COMTREND CORPORATION

CT-535
Wireless ADSL Router
User's Manual

Version A1.1, May 22, 2003

261035-009

Preface

It is designed to provide 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.

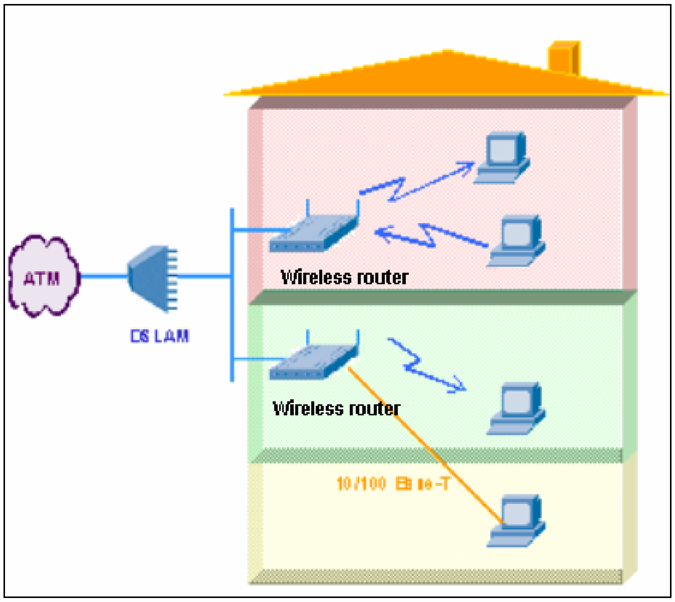
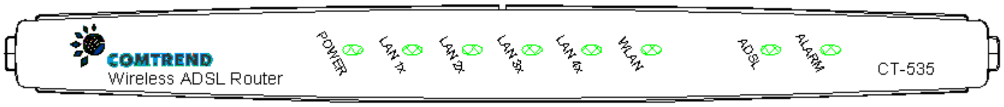


Figure 1-1 Application

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	The router is powered up
		Off	The router is powered down.
LAN 1x~4x	Green	On	Ethernet connection is established.
		Blink	Data transmitting or receiving
		Off	Ethernet connection is not established.
WLAN	Green	Blink	Data transmitting or receiving over WLAN
		Off	The wireless is not installed.
		On	The wireless module is ready and idle.
ADSL	Green	On	The ADSL connection is established.
		Off	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:

- ❑ **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.

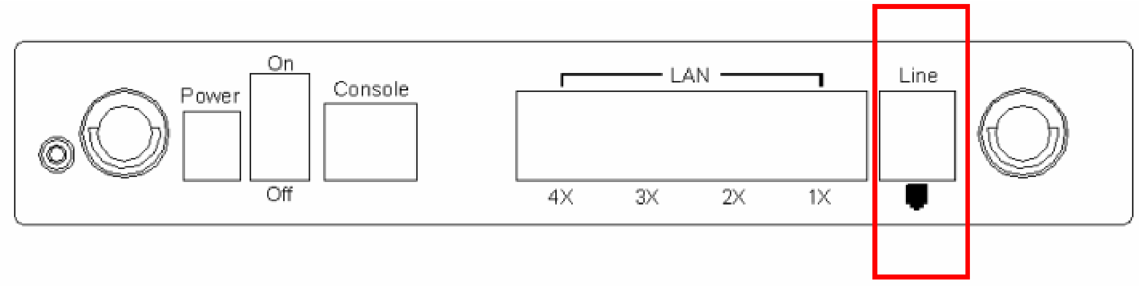
- ❑ **Optional micro filter and POTS splitter**

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

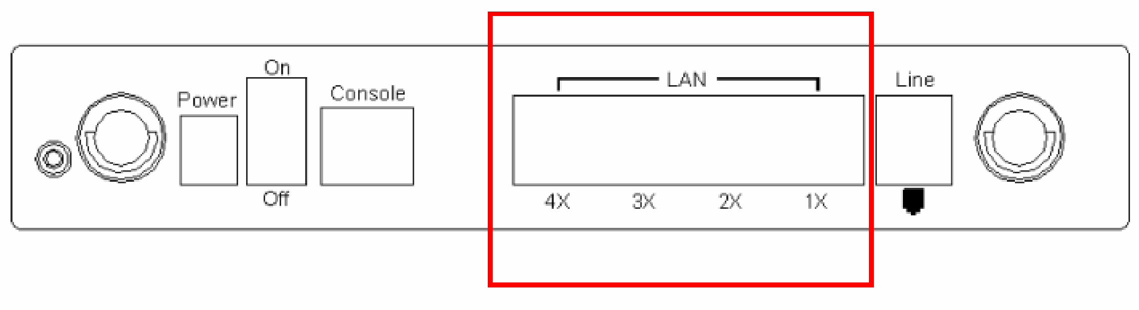
2.2 Hardware Installation

Follow the instructions below to complete the hardware connections.

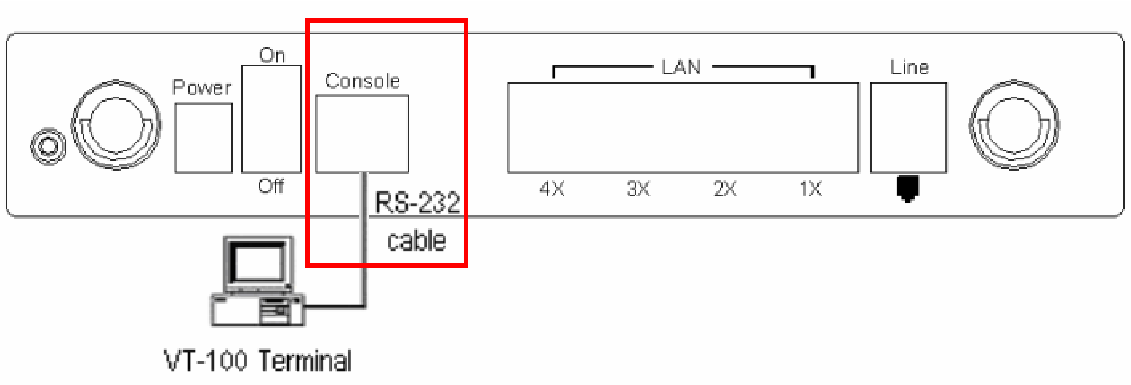
Step 1 Connect the **Line** port to a telephone-line using the supplied RJ-11 cable; or if you wish to connect both the router and a telephone, connect the ADSL port to a micro filter or POTS splitter with a RJ11 connection cable.



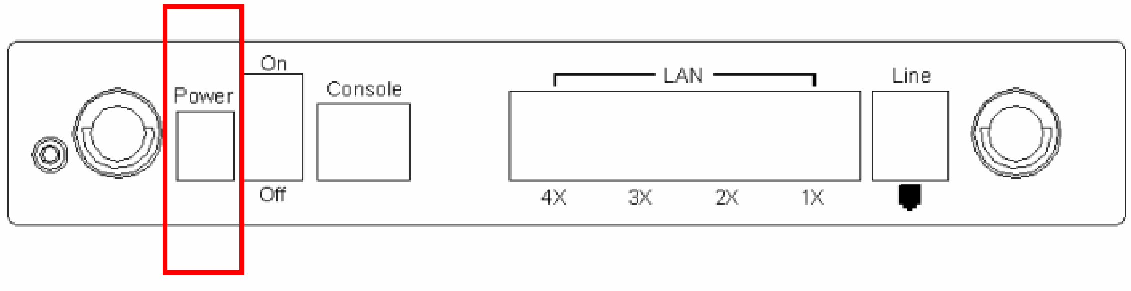
Step 2 To connect to a hub or PC, use a RJ45 cable. You can connect the router to four LAN devices. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.



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.

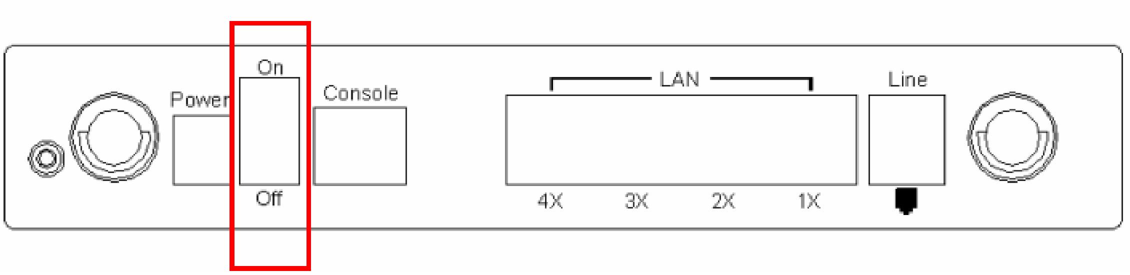


Step 4 Connect the **Power** jack to the shipped power cord.



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.

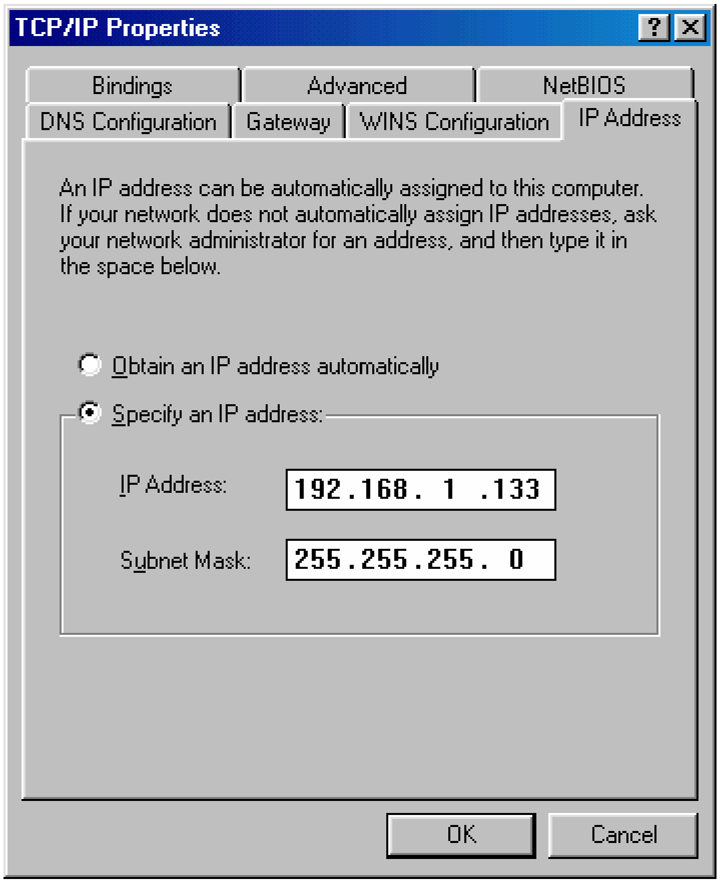
Chapter 3 Login via the Web Browser

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.

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).



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

IP Address: 192.168. 1 .133

Subnet Mask: 255.255.255. 0

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

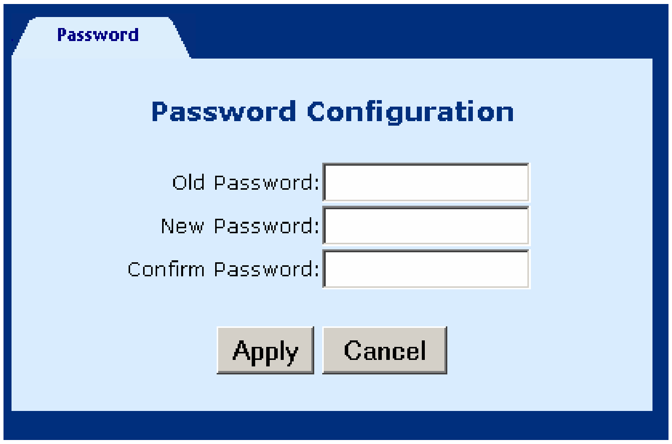
To log on to the system from the Web browser, follow the steps below:

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. Type the password, or if the password was not changed, type the default passwords. The default USER name is **root**, and the default password is **12345** (some versions require a login of 1234).

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



Password

Password Configuration

Old Password:

New Password:

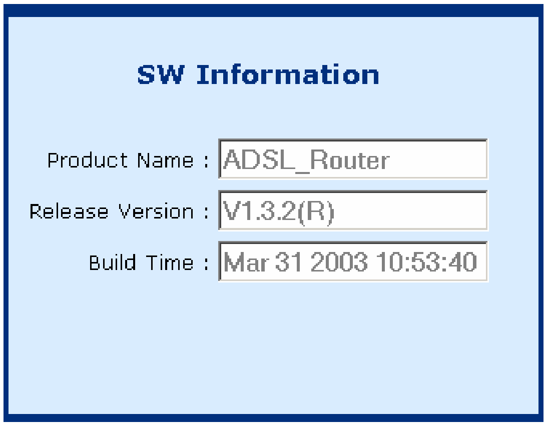
Confirm Password:

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.



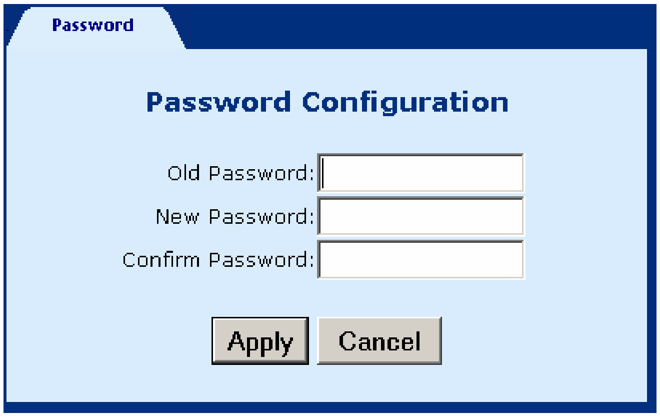
SW Information

Product Name : ADSL_Router

Release Version : V1.3.2(R)

Build Time : Mar 31 2003 10:53:40

4.2 Change the Password



Password Configuration

Old Password:

New Password:

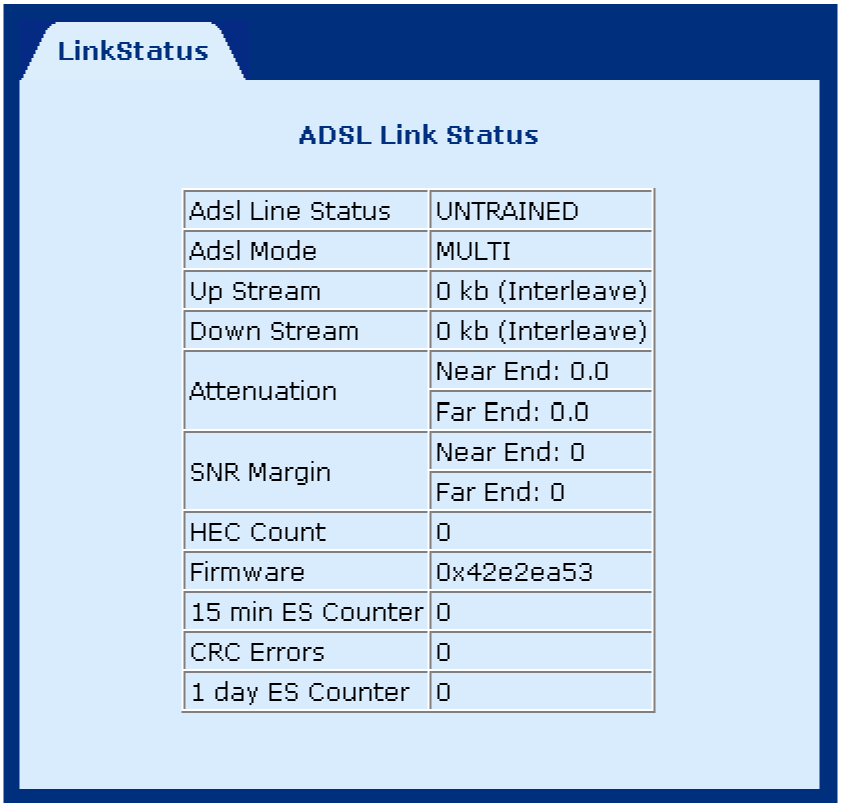
Confirm Password:

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:



LinkStatus

ADSL Link Status

Adsl Line Status	UNTRAINED
Adsl Mode	MULTI
Up Stream	0 kb (Interleave)
Down Stream	0 kb (Interleave)
Attenuation	Near End: 0.0
	Far End: 0.0
SNR Margin	Near End: 0
	Far End: 0
HEC Count	0
Firmware	0x42e2ea53
15 min ES Counter	0
CRC Errors	0
1 day ES Counter	0

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.

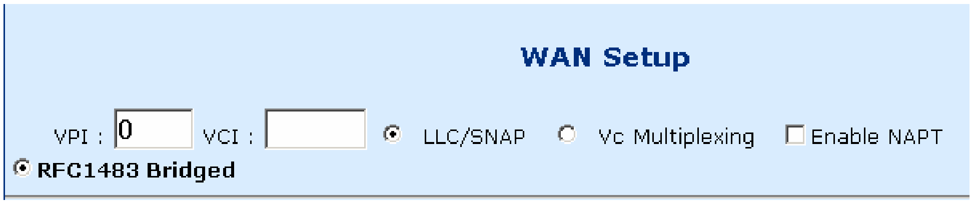
- VPI and VCI
- LLC Encapsulation: With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
- VC Multiplexing: With VC Multiplexing, no link control header 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.



WAN Setup

VPI : 0 VCI : ● LLC/SNAP ○ Vc Multiplexing □ Enable NAPT

● RFC1483 Bridged

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**.

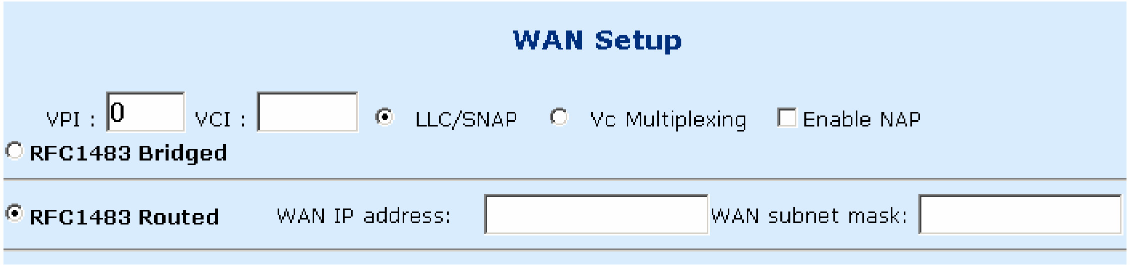
DELETE AN ENTRY

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.



WAN Setup

VPI : 0 VCI : ● LLC/SNAP ○ Vc Multiplexing □ Enable NAP

○ **RFC1483 Bridged**

● **RFC1483 Routed** WAN IP address: WAN subnet mask:

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**.

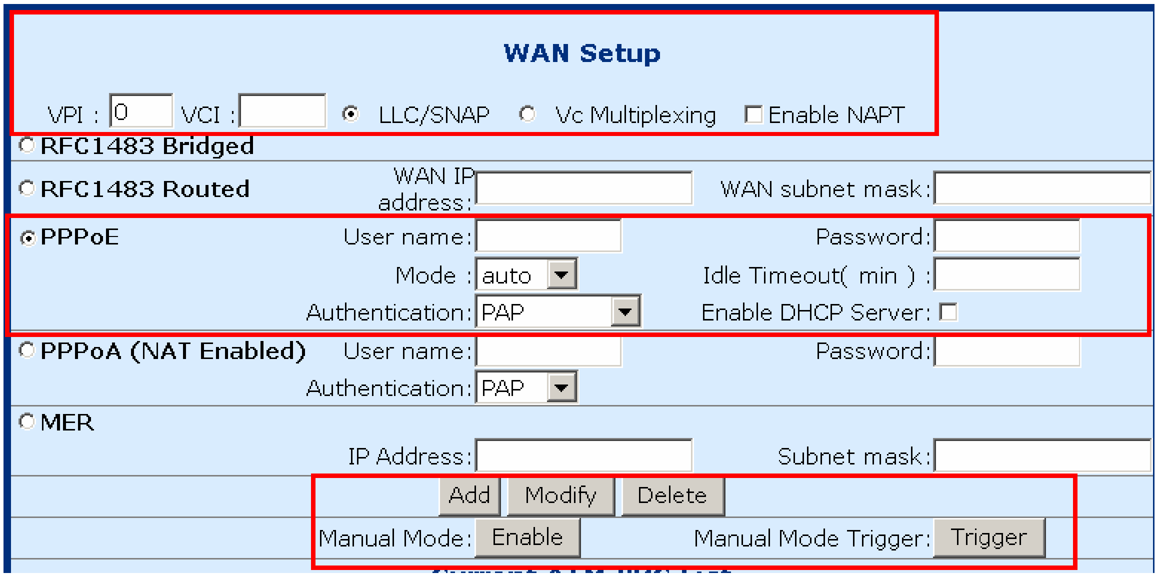
DELETE AN ENTRY

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 either 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.



WAN Setup

VPI : 0 VCI : ● LLC/SNAP ○ Vc Multiplexing □ Enable NAPT

○ RFC1483 Bridged

○ RFC1483 Routed WAN IP address: WAN subnet mask:

● PPPoE User name: Password:
Mode : auto Idle Timeout(min) :
Authentication: PAP Enable DHCP Server: □

○ PPPoA (NAT Enabled) User name: Password:
Authentication: PAP

○ MER
IP Address: Subnet mask:

Manual Mode: Manual Mode Trigger:

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, c**licking 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, and CHAP
- ◆ **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

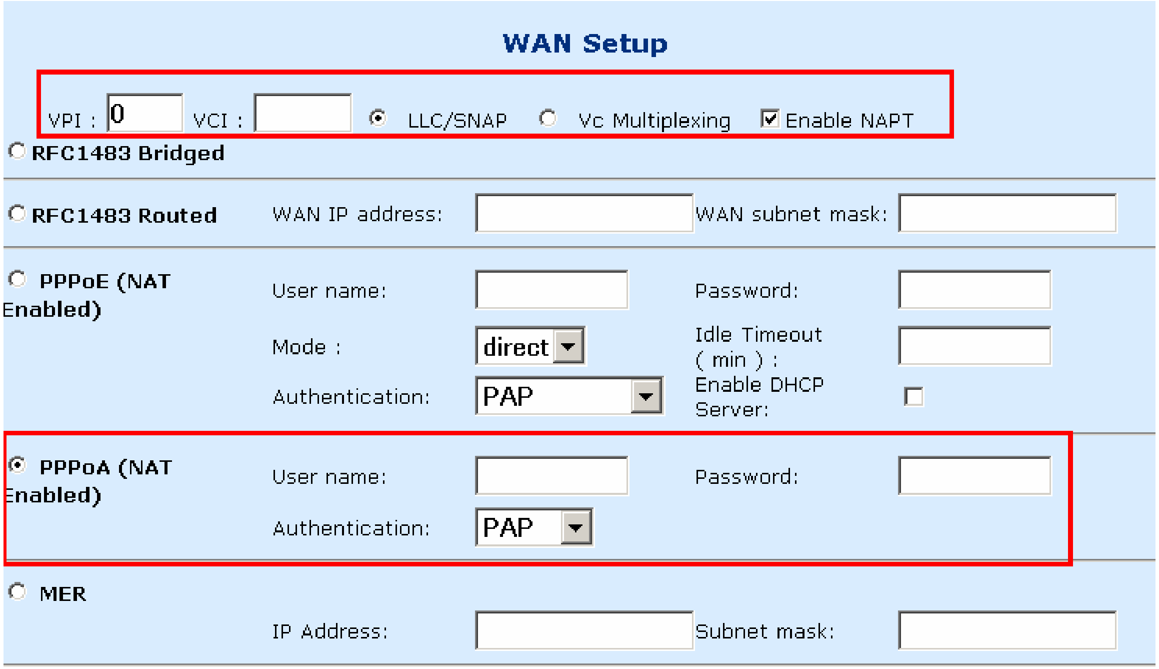
To delete an entry, Select it from the **Current ATM PVC List,** at the bottom of the WAN Setup page, and click the **Delete** button.

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. The **Authentication** field defines the authentication code: PAP or CHAP.
- **Authentication:** defines the authentication code (PAP, CHAP).



WAN Setup

VPI : 0 VCI : ● LLC/SNAP ○ Vc Multiplexing ☑ Enable NAPT

○ RFC1483 Bridged

○ RFC1483 Routed WAN IP address: WAN subnet mask:

○ PPPoE (NAT Enabled) User name: Password:
Mode : direct Idle Timeout (min) :
Authentication: PAP Enable DHCP Server: □

● PPPoA (NAT Enabled) User name: Password:
Authentication: PAP

○ MER IP Address: Subnet mask:

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**.

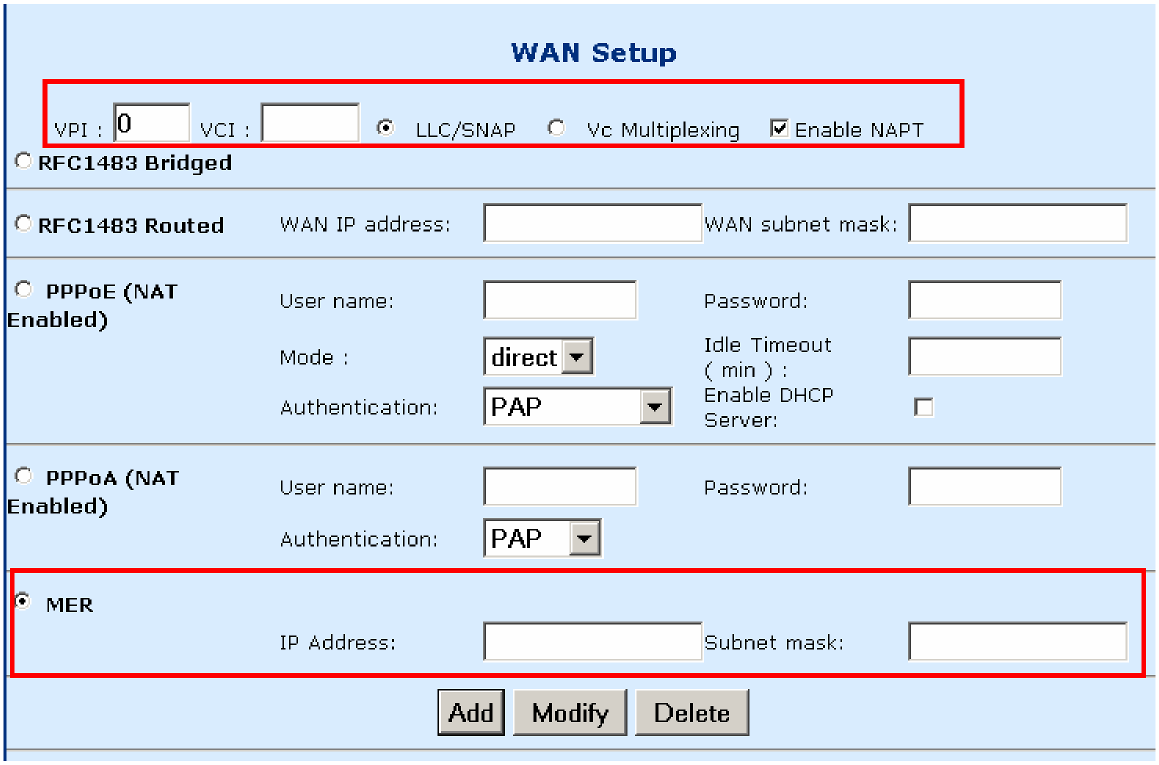
DELETE AN ENTRY

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.



WAN Setup

VPI : 0 VCI : ● LLC/SNAP ○ Vc Multiplexing ☑ Enable NAPT

○ RFC1483 Bridged

○ RFC1483 Routed WAN IP address: WAN subnet mask:

○ PPPoE (NAT Enabled) User name: Password:
Mode : direct Idle Timeout (min) :
Authentication: PAP Enable DHCP Server: □

○ PPPoA (NAT Enabled) User name: Password:
Authentication: PAP

● MER IP Address: Subnet mask:

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.

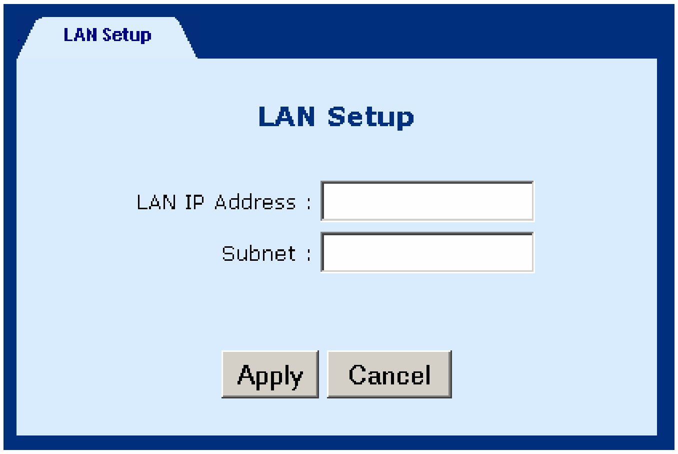
STEP 2: Change the parameters.

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.

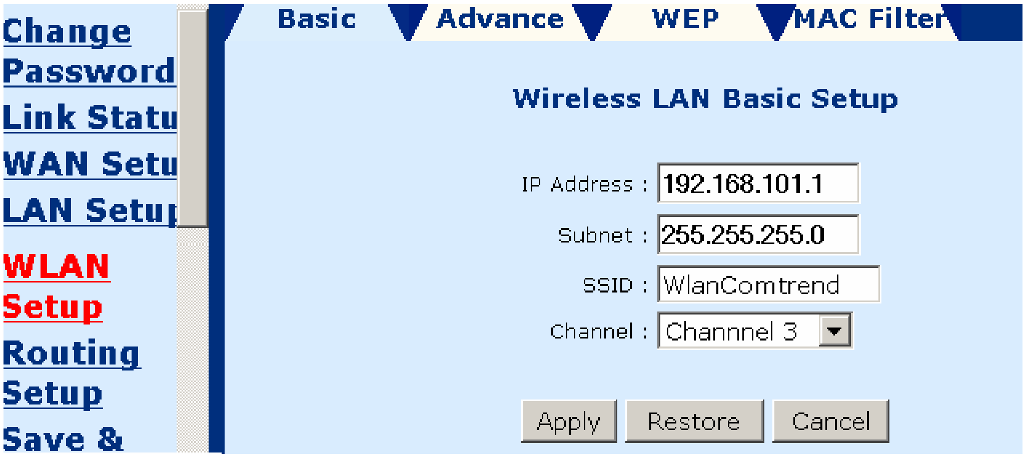
4.5 LAN IP Address

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 three menus: WLAN Basic, WLAN Advanced, and WLAN WEP. Each of these menus will be covered below.



Wireless LAN Basic Setup

IP Address : 192.168.101.1

Subnet : 255.255.255.0

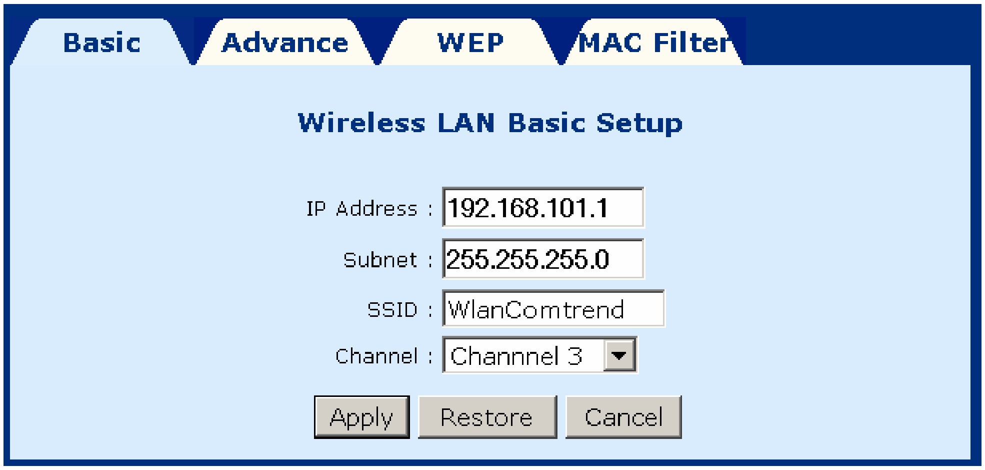
SSID : WlanComtrend

Channel : Channnel 3

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.



Wireless LAN Basic Setup

IP Address : 192.168.101.1

Subnet : 255.255.255.0

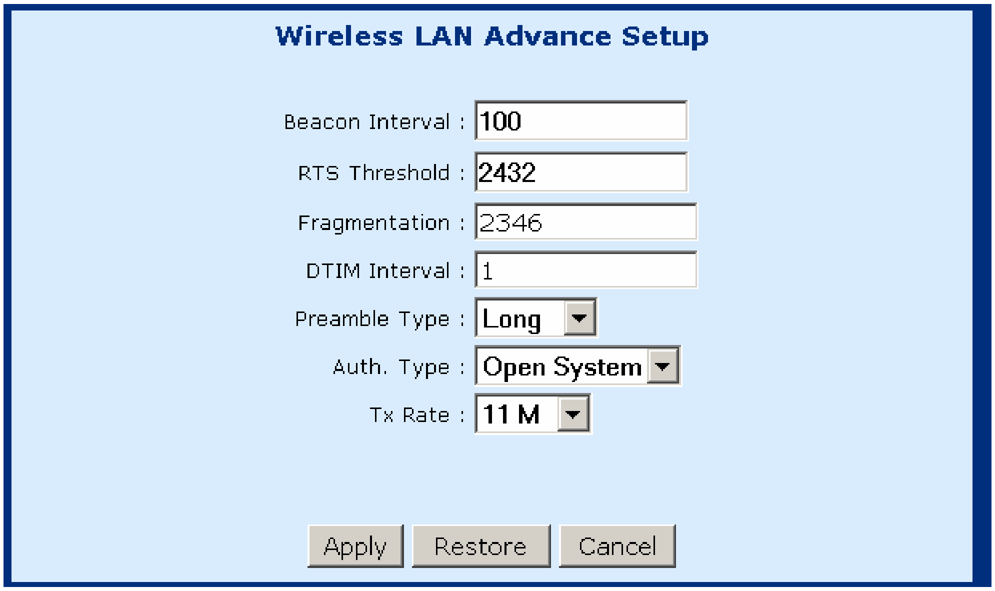
SSID : WlanComtrend

Channel : Channnel 3

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], **Shared Key** [select this option if you wish to enable WEP security], if you select **both,** then both Open System and Shared Key will be simultaneously enabled.
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).



Wireless LAN Advance Setup

Beacon Interval : 100

RTS Threshold : 2432

Fragmentation : 2346

DTIM Interval : 1

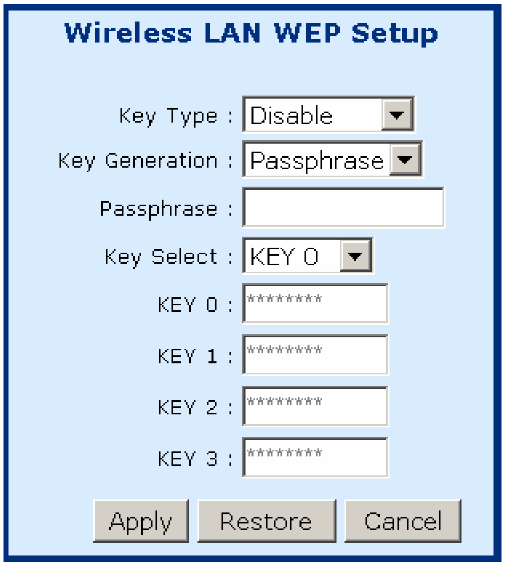
Preamble Type : Long

Auth. Type : Open System

Tx Rate : 11 M

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.



Wireless LAN WEP Setup

Key Type : Disable

Key Generation : Passphrase

Passphrase :

Key Select : KEY 0

KEY 0 : *********

KEY 1 : *********

KEY 2 : *********

KEY 3 : *********

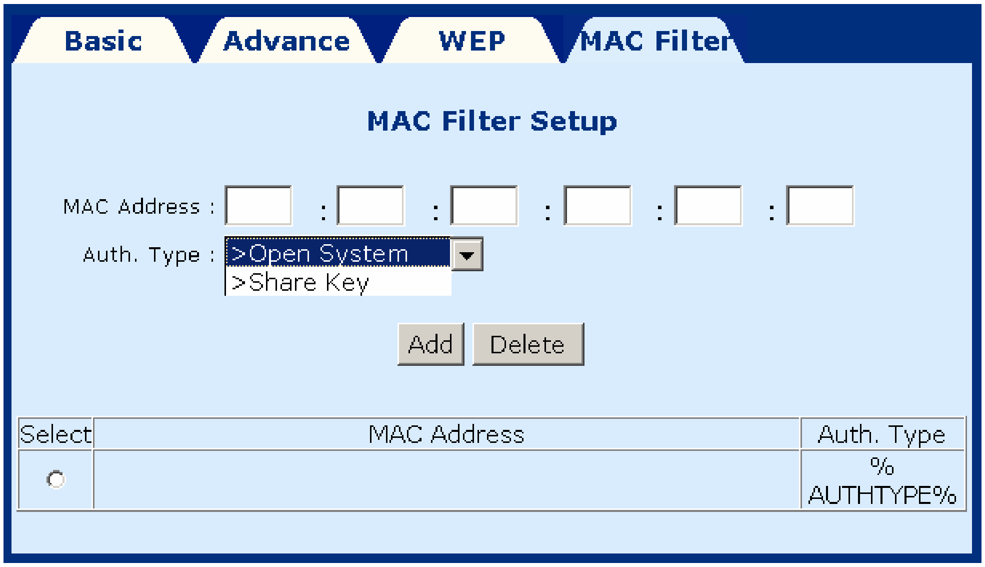
Key Type	**Disabled, 64 bits, 128 bits**. This parameter determines the level of security. Disabled means no security, 128 bits provides the highest security. This parameter must match with the remote-clients.
Key Generation	Select **Passphrase** to enable automatic key generation, or **Manual** to manually enter each key
Passphrase	Enter a Passphrase if you wish clients to require a Passphrase to connect with the access point.
KeySelect	Select a Key from 0~3. This key will be the active hexadecimal password for access.
Key 0~3	If you are using a manual Passphrase enter a hexadecimal password for each key. This hexadecimal 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 access to be restricted/enabled based on a MAC address. Enter the following parameters and then click the **Add** button.

MAC address: Enter the MAC address of the access point.

Auth Type: enter **Open System** to allow unrestricted access to the access point, or **Share Key** to require confirmation with the parameters of the WEP security keys (Click the WEP tab to verify these settings).



MAC Filter Setup

MAC Address : ____ : ____ : ____ : ____ : ____ : ____

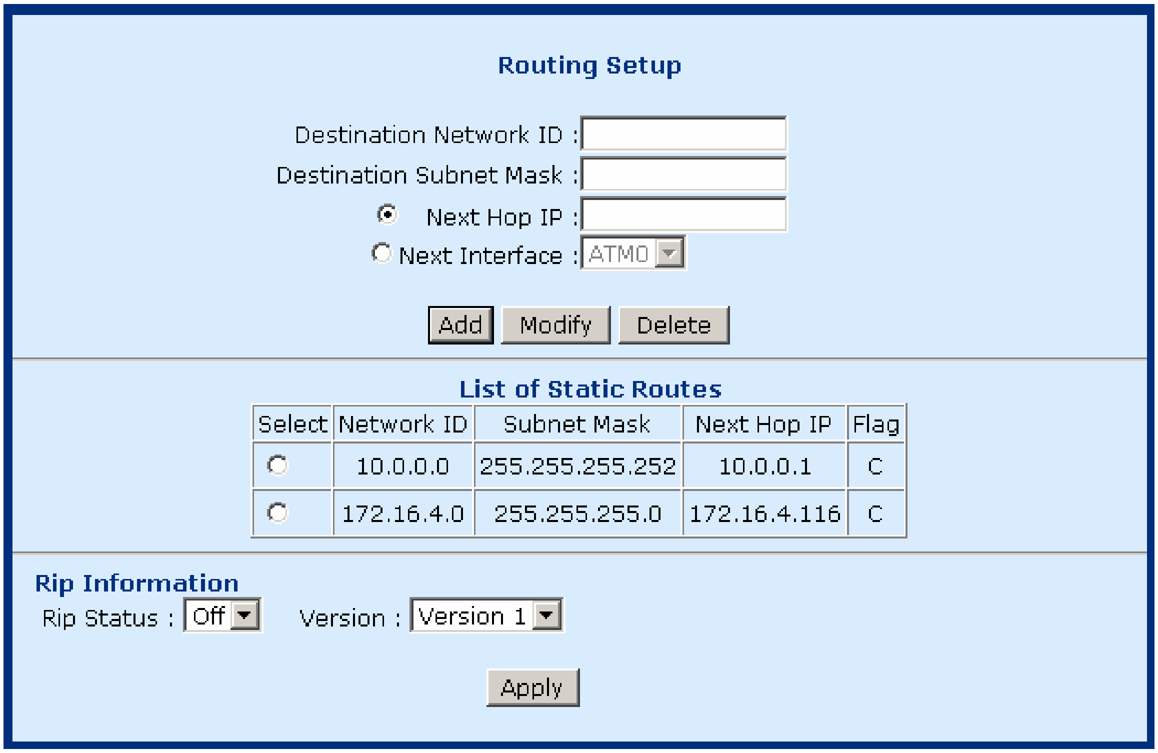
Auth. Type : >Open System
>Share Key

Select	MAC Address	Auth. Type
○		% AUTHTYPE%

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. You can display the RIP information by clicking the **RIP information** button.



Routing Setup

Destination Network ID :

Destination Subnet Mask :

● Next Hop IP :

○ Next Interface : ATM0

List of Static Routes

Select	Network ID	Subnet Mask	Next Hop IP	Flag
○	10.0.0.0	255.255.255.252	10.0.0.1	C
○	172.16.4.0	255.255.255.0	172.16.4.116	C

Rip Information

Rip Status : Off　Version : Version 1

4.7.1 Enable RIP

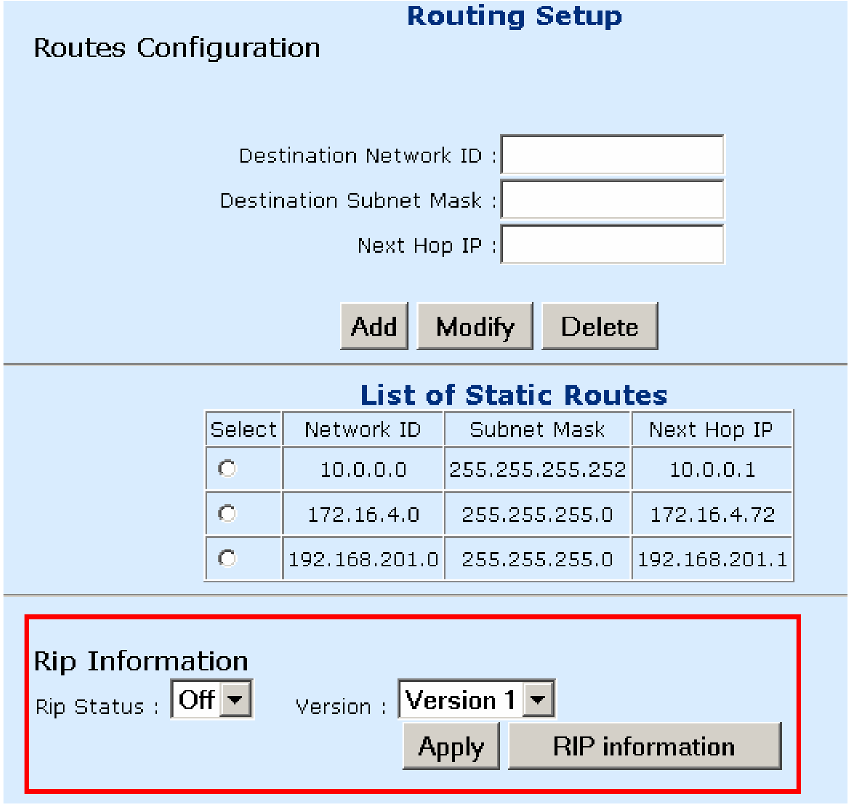
To enable the RIP, complete the following steps:

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.



Routing Setup

Routes Configuration

Destination Network ID :

Destination Subnet Mask :

Next Hop IP :

List of Static Routes

Select	Network ID	Subnet Mask	Next Hop IP
○	10.0.0.0	255.255.255.252	10.0.0.1
○	172.16.4.0	255.255.255.0	172.16.4.72
○	192.168.201.0	255.255.255.0	192.168.201.1

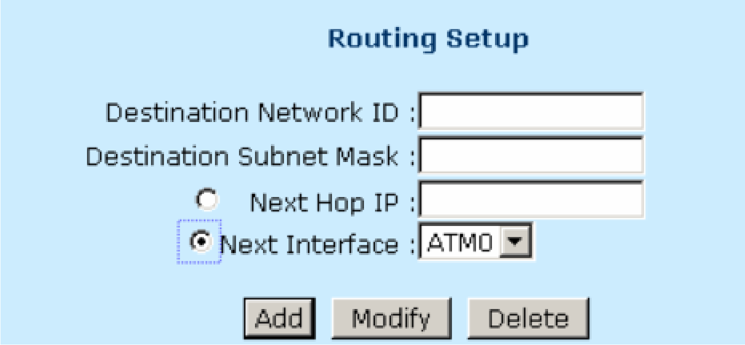
Rip Information

Rip Status : Off

Version : Version 1

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.



Routing Setup

Destination Network ID :

Destination Subnet Mask :

○ Next Hop IP :

● Next Interface : ATM0

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:

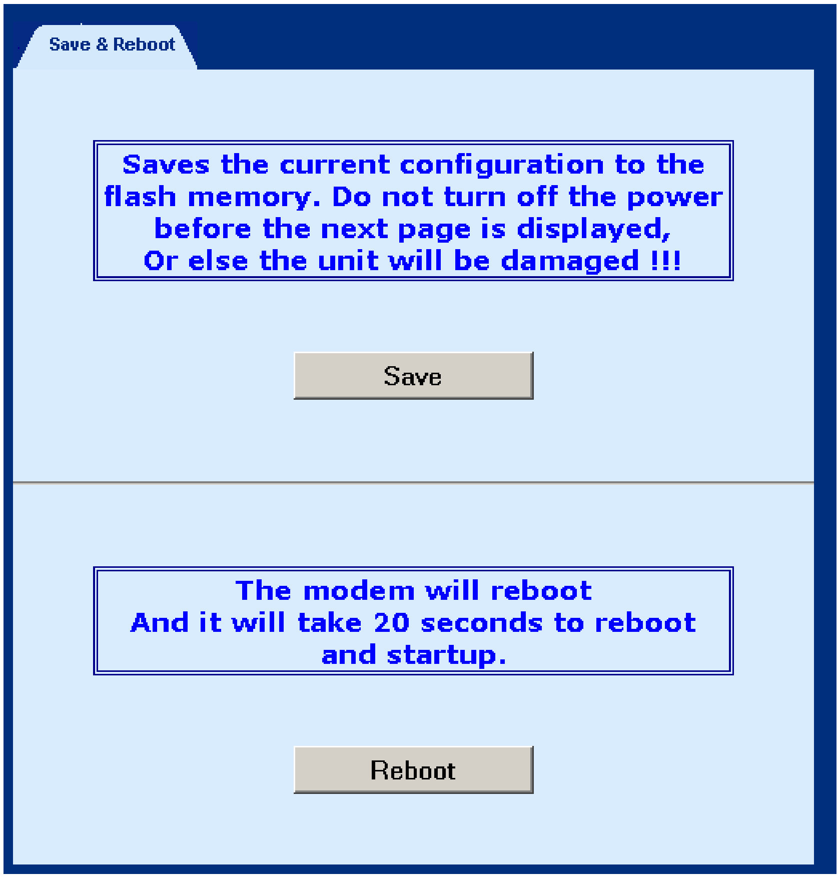
STEP 1: Select the entry you wish to **delete** from the List of Static Routes

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**.

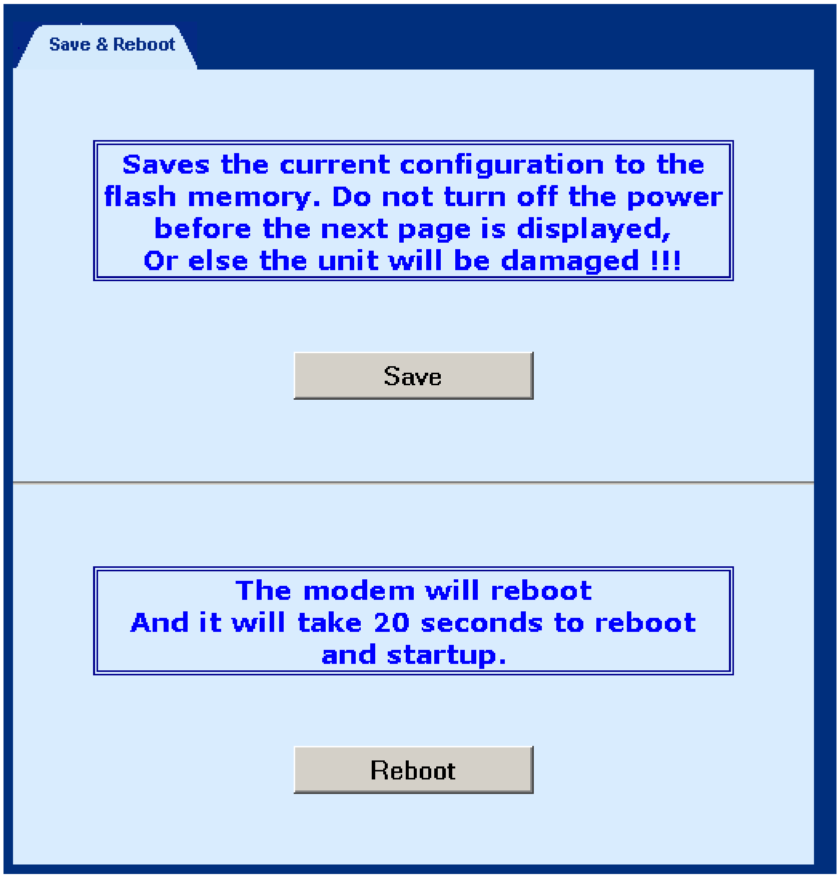


Saves the current configuration to the flash memory. Do not turn off the power before the next page is displayed, Or else the unit will be damaged !!!

The modem will reboot And it will take 20 seconds to reboot and startup.

4.9 Reboot

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

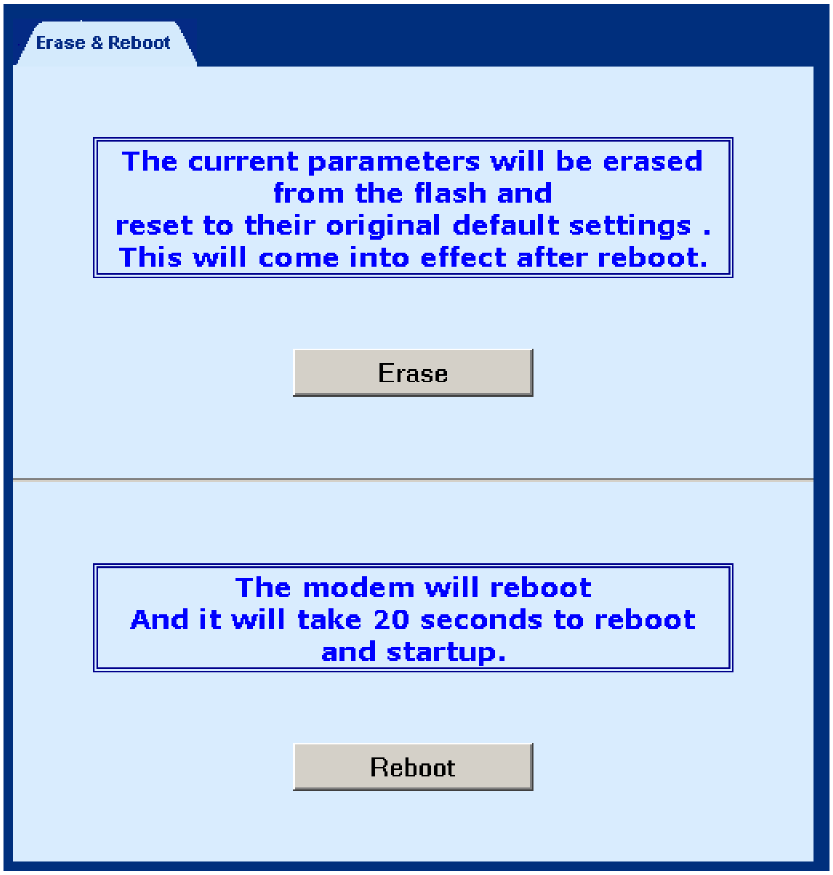


Saves the current configuration to the flash memory. Do not turn off the power before the next page is displayed,
Or else the unit will be damaged !!!

The modem will reboot
And it will take 20 seconds to reboot and startup.

4.10 Retrieve default settings

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



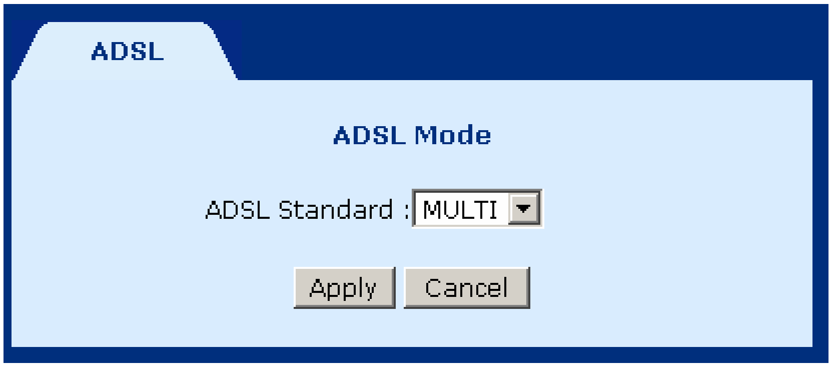
The current parameters will be erased from the flash and
reset to their original default settings .
This will come into effect after reboot.

The modem will reboot
And it will take 20 seconds to reboot and startup.

Chapter 5 WEB Advanced Configuration

5.1 ADSL Mode

The ADSL modes are: ANSI, G.DMT, G.LITE, MULTI. MULTI mode enables the device to auto-adjust its mode to match the remote CO DLSAM. You can specify an ADSL mode on this page, and click the Apply button to submit the settings.



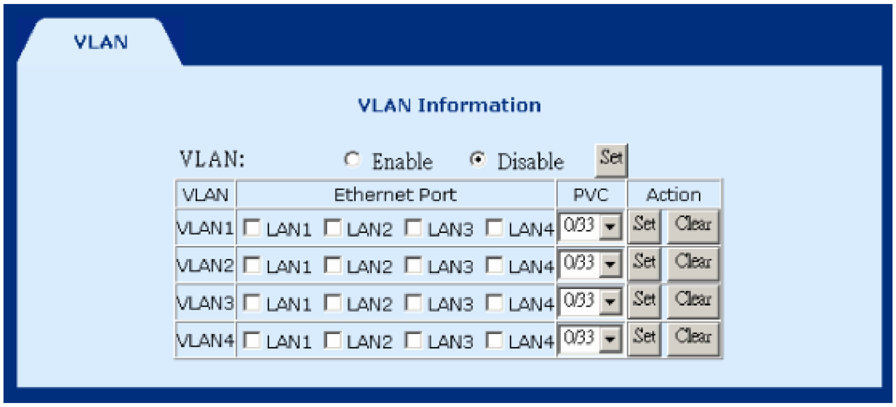
ADSL Standard : MULTI

5.2 VLAN

To configure the VLAN function, click **VLAN** from the Advanced menu bar. VLAN is disabled by factory default. To enable it, tick **Enable** and click the **Set** button. Then you can proceed to create the VLAN groups. The ATU-R supports four VLAN groups, VLAN groups 1 to 4. You can choose and join different Ethernet ports to the PVC running in RFC 1483 bridged mode. Packets will be transmitted or received from these ports to the appointed PVC. The packets of the VLAN groups are not routable. Packets that don't belong to the VLAN group are routable.

Parameters and buttons

The PVC field displays the options of the PVCs set up in RFC 1483 Bridged mode (refer to section 5.4, WAN Setup). Click the Set button to apply the settings, or click the Clear button to delete a VLAN group.



VLAN: ○ Enable ● Disable Set

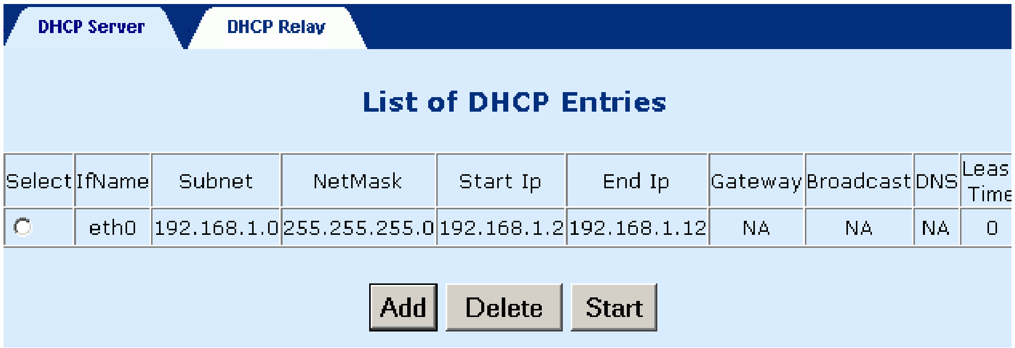
VLAN	Ethernet Port	PVC	Action
VLAN1	☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4	0/33	Set Clear
VLAN2	☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4	0/33	Set Clear
VLAN3	☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4	0/33	Set Clear
VLAN4	☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4	0/33	Set Clear

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 function of the device is disabled by factory default.

5.3.1 Enable DHCP

STEP 1: Click the **DHCP** tab.



List of DHCP Entries

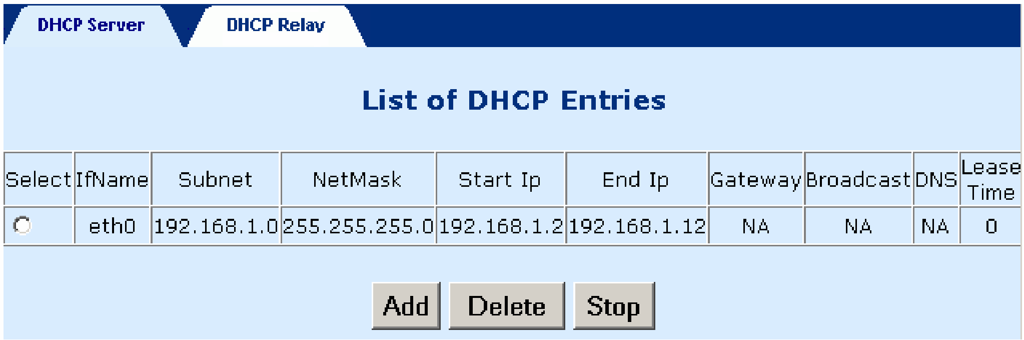
Select	IfName	Subnet	NetMask	Start Ip	End Ip	Gateway	Broadcast	DNS	Leas Time
○	eth0	192.168.1.0	255.255.255.0	192.168.1.2	192.168.1.12	NA	NA	NA	0

STEP 2: Chose the entry and click the **Start** button

5.3.2 Disable DHCP

STEP 1: Click the **DHCP** tab.

STEP 2: Chose the entry and click the **Stop** button

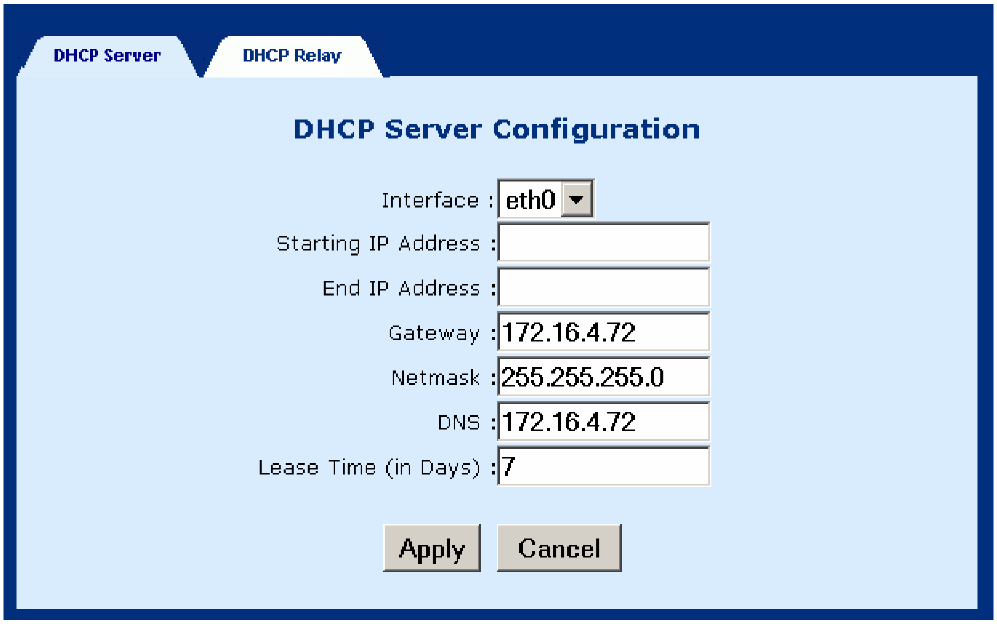


List of DHCP Entries

Select	IfName	Subnet	NetMask	Start Ip	End Ip	Gateway	Broadcast	DNS	Lease Time
○	eth0	192.168.1.0	255.255.255.0	192.168.1.2	192.168.1.12	NA	NA	NA	0

5.3.3 Add a DHCP Entry

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



DHCP Server Configuration

Interface :	eth0
Starting IP Address :	
End IP Address :	
Gateway :	172.16.4.72
Netmask :	255.255.255.0
DNS :	172.16.4.72
Lease Time (in Days) :	7

- **Interface: eth0 only.** This displays the interface that will provide the DHCP function.
- **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
- **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.

5.3.4 Disable DHCP

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

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

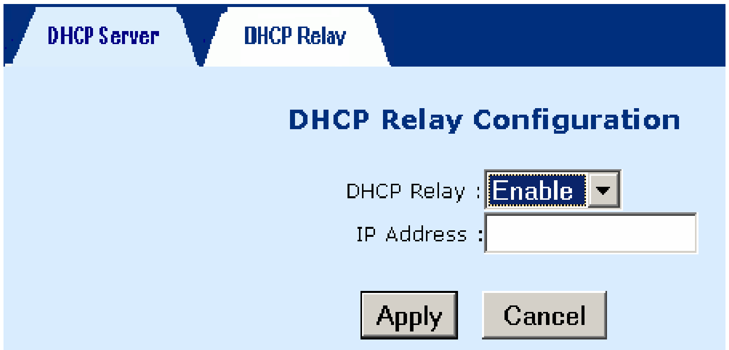
5.4 DHCP Relay

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.



DHCP Relay Configuration

DHCP Relay : Enable

IP Address :

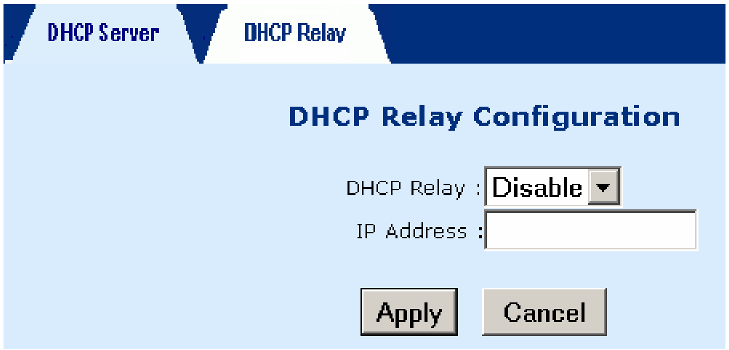
STEP 2: In the DHCP Relay field, select **Enable**, and enter the IP Address you want to receive BOOT REQUEST or DHCP packets from clients.

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.



DHCP Relay Configuration

DHCP Relay : Disable

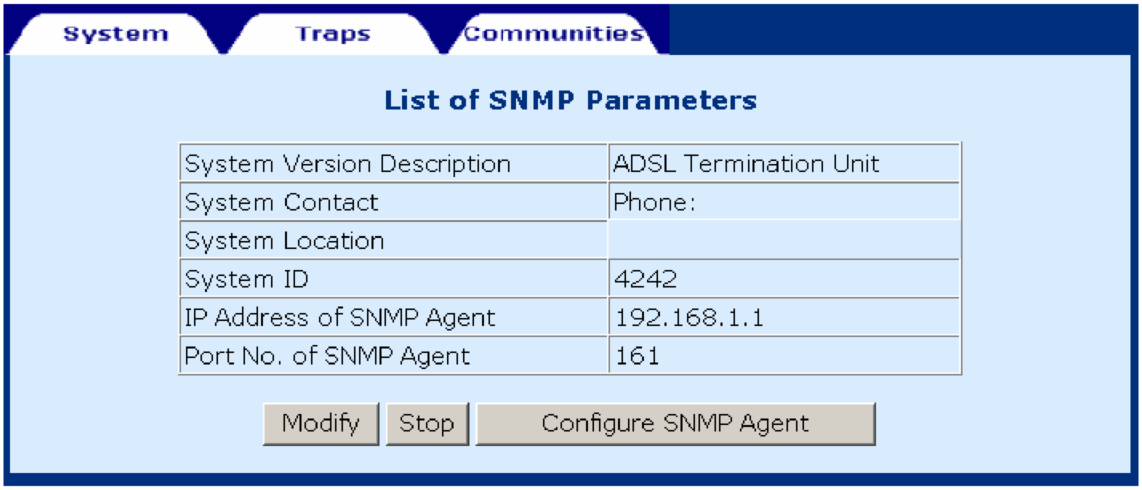
IP Address :

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 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.

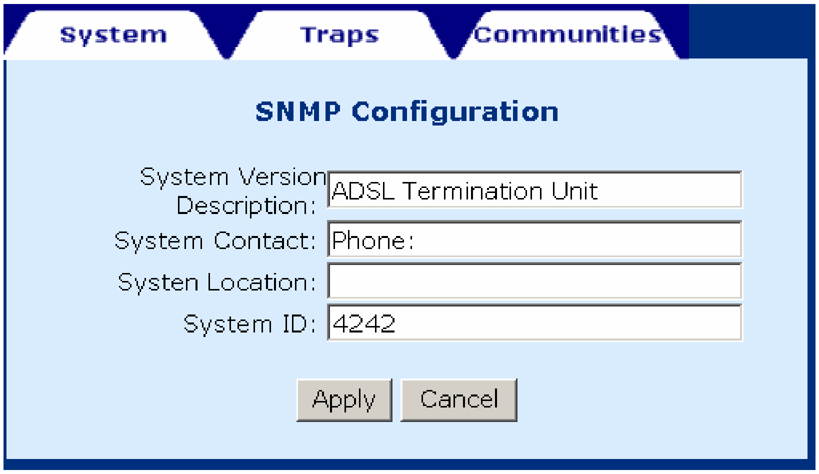


List of SNMP Parameters

System Version Description	ADSL Termination Unit
System Contact	Phone:
System Location	
System ID	4242
IP Address of SNMP Agent	192.168.1.1
Port No. of SNMP Agent	161

5.5.1 Modifying SNMP Parameters

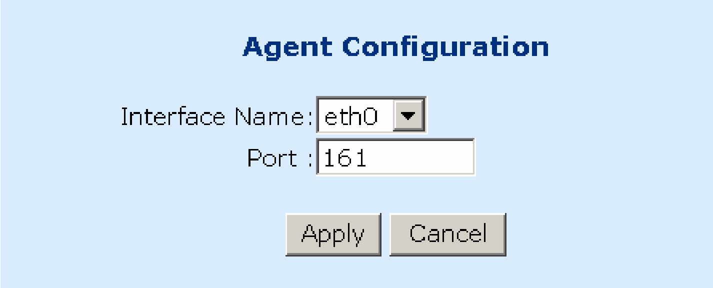
To modify the SNMP parameters, click the Modify button at the bottom of the screen. Click Apply to submit the settings.



SNMP Configuration

System Version Description: ADSL Termination Unit
System Contact: Phone:
Systen Location:
System ID: 4242

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

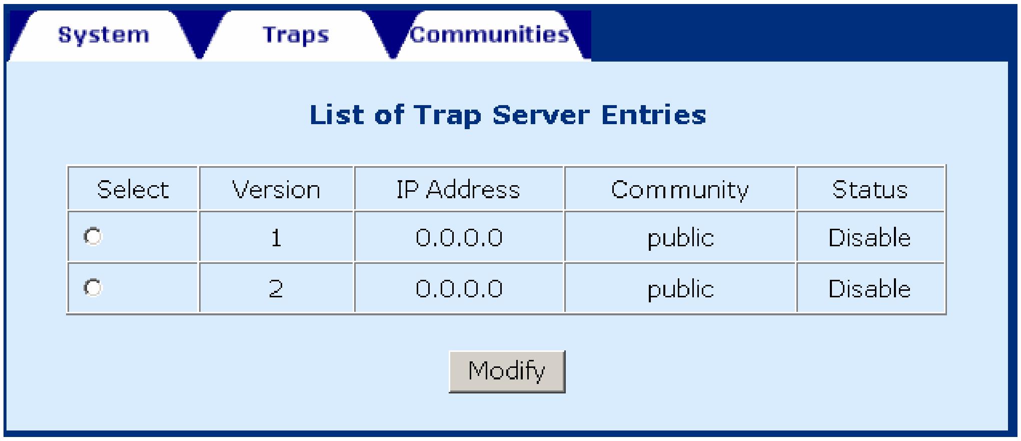


Agent Configuration

Interface Name: eth0
Port : 161

5.5.2 Modifying Traps

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

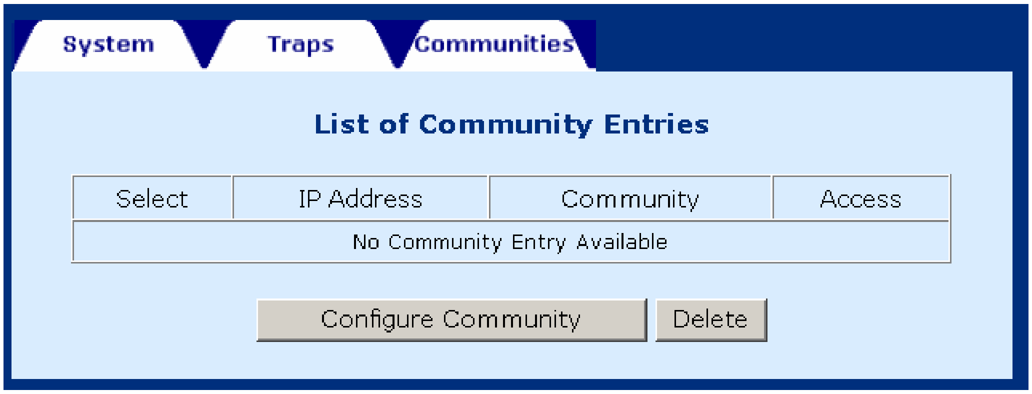


List of Trap Server Entries

Select	Version	IP Address	Community	Status
○	1	0.0.0.0	public	Disable
○	2	0.0.0.0	public	Disable

5.5.3 Modifying Communities

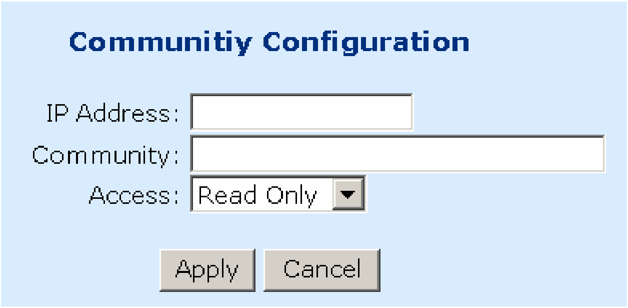
Click the Communities tab to display the community entry. After filling out the parameters, click Submit to apply the settings.



List of Community Entries

Select	IP Address	Community	Access
No Community Entry Available			

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.



Communitiy Configuration

IP Address:

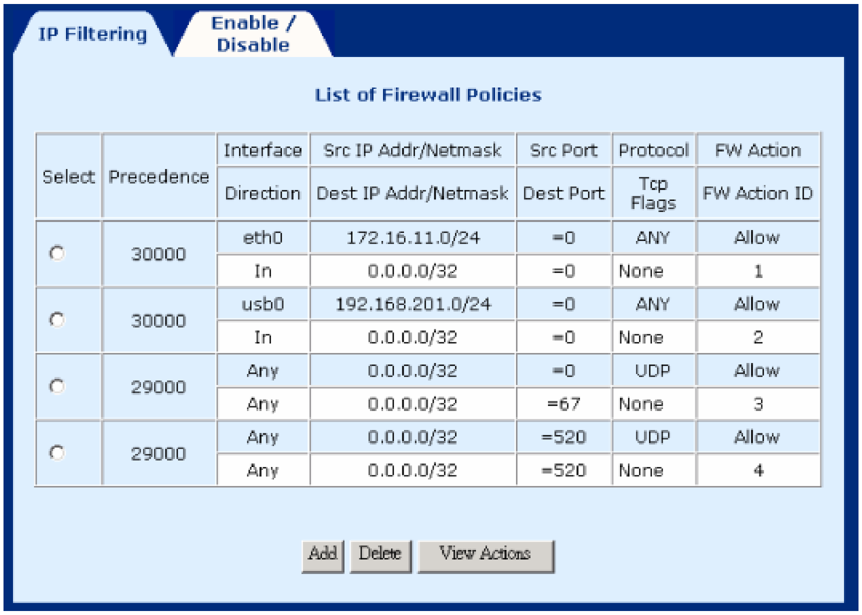
Community:

Access: Read Only

5.6 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. Each of theses actions will be discussed below.

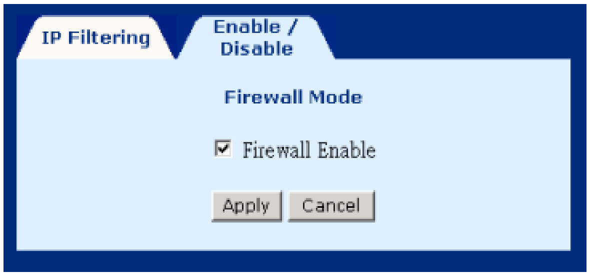


List of Firewall Policies

Select	Precedence	Interface	Src IP Addr/Netmask	Src Port	Protocol	FW Action
		Direction	Dest IP Addr/Netmask	Dest Port	Tcp Flags	FW Action ID
○	30000	eth0	172.16.11.0/24	=0	ANY	Allow
		In	0.0.0.0/32	=0	None	1
○	30000	usb0	192.168.201.0/24	=0	ANY	Allow
		In	0.0.0.0/32	=0	None	2
○	29000	Any	0.0.0.0/32	=0	UDP	Allow
		Any	0.0.0.0/32	=67	None	3
○	29000	Any	0.0.0.0/32	=520	UDP	Allow
		Any	0.0.0.0/32	=520	None	4

5.6.1 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.



Firewall Mode

☑ Firewall Enable

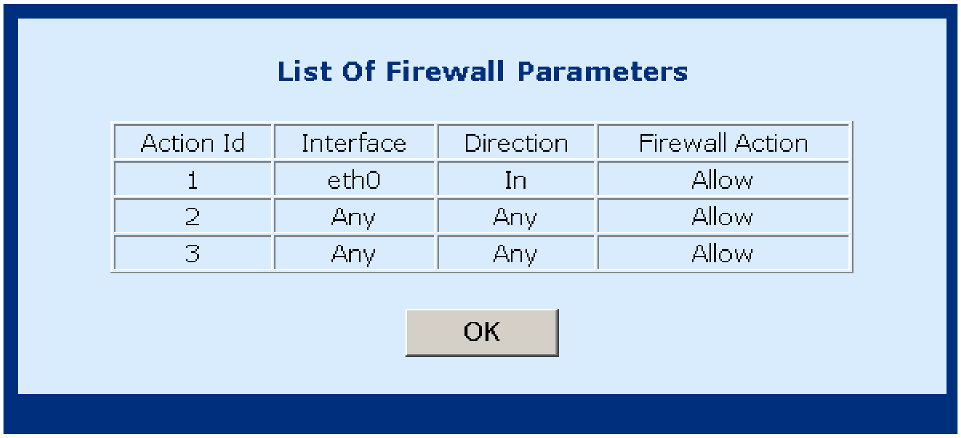
5.6.2 View Firewall Actions

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.

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.



List Of Firewall Parameters

Action Id	Interface	Direction	Firewall Action
1	eth0	In	Allow
2	Any	Any	Allow
3	Any	Any	Allow

5.6.3 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

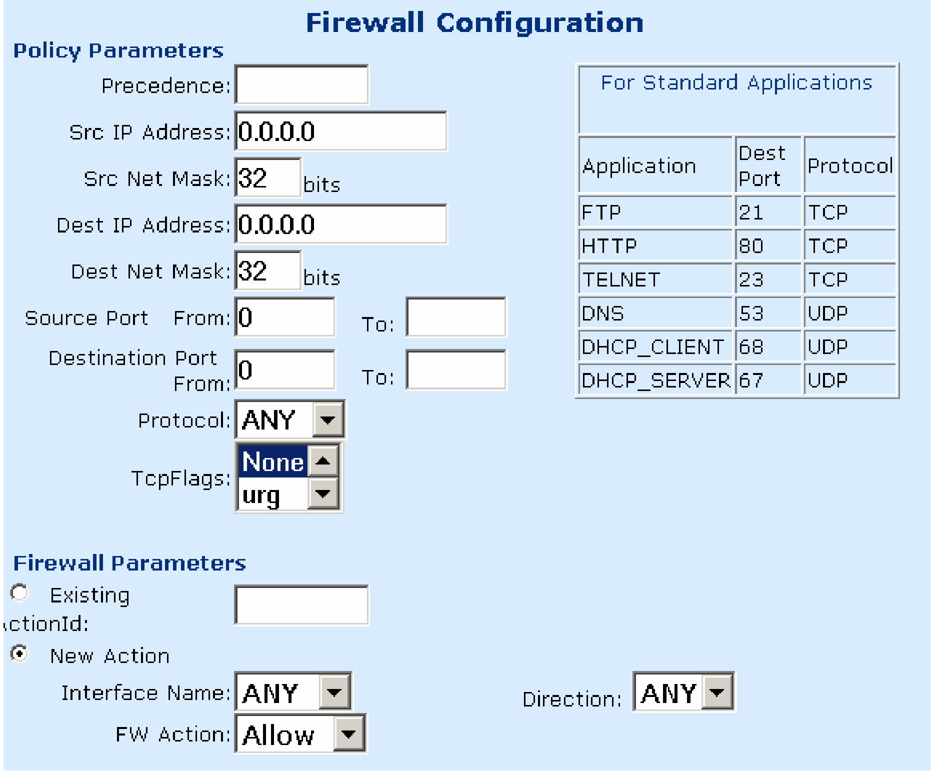
TCP Flags: Select the TCP FLAG from the following: none, urg, ack, psh, rst, syn, fin.

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.



Firewall Configuration

Policy Parameters

Precedence:

Src IP Address: 0.0.0.0

Src Net Mask: 32 bits

Dest IP Address: 0.0.0.0

Dest Net Mask: 32 bits

Source Port From: 0 To:

Destination Port From: 0 To:

Protocol: ANY

TcpFlags: None urg

For Standard Applications

Application	Dest Port	Protocol
FTP	21	TCP
HTTP	80	TCP
TELNET	23	TCP
DNS	53	UDP
DHCP_CLIENT	68	UDP
DHCP_SERVER	67	UDP

Firewall Parameters

○ Existing ctionId:

● New Action

Interface Name: ANY

Direction: ANY

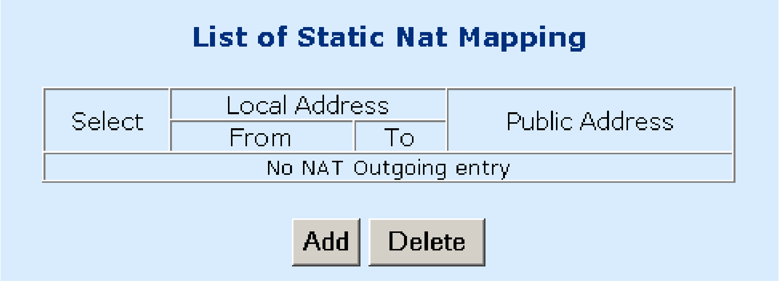
FW Action: Allow

5.7 NAT

The NAT function can be accessed by clicking the **NAT** tab on the **Advanced** menu. From this screen you can add or delete a Static Wan Address, static NAT mapping or Port Range Mapping.

5.7.1 Static NAT Mapping

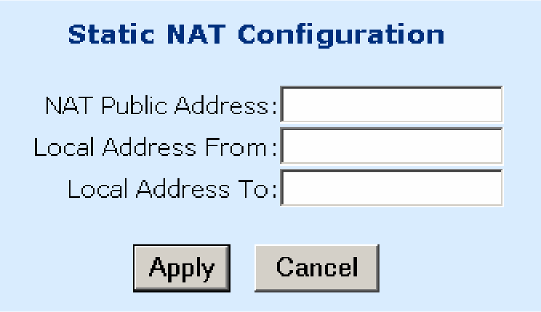
Any Static NAT mapping entries that are set up will be listed, click on the **Add** button add a new entry or select an entry and click on the **Delete** button.



List of Static Nat Mapping

Select	Local Address		Public Address
	From	To	
No NAT Outgoing entry			

Add an Entry
To add an entry click on the **Add** button, enter the Public IP Address you wish to set for NAT, enter the Local Address From (starting point for the range), enter the Local Address To (end point for the range), and then click on the **Apply** button.

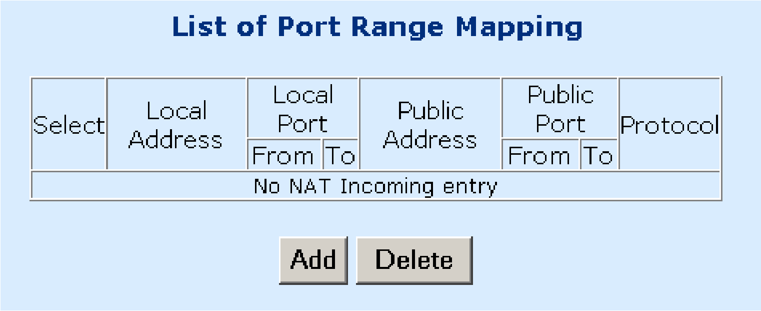


Static NAT Configuration

NAT Public Address:
Local Address From:
Local Address To:

5.7.2 Static Port Mapping

Any Static WAN address that are set up will be listed, click on the **Add** button add a new entry or select an entry and click on the **Delete** button.



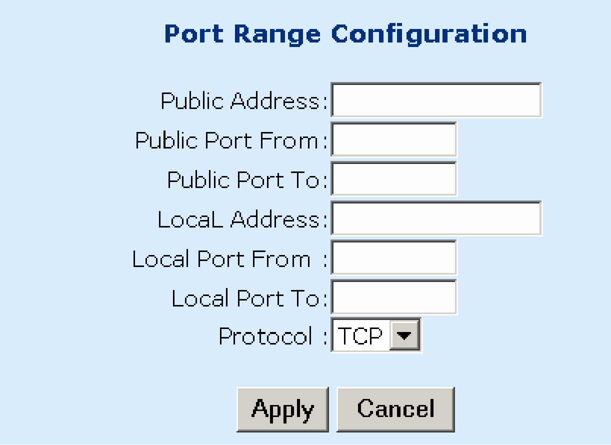
List of Port Range Mapping

Select	Local Address	Local Port		Public Address	Public Port		Protocol
		From	To		From	To	
No NAT Incoming entry							

Add an Entry

To add an entry click on the **Add** button, and then enter the following information, and then click on the **Apply** button:

Public IP Address: Enter the you wish to set the Public port range
Public Port From: Enter the starting port for the Public port-range
Public Port To: Enter the last port for the Public port-range
Local Address: Enter the Local address
Local Port From: Enter the starting port for the Local port-range
Local Port to: Enter the last port for the Local port-range
Protocol: Select UDP or TCP

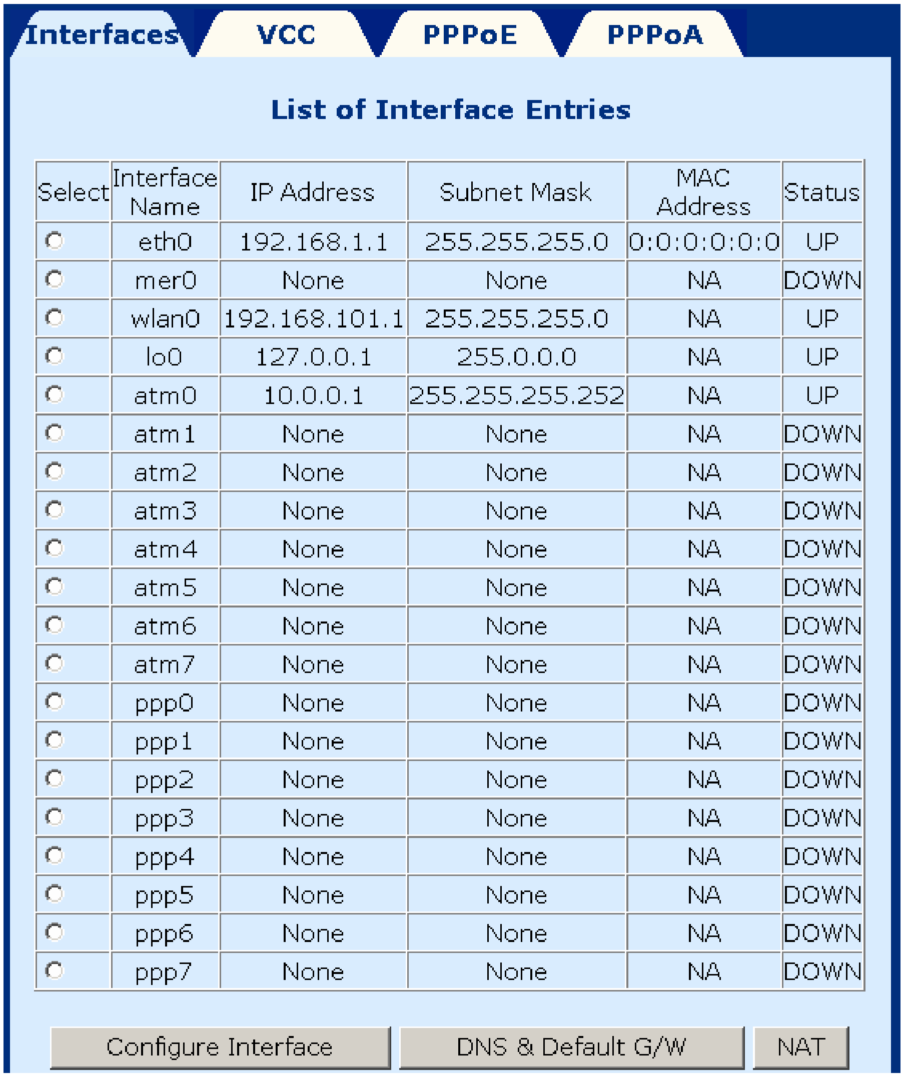


Port Range Configuration

Public Address:
Public Port From:
Public Port To:
LocaL Address:
Local Port From :
Local Port To:
Protocol : TCP

5.8 Configure

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



List of Interface Entries

Select	Interface Name	IP Address	Subnet Mask	MAC Address	Status
○	eth0	192.168.1.1	255.255.255.0	0:0:0:0:0:0	UP
○	mer0	None	None	NA	DOWN
○	wlan0	192.168.101.1	255.255.255.0	NA	UP
○	lo0	127.0.0.1	255.0.0.0	NA	UP
○	atm0	10.0.0.1	255.255.255.252	NA	UP
○	atm1	None	None	NA	DOWN
○	atm2	None	None	NA	DOWN
○	atm3	None	None	NA	DOWN
○	atm4	None	None	NA	DOWN
○	atm5	None	None	NA	DOWN
○	atm6	None	None	NA	DOWN
○	atm7	None	None	NA	DOWN
○	ppp0	None	None	NA	DOWN
○	ppp1	None	None	NA	DOWN
○	ppp2	None	None	NA	DOWN
○	ppp3	None	None	NA	DOWN
○	ppp4	None	None	NA	DOWN
○	ppp5	None	None	NA	DOWN
○	ppp6	None	None	NA	DOWN
○	ppp7	None	None	NA	DOWN

5.8.1 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:

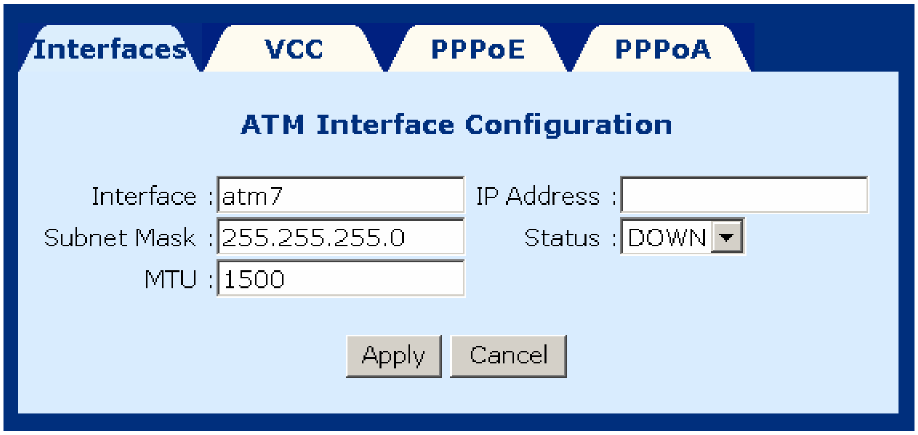
Interfaces:

- **Interface mer0** usage is reserved; its status is always **Down**.
- **Interface lo0** is the loopback interface. When an OAM loopback is performed, the status field displays UP.
- **Interfaces Atm1 to Atm7** display the interfaces configured for RFC1483 Bridged mode or RFC 1483 Routed mode.
- **Interfaces pppo to ppp7** display the interfaces configured for PPPoE or PPPoA.

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 a screen shot for the ATM interface.



ATM Interface Configuration

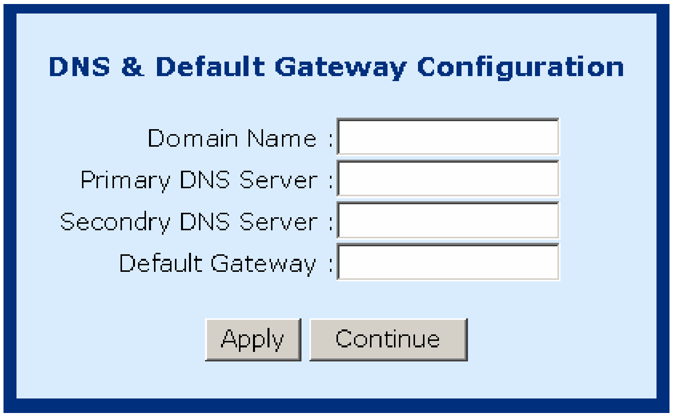
Interface : atm7
IP Address :
Subnet Mask : 255.255.255.0
Status : DOWN
MTU : 1500

5.8.2 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.



DNS & Default Gateway Configuration

Domain Name :
Primary DNS Server :
Secondry DNS Server :
Default Gateway :

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**.

5.8.3 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.

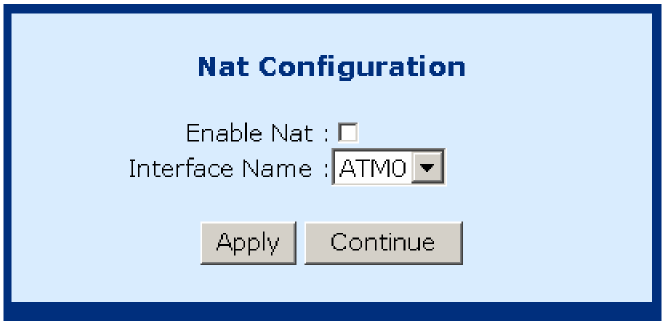
1. Form the configuration menu click on the NAT button at the bottom-right side of the screen.

2. Check the **Enable NAT** box

3. Select the interface to enable NAT

4. Click the **APPLY** button

5. Click the **CONTINUE** button



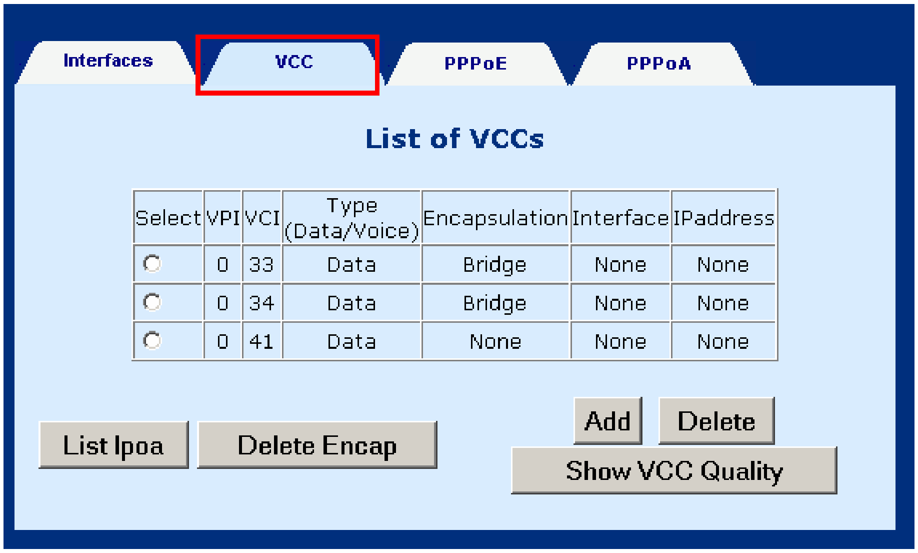
Nat Configuration

Enable Nat : □

Interface Name : ATM0

5.9 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.

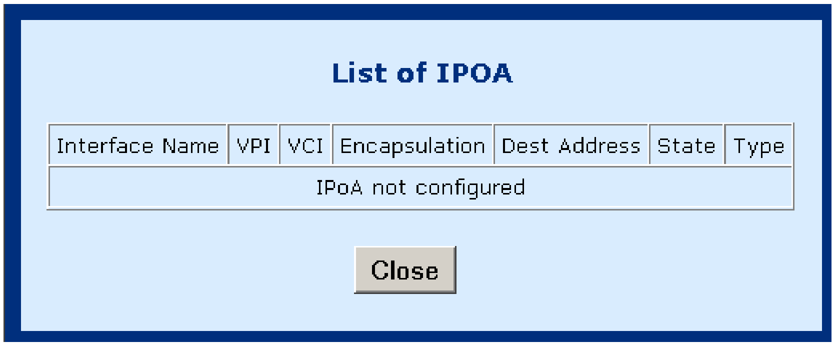


List of VCCs

Select	VPI	VCI	Type (Data/Voice)	Encapsulation	Interface	IPaddress
○	0	33	Data	Bridge	None	None
○	0	34	Data	Bridge	None	None
○	0	41	Data	None	None	None

5.9.1 List IPoA

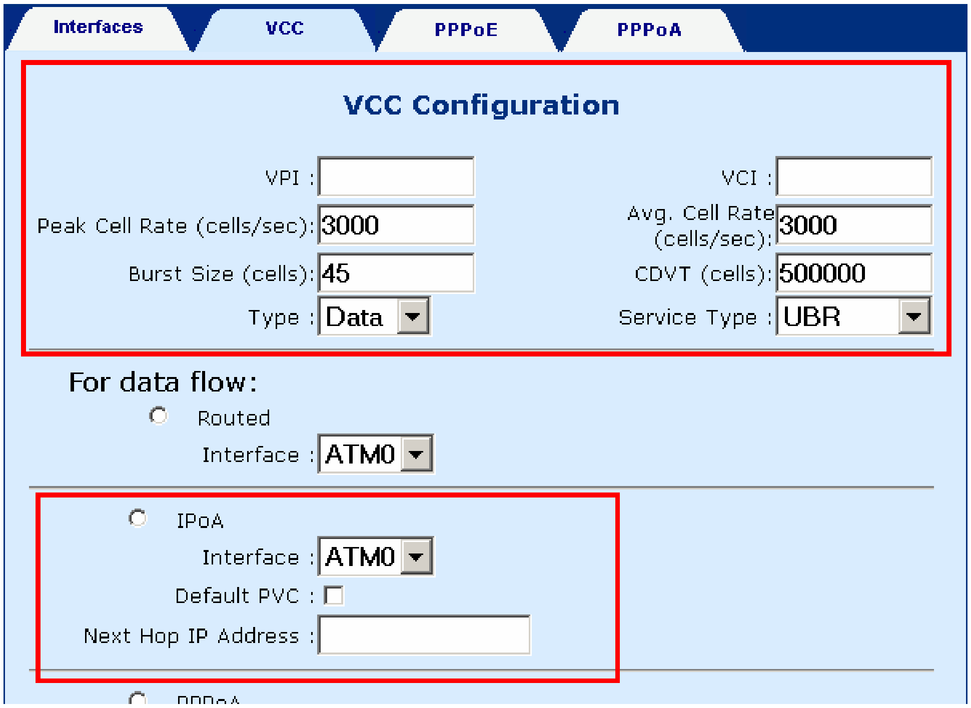
To list IP over ATM information click on the **IPoA** button at the bottom-left of the screen.



List of IPOA

Interface Name	VPI	VCI	Encapsulation	Dest Address	State	Type
IPoA not configured						

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



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

5.9.2 Delete Encapsulation

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

5.9.3 Add a VCC

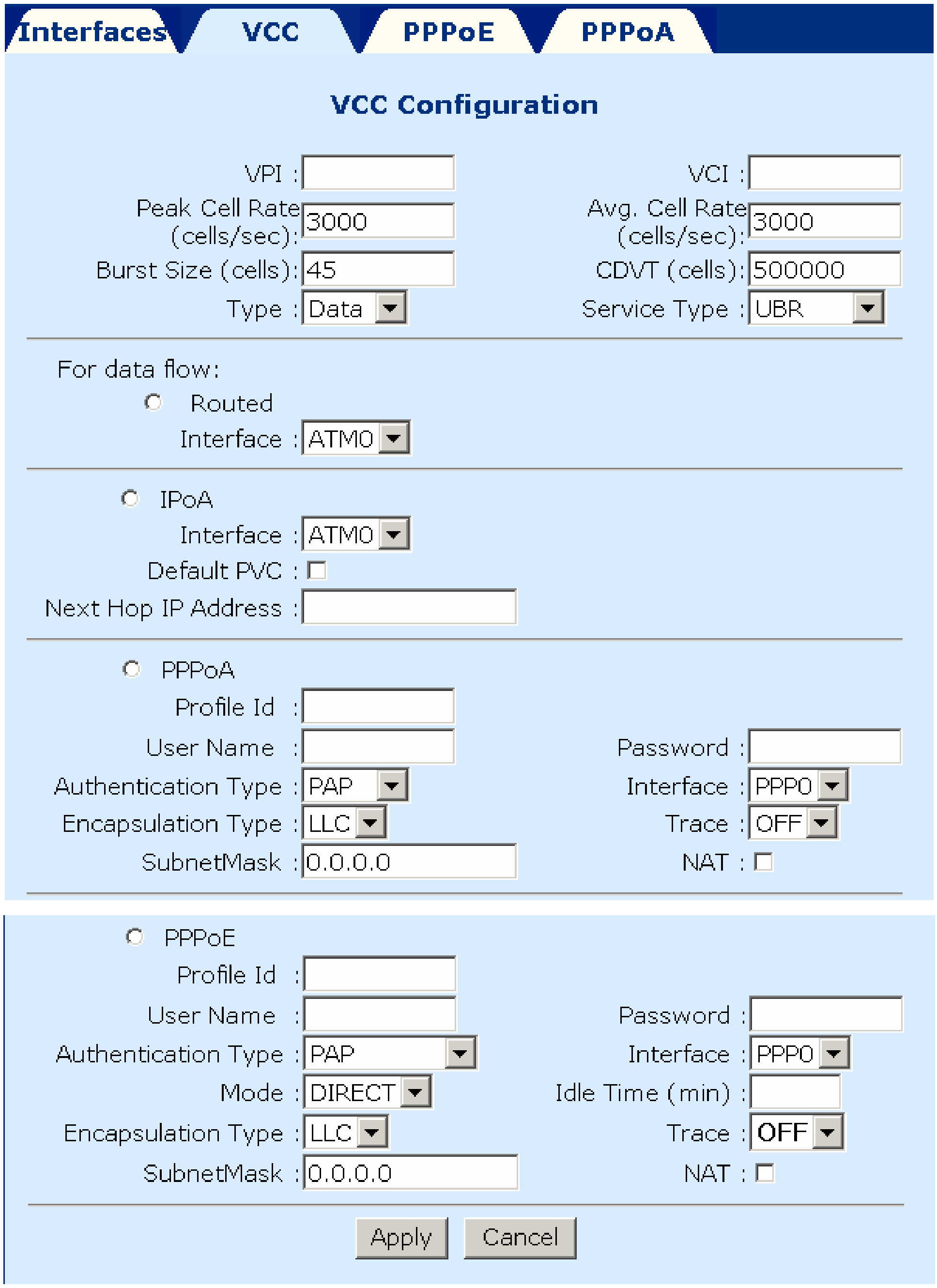
To add a VCC entry, complete the following steps:

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 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:	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.
rtvbr Real Time Variable Bit Rate:	Supports time-sensitive applications such as voice. In these applications the rate at which cells arrive are varied.
Nrtvbr Non Real Time Variable Bit Rate:	Supports applications that have no constraints on delay and delay variation, but still have variable-rate and bursty traffic characteristics.
Ubr Unspecified Bit Rate:	Best effort service that does not require tightly constrained delay and delay variation. UBR provides no specific quality of service or guaranteed throughput.



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 : PAP
Interface : PPP0
Encapsulation Type : LLC
Trace : OFF
SubnetMask : 0.0.0.0
NAT : □

○ PPPoE

Profile Id :
User Name :
Password :
Authentication Type : PAP
Interface : PPP0
Mode : DIRECT
Idle Time (min) :
Encapsulation Type : LLC
Trace : OFF
SubnetMask : 0.0.0.0
NAT : □

5.9.4 Delete a VCC

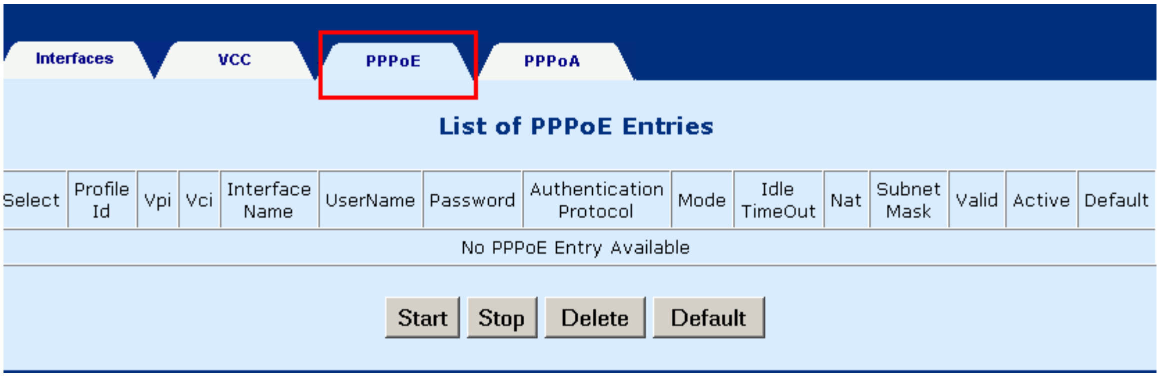
To delete a VCC entry, select the entry from the list of VCCs and then click on the **delete** button, at the bottom-right of the page.

5.9.5 Show VCC quality

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

5.9.6 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.

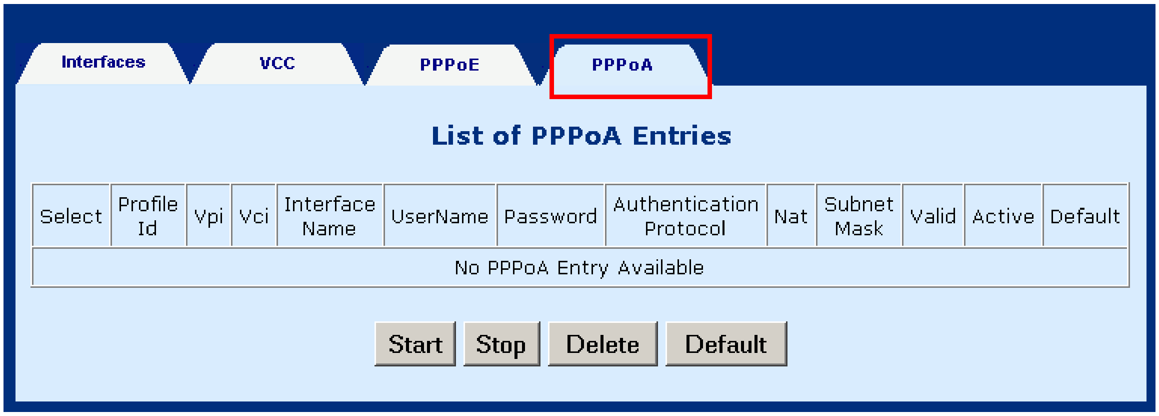


List of PPPoE Entries

Select	Profile Id	Vpi	Vci	Interface Name	UserName	Password	Authentication Protocol	Mode	Idle TimeOut	Nat	Subnet Mask	Valid	Active	Default
No PPPoE Entry Available														

5.10 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.

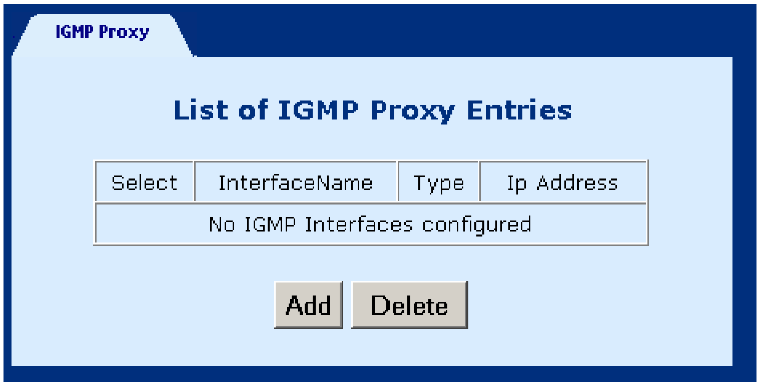


List of PPPoA Entries

Select	Profile Id	Vpi	Vci	Interface Name	UserName	Password	Authentication Protocol	Nat	Subnet Mask	Valid	Active	Default
No PPPoA Entry Available												

5.11 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.



List of IGMP Proxy Entries

Select	InterfaceName	Type	Ip Address
No IGMP Interfaces configured			

5.11.1 Add an IGMP entry

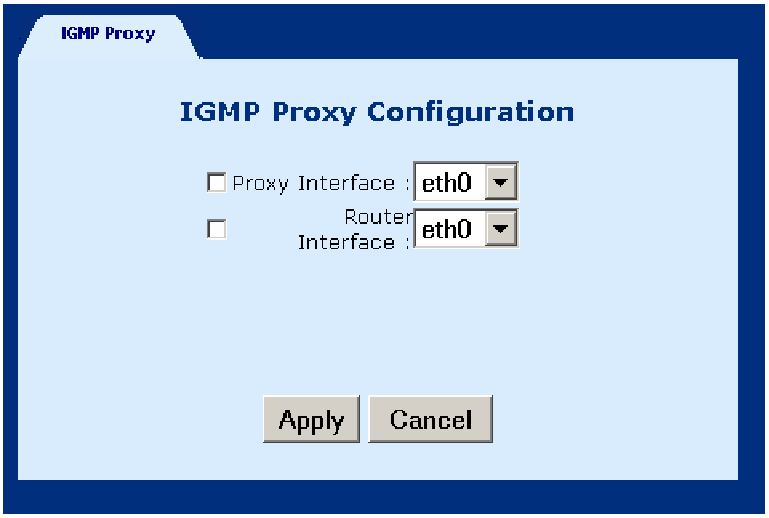
To add an IGMP proxy, complete the following steps:

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.



IGMP Proxy Configuration

□ Proxy Interface : eth0

□ Router Interface : eth0

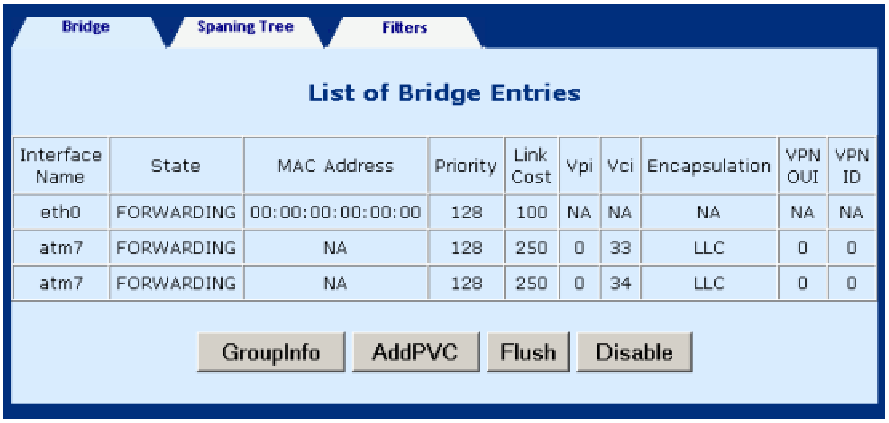
5.11.2 Delete an IGMP entry

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

5.12 Bridging

5.12.1 Bridge

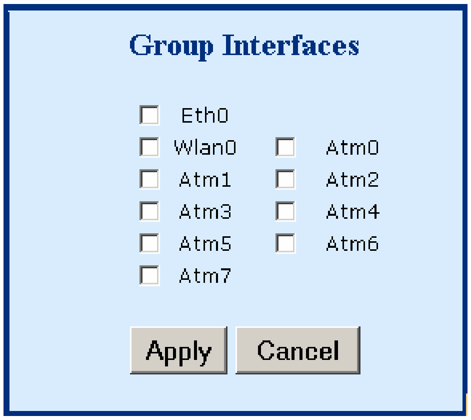
The Bridge window displays the configured Bridging PVC entries of the interfaces. There are four buttons at the bottom of the main-pane: Group Info, Add PVC, Flush, and Disable.



List of Bridge Entries

Interface Name	State	MAC Address	Priority	Link Cost	Vpi	Vci	Encapsulation	VPN OUI	VPN ID
eth0	FORWARDING	00:00:00:00:00:00	128	100	NA	NA	NA	NA	NA
atm7	FORWARDING	NA	128	250	0	33	LLC	0	0
atm7	FORWARDING	NA	128	250	0	34	LLC	0	0

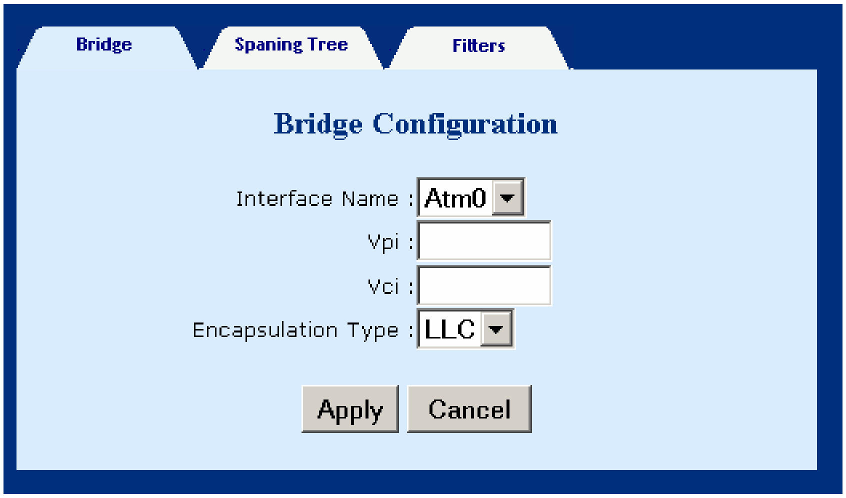
- **GroupInfo:** This configures the LAN packets that will travel through the LAN interface to the selected WAN interfaces. If you wish to change the interfaces that are configured you must first click on the **Flush button** (to remove the current ocnfiguration), and then click on the **Group Info**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



Group Interfaces

☐ Eth0
☐ Wlan0 ☐ Atm0
☐ Atm1 ☐ Atm2
☐ Atm3 ☐ Atm4
☐ Atm5 ☐ Atm6
☐ Atm7

- **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**.



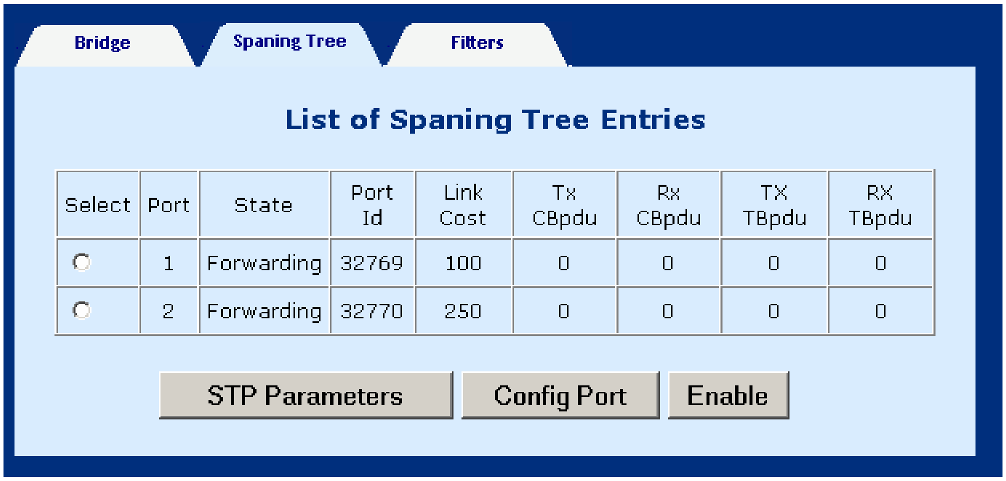
Bridge Configuration

Interface Name : Atm0
Vpi :
Vci :
Encapsulation Type : LLC

- **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.

5.12.2 Spanning tree

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

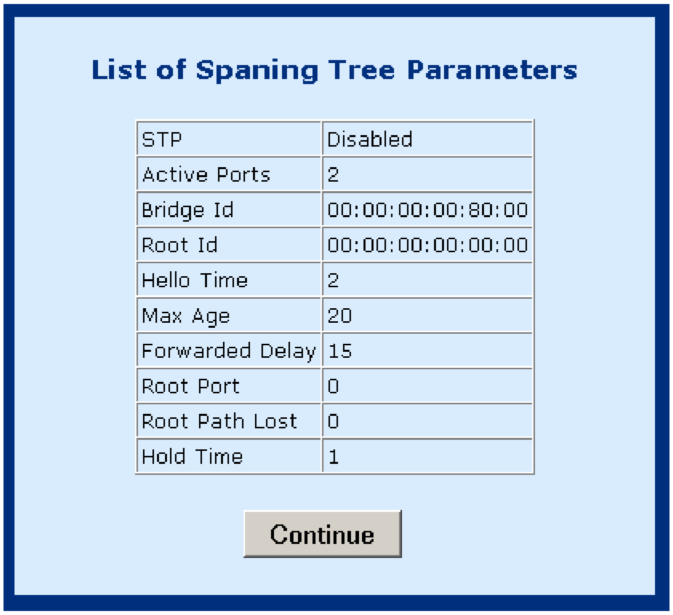


List of Spaning Tree Entries

Select	Port	State	Port Id	Link Cost	Tx CBpdu	Rx CBpdu	TX TBpdu	RX TBpdu
○	1	Forwarding	32769	100	0	0	0	0
○	2	Forwarding	32770	250	0	0	0	0

5.12.3 View STP Parameters

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



List of Spaning Tree Parameters

STP	Disabled
Active Ports	2
Bridge Id	00:00:00:00:80:00
Root Id	00:00:00:00:00:00
Hello Time	2
Max Age	20
Forwarded Delay	15
Root Port	0
Root Path Lost	0
Hold Time	1

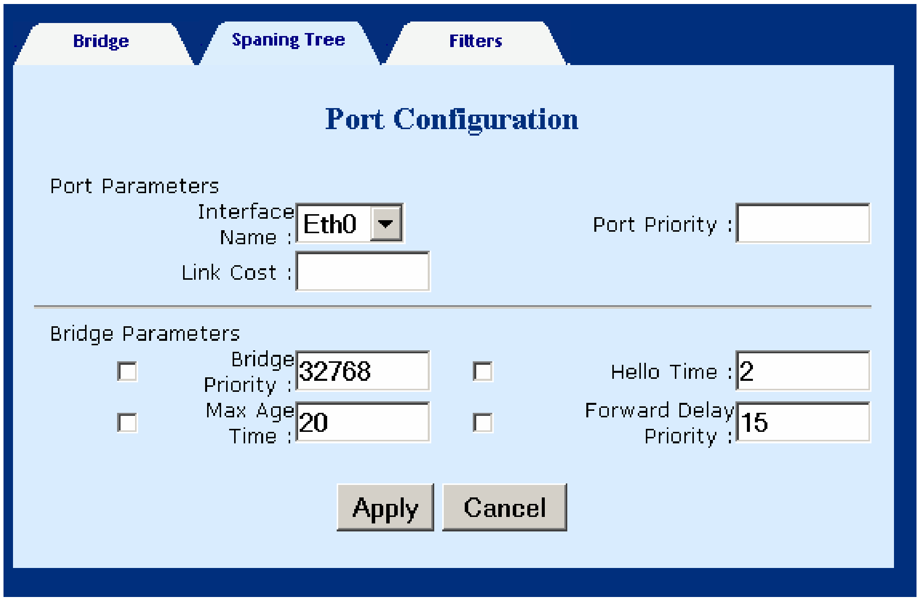
5.12.4 To configure STP parameters

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.



Port Configuration

Port Parameters

Interface Name : Eth0

Port Priority :

Link Cost :

Bridge Parameters

□ Bridge Priority : 32768

□ Hello Time : 2

□ Max Age Time : 20

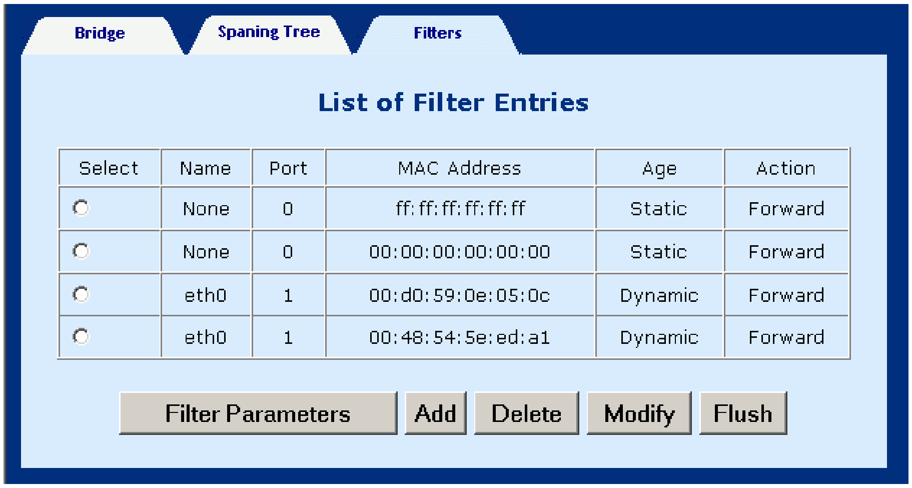
□ Forward Delay Priority : 15

5.12.5 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 Filtering

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.



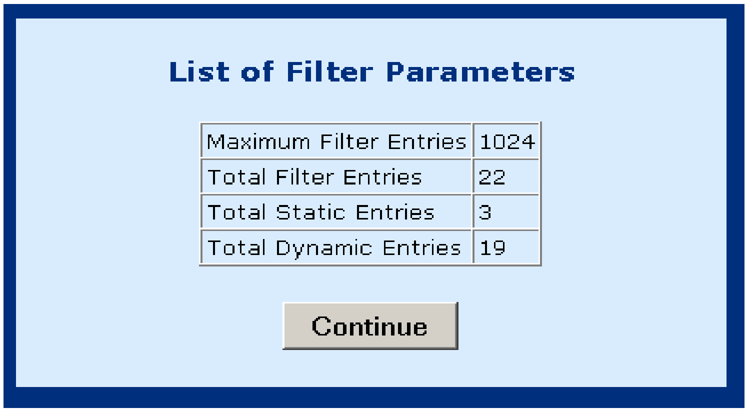
List of Filter Entries

Select	Name	Port	MAC Address	Age	Action
○	None	0	ff:ff:ff:ff:ff:ff	Static	Forward
○	None	0	00:00:00:00:00:00	Static	Forward
○	eth0	1	00:d0:59:0e:05:0c	Dynamic	Forward
○	eth0	1	00:48:54:5e:ed:a1	Dynamic	Forward

5.13.1 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



List of Filter Parameters

Maximum Filter Entries	1024
Total Filter Entries	22
Total Static Entries	3
Total Dynamic Entries	19

5.13.2 Add a filter entry

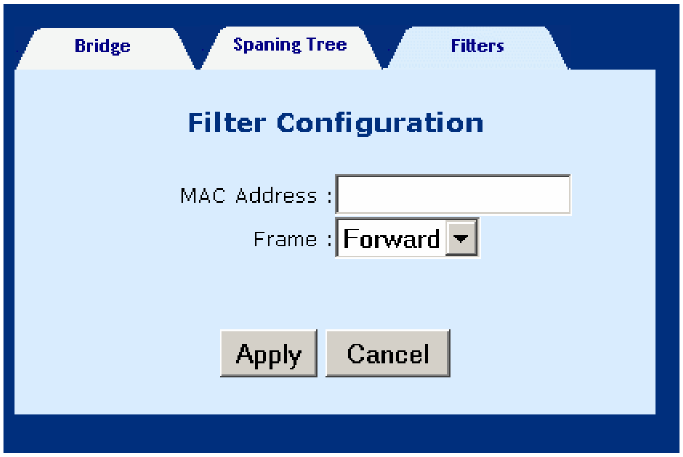
To add a filtering entry, complete the following steps:

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**.



Filter Configuration

MAC Address :

Frame : Forward

5.13.3 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.

5.13.4 Modify a filter entry

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

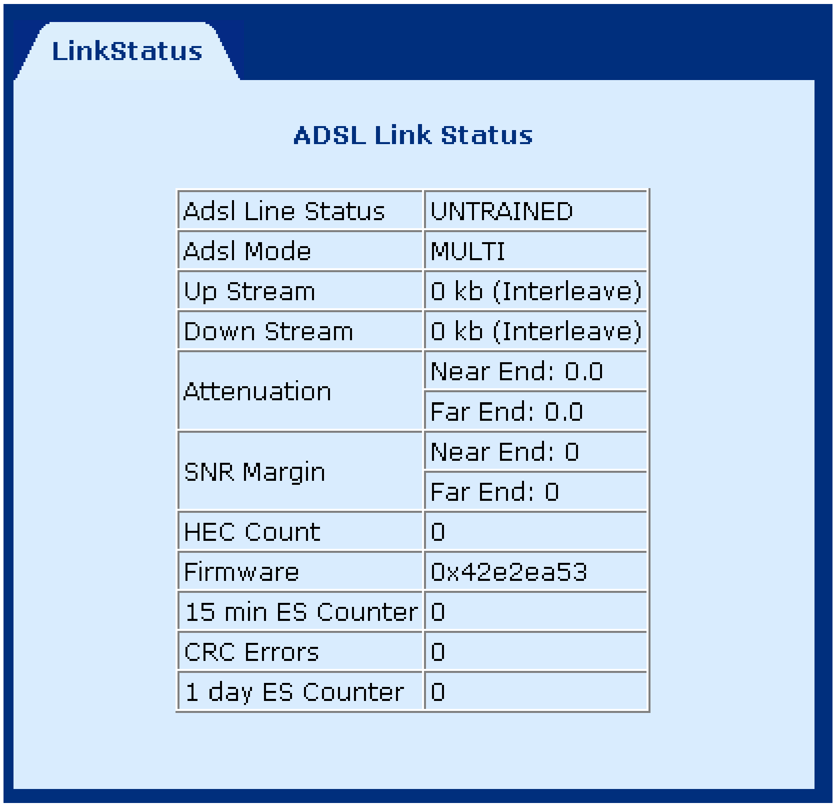
5.13.5 Flush filter entries

To flush all the filtering entries, click the **Flush** button at the bottom of the 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 Link Status

Adsl Line Status	UNTRAINED
Adsl Mode	MULTI
Up Stream	0 kb (Interleave)
Down Stream	0 kb (Interleave)
Attenuation	Near End: 0.0
	Far End: 0.0
SNR Margin	Near End: 0
	Far End: 0
HEC Count	0
Firmware	0x42e2ea53
15 min ES Counter	0
CRC Errors	0
1 day ES Counter	0

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	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

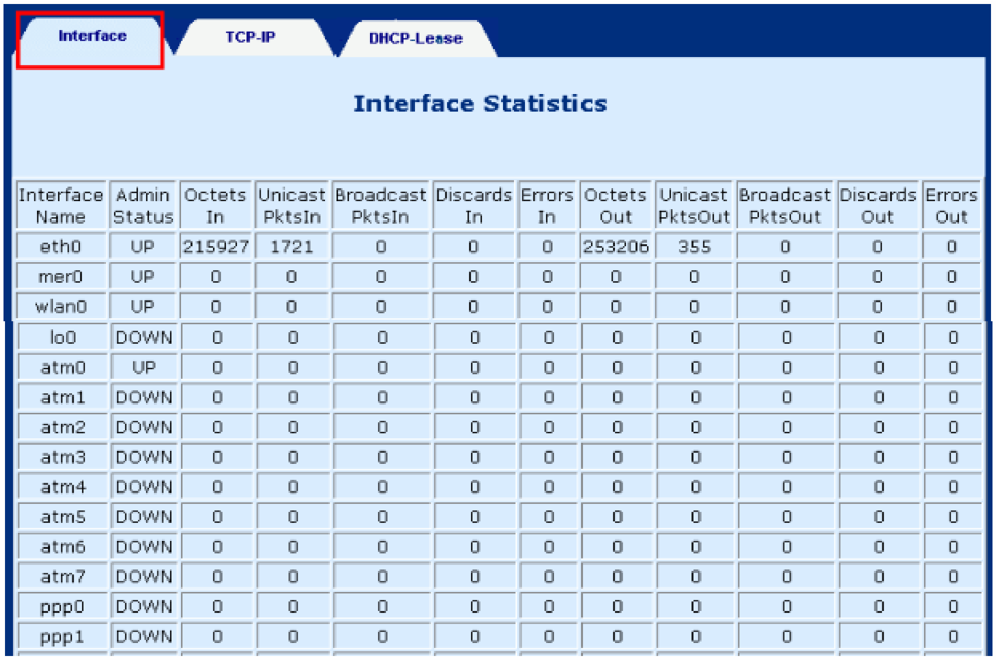
6.2 System Statistics

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

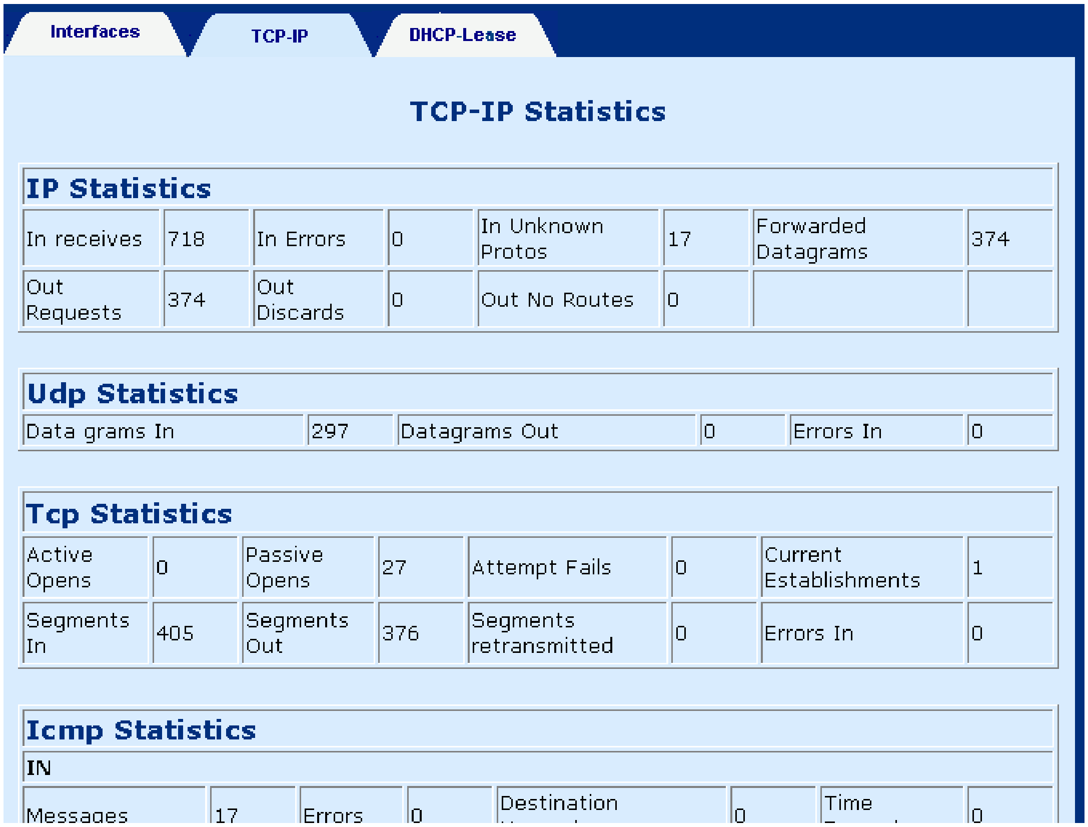


Interface Statistics

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.



TCP-IP Statistics

IP Statistics

In receives	718	In Errors	0	In Unknown Protos	17	Forwarded Datagrams	374
Out Requests	374	Out Discards	0	Out No Routes	0		

Udp Statistics

Data grams In	297	Datagrams Out	0	Errors In	0

Tcp Statistics

Active Opens	0	Passive Opens	27	Attempt Fails	0	Current Establishments	1
Segments In	405	Segments Out	376	Segments retransmitted	0	Errors In	0

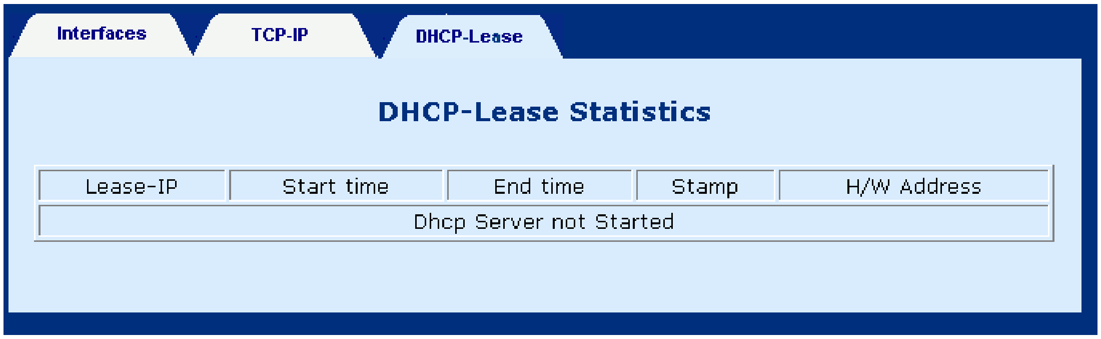
Icmp Statistics

IN

Messages	17	Errors	0	Destination	0	Time	0

6.2.3 DHCP-Lease

To view TCP-IP 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.



DHCP-Lease Statistics

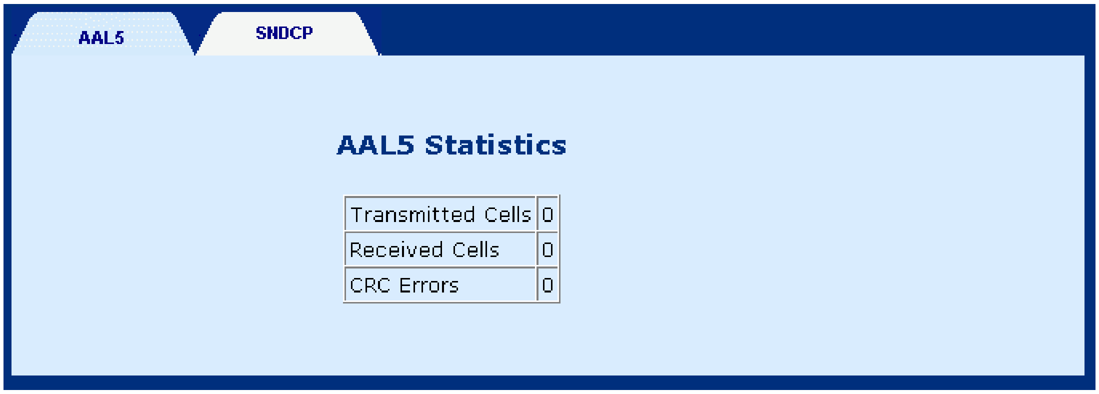
Lease-IP	Start time	End time	Stamp	H/W Address
Dhcp Server not Started				

6.3 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.

6.3.1 AAL5

The AAL5 page shows the AAl5 statistics.

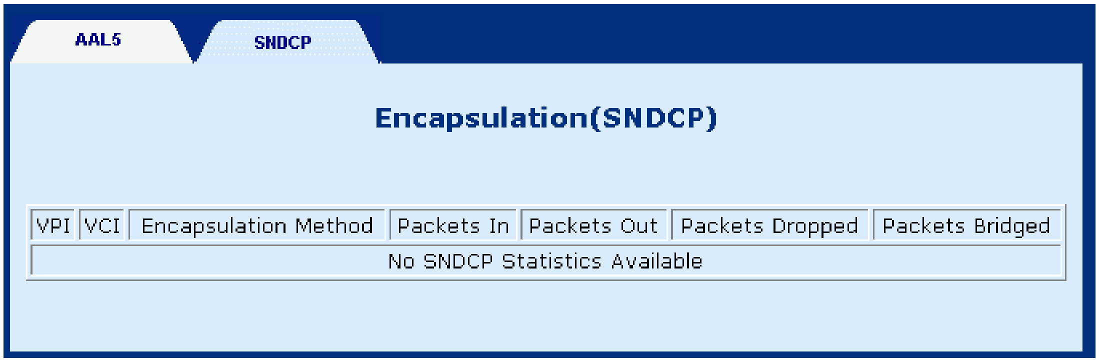


AAL5 Statistics

Transmitted Cells	0
Received Cells	0
CRC Errors	0

6.3.2 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).



Encapsulation(SNDCP)

VPI	VCI	Encapsulation Method	Packets In	Packets Out	Packets Dropped	Packets Bridged
No SNDCP Statistics Available						

Chapter 7 Web Diagnostics

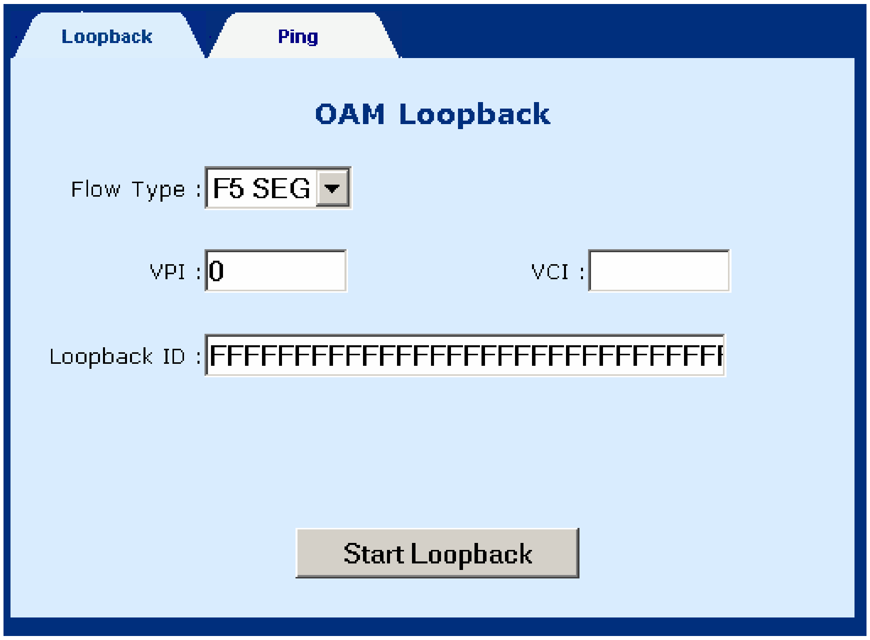
To access the Diagnostics screen, click the **Diagnostics** button, which is located on the menu bar. The Diagnostics screen has two test functions: OAM Loopback and Ping test.

7.1 OAM Loopback

STEP 1: lick 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

VPI : 0

VCI :

Loopback ID : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

- 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

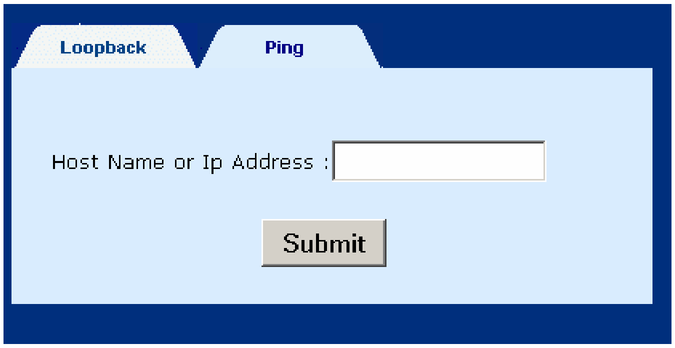
STEP 4: Click the **Start Loopback** button at the bottom of the screen.

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.

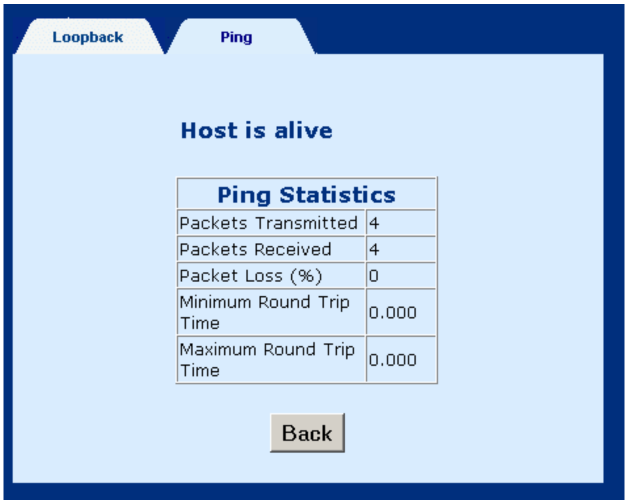
To access the Ping test screen, click the **Ping** tab on the Diagnostics screen.

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



Host is alive

Ping Statistics	
Packets Transmitted	4
Packets Received	4
Packet Loss (%)	0
Minimum Round Trip Time	0.000
Maximum Round Trip Time	0.000

Chapter 8 Firmware Upgrade

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

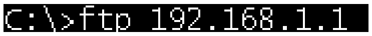
STEP 1: Connect the Router to a PC using the LAN cable. Set the PC to the same subnet as the router (192.168.1.1).

STEP 2: Restore the default parameters to the wireless router by holding down the device's **Reset** button until the **Power** LED turns red (about 5 seconds). [Or you can reboot the wireless route by running the device software and going to the **Erase and Reboot** menu and selecting the **ERASE** command.].

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

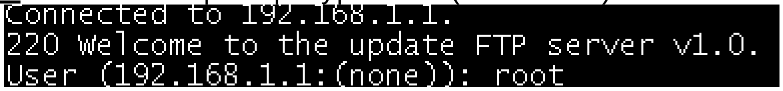
Example: C:\Upgrade

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



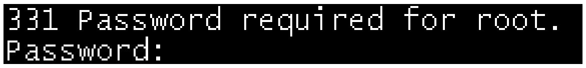
```
C:\>ftp 192.168.1.1
```

STEP 5: At the USER prompt type **root** (small case)



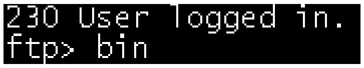
```
Connected to 192.168.1.1.
220 Welcome to the update FTP server v1.0.
User (192.168.1.1:(none)): root
```

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



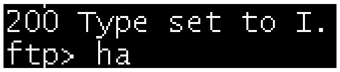
```
331 Password required for root.
Password:
```

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



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

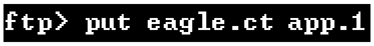
STEP 8: After you see the message Type set to I, type: **ha**



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

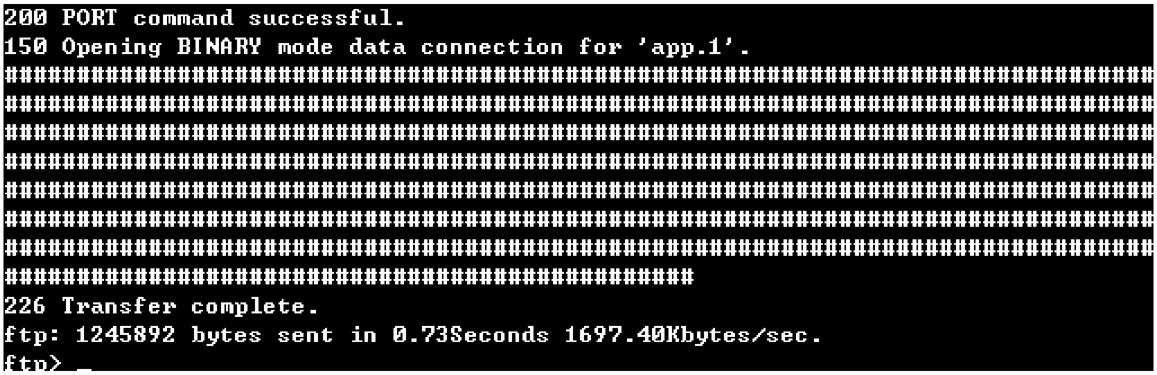
STEP 9: After you see the message Hash mark printing, type: **put <filename > app.1** (if the file name has extension, also type the extension.

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, the upgrade process is complete.



```
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> _
```

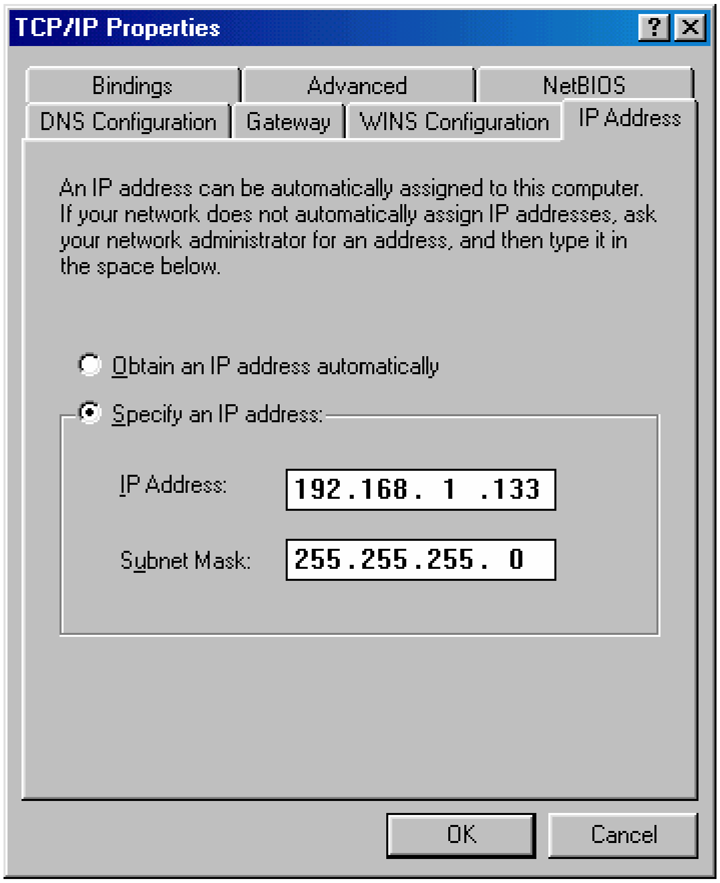
Chapter 9 Access by Telnet

This chapter will introduce the command line interface using Telnet. The chapter is divided into two parts. The first part explains how to set the PC and router to the same network segment, the second part explains how to start a Telnet session.

9.1 Setting a Common IP Address

To log on to the device using Telnet, your workstation and the router should both be on the same network segment. You can **modify the IP address of your PC** by modifying its TCP/IP. Follow the steps below:

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).



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

IP Address: 192.168. 1 .133

Subnet Mask: 255.255.255. 0

STEP 2: Click OK to submit the settings.

STEP 3: Start Telnet with the default IP address 192.168.1.1.

9.2 Telnet Access

To access Telnet to manage your router complete the following steps:

The default IP address is 192.168.1.1. Use the default IP address to log on to the router if it was not changed.

STEP 1 Make sure that the router and your Telnet-PC are on the same network segment.

STEP 2 Connect the LAN port of the router to Ethernet or PC with an RJ45 cable.

STEP 3 Click Windows Start menu and type Telnet x.x.x.x

(x.x.x.x represents the IP address)

STEP 4 You will be prompted to enter a User name and Password, enter **root** for User name and **12345** for the Password.

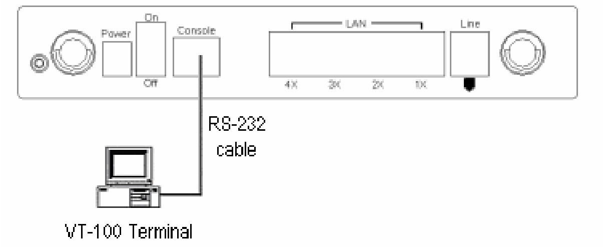
STEP 5 The first screen of the CLI interface will now display.

Chapter 10 Console Management

This section of the manual deals with console management of the router.

10.1 Hardware connection

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.



10.2 Access by Console

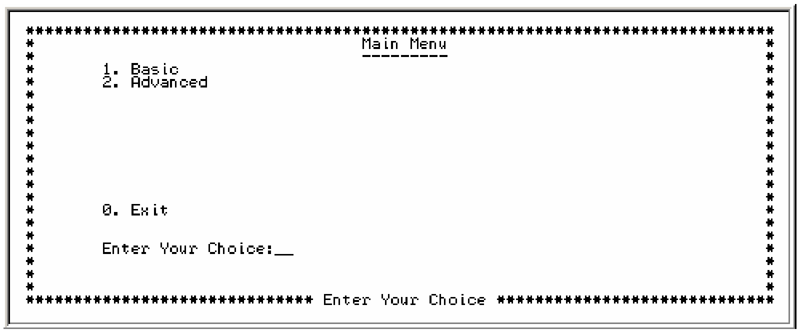
For access by console, the console PC should be installed with a standard VT-100 emulation program, such as HyperTerminal 5 or Telix. The following steps describe how to establish the console session.

Step 1 Start a standard VT-100 program such as HyperTerminal (Ver. 5 is recommended), or Telix in the local terminal; and select an open com port.

Step 2 Enter the following port settings:

- Baud rate: 9600
- Data bits: 8
- Parity: none
- Stop bit: 1
- Flow control: none

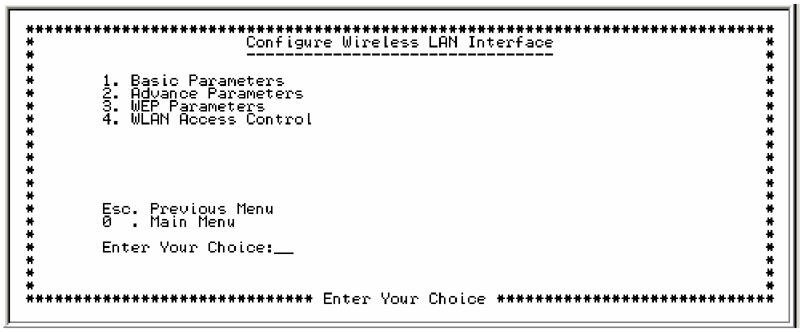
Step 3 After the session parameters are set up, as shown in Step 2, the screen will display as below. (For some versions you may need to press the **ESC** or **Enter** Key.



```
********************************************************************************
*                                   Main Menu                                  *
*                                   ---------                                  *
*       1. Basic                                                               *
*       2. Advanced                                                            *
*                                                                              *
*                                                                              *
*                                                                              *
*                                                                              *
*                                                                              *
*                                                                              *
*                                                                              *
*                                                                              *
*       0. Exit                                                                *
*                                                                              *
*       Enter Your Choice:__                                                   *
*                                                                              *
*                                                                              *
****************************** Enter Your Choice *******************************
```

10.3 Console WLAN Guide

Parameters that specifically deal with the wireless functions of your router can be accessed from the **WLAN Parameters** menu, located at BASIC/WLAN CONFIGURATION. The menu is subdivided into three menus: Basic Settings, Advanced Functions and WEP Functions. Each of these menus will be covered below.



```
******************************************************************************
*                      Configure Wireless LAN Interface                      *
*                      --------------------------------                      *
*                                                                            *
*       1. Basic Parameters                                                  *
*       2. Advance Parameters                                                *
*       3. WEP Parameters                                                    *
*       4. WLAN Access Control                                               *
*                                                                            *
*                                                                            *
*                                                                            *
*                                                                            *
*                                                                            *
*                                                                            *
*       Esc. Previous Menu                                                   *
*       0  . Main Menu                                                       *
*                                                                            *
*       Enter Your Choice:__                                                 *
*                                                                            *
*                                                                            *
*                                                                            *
****************************** Enter Your Choice *****************************
```

10.3.1 WLAN Basic Parameters

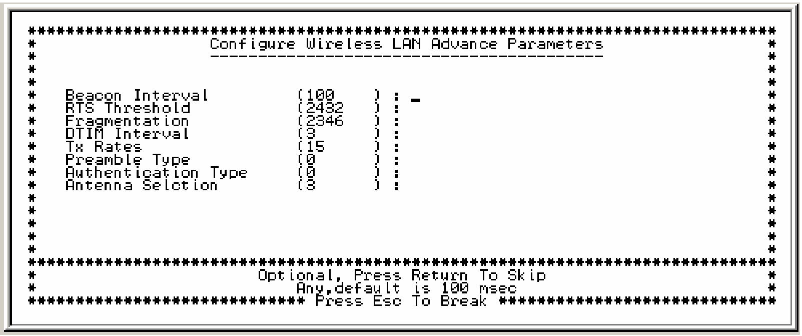
To configure WLAN basic Parameters go to BASIC/WLAN CONFIGURATIION/BASIC PARAMETERS, enter values for the required parameters and then press the **Y** key when prompted by the following message Do You Wish To Submit These Values [Y/N]. The WLAN Basic Parameters menu includes the parameters listed below:

IP Address	Enter the **IP address** for the WLAN interface
Subnet Mask	Enter a **subnet mask** for the WLAN interface
MAC Address	Enter a MAC address to limit access to the router (only packets destined for this MAC address will be accepted by the router).
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 13, restrictions apply depending on the country where the Wireless ADSL-Router is used: **FCC**: channels 1 to 11 **ETSI**: channels 1 to 13.

10.3.2 WLAN Advanced Functions

To configure WLAN Advance Parameters go to BASIC/WLAN CONFIGURATIION/ADVANCE PARAMETERS, enter values for the required parameters and then press the **Y** key when prompted by the following message Do You Wish To Submit These Values [Y/N]. The WLAN Advanced Functions menu includes the parameters listed below:

Beacon Interval	Default =100. 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. The value must be between 0-3000.
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. The value must be between 256 – 2346 and must be an even number.
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.
Tx Rates	The transfer rate of the router should be equal to or greater than the clients, the options are: 1(1M), 3(2M), 7(5M), 15(11M), 31(22M)
Preamble Type	Select **0** (Long Preamble) or **1** (Short Preamble) 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	Select **1 (Open System) or 2 (Shared Key). Open System** [no security], **Shared Key** [select this option if you wish to enable WEP security], if you select **both,** then both Open System and Shared Key will be simultaneously enabled.
Antenna Selection	Select **1** (Left spread on), **2** (Right spread on), **3** (Diversity spread on). Diversity enables both antennas, or you can select **left** or **right** to only enable one antenna.

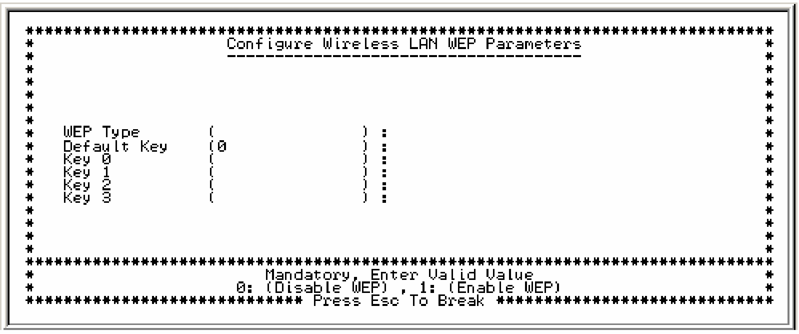


```
*******************************************************************************
*                 Configure Wireless LAN Advance Parameters                   *
*                 -----------------------------------------                   *
*                                                                             *
*                                                                             *
*   Beacon Interval          (100    ) : _                                    *
*   RTS Threshold            (2432   ) :                                      *
*   Fragmentation            (2346   ) :                                      *
*   DTIM Interval            (3      ) :                                      *
*   Tx Rates                 (15     ) :                                      *
*   Preamble Type            (0      ) :                                      *
*   Authentication Type      (0      ) :                                      *
*   Antenna Selction         (3      ) :                                      *
*                                                                             *
*                                                                             *
*                                                                             *
*                                                                             *
*                                                                             *
*******************************************************************************
*                       Optional, Press Return To Skip                        *
*                           Any,default is 100 msec                           *
***************************** Press Esc To Break *****************************
```

10.3.3 WLAN WEP Parameters:

WEP security uses an encryption keyword on all transmitted and received data. To configure WLAN basic Parameters go to BASIC/WLAN CONFIGURATIION/WEP PARAMETERS, enter values for the required parameters and then press the **Y** key when prompted by the following message Do You Wish To Submit These Values [Y/N]. The WLAN WEP menu includes the parameters listed below: The parameters are as follows:

WEP Type	**64 bits, 128 bits**. This parameter determines the level of security. 128 bits provides the highest security. This parameter must match with the remote-clients.
Default Key	Enter Valid Value to indicate which key (0~3) to use for encryption and decryption
Key 0~3	Enter a hexadecimal key.



```
*******************************************************************************
*                     Configure Wireless LAN WEP Parameters                   *
*                     -------------------------------------                   *
*                                                                             *
*                                                                             *
*                                                                             *
*                                                                             *
*                                                                             *
*   WEP Type        (                ) :                                      *
*   Default Key     (0               ) :                                      *
*   Key 0           (                ) :                                      *
*   Key 1           (                ) :                                      *
*   Key 2           (                ) :                                      *
*   Key 3           (                ) :                                      *
*                                                                             *
*                                                                             *
*                                                                             *
*                                                                             *
*******************************************************************************
*                       Mandatory, Enter Valid Value                          *
*                   0: (Disable WEP) , 1: (Enable WEP)                        *
***************************** Press Esc To Break *****************************
```

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

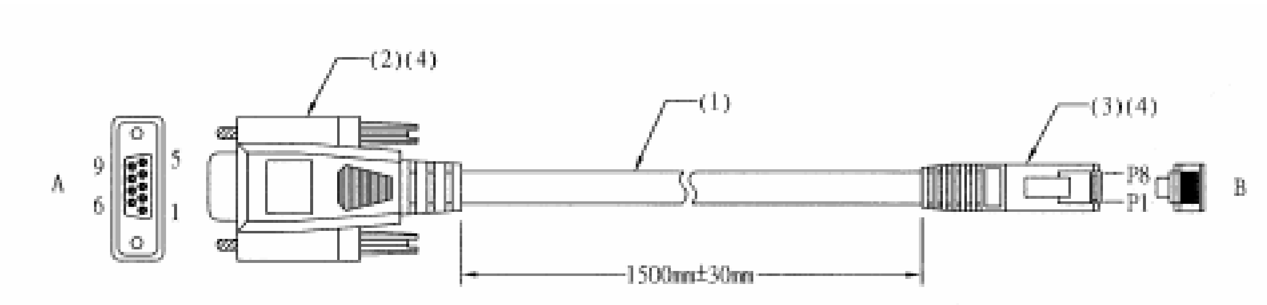
Note: NC means No connection

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