

Ethernet USB Router

User Manual

VERSION 1.0



Contents

About this Manual	7
About the Router	8
Requirements.....	8
Software.....	8
Hardware.....	8
Package Contents	9
Device Design	10
Front Panel	10
Back Panel.....	11
Getting Started	12
Remove or Disable Conflicts	13
Internet Sharing, Proxy, and Security Applications	13
Configuring TCP/IP Settings.....	14
Configuring Internet Properties.....	14
Removing Temporary Internet Files	15
Hardware Setup	16
Ethernet Connection.....	16
USB Connection	17
About the Web Interface	19

- Accessing the Web Manager..... 19
- Components 19
 - Buttons 19
 - Commands 20
 - Menus..... 20
- Basic Menu..... 21**
- Home 22
 - Connection Information 22
 - Router Information..... 22
 - Local Network Information 22
- Quick Start 22
- LAN Configuration 23
- Diagnostics 24
 - Ping Test..... 25
 - Full Modem Test..... 25
- Advanced Menu 26**
- WAN 27
 - New Connection 27
 - Connection Scan 34
- LAN..... 35
 - LAN Configuration 35
 - LAN Group Configuration..... 37
 - Assign ISP DNS, SNTP 40
 - LAN Clients 40

Applications.....	42
Universal Plug and Play	43
Simple Network Timing Protocol	44
IGMP Proxy	46
TR-068 WAN Access	48
DNS Proxy.....	49
Dynamic DNS Client.....	50
Port Forwarding.....	51
Bridge Filters	54
Web Access Control	55
Quality of Service.....	56
Egress	57
Ingress	60
QoS Shaper Configuration	65
Policy Routing Configuration.....	69
Routing	71
Static Routing	71
Routing Table	72
System Password.....	73
Firmware Update	74
Restore to Default.....	74
Security Menu	75
IP Filters.....	76
LAN Isolation	78
Status Menu	79

Connection Status.....80

System Log81

Remote Log82

Network Statistics84

DDNS Update Status85

DHCP Clients86

QoS Status87

Modem Status88

Product Information88

Help Menu..... 89

About this Manual

This manual provides a discussion of the components, basic operation, and advanced configuration options of the router.

Scope and Purpose

This manual provides installation instructions and description of the router components and the web interface.

Target Audience

This manual is designed and developed for users who are required to operate and perform first-level maintenance of the router. It assumes the user of this manual has basic knowledge and experience in configuring routers, computer networks, and computer systems.

Document Structure

The manual is divided into the following sections:

Chapter	About
2	About the Router
3	Getting Started
4	About the Web Interface
5	Setup Menu
6	Basic Menu
7	Advanced Menu
9	Security Menu
10	Status Menu
11	Help Menu

About the Router

Congratulations on the purchase of your router. This router allows you to utilize your phone circuit to access broadband Internet without restricting you to make telephone calls.

This router is designed to connect to the Internet and to your local area network (LAN) via universal serial bus (USB) or high speed Ethernet. It has full Network Address Translation (NAT) firewall, demilitarized zone (DMZ) services, and encryption security support to block unwanted users from accessing your network. Quality of Service (QoS) and Policy routing (PR) are also supported. This router is compatible with personal computers and Apple Macs.

Requirements

Your computer must meet the following minimum requirements.

Software

Operating System:

- Windows (98 SE, Me, 2000, XP, XP x64)
- Macintosh OS 10.2
- Ethernet connections are operating system independent

Browser:

- Internet Explorer 4.0
- Netscape Navigator 3.02

Hardware

- 233MHz processor

- CD-ROM Drive
- Network adapter (Ethernet or USB)

Package Contents

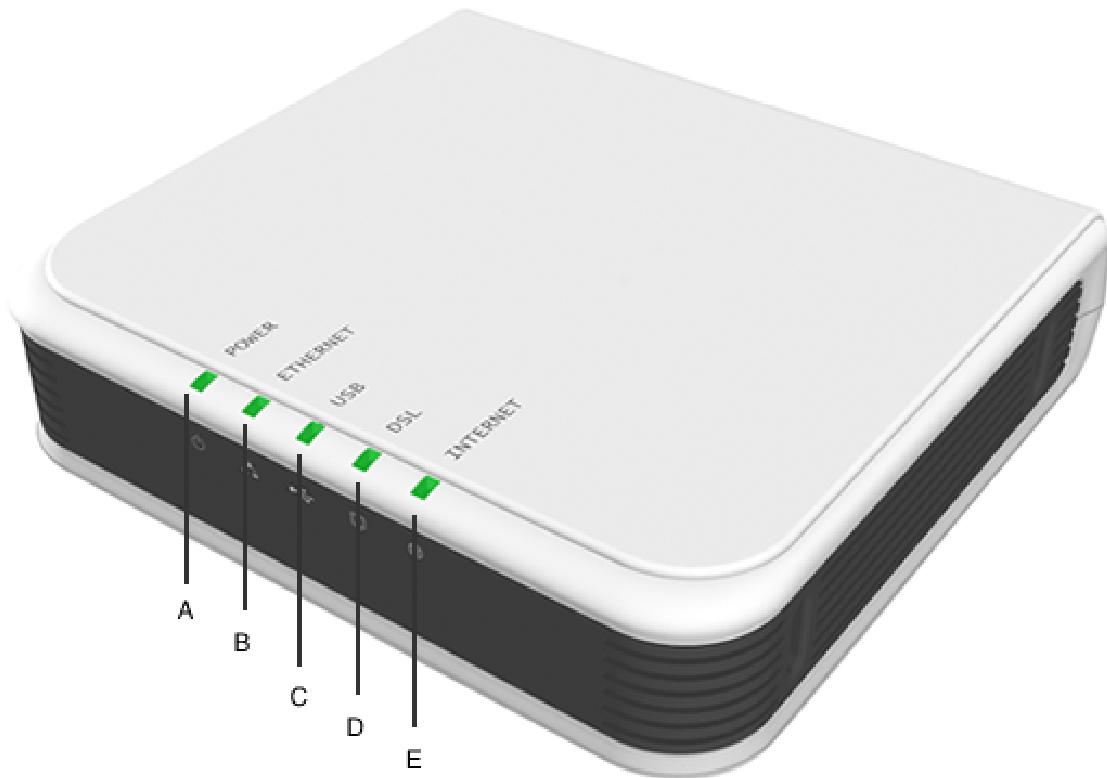
Package contents are listed below. For any missing items, please contact your dealer immediately. Product contents vary for different models.

- Router
- Ethernet cable
- Telephone cable
- USB Cable
- 9V Power Adapter
- Easy Start Guide
- Resource CD

Device Design

Front Panel

The LEDs on the front panel gives you an idea about the power and connection status.



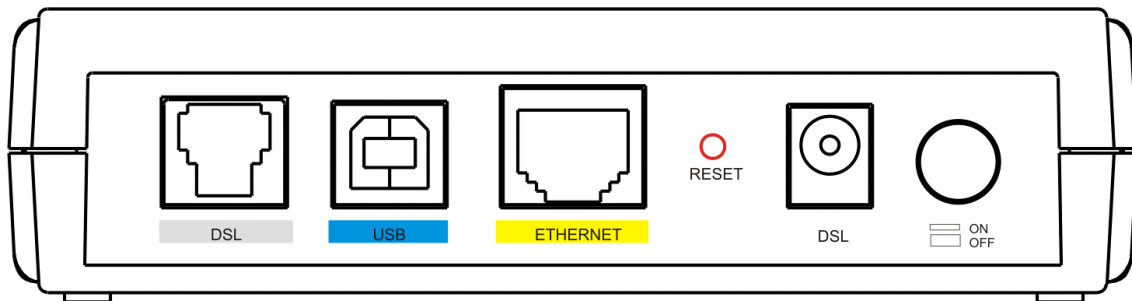
Front Panel

Label	Action	Description
POWER	Off	No power is supplied to the device
	Steady light	Connected to an AC power supply
ETHERNET	Off	No Ethernet connection
	Steady light	Connected to an Ethernet port
	Blinking light	Transmitting/Receiving data
USB	Off	No USB connection

	Steady light	Connected to a USB port
	Blinking light	Transmitting/Receiving data
DSL	Off	No DSL signal
	Blinking light	Establishing DSL signal
	Steady light	DSL signal is established
INTERNET	Off	No Internet connection
	Steady light	Connected to the Internet
	Blinking light	Transmitting/Receiving data

Back Panel

The back panel provides ports to power up and connect the router into the network.

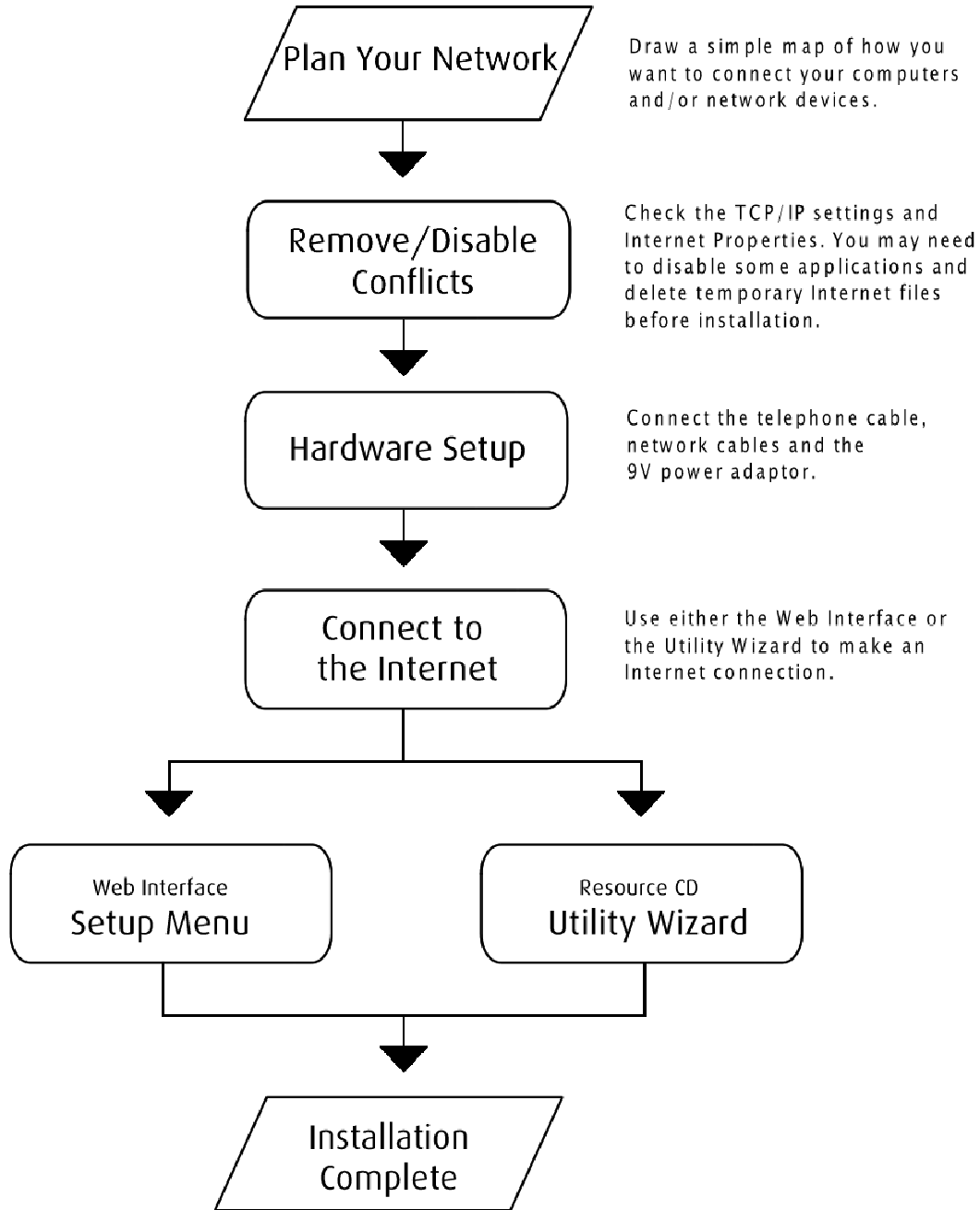


Back Panel

Label	Used for...
DSL	Connecting the telephone cable
USB	Connecting with the computer through USB cable
ETHERNET	Connecting with the computer through Ethernet cable
RESET	Resetting the device. Press for 10 seconds to reset.
9 V DC	Connecting with the 9V power adapter
ON/OFF	Switching the device on/off

Getting Started

Setting up the device is easy. The flowchart below provides an outline of the steps you need to complete the installation. There are brief descriptions beside each step to help you along. Detailed instructions are provided in the subsequent pages.



Remove or Disable Conflicts

To make sure the router installation moves on smoothly, you need to remove or disable conflicts that may interfere the installation. Probable conflicts may include:

- Internet sharing applications
- Proxy software
- Security software
- TCP/IP settings
- Internet properties
- Temporary Internet files

Internet Sharing, Proxy, and Security Applications

Internet sharing, proxy software, and firewall applications may interfere with the router installation. These should be removed or disabled before you install and configure the router.

If you have any of the following or similar applications installed on your computer, remove or disable them according to the manufacturer's instructions.

Internet Sharing Applications	Proxy Software	Security Software
Microsoft Internet Sharing	WinGate	Symantec
	WinProxy	Zone Alarm

Configuring TCP/IP Settings

Use the default TCP/IP settings to allow the router to provide a network address to the computer,

To set the TCP/IP properties:

1. Select **Start > Run**. This opens the **Run** dialog box.
2. Enter **control ncpa.cpl** and then click **OK**. This opens the **Network Connections** in your computer.
3. Right-click **LAN** and then select **Properties**. This opens the **Local Area Connection Properties** dialog box.
4. Select **Internet Protocol (TCP/IP)** and then click **Properties**. This opens the **Internet Protocol (TCP/IP)** dialog box.
5. Select **Obtain an IP address automatically**.
6. Click **OK** to close the **Internet Protocol (TCP/IP)** dialog box.
7. Click **OK** to close the **Local Area Connection Properties** dialog box.

Configuring Internet Properties

To set the Internet Properties:

1. Select **Start > Run**. This opens the **Run** dialog box.
2. Enter **control inetctl.cpl** and then click **OK**. This opens the **Internet Properties** dialog box.
3. Click **Connections** tab.
4. In the **Dial-up and Virtual Private Network settings** pane, select **Never dial a connection**.
5. Click **OK** to close the **Internet Properties** dialog box.

Removing Temporary Internet Files

Temporary Internet files are files from Web sites that are stored in your computer. Delete these files to purge the Internet cache and remove footprints left by the Web pages you visited.

To remove temporary Internet files:

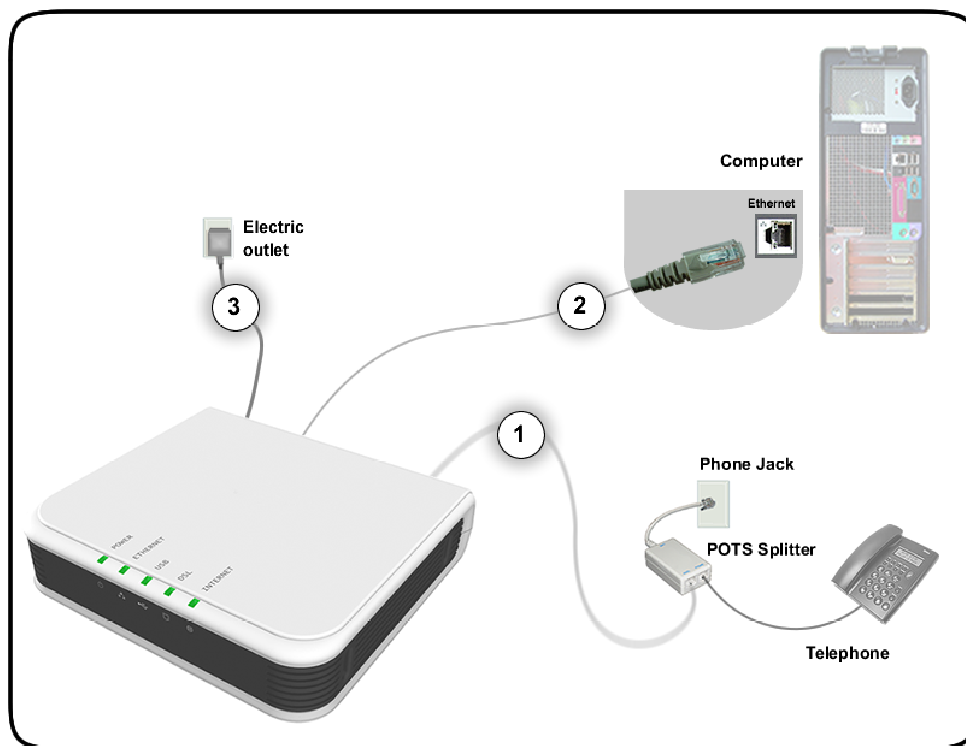
1. Select **Start > Run**. This opens the **Run** dialog box.
2. Enter **control** and then click **OK**. This opens the **Control Panel**.
3. Double-click **Internet Options**. This opens the Internet Options dialog box.
4. In the **Temporary Internet Files** pane, click **Delete Cookies**.
5. Click **Delete Files**.
6. Click **OK** to close the **Internet Properties** dialog box.

Hardware Setup

When installing the router, the common practice is to have the router, the main computer, and phone jack in the same room. The room should also have enough electrical outlets to match your needs.

Ethernet Connection

In terms of data transfer speed, the Ethernet provides the fastest mode of connection between the router and the computer.



To connect through Ethernet:

1. Plug one end of the telephone cable from the POTS Splitter's **ADSL** port and then plug the other end into the router's **DSL** port

POTS Splitter

A phone line can carry phone call and Internet signals. When you enable the phone line for high speed Internet, the connection produces high-pitched tones when using the phone. Installing a Plain Old Telephone Service (POTS) splitter separates the two

signals and eliminates the noise.

To setup the telephone POTS Splitter:

1. Locate the phone jack in your house.
2. Insert the POTS Splitter into the phone jack.
3. Plug one end of the telephone cable from the POTS Splitter's **TEL** port and then plug the other end into the telephone.

2. Plug one end of the Ethernet cable from the router's **ETHERNET** port and then plug the other end into the Ethernet port in your computer.
3. Connect the power adapter from the router's **9V DC** port into the electrical outlet and then press **ON**.

USB Connection

You can also establish an additional connection with the computer using the USB port. When using the USB, you need to install the USB driver.

To install the USB driver and connect through USB:

1. Plug one end of the USB cable from the router's **USB** port and then plug the other end into the computer's USB port.
2. Insert the **Resource CD** into your CD-ROM.
3. When the **Add Hardware Wizard** opens, follow the on-screen instructions. If asked to identify where to search for drivers, select **CD-ROM drive**.
4. Follow the on screen instructions.

For Macintosh

Unlike in Windows, Macintosh computers require that you install the USB driver first before connecting the router.

To install the USB driver for Mac:

1. Insert the **Resource CD** into your CD-ROM. This displays the CD icon on your desktop.
2. Double-click the **CD icon**. This opens a screen displaying the CD contents.
3. Double-click the **Mac** folder.
4. Double-click **USBCDCEthernetv1_2.pkg**.
5. If you set up an administrator name and password, the **Authenticate** screen opens. Enter **Name, password or phrase**, and then click OK.
6. Follow the on-screen instructions. When the installation is complete, you will be asked to restart your computer.
7. After your computer restarts, connect the USB cable from the router's **USB** port to the USB port in your computer.
8. From the dock, select **System Preferences**.
9. Under **Internet & Network**, double-click **Network**. This opens the **Network** screen.
10. From the **Show** drop-down menu, select **Ethernet Adaptor (enXX)**. This will display your IP Address and Subnet Mask as:
 - a. **IP Address** - 192.168.1.1
 - b. **Subnet Mask** - 255.255.255.0.
11. Use the web interface to configure the device settings. Please refer to Setting up Via the **Quick Start** Web Interface.

About the Web Interface

The Web Manager is used to configure the router settings.

Accessing the Web Manager

To access the Web Manager:

1. Open a browser.
2. Enter the router's IP Address. The default IP Address is **192.168.1.1**.
3. When authentication is enabled, the log in page will appear. In the login page, enter the **Username** and **Password**. The default Username and Password is admin.
4. Click **Login**.

Components

Buttons, commands, and menus make up the browser-based user interface.

Buttons

Apply

Click to implement the configuration changes. Clicking Apply will not implement the changes when the router is restarted.

Cancel

Click to revert to the last saved configuration.

Commands

Save Setting

Click to permanently apply configuration changes.

Restart Router

Restarts the router

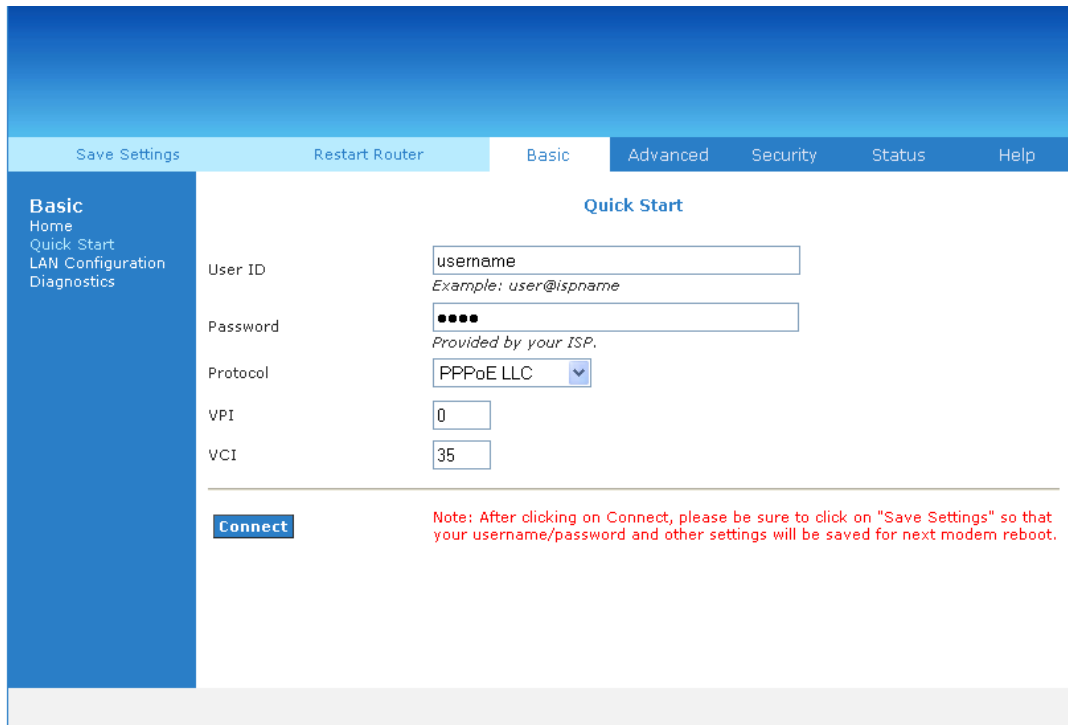
Menus

There are five menus in the web interface. These include:

- Basic Menu
- Advanced Menu
- Security Menu
- Status Menu
- Help Menu

Basic Menu

The Basic Menu provides the Home, Quick Start, LAN Configuration, and Diagnostics links.



The screenshot shows the 'Basic Menu' configuration interface. At the top, there is a navigation bar with buttons for 'Save Settings', 'Restart Router', 'Basic', 'Advanced', 'Security', 'Status', and 'Help'. The 'Basic' menu is selected, and a sidebar on the left lists 'Basic', 'Home', 'Quick Start', 'LAN Configuration', and 'Diagnostics'. The main content area is titled 'Quick Start' and contains the following fields:

- User ID:** A text input field containing 'username'. Below it, an example is provided: 'Example: user@ispname'.
- Password:** A text input field with four black dots. Below it, a note says 'Provided by your ISP.'
- Protocol:** A dropdown menu currently set to 'PPPoE LLC'.
- VPI:** A text input field containing '0'.
- VCI:** A text input field containing '35'.

At the bottom left of the form is a blue 'Connect' button. To its right, a red note reads: 'Note: After clicking on Connect, please be sure to click on "Save Settings" so that your username/password and other settings will be saved for next modem reboot.'

Basic Menu

Home

The Home page provides a one-page summary about the Connection Information, Router Information, and Local Network settings.

Connection Information

The Connection Information pane gives you an idea about the status of your Internet connection. This pane includes a Connect/Disconnect button. When clicked, the router makes an attempt to connect to the Internet using the parameters saved in the router.

Router Information

This pane provides all the necessary information to determine the model, firmware version, build, Ethernet MAC Address, NAT status, and Firewall status.

Local Network Information

The Local Network pane displays the current IP address of the router. It also provides the DHCP status, DHCP Range, and Ethernet status.

Quick Start

Quick Start gives you the ability to instantly connect to the Internet.

LAN Configuration

LAN Group Configuration allows you to configure settings for each LAN group. Notice that you can also view the status of advanced services that can be applied to a LAN group. Green indicates that the service is enabled, while red indicates that the service is disabled.

The screenshot displays the 'LAN Group 1 Configuration' window. It is divided into two main sections: 'IP Settings' and 'Services Status'.

IP Settings:

- Unmanaged
- Obtain an IP address automatically
 - IP Address:
 - Netmask:
- PPP IP Address
 - IP Address:
- Use the following Static IP address
 - IP Address:
 - Netmask:
 - Default Gateway:
 - Host Name:
 - Domain:
- Enable DHCP Server
 - Assign ISP DNS, SNTP
 - Start IP:
 - End IP:
 - Lease Time: Seconds
- Enable DHCP Relay
 - Relay IP:
- Server and Relay Off

Services Status:

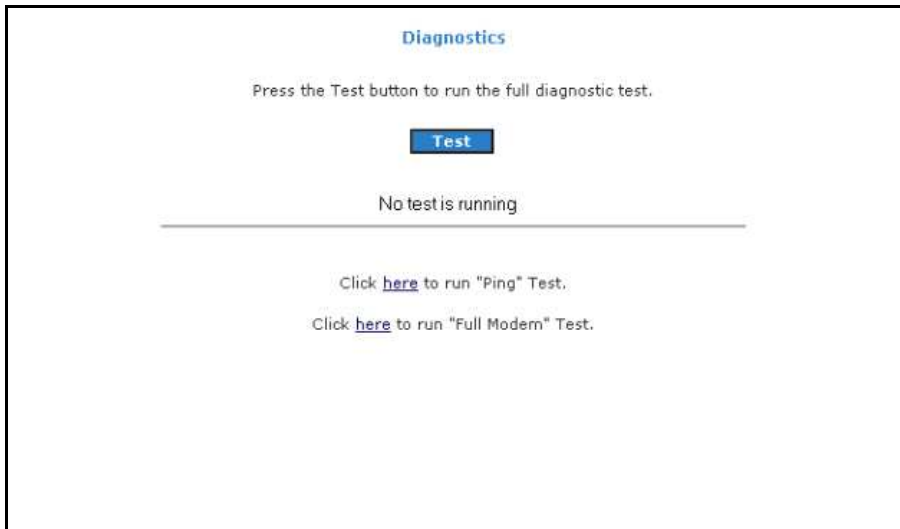
- IP Filters:
- Bridge Filters:
- UPnP:
- LAN Clients:
- Static Routing:

At the bottom right of the configuration window are two buttons: and .

LAN Group Configuration

Diagnostics

Diagnostic Test is used for investigating whether the router is properly connected to the WAN Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button. Before running this test, make sure you have a valid DSL link.



To run diagnostic test:

1. Select the **Basic Menu** and then click **Diagnostics**. This opens the **Diagnostics** page.
2. Click **Test**. The test status will appear after running the diagnostic test. If a test failed, click **Help** to get the solution.

Ping Test

Once you have your router configured, it is a good idea to make sure you can ping the network. If you can ping an IP on the WAN side successfully, you should be able to surf the Internet.

To perform a ping test:

1. Select the **Basic Menu** and then click **Diagnostics**.
2. Click **Ping Test**. This opens the **Ping Test** page.
3. Change or leave the default settings of the following fields:
 - Enter the IP address to ping
 - Packet size
 - Number of echo request
4. Click **Test**.

The ping results are displayed in the page. If the ping test was successful, it means that the TCP/IP protocol is up and running. If the Ping test failed, you should restart the router.

Full Modem Test

This test is used to check if your modem is properly connected to the network.

To perform a Full Modem test:

1. Select the **Basic Menu** and then click **Diagnostics**.
2. Click **Full Modem Test**. This opens the **Modem Test** page.

Select your connection and then click **Test**.

Advanced Menu

The Advanced mode provides advanced configuration settings for existing connections. At least one WAN connection must be configured before implementing advanced WAN configuration features. At least one LAN group must be defined before implementing advanced LAN configuration features.

The Advanced section lets you configure advanced features like LAN Configuration, SNTP, IGMP, Bridge(MAC) Filters, LAN clients, etc.

Lan Configuration	Allows changes to be made to IP addresses and option to enable DHCP server.
LAN Clients	Allows user to join specified LAN groups.
SNTP	Short for Simple Network Time Protocol, a simplified version of NTP. Allows the user to be synchronized with a specified time server.
Port Forwarding	Configure Firewall and NAT pass-through to your hosted applications.
Bridge Filter	Allows user to enable / disable bridge filters to destination ports.
LAN Clients	Configure LAN Clients.
Easy Connect Configuration	Allow user to access Internet without changes to PC Network Settings
Bridge Filters	Select to setup Bridge Filters.
IGMP Proxy	Configure Multicast pass-through for different connections.
Web Access Control	Configure access control list for remote Web access.
Policy Routing	Configure Policy Routing information.
Ingress	Configure Ingress information.
Egress	Configure Egress information.
Shaper	Configure Shaper information.
Routing	Consists of static .

Advanced Menu

WAN

Wide Area Network (WAN) is the source of your Internet connection.

New Connection

Your router can support up to eight different connections. If you have multiple virtual connections, you may need to utilize the static routing capabilities of the modem to pass data correctly.

There are five types of WAN connections:

- PPPoE Connection
- PPPoA Connection
- Static Connection
- DHCP Connection
- Bridge Connection

Before you make a new WAN connection, you should make sure you have an existing Internet connection.

PPPoE Connection

PPP, or point-to-point protocol, is a method of establishing a network connection/session between network hosts. PPPoE is a protocol for encapsulating PPP frames in Ethernet frames and is described in RFC 2516. PPPoE provides the ability to connect to a network of hosts over a simple bridging access device to a remote access concentrator. With this model, each router uses its own PPP stack. Access control, billing, and type of service control can all be done on a per-user rather than per-site basis.

The screenshot shows the 'PPPoE Connection Setup' window. At the top, there are fields for 'Name', 'Type' (set to 'PPPoE'), and 'Sharing' (set to 'Disable'). Below these are 'Options' with checkboxes for 'NAT' and 'Firewall', and 'VLAN ID' (set to 0) and 'Priority Bits' (set to 0). The window is divided into two main sections: 'PPP Settings' and 'PVC Settings'. 'PPP Settings' includes 'Encapsulation' (radio buttons for 'LLC' and 'VC', with 'LLC' selected), 'Username' (text field with 'username'), 'Password' (text field with asterisks), 'Idle Timeout' (60 secs), 'Keep Alive' (10 min), 'Authentication' (radio buttons for 'Auto', 'CHAP', and 'PAP', with 'Auto' selected), 'MTU' (1492 bytes), 'On Demand' (checkbox), 'Enforce MTU' (checkbox), 'PPP Unnumbered' (checkbox), 'Host Trigger' (checkbox), 'Default Gateway' (checkbox), 'Debug' (checkbox), and 'Valid Rx' (checkbox). 'PVC Settings' includes 'PVC' (dropdown menu with 'New'), 'VPI' (0), 'VCI' (0), 'QoS' (dropdown menu with 'UBR'), 'PCR' (0 cps), 'SCR' (0 cps), 'MBS' (0 cells), 'CDVT' (0 usecs), and 'Auto PVC' (checkbox). At the bottom, there are buttons for 'Configure', 'Connect', 'Disconnect', 'Apply', 'Delete', and 'Cancel'.

New PPPoE Connection Setup

PPPoA Connection

PPPoA is also known as RFC 2364. It is a method of encapsulating PPP packets in ATM cells that are carried over the DSL line. PPP, or point-to-point protocol, is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users. Logical link control (LLC) and virtual circuit (VC) are two different methods of encapsulating the PPP packet. Contact your service provider to determine which encapsulation is being used on your Internet connection.

PPPoA Connection Setup

Name: Type: Sharing:

Options: NAT Firewall VLAN ID: Priority Bits:

PPP Settings

Encapsulation: LLC VC

Username:

Password:

Idle Timeout: secs

Keep Alive: min

Authentication: Auto CHAP PAP

MTU: bytes

On Demand: Default Gateway:

Debug:

PPP Unnumbered: Valid Rx:

Host Trigger: **Configure**

PVC Settings

PVC:

VPI:

VCI:

QoS:

PCR: cps

SCR: cps

MBS: cells

CDVT: usecs

Auto PVC:

Connect **Disconnect**

Apply **Delete** **Cancel**

New PPPoA Connection Setup

Static Connection

Static connection type is used whenever a known static IP address is assigned to the router. Additional addressing information such as the subnet mask and the default gateway must also be specified. Up to three Domain Name Server (DNS) addresses can be identified. These servers resolve the name of the computer to the IP address mapped to it and thus enable you to access other web servers by typing the symbolic name (host name).

The screenshot shows the 'Static Connection Setup' dialog box. At the top, there is a title bar 'Static Connection Setup'. Below it, there are several input fields and checkboxes. The 'Name' field is empty. The 'Type' dropdown is set to 'Static'. The 'Sharing' dropdown is set to 'Disable'. There are two checked checkboxes for 'Options': 'NAT' and 'Firewall'. The 'VLAN ID' field is set to '0'. The 'Priority Bits' dropdown is set to '0'. Below these are two sections: 'Static Settings' and 'PVC Settings'. 'Static Settings' includes 'Encapsulation' with 'LLC' selected and 'VC' unselected, 'IP Address' set to '0.0.0.0', 'Mask' (empty), 'Default Gateway' (empty), 'DNS 1', 'DNS 2', and 'DNS 3' (all empty), and 'Mode' with 'Bridged' selected and 'Routed' unselected. 'PVC Settings' includes 'PVC' dropdown set to 'New', 'VPI' (0), 'VCI' (0), 'QoS' dropdown set to 'UBR', 'PCR' (0) cps, 'SCR' (0) cps, 'MBS' (0) cells, 'CDVT' (0) usecs, and 'Auto PVC' checkbox (unchecked). At the bottom right, there are three buttons: 'Apply', 'Delete', and 'Cancel'.

New Static Connection Setup

DHCP Connection

DHCP allows the router to automatically obtain the IP address from the server. This option is commonly used in when the IP is dynamically assigned and is not known prior to assignment.

The screenshot shows the 'DHCP Connection Setup' window. At the top, the title is 'DHCP Connection Setup'. Below the title, there are several fields: 'Name:' with an empty text box, 'Type:' with a dropdown menu set to 'DHCP', and 'Sharing:' with a dropdown menu set to 'Disable'. Below these are 'Options:' with checkboxes for 'NAT' and 'Firewall' (both checked), 'VLAN ID:' with a text box containing '0', and 'Priority Bits:' with a dropdown menu set to '0'. The window is divided into two main sections: 'DHCP Settings' and 'PVC Settings'. Under 'DHCP Settings', there is 'Encapsulation:' with radio buttons for 'LLC' (selected) and 'VC', 'IP Address:', 'Mask:', 'Gateway:', and 'Default Gateway:' with an unchecked checkbox. Below these are 'Renew' and 'Release' buttons. Under 'PVC Settings', there is 'PVC:' with a dropdown menu set to 'New', 'VPI:' with a text box containing '0', 'VCI:' with a text box containing '0', 'QoS:' with a dropdown menu set to 'UBR', 'PCR:' with a text box containing '0' and 'cps' next to it, 'SCR:' with a text box containing '0' and 'cps' next to it, 'MBS:' with a text box containing '0' and 'cells' next to it, 'CDVT:' with a text box containing '0' and 'usecs' next to it, and 'Auto PVC:' with an unchecked checkbox. At the bottom right of the window are 'Apply', 'Delete', and 'Cancel' buttons.

New DHCP Connection Setup

Bridged Connection Setup

A pure bridged connection does not assign any IP address to the WAN interface. NAT and firewall rules are not enabled. This connection method makes the router act as a bridge for passing packets between the WAN interface and the LAN interface.

Bridged Connection Setup

Name: Type: **Bridge** Sharing: **Disable**

Options: VLAN ID: Priority Bits:

Bridge Settings

Encapsulation: LLC VC

Select LAN: **LAN group 1**

PVC Settings

PVC: **New**

VPI:

VCI:

QoS: **UBR**

PCR: cps

SCR: cps

MBS: cells

CDVT: usecs

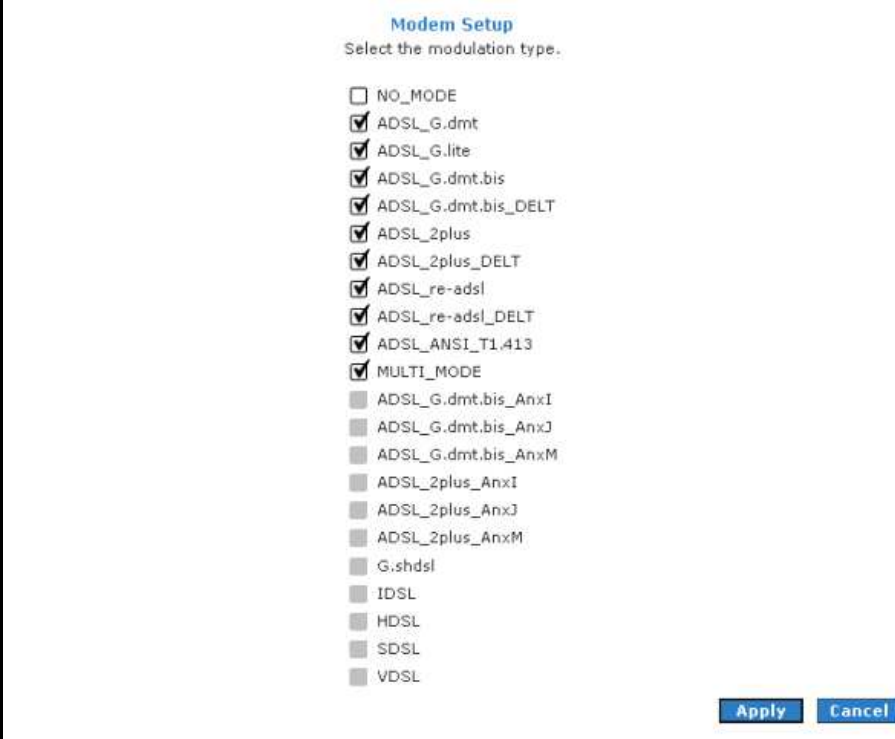
Auto PVC:

Apply **Delete** **Cancel**

New Bridge Connection Setup

ADSL Modulation

ADSL Modulation allows you to select any combination of DSL training modes. Leave the default value if you are unsure or the service provider did not provide this information. In most cases, this screen should not be modified.



The screenshot shows a dialog box titled "Modem Setup" with the instruction "Select the modulation type." Below this, there is a list of modulation options, each with a checkbox. The checked options are: NO_MODE, ADSL_G.dmt, ADSL_G.lite, ADSL_G.dmt.bis, ADSL_G.dmt.bis_DELT, ADSL_2plus, ADSL_2plus_DELT, ADSL_re-adsl, ADSL_re-adsl_DELT, ADSL_ANSI_T1.413, and MULTI_MODE. The unchecked options are: ADSL_G.dmt.bis_AnXI, ADSL_G.dmt.bis_AnXJ, ADSL_G.dmt.bis_AnXM, ADSL_2plus_AnXI, ADSL_2plus_AnXJ, ADSL_2plus_AnXM, G.shdsl, IDSL, HDSL, SDSL, and VDSL. At the bottom right of the dialog box, there are two buttons: "Apply" and "Cancel".

Modulation Type	Selected
NO_MODE	Yes
ADSL_G.dmt	Yes
ADSL_G.lite	Yes
ADSL_G.dmt.bis	Yes
ADSL_G.dmt.bis_DELT	Yes
ADSL_2plus	Yes
ADSL_2plus_DELT	Yes
ADSL_re-adsl	Yes
ADSL_re-adsl_DELT	Yes
ADSL_ANSI_T1.413	Yes
MULTI_MODE	Yes
ADSL_G.dmt.bis_AnXI	No
ADSL_G.dmt.bis_AnXJ	No
ADSL_G.dmt.bis_AnXM	No
ADSL_2plus_AnXI	No
ADSL_2plus_AnXJ	No
ADSL_2plus_AnXM	No
G.shdsl	No
IDSL	No
HDSL	No
SDSL	No
VDSL	No

ADSL Modulation

Connection Scan

This feature helps users to detect the PVC settings provided by the service provider. Before the router can begin scanning the connection, the telephone line has to be plugged into the router.



Connection Scan

To perform connections scan:

1. Select the **Advanced Menu**.
2. Select **WAN > Connection Scan**.
3. Click **Scan**.

LAN

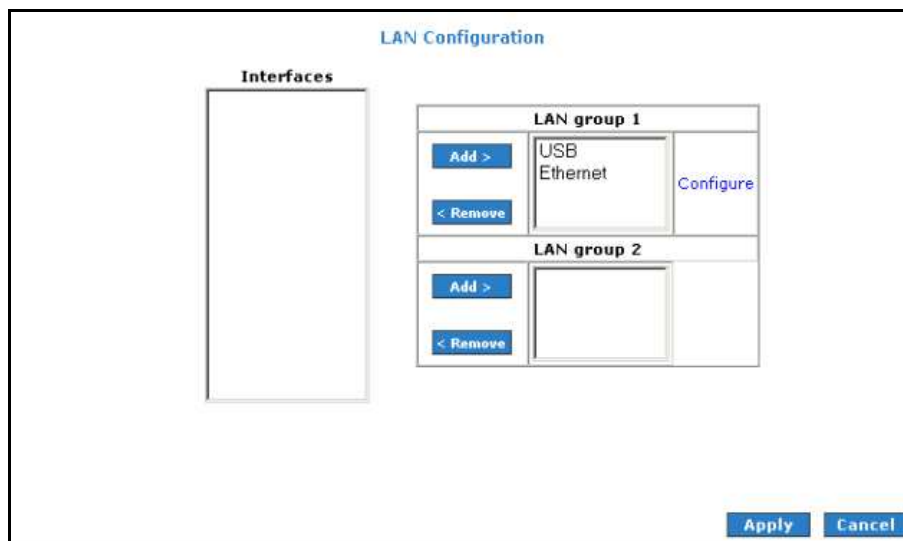
The router is preconfigured to automatically provide IP addresses to all the computers in the Local Area Network (LAN). Your router allows you to create and configure LAN groups.

LAN Configuration

The router can support up to two LAN groups through different physical interfaces. These interfaces include:

- Ethernet
- USB

You can use other LAN interfaces to a group except for the Ethernet interface, which is assigned to LAN group 1. Each LAN group can then be configured with static IP address, dynamic IP address, or be unmanaged (no IP).



LAN Configuration

To configure the LAN groupings:

1. Select the **Advanced Menu**.
2. Select **LAN > LAN Configuration**.
3. Select **USB** in **LAN group 1** and then click **< Remove**. No packets will be sent to the USB interface because it does not belong to any LAN group.
4. Select **USB** from **Interfaces** and then click **Add >** under **LAN group 2**. Just like in LAN group 1, **Configure** will appear in **LAN group 2** to allow the definition of additional configurations.
5. To temporarily activate the settings, click **Apply**.
6. To make changes permanent, click **Save Settings**.

Note: You can configure the USB interface to a different LAN group except for the Ethernet interface, which cannot be moved from LAN group 1.

LAN Group Configuration

LAN Group Configuration allows you to configure settings for each LAN group. Notice that you can also view the status of advanced services that can be applied to a LAN group. Green indicates that the service is enabled, while red indicates that the service is disabled.

LAN Group Configuration

Category	Field	Description
Unmanaged		Unmanaged is a state when the LAN group is not configured and no IP address has been assigned to the bridge.
Obtain an IP address automatically		When this function is enabled, your router acts like a client and requests an IP address from the DHCP server on the LAN side.
	IP Address	You can retrieve/renew an IP address from the DHCP server using the Release and Renew buttons.
	Netmask	The subnet mask of your router.

PPP IP Address		Enables/disables PPP unnumbered feature.
	IP Address	The IP address should be different but within the same subnet as the WAN-side IP address.
Use the following Static IP address		This field enables you to change the IP address of the router.
	IP Address	The default IP address of the router (as shown) is 192.168.1.1.
	Netmask	The default subnet mask of your router is 255.255.255.0. This subnet allows the router to support 254 users. If you want to support a larger number of users you can change the subnet mask.
	Default Gateway	The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP provides you with the IP address of the default gateway.
	Host Name	The host name is used in conjunction with the domain name to uniquely identify the router. It can be any alphanumeric word that does not contain spaces.
	Domain	The domain name is used in conjunction with the host name to uniquely identify the router. To access the web pages of the router you can type 192.168.1.1 (the IP address) or mygateway1.ar7 (Host Name.Domain).
Enable DHCP Server		Enables/disables DHCP. By default, your router has the DHCP server (LAN side) enabled. If you already have a DHCP server running on your network, you must disable one of the two DHCP servers.
	Assign ISP DNS, SNTP	Enable/disables the Assign ISP DNS, SNTP feature when the DHCP server of your router has been enabled. To learn more, please refer to Assign ISP DNS, SNTP .
	Start IP	The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the IP address value of the router. For example, if the IP address of the router is 192.168.1.1 (default), then the starting IP address must be 192.168.1.2 (or higher). Note: If you change the start or end values, make sure the values are still within the same subnet as the router. In other words, if the IP address of the router is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.168.1.2/192.168.1.100, you cannot communicate

		with the router if your host has DHCP enabled.
	End IP	<p>The End IP Address is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 254; hence the max value for the default gateway is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users do not get access to network resources. If this happens, you can increase the Ending IP address (to the limit of 254) or reduce the lease time.</p> <p>Note: If you change the start or end values, make sure the values are still within the same subnet as the IP address of the router. In other words, if the IP address of the router is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.168.1.2/192.168.1.100, you cannot communicate with the router if your host has DHCP enabled.</p>
	Lease Time	<p>The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the router using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or the DHCP server issues a new IP. The amount of time is in units of seconds. The default value is 3600 seconds (1 hour). The maximum value is 999999 seconds (About 278 hours).</p>
Enable DHCP Relay		<p>In addition to the DHCP server feature, the router supports the DHCP relay function. When the router is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the gateway is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiated between the DHCP clients and the server.</p>
	Relay IP	The IP address of the DHCP relay server.
Server and Relay Off		<p>When the DHCP server and relay functions are turned off, the network administrator must carefully configure the IP address, Subnet Mask, and DNS settings of every host on your network. Do not assign the same IP address to more than one host. Also, your router must reside on the same subnet as all the other hosts.</p>

Assign ISP DNS, SNTP

When you enable the DHCP server, the router dynamically assigns IP addresses to computers in the local network. The router provides its own LAN IP address (192.168.1.1) as both the gateway and the DNS server.

The router has a choice of advertising its own IP address (192.168.1.1) as the DNS server or providing the DNS that was received from the WAN. This can be configured by enabling/disabling **Assign ISP DNS SNTP** on the **LAN Group Configuration** page.

Note: ISP DNS, SNTP only applies when the DHCP server is enabled on the LAN Group Configuration page.

LAN Clients

LAN Clients allows you to view and add computers in a LAN group. Each computer either has a dynamic or static (manually-configured) IP address.

You can add a static IP address (belonging to the router's LAN subnet) using the LAN Clients page. Any existing static entry falling within the DHCP server's range can be deleted.

LAN Clients

To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address:

Hostname:

MAC Address:

Dynamic Addresses

Reserve	IP Address	Hostname	MAC	Type
<input type="checkbox"/>	192.168.1.2	PhushHongWen	00:10:b5:6d:e5:13	Dynamic

Apply Cancel

LAN Clients

To add LAN Clients:

1. Select **Advanced Menu**.
2. Select **LAN > LAN Clients**. This opens the **LAN Clients** page.
3. Select a **LAN Connection**, and enter **IP Address**, **Hostname**, and **MAC Address**.
4. Click **Apply**.
5. You can convert the dynamic into a static entry by clicking **Reserve**, and then click **Apply**.
6. To temporarily implement the settings, click **Apply**.
7. To make changes permanent, click **Save Settings**.

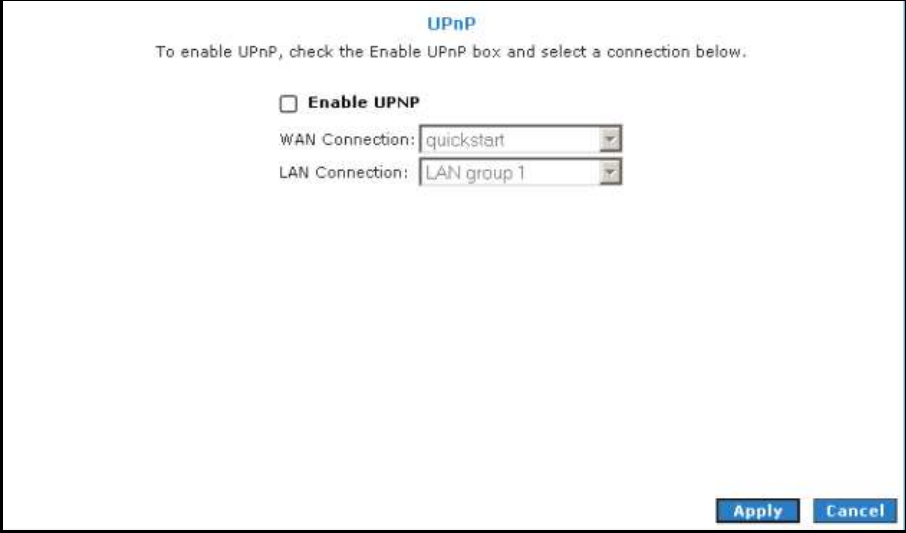
Applications

Applications include:

- Universal Plug and Play (UPnP)
- Simple Network Timing Protocol (SNTP)
- Internet Group Management Protocol (IGMP) Proxy
- TR-068 WAN Access
- DNS Proxy
- Dynamic DNS Client
- Port Forwarding
- Bridge Filters
- Web Access Control

Universal Plug and Play

Universal plug and play (UPnP), NAT, and firewall traversal allow traffic to pass through the router for applications using the UPnP protocol. This feature requires one active WAN connection. In addition, the computer should support this feature. In the presence of multiple WAN connections, select a connection on which the incoming traffic is present, for example, the default WAN connection.



UPnP

To enable UPnP, check the Enable UPnP box and select a connection below.

Enable UPnP

WAN Connection: quickstart

LAN Connection: LAN group 1

Apply **Cancel**

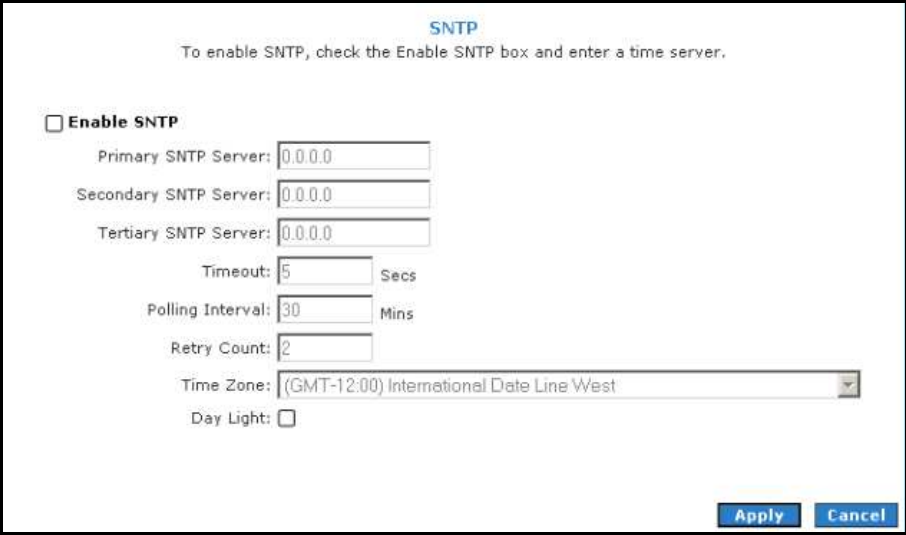
UPnP

To configure UPnP:

1. Select **Advanced**.
2. Select **Application > UPnP**.
3. Select the **WAN Connection** and **LAN Connection** that will use UPnP from the drop-down lists.
4. Click **Apply** to temporarily apply the settings.
5. To make changes permanent, click **Save Settings**.

Simple Network Timing Protocol

Simple network timing protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP servers. It uses the UDP protocol on port 123 to communicate between clients and servers.



The image shows a configuration window titled "SNTP". At the top, it says "To enable SNTP, check the Enable SNTP box and enter a time server." Below this, there is a checkbox labeled "Enable SNTP". Underneath the checkbox are several input fields: "Primary SNTP Server:" with the value "0.0.0.0", "Secondary SNTP Server:" with "0.0.0.0", and "Tertiary SNTP Server:" with "0.0.0.0". There are also fields for "Timeout:" (5) with the unit "Secs", "Polling Interval:" (30) with the unit "Mins", and "Retry Count:" (2). A "Time Zone:" dropdown menu is set to "(GMT-12:00) International Date Line West". At the bottom, there is a "Day Light:" checkbox which is unchecked. "Apply" and "Cancel" buttons are located at the bottom right of the window.

SNTP

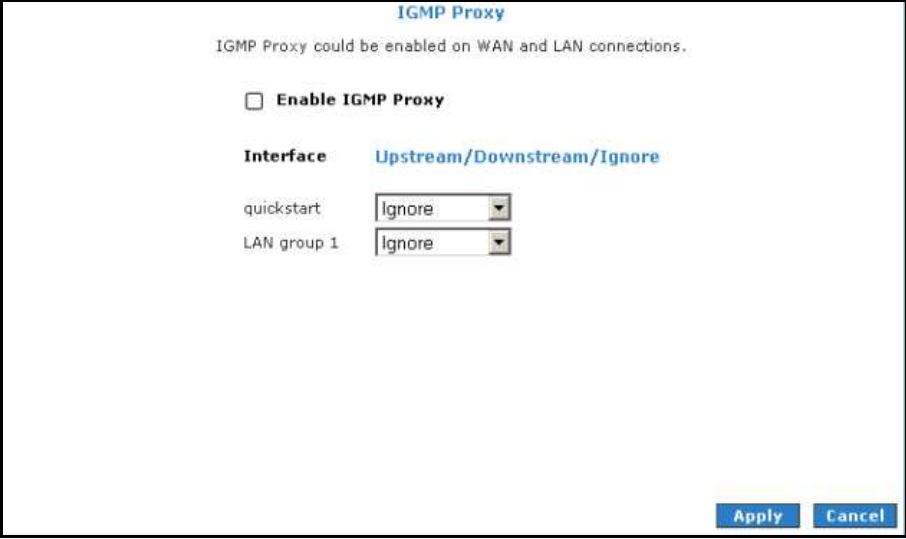
To enable SNTP:

1. Check **Enable SNTP**.
2. Configure the following fields:
 - **Primary SNTP Server** The IP address or the host name of the primary SNTP server. This can be provided by ISP or defined by user.
 - **Secondary SNTP Server** The IP address or the host name of the secondary SNTP server. This can be provided by ISP or defined by user.
 - **Tertiary SNTP Server** The IP address or the host name of the tertiary SNTP server. This can be provided by ISP or defined by user.
 - **Timeout** If the router failed to connect to an SNTP server within the Timeout period, it retries the connection.

- **Polling Interval** The amount of time between a successful connection with a SNTP server and a new attempt to connect to an SNTP server.
 - **Retry Count** The number of times the router tries to connect to an SNTP server before it tries to connect to the next server in line.
 - **Time Zone** The time zone in which the router resides.
 - **Day Light** Select this option to enable/disable daylight saving time (DST). DST is not automatically enabled or disabled. You need to manually enable and disable it.
3. Click **Apply** to temporarily apply the settings.
 4. To make changes permanent, click **Save Settings**.

IGMP Proxy

IP hosts use Internet group management protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. Your router supports IGMP proxy that handles IGMP messages. When enabled, your router acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast groups on the WAN side.



The screenshot shows the 'IGMP Proxy' configuration window. At the top, it says 'IGMP Proxy could be enabled on WAN and LAN connections.' Below this is a checkbox labeled 'Enable IGMP Proxy' which is currently unchecked. Underneath is an 'Interface' dropdown menu set to 'Upstream/Downstream/Ignore'. There are two more dropdown menus: 'quickstart' and 'LAN group 1', both set to 'Ignore'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

IGMP Proxy

Multicasting is a form of limited broadcast. UDP is used to send datagrams to all hosts that belong to what is called a Host Group. A host group is a set of one or more hosts identified by a single IP destination address. The following statements apply to host groups:

- Anyone can join or leave a host group at will.
- There are no restrictions on a host's location.
- There are no restrictions on the number of members that may belong to a host group.
- A host may belong to multiple host groups.

- Non-group members may send UDP datagrams to the host group.

Multicasting is useful when the same data needs to be sent to more than one device. For instance, if one device is responsible for acquiring data that many other devices need, then multicasting is a natural fit. Note that using multicasting as opposed to sending the same data to individual devices uses less network bandwidth. The multicast feature also enables you to receive multicast video streams from multicast servers.

The IGMP Proxy page allows you to enable multicast on available WAN and LAN connections. You can configure the WAN or LAN interface as one of the following:

- **Upstream** The interface that IGMP requests from hosts are sent to the multicast router.
- **Downstream** The interface data from the multicast router are sent to hosts in the multicast group database.
- **Ignore** No IGMP request nor data multicast are forwarded.

You can perform one of the two options:

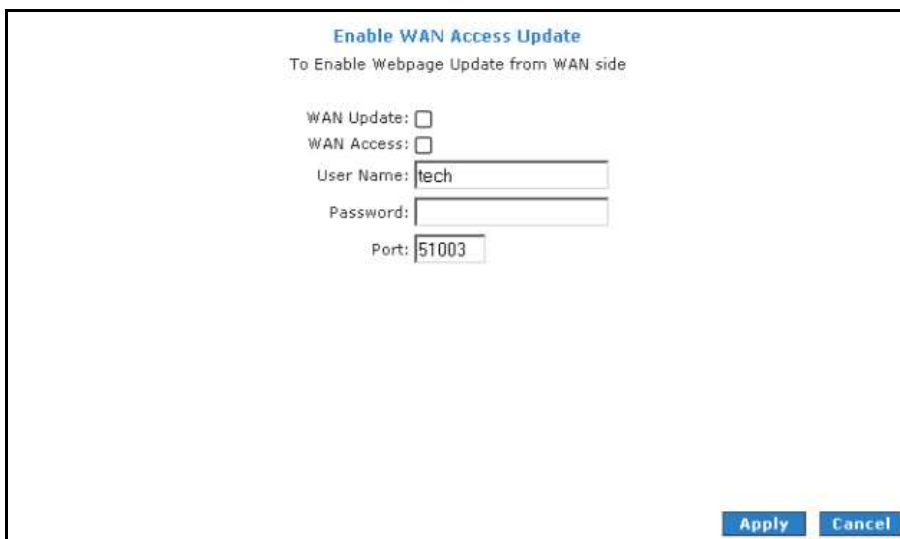
1. Configure one or more WAN interface as the upstream interface.
2. Configure one or more LAN interface as the upstream interface.

To configure the IGMP Proxy:

1. Select **Advanced**.
2. Select **Application > IGMP Proxy**.
3. Configure the following interfaces:
 - Quickstart
 - LAN group 1
4. Click **Apply** to temporarily apply the settings.
5. To make changes permanent, click **Save Settings**.

TR-068 WAN Access

The TR-068 WAN Access page enables you to give temporary permission to someone (such as technical support staff) to be able to access your router from the WAN side. From the moment the account is enabled the user is expected to log in within 20 minutes, otherwise the account expires. Once the user has logged in, if the session remains inactive for more than 20 minutes, the user will be logged out and the account expires.



Enable WAN Access Update
To Enable Webpage Update from WAN side

WAN Update:
WAN Access:
User Name:
Password:
Port:

Enable WAN Access Update

To create a temporary user account for remote access:

1. Select the **Advanced Menu**.
2. Select **Application > TR-068 WAN Access**.
3. Select **WAN Update**.
4. Select **WAN Access**.
5. Enter a user name and password in the **User Name** and **Password** fields.
6. Enter a port number In the Port field (for example, 51003).

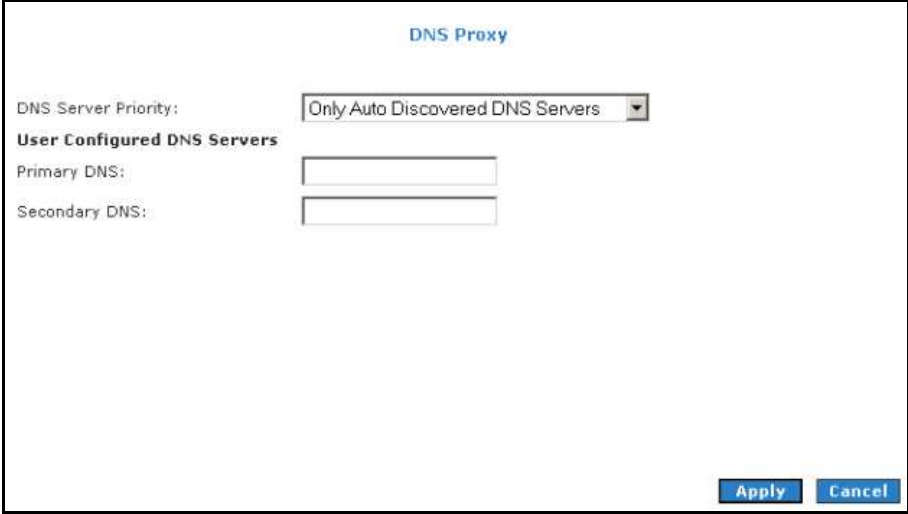
To access your router remotely, enter the following URL:

- `http(s)://10.10.10.5:51003`

- **Syntax:** http(s)://WAN IP of router:Port Number
7. Click **Apply** to temporarily apply the settings.
 8. To make changes permanent, click **Save Settings**.

DNS Proxy

This feature allows the user to select the Domain Name Server (DNS) Server Priority as well as enter IP addresses for primary DNS and secondary DNS.



The screenshot shows a configuration window titled "DNS Proxy". At the top, there is a dropdown menu labeled "DNS Server Priority" with the selected option being "Only Auto Discovered DNS Servers". Below this, there is a section titled "User Configured DNS Servers" which contains two text input fields: "Primary DNS:" and "Secondary DNS:". At the bottom right of the window, there are two buttons: "Apply" and "Cancel".

DNS Proxy

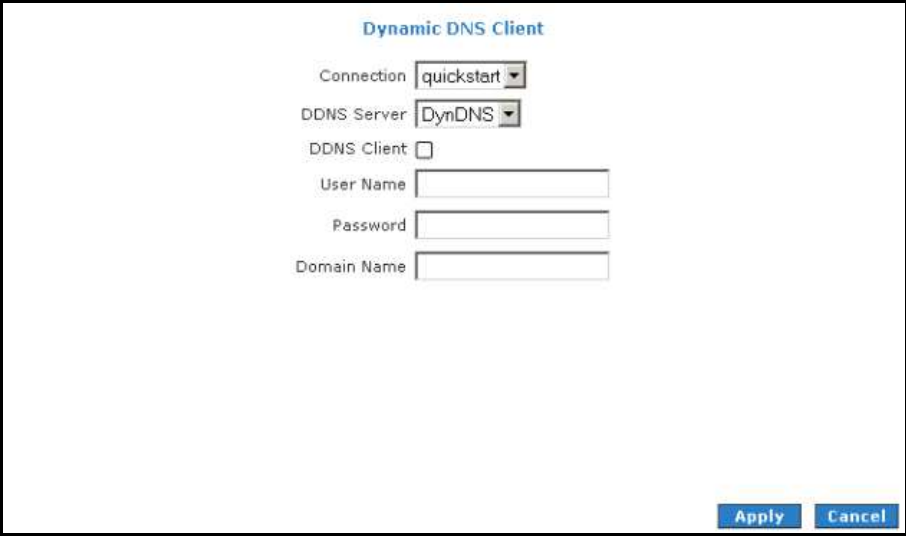
To select the DNS Server Priority:

1. Select **Advanced**.
2. Select **Application > DNS Proxy**.
3. Select the DNS Server Priority.
 - Only Auto Discovered DNS Servers
 - Only User Configured DNS Servers
 - Auto Discovered then User Configured
 - User Configured then Auto Discovered

4. Click **Apply** to temporarily apply settings.
5. To make changes permanent, click **Save Settings**.

Dynamic DNS Client

Dynamic DNS allows the user to register with a Dynamic DNS Provider. The Dynamic DNS will be linked with the WAN IP of the router even after the ISP update the WAN IP to another IP address. It can be useful in web hosting and FTP services.



The screenshot shows a configuration window titled "Dynamic DNS Client". It contains the following fields and controls:

- Connection: A dropdown menu with "quickstart" selected.
- DDNS Server: A dropdown menu with "DynDNS" selected.
- DDNS Client: An unchecked checkbox.
- User Name: A text input field.
- Password: A text input field.
- Domain Name: A text input field.
- At the bottom right, there are two buttons: "Apply" and "Cancel".

Dynamic DNS Client

Note: The User Name/Password entered should be similar to the User Name/Password you have specified during the registration of the DNS hostname.

To enable Dynamic DNS:

1. Select **Advanced**.
2. Select **Application > Dynamic DNS Client**.
3. Configure the following fields:
 - Connection
 - DDNS Server
 - DDNS Client

- User Name
 - Password
 - Domain Name
4. Click **Apply** to temporarily apply the settings.
 5. To make changes permanent, click Save **Settings**.

Port Forwarding

Port forwarding (or virtual server) allows you to direct incoming traffic to specific LAN hosts based on a protocol port number and protocol. Using the Port Forwarding page, you can provide local services (for example, web hosting) for people on the Internet or play Internet games. Port forwarding is configurable per LAN group.

Port Forwarding

A database of predefined port forwarding rules allows you to apply one or more rules to one or more members of a defined LAN group. You can view the rules associated with a predefined category and add the available rules for a given category. You can also create, edit, or delete your own port forwarding rules.

To configure port forwarding:

1. Select **Advanced**.
2. Select **Application > Port Forwarding**.
3. Select **WAN Connection**, **LAN Group**, and **LAN IP**. If the desired LAN IP is not available in the **LAN IP** drop-down menu, you can add it using the **LAN Client page**, which is accessed by clicking **New IP**.
4. Select the available rules for a given category and click **Add** to apply the rule for this category. If a rule is not in the list, you can create your own rule in the **User** category. Select **User**, and then click **New**.
5. The Rule Management page opens for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End**, and **Port Map**, and then click **Apply**.
6. Continue to add rules as they apply from each category.
7. Click **Apply** to temporarily activate the settings.
8. To make changes permanent, click **Save Settings**.

DMZ Settings

Setting a host on your local network as demilitarized zone (DMZ) forwards any network traffic that is not redirected to another host via the Port Forwarding feature to the IP address of the host. This opens the access to the DMZ host from the Internet. This function is disabled by default. By enabling DMZ, you add an extra layer of security protection for hosts behind the firewall.

To enable DMZ Settings:

1. On the **Port Forwarding** page, select **Enable DMZ**. This opens the DMZ Settings page.
2. Select the **WAN Connection**, **LAN Group**, and **LAN IP Address**.
3. Click **Apply** to temporarily apply the settings.
4. To make changes permanent, click **Save Settings**.

Custom Port Forwarding

The Custom Port Forwarding page allows you to create up to 15 custom Port Forwarding entries to support specific services or applications, such as concurrent NAT/NAPT operation.

Bridge Filters

The Bridge Filters allows you to enable, add, edit, or delete the filter rules. When bridge filtering is enabled, each frame is examined against every defined filter rule in sequence. When a match is found, the appropriate filtering action (allow or deny) is performed. Up to 20 filter rules are supported with bridge filtering.

Bridge Filters

Enable Bridge Filters
 Enable Bridge Filter Management Interface

Select LAN: LAN group 1
 Bridge Filter Management Interface: Ethernet

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Add

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete

Apply **Cancel**

Bridge Filters

To configure Bridge Filters:

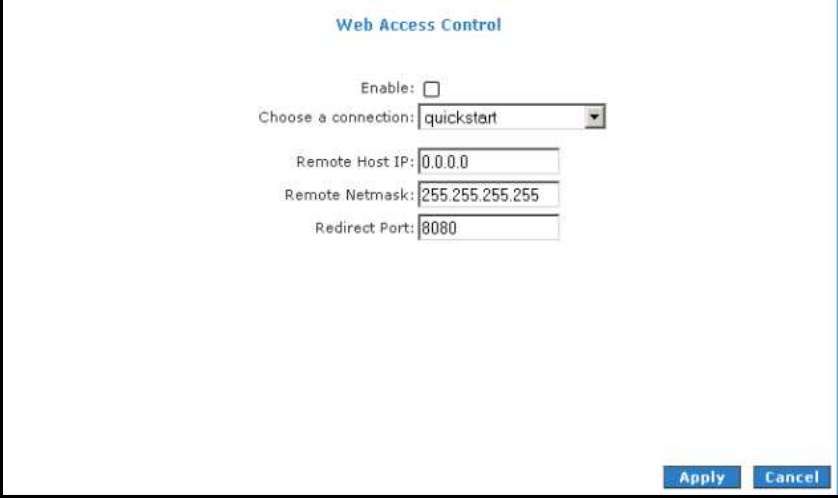
1. Select **Advanced**.
2. Select **Application > Bridge Filters**. This opens the Bridge Filters page.
3. Select **Enable Bridge Filters**.
4. To add a rule, enter the source **MAC address**, **Destination MAC addresses**, and **Protocol** with desired filtering type, then click **Add**.

Note: You can also edit a rule that you created using the **Edit** checkbox. You can delete using **Delete**.

5. Click **Apply** to temporarily activate the settings.
6. To make changes permanent, click **Save Settings**.

Web Access Control

The Web Access Control page allows you to access the router via the web from a remote location like your home or office.



Web Access Control

To configure Web Access:

1. Select **Advanced Menu**.
2. Select **Application > Web Access Control**.
3. Select **Enable**.
4. Select the connection used to connect to the Internet in the **Choose a connection**.
5. Configure the following fields:
 - Remote Host IP
 - Remote Netmask
 - Redirect Port
6. Click **Apply** to temporarily activate the settings on the page. The WAN address is now added into the IP Access List. This allows you to access your router remotely.
7. To make changes permanent, click **Save Settings**.

Quality of Service

Quality of service allows network administrators to configure the routers to meet the real time requirements for voice and video.

Different networks use different QoS markings like:

- ToS network: ToS bits in the IP header
- VLAN network: priority bits in the VLAN header
- DSCP network: uses only 5 bits of the CoS
- WLAN: WLAN QoS header.

The QoS framework is supported on all the above domains. How do you make them talk to each other? How can you make sure the priority from one network is carried over to another network? Class of service (CoS) is introduced as the common language for the QoS mappings. When QoS is enabled, the router has full control over packets from the time they enter the router till they leave the router. This is how it works: The domain mapping (ToS bits, priority bits, etc.) of a packet needs to be translated to CoS when the packet enter the router, and vice versa, the CoS of a packet needs to be translated back to the domain mapping when the packet leaves the router.

There are some additional terms you should get familiarize with:

- Ingress: Packets arriving into the router from a WAN/LAN interface.
- Egress: Packets sent from the router to a WAN/LAN interface.
- Trusted mode: Honors the domain mapping (ToS byte, WME, WLAN user priority).
- Untrusted mode: Does not honor domain mapping. This is the default QoS setting.
- Traffic Conditioning Agreement (TCA): The TCA needs to be defined for each interface:
 - Ingress mappings (Domain =>CoS)

- Egress Mappings (CoS => Domain)
- Untrusted mode (default)
- Shaper

Egress

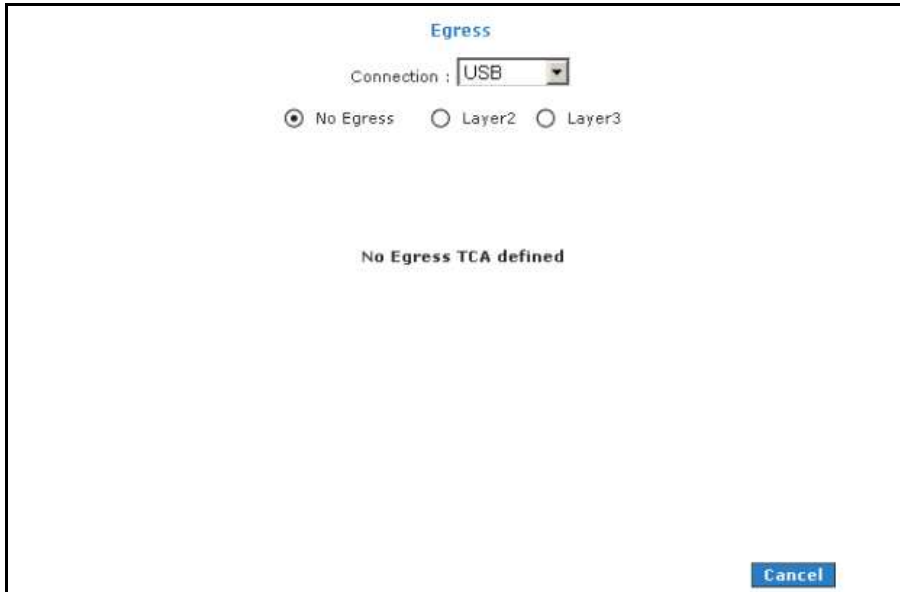
For packets going out of the router, the markings (CoS) need to be translated to the mappings understood by the network domains. The reverse CoS and domain mapping is configured using the Egress. To access **Egress**, select the **Advanced Menu** and then select **QoS > Egress**.

There are three Egress modes:

- No Egress mode
- Layer 2
- Layer 3

No Egress Mode

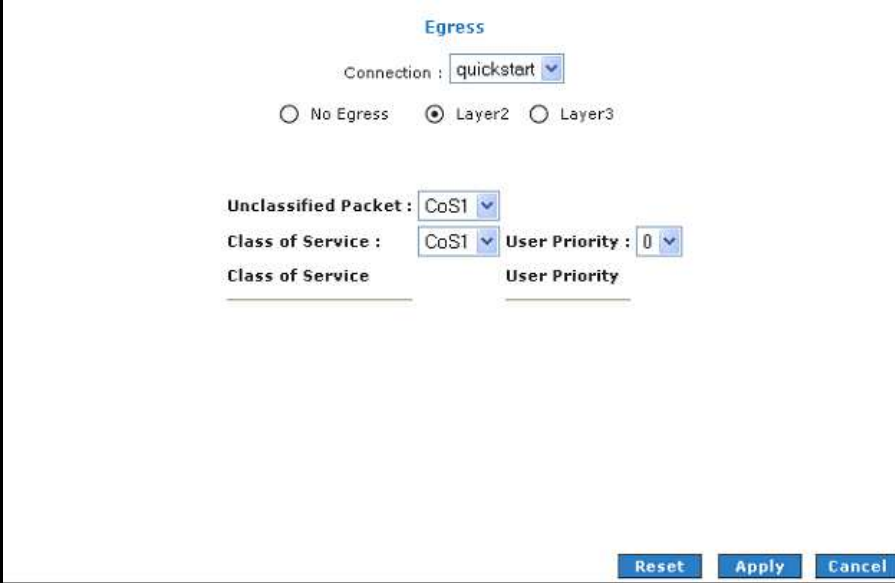
The default Egress page setting for all interfaces is No Egress. In this mode, the domain mappings of the packets are untouched.



Egress

Layer 2

The Egress Layer 2 page allows you to map the CoS of an outgoing packet to user priority bits, which is honored by the VLAN network. Again, this feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current release.

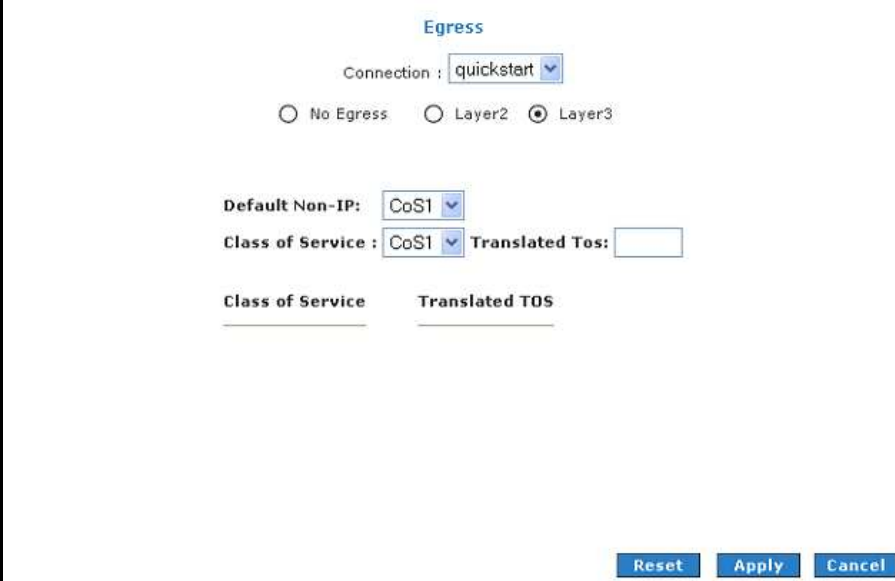


The screenshot shows the 'Egress' configuration window. At the top, the title 'Egress' is displayed. Below it, the 'Connection' is set to 'quickstart'. There are three radio buttons: 'No Egress', 'Layer2' (which is selected), and 'Layer3'. Underneath, there are two columns of settings. The first column has 'Unclassified Packet' set to 'CoS1', 'Class of Service' set to 'CoS1', and 'Class of Service' (with a horizontal line below it). The second column has 'User Priority' set to '0' and 'User Priority' (with a horizontal line below it). At the bottom right, there are three buttons: 'Reset', 'Apply', and 'Cancel'.

Layer 2

Layer 3

Egress Layer 3 enables you to map CoS to ToS so that the priority marking of outgoing packets can be carried over to the IP network.



The screenshot shows the 'Egress' configuration window. At the top, the title is 'Egress'. Below it, the 'Connection' is set to 'quickstart'. There are three radio buttons: 'No Egress', 'Layer2', and 'Layer3'. The 'Layer3' radio button is selected. Below the radio buttons, there are two dropdown menus: 'Default Non-IP:' set to 'CoS1' and 'Class of Service:' set to 'CoS1'. To the right of the 'Class of Service' dropdown is a 'Translated Tos:' text box. Below these fields, there are two columns: 'Class of Service' and 'Translated TOS', each with a horizontal line underneath. At the bottom right, there are three buttons: 'Reset', 'Apply', and 'Cancel'.

Layer 3

Ingress

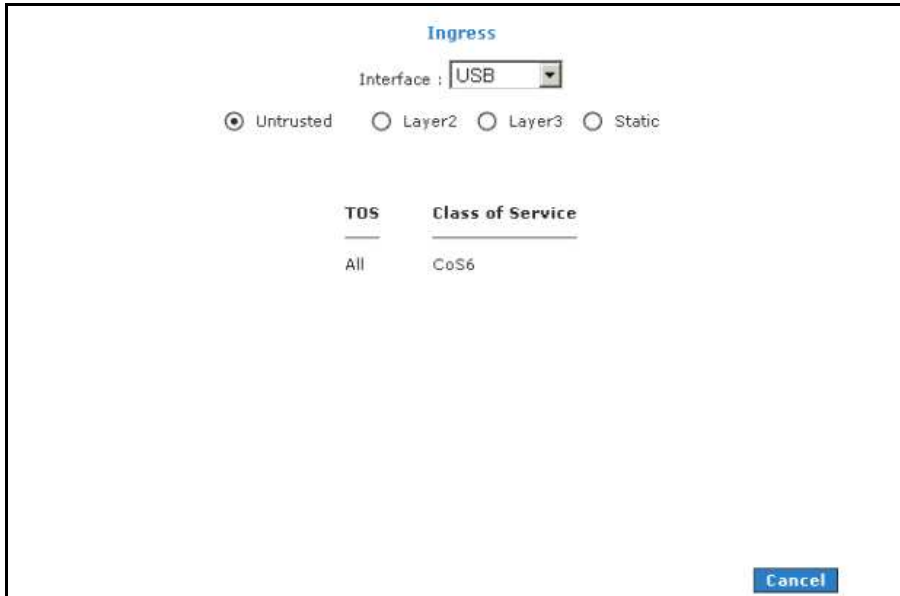
Ingress enables you to configure QoS for packets as soon as they come into the router. The domain mappings are converted to CoS (the common language) so that the priority marking is carried over.

There are four Ingress modes:

- Untrusted mode
- Layer 2
- Layer 3
- Static

Untrusted Mode

Untrusted is the default Ingress page setting for all interfaces. In this mode, no domain mapping is honored in the router. All packets are treated as CoS6 (best effort).



The screenshot shows the 'Ingress' configuration page for the 'USB' interface. The 'Interface' dropdown is set to 'USB'. There are four radio button options: 'Untrusted' (selected), 'Layer2', 'Layer3', and 'Static'. Below these are two columns: 'TOS' and 'Class of Service'. Under 'TOS', the value is 'All'. Under 'Class of Service', the value is 'CoS6'. A 'Cancel' button is located in the bottom right corner.

TOS	Class of Service
All	CoS6

Untrusted mode

Layer 2

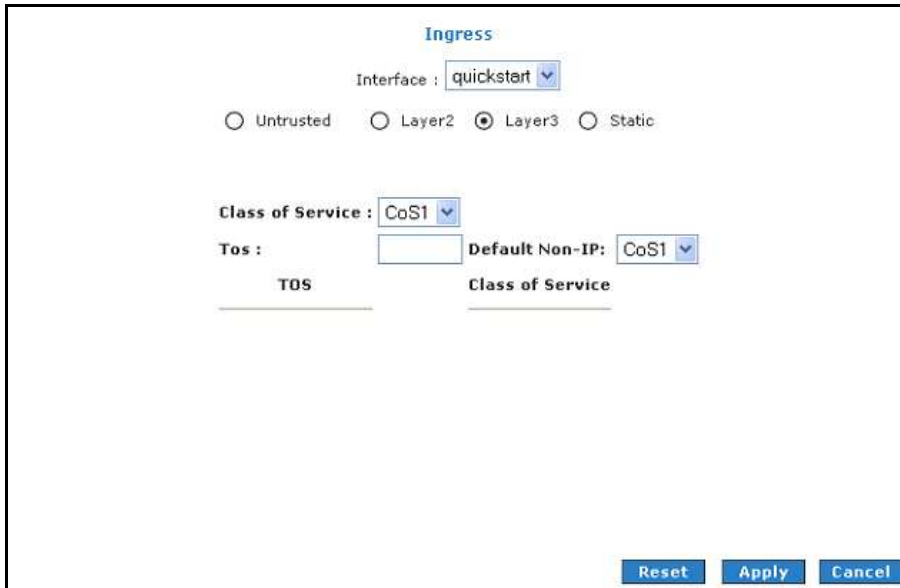
Layer 2 allows you to map an incoming packet with VLAN priority to CoS. This feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current software release.

The screenshot shows a configuration window titled "Ingress". At the top, it says "Interface : quickstart" with a dropdown arrow. Below this are four radio buttons: "Untrusted", "Layer2" (which is selected), "Layer3", and "Static". Underneath the radio buttons, there are two dropdown menus: "Class of Service : CoS1" and "User Priority : 0". Below these dropdowns, the text "User Priority" and "Class of Service" are displayed with horizontal lines underneath them. At the bottom right of the window, there are three buttons: "Reset", "Apply", and "Cancel".

Layer 2

Layer 3

The Layer 3 page allows you to map ToS bits of incoming packets from the IP network to CoS for each WAN/LAN interface.



The screenshot displays the 'Ingress' configuration page for an interface named 'quickstart'. The interface is set to 'Layer3' mode. The 'Class of Service' is configured as 'CoS1'. The 'Tos' field is empty, and the 'Default Non-IP' is also set to 'CoS1'. The page includes 'Reset', 'Apply', and 'Cancel' buttons at the bottom right.

Ingress

Interface : quickstart

Untrusted Layer2 Layer3 Static

Class of Service : CoS1

Tos : Default Non-IP: CoS1

TOS Class of Service

Reset Apply Cancel

Layer 3

Static

The Ingress - Static page enables you to configure a static CoS for all packets received on a WAN or LAN interface.

Ingress

Interface : quickstart ▼

Untrusted Layer2 Layer3 Static

Class of Service : CoS1 ▼

Reset Apply Cancel

Static

QoS Shaper Configuration

The Shaper Configuration page is accessed by selecting Shaper on the Advanced main page. Three shaper algorithms are supported:

- HTB
- Low Latency Queue Discipline
- PRIOWRR

QoS Shaper Configuration

Interface : USB

HTB Queue Discipline Max Rate:

Low Latency Queue Discipline

CoS1 : Kbits CoS2 : Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : Kbits

PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Reset Apply Cancel

QoS Shaper Configuration

Note: Egress TCA is required if shaper is configured for that interface.

Of the three shaping algorithms available on the Shaper Configuration page, only one can be enabled at a time. An example of each configuration is given as follows.

Example 1: HTB Queue Discipline Enabled

In the example below, HTB Queue Discipline is enabled. The PPPoE1 connection has a total of 300 Kbps of bandwidth, of which 100 Kbps is given to CoS1 and another 100 Kbps is given to CoS2. When there is no CoS1 or CoS2 packets, CoS6 packets have the whole 300 Kbps of bandwidth.

The screenshot shows the 'QoS Shaper Configuration' window. The 'Interface' is set to 'quickstart'. The 'HTB Queue Discipline' checkbox is checked, and the 'Max Rate' is set to 300. Under 'Low Latency Queue Discipline', CoS1 is 100 Kbits, CoS2 is 100 Kbits, CoS3 is 0 Kbits, CoS4 is 0 Kbits, CoS5 is 0 Kbits, and CoS6 is 300 Kbits. The 'PRIOWRR' section is unchecked, and all CoS percentage fields are empty. At the bottom right are 'Reset', 'Apply', and 'Cancel' buttons.

CoS	Rate (Kbits)
CoS1	100
CoS2	100
CoS3	0
CoS4	0
CoS5	0
CoS6	300

HTB Queue Discipline enabled

Example 2: Low Latency Queue Discipline Enabled

In this second example, Low Latency Queue Discipline is enabled. CoS1 is not rate controlled (hence the field is disabled). CoS2 takes 100 Kbps when there is no CoS1 packet. CoS6 has 300 Kbps when there is no CoS1 or CoS2 packets. This is similar to the HTB queue discipline as they are both rate-based algorithm, except that CoS1 is handled differently.

QoS Shaper Configuration

Interface : quickstart ▾

HTB Queue Discipline Max Rate: 300

Low Latency Queue Discipline

CoS1 : Kbits CoS2 : 100 Kbits

CoS3 : 0 Kbits CoS4 : 0 Kbits

CoS5 : 0 Kbits CoS6 : 300 Kbits

PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Low Latency Queue Discipline enabled

Example 3: PRIOWRR Enabled

In this third example, PRIOWRR is enabled. Since PRIOWRR operates only on the number of packets being transmitted, the max rate field has been disabled. Only percentage can be assigned to the CoS2 - CoS6. CoS1 is not rate controlled (hence the field is not displayed). When there is no CoS1 packet, CoS2, CoS3, CoS4 each has 10 percent, and CoS6 has 70 percent. This is similarly to the Low Latency Queue discipline, except that one is packet-based, and the other is rate-based.

The screenshot shows the 'QoS Shaper Configuration' window. At the top, the title is 'QoS Shaper Configuration'. Below it, the 'Interface' is set to 'quickstart'. There are three options for queue disciplines: 'HTB Queue Discipline' (unchecked), 'Low Latency Queue Discipline' (unchecked), and 'PRIOWRR' (checked). Under 'HTB Queue Discipline', there is a 'Max Rate' field. Under 'Low Latency Queue Discipline', there are input fields for CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6, each followed by 'Kbits'. Under 'PRIOWRR', there are input fields for CoS2, CoS3, CoS4, CoS5, and CoS6, each followed by a percentage sign. The values are: CoS2: 10%, CoS3: 10%, CoS4: 10%, CoS5: %, and CoS6: 70%. At the bottom right, there are three buttons: 'Reset', 'Apply', and 'Cancel'.

PRIOWRR enabled

Policy Routing Configuration

The Policy Routing Configuration page is accessed by selecting Policy Routing Configuration on the Advanced home page under QoS. This page enables you to configure policy routing and QoS. The policy routing configuration is discussed as follows. The QoS configuration is discussed in “Ingress Payload Database Configuration”.

Ingress Interface	DSCP	Source IP	Destination IP	Source Port	Protocol	Local Mark	Delete	Dest Interface	CoS	Mask	Mask	Destination Port	Source MAC
-------------------	------	-----------	----------------	-------------	----------	------------	--------	----------------	-----	------	------	------------------	------------

Policy Routing Configuration

Currently routing algorithms make decision based on destination address, i.e. only Destination IP address and subnet mask is supported. The Policy Routing page enables you to route packets on the basis of various fields in the packet. The following fields can be configured for Policy Routing:


- Destination IP address/mask
- Source IP address/mask
- Source MAC address
- Protocol (TCP, UDP, ICMP, etc)
- Source port

- Destination port
- Incoming interface
- DSCP

Routing

Static Routing

If the ADSL Router is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway that network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the ADSL Router.



The screenshot shows a window titled "Static Routing". At the top, there is a dropdown menu labeled "Choose a connection:" with "quickstart" selected. Below this are four input fields: "New Destination IP:" (empty), "Mask:" (containing "255.255.255.0"), "Gateway:" (empty), and "Metric:" (containing "0"). In the center of the window, the text "The Routing Table is empty." is displayed. At the bottom right, there are two buttons: "Apply" and "Cancel".

Static Routing

The New Destination IP is the address of the remote LAN network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route here. For a standard Class C IP domain, the network address is the first three fields of the New Destination IP, while the last field should be 0. The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0. The Gateway IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host

Routing Table

Routing Table displays the information used by routers when making packet forwarding decisions. Packets are routed according to the packet's destination IP address.

Routing Table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
220.255.161.1	0.0.0.0	255.255.255.255	UH	0	0	0 ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0 br0
239.0.0.0	0.0.0.0	255.0.0.0	U	1	0	0 br0
0.0.0.0	220.255.161.1	0.0.0.0	UG	0	0	0 ppp0

Routing Table

System Password

Anyone who can access the web interface can be considered an Administrator. To restrict access to the web interface, you need to set the System Password.

To change the System Password:

1. Select **Advanced Menu**
2. Click **System Password**. This opens the **System Password** page.
3. Select **Enable Authentication**.
4. Enter your password.
5. Reenter your password in the **Confirm Password** text box.
6. To temporarily implement the settings, click **Apply**.
7. To make changes permanent, click **Save Settings**.

Note: Remember your account information. If you forget the User Name and System Password, you will need to reset the router to its default settings. To reset, press **RESET** at the router's back panel for 10 seconds.

To change the timeout settings:

1. Select **Advanced Menu**
2. Click **System Password**.
3. Select **Enable Authentication**.
4. Enter the number of minutes in the **Idle Timeout** text field.
5. To temporarily implement the settings, click **Apply**.
6. To make changes permanent, click **Save Settings**.

Firmware Update

When updating the firmware, make sure you are using the correct file. Once the upgrade is complete the router will reboot. You will need to log back into the router after the firmware upgrade is completed.

To update the firmware:

1. Select the **Advanced Menu** and then click **Firmware Upgrade**. This opens the **Firmware Upgrade** page.
2. Click **Browse** and then locate the firmware file.
3. Click **Update Gateway**. The update may take a few minutes. Make sure that the power is not turned off during the update process.

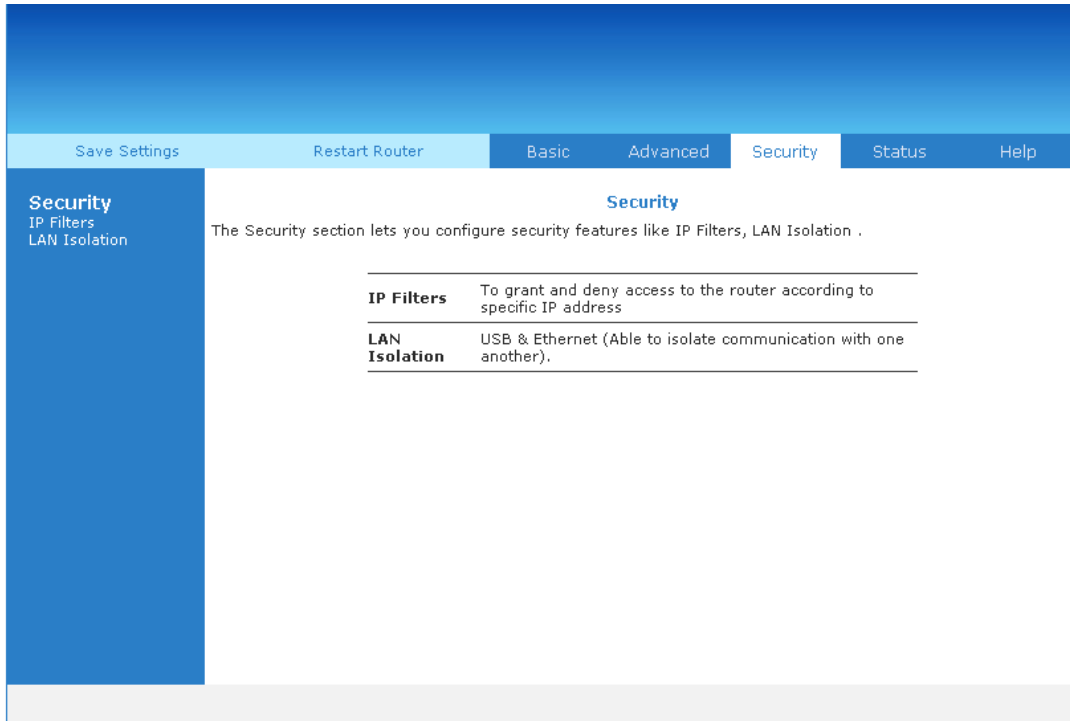
Restore to Default

To reset to the default factory settings, press **RESET** for 10 seconds. This can be found at the router's back panel. When you reset, all the firmware updates will be lost.

To access the web interface again, you need to install the router anew.

Security Menu

Security Menu allows you to configure security tools like IP Filters and LAN Isolation.



The screenshot shows the Security Menu interface. At the top, there is a navigation bar with buttons for 'Save Settings', 'Restart Router', 'Basic', 'Advanced', 'Security' (which is highlighted), 'Status', and 'Help'. On the left side, there is a sidebar menu with 'Security' (highlighted), 'IP Filters', and 'LAN Isolation'. The main content area is titled 'Security' and contains the following text: 'The Security section lets you configure security features like IP Filters, LAN Isolation .'. Below this text, there is a table with two rows:

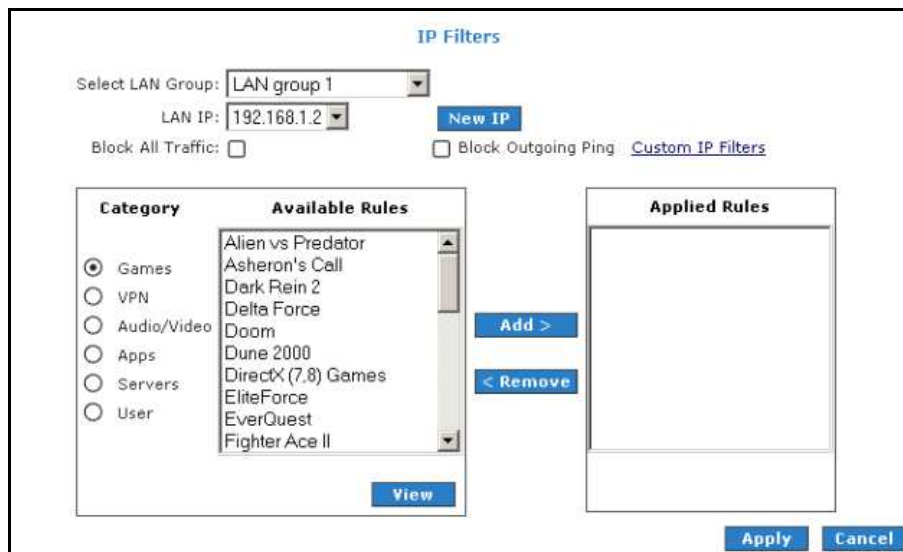
IP Filters	To grant and deny access to the router according to specific IP address
LAN Isolation	USB & Ethernet (Able to isolate communication with one another).

Security Menu

IP Filters

IP filtering allows you to block specific applications/services based on the IP address of the LAN device. In this page, you can block specific traffic (for example, block web access) or any traffic from a host on your local network.

A database of predefined IP filters allows you to apply one or more filtering rules to one or more members of a defined LAN group. You can view the rules associated with a predefined filter and add the available rules for a given category. You can also create, edit, or delete your own IP filter rules.



IP Filters

To configure IP Filters:

1. Select the **Security Menu** and then click **IP Filters**.
2. On the **IP Filters** page, select **LAN Group** and **LAN IP**. If the desired LAN IP is not available in the LAN IP drop-down menu, you can add it using the **LAN Client** page, which is accessed by clicking **New IP**.
3. Select the available rules for a given category. Click **View** to view the rule associated with a predefined filter. Click **Add** to apply the rule for this category.
4. If a rule is not in the list, you can create your own rule in the **User category**. Select **User**, and then click **New**.

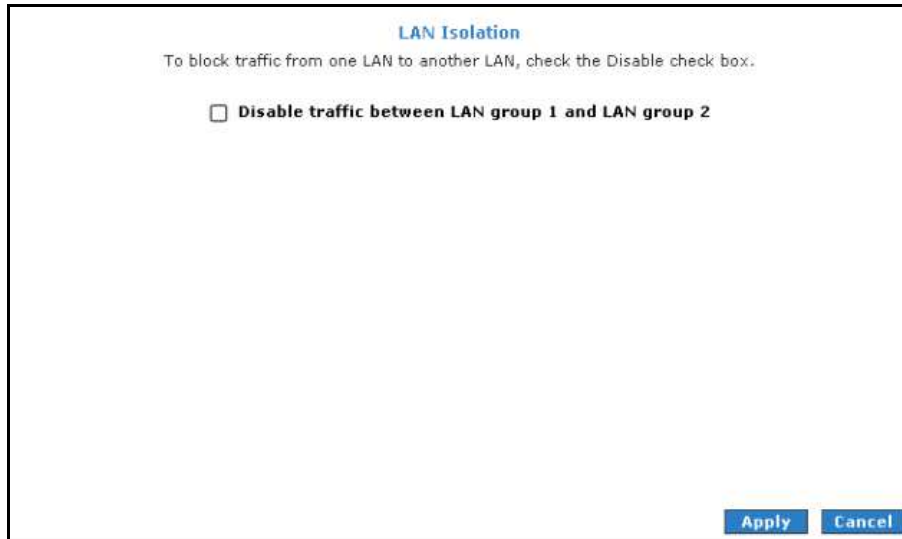
5. The Rule Management page opens for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End**, and **Port Map**, and then click **Apply**.

The rules you create will appear in the **Available Rules** pane in the User category. You can view or delete the rules you create.

6. Continue to add rules as they apply from each category using the **Add** button.
7. To temporarily implement the changes, click **Apply**.
8. To make the change permanent, click **Save Settings**.

LAN Isolation

LAN isolation allows you to disable the flow of packets between two LAN groups. This allows you to secure information in private portions of the LAN from other publicly accessible LAN segments.



LAN Isolation

To enable LAN Isolation:

1. Select the **Security Menu** and then click **LAN Isolation**.
2. On the **LAN Isolation** page, select the checkbox for **Disable traffic between LAN group 1 and LAN group 2**.
3. To temporarily implement the changes, click **Apply**.
4. To make changes permanent, click **Save Settings**.

Status Menu

The Status Menu provides the status for different connections or interfaces.

The Status section allows you to view the Status/Statistics of different connections and interfaces.

Connection Status	Shows WAN IP Address, uptime and protocol connection
System Log	Shows log information for diagnostic purposes and references.
Remote Log	Shows log information for diagnostic purposes and references from a remote area.
Network Statistics	Shows the Statistics of different interfaces - Ethernet/USB//DSL.
DHCP Clients	Shows the system that's connected to the router
Modem Status	Shows the Status and Statistics of your broadband (DSL) connection.
Product Information	Shows the Product Information and Software Versions.

Status Menu

Your router allows you to view the following status and product information:

- Connection Status
- System Log
- Remote Log
- Network Statistics
- DDNS Update Status
- DHCP Clients
- QoS Status

- Modem Status
- Product Information

Connection Status

Connection Status displays the type of protocol, the WAN IP address, the connection state and the duration of your Internet connection.



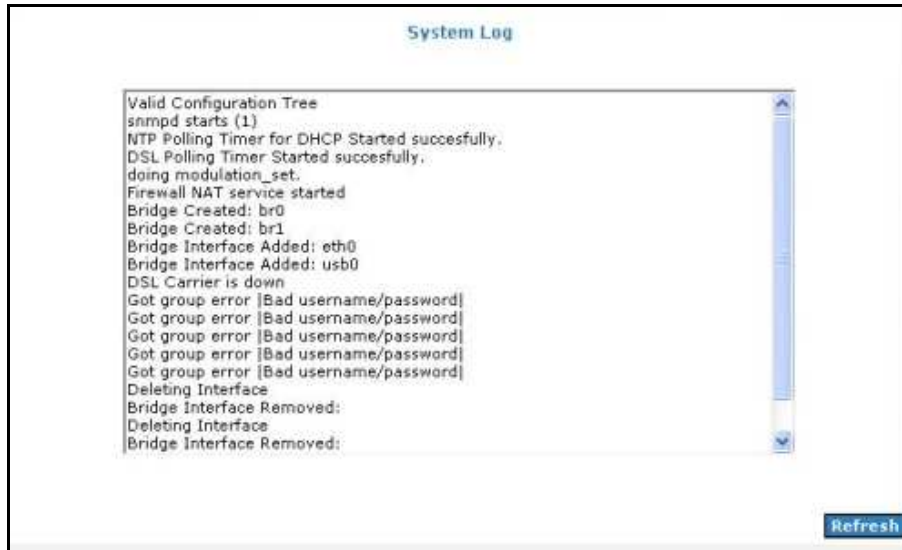
Description	Type	IP	State	Online	Disconnect Reason
quickstart	pppoe	N/A	Not Connected	0	DSL Line is Disconnected

Connection Status

To view the Connection Status, select the **Status Menu** and then click **Connection Status**.

System Log

System Log displays the router log. Depending on the severity level, the information log will generate log reports to a remote host if remote logging is enabled.



System Log

To view the System Log, select the **Status Menu** and then click **System Log**.

Remote Log

Remote Log allows you to forward all logged information to one (or more) remote computer. The type of information forwarded to the remote computer depends on the Log level. Each log message belongs to a certain log level, which indicates the severity of the event.

When you configure remote logging, you must specify a severity level. Log messages that are rated at that level or higher are sent to the log server and can be viewed using the server log application, which can be downloaded from the web.



The screenshot shows a web-based configuration window titled "Remote Log Settings". At the top, there is a "Log Level" section with a dropdown menu currently set to "Notice". Below this, there is a field labeled "Add an IP Address:" followed by an empty text input box and a blue "Add" button. Underneath that, there is a field labeled "Select a logging destination:" with a dropdown menu set to "None" and a blue "Delete" button. At the bottom right of the window, there are two blue buttons: "Apply" and "Cancel".

Remote Log Settings

To enable remote logging:

1. Select the **Status Menu** and then click **Remote Log**.
2. Select a **Log Level**. There are 8 log levels listed below in order of severity.
 - **Panic** System panic or other condition that causes the router to stop functioning.
 - **Alert** Conditions that require immediate correction, such as a corrupted system database.
 - **Critical** Critical conditions such as hard drive errors.

- **Error** Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
 - **Warning** Conditions that warrant monitoring.
 - **Notice** (Default) Conditions that are not errors but might warrant special handling.
 - **Info** Events or non-error conditions of interest.
 - **Debug** Software debugging message. Specify this level only when directed by a technical support representative.
3. Enter the **IP Address** where the log will be sent to and then click **Add**.
 4. Click **Apply**. The IP address will appear in the **Select a logging destination** drop-down menu.
 5. To make changes permanent, click **Save Settings**.

Note: When you select a log level, all log information within this severity level and levels above (meaning, more severe levels) will be sent to the remote host.

To disable a remote log:

1. Select the IP address to be deleted from the **Select a logging destination** drop-down menu.
2. To temporarily implement the changes, click **Apply**.
3. To make changes permanent, click **Save Settings**.

Network Statistics

The Ethernet, USB, and DSL line statuses are displayed in this page.

Network Statistics

Choose an interface to view your network statistics:

Ethernet USB DSL

Transmit

Good Tx Frames	17955
Good Tx Broadcast Frames	1
Good Tx Multicast Frames	0
Tx Total Bytes	20046294
Collisions	0
Error Frames	0
Carrier Sense Errors	0

Receive

Good Rx Frames	12085
Good Rx Broadcast Frames	161
Good Rx Multicast Frames	0
Rx Total Bytes	1235884
CRC Errors	0
Undersized Frames	0
Overruns	0

[Refresh](#)

Network Statistics – Ethernet

Network Statistics

Choose an interface to view your network statistics:

Ethernet USB DSL

Transmit

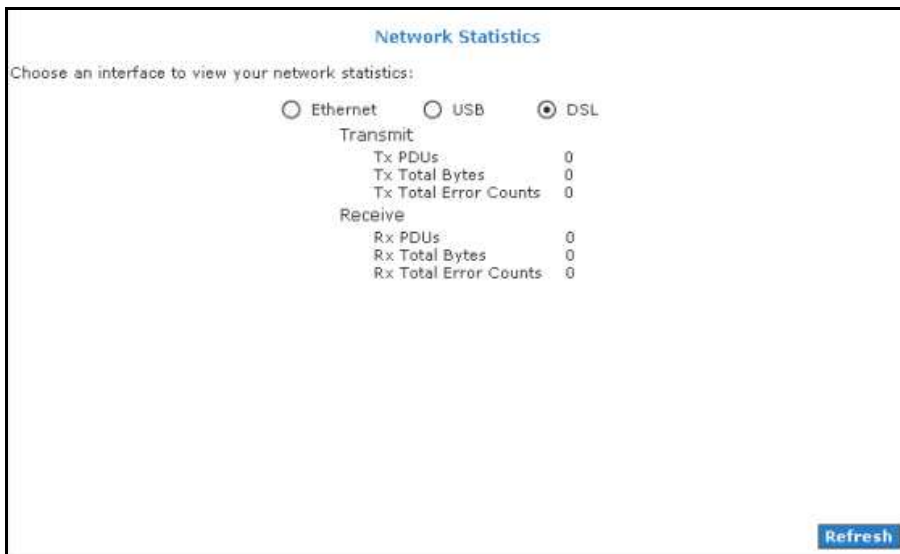
Good Tx Frames	0
Good Tx Broadcast Frames	0
Good Tx Multicast Frames	0
Tx Total Bytes	0

Receive

Good Rx Frames	0
Good Rx Broadcast Frames	0
Good Rx Multicast Frames	0
Rx Total Bytes	0

[Refresh](#)

Network Statistics – USB

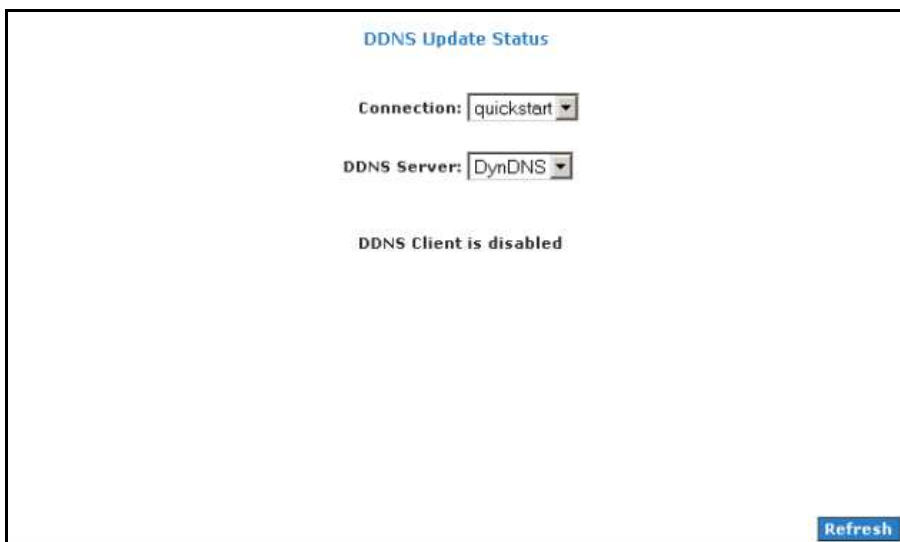


Network Statistics - DSL

To view the Network Statistics, select the **Status Menu** and then click **Network Statistics**.

DDNS Update Status

DDNS Update Status displays the WAN connection status. By default, DDNS is disabled. When the DDNS is enabled, the DDNS client updates every time the router gets a new IP address.



DDNS Update Status

To view the DDNS Update Status, select the **Status Menu** and then click **DDNS Update Status**.

DHCP Clients

DHCP Clients displays the MAC address, IP address, host name, and lease time. To view the DHCP Clients, select the **Status Menu** and then click **DHCP Clients**.



DHCP Clients (1)

Select LAN: LAN group 1

<u>MAC Address</u>	<u>IP Address</u>	<u>Host Name</u>	<u>Lease Time</u>
00:10:b5:6d:e5:13	192.168.1.2	PhuahHongWen	0 days 0:39:8

Refresh

DHCP Clients

QoS Status

This page displays the Quality of Service and the packet statistics. To view the QoS Status, select the **Status Menu** and then click **QoS Status**.

QOS STATUS

QOS Framework : Enabled
Scheduling Algorithm : Strict Round-Robin

NQM Received Statistics	NQM Dropped Statistics
Cos1 Pkts received : 0	Cos1 Pkts received : 0
Cos2 Pkts received : 0	Cos2 Pkts received : 0
Cos3 Pkts received : 0	Cos3 Pkts received : 0
Cos4 Pkts received : 0	Cos4 Pkts received : 0
Cos5 Pkts received : 0	Cos5 Pkts received : 0
Cos6 Pkts received : 8015	Cos6 Pkts received : 0

NQM Congestion Control	Translation Statistics
Cos1 Queue : Empty	Packets Remarkd : 0
Cos2 Queue : Empty	Packets Unchanged : 0
Cos3 Queue : Empty	Non-Ip Packets Marked : 0
Cos4 Queue : Empty	Unclassified Ip Packets Marked : 0
Cos5 Queue : Empty	Unclassified Non-Ip Packets Marked : 0
Cos6 Queue : Empty	Unclassified Layer2 Packets : 0

Congestion State : Not Congested

Classification Statistics
Classification Errors : 0
UnClassified Packets : 0 Fragmented Packets = 0

QoS Status

Modem Status

This page displays the model status.

The screenshot shows a web interface titled "Modem Status". It contains two main sections: "Modem Status" and "DSL Statistics". The "Modem Status" section lists various connection parameters such as Us Rate, Ds Rate, and Line Attenuation. The "DSL Statistics" section shows loop back counts. A "Refresh" button is located at the bottom right of the interface.

Modem Status	
Connection Status	Connected
Us Rate (Kbps)	512
Ds Rate (Kbps)	3488
US Margin	25
DS Margin	22
Trained Modulation	ADSL_G.dmt
LOS Errors	0
DS Line Attenuation	34
US Line Attenuation	21
Peak Cell Rate	1207 cells per sec
CRC Rx Fast	0
CRC Tx Fast	1
CRC Rx Interleaved	0
CRC Tx Interleaved	0
Path Mode	Fast Path

DSL Statistics	
Near End F4 Loop Back Count	0
Near End F5 Loop Back Count	0

[Refresh](#)

Modem Status

To view the Modem Status, select the **Status Menu** and then click **Modem Status**.

Product Information

This page displays the product information and software versions.

The screenshot shows a web interface titled "Product Information". It is divided into two sections: "Product Information" and "Software Versions". The "Product Information" section lists hardware identifiers like Model Number, USB VID, and Ethernet MAC. The "Software Versions" section lists various software components and their versions.

Product Information	
Model Number	ADSL2+ Ethernet and USB Modem
USB PID	0x6060
USB VID	0x0451
Ethernet MAC	00:30:0A:66:D8:BB
DSL MAC	00:30:0A:66:D8:BC
USB MAC	00:30:0A:66:D8:BB
USB Host MAC	00:30:0A:66:D8:BD

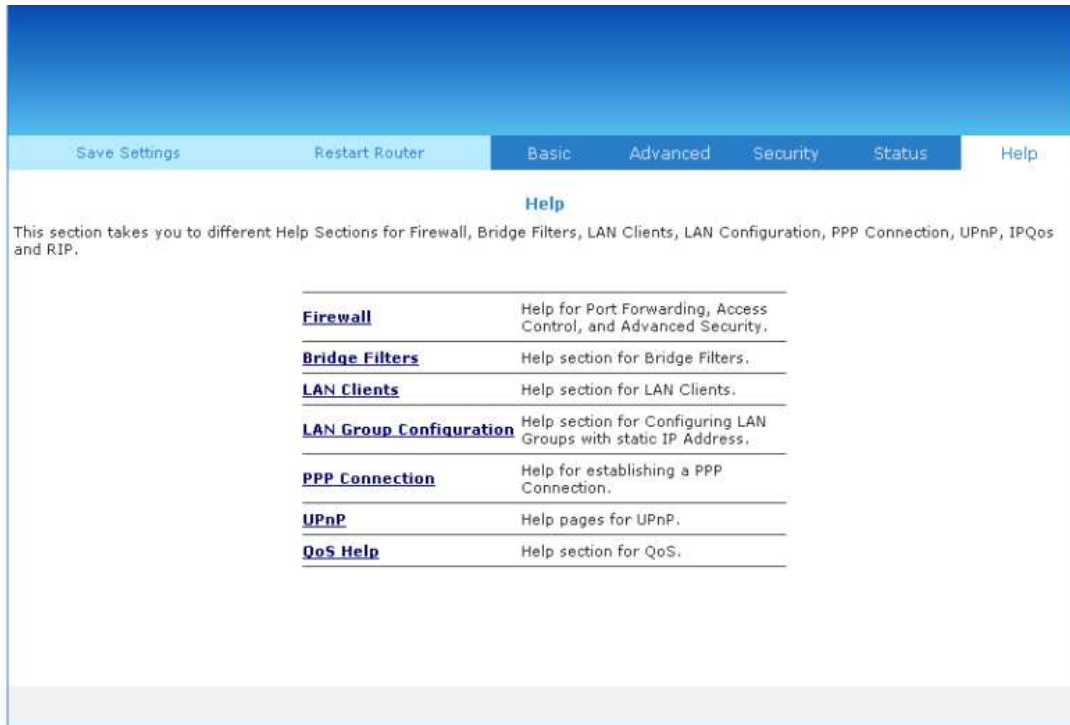
Software Versions	
Gateway	3.7.0
Firmware	
ATM Driver	6.00.01.00
DSL HAL	6.00.01.00
DSL Datapump	6.00.04.00 Annex A
SAR HAL	01.07.2b
PDSP Firmware	0.54
Boot Loader	1.4.0.4

Product Information

To view the Product Information, select **Status** and then click **Product Information**.

Help Menu

The Help page provides documentation for various topics like Firewall, Bridge Filters, LAN Clients, LAN Group Configuration, PPP Configuration, UPnP, IP QoS, and Routing Information Protocol. To access Help, select the **Help Menu**.



Help Menu

Safety Precautions

- Do not open, service, or change any component.
- Only qualified technical specialists are allowed to service the equipment.
- Observe safety precautions to avoid electric shock
- Check voltage before connecting to the power supply. Connecting to the wrong voltage will damage the equipment.

Copyright © 2007. All rights reserved.

No part of this document may be reproduced, republished, or retransmitted in any form or by any means whatsoever, whether electronically or mechanically, including, but not limited to, by way of photocopying, recording, information recording, or through retrieval systems without the express written permission of the owner. Product specifications contained in this document are subject to change without notice. All other company or product names mentioned are used for identification purposes only and may be trademarks of their respective owners.