ASANTÉ

FriendlyNET® FR1104-G

Cable/DSL 802.11g Wireless Firewall Router
With Integrated 4-Port 10/100 Switch

User's Manual

Asanté Technologies, Inc.
821 Fox Lane
San Jose, CA 95131
USA

FriendlyNET FR1104-G
User's Manual, Version 1.21

TECHNICAL SUPPORT
www.asante.com/support

COVER: Asanté FriendlyNET FR1104-G

Contents

Chapter 1. Introduction

The Asanté FriendlyNET FR1104-G routers give you the freedom to share your Internet connection without wires. Megapixel photos, streaming video and everyday emails with large attachments move faster through this router. With numerous international awards and accolades, Asanté has consistently delivered world-class features in all of its products. This third-generation FriendlyNET router provides higher levels of security, reliability and performance—all at an affordable price.

This *User's Manual* is a reference guide for advanced users and system administrators who configure the special features of the FR1104-G router. See the accompanying *Quick Start Guide* for basic installation information.

Tip: To understand the technical terms used in this document, use an online glossary of computer terms, like http://www.webopedia.com.

1.1 KEY FEATURES

The FriendlyNET router performs 5 key functions:

1. Shares a broadband (cable or DSL) Internet connection with multiple computers.
2. Provides a wireless access point to connect wireless computers.
3. Routes and switches traffic between the Internet (WAN), local wired network (LAN) and local wireless network (WLAN).
4. Establishes a double firewall (NAT with PF/DF) to protect against unauthorized access to the local network (LAN or WLAN).
5. Automatically issues network configuration information (DHCP service) for all computers connected on the local network (LAN or WLAN).

With over a dozen years' experience connecting Apple® Macintosh®, Windows and Linux/UNIX systems together, this FriendlyNET router incorporates several innovative features.

For medium-sized businesses, the FriendlyNET router provides advanced security and network administration features.

- Security: In addition to standard 64/128-bit WEP, there's also 256-bit WEP, stealth SSID, 802.1X RADIUS authentication, WPA, denial of service (DoS) protection and VPN pass-through tunnels.
- Administration: Wake-on-LAN management, syslog, email alerts, firewall, routing tables, NAT and SNMP (v1 and v2c). Control access by time and by content (URL, keyword).
- Performance: High-speed RISC microprocessor and Internet (WAN) port provides 10/100 Mbps (Fast Ethernet) connections.

Small businesses with limited resources can take advantage of these features.

- Forward web service requests to multiple servers (via virtual servers), hosting web servers with a single dynamic IP address (dynamic DNS).
- Simplified installation with universal plug-and-play (UPnP) support for Microsoft NetMeeting and other messaging applications.
- Support for multiple computer systems, including Windows, Mac OS and Linux/UNIX.
- Comprehensive activity log records network activities, including logins and potential security threats.

Home users will appreciate the on-screen configuration wizard and other integrated tools.

- Upgradeable wireless antenna for greater directional range.
- Compatible with dynamically configured devices, like the Microsoft Xbox game console and MSN Messenger. Application-sensing tunnels for RealPlayer, QuickTime, AOL Instant Messenger, ICQ, mIRC, Dialpad, Quake, Half-Life, Star Craft Unreal Tournament and others (user-definable).
- Integrated network utilities: ping, firmware updates and remote administration.
- Schedule parental controls: block websites by name or keywords.
- Protect wireless and wired network with hardware address (MAC) controls, advanced encryption (256-bit WEP, WPA-PSK) and stealth SSID.

1.2 Feature Enhancements

In April 2004, Asanté released firmware G1.1 which addressed some minor bugs and added three significant features:

- Wi-Fi Protected Access (WPA) security; see section 6.12, “Wireless Setting,” for more information.
- Enhanced syslog (system log); see section 9.2 for details.
- AppleTalk support.

To download the latest firmware, visit www.asante.com/support.

1.3 Special Terms

The following words have these meanings when used in this document:

- **Client**. A computer or device connected to the router’s local network (LAN) or wireless network (WLAN).
- **Internet**. The network connected to the router’s Internet port.
- **LAN**. Local area network. All clients directly (and indirectly) connected to the router’s 10/100 ports (numbered 1–4).
- **Local network**. All clients connected to the router.
- **WAN**. Wide area network. The network connected to the router’s Internet port.
- **WLAN**. Wireless local area network. All clients wirelessly connected to the router.

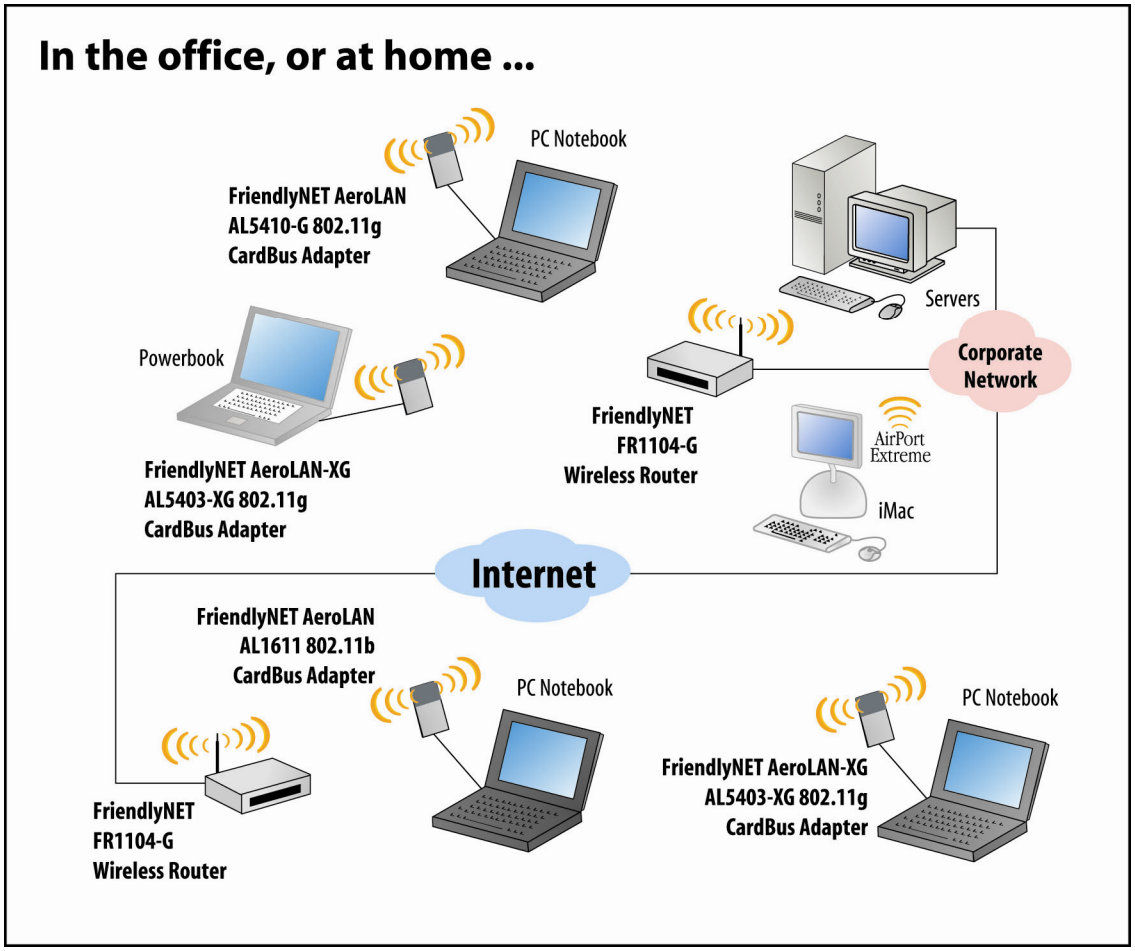
1.4 FriendlyNET Router Family

Members of Asanté’s FriendlyNET FR1000 Series include:

- FR1004, cable/DSL firewall router with integrated 4-port 10/100 switch.
- FR1004AL, same as the FR1004, but adds 802.11b wireless and parallel printer port.
- FR1104-G, same as the FR1004, but adds 802.11g wireless and advanced security and administration.

This manual only describes the **FriendlyNET FR1104-G** wireless router.

1.5 TYPICAL INSTALLATION



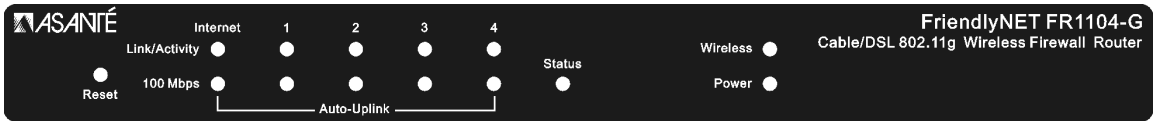
- Place the router in a central location of your business or home. This allows the router to provide maximum wireless range—while minimizing access by external users.
- Although the router supports both 802.11b (11 Mbps) and 802.11g (54 Mbps) speeds, whenever possible choose 802.11g adapters for your computers and peripherals. The router will deliver maximum performance at 802.11g.

Chapter 2. Hardware Details

This chapter describes the FriendlyNET router hardware.

2.1 FRONT PANEL

The FriendlyNET router provides color-coded indicators to show the status of various functions.



- **Reset**. To restore the router to factory default settings, hold the recessed reset button for about 5 seconds. The Status LED should flash 5 times. Release the button.

LED	Function	Description
Internet	Internet Link/Activity	On when properly linked to a cable/DSL modem. Blinks with activity.
	Internet 100 Mbps	On when connected at 100 Mbps; off at 10 Mbps.
1 through 4	LAN Link/Activity	On when properly linked to a local computer. Blinks with activity.
	LAN 100 Mbps	On when connected at 100 Mbps; off at 10 Mbps.
Status	System Status	Blinks during power-on self-test and reset.
Wireless	Wireless Activity	Blinks with activity.
Power	Power	System is powered on.

2.2 REAR PANEL

Looking at the router from the rear, the following connectors are available.

Port	Function	Description
5 VDC	Power Input	Plug in the Asanté FR1104 external **power module** rated at 5 VDC, 1.5 A (minimum).
1 through 4	LAN Ports	Plug in a cable from your **computer** to one of these ports. 10/100BaseT Fast Ethernet (RJ-45 connector). Auto-Uplink™ supports any standard or "crossover" cable. These computers are on your local area network (LAN).
Internet	Internet	Plug in a cable from your **cable/DSL modem** to this port. 10/100BaseT Fast Ethernet (RJ-45 connector). Auto-Uplink supports any standard or "crossover" cable. Sometimes this port is also called the wide area network (WAN).
Wireless	Antenna	Replaceable **antenna** (RP-SMA connector). Computers wirelessly connected to the router are known as the wireless LAN (WLAN).

The LAN (numbered 1–4) and Internet ports are wired according to standard 100BaseTX standards:

Pin Number	Signal	Direction
1	TX+	Out
2	TX-	Out
3	RX+	In
4	—	
5	—	
6	RX-	In
7	—	
8	—	

Tip: Need to connect more than 4 wired computers or devices to this router? Use a Category 5 UTP Fast Ethernet cable and connect it from your switch (or hub) to this router. The router's Auto-Uplink feature will automatically configure the port for "uplink" (MDI).

2.3 BOTTOM VIEW

The bottom of the router contains three sections:

- Holes for wall or desktop mounting (screws sold separately).
- Rubber feet (user-installable).
- Product identification label showing model number (i.e., FR1104-G), regulatory information (compliance with FCC and CE), warranty and service information and other details.

Chapter 3. Configuring Router

The FriendlyNET router is configured using any standard web browser:

- Internet Explorer (v5 and later).
- Netscape (v5 and later).
- Safari (v1 and later).

The default IP address for the router is 192.168.123.254 with default subnet mask 255.255.255.0.

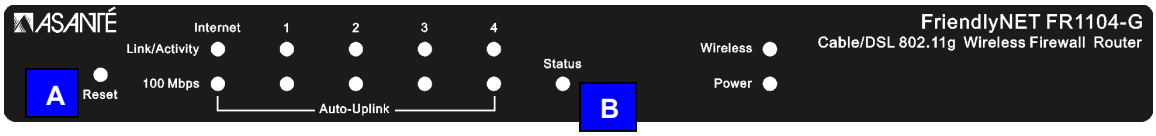
To log in:

1. Enter the router's default system password: **admin**
2. Click **Log in** button.

3.1 Troubleshooting Tips

If the main screen (as shown above) does not appear, check the following:

- Use the 10/100 Fast Ethernet cable (supplied with the router) to connect to the router. Verify that the green LED is on for both the router and your computer's network connection.
- Ping the router using this command: **ping 192.168.123.254**
- Disconnect all other network devices (if any).
- Restart the router (disconnect the power, then re-connect), then re-start your computer(s).

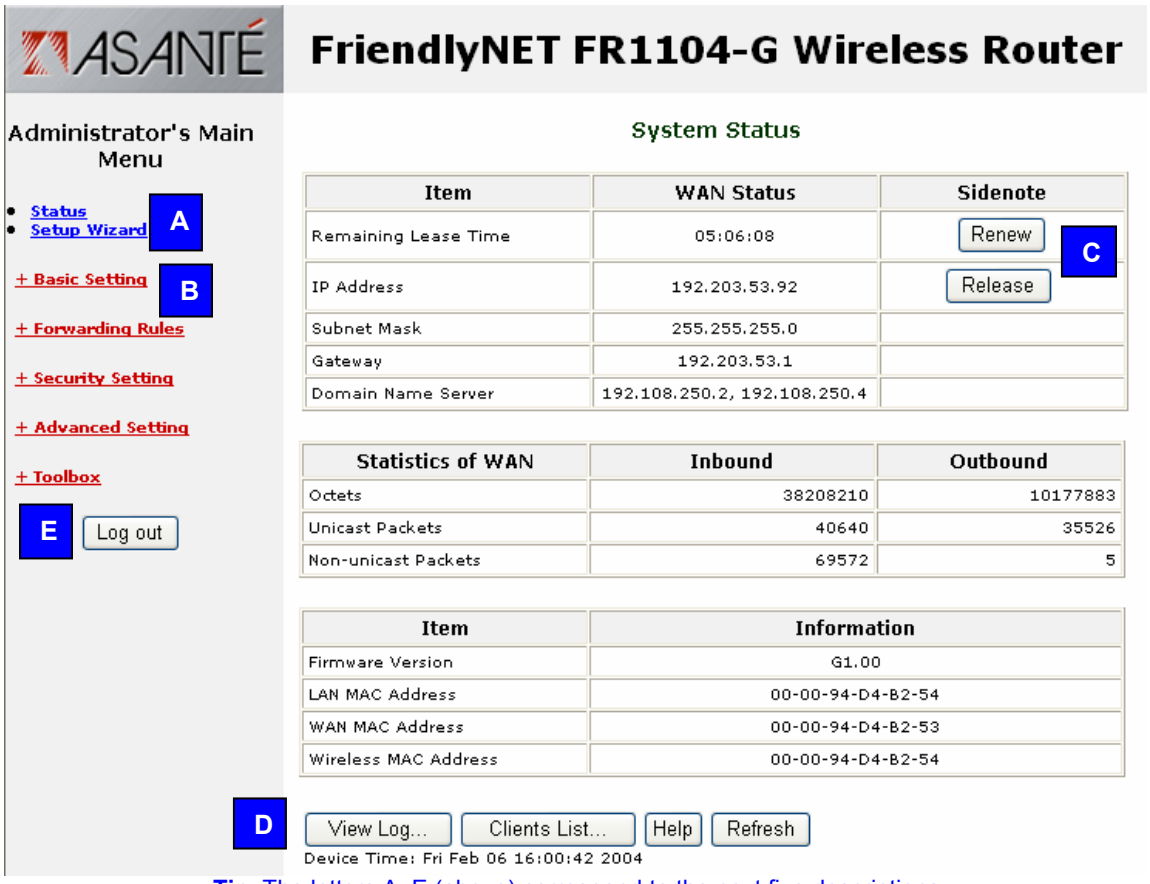


If the main screen still does not appear (or your password is not accepted), reset the router to factory default settings.

1. Locate the recessed **Reset** button on the router's front panel [A].
2. Depress the button using a pencil or blunt end of a paper clip.
3. Hold the recessed reset button for about 5 seconds. The Status LED [B] should flash 5 times.
4. Release the **Reset** button.

Chapter 4. Main Menu

Upon successfully logging into the router, the System Status page will be displayed:



Tip: The letters A–E (above) correspond to the next five descriptions.

A. This screen shows the status of the router and its connections. To return to this screen, click Status from the menu at the left. To set up this router for the first time, click **Setup Wizard**. Follow the on-screen instructions. See *Quick Start Guide* poster for details.

B. To configure the router's more advanced features, choose from the following 5 menus.

Menu	Functions
Basic Setting	Primary Setup: LAN IP, WAN type, renew IP forever, NAT DHCP Server: IP pool starting/ending address, fixed mapping Wireless: SSID, channel, WEP, 802.1X, MAC address control Change Password
Forwarding Rules	Virtual Server: service port, server IP, rule # Special Applications: trigger, incoming ports Miscellaneous: DMZ host, FTP port
Security Settings	Packet Filters: source, destination, rule # Domain Filters: log, privilege IP, domain suffix, log/drop URL Blocking: URL MAC Control: connection/association control, MAC address, IP address Miscellaneous: remote administrator, discard ping, SPI, DoS detection, VPN pass-through
Advanced Setting	System Time: NTP, manual, daylight savings System Log: syslog server, email alert, log type, view log Dynamic DNS: DDNS, provider, host, user name and password SNMP: community, IP 1–4, version Routing: dynamic, static, destination, mask, gateway, hop Schedule Rule: name, Sunday–Saturday, start/end time
Toolbox	View log, firmware upgrade, backup setting, reset to default, reboot, miscellaneous (Wake-on-LAN admin, ping domain/IP address)

C. If your router loses its connection to the Internet, click **Release** and then **Renew**.
D. **View Log** reports the status of all login and connection attempts. **Clients List** shows all the computers and other devices directly connected to the router's LAN or WLAN.
E. To maintain security, **Log out** of the router when you have finished viewing or changing settings.

4.1 WAN STATUS

Item	WAN Status	Sidenote
Remaining Lease Time	05:52:50	Renew
IP Address	192.203.53.92	Release
Subnet Mask	255.255.255.0	
Gateway	192.203.53.1	
Domain Name Server	192.108.250.2, 192.108.250.4	

These items describe the status of the router's Internet (WAN) port.

- Remaining Lease Time. The router's IP address is dynamically set by your Internet service provider (ISP). This is the time remaining for the IP address shown in the next item. When this time expires, the router can automatically re-connect (renew IP forever); see the router's Basic Settings > Primary Setup menu.
- IP Address. The router's unique identifier. Each IP address has four numbers separated by 4 periods; each number can range from 0 to 255.
- Subnet Mask. Default is 255.255.255.0. This router can handle a Class C network with up to 253 devices.
- Gateway. The IP address for the ISP that connects this router to the Internet. To verify that your ISP is up, ping this gateway address.

- Domain Name Server (DNS). The Internet server used to translate names into IP addresses. The *www.asante.com* domain name translates to *207.176.137.22.*

4.2 WAN STATISTICS

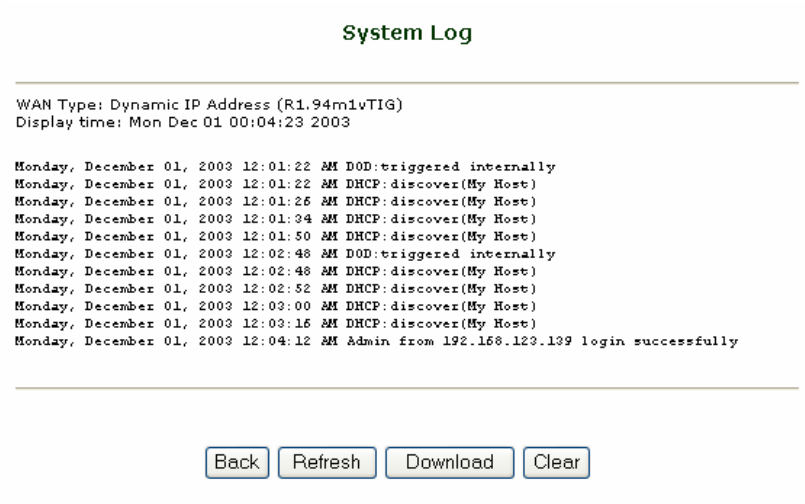
Item	WAN Status	Sidenote
Remaining Lease Time	05:52:50	Renew
IP Address	192.203.53.92	Release
Subnet Mask	255.255.255.0	
Gateway	192.203.53.1	
Domain Name Server	192.108.250.2, 192.108.250.4	

These items quantify the types of traffic received (inbound from Internet) and sent (outbound to Internet) by the router.

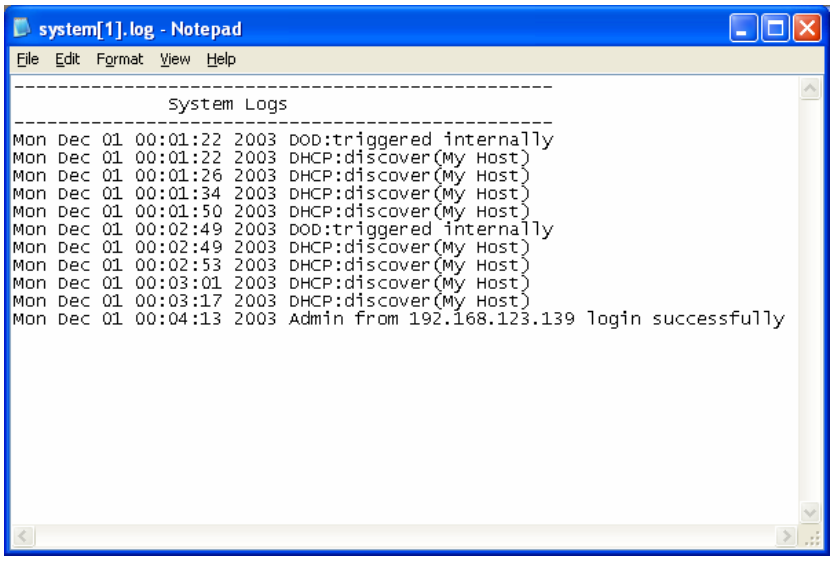
- Octets: Equivalent to a byte (8-bits) of information.
- Unicast Packets: Data sent by a single sender to a single recipient.
- Non-Unicast Packets: Other data sent. Typically by a message from a single sender to a select group of recipients (multicast) or everyone connected to the network (broadcast).

4.3 SYSTEM LOG

Click on **View Log** to display the System Log screen.

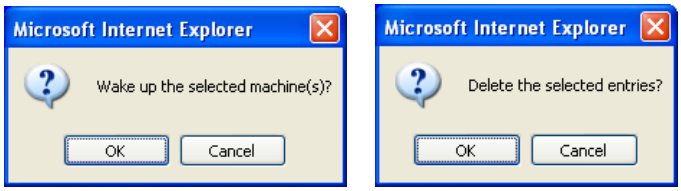


After the log information is displayed on the screen, click **Refresh** to update with the latest activities.
To save the log into a text file, click **Download**.
To reset the log, click **Clear**.
To return to the previous menu, click **Back**.



Tip: This log may be emailed or automatically stored on a syslog server. See Advanced Settings > System Log.

4.4 CLIENTS LIST



- Wake up. Wake-on-LAN (WoL) is a technology used to remotely power-up a network device. To use this feature, your target computers must be WoL-enabled. To wake up a device, select the device [A] and click **Wake up** [B]. Confirm your selection by clicking **OK** on the dialog box.
- Delete. Select client [A] and click **Delete**. Confirm your deletion by clicking **OK** on the dialog box.The entry will be deleted from this list.

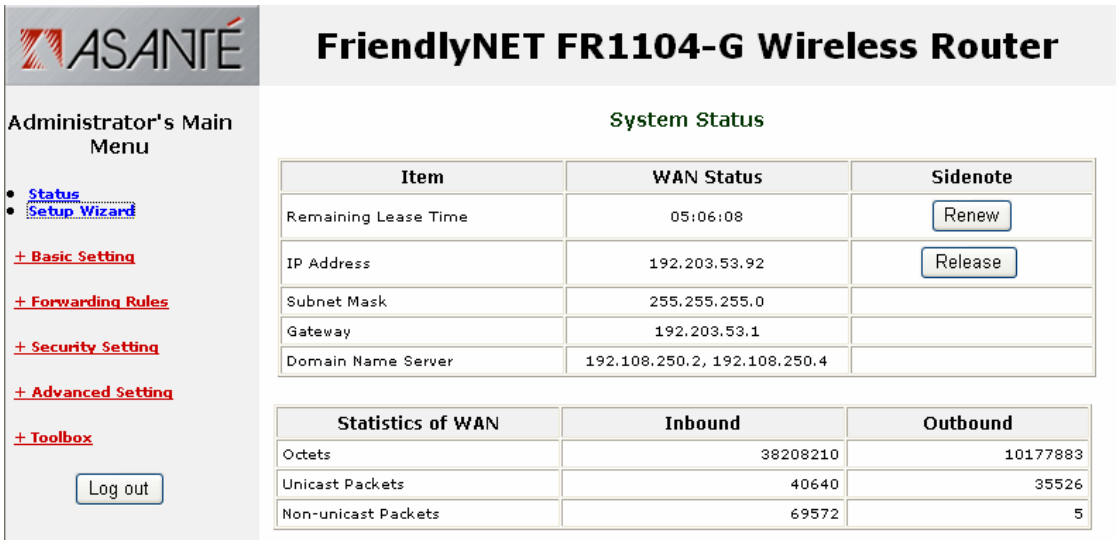
Tip: If you are sharing resources (files or printers) on the local network (LAN or WLAN), wake up the computer using the WoL feature described above.

4.4 ADMINISTRATOR TIME-OUT

For security reasons, the router administration will automatically terminate your session after a set period of inactivity. To set this idle time, see Security Settings > Miscellaneous > Administrator Time-Out.

Chapter 5. Setup Wizard

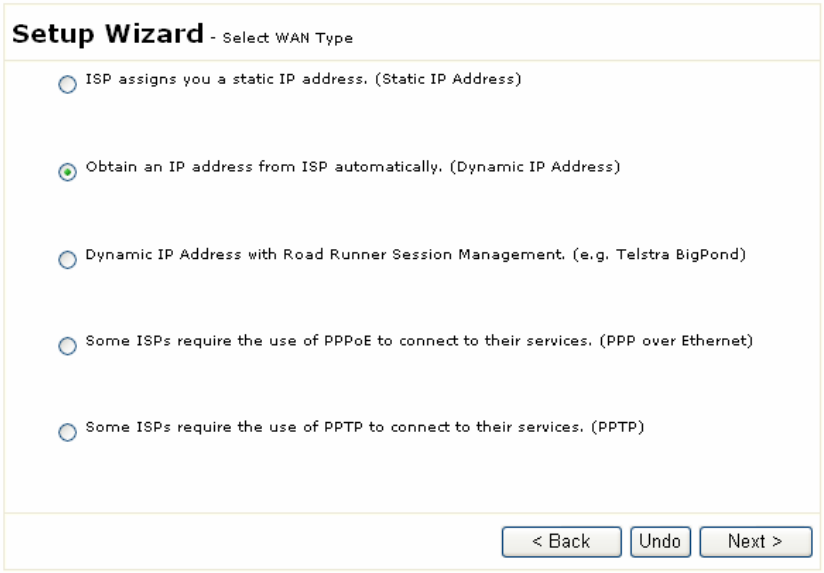
If your router has already been configured, skip to chapter 6. Otherwise, login to the router, and configure your router using the *Setup Wizard*.



From the menu on the left, click **Setup Wizard**.

Click **Next** to proceed to the next screen.

5.1 SELECT WAN TYPE



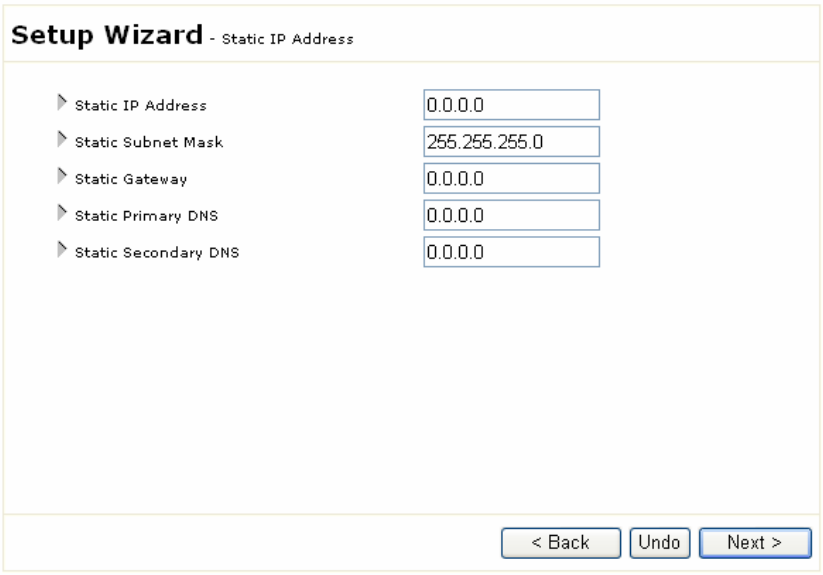
Choose from these Internet (WAN) types:

- Static IP Address. ISP assigns you a static IP address.
- Dynamic IP Address. Obtain an IP address from ISP automatically. This is the most common configuration (especially for cable modem users) and is the router's default setting.
- Dynamic IP Address (Special). Select this if your ISP is Road Runner or Telstra BigPond.
- PPP over Ethernet. Some ISPs require the use of PPPoE to connect to their services. This is the most popular setting for DSL accounts.
- PPTP. Some ISPs require the use of PPTP to connect to their services.

Tip: When in doubt, use the default (Dynamic IP Address) setting—it's the most popular setting. If it doesn't work, you can try one of the others.

This router uses context-sensitive menus. After making a selection, a detailed configuration page will prompt you to complete information specific to your Internet connection.

5.2 STATIC IP ADDRESS

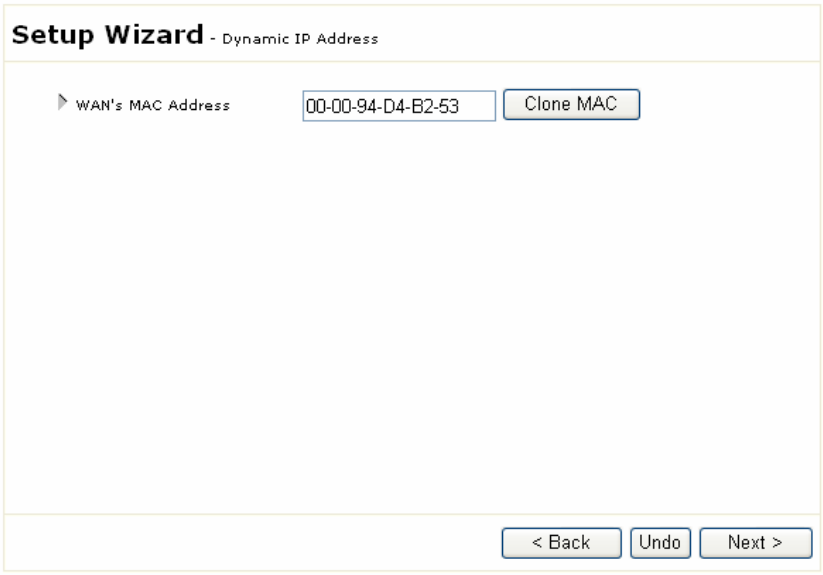


The following information must be provided by your ISP. If your ISP did not provide this info, you may have a dynamic IP address; choose one of the other settings:

- Static IP Address. The router's Internet (WAN) IP address.
- Static Subnet Mask. Default is 255.255.255.0
- Static Gateway. The IP address for the ISP that connects this router to the Internet. To verify that your ISP is up, ping this gateway address.
- Static Primary DNS. The Internet server used to translate names into IP addresses.
- Static Secondary DNS. Optional.

Click **Next** to proceed to the next screen ("Configuration Completed"); see section 5.7.

5.3 DYNAMIC IP ADDRESS



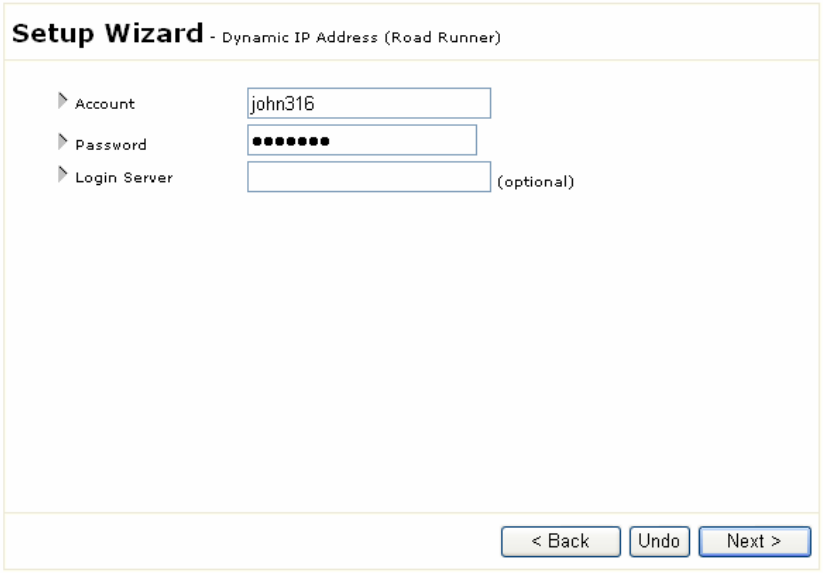
In most cases, you will not need to make any changes. Click **Next** to proceed to the next screen.

The following setting is optional. Most ISPs will not require this info.

- WAN's MAC Address. Some ISPs limit the use of routers. Click **Clone MAC** to have the router use the MAC address of this computer.

Click **Next** to proceed to the next screen ("Configuration Completed"); see section 5.7.

5.4 DYNAMIC IP ADDRESS (ROAD RUNNER)

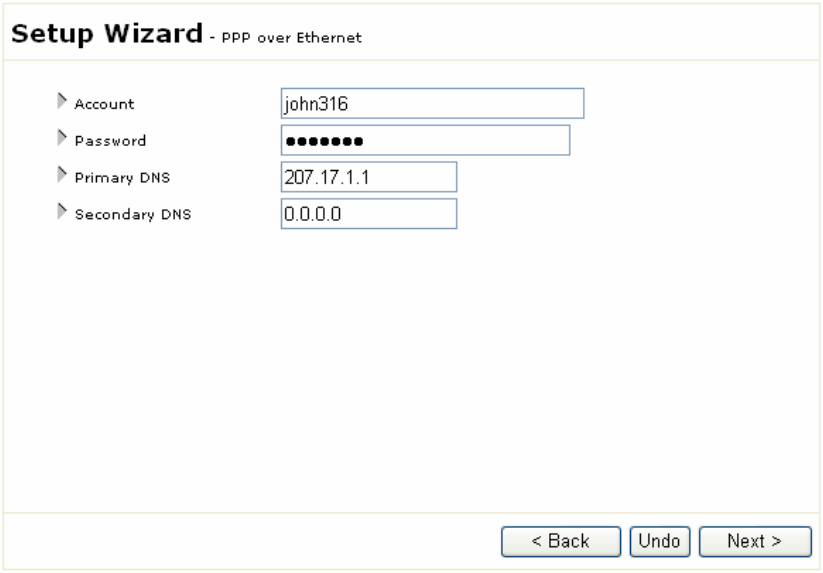


The following information must be provided by your ISP:

- Account. Your user account name.
- Password. Your account password.
- Login Server. Optional.

Click **Next** to proceed to the next screen (“Configuration Completed”); see section 5.7.

5.5 PPP OVER ETHERNET (PPPOE)

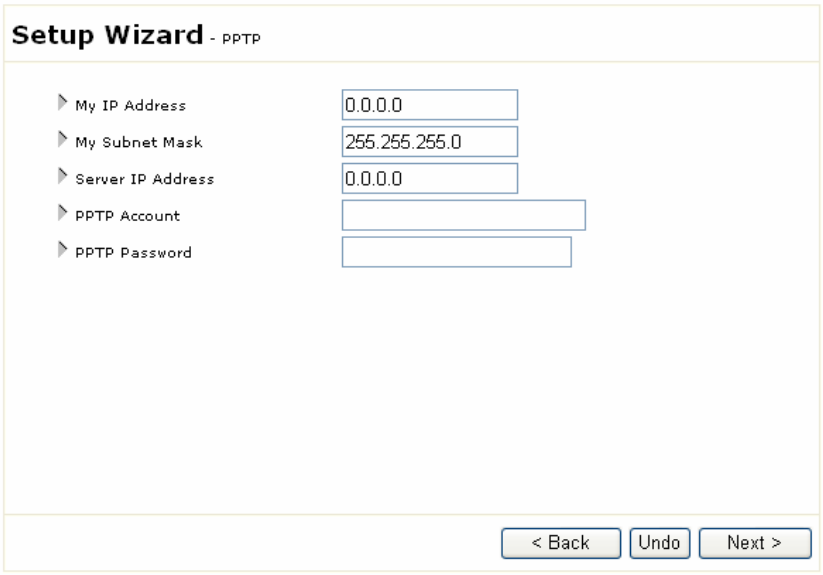


The following information must be provided by your ISP:

- Account. Your user account name. For security reasons, this field appears blank the next time you see this screen.
- Password. Your account password. For security reasons, this field appears blank the next time you see this screen.
- Primary DNS. The Internet server used to translate names into IP addresses.
- Secondary DNS. Optional.

Click **Next** to proceed to the next screen (“Configuration Completed”); see section 5.7.

5.6 POINT-TO-POINT TUNNELING PROTOCOL (PPTP)



The following information must be provided by your ISP:

- My IP Address. The router's Internet (WAN) IP address.
- My Subnet Mask. Default is 255.255.255.0
- Server IP Address. The IP address for your ISP's server (gateway) that connects this router to the Internet. To verify that your ISP is up, ping this gateway address.
- PPTP Account. Your user account name.
- PPTP Password. Your account password.

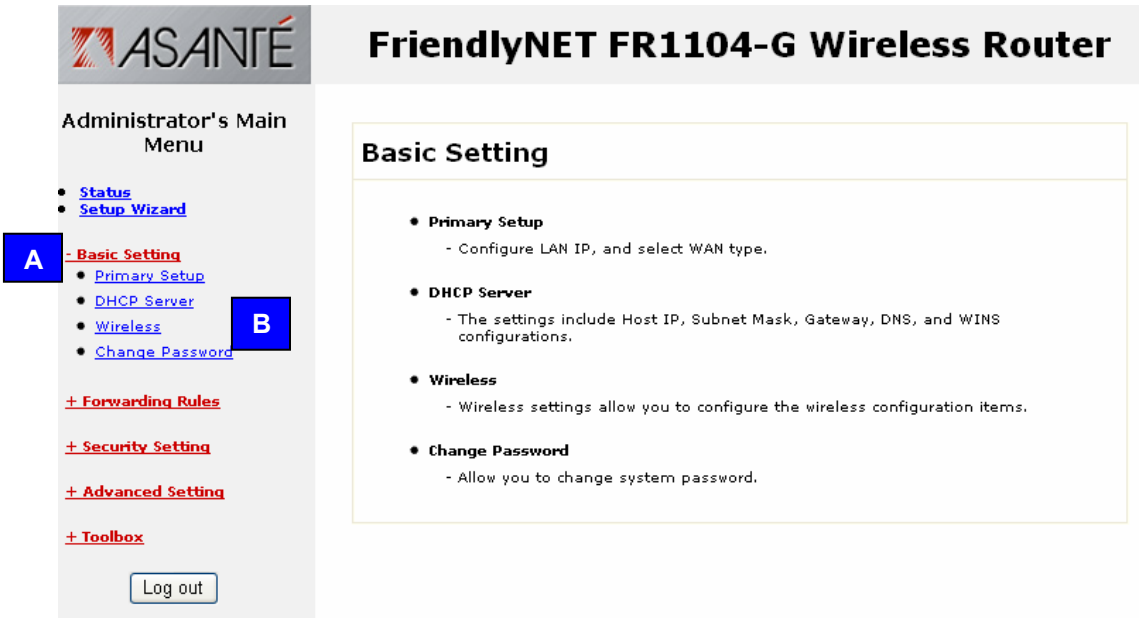
Click **Next** to proceed to the next screen ("Configuration Completed"); see section 5.7.

5.7 CONFIGURATION COMPLETED

1. Click **Reboot** to restart your router. Your installation is complete.
2. To verify your installation, visit a website, like www.asante.com. If you are unable to connect to a website, then restart your computer(s).

Chapter 6. Basic Setting

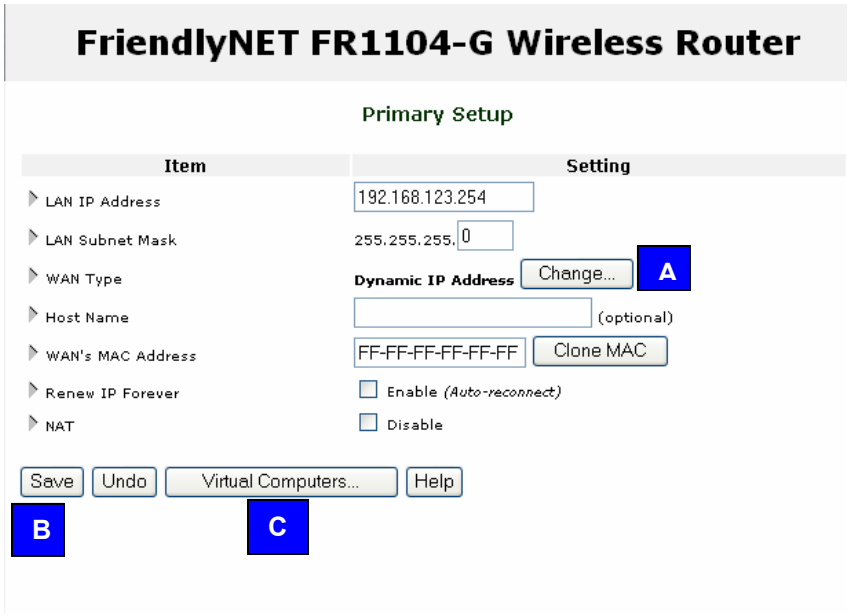
After using the Setup Wizard, described in the previous chapter, you may fine-tune your configuration.



Log in to the router, click **Basic Setting** link [A] and choose from one of the four sub-menus [B].

Basic Setting	Functions
Primary Setup	LAN IP, WAN type, renew IP forever, NAT
DHCP Server	IP pool starting/ending address, fixed mapping
Wireless	SSID, channel, WEP, 802.1X, MAC address control
Change Password	Router administration password

6.1 PRIMARY SETUP – DYNAMIC IP ADDRESS



In most cases, you will not need to make any changes.

- LAN IP Address. The router's LAN IP address and the gateway address for computers on your network (LAN and WLAN). In most cases, **do not** change the default value (192.168.123.254).
- LAN Subnet Mask. Default is 255.255.255.0

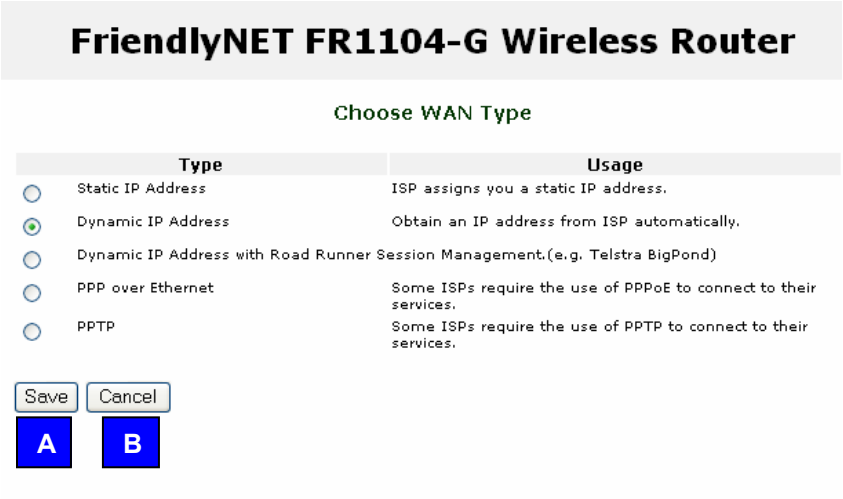
This is a dynamic screen. To minimize confusion, only the fields used in your configuration are shown here. The following fields will appear when the WAN Type is **Dynamic IP Address**. Other fields will appear when the WAN Type is changed.

- WAN Type. Dynamic IP Address is the default. See the next section for details on the various WAN Type settings. To change the specified WAN Type, click **Change.** See 6.2, "Choose WAN Type."
- Host Name. Required by some ISPs.
- WAN's MAC Address. Some ISPs limit the use of routers. Click **Clone MAC** to have the router use the MAC address of this computer.
- Renew IP Forever. Enable to allow the router to automatically re-connect when the lease time expires.
- NAT. By default, Network Address Translation (NAT) is enabled. This allows the router to share a single Internet (WAN) IP address with multiple computers connected to the LAN or WLAN. If you are using the router only as a firewall or wireless access point, you may want to disable NAT.

After making changes, be sure to click **Save** [B].
To restore the last saved settings, click **Undo**.
To assign virtual servers, click **Virtual Computers** [C]. See 6.8, "Virtual Computers."
To read on-screen information on this page, click **Help**.

6.2 CHOOSE WAN TYPE

After clicking **Change** from the Basic Setting > Primary Setup screen, you will see this:



Choose from these Internet (WAN) types:

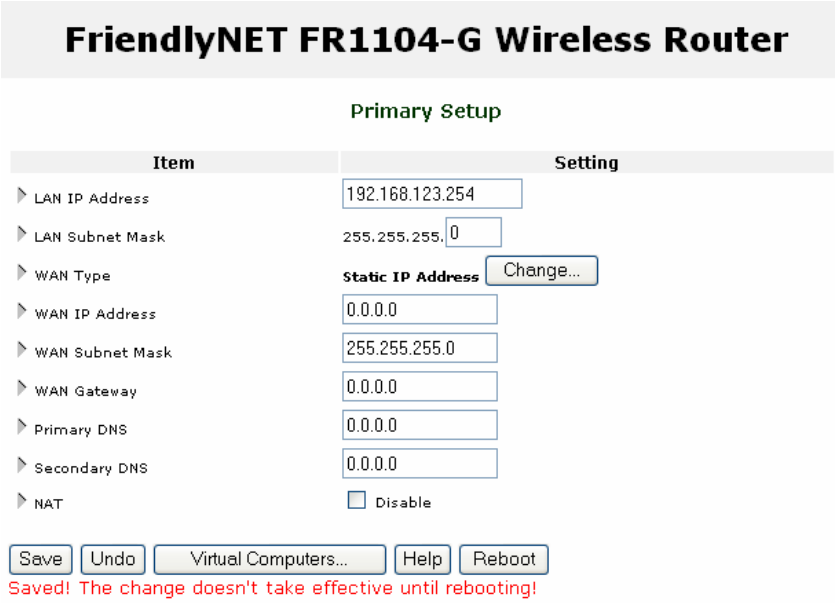
- Static IP Address. ISP assigns you a static IP address.
- Dynamic IP Address. Obtain an IP address from ISP automatically. This is the most common configuration and the router's default setting.
- Dynamic IP Address (Special). Select this if your ISP is Road Runner or Telstra BigPond.
- PPP over Ethernet. Some ISPs require the use of PPPoE to connect to their services.
- PPTP. Some ISPs require the use of PPTP to connect to their services.

After making a selection, a context-sensitive page will prompt you to complete information specific to your Internet connection. The information on the following pages provides more settings than the corresponding pages in the Setup Wizard.

Warning! You should have a comprehensive working knowledge of networking, the Internet and TCP/IP before making any changes on the following pages. Improper configuration may adversely affect your Internet connection.

A. Choose your WAN type and click **Save** to save your changes and proceed to the next screen.
B. To abandon your changes and restore your last saved changes, click **Cancel**.

6.3 PRIMARY SETUP - STATIC IP ADDRESS



- LAN IP Address. The router's LAN IP address and the gateway address for computers on your network (LAN and WLAN). In most cases, **do not** change the default value (192.168.123.254).
- LAN Subnet Mask. Default is 255.255.255.0
- WAN Type. Static IP Address.

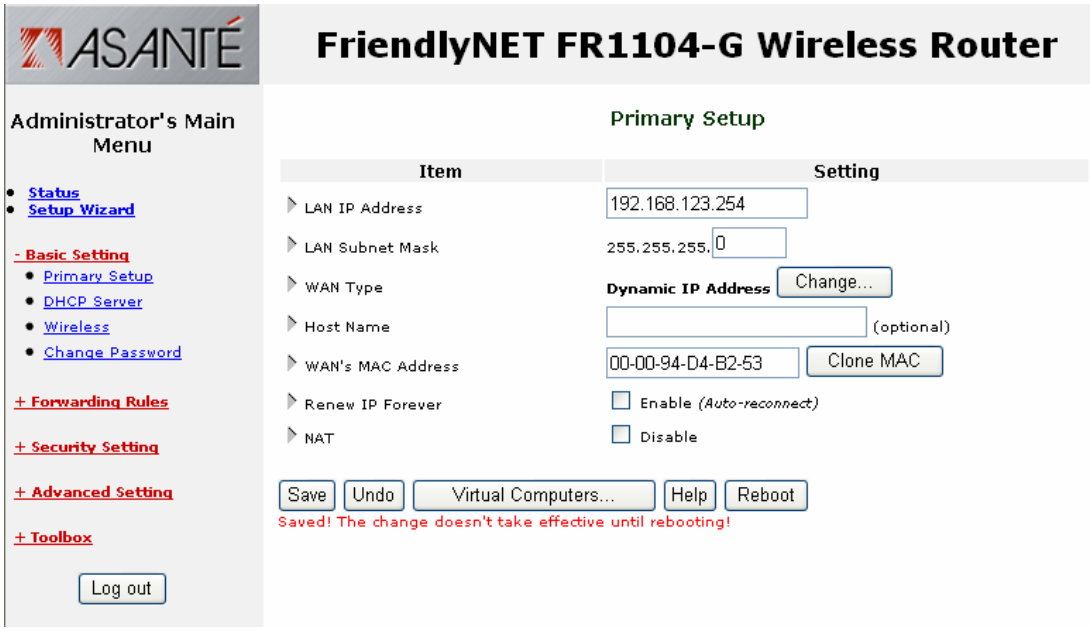
The following fields will appear when the WAN Type is **Static IP Address**. Other fields will appear when the WAN Type is changed. The following information must be provided by your ISP:

- WAN IP Address. The router's Internet (WAN) IP address.
- WAN Subnet Mask. Default is 255.255.255.0
- WAN Gateway. The IP address for the ISP that connects this router to the Internet. To verify that your ISP is up, ping this gateway address.
- Primary DNS. The Internet server used to translate names into IP addresses.
- Secondary DNS. Optional.
- NAT. By default, Network Address Translation (NAT) is enabled. This allows the router to share a single Internet (WAN) IP address with multiple computers connected to the LAN or WLAN. If you are using the router only as a firewall or wireless access point, you may want to disable NAT.

  Tip: If you disable NAT, you may need to have a DHCP server to assign IP addresses to your clients (or manually enter static IP addresses). You may also need to assign routing information.

After making changes, click **Save** and **Reboot** to restart the router.
To restore the last saved settings, click **Undo**.
To assign virtual servers, click **Virtual Computers** [C]. See 6.8, "Virtual Computers."
To read on-screen information on this page, click **Help**.

6.4 PRIMARY SETUP - DYNAMIC IP ADDRESS



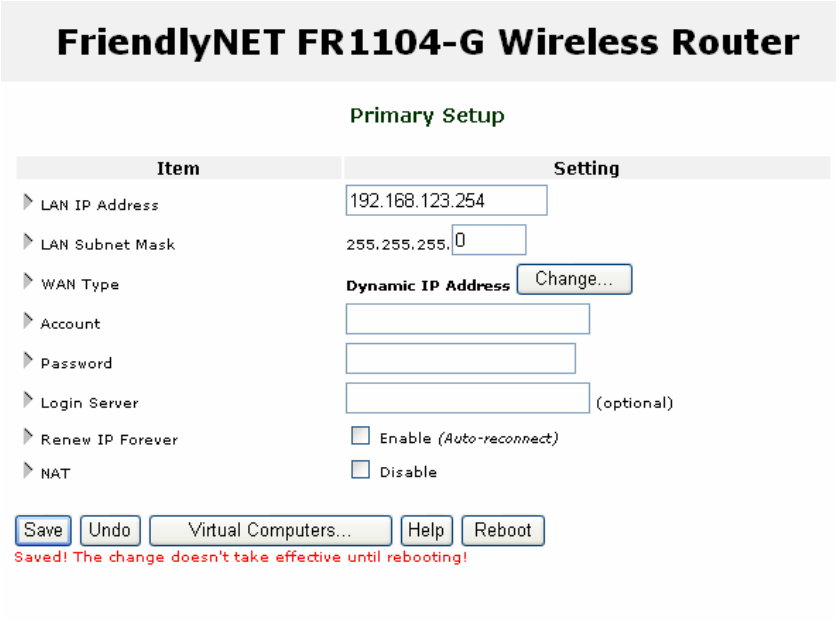
- LAN IP Address. The router's LAN IP address and the gateway address for computers on your network (LAN and WLAN). In most cases, **do not** change the default value (192.168.123.254).
- LAN Subnet Mask. Default is 255.255.255.0
- WAN Type. Dynamic IP Address.

The following fields will appear when the WAN Type is **Dynamic IP Address**. Other fields will appear when the WAN Type is changed. The following information must be provided by your ISP:

- Account. Your user account name. For security reasons, this field appears blank.
- Password. Your account password. For security reasons, this field appears blank.
- Login Server. Optional.
- Renew IP Forever. Enable to allow the router to automatically re-connect when the lease time expires.
- NAT. By default, Network Address Translation (NAT) is enabled. This allows the router to share a single Internet (WAN) IP address with multiple computers connected to the LAN or WLAN. If you are using the router only as a firewall or wireless access point, you may want to disable NAT.

After making changes, click **Save** and **Reboot** to restart the router.
To restore the last saved settings, click **Undo**.
To assign virtual servers, click **Virtual Computers** [C]. See 6.8, "Virtual Computers."
To read on-screen information on this page, click **Help**.

6.5 PRIMARY SETUP - DYNAMIC IP ADDRESS (ROAD RUNNER)



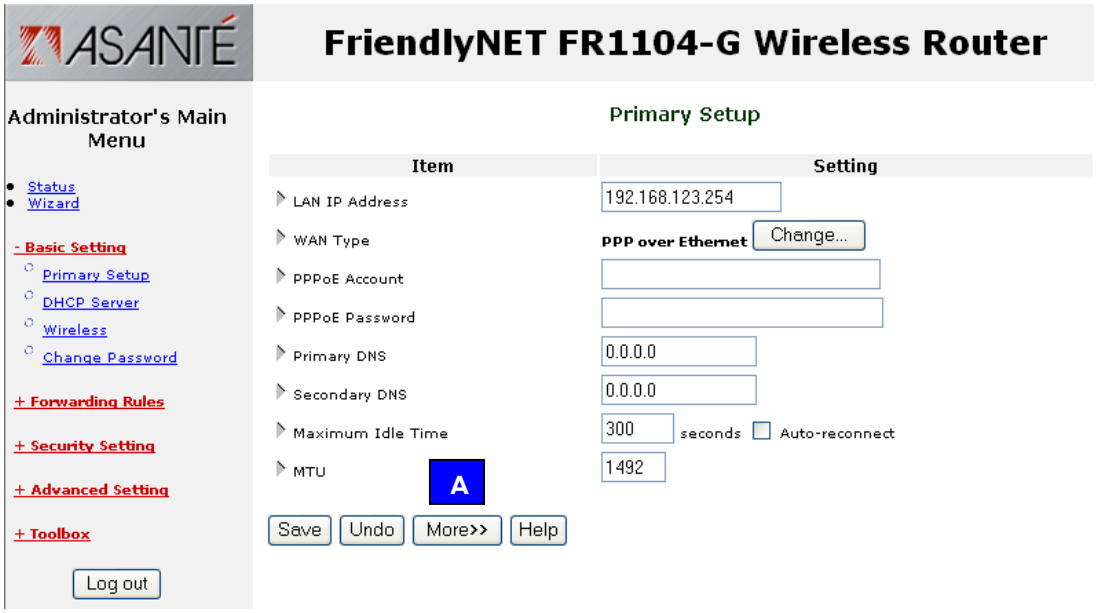
- LAN IP Address. The router's LAN IP address and the gateway address for computers on your network (LAN and WLAN). In most cases, **do not** change the default value (192.168.123.254).
- LAN Subnet Mask. Default is 255.255.255.0
- WAN Type. Dynamic IP Address.

The following fields will appear when the WAN Type is **Dynamic IP Address**. Other fields will appear when the WAN Type is changed. The following information must be provided by your ISP.

- Account. Your user account name. For security reasons, this field appears blank.
- Password. Your account password. For security reasons, this field appears blank.
- Login Server. Optional.
- Renew IP Forever. Enable to allow the router to automatically re-connect when the lease time expires.
- NAT. By default, Network Address Translation (NAT) is enabled. This allows the router to share a single Internet (WAN) IP address with multiple computers connected to the LAN or WLAN. If you are using the router only as a firewall or wireless access point, you may want to disable NAT.

After making changes, click **Save** and **Reboot** to restart the router.
To restore the last saved settings, click **Undo**.
To assign virtual servers, click **Virtual Computers** [C]. See 6.8, "Virtual Computers."
To read on-screen information on this page, click **Help**.

6.6 PRIMARY SETUP - PPP OVER ETHERNET (PPPOE)



- LAN IP Address. The router's LAN IP address and the gateway address for computers on your network (LAN and WLAN). In most cases, **do not** change the default value (192.168.123.254).
- WAN Type. PPP over Ethernet.

The following fields will appear when the WAN Type is **PPP over Ethernet**. Other fields will appear when the WAN Type is changed. The following information must be provided by your ISP.

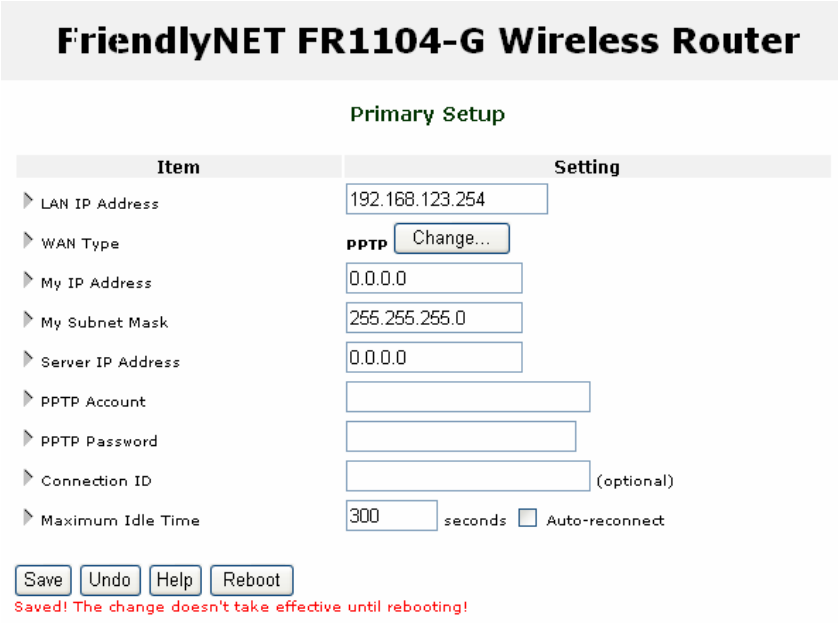
- PPPoE Account. Your user account name. For security reasons, this field appears blank.
- PPPoE Password. Your account password. For security reasons, this field appears blank.
- Primary DNS. The Internet server used to translate names into IP addresses.
- Secondary DNS. Optional.
- Maximum Idle Time. The amount of inactivity before disconnecting your session. To disable this feature, set the value to 0 or choose Auto-reconnect.
- MTU. Optional. You may set the maximum transmit unit (MTU) value. The most common setting is 1492 (bytes).

Click **More** [A] to see these additional settings.

- PPPoE Service Name. Optional.
- Assigned IP Address. Optional.

After making changes, click **Save** and **Reboot** to restart the router.
To restore the last saved settings, click **Undo**.
To assign virtual servers, click **Virtual Computers** [C]. See 6.8, "Virtual Computers."
To read on-screen information on this page, click **Help**.

6.7 PRIMARY SETUP - POINT-TO-POINT TUNNELING PROTOCOL (PPTP)



- LAN IP Address. The router's LAN IP address and the gateway address for computers on your network (LAN and WLAN). In most cases, **do not** change the default value (192.168.123.254).
- WAN Type. PPTP.

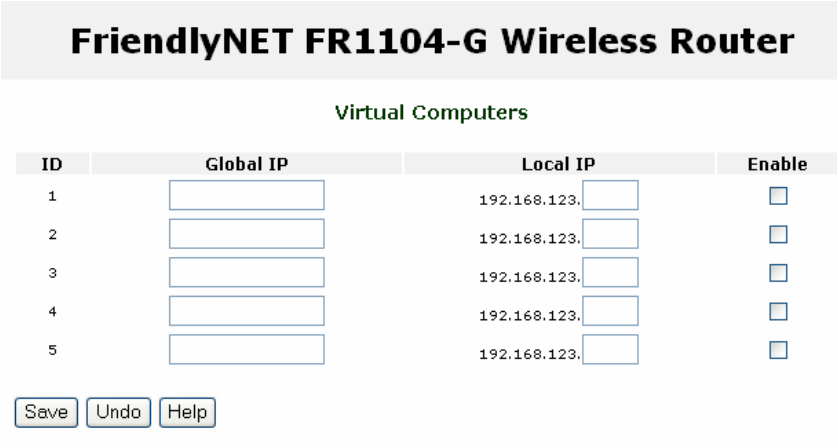
The following fields will appear when the WAN Type is **PPTP**. Other fields will appear when the WAN Type is changed. The following information must be provided by your ISP.

- My IP Address. The router's Internet (WAN) IP address.
- My Subnet Mask. Default is 255.255.255.0
- Server IP Address. The IP address for your ISP's server (gateway) that connects this router to the Internet. To verify that your ISP is up, ping this gateway address.
- PPTP Account. Your user account name. For security reasons, this field appears blank.
- PPTP Password. Your account password. For security reasons, this field appears blank.
- Connection ID. Optional.
- Maximum Idle Time. The amount of inactivity before disconnecting your session. To disable this feature, set the value to 0 or choose Auto-reconnect.

After making changes, click **Save** and **Reboot** to restart the router.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

6.8 PRIMARY SETUP - VIRTUAL COMPUTERS

From the Primary Setup screen, click **Virtual Computers**.



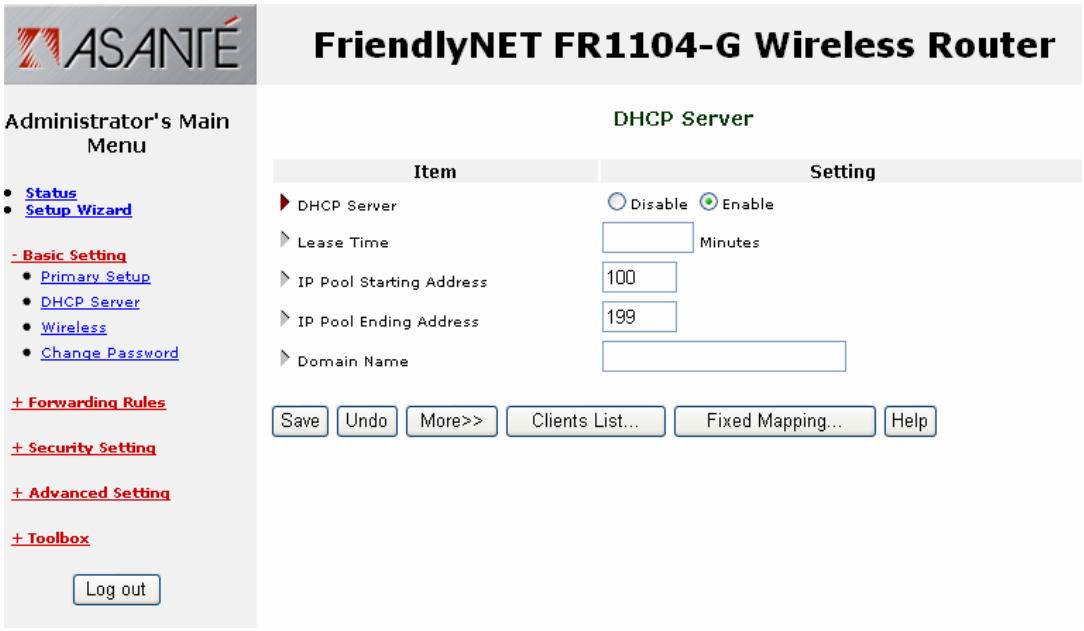
Some business-class Internet service plans provide multiple static IP addresses. If you subscribe to such a service, you can use the router's firewall and other features to protect the computers behind the router. Virtual Computer maps one external (WAN, Internet) IP Address to one local (LAN, WLAN) IP address. If you only have 1 static IP address, do not enter it into this table.

- Global IP. Enter an external IP address provided by your ISP.
- Local IP. Enter a local IP address. The first 3 octets (192.168.123) are defined in the WAN Type, LAN IP Address.
- Enable. Check this item to enable this mapping.

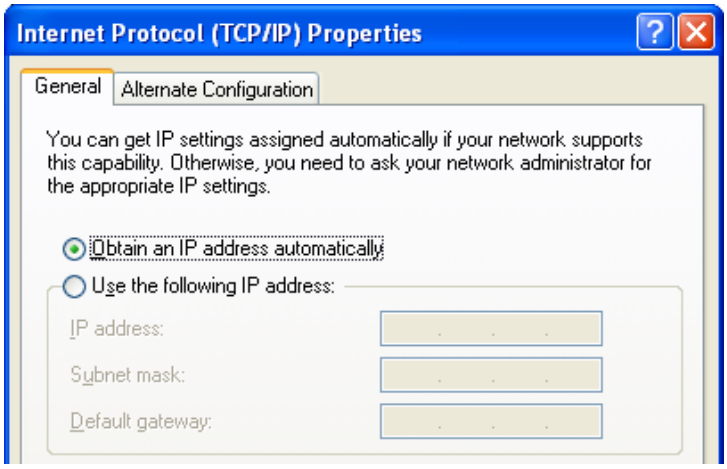
Note: A Virtual *Computer* is different from a Virtual *Server* (chapter 7). A virtual server re-directs Internet services to a specific computer. A virtual computer maps an external fixed IP address to a specific computer on the internal network.

6.9 DHCP SERVER

From the Basic Settings menu, click **DHCP Server**.



All computers and devices connected to the router need to be configured. Since TCP/IP configuration can be tedious, the router's dynamic host configuration protocol (DHCP) service can automatically configure each computer set for "Obtain an IP address automatically."



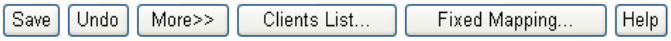
Tip: To check if your computer can accept the router's DHCP settings, see your computer's network properties. On Windows XP, it's found in the Control Panel > Network Connections > Local Area Connection (or equivalent) > Properties. In the dialog box, choose Internet Protocol (TCP/IP) > Properties.

The DHCP Server settings can be set as follows:

- DHCP Server. Default is Enable (recommended).
- Lease Time. Do not change this field (recommended).
- IP Pool Starting Address. Default is 100 (recommended), minimum value is 1. This field controls the last octet of your network (LAN and WLAN) IP address range. By default, the router uses 192.168.123.**100** through 192.168.123.**199**
- IP Pool Ending Address: 199. Maximum value is 253 (if the router is set for 192.168.123.254).
- Domain Name. Optional. This information is passed to computers and devices on your local network.

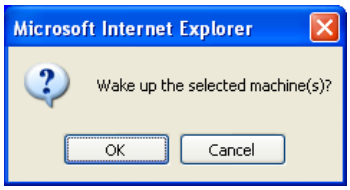
Click on **More** to configure these optional settings.

- Primary DNS. IP address of domain name server.
- Secondary DNS.
- Primary WINS. IP address of Microsoft NetBIOS name server.
- Secondary WINS.
- Gateway. IP address of alternate gateway.



To complete your settings, click **Save**.
To view computers and other devices that have been issued settings by this router, click **Clients List.**
To manually set computers with specific IP addresses, click **Fixed Mapping** (See 6.11, “Fixed Mapping and MAC Address Control”).

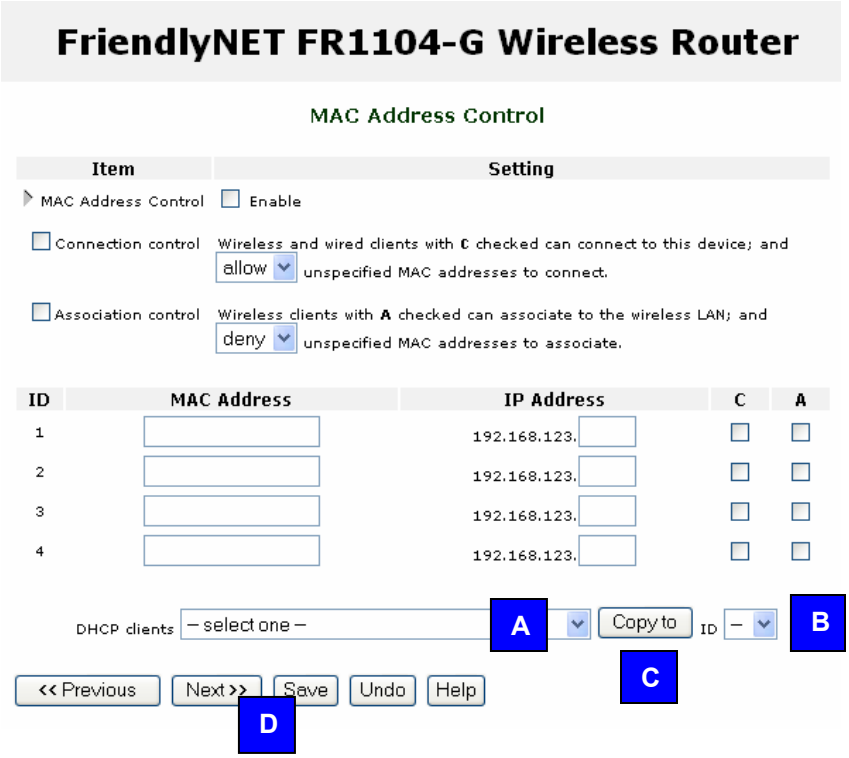
6.10 CLIENTS LIST



- Wake up. Wake-on-LAN (WoL) is a technology used to remotely power up a network device. To use this feature, your target computers must be WoL-enabled. To wake up a device, select the device [A] and click **Wake up** [B]. Confirm your selection by clicking **OK** on the dialog box.
- Delete. Select client [A] and click **Delete**. Confirm your deletion by clicking **OK** on the dialog box. The entry will be deleted from this list.

Tip: If you are sharing resources (files or printers) on the network (LAN or WLAN), wake up the computer using the WoL feature described above.

6.11 Fixed Mapping and MAC Address Control



On this screen, you can manually associate specific local (LAN or WLAN) IP addresses with a specific computer or device (client).

- MAC Address Control. Click **Enable** to allow the settings on this page to become effective.
- Connection Control. Enable this rule to allow **wired** (LAN) and **wireless** (WLAN) clients to have controlled access. Clients not explicitly described in the table will be allowed or denied access to the Internet.
- Association Control. Enable this rule to limit **wireless** clients' access to the wireless network (WLAN).

To add an entry to the control table:

A. Use the drop-down menu to select a client.
B. Choose an entry number.
C. Click **Copy to**.
D. When all 4 entries are filled, click **Next** to view the next 4 entries. You can define controls for up to 32 clients. When all settings are complete, click **Save**.

For *strong* security, grant access only to specific clients:

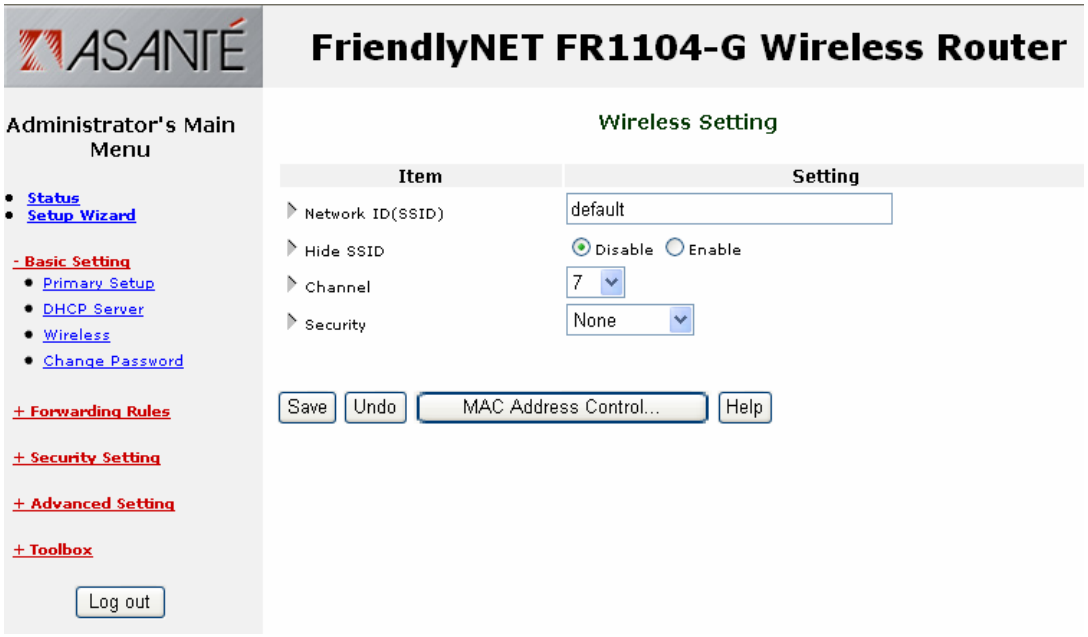
- Mac Address Control: Enable.
- Connection Control: Enable. Deny unspecified MAC addresses to connect.
- Association Control. Enable. Deny unspecified MAC addresses to associate.
- Control Table. Use the DHCP clients drop-down menu to add each client to the list. Check both **C** (connection control) and **A** (association control) for each client.
- When finished, click **Save**.

Tip: For maximum security, see the Security Settings menu.

For *medium* security, grant access to all wired clients, but only specific wireless clients:

- Mac Address Control: Enable.
- Connection Control: Enable. Allow unspecified MAC addresses to connect.
- Association Control. Enable. Deny unspecified MAC addresses to associate.
- Control Table. Use the DHCP clients drop-down menu to add each wireless client to the list. Check **A** (associate control) for each client.
- When finished, click **Save**.

6.12 WIRELESS SETTING



This screen establishes the settings for the wireless network (WLAN). You must match these settings with all wireless clients that will use this router.

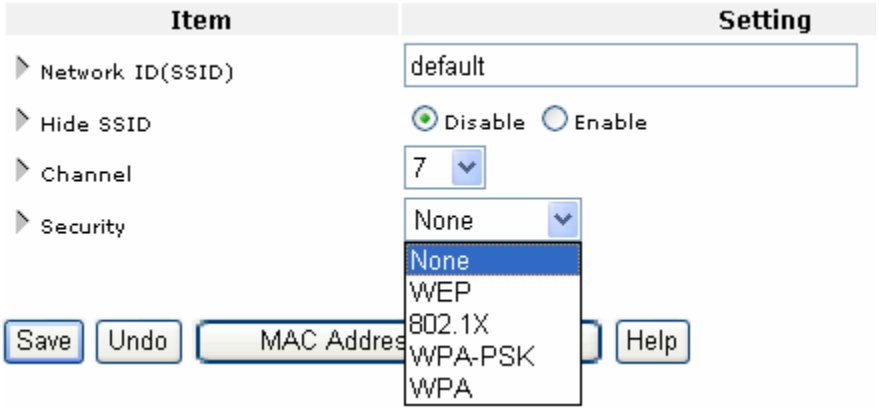
- Network ID (SSID or ESSID). Default is **default**. If you have multiple wireless access points with routers (like the FR1104-G), clients can freely roam between them without making any changes. Every wireless client using the SSID defined here will have access to the router. See MAC Address Control to enable additional security features.
- Hide SSID. During normal operation, the SSID is broadcast to every 802.11b/g device on the specified channel. To make the router's wireless AP invisible to unauthorized users, this feature hides the network ID ("stealth SSID").

  Tip: During setup, simplify your installation by leaving this setting at Disable. Afterward, change this to Enable.

- Channel. Factory defaults depend on the permissible channels defined by your local regulatory agencies. Channel 11 is the default.

Region	Available Channels	Comments
North America (US, Canada)	1–11	FCC limits: 1–11
Europe	1–11	ETSI limits: 1–13
Spain	10–11	
France	10–11	Limits: 10–13
Japan	1–11	MKK limits: 1–14

- Security. Choose the appropriate security level for your network.



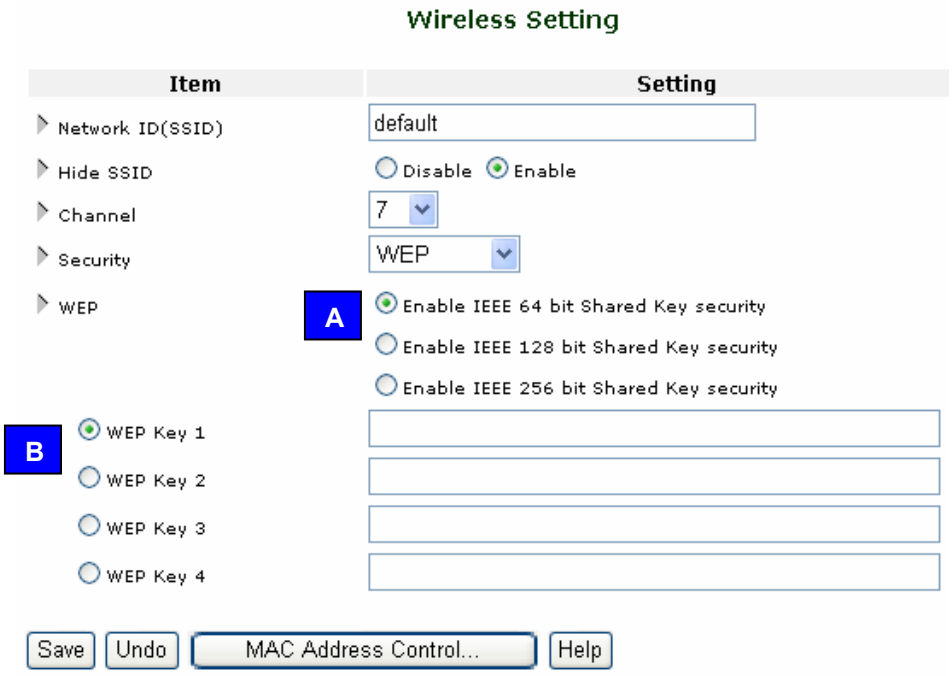
Security	Description	Comments
None	Factory default	Not recommended
WEP	Wired Equivalent Privacy	Popular choice
802.1X	Port-based authentication with RADIUS server	Popular choice for businesses
WPA-PSK	Wi-Fi Protected Access with pre-shared key	Recommended for small networks
WPA	Wi-Fi Protected Access with RADIUS server	Recommended for businesses

WPA-PSK and WPA both use temporal key integrity protocol (TKIP) instead of a static key (like WEP). If possible, choose wireless adapters that support WPA-PSK or WPA (if you have an 802.1X RADIUS authentication server). Microsoft Windows XP with Service Pack 1, Apple Mac OS X Version 10.2.8 (and above); Linux 2.4.29 (RedHat 9) may be required for each client and server.

This router uses context-sensitive menus. After making your security selection, the bottom of this menu will change to reflect your security setting.

See the following four pages for detailed information for each security setting.

SECURITY: WEP

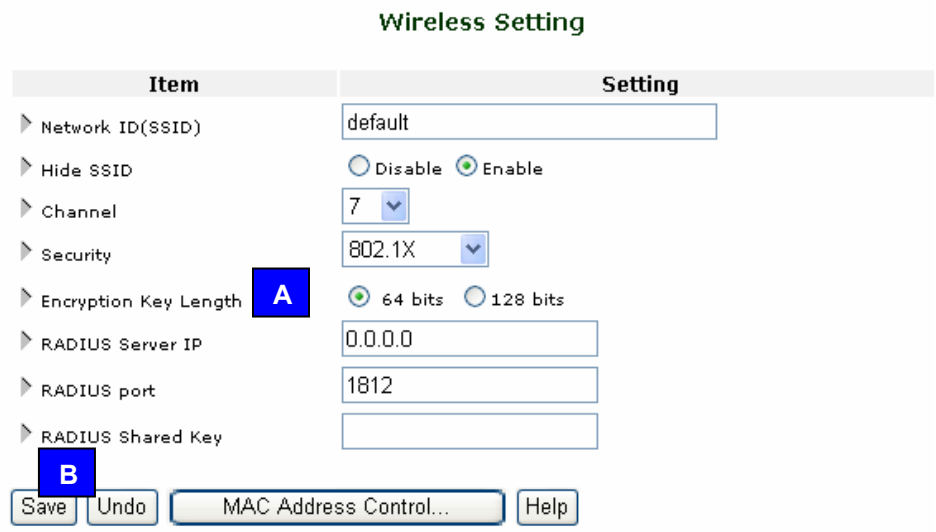


- WEP. Choose the encryption standard. The 128-bit design is more secure than 64-bit and the 256-bit is much more secure than 128-bit. However, not all wireless adapters support 256-bit WEP encryption.
- WEP Key 1, 2, 3, 4. Select one field and enter a random hexadecimal key for your selected WEP security level. A hexadecimal key uses one of these digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E or F.

WEP Key	Digits	Samples
64-bit	10	7b28202a3c
128-bit	26	44562d5539457d644255464146
256-bit	58	58663955272c68676f4741273467277a48397423575d7a3a5b673b3725

To complete your settings, click **Save** and **Reboot**.
To restore the last saved settings, click **Undo**.
To restrict access to the router by hardware port addresses, click **MAC Address Control**.
To view on-screen instructions, click **Help**.

SECURITY: 802.1X



To use this security feature, you must have an 802.1X-compatible authentication server. Use the settings provided by your remote authentication dial-in user service (RADIUS) server. Authentications using PEAP-CHAPv2 and PEAP-TLS are supported.

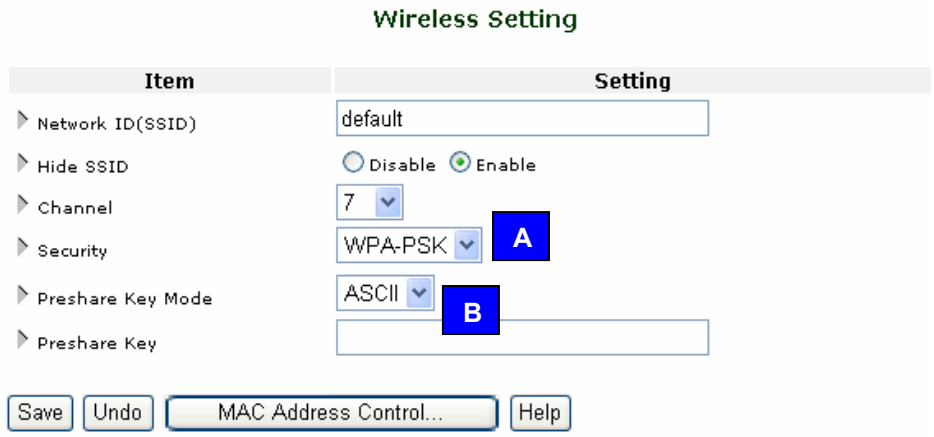
- Encryption Key Length. Choose 64 or 128 bits.
- RADIUS Server IP. Enter the server's IP address.
- RADIUS Port. Enter the authentication tcp/udp service port number. Default is 1812 (per RFC 2026).
- RADIUS Shared Key. Enter the key shared between the RADIUS server and the router.

Tip: This router is compatible with Microsoft 2000's RADIUS Server (requires Service Pack 3 and HotFix Q313664) and these clients:

- Microsoft Windows XP Professional (without Service Pack 1)
- Microsoft Windows XP Professional (with Service Pack 1a)

To complete your settings, click **Save** and **Reboot**.
To restore the last saved settings, click **Undo**.
To restrict access to the router by hardware port addresses, click **MAC Address Control**.
To view on-screen instructions, click **Help**.

SECURITY: WPA-PSK



In a home or small business network, Wi-Fi protected Access (WPA) uses a special mode called WPA-PSK. The PSK refers to a pre-shared key (or password) used to initialize authentication. This is the most common method of implementing WPA wireless security in homes and small businesses. For larger businesses and organizations with an 802.1X RADIUS authentication server, choose **WPA** mode (not WPA-PSK).

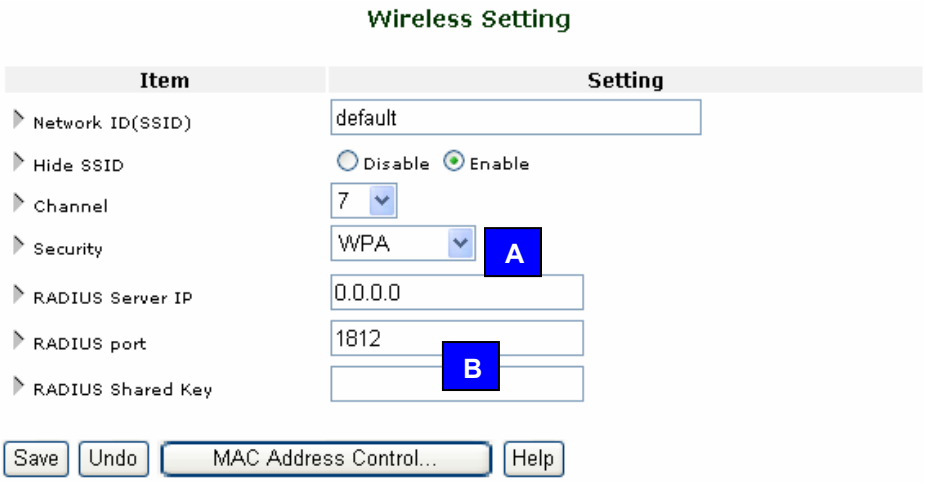
The pre-shared key is designed to be easy to setup using either simple or complex passwords that are entered into the FR1104-G router and each wireless client on the wireless network. You can input either ASCII characters or Hexadecimal digits as the pre-shared key.

- Preshare Key Mode: Choose ASCII or HEX.
- Preshare Key: Input from 8 to 32 ASCII ("printable") characters, or 64 hexadecimal digits. This key must also be used by every wireless client connecting to the router.

Mode	Samples
ASCII	0246813579, friendlynetwireless
HEX	7b28202a3c, 1a2b3c4d5e6f, 1234567890abcdef1234567890

To complete your settings, click **Save** and **Reboot**.
To restore the last saved settings, click **Undo**.
To restrict access to the router by hardware port addresses, click **MAC Address Control**.
To view on-screen instructions, click **Help**.

SECURITY: WPA



For businesses and larger organizations with an 802.1X RADIUS authentication server, choose this Wi-Fi protected Access (WPA) mode—not WPA-PSK. The PSK refers to a pre-shared key (or password) used to initialize authentication. This is the most common method of implementing WPA wireless security. For businesses and organizations with an 802.1X RADIUS authentication server, choose **WPA** mode (not WPA-PSK).

- RADIUS Server IP. Enter the server's IP address.
- RADIUS Port. Enter the authentication tcp/udp service port number. Default is 1812 (per RFC 2026).
- RADIUS Shared Key. Enter the key shared between the RADIUS server and the router.

Tip: This router is compatible with Microsoft 2000's RADIUS Server (requires Service Pack 3 and HotFix Q313664) and these clients:

- Microsoft Windows XP Professional (without Service Pack 1)
- Microsoft Windows XP Professional (with Service Pack 1a)

To complete your settings, click **Save** and **Reboot**.
To restore the last saved settings, click **Undo**.
To restrict access to the router by hardware port addresses, click **MAC Address Control**.
To view on-screen instructions, click **Help**.

6.13 WPA FOR WIRELESS CLIENTS

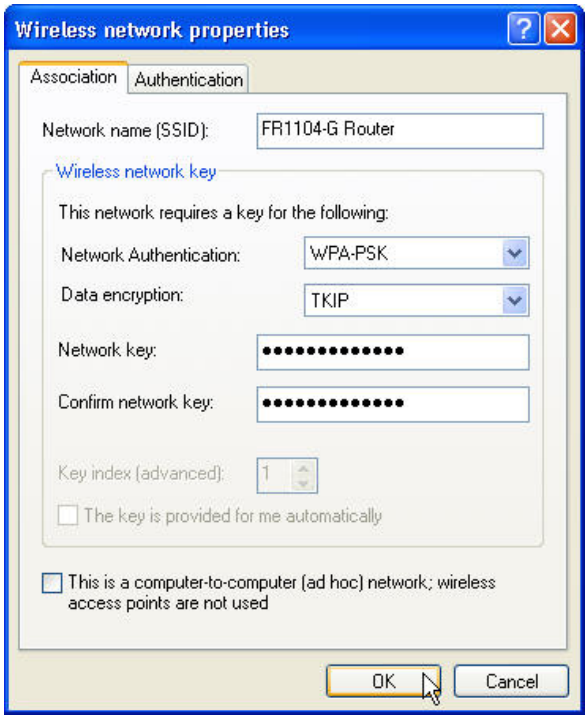
In most cases, you will need to upgrade and install your wireless client utility software and drivers before using WPA. Check with your wireless adapter manufacturer for utility software and driver updates as necessary. Follow their specific instructions to configure your wireless client for WPA.

Asanté supports WPA on these FriendlyNET wireless adapters:

- **AeroLAN AL5410-G**
  Wireless: 802.11g
  WPA: No
- **AeroLAN AL5403-XG**
  Wireless: 802.11g
  WPA: Yes (Windows XP, Mac OS X)
- **AeroLAN AL1611**
  Wireless: 802.11b
  WPA: Yes (Windows XP)

MICROSOFT WINDOWS XP

If you are planning to use Windows XP's native wireless utility and WPA, download the patch from Microsoft: http://support.microsoft.com. Be sure that you're running with Service Pack 1 (SP1). If your wireless adapter's driver already supports WPA, you may not need to install Microsoft's patch. However, by installing the Microsoft patch, many wireless adapters can use the native Windows XP wireless utility to configure WPA. Check with your wireless adapter manufacturer about using the native Windows XP wireless utility with your adapter.

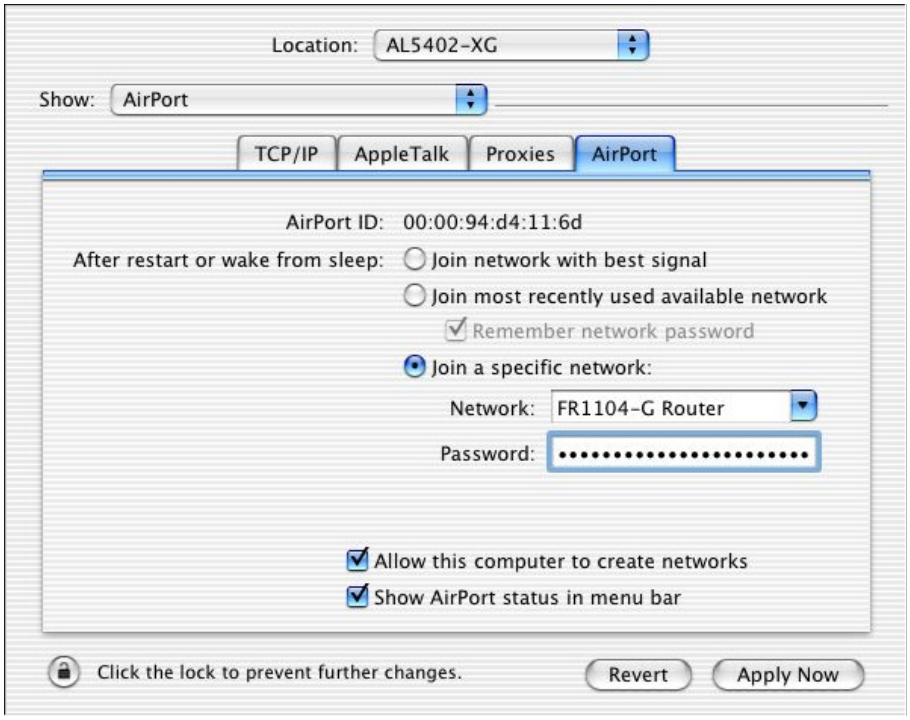


Note: Microsoft does not provide support for WPA on earlier versions of Windows (e.g., Windows 98, 95 and NT).

APPLE MACINTOSH OS X

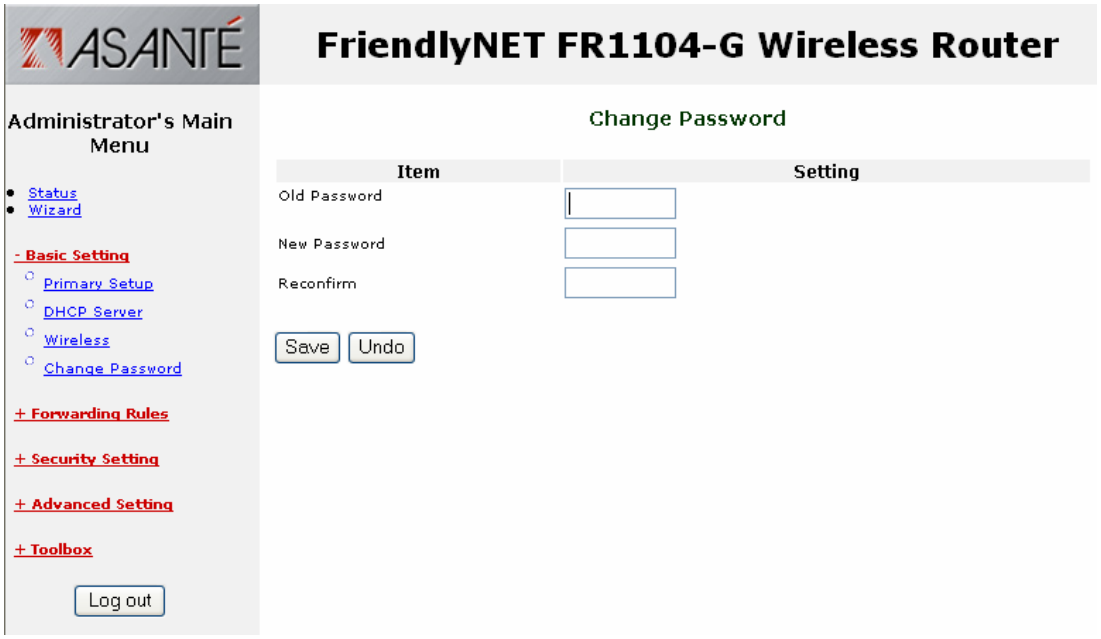
Asanté's FriendlyNET AeroLAN AL5402-XG, AL5403-XG and Apple's AirPort Extreme cards support WPA when using the current Apple AirPort driver in OS X 10.2.8 and above; earlier versions of Mac OS X and OS 9 are not supported by Apple.

Using the Apple AirPort wireless configuration utility in Mac OS X, you can enable WPA support to work with the Asanté FR1104-G router using WPA mode.



Note: WEP and WPA are mutually exclusive; they **can't** be used simultaneously.

6.14 CHANGE PASSWORD



The router's administrator's default password is **admin**.

Caution! You should change the password immediately and write down the new password in a safe place.

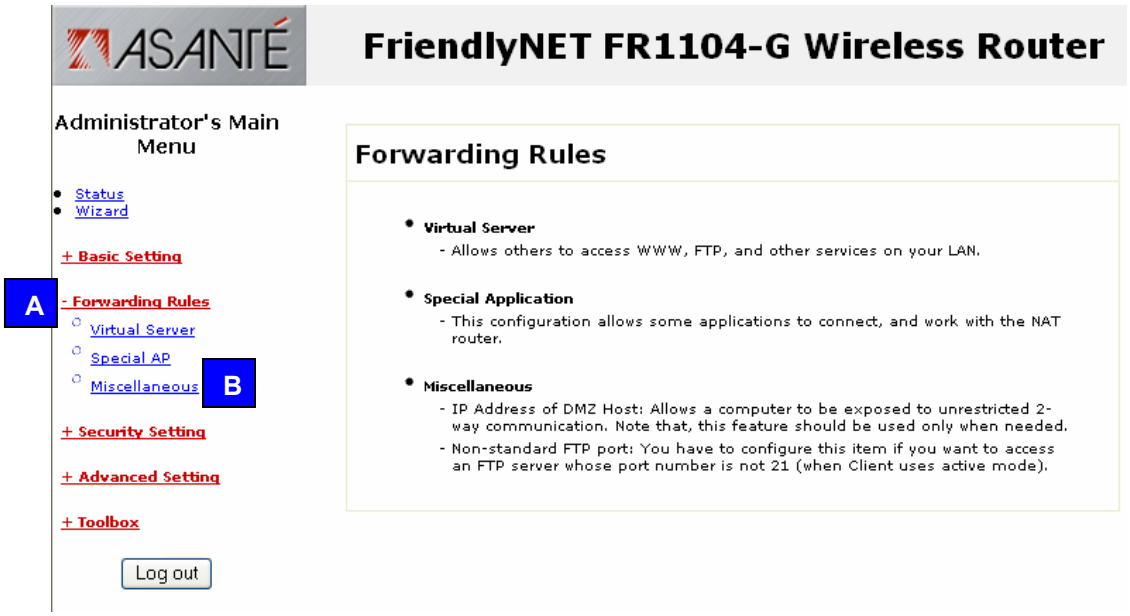
- Old password. Factory default is **admin**.
- New password. Choose your own password. For improved security, avoid using names and words that can be found in a dictionary.
- Reconfirm. Re-type your new password.

Tip: You may want to record your password in this manual or on a Post-It note attached to your router.

To complete your settings, click **Save**.
To restore the last saved settings, click **Undo**.

Chapter 7. Forwarding Rules

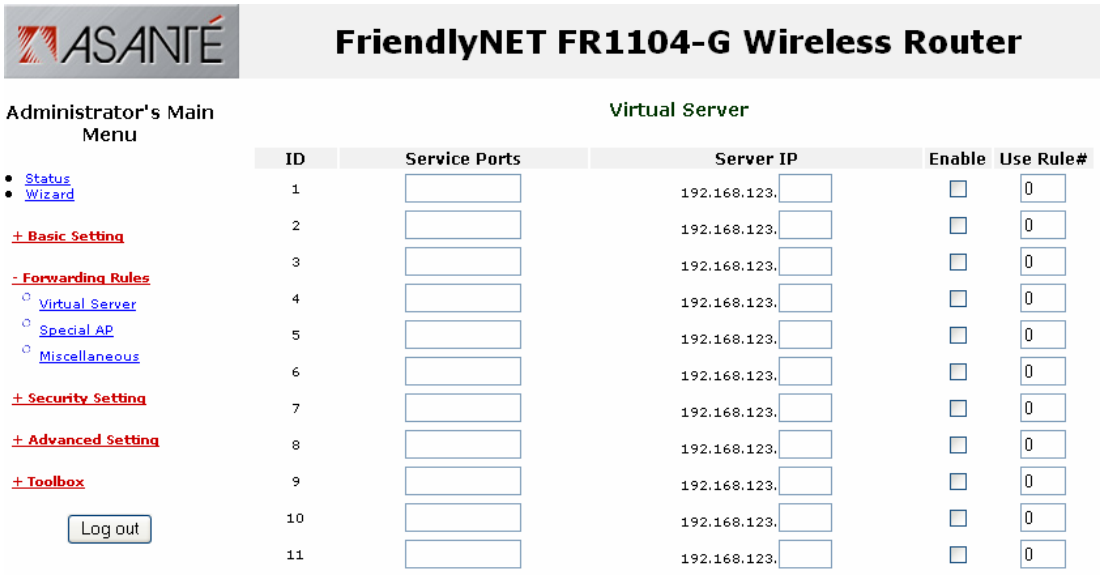
After logging into the router, click on the **Forwarding Rules** link [A]. Choose from one of the three sub-menus [B].



This chapter describes how to customize the router's forwarding rules so you may run specialized servers and applications on your local network. In most cases, you will never need to make any changes in this section.

Forwarding Rules	Description
Virtual server	Service port, server IP, rule #
Special applications	Trigger, incoming ports
Miscellaneous	DMZ host, FTP port

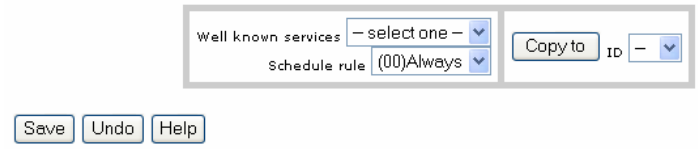
7.1 VIRTUAL SERVER



By default, the router's network address translation (NAT) firewall will block unrecognized incoming packets from the Internet (WAN) to protect internal clients on the LAN and WLAN. To allow direct external access for specific Internet services, use the Virtual Server capability.

For example, if you have FTP, web and VPN servers on your local network, you could define them as follows:

Server	ID	Service Port	Server IP	Enable	Use Rule #
FTP	1	21	192.168.123.1	Yes	0
Web	2	80	192.168.123.2	Yes	0
VPN	3	1723	192.168.123.3	Yes	0



Using the menus at the bottom of the page, define each server.

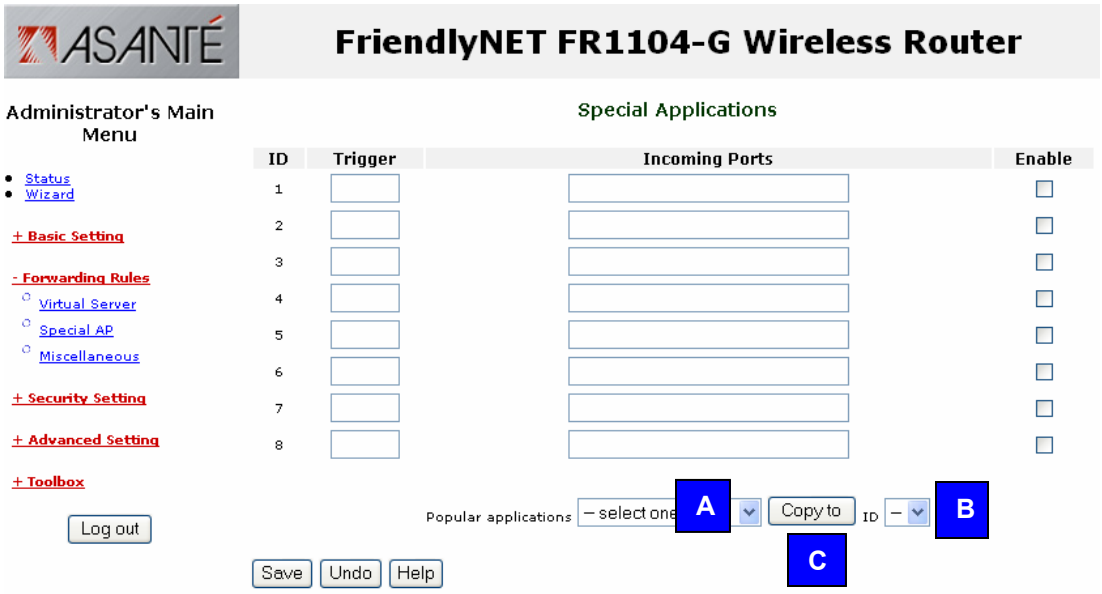
1. Select a service from the drop-down menu.
2. Choose a schedule rule. Rule 0 is always on. (Custom rules are defined in Security Setting).
3. Select an ID number (1–20).
4. Click **Copy to**.

Tip: The inbound packet filters will protect Virtual Servers. See Security Settings > Packet Filters.
Tip: Rules are scheduled in Advanced Settings > Schedule Rule.

Popular Internet Services	Service Port	Comment
Web	80	HTTP
Telnet	23	
SMTP	25	Email
POP3	110	Email
FTP	21	
ISAKMP	500	
DNS	53	
Authentication	113	
PPTP	1723	

After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

7.2 Special Applications and Games



Some applications and Internet games utilize a range of service ports that are normally blocked by the router's network address translation (NAT) firewall. This Special Applications feature lets you enable pre-defined applications and your own custom settings. Each Special Application setting can only be used by one client at a time. Your applications provider will be able to provide these settings for you.

- Trigger. The outbound port number issued by your local application.
- Incoming Ports. When a trigger packet is detected, inbound packets received through the specified ports will be permitted to pass through the router. Unlike conventional routers where ports stay open for an indefinite time, this router will automatically close the ports after 60 seconds of inactivity.

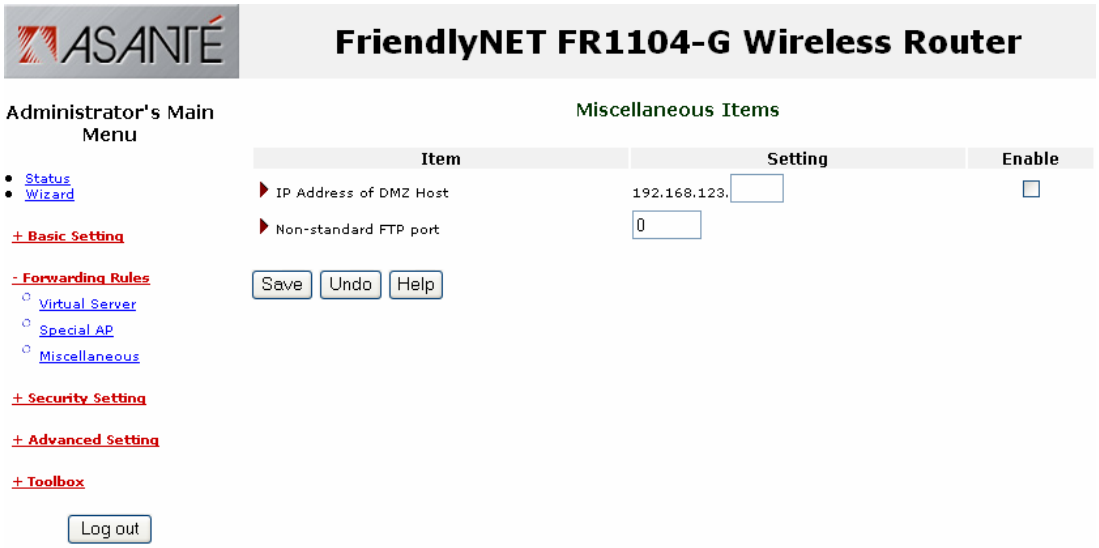
To use one of the pre-defined applications:

A. Select your application or game from the drop-down list. Choose from Battle.Net, Dialpad, ICU II, MSN Gaming Zone, PC-to-Phone and QuickTime 4.
B. Select an entry ID number (1–8).
C. Click **Copy to**.

If Special Applications are insufficient for your application, set up your client as a DMZ; see the following section for details.

After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

7.3 MISCELLANEOUS



This page defines two special services: DMZ (demilitarized zone) for unrestricted two-way communications and non-standard FTP port.

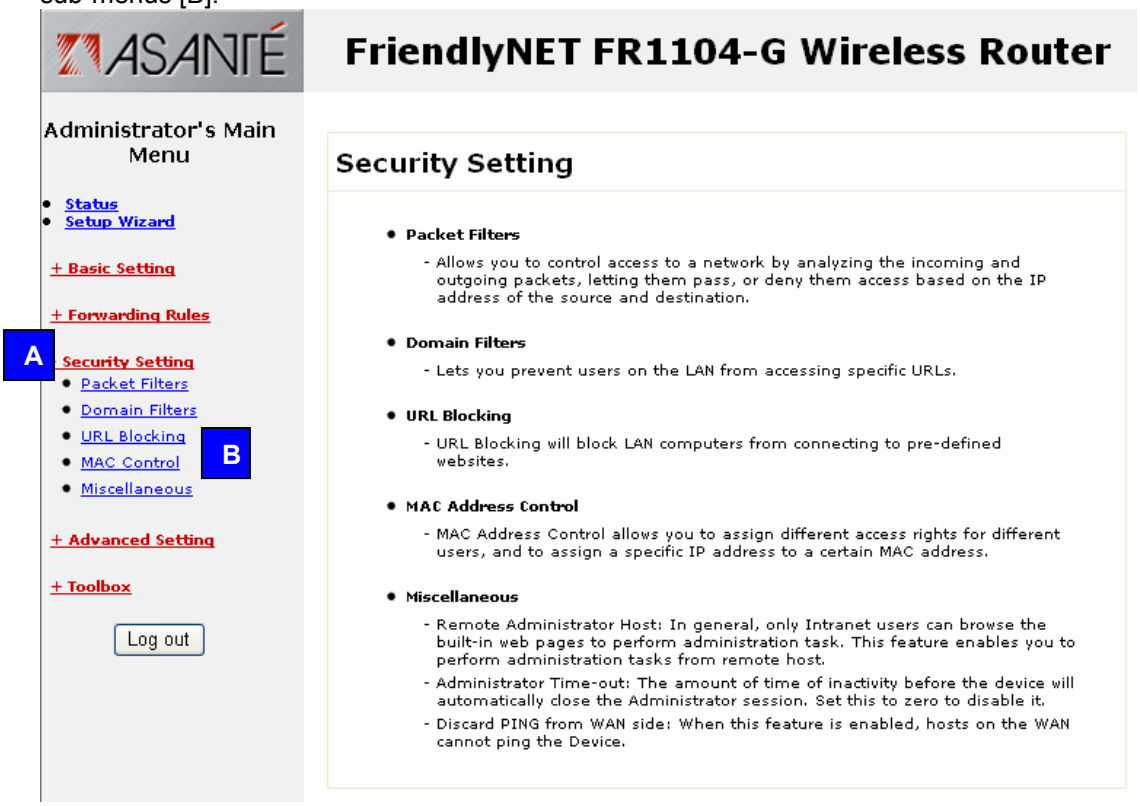
- IP Address of DMZ host. If your special application or Internet game does not work with the Special Applications settings, you can logically place it “in front” of the router’s NAT firewall. Since this exposes the computer to unauthorized users from the Internet, this feature should only be activated when necessary. The setting will correspond to the local IP address for your computer. The range will be 1 to 254.
- Enable this setting.
- Non-standard FTP port. For security reasons, you may need to use a port other than the standard (21). Remember not to choose a port that will conflict with other services. For security reasons, this setting will be cleared after you reboot the router.

Tip: The inbound packet filters will protect the DMZ host. See Security Settings > Packet Filters.

After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

Chapter 8. Security Setting

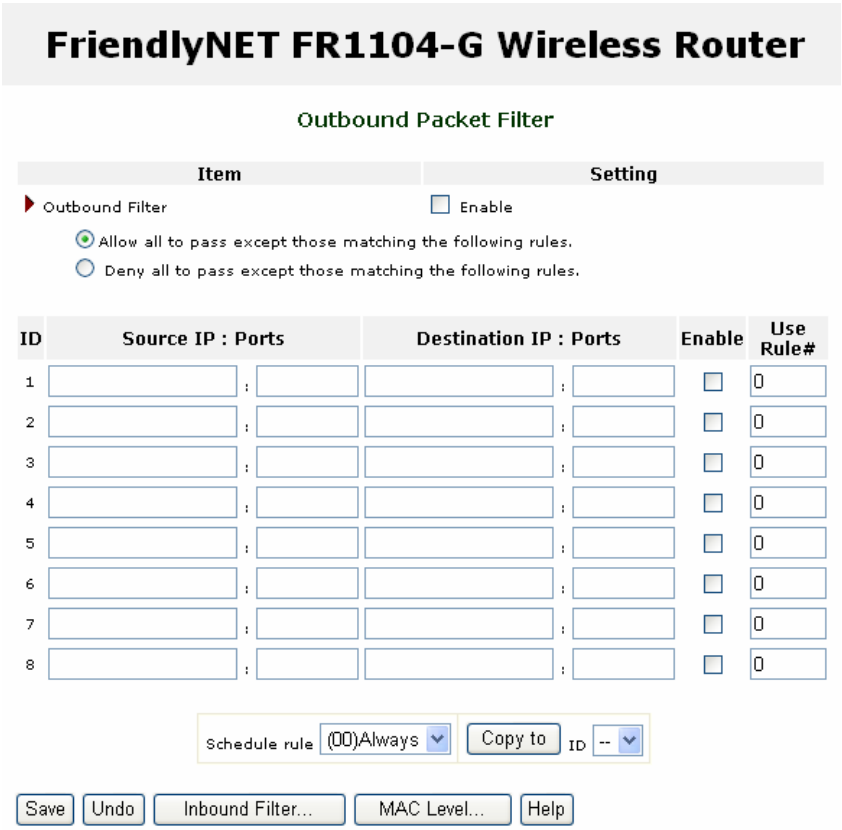
After logging into the router, click on the **Security Setting** link [A]. Choose from one of the five sub-menus [B].



This chapter lets you tailor the router's extensive security features to best protect your local network. The router uses a "double firewall" (NAT with PF/DF) to provide secure data communications.

Security Setting	Description
Packet Filters (PF)	Source, destination, rule #
Domain Filters (DF)	Log, privilege IP, domain suffix, log/drop
URL Blocking	URL
MAC Control	Connection/association control, MAC address, IP address
Miscellaneous	Remote administrator, discard ping, SPI, DoS detection, VPN pass-through

8.1 PACKET FILTERS – OUTBOUND FILTER



Packet filters allow you to control access to the network (local and Internet) by analyzing every inbound and outbound packet. Depending upon the rule you define, packets will be evaluated against source address, destination address, service port and time of day/week. Since inbound packets are naturally filtered by the router's NAT firewall, the inbound filters only protect the Virtual Servers and DMZ host.

For example, a business may limit Internet resources (including peer-to-peer file sharing, music stores and games) during business hours, Monday through Friday. With the powerful allow/deny rules, you can make this rule apply to everyone (except yourself).

- Outbound Filter. Click to enable all the rules defined on this page.
  Select one of the filtering policies:
  1. Allow all to pass except those matching the rules defined in the table.
  2. Block all except those matching the rules defined in the table.
- Source IP. Local IP address (typically in the form 192.168.123.100) or range of addresses (192.168.123.1-192.168.123.255).
- Source Port. Enter a single port (e.g., 80) or a range of ports (1000-1999). To limit the port range only to the TCP protocol, add a **T** prefix (e.g., T80) or **U** prefix (e.g., U80) for UDP. No prefix indicates both TCP and UDP. Leave the field blank to specify all port addresses.
- Destination IP. Specify a single IP address or a range of addresses.
- Destination Port. Enter a single port or range of ports.

- Enable. You may selectively enable or disable each rule.
- Use Rule #. Use the drop-down menu at the bottom of the screen to quickly fill in a scheduling rule.

Tip: Rules are scheduled in Advanced Settings > Schedule Rule.

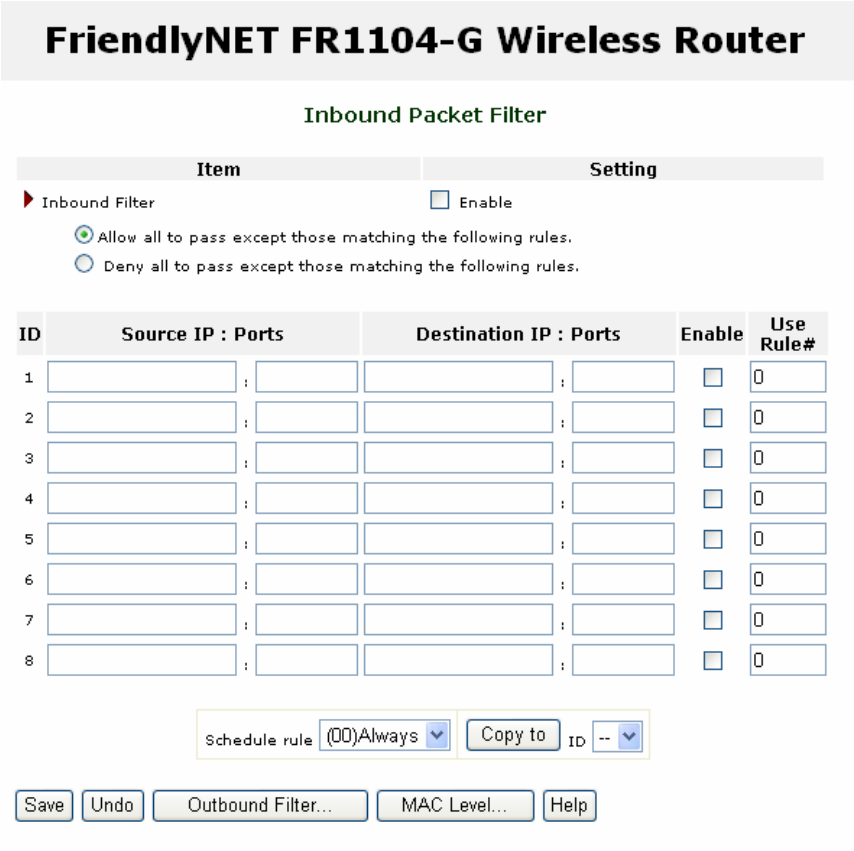
After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To assign filters for inbound traffic, click **Inbound Filter**. (See 8.2 Packet Filters – Inbound Filter)
To set MAC level access controls for specific clients, click **MAC Level**. (See 8.3 Mac Address Control.)
To read on-screen information on this page, click **Help**.

Sample	Source IP	Source Port	Dest. IP	Dest. Port	Enable	Rule
1	192.168.123.100–192.168.123.199			25–110	✓	0
2	192.168.123.10–192.168.123.20				✓	0

In the examples above:

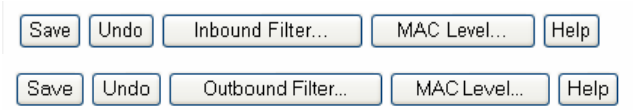
- Sample 1 allows all clients in the IP range 192.168.123.100 to 192.168.123.199 to receive services on ports 25–110, including send mail (port 25), receive mail (port 110) and browse the Internet (port 80).
- Sample 2 allows all clients in the IP range 192.168.123.10 to 192.168.123.20 to do everything. Nothing is blocked.

8.2 PACKET FILTERS – INBOUND PACKET FILTER

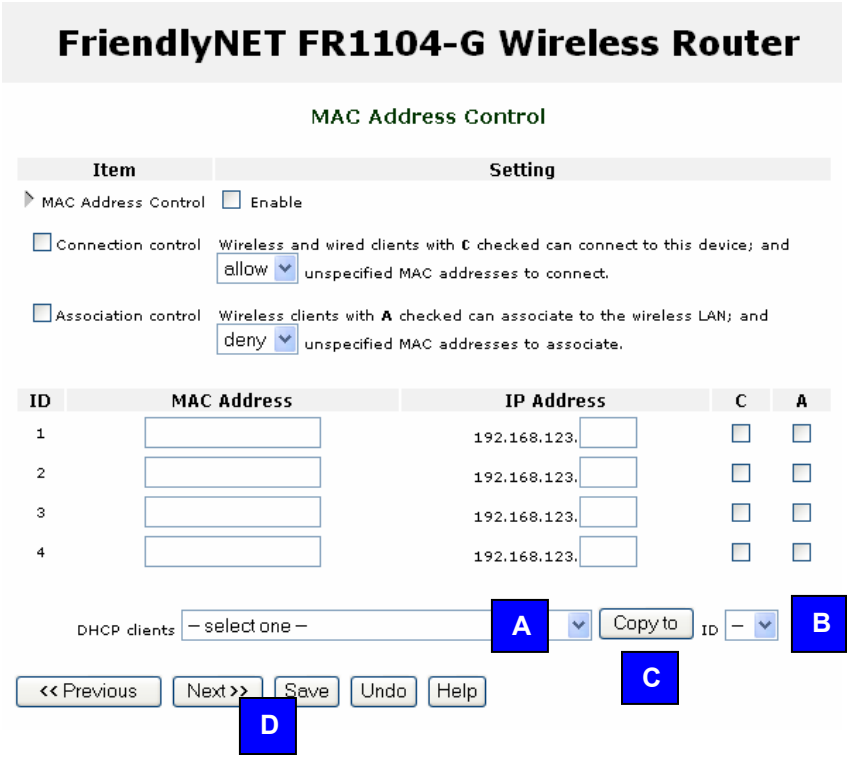


After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To assign filters for outbound traffic, click **Outbound Filter**.
To set MAC address controls for specific clients, click **MAC Level**.
To read on-screen information on this page, click **Help**.

8.3 MAC ADDRESS CONTROL



From the Inbound (or Outbound) Packet Filter screen, click **MAC Level**.



On this screen, you can manually associate specific local (LAN or WLAN) IP addresses with a specific computer or device (client).

- MAC Address Control. Click **enable** to allow the settings on this page to become effective.
- Connection Control. Enable this rule to allow wired (LAN) and wireless (WLAN) clients to have controlled access. Clients not explicitly described in the table will be allowed or denied access to the Internet.
- Association Control. Enable this rule to limit wireless clients access to the wireless network (WLAN).

To add an entry to the control table:

A. Use the drop-down menu to select a client.
B. Choose an entry number.
C. Click **Copy to**.
D. When all 4 entries are filled, click **Next** to view the next 4 entries. You can define controls for up to 32 clients. When all settings are complete, click **Save**.

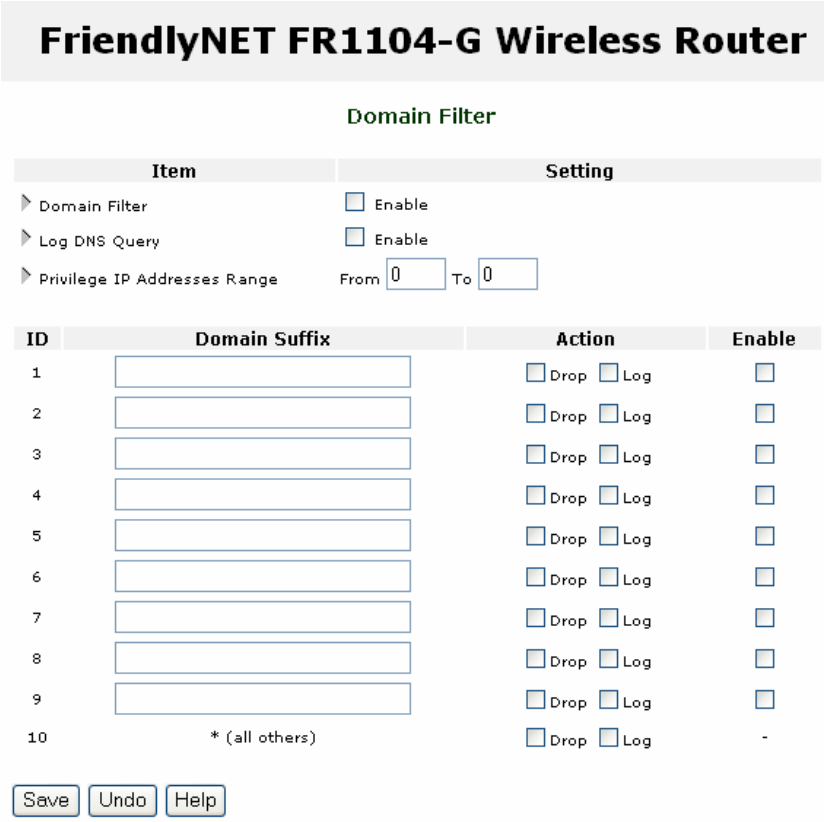
For *strong* security, grant access only to specific clients:

- Mac Address Control: Enable.
- Connection Control: Enable. Deny unspecified MAC addresses to connect.
- Association Control. Enable. Deny unspecified MAC addresses to associate.

- Control Table. Use the DHCP clients drop-down menu to add each client to the list. Check both **C** (connection control) and **A** (association control) for each client.
- When finished, click **Save**.

Tip: For maximum security, see the Security Settings menu.

8.4 DOMAIN FILTER



- Domain Filter. Check to prevent clients from accessing specific websites (URLs).
- Log DNS Query. Check to log all domain name requests. For example, a user attempting to browse www.google.com from his browser will have www.google.com entered into the log. See Status > View Log to see the on-screen log.
- Privileged IP Addresses Range. Exclude clients from the restrictions on this page.
- Domain Suffix. Exclude access to sites with this suffix. For example, **.gov** (government) or **.tv** (television).
- Action. Define the action to be taken when the above criteria are met. Drop will block access to that site. Log will add an entry to the system log.
- Enable. Individual rules may be enabled and disabled.

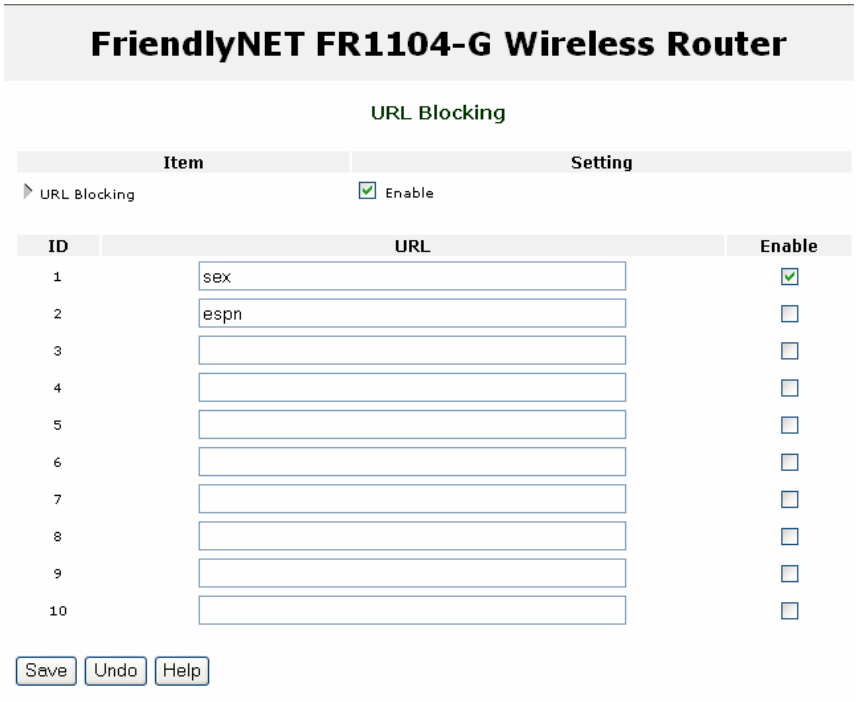
Sample	Domain Suffix	Drop	Log	Enable
1	www.microsoft.com	✓	✓	✓
2	.tv	✓		✓

In the examples above,

- Attempts to access www.microsoft.com will be blocked (dropped) and logged.
- Attempts to access any website with .tv will be blocked.

See also URL Blocking in the next section to block website accesses by keywords.

8.5 URL BLOCKING



By enabling this function, any website with the specified keyword(s) will be blocked and access attempts will be logged. See Status > View Log to view the on-screen log.

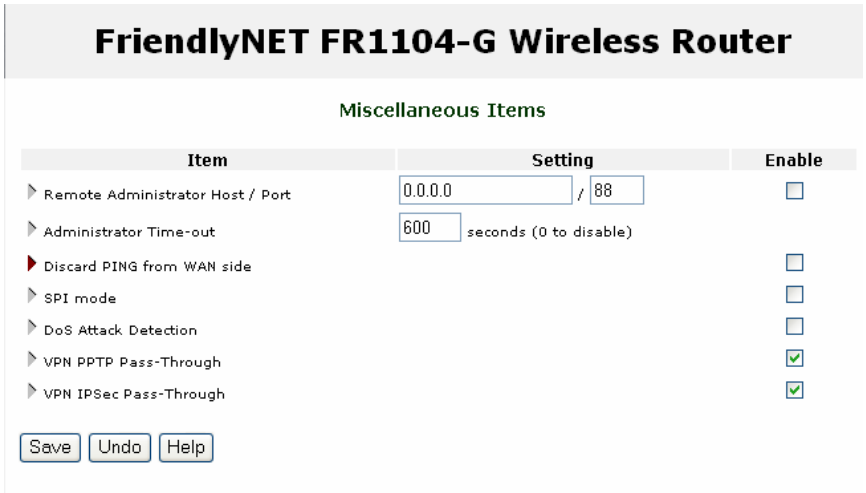
- URL Blocking. Check to block clients from accessing websites with the specified keyword in its URL.
- URL. Enter the keywords of the websites you want to block.
- Enable. Individual rules may be enabled and disabled.

Sample	URL Keywords	Enable	Websites Blocked	Not Blocked
1	sex	✓	www.sex.com, video.sexx.co.uk, www.essex.com	www.se-x.com
2	.tv	✓	www.movies.tv	www.abctv.com

Compared to the *Domain Filter*, described earlier, URL Blocking:

- Lets you block hundreds of websites with each keyword entry.
- Does not require a suffix (.com, .org, .tw).

8.6 MISCELLANEOUS SECURITY SETTINGS



This configuration page allows you to limit the vulnerabilities of your router from Internet attackers. When in doubt, do not change these default settings.

- Remote Administrator Host/Port. Changing this setting allows others to easily change the settings of this router via Internet. If you have a very trusted individual who can assist you with administering this router, then enable this feature **only** when you need assistance.

  The *first field* is the IP address of the remote administrator's computer (or router/gateway). If the address is 0.0.0.0, then anyone with this router's password can perform remote administration.

  Tip: To allow administration from any user within the subnet 193.203.53.0 through 193.203.53.255, use the "/nn" subnet mask notation: 193.203.53.0/24. For more info on this notation, visit http://www.faqs.org/rfcs/rfc1878.html.

  The *second field* is the service port. By default, the port number is 88. When this feature is enabled, the HTTP web server is also shifted to port 88.

- Administrator Time-out. After this period of inactivity, the router's administration session (local or remote) will be terminated. You will need to re-login. Set this value to **0** to disable.
- Discard PING from WAN side. When enabled, all ping requests from the Internet (WAN) will be ignored.
- Secure Packet Inspection (SPI) Mode. When enabled, the router will record packet information on all incoming packets and check for validity.
- Denial of Service (DoS) Attack Detection. When enabled, the router will detect malicious attacks, such as: SYN attack, WinNuke, Port Scan, Ping of Death and Land Attack.
- VPN PPTP/IPSec Pass-Through. Enable this feature if you need to establish a virtual private network (VPN) through this router. Additional client-specific software required to run VPN services.

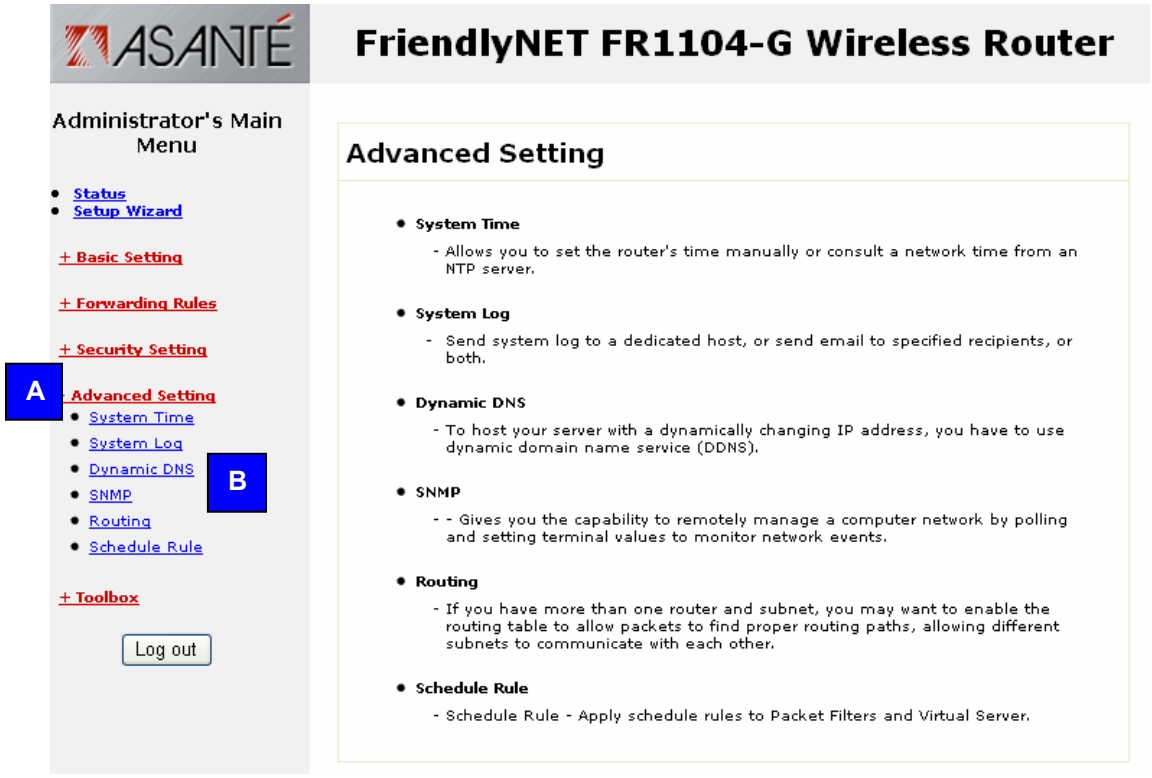
For maximum network security, Asanté recommends these settings:

Miscellaneous Security	Setting	Enable
Remote Administrator Host/Port		No
Administrator Time-out	300	✓
Discard PING from WAN side		✓
Secure Packet Inspection (SPI) Mode		✓
Denial of Service (DoS) Attack Detection		✓
VPN PPTP/IPSec Pass-Through		No

After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

Chapter 9. Advanced Setting

After logging into the router, click on the **Advanced Setting** link [A]. Choose from one of the five sub-menus [B].

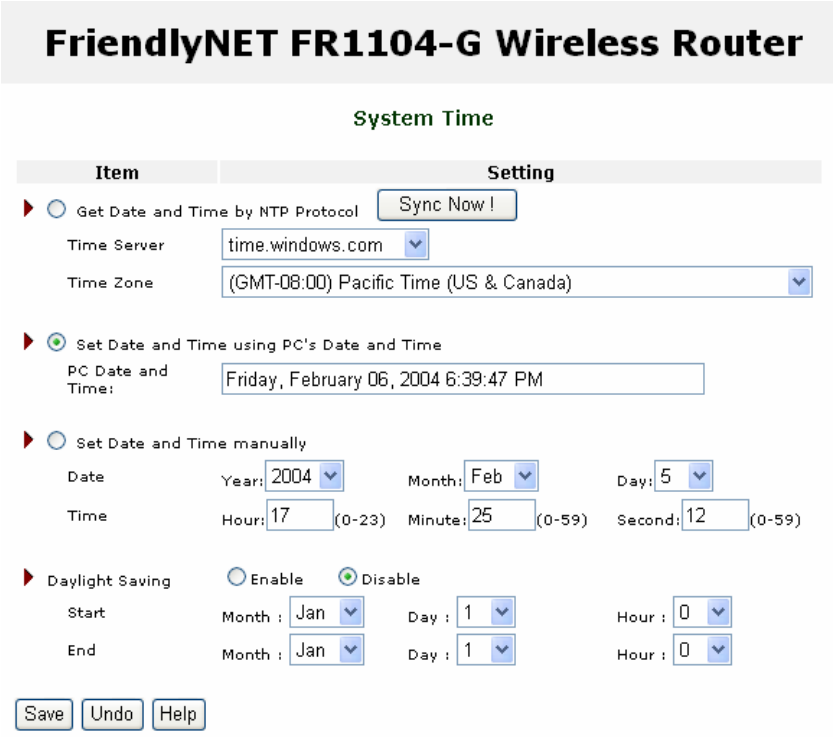


Use the settings described in this chapter to configure the router's advanced features. For most network installations, these settings are set only once or rarely. With only minor exceptions, you must have a strong working knowledge of routers and TCP/IP before making changes to the settings described here.

Advanced Settings	Description
System time	NTP, manual, daylight savings
System log	syslog server, email alert, log type, view log
Dynamic DNS	DDNS, provider, host, user name and password
SNMP	community, IP 1–4, version
Routing	dynamic, static, destination, mask, gateway, hop
Schedule rule	name, day of week, start/end time

After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

9.1 SYSTEM TIME



If this is the first time setting up the router, you will need to set the router's internal clock.

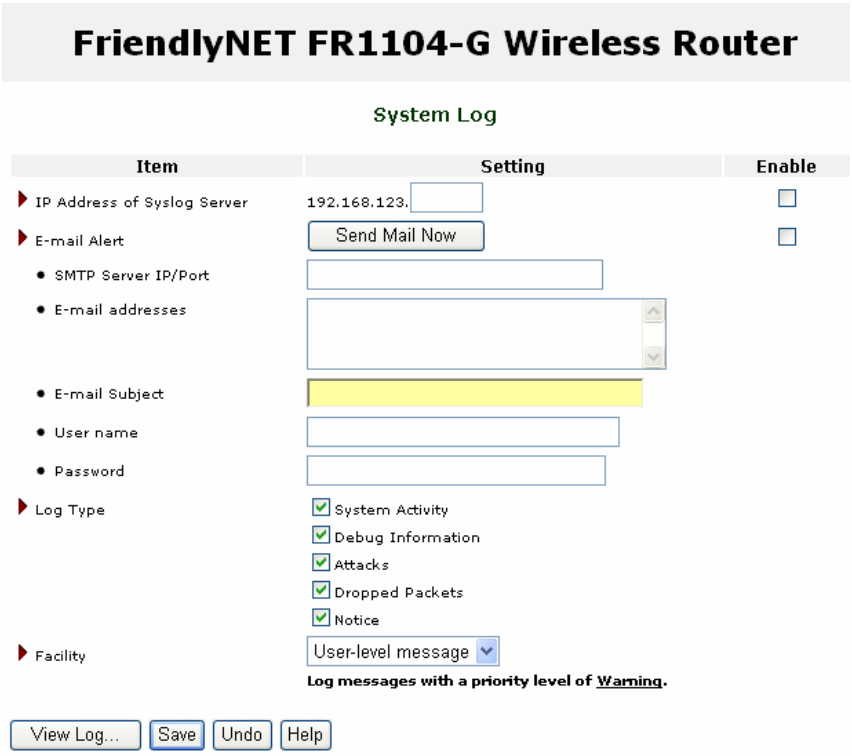
- Get Date and Time by NTP Protocol. Use the time provided by specified network time protocol (NTP) server. If enabled, then the router's real-time clock (time) will be set by the specified time server (typically, once a week). If your router is not continuously connected to the Internet, click **Sync Now!** Choose your local time zone from the drop-down menu.

  Tip: If your computer is a member of a Microsoft domain network, your clock is probably synchronized by a network time server. Some reasons why NTP may not work in your environment: no Internet connection, router's firewall has blocked the NTP signal, time server too busy. Your date must be correct or NTP will not sync the time.

- Set Date and Time using PC's Date and Time. Use the time and date from your computer.
- Set Date and Time manually. Set the date using the drop-down dialog boxes and enter the correct time.
- Daylight Saving. Since this varies by country and region, set the starting and ending dates per local rules. See this site for information on local rules: http://webexhibits.org/daylightsaving/g.html. In North America, daylight savings starts the first Sunday of April and ends the last Sunday of October.

After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

9.2 SYSTEM LOG

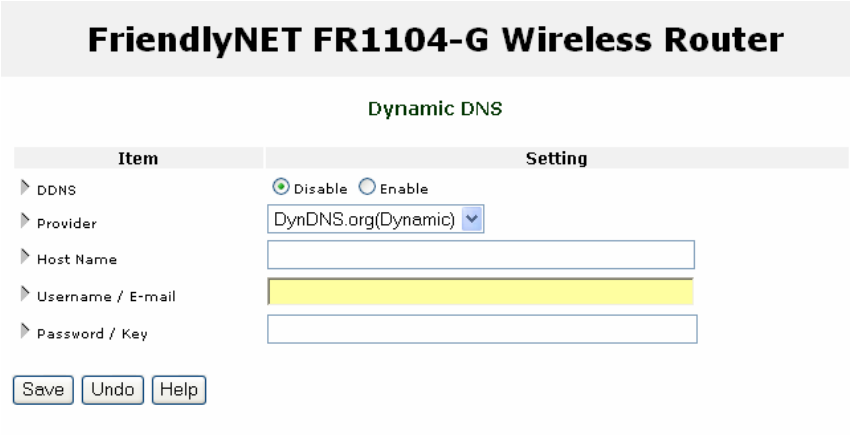


The router's system log records specified system events plus potential security threats based upon the settings in Security Setting. The log is normally saved in volatile memory. It can be manually or automatically exported to other servers or devices.

- IP Address of Syslog Server. IP address of destination syslog server. Check to enable this function.
- Email Alert. Click to immediately email the system log to the specified address.
- SMTP Server IP/Port. Enter the SMTP server IP address and service port (default is **:25**). For example, enter mail.emailserver.com or 193.203.53.1:26.
- E-mail addresses. Enter one or more email addresses. Separate multiple addresses with a comma (**,**) or semicolon (**;**). For example, enter jim@sample.com, mis@sample.com.
- E-mail Subject. Optional.
- User name. Enter your email account info. This is required.
- Password. Enter your email account info. This is required.
- Log Type. Check the activities you want logged. See also Security Settings for specific events that will be logged (domain filters, URL blocking, etc.). Your choices include system activity (login, logout), debug information (DHCP requests and responses), attacks (potential security threats), dropped packets (system availability) and notices.
- Facility. Messages from the router will be marked with the selected facility: User-level message or Local 0 through Local 7. Note: This feature requires firmware G1.1 or later.

Display the System Log screen by clicking **View Log**.
After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

9.3 DYNAMIC DNS



Unless your ISP has provided a static (fixed) IP address, it would be very difficult to host a local web server without this router's Dynamic DNS (DDNS) service. By subscribing to a DDNS, whenever your Internet IP address changes, the router will automatically communicate the new IP address to the DDNS.

- DDNS. Click to enable this service.
- Provider. Choose your DDNS service provider.
- Host Name. Supplied by your DDNS provider.
- Username/E-mail: Supplied by your DDNS provider.
- Password/Key: Supplied by your DDNS provider.

After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

9.4 DDNS SERVICES

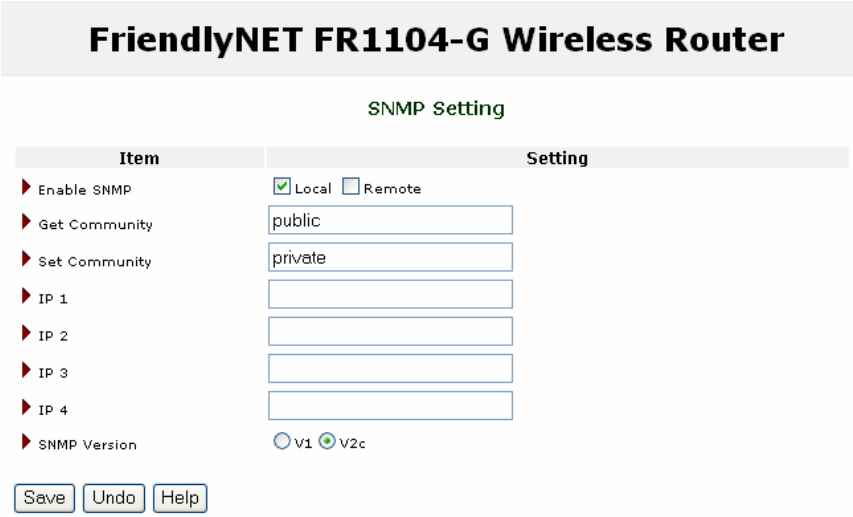
Since DDNS is a service offered by a third-party, Asanté Technologies does not endorse nor can Asanté be responsible or provide technical support for such services. You will need to open an account with a supported DDNS before enabling this feature.

Note: For business-critical websites, a dedicated web host with a static IP address is strongly recommended.

Service	Description	Link
DynDNS.org	Alias dynamic IP address to a static hostname on specified domain. Up to 5 host names provided free.	http://www.dyndns.org/services/dyndns
	Full DNS service for custom domain name ($24.95).	http://www.dyndns.org/services/custom/
TZO.com	Choice of sub-domain ($24.95) or custom domain name ($59.95).	http://www.tzo.com
dhs.org	Mandatory “donation” ($5).	https://members.dhs.org/signup

All information was current during the research for this document. Annual rates current as of December 2003. Prices subject to change; contact service provider for service, details and support.

9.5 SNMP



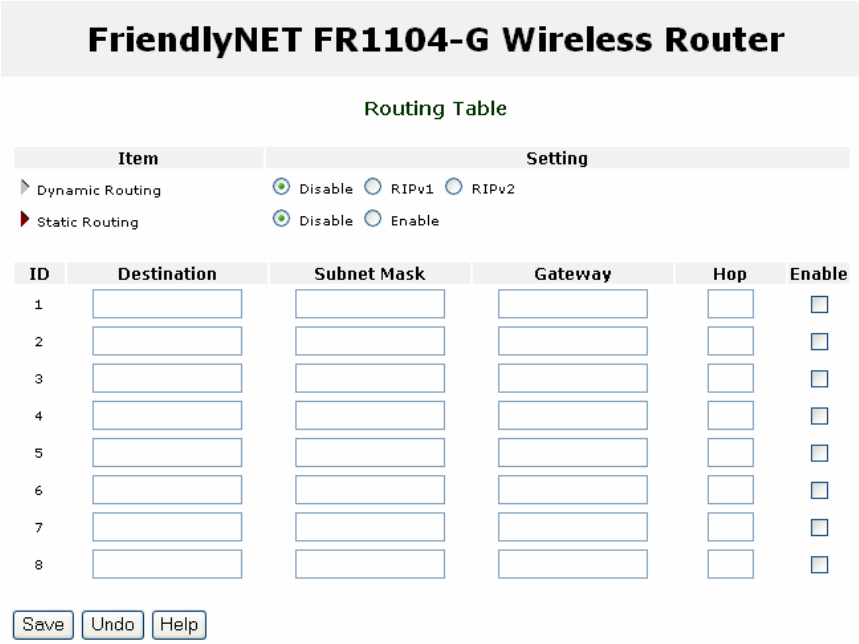
Simple Network Management Protocol (SNMP) is a standard for providing remote network management services via polling (get) and setting (set) device values.

- Enable SNMP. The router will respond to SNMP requests from Local (LAN or WLAN), Remote (Internet) or both. Unless you must have remote SNMP support, you should only enable support for Local clients.
- Get Community. Define the community the router will support for GetRequest.
- Set Community. Define the community the router will support for SetRequest.
- IP 1, 2, 3, 4. Enter the IP address of your client (computer) supporting SNMP management. The router will send SNMP trap messages to this client.
- SNMP Version. Choose the version compatible with your SNMP management software.

SNMP	Sample Settings
Enable SNMP	Local
Get Community	public
Set Community	private
IP 1	192.168.123.33
SNMP Version	V2c

After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

9.6 ROUTING



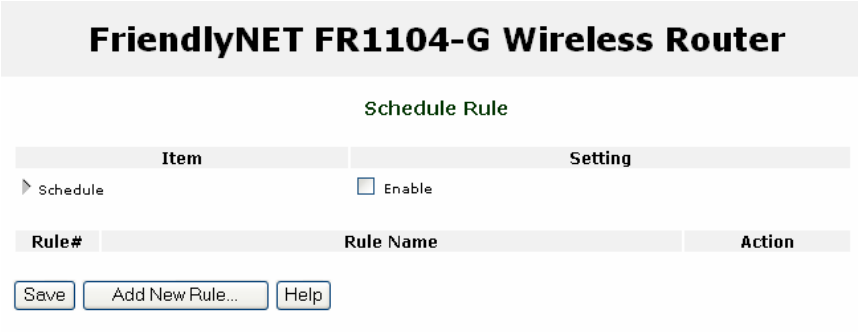
The router supports dynamic and static routing for large networks with multiple routers and subnets. If you have fewer than 255 clients (computers and devices) on the same network, skip this section.

Routing tables permit you to choose the physical interface address for determining outgoing IP packets. When you have a network with 2 or more routers and subnets, configure the routing tables so that packets will follow the proper routing path and subnets can communicate with each other.

- Dynamic Routing. Choose RIPv2 if you have 2 or more subnets in your network. Otherwise, choose RIPv1 or Disable.
- Static Routing. You may manually define up to 8 routing rules. In the table, enter the destination IP address, subnet mask, gateway and hop for each rule. You may selectively enable or disable each rule.

After making changes, be sure to click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

9.7 SCHEDULE RULE



Services and filters can be individually turned on and off per schedule. For example, you can define these rules to control activities:

- Limit all outbound packets, except FTP, during OffPeak hours.
- Drop all packets to banned domains (espn, napster) during BusinessHours, except select managers.
- Log all requests to specific domains (headquarters.com) during EarlyAM.
- During AfterHours, block access to websites with specific keywords (sex, tv).

Name of Rule	Schedule	Description
BusinessHours	M-F, 08:00 to 18:00	Weekdays, 8am to 6pm
EarlyAM	M-F, 05:00 to 08:00	Weekdays, 5am to 8am
AfterHours	M-F, 18:00 to 23:00	Weekdays, 6pm to 11pm
OffPeak	Everyday 23:00 to 05:00	Everyday 11pm to 5am

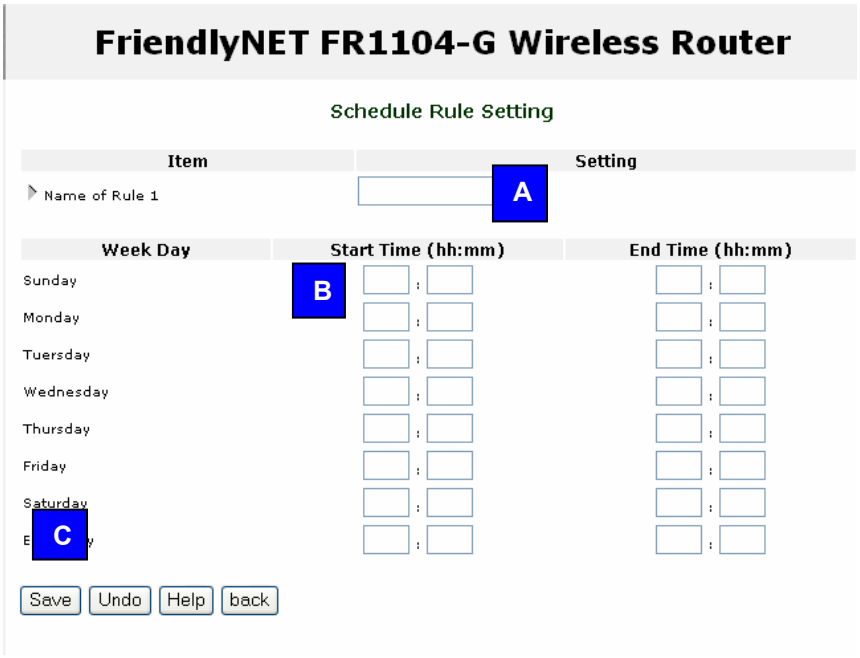
To implement rules like these:

1. Create schedule rules.
2. Create packet, domain and URL filters. See *Security Settings* menu. The rules will appear in the drop-down menu at the bottom of each screen.

To create a new rule, click **Add New Rule**.
When you have multiple rules, you may click **Edit** to modify the rule or **Delete** to remove the rule.

9.8 SCHEDULE RULE SETTING

From the Schedule Rule screen, click **Add New Rule**.

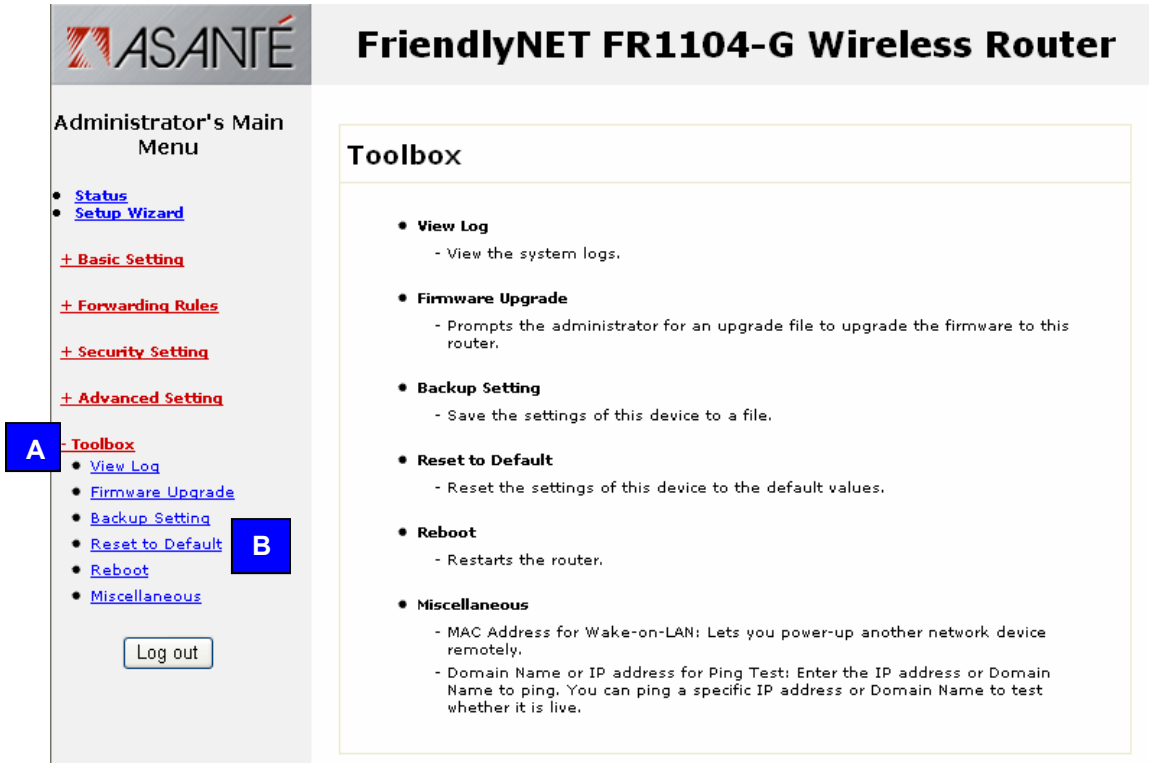


To define a schedule rule:

A. Name your rule.
B. Enter the starting and ending times for each day of the week (or every day). Be sure to use “military time” in which 08:00 is 8am and 20:00 is 8pm.
C. When you’re finished, click **Save**.

Chapter 10. Toolbox

After logging into the router, click on the **Toolbox** link [A]. Choose from one of the six sub-menus [B].

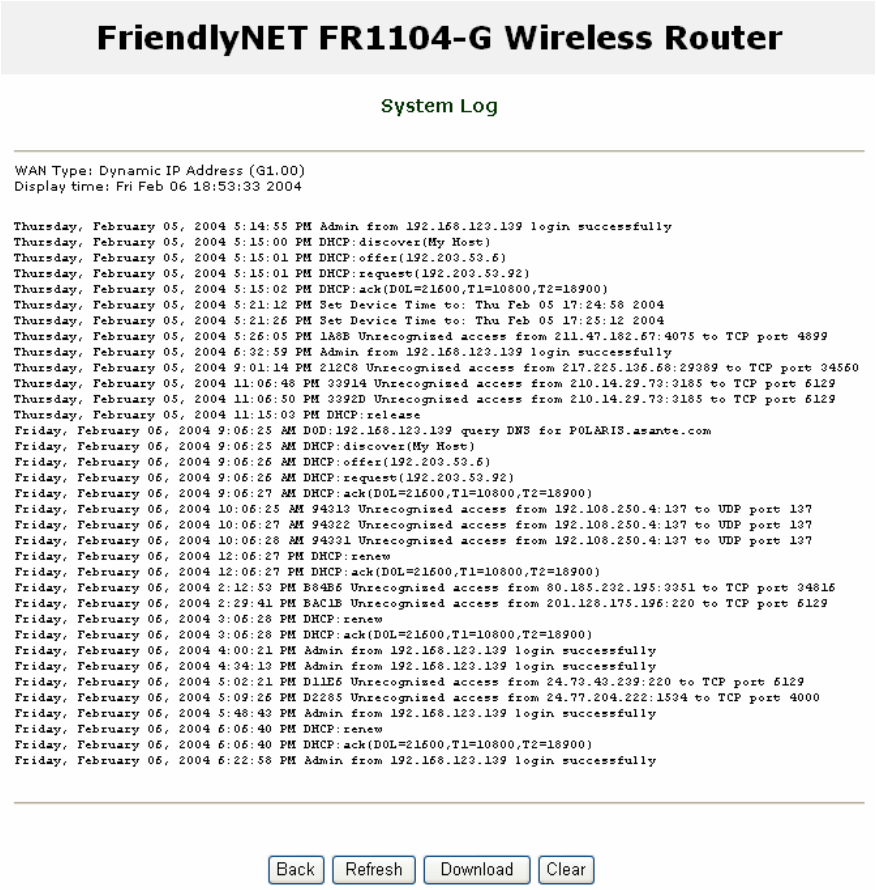


This section provides quick access to some important tools, plus specialty functions that will be valuable to only a few network administrators.

Toolbox	Description
View Log	View system log.
Firmware Upgrade	Download and then update the router's internal software.
Backup Setting	Save a copy of the router's current firmware and settings.
Reset to Default	When all else fails, go back to the original factory settings.
Reboot	Restart the router. Similar to power off/on.
Miscellaneous	Wake-on-LAN and ping.

10.1 SYSTEM LOG

Click on **View Log** to display the System Log screen.

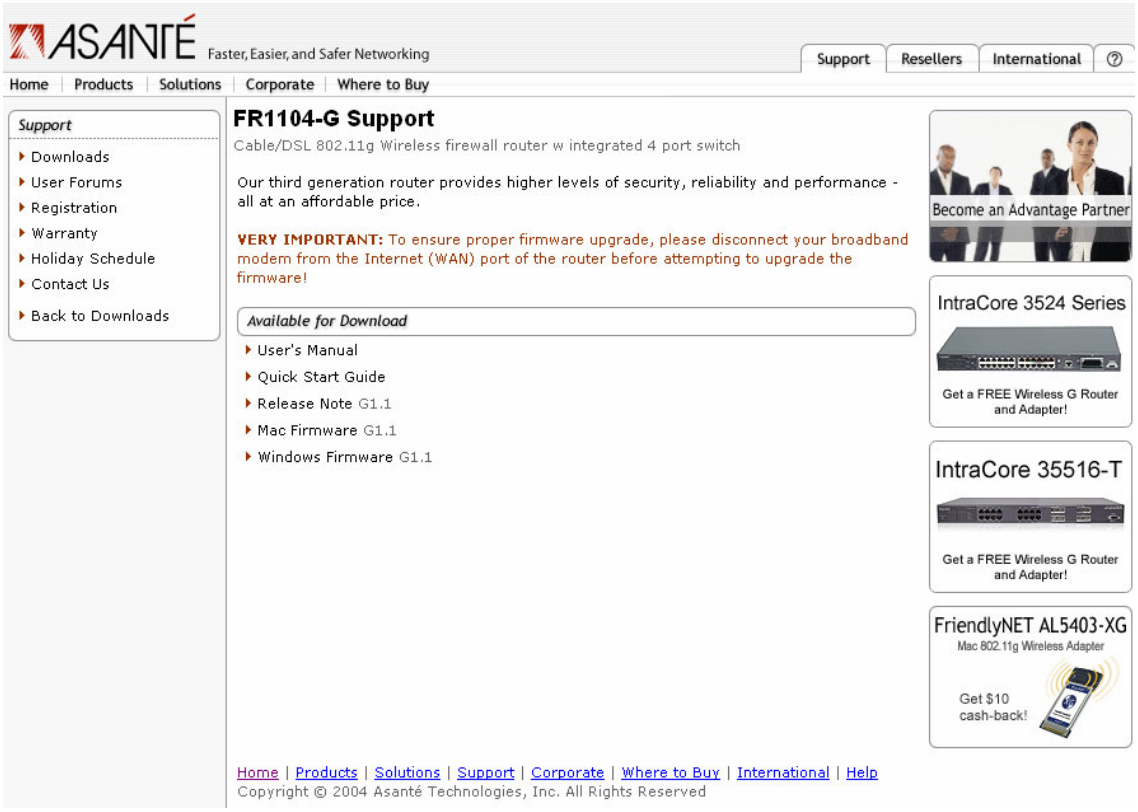


After the log information is displayed on the screen, click **Refresh** to update with the latest activities.
To save the log into a text file, click **Download**.
To reset the log, click **Clear**.
To return to the previous menu, click **Back**.

Tip: This log may be emailed or automatically stored on a syslog server. See Advanced Settings > System Log.

10.2 FIRMWARE UPGRADE

To check for the latest firmware updates for the router, open a new web browser window and visit http://www.asante.com/support/downProd.aspx?id=FR1104-G



Version G1.1 firmware is available for Mac OS (.bin) and Windows (.zip) users. Other than the compression format, the firmware for both operating systems is the same.

Firmware Update Precautions

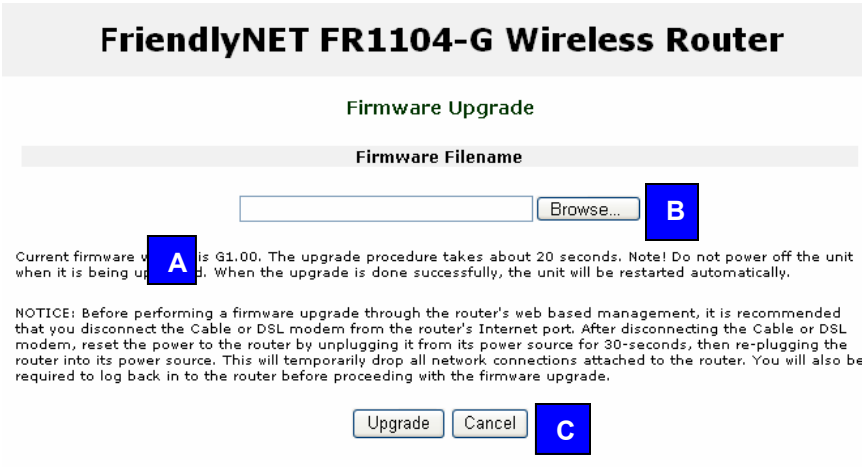
These safeguards ensure that the upgrades will be performed successfully.

Tip: If your router is already functioning properly, Asanté does not recommend upgrading firmware just to have newer firmware.

- Download the FriendlyNET FR1104-G firmware from Asanté's website (above).
- Back up your current firmware and settings. See Toolbox > Backup Settings.
- Write down your password and any special Internet settings on a separate piece of paper. Some router updates will require you to reset the router to factory defaults before it can be customized with your settings. See the release note accompanying your firmware download.
- Perform the firmware upgrade only from a computer directly connected to the router's LAN (ports 1–4) only. Disconnect the network cable connected to the router's Internet port and all other LAN ports. The firmware update process must be completed with no interruptions from other network activities.
- **DO NOT** turn off the power or unplug the router while the update is in process. This could cause your router to be permanently damaged.
- After the update is completed, follow the on-screen instructions to restart the router.

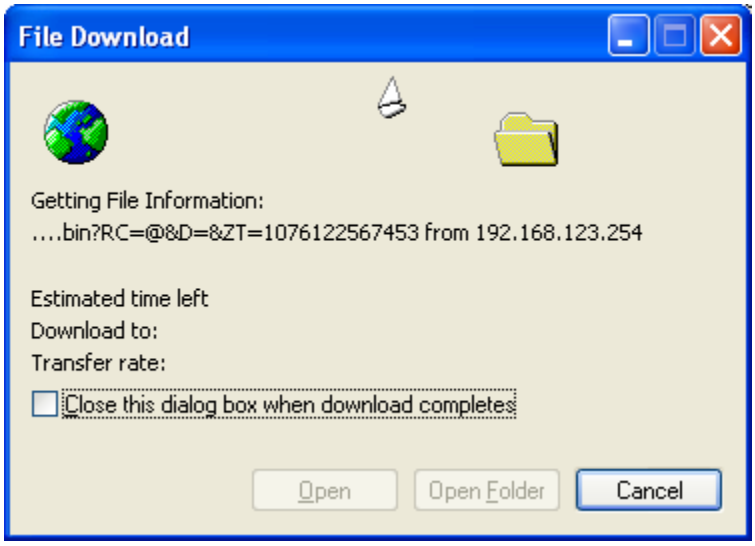
Warning! Do not download or attempt to use firmware that is not explicitly designed for your FR1104-G router by Asanté Technologies. Use of non-Asanté firmware will terminate Asanté's ability to provide technical support or warranty service for your product.

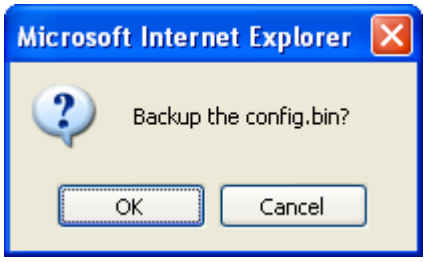
To apply the firmware, click on the **Firmware Upgrade** link in the router's administration utility.



A. Compare the router's current **firmware version** number with the file you downloaded.
B. Click on **Browse** to locate the new file you downloaded.
C. Click **Upgrade** to install the new firmware.

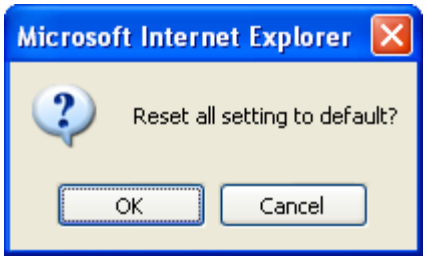
10.3 BACKUP SETTING





Click **OK** to save your router's firmware and all settings into a **config.bin** file. You will be prompted for the name and location of the file.

10.4 RESET TO DEFAULT

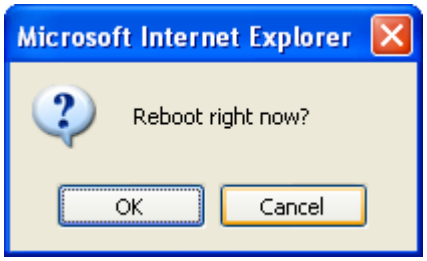


Click **OK** to restore your router's settings to the original factory defaults:

- Default IP address: 192.168.123.254
- Default administrator's password: admin
- Default WAN type: dynamic IP address

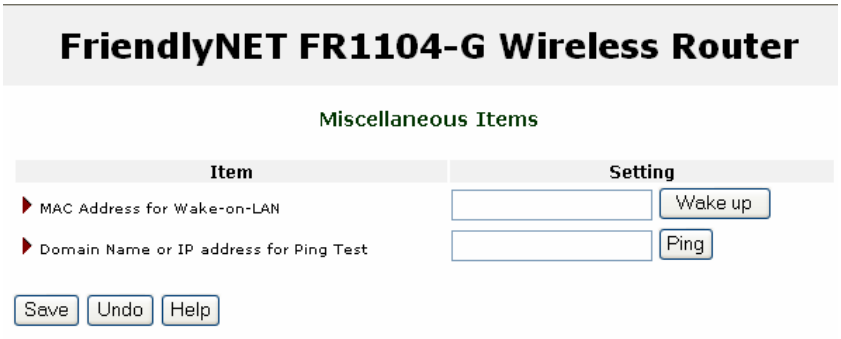
Tip: Before clicking **OK**, be sure to record all your settings on a separate piece of paper so you'll know how to restore them later.

10.5 REBOOT



Click **OK** to restart your router. This is similar to powering your router off and then on. All your saved settings will be restored.

10.6 TOOLBOX MISCELLANEOUS



- MAC Address for Wake-on-LAN (WoL). This technology is used to power up a client from another location on the local network. To use this feature, your target clients must be WoL-enabled. Enter the MAC address for the client and click **Wake up**.

  Tip: See Status > Clients List to wake up clients by name.

- Domain Name or IP address for Ping Test. This handy tool allows you to verify physical and logical connections between the router and any local client (LAN or WLAN) or on the Internet (WAN). Enter the IP address (e.g., 192.168.123.100) or domain name (e.g., www.asante.com or www.google.com).

To save these addresses for the future, click **Save**.
To restore the last saved settings, click **Undo**.
To read on-screen information on this page, click **Help**.

Appendix A. Product Specifications

Overview

LAN:	4 x 10/100 Mbps Fast Ethernet with Auto-Uplink (100BaseTX, 10BaseT): RJ-45 connector
Wireless:	54 Mbps (IEEE 802.11g), 22 Mbps (TI 802.11b+) and 11 Mbps (IEEE 802.11b)
Internet:	10/100 Mbps Fast Ethernet with Auto-Uplink (100BaseTX, 10BaseT): RJ-45 connector
Status Indicators:	Power, Status, Speed, Link/Activity (per port), Internet and Wireless
Wireless Antenna:	Single 4 dBm, upgradeable (uses RP-SMA connector)

Software

Setup:	Wizard guides you through the basic settings required for your installation
Administration:	Configure locally or remotely from any popular web browser
Remote Administration:	Allow a trusted administrator to change settings via Internet
Firmware:	Upgradeable via web browser or Windows application
Device Status:	Router IP address, LAN MAC address, WAN MAC address and firmware version
Supported WAN Types:	Dynamic IP address (default), static IP, PPPoE, PPPTP and dynamic for Road Runner/Telstra BigPond
Virtual Private Network:	VPN pass through for IPSec, PPTP and L2TP
Dynamic DNS:	Support dyndns, TZO and dhs
Routing:	Network address translation (NAT), static and dynamic routing (RIP 1/2) tables
Advanced Features:	Wake-on-LAN (WOL) management and SNMP (v1 and 2c)

Network Security Settings

Log:	Record all intrusion attempts and activities into on-screen log, syslog and email alert
Firewall:	Schedule inbound/outbound packet filter, domain filters and keyword/URL blocking
MAC Address Control:	Set access for different users and assign an IP address to a specific MAC address
Miscellaneous:	Discard ping from WAN, denial of service protection, ping device, DMZ, virtual servers and time server

Wireless Settings

Basic:	Network ID (SSID), channel, 64- and 128-bit WEP encryption
Advanced:	256-bit WEP encryption. Wi-Fi Protected Access (WPA) with RADIUS or pre-shared key
Authentication:	802.1X with 64/128-bit key for RADIUS server
Frequency:	2.412–2.497 GHZ ISM frequency band
Channels:	USA and Canada (1–11), Europe (1–11), Japan (1–11), Spain (10–11), France (10–11)
Modulation Techniques:	802.11b: CCK (11, 5.5 Mbps), DQSP (2 Mbps) and DBPSX (1 Mbps) 802.11g: OFDM (54 Mbps)
Typical Coverage:	802.11b: Indoor up to 50 M at 11 Mbps; outdoor up to 130 M at 11Mbps 802.11g: Indoor up to 20 M at 54 Mbps; outdoor up to 50 M at 54 Mbps

Performance

Microprocessor:	32-bit embedded RISC with integrated 8 KB cache
Internet:	10/100 Mbps
LAN:	10/100 Mbps

System Requirements

Microsoft:	Windows 95/98/Me, NT/2000/XP and Xbox
Apple:	Mac OS 8, 9 and X
Network Interface:	10/100 Fast Ethernet or 802.11b/g adapter
Web Browser:	Internet Explorer (v5 and later), Netscape (v5 and later), Safari (v1 and later)

Applications Interoperability

Microsoft:	Universal Plug-and-Play (UPnP) and NetMeeting
Apple:	QuickTime. AppleTalk (requires FR1104-G firmware G1.1 and later)
Messaging:	H.323, MSN Messenger, AOL Instant Messenger, ICQ and mIRC
Application Tunnels:	User-definable application-sensing tunnel
Others:	RealPlayer, Dialpad, Quake, Half-Life and Star Craft Unreal Tournament

Standards Compliance:

Network:	IEEE 802.3u Fast Ethernet over 2 pairs of UTP Category 5 (100BaseTX) IEEE 802.3 Ethernet over 2 pairs of UTP Category 3 (10BaseT) IEEE 802.11b (up to 11 Mbps) IEEE 802.11g (up to 54 Mbps)
Network Protocols:	TCP/IP, CSMA/CA with ACK
Regulatory:	FCC Class B, CE Mark

Physical

Dimensions (W x H):	7.9 x 5.9 x 1.7 inches (201 x 151 x 44 mm)
Weight:	About 1.1 pounds (0.5 Kg)
Power:	5 VDC, 1.5 A (external power module included)
Operating Temperature:	32º to 104º F (0º to 40º C)
Relative Humidity:	10% to 90% non-condensing

Support

Technical Support:	24-hour support via web and ftp. 2-year email and telephone support
Product Warranty:	2-year product warranty covers defects in manufacturing and workmanship
Product Updates:	Free download of maintenance releases from www.asante.com website

Packing List

Product:	FR1104-G router
Localized Power:	5 VDC, 2.0 A power module
Cable:	10/100 Mbps Fast Ethernet, Category 5, about 5 feet (1.5 meters)
Documentation:	Quick Start Guide
CD-ROM:	Utilities, User's Manual and other documentation

Recommended Accessories

802.11g Wireless Adapters:	AL5402-XG, AL5403-XG, AL5410-G
802.11b Wireless Adapters:	AL1011-DP, AL1211-DP, AL1511 AL1611, AL2011, AL3011

Note: Specifications subject to change without prior notice.

Asanté Product Registration

Name

Title

Company

Address 1

Address 2

City

State

Zip/Postal

Country

Phone

Fax

Email

Date of Purchase

Asanté Part Number

Product Serial Number

ASANTÉ

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 4195 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

REGISTRATION CARDS
ASANTE TECHNOLOGIES INC
821 FOX LANE
SAN JOSE CA 95131-9882