to DHCP client mode, select the **Interface** to connect to the DHCP Host and then click the **Start** button.

The Stop button can be used to stop the router form operating in DHCP client mode, and the restart button can be used to get the router to re-broadcast a request to the DHCP Host, for an IP address, subnet mask, and domain name, to be assigned.

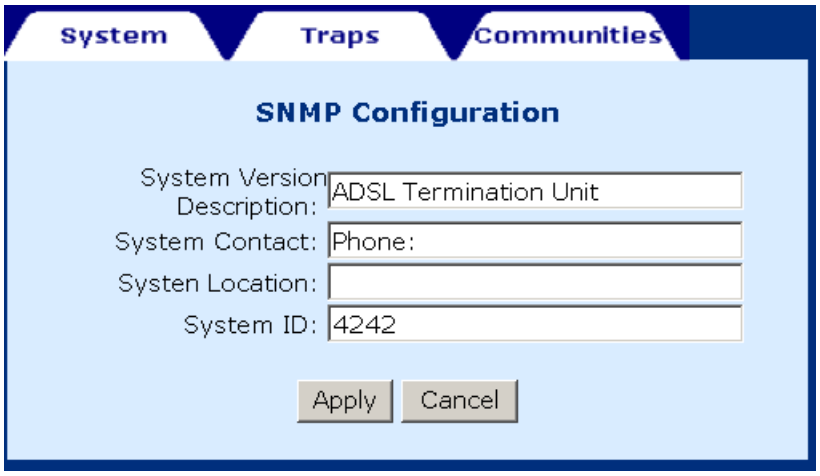
5.6 SNMP

SNMP is a software entity that responds to information and action request messages sent by a network management station. The messages exchanged enable you to access and manage objects in an active or inactive (stored) MIB on a particular router. To configure the SNMP parameters, click the **SNMP** button on the **Advanced** menu bar. The window displays the SNMP parameters.

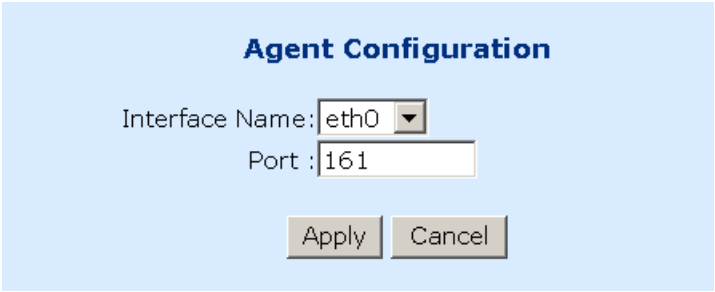


5.6.1 Modifying SNMP Parameters

To modify the SNMP parameters, click the Modify button at the bottom of the screen. Click Apply to submit the settings.

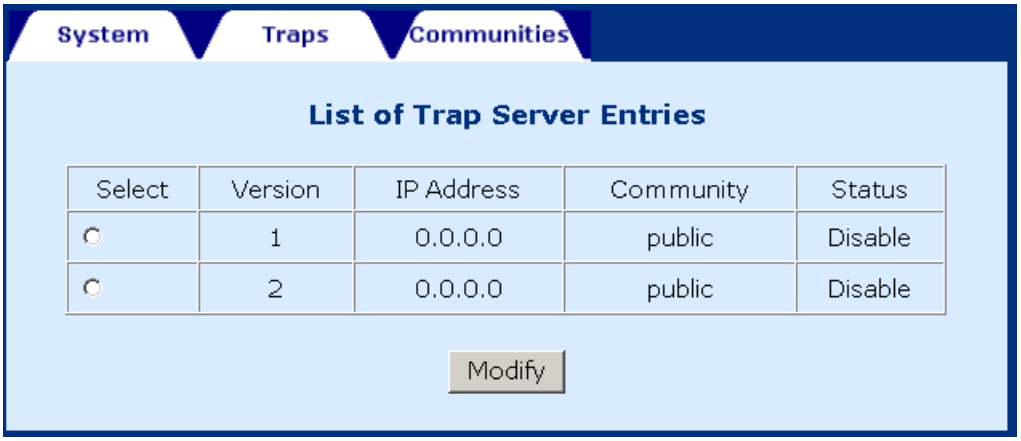


To configure the SNMP agent, click the Configure SNMP Agent button. After filling out the fields, click Apply to submit the settings.



5.6.2 Modifying Traps

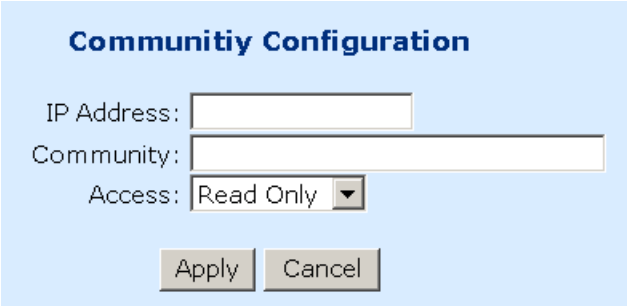
Click the Traps tab to configure the traps. After filling out the parameters, click Submit to apply the settings.



5.6.3 Modifying Communities

Click the Communities tab to display the community entry. After filling out the parameters, click Submit to apply the settings.

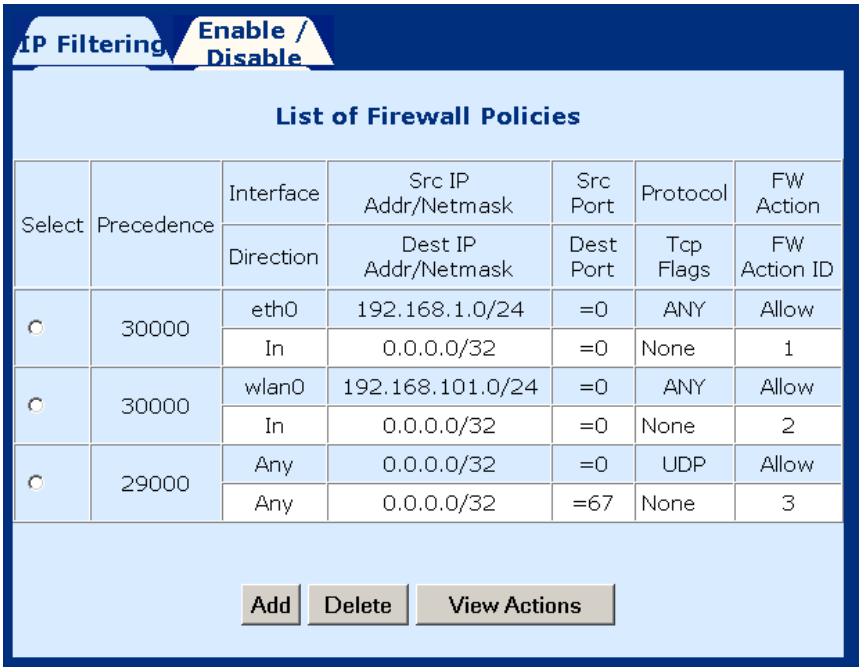
There is no community set up by factory default. To add or modify an entry, click the Configure Community button. To delete an entry, tick the entry and click the Delete button. The following screen displays after clicking the **Configure Community** button. Enter the parameters and ten click the **Apply** button.



5.7 Firewall

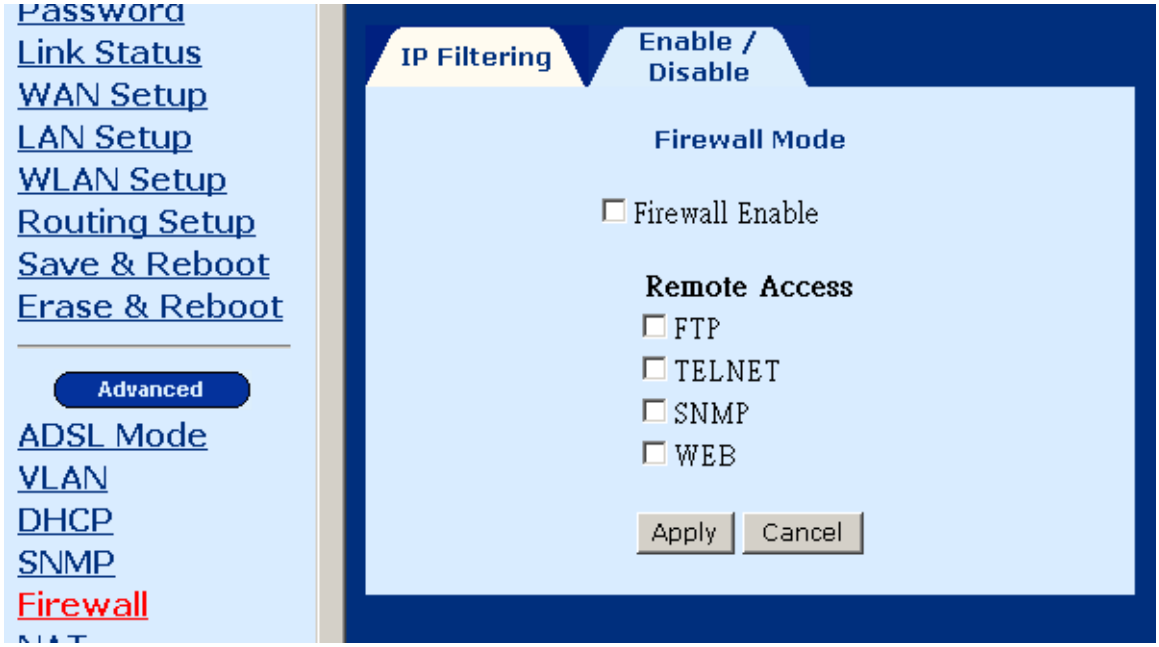
The ADSL router provides packet filtering and stateful packet inspection. It has denial of service protection against attacks such as ICMP Flood, Ping of Death, IP spoofing, Port Scans, Land Attack, Tear Drop Attack, IP Source Route and WinNuke Attack.

To access the firewall functions, select **Firewall** from the advanced menu. The screen will display as below, showing a list of the currently configured filter entries. From the Firewall page, you can turn the Firewall Mode **On** or **Off**, view Filter Parameters, **add** a filter, **delete** a filter, or **View Action** for filtered packets. All the firewall settings will take effect immediately, including enabling/disabling the firewall and addition/removal of firewall entries. Each of theses actions will be discussed below.



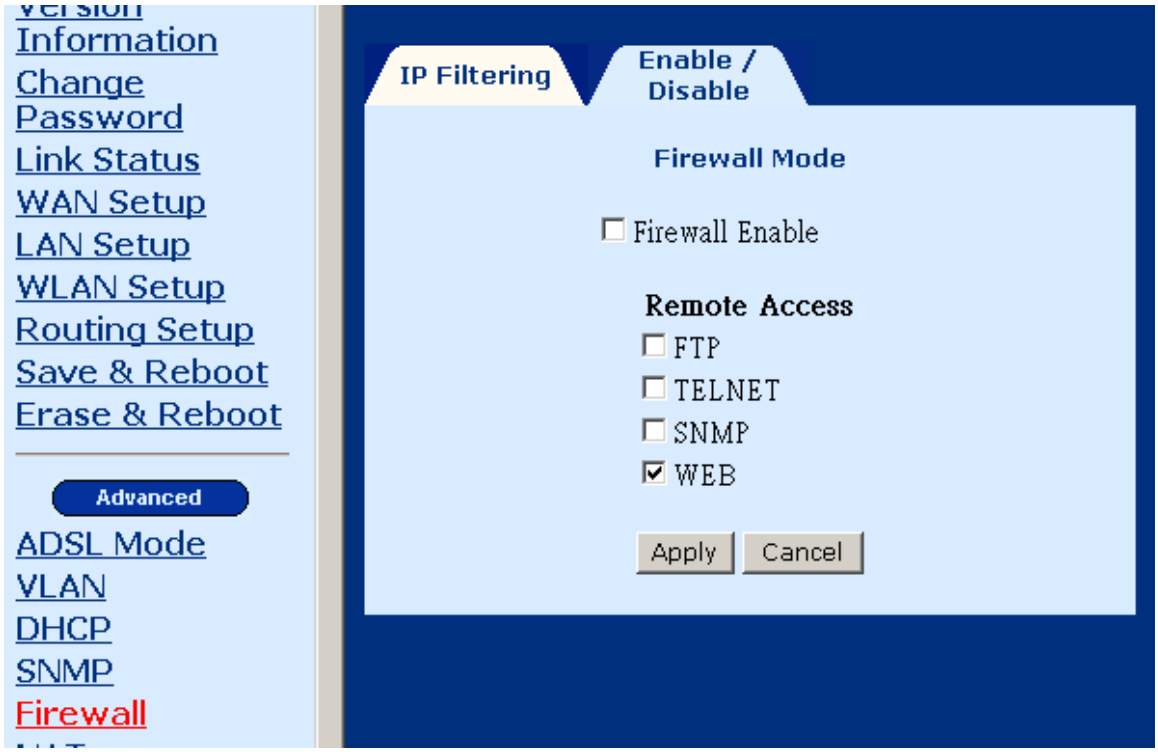
5.7.1 Enable/Disable the Firewall

To enable the firewall click on the **Enable/Disable** tab on the Firewall screen and then check the **Firewall Enable** box and click the **Apply** button. Conversely, to disable the firewall uncheck the **Firewall Enable** box and click the **Apply** button.



5.7.2 Remote Access

For each Remote Management Method that you wish to allow on the WAN port, select the method ticking its check box, and then click the **Apply** button to submit the setting. This function will in effect set up a Port Range mapping – and a Mapping entry will be created. (See section 5.8.2 for details about Port Range Mapping).



5.7.3 View Firewall Actions

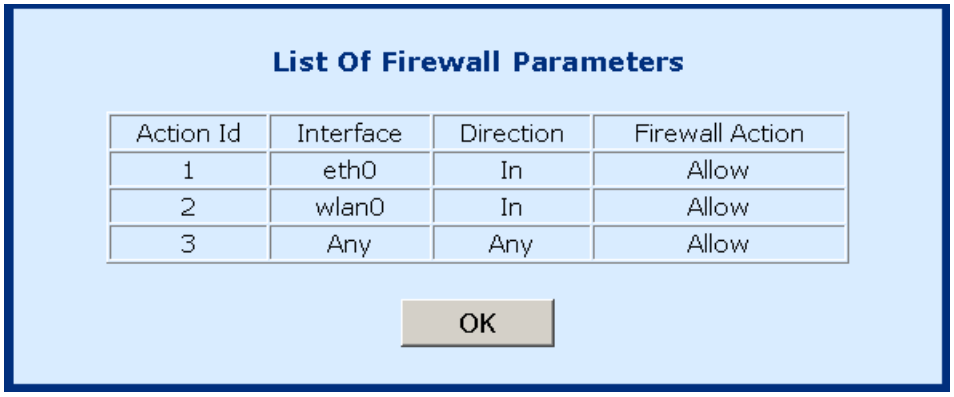
Click **View Actions** to display the list of currently configured firewall actions. The parameters are as follows:

Action ID: Item number

Interface: The interface the filtering rule is created on.

Direction: The direction can be **IN –** only packets received are affected. **OUT –**only packets sent are affected or **ANY –**both packets sent and received are affected.

Firewall Action: The action taken when packets are received that correspond to a filtering rule. **Allow** will permit packets to pass through the router, **Deny** will drop corresponding packets. **Reject** will reject packet with a response, e.g., sending a TCP reset. **Reset** rejects a packet with a reset flag.



5.7.4 IP Filtering

On the Firewall menu, click Add to configure the IP filtering entries. Fill out the parameters below and click Apply to submit the settings. The parameters are as follows:

Policy Parameters:

Precedence: This number sets the priority level of the rule, smaller numbers have higher priorities, if a conflict between rues occurs, enter a number from 1-65534.

Src IP Address: Source IP address of the packet.

Src Net Mask: Source Netmask of the packet.

Dest IP address: Destination IP address of the packet.

Dest Net Mask: Destination Net mask of the packet.

Source Port: Source port of the packet (only for TCP/UDP protocol)

Destination Port: Destination port of the packet (only for TCP/UDP protocol)

Protocol: Select the protocol from the following: Any, TCP, UDP, ICMP, GRE, AH, ESP

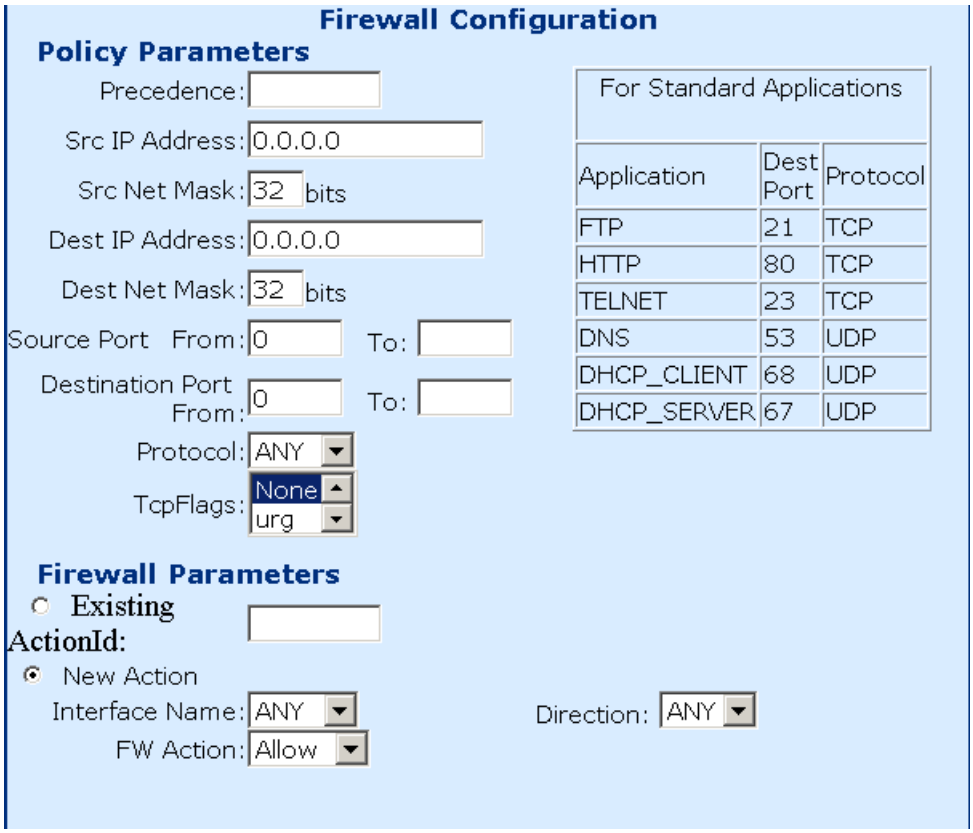
TCP Flags: Select the TCP FLAG from the following: none, urg, ack, psh, rst, syn, fin.

Firewall Parameters

Existing Action ID: If an action has already been established, check the box next to **Existing Action ID** and enter its **Action ID**.

New Action: If a new action is required check the box next to **New Action** and then enter: **Interface Name** –the interface the action applies to, **FW Action**: Enter **Allow**, to enable packets to pass through the router, **Deny** to drop corresponding packets, **Reject** to reject packet with a response, e.g., sending a TCP reset, or **Reset** to reject a packet with a reset flag.

Direction – the direction can be **IN –** only packets received are affected. **OUT –**only packets sent are affected or **ANY –**both packets sent and received are affected.



5.8 NAT

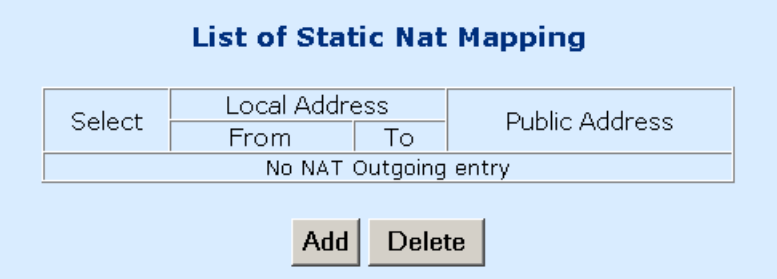
The NAT menu in the **Advanced** menu bar allows setting up the Static NAT Mapping and Port Range Mapping.

5.8.1 Static NAT Mapping

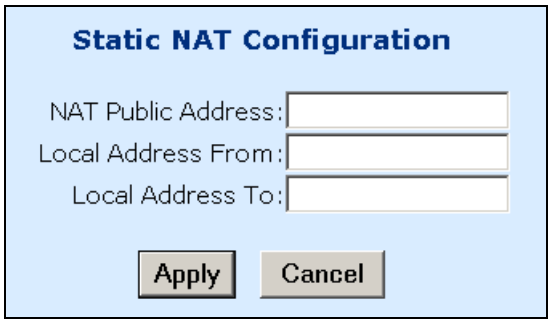
Static NAT Mapping allows a pool of local IP addresses to share a public IP address. It is a form of NAT that maps multiple Private IP addresses to a single Public IP address. It allows several virtually addressed workstations to share a single global address. PAT uses the TCP and UDP port numbers to map multiple virtual addresses to a single global address.

Follow the steps below to configure the Static NAT Mapping:

STEP 1: Click the **Static Nat Mapping** tab on the NAT menu.



STEP 2: Click **Add** to add a new entry of the static Nat mapping. Fill out the following fields and click Apply.

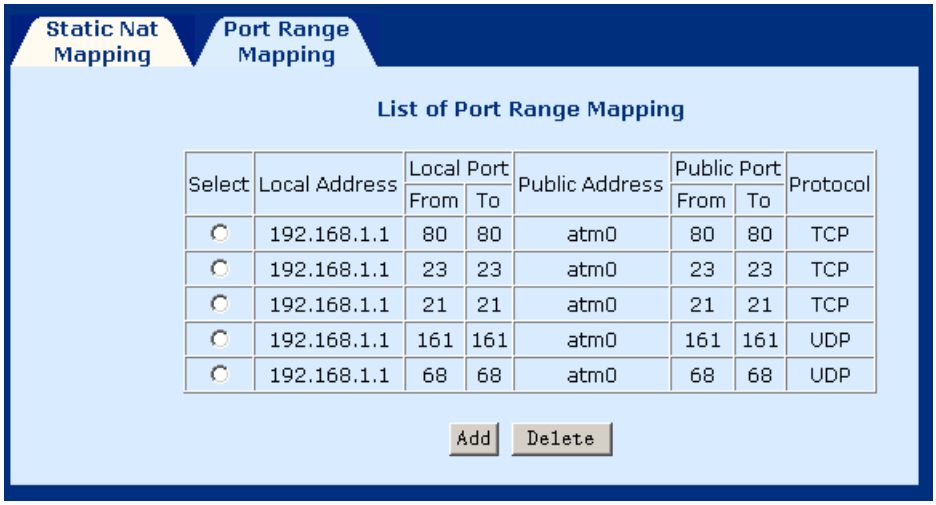


STEP 3: The new entry will be listed in previous Static NAT Mapping list.

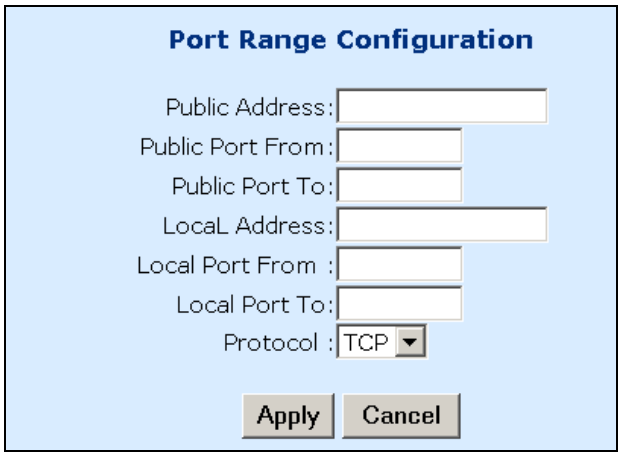
5.8.2 Port Range Mapping

The Port Range Mapping is used to set up the virtual server. A virtual server has two access ports: public and private. The public port is the open port where the Internet users access the virtual server. The local port is the port on the LAN that the virtual server is really accessed. The public port is translated to the local port to access to the virtual server. Follow the steps below to configure the Static NAT Mapping:

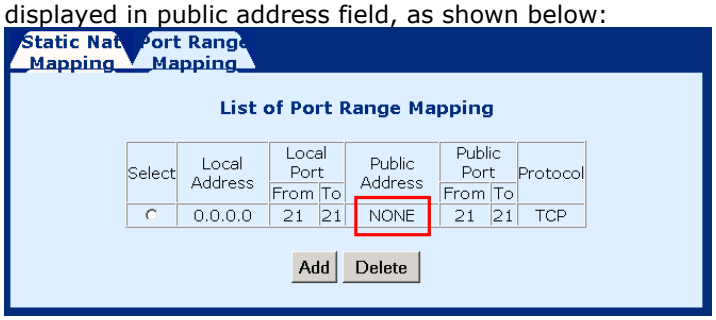
STEP 1: Click the **Port Range Mapping** tab on the NAT menu.



STEP 2: Click **Add** to add a port range mapping entry.

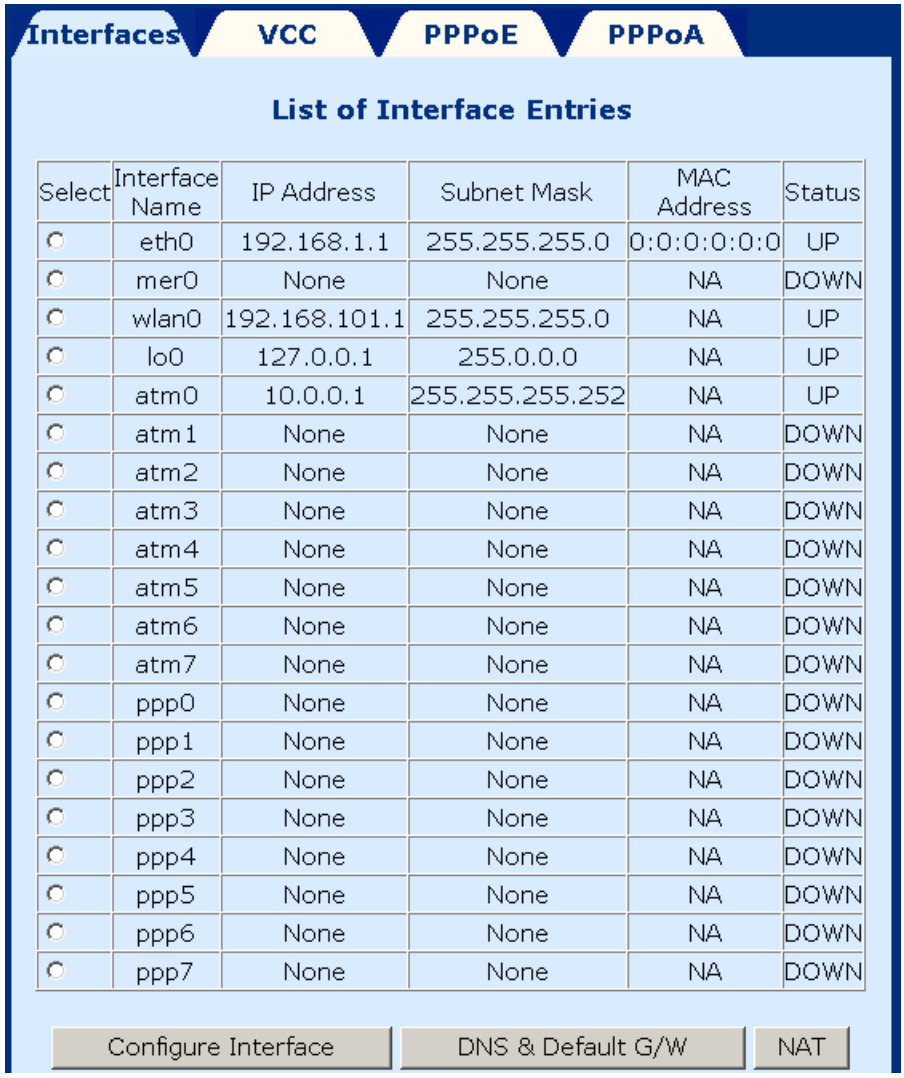


Fill out the following fields and click Apply to submit the settings.

Public Address	This is the public address where Internet users access. Enter a specific IP address, or enter 0.0.0.0 to allow any IP Address (if you wish to use the NAT interface address enter 0.0.0.0). **Note:** if you use 0.0.0.0 as the public address and the NAT interface is not active (interface is not linked-up or not configured) NONE on public address field. It means there is not any active NAT interface to do the PortMaping. NONE will be displayed in public address field, as shown below: 
Public Port From /Public Port To	Enter the public port range. These ports will be mapped or redirected to the local ports of the virtual on the LAN. Internet users access the virtual server via the public port.
Local Address	Enter the IP address of the virtual server on the LAN.
Local Port From/Local Port To	Enter the Local port range of the virtual server on the LAN.
Protocol	Specify the protocol: TCP or UDP.

5.9 Configure

From this page, you can configure the interfaces, VCC, PPPoE, PPPoA, DNS & Default Gateway, and NAT.



5.9.1 Configure Interface

To configure an interface, select it by clicking in the round-box on the left in the screen. Then click on the Configure Interface button at the bottom of the screen. Note the following:

Interfaces:

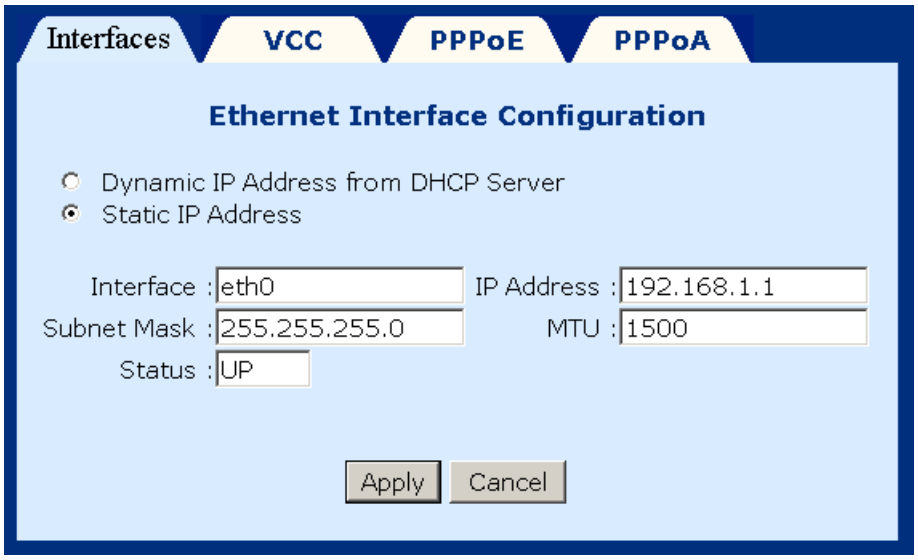
- **eth0** displays the LAN interface.
- **mer0** displays the interface configured for MER mode.
- **wlan0** displays the wireless LAN interface.
- **lo0** is the loopback interface, which is used for management. The default IP address of this interface is 127.0.0.1.
- **atm0 to atm7** display the interfaces configured for RFC1483 Bridged mode or RFC 1483 Routed mode.
- **pppo to ppp7** display the interfaces configured for PPPoE or PPPoA.

To change the interface values, select the interface from the interface list, and click the Configure Interface button.

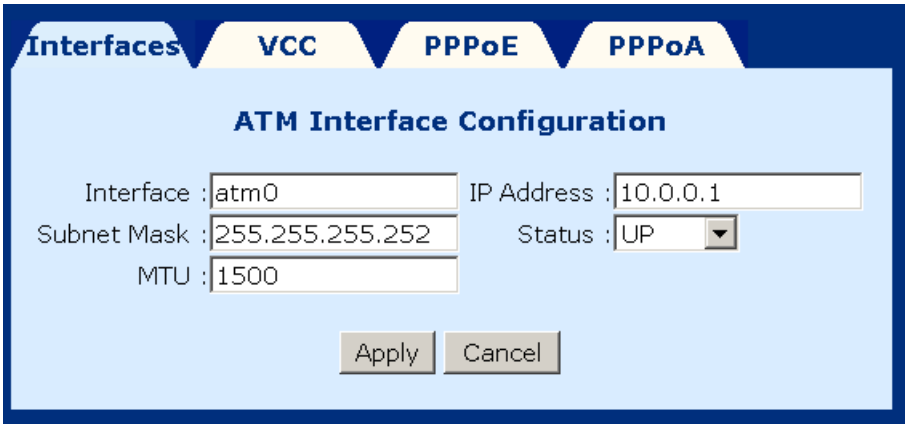
Parameters:

- **Dynamic IP address from DHCP:** Selects the IP address to be assigned by the DHCP server.
- **Static IP address:** Selects the IP address to be statically assigned.
- **Interface:** The name of the interface currently selected.
- **IP address:** The IP address of the selected interface.
- **Subnet Mask:** The subnet mask of the selected interface.
- **MTU:** Sets the maximum transmission unit of the interface. The MTU is used to limit the size of packets that are transmitted on an interface. Not all interfaces support the MTU parameter, and some interfaces, like Ethernet, have range restrictions (80 - 1500).
- **Status:** UP and Down. When an interface is set to **Down**, the system will not attempt to transmit messages through that interface. When set to **UP**, messages can be transmitted through the interface.

The following is the screen shot for the LAN interface (eth0) after choosing eth0 and clicking the Configure Interface button.



The following is a screen shot for the ATM interface.

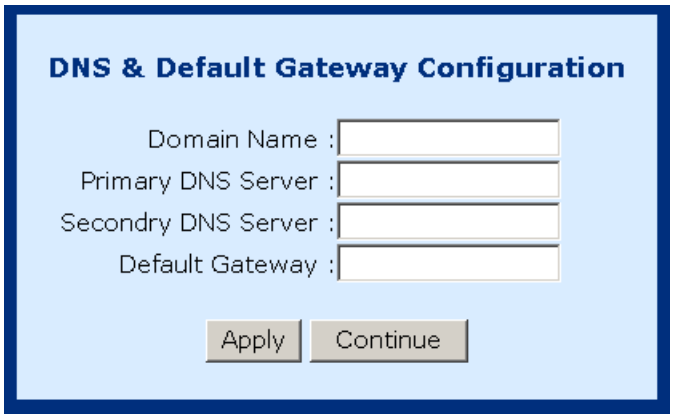


5.9.2 DNS & Default Gateway

To configure the DNS and default gateway, complete the following steps:

STEP 1: Click on **Configure** in the menu bar.

STEP 2: Click on **DNS and default gateway** at the bottom of the configuration page.



STEP 3: Complete the fields below:

- Domain Name: user-defined
- Primary DNS server: Enter the primary server IP address.
- Secondary DNS server: Enter the secondary server IP address that will be used in the event that the primary server IP address fails or is not available
- Default Gateway: The gateway IP address of the IP network

STEP 4: Submit the settings by clicking **Apply**.

5.9.3 NAT

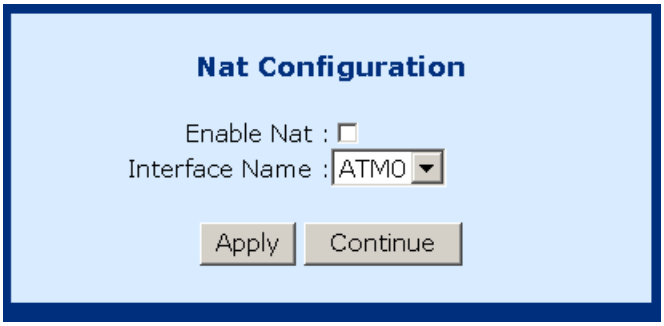
The screen below is accessed by clicking the **NAT** button on the **Configuration** screen. To enable NAT check the Enable NAT box and the select the interface that you wish to enable NAT on.

1. From the configuration menu click on the NAT button at the bottom-right side of the screen.

2. Check the **Enable NAT** box

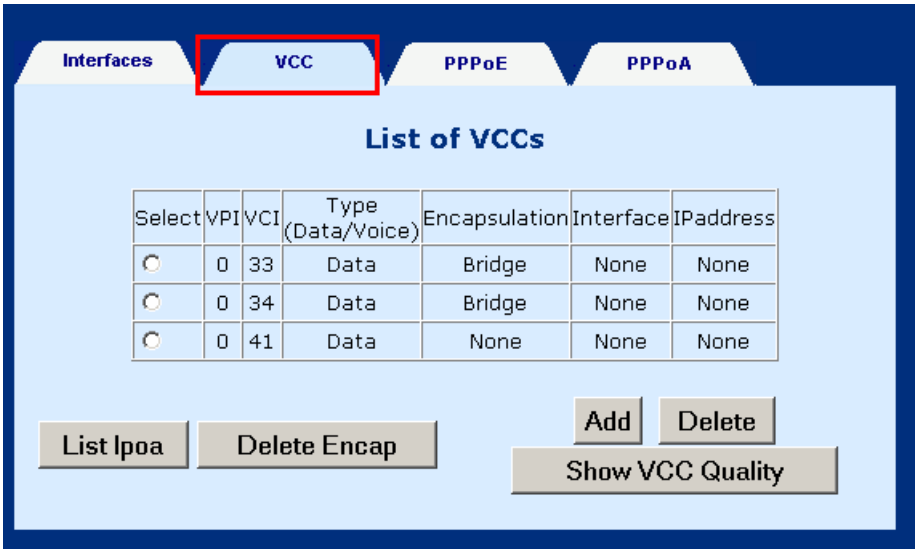
3. Select the interface to enable NAT

4. Click the **APPLY** button



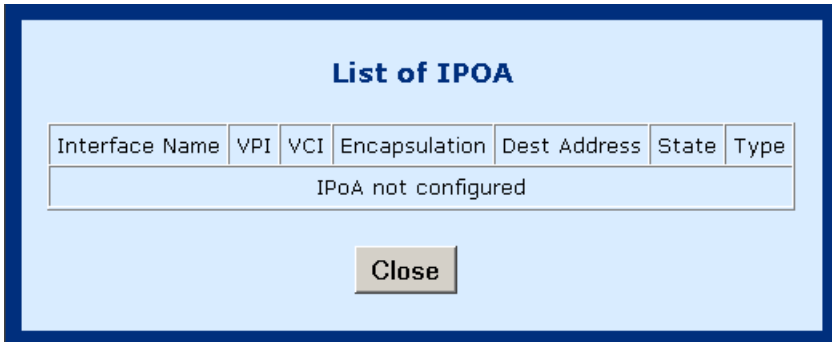
5.10 VCC

This screen lists all current VCC entries in the middle of the screen. From this screen you can also: List IPoA, Delete Encapsulation, Add a VCC, Delete a VCC, and Show VCC quality.

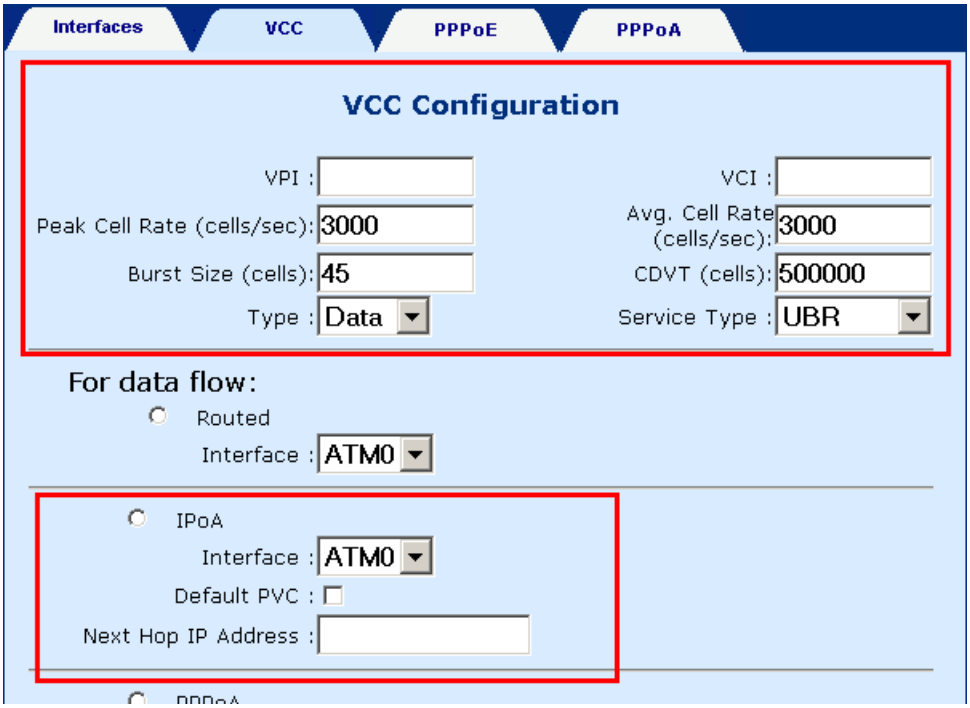


5.10.1 List IPoA

To list IP over ATM information click on the **IPoA** button at the bottom-left of the screen.



The IPoA entry is set up from Advanced>Configure>VCC, Click the Add button on the List of VCC screen.



5.10.2 Delete Encapsulation

To delete encapsulation first select a VCC entry and then click the **Delete Encap** button.

5.10.3 Add a VCC

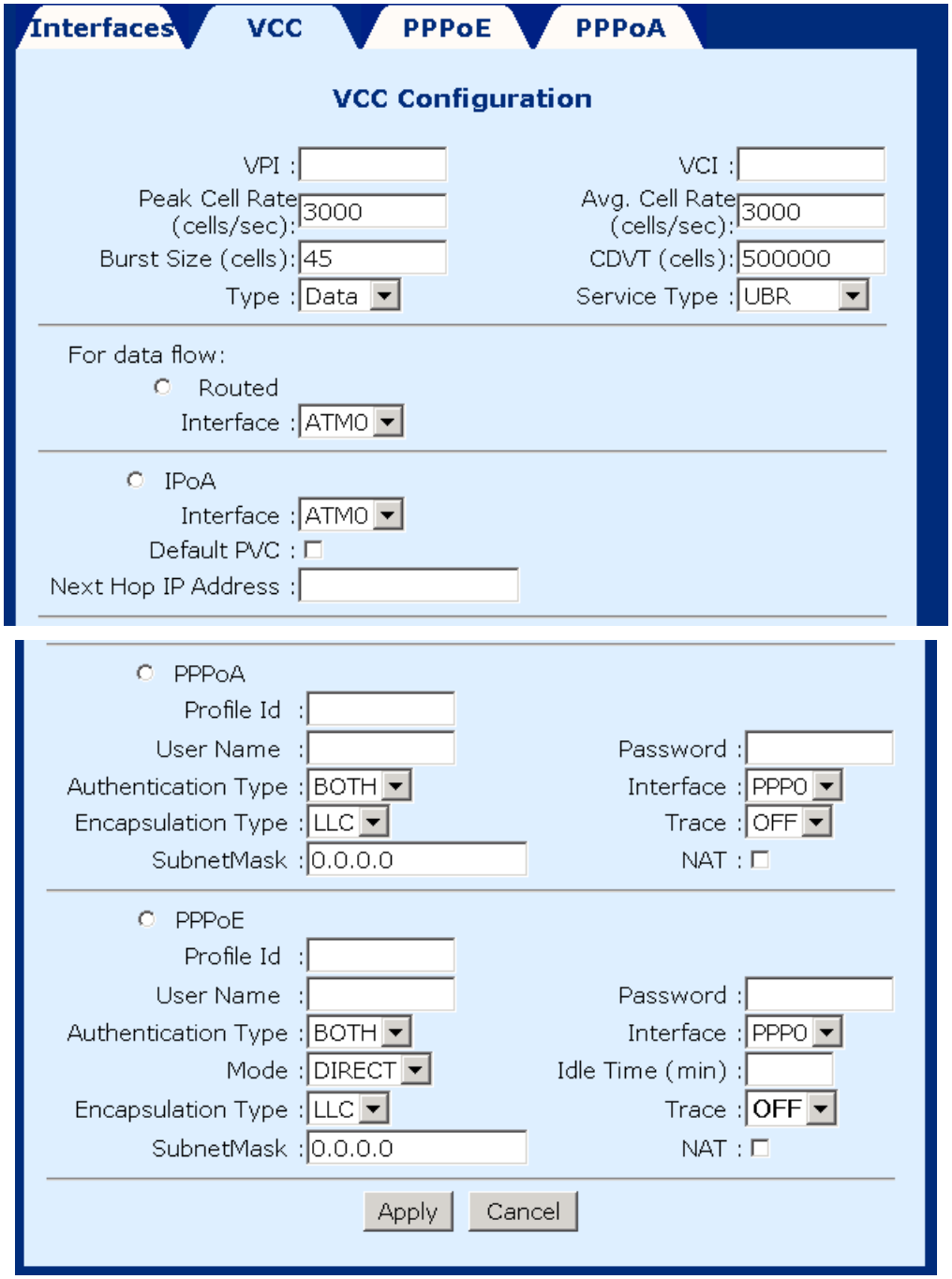
To add a VCC entry, complete the following steps:

STEP 1: Click on the Add VCC button, the VCC screen will appear.

STEP 2: Enter values for the parameters (explained below).

STEP 3: Click the **Apply** button at the bottom of the page.

vpi:	Virtual Path Identifier (VPI) that identifies this ATM connection. The vpi is integer numbers, which can range from 0 to 4095.
vci:	Virtual Channel Identifier (VCI) that identifies this ATM connection. The vci is an integer number which can range from 0 to 65,535.
Peak Cell rate (cells/sec):	Defines the fastest rate a user can send cells to the network. It is expressed in units of cells per second.
Average Cell rate (cells/sec):	Defines the maximum sustainable/average rate a user can send cells to the network. It is expressed in cells per second. This specifies the bandwidth utilization. This value must always be less than or equal to the Peak Cell Rate.
Burst size (cells):	Maximum number of cells the user can send at the peak rate in a burst, within a sustainable rate.
CDVT (cells):	Constrains the number of cells the user can send to the network at the maximum line rate.
Type:	Select data or voice
Service Type: **cbr** Constant Bit Rate: **rtvbr** Real Time Variable Bit Rate: **Nrtvbr** Non Real Time Variable Bit Rate: **Ubr** Unspecified Bit Rate:	 Supports real-time applications requiring a fixed amount of bandwidth. The applications produce data at regular intervals such as a video stream. The user can specify how much bandwidth they wish to reserve. Supports time-sensitive applications such as voice. In these applications the rate at which cells arrive are varied. Supports applications that have no constraints on delay and delay variation, but still have variable-rate and bursty traffic characteristics. Best effort service that does not require tightly constrained delay and delay variation. UBR provides no specific quality of service or guaranteed throughput.


Interfaces
VCC
PPPoE
PPPoA
VCC Configuration
VPI :
VCI :
Peak Cell Rate (cells/sec):
3000
Avg. Cell Rate (cells/sec):
3000
Burst Size (cells):
45
CDVT (cells):
500000
Type :
Data
Service Type :
UBR
For data flow:
Routed
Interface :
ATM0
IPoA
Interface :
ATM0
Default PVC :
Next Hop IP Address :
PPPoA
Profile Id :
User Name :
Password :
Authentication Type :
BOTH
Interface :
PPP0
Encapsulation Type :
LLC
Trace :
OFF
SubnetMask :
0.0.0.0
NAT :
PPPoE
Profile Id :
User Name :
Password :
Authentication Type :
BOTH
Interface :
PPP0
Mode :
DIRECT
Idle Time (min) :
Encapsulation Type :
LLC
Trace :
OFF
SubnetMask :
0.0.0.0
NAT :
Apply
Cancel

5.10.4 Delete a VCC

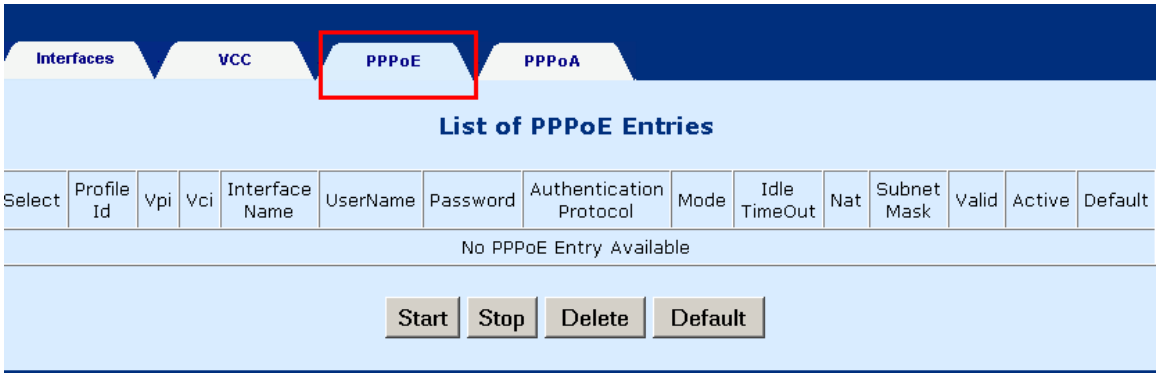
To delete a VCC entry, select the entry from the list of VCCs and then click on the **delete** button, at the bottom-right of the page.

5.10.5 Show VCC quality

To view information regarding the VCC quality, click on the **Show VCC Quality** button, at the bottom-right of the page.

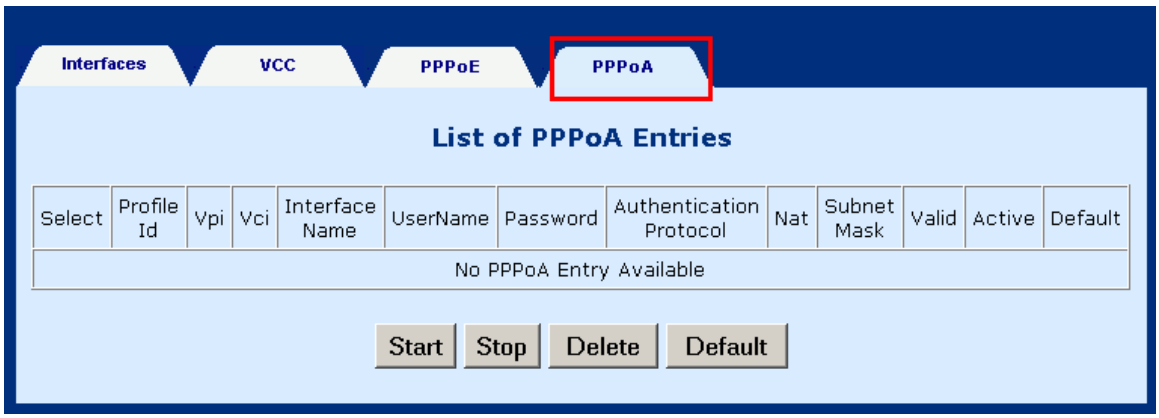
5.10.6 PPPoE

This section will describe how to start, stop, delete, and set a default PPPoE entry. The PPPoE page can be accessed by clicking on **Configure** in the Advanced menu bar. To start, stop, delete, or set as default a PPPoE entry first select the entry from the List of PPPoE entries, and then click the corresponding button at the bottom of the page.



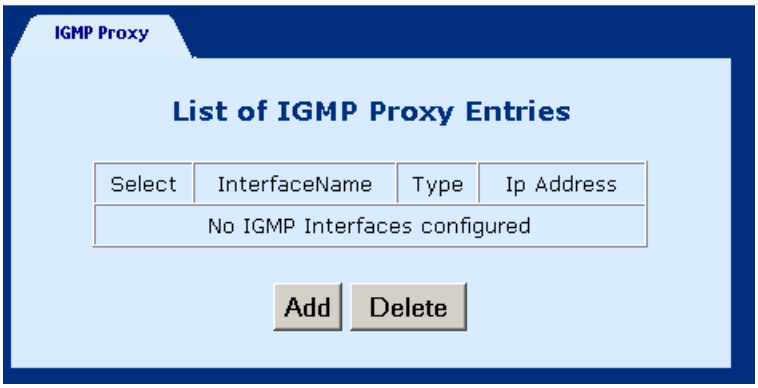
5.11 PPPoA

This section will describe how to start, stop, delete, and set a default PPPoA entry. The PPPoA page can be accessed by clicking on **Configure** in the Advanced menu bar. To start, stop, delete, or set as default a PPPoA entry first select the entry from the List of PPPoA entries, and then click the corresponding button at the bottom of the page.



5.12 IGMP

IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.



5.12.1 Add an IGMP entry

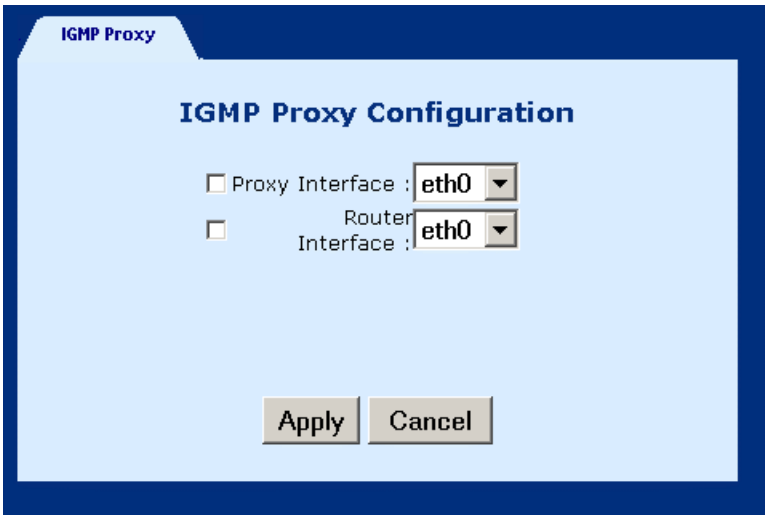
To add an IGMP proxy, complete the following steps:

STEP 1: Select **IGMP Proxy**, from the menu bar.

STEP 2: Click **Add** at the bottom of the screen.

STEP 3: Select Proxy interface, router interface, or both, by checking the box next to the interface and then use the pull-down menu to the left to select the eth, atm, or ppp Interface.

STEP 4: Click **Apply** to activate the parameters.



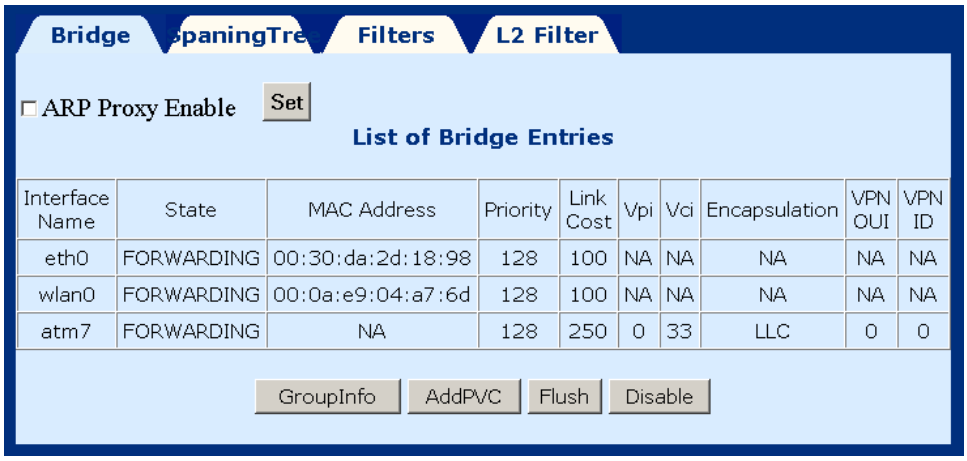
5.12.2 Delete an IGMP entry

To delete an entry, select an entry from the list, and click **Delete**.

5.13 Bridging

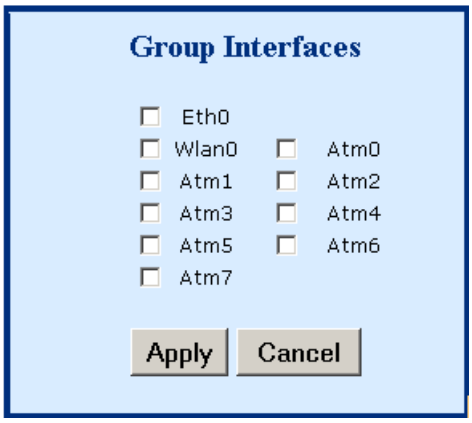
5.13.1 Bridge

The Bridge window displays the configured Bridging PVC entries of the interfaces. There are four buttons at the bottom of the main-pane: Group Info, Add PVC, Flush, and Disable.

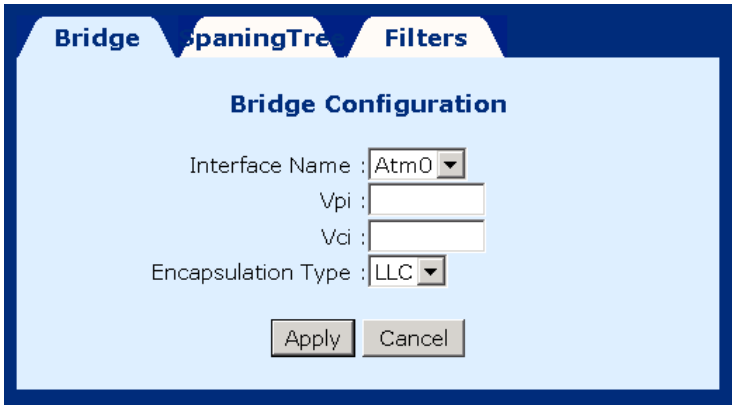


- **ARP Proxy**: You can enable the ARP Proxy function by ticking its check box and clicking the **Set** button. Proxy ARP allows a router to answer a local ARP request for a remote destination. Address Resolution Protocol (ARP) enables the router to determine a network host's physical address by binding a 32-bit IP address to a 48-bit MAC address.

- **GroupInfo:** This configures the LAN packets that will travel through the LAN interface to the selected WAN interfaces. If you wish to change the interfaces that are configured you must first click on the **Flush button** (to remove the current configuration), and then click on the **Group Info** button, select the group interfaces and then click the **Apply** button. You must select eth0, as eth1 is not enabled for this product version.



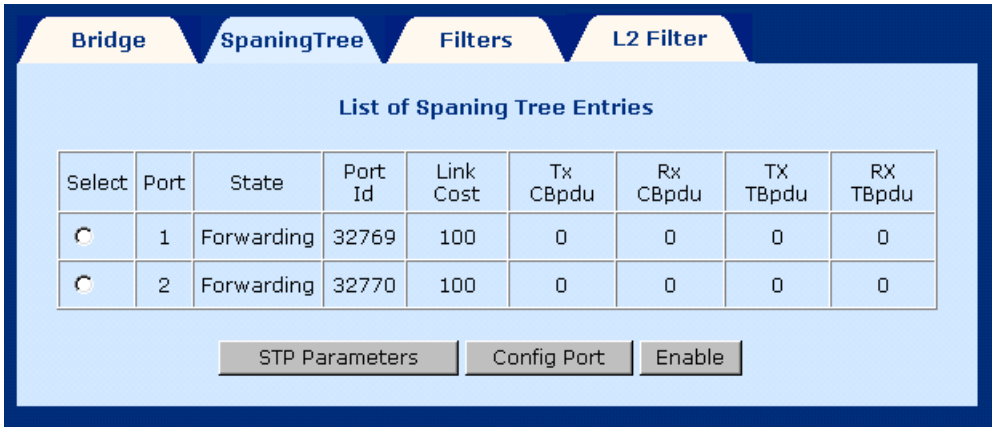
- **AddPVC:** You can add a PVC to the ATM interface. From the **Bridging** screen, select an ATM interface Vpi, Vci and Encapsulation type and then click **Apply**.



- **Flush:** Selecting this command from the **Bridging** screen, will flush all PVC entries.
- **Disable:** Selecting this command from the **Bridging** screen, will disable the PVCs but retain the parameters, so that they can be enabled at a later point.

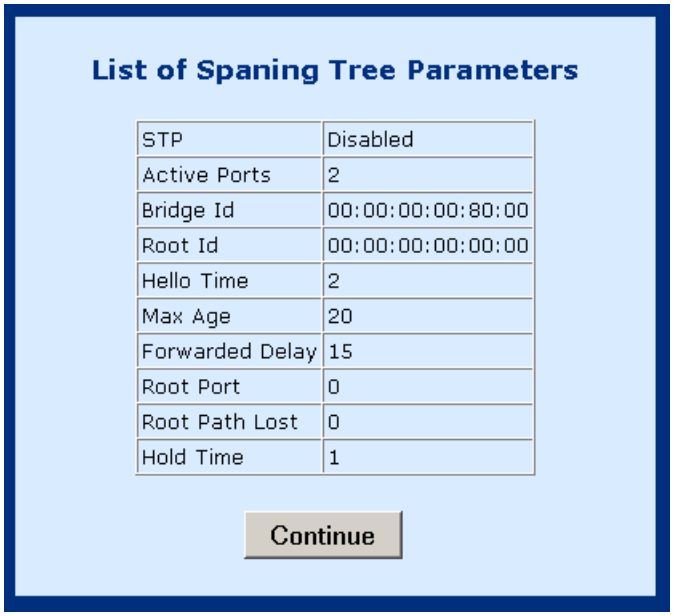
5.13.2 Spanning tree

To access the spanning tree menu click the **Spanning Tree** tab, located at the top of the **Bridging** screen.



5.13.2.1. View STP Parameters

To view the STP parameters, click the **STP parameters** tab, located at the bottom of the Spanning Tree screen.



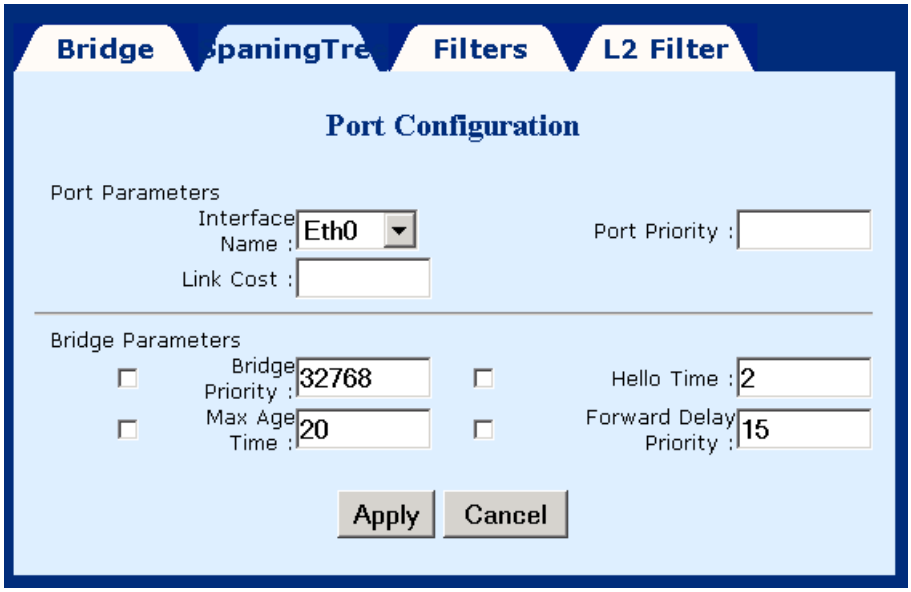
5.13.2.2. To configure STP parameters

STEP 1: Click the **Spanning Tree** tab, located at the top of the **Bridging** screen.

STEP 2: Click the Configure Port button.

STEP 3: Configure the parameters.

STEP 4: Click the Apply button.

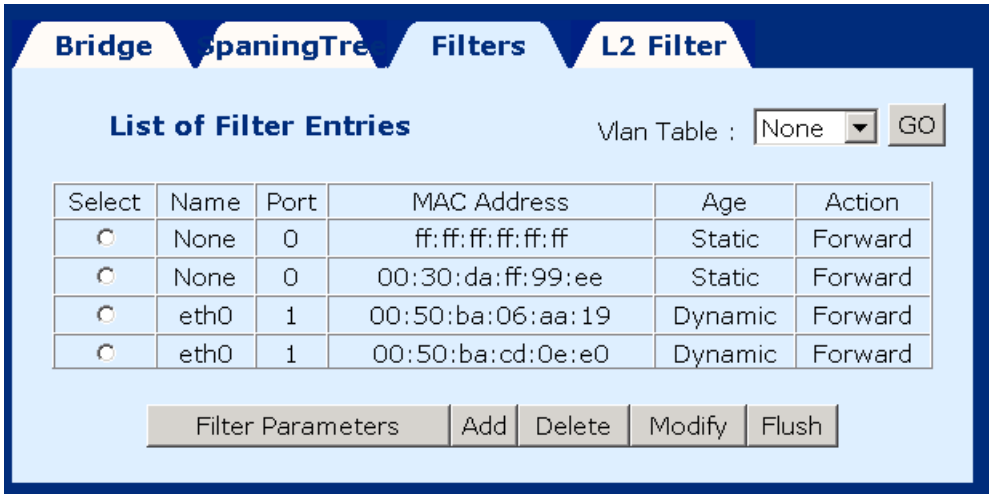


5.13.2.3. Enable/Disable STP

If you wish to Enable/Disable a STP entry, select the entry and then click the **Enable** or **Disable** Button, which is located at the bottom-right of the Spanning Tree screen. Note that if the entry is already enabled the Disable button will be present. Conversely, if the entry is disabled then the Enable button will be present.

5.13.3 Filters

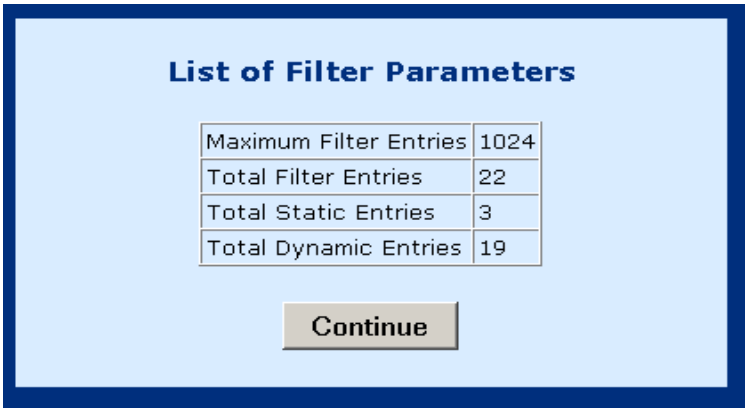
Filtering is a type of firewall that is useful to increase network security or to limit unwanted traffic. Filters for this device are based on MAC addresses. The page opens with a list of the currently configured filter entries. From this page, you can also view Filter Parameters, add a filter, delete a filter, modify a filter, or flush filter parameters. These functions are described below.



5.13.3.1. List of filter entries

To display a list of filter parameters click the **Filter parameters** button at the bottom of the Filters page. The following parameters are displayed:

Maximum filter entries	The number of filter entries that can potentially be set
Total filter entries	The number of filter entries that are currently set
Total static entries	The number of static entries that are currently set
Total dynamic entries	The number of dynamic entries that are currently set



5.13.3.2. Add a filter entry

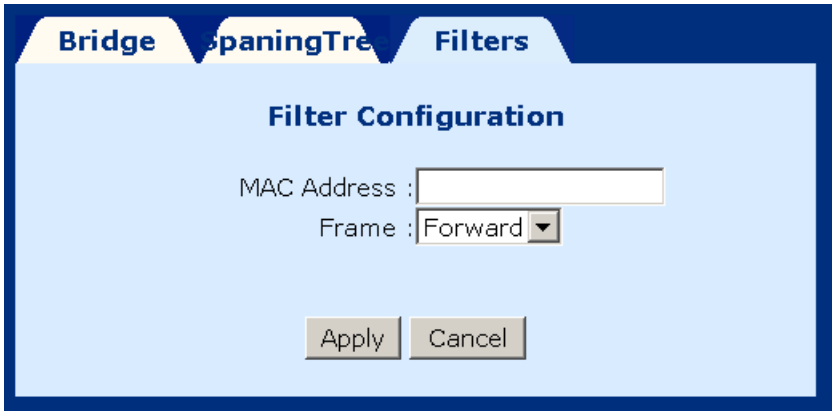
To add a filtering entry, complete the following steps:

STEP 1: Click the **Add** button at the bottom of the Filters page.

STEP 2: Enter the MAC address

STEP 3: Set the Frame to **forward** to forward packets which match the MAC address, or **Drop**, to drop matching packets.

STEP 4: Click **Apply**.



5.13.3.3. Delete a filter entry

To delete a filtering entry Select an entry and then click the **Delete** button at the bottom of the Filters page.

5.13.3.4. Modify a filter entry

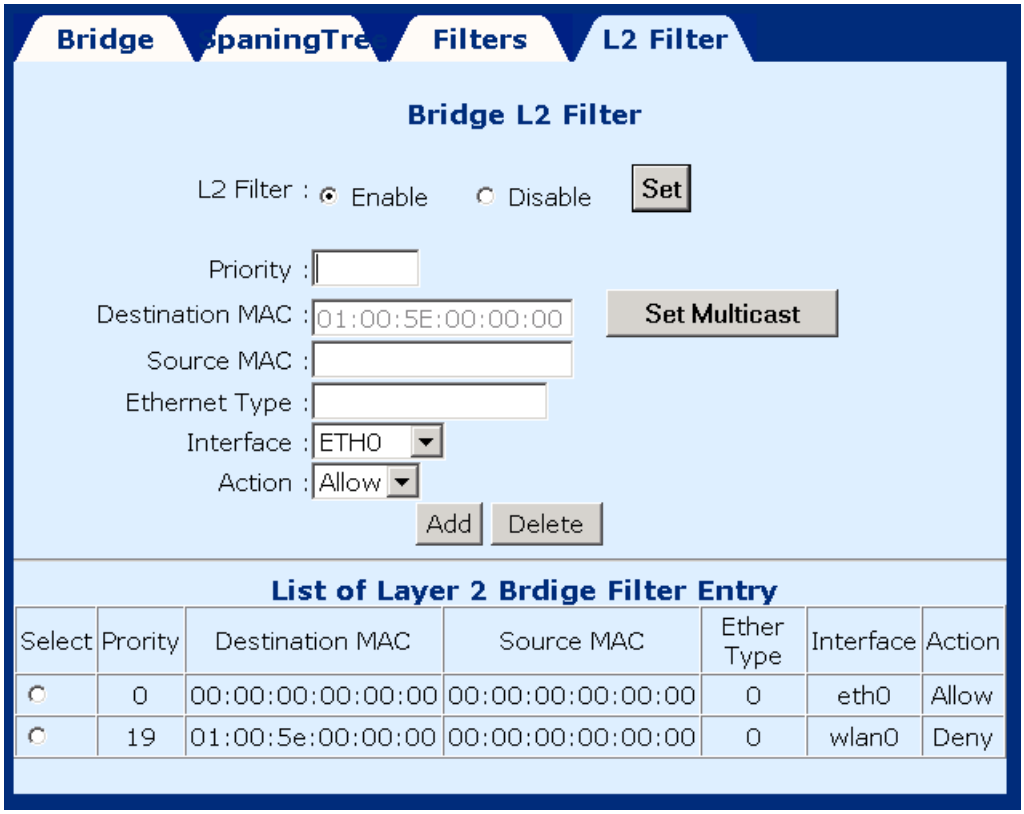
To modify a filter select the entry and then click the **Modify** button at the bottom of the Filters page.

5.13.3.5. Flush filter entries

To flush all the filtering entries, click the **Flush** button at the bottom of the Filters page.

5.13.4 Layer 2 bridge filtering

L2 Filters for this device are based on MAC addresses. The page opens with a list of the currently configured L2 bridge filter entries. Packets are dropped or accepted according to the conditions set up in each entry. From this page, you can also view Filter Parameters, add a filter, or delete a filter. These functions are described below.



5.13.4.1. Enable/Disable L2 filtering

If you wish to Enable/Disable Bridge L2 filtering, click **Enable** or **Disable** and click the **Set** button. This setting applies to the list of layer 2 bridge filtering entries.

5.13.4.2. Add a Bridge L2 filter entry

To add an L2 filtering entry, complete the following steps:

STEP 1: Complete the parameters on the screen:

- **Priority**: Enter a priority value from 0-19. The lower the priority value, the higher the entry's priority. These priority values will dictate the order of precedence in which packets will be processed.
- **Destination MAC**: This is the destination MAC address of the packet. Enter the address, or click the **Set Multicast** button to set the address to the Multicast MAC address. If the address is set to 00:00:00:00 or left blank, then this field will be ignored when verifying whether the packet should be passed through or dropped.
- **Source MAC**: This is the source MAC address of the packet. If the address is set to 00:00:00:00 or left blank, then this field will be ignored when verifying whether the packet should be passed through or dropped.
- **Ethernet Type**: Enter the Ethernet Type in hexadecimal format. For example, enter 0800 for IP address, or enter 0806 for ARP.
- **Interface**: Select the interface for the packet, from the Interface dropdown list. The available interface options are eth0, wlan0 and atm0.
- **Action**: Select either Allow or Deny, to allow or deny the packet to pass through.

STEP 2: Click the **Add** button at the bottom of the L2 Filter page to apply the settings.

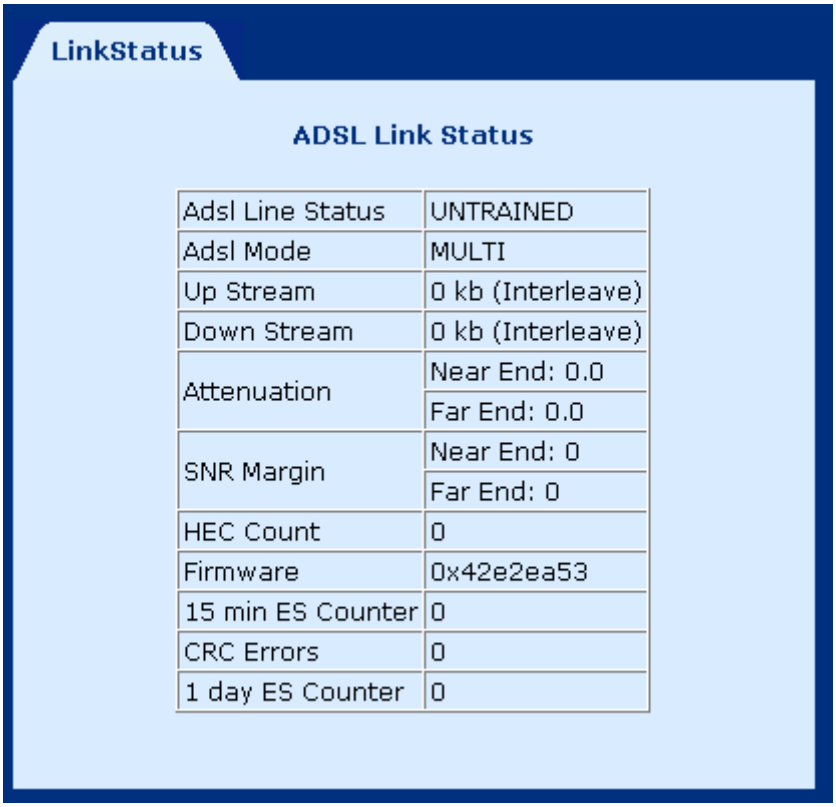
5.13.4.3. Delete an L2 filter entry

To delete an L2 filtering entry select an entry and then click the **Delete** button at the bottom of the L2 Filters page.

Chapter 6 Web Performance monitoring

6.1 ADSL Link Status

To view the ADSL link status, click **Link Status** on the tool bar.



ADSL Line Status	Shows the current status of the ADSL line
ADSL Mode	Shows the ADSL standard that is currently configured. The standards are: ANSI, G.DMT, G.LITE, MULTI.
Upstream	Upstream data rate negotiated by DSL link (Kbit/s)
Downstream	Downstream data rate negotiated by DSL link (Kbit/s)
Attenuation	Current attenuation (dB).
SNR Margin	Current SNR margin (dB)
HEC Count	Number of ATM cells received with errors since start of link.
Firmware	The version number of the firmware
15 min ES counter	Number of errored seconds for the current 15 minute period
CRC errors	Number of errors per second since training
1 day ES counter	Number of errored seconds for the current day

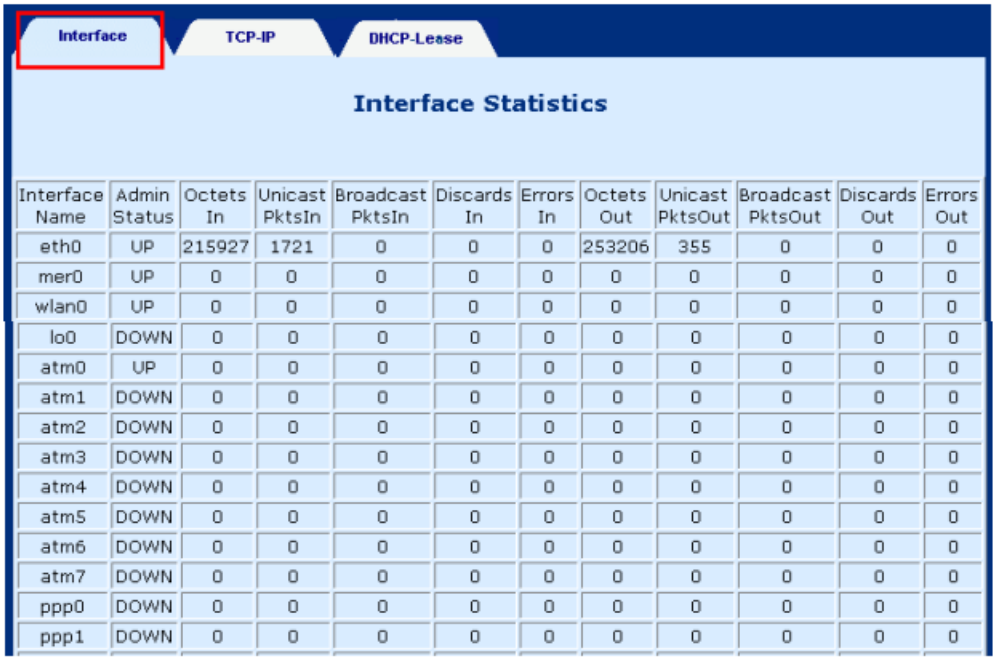
6.2 System Statistics

To view the system statistics, click on the **System Statistics** button located near the bottom of the menu-bar. Statistics are recorded regarding Interfaces, TCP-IP, and DHCP-Lease.

6.2.1 Interface Statistics

To display the interface statistics, click the **Interface** tab, located at the top-left of the System Statistics screen. The Interface Statistics page displays statistics for all interfaces. The following information is displayed:

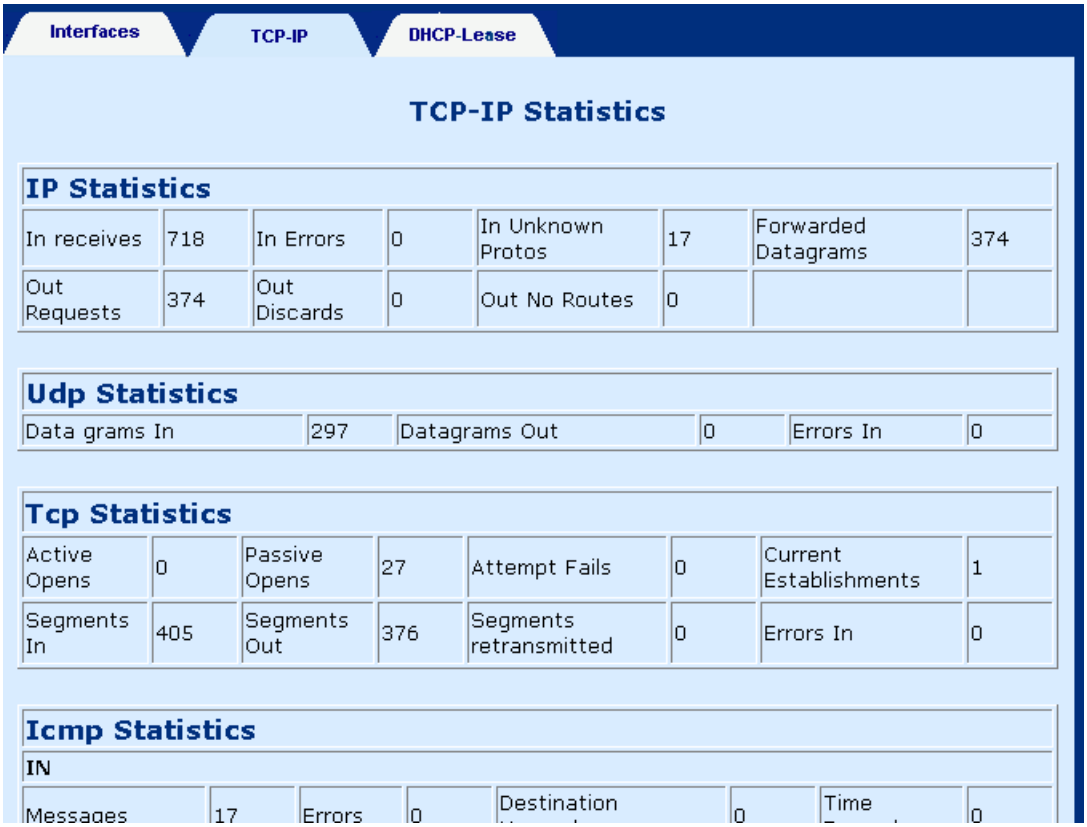
Interface Name	The name of the interface
Admin Status	Indicates whether the interface is Up or Down
Octets In	The number of Octets (bytes) recieved
Unicast PktsIn	The number of unicast packets received
Broadcast PktsIn	The number of broadcast packets received
Discards In	The number of packets received that were discarded
Errors In	The number of inward errors
Octets Out	The number of Octets (bytes) transmitted
Unicast PktsOut	The number of unicast packets transmitted
Broadcast PktsOut	The number of broadcast packets transmitted
Discards Out	The number of packets transmitted that were discarded
Errors Out	The number of outward errors



Interface Name	Admin Status	Octets In	Unicast PktsIn	Broadcast PktsIn	Discards In	Errors In	Octets Out	Unicast PktsOut	Broadcast PktsOut	Discards Out	Errors Out
eth0	UP	215927	1721	0	0	0	253206	355	0	0	0
mer0	UP	0	0	0	0	0	0	0	0	0	0
wlan0	UP	0	0	0	0	0	0	0	0	0	0
lo0	DOWN	0	0	0	0	0	0	0	0	0	0
atm0	UP	0	0	0	0	0	0	0	0	0	0
atm1	DOWN	0	0	0	0	0	0	0	0	0	0
atm2	DOWN	0	0	0	0	0	0	0	0	0	0
atm3	DOWN	0	0	0	0	0	0	0	0	0	0
atm4	DOWN	0	0	0	0	0	0	0	0	0	0
atm5	DOWN	0	0	0	0	0	0	0	0	0	0
atm6	DOWN	0	0	0	0	0	0	0	0	0	0
atm7	DOWN	0	0	0	0	0	0	0	0	0	0
ppp0	DOWN	0	0	0	0	0	0	0	0	0	0
ppp1	DOWN	0	0	0	0	0	0	0	0	0	0

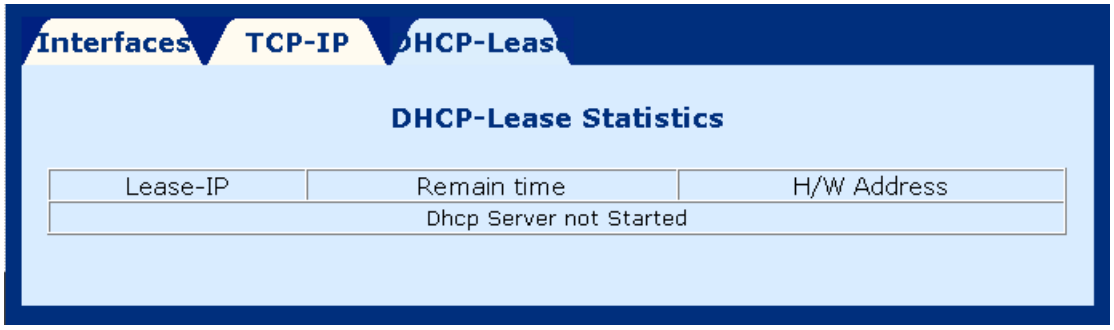
6.2.2 TCP-IP

To view TCP-IP statistics click on the **TCP-IP** tab at the top of the System Statistics page. The TCP-IP page displays the IP statistics, UDP statistics, TCP statistics, and ICMP statistics.



6.2.3 DHCP-Lease

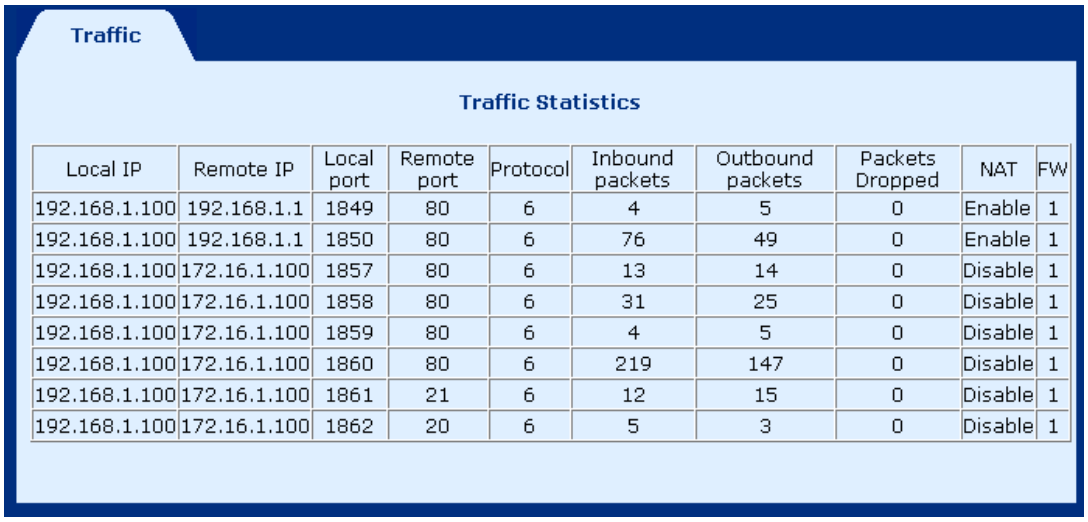
To view DHCP-Lease statistics click on the **DHCP-Lease** tab at the top of the System Statistics page. The DHCP-Lease page shows the PCs that obtained an IP address from the DHCP pool.



6.3 Firewall Statistics

To view the firewall traffic statistics, click **Firewall Statistics** from the Advanced menu. It records the session information, including TCP, UDP, ICMP, GRE, AH, and ESP. Each session protocol is represented by a number. For example, 1 is for ICMP, GRE for 47; ESP for 50, AH for 51, UDP for 17, TCP for 6. Each session covers the following information.

Local IP	Local IP address of the PC on the LAN
Remote IP	ATM IP address on the remote site
Local Port	The local port that the local PC connects to on the remote site.
Remote Port	The remote port that the local PC connects to on the remote site.
Protocol	Displays the session of protocol (TCP, UDP, ICMP ,GRE AH, ESP)
Inbound packets	Number of inbound packets
Outbound packets	Number of outbound packets
Packets dropped	Total number of packets dropped
NAT	Reserved feature
FW	Displays the status of the firewall; 1 means firewall is enabled; 0 means firewall is disabled



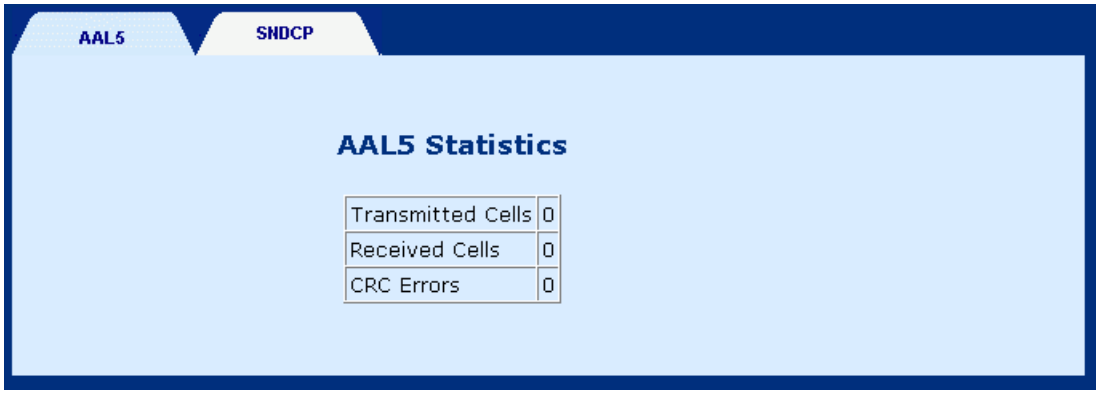
Local IP	Remote IP	Local port	Remote port	Protocol	Inbound packets	Outbound packets	Packets Dropped	NAT	FW
192.168.1.100	192.168.1.1	1849	80	6	4	5	0	Enable	1
192.168.1.100	192.168.1.1	1850	80	6	76	49	0	Enable	1
192.168.1.100	172.16.1.100	1857	80	6	13	14	0	Disable	1
192.168.1.100	172.16.1.100	1858	80	6	31	25	0	Disable	1
192.168.1.100	172.16.1.100	1859	80	6	4	5	0	Disable	1
192.168.1.100	172.16.1.100	1860	80	6	219	147	0	Disable	1
192.168.1.100	172.16.1.100	1861	21	6	12	15	0	Disable	1
192.168.1.100	172.16.1.100	1862	20	6	5	3	0	Disable	1

6.4 ATM Statistics

Click on **ATM Statistics** on the menu-bar to display the ATM Statistics. The ATM Statistics page monitors information for AAL5 and Encapsulation.

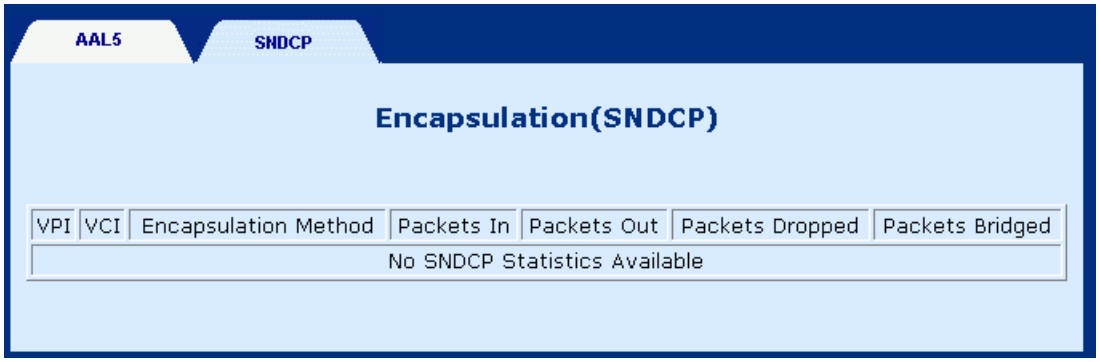
6.4.1 AAL5

The AAL5 page shows the AAL5 statistics.



6.4.2 Encapsulation

Click on the **SNDCP** tab to display encapsulation statistics. This page displays the VCs that are running. (SNDCP stands for sub-network dependency convergency protocol).



Chapter 7 Web Diagnostics

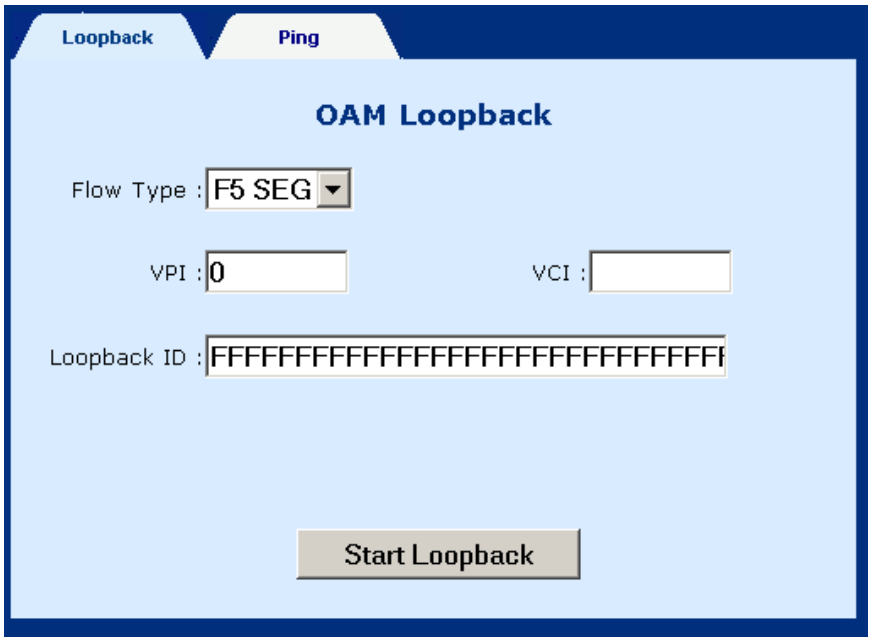
To access the Diagnostics screen, click the **Diagnostics** button, which is located on the menu bar. The Diagnostics screen has two test functions: OAM Loopback and Ping test.

7.1 OAM Loopback

STEP 1: Click the **Diagnostics** button, on the menu bar.

STEP 2: Click the **Loopback** tab on the Diagnostics screen.

STEP 3: Enter the following information to run the OAM loopback:



- Flow type: F5 SEG (Segment to Segment) and F5 ETE (End-to-End). The **SEG** loopback is from ATUR to DSLAM. The **ETE** loopback is from ATUR to the ISP RAS.
- VPI and VCI: Specify the virtual channel that will run the OAM loopback.
- Loopback ID: Type the loopback pattern for the loopback

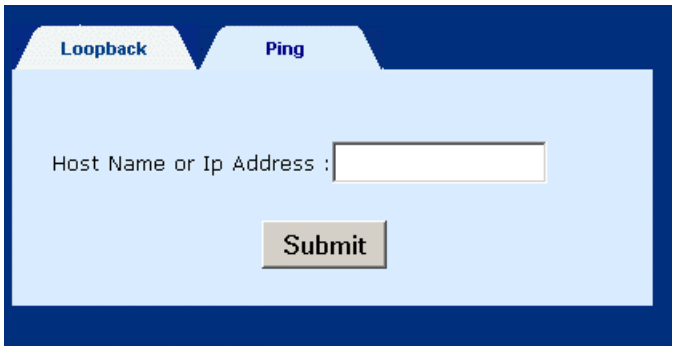
STEP 4: Click the **Start Loopback** button at the bottom of the screen.

7.2 Ping

A Ping test is used to verify the status of a network connection after the RIP or static route function is enabled. Ping sends a request message to the host and waits for a return message. This diagnostic function can verify if the remote host is reachable. Ping can also measure the round-trip time to the remote host.

To access the Ping test screen, click the **Ping** tab on the Diagnostics screen.

Enter the **Host Name** or **IP address** of the remote terminal and click **Submit** to start the ping and display the results.



The following is an example of the ping result. The information displayed is as follows:

Packets transmitted	The number of packets that were transmitted
Packets received	The number of packets that were received
Packets lost	The number of packets lost (transmitted-received)
Minimum round trip time	The fastest round-trip time
Maximum round trip time	The slowest round-trip time

Chapter 8 Firmware Upgrade

Follow the steps below to upgrade the firmware version of the wireless router via the FTP:

STEP 1: Connect the Router to a PC using the LAN cable. Set the PC to the same subnet as the router (192.168.1.x/24).

STEP 2: Restore the default parameters of the wireless router by holding down the device's **Reset** button until the **WLAN** LED starts blinking (about 5 seconds). After the device has rebooted successfully, and if the ADSL connection is established, the **WLAN** LED will stop blinking and the ADSL LED will display in green. If an error occurred, the **ALARM** LED will start blinking in red.

Note: You can also reboot the wireless router by running the device software and selecting the **ERASE** command on the **Erase and Reboot** menu.

STEP 3: Start DOS and enter the menu where the new firmware is installed:

Example: C:\Upgrade

STEP 4: Enter the command: ftp 192.168.1.1 (router's IP address)

```
C:\>ftp 192.168.1.1
```

STEP 5: At the User prompt type **root**

```
220 Welcome to the update FTP server v1.0.
User (192.168.1.1:(none)): root
```

STEP 6: At the Password prompt type **12345**

```
331 Password required for root.
Password:
```

STEP 7: After you see the message User logged in, type: **bin**

```
230 User logged in.
ftp> bin
```

STEP 8: After you see the message Type set to I, type: **hash**

```
200 Type set to I.
ftp> hash
```

STEP 9: After you see the message Hash mark printing, type: **put <filename > app.1** (if the file name has extension, also type the extension.

Example: put eagle.ct app.1

```
ftp> put eagle.ct app.1
```

STEP 10: After a moment, the file should begin transferring. After you see the message Transfer complete, reboot the ADSL router to complete the upgrade process.

```
200 PORT command successful.
150 Opening BINARY mode data connection for 'app.1'.
##################################################################################################
##################################################################################################
##################################################################################################
##################################################################################################
##################################################################################################
##################################################################################################
##################################################################################################
##################################################
226 Transfer complete.
ftp: 1245892 bytes sent in 0.73Seconds 1697.40Kbytes/sec.
ftp>
```

Appendix A: Specifications

Wireless Card

Standard	IEEE802.11b
Encryption	64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption
Channels	11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
Data Rate	11Mbps / 5.5Mbps / 2Mbps /1Mbps Auto-Fallback
RF Frequency	2412 MHz – 2484 MHz (Japan) 2412 MHz – 2462 MHz (North America) 2412 MHz – 2472 MHz (Europe) 2457 MHz – 2462 MHz (Spain) 2457 MHz – 2472 MHz (France)

Wireless Antenna Twin external Dipole Antenna

LAN Interface (Four port Ethernet switch)

Standard	IEEE802.3 10/100Base-T

WAN Interface (One ADSL port)

ADSL standard	ANSI T1.413 Issue 2, G.DMT, G.lite
G.DMT data rate	Downstream: 11 Mbps Upstream: 1 Mbps
G.lite data rate	Downstream: 1.5 Mbps Upstream: 512 Kbps

ATM Attributes

PPP over AAL5	RFC 2364
Multi-protocol over AAL5	RFC 2684 (RFC 1483) Bridge RFC 2684 (RFC 1483) Route
PPP over Ethernet	RFC 2516
VCs	8
AAL type	AAL5
ATM service class	UBR/CBR/VBR
ATM UNI support	UNI3.1
OAM F4/F5	Yes

Management

LED Indicators	Power, LAN status, LAN ACT, ADSL status, Wireless LAN status, Wireless LAN ACT
Web-based management	Yes
Telnet	Yes
SNMP	Yes
Console port	RS232/DB9

Bridge Functions

Transparent bridging and learning	IEEE 802.1d
VLAN IEEE 802.1q transparent	Yes
Spanning Tree Algorithm	Yes

Routing Functions	
Routing	Static route, RIP, and RIPv2
NAT/PAT	Yes
Security	
Authentication protocols	PAP, CHAP, MS-CHAP
VPN features	PPTP/L2TP pass through
Power Supply	100, or 220 VAC
Dimensions	205 * 145 * 48 mm

Specifications are subject to change without notice

Appendix B: Pin Assignments

Pin Definitions of the LAN port

Pin number	Definition	Pin number	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

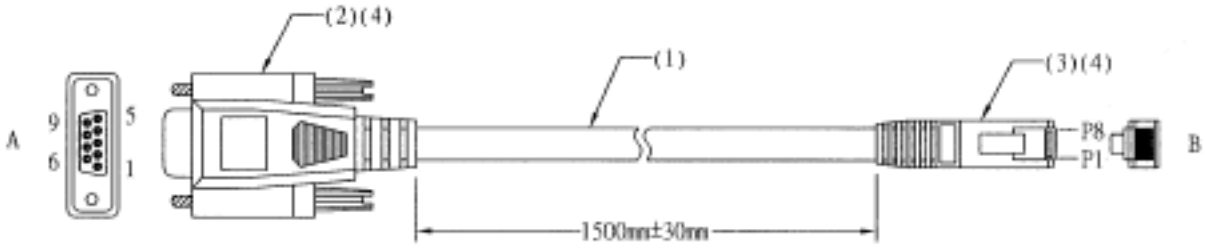
Note: NC means No connection

Pin Assignments of RJ11 Port

Pin	Definition	Pin	Definition
1	-	4	TIP
2	-	5	-
3	RING	6	-

Note: NC means No connection

Console cable



DB9 End Pins	COLOR	RJ-45 End Pins
N/C	WHITE/ORANGE	P1
N/C	ORANGE	P2
P3 (RD)	WHITE/GREEN	P3
P2 (TD)	BLUE	P4
N/C	WHITE/BLUE	P5
N/C	GREEN	P6
P5 (GRD)	WHITE/BROWN	P7
N/C	BROWN	P8