

# 802.11g Wireless ADSL Router

## Installation Guide & User's Manual

Version 1.1

---



# Table of Contents

---

## Installation Guide

<b>PACKAGE CONTENTS.....</b>	<b>I</b>
<b>PLACING AND CONNECTING YOUR ROUTER.....</b>	<b>I</b>
<b>SETTING UP YOUR TCP/IP.....</b>	<b>II</b>
WINDOWS 95/98/98SE/ME .....	II
WINDOWS 2000/XP .....	III
<b>OPENING THE WEB CONFIGURATION.....</b>	<b>IV</b>
<b>SETTING UP YOUR ROUTER.....</b>	<b>V</b>
LEASED LINE USER .....	V
DIAL-UP USER.....	VII

## User's Manual

<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 FEATURES .....	1
1.2 SYSTEM REQUIREMENTS .....	2
<b>2. KNOWING YOUR ROUTER.....</b>	<b>3</b>
2.1 FRONT PANELS .....	3
2.2 REAR PANELS.....	3
2.3 LED INDICATORS.....	4
<b>3. LOGIN .....</b>	<b>5</b>
<b>4. STATUS PAGES.....</b>	<b>6</b>
4.1 HOME PAGE.....	6
4.2 PPP PAGE.....	7
4.3 ADSL PAGE.....	8
<b>5. CONFIGURATION PAGES.....</b>	<b>10</b>
5.1 MODES.....	10
5.2 WAN CONFIGURATION .....	11
5.2.1 ATM.....	12
5.2.2 DHCP Client.....	13
5.2.3 MAC Spoofing.....	14
5.2.4 Static IP Settings .....	14
5.3 LAN CONFIGURATION .....	14

5.3.1 DHCP Server .....	15
5.3.2 Ethernet Mode Setting.....	16
5.4 PPP CONFIGURATION.....	17
5.4.1 PPP Account Configuration .....	17
5.4.2 PPP Session Configuration.....	18
5.4.3 PPP Disconnect Timer Configuration .....	20
5.4.4 PPP Miscellaneous Configuration.....	22
5.5 NAT CONFIGURATION PAGES.....	23
5.6 VIRTUAL SERVER CONFIGURATION .....	25
5.7 BRIDGE FILTERING .....	26
5.8 DNS CONFIGURATION .....	27
5.9 WIRELESS CONFIGURATION .....	29
5.9.1 Basic Settings .....	29
5.9.2 Advanced Settings .....	30
5.10 WIRELESS LAN SECURITY .....	32
5.11 USER PASSWORD CONFIGURATION .....	33
5.12 SAVE SETTINGS / REBOOT .....	34
<b>6. ADMIN PRIVILEGE .....</b>	<b>35</b>
6.1 WAN STATUS.....	35
6.2 ATM STATUS .....	36
6.3 ADSL CONFIGURATION .....	36
6.4 ROUTE TABLE .....	37
6.4.1 System Default Gateway Configuration.....	38
6.4.2 Route Configuration.....	38
6.5 LEARNED MAC TABLE .....	39
6.6 RIP CONFIGURATION .....	39
6.6.1 RIP Per Interface Configuration.....	41
6.7 MISCELLANEOUS CONFIGURATION .....	42
6.8 TCP STATUS .....	44
6.9 ADMIN PASSWORD CONFIGURATION .....	45
6.10 RESET TO FACTORY DEFAULT.....	45
6.11 DIAGNOSTIC TEST .....	46
6.12 SYSTEM LOG .....	46
6.13 LOCAL CODE IMAGE UPDATE.....	47
6.14 NETWORK CODE IMAGE UPDATE .....	48
6.14.1 Firmware.....	48
6.14.2 Boot Code.....	49
<b>APPENDIX A. COMPLIANCE STATEMENT.....</b>	<b>50</b>
<b>APPENDIX B. ENCAPSULATION MODE .....</b>	<b>51</b>

# Installation Guide

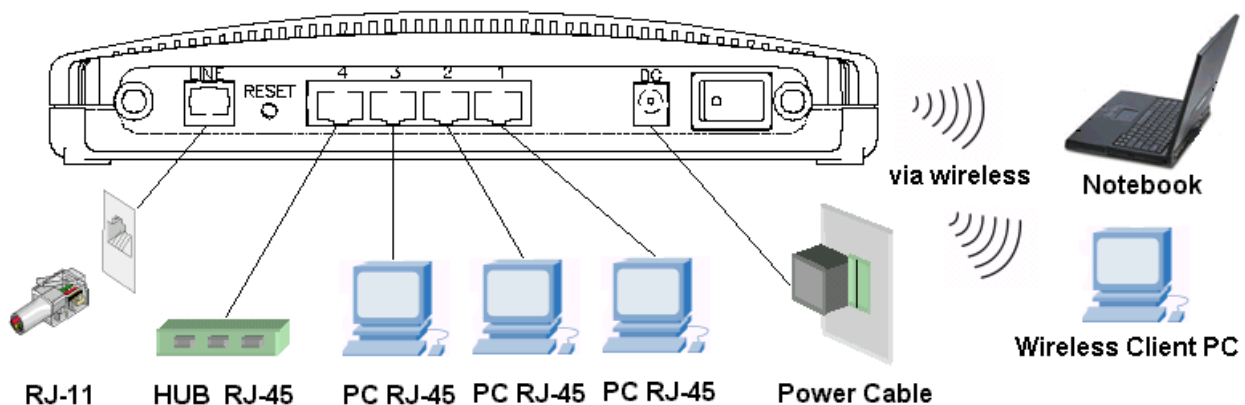
# Package Contents

Open the shipping carton and carefully remove all items. In addition to this User's Guide, ascertain that you have:

- 1\* Wireless ADSL Router
- 1\* Installation Guide & User's Manual
- 1\* Tool kit on CD-ROM
- 1\* Telephone cable with RJ-11 connectors for ADSL connection
- 1\* Network cable with RJ-45 connectors for LAN connection
- 1\* AC power adapter
- 2\* Antennas
- 1\* Splitter

## Placing and Connecting Your Router

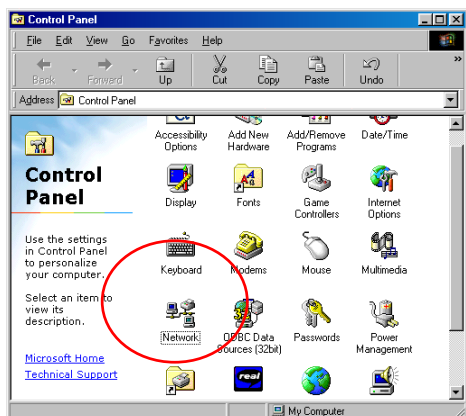
Placing your Router in a proper location is important to ensure the best performance of your wireless network. However, different types of construction materials and other large obstructions such as refrigerator, washer or dryer in a building can greatly affect the wireless signal and decrease the coverage range. Place your Router as close as possible to the center of the area that you want to cover. In multi-story homes, place the Router on an upper floor will be better. Also, the wireless signal can be affected by many things such as neighboring wireless networks, microwave ovens in operation. Try to avoid these objects when locating your Router.



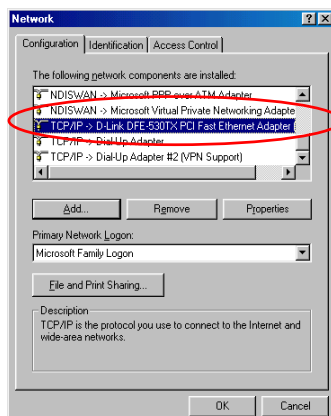
1. Attached the included antennas to the Router (if needed). The antenna should be perpendicular to the ground.
2. Insert the Power Adapter cord into the power receptacle and then plug the adapter into a nearby power source. Power on the Router, and you should see the PWR (Power) LED indicator light up and remain lit.
3. Use the twisted-pair ADSL cable (standard telephone cable) shipped with the Router to connect the Router to your telephone line. You should see the ADSL LED indicator light up and remain lit.
4. The Router may be connected to any 10/100BASE-T Ethernet LAN or Ethernet concentrating device. Connection to an Ethernet concentrating device such as a switch or hub should use standard twisted-pair cable with RJ-45 connectors.
5. Use straight-through cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use crossed cable when connecting it to an uplink (MDI-II) port on a hub or switch. You should see the LINK LED indicator of that LAN port you connected light up and remain lit.
6. Refer to User's Manual Section 2.3 for the details of LED indicators.

# Setting up Your TCP/IP

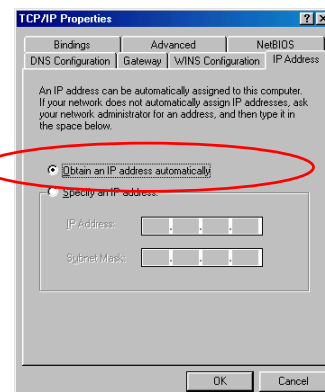
## Windows 95/98/98SE/ME



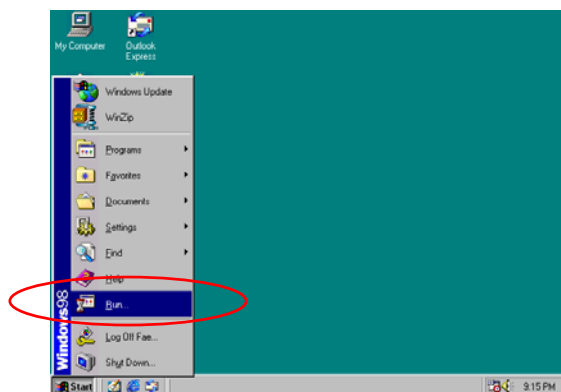
1. Double click **Network** icon from **Start→Control Panel**. Network dialog box would pop up.



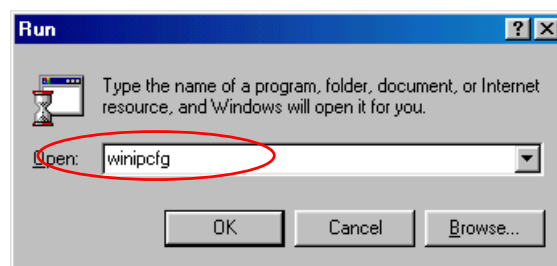
2. Under **Configuration** tab select TCP/IP->xxxxxx, where xxxxx is name of the network adapter. Click **Properties**.



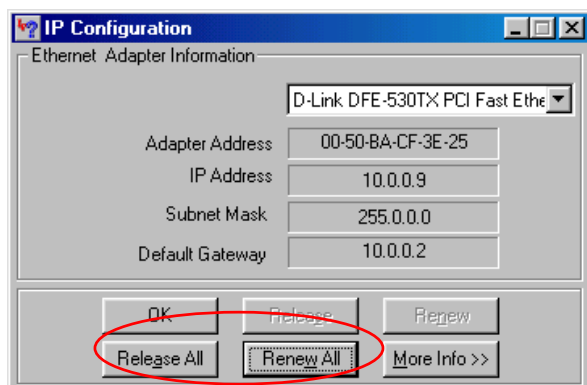
3. Click **IP Address** tab. Select "Obtain an IP Address automatically" and then click **OK**.



4. Select **Run** item from Start.



5. Enter **winipcfg** in the text field and then click **OK**.

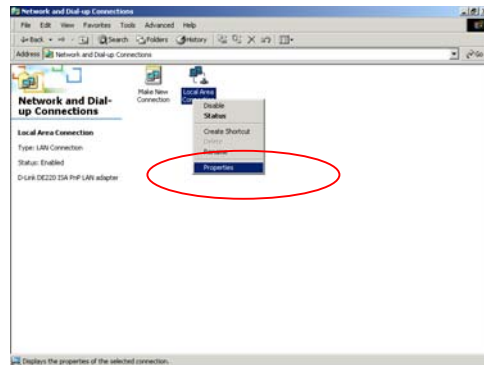


6. Select the adapter from dropdown list. Press **Release All** and then **Renew All** to get the information of adapter. If you could not obtain the related information, go back to step 3 to indicate the default gateway as **10.0.0.2** and then go through step 4 to 6 again.

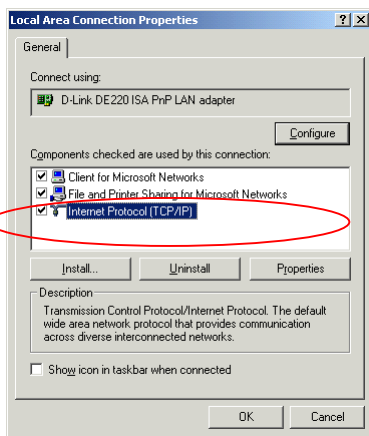
# Windows 2000/XP



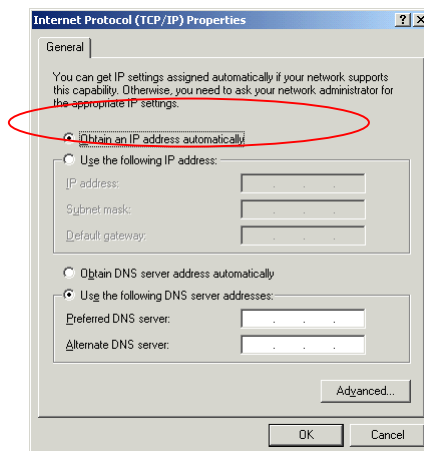
1. Double click **Network and Dial-up Connections** icon from **Start→Control Panel**. Network dialog box would pop up.



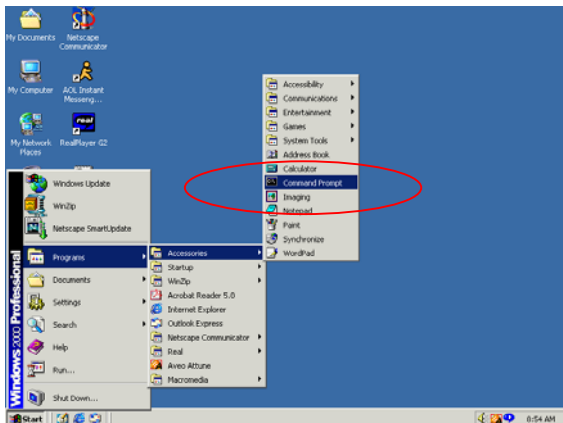
2. Select the network adapter installed in your PC and then right-click mouse to select **Properties**.



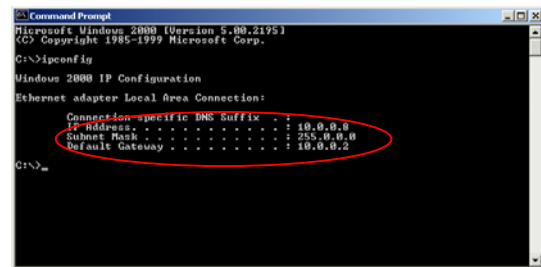
3. Highlight **Internet Protocol (TCP/IP)** and then click **Properties**.



4. Select “Obtain an IP Address automatically” and then click **OK**.



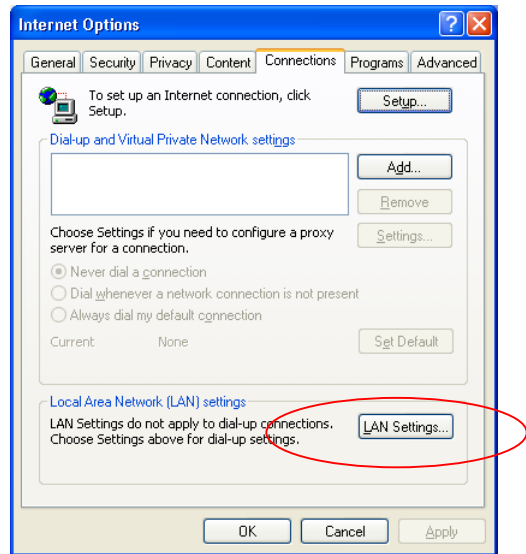
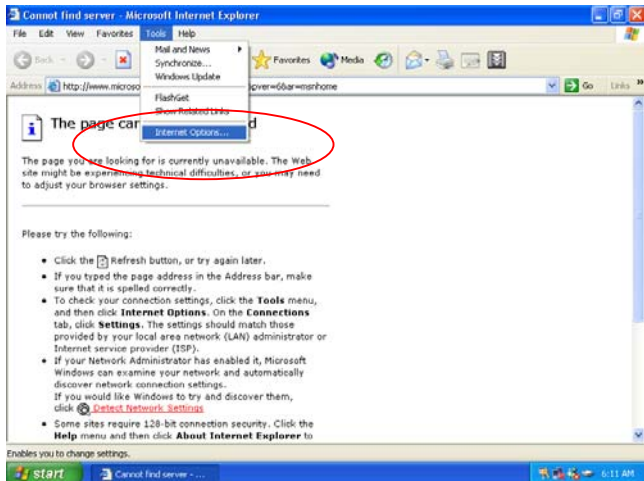
5. Select **Command Prompt** from **Start→All Programs→Accessories**.



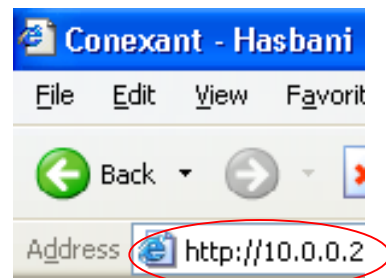
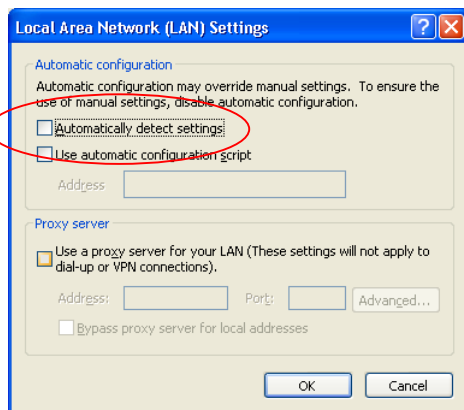
6. Type **ipconfig** then press enter. You will see the information of IP Address, Subnet Mask and Default Gateway. If you could not obtain the related information, go back to step 4 to indicate the default gateway as **10.0.0.2** and then go through step 5 to 6 again.

# Opening the Web Configuration

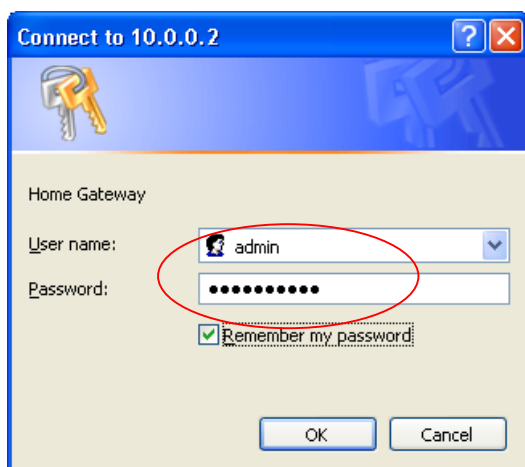
You must uncheck the Proxy server function before login into the web configuration.



1. Select **Tools>Internet Options** from your **Internet Explorer** browser.
2. Select **LAN Settings** in **Connections** tab.



3. Uncheck the check box of **Proxy server** and then click **OK**. (You may enable Proxy server function after logout if you need to use it.)
4. Type the default IP address **10.0.0.2** the address bar of the browser to open web configuration.



5. Type the User Name and Password then click Ok button. The default login name and password for administrator and user are the same. You may change them in Password Configuration page after entering the system.

**User Name : admin**  
**Password : epicrouter**



# Setting up Your Router

## Leased Line User

Go to **Configuration** > **WAN** page.

Enter the **IP Address**, **Subnet Mask** and **Gateway** provided by your ISP.

Leased line user may select **1483 Bridged IP LLC** or **1483 Routed IP LLC**. It depends on your requirements.

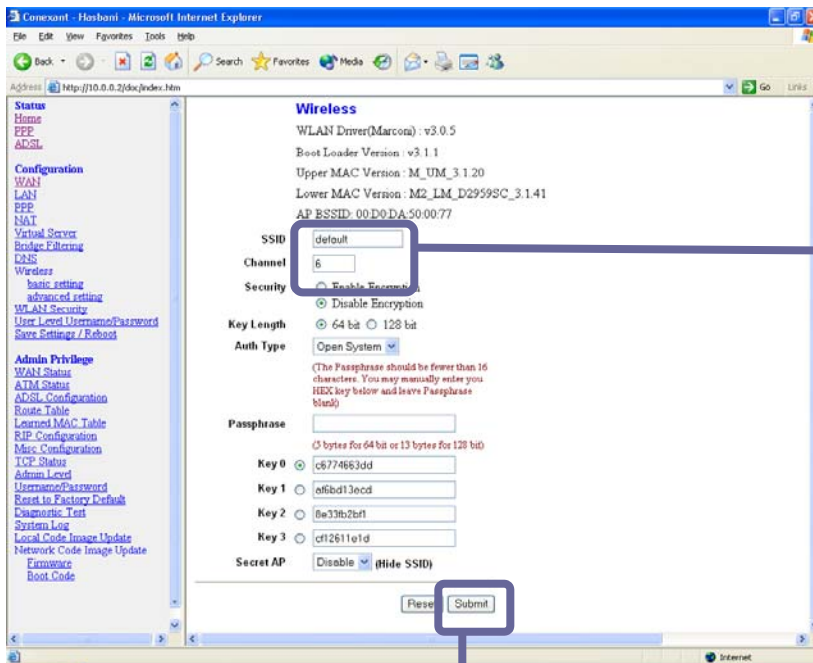
Enter the **VPI** and **VCI**, provided by your ISP.

Confirm your settings and then click **Submit**.

Go to **Configuration** > **DNS** page.

Enable DNS Proxy and then tick **Auto Discovery** and/or **User Configuration**. If User Configuration is selected, you have to enter the IP address of DNS server provided by your ISP in DNS Server field and then click **Add** to add the DNS server.

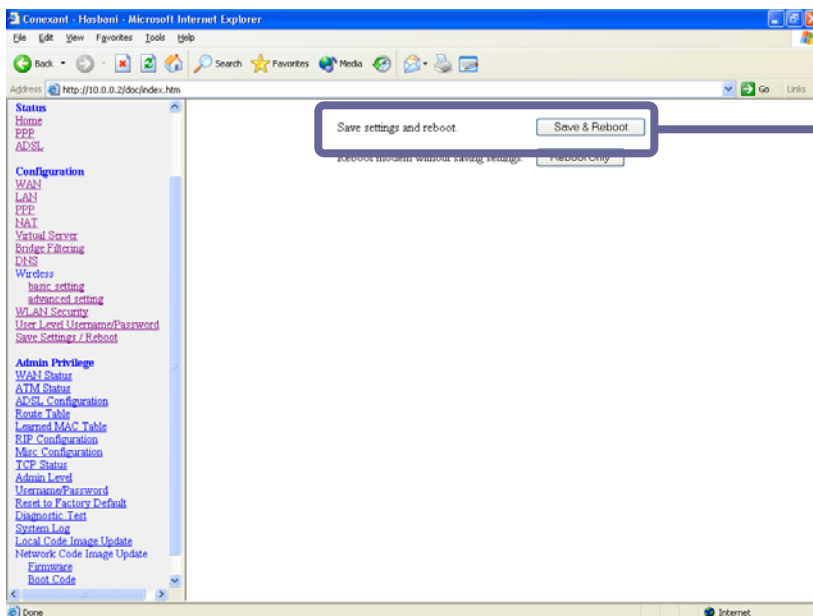
Confirm your settings and then click **Apply**. The DNS server you configured will list in the DNS Proxy Setting table on the left bottom of this page.



Go to **Configuration > Wireless > basic setting** page.

If you do not have a wireless LAN, you can use the Router's default settings. If you have an existing Wireless LAN, configure your **SSID**, **Channel** and other security settings. The Router and wireless clients must use the same SSID, Channel and security settings in order to communicate with each other.

Confirm your settings and then click **Submit**.



Go to **Configuration > Save Settings / Reboot** page.

Go to **Save Settings / Reboot** page and then click **Save & Reboot** to save the settings you made to flash ROM.

Congratulations! You have finished the settings of the Router and you may surf the Internet right now.

# Dial-up User

**Wan Configuration (Pvc 0)**

Change Adapter

Virtual Circuit: Enabled  
Bridge: Disabled  
ICMP: Disabled

Static IP Settings  
IP Address: 192.168.241.101  
Subnet Mask: 255.255.255.0  
Gateway:

Encapsulation: PPPoE LLC

ATM  
VPI: 0  
VCI: 35  
Service Category: UBR  
Peak Cell Rate: 0 kbps  
Sustainable Cell Rate: 0 kbps  
Max Burst Size: 0

DHCP Client: Disabled  
Host Name:

MAC Spoofing: Disabled  
Mac Address: 00:00:00:00:00:00

Automatic Reconnect: ☒

Submit Reset

Settings need to be saved to Flash and the router needs to be rebooted for changes to take effect.

Dial-up user may select **PPPoE LLC** or other encapsulation mode according to the information provided by your ISP.

Enter **Service Name** (if required), **Username (user ID)** and **Password** provided by your ISP.

Enter the **VPI** and **VCI**, provided by your ISP.

Tick this **Automatic Reconnect** checkbox to reconnect when connection fails.

Confirm your settings and then click **Submit**.

**Wireless**

WLAN Driver (Marconi) : v3.0.5  
Boot Loader Version : v3.1.1  
Upper MAC Version : M\_UM\_3.1.20  
Lower MAC Version : M2\_LM\_D29598C\_3.1.41  
AP BSSID : 00:00:00:00:00:77

SSID: default  
Channel: 6

Security: ☒ Disable Encryption  
☐ 64 bit ☐ 128 bit

Key Length: 64 bit  
Auth Type: Open System

(The Passphrase should be fewer than 16 characters. You may manually enter your HEX key below and leave Passphrase blank)

Passphrase:

Key 0: c6774663dd  
Key 1: af1bd13ecd  
Key 2: 8e33b2bf1  
Key 3: cf12611e1d

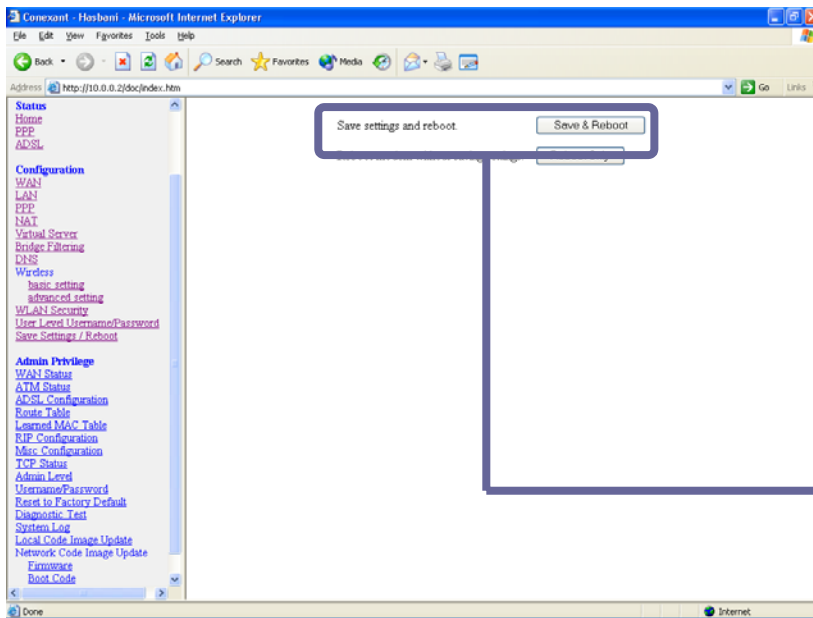
Secret AP: ☒ Disable (Hide SSID)

Reset Submit

Go to **Configuration > Wireless > basic setting** page.

If you do not have a wireless LAN, you can use the Router's default settings. If you have an existing Wireless LAN, configure your **SSID**, **Channel** and other security settings. The Router and wireless clients must use the same SSID, Channel and security settings in order to communicate with each other.

Confirm your settings and then click **Submit**.



Go to **Configuration** > **Save Settings / Reboot** page.

Go to **Save Settings / Reboot** page and then click **Save & Reboot** to save the settings you made to flash ROM.

Congratulations! You have finished the settings of the Router and you may surf the Internet right now.

# User's Manual

# 1. Introduction

---

This Router is a highly integrated, cost-effective solution. All setup and provisioning is accomplished via a simple intuitive Web interface which further enhances the user experience.

## 1.1 Features

- ADSL Compliance
  - Compliant with ADSL standards
    - ◆ Full-rate ANSI T1.413 Issue 2 and ITU G.dmt (G.992.1) standards
    - ◆ Splitterless ITU G.lite (G.992.2) specification
    - ◆ ADSL over POTS (Annex A) and ADSL over ISDN (Annex B)
  - DMT modulation and demodulation
  - Full-rate adaptive modem
    - ◆ Maximum downstream rate of 8 Mbps
    - ◆ Maximum upstream rate of 1 Mbps
- ATM Protocols
  - WAN mode support: PPP over ATM (RFC 2364) and PPP over Ethernet (RFC 2516)
  - LAN mode support: bridged/routed Ethernet over ATM (RFC 1483) and Classical IP over ATM (RFC 1577)
  - ATM Forum UNI 3.1/4.0 PVC
  - Up to 8 VCs (Virtual Circuits)
- Bridge Mode
  - Ethernet to ADSL self-learning Transparent Bridging (IEEE 802.1D)
  - Supports up to 128 MAC learning addresses
- Router Mode
  - IP routing–RIPv2
  - Static routing
  - DHCP (Dynamic Host Configuration Protocol) Server and Client
  - NAPT (Network Address and Port Translation)
  - NAT (Network Address Translation)
  - ICMP (Internet Control Message Protocol)
- Security
  - User authentication for PPP
  - PAP (Password Authentication Protocol)
  - CHAP (Challenge Authentication Protocol)
  - Password protected system management
- Wireless
  - Supports 802.11g data rates of up to 54 Mbps with automatic fallback to 48, 36, 24, 18, 12, 9, and 6 Mbps
  - Supports 802.11b data rates of up to 11 Mbps with automatic fallback to 5.5, 2, and 1 Mbps
  - Supports 64 and 128-bit WEP, WPA (Wi-Fi Protected Access) and WPA-PSK (Pre-Shared Key)
  - Supports 802.11e Quality of Service (QOS)
  - DBPSK, DQPSK and CCK modulation with full-duplex MAC and half-duplex baseband (BB)
  - Number of Channels
    - ◆ USA and Canada: CH1 ~CH11
    - ◆ Europe: CH1 - CH13
    - ◆ Spain: CH10 - CH11
    - ◆ France: CH10 - CH13
    - ◆ Japan: CH1 - CH14

## 1.2 System Requirements

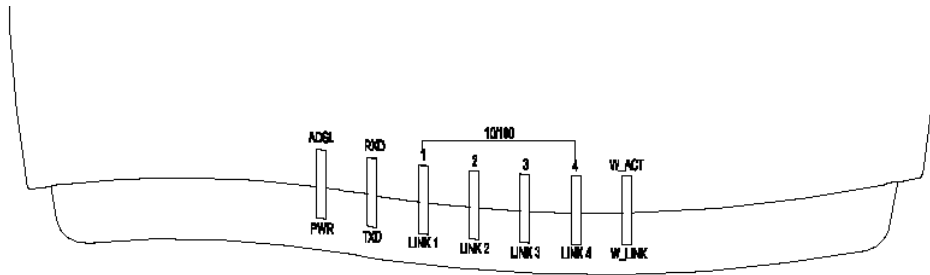
- Pentium III 266 MHz processor minimum
- 128 MB RAM minimum
- 20 MB of free disk space minimum
- Ethernet Network Interface Controller (NIC) RJ45 Port
- Internet Browser
- Ethernet (CAT5) Cable

## 2. Knowing Your Router

When selecting the location for the Router, allow room to access the connections on the rear panel. You will want to place the Router so that you will be able to see the LED indicators on the front panel. It may be convenient for you to locate the Router near the PC you intend to use for initial configuration of the Router.

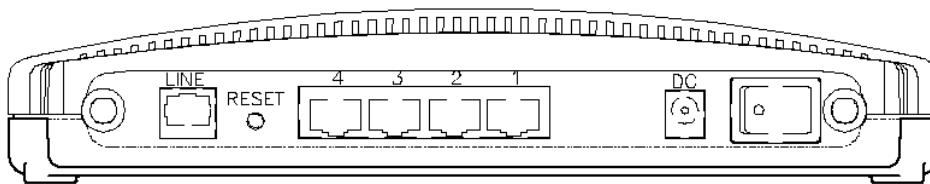
### 2.1 Front Panels

Place the Router in a location that permits an easy view of the LED indicators shown in the front panel diagram below.



### 2.2 Rear Panels

The rear panel of the Router provides access to the power adapter cord connection as well as the port connections.



**LINE:** You can use the twisted-pair ADSL cable (standard telephone cable) included with the Wireless Router to connect to your telephone line. Simply plug one end of the cable into the LINE port (RJ-11 receptacle) on the rear panel of the Wireless Router and insert the other end into the wall jack. This connection provides the link between the Router and the ISPs network including access to the Internet.

**LAN 1-4:** The Wireless Router may be connected to any 10/100BASE-T Ethernet LAN or Ethernet concentrating device. Connection to an Ethernet concentrating device such as a switch or hub should use standard twisted-pair cable with RJ-45 connectors. The dedicated RJ-45 port on the Wireless Router are a crossed (MDI-X) connection ports. Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. Use straight-through cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use crossed cable when connecting it to an uplink (MDI-II) on a hub or switch. When connecting the Router directly to a PC or server use a straight-through cable. A valid connection will be indicated by the LINK LED indicator corresponding to the connected port.



**DC port:** Insert the Power Adapter cord into the power receptacle located on the rear panel of the Router and plug the adapter into a nearby power source. You should see the PWR (Power) LED indicator light up and remain lit.

**RESET button:** The Router comes with a reset button built into the rear panel. Use this button to restore the factory default settings. If you need to reset the Router, press the reset button for 2-3 seconds and then release it. The ADSL LED will stop blinking temporarily and then blink again in about 15 seconds. It means the Router finish rebooting.

## 2.3 LED Indicators

The LED Indicators read as follows:

<b>PWR</b>	Illuminated when the unit is powered on.
<b>ADSL</b>	Illuminated when the physical layer link is activated.
<b>RXD</b>	Illuminated when receiving data.
<b>TXD</b>	Illuminated when sending data.
<b>10/100</b>	Illuminated when the connecting speed at 100 Mbps and non-illuminated indicates the connecting speed at 10 Mbps.
<b>LINK 1-4</b>	Illuminated when the device is connected to LAN port(s). Flashes when transmitting data.
<b>W_ACT</b>	Illuminated when the wireless functionality is activated. Flashes when transmitting data.
<b>W_LINK</b>	Flashes when the wireless functionality is trying to establish a wireless link. Illuminated when the wireless client(s) is connected.

# 3. Login

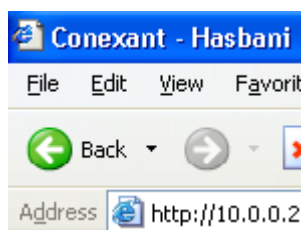
---

There are two levels of access rights/privileges for the Router:

- **Administrator:** User name admin, the administrator account has complete read/write access on all pages (Status, Configuration, Admin Privilege, and Firewall Configuration). Admin account also has FTP server access.
- **User:** User name user, the User account has read/write access to pages under the Status and Configuration sections.

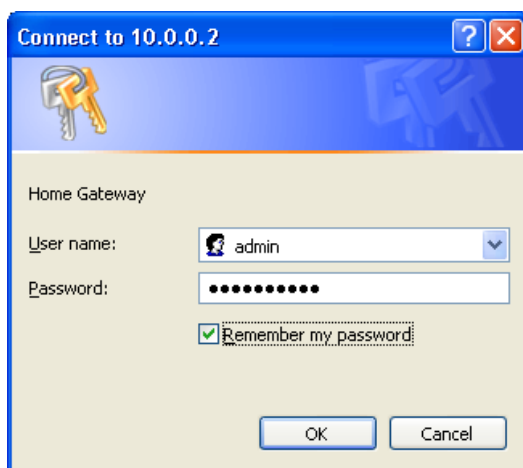
The following steps will enable you to log into the Router:

1. Launch the Web browser (Internet Explorer, Netscape, etc.).
2. Enter the LAN port default IP address (default gateway) `http://10.0.0.2` in the address bar.



3. Entry of the username and password will be prompted. Enter the default login User Name and Password:

The default login User Name of the administrator is **admin**, and the default login Password is **epicrouter**. The default login User Name for the non-administrator is **user**, and the default login Password is **password**.



4. **Remember my password checkbox:** By default, this box is not checked. Users can check this box so that Internet Explorer will remember the User name and Password for future logins. It is recommended to leave this box unchecked for security purposes.

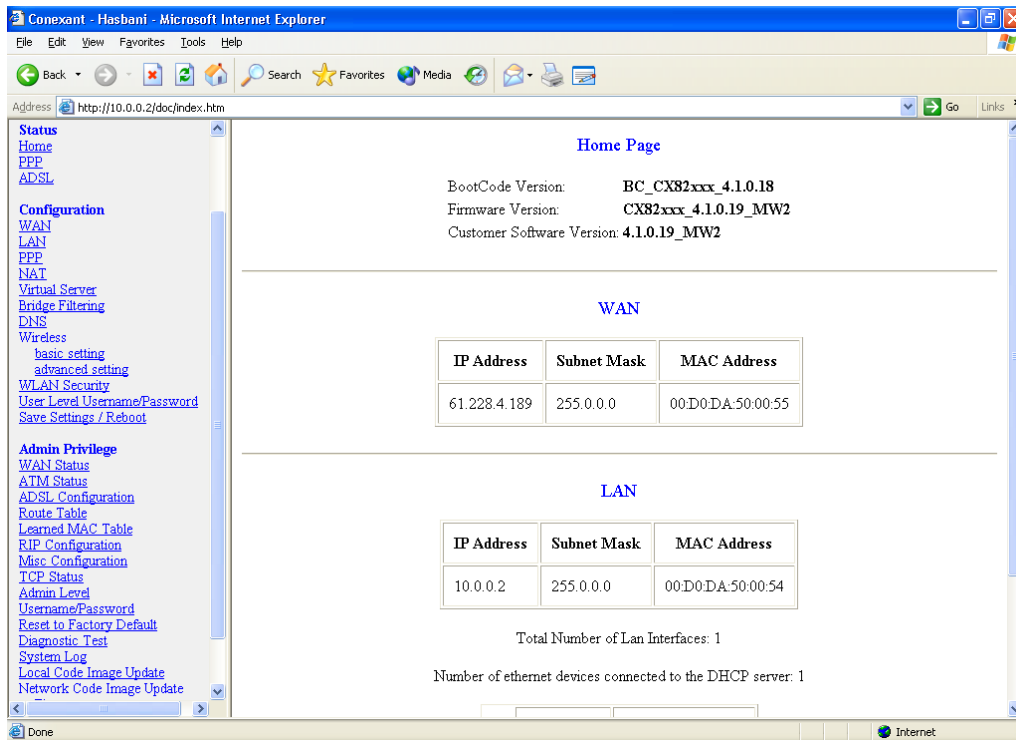
Admin and User passwords can be changed after login. Refer to Section 5.11 for User Password configuration and Section 6.9 for Admin Password configuration for further instruction.

# 4. Status Pages

The links under the **Status** column are associated with the pages that represent the status of system (computer and Router) and interfaces (connections). This includes LAN, WAN, DHCP, PPP, and ADSL status. These pages can be viewed and modified by both **user** and **admin** accounts.

## 4.1 Home Page

The Home page shows the firmware versions; LAN, WAN, and DHCP interface status; and Ethernet connection status.



**Firmware Version:** It is the default version number, which is not changeable.

**Customer Software Version:** It is the version of the firmware that is controllable by the ADSL Modem/Router manufacturer.

**WAN and LAN:** It displays the IP address, Subnet Mask and MAC address for the WAN (ADSL) and LAN interface.

**Total Number of LAN Interfaces:** It displays the total number of available interfaces for the LAN interface. The total number of available interfaces is the amount of computers that are able to hook up to the DHCP Server.

**Number of Ethernet Devices Connected to the DHCP Server:** It displays the DHCP client table with the assigned IP addresses and MAC addresses.



*If there are no devices connected to the DHCP server, then a table will not appear, otherwise a table listing all devices connected to DHCP server will appear on the bottom of the page.*

**Ethernet Link Status:** It displays the link up or down for the Ethernet connection (up if connected, down if not connected).

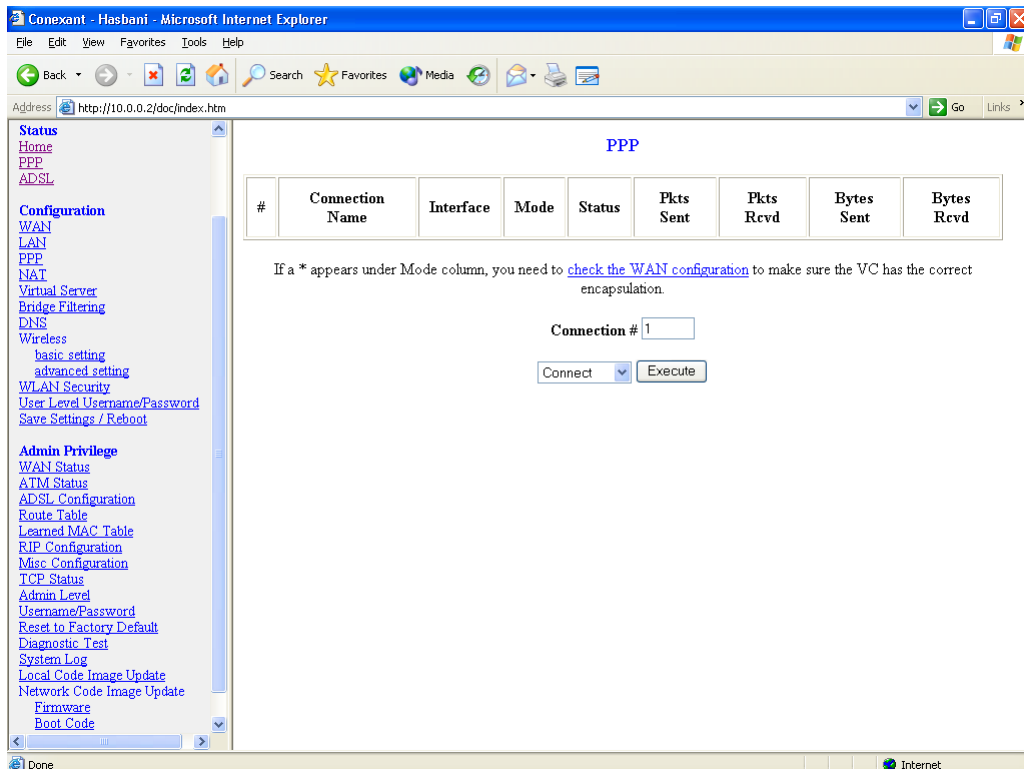
**USB Link Status (reserved function):** It displays the link up or down for the USB connection (up if connected, down if not connected).

## 4.2 PPP Page

The **PPP Status** page shows the status of each PPP session for each PPP interface. This page contains information that is dynamic and will refresh every 8 seconds.



*PPP interfaces can be created, modified, and deleted in the PPP Configuration page. Refer to Section 5.4 for further information.*



**PPP (Point-to-Point Protocol):** The table displays the following fields:

- **Connection Name:** This is user defined. User defined connections for PPP can be created in **PPP Configuration** page.
- **Interface:** States the interface that is being used (PVC0 ... PVC7).
- **Mode:** There are two available modes for the connection:
  - PPP over Ethernet (PPPoE)
  - PPP over ATM (PPPoA)
- **Status:** States whether PPP connection is Connected or Not Connected.
- **Packets Sent:** Number of packets sent by a particular PPP Connection.
- **Packets Received:** Number of packets received by a particular PPP Connection.
- **Bytes Sent:** Number of bytes sent by a particular PPP Connection.
- **Bytes Received:** Number bytes received by a particular PPP Connection.

**Connect and Disconnect:** It allows you to manually connect/disconnect the PPP connection for each PPP interface. In other words, each PPP session can be connected and disconnected individually.

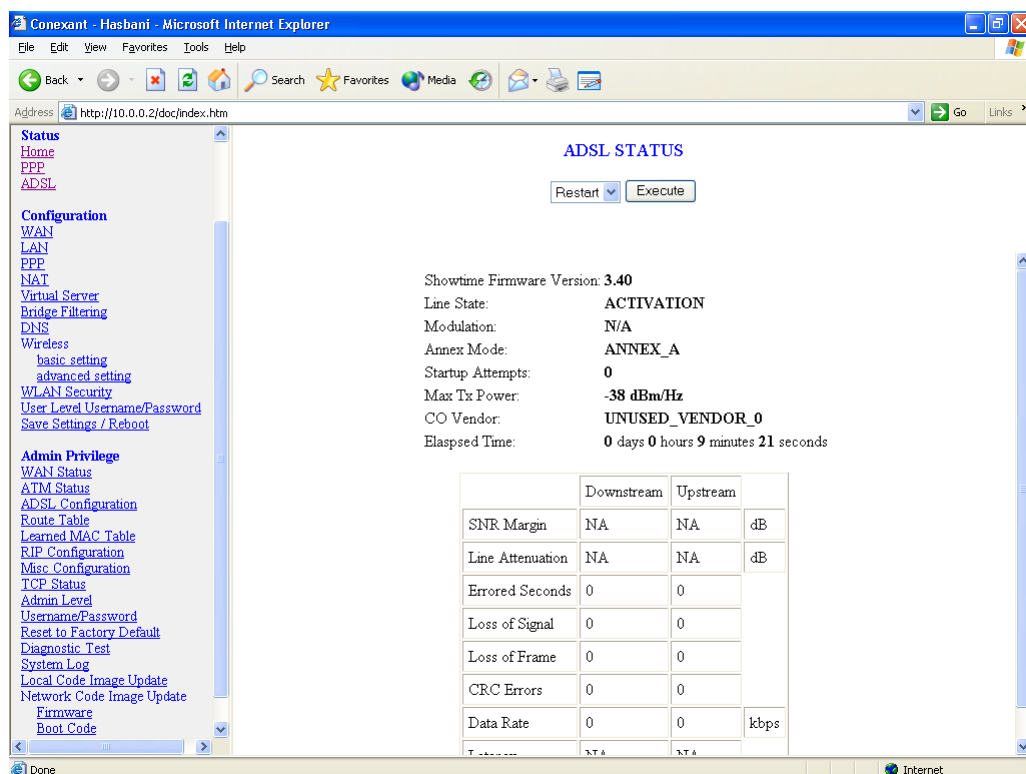
- **Connection #:** Specifies the PPP session to be connected/disconnected.
- **Connect/Disconnect Execute:** Press this button to either connect or disconnect.

Connection status dialog will be displayed below the **Execute** button after it is pressed.  
Sample dialog with explanation:

- **PPP X: Connecting...** This is displayed while the PPP session is attempting to connect to the ISP.
- **PPP X: Connect ERROR** This is displayed when a connection cannot be made due to an error.
- **PPP X: is currently not connected** This is displayed when a disconnect attempt is made on a session that is not currently connected.
- **PPP X: does not exist!** This is displayed when a connect or disconnect attempt is made on a session number that does not exist.

## 4.3 ADSL Page

The **ADSL Status** page shows the ADSL physical layer or link status. The information displayed on this page is either inherent to the Router or set by the ADSL Central Office (CO) DSLAM, neither of which cannot be changed by the user. This page contains information that is dynamic and will refresh every 2 seconds.



**ADSL STATUS**

Restart Execute

Showtime Firmware Version: 3.40

Line State: ACTIVATION

Modulation: N/A

Annex Mode: ANNEX\_A

Startup Attempts: 0

Max Tx Power: -38 dBm/Hz

CO Vendor: UNUSED\_VENDOR\_0

Elapsed Time: 0 days 0 hours 9 minutes 21 seconds

	Downstream	Upstream	
SNR Margin	NA	NA	dB
Line Attenuation	NA	NA	dB
Errored Seconds	0	0	
Loss of Signal	0	0	
Loss of Frame	0	0	
CRC Errors	0	0	
Data Rate	0	0	kbps

**Restart/Stop Execute:** It allows you to stop or restart the ADSL connection by selecting the appropriate action and clicking **Execute**.

**Showtime Firmware Version:** It displays the ADSL data pump firmware version.

**ADSL Line Status:** It displays the ADSL connection process and status. The different states for this field are as follows:

- **Activation:** The Router is in this state when it is attempting to start the activation process.
- **Initialization:** The Router is initializing handshake with the CO.
- **Training:** It is a part of the handshake process with the CO.
- **Channel Analysis:** It is a part of the handshake process with the CO.
- **Exchange:** It is a part of the handshake process with the CO.
- **Down:** It indicates that the ADSL connection is down.
- **Showtime:** It indicates that a connection has been established between the Router and the CO.

**ADSL Modulation:** It displays the ADSL modulation status, which can either be G.dmt or T1.413.

**ADSL Annex Mode:** It displays the ADSL annex mode, which can either be Annex A or Annex B.

**ADSL Startup Attempts:** It displays the number of ADSL connection attempts after loss of showtime. A connection attempt is recorded only if showtime is attained.

**ADSL Max TX Power:** It displays the transmit output power level of the CPE (Customer Premise Equipment), which is the transmit output power level of the Router.

**ADSL CO Vendor:** It displays the Central Office (CO) DSLAM vendor name, if available. If the Router is not connected to an ADSL vendor, then 'UNUSED\_VENDOR\_0' will appear in this field.

**Elapsed Time:** It displays the time of the Router has been in operation. This is the amount of time the Router is on, not the amount of time it is connected to the PC or in showtime status.

A table contained the information of **SNR Margin**, **Line Attenuation**, **Errored Seconds**, **Loss of Signal**, **Loss of Frame**, **CRC Errors**, **Data Rate**, and **Latency** is also available.

# 5. Configuration Pages

The links under **Configuration** column are associated to the pages that represent the configurations of system and interfaces. These pages can be viewed and modified by both user and admin accounts.



*When any settings are changed, please go to the Save Settings page to save the new setting(s) and reboot the Router. Changes will not take effect until the settings are saved and the Router is rebooted. If power is lost before saving, all new configurations since the last save will be lost, even if they were submitted.*

## 5.1 Modes

Table 5-1 lists the mode configurations.

Table 5-1 Mode Configuration

WAN Configuration	Bridge Mode	Router Mode (PPPoA/PPPoE)	Router Mode (Dynamic IP)	Router Mode (Static IP)	Half Bridge
IP Address	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP	Automatically assigned by ISP
Subnet Mask	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP	Automatically assigned by ISP
Gateway	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP	Automatically assigned by ISP
Encapsulation	1483 Bridged IP LLC, 1483 Bridged IP VC-Mux	PPPoA LLC/VC-Mux, PPPoE LLC/VC-Mux	1483 Bridged/Routed IP LLC, 1483 Bridged/Routed IP VC-Mux, Classical IP over ATM	1483 Bridged/Routed IP LLC, 1483 Bridged/Routed IP VC-Mux, Classical IP over ATM	PPPoA LLC/VC-Mux, PPPoE LLC/VC-Mux
Bridge	Enabled	Disabled	Disabled	Disabled	Disabled
PPP Service	N/A	Provided by ISP	N/A	N/A	Provided by ISP
PPP User Name	N/A	Provided by ISP	N/A	N/A	Provided by ISP
PPP Password	N/A	Provided by ISP	N/A	N/A	Provided by ISP
DHCP Client Enable	Unchecked	Unchecked	Checked	Unchecked	Unchecked
PPP Half Bridge	Disabled	Disabled	Disabled	Disabled	
DHCP Server	Disabled	Enabled	Enabled	Enabled	
NAT	Disabled	Enabled (Dynamic NAPT)	Enabled (Dynamic NAPT)	Enabled (Dynamic NAPT)	Disabled
DNS Proxy	Disabled	Enabled	Enabled	Enabled	Disabled

**Bridge Mode:** Bridge Mode is used when there is one PC connected to the LAN-side Ethernet port. IEEE 802.1D method of transport bridging is used to bridge between the WAN (ADSL) side and the LAN (Ethernet) side, i.e., to store and forward.

**Router Mode:** Router Mode is used when there is more than one PC connected to the LAN-side Ethernet port. This enables the ADSL WAN access to be shared with multiple nodes on the LAN. Network Address Translation (NAT) is supported so that one WAN-side IP address can be shared among multiple LAN-side devices. DHCP is used to serve each LAN-side device and IP address.

**PPP Half Bridge:** Although the Router mode is capable of terminating the PPP in the modem and hence does not require PPPoE client software on the host PC, there are some disadvantages to Router mode when only single-user support is required. For instance, Router mode uses NAT which requires ALG support. PPP Half Bridge also terminates the PPP in the modem and does not require a PPPoE client on the PC. However, PPP Half Bridge does not use NAT and is not limited by ALGs. PPP Half Bridge will work with Ethernet interface to the PC.

**Single-User Mode:** Only one computer is connected at the LAN side through Ethernet.

**Multi-User Mode:** Multiple computers are connected at the LAN side through Ethernet.

## 5.2 WAN Configuration

The **WAN configuration** page allows you to set the configuration for the WAN/ADSL ports. Before you enter the **WAN Configuration** page, you will be asked to select an adaptor (PVC0 through PVC7) first. Once you select the adaptor, then following page will appear.

**Virtual Circuit:** Select Enable to activate the current PVC configuration. The current PVC is displayed at the top of the page in parenthesis. Default is Enabled for PVC0 and Disabled for PVC1-PVC7.

**Bridge:** Enable to connect the LAN to the WAN (bridge the two connections). This is available in Bridge Mode only (see Table 5-2). Default is Disabled.

**IGMP:** IGMP (Internet Group Management Protocol) relay/proxy specification and environment, default is Disabled. IGMP is available in all modes and all encapsulations. Support IGMP proxy/relay function for Router, based on the following requirement and cases:



- On CO side, there must be at least one IGMP querier (router) present. IGMP querier will send IGMP query packet. The Router is responsible to relay these IGMP queries to Ethernet.
- End-user multicast application device sends IGMP report while receiving IGMP query or being activated by the user. The Router should be responsible to proxy (that is, change source IP to Router's WAN IP) the IGMP report to ADSL WAN side, including all PVCs. The same case is for IGMP leave packet.
- Not necessary to relay multicast routing between two ADSL PVCs or two interfaces in LAN side.
- Special purpose multicast packet (such as RIP 2 packet) should run without Interference.

Table 5-2. Packet Process

Rx Entity	Packet Class	TTL	Action
ADSL	IGMP query	1	Relay to Ethernet
	IGMP report	1	Ignore
	IGMP leave	1	Ignore
	General Multicast IP	-	Relay it to Ethernet
Ethernet	IGMP query	1	Ignore
	IGMP report	1	Relay to all ADSL PVCs
	IGMP leave	1	Relay to all ADSL PVCs
	General Multicast IP	-	Ignore



*Before the IGMP mode is enabled; please go to the Miscellaneous Configuration page to enable the IGMP proxy. Otherwise, the IGMP selection will not be valid.*



Where can I download the free software to test IGMP?

**Answer:** Please go to this link <http://manimac.itd.nrl.navy.mil/MGEN/>.

**Encapsulation:** The different types of encapsulation include PPPoA VC-Mux, PPPoA LLC, 1483 Bridged IP LLC, 1483 Routed IP LLC, 1483 Bridged IP VC-Mux, 1483 Routed IP VC-Mux, Classical IP over ATM, PPPoE VC-Mux, PPPoE LLC, and PPPoENone.

## 5.2.1 ATM

**VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.

Range: 0-255      Default: 0

**VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.

Range: 0-65535      Default: 35

**Service Category:** This field allows you to select from the following service categories.

- **UBR (default):** When configured as UBR (Unspecified Bit Rate), traffic is delivered with best efforts but with no guarantee. This allows for fluctuation in times of temporary increase of available bandwidth. For example, if a PVC with CBR is temporarily inactive, the PVC(s) with UBR will utilize that bandwidth while it is available. UBR is intended for applications that do not require any maximum bound on the transfer delay.
- **CBR:** When a PVC is specified as a CBR (Constant Bit Rate), that PVC is guaranteed a certain bandwidth, characterized by the Peak Cell Rate (PCR). The CBR does not have to transmit with a peak cell rate, and when it does, it is only when the bandwidth specified by the PCR is guaranteed.
- **VBR-nrt:** An PVC enabled with VBR-nrt (Variable Bit Rate - non real time) can transmit a cell only if the PVC has a token available. The PVC accumulates tokens at the rate of the Sustainable Cell Rate, and the PVC can only accumulate a maximum of the value specified by Maximum Burst Size tokens.

When a PVC has a token available, it can transmit cells at the rate of PCR. After a cell is transmitted, the PVC loses the token it has accumulated.



*In the case of multiple PVCs, CBR specified PVCs will have higher priority than PVCs with UBR. For example, the CBR PVCs will take their bandwidth and the remaining bandwidth will be split among the UBR PVCs. In the case of total PVC CBR bandwidth exceeding ADSL upstream, the total upstream bandwidth will be shared proportionally to the bandwidth allocated for each CBR PVC.*

**Peak Cell Rate:** This value specifies the maximum, and in some cases guaranteed, cell rate for CBR and VBR-nrt. Peak Cell Rates are typically measured in Cells/Second, however, the user entered value is in kbps and is then converted by the firmware.

Range: 0-32767

Default: 0

**Sustainable Cell Rate:** It is the sustained rate at which a PVC enabled with VBR-nrt can transmit ATM cells. Sustainable Cell Rate (SCR) can be considered as the true reserved bandwidth for a PVC.

Range: 0-32767

Default: 0

**Max Burst Size:** It is the number of cells a PVC enabled with VBR-nrt can transmit continuously at peak cell rate (PCR).

Range: 0-32767

Default: 0

## 5.2.2 DHCP Client

**DHCP Client:** It is to enable or disable (default) the Router WAN as a DHCP client, where the ISP would be the DHCP server. DHCP Client is generally used in the following encapsulations: 1483 Bridged IP LLC, 1483 Routed IP LLC, 1483 Bridged IP VC-MUX, 1483 Routed IP VC-Mux, and Classical IP over ATM. This option is for non-static (dynamic) IP addresses.

**Host Name:** When DHCP Client is Enabled, copy the ISP recognized Host Name here. The Host Name can be up to 19 characters.

### 5.2.3 MAC Spoofing

**MAC Spoofing:** Enable MAC Spoofing to make a different MAC Address appear on the WAN side. This is also used to solve the scenario where the ISP only recognizes one MAC Address. System default is Disable.

**MAC Address:** When MAC Spoofing is enabled, copy the ISP-recognized MAC address here. Format for MAC address is six pairs of hexadecimal numbers (0-9, A-F) separated by colons. System default is: 00:00:00:00:00:00.

### 5.2.4 Static IP Settings

Static IP Settings are for users who have a Static IP Address (WAN side) from their ISP.

**IP Address:** It is the static IP Address given by the ISP.

Range: x.x.x.y, where  $0 \leq x \leq 255$  and  $1 \leq y \leq 254$       Default: 192.168.241.101

**Subnet Mask:** It is the subnet mask given by the ISP.

Range: x.x.x.x, where  $0 \leq x \leq 255$       Default: 255.255.255.0

**Gateway:** It is the Gateway given by the ISP.

Range: x.x.x.y, where  $0 \leq x \leq 255$  and  $1 \leq y \leq 254$       Default: 0.0.0.0

## 5.3 LAN Configuration

The LAN configuration page allows you to set the configuration for the LAN port.

Conexant - Hasbani - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address <http://10.0.0.2/doc/index.htm> Go Links

**Status**  
[Home](#)  
[PPP](#)  
[ADSL](#)

**Configuration**  
[WAN](#)  
[LAN](#)  
[PPP](#)  
[NAT](#)  
[Virtual Server](#)  
[Bridge Filtering](#)  
[DNS](#)  
[Wireless](#)  
[basic setting](#)  
[advanced setting](#)  
[WLAN Security](#)  
[User Level Username/Password](#)  
[Save Settings / Reboot](#)

**Admin Privilege**  
[WAN Status](#)  
[ATM Status](#)  
[ADSL Configuration](#)  
[Route Table](#)  
[Learned MAC Table](#)  
[RIP Configuration](#)  
[Misc Configuration](#)  
[TCP Status](#)  
[Admin Level](#)  
[Username/Password](#)  
[Reset to Factory Default](#)  
[Diagnostic Test](#)  
[System Log](#)  
[Local Code Image Update](#)  
[Network Code Image Update](#)  
[Firmware](#)  
[Boot Code](#)

**LAN Configuration**

IP Address:

Subnet Mask:

**DHCP Server**

DHCP address pool selection:

User Defined Start Address:

User Defined End Address:

DHCP Gateway Selection:

User Defined Gateway Address:

Lease Time:  days  hours  minutes  seconds

**DHCP Relay**

DHCP Relay Target IP:

User Mode:

[Ethernet Mode Setting](#)

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.

[Save Configuration](#)

Internet

**LAN IP Address & Subnet Mask:** The LAN IP Address is what the computer uses to identify and communicate with the Router (this is the address you enter in the address bar of Internet Explorer to access these pages). You can change this to another private IP address and subnet mask, such as 192.168.1.2 and 255.255.255.0.

Range: x.x.x.x, where  $0 \leq x \leq 255$

Default is 10.0.0.2 and 255.0.0.0 (respectively)

### 5.3.1 DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that allows network administrators to manage and assign IP addresses to computers within the network. DHCP provides a unique address to a computer in the network which enables it to connect to the Internet through Internet Protocol (IP). DHCP is controlled by the DHCP Server. The following settings allow you to configure the DHCP server.

**DHCP Server:** Select Enabled (default) to activate DHCP Server.

**DHCP Address Pool Selection:** Two types of Address Pool selections are available, with System Allocated as the default.

- **System Allocated:** The DHCP address pool is based on LAN port IP address plus 12 IP addresses. For example, when the LAN IP address is 10.0.0.2; the DHCP address pool the range from 10.0.0.3 to 10.0.0.14.
- **User Defined:** When User Defined is selected, the DHCP address pool starts at the User Defined Start Address and ends at the User Defined End Address. The maximum pool size can be 253 IP addresses: 255 total IP addresses - 1 broadcast address - 1 LAN port IP address.

**User Defined Start Address:** It is the starting IP address of the DHCP pool for User Defined DHCP Address Pool Selection.

Range: x.x.x.x, where  $0 \leq x \leq 255$

Default: 10.0.0.4

**User Defined End Address:** It is the last IP address in the DHCP pool for User Defined DHCP Address Pool Selection.

Range: x.x.x.x, where  $0 \leq x \leq 255$

Default: 10.0.0.15

**DHCP Gateway Selection:** The default setting for the DHCP Gateway Selection is **Automatic**. You can select **User Defined** and specify **User Defined Gateway Address**. The DHCP server will issue the **User Defined Gateway Address** to the LAN DHCP clients.

**User Defined Gateway Address:** The purpose for the User Defined Gateway Address is to have two gateway addresses, as the LAN IP Address at the top of the **LAN Configuration** page is also a gateway address.

**Lease time:** The Lease time is the amount of time a network user will be allowed to connect with DHCP server. If all fields are 0, the allocated IP addresses will be effective forever.

**Ranges for Lease Time fields:** Days 0-36500, Hours 0-23, Minutes 0-59, Seconds 0-59, default value is 1 days 0 hours 0 minutes 0 seconds.

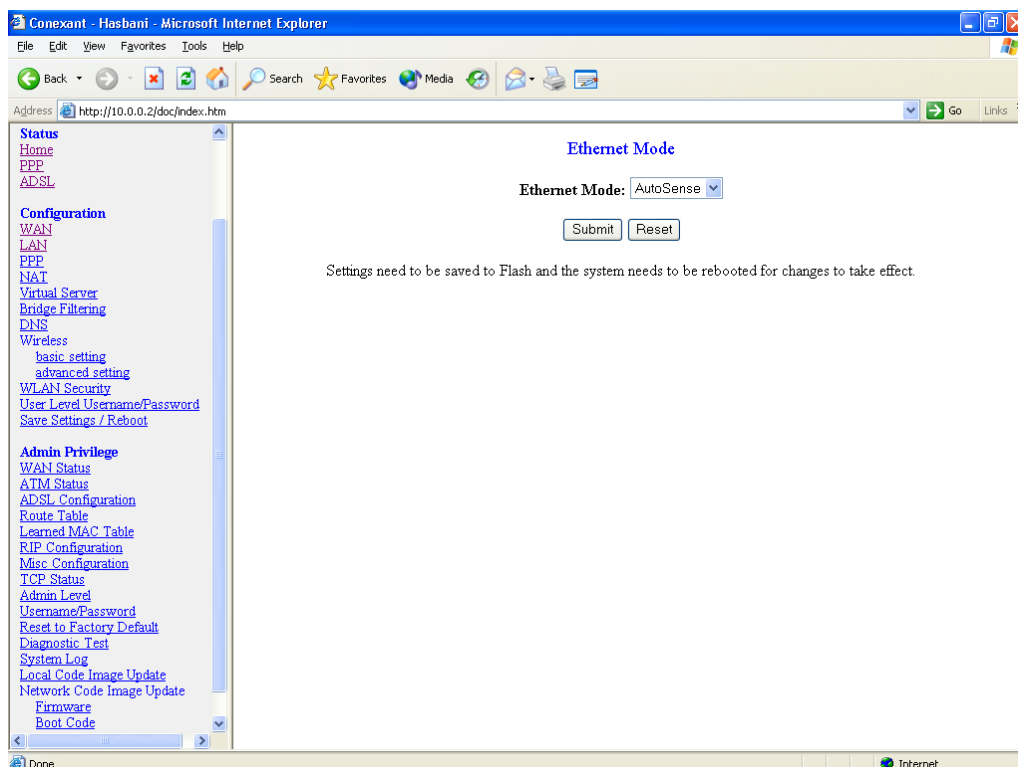
**User mode:** Under the **Single User** mode, the DHCP server only allocates one IP address to a local PC. Under the **Multiple User** mode (default), the DHCP server allocates the IP addresses specified by the DHCP address pool.

**Save Configuration:** Clicking this will link you to the **Save Settings / Reboot** page.

### 5.3.2 Ethernet Mode Setting

The Ethernet Mode configuration page allows you to set the LAN port into the following modes:

- **AutoSense (default):** The Router will automatically sense which mode to use, selecting between 100 Mbps Full Duplex, 100 Mbps Half Duplex, 10 Mbps Full Duplex, and 10 Mbps Half Duplex.
- **100 Mbps Full Duplex:** Data can be transferred and received simultaneously at the transfer rate of 100 Mega-bits per second.
- **100 Mbps Half Duplex:** Data cannot be transferred and received at the same time. For example, data can be sent, and once the transmission is complete, data can be received. This is done at a transfer rate of 100 Mega-bits per second.
- **10 Mbps Full Duplex:** Data can be transferred and received simultaneously at the transfer rate of 10 Mega-bits per second.
- **10 Mbps Half Duplex:** Data cannot be transferred and received at the same time. For example, data can be sent, and once the transmission is complete, data can be received. This is done at a transfer rate of 10 Mega-bits per second.



## 5.4 PPP Configuration

The **PPP Configuration** page allows you to configure multiple PPP sessions for each PVC. Multiple PPP sessions enables you to set up different connection settings and be able to toggle/choose those settings for each PVC. The Router can support up to total of 16 PPP sessions, and each PVC can support up to 8 PPP sessions. The multiple PPP sessions may be configured with any combination over 8 PVCs.

### 5.4.1 PPP Account Configuration

To begin PPP Session configuration, you must first go to the **PPP Account Configuration** page (below) to set up an account. The link to this page can be found on the **PPP Configuration** page. On the **PPP Account Configuration** page, you must configure the Account ID, User Name and Password.

PPP Account Configuration

Acct Id

User Name

Password

#	Account Name	User Name
1	simple ppp account Pvc 0	84443895@hinet.net

The number of PPP accounts is 1

[Go back to PPP Configuration](#)

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.

**Account ID:** It allows you to create an account ID to help distinguish different accounts, up to 16 maximum. The Account ID can be up to 31 characters.

**User Name:** Enter the PPP user name (provided by the ISP). The User Name can be up to 127 characters.



*You cannot have two different user accounts with the same account name. If a different User Name with an already existing Account ID is submitted, it will replace the previous account with that Account ID. You can have the same User Name and Password for two different accounts (Account ID).*

**Password:** Enter the PPP password (provided by the ISP). The Password is not needed to delete or modify the account. The Password can be up to 127 characters.

**PPP Account Configuration Status** table will be displayed at the bottom of this page to show all the accounts. The status table does not display the password.

**The Number of PPP Accounts:** It displays the total number of PPP Accounts entered.

## 5.4.2 PPP Session Configuration

Once you set up a PPP Account, you can begin PPP Session configuration either by clicking the **Go back to PPP Configuration** link on the **PPP Account Configuration** page or clicking on **PPP** under the **Configuration** menu on the left hand side of the browser.

**Session Name:** It allows you to enter a Session Name. This is user defined to help distinguish different session for different PPP accounts and different PVCs.

**PVC:** It allows you to choose the specific PVC for the PPP session.

**Service Name:** The Service Name of the PPP session is required by some ISPs. If the ISP does not provide the Service Name, please leave it blank.

**Account to Use:** You must select an account created in PPP Account Configuration page here.

**Disconnect Timeout:** The Disconnect Timeout allows you to set the specific period of time, in minutes, to disconnect from the ISP. The default is 0, which means never disconnect from the ISP.

Range: 0-32767

Default: 0

**PPP Idle Timer Config:** It will link you to the **PPP Disconnect Timer Configuration** page (see Section 5.4.3).

**MRU:** The MRU (Maximum Receive Unit) field indicates the maximum size IP packet that the peer of PPP connection (this device) can receive. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size.

Range: 0-32767                      Default: 1492

**MTU:** Maximum Transmission Unit (MTU) is the largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size.

Range: 0-32767                      Default: 1492

**MSS:** Maximum Segment Size is the largest size of data that TCP will send in a single, unfragmented IP packet. The LAN client and the WAN host will indicate their MSS during the TCP connection handshake.

Range: 0-32767                      Default: 1432

**Lcp Echo Interval:** It is the time interval, in seconds, between PPP session connection attempts.

Range: 0-32767                      Default: 10

**Lcp Echo Maximum Consecutive Failure:** It is the number of times a PPP session can fail while trying to connect before stopping. If a PPP session fails this number of times, you must manually reconnect the PPP session.

Range: 0-32767                      Default: 6

**Authentication:** The different types of available authentications are:

- **Auto (default):** When auto is selected, PAP mode will run by default. However, if PAP fails, then CHAP will run as the secondary protocol. This is the default setting.
- **PAP:** Password Authentication Procedure. Authentication is done through username and password.
- **CHAP:** Challenge-Handshake Authentication Protocol. Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

**Automatic Reconnect:** When it is checked, the Router will reconnect a PPP session when it is terminated by the ISP. If a PPP session is terminated under any other conditions (i.e. by Disconnect Timeout or manual disconnect), the Automatic Reconnect will not reconnect the session. This box is unchecked by default.

**PPP Configuration Status:** A table will be displayed at the bottom of this page to show all related information of PPP configuration.



### 5.4.3 PPP Disconnect Timer Configuration

The **PPP Disconnect Timer Configuration** page enables you to configure what action will bring a PPP Session out of the Idle state (disconnected state) and reset the Idle Timer. This is done by specifying criteria contained in packets, namely IP Protocol and Port. The Idle Timer refers to the Disconnect Timeout, specified on the **PPP Configuration** page.

The PPP Idle Timer is recommended to be disabled (**Disconnect Timeout** = 0 on PPP Configuration page) if you want an always-on connection. **PPP Disconnect Timer Configuration** is intended for users who do not desire an always-on connection and/or their ISP charge by connection time.

Conexant - Hasbani - Microsoft Internet Explorer

Address: http://10.0.0.2/doc/index.htm

**PPP Disconnect Timer Configuration**

The settings on this page are used to determine the traffic that will:

- 1) Reset the PPP disconnect timer counter
- 2) Re-establish a PPP connection (only if "PPP Reconnect on WAN Access" is enabled)

---

**Enable/Disable Idle Timer Filter**

☐ All Traffic will reset Idle Timer (ignore filter below)

☒ Only filtered traffic will reset Idle Timer (use filter below)

---

**Apply Filter To:**

☐ Inbound Traffic Only

☒ Outbound Traffic Only

☐ Inbound and Outbound Traffic

---

**Filter Details:**

Protocol # Port # Action

0 0 Add

#	IP Protocol	Protocol #	Port #
1	TCP	6	80
2	TCP	6	23
3	TCP	6	21
4	TCP	6	20
5	UDP	17	53

Number of Entries is 5

**Well Known Ports**

Application	Port Number
Any	0
FTP-Data	TCP 20
FTP-Control	TCP 21
Telnet	TCP 23
SMTP	TCP 25
HTTP	TCP 80
DNS	UDP 53

#### 5.4.3.1 Enable/Disable Idle Timer Filter

**All Traffic will reset Idle Timer (ignore filter below):** Selecting this option will disable the PPP Idle Timeout filter and allow any traffic through any protocol or port to reset the idle timer. The only dependency is that the traffic must correspond with the Filter Application (Inbound and/or Outbound). For example, if **Outbound Traffic Only** is selected, only traffic in the outbound direction will reset the idle timer. When this option is selected, all user configured criteria (displayed in the filter table) is bypassed.

**Only filtered traffic will reset the Idle Timer (use filter below):** Selecting this option will enable the PPP Idle Timeout filter and only allow traffic specified in the filter table to reset the idle timer. The traffic specified in the filter table must also correspond with the Filter Application selection. For example, outbound traffic with criteria matching that of the filter table will only be allowed to pass if either **Outbound Traffic Only** or **Inbound and Outbound Traffic** is selected.



*PPP reconnect on WAN access must be enabled for the Idle Timer to reconnect a PPP Session when a request is made from the LAN to the WAN.*

#### 5.4.3.2 Filter Application

The Filter Application consists of three options that determine which sources (LAN and/or WAN) will be able to reset the Idle Timer and reconnect the PPP session.

**Inbound Traffic Only:** Selecting this option will allow PPP requests from the WAN side to reset the Disconnect Timeout timer. Note that requests from the WAN side cannot bring a PPP Session out of Idle state. This is because when a PPP Session is in Idle state, the connection is down (if they match the filter table criteria).

**Outbound Traffic Only (default):** When this option is selected, PPP sessions can only be activated (Idle Timeout) when a request is made on the LAN side to the WAN side. The disconnect timer will reset when outbound traffic is detected (if they match the filter table criteria).

**Inbound and Outbound Traffic:** Selecting this will allow both WAN and LAN source packets to reset the idle timer.

#### 5.4.3.3 Filter Details

The table displayed in the Filter Details section of the page shows all the current Idle Filters. Traffic must match the criteria of one of these filters in order to cause an Idle Timeout, unless **All Traffic will reset Idle Timer** is selected. As a default and starting point for configuration, WWW browsing (HTTP), FTP, and Telnet related packets are part of the filter table.

**IP Protocol:** It is the IP Protocol name corresponding to the Protocol Number.

**Protocol #:** It is the IP protocol (number) through which the PPP session can be activated. The Protocol Numbers for filters are:

- TCP Protocol Number: 6
- UDP Protocol Number: 17
- ICMP Protocol Number: 1
- IGMP Protocol Number: 2

**Port #:** It is the Port through which the PPP session can be activated. The default filters are:

- HTTP TCP Port: 80
- FTP TCP Port: 20 and 21

- Telnet TCP Port: 23
- DNS UDP: 53

**Action:** You can add a rule by entering the appropriate information, selecting **Add** on the **Action** dropdown menu, and clicking **Submit**. To delete an entry, you can enter the information of an entry that already exists on the table, select **Delete** on the **Action** dropdown menu, and click **Submit**.

#### 5.4.4 PPP Miscellaneous Configuration

These options can be found on the **Miscellaneous Configuration** page under **Admin Privilege**.

**PPP Half Bridge:** When PPP Half Bridge is enabled, only one PC is able to access the Internet, and the DHCP server will duplicate the WAN IP address from the ISP to the local client PC. Only the PC with the WAN IP address can access the Internet. System default is Disabled.

**PPP reconnect on WAN access:** If enabled, the PPP session will automatically establish a connection when a packet tries to access the WAN. System default is Disabled.

**Connect PPP when ADSL link is up:** If this option is enabled, the Router will connect the PPP session whenever an ADSL connection is established. If this option is disabled, the PPP session will not connect whenever the ADSL Showtime is reached. System default is Enabled.



If the PPP session is disconnected after the Disconnect Timeout, how can I reconnect it?

**Answer:** You have to go to the PPP Status page, enter the correct connection number, select the Connect option in the dropdown menu, and then click Execute. This will restart the PPP session.



What can I do to ensure an always-on connection with my PPP session?

**Answer:** There are two things you should do: 1) Make sure you have '0' in the **Disconnect Timeout** field. This will make sure that the PPP session is not disconnected from the user side. 2) Make sure the **Automatic Reconnect** box is checked. This will cause the Router to automatically reconnect if the connection is severed from either the ISP side or the user side.

Action	Manual PPP (Fee Based)	PPP Timeout (Fee Based)	PPP Always-on
Connect PPP when ADSL link is up	Disabled	Enabled	Enabled
Disconnect Timeout	0	Set Timeout	0
PPP Reconnect on WAN access	Disabled	Enabled	Disabled
Automatic Reconnect	Disabled	Disabled	Enabled



What is the difference between PPP Connect on WAN Access and the Automatic Reconnect?

**Answer:** For the PPP connect on WAN access, the PPP will be automatically reconnected when an URL is entered in the browser (packet interested in going out the WAN). For the Automatic Reconnect, it will reconnect the PPP session whenever it is terminated by ISP.

## 5.5 NAT Configuration Pages

The **NAT Configuration** page allows you to set the configuration for the Network Address Translation. The NAT module provides Dynamic Network Address and Port Translation (**Dynamic NAPT**) capability between LAN and multiple WAN connections, and the LAN traffic is routed to appropriate WAN connections based on the destination IP addresses and the Route Table. This eliminates the need for the static NAT session configuration between multiple LAN clients and multiple WAN connections.

When **Dynamic NAPT** is chosen (default), there is no need to configure the NAT Session and NAT Session Name Configuration.

**NAT Session Name Configuration**

Session Name	Interface	Action
<input type="text"/>	Ip Pvc 0	Add

#	Session Name	Interface
---	--------------	-----------

[Go back to NAT Configuration](#)

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.

Number of NAT Sessions 0

**Session Name:** It allows you to enter a Session Name to help distinguish different NAT Sessions for different interfaces among different PPP sessions and PVCs.

The Session Name can be up to 31 characters, and there can be up to 16 different NAT session names.

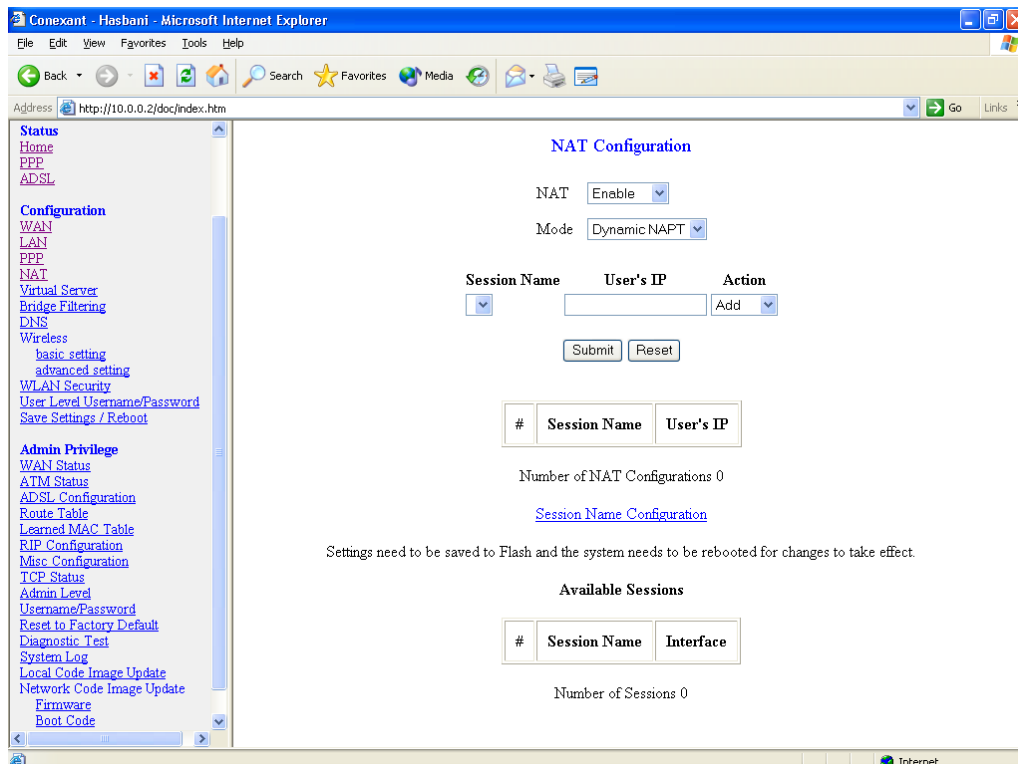
**Interface:** It allows you to choose specific WAN Interfaces (PVC or PPP Session) for NAT Session. The options for this field are PVC0 ... PVC7 and any PPP session that was created by the user.

**NAT Session Name Status:** This table is displayed at the bottom of this page to show all the NAT Session Names with their corresponding WAN Interfaces.

**Number of NAT Configurations:** It displays the total number of NAT Sessions entered.



*NAT allows only one entry (User IP) per session, while NAPT allows many entries (User IPs) per session.*



**NAT:** Use this field to Enable/Disable NAT. Default is Enable.

**Mode:** Options for the NAT dropdown menu are:

- **NAT:** Static peer-to-peer mode (1x1).
- **NAPT:** Static multiple mapping mode (1xN).
- **Dynamic NAPT (default):** Dynamic multiple mapping mode (NxN).

**Session Name:** It allows you to select the session from the configured NAT Session Name Configuration.

**User's IP:** It allows you to assign the IP address to map the corresponding NAT/NAPT sessions.

**Session Name Status:** This table will be displayed at the middle of the page to show the Session Name with its corresponding IP Address.

**Number of NAT Configurations:** It displays the total number of NAT Sessions entered.

**Available Sessions:** This table will be displayed at the bottom of the page to show all the available Session Names with their corresponding WAN Interface.

**Number of Sessions:** It displays the total number of NAT Sessions entered.

## 5.6 Virtual Server Configuration

The **Virtual Server Configuration** page allows you to set the configuration of the Virtual Server. Virtual Servers are used for port forwarding from the WAN to LAN networks. All UDP/TCP ports are protected from intrusion. If any specific local PCs need to be mapped to the UDP/TCP port on WAN side, please input the mappings here. There can be up to 20 different Virtual Server Configurations.

The screenshot shows a web browser window titled "Conexant - Hasbani - Microsoft Internet Explorer". The address bar shows "http://10.0.0.2/doc/index.htm". The left sidebar contains a navigation menu with sections: Status (Home, PPP, ADSL), Configuration (WAN, LAN, PPP, NAT, Virtual Server, Bridge Filtering, DNS, Wireless, basic setting, advanced setting, WLAN Security, User Level Username/Password, Save Settings / Reboot), Admin Privilege (WAN Status, ATM Status, ADSL Configuration, Route Table, Learned MAC Table, RIP Configuration, Misc. Configuration, TCP Status, Admin Level, Username/Password, Reset to Factory Default, Diagnostic Test, System Log, Local Code Image Update, Network Code Image Update, Firmware, Boot Code). The main content area is titled "Virtual Server Configuration" and contains a table with the following headers: ID, Public Port - Start, Public Port - End, Private Port, Port Type, and Host IP Address. There is one row with ID "1", empty fields for Public Port - Start, Public Port - End, and Private Port, and radio buttons for Port Type (TCP is selected, UDP is unselected). There is an "Add This Setting" button to the right of the row. Below the table, a message states: "Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect. The maximum number of entries above is 20. The maximum number of mapped ports is 20".

ID	Public Port - Start	Public Port - End	Private Port	Port Type	Host IP Address
1				<input checked="" type="radio"/> TCP <input type="radio"/> UDP	

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.  
The maximum number of entries above is 20. The maximum number of mapped ports is 20

**ID:** It is the ID number corresponding to the Virtual Server configuration.

**Public Port - Start:** It allows you to enter the port number of the Public Network (WAN or external network). If you are entering a range of ports, this is the first port.

**Public Port - End:** It represents the last port number in a port range. If you only want one port number (no port range), simply enter the same number here as in the **Public Port - Start** field. The maximum number of the mapped Port is 20.

**Private Port:** It allows you to enter the port number of the Private Network (LAN or internal network). In most cases, the private port number is same as public port number. This port number cannot be seen from the WAN side.

**Host IP Address:** It allows you to enter the private network IP address for the particular server.

## 5.7 Bridge Filtering

Bridge Filtering allows packets to be forwarded or blocked, depending on the MAC address. The **Bridge Filtering** configuration page allows you to set the configuration of MAC filtering. There can be up to 4 different Bridge Filtering configurations.

The screenshot shows a web browser window titled "Conexant - Hasbani - Microsoft Internet Explorer". The address bar shows "http://10.0.0.2/doc/index.htm". The page content is titled "Bridge Filtering".

Configuration options:

- Filtering Enable: ☐ Yes ☒ No
- Filtering Action: ☐ Block ☒ Forward

ID	Src MAC	Dest MAC	Type
1	<input type="text"/>	<input type="text"/>	<input type="text"/> <input type="button" value="Add"/>

Instructions:

- (1) MAC address format : aabbccddeeff, 000000000000 indicates DON'T CARE
- (2) Ethernet type format: aabb, 0000 indicates DON'T CARE

The sidebar on the left contains the following links:

- Status
  - Home
  - PPP
  - ADSL
- Configuration
  - WAN
  - LAN
  - PPP
  - NAT
  - Virtual Server
  - Bridge Filtering
  - DNS
  - Wireless
    - basic setting
    - advanced setting
  - WLAN Security
  - User Level Username/Password
  - Save Settings / Reboot
- Admin Privilege
  - WAN Status
  - ATM Status
  - ADSL Configuration
  - Route Table
  - Learned MAC Table
  - RIP Configuration
  - Misc Configuration
  - TCP Status
  - Admin Level
  - Username/Password
  - Reset to Factory Default
  - Diagnostic Test
  - System Log
  - Local Code Image Update
  - Network Code Image Update
  - Firmware
  - Boot Code

**Source MAC:** This is the Source MAC to block or from which to forward. See the next page for instructions on how to configure this. The Source MAC must consist of 12 hexadecimal characters.

**Destination MAC:** This is the Destination MAC to block or to forward to. See the next page for instructions on how to configure this. The Destination MAC must consist of 12 hexadecimal characters.

**Type:** Enter the hexadecimal number for the Ethernet type field in Ethernet\_II packets. For example, 0800 is for IP protocol. The Type must consist of 4 hexadecimal characters.

**Block:** When block is selected, everything from the **Source MAC** with destination **Destination MAC** will be blocked.

**Forward:** When forward is selected, everything from the **Source MAC** will be forwarded to the **Destination MAC**.



How do I block packets from MAC address 000002fa6fab through IP protocol?

**Answer:** First go to the **Bridge Filtering** page under Configuration. Then type 000002fa6fab in the **ID Source MAC** field and 0800 in the **Type** field. If bridge filtering is not already enabled, select **Yes** under the **Enable Bridge Filtering** field. Then select **Block** and click **Submit**.



How do I block incoming packets with destination MAC address 000003dc8faa through IP protocol?

**Answer:** First go to the **Bridge Filtering** page under Configuration. Then type 000003dc8faa in the **Destination MAC** field, and 0800 in the **Type** field. If bridge filtering is not already enabled, select **Yes** under the **Enable Bridge Filtering** field. Then select **Block** and click **Submit**.



How do I forward packets with MAC address 000002fa6fab to destination MAC 000003dc8faa through IP protocol?

**Answer:** First go to the **Bridge Filtering** page under **Configuration**. Then type 000002fa6fab in the **ID Source MAC** field, 000003dc8faa in the **Destination MAC** field, and 0800 in the **Type** field. If bridge filtering is not already enabled, select **Yes** under the **Enable Bridge Filtering** field. Then select **Forward** and click **Submit**.

## 5.8 DNS Configuration

The **DNS Configuration** page allows you to set the configuration of the DNS proxy.

For the DHCP requests from local PCs, the DHCP server will set the LAN port IP as the default DNS server. Thus, all DNS query messages will come into LAN port first. The DNS proxy on the Router records the available DNS servers and forwards DNS query messages to one of DNS servers.

**DNS Configuration**

DNS Proxy:    
 Auto Discovery: ☒  
 User Configuration: ☐  
 DNS Server:

DNS Server:    
 Url Name:   
 Host Ip:

DNS Proxy Setting		DNS Server Setting		
#	DNS Server IP	#	Url Name (Host.Domain)	Host IP

Settings take effect immediately, no system reboot is required

[Save Configuration](#)

**DNS Proxy Enable/Disable:** When the DNS Proxy is Disabled, the LAN port does not process the DNS query message. For the DHCP requests from local PCs, the DHCP server will set the user-configured DNS server as the DNS server. Then all DNS query messages will be directly sent to the DNS servers. DNS Proxy is enabled by default.



**Auto Discovered:** When enabled (default), the DNS proxy will store the DNS server IP addresses obtained from DHCP client or PPP into the table. All DNS query messages will be sent to the dynamically obtained DNS server. Select this option when the DNS Server address is unknown but provided (automatically) by the ISP.

**User Configured:** When enabled, the DNS proxy will use the user-configured DNS server. All DNS query messages will be sent to the DNS server. Enter the DNS IP in the DNS Server field. Select this option when the DNS Server address assigned by the ISP is known. User Configured is disabled by default.

**Auto Discovery + User Configured:** Selecting both options will cause the DNS proxy's table to have all the IP addresses of dynamically obtained and user configured DNS servers.



*When **User Configured** is ticked, you have to enter the IP of DNS server(s) to make the feature take effect.*

**DNS Server:** It is the user defined DNS server URL name and IP. Default is Disabled.

- **URL Name (Add/Delete):** It is the URL name for the DNS server. This can be up to 255 characters.
- **Host IP (Add Only):** It is the IP address of the DNS Server.

**DNS Proxy Setting:** It is a table of all DNS server IP addresses.

**DNS Server Setting:** It is a table of all DNS sever URL names.

**Save Configuration:** Clicking this will link the user to the **Save Settings / Reboot** page.

## 5.9 Wireless Configuration

### 5.9.1 Basic Setting

This page allows you to configure basic wireless properties and security.

The screenshot shows a web browser window titled "Conexant - Hasbani - Microsoft Internet Explorer". The address bar shows "http://10.0.0.2/doc/index.htm". The page is titled "Wireless" and contains the following settings:

- WLAN Driver(Marconi) : v3.0.5
- Boot Loader Version : v3.1.1
- Upper MAC Version : M\_UM\_3.1.20
- Lower MAC Version : M2\_LM\_D2959SC\_3.1.41
- AP BSSID: 00:D0:DA:50:00:56

The configuration fields are:

- SSID: default
- Channel: 6
- Security: ☐ Enable Encryption, ☒ Disable Encryption
- Key Length: ☒ 64 bit, ☐ 128 bit
- Auth Type: Open System (dropdown menu)
- Passphrase: (The Passphrase should be fewer than 16 characters. You may manually enter you HEX key below and leave Passphrase blank)
- Key 0: c6774663dd
- Key 1: af6bd13ecd
- Key 2: 8e33fb2bfl
- Key 3: cf12611e1d
- Secret AP: Disable (Hide SSID)

Buttons: Reset, Submit

**SSID:** The Service Set Identifier (SSID) is a unique name for your wireless network. If you have other wireless access points in your network, they must share the same SSID.

The SSID can be up to 31 characters. System default is **default**.

**Channel:** Select the appropriate channel to correspond with your network settings, between 1 and 14. All access points and wireless PC adaptors must share the same channel to interoperate. Range is for Channel field is 1 - 14, default is 6. If any number greater than 14 is entered, the field will default to the value 14.

**Security:** The ADSL Router provides a security encryption tool known as WEP (Wired Equivalent Privacy). WEP is designed to provide security and privacy equivalent to that found in a wired network. This is done by encrypting the data packets sent between client and host with an encryption key. Both the client (PC) and the host (access point/router) must have the same WEP key in order to communicate. The available WEP settings are 64 bit and 128 bit. The higher the bit value on the encryption, the more secure the data transmission. Select Enable Encryption to activate this feature.

**Key Length:** Choose between 64 bit (default) and 128 bit. 128 bit offers more security, but at the cost of slower packet processing.

**Auth Type (Authentication Type):** For Open System authentication, the sender and the receiver do not use a WEP key for authentication while Shared Key authentication uses a WEP key for authentication. System default is Open System.



*The authentication scheme is separate from the data encryption. You can choose an authentication scheme which requires a shared key but still leave the data transmission unencrypted. If you require stronger security, use both the Shared Key and WEP encryption settings.*

**Passphrase:** Passphrase is used much like a password. It simplifies the WEP encryption process by automatically generating the WEP keys for this Wireless Router. Enter any word, up to 16 characters, or manually enter up to four sets of your hexadecimal digits in Key 0 - 3 fields.

**Key 0-3:** You are able to manually enter 4 encryption keys, only one of which is enabled at any given time. All devices on the network must share the selected key in order to communicate with the Wireless Router. The key length for 64 bit is 10 hexadecimal digits (0-9, a-f and A-F, e.g. 1234567890) and the key length for 128 bit is 26 hexadecimal digits (e.g. 11223344556677889900abcdef). Select which key (0-3) will be used when the Wireless Router sends data. Make sure the receiving device is using the same key.

**Secret AP:** If you enable Secret AP (to hide your SSID), only devices that have the correct SSID can connect. Enabling Secret AP broadcast nullifies the wireless network 'discovery' feature of some devices such as Windows XP. System default is disabled.

## 5.9.2 Advanced Setting

This page allows you to configure advanced wireless properties and security.

Advanced Wireless Configuration Page	
802.11G	
Beacon Interval (1-4095)	100 msec.
DTIM Interval (1-65535)	1 beacons
Fragmentation Threshold (256-2346)	2346 (even number only)
RTS Threshold (0-3000)	2342
Basic Rate	<input checked="" type="checkbox"/> 1M <input checked="" type="checkbox"/> 2M <input checked="" type="checkbox"/> 5.5M <input type="checkbox"/> 6M <input type="checkbox"/> 9M <input checked="" type="checkbox"/> 11M <input type="checkbox"/> 12M <input type="checkbox"/> 18M <input type="checkbox"/> 24M <input type="checkbox"/> 36M <input type="checkbox"/> 48M <input type="checkbox"/> 54M
Support/TX Rate	<input checked="" type="checkbox"/> 1M <input checked="" type="checkbox"/> 2M <input checked="" type="checkbox"/> 5.5M <input type="checkbox"/> 6M <input type="checkbox"/> 9M <input checked="" type="checkbox"/> 11M <input checked="" type="checkbox"/> 12M <input checked="" type="checkbox"/> 18M <input checked="" type="checkbox"/> 24M <input checked="" type="checkbox"/> 36M <input checked="" type="checkbox"/> 48M <input checked="" type="checkbox"/> 54M
Preamble	Long/Short Preamble
Adjacent Network Protection	Enabled
Channel Protection	RTS/CTS
Dynamic Antenna Switching	Enabled
BSS Slot Time	Long

**Beacon Interval (1-4095):** This field indicates the time interval in milliseconds that a system broadcast packet, or beacon, is sent to synchronize the wireless network. System default is 100 (milliseconds).

**DTIM Interval (1-65535):** DTIM (Delivery Traffic Indication Message) is a wireless message used to inform clients in Power Saving Mode when the system should wake up to receive broadcast and multicast messages. Type the time interval in which the system will broadcast a

DTIM for clients in Power Saving Mode. The default value 1 beacon is recommended.

**Fragmentation Threshold (256-2346):** Fragmentation is used to divide 802.11 frames into smaller pieces (fragments) that are sent separately to the destination. Enable fragmentation by setting a specific packet size threshold. If there is an excessive number of collisions on the WLAN, experiment with different fragmentation values to increase the reliability of frame transmissions. The default value 2346 is recommended for normal use.

**RTS Threshold (0-3000):** The RTS/CTS (Request to Send/Clear to Send) function is used to minimize collisions among wireless stations. When RTS/CTS is enabled, the router refrains from sending a data frame until another RTS/CTS handshake is completed. Enable RTS/CTS by setting a specific packet size threshold. System default is 2342.

**Basic Rate/Support/TX Rate:** This option allows you to specify the data transmission rate. Select from 11, 5.5, 2 and 1 Mbps data transfer rate.

**Preamble:** A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes:

- **Long/Short Preamble:** Select **Long/Short Preamble** to have the Wireless Router automatically use short preamble when all wireless clients support it, otherwise the device uses long preamble.
- **Always Long Preamble:** Select **Always Long preamble** if you have a 'noisy' network, to ensure interpretability between the Wireless Router and the wireless stations and to provide more reliable communication in 'noisy' networks.

**Adjacent Network Protection:** Enable this option to make Channel Protection setting take effect.

**Channel Protection:** The encoding used by 802.11g will not be recognized by 802.11b stations. If you have 802.11g and 802.11b devices in your network or you are not sure the wireless type of your devices, keep the default setting, **RTS/CTS**. If you have only 802.11g devices, select **CTS to Self**.

**Dynamic Antenna Switching:** Enable this function allows the device switching to the antenna which gains the better signal.

**BSS Slot Time:** Select **Short** if you are sure all the clients in your network support 802.11g, otherwise please select **Long**. Because mixed mode requires more slot time. Or select **Dynamic** to allow Wireless Router switching between Short and Long dynamically.

## 5.10 Wireless LAN Security

The Wireless LAN Security page allows you to configure advanced security options. WPA (Wi-Fi Protected Access) authorizes and identifies users based on a secret key that change automatically at a regular interval.

The screenshot shows a web browser window titled "Conexant - Hasbani - Microsoft Internet Explorer". The address bar shows "http://10.0.0.2/doc/index.htm". The left sidebar contains a navigation menu with links: Status, Home, PPP, ADSL, Configuration, WAN, LAN, PPP, NAT, Virtual Server, Bridge Filtering, DNS, Wireless, basic setting, advanced setting, WLAN Security, User Level Username/Password, Save Settings / Reboot, Admin Privilege, WAN Status, ATM Status, ADSL Configuration, Route Table, Learned MAC Table, RIP Configuration, Misc Configuration, TCP Status, Admin Level, Username/Password, Reset to Factory Default, Diagnostic Test, System Log, Local Code Image Update, Network Code Image Update, Firmware, and Boot Code. The main content area is titled "Wi-Fi Protected Access (WPA)" and contains the following configuration fields:

Firmware Version	CX_WLANSEC_4.2.0
WPA Mode	<input type="button" value="Disable"/>
Network Authentication	<input type="button" value="WPA Pre-Shared Key"/>
Data Encryption	<input type="button" value="TKIP"/>
WPA Pre-Shared Key	<input type="password" value="....."/>
WPA Group Rekey Interval	<input type="text" value="0"/> seconds
RADIUS Server Address	<input type="text" value="0.0.0.0"/>
RADIUS Server Port	<input type="text" value="1812"/>
RADIUS Shared Secret	<input type="password" value="...."/>

At the bottom of the form are two buttons: "Submit" and "Reset".

**Firmware Version:** This is the version of the Wireless Security firmware.

**WPA Mode:** This option allows you to enable or disable WPA feature. WPA insures much greater security than the standard WEP security.

**Network Authentication:** This field enables you to set different authentication methods which determine different encryption schemes. If you are not using a RADIUS server in a home environment and all your clients support WPA, using WPA Pre-Shared Key is recommended for better security. If there is a RADIUS server in your network, selecting WPA RADIUS.

**Data Encryption:** When WPA Pre-Shared Key authentication method is used, the TKIP (Temporal Key Integrity Protocol) encryption scheme is applied.

**WPA Pre-Shared Key:** This is the pre-shared key for use in WPA Pre-Shared Key security method.

**WPA Group Rekey Interval:** This field specified the time interval (in seconds) after which a WPA group key is changes. Set to '0' (zero) to indicate that a periodic key-change is not required.

**RADIUS Server Address:** This field specifies the IP address of the RADIUS server.

**RADIUS Server Port:** This field specifies the UDP port number used by the RADIUS server.

**RADIUS Shared Secret:** This field specifies the password shared between an 802.11 access point and the RADIUS server.



*A RADIUS (Remote Authentication Dial-In User Service) server is used for remote user authentication and accounting. It can be used on any network that needs a centralized user authentication, dynamic key management and accounting function for its workstations.*

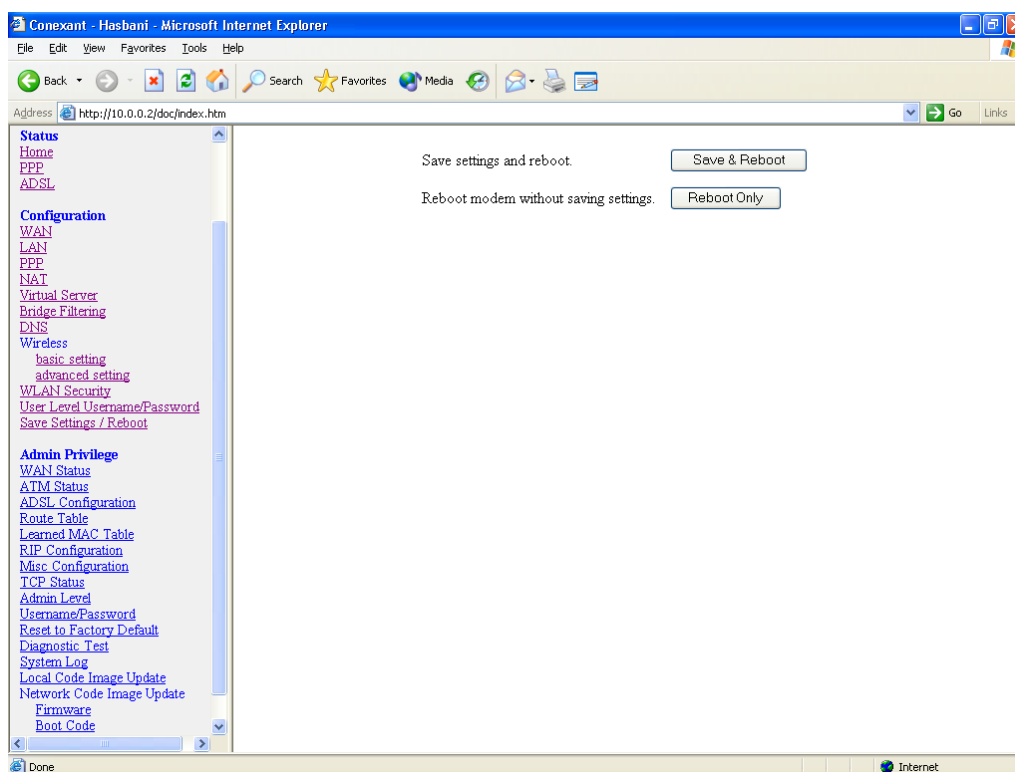
## 5.11 User Password Configuration

The User Password Configuration page allows the user or admin to set the password for the user account. The User Password can be up to 65 characters (excluding '&').

The screenshot shows a web browser window titled "Conexant - Hasbani - Microsoft Internet Explorer". The address bar shows "http://10.0.0.2/doc/index.htm". The left sidebar contains a navigation menu with the following items: Status, Home, PPP, ADSL, Configuration, WAN, LAN, PPP, NAT, Virtual Server, Bridge Filtering, DNS, Wireless, basic setting, advanced setting, WLAN Security, User Level Username/Password, Save Settings / Reboot, Admin Privilege, WAN Status, ATM Status, ADSL Configuration, Route Table, Learned MAC Table, RIP Configuration, Misc Configuration, TCP Status, Admin Level, Username/Password, Reset to Factory Default, Diagnostic Test, System Log, Local Code Image Update, Network Code Image Update, Firmware, and Boot Code. The main content area is titled "User Level Username/Password Configuration" and contains the following text: "Do not use '&' in the password." Below this text are four input fields: "Current Password", "Select Username" (with the value "user" entered), "Select Password", and "Retype Password". Below the input fields are two buttons: "Submit" and "Reset". At the bottom of the page, there is a message: "Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect."

## 5.12 Save Settings / Reboot

The **Save Settings / Reboot** page allows you to either save the new configuration to the flash and reboot the Router or simply reboot the Router without saving changes.



**Save & Reboot:** Click this to apply all changes.

**Reboot Only:** Do this to discard all changes since last save.

After either one of these buttons are clicked, the Router will do the following:

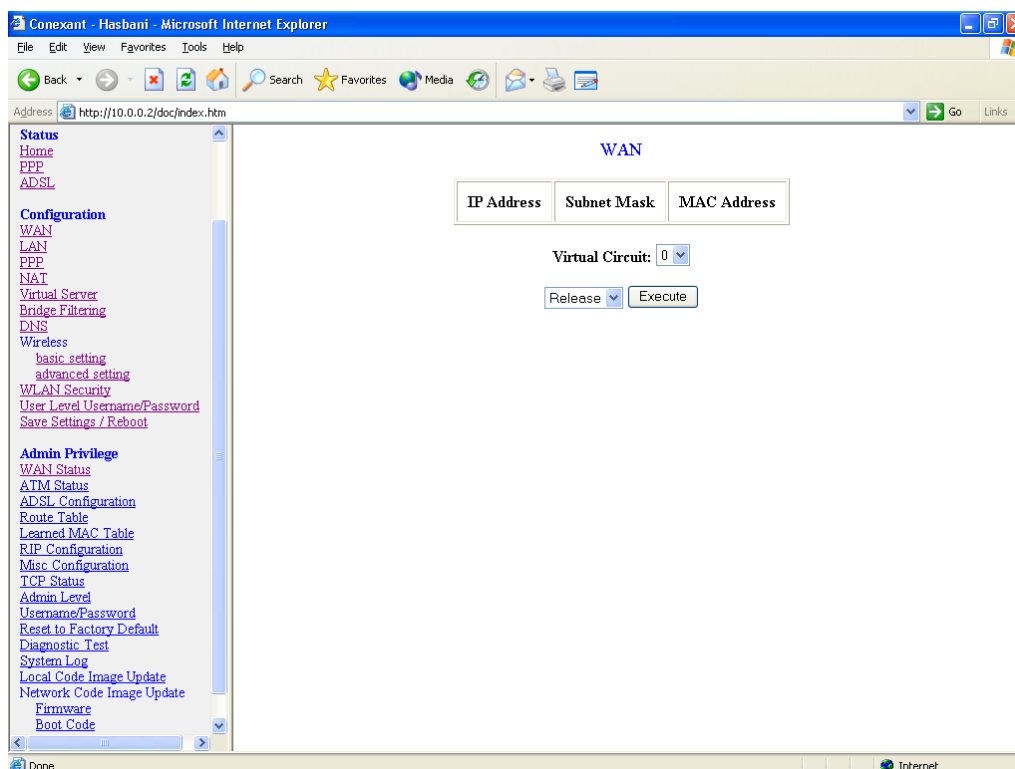
- **Save & Reboot:** Two pages will appear after pressing this button. The first one states: **“Your settings are being saved and the modem being rebooted. Save-reboot in progress, please wait....”** Followed by **“Your settings have been saved and the modem has rebooted. Done.”**
- **Reboot Only:** Two pages will appear after pressing this button. The first one states: **“The modem is being rebooted. Reboot in progress, please wait....”** Followed by **“The modem is being rebooted. Done.”**

# 6. Admin Privilege

The links under **Admin Privilege** are only accessible when user is logged in as **Admin**. Regular user account does not have authorization to view or alter the content on the pages in the **Admin Privilege** section.

## 6.1 WAN Status

The **WAN Status** page shows the information and status of WAN PVCs.



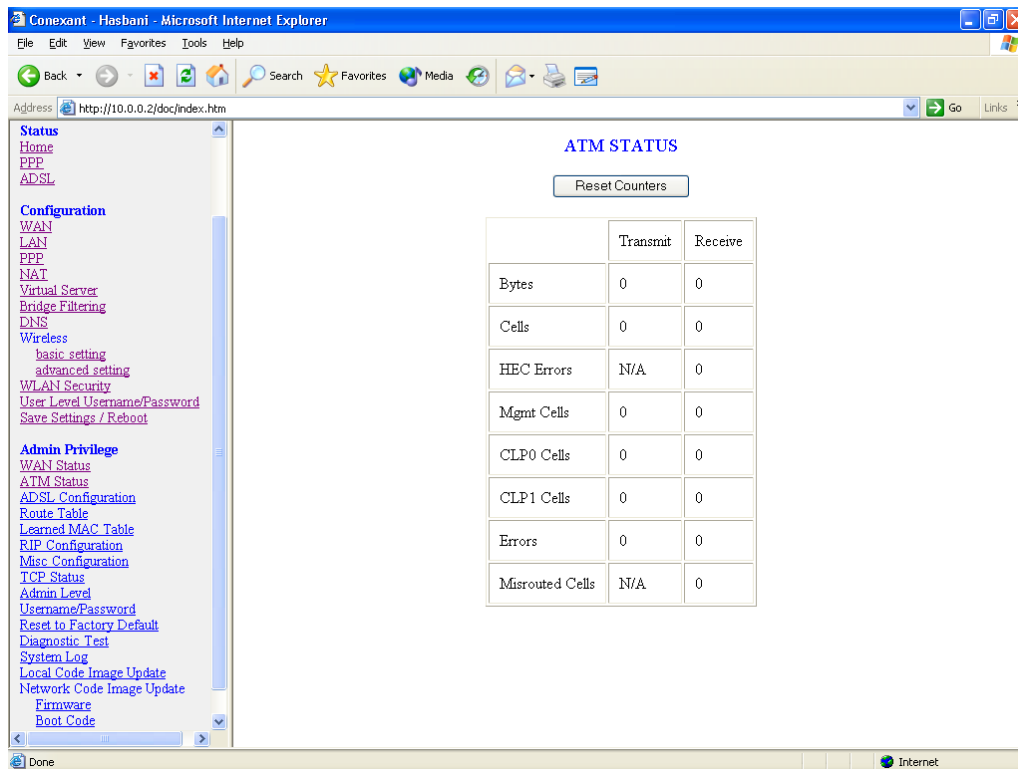
**WAN:** It displays the IP address, Subnet Mask and MAC address for the WAN (ADSL) interface. Use the Virtual Circuit selection to select different PVCs for status display.

**Virtual Circuit:** Select the Virtual Circuit that you want to release/renew, select the appropriate option on the menu dropdown and click **Execute**.



## 6.2 ATM Status

The **ATM Status** page shows all the statistics information of ATM cells. This page contains information that is dynamic and will refresh every 2 seconds.



The screenshot shows a web browser window titled "Conexant - Hasbani - Microsoft Internet Explorer". The address bar shows "http://10.0.0.2/doc/index.htm". The left sidebar contains a navigation menu with the following items:

- Status
  - Home
  - PPP
  - ADSL
- Configuration
  - WAN
  - LAN
  - PPP
  - NAT
  - Virtual Server
  - Bridge Filtering
  - DNS
  - Wireless
    - basic setting
    - advanced setting
  - WLAN Security
  - User Level Username/Password
  - Save Settings / Reboot
- Admin Privilege
  - WAN Status
  - ATM Status
  - ADSL Configuration
  - Route Table
  - Learned MAC Table
  - RIP Configuration
  - Misc Configuration
  - TCP Status
  - Admin Level
  - Username/Password
  - Reset to Factory Default
  - Diagnostic Test
  - System Log
  - Local Code Image Update
  - Network Code Image Update
  - Firmware
  - Boot Code

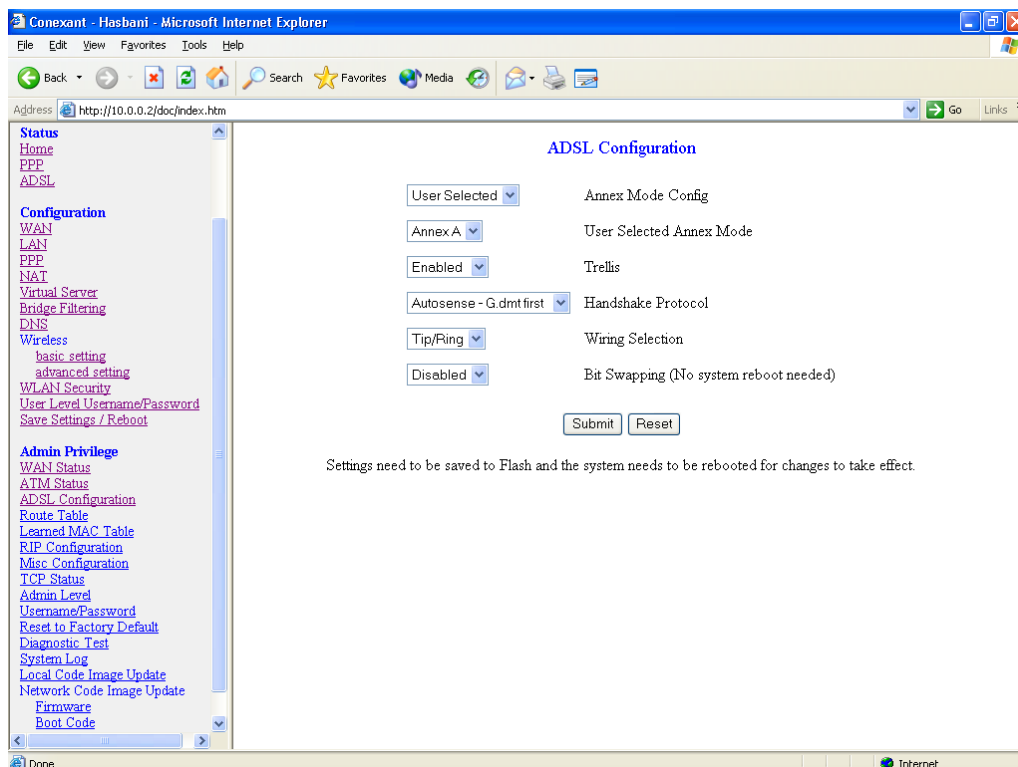
The main content area is titled "ATM STATUS" and contains a "Reset Counters" button. Below the button is a table showing ATM statistics:

	Transmit	Receive
Bytes	0	0
Cells	0	0
HEC Errors	N/A	0
Mgmt Cells	0	0
CLP0 Cells	0	0
CLP1 Cells	0	0
Errors	0	0
Misrouted Cells	N/A	0

**Reset Counters:** This button allows user to reset the ATM Status counter.

## 6.3 ADSL Configuration

The **ADSL Configuration** page allows you to set the configuration for ADSL protocols.



The screenshot shows a web browser window titled "Conexant - Hasbani - Microsoft Internet Explorer". The address bar shows "http://10.0.0.2/doc/index.htm". The left sidebar contains a navigation menu with the following items:

- Status
  - Home
  - PPP
  - ADSL
- Configuration
  - WAN
  - LAN
  - PPP
  - NAT
  - Virtual Server
  - Bridge Filtering
  - DNS
  - Wireless
    - basic setting
    - advanced setting
  - WLAN Security
  - User Level Username/Password
  - Save Settings / Reboot
- Admin Privilege
  - WAN Status
  - ATM Status
  - ADSL Configuration
  - Route Table
  - Learned MAC Table
  - RIP Configuration
  - Misc Configuration
  - TCP Status
  - Admin Level
  - Username/Password
  - Reset to Factory Default
  - Diagnostic Test
  - System Log
  - Local Code Image Update
  - Network Code Image Update
  - Firmware
  - Boot Code

The main content area is titled "ADSL Configuration" and contains several configuration options:

- User Selected (dropdown menu)
- Annex Mode Config (text label)
- Annex A (dropdown menu)
- User Selected Annex Mode (text label)
- Enabled (checkbox)
- Trellis (text label)
- Autosense - G.dmt first (dropdown menu)
- Handshake Protocol (text label)
- Tip/Ring (dropdown menu)
- Wiring Selection (text label)
- Disabled (checkbox)
- Bit Swapping (No system reboot needed) (text label)

Below the configuration options are "Submit" and "Reset" buttons. At the bottom of the page, a message states: "Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect."

**Annex Mode Config:** It allows you to manually configure the Router for Annex A or Annex B mode by selecting User Configured and choosing the Annex Mode in the next field.

**User Selected Annex Mode:** It allows you to select from Annex A and Annex B.



*Please DO NOT change the default setting of Annex Mode unless you are instructed to do this by your ISP.*

**Trellis:** Trellis Code is an advanced method of FEC (Forward Error Correction). It allows you to enable or disable the Trellis Code. By default, it is always enabled.

**Handshake Protocol:** It allows you to select from the following ADSL handshake protocols: Autosense - G.dmt first (default), Autosense - T1.413 first, G.dmt/G.lite, T1.413, G.dmt, and G.lite.

**Wiring Selection:** It allows you to enter the wiring selection for the RJ-11.

Tip/Ring is the default for the Router without the inner/outer pair relay. Available types are Auto, Tip/Ring (default), and A/A1, where Tip/Ring is the inner-most pair of wires on the RJ11 and A/A1 is the second inner-most pair.

**Bit Swapping:** It allows you to enable or disable the upstream bit swapping. Bit Swapping is disabled by default.

## 6.4 Route Table

The **Route Table** page displays the routing table and allows you to manually enter a routing entry. The routing table will display the routing status of Destination, Netmask, Gateway, and Interface. The interface br0 indicates the USB interface (reserved function); lo0 indicates the loopback interface; ppp1 indicates the PPP interface. The Gateway is the learned Gateway.

**Route Table**

Destination	Netmask	Gateway	Interface
10.0.0.0	255.0.0.0	10.0.0.2	br0
127.0.0.1	255.0.0.0	127.0.0.1	lo0

---

**System Default Gateway Configuration**

☐ None  
☒ Auto  
☐ Select Interface   
☐ Specify IP

---

**Route Configuration**

Destination  Netmask  Gateway

☒ Specify IP  
☐ Select Interface

Note: Save changes to flash to restore on power up.

**Manually Configured Routes**

#	Destination	Netmask	Gateway
---	-------------	---------	---------

- The Gateway field of the static route entry allows users to either enter a Gateway IP address or select a Network Interface.
- All user-defined routes retained in the CPE memory, regardless if they are already in the Routing Table, are displayed on the same Route Table page.
- All user defined route entries kept in the CPE memory during run time are saved to flash when the user chooses to save and reboot the CPE. When the CPE restarts, it reloads all saved user-defined routes to the CPE memory and tries to apply to the system.
- A user-defined route entry is added to the Routing Table whenever the system provides an environment that makes the route entry applicable. It is removed from the Routing Table whenever the route entry becomes not applicable. e.g. If the route entry's Gateway is associated with a dynamic Network Interface but the connection is not established, then the route entry does not appear in the Routing Table. When that interface comes up later, the route entry is then added.
- If the selected Network Interface is static or dynamic and the connection is already up, then the route entry appears in the Routing Table immediately. If there is a Gateway associated with the selected Network Interface, then that Gateway's IP address appears in the Gateway field of the route entry.

If the selected Network Interface is dynamic but the connection is not established, then the route entry does not appear in the Routing Table. When the interface comes up later, the route entry is then added.

#### 6.4.1 System Default Gateway Configuration

The system-wide Default Gateway provides three options: Auto (default), User-selected Network Interface, and None.

- **None:** It allows you to choose to have no Default Gateway in the CPE.
- **Auto (default):** It allows you to enable the Router to automatically decide the Default Gateway.
- **User-selected Network Interface:** It allows you to select a Network Interface from a list (PVCs, PPP Sessions and LAN). This option allows you to associate the system-wide Default Gateway to a Network Interface, static or dynamic, and provides a way to fix the Default Gateway to a dynamic Network Interface before the interface is established.



*The options for this field are IP PVC0 ... IP PVC7, IP Ethernet 0, IP BridgeMux0, and any PPP session that was created by the user.*

- **Specify IP:** It allows you to specify the IP address of the default gateway.

#### 6.4.2 Route Configuration

**Destination:** It allows you to enter the remote network or host IP address for the static routing.

**Netmask:** It allows you to enter the Subnet Mask for the static routing.

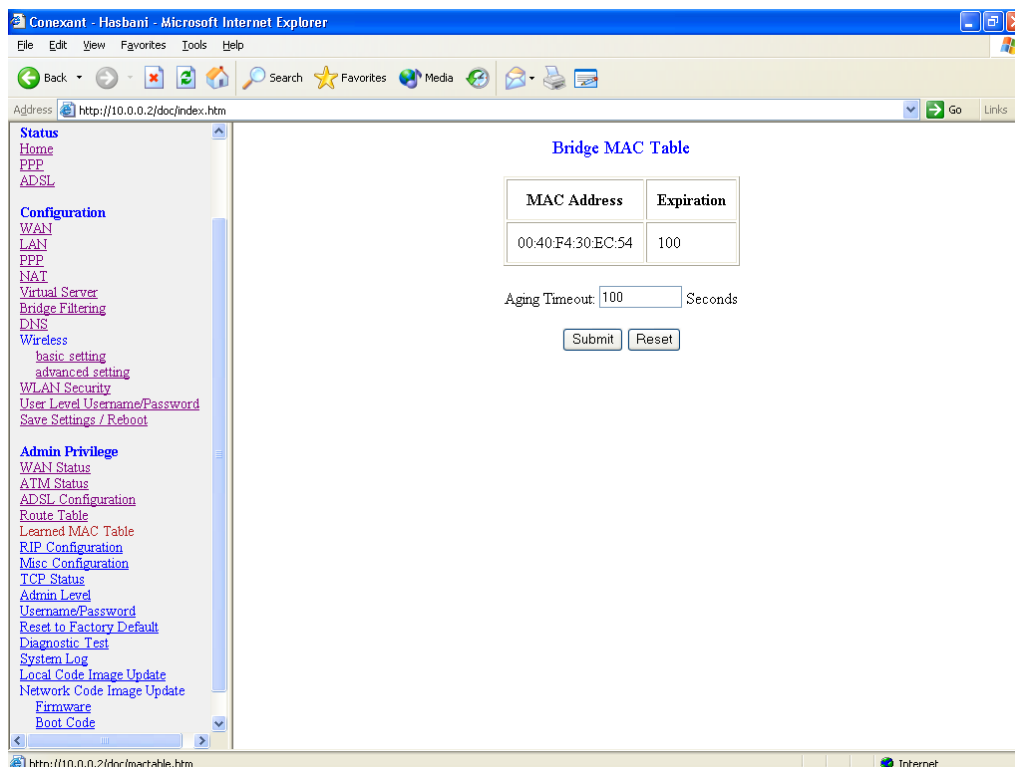
**Gateway:** It allows you to enter the IP address of the gateway device that allows the router to contact the remote network or the host for Specified IP or select an Interface for the Gateway.

**Manually Configured Routes:** It displays the static route entries entered by the user.

## 6.5 Learned MAC Table

Network bridges operate at the physical network layer. The purpose of a bridge is to connect two or more networks and enable packet sharing between them. Bridges are different from routers because they forward packets based on physical addresses, whereas routers use IP address to forward packets. Bridges must learn all the physical (MAC) addresses of the devices so it can forward the packets reliably. The purpose of the Learned MAC Table is to store and display these bridge-recognized MAC addresses.

The **Learned MAC Table** page shows the current learned Bridge MAC table. This page contains information that is dynamic and will refresh every 8 seconds.



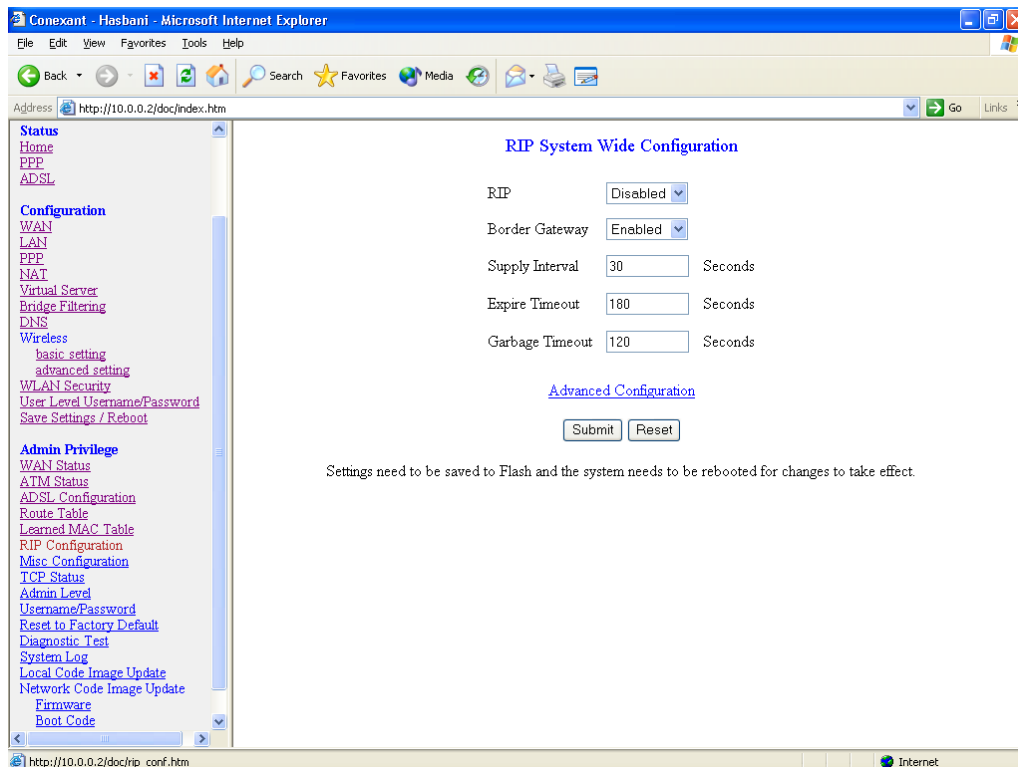
**Aging Timeout:** It allows you to enter the update period for the MAC table. Have this number lower if you want a more frequent refresh rate.

Range: 0 - 32767      Default: 100

## 6.6 RIP Configuration

RIP (Routing Information Protocol) is a management protocol that ensures that all hosts in a particular network share the same information about routing paths.

The **RIP Configuration** page allows you to set the configuration for the system wide configuration of RIP. The actual RIP configuration is in the RIP Per Interface Configuration.



**RIP:** It allows you to Enable or Disable the RIP session. The resulting RIP session will monitor all network interfaces that are currently available for messages from other RIP routers. RIP is disabled by default.

**Border Gateway:** RIP implements Border Gateway as specified in RFC 1058 and RFC 1723. This limits all subnet routes and host routes to routers within that same network. Updates sent outside that network will only include a single entry representing the entire network, including all subnets and host-specific routes. The Border Gateway is enabled by default.

**Supplier Interval:** It allows you to enter the Supplier Interval timer in seconds. This timer specifies how often the RIP sends announcements as a RIP Supplier.

Range: 0 - 2147483647      Default: 30

**Expire Timeout:** It allows you to enter the Expire Timeout in seconds. This timer specifies the expiration time of a route. When a route has not been updated for more than the “expire” period of time, it is removed from the Route Table. This route is then invalidated and remains in the internal RIP Route Table. It will be included in the RIP announcements to let other routers know the changes.

Range: 0 - 2147483647      Default: 180

**Garbage Timeout:** It allows you to enter the Garbage timer in seconds. This timer specifies how long the expired and invalidated routes are kept in the Internal RIP Route Table before they are removed from it.

Range: 0 - 2147483647      Default: 120

## 6.6.1 RIP Per Interface Configuration

The RIP Per Interface Configuration page allows you to set the configuration for each Interface (PVCs, PPP Sessions and LAN).

#	Interface	Enabled?	Supplier Mode	Listener Mode
1	Ip Ethernet 0	No	V2 BC	V1+V2
2	Ip Ustb 0	No	V2 BC	V1+V2
3	Ip Pvc 0	No	Disabled	V1+V2
4	Ip Pvc 1	No	Disabled	V1+V2
5	Ip Pvc 2	No	Disabled	V1+V2
6	Ip Pvc 3	No	Disabled	V1+V2
7	Ip Pvc 4	No	Disabled	V1+V2

**Interface:** It allows you to choose the Interface (PVCs, PPP Sessions and LAN), for the RIP to be configured. The available selections are: IP Ethernet 0, IP USB 0, IP PVC0...IP PVC7, IP BridgeMux 0, and any PPP user defined sessions (maximum of 16):

**Enable:** It allows you to Enable (Yes) or Disable (No) the specified interface for RIP.

**Supplier:** It allows you to select the Supplier Mode (RIP Transmit).

- **Disabled:** The supplier transmit is disabled.
- **V1 BC:** The supplier transmits in RIPv1 Broadcast.
- **V2 BC:** The supplier transmits in RIPv2 Broadcast.
- **V2 MC:** The supplier transmits in RIPv2 Multicast.

**Listener:** It allows you to select the Listener Mode (RIP Receive).

- **V1:** The listener receives the RIPv1 only.
- **V2:** The listener receives the RIPv2 only.
- **V1+V2:** This listener receives the both RIPv1 and RIPv2.

**Current RIP Settings:** It displays the each interface's RIP status.

## 6.7 Miscellaneous Configuration

The **Miscellaneous Configuration** page allows you to set miscellaneous configurations for the following: HTTP, FTP, TFTP, DMZ, Command Line Interface, DHCP, PPP, IGMP, and SNTP.

The screenshot shows a web browser window titled "Conexant - Hasbani - Microsoft Internet Explorer". The address bar shows "http://10.0.0.2/doc/index.htm". The left sidebar contains a navigation menu with the following sections:

- Status**
  - Home
  - PPP
  - ADSL
- Configuration**
  - WAN
  - LAN
  - PPP
  - NAT
  - Virtual Server
  - Bridge Filtering
  - DNS
  - Wireless
    - basic setting
    - advanced setting
  - WLAN Security
  - User Level Username/Password
  - Save Settings / Reboot
- Admin Privilege**
  - WAN Status
  - ATM Status
  - ADSL Configuration
  - Route Table
  - Learned MAC Table
  - RIP Configuration
  - Misc Configuration
  - TCP Status
  - Admin Level
  - Username/Password
  - Reset to Factory Default
  - Diagnostic Test
  - System Log
  - Local Code Image Update
  - Network Code Image Update
    - Firmware
    - Boot Code

The main content area is titled "Miscellaneous Configuration" and contains the following settings:

- HTTP server access**
  - ☐ All
  - ☒ Restricted
    - ☒ LAN
    - ☐ WAN Specify IP:
    - Subnet Mask:
- HTTP server port**:
- HTTP Password Protection**:
- FTP server**:
- ☐ Disable WAN side FTP access
- TFTP server**:
- Command Line Interface**:
- ☐ by Console
- ☒ by Telnet
  - ☒ Disable WAN side access
- DMZ**:
- DMZ HOST IP**:
- IGMP Proxy**:
- PPP Half Bridge**:
- PPP Reconnect on WAN Access**:
- Connect PPP when ADSL link is up**:
- SNTP**
  - Time Zone**:
  - Daylight Saving Time**:
  - User defined Time server**:

At the bottom of the form are two buttons:  and .

Below the buttons, a message states: "Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect."

The browser's status bar at the bottom shows "Done" and "Internet".

**HTTP Server Access:** It allows you to configure where these Web pages could be accessed from.

- **All (default):** When this field is checked, it allows both WAN and LAN access to the Web pages.
- **Restricted LAN:** It allows the Web pages access from LAN side.
- **Restricted WAN Specified IP & Subnet Mask:** It allows the Web access from WAN side with a specify IP and subnet mask.

**HTTP Server Port:** It allows you to specify the port of the Web access. For example, when it is changed to 8080, the HTTP server address for the LAN side is <http://10.0.0.2:8080>.

Range: 0 - 32767          Default: 80

**FTP server:** It allows you to enable or disable the FTP server connection. System default is Enabled.

- **Disable WAN side FTP access:** This will disable WAN side access to the FTP server, default is Disabled.

**TFTP server:** It allows you to enable or disable the TFTP connection. System default is Disabled.

**DMZ:** A DMZ (De-Militarized Zone) is added between a protected network and an external network, in order to provide an additional layer of security. When there is a suspected packet coming from WAN, the firewall will forward this packet to the DMZ host.

**DMZ Host IP:** The IP address of the DMZ host viewable at the WAN (external) side.

**DHCP** Dynamic Host Configuration Protocol is a communications protocol that allows network administrators to manage and assign IP addresses to computers within the network. DHCP provides a unique address to a computer in the network which enables it to connect to the Internet through Internet Protocol (IP).

- **NONE:** It will disable the DHCP server. Note that this setting will override the DHCP Server Enable/Disable on the LAN configuration page.
- **DHCP Server (default):** Select this to activate the DHCP server.
- **DHCP Relay:** If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please disable the NAT to run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.

**DHCP Relay Target IP:** If DHCP Relay is enabled, DHCP requests are relayed to DHCP Target IP on the WAN side.

**IGMP Proxy:** It is the global setting for IGMP Proxy. If it is enabled, then the enabled IGMP Proxy on WAN PVCs will be working. Otherwise, no WAN PVC can have IGMP Proxy working on it. System default is Disabled.



**PPP Half Bridge:** When PPP Half Bridge is enabled, only one PC is able to access the Internet, and the DHCP server will duplicate the WAN IP address from the ISP to the local client PC. Only the PC with the WAN IP address can access the Internet. System default is Disabled.

**PPP reconnect on WAN access:** If enabled, the PPP session will automatically establish a connection when a packet tries to access the WAN. System default is Disabled.

**Connect PPP when ADSL link is up:** If this option is enabled, the Router will connect the PPP session whenever an ADSL connection is established. If this option is disabled, the PPP session will not connect whenever the ADSL Showtime is reached. System default is Enabled.



*For more information, please refer to Section 5.4: PPP Configuration.*

**SNTP:** Simple Network Time Protocol is an efficient method of obtaining the time from a Time Server.

**Time Zone:** It specifies the time zone (geographical location).

**Daylight Saving Time:** You can select yes to activate Daylight Savings Time.

**User defined Time server:** This is the time server from which the Router retrieves the time.

## 6.8 TCP Status

The **TCP Status** page shows the statistics for all TCP connections. This page contains information that is dynamic and will refresh every 2 seconds.

The screenshot shows a web browser window with the address <http://10.0.0.2/doc/index.htm>. The page title is "TCP STATUS". There is a "Reset Counters" button. The page is divided into three main sections: General, Discarded Packets, and Connections.

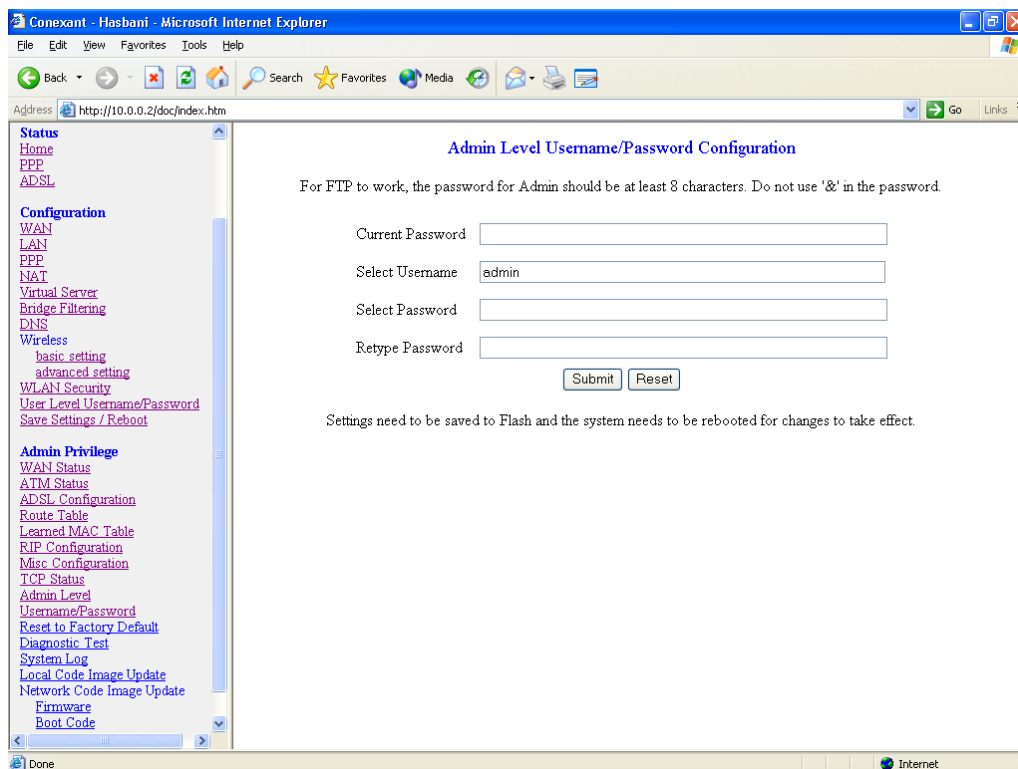
General		
	Transmit	Receive
Total Packets	1121	856
Data Packets	768	116
Data Bytes	508172	38945
Out of Order Packets	N/A	115
Out of Order Bytes	N/A	0

Discarded Packets	
Bad Checksum	0
Bad Header Offset	0
Too Short	0

Connections	
Initiated	0
Accepted	116
Established	116
Closed	111

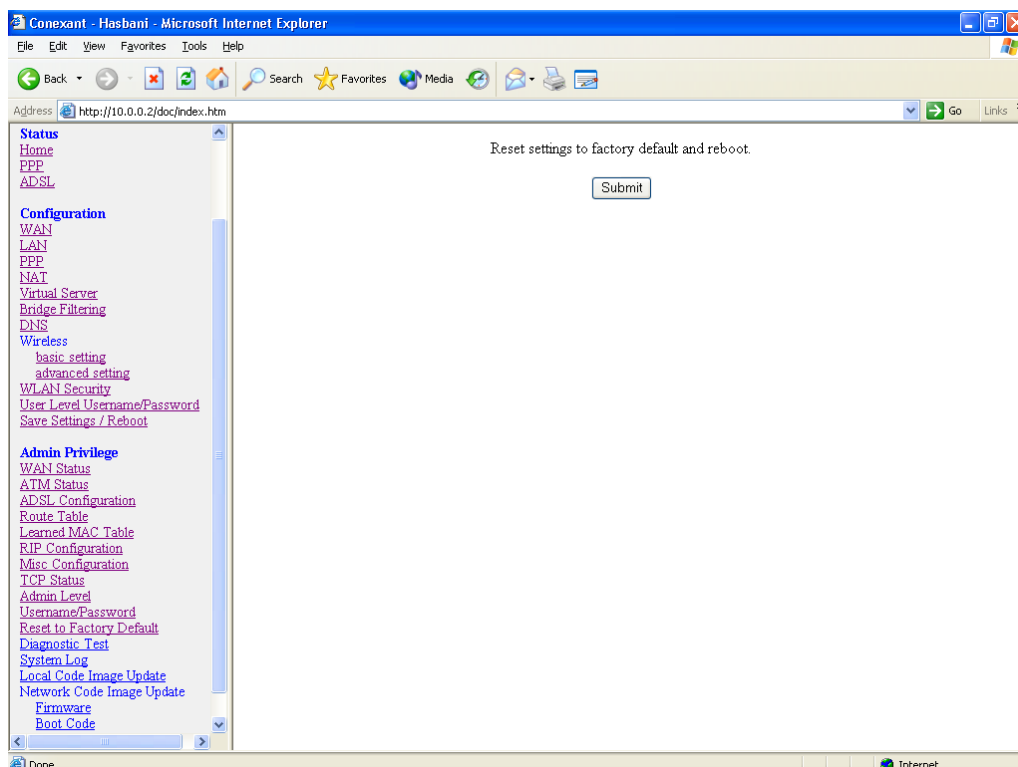
## 6.9 Admin Password Configuration

The Admin Password Configuration page allows you to set the password for administrator. The Admin password can be up to 65 characters (excluding '&').



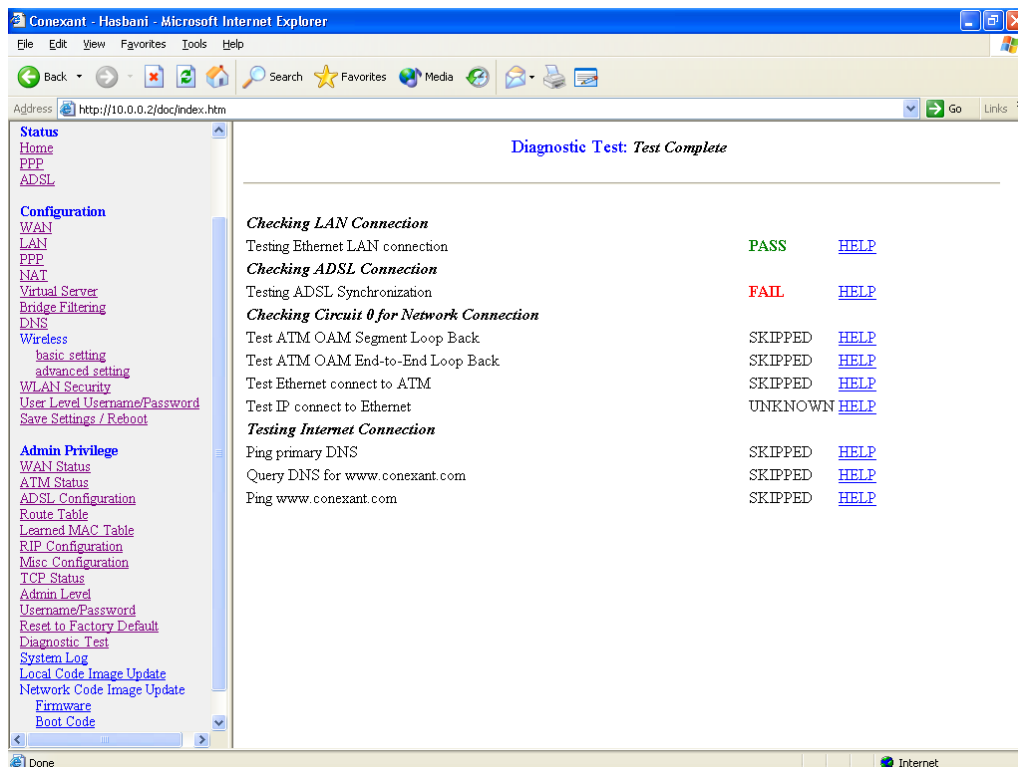
## 6.10 Reset to Factory Default

The **Reset to Factory Default** page allows you to reset the Router to original factory default configuration.



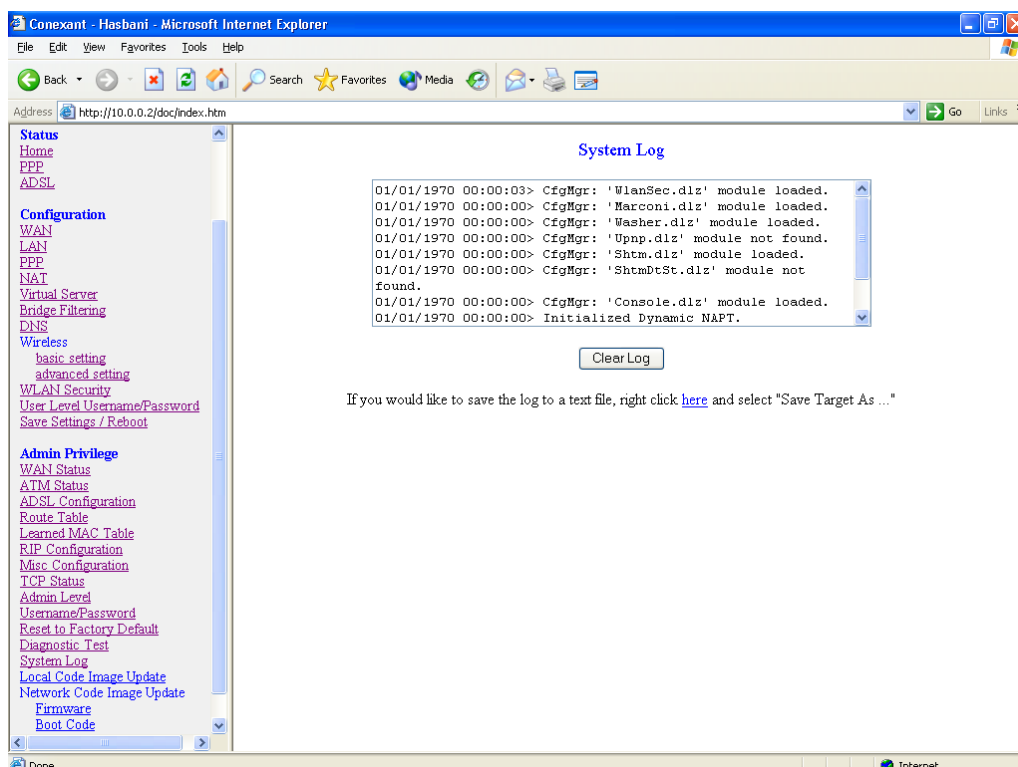
## 6.11 Diagnostic Test

The **Diagnostic Test** page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides. This page will continually refresh every 2 seconds until all tests are complete.



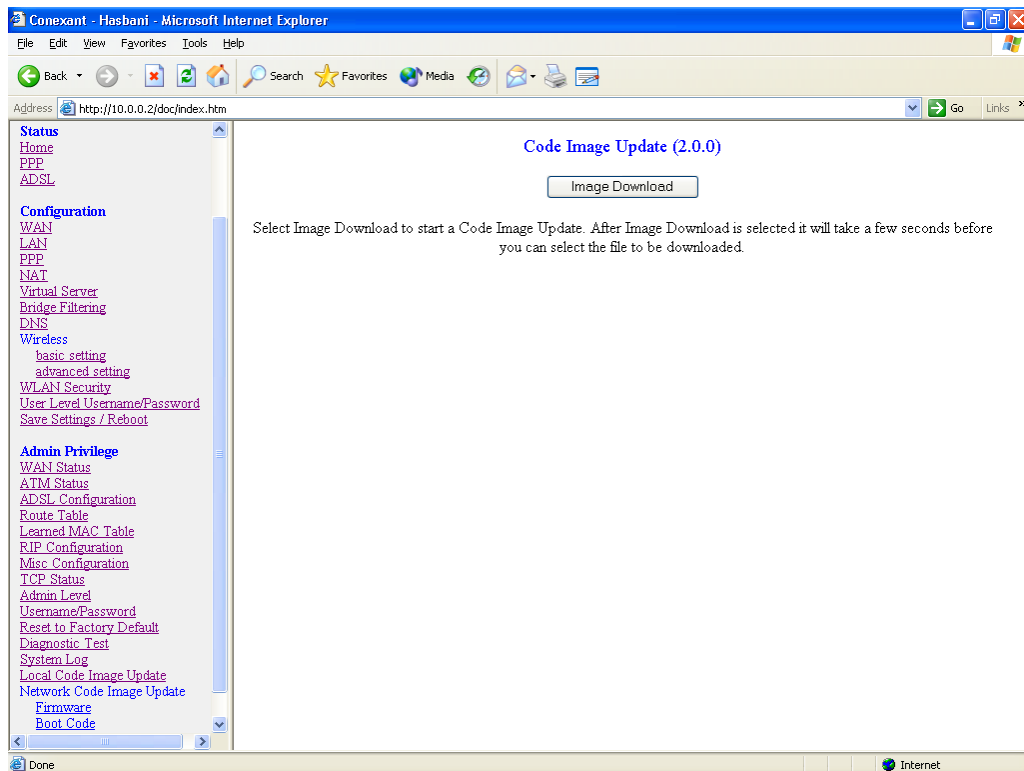
## 6.12 System Log

The **System Log** page shows the events triggered by the system. This page contains information that is dynamic and will refresh every 5 seconds.



## 6.13 Local Code Image Update

The **Local Code Image Update** page allows you to upgrade the image code locally.



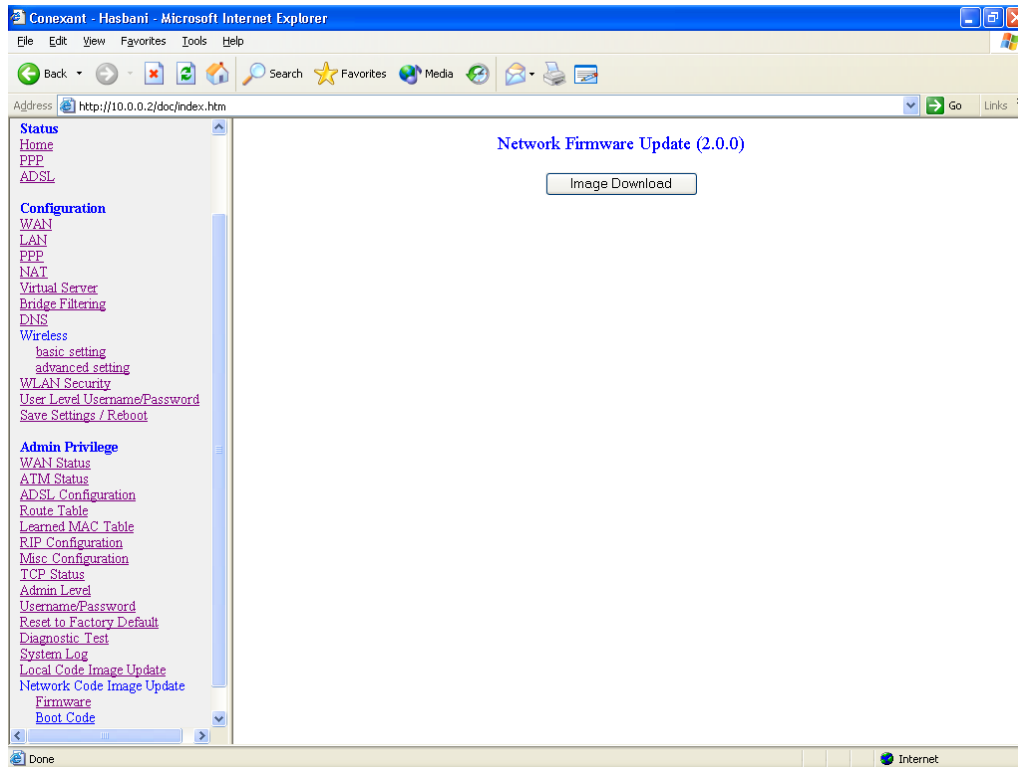
Browse the location of file, firmware.dlf or bootrom.dlf file, and click the **Upload** to start the update. The system will reboot as part of the process of updating code.

## 6.14 Network Code Image Update

The **Network Code Image Update** page allows you to upgrade the image code from the remote FTP server.

### 6.14.1 Firmware

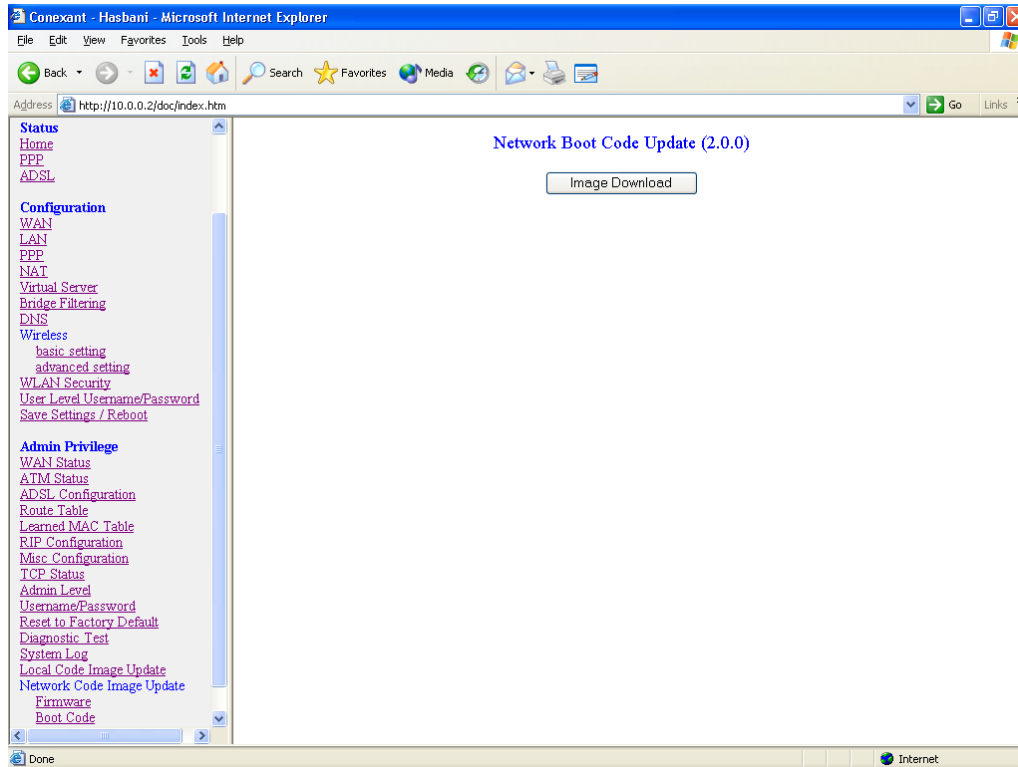
Assume an FTP server stores the updated image firmware.dlf on Internet. Click **Image Download** to initiate the updating. The system will reboot as part of the process of updating code.



Browse the location of file, firmware.dlf, and click the **Upload** to start the update. The system will reboot as part of the process of updating code.

## 6.14.2 Boot Code

Assume an FTP server stores the updated image boorom.dlf on Internet. Click **Image Download** to initiate the updating. The system will reboot as part of the process of updating code.



# Appendix A. Compliance Statement

---

## **FCC Warning**

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## **FCC RF Radiation Exposure Statement**

The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment must be installed and operated with a minimum distance of 20 centimeters between the radiator and your body. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

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

## **CE Mark Warning**

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

# Appendix B. Encapsulation Mode

---

## **Bridged mode ( RFC-1483 )**

RFC-1483 provides the simplest method of connecting end station over an ATM network. User data in the form of Ethernet frames is encapsulated into AAL5-PDU for transport over ATM. RFC-1483 provides no authentication and configuration such as would be provided by PPP. RFC-1483 implementation supports VC multiplexing and LLC/SNAP encapsulation in both routed and bridged configurations.

## **Classical IP over ATM-IPOA ( RFC1577 )**

User data in the form of IP packets is encapsulated into AAL-5 PDUs for transport over ATM. The fact that the user data is routed at an IP layer instead of bridged MAC layer allows the source and destination to be on different subnets. A notable drawback of IPoA is the lack of authentication and configuration such as would be provided by PPP.

## **PPP over ATM-PPPoA ( RFC-2364 )**

The use of PPPoA is similar to IPoA. However, a PPP session is established to the remote access server (RAS). The PPP packets are encapsulated according to RFC-2364 for transmission over an ATM link. On the receive side, the de-encapsulation is performed. The PPP session is terminated and the IP packets can be delivered to the end user over Ethernet or other medium.

## **PPP over Ethernet-PPPoE ( RFC-2516 )**

The PPP over Ethernet ( PPPoE ) encapsulation is used to transport PPP traffic from a PC to a DSL device over Ethernet and then over the DSL link using RFC-1483 encapsulation. There may be multiple PPP sessions, each terminated in a PC or in the CPE device and in a PPP aggregator on the CO side.

- The PPPoE Client terminates PPPoE session within the CPE device, this configuration enables PPPoE session without a need for additional software.
- The PPP traffic for a Relay Agent is not terminated in the DSL device, rather it is relayed over the DSL link to a PPP aggregator in the CO. PPPoE relay agent determines on which session locally originated PPPoE traffic belongs. The relay agent forwards that traffic, without any unnecessary processing to the correct destination only. Similarly, received data is immediately relayed only to the appropriate client PC. Not only does this approach enhance performance by eliminating additional process, it also provides a critical security feature, so it prevents for example corporate bound data from being exposed to the Internet.