

ADSL Broadband Router



AR-6024

User's Manual

Table of Contents

Specification.....	2
Package Contents.....	5
Hardware Connecting.....	6
LED Indicators.....	7
General Setting	8
One Page Setup-----	12
Status -----	14
Router	14
ADSL	16
PPP.....	17
Advanced Setting	22
ADMINISTRATION -----	23
WAN.....	23
LAN.....	29
DNS	31
NAT.....	32
Port Forwarding	34
ADSL Configuration	35
RIP Configuration.....	36
Firewall	37
Service Filtering	41
Diagnostic Test.....	49
Router Table.....	51
MAC Filtering	52
Security-----	53
Admin Password	53
User Password.....	54
Misc Configuration	55
System Log	57
Code Update.....	58
Status -----	59
Router	59
ADSL	61
WAN Status.....	62
ATM Status.....	63
TCP connections.....	64
Learned MAC Table	65
PPP Status.....	66
Save Settings/Reboot	67
Appendix	68

Specification

4-Port Ethernet ADSL Router

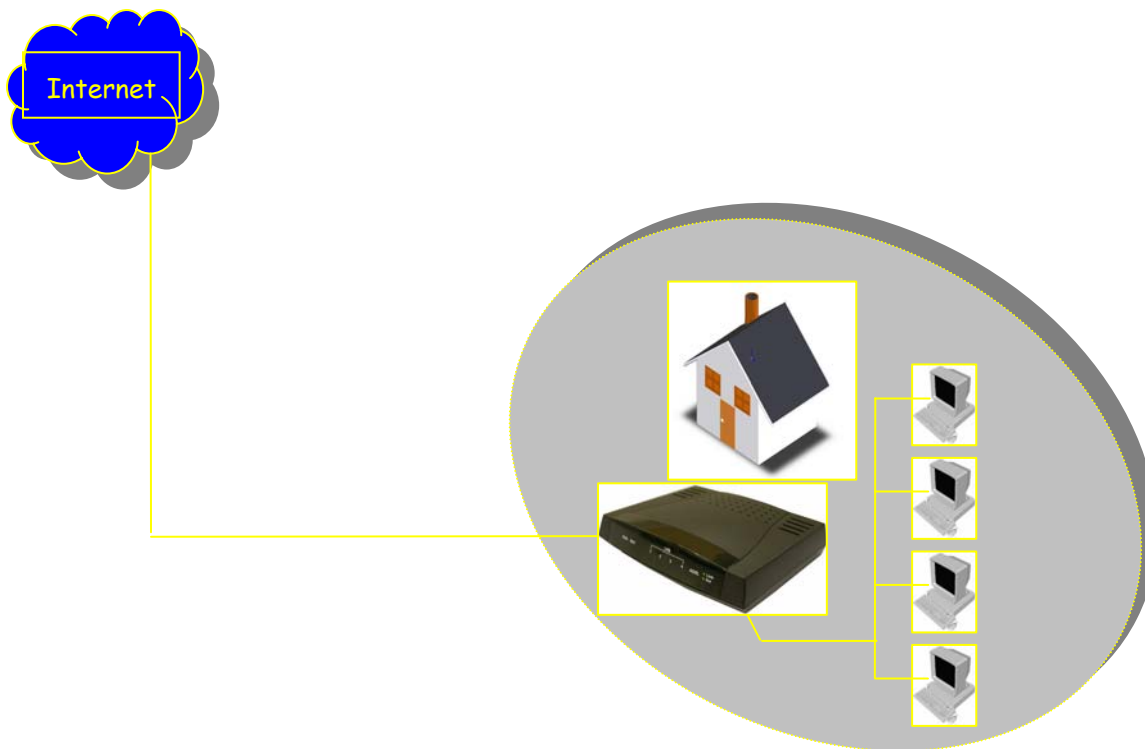
Features

- ◆ ADSL Compliance
 - ANSI T1.413 i2
 - ITU G.992.1 (G.dmt) Annex A, B
 - ITU G.992.2 (G.lite)
 - Maximum downstream rate of 8Mbps
 - Maximum upstream rate of 1Mbps
 - Dying Gasp (optional)
- ◆ ATM Protocols and Encapsulations
 - PPP over ATM (RFC 2364)
 - PPP over Ethernet (RFC 2516)
 - Bridged/Routed Ethernet over ATM (RFC 1483)
 - Classical IP over ATM (RFC 1577)
 - ATM Forum UNI 3.1/4.0 PVC
 - 10 PVCs (simultaneous and encapsulation independent)
 - VPI/VCI range 0-255, 0-65536
 - Encapsulation hunting of up to 8 pre-defined VPI/VCI & encapsulation sets
 - ATM AAL5 (Adaption Layer type 5) UBR & CBR
 - OAM F4/F5
- ◆ Bridging Functionality
 - IEEE 802.1D (self learning transparent bridge)
 - 256 MAC Addresses support
 - PPP Half Bridge - No 3rd party PPPoE client software required
- ◆ Routing Functionality
 - Static IP routing (configurable route table)
 - RIPv2 (backward compatible with RIPv1)

- DHCP server/client/relay agent
- PPP auto reconnect and configurable timeouts
- PPP auto reconnect on WAN access
- PPP Auto, PAP, and CHAP
- 128 character support for PPPx username/passwords
- DNS proxy
- NAT, NAT & Dynamic NAT
- ALG support (FTP, SMTP/POP3, ICMP, NNTP, RTSP, IRC, CuSeeMe, Telnet, Messenger, EPIC games, id games, Sierra studios games)
- Wild Card DMZ
- Virtual server (Port mapping)
- VPN pass through (IPSec - ESP Tunnel mode, L2TP, PPTP)
- Bridge filtering
- ICMP
- IGMP
- MAC Address Spoofing
- Auto VPI/VCI PPPoE/PPPoA detection
- Multiple PPP sessions per PVC
- ◆ Management
 - HTTP client and server
 - Password protection (2 levels)
 - Configurable Web pages
 - FTP server and client (for network upgrade)
 - Local firmware upgrade via Web configuration pages
 - Remote firmware upgrade via FTP client
 - Restore to Factory defaults via Web or hardware reset
 - 7 layer diagnostics with links to help pages
 - System logging
 - Inner pair / Outer pair / Auto-detection of RJ-11
- ◆ Ethernet Features
 - IEEE 802.3/802.3u auto-negotiation compliant
 - Auto sense 10/100 Full or Half duplex mode
 - Half duplex - back pressure flow control
 - Full duplex - IEEE 802.3x flow control
 - Crossover Detection and Auto Correction

- ◆ Hardware
 - LAN: 4-Port 10/100Base-T (RJ-45)
 - ADSL: One Port (RJ-11)
 - Power: 9VAC 800mA
 - LED indicators: Power, Ready (Status), ADSL, LAN * 4
 - Reset button
- ◆ Certification: FCC Part 15/Part 68, CE, LVD

Application Diagram

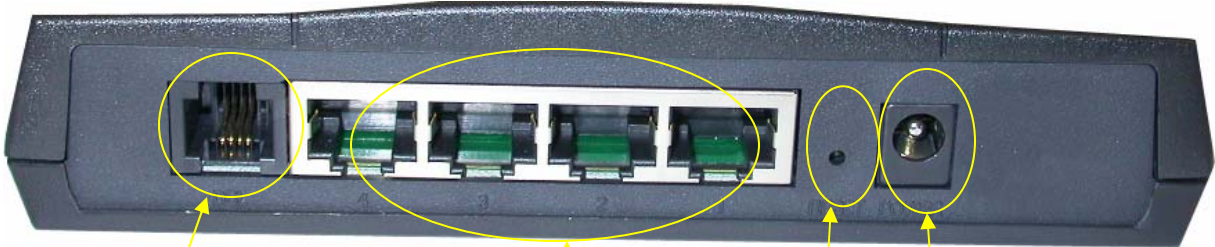


Package Contents

- ◆ ADSL Router
- ◆ CD-ROM containing Manual
- ◆ Ethernet Cable (CAT5 UTP Straight-Through)
- ◆ ADSL Cable (Standard telephone cable)
- ◆ USB Cable (Optional)
- ◆ Power Adapter
- ◆ Quick Installation Guide hardcopy

Hardware Connecting

4 Port Ethernet ADSL Router



Splitter (optional and changes depending on country specification)



RJ-45 Ethernet port connect Ethernet cable here



RJ-11 ADSL port connect ADSL cable here

Factory Reset



Power Adapter (9VAC/800mA)
Power cord connect here

LED Indicators

4 Port Ethernet ADSL Router

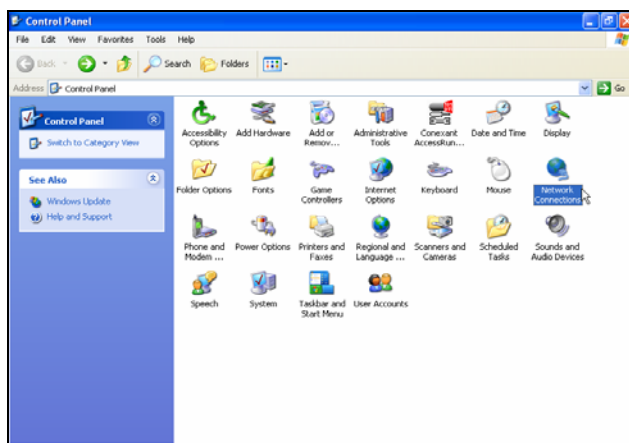
Label	Meaning	Status	Indicates
PWR	Power	On	Power is on
		Off	Power is off
RDY	WAN Link	Flashing	Link being attempted by router.
		On	Link established
		Off	No link
LAN 1/ LAN 2/ LAN 3/ LAN 4	LAN Link	Flashing	Flashes when data is being sent or received on the LAN connection.
		On	Indicates a link to your LAN or Network card is active.
		Off	Indicates no link to LAN

General Setting

You can use the RJ 45 cable or the USB cable connect to the ADSL Router. Please see the connecting procedures as below:

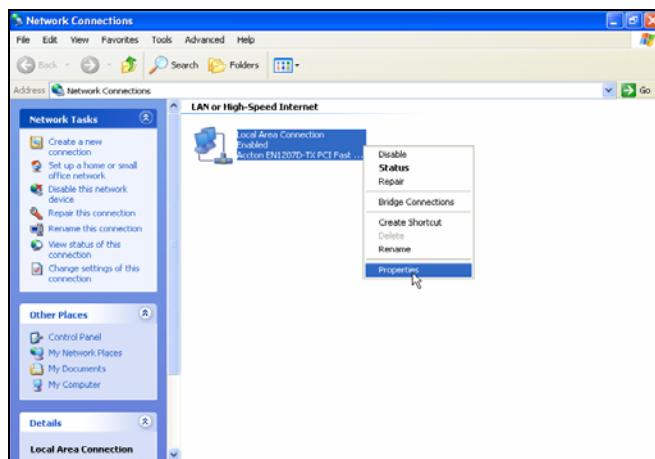
Step 1

Move your cursor as following sequence **Start \ Settings \ Control Panel** and click **Control Panel**. Then double-click on the **Network Connections**



Step 2

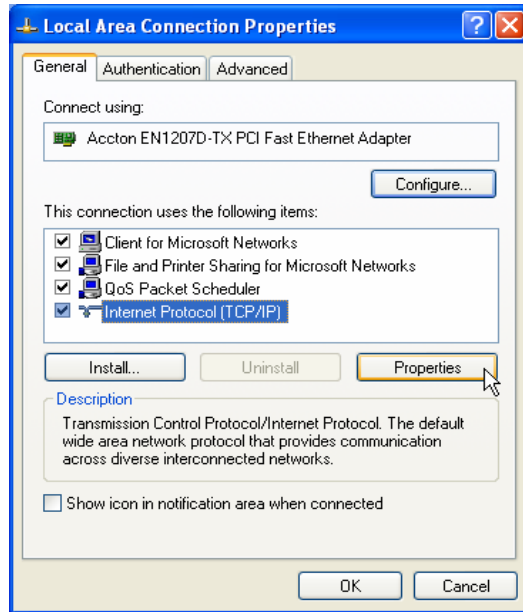
In the **LAN or High-Speed Internet** window, right-click on icon corresponding to your network interface card (NIC) and select **Properties**. (This icon may be labeled Local Area Connection).



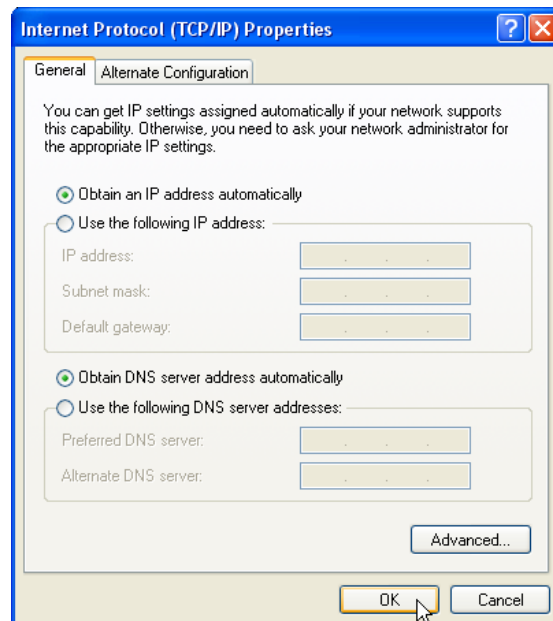
Step 3

In the **General** Tab of the **Local Area Connection Properties** menu.

Highlight **Internet Protocol (TCP/IP)** under “This connection uses the following items.” by click on it once. Click on the **Properties** button.



Select **Obtain an IP address automatically**: by clicking once in the circle. Click **OK** button to confirm and save your changes, and the close the Control Panel.



Release IP & Renew IP, then Check Default Gateway: **10.0.0.2**

```
Command Prompt
C:\Documents and Settings\Eve>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\Documents and Settings\Eve>ipconfig /renew

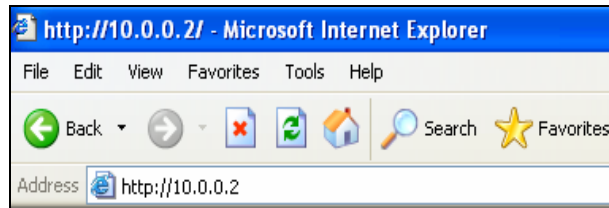
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 10.0.0.8
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 10.0.0.2
```

Step 6

Launch your PC web browser and enter the URL: **10.0.0.2**



Step 7

In the **User name/Password** prompt, please type in **admin/epicrouter** as default.



Step 8

Now you can start browsing the web through the ADSL device.

Main Menu (Simple)

BASIC

- [OnePage Setup](#)
- [show advanced settings](#)

Status

- [Router](#)
- [ADSL](#)
- [PPP](#)

[Save Setting and Reboot](#)

OnePage Configuration

LAN

IP Address:

Subnet Mask:

WAN

Service Name:

Username:

Password:

Disconnect Timeout: seconds (Max:32767)

WAN Type:

VC Settings

VPI:

VCI:

Static IP Address:

Subnet Mask:

Default Gateway:

BRIDGE

One Page Setup

When working with wide area connections, the first thing you must do is to have the handle of the connection. Once you have the handle for a Connection you must define the PVC and protocol settings for it.

The screenshot shows the 'OnePage Configuration' interface. On the left is a 'Main Menu' with 'BASIC' settings (OnePage Setup, show advanced settings) and 'Status' (Router, ADSL, PPP). A 'Save Setting and Reboot' button is at the bottom of the menu. The main area is titled 'OnePage Configuration' and contains the following fields:

- LAN**
 - IP Address: 10.0.0.2
 - Subnet Mask: 255.255.255.0
- WAN**
 - Service Name: [empty]
 - Username: [empty]
 - Password: [empty]
 - Disconnect Timeout: 0 seconds (Max:32767)
 - WAN Type: PPPoE/LLC
- VC Settings**
 - VPI: 8
 - VCI: 35
 - Static IP Address: 192.168.241.101
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 0.0.0.0
- BRIDGE**

This screenshot shows the same configuration page but with the 'BRIDGE' section expanded. It includes a 'mode' dropdown menu set to 'Disabled'. Below the settings, the 'Connection Status' is 'Not Connected'. There are 'Connect' and 'Disconnect' buttons. At the bottom, there are 'Submit' and 'Reset' buttons. A red message at the bottom states: 'You must click the 'Submit' button and then 'Save setting and Reboot' button to commit changes.'

LAN IP Address & Subnet Mask: The default is 10.0.0.2 and 255.255.255.0 you can change it to another private IP address, such as 211.22.10.191 and 255.0.0.0.

For most configurations it is recommended to leave it as default.

Service Name: Enter the name of your ISP. This information is for identification purposes only.

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Disconnect Timeout: Disconnect Timeout means the router will disconnect after being idle for a preset amount of time.

WAN Type: Select type from the list.

VC Settings

VPI: If instructed to change this, type in the VPI value for the initial connection (using PVC 0). Default = **8**.

VCI: If instructed to change this, type in the VCI value for the initial connection (using PVC 0). Default = **35**.

Static IP Address: Enter the IP address provided by your ISP. such as 192.168.241.101.

Subnet Mask: Set your Subnet Mask such as 255.255.255.0

BRIDGE

Mode: Select **Enable** or **Disable** from the list.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Status

Router

The Home page shows the Firmware Version and WAN and LAN interface status.

The screenshot shows the router's Home Page. On the left is a navigation menu with sections: ADMINISTRATION (WAN, LAN, DNS, NAT, Port Forwarding, ADSL Configuration, RIP Configuration, Firewall, Diagnostic Test, Route Table, MAC Filtering), SECURITY (Admin Password, User Password, Misc Configuration, System Log, Code Update), and Status (Router, ADSL, WAN, ATM, TCP connections, Leamed MAC Table, PPP Status). A 'Save Setting and Reboot' button is at the bottom left. The main content area is titled 'Home Page' and displays: BootCode Version: BC_CX82xxx_4.1.0.21, Firmware Version: CX82xxx_4.1.0.21_S, and Customer Software Version: 4.1.0.21_S. Below this is the WAN section with a table for IP Address, Subnet Mask, and MAC Address. The LAN section has a table with IP Address, Subnet Mask, and MAC Address, showing 10.0.0.2, 255.255.255.0, and 00:09:F3:00:00:8D. It also shows 'Total Number of Lan Interfaces: 1' and 'Number of ethernet devices connected to the DHCP server: 1'. At the bottom, there is a table for IP Address and MAC Address.

This screenshot shows the WAN and LAN status page. The navigation menu is the same as in the previous screenshot. The main content area displays the WAN section with a table for IP Address, Subnet Mask, and MAC Address. Below this is the LAN section with a table for IP Address, Subnet Mask, and MAC Address, showing 10.0.0.2, 255.255.255.0, and 00:09:F3:00:00:8D. It also shows 'Total Number of Lan Interfaces: 1' and 'Number of ethernet devices connected to the DHCP server: 1'. At the bottom, there is a table for IP Address and MAC Address with one entry: 1, 10.0.0.3, 72:0B:49:E7:2B:23. Below the table, it shows 'Ethernet Link Status: UP' and 'USB Link Status: DOWN'.

Firmware Version: This field displays the Firmware Version number.

WAN: These fields display the IP Address, Subnet Mask, MAC Address for WAN interface.

LAN: These fields display the IP Address, Subnet Mask, MAC Address for LAN interface.

Number of Ethernet devices connected to the DHCP server: This field displays the number of DHCP clients connected to the ADSL Router. It also shows the IP address and MAC address of the attached DHCP clients.

ADSL

The ADSL Status page shows the ADSL physical layer status.

The screenshot shows the ADSL STATUS page with a left sidebar menu and a main content area. The sidebar includes 'Main Menu (Simple)', 'BASIC' (OnePage Setup, show advanced settings), and 'Status' (Router, ADSL, PPP). A 'Save Setting and Reboot' button is at the bottom of the sidebar. The main content area has a title 'ADSL STATUS' and 'Restart' and 'Execute' buttons. It displays the following parameters:

- Showtime Firmware Version: 3.46
- 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 16 minutes 48 seconds

Below the parameters is a table with the following data:

	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

Showtime Firmware Version: This field displays the ADSL data pump firmware version number.

Line State: This field displays the ADSL connection process and status.

Modulation: This field displays the ADSL modulation status for G.dmt or T1.413.

Annex Mode: This field displays the ADSL Annex modes for Annex A or Annex B.

Startup Attempts: This field displays the ADSL connection attempts after loss of showtime.

Max Tx Power: This field displays the transmit output power level of the CPE.

Co Vendor: This field displays the Central Office DSLAM vendor name. If available.

Elapsed Time: This field displays the time of the modem has been in operation.

PPP

The PPP Status page shows the status of PPP for each PPP interface. See PPP.

PPP

#	Connection Name	Interface	Mode	Status	Pkts Sent	Pkts Rcvd	Bytes Sent	Bytes Rcvd
1	PPPoPvc 0	Pvc 0	PPPoE	Not Connected	N/A	N/A	N/A	N/A

If a * appears under Mode column, you need to [check the WAN configuration](#) to make sure the VC has the correct encapsulation.

Connection #:

These fields display the following information on each PPP interface:

- ◆ Connection Name (user defined)
- ◆ Interface (PVC)
- ◆ Mode (PPPoE or PPPoA)
- ◆ Status (Connected or Not Connected)
- ◆ Packets Sent
- ◆ Packets Received
- ◆ Bytes Sent
- ◆ Byte Received

Connect and Disconnect: Each PPP session can be individually controlled, simply enter the desired connection number into the “Connection #” field and select either connect or disconnect from the drop down menu and click on the “Execute” button.

WAN Configuration: The WAN configuration page allows the user to set the configuration WAN/ADSL ports.

The image displays two screenshots of the WAN Configuration web interface. The top screenshot is the 'Advanced' view, showing a 'Main Menu' on the left with categories like BASIC, ADMINISTRATION, SECURITY, and Status. The main content area is titled 'WAN Configuration (Pvc 0)' and includes a 'Change Adapters' button. It features several configuration sections: 'Virtual Circuit' (Enabled), 'Bridge' (Disabled), 'IGMP' (Disabled), 'Encapsulation' (PPPoE LLC), 'Static IP Settings' (IP Address: 192.168.241.101, Subnet Mask: 255.255.255.0, Gateway: 0.0.0.0), 'ATM' (VPI: 8, VCI: 35, Service Category: UBR, Peak Cell Rate: 0 kbps, Sustainable Cell Rate: 0 kbps, Max Burst Size: 0), 'DHCP Client' (Disabled), and 'PPP' (Advanced PPP configuration, Service Name, Username, Password, Disconnect Timeout: 0 minutes, MRU: 1492, MTU: 1492, MSS: 1432, Lcp Echo Interval: 10 seconds). The bottom screenshot is the 'Simple' view, showing a 'Main Menu' with 'show advanced settings' and 'Save Setting and Reboot' buttons. The main content area includes 'VPI' (8), '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), 'Service Name', 'Username', 'Password', 'Disconnect Timeout' (0 minutes), 'PPP Disconnect Timer Config', 'MRU' (1492), 'MTU' (1492), 'MSS' (1432), 'Lcp Echo Interval' (10 seconds), 'Lcp Echo Maximum' (6), 'Consecutive Failure', 'Authentication' (Auto), and 'Automatic Reconnect' (checked). At the bottom, there are 'Submit' and 'Reset' buttons, a note that 'Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.', and a 'Save Configuration' link.

Per VC Settings

Virtual Circuit: Selection Enable or Disable.

VPI: If instructed to change this, type in the VPI value for the initial connection (using PVC 0). Default = 0.

VCI: If instructed to change this, type in the VCI value for the initial connection (using PVC 0). Default = 0

MAC Spoofing: MAC Spoofing is developed to solve the scenario when the ISP only recognizes one MAC address. Copy the ISP-recognized MAC address here.

ATM

Service Category: UBR and CBR are supported from the ATM.

Bandwidth: Bandwidth setting takes effect only when the CBR is selected. The maximum available bandwidth is from the upstream data rate of ADSL status page.

ENCAPSULATION: Selection follow as Table-1 Configuration

BRIDGE: Enabling bridge mode will place the unit into Transparent bridge mode (like a Ethernet ADSL modem) to use this mode you should also set your WAN type to a Bridging option (e.g RFC1482 Bridge using LLC).

IGMP: IGMP relay/proxy specification and environment:

Support IGMP proxy/relay function for ADSL modem, based on the following requirement and case:

On CO side, there must be at least one IGMP querier (router) present. IGMP querier will send IGMP query packet. The ADSL modem is responsible to relay these IGMP query to Ethernet.

End-user multicast application device send IGMP report while receiving IGMP query or being activated by user, the ADSL modem should be responsible to proxy (that is, change source IP to ADSL modem's WAN IP) the IGMP report to ADSL WAN side, include 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-1 Configuration

WAN Configuration	Bridge Mode	Router Mode (PPPoA/PPPoE)	Router Mode (Dynamic IP)	Router Mode (Static IP)
IP address	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP
Subnet Mask	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP
WAN Type	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 VC-Mux, Classical IP over ATM	1483 Bridged/Routed IP LLC, 1483 Bridged/Routed VC-Mux, Classical IP over ATM
Bridge	Enabled	Disabled	Disabled	Disabled
PPP Service	N/A	Provided by ISP	N/A	N/A
PPP User name	N/A	Provided by ISP	N/A	N/A
PPP Password	N/A	Provided by ISP	N/A	N/A
DHCP Client enable	Unchecked	Unchecked	Checked	Unchecked

Table-2

Rx Entity	Packet Class	TTL	Action	Notes
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 PVC	
	IGMP leave	1	Relay to all ADSL PVC	
	General Multicast IP	-	Ignore	

PPP: The current release supports multiple PPP sessions per PVC. The PPP configuration in the WAN configuration page is for the first PPP session for each PVC. The predefined PPP Account Name (Account ID) is “Simple PPP Account 0” for PVC0 and predefined PPP Connection Name is “Simple PPP Session 0” for PVC0. For the other PVC X, the predefined account name and connection name will be Simple PPP Account X and Simple PPP Session X. X is the PVC number from 1 to 7.

It 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.

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

Username: Your user name provided by your ISP.

Password: Your password provided by your ISP.

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

MRU: Maximum Receive Unit indicates the peer of PPP connection the maximum size of the PPP information field this device can be received. The default value is 1492 and is used in the beginning of the PPP negotiation. In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

MTU: Maximum Transmission Unit indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer’s MRU. The default is value 1492.

MSS: Maximum Segment Size is the largest size of data that TCP will send in a single IP packet. When a connection is established between a LAN client and a host in the WAN side, the LAN client and the WAN host will indicate their MSS during the TCP connection handshake. The default value is 1432.

Automatic Reconnect: When it is checked, it will maintain the PPP connection all the time. If the ISP shut down the PPP connection, it will automatically reconnect PPP session.

DHCP: Use Table-1 to configure a valid setting for each PVC.

Host Name: Required by some ISPs. If the ISP does not provide the Host name,

please leave it blank.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Advanced Setting

ADMINISTRATION

The links under the ADMINISTRATION column are associated to the pages that represent the configurations of system and interfaces.

*Note: When the configurations are changed, please click the **Save Setting** and **Reboot** button.*

WAN

The WAN configuration page allows the user to set the configuration for WAN/ADSL ports.

The screenshot displays the WAN Configuration (Pvc 0) page. The left sidebar contains a navigation menu with the following items:

- Main Menu (Advanced)
- BASIC
 - OnePage Setup
 - hide advanced settings
- ADMINISTRATION
 - WAN
 - LAN
 - DNS
 - NAT
 - Port Forwarding
 - ADSL Configuration
 - RIP Configuration
 - Firewall
 - Diagnostic Test
 - Route Table
 - MAC Filtering
- SECURITY
 - Admin Password
 - User Password
 - Misc Configuration
 - System Log
 - Code Update
- Status
 - Router
 - ADSL
 - WAN
 - ATM
 - TCP connections
 - Learned MAC Table

The main content area is titled "WAN Configuration (Pvc 0)" and includes a "Change Adapter" button. The configuration options are as follows:

- Virtual Circuit:** Enabled (dropdown)
- Bridge:** Disabled (dropdown)
- IGMP:** Disabled (dropdown)
- Encapsulation:** PPPoE/LLC (dropdown)
- Static IP Settings:**
 - IP Address: 192.168.241.101
 - Subnet Mask: 255.255.255.0
 - Gateway: 0.0.0.0
- ATM:**
 - VPI: 8
 - VCI: 35
 - Service Category: UBR (dropdown)
 - Peak Cell Rate: 0 kbps
 - Sustainable Cell Rate: 0 kbps
 - Max Burst Size: 0
- PPP:**
 - Advanced PPP configuration (link)
 - Service Name: [text input]
 - Username: [text input]
 - Password: [text input]
 - Disconnect Timeout: 0 minutes (Max:32767)
 - PPP Disconnect Timer Config (link)
 - MRU: 1492
 - MTU: 1492
 - MSS: 1432
 - Lcp Echo Interval: 10 seconds
 - Lcp Echo: [text input]
- DHCP Client:** Disabled (dropdown)
- Host Name: [text input]

Per VC Settings

Virtual Circuit: Selection Enable or Disable.

VPI: If instructed to change this, type in the VPI value for the initial connection (using PVC 0). Default = 0.

VCI: If instructed to change this, type in the VCI value for the initial connection (using PVC 0). Default = 0

MAC Spoofing: MAC Spoofing is developed to solve the scenario when the ISP only recognizes one MAC address. Copy the ISP-recognized MAC address here.

ATM

Service Category: UBR and CBR are supported from the ATM.

Bandwidth: Bandwidth setting takes effect only when the CBR is selected. The maximum available bandwidth is from the upstream data rate of ADSL status page.

ENCAPSULATION: Selection follow as Table-1 Configuration

BRIDGE: Enabling bridge mode will place the unit into Transparent bridge mode (like a Ethernet ADSL modem) to use this mode you should also set your WAN type to a Bridging option (e.g RFC1482 Bridge using LLC).

IGMP: IGMP relay/proxy specification and environment:

Support IGMP proxy/relay function for ADSL modem, based on the following requirement and case:

On CO side, there must be at least one IGMP querier (router) present. IGMP querier will send IGMP query packet. The ADSL modem is responsible to relay these IGMP query to Ethernet.

End-user multicast application device send IGMP report while receiving IGMP query or being activated by user, the ADSL modem should be responsible to proxy (that is, change source IP to ADSL modem's WAN IP) the IGMP report to ADSL WAN side, include 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-1 Configuration

WAN Configuration	Bridge Mode	Router Mode (PPPoA/PPPoE)	Router Mode (Dynamic IP)	Router Mode (Static IP)
IP address	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP
Subnet Mask	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP
WAN Type	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 VC-Mux, Classical IP over ATM	1483 Bridged/Routed IP LLC, 1483 Bridged/Routed VC-Mux, Classical IP over ATM
Bridge	Enabled	Disabled	Disabled	Disabled
PPP Service	N/A	Provided by ISP	N/A	N/A
PPP User name	N/A	Provided by ISP	N/A	N/A
PPP Password	N/A	Provided by ISP	N/A	N/A
DHCP Client enable	Unchecked	Unchecked	Checked	Unchecked

Table-2

Rx Entity	Packet Class	TTL	Action	Notes
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 PVC	
	IGMP leave	1	Relay to all ADSL PVC	
	General Multicast IP	-	Ignore	

PPP: The current release supports multiple PPP sessions per PVC. The PPP configuration in the WAN configuration page is for the first PPP session for each PVC. The predefined PPP Account Name (Account ID) is “Simple PPP Account 0” for PVC0 and predefined PPP Connection Name is “Simple PPP Session 0” for PVC0. For the other PVC X, the predefined account name and connection name will be Simple PPP Account X and Simple PPP Session X. X is the PVC number from 1 to 7.

It 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.

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

Username: Your user name provided by your ISP.

Password: Your password provided by your ISP.

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

MRU: Maximum Receive Unit indicates the peer of PPP connection the maximum size of the PPP information field this device can be received. The default value is 1492 and is used in the beginning of the PPP negotiation. In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

MTU: Maximum Transmission Unit indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer’s MRU. The default is value 1492.

MSS: Maximum Segment Size is the largest size of data that TCP will send in a single IP packet. When a connection is established between a LAN client and a host in the WAN side, the LAN client and the WAN host will indicate their MSS during the TCP connection handshake. The default value is 1432.

Automatic Reconnect: When it is checked, it will maintain the PPP connection all the time. If the ISP shut down the PPP connection, it will automatically reconnect PPP session.

DHCP: Use Table-1 to configure a valid setting for each PVC.

Host Name: Required by some ISPs. If the ISP does not provide the Host name,

please leave it blank.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

LAN

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

The screenshot shows the LAN Configuration page with the following settings:

- IP Address: 10.0.0.2
- Subnet Mask: 255.255.255.0
- DHCP Server: Enabled
- DHCP address pool selection: System Allocated
- User Defined Start Address: 10.0.0.4
- User Defined End Address: 10.0.0.15
- DHCP Gateway Selection: Automatic
- User Defined Gateway Address: (empty)
- Lease Time: 1 days 0 hours 0 minutes 0 seconds
- DHCP Relay: Disabled
- DHCP Relay Target IP: 0.0.0.0
- User Mode: Multi-User

The screenshot shows the DHCP Server configuration page with the following settings:

- DHCP Server: Enabled
- DHCP address pool selection: System Allocated
- User Defined Start Address: 10.0.0.4
- User Defined End Address: 10.0.0.15
- DHCP Gateway Selection: Automatic
- User Defined Gateway Address: (empty)
- Lease Time: 1 days 0 hours 0 minutes 0 seconds
- DHCP Relay: Disabled
- DHCP Relay Target IP: 0.0.0.0
- User Mode: Multi-User

Buttons: [Ethernet Mode Setting](#), ,

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

[Save Configuration](#)

LAN IP Address & Subnet Mask: The default is 10.0.0.2 and 255.0.0.0 you can change it to another private IP address, such as 211.22.10.191 and 255.255.255.0. For most configurations it is recommended to leave it as default.

DHCP Server: System Allocated. The DHCP address pool is based on LAN port IP address plus 12 IP address. For example, the LAN IP address is 10.0.0.2; the DHCP address pool is at the range of 10.0.0.3 to 10.0.0.14.

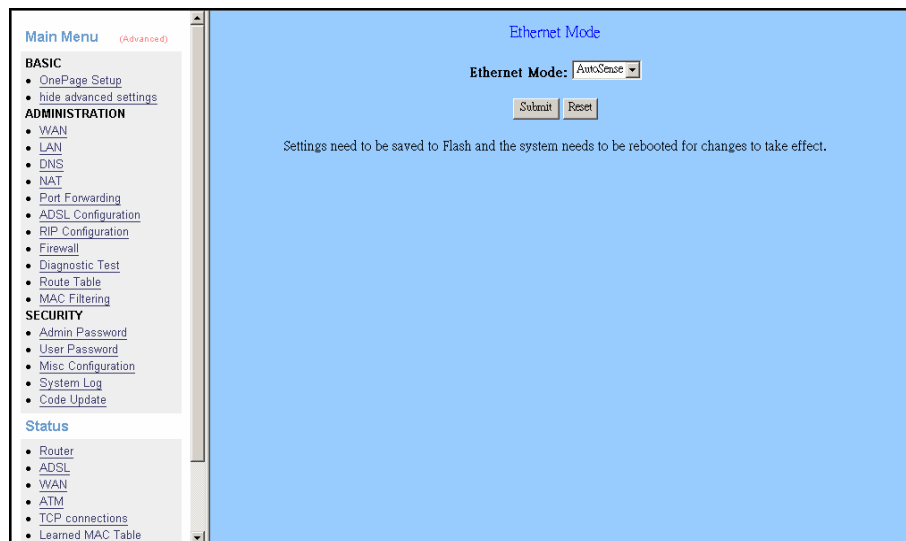
User Defined: The DHCP address pool is at the range of User Defined Start Address and User Defined End Address. The maximum pool size can be 253 IP address:255 total IP address-1 broadcast address-1 LAN port IP address.

DHCP Gateway Selection: The default setting for the DHCP Gateway Selection is “Automatic”. The user can select the “User Defined” to specify “User Defined Gateway Address”. The DHCP server will issue the “ User Defined Gateway Address” to the LAN DHCP client.

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

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

Ethernet Mode Setting: The Ethernet Mode Configuration page allows the user to set the LAN port into Auto Sense, 100 Mbps Full Duplex, 100 Mbps Half Duplex, 10 Mbps Full Duplex or 10 Mbps Half Duplex.



Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

DNS

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

The screenshot shows the DNS Configuration page. The left sidebar lists various system settings. The main area is titled 'DNS Configuration' and includes the following elements:

- DNS Proxy:** A dropdown menu set to 'Enabled'.
- Auto Discovery:** A checked checkbox.
- User Configuration:** An unchecked checkbox.
- DNS Server:** An input field with an 'Add' button.
- DNS Server:** A dropdown menu set to 'Disabled'.
- Url Name:** An input field.
- Host Ip:** An input field with an 'Add' button.
- Buttons:** 'Apply' and 'Reset' buttons.
- Tables:**
 - DNS Proxy Setting:** A table with one row: # DNS Server IP.
 - DNS Server Setting:** A table with two rows: # Url Name (Host.Domain) and # Host IP.
- Text:** 'Settings take effect immediately, no system reboot is required'.
- Link:** [Save Configuration](#).

Disable DNS Proxy: 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 preferred DNS server or alternate DNS server whichever is available as the DNS server. Then all DNS query messages will be directly sent to the DNS servers.

Use Auto Discovered DNS Servers Only: The DNS proxy will store the DNS server IP addresses obtained from DHCP client or PPP into the table. And all DNS query messages will be sent to one of the dynamically obtained DNS servers.

Use User Configured DNS Servers Only: The DNS proxy will use the user-configured preferred DNS server and alternate DNS server. And all DNS query message will be sent to one of DNS servers.

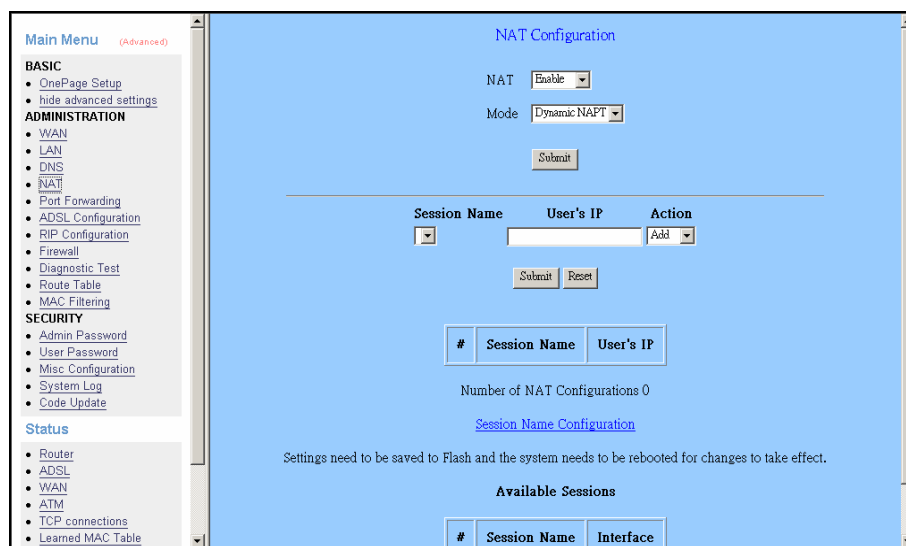
Auto Discovery + User Configured: The DNS proxy's table has all the IP addresses of dynamically obtained and user configured DNS servers.

User Configuration: Place your primary and secondary DNS addresses here.

NAT

The NAT Configuration page allows users to set the configuration for the Network Address Translation. The default setting is Dynamic NAT. It provides dynamic Network Address Translation capability between LAN and multiple WAN connections, and the LAN traffic is routed to appropriate WAN connections based on the destination IP address and Route Table. This eliminates the need for the static NAT session configuration between multiple LAN clients and multiple WAN connections.

When the Dynamic NAT is chosen, there is no need to configure the NAT Session and NAT Session Name Configuration.



The NAT option only maps single WAN IP address to the local PC IP address. It is peer-to-peer mapping. (1x1) for each WAN interface, only one local PC IP address can be associated with each WAN interface. Click the link Session Name Configuration to add the session name for WAN interface.

The NATP option only maps single WAN IP address to many local PCs IP address. (1xN). It is the multiple-mapping mechanism. For each WAN Interface, more than one local PC can be associated with one WAN Interface. Click the link Session Name Configuration to add the session name for WAN interface.

Session Name: This field allows the user to select the session form the configured NAT Session Name Configuration.

User's IP: This field allows the user to assign the IP address to map the corresponding NAT/NAPT sessions.

Session Name Status will be displayed at the middle of this page to show the corresponding Session Name with its IP address.

Number of NAT Configurations: This field displays the total number of NAT Sessions is entered.

Available Sessions Status will be displayed at the end of this page to show all the Session Name with its WAN Interface.

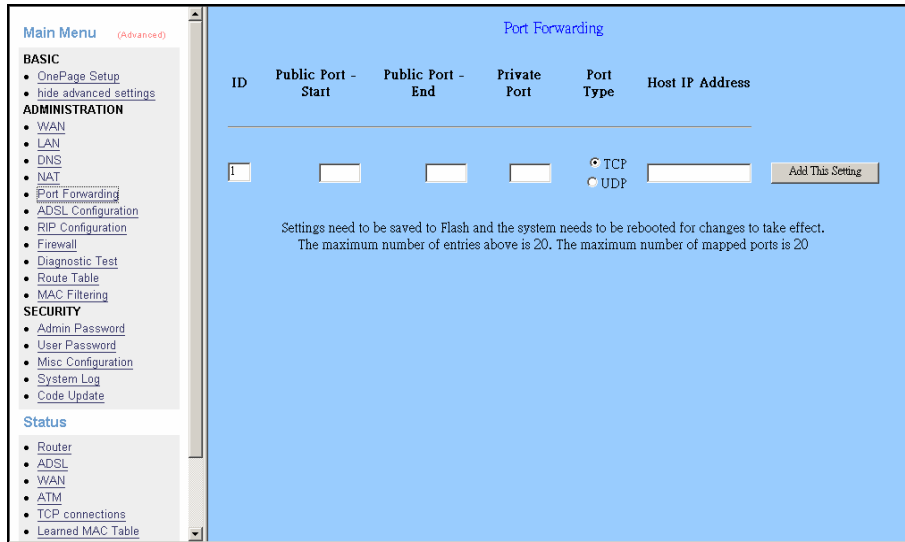
Interface: This field allows the user to choose specific WAN Interface (PVC or PPP Session) for NAT Session.

Number of Session: This field displays the total number of NAT Sessions Name is entered.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Port Forwarding

The Port Forwarding page allows the user define a port forwarding rule without using the firewall policy database definitions and apply it to the connection.



Public Port: This field allows the user to enter the port number of Public Network.

Private Port: This field allows the user to enter the port number of the Private Network.

Host IP Address: This field allows the user to enter the private network IP address for the particular server.

Well Known Ports:

Port	Protocol
21	FTP
23	Telnet
25	SMTP
43	Whois
53	DNS
69	TFTP
70	Gopher
79	Finger
80	HTTP
110	POP3
115	SFTP
161	SNMP
162	SNMP traps

ADSL Configuration

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

The screenshot shows the ADSL Configuration page. The left sidebar contains a navigation menu with the following items: Main Menu (Advanced), BASIC (OnePage Setup, hide advanced settings), ADMINISTRATION (WAN, LAN, DNS, NAT, Port Forwarding, ADSL Configuration, RIP Configuration, Firewall, Diagnostic Test, Route Table, MAC Filtering), SECURITY (Admin Password, User Password, Misc Configuration, System Log, Code Update), and Status (Router, ADSL, WAN, ATM, TCP connections, Learned MAC Table). The main content area is titled 'ADSL Configuration' and features four configuration options, each with a dropdown menu: 'Trellis' (set to 'Enabled'), 'Handshake Protocol' (set to 'Autoselect - G.dmt first'), 'Wiring Selection' (set to 'Tip/Ring'), and 'Bit Swapping (No system reboot needed)' (set to 'Enabled'). Below these options are 'Submit' and 'Reset' buttons. A note at the bottom states: 'Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.'

Trellis: This field allows the user to enable or disable the Trellis Code. By default, it is always enabled.

Handshake Protocol: This field allows the user to select the ADSL handshake protocol.

Wiring Selection: This field allows the user to enter the wiring selection for the RJ-11. Tip/Rip is the default for the board without the inner/outer pair relay.

Bit Swapping: This field allows the user to enable or disable the upstream bit swapping.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

RIP Configuration

The RIP System Wide Configuration page allows the user to set the configuration for each Interface (PVCs, PPP Sessions, USB and LAN).

The screenshot shows the 'RIP System Wide Configuration' page. On the left is a 'Main Menu' sidebar with categories: BASIC (OnePage Setup, hide advanced settings), ADMINISTRATION (WAN, LAN, DNS, NAT, Port Forwarding, ADSL Configuration, RIP Configuration, Firewall, Diagnostic Test, Route Table, MAC Filtering), SECURITY (Admin Password, User Password, Misc Configuration, System Log, Code Update), and Status (Router, ADSL, WAN, ATM, TCP connections, Learned MAC Table). The main area is titled 'RIP System Wide Configuration' and contains the following settings:

- RIP: Disabled
- Border Gateway: Enabled
- Supply Interval: 30 Seconds
- Expire Timeout: 180 Seconds
- Garbage Timeout: 120 Seconds

Below these settings is a link for 'Advanced Configuration' and two buttons: 'Submit' and 'Reset'. At the bottom, a note reads: 'Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.'

Interface: This field allows the user to choose the Interface (PVCs, PPP Sessions, USB and LAN), for the RIP to be configured.

Enable: This field allows the user to Enable (Yes) or Disable (No) the Specified interface for RIP.

Supplier: This field allows the user 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: This field allows the user 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.

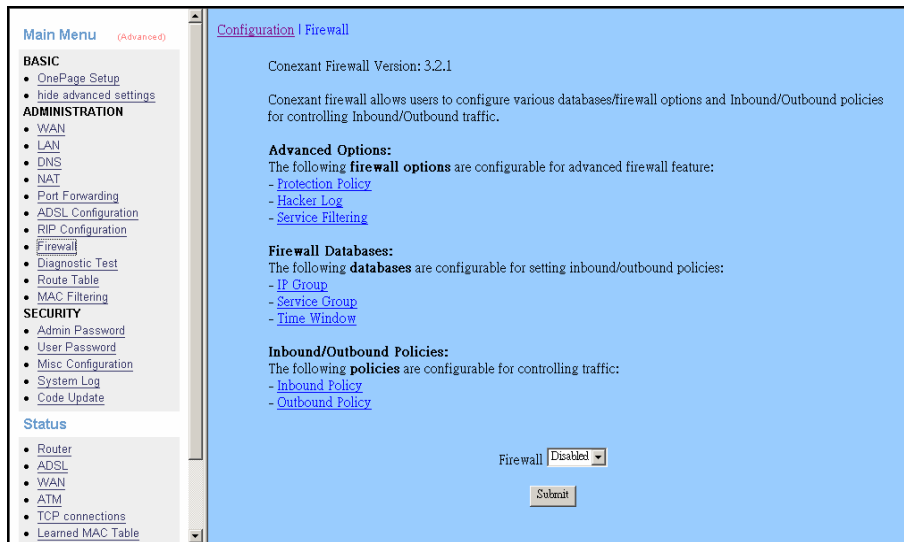
Supplier and Listener are based on section 4.1 "Compatibility Switch" in RFC 1723.

Current RIP Settings: This field displays the each interface's RIP status.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Firewall

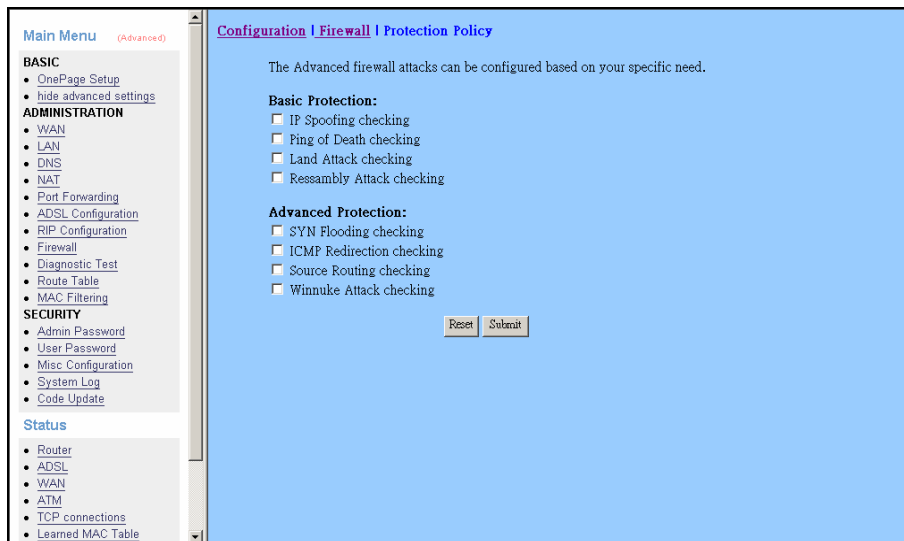
The Firewall page allows users to configure various database/firewall options and Inbound/Outbound policies for controlling Inbound/Outbound traffic.



Firewall: This field allows the user to Disabled or Enabled Firewall.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Protection Policy



IP Spoofing checking: IP spoofing is when an unauthorized user inserts the IP address of an authorized user into the IP packets in order to gain access to a network. Selecting this option will allow the firewall to check for and filter out this discrepancy.

Ping of Death checking: Ping of Death is a type of DoS attack that uses a malformed ICMP data packet that contains unusually large amounts of data that causes TCP/IP to crash or behave irregularly. Enabling this will allow the firewall to filter out packets containing Ping of Death properties.

Land Attack checking: Land attack is a type of DoS attack that works by sending a spoofed packet containing the same source and destination IP address and port (the victim's IP address). This packet contains a connection request, resulting in a handshake process. At the end of the handshake, the victim sends out an ACK (ACKnowledge) request. Since the source and the destination are the same, the victim receives the ACK request it just sent out. The received data does not match what the victim is expecting, so it retransmits the ACK request. This process repeats until the network crashes. Enabling the will allow the firewall to filter out possible Land Attack packets.

Reassembly Attack checking: Reassembly Attack is a type of DoS attack that exploits the weakness of the IP protocol reassembly process. As discussed earlier in this user guide, packets undergo fragmentation when they exceed a certain maximum size. Certain criteria define the packet fragmentation process so that packets can be reassembled properly. In reassembly attack, the sub-packets have malformed criteria (fragment offset), which can easily cause a system to crash, freeze, or reboot. Enable this option to check for and filter out Reassembly Attack packets.

SYN Flooding checking: Syn flooding is a type of DoS attack that is accomplished by not sending the final acknowledgement to the receiving server's SYN-ACK (SYN chronize-ACKnowledge) in the final part of the handshake process. This causes the serve to keep signaling until it is timed out. When a flood (many) of these attacks are sent simultaneously, the server will probably overload and crash. Enable SYN Flooding checking to filter out possible SYN flood packets.

ICMP Redirection checking: Also known as an ICMP storm attack or smurf attack, ICMP redirection is another form of DoS. This attack is performed by sending ICMP echo requests to a broadcast network node. The return IP address is spoofed and replaced by the victim's own address, causing it to send the request back to itself. This causes the broadcast address to send it out to all the network nodes in the broadcast area (usually the entire LAN). In turn, all those recipients resend it back to the broadcast. The process repeats itself, gaining more amplitude through each iteration and eventually causing a traffic overload and crashing the network. Enable ICMP Redirection checking to filter out packets

containing the threat.

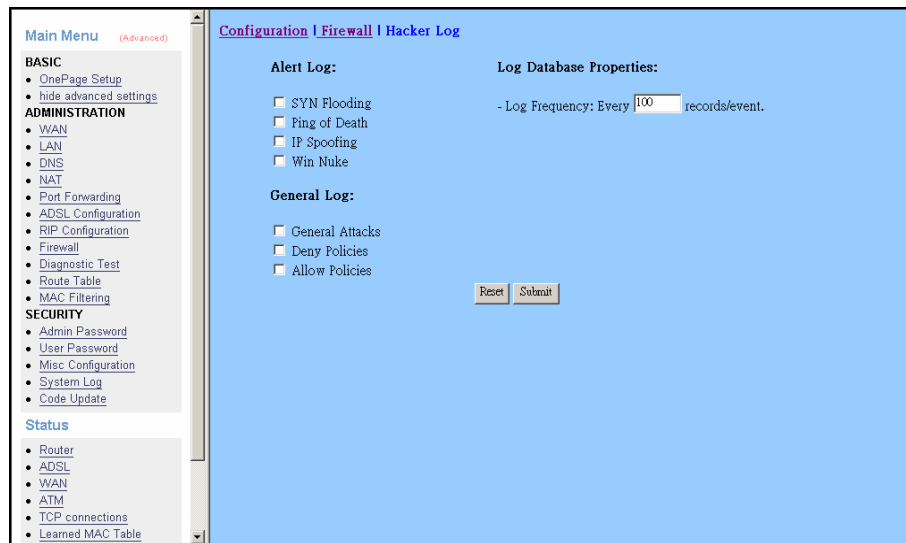
Source Routing checking: Source routing gives the sender of a packet the ability to determine the exact route that an IP packet takes to get to the destination. However, source routing can be used for malicious reasons. Using a source routed packet, the sender could find out important information about nodes in a network, making it easy to exploit any weakness. Enabling Source Routing checking will cause the firewall to filter out any packet with Source Routing properties.

WinNuke Attack checking: WinNuke exploits a large networking bug found in Windows 95 and NT. WinNuke sends erroneous OOB (Out-of Band) data that Windows is unable to process, causing the target computer to crash. Enable this if you are running an early (95 or NT) version of Windows that is vulnerable to this attack.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Hacker Log

This page allows you to configure which Protection Policy (see previous section) violations to log for admin viewing.



Alert Log: Enable/ Disable for SYN Flooding, Ping of Death, IP Spoofing, and WinNuke (all of these are explained in the previous section). Enable to log violations of individual policies.

General Log

Deny Policies: Enabling this will add Deny Policy violations to the log.

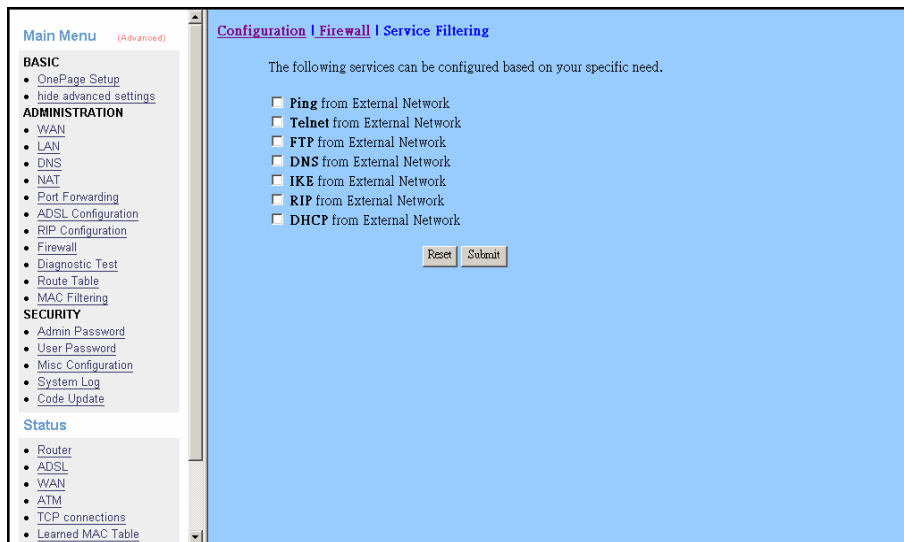
Allow Policies: Enabling this will add Allow Policy acceptances to the log.

Log Frequency: This field lets you specify how many records to keep of each event. Default is 100. Range for Log Frequency Field is 1-65535.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Service Filtering

Service Filtering allows you to disable service request from certain sources.



Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Firewall Databases:

IP Group

The IP Group lets you specify IP Addresses (Single or Range) and Subnet Masks and assign them to a group name for easy use when configuring inbound and out bound policies for the firewall.

The screenshot shows a web interface for configuring the Firewall IP Group. On the left is a navigation menu with categories: Main Menu (Advanced), BASIC (OnePage Setup, hide advanced settings), ADMINISTRATION (WAN, LAN, DNS, NAT, Port Forwarding, ADSL Configuration, RIP Configuration, Firewall, Diagnostic Test, Route Table, MAC Filtering), SECURITY (Admin Password, User Password, Misc Configuration, System Log, Code Update), and Status (Router, ADSL, WAN, ATM, TCP connections, Learned MAC Table). The main content area is titled 'Configuration | Firewall | IP Group' and displays 'No Entries in IP Group Database'. Below this is a table with the following structure:

IP Entry Name	IP addr. 1	IP addr. 2	IP/Mask	
<input type="text"/>	<input type="text"/>	<input type="text"/>	Single IP	<input type="button" value="Add/Modify this entry"/>

IP Entry Name: This is the name you assign to the group of IP addresses and subnet masks. (The IP Entry Name can be up to 19 characters.)

IP addr. 1: This is the IP address or subnet mask you are specifying when creating a groups.

IP addr. 2: This field is only active if you select to group a range of IP addresses or subnet masks, in which case this is the end address of that range whereas the IP addr 1 is the first address of that range.

IP/Mask: This field allows you to specify the address type assigned to the group.


Single IP: This will let you specify one IP address for a given group.

IP Range: This will let you specify a range of IP addresses for a given group, starting with IP addr 1 and ending with IP addr 2.

Subnet Mask: This will let you specify a range of subnet masks for a given group.

Service Group

The Service Group lets you specify a Port and assign it to a group name for easy use when configuring inbound and outbound policies for the firewall.



The screenshot shows a web interface for configuring a Service Group. The page title is "Configuration | Firewall | Service Group". The main content area has a light blue background and displays the message "No Entries in Service Group Database". Below this message is a table with three columns: "Service Entry Name", "TCP/UDP", and "Port #". The "TCP/UDP" column contains a dropdown menu with "TCP" selected. To the right of the "Port #" column is a button labeled "Add/Modify this entry". On the left side of the interface is a navigation menu with sections: "Main Menu (Advanced)", "BASIC", "ADMINISTRATION", "SECURITY", and "Status".

Service Entry Name	TCP/UDP	Port #
<input type="text"/>	TCP	<input type="text"/>

Service Entry Name: This is the name you assign to the group containing the port number. (The Service Entry Name can be up to 19 characters.)

TCP/UDP: This specifies whether the port goes through TCP or UDP.

Port #: This is the port number associated with the group name. Range for Port # 1-65535.

Time Window

The Time Window lets you specify certain time periods and assign them to a group name for easy use when configuring inbound and outbound policies for the firewall.

The screenshot shows a web-based configuration interface for a firewall. The page title is "Configuration | Firewall | Time Group". The main content area is light blue and contains the text "No Entries in Time Window Database". Below this text is a form with two columns: "Time Window Name" and "Time Period". The "Time Window Name" column has a text input field. The "Time Period" column has two rows of dropdown menus: "from" and "to". Each row has dropdowns for day (Monday), hour (01), minute (00), and AM/PM. To the right of the form is a button labeled "Add/Modify this entry". On the left side of the interface is a navigation menu with sections: "Main Menu (Advanced)", "BASIC", "ADMINISTRATION", "SECURITY", and "Status".

Time Window Name: This is the name you assign to the group that is given the time designation. (The Time Window Name can be up to 19 characters.)

Time Period: This field allows you to specify the time period for both start time and end time by selecting the day, hour, minute, and AM/PM.

Inbound/ Outbound Policies:

Inbound Policy

The Inbound Policy allows you to filter inbound (from the WAN into the user side LAN) packets based on a set of rules. This enables you to deny access from different sources and thus increase security.

The screenshot shows a web-based configuration interface for an Inbound Policy. The page has a blue header with the title 'Inbound Policy' and a sub-header 'No Entries in Inbound Policy Database'. Below this is a form titled '... Adding New Policy ...'. The form contains several fields: 'Src IP:' with two input boxes and a dropdown menu set to 'Any IP'; 'Dest IP:' with two input boxes and a dropdown menu set to 'Any IP'; 'Src Port:' with two input boxes and a dropdown menu set to 'Any Port'; 'Dest Port:' with two input boxes and a dropdown menu set to 'Any Port'; 'Transport Protocol:' with a dropdown menu set to 'All Protocol'; 'Filtering Action:' with a dropdown menu set to 'Allow'; and 'Time Window Filtering:' with a dropdown menu set to 'None'. At the bottom of the form is a button labeled 'Add/Modify Inbound Policy'. On the left side of the interface is a navigation menu with categories like 'BASIC', 'ADMINISTRATION', and 'SECURITY', with 'Firewall' selected under 'ADMINISTRATION'.

Src IP: This specifies the Source IP for the Inbound Policy. This is the external (WAN side, outside of the firewall) IP address or addresses and Subnet Masks that will be affected by the policy. In this field there are two IP Address entry fields and a dropdown menu has four options:

Any IP: Selecting this will cause all IPs to be affected by the policy. When this is selected, you will be unable to enter any information into the IP Address entry fields.

Single IP: Selecting this will cause only one IP Address to be affected by the policy. This IP Address will need to be specified by the user in the first IP Address entry field.

IP Range: Selecting this will enable you to select a range of IP Addresses to which the policy will apply. The first IP Address in the range must be entered into the first IP Address entry field and the last IP Address in the range must be entered into the second IP Address entry field.

Mask Range: Selecting this will enable you to select a network to which the policy will apply. The Network IP Address must be entered into the first entry field and the Subnet Mask of Network IP address must be entered into the second entry field.

Dest IP: This specifies the Destination IP for the Inbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and network that will be

affected by the policy. See Src IP above for configuration detail.

Src Port: This specifies the Source Port for the Inbound Policy. This is the external (WAN side, outside of the firewall) port(s) that will be affected by the policy. In this field, there are two port entry fields and a dropdown menu. The dropdown menu has four options:

Any Port: Selecting this will cause all Ports to be affected by the policy. When this is selected, you will be unable to enter any information into the Port entry fields.

Single Port: Selecting this will cause only one Port to be affected by the policy. This port will need to be specified by the user in the first Port entry field.

Port Range: Selecting this will enable you to select a range of Ports to which the policy will apply. The first Port in the range must be entered in the first Port entry field and the last Port in the range must be entered in the second Port entry field.

Safe Ports: Any port greater than 1024 (1025-65535) is considered a safe port.

Dest Port: This specifies the Destination Port for the Inbound Policy. This is the internal (LAN side, behind the firewall) Port that will be affected by the policy. See Src Port above for configuration detail.

Transport Protocol: This specifies the Transport/ Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP and GRE.

Filtering Action: This specifies what action the policy takes:

Allow: Selecting this will cause the policy to allow packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.

Deny: Selecting this will cause the policy to deny packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.

Time Window Filtering: This field allows you to select a certain time frame from the Time Group in which this policy will be active.

DB: Short for Database, this field allows you to select a user-defined IP Group for the Src IP and Dest IP fields and user-defined Service Group for the Dest Port. User-defined IP and Service Groups are created in IP Group and Service Group pages.

Outbound Policy

The Outbound Policy allows you to filter outbound (from the user side LAN to the WAN) packets based on a set of rules. This enables you to deny access to different sources and thus increase security.

The screenshot shows a web-based configuration interface for an Outbound Policy. The left sidebar contains a navigation menu with categories like BASIC, ADMINISTRATION, SECURITY, and Status. The main content area is titled 'Outbound Policy' and displays 'No Entries in Outbound Policy Database'. Below this is a form for adding a new policy, with fields for Source IP (Src IP), Destination IP (Dest IP), Source Port (Src Port), Destination Port (Dest Port), Transport Protocol, Filtering Action, and Time Window Filtering. A button labeled 'Add/Modify Outbound Policy' is located at the bottom of the form.

Src IP: This specifies the Source IP for the Outbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and Subnet Mask(s) that will be affected by the policy. In this field there are two IP Address entry fields and a dropdown menu has four options:

Any IP: Selecting this will cause all IPs to be affected by the policy. When this is selected, you will be unable to enter any information into the IP Address entry fields.

Single IP: Selecting this will cause only one IP Address to be affected by the policy. This IP Address will need to be specified by the user in the first IP Address entry field.

IP Range: Selecting this will enable you to select a range of IP Addresses to which the policy will apply. The first IP Address in the range must be entered into the first IP Address entry field and the last IP Address in the range must be entered into the second IP Address entry field.

Mask Range: Selecting this will enable you to select a network to which the policy will apply. The Network IP Address must be entered into the first entry field and the Subnet Mask of Network IP address must be entered into the second entry field.

Dest IP: This specifies the Destination IP for the Outbound Policy. This is the external (WAN side, outside of the firewall) IP address or addresses and network that will be affected by the policy. See Src IP above for configuration detail.

Src Port: This specifies the Source Port for the Outbound Policy. This is the internal (LAN side, behind firewall) port(s) that will be affected by the policy. In this field, there are two port entry fields and a dropdown menu. The dropdown menu has four options:

Any Port: Selecting this will cause all Ports to be affected by the policy. When this is selected, you will be unable to enter any information into the Port entry fields.

Single Port: Selecting this will cause only one Port to be affected by the policy. This port will need to be specified by the user in the first Port entry field.

Port Range: Selecting this will enable you to select a range of Ports to which the policy will apply. The first Port in the range must be entered in the first Port entry field and the last Port in the range must be entered in the second Port entry field.

Safe Ports: Any port greater than 1024 (1025-65535) is considered a safe port.

Dest Port: This specifies the Destination Port for the Outbound Policy. This is the external (WAN side, outside of the firewall) Port that will be affected by the policy. See Src Port above for configuration detail.

Transport Protocol: This specifies the Transport/ Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP and GRE.

Filtering Action: This specifies what action the policy takes:

Allow: Selecting this will cause the policy to allow packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.

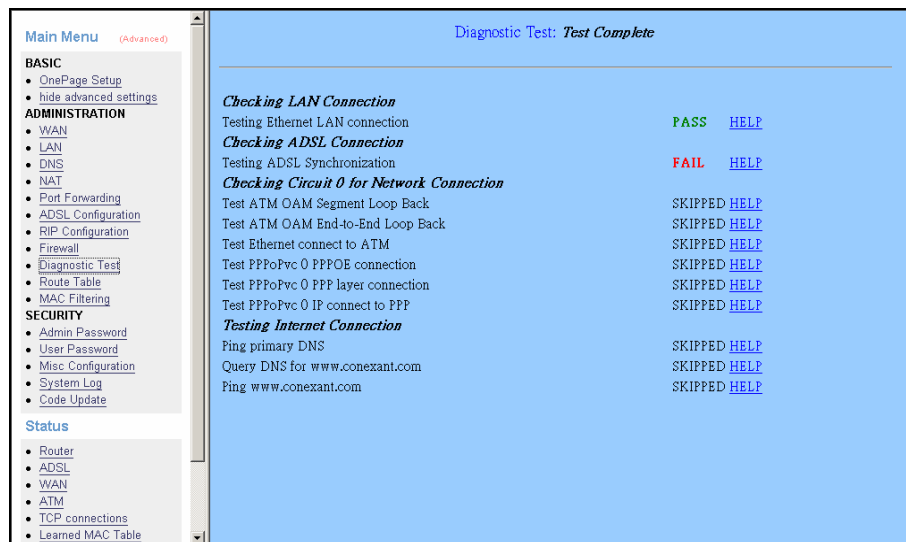
Deny: Selecting this will cause the policy to deny packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.

Time Window Filtering: This field allows you to select a certain time frame from the Time Group in which this policy will be active.

DB: Short for Database, this field allows you to select a user-defined IP Group for the Src IP and Dest IP fields and user-defined Service Group for the Dest Port. User-defined IP and Service Groups are created in IP Group and Service Group pages.

Diagnostic Test

The Diagnostic Test page shows the test results for the physical layer and protocol layer for both LAN and WAN sides.



Testing Ethernet LAN Connection: This test checks the Ethernet LAN interface connection.

Testing ADSL Synchronization: This test checks the ADSL showtime. If this test returns FAIL, all other tests will be skipped.

Test ATM OAM segment Loop Back: This test sends ATM OAM F5 Segment loop-back request cells to the CO. This test will pass if response cell is received. Some service providers might not support this test. If this test fails consistently and the ADSL modem does not seem to be working, make sure the VPI and VCI are configured correctly.

Test ATM OAM End-to-End Loop Back: This test sends ATM OAM F5 End to End loop back request cells to the CO. This test will pass if response cell is received. Some service providers might not support this test. If this test return FAIL consistently and the ADSL modem does not seem to be working, make sure the VPI and VCI are configured correctly.

Test Ethernet Connect to ATM: This test checks the ATM AAL5 module is loaded correctly.

Test PPP Layer Connection: This test checks the PPP authentication.

Test IP Connect to PPP: This test checks a valid IP address assigned from the service provider. Please note that on some ADSL services this test may fail despite the fact that you have connected correctly.

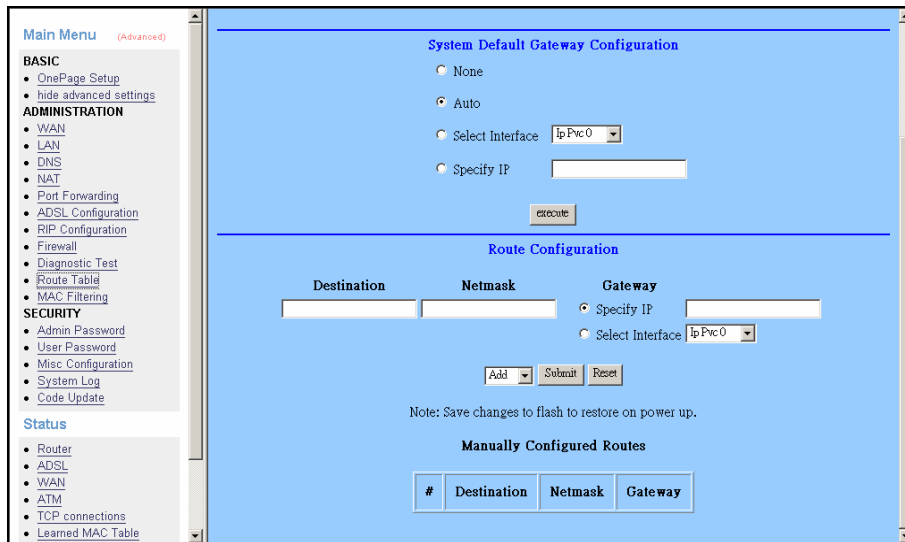
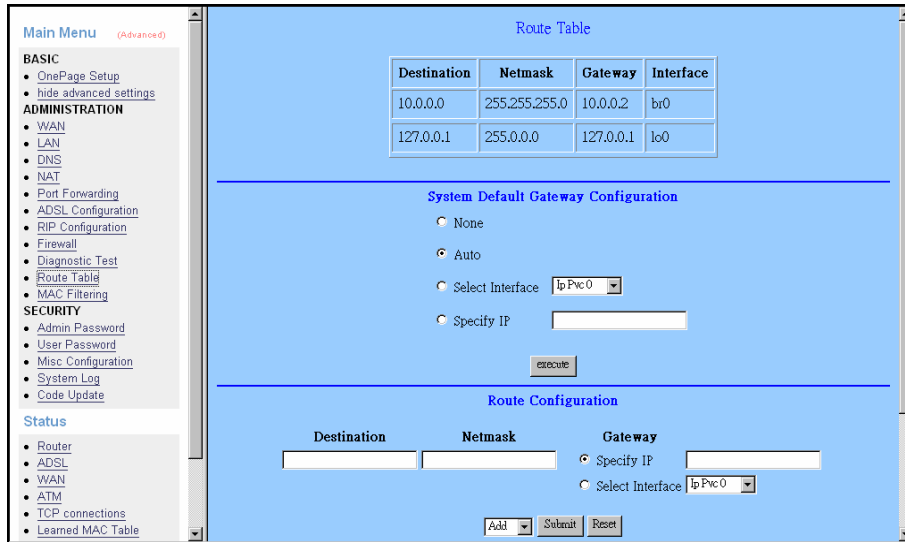
Ping Primary DNS: This test checks the primary DNS can be reached through pin request.

Query DNS for www.conexant.com: This test checks the host name can be resolved to IP address through domain name servers.

Ping www.conexant.com: This test checks the specified host can be reached through pin request.

Router Table

The Router Table page displays routing table and allows the user to manually enter the routing entry. The routing table will display the routing status of Destination, Netmask, Gateway and Interface. The interface br0 means the USB interface; lo0 means the loopback interface and ppp1 means the PPP interface. The Gateway is the learned Gateway.



Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

MAC Filtering

The MAC Filtering configuration page allows the user to set the configuration of IP filtering. Enable and Disable MAC filtering by selecting the “Yes” or “No” radio buttons.

MAC Filtering

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"/>

(1) MAC address format : aabbccddeeff, 000000000000 indicates DON'T CARE
(2) Ethernet type format: aabb, 0000 indicates DON'T CARE
(3) The maximum number of entries is 16

Source MAC: When the bridge filtering is enabled, enter the Source Mac address, Select Block and click Add. Then all incoming WAN and LAN Ethernet packets matched with this source MAC address will be filtered out. If the Forward is selected, then the packets will be forwarded to the destination PC.

Destination MAC: When the bridge filtering is enabled, enter the Destination MAC address, select Block and click Add. Then all incoming WAN and LAN Ethernet packets matched with this destination MAC address will be filtered out. If the Forward is selected, then the packets will be forwarded to the destination PC.

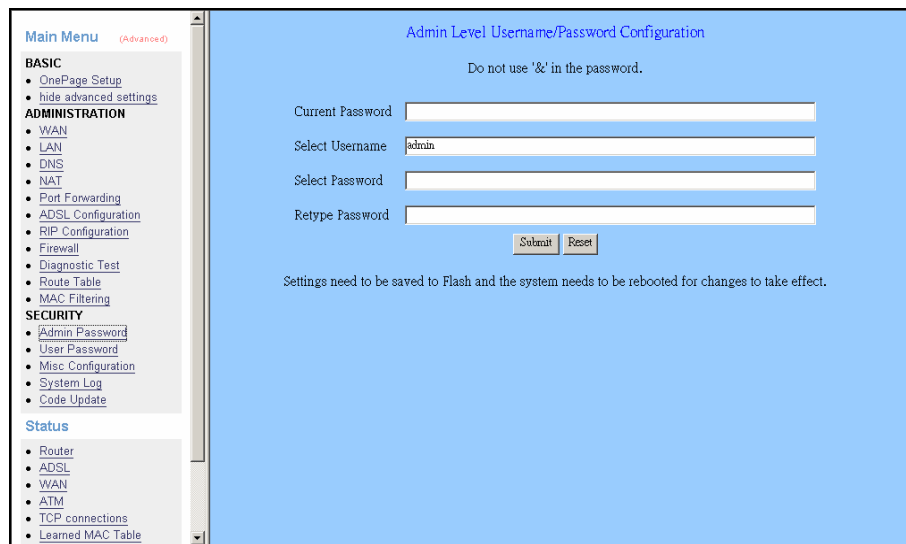
Type: Enter the hexadecimal number for the Ethernet type field in Ethernet_II packets.

Security

The links under Security are only to be accessed and configured, when it is login with administrator login name and password.

Admin Password

The Admin Password Configuration page allows the user to set the password for administrator.



The screenshot shows a web interface for configuring the administrator's password. On the left is a navigation menu with categories: BASIC, ADMINISTRATION, SECURITY, and Status. The SECURITY section is expanded, showing 'Admin Password' as the selected option. The main content area is titled 'Admin Level Username/Password Configuration' and includes a warning: 'Do not use '&' in the password.' Below this are four input fields: 'Current Password', 'Select Username' (with 'admin' entered), 'Select Password', and 'Retype Password'. At the bottom of the form are 'Submit' and 'Reset' buttons. A note at the bottom states: 'Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.'

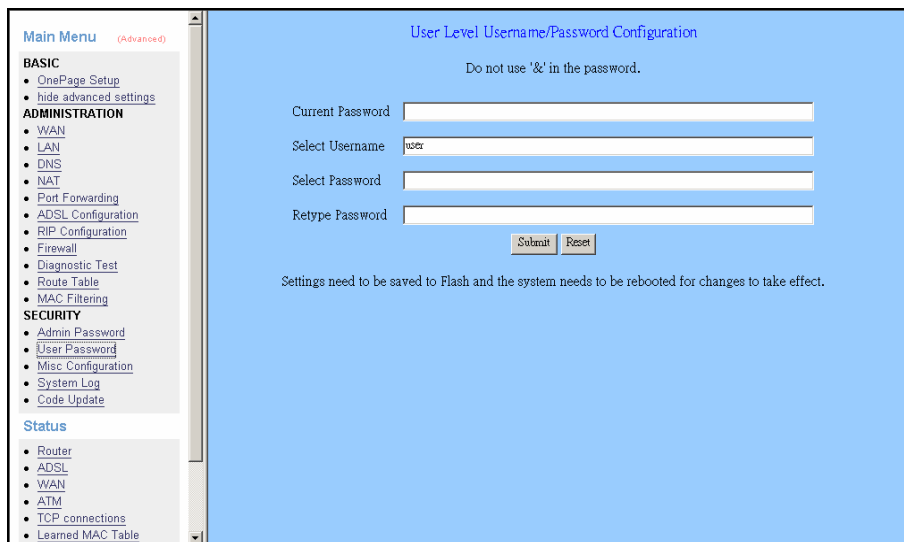
User Name: admin

Password (default): epicrouter

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

User Password

The User Password Configuration page allows the Admin user to set the password for the general user. When logged in as a general user you can view the basic status.



The screenshot shows a web interface for configuring user passwords. On the left is a 'Main Menu' sidebar with categories: BASIC (OnePage Setup, hide advanced settings), ADMINISTRATION (WAN, LAN, DNS, NAT, Port Forwarding, ADSL Configuration, RIP Configuration, Firewall, Diagnostic Test, Route Table, MAC Filtering), SECURITY (Admin Password, User Password, Misc Configuration, System Log, Code Update), and Status (Router, ADSL, WAN, ATM, TCP connections, Learned MAC Table). The main content area is titled 'User Level Username/Password Configuration' and includes a warning: 'Do not use '&' in the password.' Below this are four input fields: 'Current Password' (empty), 'Select Username' (containing 'user'), 'Select Password' (empty), and 'Retype Password' (empty). There are 'Submit' and 'Reset' buttons. A note at the bottom states: 'Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.'

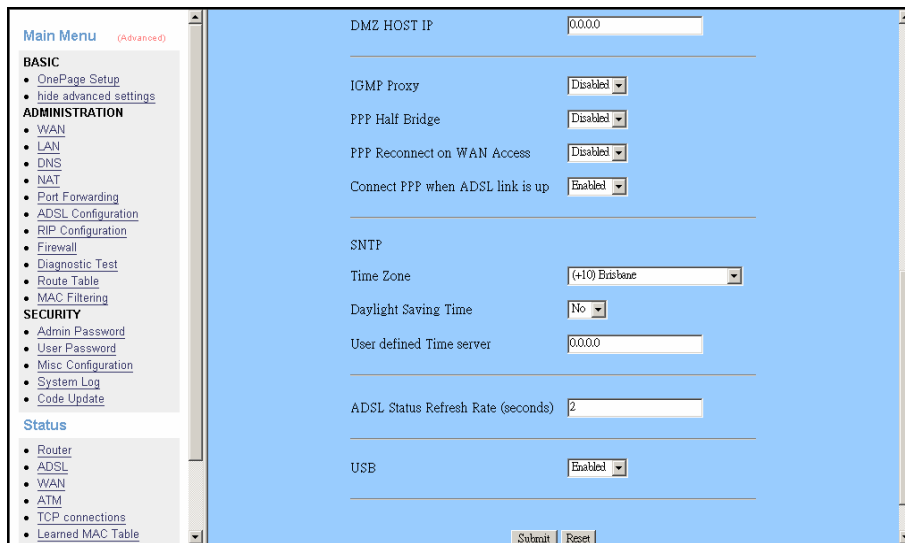
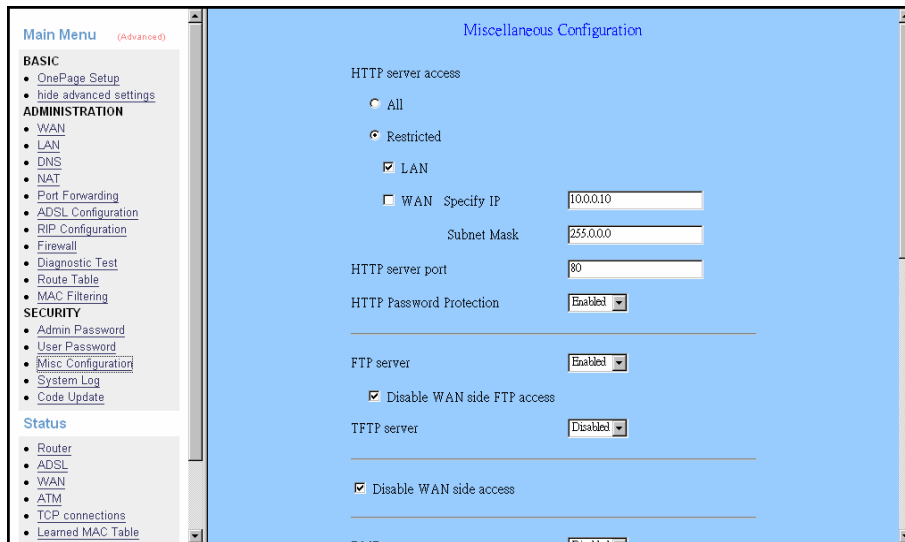
User Name: user

Password (default): password

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Misc Configuration

The Miscellaneous Configuration allows the user to set all the miscellaneous configurations.



HTTP server access: This field allows the user to configure the Web pages can be accessed from.

ALL: When this field is checked, it allows both WAN and LAN access to the Web pages.

Restricted LAN: This field allows the Web pages access from LAN side.

Restricted WAN Specified IP & Subnet Mask: This field allows the Web access from WAN side with a specify IP and Subnet Mask.

HTTP server port: This field allows the user to specify the port of the Web access.

FTP server: This field allows the user to Enable or Disable the FTP connection. If you want FTP access from the WAN side you must ensure there are no port forwards for port 21.

TFTP server: This field allows the user to Enable or Disable the TFTP connection.

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 at LAN side.

DHCP Relay: If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on the WAN side of a network. 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 Target IP: The DHCP server runs on WAN side.

IGMP Proxy: Here 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.

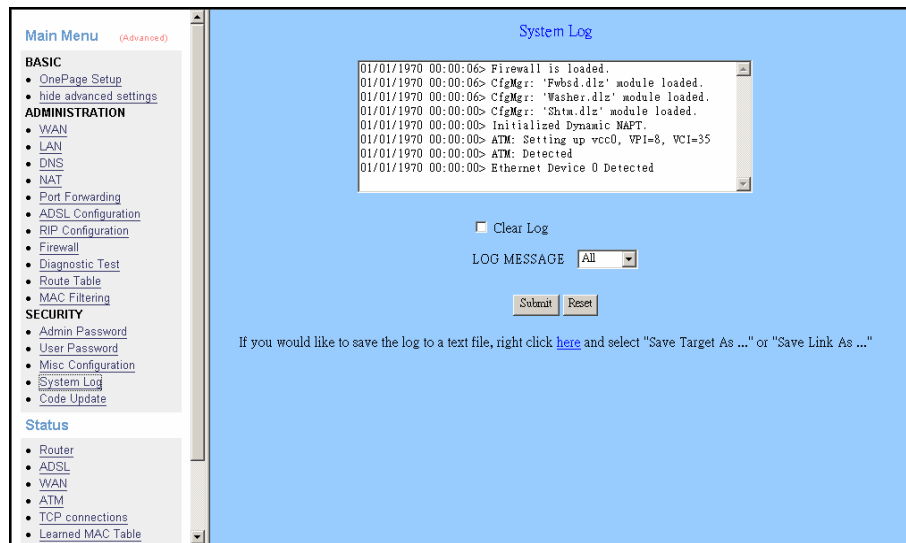
PPP connect on WAN access: If it is enabled, the PPP session will be automatically established when there is packet wants to go out the WAN.

PPP Half Bridge: When the 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. This function should only be used if one computer will be allowed to connect to the internet (E.G a Software firewall computer or Proxy server).

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

System Log

The System Log page shows the events triggered by the system.

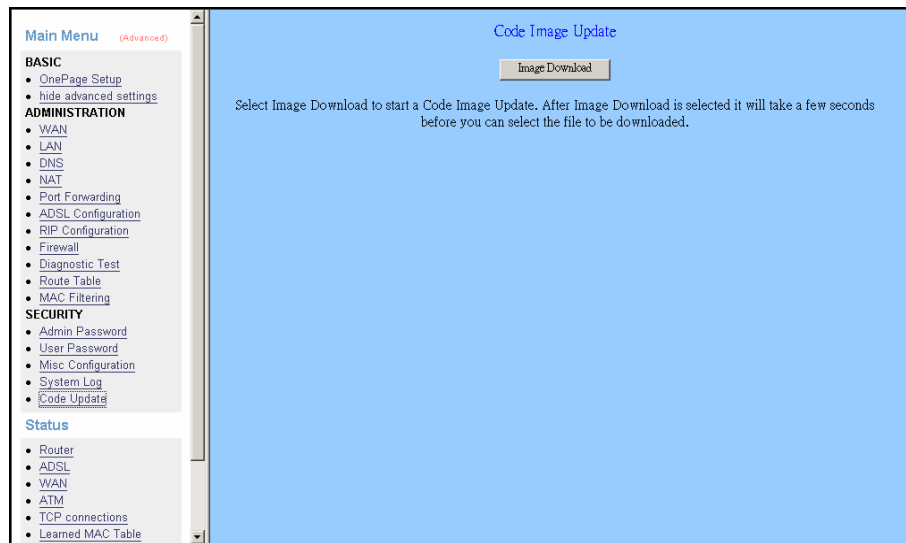


To clear the System Log simply click on the **Clear Log** button.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Code Update

The code Update page allows the user to upload new firmware to the ADSL Router.



To upload new firmware:

1. Download the latest firmware image from the website.
2. Save the file to your Desktop or other location.
3. Select the Browse button and locate the file saved in step 2.
4. Click on the Update button to start the process.
5. Once the upgrade has been completed the router will need to reboot.

Status

Router

The Home page shows the Firmware Version and WAN and LAN interface status.

The screenshot shows the router's Home Page. On the left is a navigation menu with categories: ADMINISTRATION (WAN, LAN, DNS, NAT, Port Forwarding, ADSL Configuration, RIP Configuration, Firewall, Diagnostic Test, Route Table, MAC Filtering), SECURITY (Admin Password, User Password, Misc Configuration, System Log, Code Update), and Status (Router, ADSL, WAN, ATM, TCP connections, Learned MAC Table, PPP Status). A 'Save Setting and Reboot' button is at the bottom of the menu.

The main content area is titled 'Home Page' and displays the following information:

- BootCode Version: BC_CX82xxx_4.1.0.21
- Firmware Version: CX82xxx_4.1.0.21_S
- Customer Software Version: 4.1.0.21_S

WAN

IP Address	Subnet Mask	MAC Address
------------	-------------	-------------

LAN

IP Address	Subnet Mask	MAC Address
10.0.0.2	255.255.255.0	00:09:F3:00:00:8D

Total Number of Lan Interfaces: 1

Number of ethernet devices connected to the DHCP server: 1

IP Address	MAC Address
------------	-------------

This screenshot shows the WAN and LAN interface status page. The navigation menu is identical to the previous screenshot.

The main content area is titled 'WAN' and displays the following information:

IP Address	Subnet Mask	MAC Address
------------	-------------	-------------

LAN

IP Address	Subnet Mask	MAC Address
10.0.0.2	255.255.255.0	00:09:F3:00:00:8D

Total Number of Lan Interfaces: 1

Number of ethernet devices connected to the DHCP server: 1

	IP Address	MAC Address
1	10.0.0.3	72:0B:49:E7:2B:23

Ethernet Link Status: UP

USB Link Status: DOWN

Firmware Version: This field displays the Firmware Version number.

WAN: These fields display the IP Address, Subnet Mask, MAC Address for WAN interface.

LAN: These fields display the IP Address, Subnet Mask, MAC Address for LAN interface.

Number of Ethernet devices connected to the DHCP server: This field displays the

number of DHCP clients connected to the ADSL Wireless Router. It also shows the IP address and MAC address of the attached DHCP clients.

ADSL

The ADSL Status page shows the ADSL physical layer status.

The screenshot shows a web interface for ADSL status. On the left is a navigation menu with categories like ADMINISTRATION, SECURITY, and Status. The main content area is titled 'ADSL STATUS' and contains the following text:

Showtime Firmware Version: **3.46**
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 30 minutes 22 seconds**

Below this text is a table with the following data:

	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

Showtime Firmware Version: This field displays the ADSL data pump firmware version number.

Line State: This field displays the ADSL connection process and status.

Modulation: This field displays the ADSL modulation status for G.dmt or T1.413.

Annex Mode: This field displays the ADSL Annex modes for Annex A or Annex B.

Startup Attempts: This field displays the ADSL connection attempts after loss of showtime.

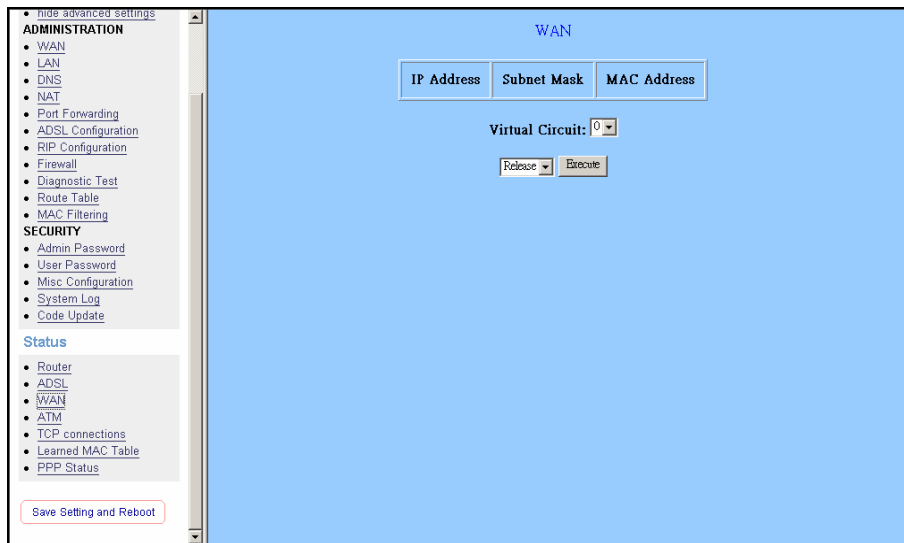
Max Tx Power: This field displays the transmit output power level of the CPE.

Co Vendor: This field displays the Central Office DSLAM vendor name. If available.

Elapsed Time: This field displays the time of the modem has been in operation.

WAN Status

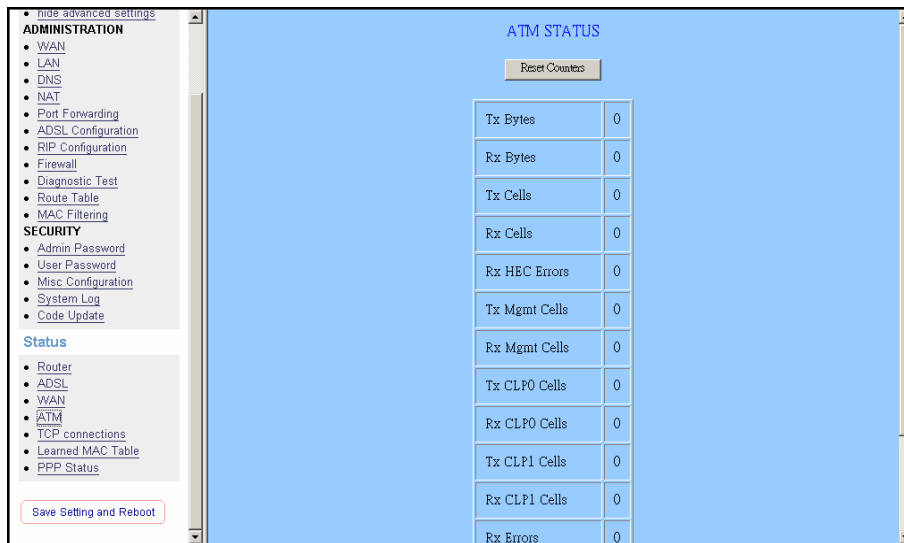
The WAN Status page shows the information and status of WAN PVCs.



WAN: These fields display the IP Address, Subnet Mask and MAC Address for the WAN (ADSL) interface. Use the Virtual Circuit selection to selection different PVC for status display.

ATM Status

The ATM Status page shows all the statistics information of ATM cells.



The screenshot shows a web interface for ATM status. On the left is a sidebar with navigation menus. The main content area is titled "ATM STATUS" and contains a "Reset Counters" button and a table of statistics.

Category	Value
Tx Bytes	0
Rx Bytes	0
Tx Cells	0
Rx Cells	0
Rx HEC Errors	0
Tx Mgmt Cells	0
Rx Mgmt Cells	0
Tx CLPO Cells	0
Rx CLPO Cells	0
Tx CLP1 Cells	0
Rx CLP1 Cells	0
Rx Errors	0

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

TCP connections

The TCP Status page shows the statistics for all TCP connections.

TCP STATUS

[Reset Counters](#)

General		
	Transmit	Receive
Total Packets	2007	1613
Data Packets	1233	244
Data Bytes	797700	107479
Out of Order Packets	N/A	242
Out of Order Bytes	N/A	0

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

Connections	
Initiated	0
Accepted	244
Established	244
Closed	214

Navigation Menu:

- OnePage Setup
- [hide advanced settings](#)
- ADMINISTRATION**
- WAN
- LAN
- DNS
- NAT
- Port Forwarding
- ADSL Configuration
- RIP Configuration
- Firewall
- [Diagnostic Test](#)
- Route Table
- MAC Filtering
- SECURITY**
- Admin Password
- User Password
- Misc Configuration
- System Log
- Code Update
- Status**
- Router
- ADSL
- WAN
- ATM
- [TCP connections](#)
- [Learned MAC Table](#)
- [PPP Status](#)

[Save Setting and Reboot](#)

Learned MAC Table

The Learned MAC Table page shows the current learned Bridge MAC table.

MAC Table

MAC Address	Expiration
00:11:2F:0F:71:5F	100

Aging Timeout: Seconds

ADMINISTRATION

- OnePage Setup
- hide advanced settings
- WAN
- LAN
- DNS
- NAT
- Port Forwarding
- ADSL Configuration
- RIP Configuration
- Firewall
- Diagnostic Test
- Route Table
- MAC Filtering

SECURITY

- Admin Password
- User Password
- Misc Configuration
- System Log
- Code Update

Status

- Router
- ADSL
- WAN
- ATM
- TCP connections
- Learned MAC Table
- PPP Status

Aging Timeout: This field allows the user to enter the update period for the MAC table.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

PPP Status

The PPP Status page shows the status of PPP for each PPP interface. See PPP.

#	Connection Name	Interface	Mode	Status	Pkts Sent	Pkts Rcvd	Bytes Sent	Bytes Rcvd
1	PPPoPvc 0	Pvc 0	PPPoE	Not Connected	N/A	N/A	N/A	N/A

If a * appears under Mode column, you need to [check the WAN configuration](#) to make sure the VC has the correct encapsulation.

Connection #:

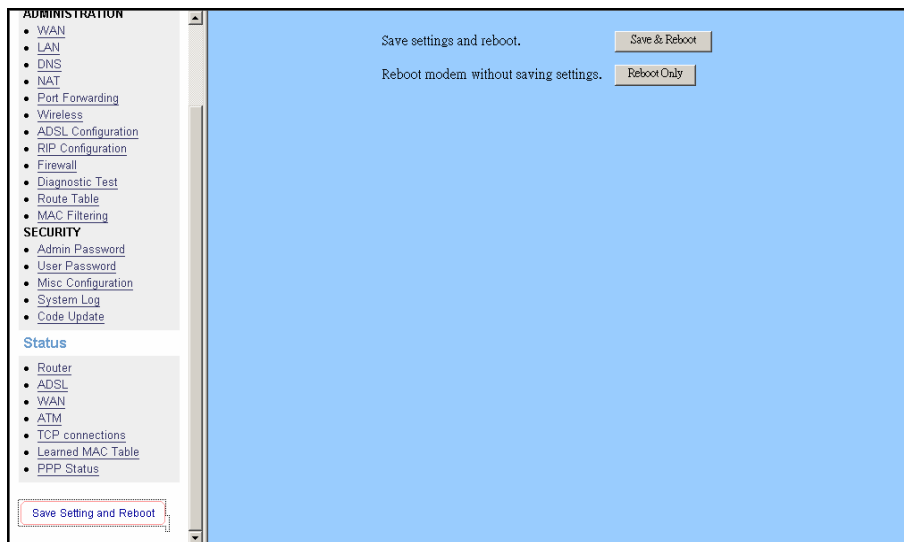
These fields display the following information on each PPP interface:

- ◆ Connection Name (user defined)
- ◆ Interface (PVC)
- ◆ Mode (PPPoE or PPPoA)
- ◆ Status (Connected or Not Connected)
- ◆ Packets Sent
- ◆ Packets Received
- ◆ Bytes Sent
- ◆ Byte Received

Connect and Disconnect: Each PPP session can be individually controlled, simply enter the desired connection number into the “Connection #” field and select either connect or disconnect from the drop down menu and click on the “Execute” button.

Save Settings/Reboot

The Save Settings/Reboot page allows users to save the new configuration to the flash and reboot the system.



When the configurations are changed via the Web pages, the settings need to be saved into the flash, so it is necessary to go to this Save Settings/Reboot page to save and reboot the system for the changes to be taken effect.

During the Save and Reboot, the following Web page will be displayed “Your setting are being saved and the modem is being rebooted. Please wait.... After the Save and Reboot, the following Web page will be displayed “Your setting have been saved and the modem has rebooted.”

The Reboot without Saving page allows the user to reboot the system without save the new configuration to the flash.

During the Reboot, the following Web page will be displayed “The modem is being rebooted. Please wait....” After the Reboot, the following Web page will be displayed “The modem has rebooted”.

Appendix

Country	ISP	PVC
Australia	All Internet providers	VPI:8
		VCI:35
Belgium		VPI:0
		VCI:33
Canada	Telus	VPI:0
		VCI:35
Danmark	Cybercity	VPI:8
		VCI:35
	Tiscali	VPI:8
		VCI:35
Deutschland	1 & 1 Internet DSL	VPI:1
		VCI:32
	AOL DSL	VPI:1
		VCI:32
	Arcor DSL	VPI:8
		VCI:35
	Freenet DSL	VPI:1
		VCI:32
	Fireline networks	VPI:1
		VCI:32
	GMX Internet	VPI:1
		VCI:32
	Hansenet	VPI:8
		VCI:35
	Netcologne	VPI:8
		VCI:35
	Schlund	VPI:1
		VCI:35
Snafu ADSL	VPI:1	
	VCI:32	

Country	ISP	PVC
	Tiscali	VPI:1
		VCI:32
	T-online	VPI:1
		VCI:32
	Anderer Anbieter	VPI:1
		VCI:32
France	Wannadoo	VPI:8
		VCI:35
	Tiscali	VPI:8
		VCI:35
ISRAEL	KPN PPPoE LLC	VPI:8
		VCI:48
Italian	Telecom Italia	VPI:8
		VCI:35
	Rest oil presente	VPI:8
		VCI:35
Netherlands	KPN PPPoA VC-MuX	VPI:8
		VCI:48
	BBeyond Bridge LLC	VPI:0
		VCI:33
	BBeyond PPPoA VC-MuX	VPI:0
		VCI:35
New Zealand	New Zealand Telecom	VPI:0
		VCI:100
Portugal	Todos os apresentador	VPI:0
		VCI:35
Spanish	Albura	VPI:1
		VCI:32
	Colt Teecom	VPI:0
		VCI:35
	Earth	VPI:8
		VCI:32

Country	ISP	PVC
Spanish	Eresmas	VPI:8
		VCI:35
	Jazztel	VPI:8
		VCI:35
	Ola Internet	VPI:8
		VCI:35
	Retevision	VPI:0
		VCI:35
	Terra	VPI:8
		VCI:32
	Tiscali	VPI:1
		VCI:32
	Telefonica	VPI:8
		VCI:32
Telepac	VPI:8	
	VCI:35	
Uni2	VPI:1	
	VCI:33	
Ya.com	VPI:8	
	VCI:32	
Wanadoo	VPI:8	
	VCI:32	
Suomi	Island ssimi	VPI:0
		VCI:35
	Landssimi	VPI:8
		VCI:48
	Vortex	VPI:8
		VCI:48
Switzerland	Alle anbieter	VPI:1
		VCI:32
Sverige	Skanova	VPI:8
		VCI:35

Country	ISP	PVC
Taiwan	Hinet	VPI:0
		VCI:33
	Seednet	VPI:0
		VCI:33
United Arab Emirates	Etisalat Classical IP Single User	VPI:8
		VCI:35
	Etisalat Classical IP for Business	VPI:8
		VCI:35
United Kingdom	British Telecom	VPI:0
		VCI:38

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>