CWR-901

54Mbps Wireless-G Router

User's Guide

1 INTRODUCTION 4

Installing The Wireless Router 4
System Requirements 4
Installation Instructions 4

2 PREPARING THE NETWORK 6

Preparing the Network 6
Collecting ISP Information 6
Configuring Windows for IP Networking 6

3 CONFIGURING THE WIRELESS-G ROUTER 12

3.1 Setup Wizard 12
3.1.1 Time Zone Settings 13
3.1.2 LAN Interface Setup 13
3.1.3 WAN Interface Setup 14
3.1.4 Wireless Basic Settings 15
3.2 LAN Settings 15
3.3 WAN Settings 16
3.3.1 Static IP 16
3.3.2 DHCP Client 17
3.3.3 PPPoE 17
3.3.4 WAN type: Unnumbered PPPoE 18
3.3.5 PPTP 20
3.3.6 L2TP 21
3.3.7 DHCP + L2TP 22
3.4 Wireless 22
3.4.1 Basic Settings 22
3.4.2 Advanced Settings 23
3.4.3 Security 25
3.4.4 Access Control 28
3.4.5 WDS 29
3.5 Firewall 30
3.5.1 Access Control list 30
3.5.2 URL Filter 31
3.5.3 ALG 31
3.5.4 Anti-DoS 32
3.5.5 UDP Blocking 34
3.5.6 Protocol-based NAT 35
3.5.7 NAPT options 35
3.6 VPN Settings 36
3.7 QoS Settings 38
3.7.1 Port/L4 App Based QoS 38
3.7.2 Rate Policing QoS 39
3.8 Advanced 40
3.8.1 Port Forwarding 40
3.8.2 Static Route 40
3.8.3 RIP 41
3.8.4 Dynamic DNS 42
3.8.5 Special Application 42
3.8.6 DMZ Host 43
3.8.7 Ping toolkit 44
3.8.8 Pseudo-VLAN 44
3.8.9 PPPoE/IPv6 Passthru 45
3.8.10 IP Multicast 45
3.8.11 Samba Server 45
3.9 Management 46
3.9.1 Status 46

3.9.2 DHCP Settings *48*
3.9.3 Password *49*
3.9.4 Time Zone Settings *49*
3.9.5 Upgrade Firmware *50*
3.9.6 Remote Management *50*
3.9.7 Reload Settings *51*
3.9.8 System Restart *51*
3.10 EVENT LOG 51
3.10.1 System Log *52*
3.10.2 ACL Log *52*
3.10.3 URL Filter Log *52*
3.10.4 DoS Log *52*
3.10.5 New Connection Log *53*
APPENDIX A: TROUBLESHOOTING 54
APPENDIX B: FREQUENTLY ASKED QUESTIONS 57

1 Introduction

Installing the Wireless Router

In this chapter, you'll learn how to connect your wireless router.

System Requirements

- One or more PCs (desktop or notebook) with Ethernet interface
- Broadband Internet access
- Ethernet cables
- Wireless interface (if planning to use wireless)

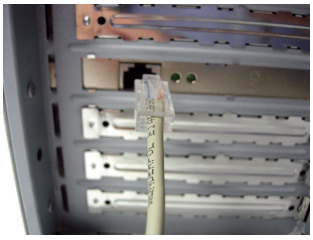
Installation Instructions

Connecting the Wireless Router:

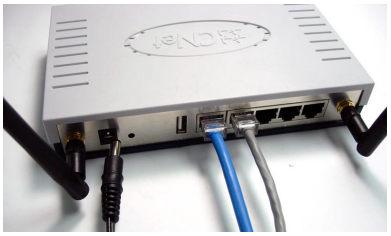
1. Make sure all **systems (**wireless router, PC(s), and the cable or DSL modem if applicable) are turned off,.

2. Connect the **WAN port** on the wireless router to the cable/**DSL** modem, Ethernet Server, or hub.

3. Connect one or more client PCs to **LAN port(s) on the router**.



4. Connect the power adapter to the **power jack** on the wireless router. Then, plug the power cable into a wall outlet.



5. Turn on your PC(s).

2 Preparing the Network

Preparing the Network

This section of the manual covers the tasks that are to be done before configuring the wireless router. First thing is to have all ISP information as described below and second is to make sure that all computers on the network are configured for TCP/IP networking.

Collecting ISP Information

The following information needs to be gathered from the ISP before configuring the wireless router:

- Is IP assignment static or dynamic? If static, what are the IP address, Subnet Mask, Default Gateway and DNS addresses used for this connection?
- Is the connection type PPPoE? If so, what are the PPPoE username and password?
  Call your ISP if you're not sure of the answers to these questions.

Configuring Windows for IP Networking

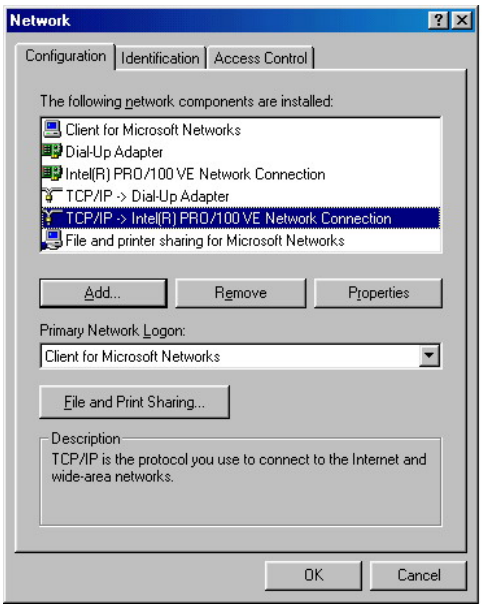
Each computer connecting to the router needs to be configured for TCP/IP networking. If you plan to use the DHCP where the router assigns IP addresses for local network, (recommended), you should configure each computer to obtain IP automatically. See the procedure below.

If you don't plan to use DHCP, you'll need to manually assign an IP address to each computer. Refer to your Windows documentation for instructions on IP assignment.

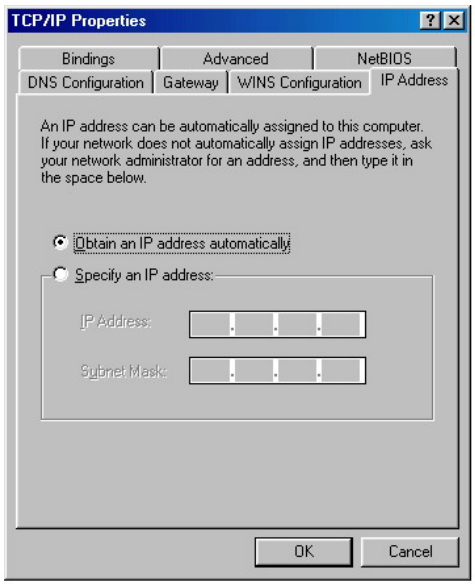
To configure Windows to receive dynamic IP address:

Configuring Windows 98 and Millennium PCs

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Double-click the **Network** icon.
2. On the Configuration tab, select the **TCP/IP** line for the applicable Ethernet adapter. Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN, or AOL. If the word **TCP/IP** appears by itself, select that line. Click the **Properties** button.



3. Click the **IP Address** tab. Select **Obtain an IP address automatically**



4. Now click the **Gateway** tab, and verify that the *Installed Gateway* field is Blank. Click the **OK** button.

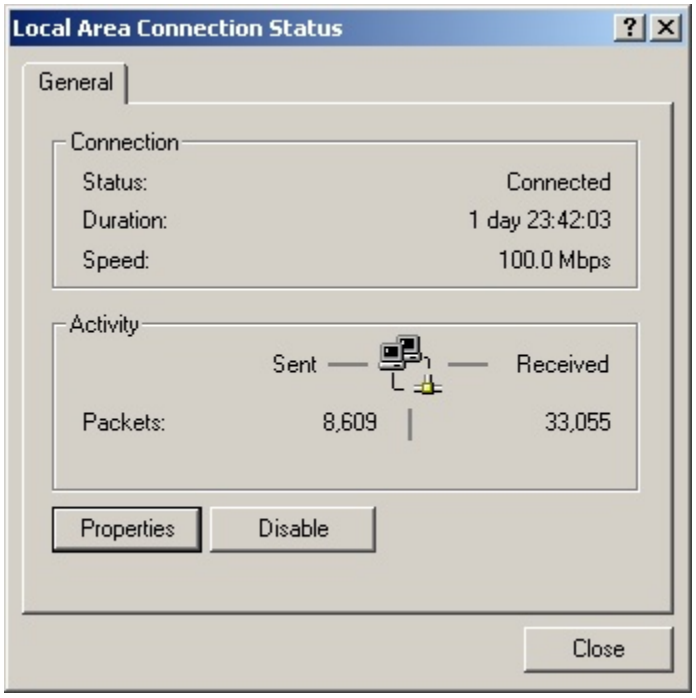
5. Click the **OK** button again. Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CDROM drive and check the correct file location, e.g., D:\win98, D:\win9x, etc. (if "D" is the letter of your CD-ROM drive).

6. Windows may ask you to restart your PC. Click the **Yes** button. If Windows does not ask you to restart, restart your computer anyway.

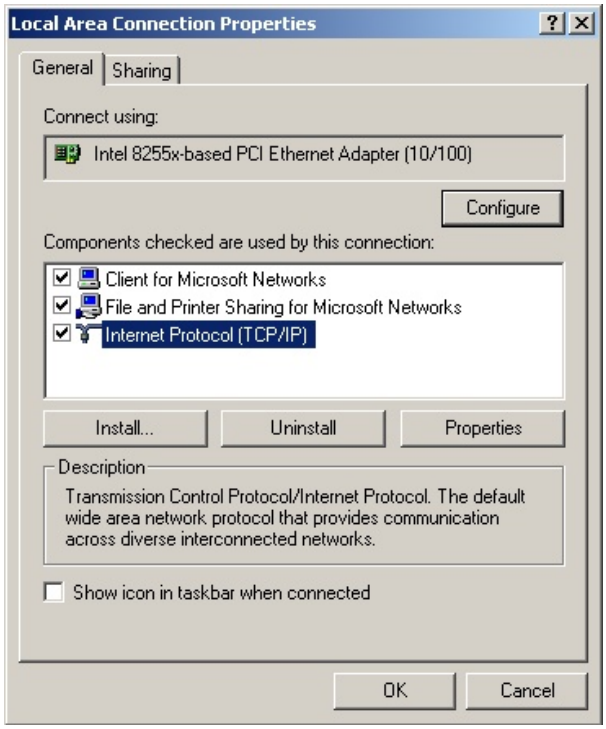
Configuring Windows 2000 PCs

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Double-click the **Network and Dial-up Connections** icon.

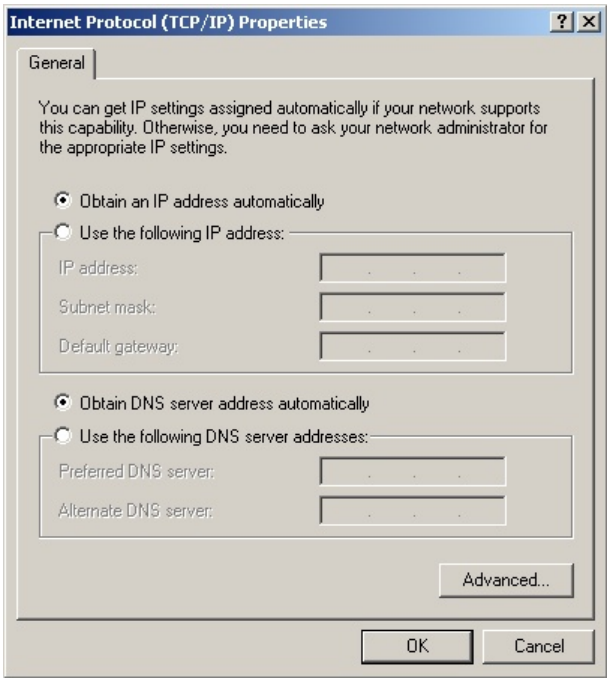
2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. Click the **Properties** button



3. Make sure the box next to *Internet Protocol (TCP/IP)* is checked. Highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button.



4. Select **Obtain an IP address automatically**. Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration.



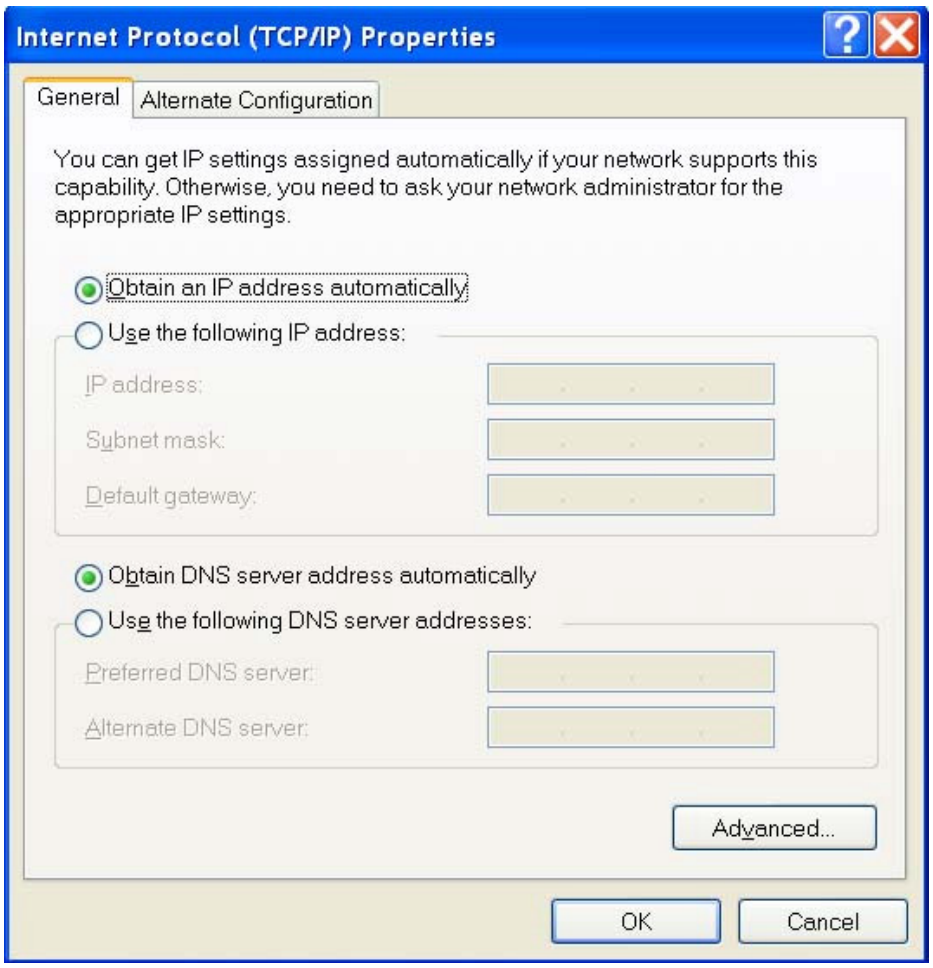
5. Restart your computer.

Configuring Windows XP PCs

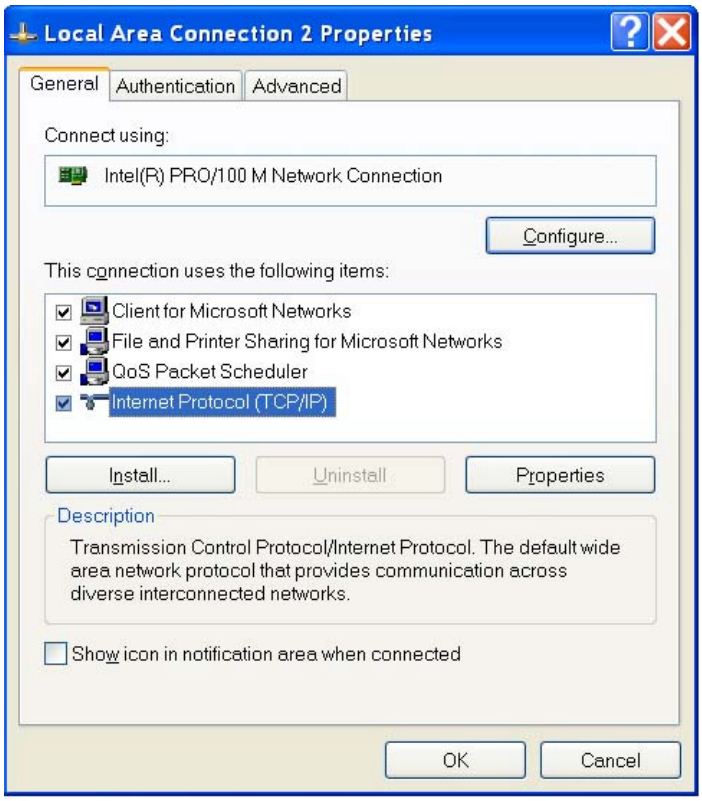
The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

1. Click the Start button and then the Control Panel icon. Click the Network and Internet Connections icon. Then click the Network Connections icon.

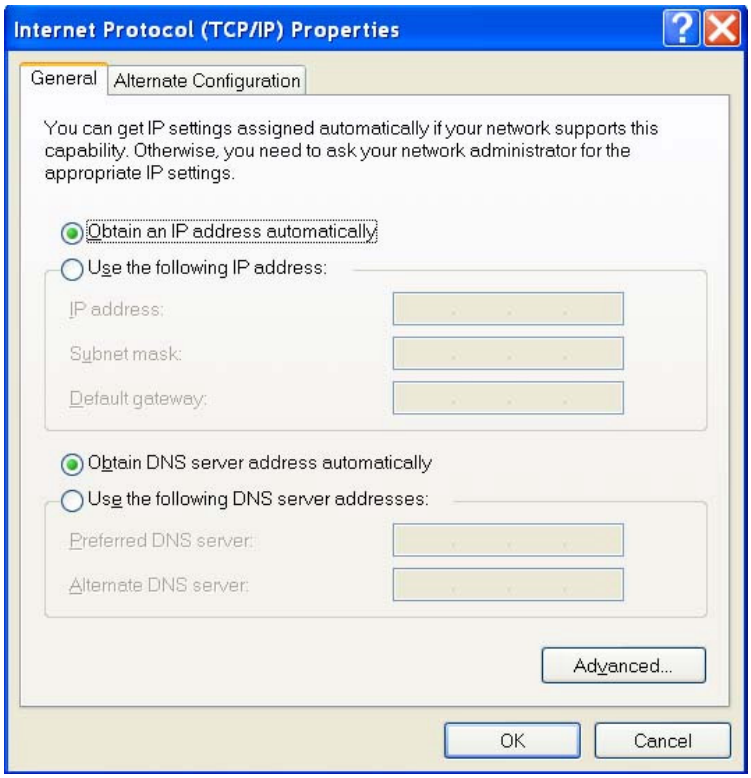
2. Select the Local Area Connection icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the Local Area Connection. Click the Properties button.



3. Make sure the box next to *Internet Protocol (TCP/IP)* is checked. Highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button.



4. Select **Obtain an IP address automatically**. Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration.

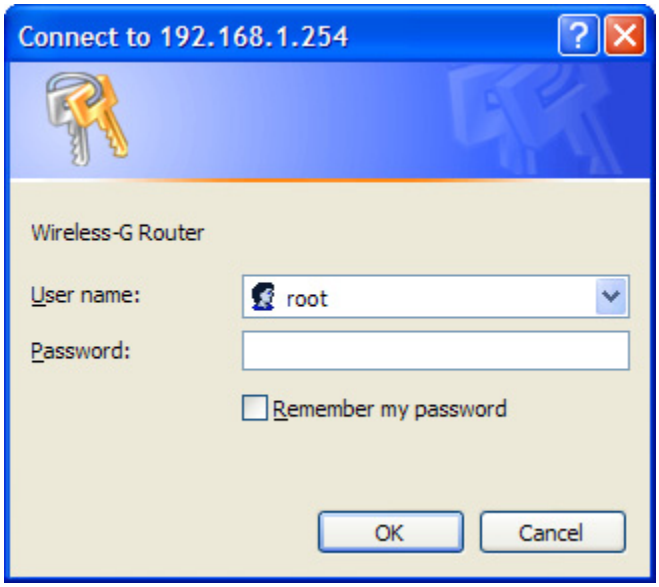


3 Configuring the Wireless-G Router

This chapter describes how to use the web management tool, a web browser-based utility that allows remotely configuring and managing this wireless router.

Open the Web browser and type the router's IP address "**http://192.168.1.254"** and press **<ENTER>**.

Enter the User name and Password when prompted, **default User name** is "**root**", and **default Password** is "**1234**".



3.1 Setup Wizard

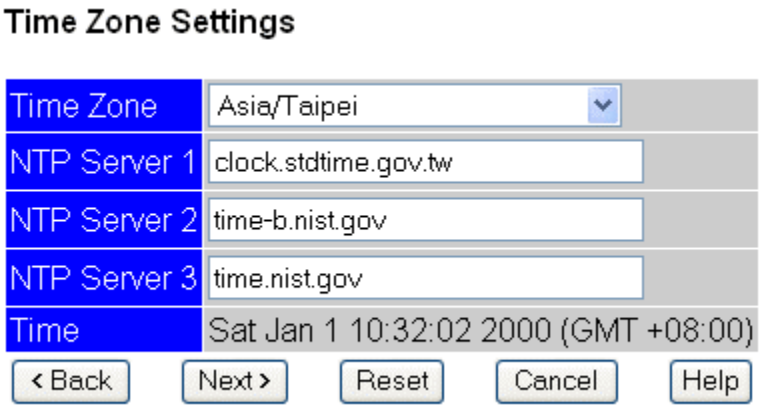
After a successful connection to the configuration web page, the setup page will be shown as in the figure below.

To make the installation easy, the wireless router offers a Setup Wizard that will go through the

configuration. Click on “**Next”** to continue.

3.1.1 Time Zone Settings

The first step in Setup Wizard is Time Zone Settings. Users can synchronize the local clock to an available NTP server. Enable NTP client update and select the correct Time Zone.

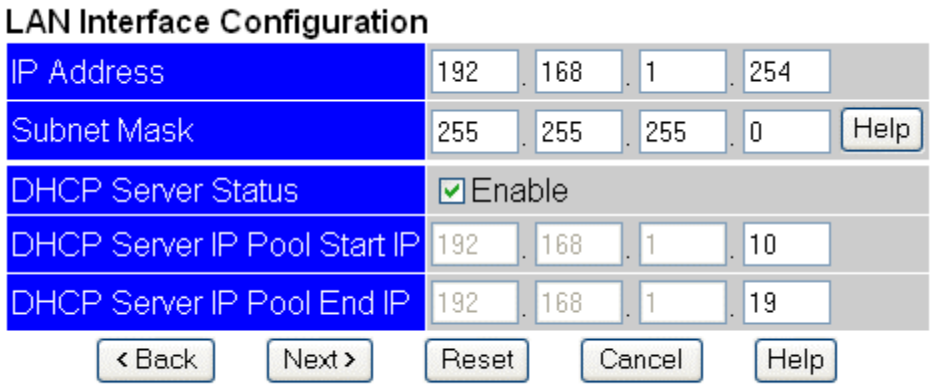


- **Time Zone Select**: Select the time zone of the country where this wireless router is located.
- **NTP server1**: Default NTP server address (clock.stdtime.gov.tw) .
- **NTP server2**: NTP server 2 (time-b.nist.gov).
- **NTP server3**: NTP server3 (time.nist.gov).
- **Back**: To skip current settings and go back to the last page.
- **Next:** Go to the next page.
- **Reset:** Click on “Reset” button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page.
- **Help**: To request help information.

After selecting the NTP server, click on “**Next**” button. LAN Interface Setup page is the next screen.

3.1.2 LAN Interface Setup

In the LAN interface Setup page, users can change the LAN IP address and Subnet Mask of the router. **Most Users will not need to change these values**.



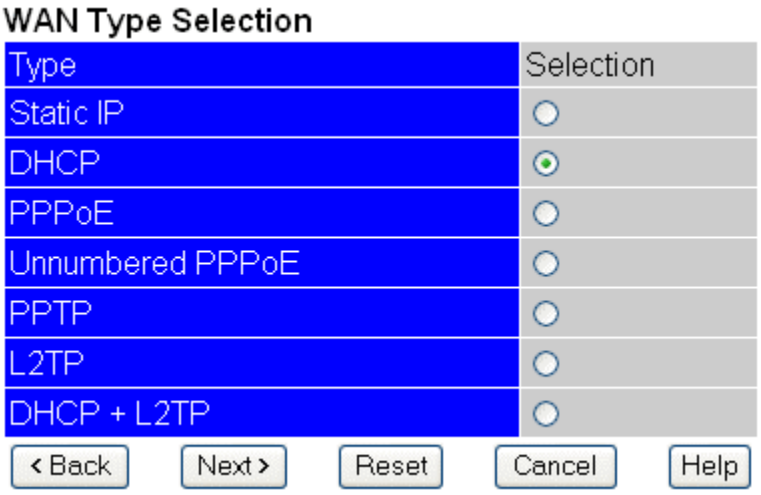
- **IP Address**: Enter IP address for this wireless router.

- **Subnet Mask**: Enter the subnet mask for this wireless router.
- **DHCP Server Status**: Select to enable the DHCP Server feature.
- **DHCP Server IP Pool Start IP**: Enter the Start IP address assigned by the DHCP server.
- **DHCP Server IP Pool End IP**: Enter the End IP address assigned by the DHCP server.
- **Back**: To skip the current settings and go back to the last page.
- **Next:** Go to the next page.
- **Reset:** Click on "Reset" button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page.
- **Help**: To request help information.

After typing in the IP Address and Subnet Mask, click on "**Next**" button to go to the WAN Interface Setup page.

3.1.3 WAN Interface Setup

The WAN Type Selection screen will pop up as below.



- **Back**: To skip the current settings and go back to the last page.
- **Next:** Go to the next page.
- **Reset:** Click on "Reset" button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page.
- **Help**: To request help information.

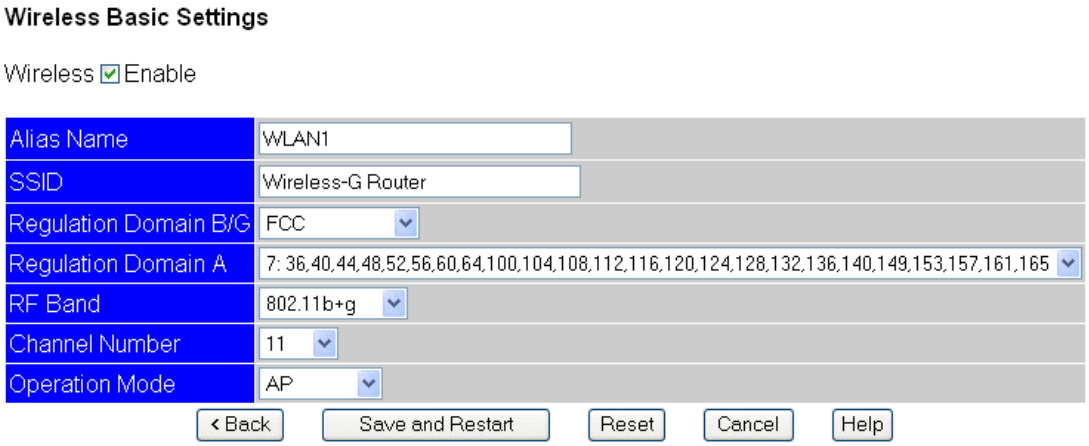
After specifying your WAN access type, click on "**Next**" button. The screen below will pop up.

- **Back**: To skip the current settings and go back to the last page.
- **Next:** Go to the next page.
- **Reset:** Click on "Reset" button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page.
- **Help**: To request help information.

Users have to fill up the data in the blank and then click “**Next**” button. You will enter the Wireless Basic Settings page.

3.1.4 Wireless Basic Settings

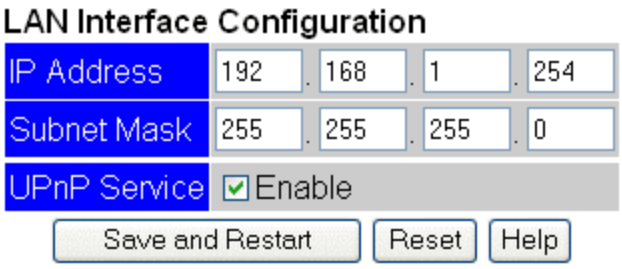
In the Wireless Basic Settings page, users can configure: “Alias Name”, “SSID”, “Regulation Domain B/G”, “RF Band”, “Channel Number”, and “Operation Mode”.



- **Alias Name**: Users can assign a unique name to this wireless router. The alias name is especially important for identification when there are more than one wireless router used in a network.
- **SSID**: The SSID differentiates one WLAN from another, therefore, all wireless routers and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters.
- **Regulation Domain B/G**: Different countries have different Regulation Domains for wireless 11b and 11g devices. There are six regulation domains: FCC, Canada, Europe, Spain, France and Japan.
- **RF Band**: This wireless router can support three RF bands: 11b+11g, 11b only and 11g only.
- **Channel Number**: The number of channels supported depends on the region of this wireless router. All stations communicating with this wireless router must use the same channel.
- **Operation Mode**: This wireless router can support two operation modes: AP and AP+WDS.
- **Back**: To skip the current settings and go back to the last page.
- **Save and Restart:** Save the parameters and reboot this wireless router.
- **Reset:** Click on “Reset” button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page
- **Help**: To request help information.

3.2 LAN Settings

“LAN Interface Setup” allows configuring the parameters for local area network connected to LAN ports of the wireless router.



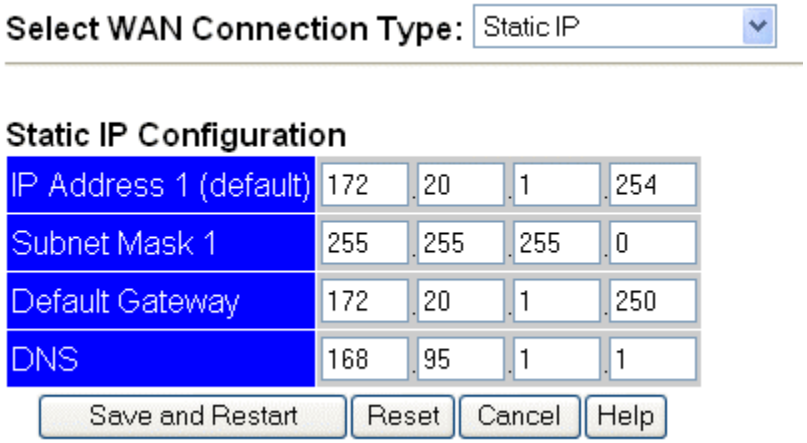
- **IP Address**: Default IP address of the wireless router.
- **Subnet Mask**: Default subnet mask for this wireless router.
- **Enable UPnP**: Users can enable or disable uPNP feature here. If enabled, all client systems that support uPNP, like Windows XP, can automatically discover the wireless router and access the Internet through it without any configuration.
- **Save and Restart:** Save the parameters and reboot the wireless router.
- **Reset:** Click on "Reset" button to undo your changes.
- **Help**: To request help information.

3.3 WAN Settings

"WAN Interface Setup" is the page to configure the parameters for the WAN port connecting to the Internet Service Provider. There are seven WAN access types supported by this router: Static IP, DHCP, PPPoE, Unnumbered PPPoE, PPTP, L2TP, and DHCP + L2TP:

3.3.1 Static IP

This is the connection type where the user has a static IP address from their service provider.. Select Static IP and enter the IP Address, Subnet Mask, Default Gateway and DNS Server associated with this connection.

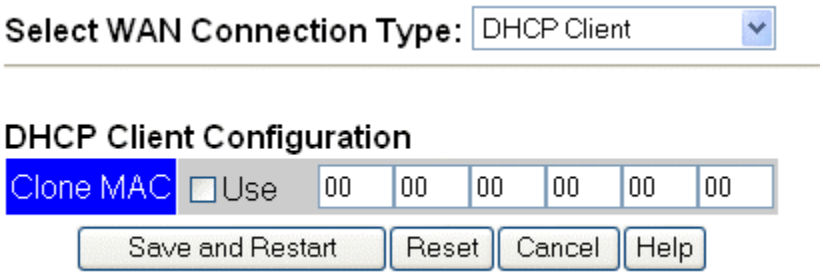


- **Select WAN Connection Type**: Select **Static IP** connection
- **IP Address 1(default)**: Enter the IP address assigned by ISP
- **Subnet Mask 1**: Enter the subnet mask provided by ISP
- **Default Gateway**: Enter the default gateway address provided by ISP
- **DNS**: Enter the DNS address provided by the service provider.
- **Save and Restart: S**ave the parameters and reboot the wireless router.
- **Reset:** Click on "Reset" button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page.

- **Help**: To request help information.

3.3.2 DHCP Client

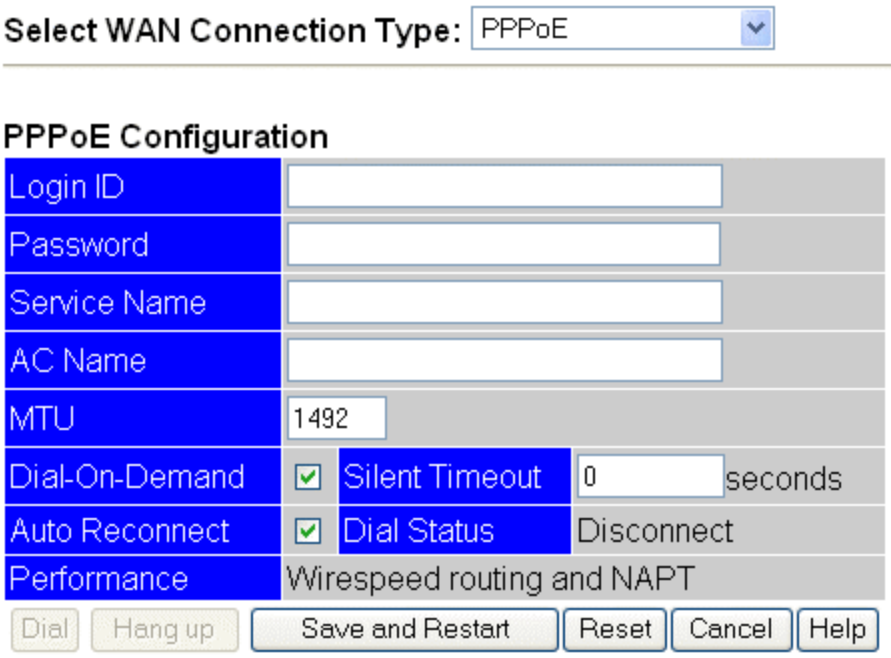
DHCP client also called “Dynamic IP Address” is the connection type offered by most cable broadband service providers. In this mode the WAN port will automatically receive all it’s parameters like IP, Subnet, Gateway and DNS addresses from the ISP.



- **Select WAN Connection Type**: Select **DHCP Client** connection
- **Clone MAC**: If the MAC address of a network card is used for authentication by an ISP, you may use “Clone MAC Address” to duplicate the network card’s MAC address to the MAC address of the router’s WAN port. Check the **Use** box and enter the NIC MAC address provided by ISP.
- **Save and Restart:** Save the parameters and reboot the wireless router.
- **Reset:** Click on “Reset” button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page.
- **Help**: To request help information.

3.3.3 PPPoE

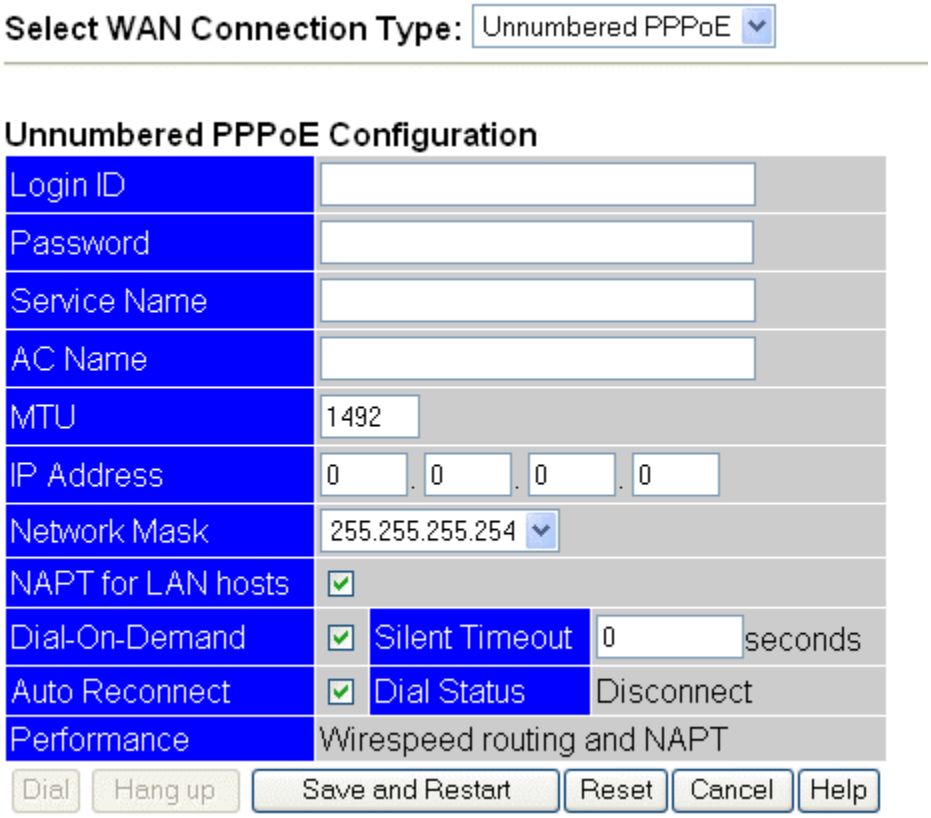
PPPoE stands for “Point-to-Point Protocol over Ethernet”. PPP is the technology used for dialup Internet access. PPPoE works similar to PPP except it works over a network connection. In this mode users need to enter their PPPoE username and password. Some ISPs also require a service name to be entered. Usually, the IP/DNS addresses are assigned dynamically. However, if users have a static IP through PPPoE, then they will need to enter IP and DNS addresses provided by the ISP.



- **Select WAN Connection Type**: Select **PPPoE** connection
- **Login ID**: Enter the login ID provided by ISP
- **Password**: Enter the Password provided by ISP
- **Service Name**: The Service Name set on the access concentrator. Many ISPs give user-name and address in the form of user-name@service-name. The Service Name provided by your ISP, if one is required, otherwise, leave it blank.
- **AC Name**: Access concentrator name provided by the ISP, if one is required, otherwise, leave it blank.
- **MTU**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, 1492, to have the wireless router select the best MTU for your Internet connection. Sometimes ISP sets different MTU size than 1492.
- **Dial-On-Demand**: If checked, the wireless router will only dial this session when a LAN -> WAN packet is received. If unchecked, it immediately dials the session when powered up.
- **Silent timeout**: Only used when connection type is set to **Dial-On-Demand.** The **Silent timeout** value is defined as the time for the WAN port to disconnect if the connection is idle (not used).
- **Auto Reconnect**: If checked, the wireless router redials the session if session previously terminated by ISP.
- **Dial Status**: Current status of the session. Maybe “connected”, “connecting” or “disconnect”.
- **Dial:** Click on this button to manually connect to ISP.
- **Hang Up:** Click on this button to disconnect the wireless router from ISP.
- **Save and Restart:** Save the parameters and reboot the wireless router.
- **Reset:** Click on “Reset” button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page.
- **Help**: To request help information.

3.3.4 WAN type: Unnumbered PPPoE

Unnumbered PPPoE WAN type is a required feature in Japan. ISP assigns Login ID and Password to users for login when connecting to Internet. Service Name and AC Name are usually optional.

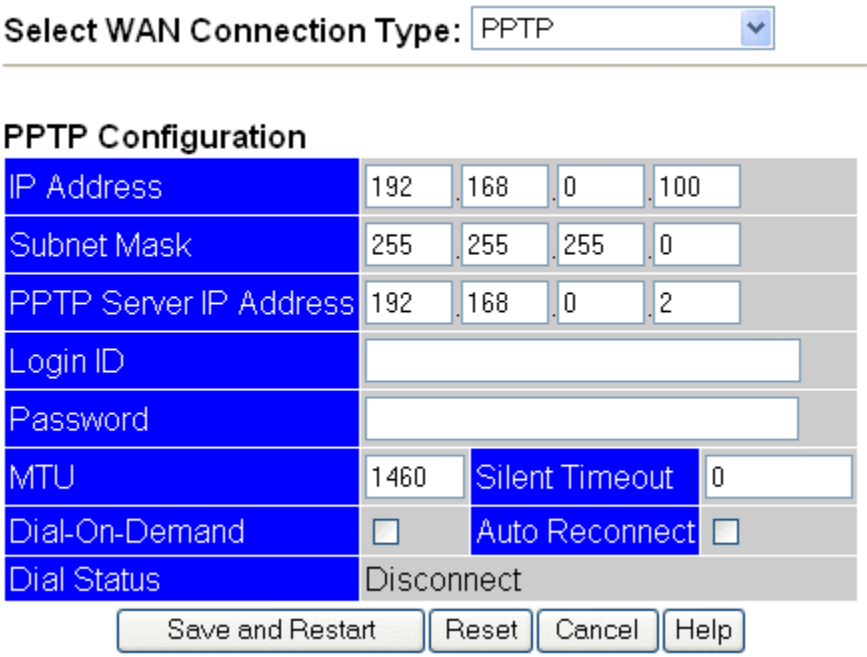


- **Select WAN Connection Type**: Select the **Unnumbered PPPoE** connection
- **Login ID**: Enter the login ID provided by ISP
- **Password**: Enter the Password provided by ISP
- **Service Name**: The Service Name set on the access concentrator. Many ISPs give user-name and address in the form of user-name@service-name. The Service Name provided by ISP, if one is required, otherwise, leave it blank.
- **AC Name**: Access concentrator name provided by ISP, if one is required, otherwise, leave it blank.
- **MTU**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, 1492, to have the wireless router select the best MTU for your Internet connection. Sometimes ISP sets different MTU size than 1492.
- **IP Address:** The unnumbered IP subnet address, assigned by ISP.
- **Network Mask:** Network size of the unnumbered IP subnet. If network mask is 255.255.255.248, then this wireless router supports five unnumbered IP hosts in LAN and uses one IP in allocated IP subnet for gateway itself.
- **NAPT for LAN hosts:** If checked, the wireless router enables NAPT function for LAN PCs using configured LAN IP address (ex: 192.168.1.x). If unchecked, NAPT is disabled and the wireless router will route packets to and from LAN PCs using unnumbered IP addresses.
- **Dial-On-Demand**: If checked, the wireless router will only dial this session when a LAN -> WAN packet is received. If unchecked, the wireless router immediately dials the session when powered up.
- **Silent timeout**: Only used when connection type is set to **Dial-On-Demand.** The **Silent timeout** value is defined as the time for the WAN port to disconnect if the connection is idle. (not used).
- **Auto Reconnect**: If checked, the router redials the session if previously terminated by ISP.

- **Dial Status**: Current status of this session. Maybe “connected”, “connecting” or “disconnect”.
- **Dial:** Click on this button to manually connect to ISP.
- **Hang Up:** Click on this button to disconnect the wireless router from ISP.
- **Save and Restart:** Save the parameters and reboot the wireless router.
- **Reset:** Click on “Reset” button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page.
- **Help**: To request help information.

3.3.5 PPTP

PPTP stands for “Point-to-Point Tunneling Protocol”. PPTP is used to join 2 networks using the Internet as an intermediary network. It allows users to connect a home or work network over the Internet. The key is to enter the PPPTP user ID, password, and PPTP Gateway IP address. The IP addresses, subnet mask, and default gateway may or may not be required.



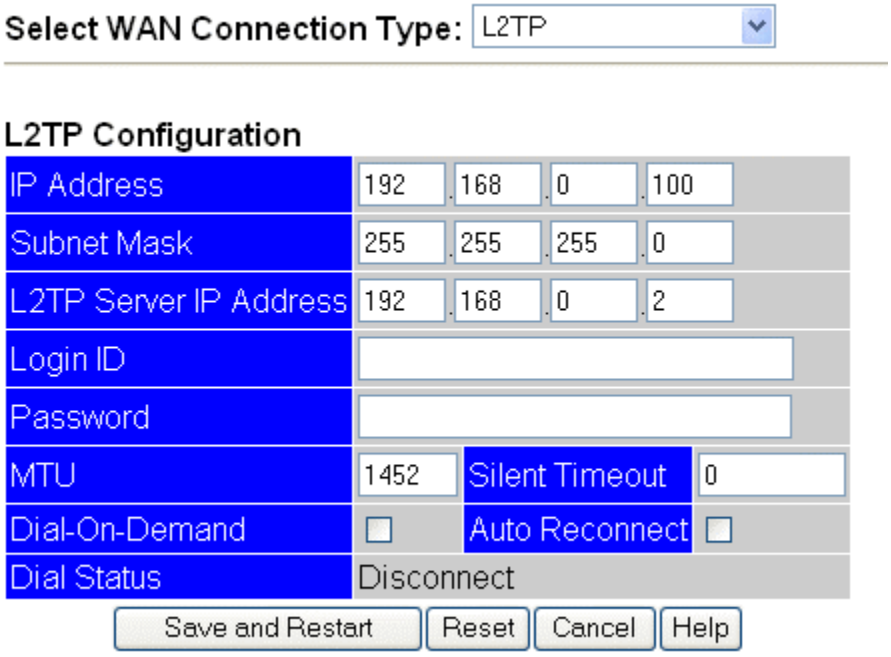
- **Select WAN Connection Type**: Select **PPTP** connection
- **IP Address**: Enter the IP address provided by ISP
- **Subnet Mask**: Enter the Subnet Mask provided by ISP
- **PPTP Server IP Address**: Enter the Server IP address provided by ISP
- **Login ID**: Enter the Login ID provided by ISP
- **Password**: Enter the Password provided by ISP
- **MTU Size**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, 1460, to have the router select the best MTU for your Internet connection.
- **Silent Timeout**: Only used when connection type is set to **Dial-On-Demand.** The **Silent timeout** value is defined as the time for the WAN port to disconnect if the connection is idle. (not used).
- **Dial-on-demand**: If checked, the wireless router will only dial this session when a LAN -> WAN packet is received. If unchecked, the wireless router immediately dials the session when powered up.
- **Auto Reconnect**: If checked, the wireless router redials the session if previously terminated by ISP.
- **Dial Status**: Current status of the session. Maybe “connected”, “connecting” or

"disconnect".

- **Save and Restart:** Save the parameters and reboot the wireless router.
- **Reset:** Click on "Reset" button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page.
- **Help**: To request help information.

3.3.6 L2TP

Select L2TP when ISP requires the L2TP protocol for WAN connection. The ISP should provide all the information required for this connection.

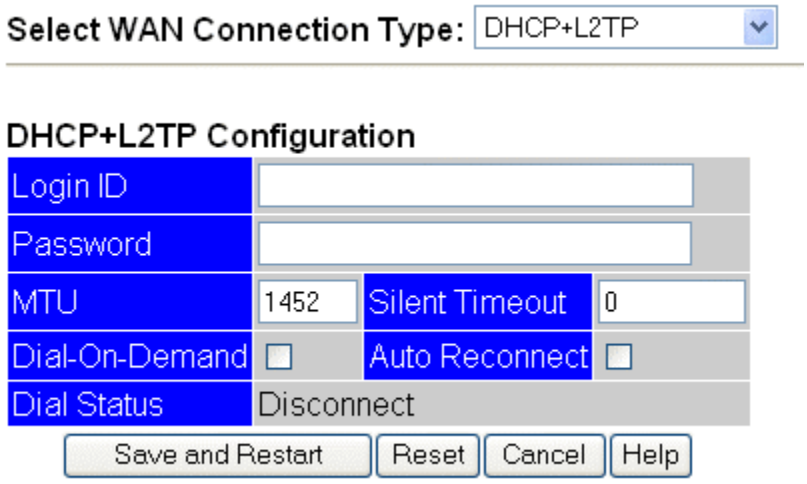


- **Select WAN Connection Type**: Select **L2TP** connection
- **IP address**: Enter the IP address provided by ISP. The IP address is used to communicate with remote L2TP server.
- **Subnet Mask**: Enter the Subnet Mask provided by ISP.
- **L2TP Server IP Address**: Remote L2TP server's IP address used by the L2TP client to dialup to.
- **Login ID**: Enter the Login ID provided by ISP
- **Password**: Enter the Password provided by ISP
- **MTU Size**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, 1452, to have the wireless router select the best MTU for your Internet connection.
- **Silent Timeout**: Only used when connection type is set to **Dial-On-Demand.** The **Silent timeout** value is defined as the time for the WAN port to disconnect if the connection is idle. (not used).
- **Dial-on-Demand**: If checked, the wireless router will only dial this session when a LAN -> WAN packet is received. If unchecked, the wireless router immediately dials the session when powered up.
- **Auto Reconnect**: If checked, the wireless router redials the session if previously terminated by ISP.
- **Dial Status**: Current status of the session. Maybe "connected", "connecting" or "disconnect".
- **Save and Restart:** Save the parameters and reboot this wireless router.
- **Reset:** Click on "Reset" button to undo your changes.

- **Cancel**: To skip the current settings and jump to the **Status** page.
- **Help**: To request help information.

3.3.7 DHCP + L2TP

Same as L2TP WAN type, but user only needs to specify Login ID and Password since gateway's IP address (as L2TP client) is obtained automatically using DHCP.

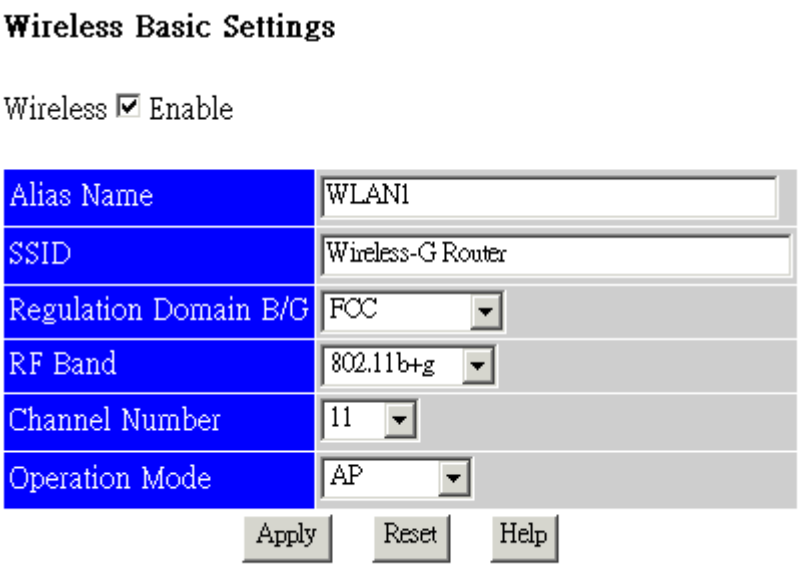


- **Select WAN Connection Type**: Select the **DHCP + L2TP** connection
- **Login ID**: Enter the Login ID provided by your ISP
- **Password**: Enter the Password provided by your ISP
- **MTU Size**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, 1452, to have the wireless router select the best MTU for your Internet connection.
- **Silent Timeout**: Only used when connection type is set to **Dial-On-Demand.** The **Silent timeout** value is defined as the time for the WAN port to disconnect if the connection is idle. (not used).
- **Dial-on-demand**: If checked, the wireless router will only dial this session when a LAN -> WAN packet is received. If unchecked, the wireless router immediately dials the session when powered up.
- **Auto Reconnect**: If checked, the wireless router redials the session if previously terminated by ISP.
- **Dial Status**: Current status of this session. Maybe "connected", "connecting" or "disconnect".
- **Save and Restart:** Save the parameters and reboot the wireless router.
- **Reset:** Click on "Reset" button to undo your changes.
- **Cancel**: To skip the current settings and jump to the **Status** page.
- **Help**: To request help information.

3.4 Wireless

3.4.1 Basic Settings

The Wireless Basic Settings include Alias Name, SSID, Regulation Domain, RF Band, Channel Number and Operation Mode.

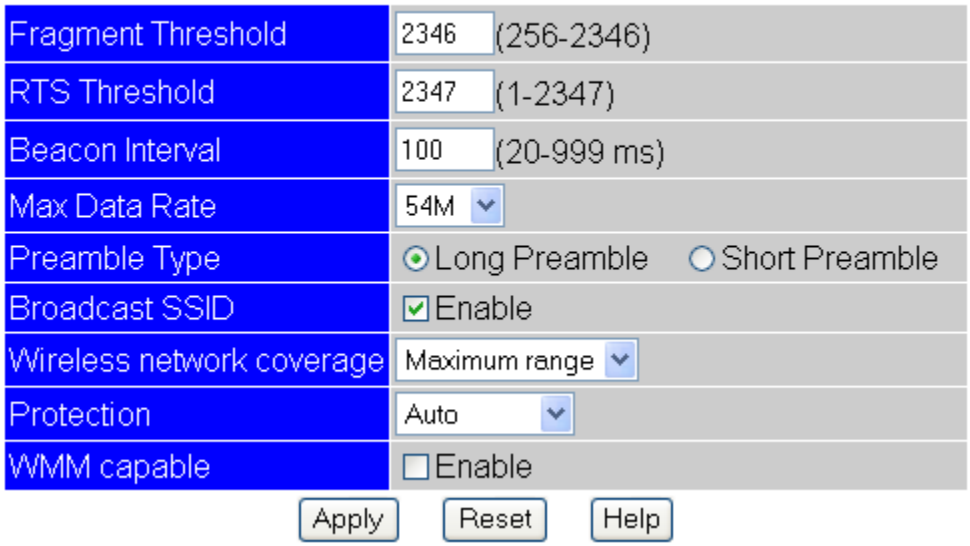


- **Enable Wireless**: Check or uncheck (Enable or Disable this wireless interface).
- **Alias Name**: You can assign a unique name to the wireless router. The alias name is especially important for identification when there are more than one wireless router applied in a network.
- **SSID**: The SSID differentiates one WLAN from another; therefore, all wireless routers and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters.
- **Regulation Domain B/G**: Different countries have different Regulation Domains for 11b and 11g wireless devices. There are six regulation domains: FCC, Canada, Europe, Spain, France and Japan.
- **RF Band**: The wireless router supports three RF bands: 11b+11g, 11b only and 11g only.
- **Channel Number**: The number of channels supported depends on the region of the wireless router. All stations communicating with the wireless router must use the same channel.
- **Operation Mode**: This wireless router supports two operational modes: AP and AP+WDS.
- **Apply:** Save the parameters.
- **Reset:** Click on “Reset” button to undo your changes.
- **Help**: To request help information.

3.4.2 Advanced Settings

In Advanced Settings page, more 802.11 related parameters are tunable.

Wireless Advance Settings



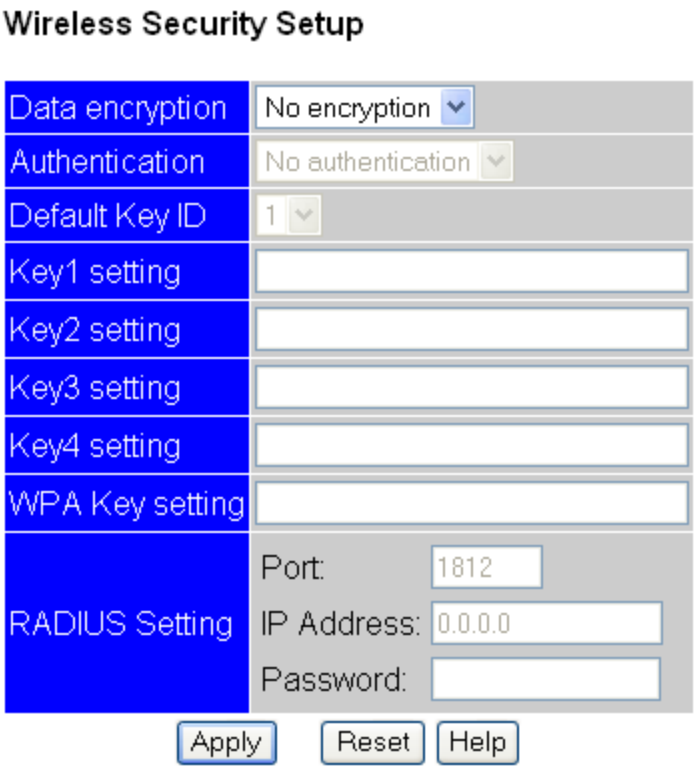
- **Fragment Threshold**: Fragmentation mechanism is used for improving the efficiency when high traffic flows through the wireless network. If a wireless client often transmits large files, users can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is 2346.
- **RTS Threshold**: RTS Threshold is a mechanism implemented to prevent the "Hidden Node" problem. "Hidden Node" is a situation in which two stations are within range of the same wireless access point/router, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the Wireless-G Router, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Wireless-G Router. The collision will most certainly result in a loss of messages of both stations. If the "Hidden Node" problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set. The default value is 2347.
- **Beacon Interval:** Beacon interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the wireless router).
- **Max Data Rate**: By default, it selects the highest rate for transmission.
- **Preamble Type**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired.
- **Broadcast SSID**: Select enabled to allow all the wireless stations to detect the SSID of this wireless router.
- **Wireless network coverage**: There are four options defining the Wireless network coverage: Minimum, Limited, Normal and Maximum range.
- **Protection**: CCK and OFDM are the modulation schemes used for 802.11b and 802.11g respectively. Since packet collision increases when both standards are used at the same time, enabling the Protection mode increases the performance. User can choose from Auto, On, and Off.
    - Auto: STA will dynamically change as AP announcement.
    - Always On: Always send frame with protection.
    - Always Off: Always send frame without protection.

- **WMM capable**: Check the Enable box to enable the WMM (Wireless Multi Media) capability.
- **Apply:** Save the parameters.
- **Reset:** Click on “Reset” button to undo your changes.
- **Help**: To request help information.

3.4.3 Security

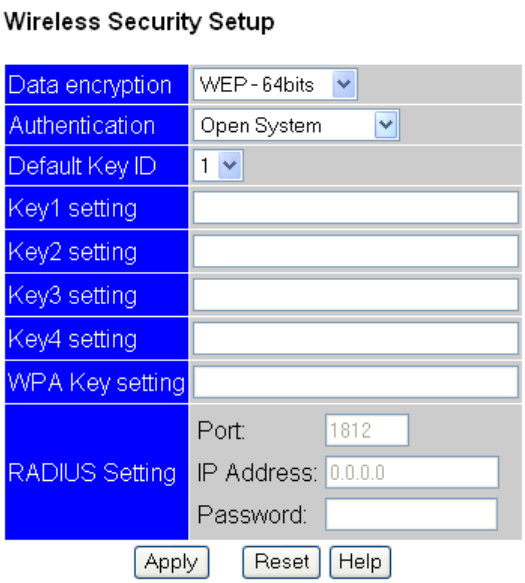
In this page the security level and type for the wireless network can be defined. **Please note that using any encryption may be a significant degradation of the data throughput on the wireless link**. There are four Encryption types: “None”, “WEP”, “TKIP” and ”AES” supported on this router.

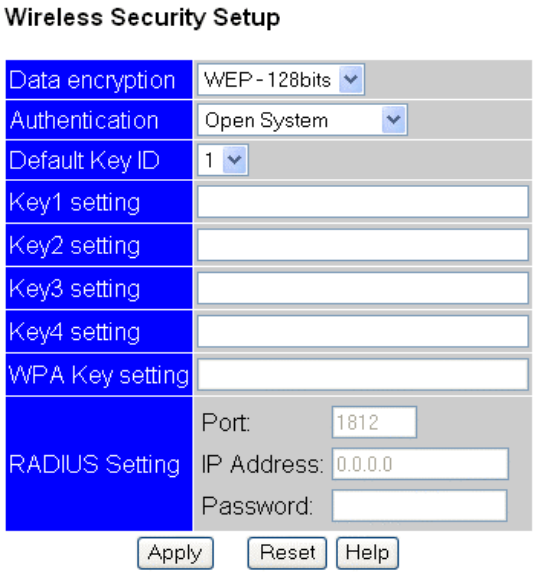
Encryption – No encryption



- **Data encryption: “No encryption”** means all wireless data packets are transmitted without encryption.
- **Apply:** Save the parameters.
- **Reset:** Click on “Reset” button to undo your changes.
- **Help**: To request help information.

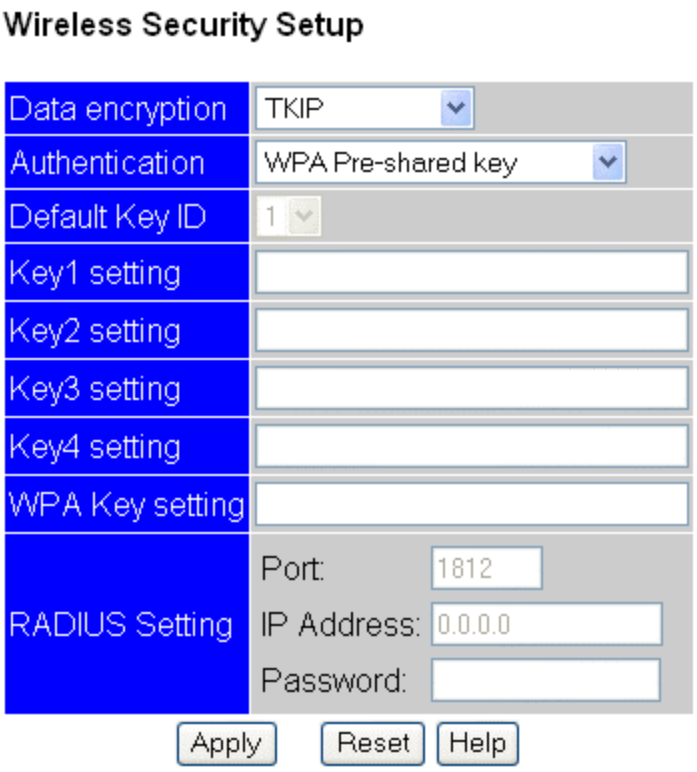
Encryption – WEP - 64bits or WEP - 128bits





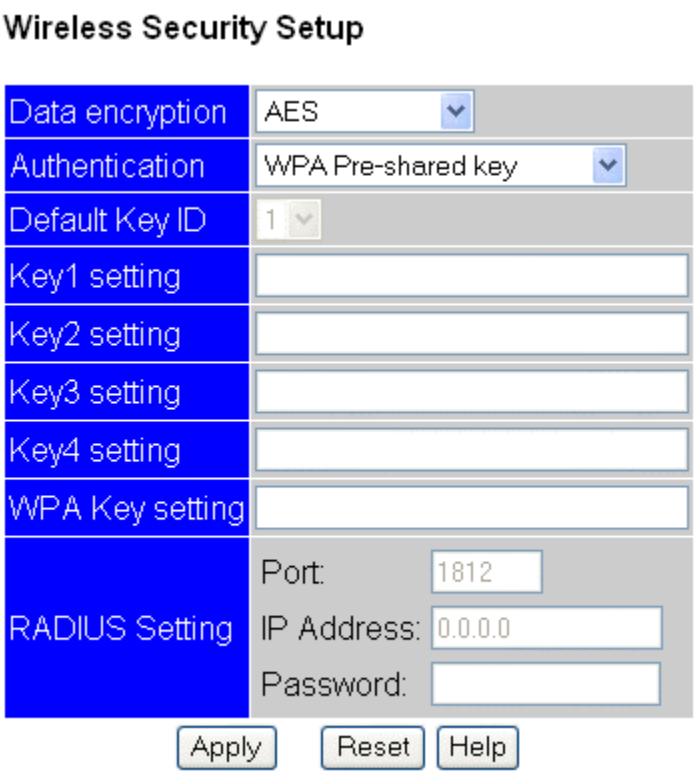
- **Data encryption:**
  - **"WEP – 64bits"**: Wired Equivalent Privacy encryption method with 64 bits encryption key length.
  - **"WEP – 128bits"**: Wired Equivalent Privacy encryption method with 128 bits encryption key length. The longer encryption length, the more security but the lower performance.
- **Authentication: There are four authentication types –**
  - **"Open System"**: Need no authentication.
  - **"Shared Key"**: Using a Shared Key to authenticate wireless clients.
  - **"Auto"**: Auto authentication.
  - **"By RADIUS server"**: Using a RADIUS server to authenticate wireless clients.
- **Default Key ID**: It is only active when WEP data encryption and Open System/Shared Key/Auto Authentication modes are selected. Default encryption Keys (1 to 4) can be selected to be transmitted.
- **Key 1 Setting**: Enter any key code for Encryption Key 1.
- **Key 2 Setting**: Enter any key code for Encryption Key 2.
- **Key 3 Setting**: Enter any key code for Encryption Key 3.
- **Key 4 Setting**: Enter any key code for Encryption Key 4.
- **RADIUS Setting:** When users choose RADIUS server authentication, there are three parameters for RADIUS server needed, – Port, IP address and Password.
- **Apply:** Save the parameters.
- **Reset:** Click on "Reset" button to undo your changes.
- **Help**: To request help information.

Encryption – TKIP



- **Data encryption: "TKIP"** means Temporal Key Integrity Protocol**.**
- **Authentication: There are four authentication types –**
  - **"WPA Pre-shared key"**: Using Pre-shared key to perform the WPA authentication
  - **"WPA2 Pre-shared key"**: Using Pre-shared key to perform the WPA2 authentication
  - **"WPA By RADIUS server"**: Using RADIUS server to perform the WPA authentication
  - **"WPA2 By RADIUS server"**: Using RADIUS server to perform the WPA2 authentication
- **WPA Key setting:** It is only active when you select the WPA Pre-shared key or WPA2 Pre-shared key. Enter any key code for this Pre-shared key.
- **RADIUS Setting:** When user chooses WPA – By RADIUS server or WPA2 – By RADIUS server authentication, there are three parameters of RADIUS server being set – Port, IP address and Password.
- **Apply:** Save the parameters.
- **Reset:** Click on "Reset" button to undo your changes.
- **Help**: To request help information.

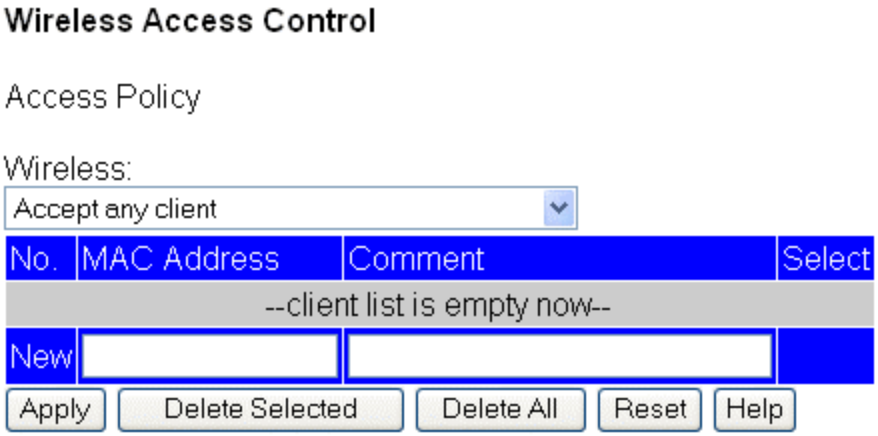
Encryption – AES



- **Data Encryption: "AES"** means Advanced Encryption Standard**.**
- **Authentication: There are four authentication type –**
  - **"WPA Pre-shared key"**: Using Pre-shared key to perform the WPA authentication
  - **"WPA2 Pre-shared key"**: Using Pre-shared key to perform the WPA2 authentication
  - **"WPA By RADIUS server"**: Using RADIUS server to perform the WPA authentication
  - **"WPA2 By RADIUS server"**: Using RADIUS server to perform the WPA2 authentication
- **WPA Key setting:** It is only active when you select the WPA Pre-shared key or WPA2 Pre-shared key. Enter any key code for this Pre-shared key.
- **RADIUS Setting:** When user chooses WPA – By RADIUS server or WPA2 – By RADIUS server authentication, there are three parameters of RADIUS server being set – Port, IP address and Password.
- **Apply:** Save the parameters.
- **Reset:** Click on "Reset" button to undo your changes.
- **Help**: To request help information.

3.4.4 Access Control

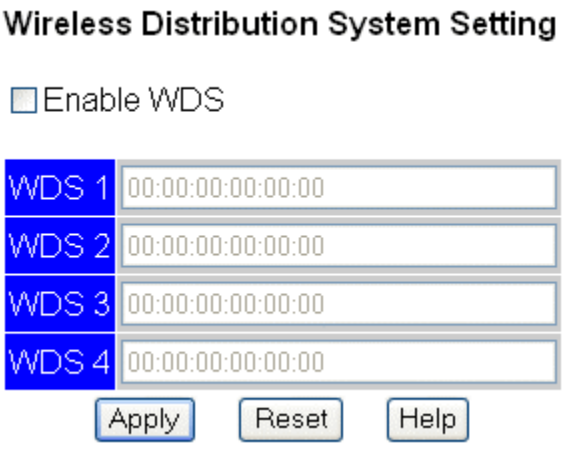
Access Control allows users to block or permit wireless clients to access this router. Users can add a new MAC address with a simple comment and then click on "Apply" button to apply.



- **Wireless Access Policy**: There are three types of access policy options:
  - **Accept any client**: If you choose "**Accept any client**", any wireless client will be allowed to connect to this wireless router.
  - **Accept clients in the list and reject all others:** If you choose this option, only those clients whose wireless MAC addresses are in the access control list will be allowed to connect to this wireless router.
  - **Reject clients in the list and accept all others**: When this option is selected, the wireless clients on the list will not be able to connect to this wireless router.
- **MAC Address**: You need to fill the client's MAC address which you want to allow or deny.
- **Comment:** You can add any comment in this blank field.
- **Apply**: To add new MAC address and Comments to the list.
- **Delete Selected**: Delete the selected client.
- **Delete All**: Delete all the MAC Addresses which are in the Client list table
- **Reset**: To clear all the input in the blank.
- **Help**: To request help information.

3.4.5 WDS

When the router's operational mode is set to AP+WDS, the Wireless Distribution System (WDS) feature will set the wireless router in "Bridge Mode". Two or more wireless routers in bridge mode can communicate with each other through their wireless interfaces. To do this, all routers must be set to operate in the same channel and have their MAC addresses entered in the WDS table.



- **Enable WDS**: When you check the box and enable the WDS function. This

wireless router enters the AP-WDS mode automatically.

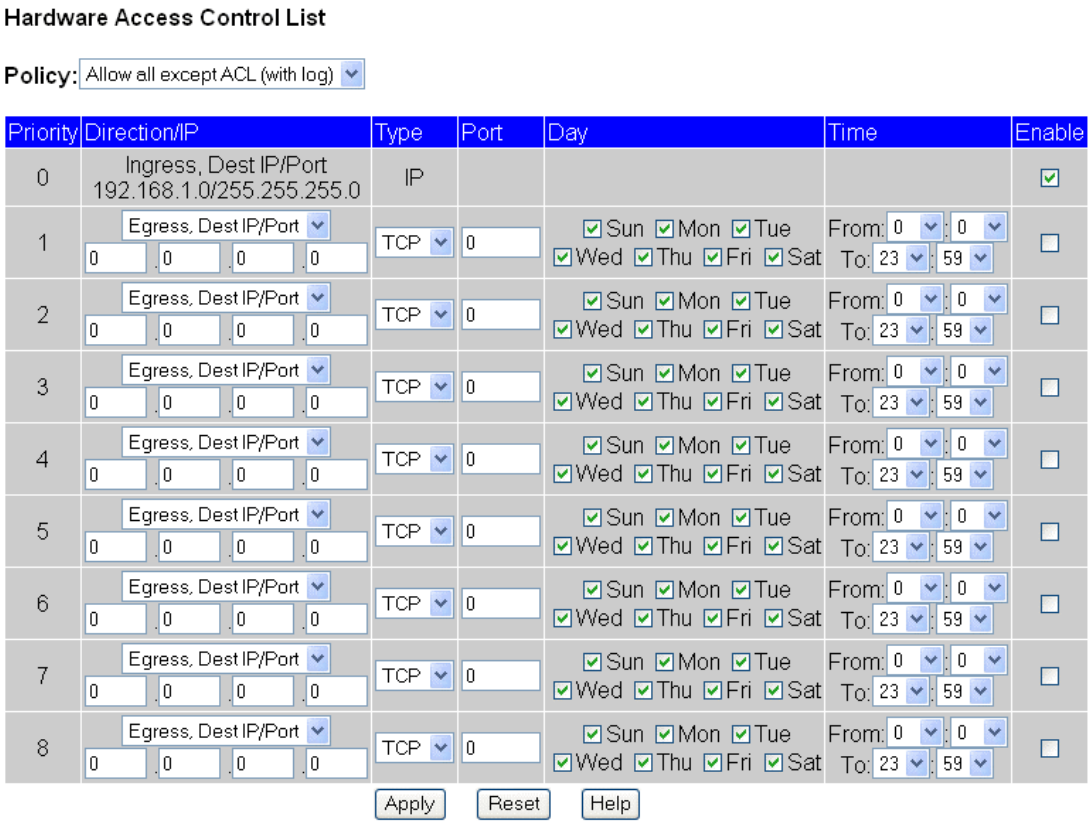
- **WDS1/WDS2/WDS3/WDS4**: You need to enter MAC addresses of other wireless routers you want to communicate with. There are a maximum of four WDS wireless routers that can join together.
- **Apply:** Save the parameters.
- **Reset:** Click on “Reset” button to undo your changes.
- **Help**: To request help information.

3.5 Firewall

3.5.1 Access Control list

ACLs are used to block IP packets from being forwarded by the wireless router. The ACL web page lets users specify a “Black list” ACL rules. There is one Policy - to log packets matching a configured ACL, the packet would be sent to software for logging. In the Direction column, Ingress means packets from LAN to Gateway and Egress means packets from Gateway to WAN.
You can use any combination or all of these items simultaneously to define an ACL.

1. Egress / Ingress
2. Dest IP port /Src IP port
3. IP address
4. IP/TCP/UDP
5. Port number
6. Day: Monday/Tuesday/Wednesday/Thursday/Friday/Saturday/Sunday
7. Time: select time range



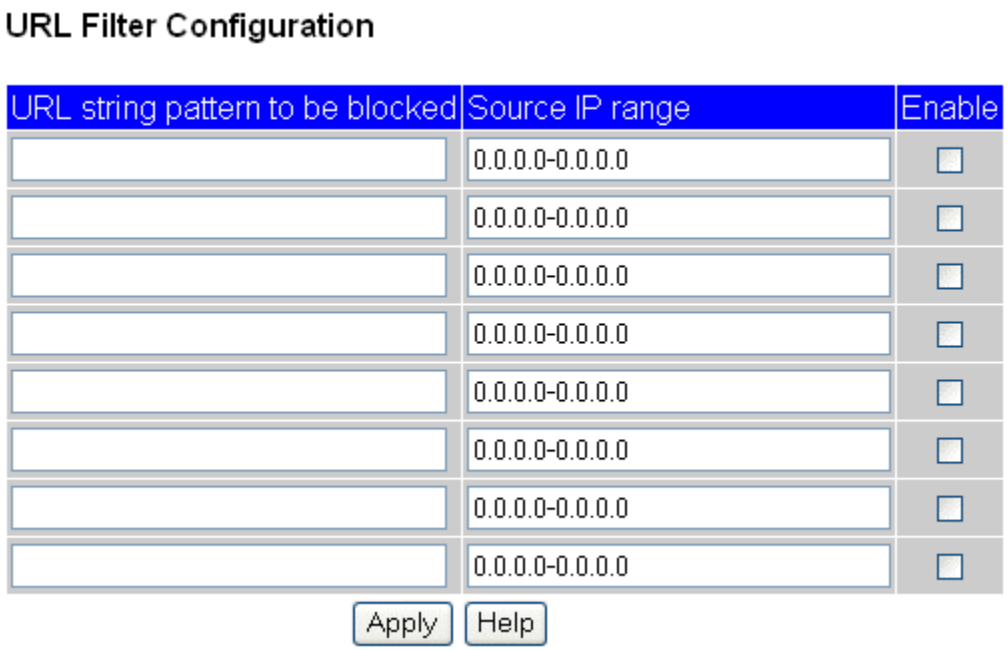
- **Policy**: There is only one policy – allow all packets except those defined in ACL. And log packets matching a configured ACL
- **Priority**: Users can define eight control lists. Their handling priority is depended on this priority number, the lower the number, the higher the priority.
- **Direction/IP**: There are four options to specify packets in LAN port:
  - **Egress, Dest IP/Port**: select the packet with an outgoing destination IP.

- **Ingress, Dest IP/Port**: select the packet with an incoming destination IP.
- **Egress, Src IP/Port**: select the packet with an outgoing source IP.
- **Ingress, Src IP/Port**: select the packet with an incoming source IP.

- **Type**: Define the packet type – TCP, UDP or IP
- **Port**: Enter the port number.
- **Day**: Select the Day – Sun, Mon, Tue, Wed, Thu, Fri or Sat.
- **Time**: Define the Time range.
- **Enable**: Check the box and enable this ACL group.
- **Apply:** Save the parameters.
- **Reset:** Click on "Reset" button to undo your changes.
- **Help**: To request help information.

3.5.2 URL Filter

URL filter can identify URL strings inside any packet, with any TCP/UDP port number and filter them. It provides eight entries and can filter packets by their source IP range.



- **URL String pattern to be blocked**: Enter the URL strings to be blocked.
- **Source IP range**: Enter the Source IP range that you want to block the URL string.
- **Enable**: Check the box and enable this URL condition.
- **Apply:** Save the parameters.
- **Reset:** Click on "Reset" button to undo your changes.
- **Help**: To request help information.

3.5.3 ALG

Some applications embed their IP and port information in their payload which is not NAT friendly. An Application Layer Gateway (ALG) is a plug-in module on NAT firewall to masquerade such application layer payloads.

ALG Configuration

ALG	Enable
PPTP (Enable software solution ☐)	☑ Client/Server(IP: 0.0.0.0)
IPSec	☑ Client/Server(IP: 0.0.0.0)
L2TP	☑ Client
FTP	☑ Client/Server(IP: 0.0.0.0)
Net Meeting	☑ Client/Server(IP: 0.0.0.0)
DirectX 7	☑ Client/Server(IP: 0.0.0.0)
SIP	☑ Client/Server(IP: 0.0.0.0)
ICUII	☑ Client/Server(IP: 0.0.0.0)
ICQ / AOL Instant Messenger	☑ Client/Server
Yahoo Messenger	☑ Client/Server
mIRC	☑ Client/Server
VDOlive	☑ Client
Quake	☑ Client
Counter Strike / Half Life	☑ Client
Blizzard Battlenet (StarCraft, DiabloII)	☑ Client
RealAudio	☑ Client
CUseeMe	☑ Client

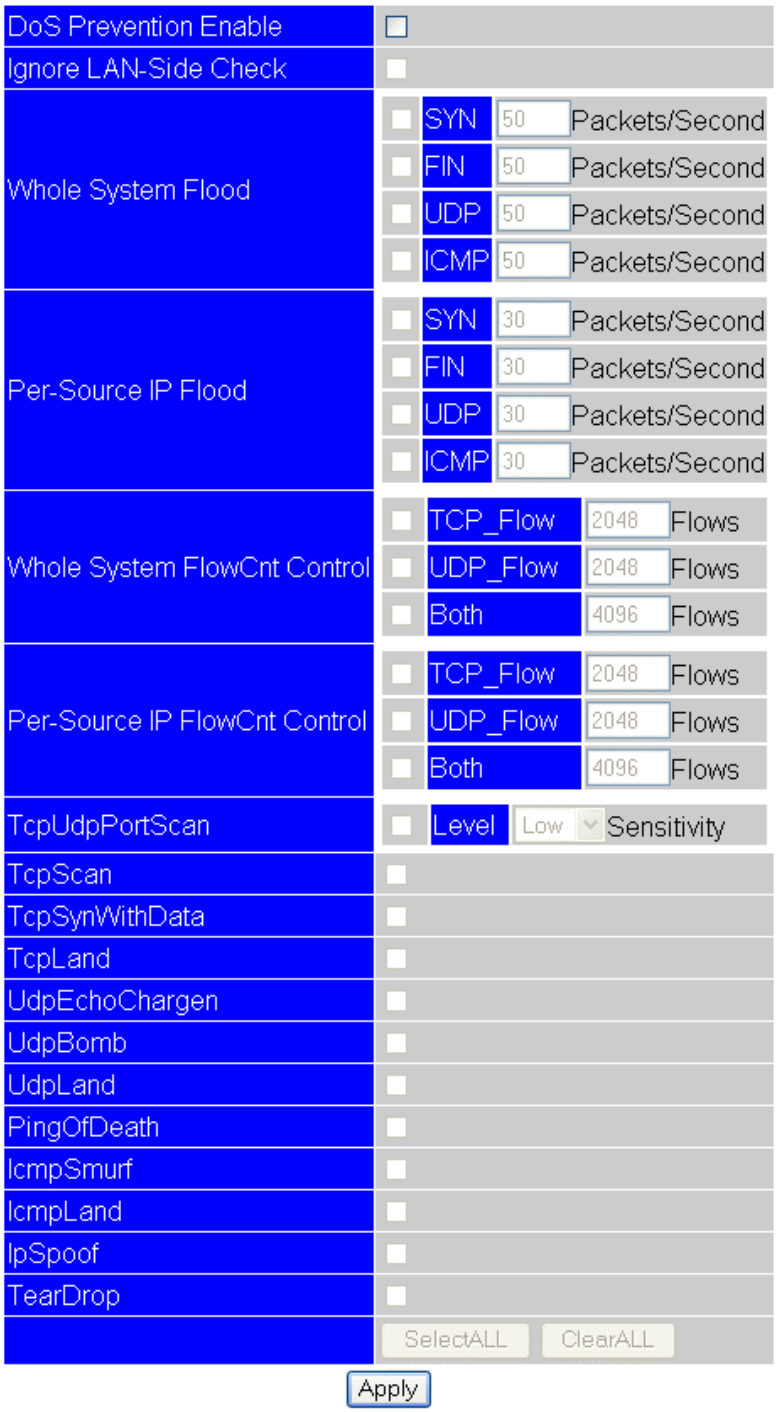
Apply Help

- **Enable:** Check the Enable Box, to enable ALG of an application and then the wireless router will let that application correctly pass though the NAT gateway.
- **Apply:** Save the parameters.
- **Help**: To request help information.

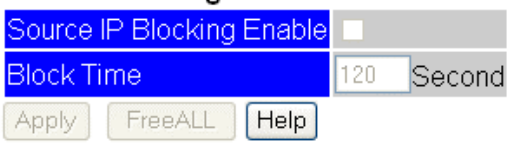
3.5.4 Anti-DoS

DoS (Denial of Service) defense function protect network servers, hosts, routers and other devices from the attack of a villain using mass data transmission.

DoS Configuration



Source Blocking

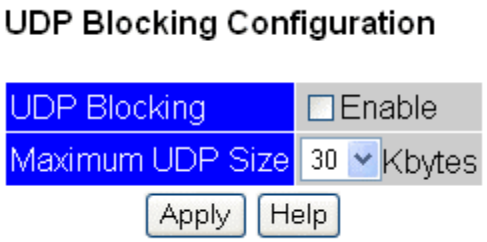


- **DoS Prevention Enable**: check – enable this DoS feature.

- **Ignore LAN-Side Check**: Skip DoS checks for all LAN to WAN packets
- **Whole System Flood**: The wireless router will ignore all packets, when the number of received packets for SYN, FIN, UDP or ICMP exceeds the settings (packets/second).
- **Per-Source IP Flood**: The wireless router will ignore all packets from this source IP, when the number of received packets for SYN, FIN, UDP or ICMP exceeds the settings (packets/second).
- **Whole System Flow Control:** The router can control the whole system flow for TCP, UDP or TCP+UDP packets.
- **Per-Source IP Flow Control**: The router can control the source IP flow for TCP, UDP or TCP+UDP packets.
- **TcpUdpPortScan:** Sending SYN packets to find out which ports are open on which machines is known as port scanning. The router would allow the user to set a sensitivity level (low or high) to reflect how tolerant their network or servers are to traffic surge.
- **TcpScan**: You can allow the router to respond to TCP port scanner packets or not.
- **TcpSynWithData**: In a TCP SYN flood attack, the attacker creates half-open TCP connections by sending the initial SYN packet with a forged IP address, and never acknowledges the SYN /ACK from the host with an ACK. This will eventually lead to the host reaching a limit and stop accepting connections from legitimate users as well. Without these preventive measures, the server could eventually run out of memory, causing it to crash entirely.
- **TcpLand**: Are TCP packets with the same source and destination address.
- **UdpEchoChargen**: Are UDP echo and chargen service packets with the same source and destination address.
- **UdpBomb**: Are UDP packets with incorrect information in the header.
- **UdpLand**: Are UDP packets with the same source and destination address.
- **PingOfDeath**: These are ping packets with modified IP portion of header, indicating that there is more data in the packet than there actually is, or packets with data payload exceeding the maximum allowed packet size.
- **IcmpSmurf**: Are attacks by sending a large amount of ICMP Echo Request (ping) traffic to a broadcast address.
- **IcmpLand**: Are attacks using an ICMP packet with the same source and destination address.
- **IpSpoof**: Are attacks caused by sending a SYN packet to a server, using victim's IP address.
- **TearDrop**: The attacks take advantage of some implements of the TCP/IP IP fragmentation reassembly code that do not properly handle overlapping IP fragments, causing a memory buffer overrun.
- **SelectALL:** Check all the check boxes in DoS Configuration.
- **ClearALL:** Uncheck all the check boxes in DoS Configuration.
- **Apply:** Save the parameters.
- **Source IP Blocking Enable**: Offending host would be blocked.
- **Block Time**: Define the time for source IP blocking feature, default value is 120 seconds.
- **Enable:** Check the Enable Box, to enable ALG of an application and then the router will let that application correctly pass though the NAT gateway.
- **Apply:** Save the parameters.
- **Help**: To request help information.

3.5.5 UDP Blocking

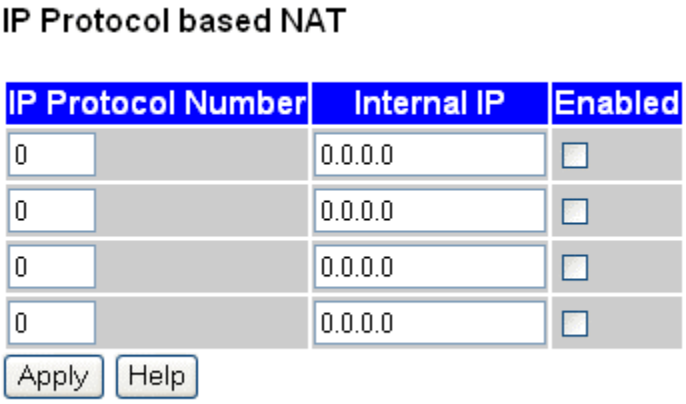
Large UDP packets can be blocked in case malicious attackers use such packets to attack LAN PCs. UDP packets larger than Maximum UDP size would be dropped if UDP Blocking is enabled.



- **UDP Blocking:** Check the Enable Box, to enable the UDP Blocking feature.
- **Maximum UDP Size:** The router will block UDP packets larger the set size.
- **Apply:** Save the parameters.
- **Help**: To request help information.

3.5.6 Protocol-based NAT

This wireless router supports NAT by IP protocol. Users can specify an IP protocol number and internal host's IP address to let the gateway masquerade IP header then forward to that internal host. This could be useful if user wants to setup a protocol proxy inside LAN.

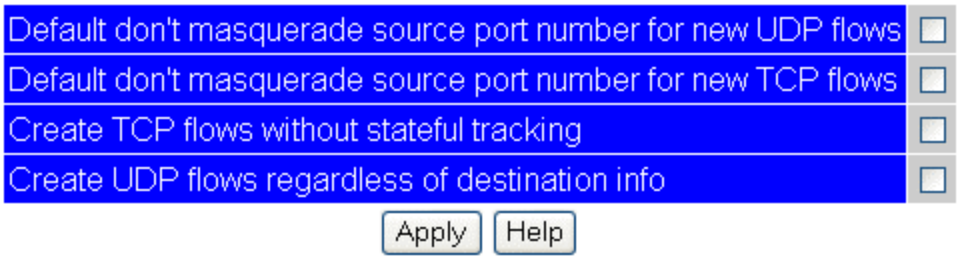


- **IP Protocol Number:** Enter the IP protocol number for a specific internal IP.
- **Internal IP:** Enter the relative Internal IP that you want to masquerade this IP.
- **Enable:** Check the Enable Box, to enable this feature.
- **Apply:** Save the parameters.
- **Help**: To request help information.

3.5.7 NAPT options

We provide additional features for NAPT.

NAPT Option

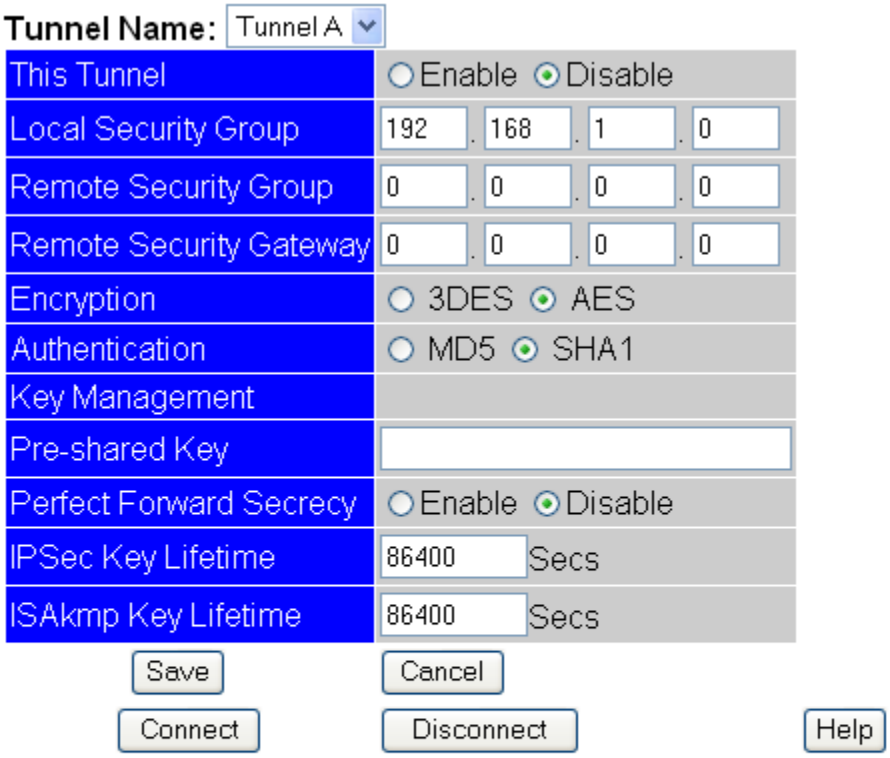


- **Default don't masquerade source port number for new UDP flows:** The wireless router will try to keep LAN to WAN source UDP port number when doing NAPT if possible. Doing so helps some NAT unfriendly application without ALG module pass NAT gateway.
- **Default don't masquerade source port number for new TCP flows:** The wireless router will try to keep LAN to WAN source TCP port number when doing NAPT if possible. Doing so helps some NAT unfriendly application without ALG module pass NAT gateway.
- **Create TCP flows without stateful tracking:** The wireless router will keep strict state tracking for each TCP flow created. This option is provided to help performance test tools such as SmartBits or IXIA perform tests on our claimed wirespeed features. Unless you are doing benchmarking test with such tools, we discourage user to turn on this option since it violates NAT gateway's natural firewall and DoS prevention feature.
- **Create TCP flows regardless of destination info:** Discard new UDP flow's destination info so any incoming UDP packets, wherever it comes from, if destined to the same external UDP port, would be accepted by NAT hardware. This helps some NAT unfriendly applications pass NAT gateway but compromises system security.
- **Apply:** Save the parameters.
- **Help**: To request help information.

3.6 VPN Settings

Virtual Private Network (VPN), is a connection between two end points. It allows private data to be sent securely over the Internet. VPN establishes a private network that can send data securely between two networks. We call this is by creating a "tunnel".

Note: we only support Router to Router VPN connection.



Status

- **Tunnel Name**: The wireless router can create three simultaneous tunnels, Tunnel A, Tunnel B and Tunnel C.
- **This tunnel**: Enable or disable this selected tunnel.
- **Local security group**: Private network on this VPN router.
- **Remote security group**: Private network on the remote peer VPN router.
- **Remote security gateway**: Private network on the remote side security gateway.
- **Encryption**: There are two encryption methods available: 3DES and AES.
- **Authentication**: There are two authentications available: MD5 and SHA1.

Key management:

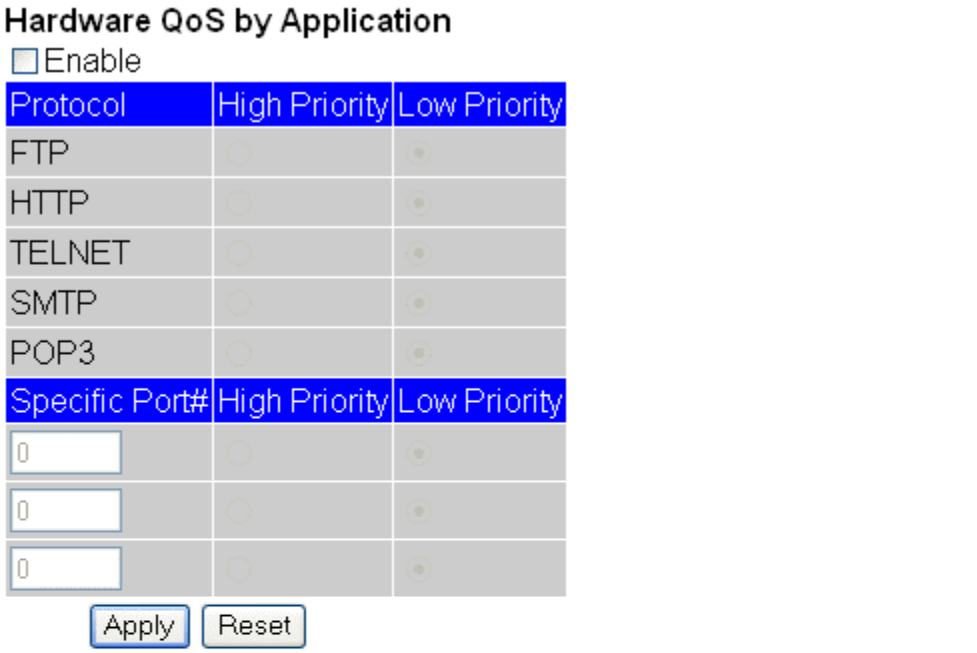
- **Pre-shared Key**: Pre-shared keys are used for user authentication between a VPN Client and a gateway. IKE (Internet Key Exchange Protocol) will use the Pre-shared key to authenticate the remote IKE peer.
- **Prefect Forward Secrecy**: If enabled, IKE Phase 2 negotiation will generate a new key material for IP traffic encryption and authentication.
- **IPSec Key Lifetime**: IPSec (IP Security) can support encryption on large networks by using digital certificates for device authentication. This field allows configuring the length of time for IPSec Key to be active. The default value is 86400 seconds.
- **ISAkmp Key Lifetime**: ISAkmp (Internet Security Association and Key Management Protocol. The basis for IKE. This field allows you to configure the length of time for ISAkmp Key being active. The default value is 86400 seconds.
- **Save:** Save the parameters.
- **Cancel:** To undo your changes.
- **Connect:** Start to connect this VPN.

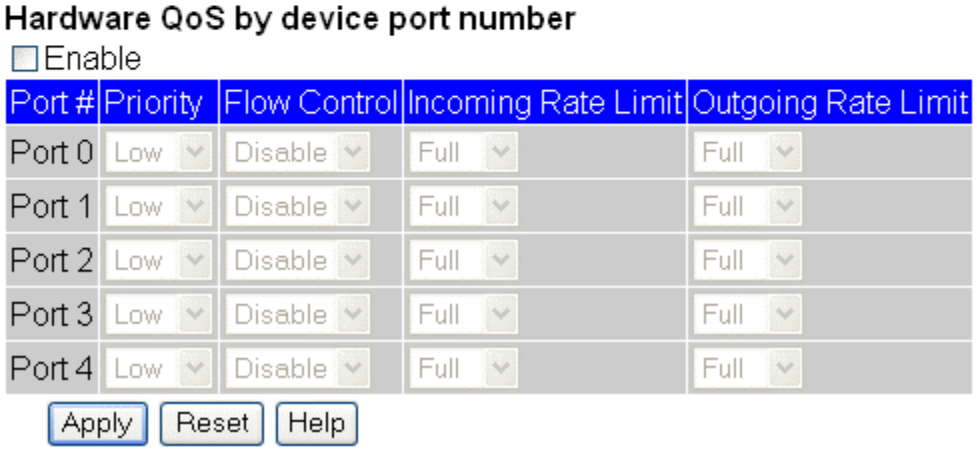
- **Disconnect:** Start to disconnect this VPN.
- **Help**: To request help information.
- **Status:** It will display your connection status when you have established the IPSec tunnel.

3.7 QoS Settings

3.7.1 Port/L4 App Based QoS

This web page supports two types of QoS: Port based QoS and L4 application based QoS.
For Application based QoS, users can specify a destination port number and associate it with an egress priority (high or low).
For Port based QoS, user can specify the High/Low queue priority for each Ethernet port and apply total rate limit from 128Kbps to 32Mbps or full-rate (100Mbps) to any port. Flow control can also be enabled/disabled on a per-port basis.





Hardware QoS by Application

- **Enable:** Check the box to enable this feature.
- **Protocol:** There are six popular protocols being defined – FTP, HTTP, TELNET, SMTP and POP3.

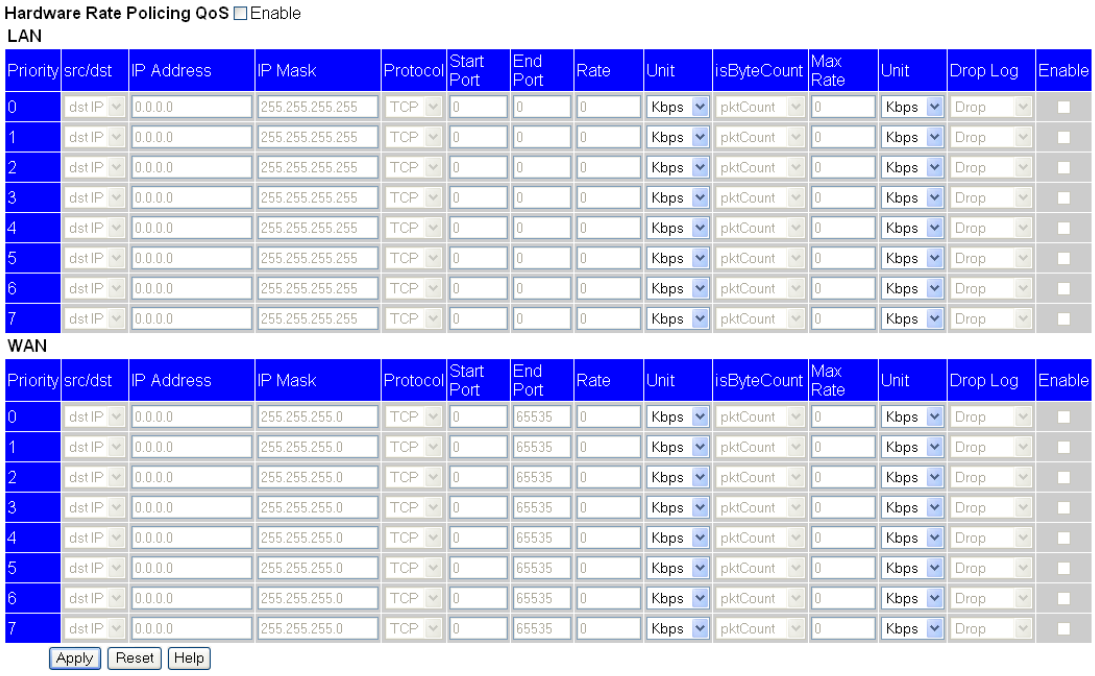
- **High Priority:** Select to set high priority level.
- **Low Priority:** Select to set Low priority level.
- **Specific Port#:** Priority can also be assigned based on the port numbers used by applications. For example FTP uses port 21 and Telnet uses port # 23.
- **Apply:** Save the parameters.
- **Reset:** Click on “Reset” button to undo your changes.

Hardware QoS by device port number

- **Enable:** Check the box to enable this feature.
- **Port #:** There are five physical ports –
  - **Port 0 : WAN port**
  - **Port 1 : LAN’s port 1.**
  - **Port 2 : LAN’s port 2.**
  - **Port 3 : LAN’s port 3.**
  - **Port 4 : LAN’s port 4.**
- **Priority:** Assigning priority levels to each LAN port.
- **Flow control:** Enable or disable flow control for individual ports.
- **Incoming Rate Limit:** Bandwidth of incoming packets for individual ports.
- **Outgoing Rate Limit:** Bandwidth of outgoing packets for individual ports.
- **Apply:** Save the parameters.
- **Reset:** Click on “Reset” button to undo your changes.
- **Help**: To request help information.

3.7.2 Rate Policing QoS

Users can specify a L3/L4 criterion and associate it with a maximum token (packet rate or data rate based). If a packet arrives and it matches to a rate policing entry, the wireless router decreases entry’s allocated token by one (if pps based) or by packet length in bytes (if bps based). If the packet just run out of allocated tokens, then it would be dropped directly or logged to software, depending on the setting of Drop Log field.
To classify all TCP or UDP packets within same IP address/mask (regardless of port number) as same rate policy, set 0 to both Start Port and End Port.



- **Enable:** Check the box to enable this feature.
- **Priority:** There are eight priority levels for LAN and WAN side individually.
- **src/dst**: Source or destination address.

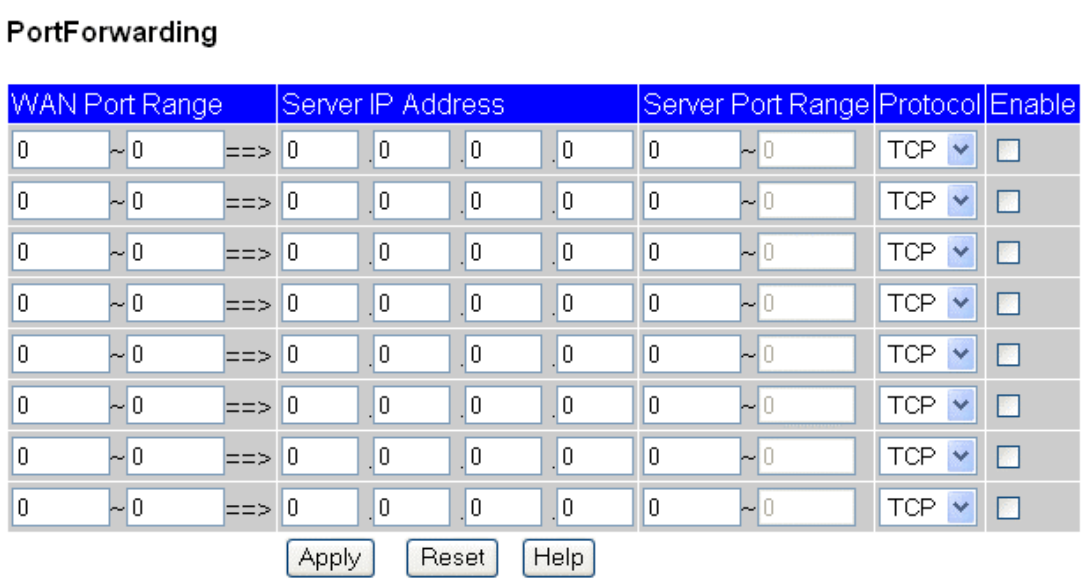
- **IP Address**: Enter the IP address.
- **IP Mask**: Enter the IP Subnet Mask.
- **Protocol:** Select the IP protocol – TCP, UDP or IP.
- **Start port:** Enter the Starting port number.
- **End port:** Enter the Ending port number.
- **Rate:** Enter the average rate value.
- **Unit:** Select the unit for this average rate.
- **IsByteCount:** Select the counting method based on bytes or packets.
- **Max Rate:** Enter the maximum rate value.
- **Unit:** Select the unit for this maximum rate.
- **Enable:** Check the box to enable this relative priority.
- **Apply:** Save the parameters.
- **Reset:** Click on "Reset" button to undo your changes.
- **Help**: To request help information.

3.8 Advanced

3.8.1 Port Forwarding

When port forwarding is enabled, users can run any network service (ex: Web, FTP, P2P software etc….) inside LAN and open a "hole" on router's built-in firewall to let traffic redirected to relevant server.

Note: If user wants to run a FTP virtual server in LAN, don't add an entry here. FTP requires an additional ALG module which is available in the ALG web page. User should turn on FTP ALG and configure a server IP instead.

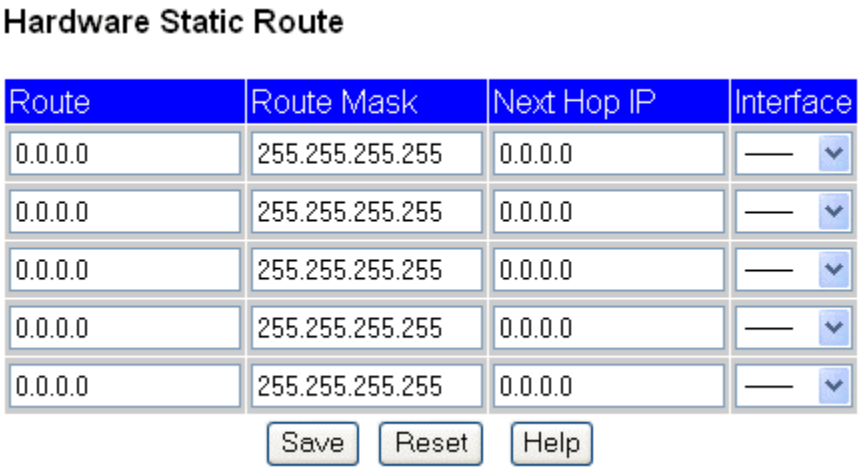


- **WAN Port Range:** Enter the port number range on WAN side.
- **Server IP Address:** Enter the virtual server IP address
- **Server Port Range:** Enter the virtual server port range
- **Protocol:** Select the protocol to be TCP or UDP.
- **Enable:** Check the box to enable this port forwarding.
- **Apply:** Save the parameters.
- **Reset:** Click on "Reset" button to undo your changes.
- **Help**: To request help information.

3.8.2 Static Route

A network with a limited number of gateways to other TCP/IP networks can be configured with static routing. When a network has only one gateway, a static route is the best choice. Static

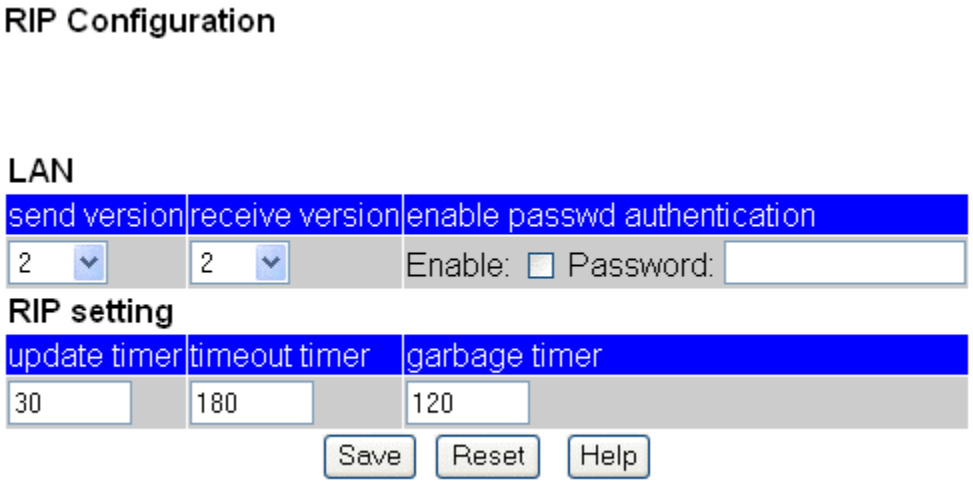
routing tables do not adjust to network changes, so they work best where routes do not change.



- **Route**: The network address of the destination LAN segment. Packets with destination IP addresses matching this field will be routed to the device set in the Next Hop IP field.
- **Route Mask**: Destination Network mask
- **NextHop IP**: Next hop router for this packet.
- **Interface**: You can select to use LAN or WAN as the physical interface from where the packets will be sent.
- **Save:** Save the parameters.
- **Reset:** Click on “Reset” button to undo your changes.
- **Help**: To request help information.

3.8.3 RIP

You can configure this wireless router to receive and send RIP Version 1 or RIP Version 2 packets. RIP Version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, RIP authentication can be enabled on an interface.
Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and etc. You can adjust these timers to tune routing protocol performance to better suit your network needs. The following timer adjustments are available :



LAN

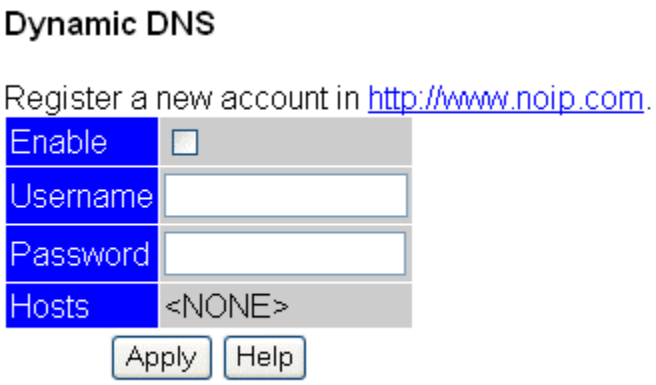
- **send version**: Select the RIP version for send packet – version 1, 2 or 1&2.
- **receive version**: Select the RIP version for receive packet – version 1, 2 or 1&2.
- **enable passwd authentication**: Enter the password and check it to enable this authentication.

RIP setting

- **update timer** (in seconds): The rate at which routing updates are sent.
- **timeout timer** (in seconds): Time period after the router decides a route is not valid anymore.
- **garbage timer** (in seconds): Time period after invalid routes are dropped from the routing table.
- **Save:** Save the parameters.
- **Reset:** Click on "Reset" button to undo your changes.
- **Help**: To request help information.

3.8.4 Dynamic DNS

You can assign a fixed host and domain name to a dynamic Internet IP address.
Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider. This is how Internet users can access the router through a domain name instead of its IP address.
Note: make sure that you have registered with a DDNS service provider before enabling this feature.



- **Enable**: Check or uncheck (enable DDNS or disable DDNS)
- **Username**: Enter the user name required to log into the DDNS account
- **Password**: Enter the password required to log into the DDNS account.
- **Hosts**: Display the host name.
- **Apply:** Save the parameters.
- **Help**: To request help information.

3.8.5 Special Application

This is a feature for users to open "holes" on the router's built-in firewall triggered by outgoing packets. Some NAT unfriendly applications require users to do so for normal operation. For example, QuickTime requires users to add a special application rule to turn on WAN port 6970 to 6999 when an outbound packet using source TCP port 554 is received.

Special Application

Name	Incoming Type	Incoming Port Range	Trigger Type	Trigger Start Port	Trigger Finish Port	Enable
Quick Time 4	UDP	6970-6999	TCP	554	554	☐
MSN Gaming Zone	TCP	28800-29000	TCP	6667	6667	☐
	TCP		TCP	0	0	☐
	TCP		TCP	0	0	☐
	TCP		TCP	0	0	☐
	TCP		TCP	0	0	☐
	TCP		TCP	0	0	☐
	TCP		TCP	0	0	☐

Apply Reset Help

- **Name:** Enter the application name.
- **Incoming Type:** Select the incoming packet to be TCP, UDP or Both.
- **Incoming Port Range:** Enter the port range of incoming packets for this type of application.
- **Trigger Type:** Select the outbound port protocol to be to be TCP, UDP or Both.
- **Trigger Start Port:** Enter the trigger start port number. This is the outgoing start port number for this particular application.
- **Trigger Finish Port:** Enter the trigger end port number. This is the outgoing end port number for this particular application.
- **Enable:** Check the box and enable this item.
- **Apply:** Save the parameters.
- **Reset:** Click on “Reset” button to undo your changes.
- **Help**: To request help information.

3.8.6 DMZ Host

The DMZ (Demilitarized) Host feature allows one local computer to be exposed to the Internet.

Designate a DMZ host when:

- You wish to use a special-purpose Internet service, such as an on-line game or video-conferencing program, that is not present in the Local Servers list and for which no port range information is available.
- You are not concerned with security and wish to expose one computer to all services without restriction.

Warning: A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

DMZ Configuration

DMZ Host #1 (default)	0 . 0 . 0 . 0	☐ Enable
General L4 protocol forward	☐ Enable	
ICMP forward	☐ Enable	

Apply Help

- **DMZ Host #1 (default):** Enter the IP address of this DMZ host. Check the box and enable this DMZ feature.
- **General L4 protocol forward:** When checked L4 protocol forwarding feature is enabled.
- **ICMP forward:** When checked ICMP packet forwarding feature is enabled.
- **Apply:** Save the parameters.
- **Help**: To request help information.

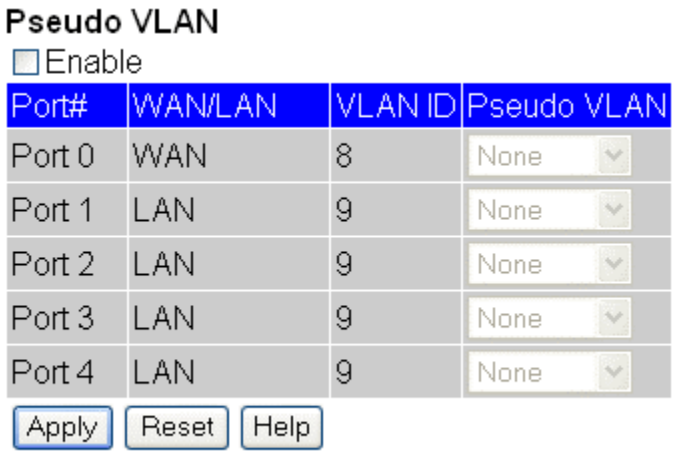
3.8.7 Ping toolkit

This is a handy tool for users to test LAN or WAN connectivity using ping command.

- **IP Address/Host Name:** Enter the IP address or host name which you want to ping.
- **Ping:** Start the ping command.
- **Response:** Show ping results.
- **Help**: To request help information.

3.8.8 Pseudo-VLAN

This wireless router can support a VLAN mapping with fixed VLAN ID 8 for WAN port and VLAN ID 9 for all LAN ports. Users can define the VLAN group for each port.



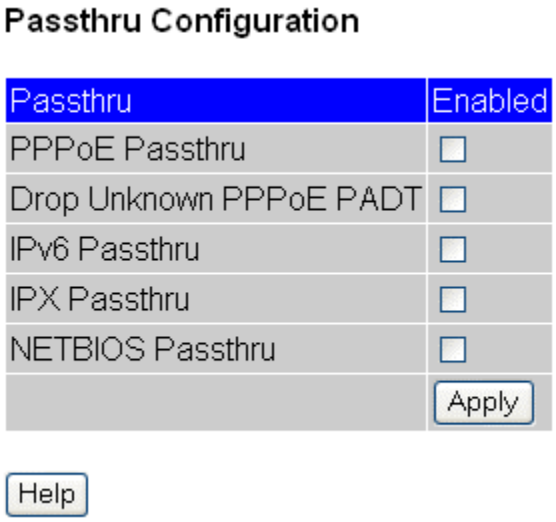
- **Enable:** Check the box to enable pseudo VLAN feature.
- **Port#:** Show the logical port number for this router.
- **WAN/LAN:** Show WAN/LAN port for the corresponding physical port.
- **VLAN ID:** Show the VLAN ID for corresponding port.
- **Pseudo VLAN:** Assign a subnet for this port. There are only 6 VLAN groups being defined.
- **Apply:** Save the parameters.
- **Reset:** Click on “Reset” button to undo your changes.

- **Help**: To request help information.

3.8.9 PPPoE/IPv6 Passthru

There are some specific packets to be defined as pass through.

- PPPoE
- Drop Unknown PPPoE PADT
- IPv6
- IPX
- NETBIOS



- **Enabled:** Check the box and enable the corresponding passthru protocol.
- **Apply:** Save the parameters.
- **Help**: To request help information.

3.8.10 IP Multicast

User can disable or enable the IP multicast function.

- **IP Multicast:** Check the box and enable the IP multicast feature.
- **Apply:** Save the parameters.
- **Help**: To request help information.

3.8.11 Samba Server

The SAMBA server is basically a file server running on embedded Linux. This wireless router supports a simple file server through its USB port. User can plug in any USB pendrive or USB hard disk if they are of the FAT16 format.

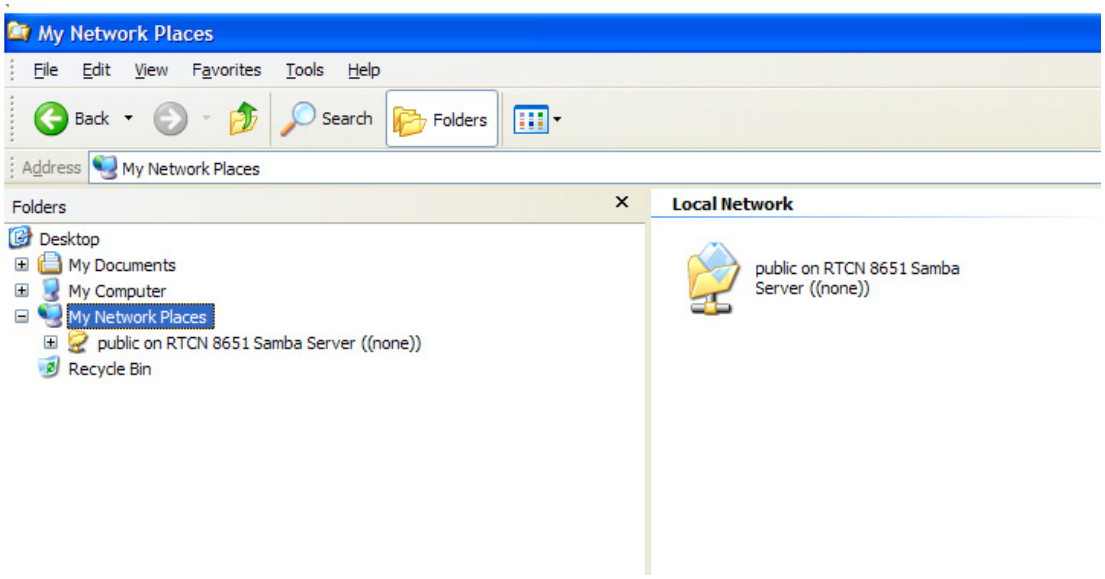
Any LAN side client PC can read/write files from this USB device by browsing network neighborhood using the wireless router's IP.

Note 1: Please make sure that the PC's IP address is within the file server's IP address

range.
Note 2: Since some pendrives are not well protected by its hardware. We recommend the pendrive to be plugged in or out when the router is power off.

- **Samba Server:** Check the box and enable this feature.
- **Apply:** Save the parameters.
- **Help**: To request help information.

For Windows XP, you can find the Samba Server in the My Network Places.



3.9 Management

3.9.1 Status

The status page provides a brief read-only report for system, LAN and WAN configuration information. The data displayed may be different depending on your current configuration.

System

Product Model	Wireless-G Router
Firmware Version	1.00
Firmware Date	2005/10/05 14:23:24
Loader Version	0.0.19
Wireless AP Version	1.0.1.0
Rome Driver Version	3.5-2

LAN

IP Address	192.168.1.254
Subnet Mask	255.255.255.0
MAC Address	00:00:10:11:12:15
DHCP Server	Enable
Port 1	Link is down. No cable detected
Port 2	Link is Up. 100Mbps, full- duplex
Port 3	Link is down. No cable detected
Port 4	Link is down. No cable detected

WAN

Connection Method	DHCP Client
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS IP Address	0.0.0.0
MAC Address	00:00:10:11:12:14
Port 0	Link is down. No cable detected

Wireless WLAN1

Status	Enabled
SSID	Wireless-G Router
BSSID	00:0C:43:25:61:01
Summary	AP start in Channel 11

Help

System

- **Product Model**: Shows the model name of this product.
- **Firmware Version**: Shows the current firmware version.
- **Firmware Date:** Shows the current firmware building date.
- **Loader Version:** Shows the current boot loader driver version.
- **Wireless AP Version:** Shows the current wireless driver version.
- **Rome Driver Version**: Shows the current Rome Driver version.

LAN

- **IP Address**: Shows the router's LAN port IP address
- **Subnet Mask**: Shows subnet mask on your local network.

- **MAC Address**: Shows the MAC address on your LAN port.
- **DHCP Server**: Shows the DHCP server status.
- **Port 1**: Shows the LAN's port 1 status.
- **Port 2**: Shows the LAN's port 2 status.
- **Port 3**: Shows the LAN's port 3 status.
- **Port 4**: Shows the LAN's port 4 status.

WAN Configuration

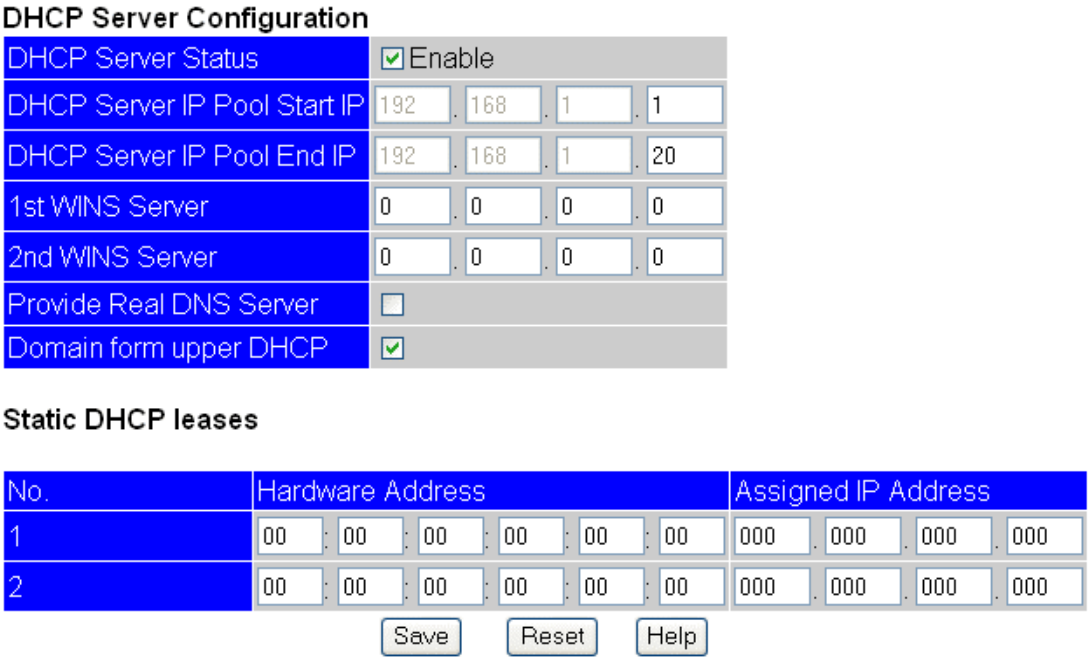
- **Connection Method**: Shows the connection method being used on WAN.
- **IP Address**: Shows the router's WAN port IP address
- **Subnet Mask**: Shows subnet mask on your public network.
- **Default Gateway**: Shows the defined Default Gateway on your public network.
- **DNS IP Address**: Shows the IP address of DNS being used.
- **MAC Address**: Shows the MAC address on your WAN port.
- **Port 0**: Shows the WAN port status.

Wireless Configuration

- **Status**: Shows the current wireless status – enable or disable.
- **SSID**: Shows the current SSID.
- **BBSID**: Shows the current BBSID on your Wireless LAN port.
- **Summary**: Shows the operational mode and channel being used.
- **Help**: To request help information.

3.9.2 DHCP Settings

There is a DHCP server running on LAN interface. It serves dynamic IP addresses to LAN hosts running DHCP client. Both dynamic and static DHCP leases are supported. The service is turned on by default.

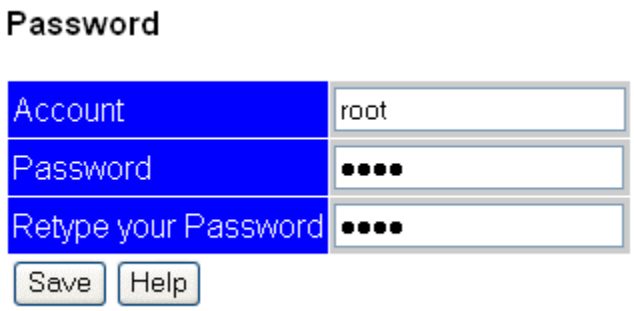


- **DHCP Server Status**: Check to enable the DHCP Server feature.
- **DHCP Server IP Pool Start IP**: Enter the Start address assigned by DHCP server.

- **DHCP Server IP Pool End IP**: Enter the End address assigned by DHCP server.
- **1st WINS Server**: The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP address here. Otherwise, leave this blank.
- **2nd WINS Server:** Enter the second WINS server IP**.**
  - **Note:** Like DNS, WINS employs a distributed client/server system to maintain the mapping of computer names to addresses. Windows clients can be configured to use primary and secondary WINS servers that dynamically update name/address pairings as computers join and leave the network. The dynamic behavior of WINS means that it also supports networks using DHCP.
- **Static DHCP leases**: User can assign a fixed IP to the client with its specific MAC address (Hardware address).
- **Hardware Address:** Enter the MAC address that was specified for the reserved IP address.
- **Assigned IP Address:** Enter the IP address that you would like to reserve for a specified MAC address.
- **Save**: Save the settings.
- **Reset:** Click on "Reset" button to undo your changes.
- **Help**: To request help information.
- **Dynamic DHCP Client List**: Shows all IP addresses already assigned and the corresponding LAN PC hostname and their MAC addresses.

3.9.3 Password

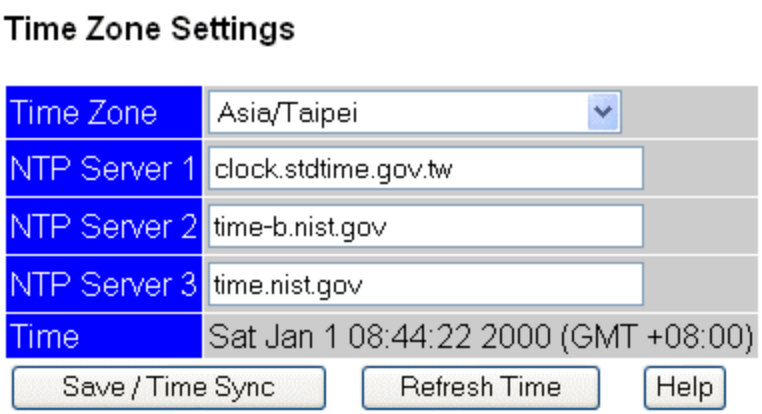
Users can change Login ID and Password here. The default Login ID is "root" with Password '1234'.



- **Account**: Enter the new login id. The login id can contain 0 to 30 characters and is case sensitive.
- **Password**: Enter the new login password. The password can contain 0 to 30 characters and is case sensitive.
- **Retype your Password**: Enter the new login password again.
- **Save**: Save the settings.
- **Help**: To request help information.

3.9.4 Time Zone Settings

This wireless router provides a NTP (Network Time Protocol) client that can synchronize time with configured NTP servers. Pressing the Refresh Time button refreshes system timestamp and the Save/Time Sync button forces NTP client sync time with NTP server.



- **Time Zone**: Select the time zone of the country where the wireless router is located.
- **NTP server1**: Default NTP server address (clock.stdtime.gov.tw).
- **NTP server2**: Default NTP server address (time-b.nist.gov).
- **NTP server3**: Default NTP server address (time.nist.gov).
- **Time:** Display current time of the wireless router.
- **Save/Time Sync:** Save the settings and update the time from selected servers.
- **Refresh Time:** Update the time from selected servers.
- **Help**: To request help information.

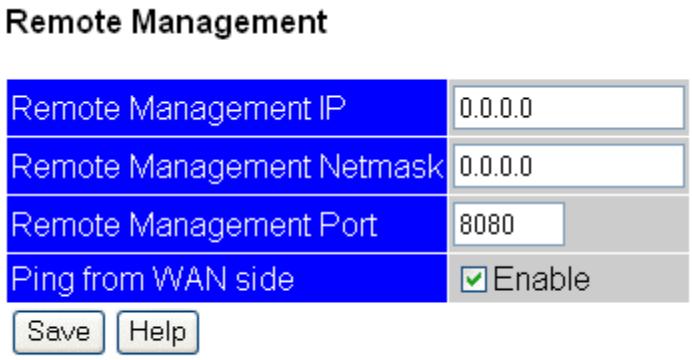
3.9.5 Upgrade Firmware

The firmware on the wireless router can easily be updated.
Firmware Update: Click on the Browse button to select the firmware and then click on the Update button.
After the firmware upgrade is completed, the wireless router will restart.
Note: Do not power off the wireless router while firmware is being upgraded.

- **Firmware Version:** Current firmware version.
- **Firmware Update**: Enter the location and name of the file containing the new firmware. Use the Browse button to browse for the file.
- **Update:** Click on the button to update the wireless router's firmware.
- **Help**: To request help information.

3.9.6 Remote Management

Users can connect to this wireless router from WAN side using the wireless router's WAN IP. The wireless router's current WAN IP is shown in the WAN status page. To avoid conflicting with virtual server at port 80, users can specify a different port number for "Remote Management Port" for WAN side access.



- **Remote Management IP:** Enter the remote management IP of the wireless router.
- **Remote Management Netmask**: Enter the remote management netmask of this router.
- **Remote Management Port:** Define the remote management port of this wireless router.
- **Ping from WAN side**: Allow users to ping this wireless router from WAN side. It is turned on by default and could be turned off if the enable box is unchecked..
- **Save:** Save the settings.
- **Help**: To request help information.

3.9.7 Reload Settings

You can reset the wireless router back to its default settings by clicking on the Factory Default button.

Note: you can also hold down the reset button on the wireless router's back panel for more than 5 seconds to reset it back to its default settings.

- **Factory Default:** Start to reload the default settings.
- **Help**: To request help information.

3.9.8 System Restart

In some special cases, you may restart this wireless router manually without unplugging the power cable. Click on the System Restart button to reset the wireless router.

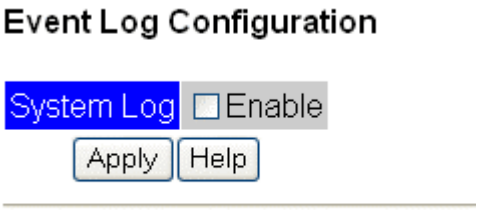
- **System Restart:** Start to reset the system.
- **Help**: To request help information.

3.10 Event Log

This wireless router supports five types of Log messages: System Log, ACL Log, URL filter, DoS Log and New NAPT Log. This data is useful for monitoring and troubleshooting the network.

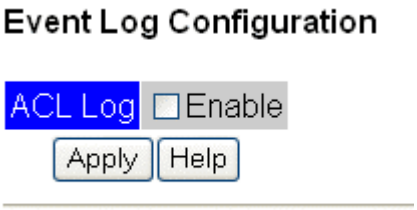
Note: enabling all logs will generate a large amount of data and adversely affect performance.

3.10.1 System Log
Log the internal system information



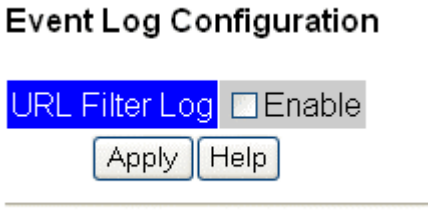
- **System Log:** Check the box and enable this feature.
- **Apply:** Save the settings.
- **Help**: To request help information.

3.10.2 ACL Log
Log the Access Control List information



- **ACL Log:** Check the box and enable this feature.
- **Apply:** Save the settings.
- **Help**: To request help information.

3.10.3 URL Filter Log
Log the URL Filter information.



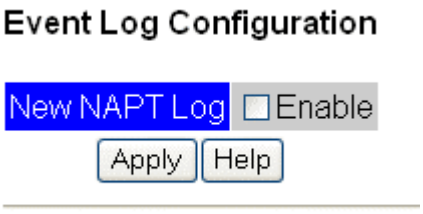
- **URL Filter Log:** Check the box and enable this feature.
- **Apply:** Save the settings.
- **Help**: To request help information.

3.10.4 DoS Log
Log the DoS information.

- **DoS Log:** Check the box and enable this feature.
- **Apply:** Save the settings.
- **Help**: To request help information.

3.10.5 New Connection Log

Log the WAN connection information



- **New NAPT Log:** Check the box and enable this feature.
- **Apply:** Save the settings.
- **Help**: To request help information.

Appendix A: Troubleshooting

Symptom	Possible Causes	Things to Do
Inability to access the router	• Incorrect or incompatible wireless network configuration. For example, shared key authentication is configured on the wireless AP/Router and the wireless client is attempting open system authentication • Inadvertent media access control (MAC) address filtering • The wireless network name is not visible	• Verify that the wireless network configurations between the wireless client and wireless AP/Router are compatible. Make sure that the client system's network card is set to receive IP automatically. •Use "Ipconfig" utility to verify that the client is getting an IP address from the router: 1. Click Start > Programs and select Command Prompt. 2. Type ipconfig /all at the command prompt. 3. With default settings on the router, client should get an IP address in the range of 192.168.1.XX with a default gateway IP of 192.168.1.254.
	• The wireless AP/Router and wireless network adapter are not using the same 802.11 standard (for example, you are using an 802.11a network adapter and a 802.11g wireless AP/Router)	• Use the same 802.11 standard for wireless AP/Router and wireless network adapter.
	• Radio frequency (RF) interference from nearby devices such as cordless phones and Bluetooth devices	• Remove the device causing the interference.
	• Wireless client is at the periphery of the RF range of the wireless AP/Router	• Move the wireless client closer or re-locate the wireless AP/Router.
	• Improperly functioning or outdated wireless network adapter driver	• Obtain and install the most recent version of the wireless network adapter driver.
	• Cable failure (when wired to the router)	• Check the "Link" LED next to the port on the router. Make sure that Ethernet cables are connected properly.

	• AP/Router is not power on	• Check the “Power” LED. Make sure that you've plugged in the power cord.
Intermittent connectivity	• IEEE 802.1X authentication is enabled on the wireless client and is not enabled on the wireless AP/Router • Improperly functioning or outdated wireless network adapter driver • Improperly functioning wireless AP/Router	• The symptom of this issue is when the wireless client loses connectivity every 3 minutes or so. Disable the authentication feature on the wireless client. • Obtain and install the most recent version of the wireless network adapter driver. Contact CNet Technical Support
Incorrect, missing, or stale visible networks	• Improperly functioning or outdated wireless network adapter driver • Improperly functioning radio equipment on wireless AP/Router or wireless network adapter	• Obtain and install the most recent version of the wireless network adapter driver. • Run diagnostic functions on the wireless network adapter.
Wireless client has associated but there is no valid IP address configuration or no network connectivity	• Authentication problem • Incorrect encryption key • Bad or missing certificates • Improperly functioning wireless AP	• Verify that the wireless network configurations between the wireless client and wireless AP/Router are compatible. • If you are using a static WEP key, verify that it has been correctly configured. • Verify whether other computers connected to the wireless AP have the same problem. If all wireless clients of the same wireless AP/Router have the same problem, check the wireless AP/Router settings. • IEEE 802.1X authentication might be failing. Check it again.
Wireless connection problems when performing a suspend and resume with a laptop computer	• The Wireless Zero Configuration or Wireless Configuration services are not running • Improperly functioning or outdated wireless network adapter driver	• Check to see if the Wireless Zero Configuration or Wireless Configuration services are running with the sc query wzcsvc command. • With the Services snap-in, ensure that the Wireless Zero Configuration or Wireless

	• On a laptop computer, the wireless radio button might be in the off position	Configuration services are configured to start automatically. • A wireless network adapter driver failing in early stages of service startup may result in the Wireless Zero Configuration or Wireless Configuration service not initializing over that interface.
Client can't connect to the AP/Router's configuration utility.	• Wrong IP address	• Make sure that your PC is using an IP address within the correct range. It should be 192.168.1.2 to 192.168.1.254 for the default value. • Make sure that the address of the subnet mask is 255.255.255.0. • Try to use “Ping” utility to ping the AP/Router’s IP, the default IP should be at 192.168.1.253 or 192.168.1.254 for AP and Router respectively.

Appendix B: Frequently Asked Questions

Q1: What is wireless networking?
Ans: The term wireless networking refers to the technology that enables two or more computers to communicate using standard network protocols, but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. The current buzzword however generally refers to wireless LANs. This technology, fuelled by the emergence of cross-vendor industry standards such as IEEE 802.11, has produced a number of affordable wireless solutions that are growing in popularity with business and schools as well as sophisticated applications where network wiring is impossible, such as in warehousing or point-of-sale handheld equipment.

Q2: What is a wireless network made up of?
Ans: There are two kinds of wireless networks:
a. An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. (This is called "bridging")

Figure A1: Ad-Hoc or Peer-to Peer Networking.
Each computer with a wireless interface can communicate directly with all of the others.

b. A wireless network can also use an access point, or base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect (or "bridge") the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity.
There are two types of access points:
I. Dedicated hardware access points (HAP) such as Lucent's WaveLAN, Apple's Airport Base Station or WebGear's AviatorPRO. (See Figure A2). Hardware access points offer comprehensive support of most wireless features, but check your requirements carefully.

ii. Software Access Points which run on a computer equipped with a wireless network interface card as used in an ad-hoc or peer-to-peer wireless network. (See Figure A3) The Vicomsoft InterGate suites are software routers that can be used as a basic Software Access Point, and include features not commonly found in hardware solutions, such as Direct PPPoE support and extensive configuration flexibility, but may not offer the full range of wireless features defined in the 802.11 standard.
With appropriate networking software support, users on the wireless LAN can share files and printers located on the wired LAN and vice versa. Vicomsoft's solutions support file sharing using TCP/IP.

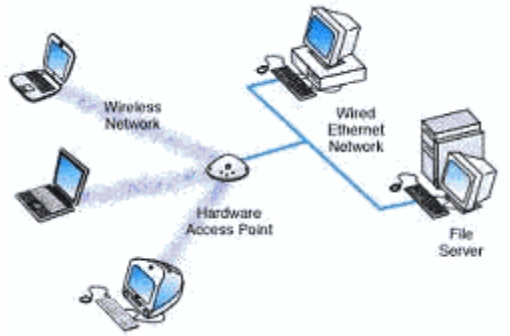


Figure A2: Hardware Access Point.
Wireless connected computers using a Hardware Access Point.

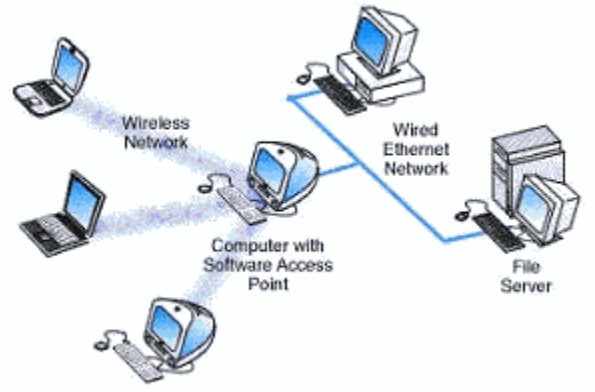


Figure A3: Software Access Point.
Wireless connected computers using a Software Access Point.

Q3: Can I mix wireless equipment from different vendors?
Ans: Because most wireless networking hardware vendors support the 802.11 standard they can inter operate. However, we recommend verification as the standard is a fairly recent one, and does specify two different methods for wireless communications; Frequency Hopping (FH) and Direct Sequence Spread Spectrum (DSSS or DS), which are not interoperable.
When purchasing wireless networking hardware from separate vendors be sure to obtain guarantees from the vendors that the hardware will interoperate and follows the standards.
Within a short time we expect all new wireless cards, like Ethernet cards, to become inexpensive, ubiquitous and totally interoperable.
Also of note is that the latest version of the standard defines 11mbps and 5.5mbps networking, with support for the older standard 1mbps and 2mbps speeds. This provides some compatibility with different or older equipment. Note that this new standard covers DS-type Networks, not FH types.
Software access points such as InterGate which uses the wireless interface of the host computer should have no compatibility issues with third party wireless hardware, as long as standards are followed. Typically wireless hardware is identified to the software as a network interface, and therefore can be used in the same way as any other network card.

Q4:If my computer is connected to a wireless LAN, can it communicate with computers on a wired LAN as well?
Ans: To do this you will need some sort of bridge between the wireless and wired network. This can be accomplished either with a hardware access point or a software access point. Hardware access points are available with various types of network interfaces, such as Ethernet or Token Ring, but typically require extra hardware to be purchased if your networking requirements change.
If networking requirements go beyond just interconnecting a wired network to a small wireless network, a software access point may be the best solution.
A software access point does not limit the type or number of network interfaces you use. It may

also allow considerable flexibility in providing access to different network types, such as different types of Ethernet, Wireless and Token Ring networks. Such connections are only limited by the number of slots or interfaces in the computer used for this task.
Further to this the software access point may include significant additional features such as shared Internet access, web caching or content filtering, providing significant benefits to users and administrators.

Q5: What is Roaming?
Ans: A wireless computer can "roam" from one access point to another, with the software and hardware maintaining a steady network connection by monitoring the signal strength from in-range access points and locking on to the one with the best quality. Usually this is completely transparent to the user; they are not aware that a different access point is being used from area to area. Some access point configurations require security authentication when swapping access points, usually in the form of a password dialog box.
Access points are required to have overlapping wireless areas to achieve this as can be seen in the following diagram:

Figure A6: Roaming.
A user can move from Area 1 to Area 2 transparently. The Wireless networking hardware automatically swaps to the Access Point with the best signal.

Not all access points are capable of being configured to support roaming. Also of note is that any access points for a single vendor should be used when implementing roaming, as there is no official standard for this feature.

Q6: What about security?
Ans: Wireless communications obviously provide potential security issues, as an intruder does not need physical access to the traditional wired network in order to gain access to data communications. However, 802.11 wireless communications cannot be received --much less decoded-- by simple scanners, short wave receivers etc. This has led to the common misconception that wireless communications cannot be eavesdropped at all. However, eavesdropping is possible using special equipment.
To protect against any potential security issues, 802.11 wireless communications have a function called WEP (Wired Equivalent Privacy), a form of encryption which provides privacy comparable to that of a traditional wired network. If the wireless network has information that should be secure then WEP should be used, ensuring the data is protected at traditional wired network levels.
Also it should be noted that traditional Virtual Private Networking (VPN) techniques will work over wireless networks in the same way as traditional wired networks.
Section Two - Wireless Networking and the Internet

Q7: How can I use a wireless network to share an Internet connection?
Ans: Once you realize that wireless cards are analogous to Ethernet cards and that empty space

is analogous to Ethernet cabling, the answer to this question becomes clear. To share an Internet connection across a LAN you need two things:

(1) an Internet sharing hardware device or software program

(2) connection to a LAN

If your LAN is wireless, the same criteria apply. You need hardware or software access point and a wireless LAN. Any computer equipped with a wireless network card running suitable Internet sharing software can be used as a software access point. (See Figure A8) A number of vendors offer hardware access points.

A hardware access point may provide Internet Sharing capabilities to Wired LAN computers, but does not usually provide much flexibility beyond very simple configurations. (See Figure A9)

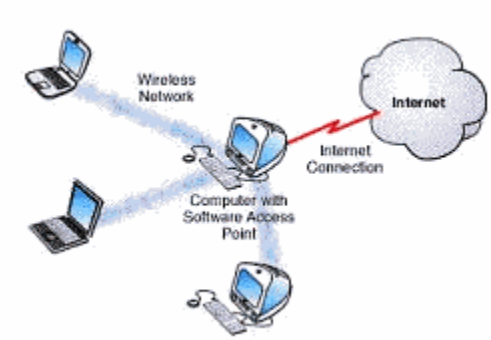


Figure A8: Software Access Point.
Wireless connected computers using a Software Access Point for shared Internet access.

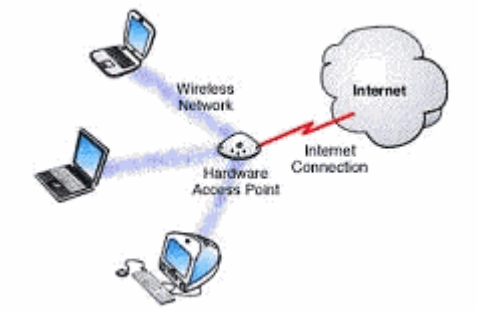


Figure A9: Hardware Access Point.
Wireless connected computers using a Hardware Access Point for shared Internet access.

Q8: How can I secure my wireless home network?

Ans: Here are 3 quick steps to help you secure your wireless network from unauthorized access. These steps are provided as general guidelines - for detailed help, please contact your hardware vendor.

1. Change the administrator password.
2. Change your SSID and turn off SSID Broadcasting
3. Enable WEP

Q9: What is Virtual Private Networking?

Ans: Typically, a Virtual Private Network (VPN) is defined as a group of two or more computer systems connected to a private network with limited public-network access that communicates securely over a public network, such as the internet: Security experts agree that VPNs include encryption, authentication of remote users or hosts, and mechanisms for hiding or masking information about private network topology from potential attackers on the public network:

Q10: What is encryption?

Ans: Encryption is a mathematical operation that transforms data from standard text to cipher text. Usually the mathematical operation requires that an alphanumeric key be supplied along with the standard text. The key plus standard text is processed by the encryption operation, which

produces secure scrambled text. Decryption is the opposite of encryption; it is the mathematical operation that transforms cipher text to standard text.

Q11: Why do I need a router?
Ans: The increased reliance on computers to store valuable information and the development of applications that share information over the internet through networked personal computers, in combination with the advent of computer hacking, has made information and network security an important issue. Typical analog modems and/or the higher-speed cable/DSL modems do not provide the necessary security to prevent someone from hacking into a computer. Having a device that provides network address translation (NAT) capability provides a simple solution to the hacking issue.

Q12: What is NAT?
Ans: Network Address Translation is used in a router to prevent hacking into the local area network (LAN). NAT substitutes a "private" IP address of devices located on the LAN side of the router with a new "public" IP address that is visible on the internet side of the router. By virtue of this simple implementation, any of up to 253 devices located on the LAN will be hidden from internet hackers. Only the router's IP address is visible on the internet.

Q13: Isn't NAT the same as "firewall"?
Ans: No. Though the term "firewall" has been used when describing a router's ability to hide the LAN IP addresses, a true firewall employs a technology called Stateful Packet Inspection (SPI). Firewalls provide a greater level of security and are generally more expensive than a NAT router. Firewalls give the administrator the ability to set up specific IP addresses or domain names that are allowed to be accessed, while refusing any other attempt to access the LAN. This is often referred to as filtering. Firewalls can also allow remote access to the private network through the use of secure login procedures and authentication certificates (VPN). Firewalls are used to prevent Denial of Service (DoS) attacks and can use software to provide content filtering to deny access to unwanted web sites.

Q14: Can the Access Point act as my DHCP Server?
Ans: No. The Access Point is nothing more than a wireless hub, and as such cannot be configured to handle DHCP capabilities.

Q15: Can I run an application from a remote computer over the wireless network?
Ans: This will depend on whether or not the application is designed to be used over a network. See the application's user guide to determine if it supports operation over a network.

Q16: What is Ad-hoc?
Ans: An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. An Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

Q17: What is Infrastructure?
Ans: An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to a central database, or wireless application for mobile workers.

Q18: What is WEP?
Ans: WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40-bit shared-key algorithm, as described in the IEEE 802.11 standard.

Q19: How do I reset the Access Point or Router?
Ans: Press the Reset button on the back of the Access Point for about ten seconds. This will reset the unit to its default settings.

Q20: Does the Access Point function as a firewall?
Ans: No. The Access Point is only a bridge from wired Ethernet to wireless clients.

Q21: What is the maximum number of users the Access Point facilitates?
Ans: It depends on the volume of data and may be less if many users create a large amount of network traffic.

Q22: What is the maximum number of IP addresses that the Router will support?
Ans: The Router will support up to 253 IP addresses.

Q23: Where is the Router installed on the network?
Ans: In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem's Ethernet port.

Q24: Does the Internet connection of the Router support 100Mbps Ethernet?
Ans: The Router's current hardware design supports up to 100Mbps Ethernet on its Internet port; however, the Internet connection speed will vary depending on the speed of your broadband connection. The Router also supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Router.

Q25: Does the Router support any operating system other than Windows 98, Windows Millennium, Windows 2000, or Windows XP?
Ans: Yes, at this time, provide technical support to setup, configuration or troubleshooting of any non-Windows operating systems.

Q26: When all else fails in the installation, what can I do?
Ans: Reset the Router by holding down the reset button until the Power LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available.

Q27: I am not able to get the web configuration screen for the Router. What can I do?
Ans :You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to direct connection to the Internet.

Q28: Can the Router act as my DHCP server?
Ans: Yes. The Router has DHCP server software built-in.

Q29: How to use Virtual Server in Wireless/Broadband Router?
Ans: It’s also called Port forwarding. Virtual Server feature allows Internet users to access standard Servers on your LAN, via the Internet IP Sharer. Normally, Internet users would not be able to access a server on your LAN because your Server does not have a valid external IP Address.

Q30: Why Wireless/Broadband Router always has problem under Cable connection but not ADSL connection?
Ans: For ADSL, one subscriber shares one line. If your ISP provides you a 512K account then you can enjoy the full 512Kbps on your side. But Cable is different. Many subscribers share the same line. For example, the bandwidth of Cable is 1.5Mbps. If there are 25 users accessing the Internet at the same time then the bandwidth of each user is 1500K/25 near 60K. The speed is just like the traditional modem connection. If there are only 5 users on line at this moment then each user can share the bandwidth to nearly 300K (1500K/5). So, the speed over ADSL is more stable than Cable. The access will hang up when the traffic is heavy over the Cable. It is the reason why many problems only happen over Cable.