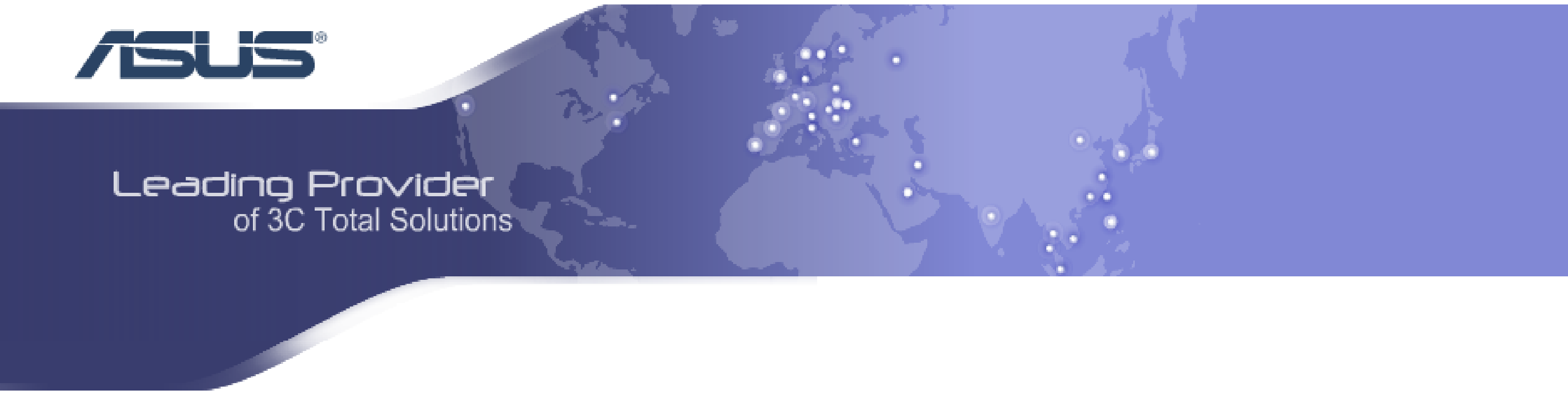


4-Port Ethernet Switch +
Wi-Fi Router
AAM6X20VI-F1

User Manual

Version 1.2

Version Date: October 4, 2005
Document #: BD-AU0011-12

Revision Documentation

9/15/05	Version 1.1 shows changes for upgraded firmware to version 1.5.34.2-0-1.1.3.6.0.2-GEN-0-EW-16.2
10/4/05	Version 1.2 includes a section on how to mount the router (p.9).

Table of Contents

General Information

Thank you for purchasing the ASUS 4-Port Ethernet Switch with Wi-Fi Router. It features wireless access and four LAN ports for added convenience and accessibility.

The following guide will explain how to install and configure your router for both a quick start and an advanced setup.

Package Contents

The router is packaged with one of each of the following–

- ASUS 4-Port Ethernet Switch + Wi-Fi Router
- RJ-45 Ethernet cable
- RJ-11 telephone cable
- 15 VAC AC power adapter
- Splitter
- User Manual / Quick Guide

⚠ Safety Instructions–Please read.

- Place your router on a flat surface close to the cables in a location with sufficient ventilation.

- To prevent overheating, do not obstruct the ventilation openings of this equipment.

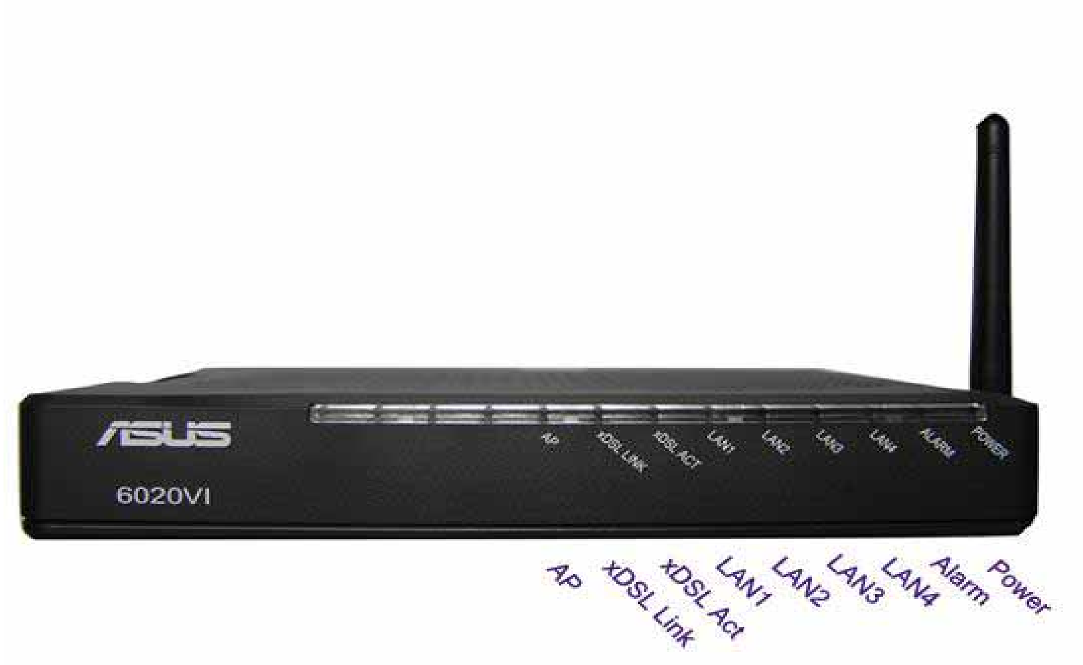
- Plug this equipment into a surge protector to reduce the risk of damage from power surges and lightning strikes.

- Operate this equipment only from an electrical outlet with the correct power source as indicated on the adapter.

- Do not open the cover of this equipment. Opening the cover will void any warranties on the equipment.

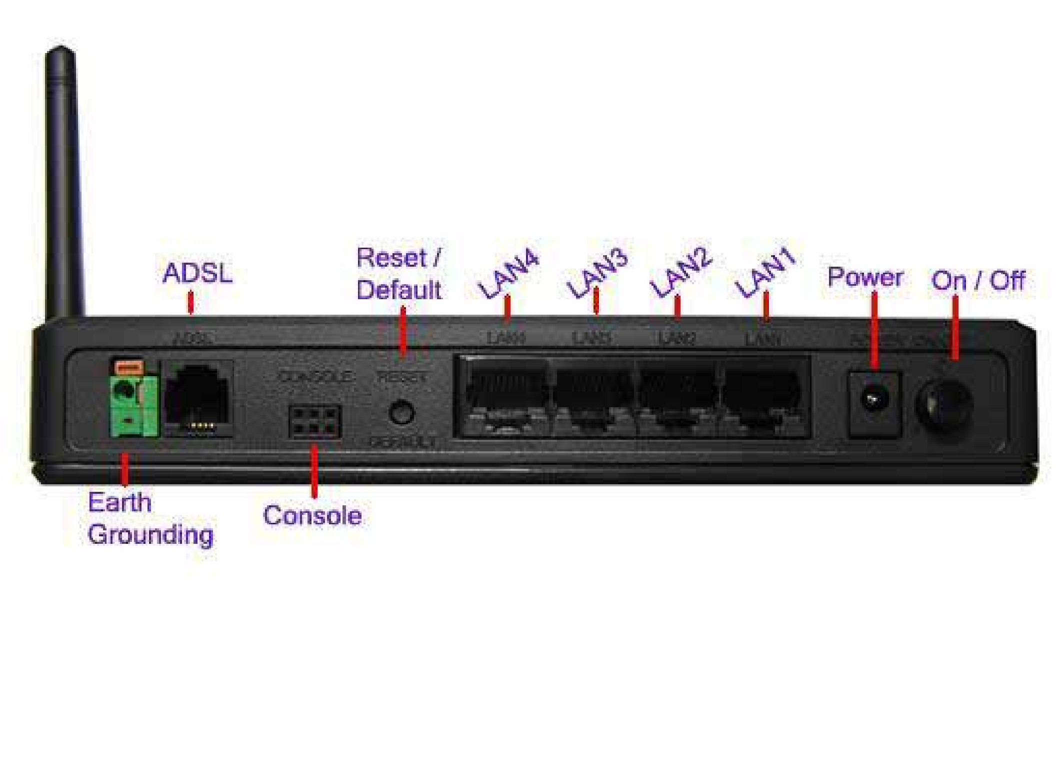
- Unplug equipment first before cleaning. A damp cloth can be used to clean the equipment. Do not use liquid / aerosol cleaners or magnetic / static cleaning devices.

Front Panel View



LED	Mode	Indication
AP	Solid	Wireless is enabled.
	No light	Wireless is disabled.
	Blinking	Presence of wireless traffic.
xDSL Link	Solid	ADSL is connected.
	No light	ADSL is not connected. ALARM LED will be red.
	Blinking	Router is connected to ADSL.
xDSL Act	Solid	ADSL is connected; no traffic.
	No light	ADSL is not connected.
	Blinking	Presence of ADSL traffic.
LAN1-4	Solid	Router is connected to LAN.
	No light	No connection to LAN. Check if LAN cable is connected to router.
	Blinking	Presence of LAN traffic.
Alarm	Solid (red)	ADSL is not connected.
	No light	ADSL is connected.
Power	Solid	Router is powered on.
	No light	Router is not powered on. Check if router is plugged in and if the power switch is turned on.

Back Panel View



Port	Description
ADSL	RJ-11 cable connects to the splitter provided.
Console	Note: To be used for maintenance purposes by service professionals only. If the router needs repair, bring it to a service professional.
Reset / Default	*Restart*–press the button for less than 4 seconds. *Default Settings*–press the button for 4 seconds or longer.
LAN1-4	RJ-45 cable connects the unit to an Ethernet device such as a PC or a switch.
Power	Connects to a 15VAC AC power adapter.
On / Off	Press to turn the router on or off.

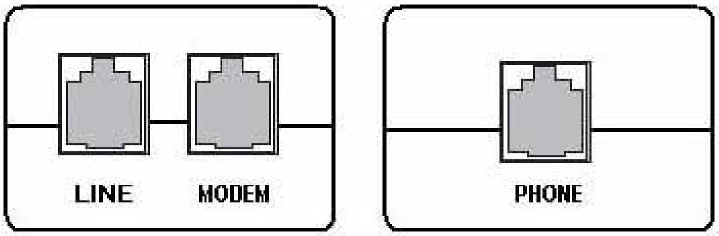
Installing the Router

Connect the ADSL Line and Telephone

- Use an RJ-11 cable to connect the wall phone jack to the line-end of the splitter (see below illustration of splitter).

- Attach another RJ-11 cable to the splitter, the modem-end, and connect the other end to the router port labeled ADSL.

- The final RJ-11 cable will be connected between the phone-end of the splitter and the telephone.



NOTE: See connections on the installation diagram.

Connect the PC to the Router

- Connect one end of the RJ-45 cable to one of the 4 LAN ports on the back of the router and the other end to the Ethernet port of your computer.

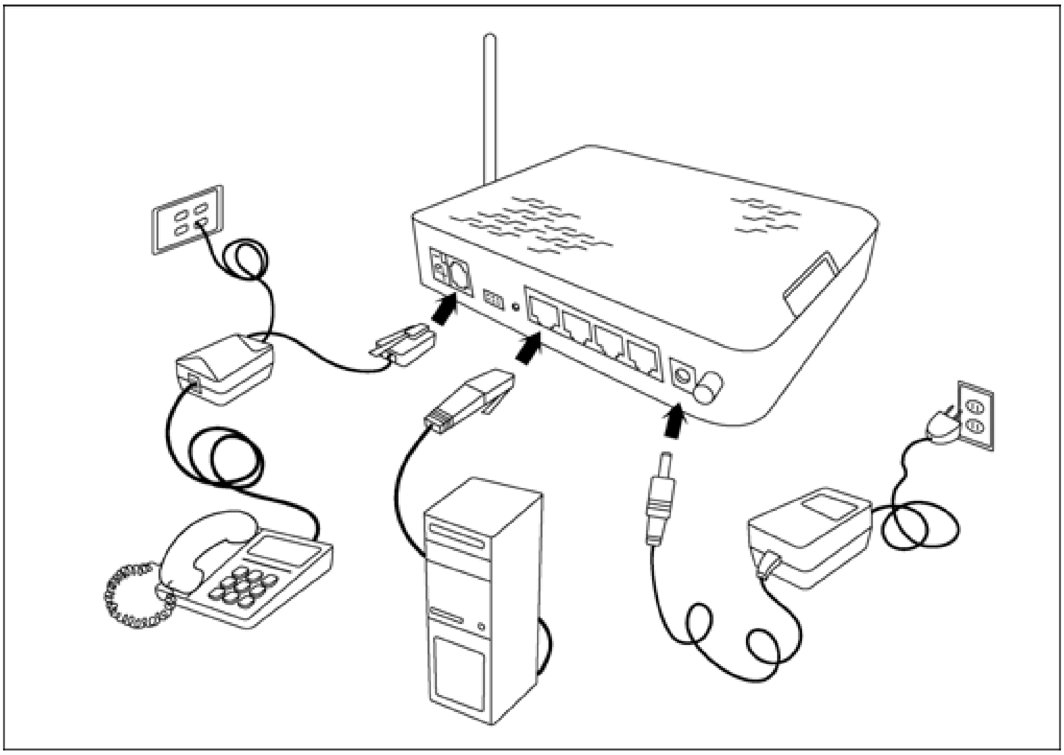
- Attach any additional PCs to the router using RJ-45 cables to the LAN ports on the back panel of the router.

Connect the Power Adapter

- Finish up by connecting the AC power adapter to the POWER connector on the back of the router and plug the adapter into a wall outlet or power strip.

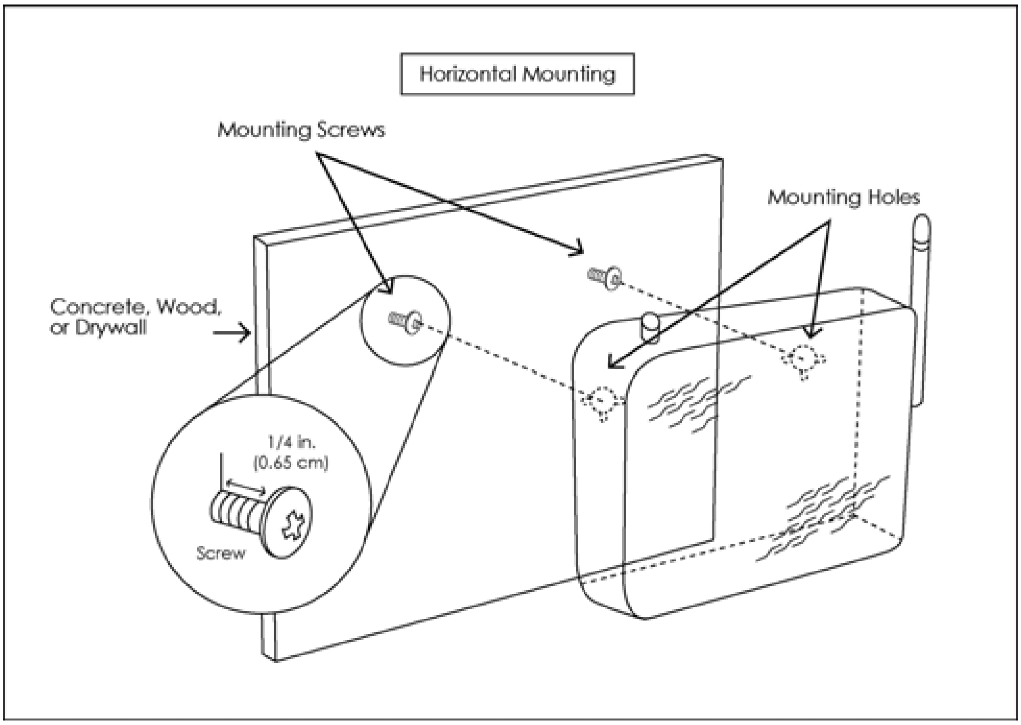
- Turn on and boot up your PC and any LAN devices, such as hubs or switches, and any computers connected to them.

Installation Diagram



Mounting the Router

The router can be mounted on the wall with the screws provided. Mounting can be done on wall material including concrete, wood, or drywall. Select an appropriate location free from obstructions or any possible interference. Make sure the cables can be easily attached to the router without strain. The illustration below shows how to mount the router horizontally on a wall.



Configuring Your Computer

Prior to accessing the router through the LAN port, note the following necessary configurations–

- Your PC's TCP/IP address: 192.168.1.__(the last number is any number between 3 and 254)

- The router's default IP address: 192.168.1.1

- Subnet mask: 255.255.255.0

Below are the procedures for configuring your computer. Follow the instructions for the operating system that you are using.

Windows 2000

1. In the Windows taskbar, click on the Start button and point to Settings, Control Panel, and Network and Dial-up Connections (in that order).

2. Click on Local Area Connection. When you have the Local Area Connection Status window open, click on Properties.

3. Listed in the window are the installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled, and you can skip to Step 10.

4. If Internet Protocol (TCP/IP) does not appear as an installed component, then click on Install.

5. In the Select Network Component Type window, click on protocol and then the Add button.

6. Select Internet Protocol (TCP/IP) from the list and then click on OK.

7. If prompted to restart your computer with the new settings, click OK.

8. After your computer restarts, click on the Network and Dial-up Connections icon again, and right click on the Local Area Connection icon and then select Properties.

9. In the Local Area Connection Properties dialog box, select Internet Protocol (TCP/IP) and then click on Properties.

10. In the Internet Protocol (TCP/IP) Properties dialog box, click in the radio button labeled Use the following IP address and type 192.168.1.x (where x is any number between 2 and 254) and 255.255.255.0 in the IP address field and Subnet Mask field.

11. Click on OK twice to save your changes and then close the Control Panel.

Windows XP

1. In the Windows taskbar, click on the Start button and point to Settings and then click Network Connections.

2. In the Network Connections window, right click on the Local Area Connection icon and click on properties.

3. Listed in the Local Area Connection window are the installed network components. Make sure the box for Internet Protocol (TCP/IP) is checked and then click on Properties.

4. In the Internet Protocol (TCP/IP) Properties dialog box, click in the radio button labeled Use the following IP address and type 192.168.1.x (where x is any number between 2 and 254) and 255.255.255.0 in the IP address field and Subnet Mask field.

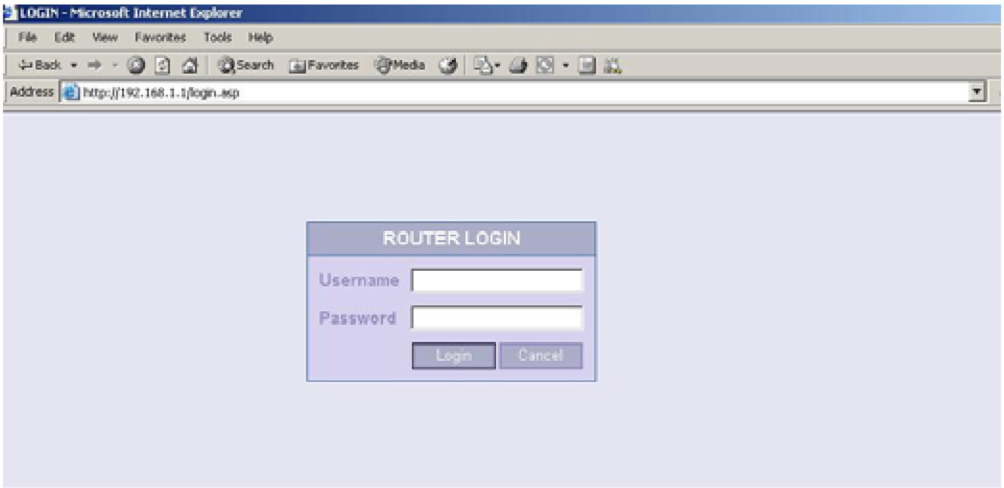
5. Click on OK twice to save your changes and then close the Control Panel.

Log in to the Router

After installing the hardware portion of your router, you will need to configure the router through the user interface. Below are the steps for logging into the router.

Steps:

1. Launch your web browser.
2. Type http://192.168.1.1 in the URL address bar and press Enter.
3. The below login screen will be displayed.


LOGIN - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/login.asp
ROUTER LOGIN
Username
Password
Login
Cancel

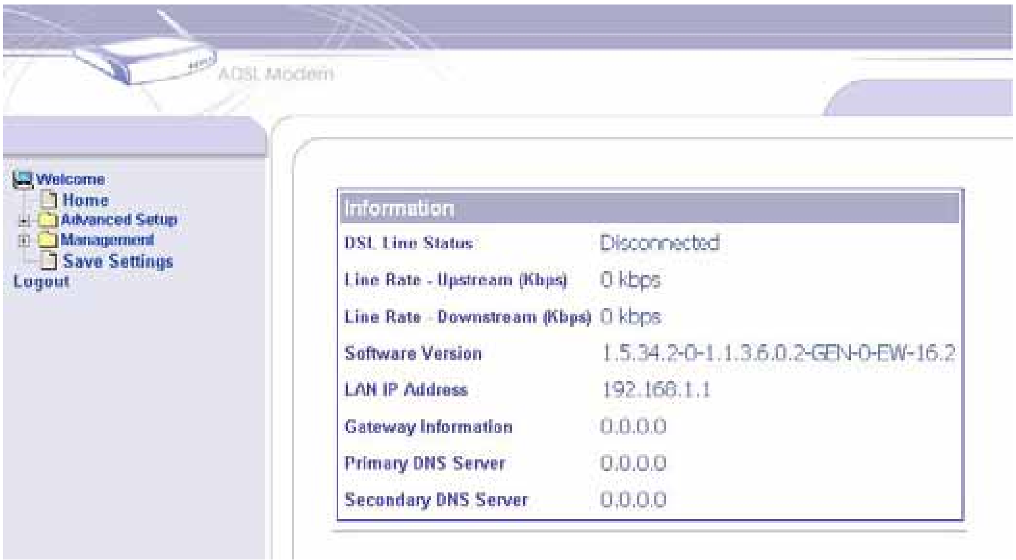
4. Enter the below username / password and click on **LOGIN**.

Username	root
Password	admin

5. After logging in, you will be able to configure the router.

Home Screen

After logging in, the home screen shows information on the router, including the connection status, the upstream / downstream line rate, software version, IP address, etc.



Information	
DSL Line Status	Disconnected
Line Rate - Upstream (Kbps)	0 kbps
Line Rate - Downstream (Kbps)	0 kbps
Software Version	1.5.34.2-0-1.1.3.6.0.2-GEN-0-EW-16.2
LAN IP Address	192.168.1.1
Gateway Information	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

Advanced Setup

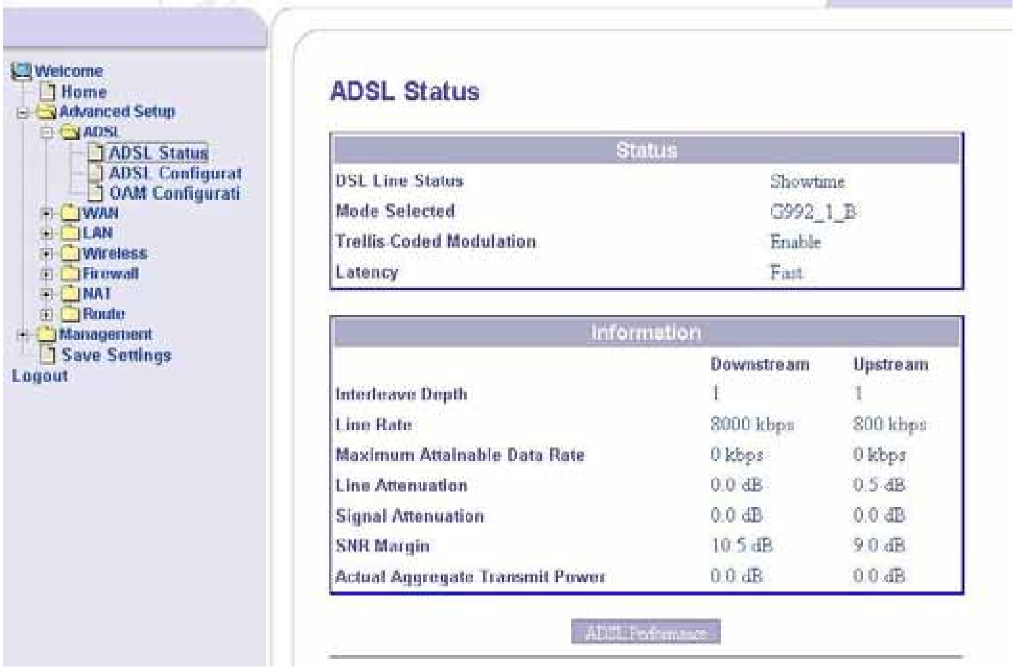
This section of the user manual is on the advanced configurations of the router. The topics under Advanced Setup are *ADSL, WAN, LAN, VLAN, Firewall, NAT,* and *Route.*

ADSL

The following section will explain the ADSL portion of the configurations, including a status screen as shown below.

ADSL Status

This section of the router displays statuses and information on your ADSL connection. You can also perform an ADSL performance test.

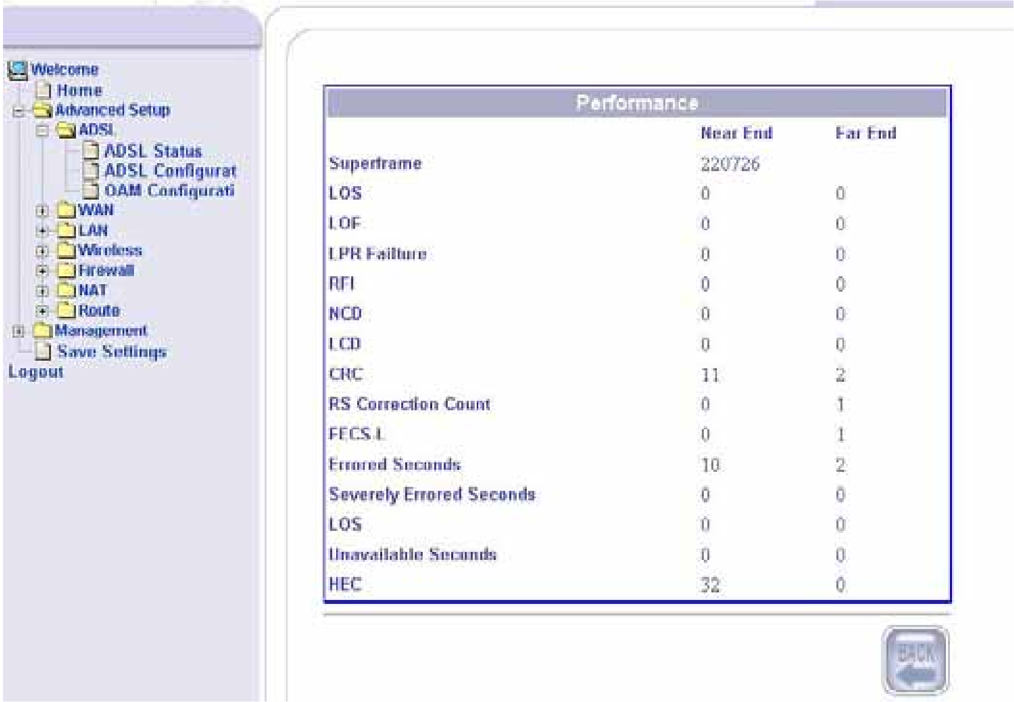


ADSL Status

Status	
DSL Line Status	Showtime
Mode Selected	G992_1_B
Trellis Coded Modulation	Enable
Latency	Fast

Information	Downstream	Upstream
Interleave Depth	1	1
Line Rate	8000 kbps	800 kbps
Maximum Attainable Data Rate	0 kbps	0 kbps
Line Attenuation	0.0 dB	0.5 dB
Signal Attenuation	0.0 dB	0.0 dB
SNR Margin	10.5 dB	9.0 dB
Actual Aggregate Transmit Power	0.0 dB	0.0 dB

Clicking the **ADSL Performance** button at the bottom of the ADSL Status page displays the following screen.

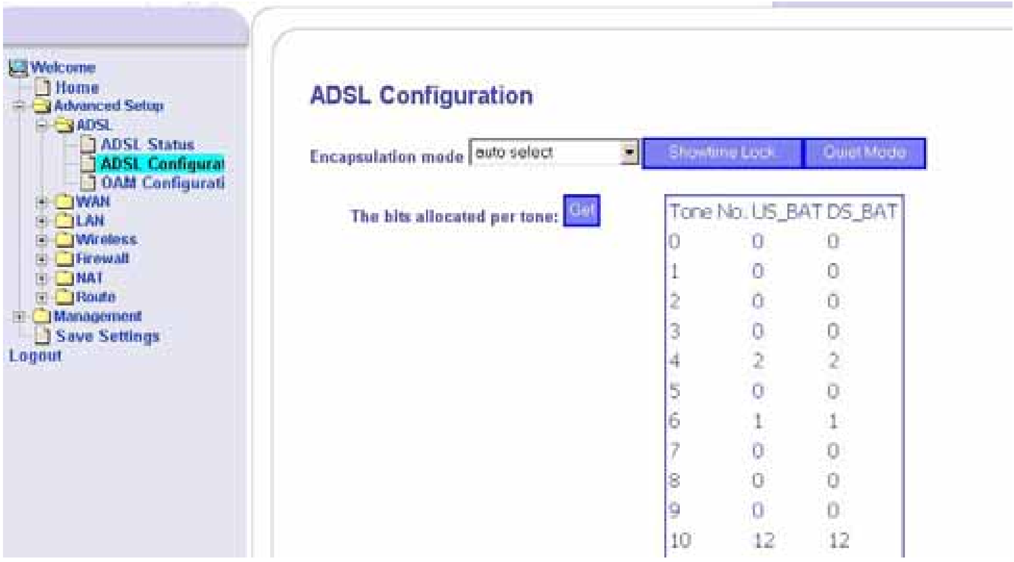


Performance

	Near End	Far End
Superframe	220726	
LOS	0	0
LOF	0	0
LPR Failure	0	0
RFI	0	0
NCD	0	0
LCD	0	0
CRC	11	2
RS Correction Count	0	1
FECS-L	0	1
Errored Seconds	10	2
Severely Errored Seconds	0	0
LOS	0	0
Unavailable Seconds	0	0
HEC	32	0

ADSL Configuration

In the ADSL Configuration screen, select the encapsulation mode that you will be using, which include auto select, ADSL, ADSL2, and ADSL2+, G.992.3 Annex I/J/M, G.992.5 Annex I/J/M, Annex B auto select, and Annex M auto select. The table shows tone numbers 0-511. There are also two buttons–showtime lock and quiet mode–which you can select. Click **Apply** after making your selection to save and reboot the router.



ADSL Configuration

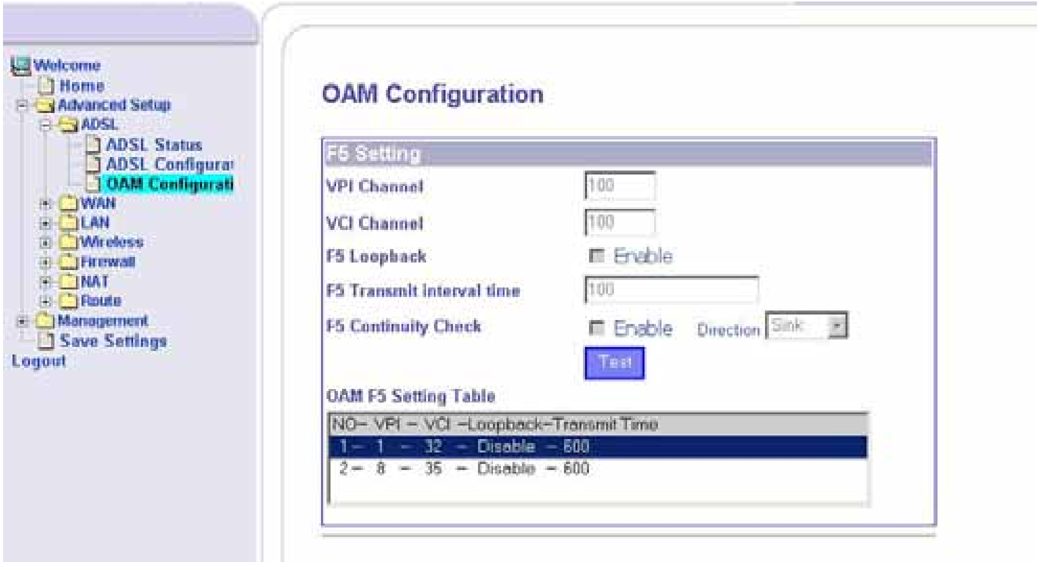
Encapsulation mode: auto select

The bits allocated per tone:

Tone No.	US_BAT	DS_BAT
0	0	0
1	0	0
2	0	0
3	0	0
4	2	2
5	0	0
6	1	1
7	0	0
8	0	0
9	0	0
10	12	12

OAM Configuration

The OAM (Operation Administration Maintenance) Test performs fault detection and notification for each connection with the option to enable standard loopback (end-to-end or segment).



OAM Configuration

F5 Setting

VPI Channel	100
VCI Channel	100
F5 Loopback	□ Enable
F5 Transmit interval time	100
F5 Continuity Check	□ Enable Direction Sink

OAM F5 Setting Table

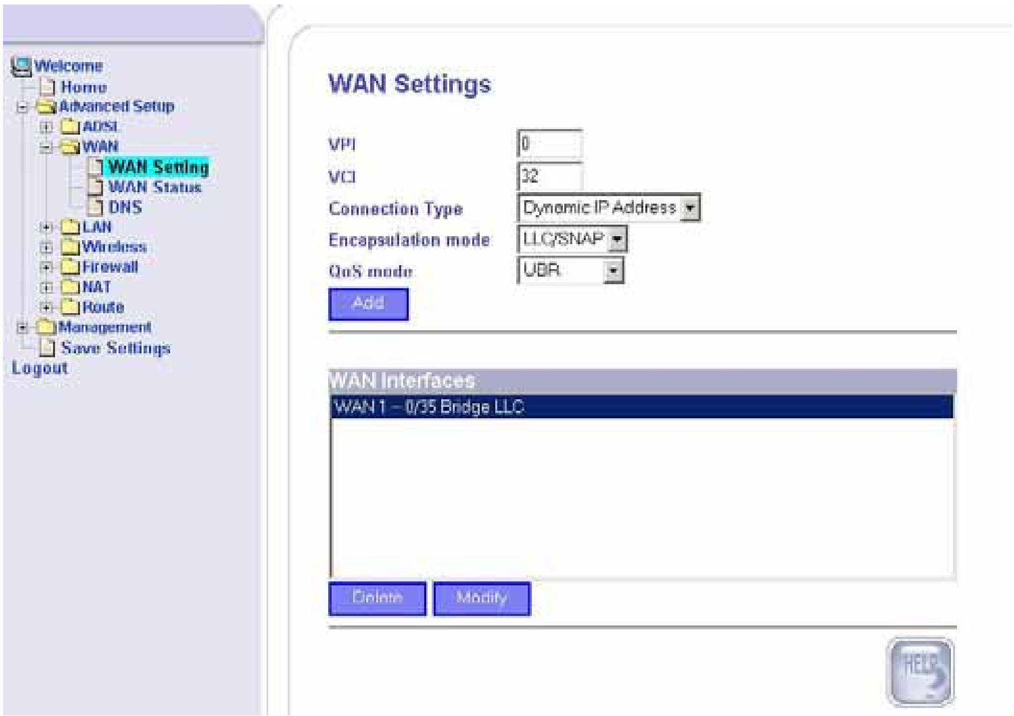
```
NO- VPI - VCI -Loopback-Transmit Time
 1-  1  -  32  - Disable  - 600
 2-  8  -  35  - Disable  - 600
```

WAN

To configure the WAN settings, access the ADSL configuration screens by clicking on the WAN folder on the left menu bar under Advanced Setup.

WAN Settings

Below is the first page of the WAN Settings section which allows you to enter the VPI / VCI, connection type, encapsulation mode, and QoS mode for your WAN interface. After you make your selections, click on *Add* to make specific settings for the connection that you choose.



WAN Settings

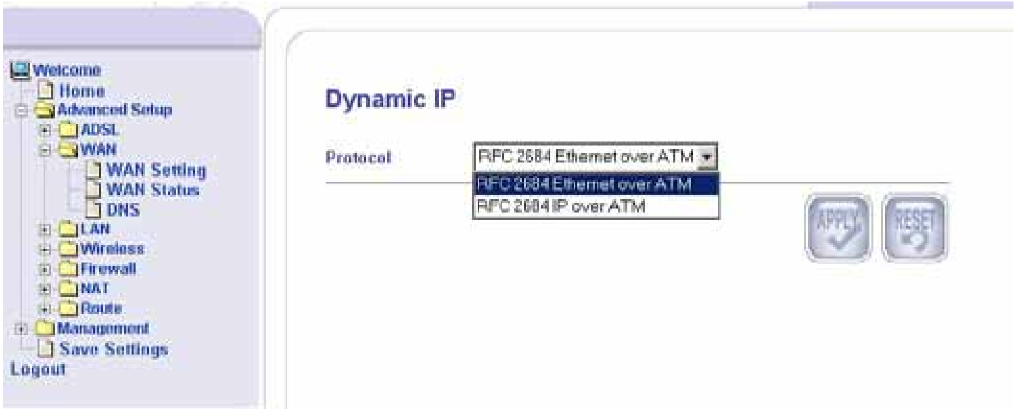
VPI 0
VCI 32
Connection Type Dynamic IP Address
Encapsulation mode LLC/SNAP
QoS mode UBR

WAN Interfaces
WAN 1 – 0/35 Bridge LLC

The connection types include the following–

- Dynamic IP Address
- Static IP Address
- PPPoE
- PPPoA
- Bridge

Below is the screen you will see if you select Dynamic IP Address and click on Apply. There are no fields to enter except to select the protocol that you are using.



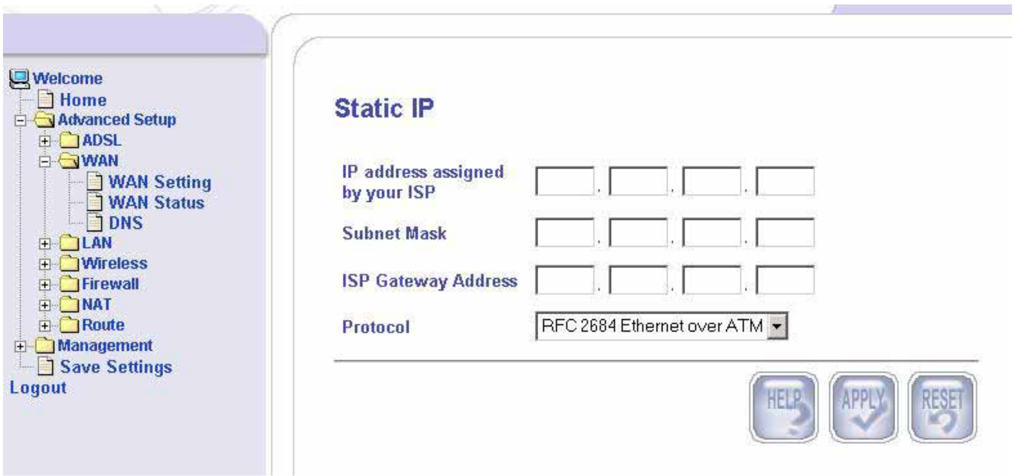
Dynamic IP

Protocol: RFC 2684 Ethernet over ATM

RFC 2684 Ethernet over ATM
RFC 2684 IP over ATM

If you are using a Static IP, then the below screen includes fields that need to be filled out with information from your ISP. You will need to find out the following information–

- IP Address assigned by your ISP
- Subnet Mask
- ISP Gateway Address
- Protocol (either RFC 2684 Ethernet over ATM or RFC 2684 IP over ATM)



Static IP

IP address assigned by your ISP: ___ . ___ . ___ . ___

Subnet Mask: ___ . ___ . ___ . ___

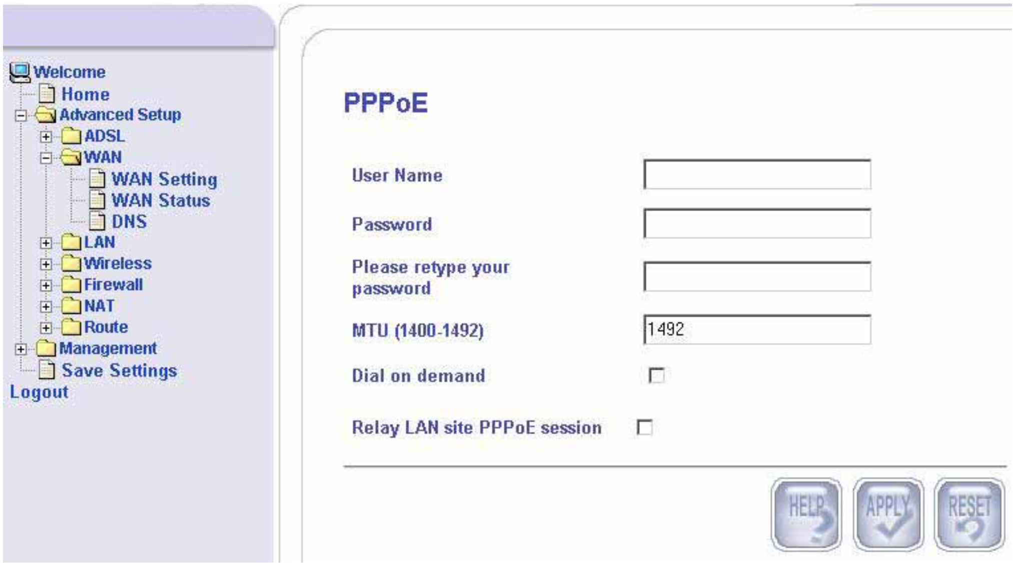
ISP Gateway Address: ___ . ___ . ___ . ___

Protocol: RFC 2684 Ethernet over ATM

If you are using PPPoE or PPPoA, then obtain the following information from your ISP–

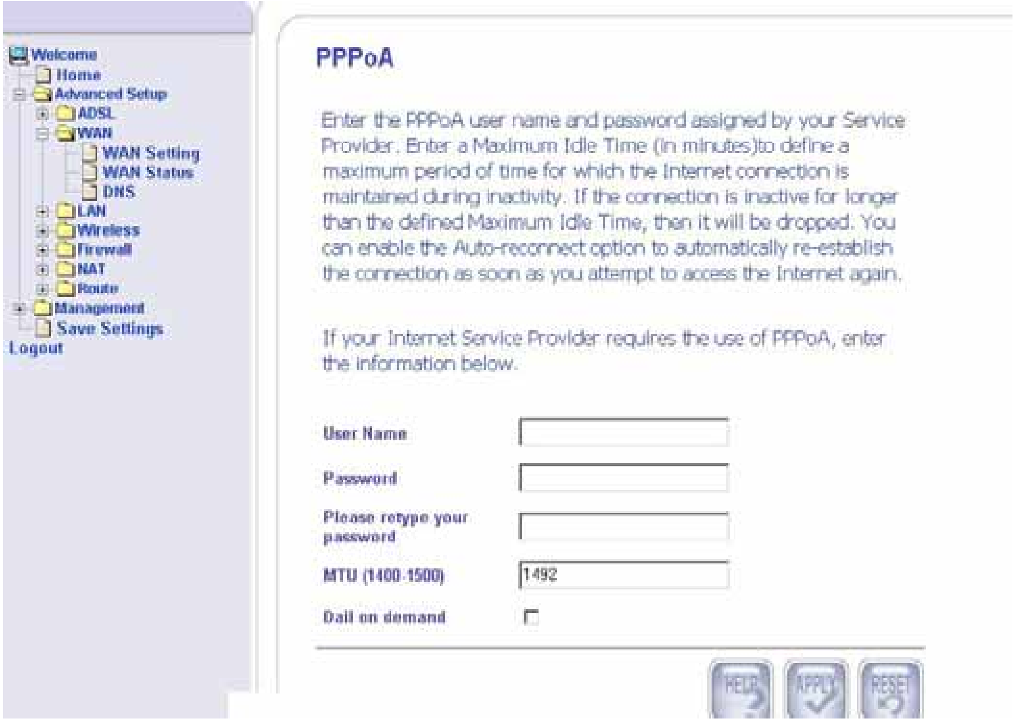
- Username / Password
- MTU–Maximum Transmission Unit, it is the largest physical packet size, measured in bytes that a network can transmit before it must be divided into a smaller sized-packet.
- Dial On Demand (enable or disable)–this feature allows for automatic reconnecting to your ISP if your connection is lost.

- Relay LAN site PPPoE session–this feature is where you can relay pppoe packets coming from the pc to the server instead of the router sending the pppoe packets from the router itself.



PPPoE

User Name	
Password	
Please retype your password	
MTU (1400-1492)	1492
Dial on demand	□
Relay LAN site PPPoE session	□



PPPoA

Enter the PPPoA user name and password assigned by your Service Provider. Enter a Maximum Idle Time (in minutes)to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the defined Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.

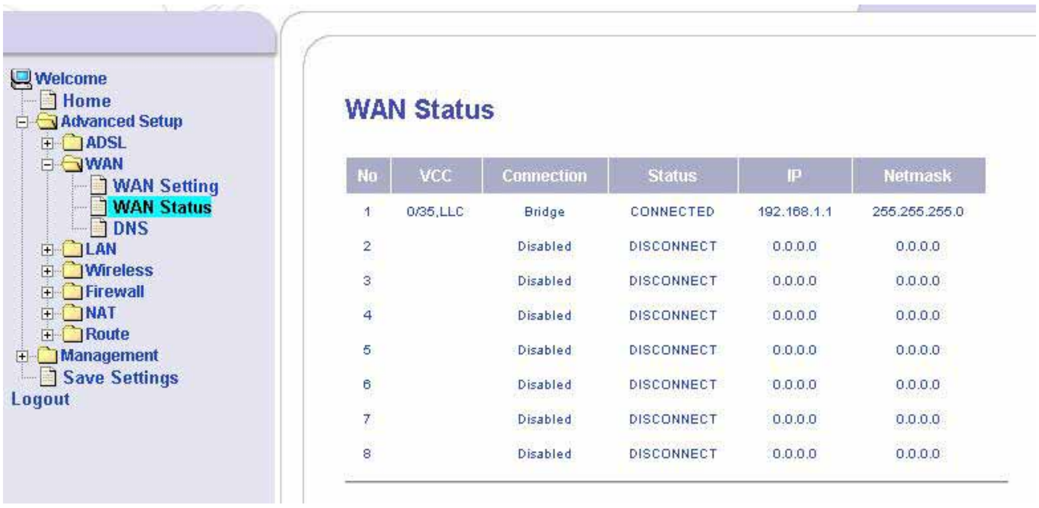
If your Internet Service Provider requires the use of PPPoA, enter the information below.

User Name	
Password	
Please retype your password	
MTU (1400-1500)	1492
Dail on demand	□

Selecting Bridge Mode automatically changes your connection type to bridge, which changes the WAN status as shown in the screen below (same as the WAN status page).

WAN Status

The WAN status page is an informational page that shows which connection type has been selected for the WAN(s).

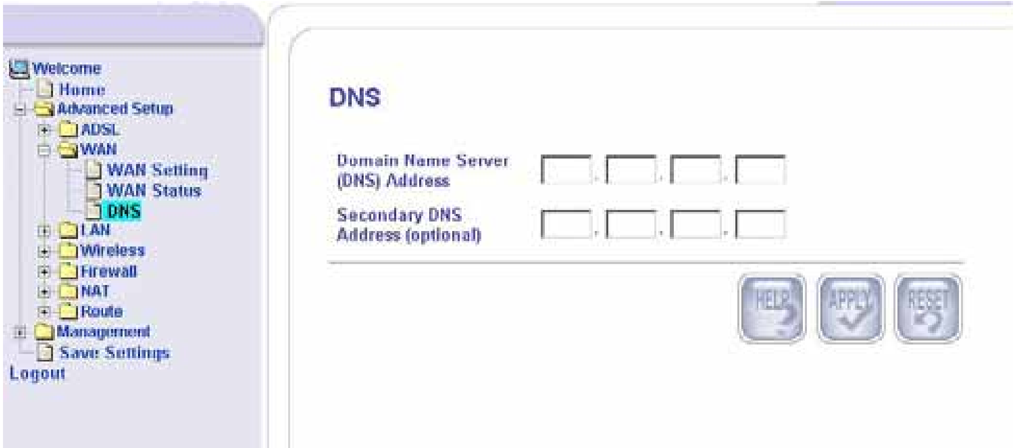


WAN Status

No	VCC	Connection	Status	IP	Netmask
1	0/35,LLC	Bridge	CONNECTED	192.168.1.1	255.255.255.0
2		Disabled	DISCONNECT	0.0.0.0	0.0.0.0
3		Disabled	DISCONNECT	0.0.0.0	0.0.0.0
4		Disabled	DISCONNECT	0.0.0.0	0.0.0.0
5		Disabled	DISCONNECT	0.0.0.0	0.0.0.0
6		Disabled	DISCONNECT	0.0.0.0	0.0.0.0
7		Disabled	DISCONNECT	0.0.0.0	0.0.0.0
8		Disabled	DISCONNECT	0.0.0.0	0.0.0.0

DNS

Enter the IP address of the Domain Name Server and the secondary DNS Address (if available) and click **Apply**.



DNS

Domain Name Server (DNS) Address ___ . ___ . ___ . ___

Secondary DNS Address (optional) ___ . ___ . ___ . ___

LAN

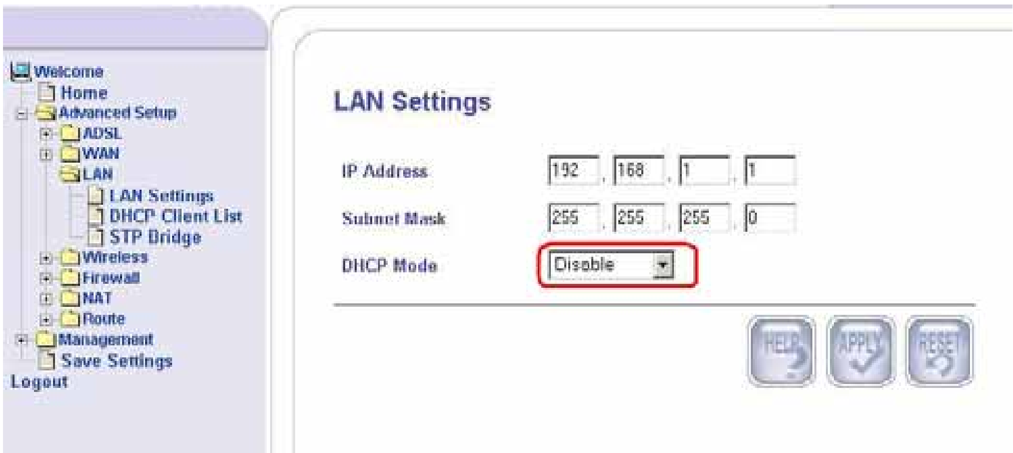
To configure the LAN settings of the router, click on the LAN folder on the left menu bar.

LAN Settings

Enter the LAN interface IP address and the LAN subnet mask of the router. Then select the DHCP mode from the list of choices–

- Disable
- Server
- Relay Agent

Click on **Apply** after you have finished completing the fields. Below is a screen showing a disabled DHCP mode. Notice that there are no additional required settings after you disable DHCP mode.



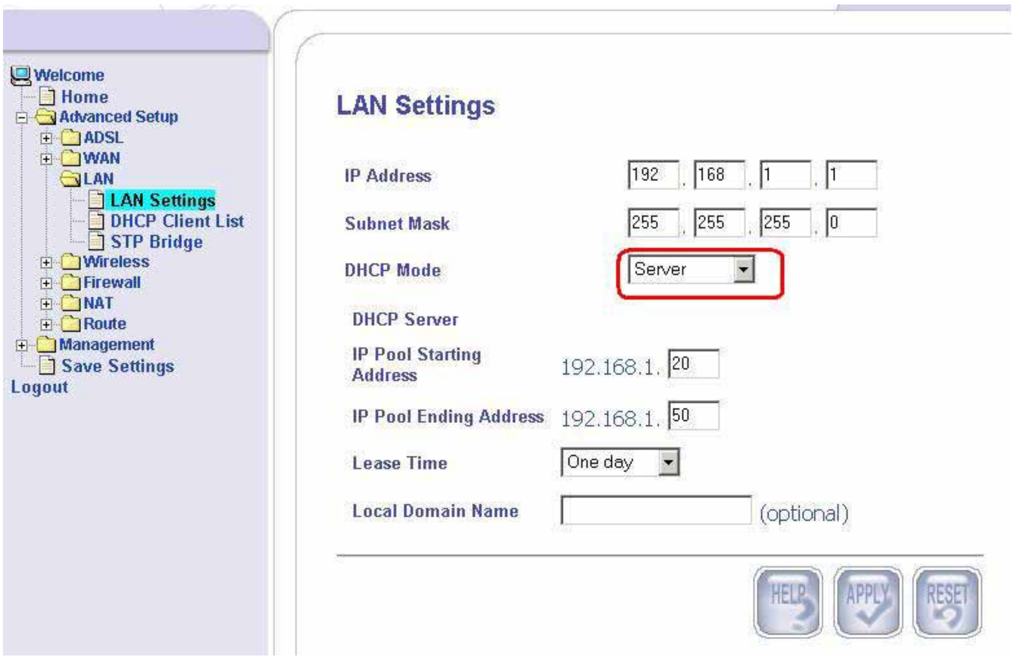
LAN Settings

IP Address 192 . 168 . 1 . 1

Subnet Mask 255 . 255 . 255 . 0

DHCP Mode Disable

If you select a Server DHCP mode, then enter the range of IP addresses that can be assigned in the **IP Pool Starting Address** and **IP Pool Ending Address**. Also enter the lease time (from a half hour to a maximum of two weeks) for the use of these IP addresses before they must be renewed. Click on **Apply** to save these settings.



LAN Settings

IP Address 192 . 168 . 1 . 1

Subnet Mask 255 . 255 . 255 . 0

DHCP Mode Server

DHCP Server

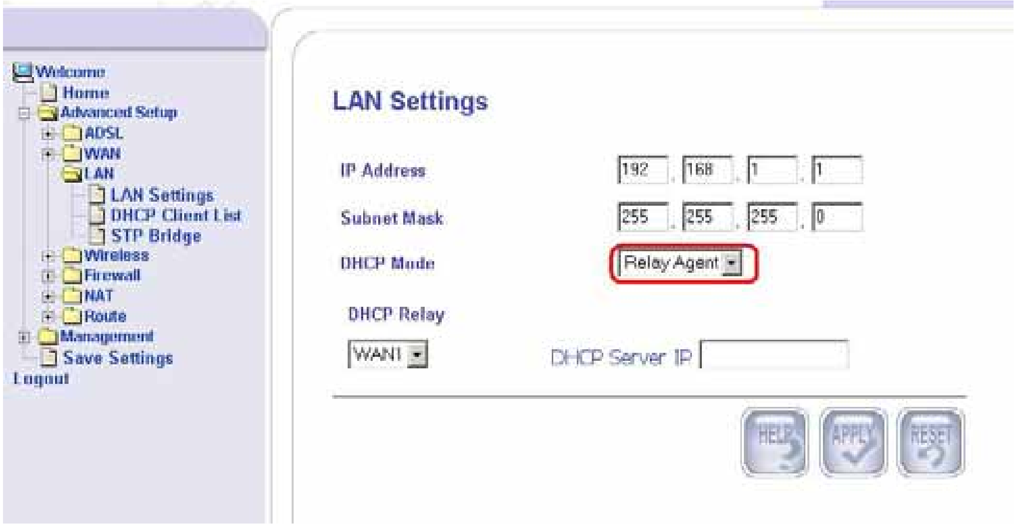
IP Pool Starting Address 192.168.1. 20

IP Pool Ending Address 192.168.1. 50

Lease Time One day

Local Domain Name (optional)

If you set your router as the relay agent, then enter the DHCP Server's IP address that the router will be routing requests from the PC(s) to the DHCP server. Also select the WAN channel that you are connected to. Each channel can be unique PVC and can be assigned one protocol. Find out from your ISP what protocol and PVC to use.



LAN Settings

IP Address 192 . 168 . 1 . 1

Subnet Mask 255 . 255 . 255 . 0

DHCP Mode Relay Agent

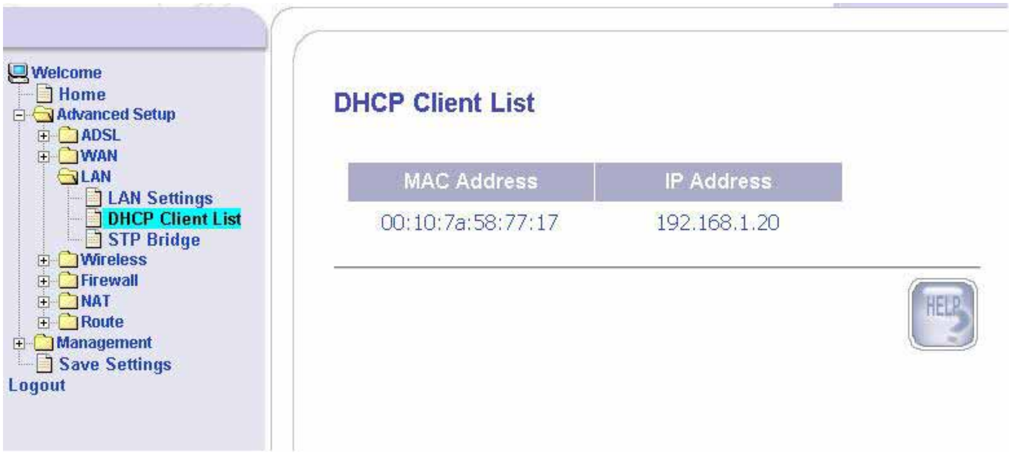
DHCP Relay

WAN1

DHCP Server IP

DHCP Client List

This screen shows the list of IP addresses that have been obtained through a DHCP server.

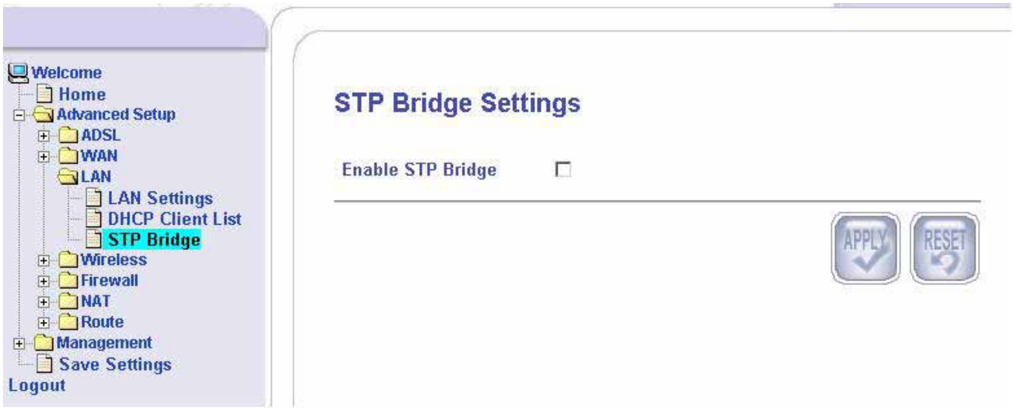


DHCP Client List

MAC Address	IP Address
00:10:7a:58:77:17	192.168.1.20

STP Bridge

If you decide to enable the STP Bridge function of the router, then click on the box and then Apply to save.



STP Bridge Settings

Enable STP Bridge □

Wireless

This section allows you to configure wireless settings on your router.

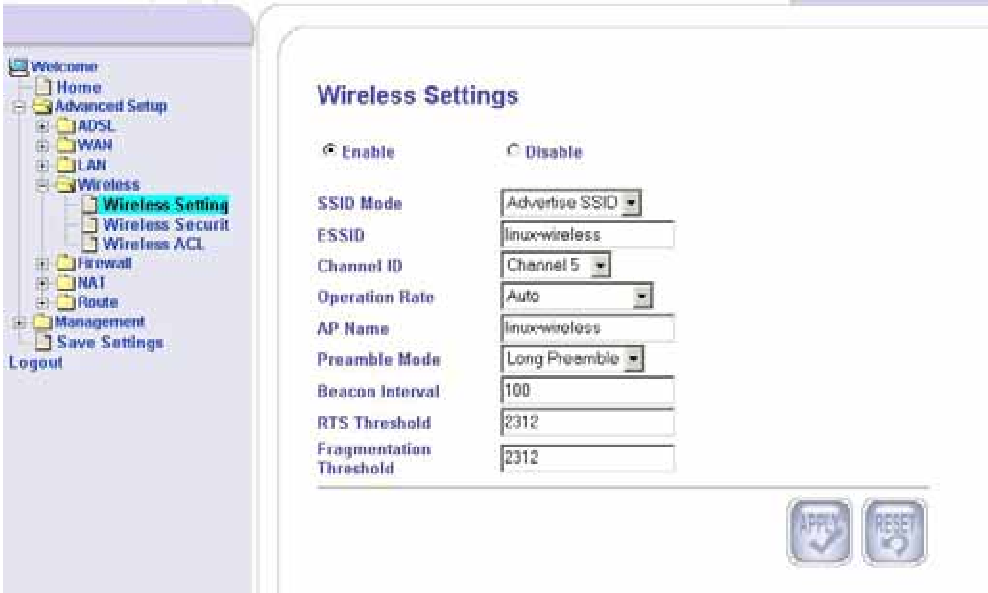
Wireless Settings

This section is the wireless settings page with all the fields already filled in with the router's default information. You will not need to change the information unless you have specific changes. Below is a description of the wireless settings–

AP Name–this is the name for your router
SSID Mode–includes *Advertise SSID* and *Hide SSID*
ESSID–this is the same as the AP name
Channel ID–includes channel 1 to 14
Preamble Mode–includes short and long preamble and auto
Operation Mode–includes 802.11b rate only, 802.11g rate only, and auto
Beacon Interval–a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms).
RTS Threshold (Request to Send Threshold)–determines the packet size of a transmission through the use of the router to help control traffic flow.
Fragmentation Threshold-- used to fragment packets that help

improve performance in the presence of radio frequency (RF) interference.

If you wish to disable wireless, then click on the Disable radio button and click on *Apply*.



Wireless Settings

● Enable ○ Disable

SSID Mode	Advertise SSID
ESSID	linux-wireless
Channel ID	Channel 5
Operation Rate	Auto
AP Name	linux-wireless
Preamble Mode	Long Preamble
Beacon Interval	100
RTS Threshold	2312
Fragmentation Threshold	2312

Wireless Security

Security settings can be changed on this page. Below are the fields that can be configured.

- Authentication Type–
    - Open–anyone can access the network. The default is a disabled WEP encryption setting.
    - Shared–WEP encryption is enabled and encryption key strength of 64-bit or 128-bit needs to be selected. Click on Set Encryption Keys to manually set the network encryption keys. Up to 4 different keys can be set and you can come back to select which one to use at anytime.
    - WPA-TLS (Wi-Fi Protected Access - Transport Layer Protocol)
    - WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key)–WPA for home and SOHO environments also using the same strong TKIP encryption, per-packet key construction, and key management that WPA provides in the enterprise environment.

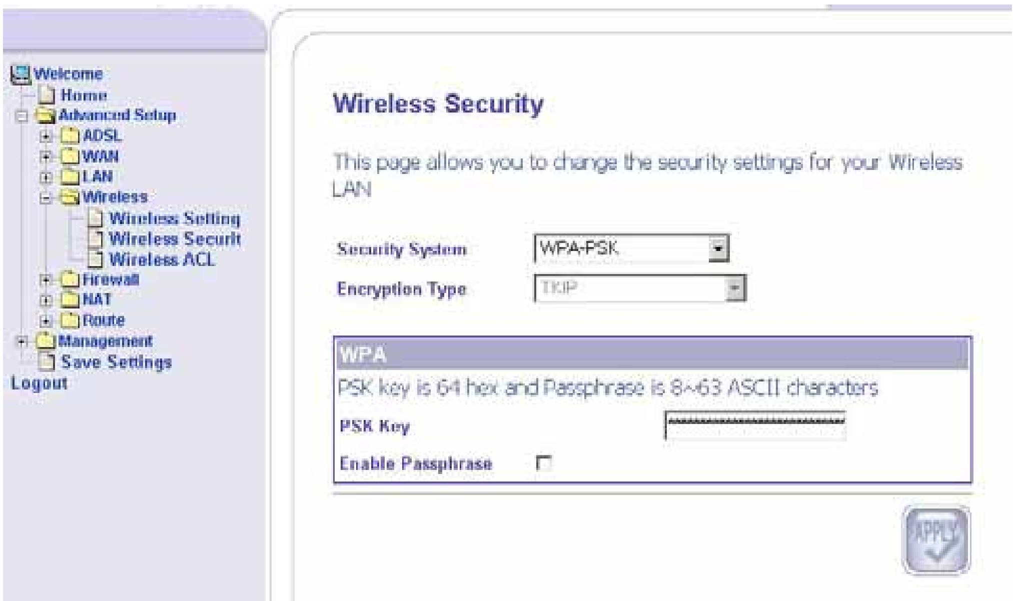
The main difference is that the password is entered manually. A group re-key interval time is also required.

- Encryption Type– to encrypt data, select the encryption type that you wish to use. The range is from no encryption at all to the stronger encryption type, TKIP.
  - No Encryption
  - WEP 64 (10 digits)
  - WEP 128 (26 digits)
  - Standard 802.1X (WEP)
  - TKIP
- Active Key–select which key you wish to be active.
  - None
  - Key 1 to Key 4

If you have a radius server, then continue onto the next section. Fill in the following information regarding your radius server–

- NAS Identifier
- Radius server address
- Radius Server Port
- Radius Server Secret
- 1x Key Length

The next section is only required if you select authentication type WPA-PSK. Enter the PSK Key and click to enable passphrase.



Wireless Security

This page allows you to change the security settings for your Wireless LAN

Security System: WPA-PSK

Encryption Type: TKIP

WPA

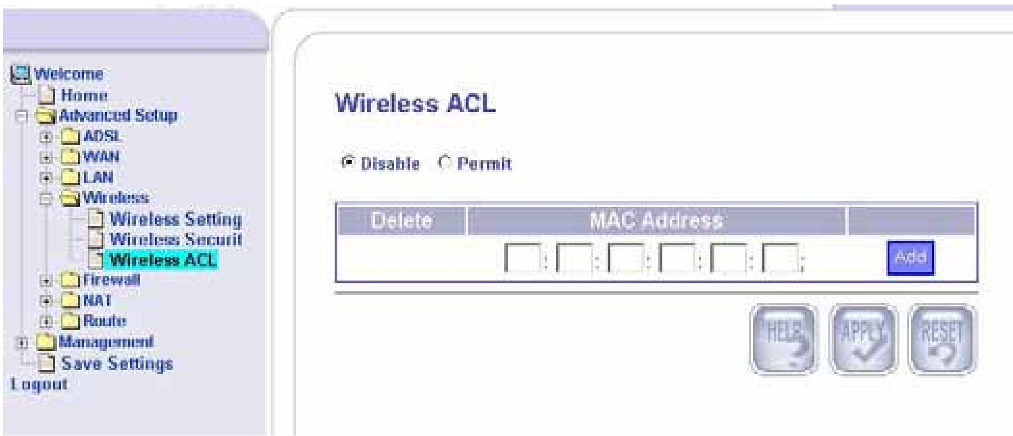
PSK key is 64 hex and Passphrase is 8~63 ASCII characters

PSK Key: ****************************

Enable Passphrase □

Wireless ACL

The Wireless ACL (Access Control List) page allows you to enter the MAC addresses that you will permit access to your wireless router. If you wish to disable this feature, then click on the disable radio button and click on *Apply*.



Wireless ACL

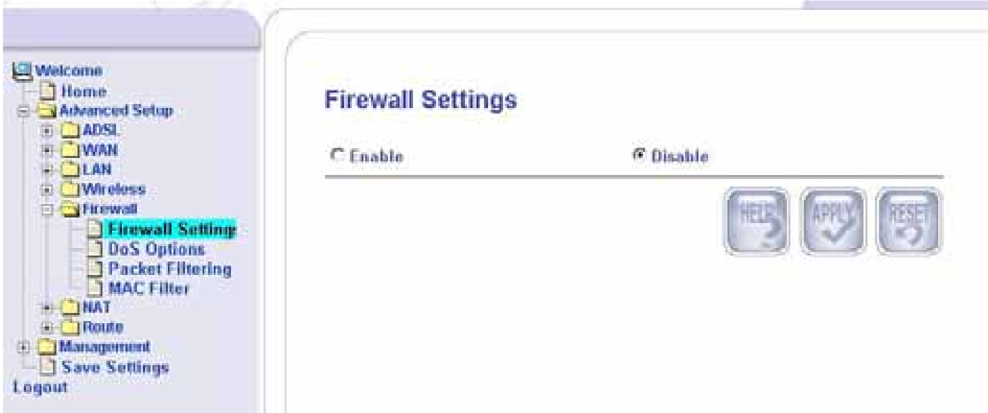
● Disable ○ Permit

Delete	MAC Address	
	□ : □ : □ : □ : □ : □	Add

Firewall

Firewall Settings

To enable / disable your router’s built-in firewall, select your choice here and click on **Apply** to save the settings.



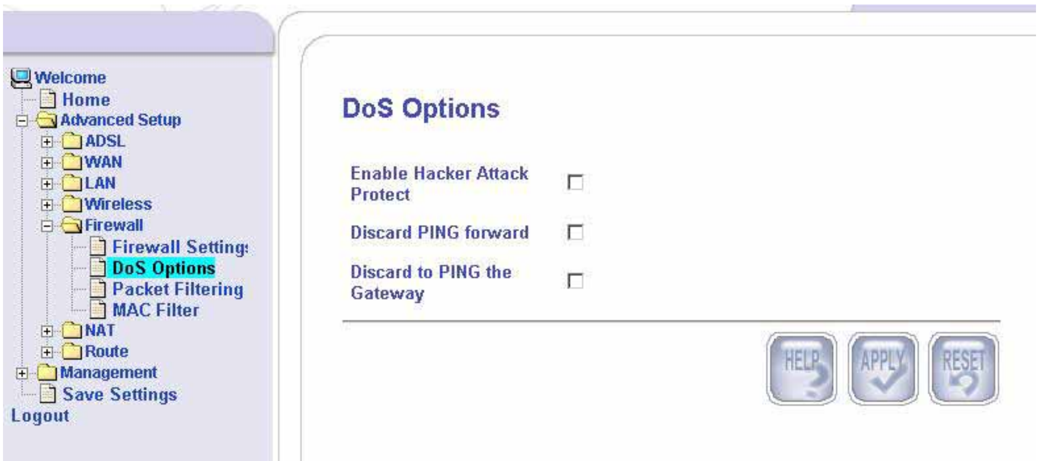
Firewall Settings

○ Enable ● Disable

DoS Options

This page lets you configure DoS (Denial of Service) firewall options. Options include the following–

- Enable Hacker Attack Protect–if this box is checked, then all hacker attack events are logged and dropped.
- Discard PING Forward–if this box is checked, then all PING from the WAN side are dropped.
- Discard PING the Gateway–if this box is checked, then all PING from the router LAN side is dropped.



DoS Options

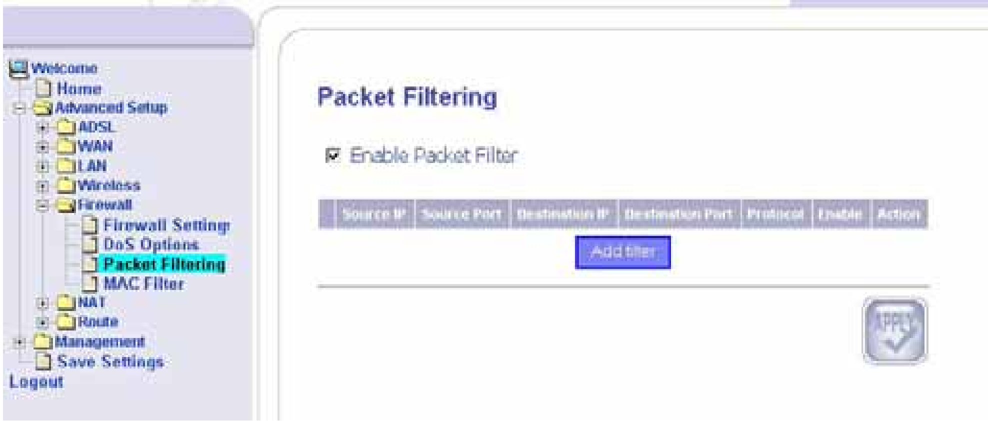
Enable Hacker Attack Protect □

Discard PING forward □

Discard to PING the Gateway □

Packet Filtering

This page allows you to permit or deny network traffic based on the data source, destination, service or protocol of the data packets. To set a filter, make sure that *Enable Packet Filter* is checked and then click on *Add* to proceed.

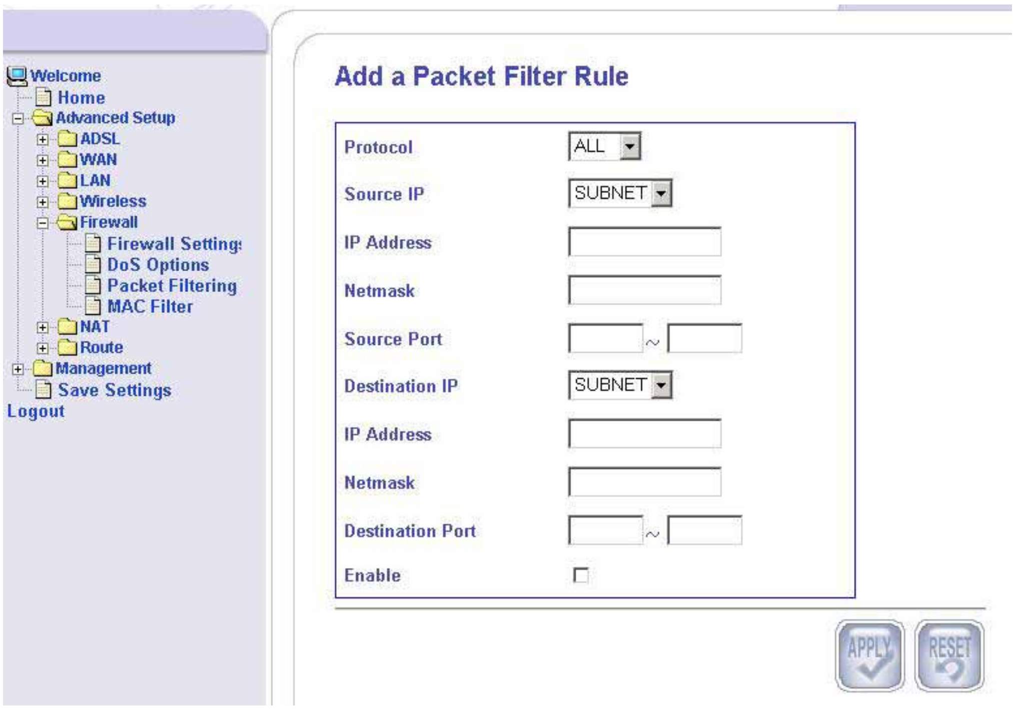


Packet Filtering

☑ Enable Packet Filter

Source IP	Source Port	Destination IP	Destination Port	Protocol	Enable	Action

Then you will continue to the below screen which allows you to enter the rule by which you wish to filter incoming data packets.



Add a Packet Filter Rule

Protocol	ALL
Source IP	SUBNET
IP Address	
Netmask	
Source Port	~
Destination IP	SUBNET
IP Address	
Netmask	
Destination Port	~
Enable	□

Select from the following protocols–

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

- ICMP (Internet Control Message Protocol)
- AH (Authentication Header)
- ESP (Encapsulation Security Protocol)
- ALL–all protocols

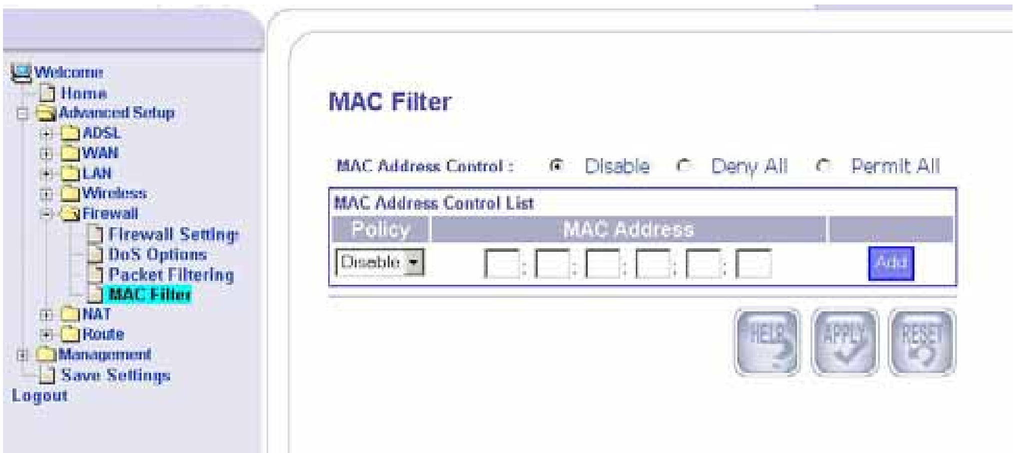
When a source host sends secure datagrams to a destination host, it does so with either the AH protocol or with the ESP protocol. The AH protocol provides source authentication and data integrity but does not provide secrecy. The ESP protocol provides data integrity and secrecy.

- Source IP / Destination IP–select from all, single, or subnet
- IP Address-- this is the IP address of the host from where the packet is coming from and where the packet is going.
- Netmask–this is the subnet mask of the source and destination of the packet.
- Source Port / Destination Port–enter the port numbers of the packet's source and destination.
- Enable–click if you want to enable packet filtering.

MAC Filter

To control traffic by using MAC addresses, configurations can be set as follows–

For MAC Address Control, select disable if you do not want to filter by MAC addresses at all. Selecting Deny All means that you will not allow any MAC addresses to enter and Permit All means that you will let all MAC addresses to enter. The MAC Address Control List allows you to control certain MAC addresses by permitting or denying their access.



MAC Filter

MAC Address Control : ● Disable ○ Deny All ○ Permit All

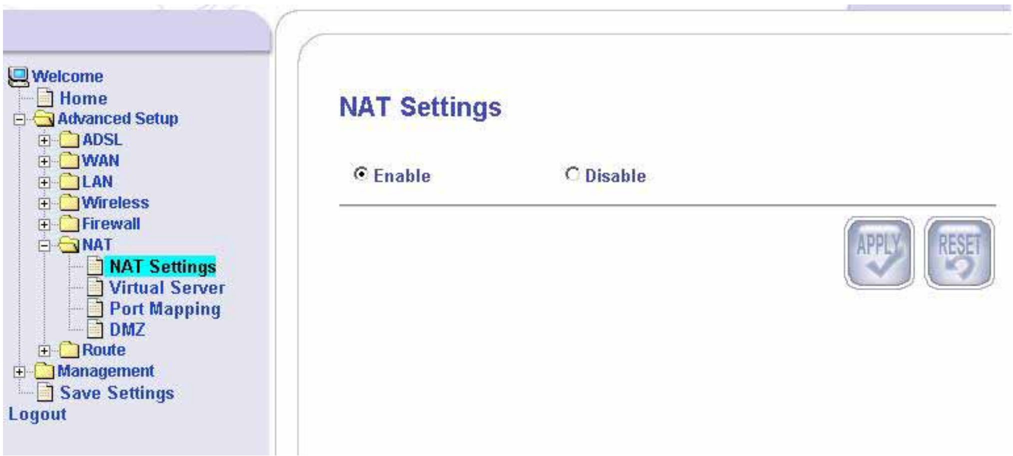
MAC Address Control List

Policy	MAC Address	
Disable	__ : __ : __ : __ : __ : __	Add

NAT

NAT Settings

NAT (Network Address Translation) is a technique in which the source and/or destination address of IP packets are rewritten as they pass through a router or firewall. Generally, it is used to allow several hosts on a private network to access the Internet using a single public IP address. This screen allows you to enable or disable NAT.

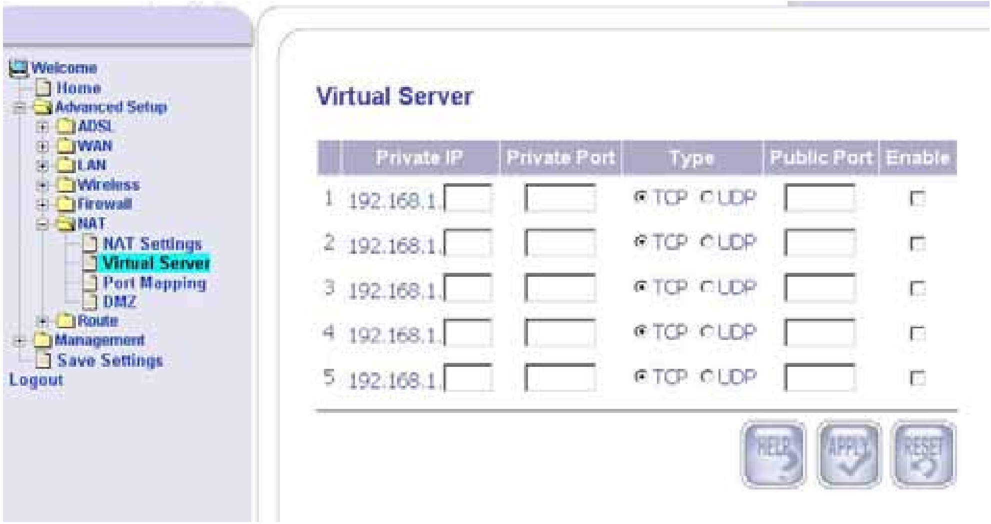


NAT Settings

● Enable ○ Disable

Virtual Server

Your router has the option to be configured as a virtual server. The private IP and private port is the LAN IP and port number that the public port is redirected to. The WAN side will only see the public port. Depending on the requested service (TCP / UDP port number), the router will redirect the external service request to the appropriate server.



Virtual Server

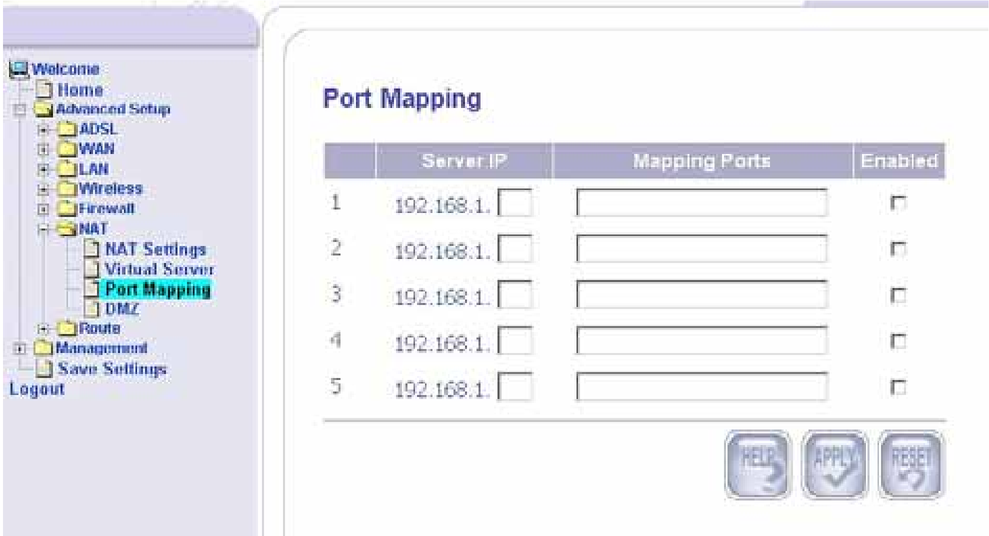
	Private IP	Private Port	Type	Public Port	Enable
1	192.168.1.		● TCP ○ UDP		□
2	192.168.1.		● TCP ○ UDP		□
3	192.168.1.		● TCP ○ UDP		□
4	192.168.1.		● TCP ○ UDP		□
5	192.168.1.		● TCP ○ UDP		□

Port Mapping

Port Mapping allows WAN clients to access services on the LAN by controlling the incoming port ranges assigned to the server IP. The LAN side acts as the server and the WAN side acts as the client. Enter the IP address of the LAN and a set or a range of port numbers that you will allow to access the specific server.

The Port Mapping screen has several fields that need to be filled out before the setup is complete. Below is the required information–

- Server IP–the IP address of the local machine.
- Mapping Ports–a range of ports or a specified port where packets are to be routed.
- Enabled–to enable a specified entry of the port mapping.



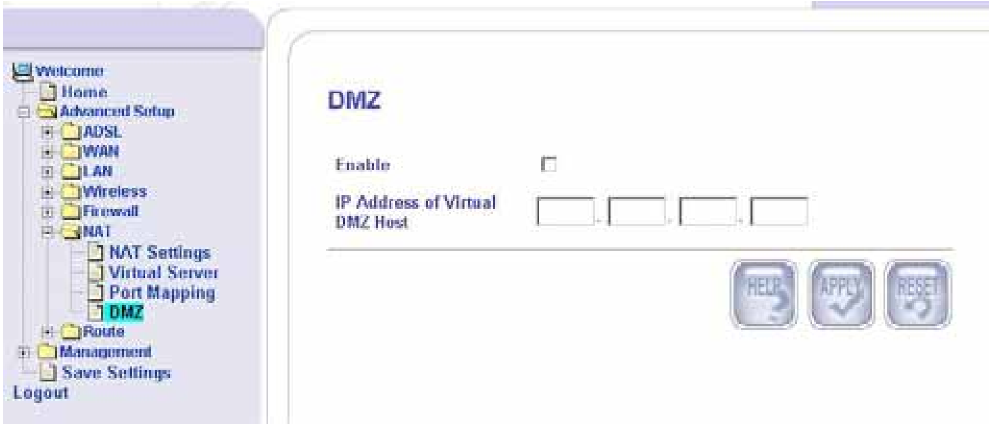
Port Mapping

	Server IP	Mapping Ports	Enabled
1	192.168.1.		□
2	192.168.1.		□
3	192.168.1.		□
4	192.168.1.		□
5	192.168.1.		□

DMZ

DMZ (demilitarized zone) allows contained hosts to provide services to the external network, while protecting the internal network from possible intrusions into those hosts.

Click to enable and then enter the IP address of the DMZ host.



DMZ

Enable □

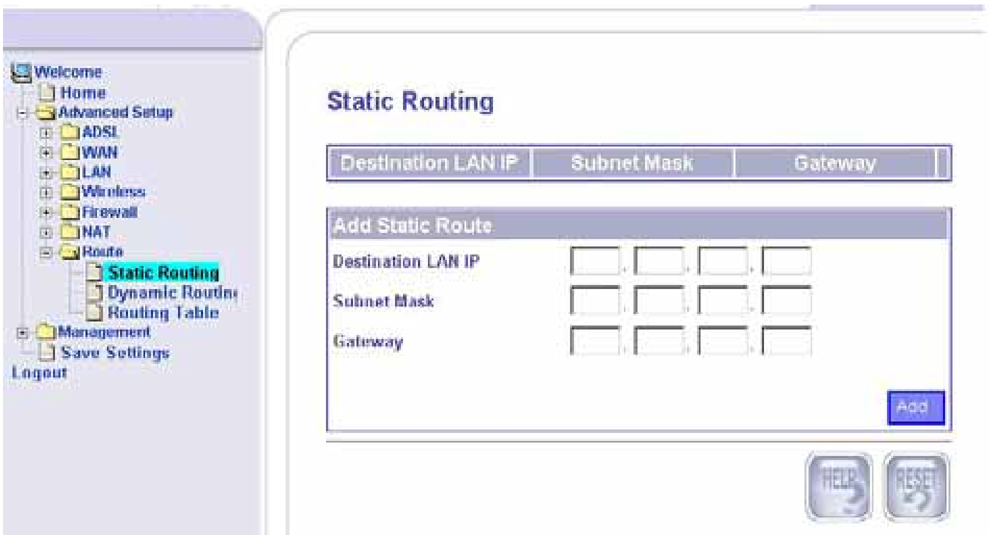
IP Address of Virtual DMZ Host □.□.□.□

Route

Static Routing

To add a static route, you will need to enter the following information–

- Destination LAN IP
- Subnet Mask
- Gateway



Static Routing

Destination LAN IP	Subnet Mask	Gateway

Add Static Route

Destination LAN IP □.□.□.□

Subnet Mask □.□.□.□

Gateway □.□.□.□

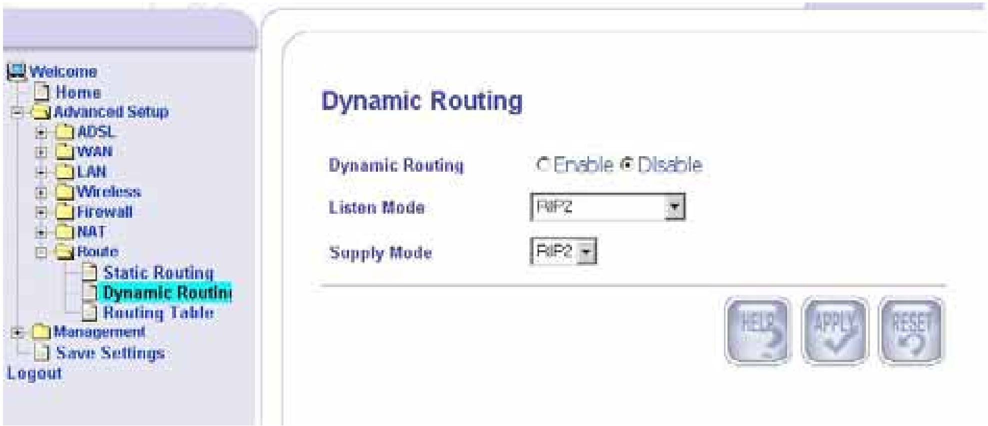
Dynamic Routing

Dynamic routing can be enabled or disabled here. If you enable, then select the listen mode to be used. Selections include the following–

- RIP1

- RIP2
- Both (RIP1 + RIP2)

Also needed is the supply mode, which include RIP1 and RIP2. When finished, click on Apply to save the selections.



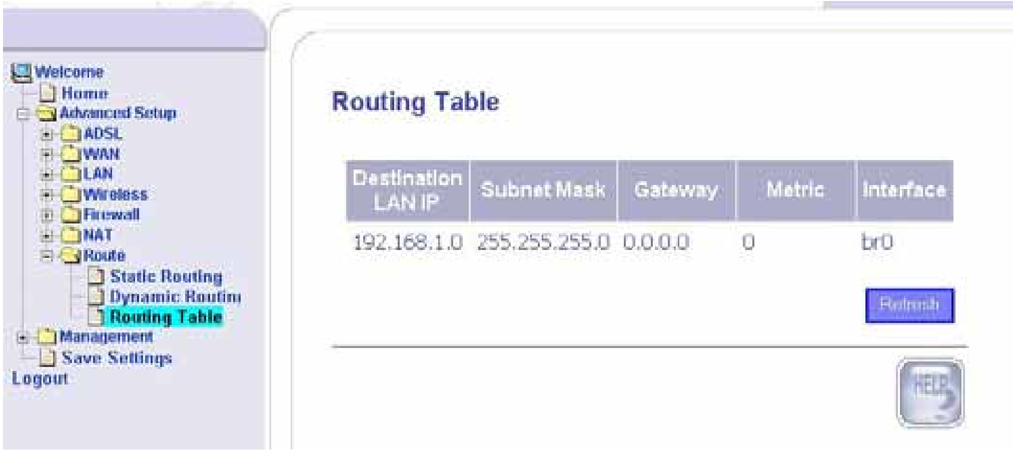
Dynamic Routing

Dynamic Routing ○ Enable ● Disable
Listen Mode RIP2
Supply Mode RIP2

Routing Table

The routing table is an informational page that allows you to see how many routings are on your routing table. The table displays the following information–

- Destination LAN IP
- Subnet mask
- Gateway
- Metric–this counts the number of hops.
- Interface



Routing Table

Destination LAN IP	Subnet Mask	Gateway	Metric	Interface
192.168.1.0	255.255.255.0	0.0.0.0	0	br0

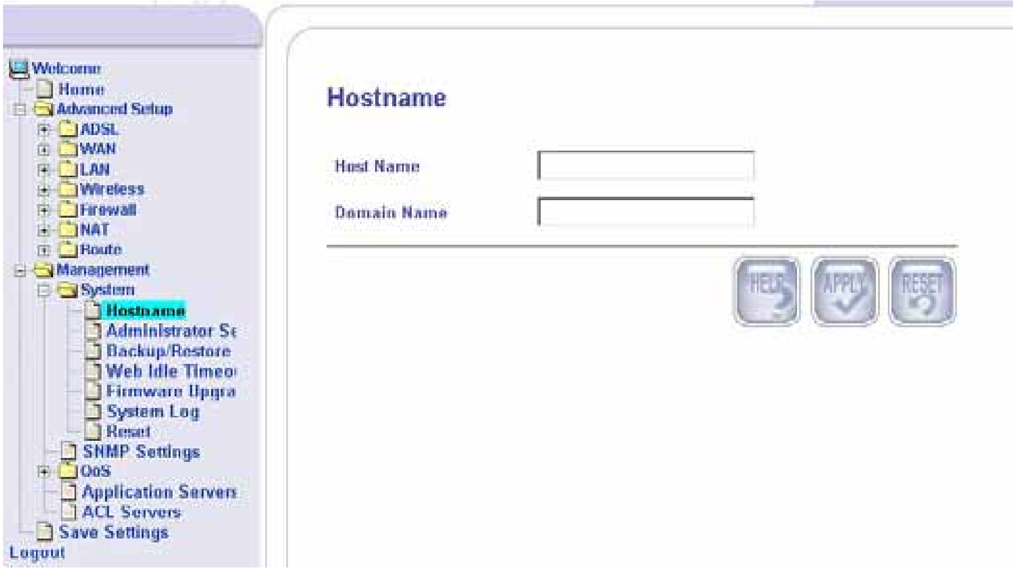
Management

This section of the router allows you to set up any controls you may want to have on your network as well as to maintain the system with firmware upgrades, etc. Also in this section is the system log that allows you to view system information.

System

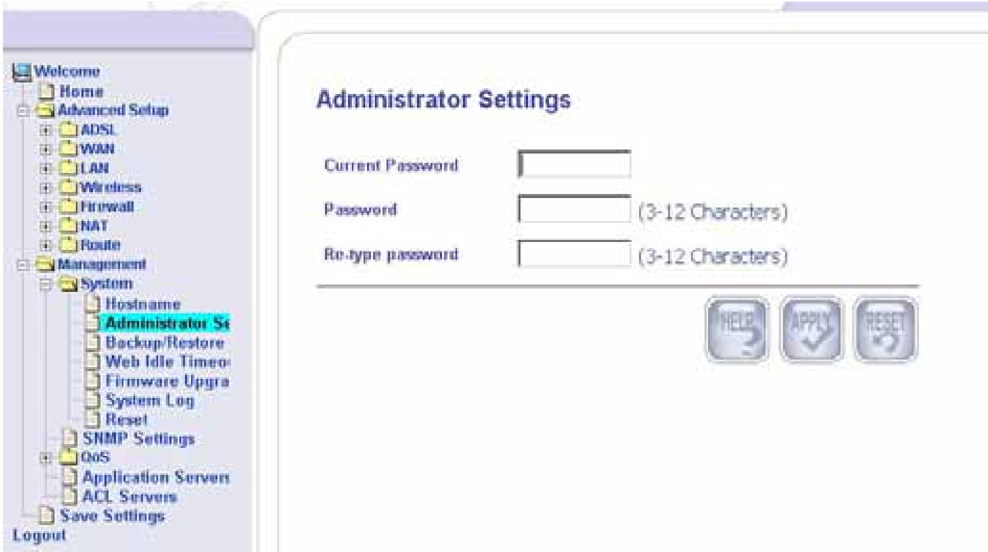
Hostname

Enter the hostname representing your host and the domain name so you won’t have to enter the IP address anymore and only need to type the hostname.



Administrator Settings

To set a password so you can restrict management access to your router, enter the current password and the new password that you wish to change to and reconfirm it again.



Administrator Settings

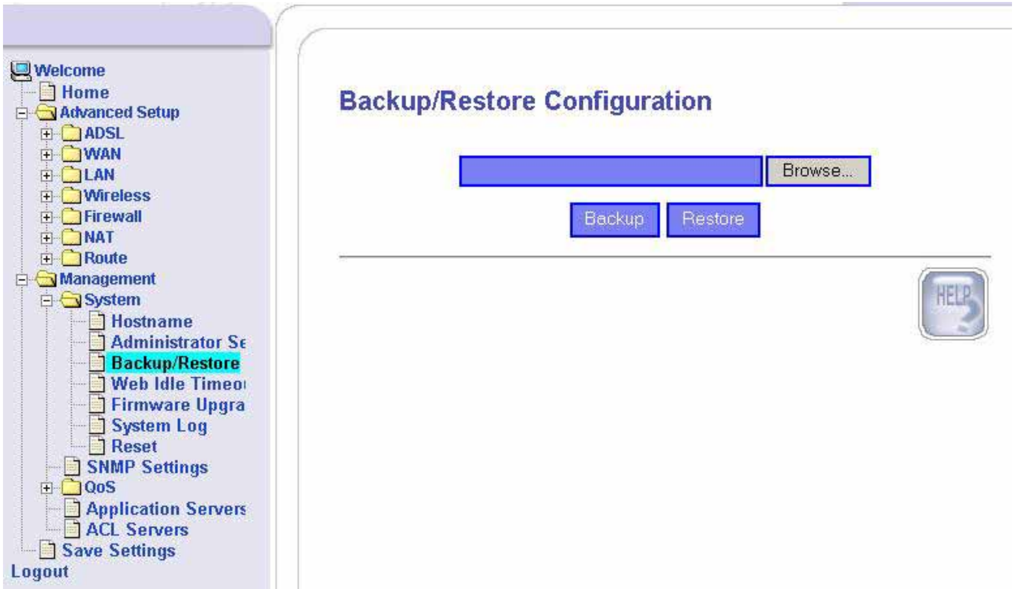
Current Password

Password (3-12 Characters)

Re-type password (3-12 Characters)

Backup / Restore

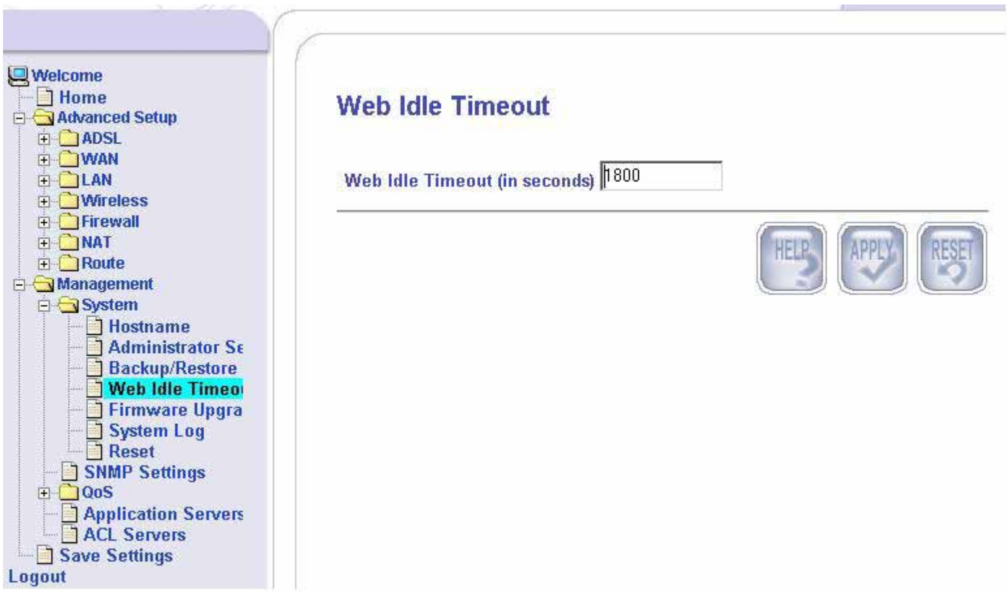
This page allows you to save a backup copy of your configurations or to restore previously saved configurations.



Backup/Restore Configuration

Web Idle Timeout

This page allows you to set the number of minutes (in seconds) that the router will log due to inactivity.

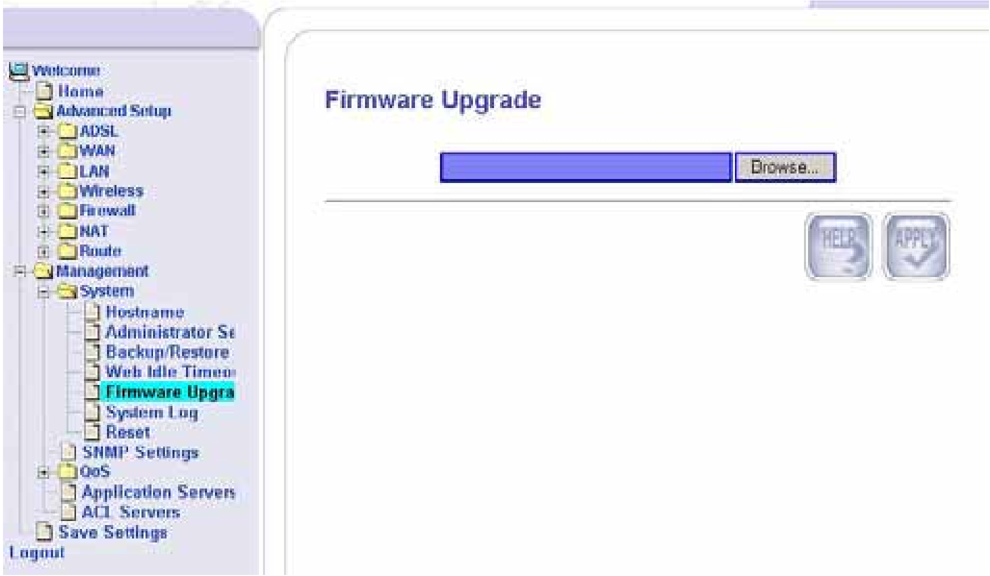


Web Idle Timeout

Web Idle Timeout (in seconds) 1800

Firmware Upgrade

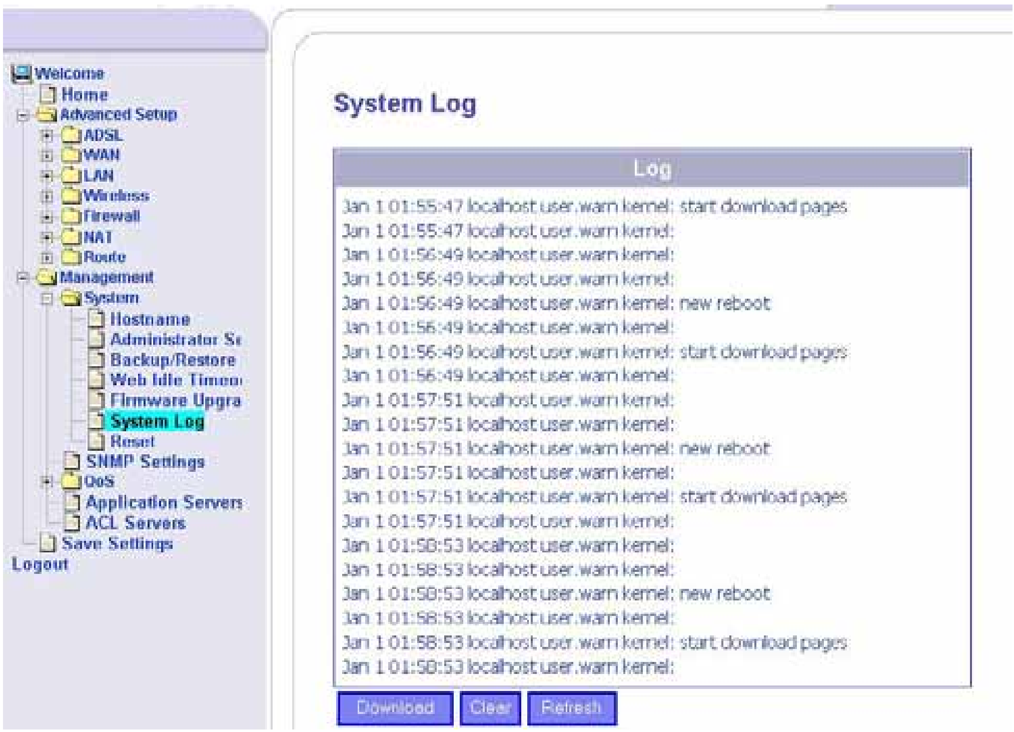
To upgrade the router with the newest firmware, click **Browse** to find the file on your pc (after downloading it from the firmware site). Then click on **Apply** to continue with the upgrade.



Firmware Upgrade

System Log

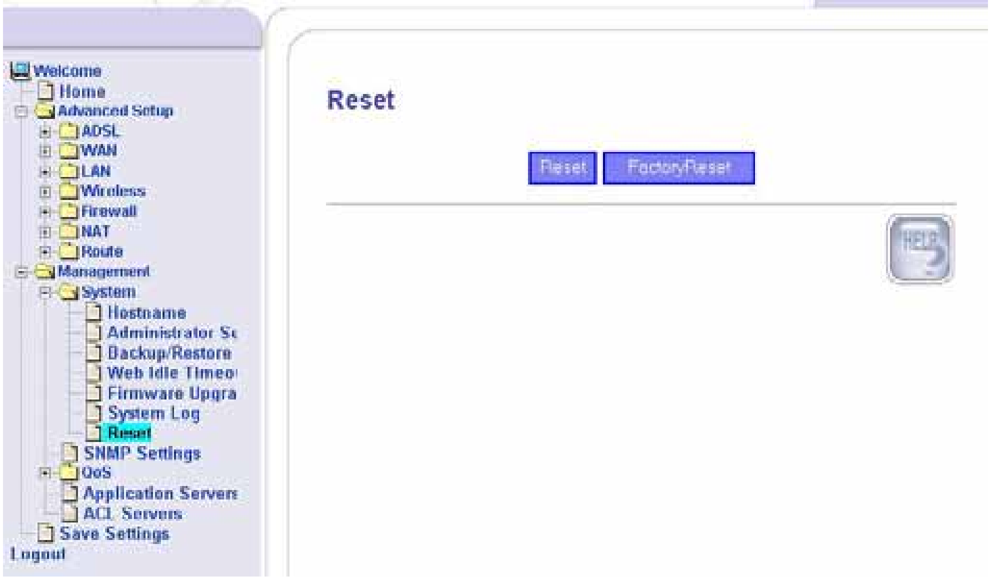
This screen shows a log of the system's activity.



```
Jan 1 01:55:47 localhost user.warn kernel: start download pages
Jan 1 01:55:47 localhost user.warn kernel:
Jan 1 01:56:49 localhost user.warn kernel:
Jan 1 01:56:49 localhost user.warn kernel:
Jan 1 01:56:49 localhost user.warn kernel: new reboot
Jan 1 01:56:49 localhost user.warn kernel:
Jan 1 01:56:49 localhost user.warn kernel: start download pages
Jan 1 01:56:49 localhost user.warn kernel:
Jan 1 01:57:51 localhost user.warn kernel:
Jan 1 01:57:51 localhost user.warn kernel:
Jan 1 01:57:51 localhost user.warn kernel: new reboot
Jan 1 01:57:51 localhost user.warn kernel:
Jan 1 01:57:51 localhost user.warn kernel: start download pages
Jan 1 01:57:51 localhost user.warn kernel:
Jan 1 01:58:53 localhost user.warn kernel:
Jan 1 01:58:53 localhost user.warn kernel:
Jan 1 01:58:53 localhost user.warn kernel: new reboot
Jan 1 01:58:53 localhost user.warn kernel:
Jan 1 01:58:53 localhost user.warn kernel: start download pages
Jan 1 01:58:53 localhost user.warn kernel:
```

Reset

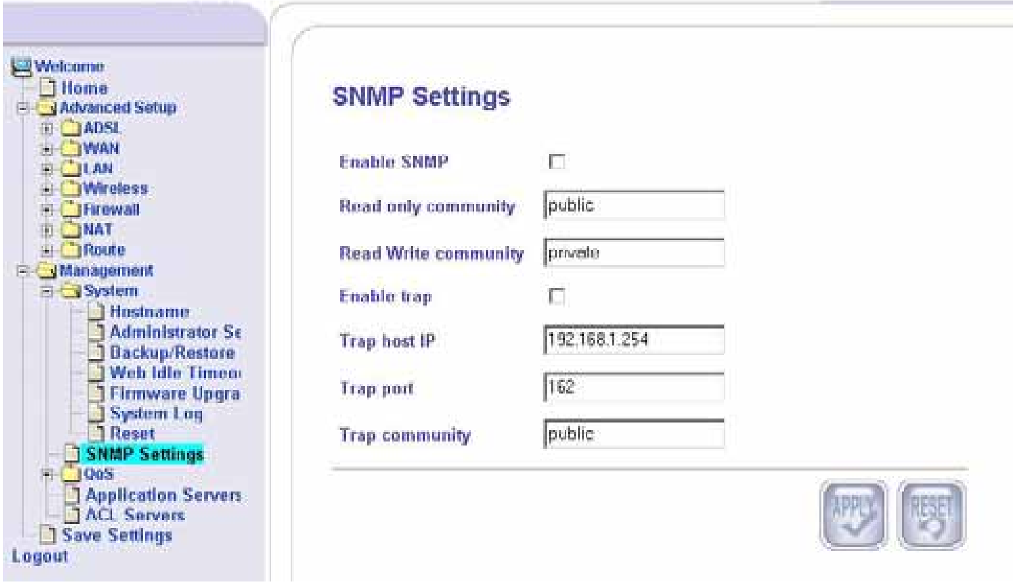
To reset the router without changing all the configured settings, click on **Reset**. To reset the router back to its factory settings, click on **Factory Reset**.



SNMP Settings

SNMP (Simple Network Management Protocol) settings can be accessed here. Settings here include the following–

- Enable SNMP–to enable this feature, click the box.
- Read Only Community--The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to device. The router is shipped with a default password of "public". It’s a good idea to change the community string to keep intruders from getting information about the network setup. Even if it's only read-access, SNMP can divulge a lot of information about the network that could be used to compromise it.
- Read Write Community–this is set to private (this should never be set to public).
- Enable Trap–to enable the trap, click the box. A SNMP Trap is an unsolicited message from a device to an SNMP console that the device is in an interesting state. Traps might indicate power-up or link-up/down conditions temperatures exceeding certain thresholds, high traffic, etc. Traps provide an immediate notification for an event that might only be discovered during occasional polling.
- Trap Host IP–the IP address of the trap host.
- Trap Port–the port number of the trap host.
- Trap Community–public or private.



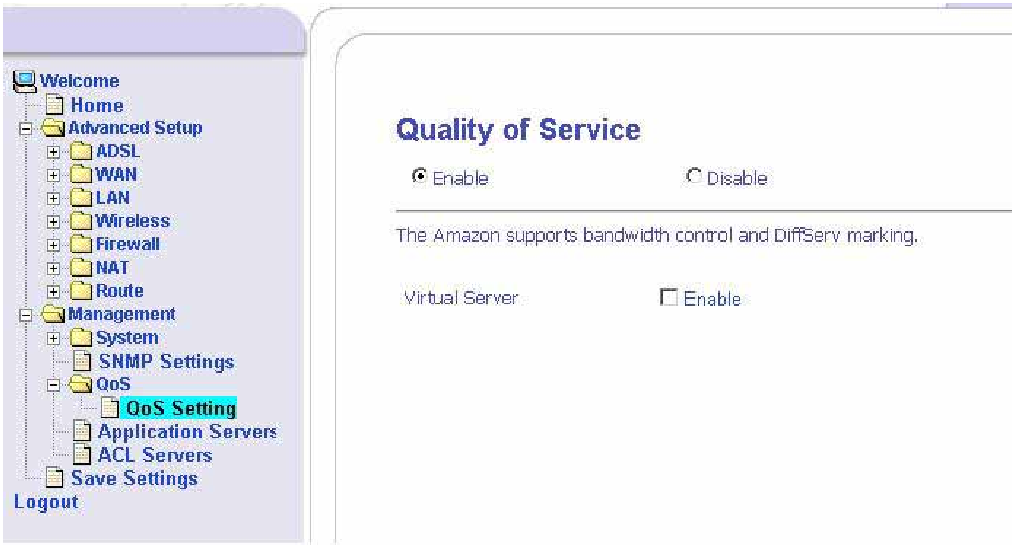
SNMP Settings

Enable SNMP	□
Read only community	public
Read Write community	private
Enable trap	□
Trap host IP	192.168.1.254
Trap port	162
Trap community	public

QoS *(Under Development)*

QoS Settings

This screen allows you to enable or disable quality of service for your router. You can also enable or disable the bandwidth control and DiffServ marking.



Quality of Service

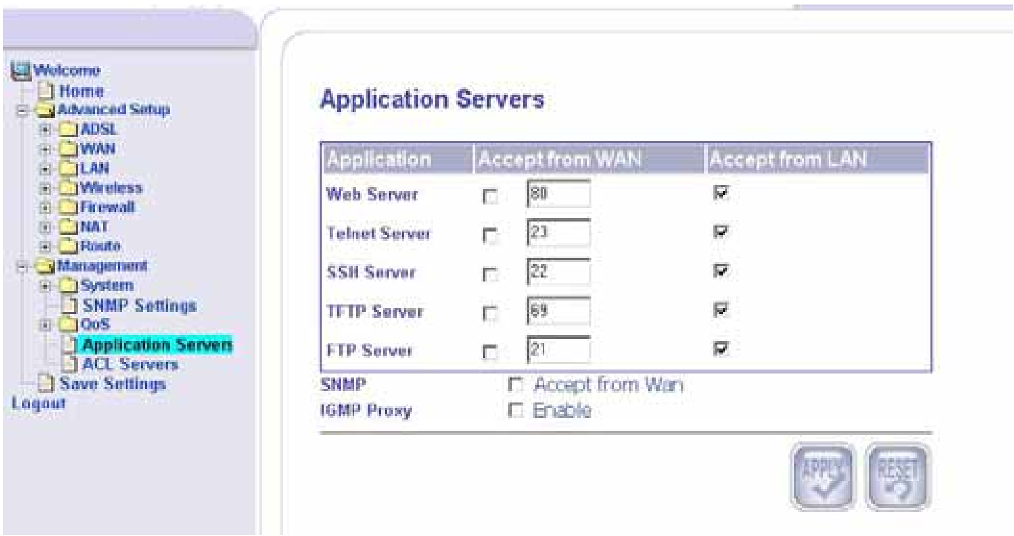
● Enable ○ Disable

The Amazon supports bandwidth control and DiffServ marking.

Virtual Server □ Enable

Application Servers

To configure application server settings, for each of the listed applications, select whether or not to accept from the WAN and/or LAN and enter the port number assigned. Also, if you want to enable the IGMP (Internet Group Management Protocol) Proxy, click on the **Enable** box.



Application Servers

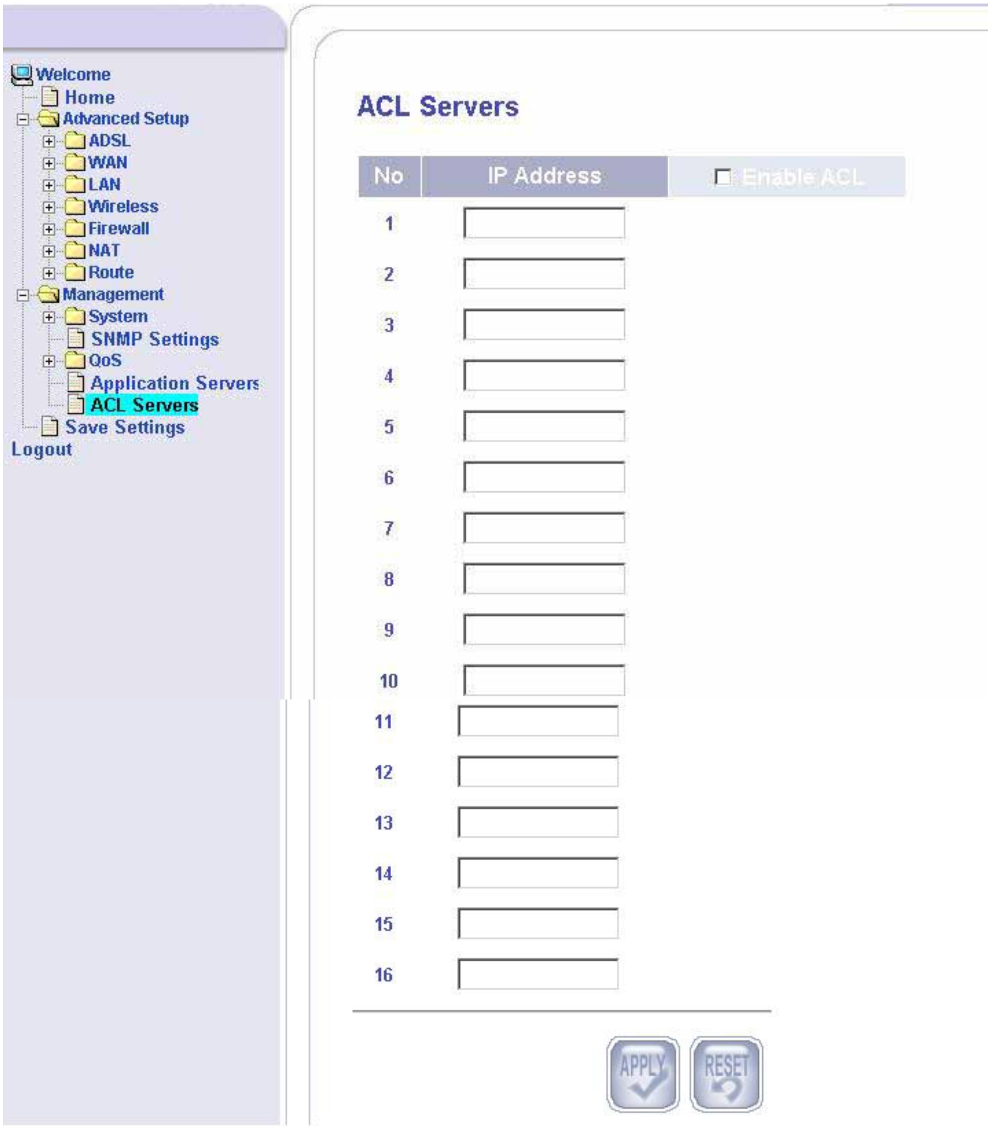
Application	Accept from WAN		Accept from LAN
Web Server	□	80	☑
Telnet Server	□	23	☑
SSH Server	□	22	☑
TFTP Server	□	69	☑
FTP Server	□	21	☑

SNMP □ Accept from Wan

IGMP Proxy □ Enable

ACL Servers

The ACL (Access Control List) Server page allows you to enter the IP addresses that you will allow to access your router.



ACL Servers

No	IP Address	□ Enable ACL
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		

Appendix

FCC Warning Statement

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

This equipment has been tested and found to comply with thelimits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
--- Reorient or relocate the receiving antenna.
--- Increase the separation between the equipment and receiver.
--- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
--- Consult the dealer or an experienced radio/TV technician for help.

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

This device and its antenna(s) must not be co-located or operating in onjunction with any other antenna or transmitter

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna.

Declaration of Conformity for R&TTE directive 1999/5/EC

Essential requirements – Article 3
Protection requirements for health and safety – Article 3.1a
Testing for electric safety according to EN 60950 has been conducted. These are considered relevant and sufficient. Protection requirements for electromagnetic compatibility – Article 3.1b
Testing for electromagnetic compatibility according to EN 301 489-1 and EN 301 489-17 has been conducted. These are considered relevant and sufficient.
Effective use of the radio spectrum – Article 3.2
Testing for radio test suites according to EN 300 328 has been conducted. These are considered relevant and sufficient.

CE Mark Warning

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