USER GUIDE

Cisco Small Business

WRP400 Wireless-G Broadband Router with 2 Phone Ports

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Contents

Finding Information in PDF Files

The WRP400 documents are published as PDF files. The PDF Find/Search tool within Adobe® Reader® lets you find information quickly and easily online. You can perform the following tasks:

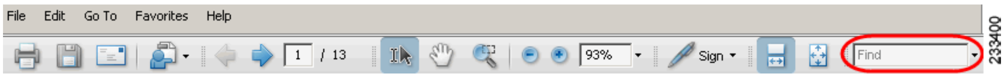
- Search an individual PDF file.
- Search multiple PDF files at once (for example, all PDFs in a specific folder or disk drive).
- Perform advanced searches.

Finding Text in a PDF

Follow this procedure to find text in a PDF file.

STEP 1 Enter your search terms in the Find text box on the toolbar.

NOTE By default, the Find tool is available at the right end of the Acrobat toolbar. If the Find tool does not appear, choose **Edit > Find.**



STEP 2 Optionally, click the arrow next to the Find text box to refine your search by choosing special options such as Whole Words Only.

STEP 3 Press **Enter.**

STEP 4 Acrobat displays the first instance of the search term.

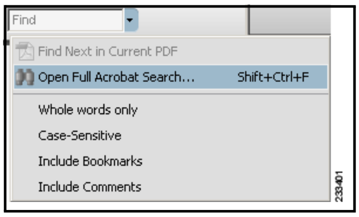
STEP 5 Press **Enter** again to continue to more instances of the term.

Finding Text in Multiple PDF Files

The *Search* window lets you search for terms in multiple PDF files that are stored on your PC or local network. The PDF files do not need to be open.

STEP 1 Start Acrobat Professional or Adobe Reader.

STEP 2 Choose **Edit** > **Search**, or click the arrow next to the *Find* box and then choose **Open Full Acrobat Search.**



STEP 3 In the *Search* window, complete the following steps:

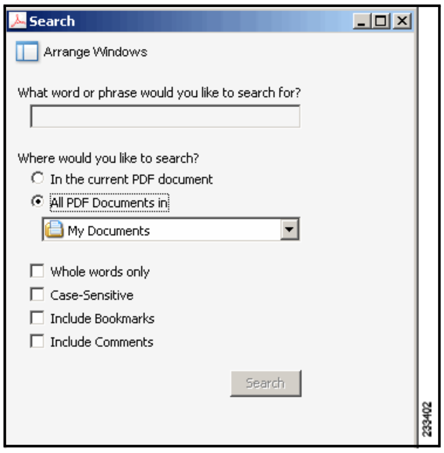
a. Enter the text that you want to find.

b. Choose **All PDF Documents in.**

From the drop-down box, choose **Browse for Location.** Then choose the location on your computer or local network, and click **OK.**

c. If you want to specify additional search criteria, click **Use Advanced Search Options**, and choose the options you want.

d. Click **Search.**


Search

Arrange Windows

What word or phrase would you like to search for?

Where would you like to search?

○ In the current PDF document

● All PDF Documents in

My Documents

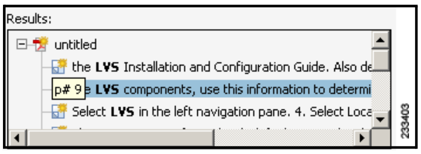
□ Whole words only

□ Case-Sensitive

□ Include Bookmarks

□ Include Comments

STEP 4 When the Results appear, click + to open a folder, and then click any link to open the file where the search terms appear.



Results:

untitled

the **LVS** Installation and Configuration Guide. Also de

p# 9 e **LVS** components, use this information to determi

Select **LVS** in the left navigation pane. 4. Select Loca

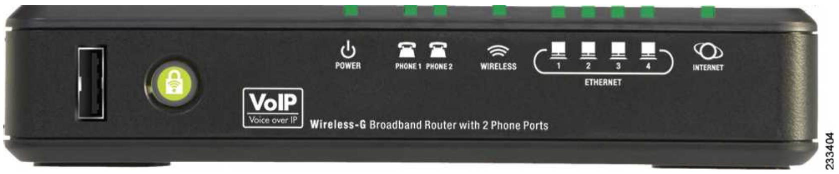
For more information about the Find and Search functions, see the Adobe Acrobat online help.

1

Getting to Know the WRP400

Thank you for choosing the Cisco WRP400 Wireless-G Broadband Router with 2 Phone Ports. The WRP400 lets you access the Internet via a wireless connection or through one of its four switched ports. You can also use the WRP400 to share resources such as computers, printers and files. The built-in phone adapter enables Voice-over-IP (VoIP) calls even while you are using the Internet.

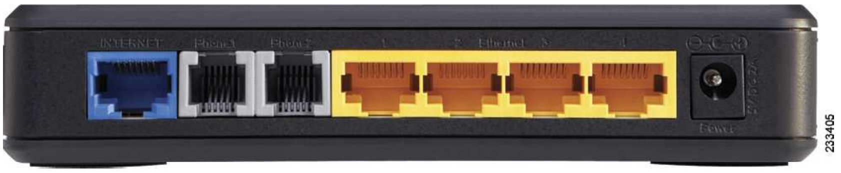
Front Panel



LED	Description
	USB: For information about supported USB devices, visit the WRP400 product page on Cisco.com: http://www.cisco.com/en/US/products/ps10028/index.html
🔒	Wi-Fi Protected Setup (White/Orange): If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to automatically configure wireless security for your wireless network(s). To use Wi-Fi Protected Setup, run the Setup Wizard, or refer to **“Wireless > Basic Wireless Settings,” on page 39**. The Wi-Fi Protected Setup button lights up white and stays on while wireless security is enabled on your wireless network(s). The LED lights up orange if there is an error during the Wi-Fi Protected Setup process. Make sure the client device supports Wi-Fi Protected Setup. Wait until the LED is off, and then try again.
⏻ POWER	**Power (Green/Red/Orange):** This LED indicates the status of power and the progress of the self-diagnostic test upon bootup. If a USB modem is connected to the USB port, this LED indicates the progress of initialization and the status of the mobile network connection. ▪ **Power:** The Power LED shines green and stays on while the WRP400 is powered on. If the LED shines red, verify that the correct power adapter is used. If the LED remains red, contact your service provider for support. ▪ **Self-diagnostic test:** During boot-up, the LED flashes green to indicate that the self-diagnostic test is in progress. When the test is complete, the LED shines steady green. ▪ **Initialization of a USB modem:** When you connect a device to the USB port, the Power LED flashes green and orange, indicating that initialization is in progress. After the device initializes, the Power LED shines steady green. If the device fails to initialize, the LED continues to flash green and orange.

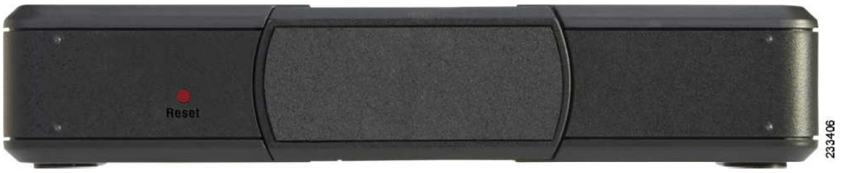
LED	Description
	▪ **Mobile network connection:** If a USB modem is installed, the mobile network connection is used as a failover when an Ethernet connection is unavailable. The Power LED shows the status of the mobile network: ▪ **Flashing Orange:** The WRP400 is attempting to connect to the Internet through the mobile network connection. ▪ **Steady Orange:** The WRP400 is connected to the Internet through the mobile network connection. ▪ **Continuous Flashing Orange:** The WRP400 failed to connect to the Internet through the mobile network connection and is trying again. ▪ **Steady Green:** If a USB device is connected, this LED behavior indicates that the device was successfully initialized and that the WRP400 is not using the mobile network connection. If the USB device is removed, this LED behavior indicates that theWRP400 has power.
☎ PHONE	**Phone 1-2 (Green):** The Phone 1 or 2 LED lights up and stays on when an active line is registered to the corresponding port on the back panel. The LED slowly flashes when voicemail messages are waiting.
WIRELESS	**Wireless (Green):** The Wireless LED lights up when the wireless feature is enabled. It flashes when the WRP400 is actively sending or receiving data over the network.
ETHERNET	**Ethernet 1-4 (Green):** These numbered LEDs, corresponding with the numbered ports on the back panel, serve two purposes. If the LED is solidly lit, the WRP400 is connected to a device through that port. It flashes to indicate network activity over that port.
INTERNET	**Internet (Green):** The Internet LED lights up and stays on when an Internet connection is made through the Internet port. It flashes to indicate network activity over the Internet port. **NOTE:** The Power LED indicates Internet connectivity through the mobile network connection. See the information for the Power LED in this table.

Back Panel



Port	Description
🟦	**Internet:** Use this port to connect the WRP400 to a cable or DSL Internet connection.
⬜	**Phone 1-2:** Use these ports to connect standard analog telephones to the WRP400.
🟨	**Ethernet 1, 2, 3, 4:** Use these Ethernet ports to connect the WRP400 to wired computers and other Ethernet network devices.
⬛	**Power:** Use the power port to connect the power adapter.

Side Panel



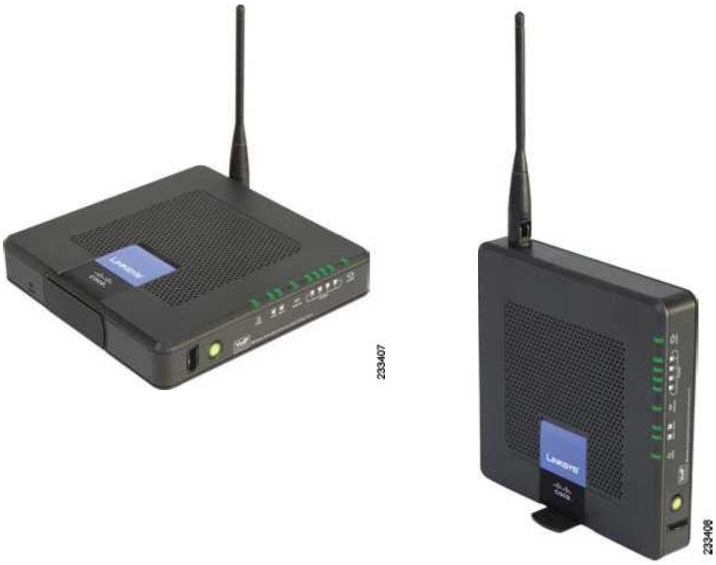
	Reset: There are two ways to reset the WRP400 to the factory default settings. Either press and hold the Reset button for approximately ten seconds, or restore the defaults from the Administration >Factory Defaults screen of the administration web server. (The Factory Defaults screen allows you to restore the router and voice defaults separately.) **NOTE:** Restoring the voice defaults may require your login (the default user name and password are admin). If the defaults do not work, contact your service provider for more information.
	Stand: To place the WRP400 in a vertical position, rotate the stand 90 degrees.

Placement Positions

There are three ways to physically install the WRP400:

- **Horizontal Placement:** The WRP400 has four rubber feet on the bottom panel. Place the WRP400 on a level surface near an electrical outlet.
- **Vertical Placement:** The WRP400 has a stand on the side panel opposite to the antenna. Rotate the stand 90 degrees, and place the WRP400 on a level surface near an electrical outlet.
- **Wall-Mounting Placement:** The WRP400 has four wall-mount slots on its back panel.

Figure 1 Horizontal and Vertical Placement Options

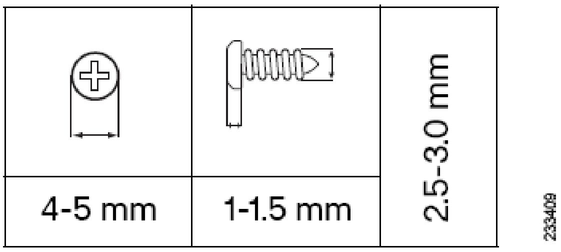


To mount the WRP400 on a wall, follow these instructions:

STEP 1 Choose a wall that is smooth, flat, dry, and sturdy. Make sure that an electrical outlet is nearby.

STEP 2 Obtain mounting hardware. Suggested hardware is illustrated below (not true to scale).

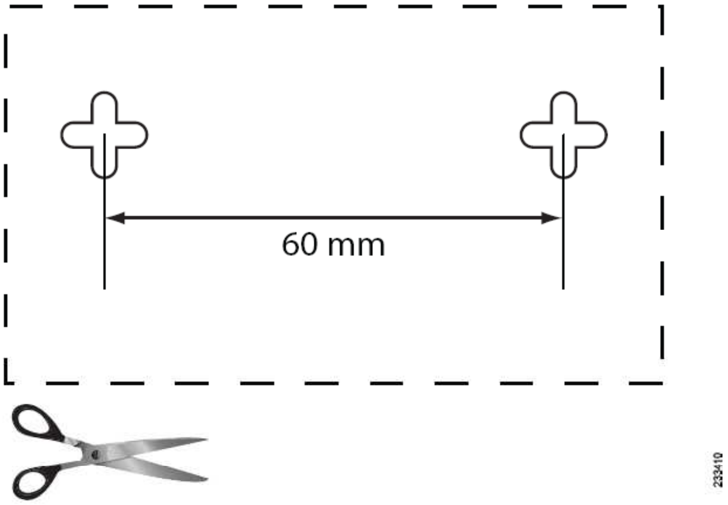
Figure 2 Mounting Hardware



STEP 3 Drill two holes, 60 mm (2.36 inches) apart. Insert a screw into each hole and leave 3 mm (0.12 inches) of the head exposed.

To create a template to position the screws, you can print this page at 100 percent. Then cut along the dotted line. Affix this template to the wall where you want to drill the holes.

Figure 3 Wall Mount Template



NOTE Cisco is not responsible for damages incurred by insecure wall-mounting hardware.

STEP 4 Position the WRP400 so that two of the wall-mount slots are over the two screws. Slide the WRP400 down until the screws fit snugly into the wall-mount slots.

2

Before You Begin: Understanding Wireless Security

Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. Because you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.

NOTE The Setup Wizard guides you through the process of completing the tasks that are described below. You are strongly encouraged to use the Setup Wizard for initial configuration of the WRP400.

Change the Default Wireless Network Name or SSID

Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. To distinguish your wireless network from other wireless networks that may exist around you, you should change the default wireless network name to something easily recognizable, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks. For more information, see **"Wireless > Basic Wireless Settings," on page 51**.

Change the Default Router Password

When you connect to the administration web server, you will be asked for a password. The WRP400 has a default password set by the factory. The default password is **admin**. Hackers know the defaults and may try to use them to access your wireless device and change your network settings. To prevent unauthorized access, change the password to one that is hard to guess. For more information, see **"Administration > Management," on page 88**.

Enable MAC Address Filtering for Wireless Access

The Cisco WRP400 gives you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network. For more information, see **"Wireless > Wireless MAC Filter," on page 62**.

Enable Encryption

Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication.

A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

For more information, see **"Wireless > Wireless Security," on page 56**.

General Network Security Guidelines

Wireless network security is effective only when combined with good network security practices.

- Password protect all computers on the network and individually password protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge.

Additional Security Tips

To help prevent security problems, follow these guidelines:

- Keep wireless routers, access points, or gateways away from exterior walls and windows.
- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.

3

Using the Web-Based Utility for Advanced Configuration

After you set up the WRP400 with the Setup Wizard (located on the CD-ROM), the router will be ready for use. However, if you'd like to change its advanced settings, use the web-based utility. This chapter describes each web page of the utility and each page's key functions. You can access the utility via a web browser on a computer connected to the router.

The web-based utility has these main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, Status, and Voice. Additional tabs will be available after you click one of the main tabs.

✓ NOTE When first installing the WRP400, you should use the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter to learn about the web-based utility.

The web-based utility has the following main tabs:

- **Setup:** On the Setup screens, you can configure general settings, such as Internet connection, IP address, DHCP server settings, DDNS, time settings, and advanced router settings. For more information, see **Chapter 4, "Basic Settings."**
- **Mobile Network:** You can connect a Mobile Broadband USB modem to the USB port of the WRP400 and configure the mobile network connection.For more information, see **Chapter 5, "Installing and Configuring Your Mobile Network."**
- **Wireless:** You can use the Wireless screens to set up and secure your wireless network.For more information, see **Chapter 6, "Configuring Your Wireless Network."**
- **Security and Access Restrictions:** You can use the Security screens to enable a firewall, add filters, or allow VPN tunnels. You can use the Access Restrictions screen to control Internet usage.For more information, see

Chapter 7, "Configuring Network Security and Controlling Internet Access."

- **Applications & Gaming:** You can use the Applications and Gaming screens to configure your WRP400 to support applications, services, and gaming. For more information, see **Chapter 8, "Configuring Applications and Gaming."**
- **Administration:** You can use the Administration screens to manage access, configure Universal Plug and Play, support multimedia streaming, enable logging and diagnostics, restore factory default settings, upgrade firmware, and back up and restore configurations. For more information, see **Chapter 9, "Administration."**
- **Status:** You can use the Status screens to view information about your WRP400. For more information, see **Chapter 10, "Using the Status Screens."**
- **Voice:** You can use the Voice screens to manage the voice gateway features of the WRP400.For more information, see **Chapter 11, "Configuring Voice Services."**

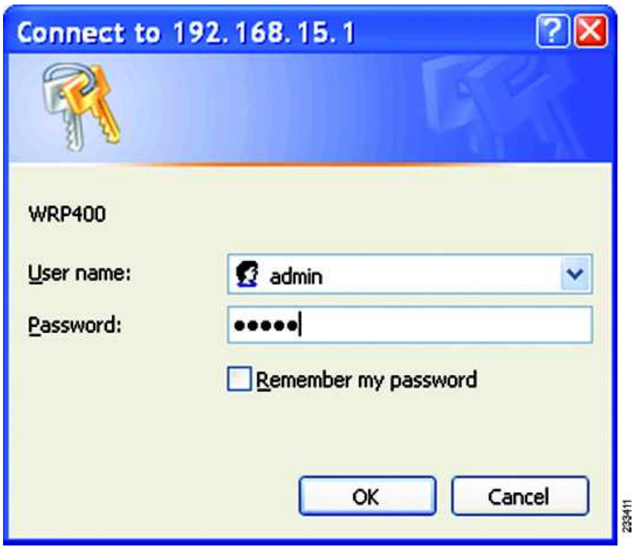
How to Access the Web-Based Utility

To access the web-based utility, launch the web browser on your computer, and enter the default IP address of the WRP400, **192.168.15.1**, in the *Address* field. Then press **Enter**.

NOTE If you place the WRP400 behind a primary router with the IP address of 192.168.15.1, then the WRP400 will automatically assume a new default IP address, 192.168.16.1.

When the login screen appears, use the default user name and password, **admin**. Then click **OK** to continue. Later, you can set a new password from the Administration tab > Management page. See **"Administration > Management," on page 88**.

Figure 4 Web-Based Utility Login Window



Connect to 192.168.15.1

WRP400

User name: admin

Password: ●●●●●

□ Remember my password

4

Basic Settings

On the Setup screens, you can configure general settings, such as Internet connection, IP address, DHCP server settings, DDNS, time settings, and advanced router settings.

How Do I...

- **Change the Internet Connection type, IP address, DHCP Server settings, and other basic settings?**
  See **"Setup > Basic Setup," on page 23**.
- **Set up DDNS for my web server or FTP server?**
  See **"Setup > DDNS," on page 34**.
- **Clone a MAC address to access my Internet service?**
  See **"Setup > MAC Address Clone," on page 37**.
- **Change the time settings?**
  See **"Time Setting," on page 33**.
- **Configure advanced settings for PPPoE Relay, NAT, Dynamic Routing (RIP), or Static Routing?**
  See **"Setup > Advanced Routing," on page 38**.

NOTE For information about using the Setup screens to configure mobile network settings, see **Chapter 5, "Installing and Configuring Your Mobile Network."**

Setup > Basic Setup

You can use the Basic Setup page to configure the Internet connection and local network settings. Complete the following sections of the page:

- **Internet Setup**
- **Network Setup**
- **Time Setting**

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Internet Setup

You can use the Internet Setup section to configure the WRP400 for your Internet connection. Most of the entries in this section require information that you can obtain from your service provider.

Internet Connection Type

Select the type of Internet connection that your service provider supports:

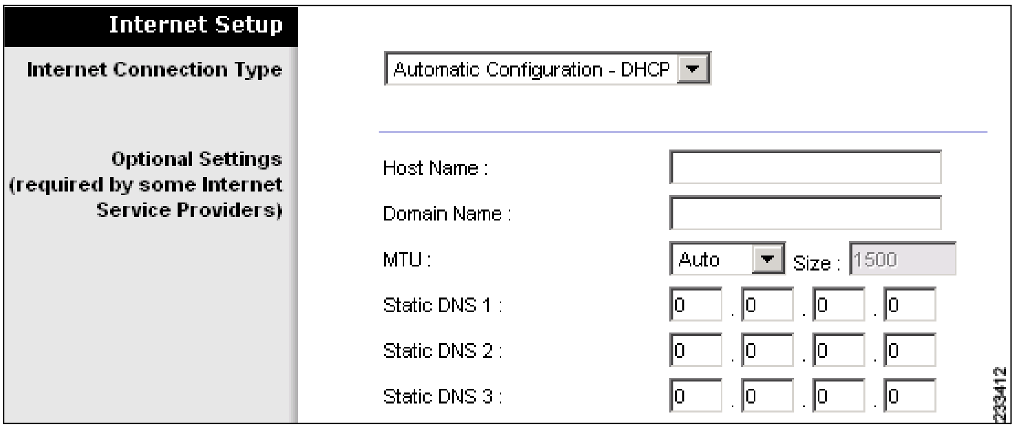
- Automatic Configuration - DHCP
- Static IP
- PPPoE
- PPTP
- L2TP
- Telstra Cable

Automatic Configuration - DHCP

By default, the Internet Connection Type is set to **Automatic Configuration - DHCP**, which should be kept only if your service provider supports DHCP or you are connecting through a dynamic IP address.

This option usually applies to cable connections.

Figure 5 Setup > Basic Setup > Internet Connection Type > Automatic Configuration - DHCP



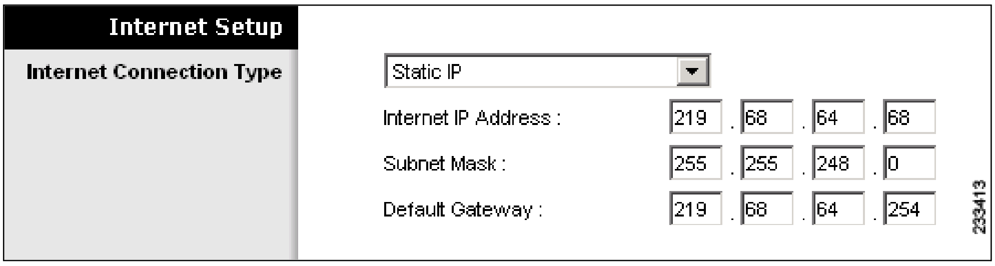
Internet Setup

Internet Connection Type		Automatic Configuration - DHCP
Optional Settings (required by some Internet Service Providers)	Host Name :	
	Domain Name :	
	MTU :	Auto Size : 1500
	Static DNS 1 :	0 . 0 . 0 . 0
	Static DNS 2 :	0 . 0 . 0 . 0
	Static DNS 3 :	0 . 0 . 0 . 0

Static IP

If you are required to use a permanent IP address to connect to the Internet, select Static IP.

Figure 6 Setup > Basic Setup > Internet Connection Type > Static IP



Internet Setup

Internet Connection Type		Static IP
	Internet IP Address :	219 . 68 . 64 . 68
	Subnet Mask :	255 . 255 . 248 . 0
	Default Gateway :	219 . 68 . 64 . 254

Enter the information that was provided by your service provider.

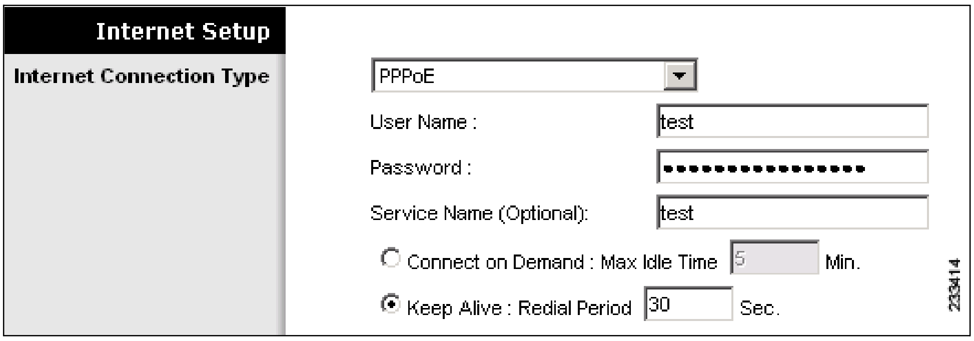
- **Internet IP Address:** The IP address of your WRP400, as seen from the Internet.
- **Subnet Mask:** The subnet mask, as seen by users on the Internet (including your service provider).
- **Default Gateway:** The IP address of your service provider server.

PPPoE

Some DSL-based service providers use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your service provider to see if they use PPPoE. If they do, you will have to enable PPPoE.

This option applies to some DSL services.

Figure 7 Setup > Basic Setup > Internet Connection Type > PPPoE



Internet Setup

Internet Connection Type

PPPoE

User Name : test

Password : ••••••••••••••••

Service Name (Optional): test

○ Connect on Demand : Max Idle Time 5 Min.

● Keep Alive : Redial Period 30 Sec.

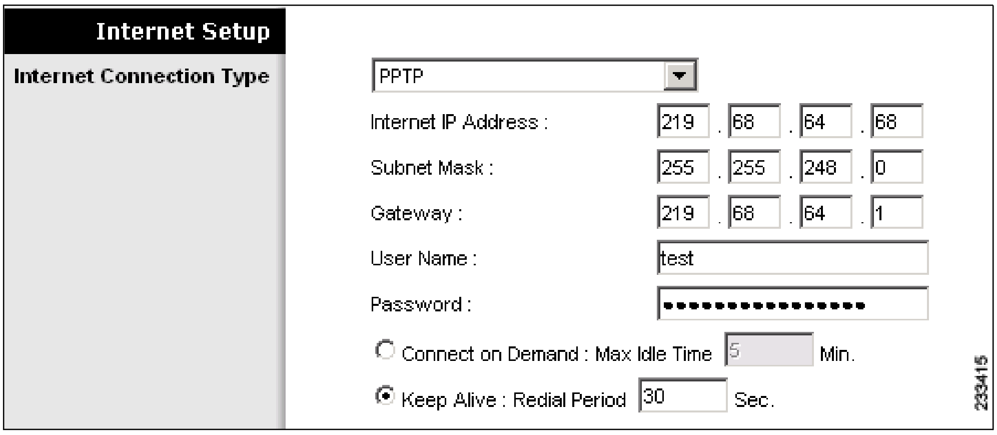
Enter the information that was provided by your service provider, and select the Connect On Demand or Keep Alive feature, if desired.

- **User Name and Password:** The login information for your account.
- **Service Name (Optional):** The service name (if provided).
- **Connect on Demand: Max Idle Time:** A feature that allows your WRP400 to re-establish a terminated connection when a user attempts to access the Internet. To enable this feature, select **Connect on Demand**. Use the Max Idle Time field to specify the period of inactivity that causes a connection to terminate. Keep the default Max Idle Time of 5 minutes, or specify the maximum period of inactivity that you want to allow.
- **Keep Alive: Redial Period:** A feature that allows your WRP400 to check your Internet connection at a specified interval (Redial Period). If you are disconnected, then the WRP400 automatically re-establishes your connection. To enable this option, select **Keep Alive.** Keep the default Redial Period of 30 seconds, or specify the interval at which you want the WRP400 to check the Internet connection.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only.

Figure 8 Setup > Basic Setup > Internet Connection Type > PPTP



Internet Setup

Internet Connection Type: PPTP

Internet IP Address : 219 . 68 . 64 . 68

Subnet Mask : 255 . 255 . 248 . 0

Gateway : 219 . 68 . 64 . 1

User Name : test

Password : ••••••••••••••••

○ Connect on Demand : Max Idle Time 5 Min.

● Keep Alive : Redial Period 30 Sec.

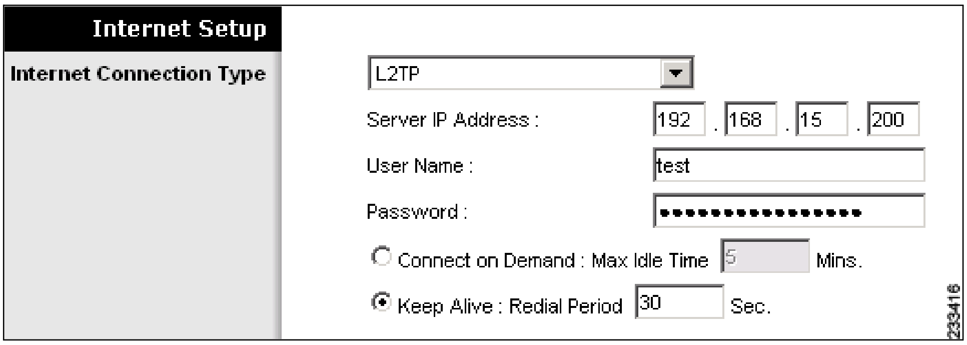
Enter the information that was provided by your service provider, and select the Connect On Demand or Keep Alive feature, if desired.

- **Internet IP Address:** The IP address of your WRP400, as seen from the Internet.
- **Subnet Mask:** The subnet mask, as seen by users on the Internet (including your service provider).
- **Default Gateway:** The IP address of your service provider server.
- **User Name and Password:** The login information for your account.
- **Connect on Demand: Max Idle Time:** A feature that allows your WRP400 to re-establish a terminated connection when a user attempts to access the Internet. To enable this feature, select **Connect on Demand**. Use the Max Idle Time field to specify the period of inactivity that causes a connection to terminate. Keep the default Max Idle Time of 5 minutes, or specify the maximum period of inactivity that you want to allow.
- **Keep Alive: Redial Period:** A feature that allows your WRP400 to check your Internet connection at a specified interval (Redial Period). If you are disconnected, then the WRP400 automatically re-establishes your connection. To enable this option, select **Keep Alive**. Keep the default Redial Period of 30 seconds, or specify the interval at which you want the WRP400 to check the Internet connection.

L2TP

L2TP is a service that applies to connections in Europe and Israel.

Figure 9 Setup > Basic Setup > Internet Connection Type > L2TP



Internet Setup

Internet Connection Type: L2TP

Server IP Address : 192 . 168 . 15 . 200

User Name : test

Password : ••••••••••••••••

○ Connect on Demand : Max Idle Time 5 Mins.

● Keep Alive : Redial Period 30 Sec.

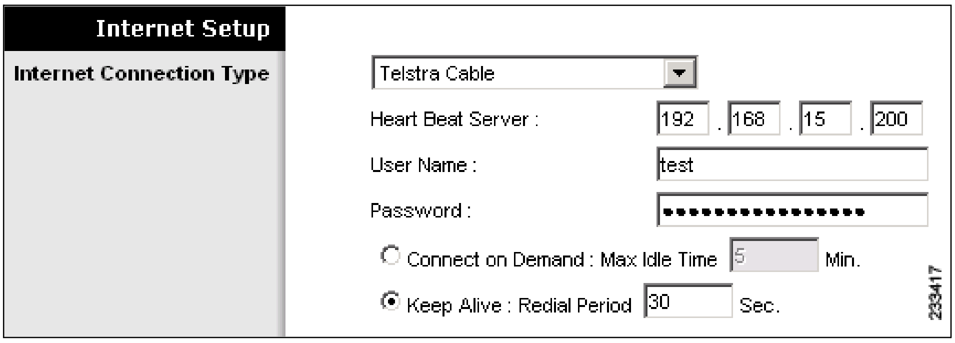
Enter the information that was provided by your service provider, and select the Connect On Demand or Keep Alive feature, if desired.

- **Server IP Address:** The IP address of the L2TP Server.
- **User Name and Password:** The login information for your account.
- **Connect on Demand: Max Idle Time:** A feature that allows your WRP400 to re-establish a terminated connection when a user attempts to access the Internet. To enable this feature, select **Connect on Demand**. Use the Max Idle Time field to specify the period of inactivity that causes a connection to terminate. Keep the default Max Idle Time of 5 minutes, or specify the maximum period of inactivity that you want to allow.
- **Keep Alive: Redial Period:** A feature that allows your WRP400 to check your Internet connection at a specified interval (Redial Period). If you are disconnected, then the WRP400 automatically re-establishes your connection. To enable this option, select **Keep Alive.** Keep the default Redial Period of 30 seconds, or specify the interval at which you want the WRP400 to check the Internet connection.

Telstra Cable

Telstra Cable is a service used in Australia only.

Figure 10 Setup > Basic Setup > Internet Connection Type > Telstra Cable



Internet Setup

Internet Connection Type: Telstra Cable

Heart Beat Server : 192 . 168 . 15 . 200

User Name : test

Password : ••••••••••••••••

○ Connect on Demand : Max Idle Time 5 Min.

● Keep Alive : Redial Period 30 Sec.

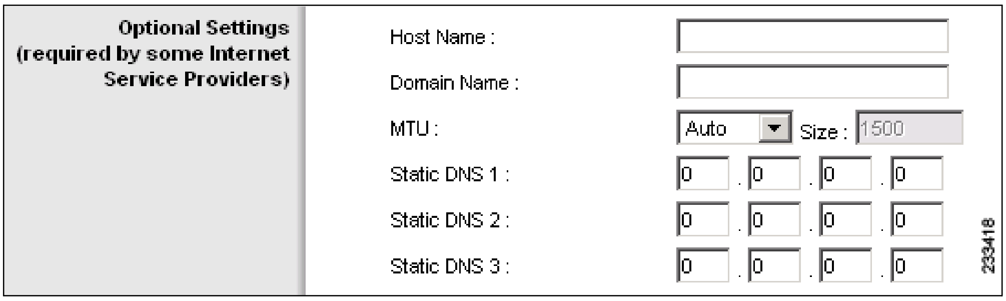
Enter the information that was provided by your service provider, and select the Connect On Demand or Keep Alive feature, if desired.

- **Heart Beat Server:** The IP address of the Heart Beat Server.
- **User Name and Password:** The login information for your account.
- **Connect on Demand: Max Idle Time:** A feature that allows your WRP400 to re-establish a terminated connection when a user attempts to access the Internet. To enable this feature, select **Connect on Demand**. Use the Max Idle Time field to specify the period of inactivity that causes a connection to terminate. Keep the default Max Idle Time of 5 minutes, or specify the maximum period of inactivity that you want to allow.
- **Keep Alive: Redial Period:** A feature that allows your WRP400 to check your Internet connection at a specified interval (Redial Period). If you are disconnected, then the WRP400 automatically re-establishes your connection. To enable this option, select **Keep Alive.** Keep the default Redial Period of 30 seconds, or specify the interval at which you want the WRP400 to check the Internet connection.

Optional Settings

Some of these settings may be required by your service provider. Verify with your service provider before making any changes.

Figure 11 Setup > Basic Setup > Optional Settings



Optional Settings (required by some Internet Service Providers)

Host Name :	
Domain Name :	
MTU :	Auto ▾ Size : 1500
Static DNS 1 :	0 . 0 . 0 . 0
Static DNS 2 :	0 . 0 . 0 . 0
Static DNS 3 :	0 . 0 . 0 . 0

- **Host Name and Domain Name:** A host and domain name for the WRP400. Some service providers, usually cable service providers, require these names as identification. In most cases, leaving these fields blank will work.
- **MTU:** MTU is the Maximum Transmission Unit. The largest packet size that is permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that is transmitted. To have the WRP400 select the best MTU for your Internet connection, keep the default setting, **Auto**.
- **Size:** When Manual is selected in the *MTU* field, this option is enabled. Leave this value in the 576 to 1500 range. The default size depends on the Internet Connection Type:
  - **DHCP or Static IP:** 1500
  - **PPPoE:** 1492
  - **PPTP or L2TP:** 460
  - **Telstra Cable:** 1500
- **Static DNS 1-3:** The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Enter the IP address of the DNS server, which is provided by your service provider. If you wish to use a different DNS server, enter its IP address in one of these fields. You can enter up to three DNS server IP addresses here. The WRP400 will use these for quicker access to functioning DNS servers. By default, the WRP400 uses 192.168.15.1 for DNS.

Network Setup

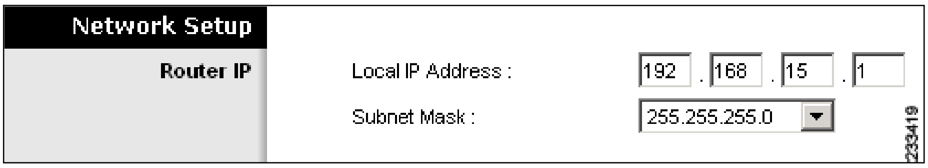
You can use the Network Setup section to change the IP address of the WRP400 and configure the DHCP server settings.

NOTE For wireless setup, use the Wireless tab. See **Chapter 6, "Configuring Your Wireless Network."**

Router IP

You can enter the Local IP Address and Subnet Mask of the WRP400, as seen by your network.

Figure 12 Setup > Basic Setup > Network Setup



Network Setup

Router IP

Local IP Address : 192 . 168 . 15 . 1

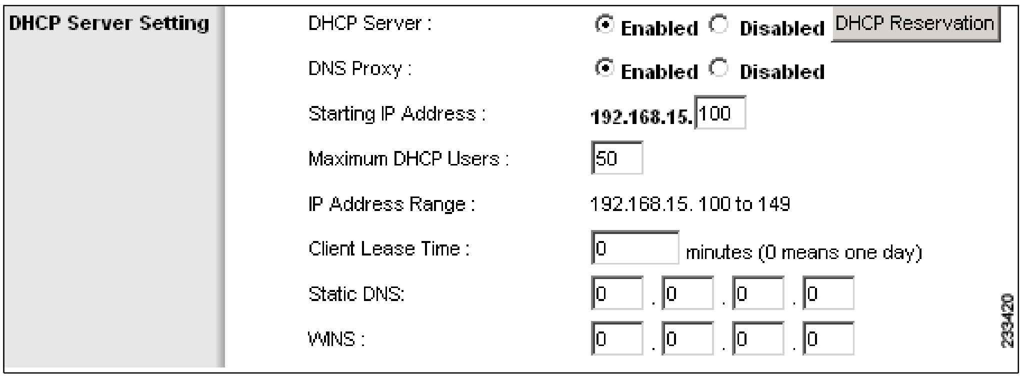
Subnet Mask : 255.255.255.0

DHCP Server Setting

You can use these settings to configure the Dynamic Host Configuration Protocol (DHCP) server function. The WRP400 can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network.

NOTE If you choose to enable the DHCP server option, make sure there is no other DHCP server on your network.

Figure 13 Setup > Basic Setup > DHCP Server Setting



DHCP Server Setting

DHCP Server :	● Enabled ○ Disabled DHCP Reservation
DNS Proxy :	● Enabled ○ Disabled
Starting IP Address :	192.168.15. 100
Maximum DHCP Users :	50
IP Address Range :	192.168.15. 100 to 149
Client Lease Time :	0 minutes (0 means one day)
Static DNS:	0 . 0 . 0 . 0
WINS :	0 . 0 . 0 . 0

- **DHCP Server:** DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't want a DHCP server, then select **Disabled** (no other DHCP features will be available).
- **DHCP Reservation:** Click this button if you want to reserve IP addresses for clients. See **"DHCP Reservation," on page 32**.
- **DNS Proxy:** To enable the DNS Proxy feature, select **Enabled.** To disable the DNS Proxy feature, keep the default, **Disabled.**

NOTE The DNS proxy relays DNS requests to the current public network DNS server for the proxy, and it replies as a DNS resolver to the client device on the network.

- **Starting IP Address:** Enter a value for the DHCP server to start with when issuing IP addresses. The Starting IP Address must be greater than the default IP address of the WRP400, 192.168.15.1, and less than 192.168.15.253. The default Starting IP Address is **192.168.15.100.**
- **Maximum DHCP Users:** Enter the maximum number of computers that will receive IP addresses from the DHCP server. This number cannot be greater than 253. The default is **50.**
- **IP Address Range:** You can view the range of available IP addresses.
- **Client Lease Time:** Enter the maximum connection time in minutes that a a dynamic IP address is "leased" to a network user. When the time elapses, the user is automatically assigned a new dynamic IP address. The default is 0 minutes, which means one day.

- **Static DNS:** Enter the local IP address of the DNS server, which is provided by your service provider. If you wish to use a different DNS server, enter that IP address in this field.

NOTE The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs.

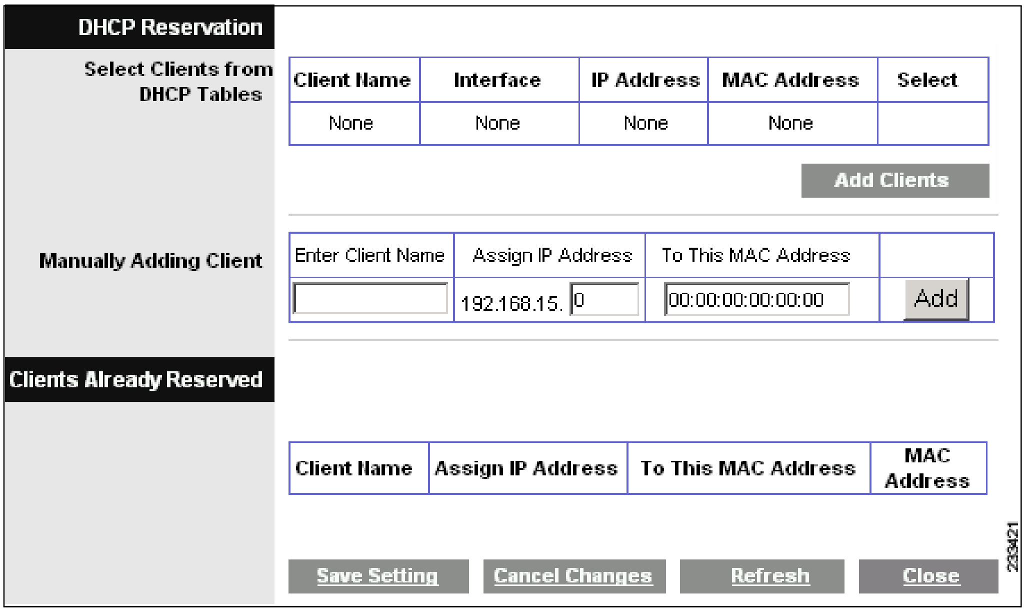
- **WINS:** If you use a WINS server, enter that server's IP address here. Otherwise, when DHCP is enabled, the field is field with the value 0.0.0.0.

NOTE The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. I

DHCP Reservation

This page appears if you click the DHCP Reservation button on the Basic Setup page. Use this page to assign a fixed local IP address to a computer on the network.

Figure 14 DHCP Reservation



Client Name	Interface	IP Address	MAC Address	Select
None	None	None	None	

Enter Client Name	Assign IP Address	To This MAC Address	
	192.168.15. 0	00:00:00:00:00:00	Add

Client Name	Assign IP Address	To This MAC Address	MAC Address

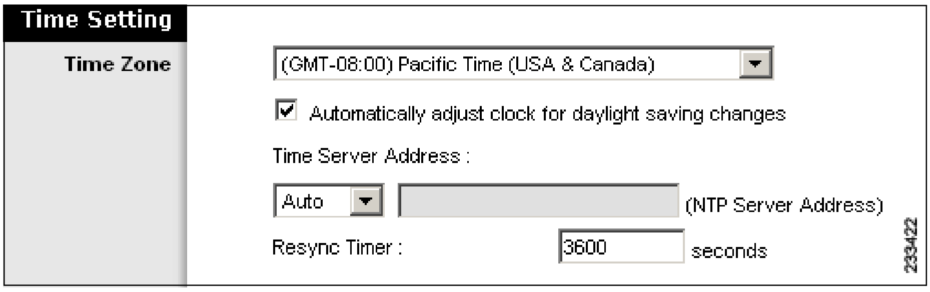
- **Select Clients from DHCP Tables:** To reserve an IP address for a client in the table, check the **Select** check box, and then click **Add Clients.**
- **Manually Adding Client:** To reserve an IP address for a client that is not listed in the Select Clients table, enter the Client Name, the desired IP Address, and the client MAC Address in the Manually Adding Client section. Then click **Add.**
- **Clients Already Reserved:** If you want to remove a client from this list, click **Remove.**

  Click **Save Setting** to apply your changes, or click **Cancel Changes** to cancel your changes. To view the most up-to-date information, click **Refresh.** To exit this screen, click **Close.**

Time Setting

In the Time Setting section of the Basic Setup page, you can choose your time zone and Time Server Address, if needed.

Figure 15 Setup > Basic Setup > Time Setting



Time Setting

Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

☑ Automatically adjust clock for daylight saving changes

Time Server Address : Auto (NTP Server Address)

Resync Timer : 3600 seconds

- **Time Zone:** Select the time zone for the location.
- **Automatically adjust clock for daylight saving changes:** Select this option if you want the WRP400 to automatically adjust the clock for daylight saving time. This option is enabled by default.
- **Time Server Address:** If you want to use the default Network Time Protocol (NTP) server, keep the default, **Auto.** If you want to specify the NTP server, select **Manual**, and enter the URL or IP address of the NTP server that you want to use.
- **Resync Timer:** Enter the number of seconds that elapse before the WRP400 resyncs with the NTP server. The default is **3600** seconds.

Setup > DDNS

You can use the DDNS page to configure the Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the WRP400.

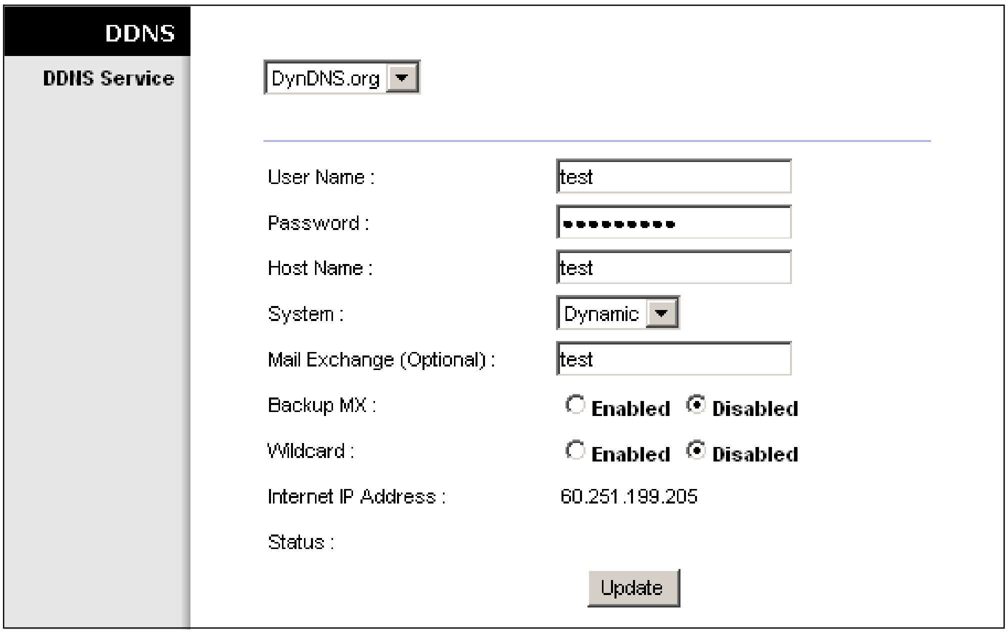
Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, such as www.dyndns.org or www.TZO.com. If you do not want to use this feature, keep the default setting, **Disabled.**

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Choose your DDNS service from the drop-down list, and then enter the information for your service.

DynDNS.org

Figure 16 Setup > DDNS > DynDNS.org

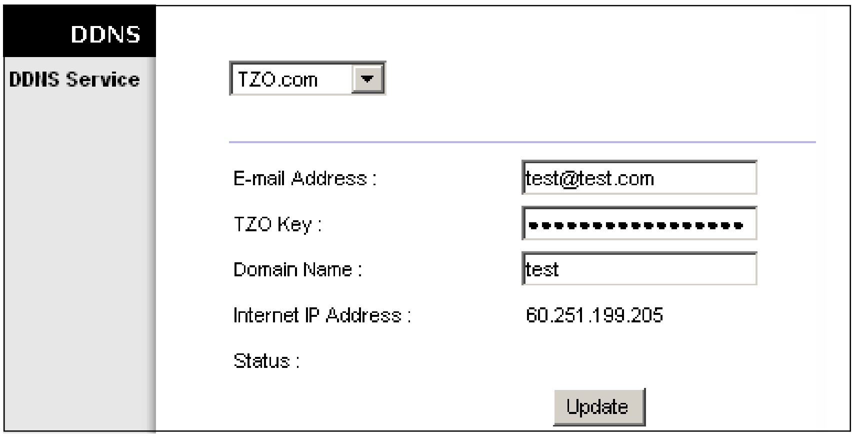


DDNS Service	DynDNS.org
User Name :	test
Password :	••••••••••
Host Name :	test
System :	Dynamic
Mail Exchange (Optional) :	test
Backup MX :	○ Enabled ● Disabled
Wildcard :	○ Enabled ● Disabled
Internet IP Address :	60.251.199.205
Status :	

- **User Name:** Enter the User Name for your DDNS account.
- **Password:** Enter the Password for your DDNS account.
- **Host Name:** Enter the DDNS URL assigned by the DDNS service.
- **System:** Choose the DynDNS service you use: **Dynamic**, **Static**, or **Custom.** The default selection is **Dynamic**.
- **Mail Exchange (Optional):** Enter the address of your mail exchange server, so emails to your DynDNS address go to your mail server.
- **Backup MX:** This feature allows the mail exchange server to be a backup. To enable the feature, select **Enabled.** To disable this feature, keep the default, **Disabled.** If you are not sure which setting to use, keep the default, **Disabled.**
- **Wildcard:** This setting enables or disables wildcards for your host. For example, if your DDNS address is *myplace.dyndns.org* and you enable wildcards, then *x.myplace.dyndns.org* will work as well (x is the wildcard). To enable wildcards, select **Enabled.** To disable wildcards, keep the default, **Disabled.** If you are not sure which setting to use, keep the default, **Disabled.**
- **Internet IP Address:** The Internet IP address of the WRP400 is displayed here. Because it is dynamic, it will change.
- **Status:** The status of the DDNS service connection is displayed here.
- **Update:** To manually trigger an update, click this button.

TZO.com

Figure 17   Setup > DDNS > TZO.com



TZO.com

E-mail Address : test@test.com

TZO Key : ••••••••••••••••••

Domain Name : test

Internet IP Address : 60.251.199.205

Status :

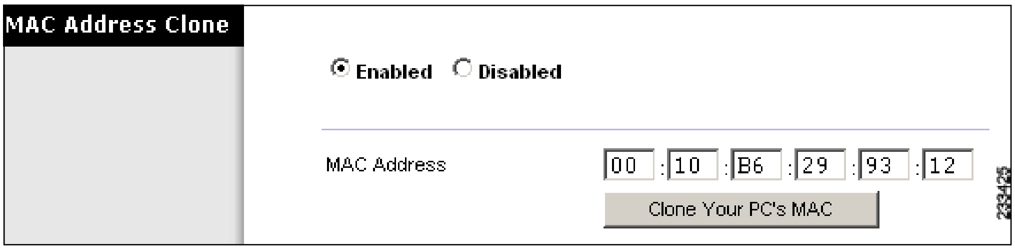
- **E-mail Address**, **TZO Key**, and **Domain Name:** Enter the settings for your account with TZO.
- **Internet IP Address:** The Internet IP address of the WRP400 is displayed here. Because it is dynamic, it will change.
- **Status:** The status of the DDNS service connection is displayed here.
- **Update:** To manually trigger an update, click this button.

Setup > MAC Address Clone

A MAC address is a unique 12-digit code that is assigned to a piece of hardware for identification. Some service providers require you to register a MAC address in order to access the Internet. If you previously registered a MAC address with your service provider for this purpose, you can reassign that MAC address to the WRP400. In this sense, you are “cloning” the MAC address to be used by this router.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 18 Setup > MAC Address Clone



MAC Address Clone

● Enabled ○ Disabled

MAC Address 00 : 10 : B6 : 29 : 93 : 12

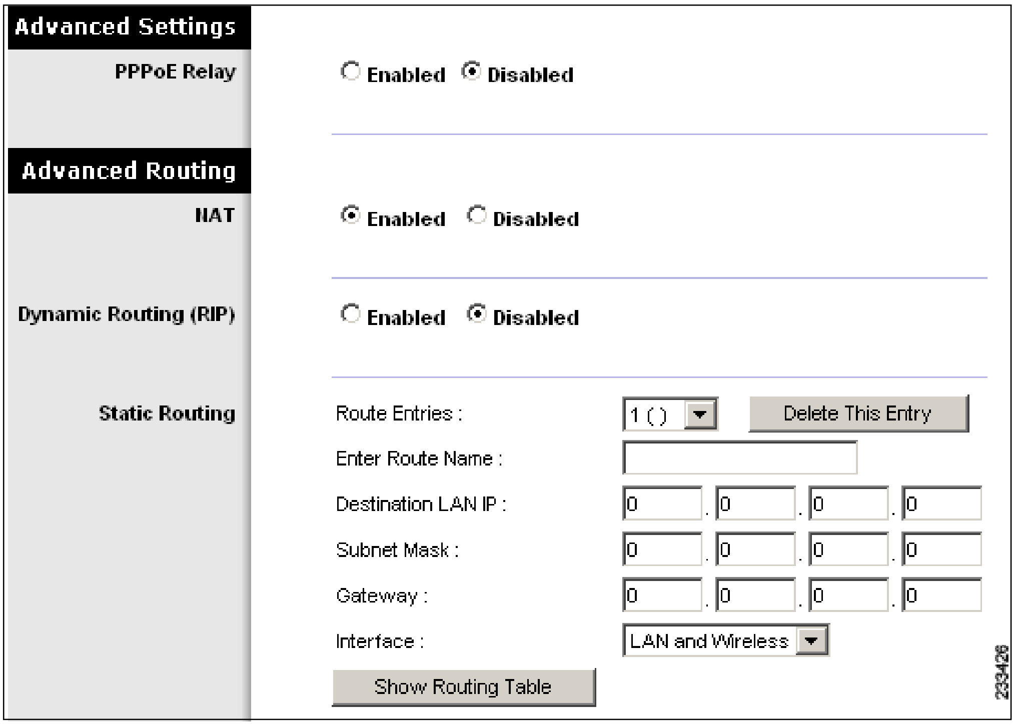
- **Enabled**, **Disabled:** To assign a previously registered MAC address to the WRP400, select **Enabled.** Otherwise, select **Disabled.**
- **MAC Address:** Enter the MAC address that you previously registered with your service provider.
- **Clone Your PC’s MAC:** Click this button to clone the MAC address of the computer you are using.

Setup > Advanced Routing

You can use the Advanced Routing page to set up PPPoE Relay, NAT, Dynamic Routing (RIP), or Static Routing.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 19 Setup > Advanced Routing



Advanced Settings

PPPoE Relay ○ Enabled ● Disabled

Advanced Routing

NAT ● Enabled ○ Disabled

Dynamic Routing (RIP) ○ Enabled ● Disabled

Static Routing

Route Entries : 1 ( ) ▾ Delete This Entry

Enter Route Name :

Destination LAN IP : 0 . 0 . 0 . 0

Subnet Mask : 0 . 0 . 0 . 0

Gateway : 0 . 0 . 0 . 0

Interface : LAN and Wireless ▾

Show Routing Table

Advanced Settings: PPPoE Relay

The PPPoE Relay feature enables an L2TP Access Concentrator (LAC) to relay active discovery and service selection functionality for PPP over Ethernet (PPPoE), over a Layer 2 Tunneling Protocol (L2TP) control channel, to an L2TP Network Server (LNS) or tunnel switch (multihop node). The relay functionality of this feature allows the LNS or tunnel switch to advertise its services to the client, thereby providing end-to-end control of services between the LNS and a PPPoE client.

To enable the PPPoE Relay feature for the Internet side, select **Enabled.** To disable the PPPoE Relay feature, keep the default, **Disabled.**

Advanced Routing

Choose the features that you want to enable.

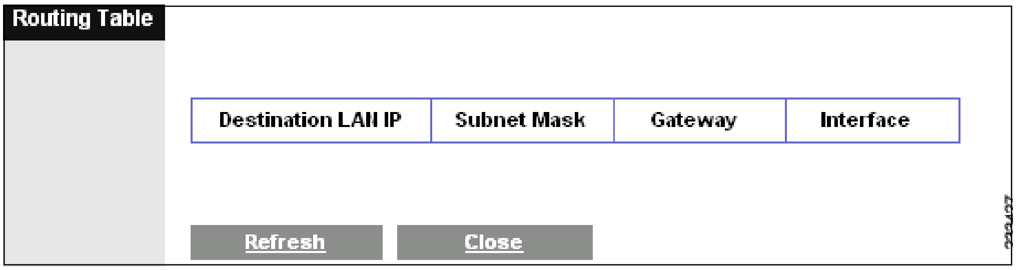
- **NAT:** If the WRP400 is hosting your network's connection to the Internet, keep the default, **Enabled.** If another router exists on your network, select **Disabled.** When the NAT setting is disabled, dynamic routing will be enabled.
- **Dynamic Routing (RIP):** This feature enables the WRP400 to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The WRP400 determines the route of the network packets based on the fewest number of hops between the source and the destination. When the NAT setting is enabled, the Dynamic Routing feature is automatically disabled. When the NAT setting is disabled, this feature is available. Select **Enabled** to use the Dynamic Routing feature.
- **Static Routing:** A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Enter the information described below to set up a new static route.
  - **Route Entries:** To set up a static route between the WRP400 and another network, select a number from the drop-down list. Click **Delete This Entry** to delete a static route.
  - **Enter Route Name:** Enter a name for the Route here, using a maximum of 25 alphanumeric characters.
  - **Destination LAN IP:** The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

- **Subnet Mask:** The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.
- **Gateway:** This is the IP address of the gateway device that allows for contact between the WRP400 and the remote network or host.
- **Interface:** This interface tells you whether the Destination LAN IP address is on the **LAN and Wireless** (Ethernet and wireless networks) or the **Internet (WAN)**.

- **Show Routing Table:** Click this button to view the static routes you have already set up.

  For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click **Refresh** to update the information. Click **Close** to exit this screen.

Figure 20 Routing Table



Routing Table

Destination LAN IP	Subnet Mask	Gateway	Interface

5

Installing and Configuring Your Mobile Network

You can connect a Mobile Broadband USB modem to the USB port of the WRP400 and configure the mobile network connection.

How Do I...

- **Connect a USB modem to my WRP400?**
  See **"Installing Your USB Modem," on page 42**
- **Enter the account information for my mobile network connection?**
  See **"Setup > Mobile Network," on page 43**
- **Ensure continued Internet access through the mobile network connection and the Ethernet connection?**
  See **"Setup > Connection Recovery," on page 46**
- **Know when the WRP400 is connected to the Internet through the mobile network?**
  See **"Understanding the LED Behavior for Mobile Network," on page 49**

Installing Your USB Modem

You can install a supported Mobile Broadband USB Modem into the USB port of the WRP400 for the purpose of accessing a mobile network.

NOTE For more information about supported USB devices, visit the WRP400 product page on Cisco.com: http://www.cisco.com/en/US/products/ps10028/index.html

Connect a supported USB Modem into the USB port of the WRP400. The Power LED flashes green and orange, indicating that a device is connected to the USB port and that initialization is in progress.

After the device initializes, the Power LED shines steady green. If the device fails to initialize, the LED continues to flash green and orange.

By default, the WRP400 connects to the Internet through the local Ethernet, if available. The mobile network connection is used as a failover when an Ethernet connection is unavailable.

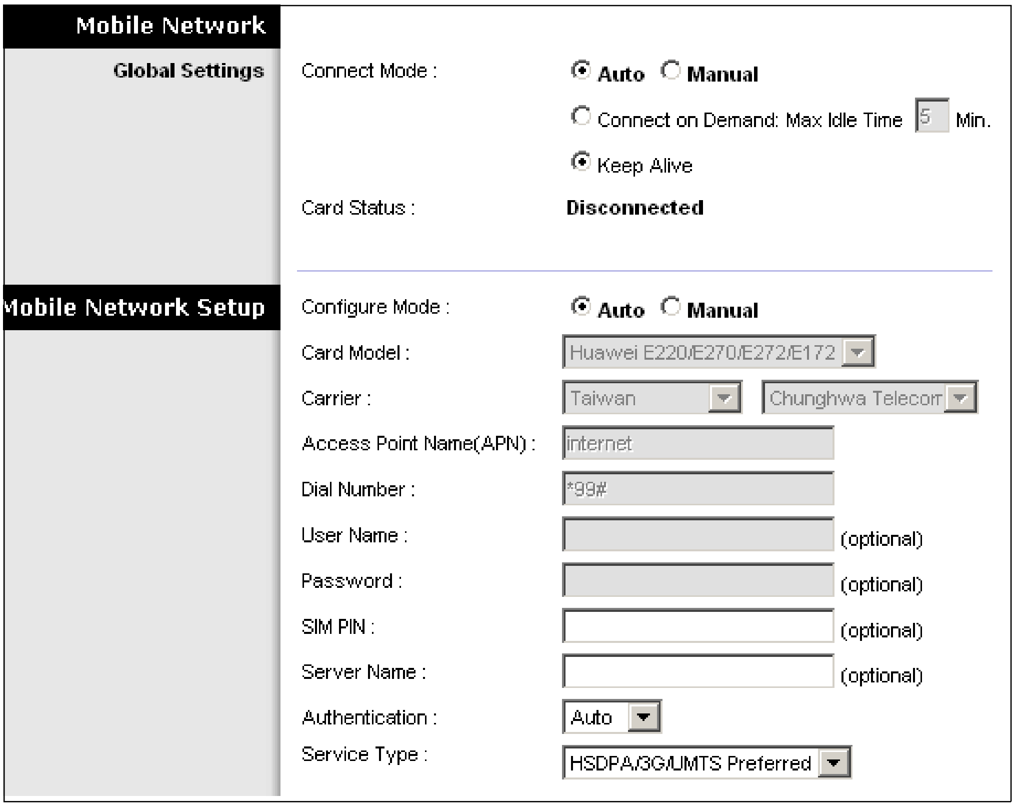
NOTE For more information about configuring your mobile network, see **"Setup > Mobile Network," on page 43**.

Setup > Mobile Network

You can use this page to choose the connect mode and to enter the settings for the mobile network. You also can use this page to view the current connection status.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 21 Setup > Mobile Network



Mobile Network

Global Settings

Connect Mode : ● **Auto** ○ **Manual**
○ Connect on Demand: Max Idle Time 5 Min.
● Keep Alive

Card Status : **Disconnected**

Mobile Network Setup

Configure Mode : ● **Auto** ○ **Manual**
Card Model : Huawei E220/E270/E272/E172
Carrier : Taiwan / Chunghwa Telecom
Access Point Name(APN) : internet
Dial Number : *99#
User Name : (optional)
Password : (optional)
SIM PIN : (optional)
Server Name : (optional)
Authentication : Auto
Service Type : HSDPA/3G/UMTS Preferred

NOTE Ethernet Connection Recovery and Interface Connection Failover will work only if the Connection Mode is set to Auto. For more information about these features, see **"Setup > Connection Recovery," on page 46**..

- **Connect Mode:**
  - Select **Auto** to enable your modem to establish connection automatically.
  - Select **Manual** to connect or disconnect your modem connection manually.
  - If you change your selection from Auto to Manual, a message appears. Click **OK** to acknowledge that Connection Recover will be disabled, or click **Cancel** to cancel.
  - If you change your selection from Manual to Auto, a message appears. Click **OK** to also enable Ethernet Connection Recovery, or click **Cancel** to set the Connect Mode to Auto without enabling Ethernet Connection.
- **Connect on Demand with Max. Idle Time:** You can configure the WRP400 to terminate the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the modem to automatically re-establish a terminated connection when a user attempts to access the Internet again. To enable this feature, select Connect on Demand. In the Max Idle Time field, enter the number of minutes that can elapse without activity before your Internet connection terminates. The default Max Idle Time is 5 minutes.
- **Keep Alive:** If you select this option, the WRP400 will periodically check your Internet connection. If you are disconnected, then the WRP400 will automatically re-establish your connection.
- **Card Status:** This field shows the current modem connection status as Detecting, Connecting, or Connected. If your Connect Mode is Manual, there will be a button for you to click to connect or disconnect your Modem.
- **Configure Mode:** Select Auto to allow the WRP400 to automatically detect which card model was inserted and which carrier is available. Select Manual to set up the connection manually. To allow the WRP400 to automatically configure modem & mobile network settings, keep the default, Auto.

NOTE Some Internet Service Providers (ISPs) will require that you enter specific information, such as User Name and Password. This information can be obtained from your ISP, if required.

- **Card Model:** The data card model that is inserted in the USB port.
- **Carrier:** The mobile network service provider for Internet connection. This setting is required when you are using HSDPA/UMTS/GPRS Internet service.
- **Country:** Select the card issue country from the first drop-down menu.
- **Carrier:** Select the card issue provider from the second drop-down menu.
- **Access Point Name (APN):** The Internet network to which the mobile device is connecting to. Enter the Access Point Name provided by your mobile network service provider.
- **Dial Number:** The dial number for the Internet connection. Enter the Dial Number provided by your mobile network service provider.
- **Optional Settings:** Some of these settings may be required by your mobile network service provider. Verify with your mobile network service provider before making any changes.
- **User Name and Password (Optional):** Enter the User Name provided by your mobile network service provider.
- **SIM PIN (Optional):** The PIN code associated with your SIM card. Enter your SIM PIN number here.
- **Server Name (Optional):** The name of the server for the Internet connection.
- **Authentication:** The type of authentication used by your service provider. Select your authentication type, if you do not know which type to use, keep the default setting, Auto.
- **Service Type:** Select the most commonly available type of mobile data service connection based on your area service signal. If your location supports only one mobile data service, you may set up for enhance build up connection. The first selection will always search for HSPDA/3G/UMTS service or switch to GPRS automatically only when it is available.

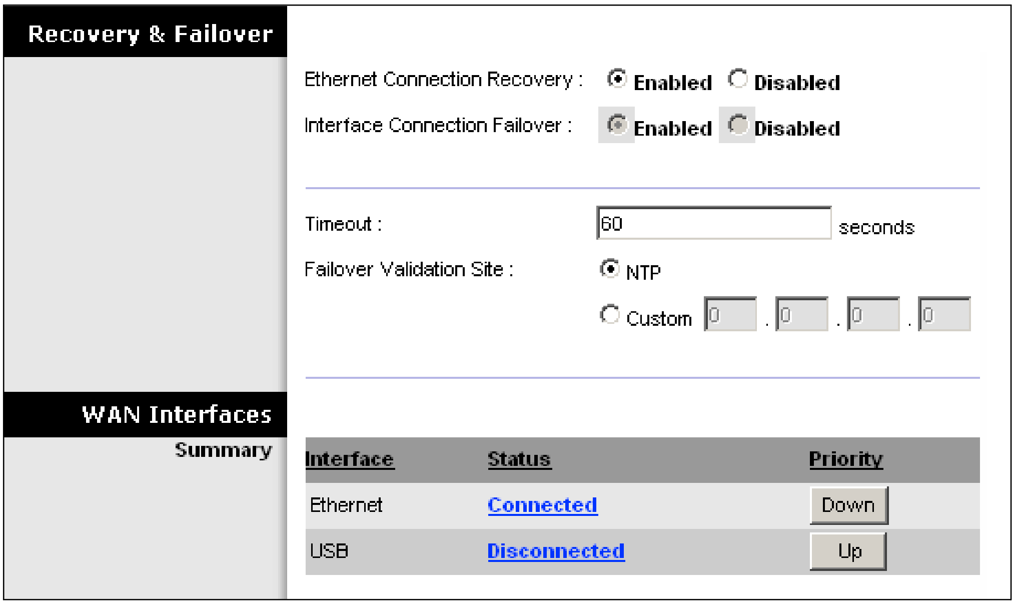
Setup > Connection Recovery

An Internet connection can be established via the Ethernet Internet port or a USB modem connected to the USB port. While both Ethernet and USB interfaces may be connected, only one of them can be used to establish a link at a time.

By default, the WRP400 uses the Ethernet Internet connection when available. If the Ethernet Internet connection fails, the WRP400 automatically attempts to bring up another connection on another interface. This feature is called failover. Whenever the Ethernet Internet connection recovers, the WRP400 automatically attempts to bring back and recover the Ethernet Internet connection. This feature is called Recovery.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 22 Setup > Connection Recovery



Recovery & Failover

Ethernet Connection Recovery : ● Enabled ○ Disabled

Interface Connection Failover : ● Enabled ○ Disabled

Timeout : 60 seconds

Failover Validation Site : ● NTP

○ Custom 0 . 0 . 0 . 0

WAN Interfaces

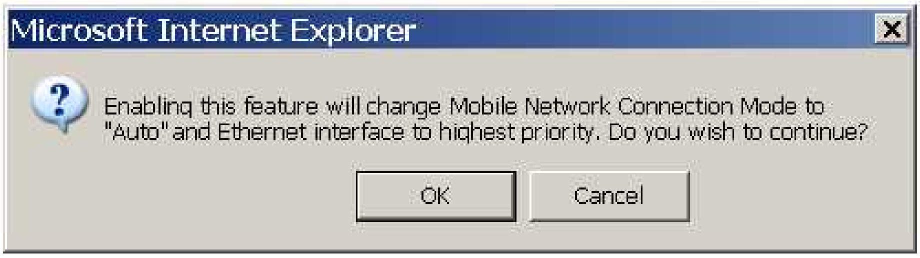
Summary

Interface	Status	Priority
Ethernet	Connected	Down
USB	Disconnected	Up

Recovery & Failover

- **Ethernet Connection Recovery:** This feature ensures that your Internet connection is made through the Ethernet interface if it is available. Enabling this feature also enables the Interface Connection Failover, which ensures that if the Internet connection fails on the Ethernet interface, the WRP400 automatically attempts to bring up the connection through the mobile network if available. Whenever the Ethernet Internet connection recovers, the WRP400 automatically attempts to bring back and recover the Ethernet Internet connection.

NOTE Ethernet Connection Recovery requires that your Mobile Connection Mode is set to Auto and your Ethernet interface is set to the high priority. When you enable this feature, a message appears. Click **OK** to confirm that you want to change the Mobile Connection Mode and the Ethernet interface priority.


Microsoft Internet Explorer

Enabling this feature will change Mobile Network Connection Mode to "Auto" and Ethernet interface to highest priority. Do you wish to continue?

- **Interface Connection Failover:** Failover detection works by detecting the physical connection and/or presence of traffic on the Internet link. If the link is idle for some time, the WRP400 will attempt to ping a destination. If the ping does not reply, the WRP400 assumes the link is down and attempts to fail over to another interface. Click Enabled if you want to use this feature, or otherwise click Disabled. This feature is automatically enabled if you enable Ethernet Connection Recovery.

- **Timeout:** Specify the time interval at which the WRP400 detects the status of the Internet connection. The default timeout interval is 60 seconds.

- **Failover Validation Site:** A ping target for the WRP400 to use to detect the status of the Internet connection. By default the WRP400 pings the Network Time Protocol (NTP) servers. You may specify a different IP address as a target here.

WAN Interfaces

The Summary table includes one row of information for the Ethernet interface and one row of information for the USB interface.

- **Status:** The link status of this interface:
  - **Disconnected:** The device is plugged in and available but not active.
  - **Connecting:** The WRP400 is attempting to bring up the link over the device.
  - **Connected:** The link is up and running on the device.
  - **Wait Recovery:** When the WRP400 is connected to the Ethernet, this status means that the Ethernet is waiting recovered to route to the Failover Validation Site.

NOTE You can click the **Status** hyperlink to view the Status page for the interface. To return to the Connection Recovery screen, click the **Back** button on the browser toolbar. For more information, see**"Router Information," on page 102** and **"Mobile Network Status," on page 104** .

- **Priority:** The priority setting determines which interface is used when both interfaces are available. By default, the Ethernet interface has top priority. However, you can change the priority setting by clicking **Up** to move an interface to the top priority level or by clicking **Down** to move an interface to the low priority level.

NOTE The interface priority setting is configurable only when Ethernet Connection Recovery is disabled.

Understanding the LED Behavior for Mobile Network

The Internet LED indicates connectivity to the Internet through the Ethernet connection only. The Power LED indicates the progress of USB initialization or the status of the mobile network connection.

LED Behavior During USB Modem Installation

The Power LED indicates the progress of the initialization.

- Before you connect the USB modem, the Power LED shines steady green to show that the WRP400 has power.
- After you connect the USB modem, the Power LED flashes green and orange to show that a device is connected to the USB port and that initialization is in progress.
- If the initialization is successful, the Power LED shines steady green. If the initialization fails, the LED continues to flash green and orange.

By default, the WRP400 connects to the Internet through the wired Ethernet, if available. The mobile network connection is used as a failover when an Ethernet connection is unavailable.

LED Behavior During Mobile Network Connectivity

After you successfully install a USB modem, the Power LED indicates the status of the mobile network connection:

- **Flashing Orange:** The WRP400 is attempting to connect to the Internet through the mobile network connection.
- **Steady Orange:** The WRP400 is connected to the Internet through the mobile network connection.
- **Continuous Flashing Orange:** The WRP400 failed to connect to the Internet through the mobile network connection and is trying again.
- **Steady Green:**
  - If a USB device is connected, this LED behavior indicates that the device was successfully initialized and that the WRP400 is not using the mobile network connection. If an Internet connection is active through the Ethernet, then the Internet LED is illuminated.

- If the USB device was removed, this LED behavior indicates that the WRP400 has power.

To check the status of the USB Modem, or modify the settings for the mobile network, connection recovery, and failover, you can use the administration web server.

6

Configuring Your Wireless Network

You can use the Wireless screens to set up and secure your wireless network.

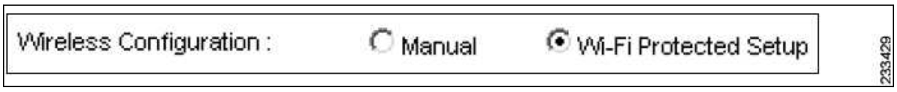
How Do I...

- **Set up my wireless network?**
  See **"Wireless > Basic Wireless Settings," on page 51**.
- **Secure my wireless network?**
  See **"Wireless > Wireless Security," on page 56**.
- **Specify computers that can or cannot access my network?**
  See **"Wireless > Wireless MAC Filter," on page 62**
- **Configure special router functions for my wireless network?**
  See **"Wireless > Advanced Wireless Settings," on page 64**.

Wireless > Basic Wireless Settings

You can use the Basic Wireless Settings page to configure your wireless network manually or to use Wi-Fi Protected Setup.

Figure 23 Wireless > Basic Wireless Settings > Wireless Configuration



Wireless Configuration : ○ Manual ● Wi-Fi Protected Setup

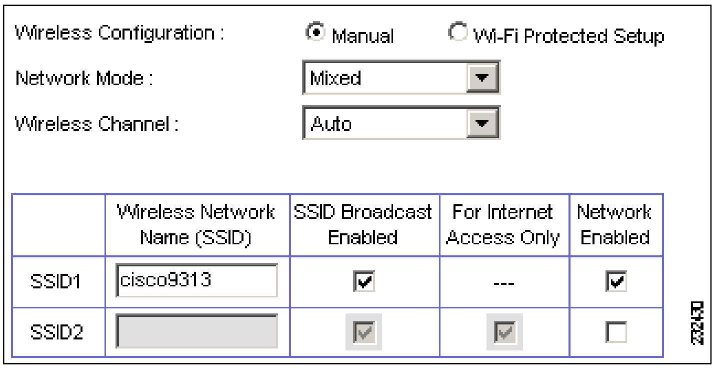
The options on the page change after you choose Manual or Wi-Fi Protected Setup.

- Choose **Manual** if you want to manually configure your network, if you are setting up your secondary network (SSID2), of if you do not have client devices that support Wi-Fi Protected Setup. See **"Manual Configuration of the Network," on page 52**.
- Choose **Wi-Fi Protected Setup** if you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup. For more information, see **"Wi-Fi Protected Setup," on page 54**.

Manual Configuration of the Network

After you choose Manual for the Wireless Configuration method, additional fields appear. You can change the SSID of the wireless network and enable a second network, or guest network.

Figure 24 Wireless > Basic Wireless Settings > Manual Configuration



Wireless Configuration : ● Manual ○ Wi-Fi Protected Setup

Network Mode : Mixed

Wireless Channel : Auto

	Wireless Network Name (SSID)	SSID Broadcast Enabled	For Internet Access Only	Network Enabled
SSID1	cisco9313	☑	---	☑
SSID2		☑	☑	□

- **Network Mode:** Select the wireless standards that are running on your network. If you have Wireless-G and Wireless-B devices, keep the default setting, **Mixed.** If you have only Wireless-G devices, select **Wireless-G only.** If you have only Wireless-B devices, select **Wireless-B only.**
- **Wireless Channel:** Select the channel that you want to use. To allow the WRP400 to select the best available wireless channel, keep the default, **Auto.**

- **SSID1**, **SSID2:** The SSID is the network name shared among all devices in a wireless network. The WRP400 can support up to two wireless networks. By default, one wireless network is enabled, and you can create a second wireless network.

  Configure the following settings for each wireless network:

  - **Wireless Network Name (SSID):** The default wireless network uses this name: “cisco” followed by the last four digits of the wireless MAC address of the WRP400. To rename the default wireless network, enter a unique Wireless Network Name, which is case-sensitive and must not exceed 32 characters. You can use any of the characters on the keyboard. To create a second wireless network, select **Network Enabled** for the SSID2 setting. Then enter a unique Wireless Network Name.

    NOTE If you are unable to configure the SSID2 settings, contact your service provider for more information.

  - **SSID Broadcast Enabled:** When wireless clients survey the local area for wireless networks, they detect the SSID broadcast by the WRP400. If you want to broadcast the SSID, keep the check box selected. If you do not want to broadcast the SSID, deselect the check box.

  - **For Internet Access Only:** On your second wireless network (SSID2), you can set up guest access, which allows access to the Internet while blocking access to your local network. For example, a guest cannot access the data stored on your local computers. To limit guests to Internet access only, keep the check box selected. To allow local network access, deselect the check box.

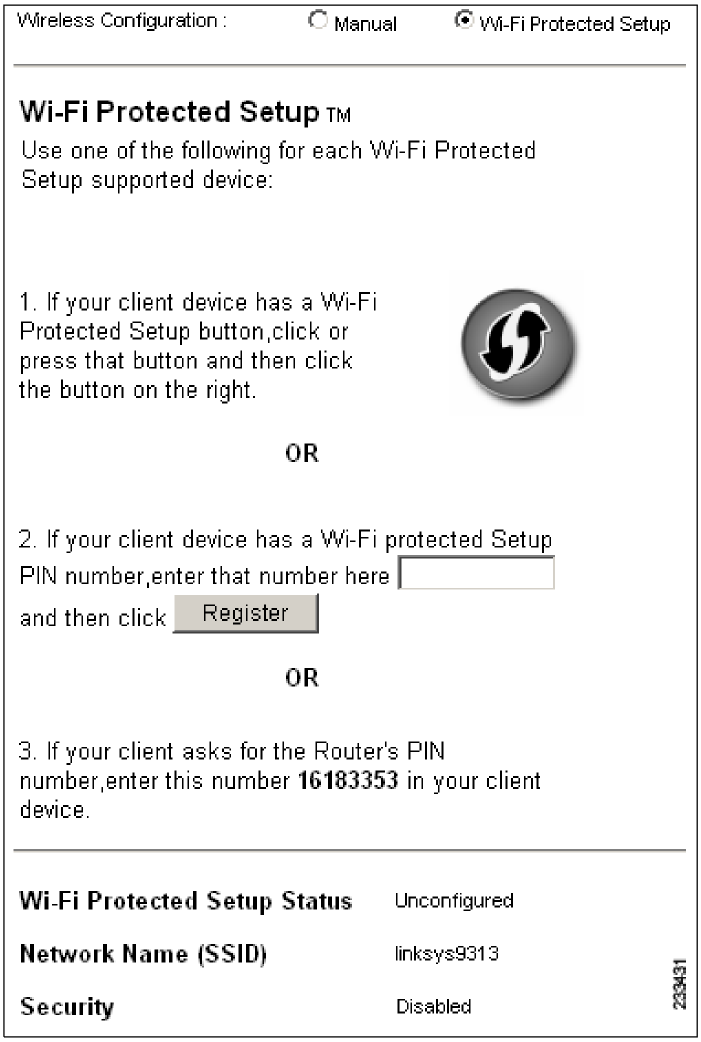
    NOTE The For Internet Access Only feature applies only to SSID2.

  - **Network Enabled:** To enable the wireless network, select the check box. To disable the wireless network, deselect the check box.

Wi-Fi Protected Setup

After you choose Wi-Fi Protected Setup for the Wireless Configuration, the instructions, fields, and buttons appear on the screen. Three setup methods are available.

NOTE Wi-Fi Protected Setup is available for your primary wireless network (SSID1) only. To configure your second wireless network (SSID2), select **Manual**. If you are unable to configure the second wireless network, contact your service provider for more information (these settings may be controlled by your service provider).



Wireless Configuration : ○ Manual ● Wi-Fi Protected Setup

Wi-Fi Protected Setup TM

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button,click or press that button and then click the button on the right.

OR

2. If your client device has a Wi-Fi protected Setup PIN number,enter that number here [ ] and then click [Register]

OR

3. If your client asks for the Router's PIN number,enter this number **16183353** in your client device.

Wi-Fi Protected Setup Status	Unconfigured
Network Name (SSID)	linksys9313
Security	Disabled

- **Method #1:** To configure a client device that has a Wi-Fi Protected Setup button, click or press the **Wi-Fi Protected Setup** button on the client device. Then click the button shown on the screen. After the client device has been configured, click **OK**. Then refer to your client device or its documentation for further instructions. Repeat for any additional devices that you need to configure.

- **Method #2:** To configure a client device that has a Wi-Fi Protected Setup PIN number, enter the PIN number in the field on this screen. Click **Register**. After the client device has been configured, click **OK**. Then refer to your client device or its documentation for further instructions. Repeat for any additional devices that you need to configure.

- **Method #3:** If your client device asks for the PIN number of the WRP400, enter the PIN number that is shown on the screen. This number also appears on the label on the bottom of the WRP400. After the client device has been configured, click **OK**. Then refer to your client device or its documentation for further instructions. Repeat for any additional devices that you need to configure.

Wireless > Wireless Security

You can use the Wireless Security page to configure the security of your wireless network(s). The WRP400 supports the following wireless security mode options: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, and WEP.

WEP (Wired Equivalent Privacy) is an older security standard. WPA (Wi-Fi Protected Access) is a newer security standard that is stronger than WEP encryption. A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

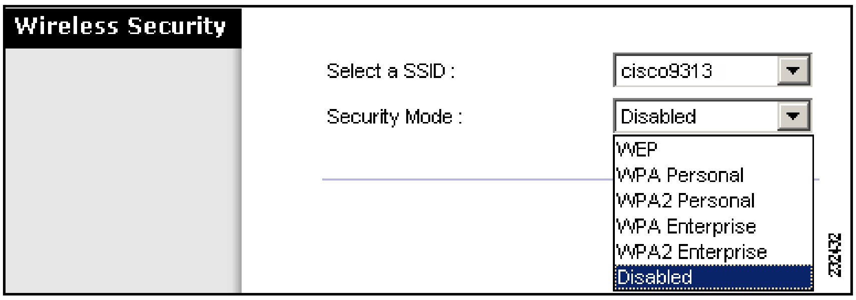
These options are briefly discussed here. For additional guidelines, refer to **Chapter 2, "Before You Begin: Understanding Wireless Security."**

NOTE If you used Wi-Fi Protected Setup to configure your wireless network(s), then wireless security has already been set up for your primary wireless network. Do not make changes to the Wireless Security screen for your primary wireless network.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Select the SSID that you want to configure. Then choose the Security Mode. If you do not want to use wireless security, keep the default, **Disabled**.

Figure 25 Wireless > Wireless Security



Wireless Security

Select a SSID : cisco9313

Security Mode : Disabled

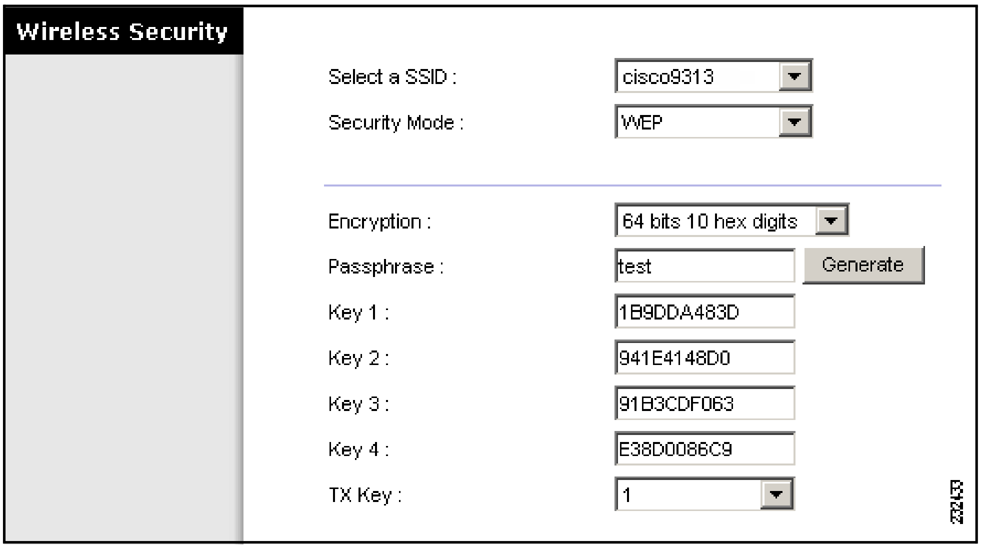
NOTE If you enabled the second wireless network on the Basic Wireless Settings screen, you will need to set up wireless security for each SSID.

Depending on the selected Security Mode, additional fields appear.

WEP

WEP is a basic encryption method, which is not as secure as WPA

Figure 26 Wireless Security > WEP



Wireless Security

Select a SSID : cisco9313

Security Mode : WEP

Encryption : 64 bits 10 hex digits

Passphrase : test

Key 1 : 1B9DDA483D

Key 2 : 941E4148D0

Key 3 : 91B3CDF063

Key 4 : E38D0086C9

TX Key : 1

- **Encryption:** Select a level of WEP encryption, **64 bits 10 hex digits** or **28 bits 26 hex digits.** The default is **64 bits 10 hex digits.**

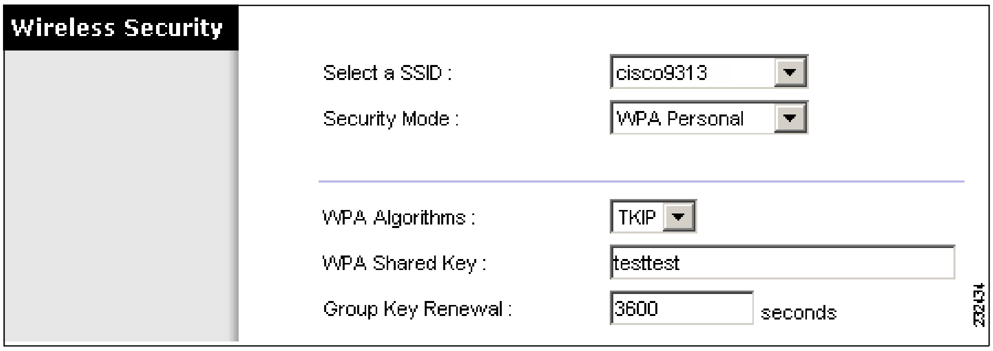
- **Passphrase:** Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.
- **Key 1-4:** If you did not enter a Passphrase, enter the WEP key(s) manually.
- **TX Key:** Select which TX (Transmit) Key to use. The default is **1**.

WPA Personal

Wi-Fi Protected Access (WPA) is a security mode that uses a shared key to restrict access to authorized users.

NOTE If you are using WPA, always remember that each device in your wireless network MUST use the same WPA method and shared key, or else the network will not function properly.

Figure 27 Wireless Security > WPA Personal



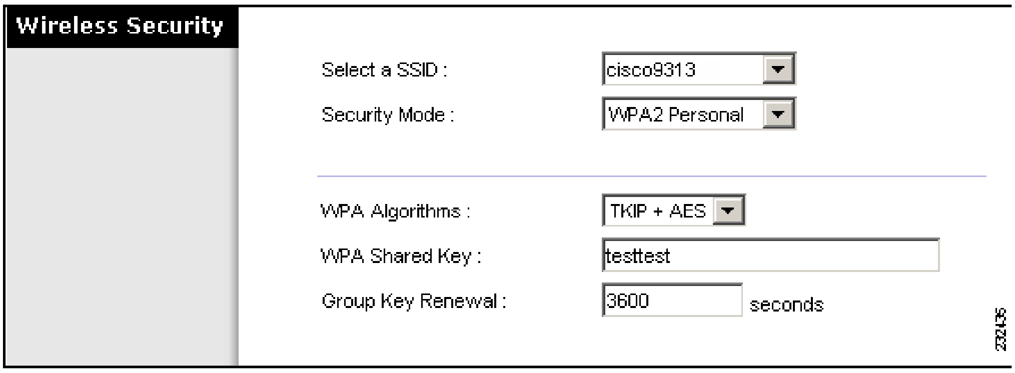
Select a SSID : cisco9313
Security Mode : WPA Personal
WPA Algorithms : TKIP
WPA Shared Key : testtest
Group Key Renewal : 3600 seconds

- **WPA Algorithms:** WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP**.
- **WPA Shared Key:** Enter a WPA Shared Key of 8-63 characters.
- **Group Key Renewal:** Enter a Group Key Renewal period, which instructs the WRP400 how often it should change the encryption keys. The default is **3600** seconds.

WPA2 Personal

Like WPA Personal, WPA2 Personal uses a shared key to restrict access to your wireless network. WPA2 can combine TKIP and AES encryption.

Figure 28 Wireless Security > WPA2 Personal



Wireless Security

Select a SSID : cisco9313

Security Mode : WPA2 Personal

WPA Algorithms : TKIP + AES

WPA Shared Key : testtest

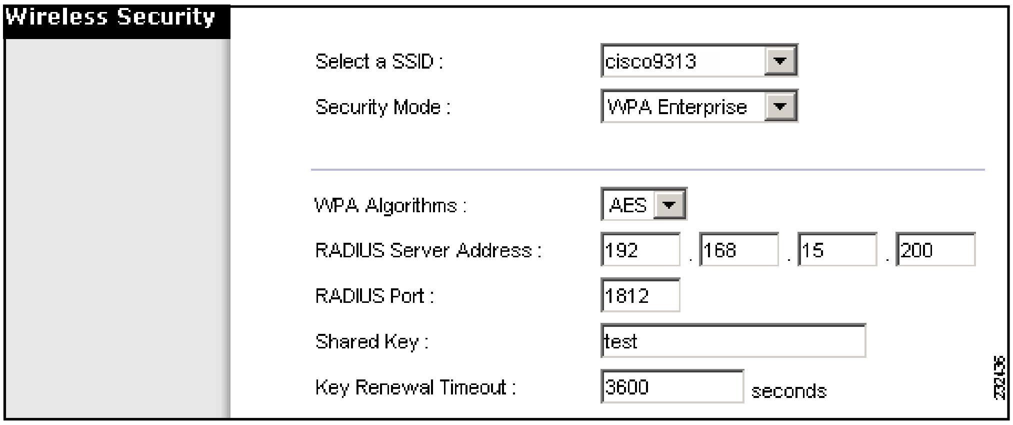
Group Key Renewal : 3600 seconds

- **WPA Algorithms:** WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or TKIP + AES. The default is TKIP + AES.
- **WPA Shared Key:** Enter a WPA Shared Key of 8-63 characters.
- **Group Key Renewal:** Enter a Group Key Renewal period, which instructs the WRP400 how often it should change the encryption keys. The default is 3600 seconds.

WPA Enterprise

This option features WPA used in coordination with a RADIUS (Remote Authentication Dial-In User Service) server. This option should only be used when a RADIUS server is connected to the WRP400.

Figure 29 Wireless Security > WPA Enterprise



Wireless Security

Select a SSID : cisco9313
Security Mode : WPA Enterprise

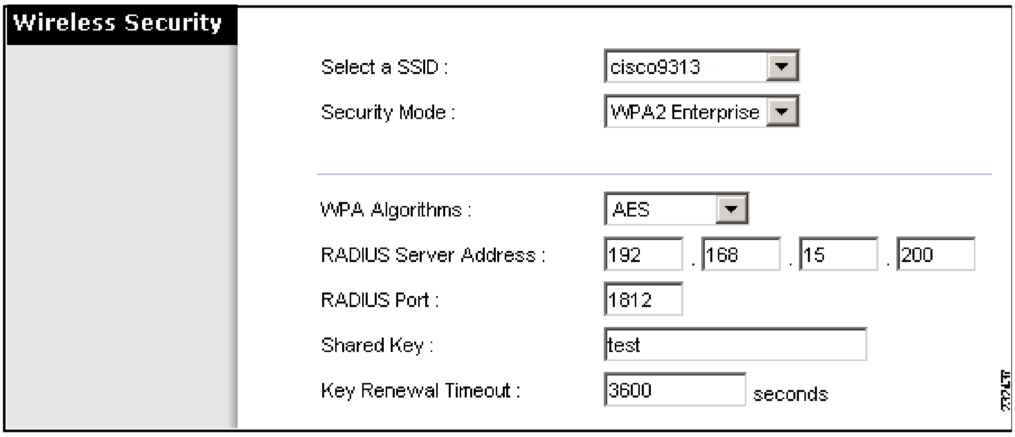
WPA Algorithms : AES
RADIUS Server Address : 192 . 168 . 15 . 200
RADIUS Port : 1812
Shared Key : test
Key Renewal Timeout : 3600 seconds

- **WPA Algorithms:** WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES.** The default is **TKIP.**
- **RADIUS Server Address:** Enter the IP address of the RADIUS server.
- **RADIUS Port:** Enter the port number of the RADIUS server. The default value is **1812.**
- **Shared Key:** Enter the key shared between the WRP400 and the server.
- **Key Renewal Timeout:** Enter a Key Renewal Timeout period, which instructs the WRP400 how often it should change the encryption keys. The default is **600** seconds.

WPA2 Enterprise

This option features WPA2 used in coordination with a RADIUS (Remote Authentication Dial-In User Service) server. This option should only be used when a RADIUS server is connected to the WRP400.

Figure 30 Wireless > Wireless Security > WPA2Enterprise



Wireless Security

Select a SSID : cisco9313
Security Mode : WPA2 Enterprise
WPA Algorithms : AES
RADIUS Server Address : 192 . 168 . 15 . 200
RADIUS Port : 1812
Shared Key : test
Key Renewal Timeout : 3600 seconds

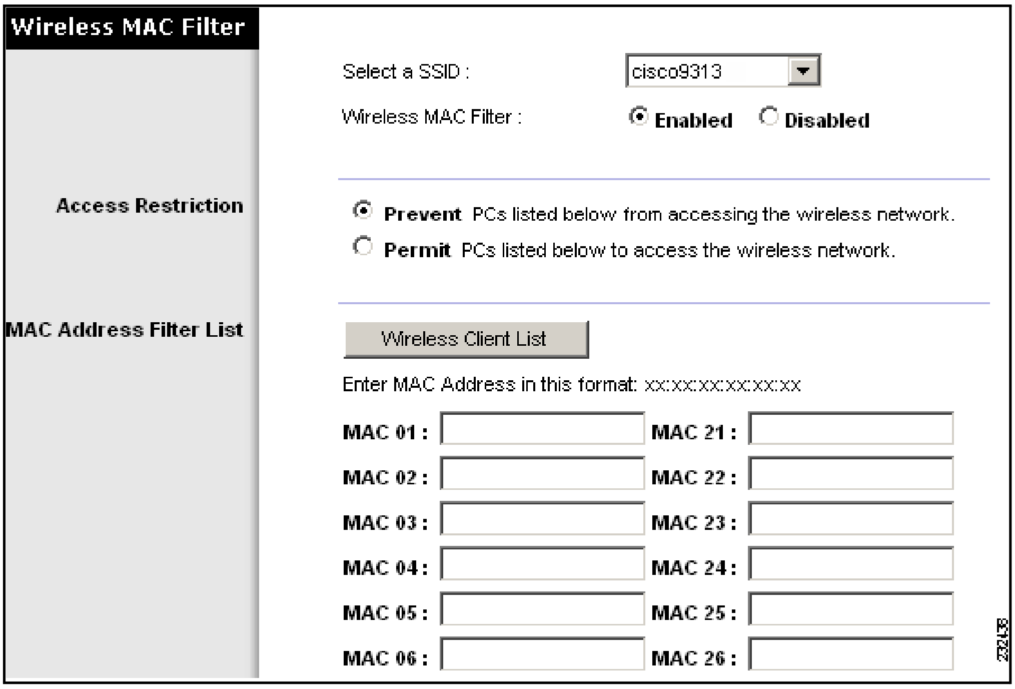
- **WPA Algorithms:** WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES** or **TKIP + AES**. The default is **TKIP + AES**.
- **RADIUS Server Address:** Enter the IP address of the RADIUS server.
- **RADIUS Port:** Enter the port number of the RADIUS server. The default value is **1812**.
- **Shared Key:** Enter the key shared between the WRP400 and the server.
- **Key Renewal Timeout:** Enter a Key Renewal Timeout period, which instructs the WRP400 how often it should change the encryption keys. The default is **600** seconds.

Wireless > Wireless MAC Filter

Wireless access can be filtered by using the MAC addresses of the wireless devices within your network's radius.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 31 Wireless > Wireless MAC Filter



Wireless MAC Filter

Select a SSID : cisco9313

Wireless MAC Filter : ● Enabled ○ Disabled

Access Restriction

● **Prevent** PCs listed below from accessing the wireless network.
○ **Permit** PCs listed below to access the wireless network.

MAC Address Filter List

Enter MAC Address in this format: xx:xx:xx:xx:xx:xx

MAC 01 :		MAC 21 :	
MAC 02 :		MAC 22 :	
MAC 03 :		MAC 23 :	
MAC 04 :		MAC 24 :	
MAC 05 :		MAC 25 :	
MAC 06 :		MAC 26 :	

- **Select a SSID:** Select the SSID that you want to configure.

NOTE If you enabled the second wireless network on the Basic Wireless Settings screen, then you can set up wireless MAC filtering for each SSID.

- **Wireless MAC Filter:** To filter wireless users by MAC address, select **Enabled** If you do not wish to filter users by MAC address, keep the default setting, **Disabled**.

Access Restriction

In this section, you choose how to use the MAC Address Filter List: to prevent access or to permit access.

- **Prevent:** Select this option to block wireless access to devices with the specified MAC addresses. This button is selected by default.
- **Permit:** Select this to allow wireless access by devices with the specified MAC addresses.

MAC Address Filter List

In this section, you identify the clients to filter. You can choose clients from the Wireless Client List, or you can enter the MAC addresses individually.

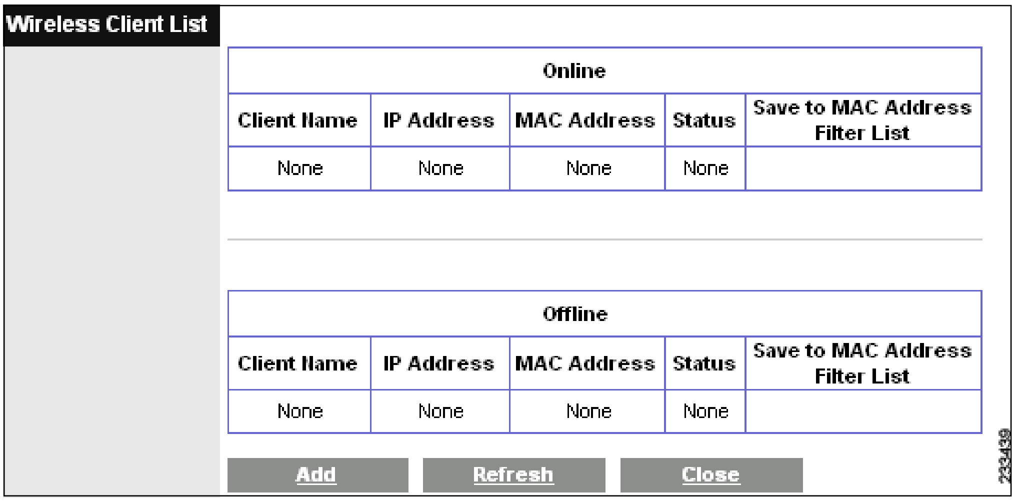
- **Wireless Client List:** Click this button if you want to choose the clients from the Wireless Client List screen. See **"Wireless Client List."** below.
- **MAC 01-40:** Enter the MAC addresses of the devices whose wireless access you want to block or allow.

Wireless Client List

Check the **Save to MAC Address Filter List** check box to select a device. Then click **Add** to add the device to the MAC Address Filter List.

To retrieve the most up-to-date information, click **Refresh**. To exit this screen and return to the Wireless MAC Filter screen, click **Close**.

Figure 32 Wireless Client List



Wireless Client List

Online				
Client Name	IP Address	MAC Address	Status	Save to MAC Address Filter List
None	None	None	None	

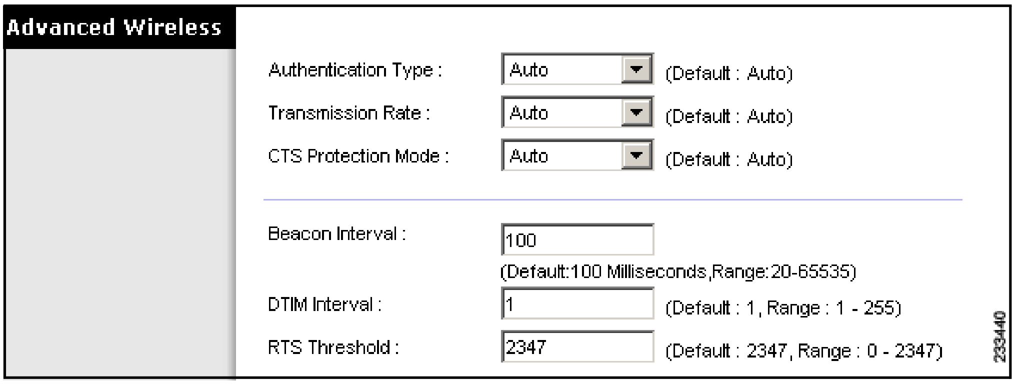
Offline				
Client Name	IP Address	MAC Address	Status	Save to MAC Address Filter List
None	None	None	None	

Wireless > Advanced Wireless Settings

The Advanced Wireless Settings screen is used to set up the advanced wireless functions of the WRP400. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 33 Wireless > Advanced Wireless Settings



Advanced Wireless

Authentication Type : Auto (Default : Auto)
Transmission Rate : Auto (Default : Auto)
CTS Protection Mode : Auto (Default : Auto)

Beacon Interval : 100
(Default:100 Milliseconds,Range:20-65535)
DTIM Interval : 1 (Default : 1, Range : 1 - 255)
RTS Threshold : 2347 (Default : 2347, Range : 0 - 2347)

- **Authentication Type:** The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. With Open System authentication, the sender and the recipient *do not* use a WEP key for authentication. With Shared Key authentication, the sender and recipient use a WEP key for authentication. Select **Shared Key** to only use Shared Key authentication.

- **Transmission Rate:** The rate of data transmission should be set depending on the speed of your wireless network(s). You can select from a range of transmission speeds, or you can select **Auto** to have the WRP400 automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the WRP400 and a wireless client. The default is **Auto**.

- **CTS Protection Mode:** The WRP400 will automatically use CTS (Clear-To-Send) Protection Mode when your Wireless-G products are experiencing severe problems and are not able to transmit to the WRP400 in an environment with heavy 802.11b traffic. This function boosts the ability of the WRP400 to catch all Wireless-G transmissions but will severely decrease performance. The default is **Auto**.

- **Beacon Interval:** Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the WRP400 to synchronize the wireless network(s). The default value is **100**.

- **DTIM Interval:** This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the WRP400 has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

- **RTS Threshold:** If you encounter inconsistent data flow, only minor reduction of the default value, **2347**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The WRP400 sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2347**.

7

Configuring Network Security and Controlling Internet Access

You can use the Security screens to enable a firewall, add filters, or allow VPN tunnels. You can use the Access Restrictions screen to control Internet usage.

How Do I...

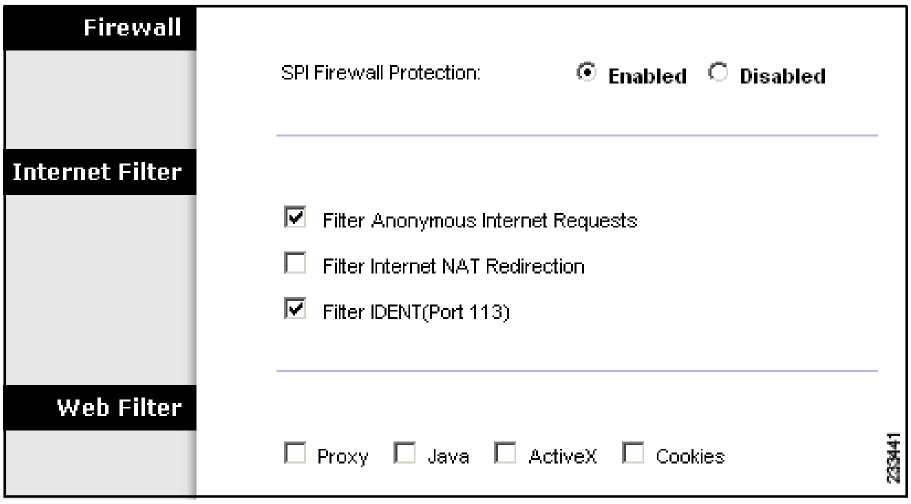
- **Enable a firewall, Internet filters, or Web filters?**
  See "Security > Firewall," on page 66
- **Allow VPN tunnels to pass through the firewall?**
  See "Security > VPN Passthrough," on page 68
- **Block or allow specific types of Internet usage and traffic?**
  See "Access Restrictions > Internet Access," on page 69.

Security > Firewall

The Firewall screen is used to configure a firewall that can filter out various types of unwanted traffic on the local network.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 34 Security > Firewall



Firewall

SPI Firewall Protection: ● Enabled ○ Disabled

Internet Filter

☑ Filter Anonymous Internet Requests

□ Filter Internet NAT Redirection

☑ Filter IDENT(Port 113)

Web Filter

□ Proxy □ Java □ ActiveX □ Cookies

Firewall

- **SPI Firewall Protection:** To use firewall protection, keep the default, **Enabled.** To turn off firewall protection, select **Disabled.**

Internet Filter

- **Filter Anonymous Internet Requests:** This feature makes it more difficult for outside users to work their way into your network. This feature is selected by default. Deselect the feature to allow anonymous Internet requests.
- **Filter Internet NAT Redirection:** This feature uses port forwarding to block access to local servers from local networked computers. Select this feature to filter Internet NAT redirection. It is not selected by default.
- **Filter IDENT (Port 113):** This feature keeps port 113 from being scanned by devices outside of your local network. This feature is selected by default. Deselect this feature to disable it.

Web Filter

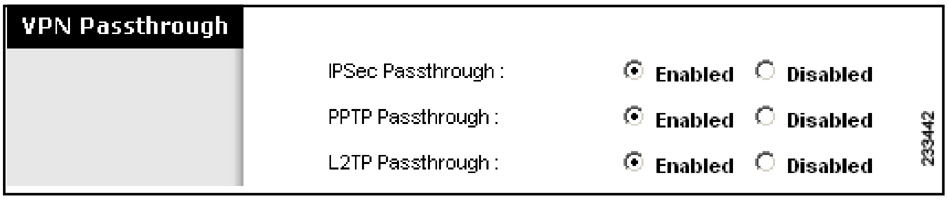
- **Proxy:** Use of WAN proxy servers may compromise the security of the WRP400. Denying Proxy will disable access to any WAN proxy servers. Select this feature to enable proxy filtering. Deselect the feature to allow proxy access.
- **Java:** Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. Select this feature to enable Java filtering. Deselect the feature to allow Java usage.
- **ActiveX:** ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. Select this feature to enable ActiveX filtering. Deselect the feature to allow ActiveX usage.
- **Cookies:** A cookie is data stored on your computer and used by Internet sites when you interact with them. Select this feature to filter cookies. Deselect the feature to allow cookie usage.

Security > VPN Passthrough

The VPN Passthrough screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the firewall of the WRP400.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 35 Security > VPN Passthrough


VPN Passthrough

IPSec Passthrough : ● Enabled ○ Disabled
PPTP Passthrough : ● Enabled ○ Disabled
L2TP Passthrough : ● Enabled ○ Disabled

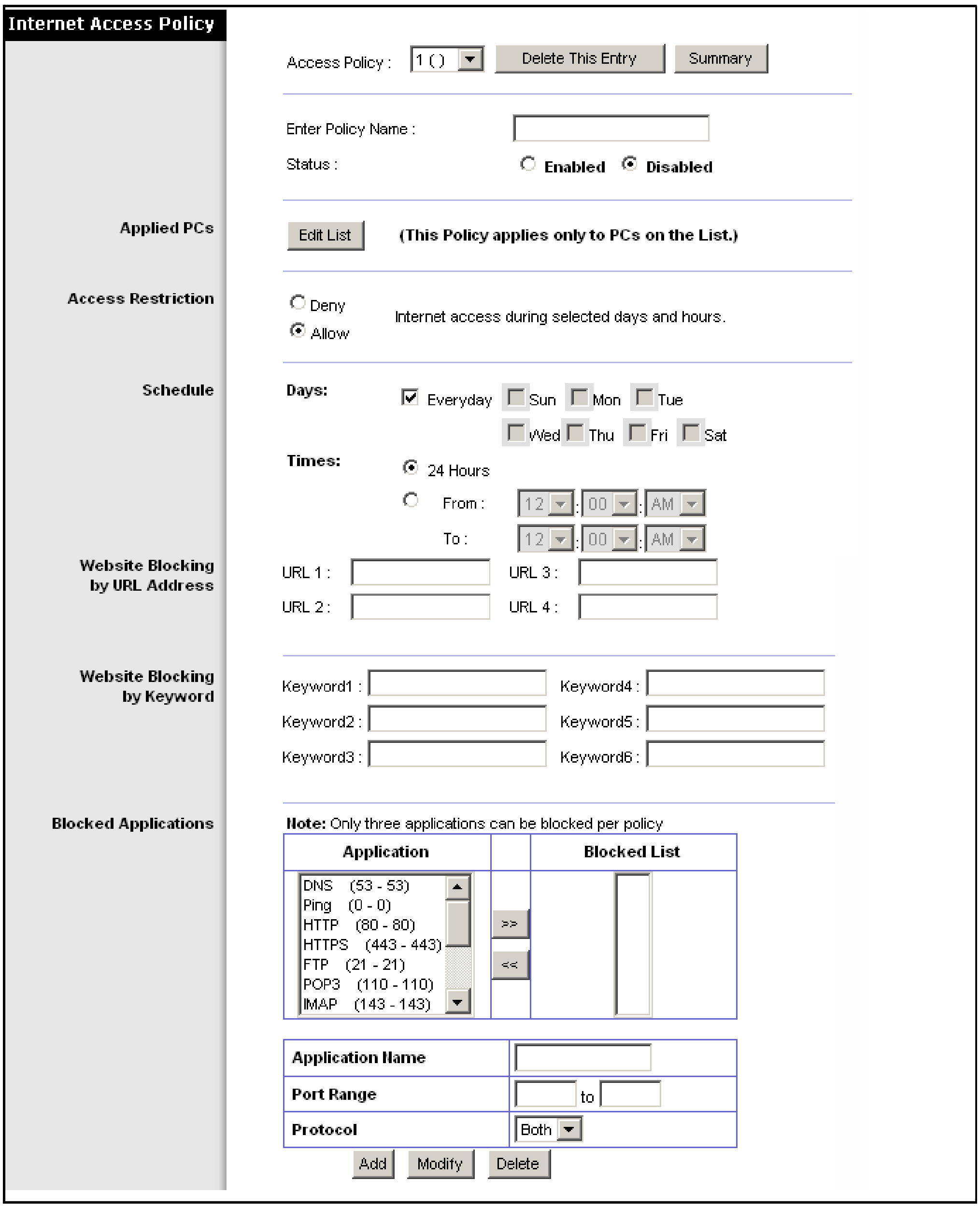
- **IPSec Passthrough:** Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the WRP400, keep the default, **Enabled.**
- **PPTP:** Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the WRP400, keep the default, **Enabled.**
- **L2TP Passthrough:** Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the WRP400, keep the default, **Enabled.**

Access Restrictions > Internet Access

You can use the Internet Access Policy screen to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites during specific days and times.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 36 Access Restrictions > Internet Access



Internet Access Policy

Access Policy : 1 () ▾ [Delete This Entry] [Summary]

Enter Policy Name :

Status : ○ Enabled ● Disabled

Applied PCs [Edit List] **(This Policy applies only to PCs on the List.)**

Access Restriction ○ Deny ● Allow Internet access during selected days and hours.

Schedule

Days: ☑ Everyday □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Times: ● 24 Hours
○ From : 12 ▾ : 00 ▾ : AM ▾
To : 12 ▾ : 00 ▾ : AM ▾

Website Blocking by URL Address
URL 1 : URL 3 :
URL 2 : URL 4 :

Website Blocking by Keyword
Keyword1 : Keyword4 :
Keyword2 : Keyword5 :
Keyword3 : Keyword6 :

Blocked Applications

Note: Only three applications can be blocked per policy

Application		**Blocked List**
DNS (53 - 53) Ping (0 - 0) HTTP (80 - 80) HTTPS (443 - 443) FTP (21 - 21) POP3 (110 - 110) IMAP (143 - 143)	>> <<	

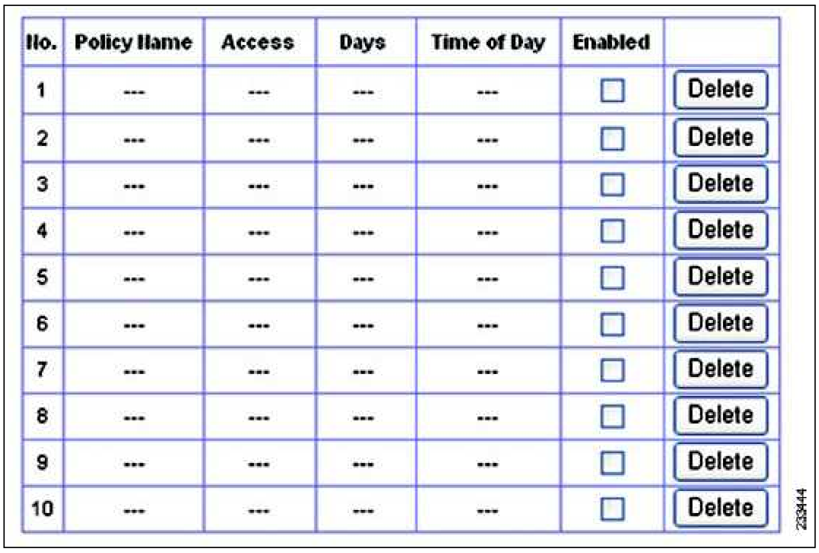
Application Name	
Port Range	to
Protocol	Both ▾

[Add] [Modify] [Delete]

- **Access Policy:** Select a policy from the drop-down list to display that policy's settings. You can then enter or modify the settings. Be sure to save your changes before selecting another policy from the drop-down list.

- **Delete This Entry:** To delete an access policy, select the policy's number from the Access Policy list, and then click this button.

- **Summary:** To view all policies, click this button. The Summary appears in a separate window. The policies are listed with the following information: No. (number), Policy Name, Access, Days, Time of Day, and status (Enabled). To enable a policy, check **Enabled.** To delete a policy, click **Delete.** Click **Save Settings** to save your changes, or click **Cancel Changes** to cancel your changes. To return to the Internet Access Policy screen, click **Close.**

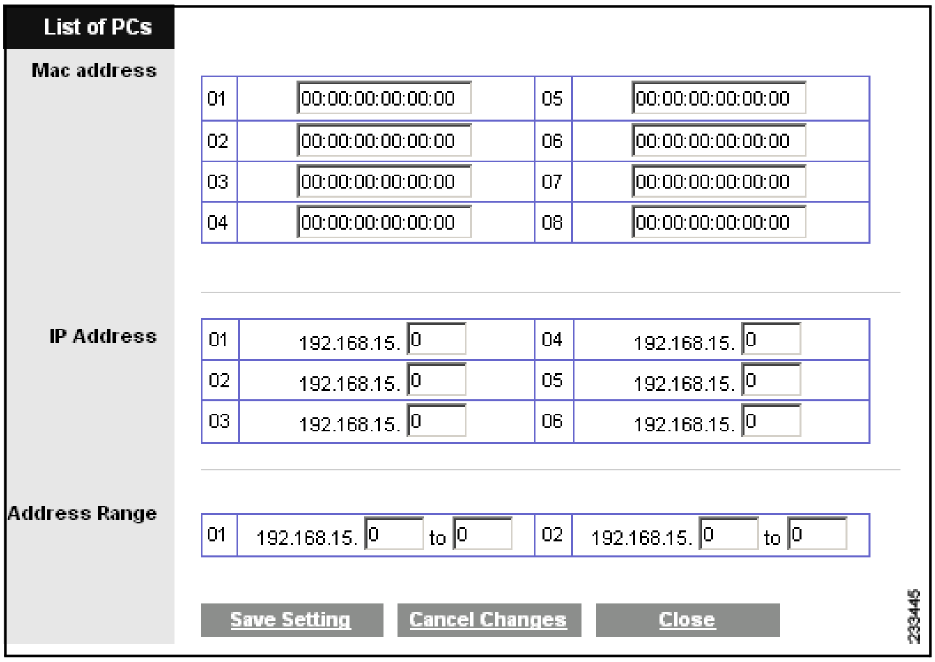


No.	Policy Name	Access	Days	Time of Day	Enabled	
1	---	---	---	---	□	Delete
2	---	---	---	---	□	Delete
3	---	---	---	---	□	Delete
4	---	---	---	---	□	Delete
5	---	---	---	---	□	Delete
6	---	---	---	---	□	Delete
7	---	---	---	---	□	Delete
8	---	---	---	---	□	Delete
9	---	---	---	---	□	Delete
10	---	---	---	---	□	Delete

- **Enter Policy Name:** Enter a name for the policy that you selected in the Access Policy list.

- **Status:** Policies are disabled by default. To enable the selected policy, select **Enabled.**

- **Applied PCs:** Click **Edit List** to select the computers that will be affected by the policy that you selected in the Access Policy list. The List of PCs window appears.



List of PCs

Mac address

01	00:00:00:00:00:00	05	00:00:00:00:00:00
02	00:00:00:00:00:00	06	00:00:00:00:00:00
03	00:00:00:00:00:00	07	00:00:00:00:00:00
04	00:00:00:00:00:00	08	00:00:00:00:00:00

IP Address

01	192.168.15. 0	04	192.168.15. 0
02	192.168.15. 0	05	192.168.15. 0
03	192.168.15. 0	06	192.168.15. 0

Address Range

01	192.168.15. 0 to 0	02	192.168.15. 0 to 0

Choose the PCs that will be affected by this policy:

- **MAC Address:** Enter a MAC address that you want to add to the list.
- **IP Address:** Enter the final octet of an IP address that you want to add to the list.
- **IP Address Range:** Enter the final octet of an IP address in the first box, and then enter the final octet of another IP address in the second box, to create a range of IP addresses to add to the list.

Click **Save Settings** to save your changes, or click **Cancel Changes** to cancel your changes. To return to the Internet Access Policy screen, click **Close**.

- **Access Restriction:** Select the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the computers that are listed on the List of PCs screen.

- **Schedule:** Decide which days and what times you want the selected policy to be enforced. Select the individual days during which the policy will be in effect, or select Everyday. Then enter a range of hours and minutes during which the policy will be in effect, or select 24 Hours.
- **Website Blocking by URL Address:** You can block websites with specific URL addresses. Enter each URL in a separate URL field.
- **Website Blocking by Keyword:** You can block websites using specific keywords. Enter each keyword in a separate Keyword field.
- **Blocked Applications:** You can filter access to various services accessed over the Internet, such as FTP or telnet. You can block up to three applications per policy.
  - From the Application list, select the application you want to block. Then click the **>>** button to move it to the Blocked List. To remove an application from the Blocked List, select it and click the **<<** button.
  - If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the Application Name field. Enter its range in the Port Range fields. Select its protocol from the Protocol drop-down menu. Then click **Add**.
  - To modify a service, select it from the Application list. Change its name, port range, and/or protocol setting. Then click **Modify**.
  - To delete a service, select it from the Application list. Then click **Delete**.

Creating or Modifying an Internet Access Policy

Follow this procedure to create or modify an Internet Access Policy.

STEP 1 Select a number from the **Access Policy** drop-down menu.

STEP 2 Enter a name in the **Policy Name** field.

STEP 3 To enable this policy, select **Enabled**.

STEP 4 Click **Edit List** to select the computers that will be affected by this policy.

a. In the List of PCs window, enter individual MAC addresses or IP addresses, or enter IP address ranges.

b. Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Then click **Close** close the window.

STEP 5 In the **Access Restriction** section, choose to **Deny** Internet access or to **Allow** Internet access for the computers that you listed on the List of PCs screen.

STEP 6 In the **Schedule** section, select the days and times when this policy applies, as described above.

STEP 7 In the remaining sections of the page, enter the URLs, keywords, and applications that you want to block with this policy, as described above.

STEP 8 Click **Save Settings** to save the settings. To cancel the settings, click **Cancel Changes.**

STEP 9 Repeat these steps to create additional policies, one at a time.

8

Configuring Applications and Gaming

You can use the Applications and Gaming screens to configure your WRP400 to support applications, services, and gaming.

How Do I...

- **Customize port services for common applications?**
  See **"Applications and Gaming > Single Port Forwarding," on page 76**.
- **Support public services such as web servers, FTP servers, e-mail servers, and Internet gaming?**
  See **"Applications and Gaming > Port Range Forward," on page 77**.
- **Specify the ports that are opened for specific applications?**
  See **"Applications & Gaming > Port Range Triggering," on page 79**.
- **Specify one computer to be exposed to the Internet for public services?**
  See **"Applications and Gaming > DMZ," on page 80**
- **Prioritize service for real-time applications such as video-conferencing?**
  See **"Applications and Gaming > QoS," on page 81**.

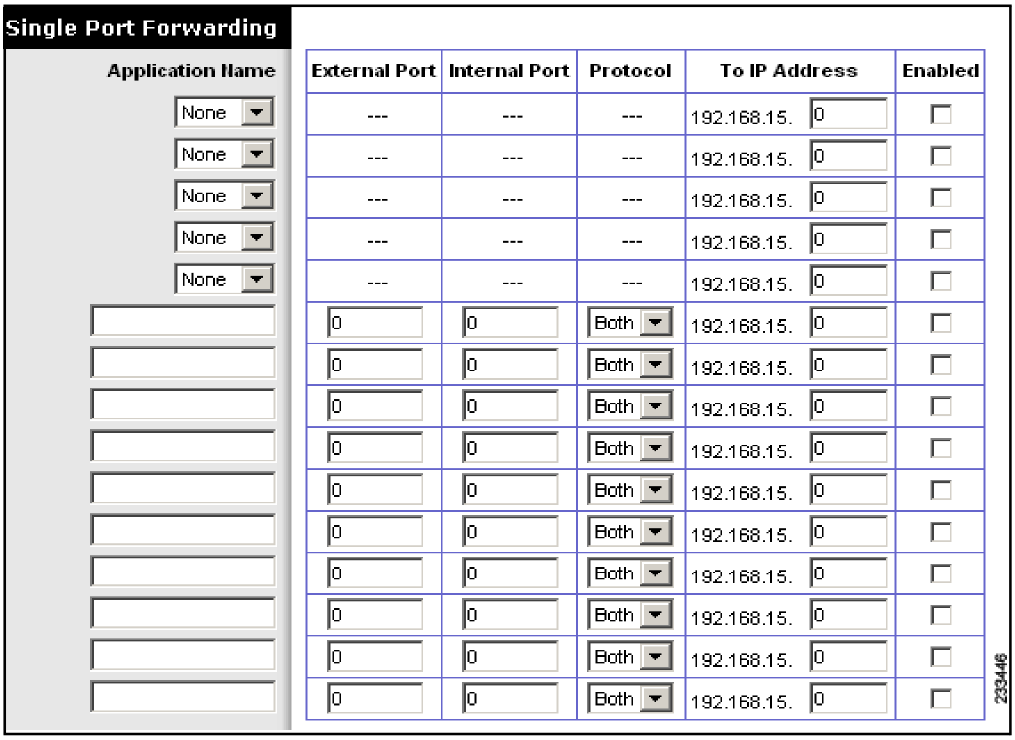
Applications and Gaming > Single Port Forwarding

The Single Port Forwarding screen allows you to customize port services for common applications on this screen.

When users send these types of requests to your network via the Internet, the WRP400 will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the Basic Setup screen). See **"DHCP Reservation," on page 32**.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 37 Applications and Gaming > Single Port Forwarding



Single Port Forwarding

Application Name	External Port	Internal Port	Protocol	To IP Address	Enabled
None	---	---	---	192.168.15. 0	□
None	---	---	---	192.168.15. 0	□
None	---	---	---	192.168.15. 0	□
None	---	---	---	192.168.15. 0	□
None	---	---	---	192.168.15. 0	□
	0	0	Both	192.168.15. 0	□
	0	0	Both	192.168.15. 0	□
	0	0	Both	192.168.15. 0	□
	0	0	Both	192.168.15. 0	□
	0	0	Both	192.168.15. 0	□
	0	0	Both	192.168.15. 0	□
	0	0	Both	192.168.15. 0	□
	0	0	Both	192.168.15. 0	□
	0	0	Both	192.168.15. 0	□
	0	0	Both	192.168.15. 0	□

Common applications are available for the first five entries. Select the appropriate application. Then enter the IP address of the server that should receive these requests. Select **Enabled** to activate this entry.

For additional applications, complete the following fields:

- **Application Name:** Enter the name you wish to give the application. Each name can be up to 12 characters.
- **External Port:** Enter the external port number used by the server or Internet application. Check with the Internet application documentation for more information.
- **Internal Port:** Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information.
- **Protocol:** Select the protocol used for this application, either TCP, UDP, or oth.
- **To IP Address:** For each application, enter the IP address of the PC that should receive the requests. If you assigned a static IP address to the PC, then you can click DHCP Reservation on the Basic Setup screen to look up its static IP address.
- **Enabled:** For each application, select Enabled to enable port forwarding.

Applications and Gaming > Port Range Forward

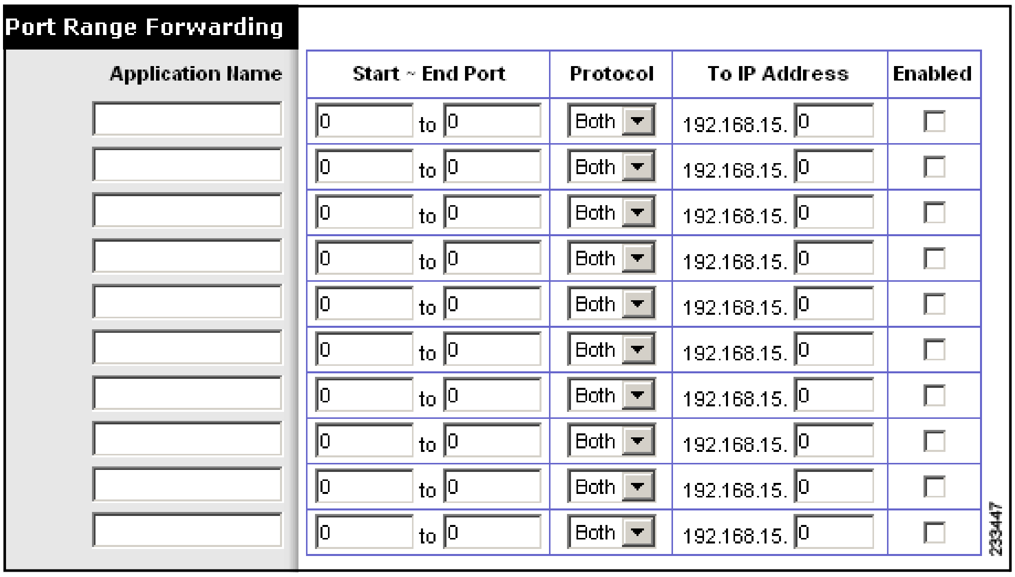
The Port Range Forward screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send these types of requests to your network via the Internet, the WRP400 will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the Basic Setup screen).

If you need to forward all ports to one computer, click the DMZ tab.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 38 Applications and Gaming > Port Range Forwarding



Port Range Forwarding

Application Name	Start ~ End Port	Protocol	To IP Address	Enabled
	0 to 0	Both ▼	192.168.15. 0	□
	0 to 0	Both ▼	192.168.15. 0	□
	0 to 0	Both ▼	192.168.15. 0	□
	0 to 0	Both ▼	192.168.15. 0	□
	0 to 0	Both ▼	192.168.15. 0	□
	0 to 0	Both ▼	192.168.15. 0	□
	0 to 0	Both ▼	192.168.15. 0	□
	0 to 0	Both ▼	192.168.15. 0	□
	0 to 0	Both ▼	192.168.15. 0	□
	0 to 0	Both ▼	192.168.15. 0	□

To forward a port, enter the information on each line for the criteria required.

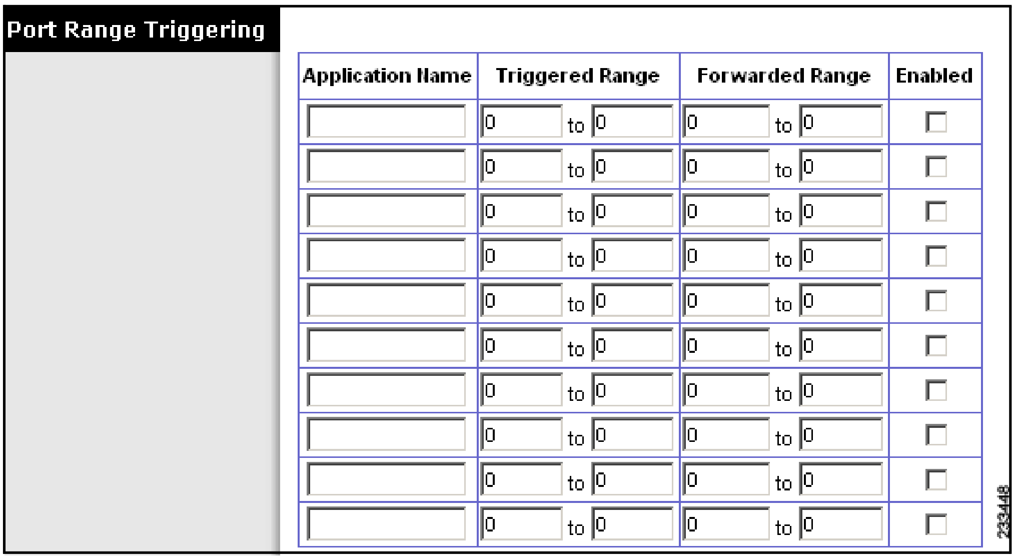
- **Application Name:** In this field, enter the name you wish to give the application. Each name can be up to 12 characters.
- **Start~End Port:** Enter the number or range of port(s) used by the server or Internet applications. Check with the Internet application documentation for more information.
- **Protocol:** Select the protocol used for this application, either TCP, UDP, or oth.
- **To IP Address:** For each application, enter the IP address of the PC running the specific application. If you assigned a static IP address to the PC, then you can click the **DHCP Reservation** button on the Basic Setup screen to look up its static IP address. See **"Setup > Basic Setup," on page 23**.
- **Enabled:** Select **Enabled** to enable port forwarding for the applications you have defined.

Applications & Gaming > Port Range Triggering

The Port Range Triggering screen allows the WRP400 to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the WRP400, so that when the requested data returns through the WRP400, the data is pulled back to the proper computer by way of IP address and port mapping rules.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 39 Applications and Gaming > Port Range Triggering



Port Range Triggering

Application Name	Triggered Range	Forwarded Range	Enabled
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□
	0 to 0	0 to 0	□

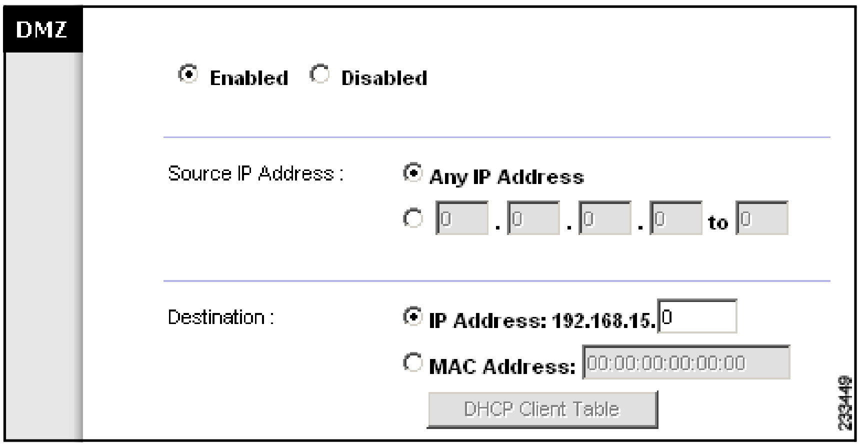
- **Application Name:** Enter the application name of the trigger.
- **Triggered Range:** For each application, enter the starting and ending port numbers of the triggered port number range. Check with the Internet application documentation for the port number(s) needed.
- **Forwarded Range:** For each application, enter the starting and ending port numbers of the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.
- **Enabled:** Select **Enabled** to enable port triggering for the applications you have defined.

Applications and Gaming > DMZ

The DMZ feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 40 Applications and Gaming > DMZ



DMZ

● Enabled ○ Disabled

Source IP Address : ● Any IP Address
○ 0 . 0 . 0 . 0 to 0

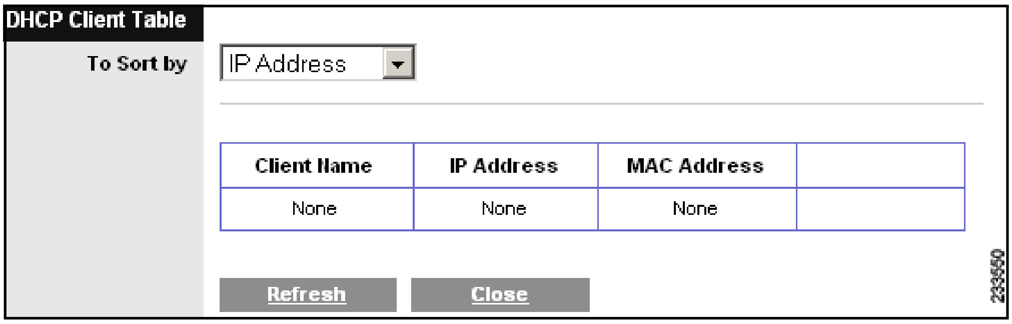
Destination : ● IP Address: 192.168.15.0
○ MAC Address: 00:00:00:00:00:00

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

- **Enabled/Disabled:** To disable DMZ hosting, select **Disabled.** To expose one PC, select **Enabled.** Then configure the following settings:
- **Source IP Address:** If you want any IP address to be the source, select **Any IP Address.** If you want to specify an IP address or range of IP addresses as the designated source, select and complete the IP address range fields.

- **Destination:** If you want to specify the DMZ host by IP address, select **IP Address** and enter the IP address in the field provided. If you want to specify the DMZ host by MAC address, select **MAC Address** and enter the MAC address in the field provided.
- **DHCP Client Table:** Click this button to view a list of DHCP clients. See **"DHCP Client Table."** This button becomes available when you select the MAC Address option.

DHCP Client Table



To Sort by: IP Address

Client Name	IP Address	MAC Address	
None	None	None	

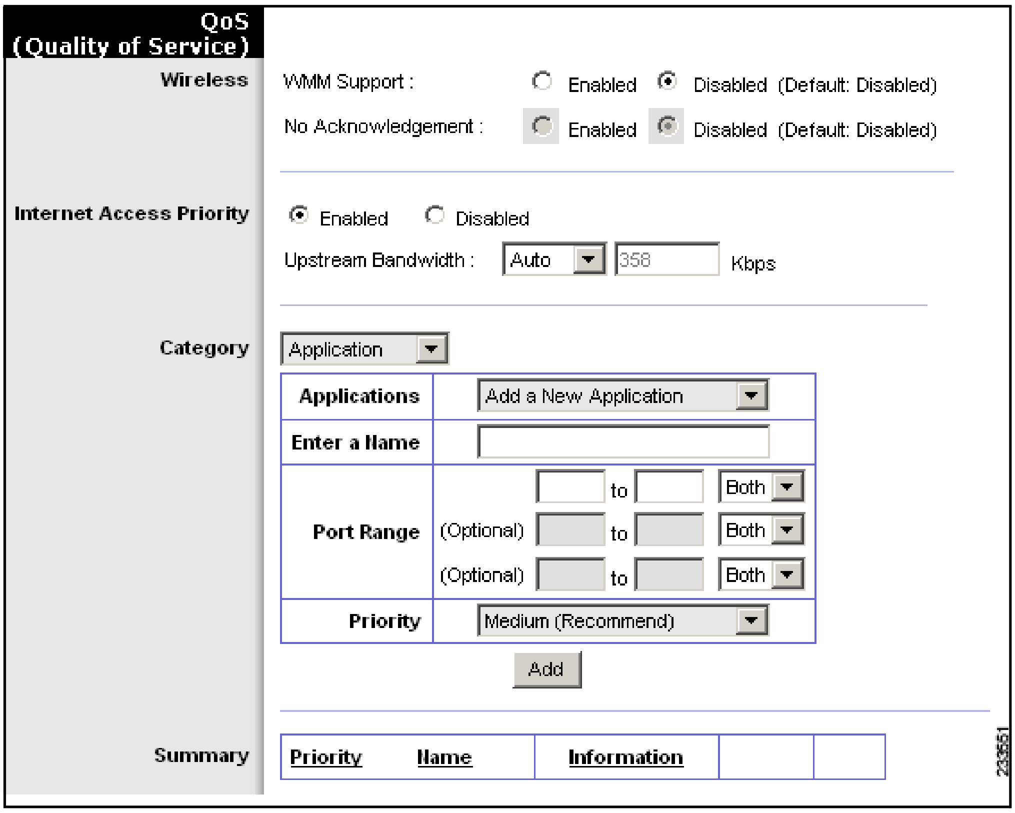
The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the WRP400. The list can be sorted by Client Name, IP Address, and MAC Address. To select a DHCP client, click **Select**. To retrieve the most up-to-date information, click **Refresh**. To exit this screen and return to the DMZ screen, click **Close**.

Applications and Gaming > QoS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.

NOTE Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 41 Applications and Gaming > QoS



QoS (Quality of Service)

Wireless

WMM Support : ○ Enabled ● Disabled (Default: Disabled)

No Acknowledgement : ○ Enabled ● Disabled (Default: Disabled)

Internet Access Priority

● Enabled ○ Disabled

Upstream Bandwidth : Auto ▾ 358 Kbps

Category

Application ▾

Applications	Add a New Application ▾				
Enter a Name					
Port Range			to		Both ▾
	(Optional)		to		Both ▾
	(Optional)		to		Both ▾
Priority	Medium (Recommend) ▾				

Add

Summary

Priority	Name	Information		

Wireless

- **WMM Support:** If you have other devices that support Wi-Fi Multimedia (WMM) on your network, select **Enabled.** Otherwise, keep the default, **Disabled.**
- **No Acknowledgement:** To prevent the WRP400 from resending data if an error occurs, select **Enabled.** Otherwise, keep the default, **Disabled.**

Internet Access Priority

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels priority: High, Medium, Normal, or Low. When you set priority, do not set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select Low. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority.

- **Enabled/Disabled:** To use the QoS policies you have set, keep the default, **Enabled**. Otherwise, select **Disabled.**
- **Upstream Bandwidth:** To allow the WRP400 to control the maximum bandwidth for upstream data transmissions, keep the default, **Auto**. To manually set the maximum, select **Manual**, and enter the appropriate number in the field provided.

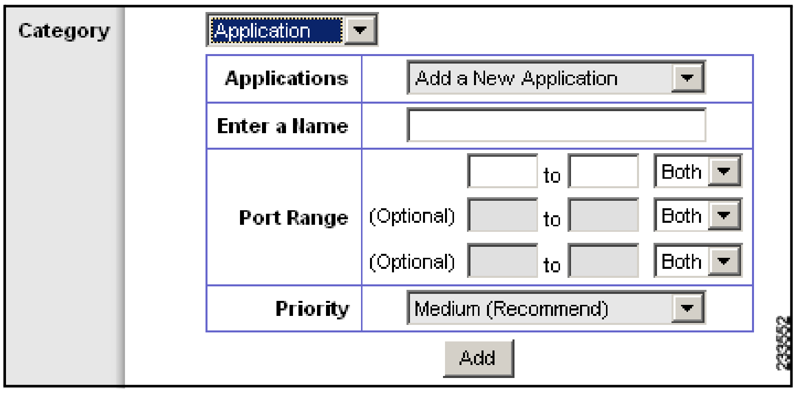
Category

There are four categories available. Select one of the following: Application, Online Games, MAC Address, or Ethernet Port. Proceed to the instructions for your selection.

Application

- **Application:** Select the appropriate application. If you select Add a New Application, follow the instructions for adding a new application.
- **Priority:** Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low.**

Adding a New Application



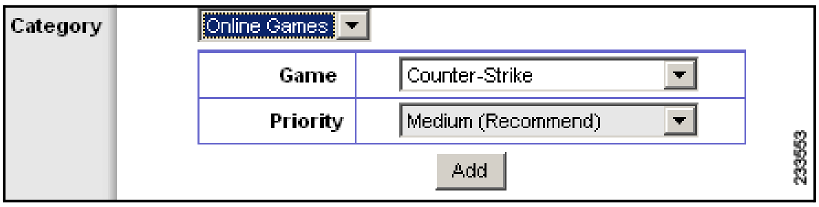
Category: Application

Applications	Add a New Application				
Enter a Name					
Port Range			to		Both
	(Optional)		to		Both
	(Optional)		to		Both
Priority	Medium (Recommend)				

- **Enter a Name:** Enter any name to indicate the name of the entry.
- **Port Range:** Enter the port range in the text boxes, and choose a protocol: **TCP**, **UDP**, or **Both**. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.
- **Priority:** Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low**.
- Click **Add** to save your changes. Your new entry will appear in the Summary list.

Online Games

You can add an Online Game to the Summary list or change the Priority setting for an existing game.



Category: Online Games

Game: Counter-Strike

Priority: Medium (Recommend)

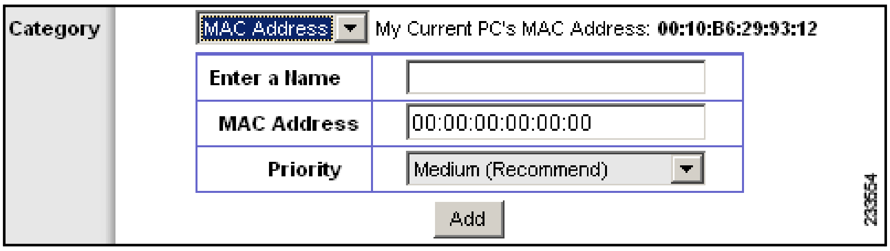
- **Game:** Select the appropriate game. If you select Add a New Game, follow the instructions for adding a new game.
- **Priority:** Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low**.

Adding a New Game

- **Enter a Name:** Enter any name to indicate the name of the entry.
- **Port Range:** Enter the port range in the text boxes, and choose a protocol: **TCP**, **UDP**, or **Both**. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.
- **Priority:** Select the appropriate priority: High, Medium (Recommend), Normal, or Low.

- Click **Add** to save your changes. Your new entry will appear in the Summary list.

MAC Address

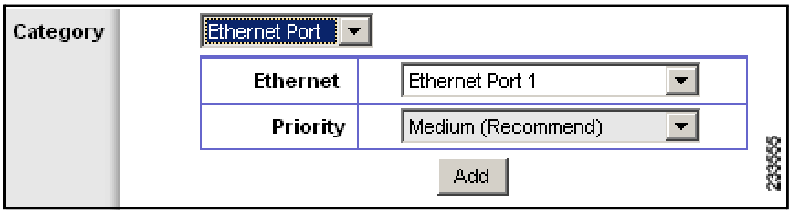


Category: MAC Address ▼ My Current PC's MAC Address: **00:10:B6:29:93:12**

Enter a Name	
MAC Address	00:00:00:00:00:00
Priority	Medium (Recommend) ▼

- **Enter a Name:** Enter a name for the device.
- **MAC Address:** Enter the MAC address of the device.
- **Priority:** Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low.**
- **Add:** Click this button to add your new entry to the Summary list.

Ethernet Port



Category: Ethernet Port ▼

Ethernet	Ethernet Port 1 ▼
Priority	Medium (Recommend) ▼

- **Ethernet:** Select the appropriate Ethernet port.
- **Priority:** Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low.**
- **Add:** Click this button to add your new entry to the Summary list.

Summary

The Summary table lists the QoS entries that you have created for your applications and devices.

- **Priority:** This column displays the bandwidth priority of High, Medium, Normal, or Low.
- **Name:** This column displays the application, device, or port name.
- **Information:** This column displays the port range or MAC address entered for your entry. If a pre-configured application or game was selected, there will be no valid entry shown in this section.
- **Remove:** Click this button to remove an entry.
- **Edit:** Click this button if you want to change the information. The information will appear in the Category section of the page for editing.

9

Administration

You can use the Administration screens to manage access, configure Universal Plug and Play, support multimedia streaming, enable logging and diagnostics, restore factory default settings, upgrade firmware, and back up and restore configurations.

How Do I...

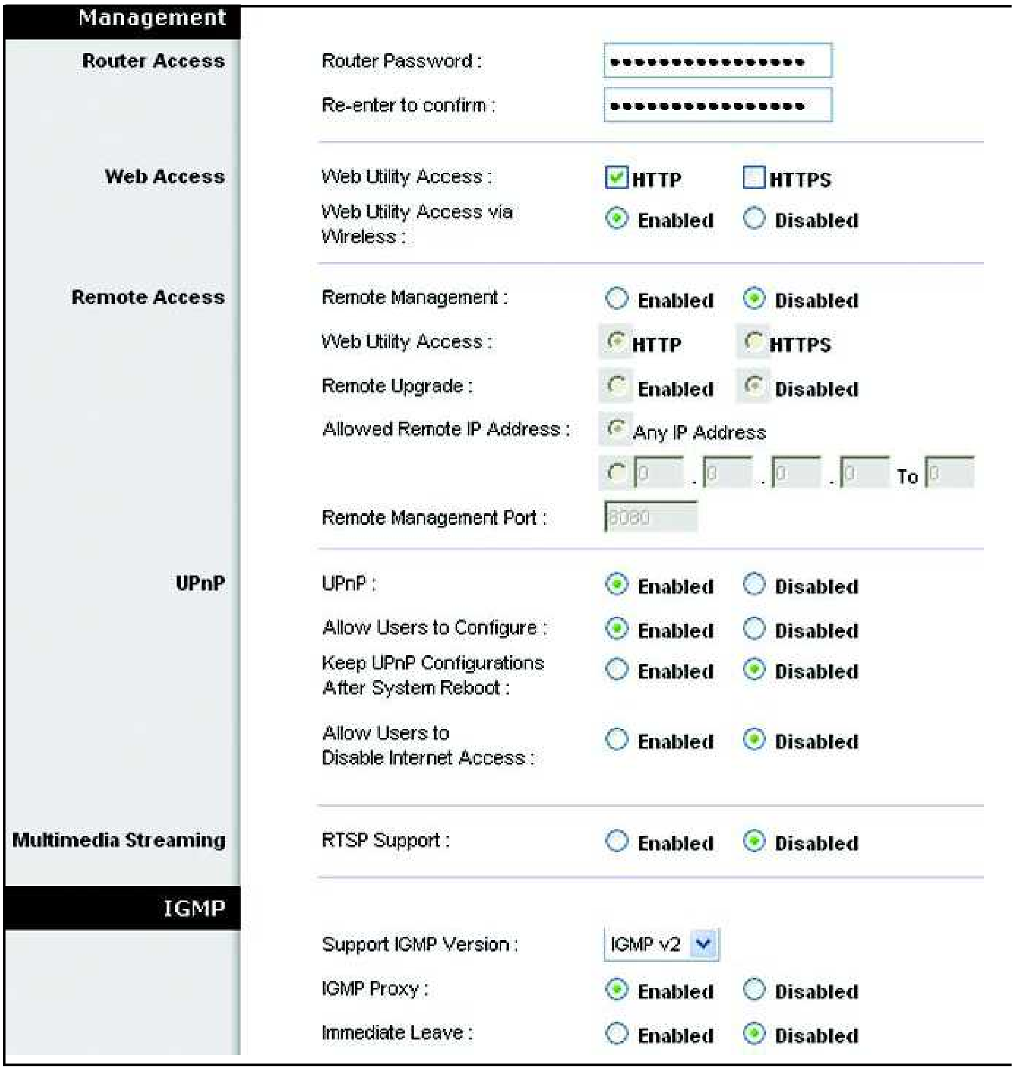
- **Change the admin password?**
  See **"Administration > Management," on page 88**.
- **Enable remote management of my network?**
  See **"Administration > Management," on page 88**.
- **Configure UPnP (Universal Plug and Play)?**
  See **"Administration > Management," on page 88**.
- **Enable support for multimedia streaming?**
  See **"Administration > Management," on page 88**.
- **Enable and view logs?**
  "Administration > Log," on page 91
- **Enable and view diagnostics?**
  "Administration > Diagnostics," on page 93
- **Restore factory default settings?**
  "Administration > Factory Defaults," on page 96
- **Upgrade the firmware?**
  See **"Administration > Firmware Upgrade," on page 97**.
- **Back up and restore settings?**
  See **"Administration > Config Management," on page 99**.
- **Reboot the device?**
  See **"Administration > Reboot," on page 100**.

Administration > Management

You can use the Administration > Management screen to change the password, to manage access, to enable remote management, to configure UPnP (Universal Plug and Play), and to enable support for multimedia streaming.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 42 Administration > Management



Management

Router Access	Router Password :	●●●●●●●●●●●●●●●●	
	Re-enter to confirm :	●●●●●●●●●●●●●●●●	
Web Access	Web Utility Access :	☑ HTTP	☐ HTTPS
	Web Utility Access via Wireless :	● Enabled	○ Disabled
Remote Access	Remote Management :	○ Enabled	● Disabled
	Web Utility Access :	● HTTP	○ HTTPS
	Remote Upgrade :	○ Enabled	● Disabled
	Allowed Remote IP Address :	● Any IP Address	
		○ 0 . 0 . 0 . 0 To 0	
	Remote Management Port :	8080	
UPnP	UPnP :	● Enabled	○ Disabled
	Allow Users to Configure :	● Enabled	○ Disabled
	Keep UPnP Configurations After System Reboot :	○ Enabled	● Disabled
	Allow Users to Disable Internet Access :	○ Enabled	● Disabled
Multimedia Streaming	RTSP Support :	○ Enabled	● Disabled

IGMP

	Support IGMP Version :	IGMP v2	
	IGMP Proxy :	● Enabled	○ Disabled
	Immediate Leave :	○ Enabled	● Disabled

Management

Router Access

Use this section of the page to enter a password to prevent unauthorized access to the web-based utility, you will be asked for your password when you access the web-based utility of the WRP400. The default is **admin**.

- **Router Password:** Enter a new password for the WRP400.
- **Re-enter to Confirm:** Enter the password again to confirm.

Web Access

- **Web Utility Access:** HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select **HTTP** or **HTTPS**. **HTTP** is the default.
- **Web Utility Access via Wireless:** If you are using the WRP400 in a public domain where you are giving wireless access to your guests, you can disable wireless access to the web-based utility of the WRP400. You will only be able to access the utility via a wired connection if you disable the setting. Keep the default, **Enabled**, to allow wireless access to the utility, or select **Disabled** to block wireless access to the utility.

Remote Access

- **Remote Management:** To permit remote access of the WRP400, from outside the local network, select **Enabled**. Otherwise, keep the default, **Disabled**.
- **Web Utility Access:** HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select **HTTP** or **HTTPS**. **HTTP** is the default.
- **Remote Upgrade:** If you want to be able to upgrade the WRP400 remotely, from outside the local network, select **Enabled**. (You must have the Remote Management feature enabled as well.) Otherwise, keep the default, **Disabled**.
- **Allowed Remote IP Address:** If you want to be able to access the WRP400 from any external IP address, select **ny IP Address**. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided.

- **Remote Management Port:** Enter the port number that will be open to outside access.

NOTE When you are in a remote location and wish to manage the WRP400, you can use HTTP or HTTPS to connect to the IP address of the WRP400, at the remote management port number, as shown:
http://<*Internet_IP_address*>**:***port* or **https://**<*Internet_IP_address*>**:***port*

- <*Internet_IP_address*>: The Internet IP address of the WRP400
- *port*: The Remote Management Port number

UPnP

Universal Plug and Play (UPnP) allows Windows XP and Vista to automatically configure the WRP400 for various Internet applications, such as gaming and videoconferencing.

- **UPnP:** If you want to use UPnP, keep the default, **Enabled.** Otherwise, select **Disabled.**
- **Allow Users to Configure:** Keep the default, **Enabled**, if you want to be able to make manual changes to the WRP400 while using the UPnP feature. Otherwise, select **Disabled.**
- **Keep UPnP Configurations After System Reboot:** If you enable the Allow Users to Configure option, then this option will be available. Select **Enabled**, if you want to keep UPnP configuration settings after the WRP400 reboots. Otherwise, keep the default, **Disabled.**
- **Allow Users to Disable Internet Access:** Select **Enabled**, if you want to be able to prohibit any and all Internet connections. Otherwise, keep the default, **Disabled.**

Multimedia Streaming

- **RTSP Support:** If you experience issues with video-on-demand applications, select **Enabled** to improve multimedia transmissions. Using this option, the WRP400 will establish channels with the Real Time Streaming Protocol) RTSP server, which is located at the service provider. Otherwise, keep the default, **Disabled.**

IGMP

Internet Group Multicast Protocol (IGMP) is used to establish membership in a multicast group and is commonly used for multicast streaming applications. For example, you may have Internet Protocol Television (IPTV) with multiple setup boxes on the same local network. These setup boxes have different video streams running simultaneously, so you should use the IGMP feature of the WRP400.

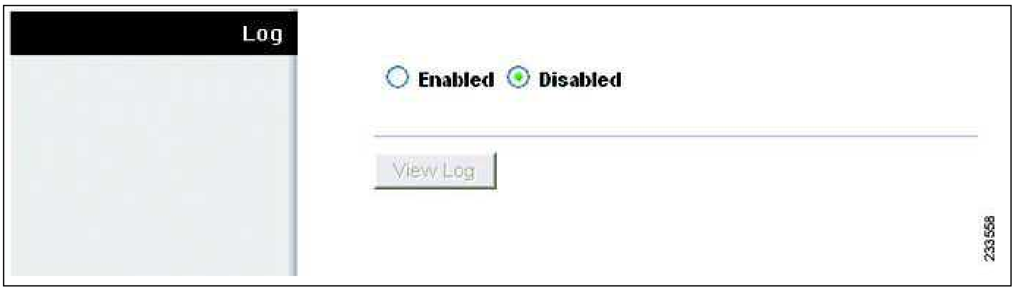
- **Support IGMP Version:** Select the version you want to support, **IGMP 1**, **IGMP v2**, or **IGMP 3**. If you are not sure which version to select, keep the default, **IGMP v2**.
- **IGMP Proxy:** Keep the default, **Enabled**, if you want to allow multicast traffic through the WRP400 for your multimedia application devices. Otherwise, select **Disabled**.
- **Immediate Leave:** Select **Enabled**, if you use IPTV applications and want to allow immediate channel swapping or flipping without lag or delays. Otherwise, keep the default, **Disabled**.

Administration > Log

The WRP400 can keep logs of all traffic for your Internet connection.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 43 Administration > Log



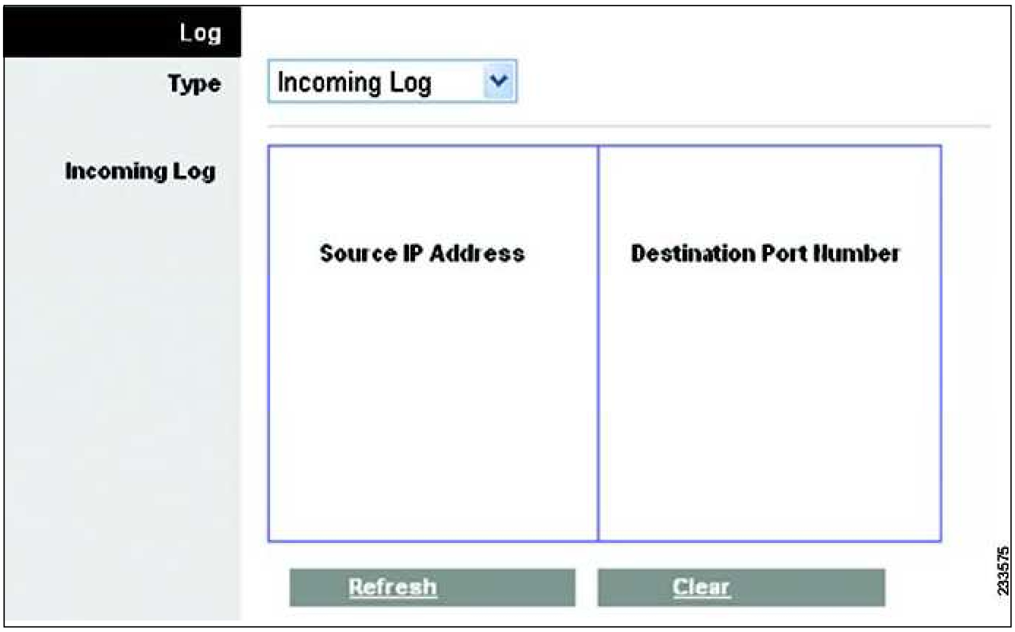
Log

○ Enabled ● Disabled

- **Log:** To disable the Log function, keep the default, **Disabled**. To monitor traffic between the network and the Internet, select **Enabled**. With logging enabled, you can choose to view temporary logs.

- **View Log:** To view the logs, click **View Log**.

Figure 44 Log > View Log



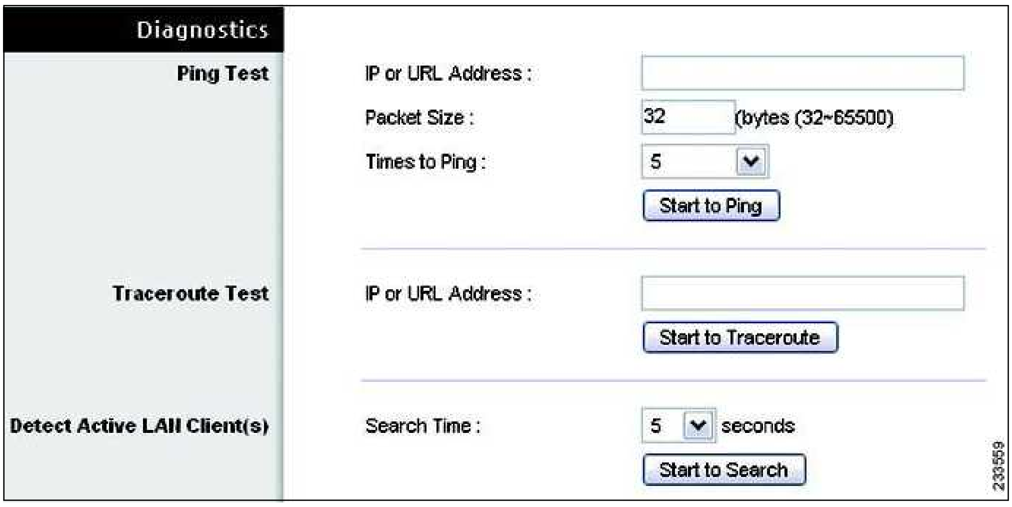
- **Type:** Select **Incoming Log**, **Outgoing Log**, **Security Log**, or **DHCP Client Log**.
- The **Incoming Log** will display a temporary log of the source IP addresses and destination port numbers for the incoming Internet traffic.
- The **Outgoing Log** will display a temporary log of the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic.
- The **Security Log** will display the login information for the web-based utility.
- The **DHCP Client Log** will display the LAN DHCP server status information.

Click **Refresh** to update the log. Click **Clear** to clear all the information that is displayed.

Administration > Diagnostics

The diagnostic tests (Ping, Traceroute, and Detect Active LAN Clients) allow you to check the connections of your network devices, including connection to the Internet.

Figure 45 Administration > Diagnostics



Diagnostics

Ping Test

IP or URL Address :

Packet Size : 32 (bytes (32~65500)

Times to Ping : 5

Traceroute Test

IP or URL Address :

Detect Active LAN Client(s)

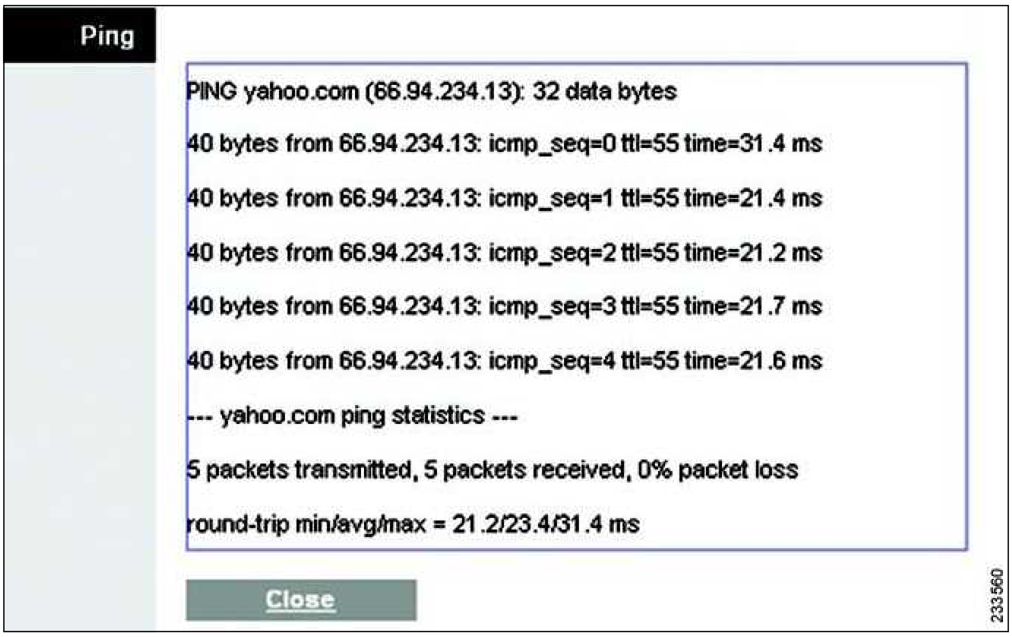
Search Time : 5 seconds

Ping Test

The Ping test checks the status of a connection.

- **IP or URL Address:** Enter the address of the PC whose connection you wish to test.
- **Packet Size:** Enter the packet size you want to use. The default is **32** bytes.
- **Times to Ping:** Enter many times you wish to test it.
- **Start to Ping:** To run the test, click this button. The Ping Test screen will show if the test was successful. Click **Close** to return to the Diagnostics screen.

Figure 46 Diagnostics > Ping



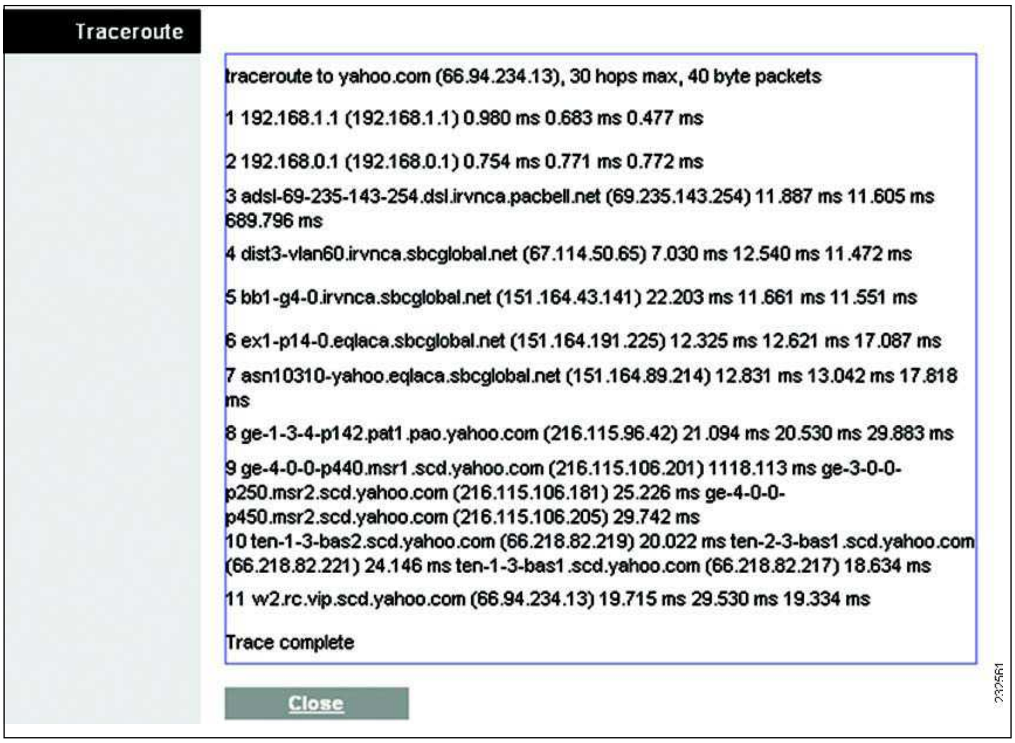
```
PING yahoo.com (66.94.234.13): 32 data bytes
40 bytes from 66.94.234.13: icmp_seq=0 ttl=55 time=31.4 ms
40 bytes from 66.94.234.13: icmp_seq=1 ttl=55 time=21.4 ms
40 bytes from 66.94.234.13: icmp_seq=2 ttl=55 time=21.2 ms
40 bytes from 66.94.234.13: icmp_seq=3 ttl=55 time=21.7 ms
40 bytes from 66.94.234.13: icmp_seq=4 ttl=55 time=21.6 ms
--- yahoo.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 21.2/23.4/31.4 ms
```

Traceroute Test

The Traceroute test tests the performance of a connection.

- **IP or URL Address:** Enter the address of the PC whose connection you wish to test.
- **Start to Traceroute:** To run the test, click this button. The Traceroute Test screen will show if the test was successful. Click **Close** to return to the Diagnostics screen.

Figure 47 Diagnostics > Traceroute



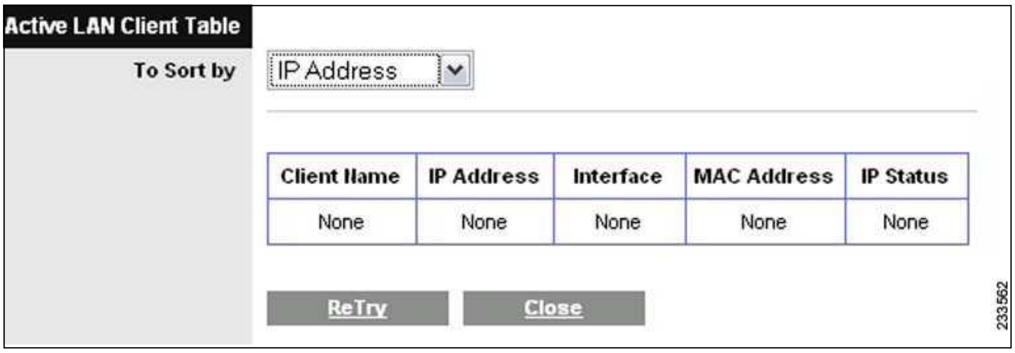
```
traceroute to yahoo.com (66.94.234.13), 30 hops max, 40 byte packets
1 192.168.1.1 (192.168.1.1) 0.980 ms 0.683 ms 0.477 ms
2 192.168.0.1 (192.168.0.1) 0.754 ms 0.771 ms 0.772 ms
3 adsl-69-235-143-254.dsl.irvnca.pacbell.net (69.235.143.254) 11.887 ms 11.605 ms
689.796 ms
4 dist3-vlan60.irvnca.sbcglobal.net (67.114.50.65) 7.030 ms 12.540 ms 11.472 ms
5 bb1-g4-0.irvnca.sbcglobal.net (151.164.43.141) 22.203 ms 11.661 ms 11.551 ms
6 ex1-p14-0.eqlaca.sbcglobal.net (151.164.191.225) 12.325 ms 12.621 ms 17.087 ms
7 asn10310-yahoo.eqlaca.sbcglobal.net (151.164.89.214) 12.831 ms 13.042 ms 17.818
ms
8 ge-1-3-4-p142.pat1.pao.yahoo.com (216.115.96.42) 21.094 ms 20.530 ms 29.883 ms
9 ge-4-0-0-p440.msr1.scd.yahoo.com (216.115.106.201) 1118.113 ms ge-3-0-0-
p250.msr2.scd.yahoo.com (216.115.106.181) 25.226 ms ge-4-0-0-
p450.msr2.scd.yahoo.com (216.115.106.205) 29.742 ms
10 ten-1-3-bas2.scd.yahoo.com (66.218.82.219) 20.022 ms ten-2-3-bas1.scd.yahoo.com
(66.218.82.221) 24.146 ms ten-1-3-bas1.scd.yahoo.com (66.218.82.217) 18.634 ms
11 w2.rc.vip.scd.yahoo.com (66.94.234.13) 19.715 ms 29.530 ms 19.334 ms
Trace complete
```

Detect Active LAN Client(s)

- **Search Time:** Select how many seconds you wish to perform this search: 5, 0, or 15.
- **Start to Search:** To run the search, click this button. The Active LAN Client Table screen will show the search results. You can sort the results by IP Address, MAC Address, Interface, Client Name, or IP Status.

To re-run the search, click **Retry**. Click **Close** to return to the Diagnostics screen.

Figure 48 Diagnostics > Active LAN Client Table



Active LAN Client Table

To Sort by: IP Address

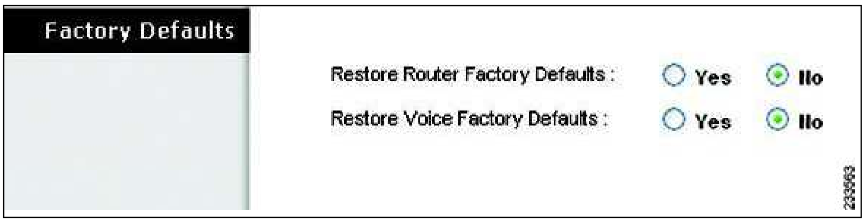
Client Name	IP Address	Interface	MAC Address	IP Status
None	None	None	None	None

Administration > Factory Defaults

The Administration > Factory Defaults screen allows you to restore the default configuration to the router settings and/or voice settings.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 49 Administration > Factory Defaults



Factory Defaults

Restore Router Factory Defaults : ○ Yes ● No

Restore Voice Factory Defaults : ○ Yes ● No

NOTE Restoring factory defaults deletes custom settings. Note your custom settings before restoring the factory defaults.

- **Restore Router Factory Defaults:** To reset the router settings to the default values, select **Yes.** Then click **Save Settings.** Any custom router settings you have saved will be lost when the default settings are restored.

- **Restore Voice Factory Defaults:** To reset the voice settings to the default values, select **Yes**. Then click **Save Settings**. Any custom Voice settings you have saved will be lost when the default settings are restored.

NOTE Restoring the voice defaults may require your login (the default user name and password are **admin**). If the defaults do not work, contact your service provider for more information.

Administration > Firmware Upgrade

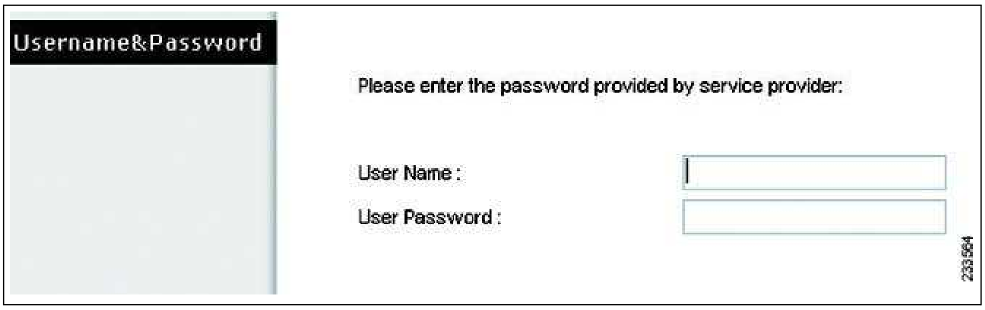
The Firmware Upgrade screen allows you to upgrade the firmware of the WRP400. Do not upgrade the firmware unless you are experiencing problems with the WRP400 or the new firmware has a feature you want to use.

If you want to upgrade the firmware, then you may need a user name and password available only from your service provider. Contact your service provider for more information.

Username & Password

If you see the Username & Password screen, enter the User Name and Password provided by your service provider. (The factory default User Name and Password are **admin**.) Then click **OK**.

Figure 50 Administration > Username & Password



Username&Password

Please enter the password provided by service provider:

User Name :

User Password :

NOTE The WRP400 may lose the settings you have customized. Before you upgrade the firmware, use the Config Management screen to back up your settings. For more informaiton, see **"Administration > Config Management," on page 99**.

Firmware Upgrade

Download the latest firmware from Cisco.com, and then upgrade the firmware on your WRP400.

Downloading the Firmware

STEP 1 Go to the WRP400 product page on Cisco.com: http://www.cisco.com/en/US/products/ps10028/index.html

NOTE This site requires a login. If you do not have a user account, you can register for free.

STEP 2 Click the **Download Software** link.

STEP 3 When the Download Software page appears, click the link under the Latest Releases folder.

STEP 4 On the right side of the page, click the link for the BIN file.

STEP 5 When the Download Image page appears, click **Download**.

STEP 6 Read the license agreement, and then click **Agree** at the end of the page.

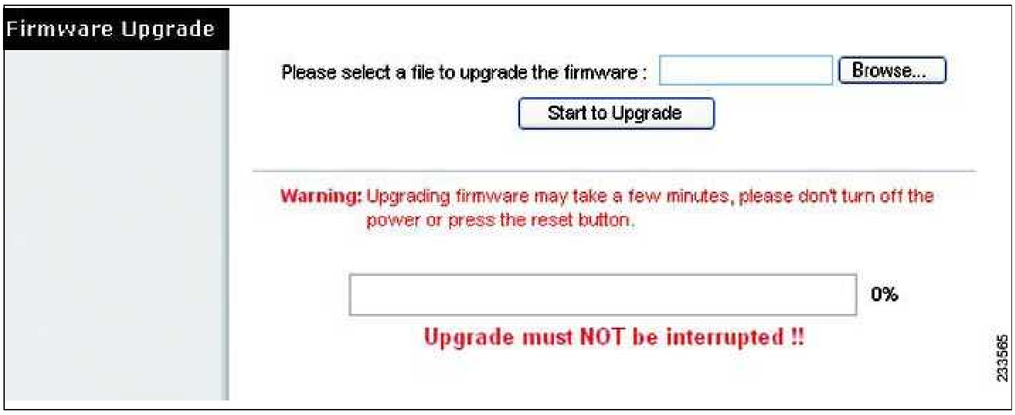
STEP 7 When the File Download window appears, click **Save**, and then save the file in the desired location, such as your Windows Desktop.

STEP 8 When the Download Complete window appears, click **Close**.

Firmware Upgrade

After you download the firmware from Cisco.com, you can upgrade the WRP400.

Figure 51 Administration > Firmware Upgrade



Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.

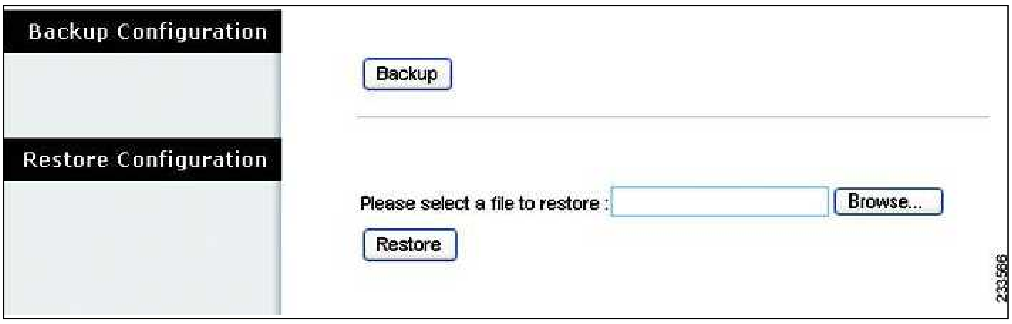
Upgrade must NOT be interrupted !!

- **Please select a file to upgrade the firmware:** Click **Browse** and select the firmware upgrade file that you downloaded from Cisco.com.
- **Start to Upgrade:** After you have selected the appropriate file, click this button, and follow the on-screen instructions.

Administration > Config Management

The Config Management screen allows you to back up or restore the settings by using a configuration file.

Figure 52 Administration > Config Management



Backup Configuration

- **Backup:** To save the settings in a configuration file, click this button and follow the on-screen instructions.

Restore Configuration

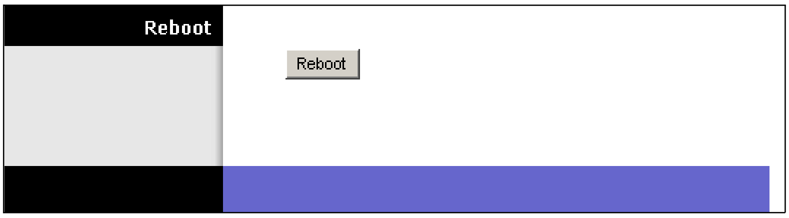
To use this option, you must have previously backed up its configuration settings.

- **Please select a file to restore:** Click the **Browse** button and select the configuration file.
- **Restore:** To restore the configuration settings, click this button and follow the on-screen instructions.

Administration > Reboot

The Reboot screen allows you to reboot the device from the administration web server. Click the **Reboot** button.

Figure 53 Administration > Config Management



10

Using the Status Screens

You can use the Status screens to view information about your WRP400.

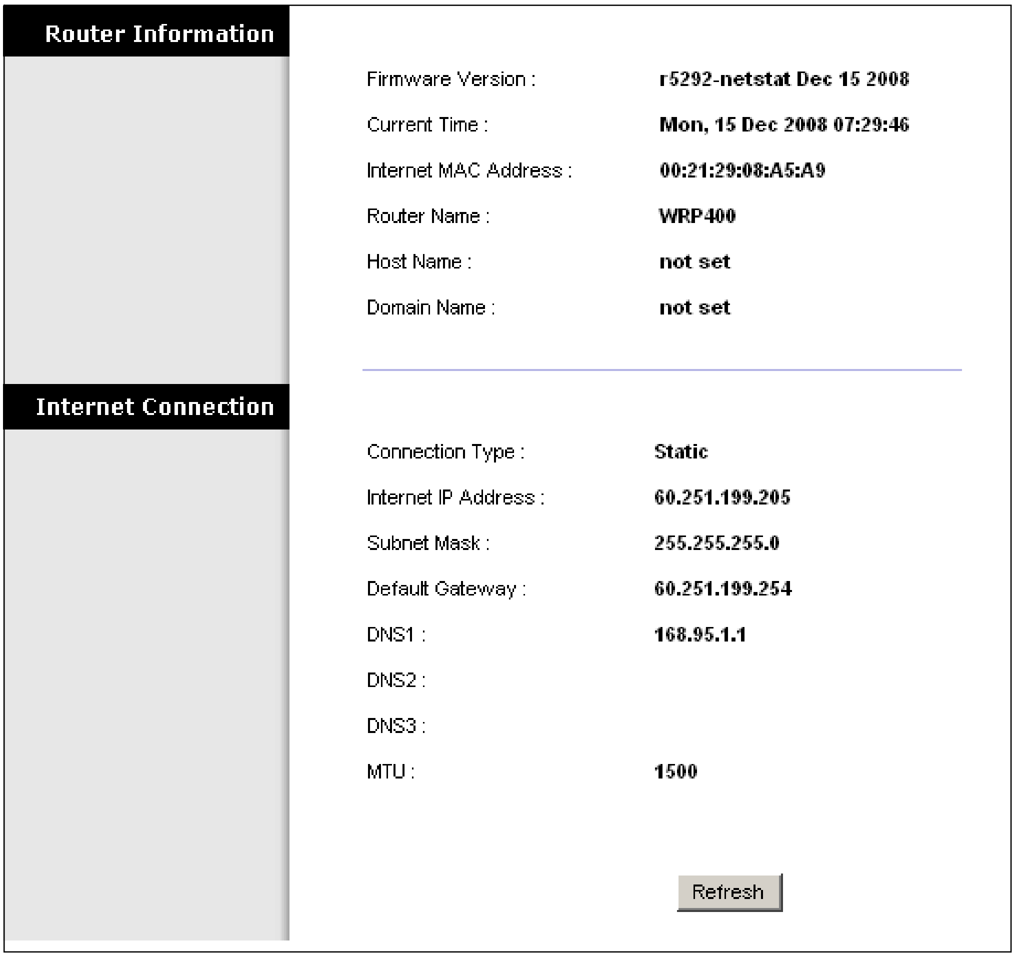
How Do I...

- **View the firmware version, the router name, the host name, the Internet MAC address and the current time?**
  See **"Status > Router," on page 102**.
- **View the status of the Internet connection?**
  See **"Internet Connection," on page 103**.
- **View the status and basic information about my mobile network?**
  See **"Status > Mobile Network," on page 104**
- **View information about my local wired network?**
  See **"Status > Local Network," on page 106**.
- **View information about the DHCP server and DHCP Table?**
  See **"Status > Local Network," on page 106**
- **View information about my wireless network?**
  See **"Status > Wireless Network," on page 108**.

Status > Router

The Router screen displays information about the WRP400.

Figure 54 Status > Router



Firmware Version : r5292-netstat Dec 15 2008

Current Time : Mon, 15 Dec 2008 07:29:46

Internet MAC Address : 00:21:29:08:A5:A9

Router Name : WRP400

Host Name : not set

Domain Name : not set

Connection Type : Static

Internet IP Address : 60.251.199.205

Subnet Mask : 255.255.255.0

Default Gateway : 60.251.199.254

DNS1 : 168.95.1.1

DNS2 :

DNS3 :

MTU : 1500

Router Information

- **Firmware Version:** The version number of the current firmware is displayed.
- **Current Time:** The time set on the WRP400 is displayed.

- **Internet MAC Address:** The MAC address, as seen by your service provider, is displayed.
- **Router Name:** The name of the WRP400 is displayed.
- **Host Name:** If required by your service provider, this was entered on the Basic Setup screen.
- **Domain Name:** If required by your service provider, this was entered on the Basic Setup screen.

Internet Connection

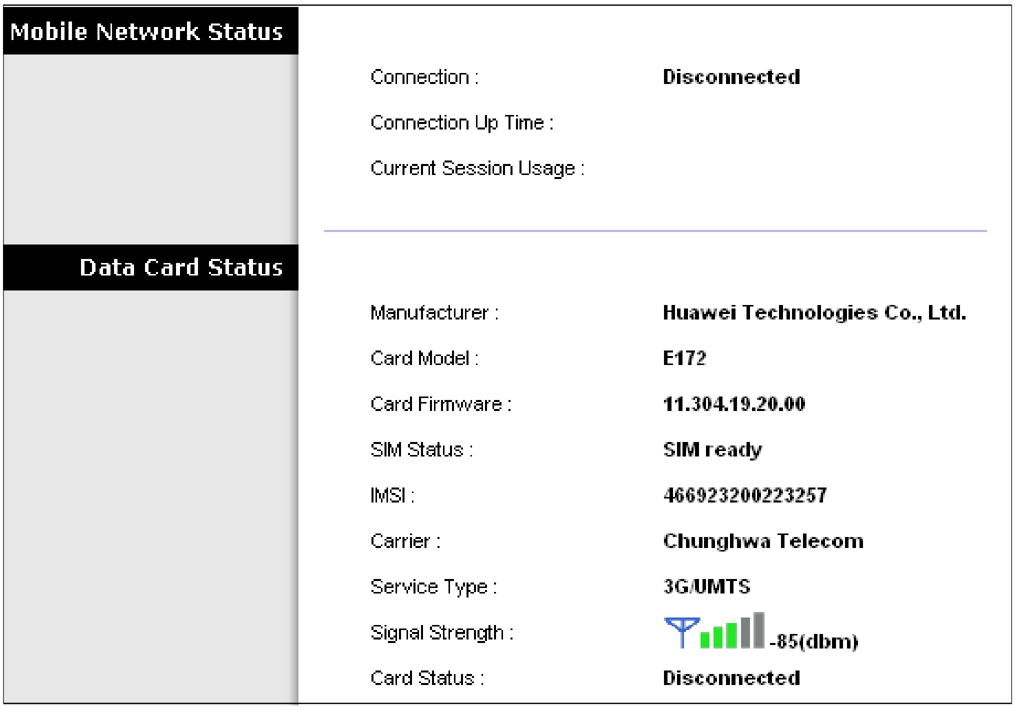
This section shows the current network information. It varies depending on the Internet connection type selected on the Basic Setup screen.

Click **Refresh** to update the on-screen information.

Status > Mobile Network

The Mobile Network Status screen shows the status of the mobile network and displays information about the data card. The screen automatically refreshes periodically.

Figure 55 Status > Mobile Network Status



Mobile Network Status

Connection : Disconnected

Connection Up Time :

Current Session Usage :

Data Card Status

Manufacturer : Huawei Technologies Co., Ltd.

Card Model : E172

Card Firmware : 11.304.19.20.00

SIM Status : SIM ready

IMSI : 466923200223257

Carrier : Chunghwa Telecom

Service Type : 3G/UMTS

Signal Strength : -85(dbm)

Card Status : Disconnected

Mobile Network Status

- **Connection:** The status of the mobile network connection, either Disconnected or Connected
- **Connection Up Time:** The period of time that the Mobile USB modem has been connected to the Internet during this session
- **Current Session Usage:** The number of packets have been downloaded and uploaded during this session

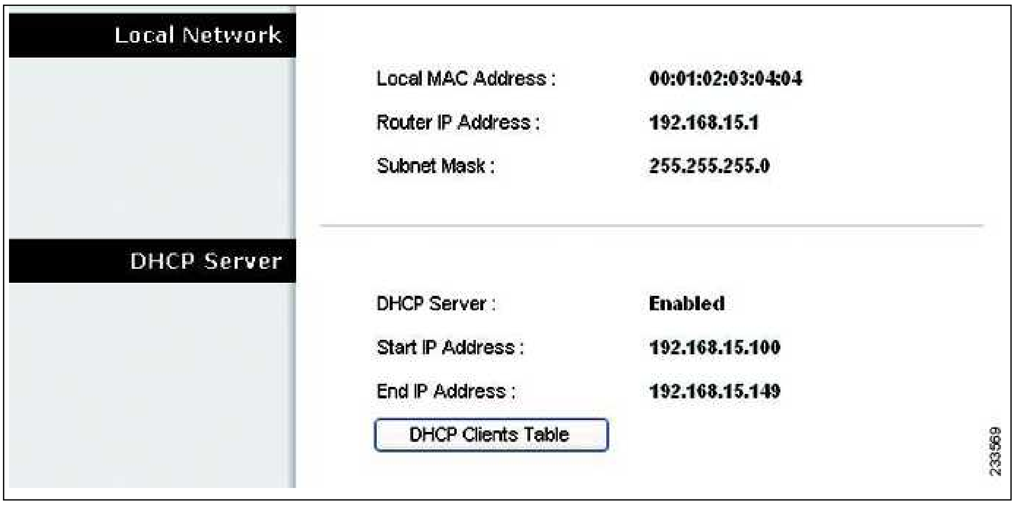
Data Card Status

- **Manufacturer:** The manufacturer of the Mobile USB modem data card
- **Card Model:** The model number of your Mobile USB modem data card
- **Card Firmware:** The firmware that is installed on your Mobile USB modem data card
- **SIM Status:** The status of your SIM card
- **IMSI:** International Mobile Subscriber Identity is a unique number that is stored in the Subscriber Identity Module (SIM) associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users
- **Carrier:** The network service provider that is used for Internet connection
- **Service Type:** Displayed your current UMTS/GPRS/EVDO service for Internet connection.
- **Signal Strength:** Indicated the signal strength of your current UMTS/GPRS/EVDO service to your location.
- **Card Status:** Indicated current Mobile WAN connection status.

Status > Local Network

The Local Network screen displays information about the local, wired network.

Figure 56 Status > Local Network



Local Network

Local MAC Address : 00:01:02:03:04:04

Router IP Address : 192.168.15.1

Subnet Mask : 255.255.255.0

DHCP Server

DHCP Server : Enabled

Start IP Address : 192.168.15.100

End IP Address : 192.168.15.149

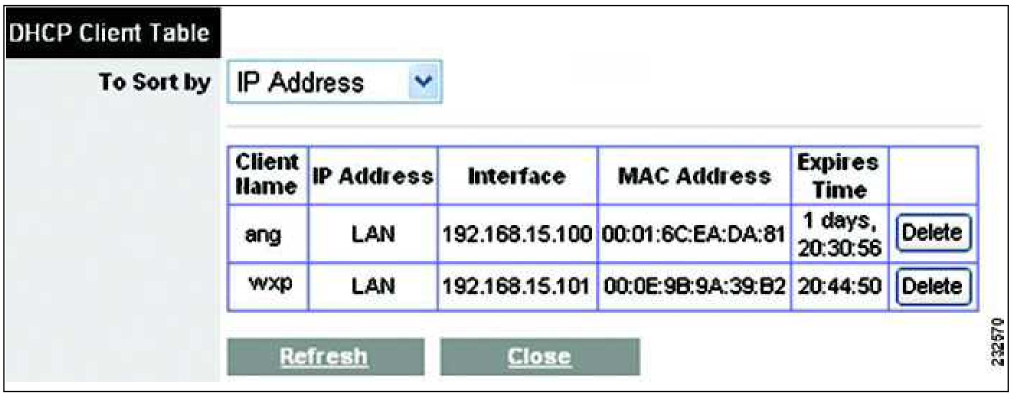
Local Network

- **Local MAC Address:** The MAC address of the local, wired interface of the WRP400 is displayed.
- **Router IP Address:** The IP address of the WRP400, as it appears on your local network, is displayed.
- **Subnet Mask:** The Subnet Mask of the WRP400 is displayed.

DHCP Server

- **DHCP Server:** The status of the DHCP server function is displayed.
- **Start IP Address:** For the range of IP addresses used by devices on your local network, the starting IP address is displayed.
- **End IP Address:** For the range of IP addresses used by devices on your local network, the ending IP address is displayed.
- **DHCP Clients Table:** Click this button to view a list of computers that are using the WRP400 as a DHCP server.

Figure 57 DHCP Clients Table



DHCP Client Table

To Sort by: IP Address

Client Name	IP Address	Interface	MAC Address	Expires Time	
ang	LAN	192.168.15.100	00:01:6C:EA:DA:81	1 days, 20:30:56	Delete
wxp	LAN	192.168.15.101	00:0E:9B:9A:39:B2	20:44:50	Delete

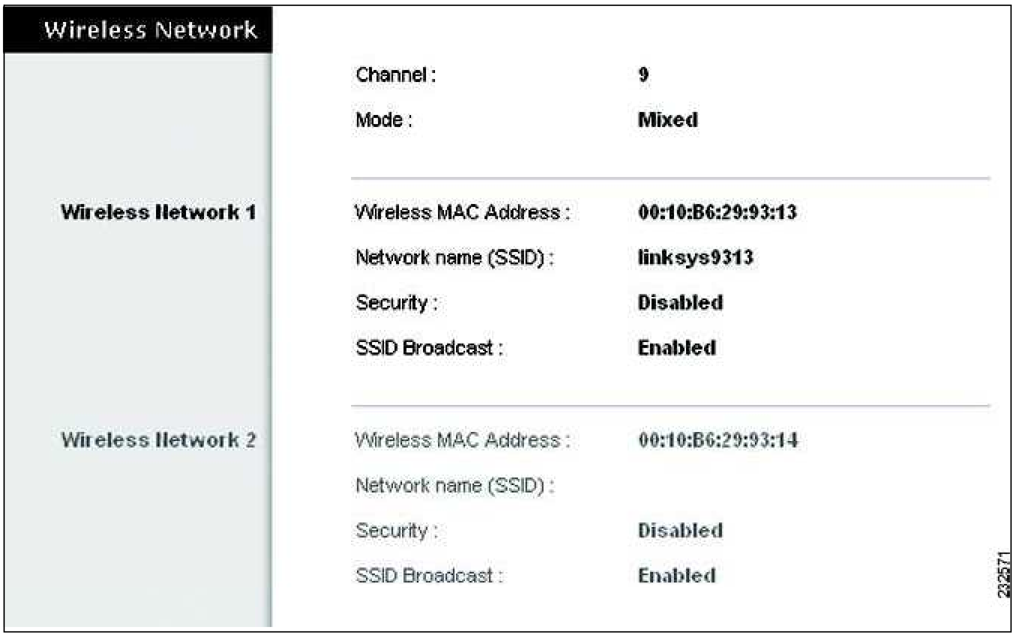
DHCP Client Table

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the WRP400. The list can be sorted by Client Name, IP Address, Interface, MAC Address, and Expires Time (how much time is left for the current IP address). To remove a DHCP client, click **Delete.** To retrieve the most up-to-date information, click **Refresh.** To exit this screen and return to the Local Network screen, click **Close.**

Status > Wireless Network

The Wireless Network screen displays information about your wireless network(s).

Figure 58 Status > Wireless Network



Wireless Network

	Channel :	9
	Mode :	Mixed
Wireless Network 1	Wireless MAC Address :	00:10:B6:29:93:13
	Network name (SSID) :	linksys9313
	Security :	Disabled
	SSID Broadcast :	Enabled
Wireless Network 2	Wireless MAC Address :	00:10:B6:29:93:14
	Network name (SSID) :	
	Security :	Disabled
	SSID Broadcast :	Enabled

- **Channel:** The channel of the wireless network(s) is displayed.
- **Mode:** The wireless mode is displayed.

Status information for each wireless network is displayed.

- **Wireless MAC Address:** The wireless MAC address of the local, wireless interface is displayed.
- **Network Name (SSID):** The network name, which is also called the SSID, is displayed.
- **Security:** The wireless security method is displayed.
- **SSID Broadcast:** The status of the SSID Broadcast feature is displayed.

11

Configuring Voice Services

You can use the Voice screens to manage the voice gateway features of the WRP400.

How Do I...

- **View the Voice screens?**
  See "Access to the Voice Screens," on page 109
- **View product information, system status, and line status?**
  See "Voice > Info," on page 110
- **Change the password for user access to the Voice screens?**
  See "Voice > System," on page 113
- **Set call forwarding, speed dial, supplementary services, and ring settings?**
  See "Voice > User 1/2," on page 114
- **Configure the Admin login?**
  See "Voice > Admin Login," on page 118

Access to the Voice Screens

There are two level of access, user and Admin Login. When you click the Voice tab, the Info screen is automatically displayed. If you set a User Password on the System screen, then you will be asked to enter it before the Info screen is displayed.

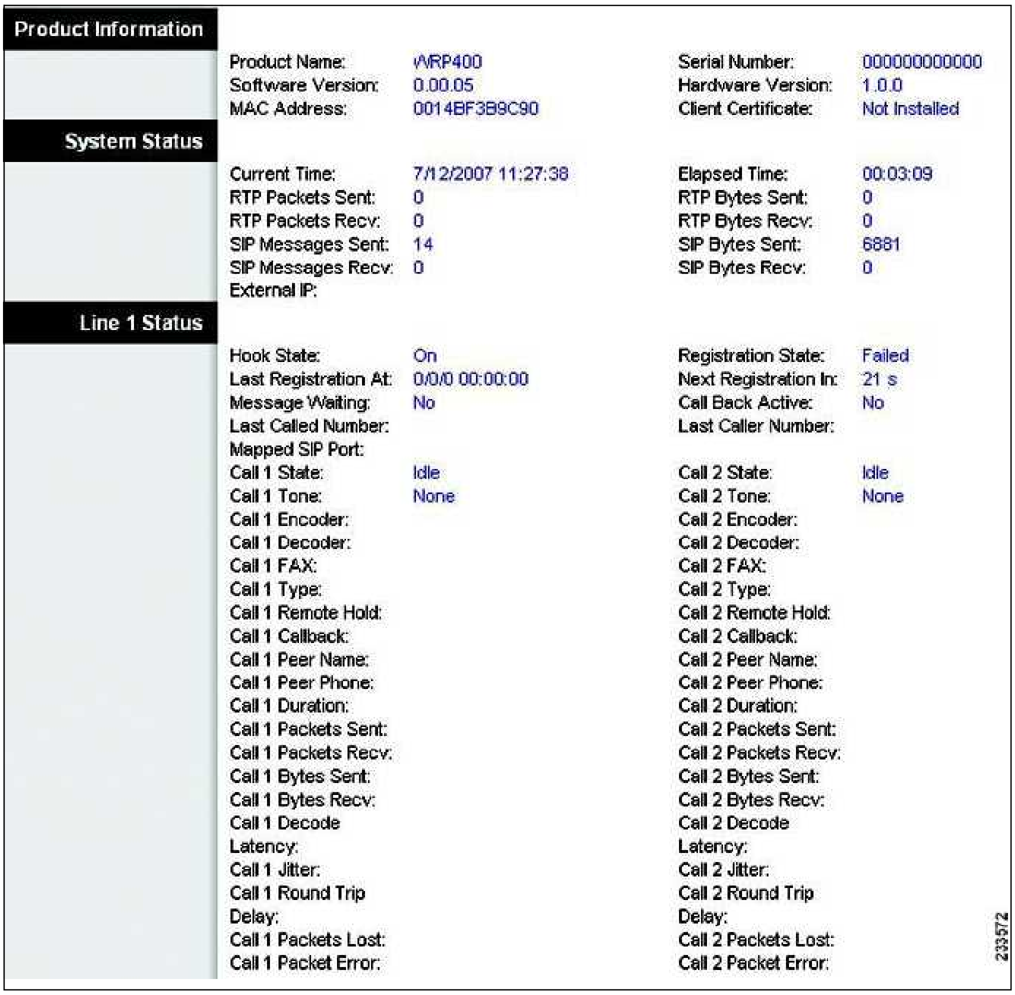
The Admin Login allows access to more advanced settings. To access administrative screens, click **Admin Login**, and enter the user name and password provided by your service provider. Contact your service provider for more information. (The factory default Admin Login name and password are **admin**.)

NOTE In most cases, you do not need to use the administrative screens. Contact your service provider for more information.

Voice > Info

The Info screen displays Voice over Internet Protocol (VoIP) information about the WRP400.

Figure 59 Voice > Info



Product Information

Product Name:	WRP400	Serial Number:	000000000000
Software Version:	0.00.05	Hardware Version:	1.0.0
MAC Address:	0014BF3B9C90	Client Certificate:	Not Installed

System Status

Current Time:	7/12/2007 11:27:38	Elapsed Time:	00:03:09
RTP Packets Sent:	0	RTP Bytes Sent:	0
RTP Packets Recv:	0	RTP Bytes Recv:	0
SIP Messages Sent:	14	SIP Bytes Sent:	6881
SIP Messages Recv:	0	SIP Bytes Recv:	0
External IP:			

Line 1 Status

Hook State:	On	Registration State:	Failed
Last Registration At:	0/0/0 00:00:00	Next Registration In:	21 s
Message Waiting:	No	Call Back Active:	No
Last Called Number:		Last Caller Number:	
Mapped SIP Port:			
Call 1 State:	Idle	Call 2 State:	Idle
Call 1 Tone:	None	Call 2 Tone:	None
Call 1 Encoder:		Call 2 Encoder:	
Call 1 Decoder:		Call 2 Decoder:	
Call 1 FAX:		Call 2 FAX:	
Call 1 Type:		Call 2 Type:	
Call 1 Remote Hold:		Call 2 Remote Hold:	
Call 1 Callback:		Call 2 Callback:	
Call 1 Peer Name:		Call 2 Peer Name:	
Call 1 Peer Phone:		Call 2 Peer Phone:	
Call 1 Duration:		Call 2 Duration:	
Call 1 Packets Sent:		Call 2 Packets Sent:	
Call 1 Packets Recv:		Call 2 Packets Recv:	
Call 1 Bytes Sent:		Call 2 Bytes Sent:	
Call 1 Bytes Recv:		Call 2 Bytes Recv:	
Call 1 Decode Latency:		Call 2 Decode Latency:	
Call 1 Jitter:		Call 2 Jitter:	
Call 1 Round Trip Delay:		Call 2 Round Trip Delay:	
Call 1 Packets Lost:		Call 2 Packets Lost:	
Call 1 Packet Error:		Call 2 Packet Error:	

Product Information

- **Product Name:** The model number of the WRP400
- **Serial Number:** The serial number of the WRP400
- **Software Version:** The version number of the WRP400 software
- **Hardware Version:** The version number of the WRP400 hardware
- **MAC Address:** The MAC address of the WRP400
- **Client Certificate:** The status of the client certificate, which indicates that the WRP400 has been authorized by your service provider,

System Status

- **Current Time:** The current date and time of the WRP400 are displayed.
- **Elapsed Time:** The amount of time elapsed since the last reboot of the WRP400
- **RTP Packets Sent:** The number of RTP packets sent by the WRP400
- **RTP Bytes Sent:** The number of RTP bytes sent by the WRP400
- **RTP Packets Recv:** The number of RTP packets received by the WRP400
- **RTP Bytes Recv:** The number of RTP bytes received by the WRP400
- **SIP Messages Sent:** The number of SIP messages sent by the WRP400
- **SIP Bytes Sent:** The number of SIP bytes sent by the WRP400
- **SIP Messages Recv:** The number of SIP messages received by the WRP400
- **SIP Bytes Recv:** The number of SIP bytes received by the WRP400
- **External IP:** The external IP address used for NAT mapping

Line 1/2 Status

Lines 1 and 2 have the same status information available.

- **Hook State:** The status of the Internet phone line's readiness. "On" indicates that it is ready for use, while "Off" indicates that it is in use.
- **Registration State:** The status of the line's registration with the service provider
- **Last Registration At:** The last date and time the line was registered are displayed.
- **Next Registration In:** The number of seconds until the next registration
- **Message Waiting:** This indicates whether you have new voicemail waiting.
- **Call Back Active:** This indicates whether a call back request is in progress.
- **Last Called Number:** The last number called
- **Last Caller Number:** The number of the last caller
- **Mapped SIP Port:** The port number of the NAT mapped SIP port

Calls 1 and 2 have the same status information available.

- **Call 1/2 State:** The status of the call
- **Call 1/2 Tone:** The type of tone used by the call
- **Call 1/2 Encoder:** The codec used for encoding
- **Call 1/2 Decoder:** The codec used for decoding
- **Call 1/2 FAX:** The status of the fax pass-through mode
- **Call 1/2 Type:** The direction of the call
- **Call 1/2 Remote Hold:** This indicates whether the far end has placed the call on hold.
- **Call 1/2 Callback:** This indicates whether the call was triggered by a call back request.
- **Call 1/2 Peer Name:** The name of the internal phone
- **Call 1/2 Peer Phone:** The phone number of the internal phone
- **Call 1/2 Duration:** The duration of the call

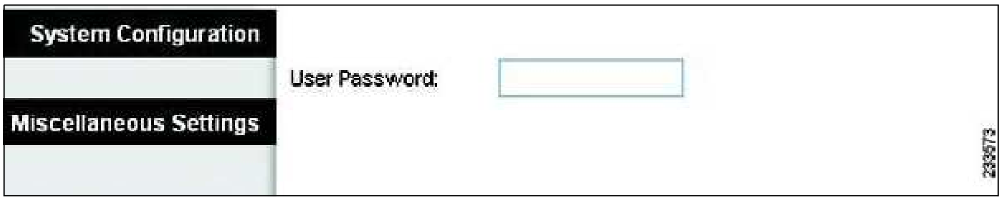
- **Call 1/2 Packets Sent:** The number of packets sent
- **Call 1/2 Packets Recv:** The number of packets received
- **Call 1/2 Bytes Sent:** The number of bytes sent
- **Call 1/2 Bytes Recv:** The number of bytes received
- **Call 1/2 Decode Latency:** The number of milliseconds for decoder latency
- **Call 1/2 Jitter:** The number of milliseconds for receiver jitter
- **Call 1/2 Round Trip Delay:** The number of milliseconds for delay
- **Call 1/2 Packets Lost:** The number of packets lost
- **Call 1/2 Packet Error:** The number of invalid packets received
- **Call 1/2 Mapped RTP Port:** The number of the NAT mapped RTP port
- **Call 1/2 Media Loopback:** The Media Loopback feature allows the service provider to test the quality of the connection to the WRP400. The status of the feature

Voice > System

The System screen displays the User Password setting.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 60 Voice > System



User Password:

System Configuration

- **User Password:** Enter the password for user access to the Voice screens. (By default, there is no password.)

Miscellaneous Settings

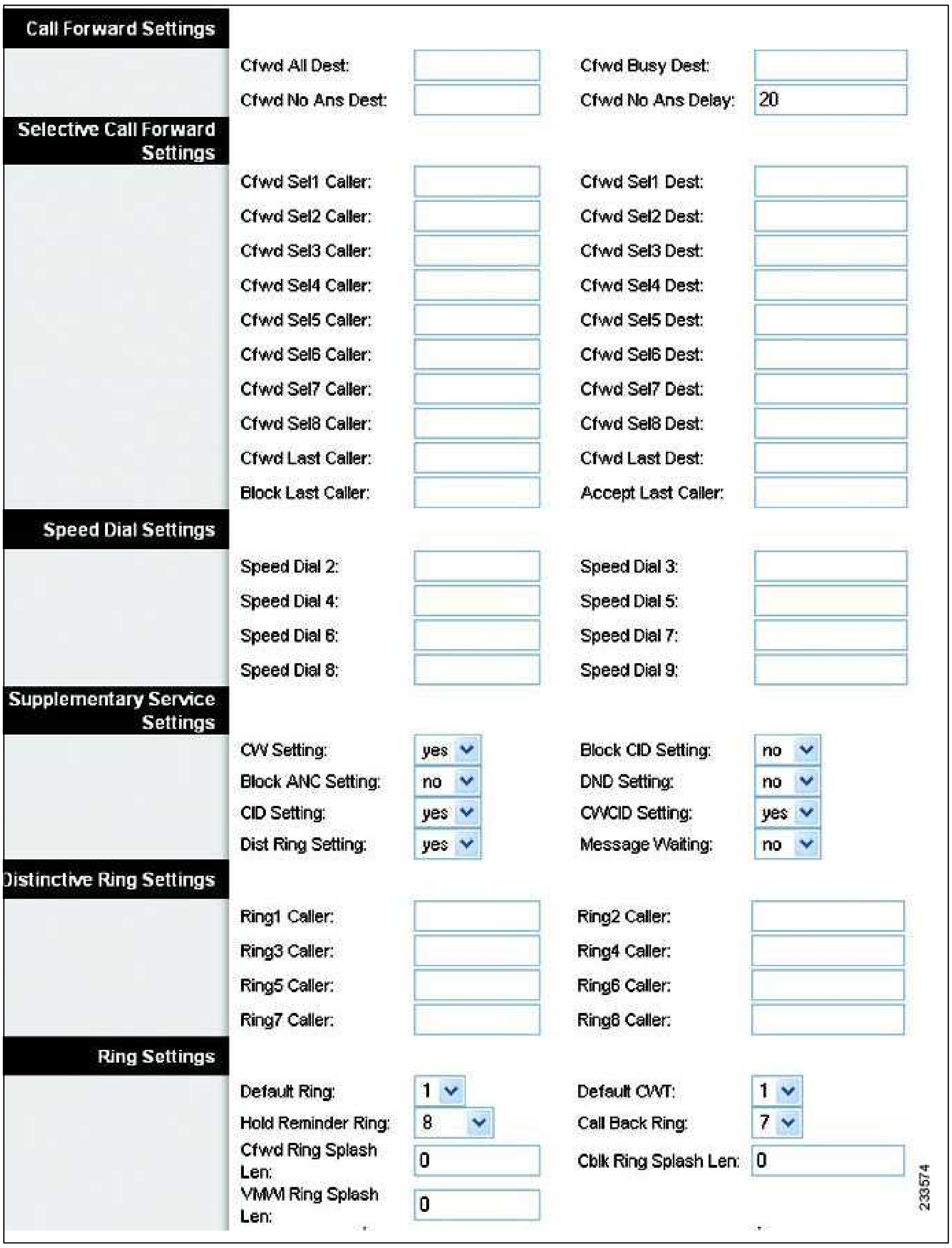
No settings are displayed.

Voice > User 1/2

The User 1 and 2 screens display similar settings. The User 1 screen displays settings for users of phone line 1, and the User 2 screen displays settings for users of phone line 2.

NOTE After you enter settings on this page, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Figure 61 Voice > User 1



Call Forward Settings

Cfwd All Dest:		Cfwd Busy Dest:	
Cfwd No Ans Dest:		Cfwd No Ans Delay:	20

Selective Call Forward Settings

Cfwd Sel1 Caller:		Cfwd Sel1 Dest:	
Cfwd Sel2 Caller:		Cfwd Sel2 Dest:	
Cfwd Sel3 Caller:		Cfwd Sel3 Dest:	
Cfwd Sel4 Caller:		Cfwd Sel4 Dest:	
Cfwd Sel5 Caller:		Cfwd Sel5 Dest:	
Cfwd Sel6 Caller:		Cfwd Sel6 Dest:	
Cfwd Sel7 Caller:		Cfwd Sel7 Dest:	
Cfwd Sel8 Caller:		Cfwd Sel8 Dest:	
Cfwd Last Caller:		Cfwd Last Dest:	
Block Last Caller:		Accept Last Caller:	

Speed Dial Settings

Speed Dial 2:		Speed Dial 3:	
Speed Dial 4:		Speed Dial 5:	
Speed Dial 6:		Speed Dial 7:	
Speed Dial 8:		Speed Dial 9:	

Supplementary Service Settings

CW Setting:	yes	Block CID Setting:	no
Block ANC Setting:	no	DND Setting:	no
CID Setting:	yes	CWCID Setting:	yes
Dist Ring Setting:	yes	Message Waiting:	no

Distinctive Ring Settings

Ring1 Caller:		Ring2 Caller:	
Ring3 Caller:		Ring4 Caller:	
Ring5 Caller:		Ring6 Caller:	
Ring7 Caller:		Ring8 Caller:	

Ring Settings

Default Ring:	1	Default CWT:	1
Hold Reminder Ring:	8	Call Back Ring:	7
Cfwd Ring Splash Len:	0	Cblk Ring Splash Len:	0
VMWI Ring Splash Len:	0		

Call Forward Settings

Enter the call forwarding numbers you want to use.

- **Cfwd All Dest:** Enter the number for the Call Forward All Service feature (when you want to forward all calls).
- **Cfwd Busy Dest:** Enter the number for the Call Forward Busy feature (when the line is busy).
- **Cfwd No Ans Dest:** Enter the number for the Call Forward No Answer feature (when the line is not answered).
- **Cfwd No Ans Delay:** Enter the number of seconds to wait before the Call Forward No Answer feature is triggered. The default is 20.

Selective Call Forward Settings

Enter the caller numbers that will be forwarded to specific phone numbers.

- **Cfwd Sel1-8 Caller:** Enter the caller number pattern to trigger the Call Forward Selective (1-8) feature.
- **Cfwd Sel1-8 Dest:** Enter the forward number for the Call Forward Selective (1-8) feature.
- **Cfwd Last Caller:** Enter the caller number that is actively forwarded to the Cfwd Last Dest number when the Call Forward Last activation code is used.
- **Cfwd Last Dest:** Enter the forward number for the Cfwd Last Caller feature.
- **Block Last Caller:** Enter the ID of the caller blocked via the Block Last Caller service.
- **Accept Last Caller:** Enter the ID of the caller accepted via the Accept Last Caller service.

Speed Dial Settings

- **Speed Dial 2-9:** Enter the phone number for each Speed Dial setting.

Supplementary Service Settings

- **CW Setting:** Select whether you want to use the Call Waiting feature for all calls, **yes** or **no**. The default is **yes**.
- **Block CID Setting:** Select whether you want to block Caller ID for all calls, **yes** or **no**. The default is **no**.
- **Block ANC Setting:** Select whether you want to block anonymous calls, **yes** or **no**. The default is **no**.
- **DND Setting:** Select whether you want to use the Do Not Disturb (DND) feature, **Yes** or **no**. The default is **no**.
- **CID Setting:** Select whether you want to enable Caller ID generation, **yes** or **no**. The default is **yes**.
- **CWCID Setting:** Select whether you want to enable Caller ID for Call Waiting, **yes** or **no**. The default is **yes**.
- **Dist Ring Setting:** Select whether you want to use the Distinctive Ring feature, **Yes** or **no**. The default is **yes**.
- **Message Waiting:** Select whether you want to use the Message Waiting feature, **yes** or **no**. The default is **no**.

Distinctive Ring Settings

- **Ring1-8 Caller:** Enter the caller number pattern to play Distinctive Ring/Call Waiting Tone (1-8).

Ring Settings

- **Default Ring:** Select the default ringing pattern for all callers. The default is **1**.
- **Default CWT:** Select the default CWT pattern for all callers. The default is **1**.
- **Hold Reminder Ring:** Select the ring pattern that will remind you of a call on hold when the phone is on-hook. The default is **8**.
- **Call Back Ring:** Select the ring pattern for call back notification. The default is **7**.
- **Cfwd Ring Splash Len:** Enter the duration of the ring splash when a call is forwarded. The range is 0 to 10.0 seconds. The default is **0**.

- **Cblk Ring Splash Len:** Enter the duration of the ring splash when a call is blocked. The range is 0 to 10.0 seconds. The default is **0**.
- **VMWI Ring Splash Len:** Enter the duration of the ring splash when new messages arrive before the VoiceMail Waiting Indication (VMWI) signal is applied. The range is 0 to 10.0 seconds. The default is **0**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Voice > Admin Login

The Admin Login allows access to more advanced settings. To access administrative screens, click **Admin Login**, and enter the user name and password provided by your service provider. Contact your service provider for more information. (The factory default Admin Login name and password are **admin**.)

NOTE In most cases, you do not need to use the administrative screens. Contact your service provider for more information.

12

Interactive Voice Response Menu

Overview

This chapter explains how to use the Interactive Voice Response (IVR) Menu to configure the network settings. Use your telephone's keypad to enter your commands and select choices, and the WRP400 will use voice responses.

To access the IVR Menu:

STEP 1 Use a telephone connected to the Phone 1 or 2 port of the WRP400. (You can only access the IVR Menu through an analog telephone, not any of the Internet phones.)

STEP 2 Press ******** (in other words, press the star key four times).

STEP 3 Wait until you hear the response, "Configuration menu. Please enter the option followed by the # (pound) key, or hang up to exit".

Menu Commands

Refer to the following table that lists actions, commands, menu choices, and descriptions. After you select an option, press the **#** (pound) key. To exit the menu, hang up the telephone.

If the menu is inactive for more than one minute, the WRP400 will time out. To re-enter the menu, press ********.

Action	Command	Choices	Description
Enter IVR Menu	****		Use this command to enter the IVR Menu. Ignore Special Information Tones (SITs) or other tones until you hear, “Configuration menu. Please enter the option followed by the # (pound) key, or hang up to exit.”
Check DHCP	100		The IVR announces whether DHCP is enabled or disabled.
Check IP Address	110		The IVR announces the current IP address of the WRP400.
Check Subnet Mask	120		The IVR announces the current subnet mask of the WRP400.
Check Static Gateway IP Address	130		The IVR announces the current gateway IP address of the WRP400.
Check MAC Address	140		The IVR announces the MAC address of the WRP400 in hexadecimal string format.
Check Firmware Version	150		The IVR announces the version number of the firmware running on the WRP400.
Voice Factory Reset of the Router Warning: All custom settings will be lost.	73738	Confirm - Press 1. Cancel - Press * (star).	After the WRP400 requests confirmation, press 1 to confirm. After you hear, “Option successful”, hang up the phone. All voice settings will be reset to their defaults.

A

Troubleshooting

NOTE If your questions are not addressed here, refer to the Application Notes and other Technical Resources on Cisco Partner Central website for Voice and Conferencing, at the following URL:
http://www.cisco.com/web/partners/sell/smb/products/voice_and_conferencing.html

This chapter has two sections:

General Troubleshooting

Q. My computer cannot connect to the Internet.

Follow these instructions until your computer can connect to the Internet:

a. Make sure that the WRP400 is powered on. The Power LED should be green and not flashing.

b. If the Power LED is flashing, then power off all of your network devices, including the modem, the WRP400, and the computers. Wait 30 seconds. Then power on each device in the following order:

- Cable or DSL modem
- WRP400
- Computer

c. Check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the WRP400, and the modem must be connected to the Internet port on the WRP400.

Q. There is no dial tone, and the Phone 1 or 2 LED is not lit.

Follow these instructions until your problem is solved:

a. Make sure the telephone is plugged into the appropriate port, Phone 1 or 2.

b. Disconnect and re-connect the RJ-11 telephone cable between the WRP400 and telephone.

c. Make sure your telephone is set to its tone setting (not pulse).

d. Make sure your network has an active Internet connection. Try to access the Internet, and check to see if the WRP400 Internet LED is lit. If you do not have a connection, then power off all of your network devices, including the modem, the WRP400, and the computers. Wait 30 seconds. Then power on each device in the following order:

   - Cable or DSL modem
   - WRP400
   - Computers and other devices

e. Verify your account information and confirm that the phone line is registered with your Internet Telephony Service Provider (ITSP).

Q. When I place an Internet phone call, words are dropped intermittently.

Consider the following possible causes and solutions:

- **Cordless phone:** If you are using the WRP400 wireless function and a cordless phone, they may be using the same frequency and may interfere with each other. Move the cordless phone farther away from the WRP400.

- **Network activity:** There may be heavy network activity, particularly if you are running a server or using a file sharing program. Try to limit network or Internet activity during Internet phone calls. For example, if you are running a file sharing program, files may be uploaded in the background even though you are not downloading any files, so make sure you exit the program before making Internet phone calls.

- **Bandwidth:** There may not be enough bandwidth available for your Internet phone call. You may want to test your bandwidth by using one of the bandwidth tests available online. If necessary, access your Internet phone service account and reduce the bandwidth requirements for your service. For more information, refer to the website of your ITSP.

Q. The modem does not have an Ethernet port.

If your modem does not have an Ethernet port, then it is a modem for traditional dial-up service. To use the WRP400, you need a cable/DSL modem and a high-speed Internet connection.

Q. I cannot use the DSL service to connect manually to the Internet.

After you have installed the WRP400, it will automatically connect to your Internet Service Provider (ISP) or Internet Telephony Service Provider (ITSP), so you no longer need to connect manually.

Q. The DSL telephone line does not fit into the WRP400 Internet port.

The WRP400 does not replace your modem. You still need your DSL modem in order to use the WRP400. Connect the telephone line to the DSL modem, insert the setup CD into your computer, and then follow the on-screen instructions.

Q. When I double-click the web browser, I am prompted for a username and password. How can I bypass this prompt?

Launch the web browser and perform the following steps (these steps are specific to Internet Explorer but are similar for other browsers):

a. Select **Tools** > **Internet Options**.

b. Click the **Connections** tab.

c. Select **Never dial a connection**.

d. Click **OK**.

Q. The WRP400 does not have a coaxial port for the cable connection.

The WRP400 does not replace your modem. You still need your cable modem in order to use the WRP400. Connect your cable connection to the cable modem, insert the setup CD into your computer, and then follow the on-screen instructions.

Q. The computer cannot connect wirelessly to the network.

Make sure the wireless network name or SSID is the same on both the computer and the WRP400. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the WRP400.

Q. I need to modify the settings on the WRP400.

To access the web-based utility, follow these instructions:

a. Launch the web browser on your computer, and enter the default IP address of the WRP400, 192.168.15.1, in the *Address* field. Then press Enter.

NOTE If you place the WRP400 behind a primary router with the IP address of 192.168.15.1, then the WRP400 will automatically assume a new default IP address, 192.168.16.1.

b. A login screen appears. The first time you open the web-based utility, use the default user name and password, **admin**. (You can set a new password from the Administration tab's Management screen.) Then click OK.

c. Click the appropriate tab to change the settings.

Q. I cannot configure the settings for the second wireless network because the SSID2 settings are grayed out.

Your service provider may control the settings for the second wireless network (SSID2). Contact your service provider for more information.

Q. I upgraded my firmware and now the WRP400 is not working properly.

If the WRP400 is not working properly after an upgrade, you may need to perform a factory reset. There are two ways to perform a factory reset.

- Option 1: Press and hold the reset button located on the side panel for approximately ten seconds.
- Option 2: Access the web-based utility and browse to **Administration > Factory Defaults.** Select **Yes** to reset the WRP400 settings to the default values.

NOTE Service Providers: If version 2.0 or higher is installed, and you want to downgrade a device to version 1.0, first downgrade to version 1.0 1.00. Then downgrade to version 1.0. This interim firmware is designed to ensure that the version 2.0 settings are reconfigured for version 1.0.

Mobile Network Troubleshooting

Q. What do I do if the WRP400 does not recognize my USB device?

a. Make sure that you have the latest mobile-support firmware loaded on your WRP400. To download the latest firmware, go to the WRP400 product page on www.cisco.com/en/US/products/ps10028/index.html

b. Make sure that your USB device is on the list of supported Mobile Broadband USB Modems. For more information, visit the WRP400 product page on www.cisco.com/en/US/products/ps10028/index.html

c. If you're installing a Mobile Broadband USB modem, make sure that your modem is activated with a data service, and verify that it can be used on your computer.

Q. The Power LED is continuously flashing green and orange. What does it mean?

When you plug in a USB device, the Power LED indicates the progress of initialization. After successful initialization, the Power LED shines steady green.

If the device fails to initialize, the LED continues to flash green and orange. In this case, check to make sure that you have the latest firmware, that your USB device is supported, and that your modem is activated with a data service, as described above.

Q. My WRP400's Power LED continuous flashing orange. What does it mean?

When a USB modem is installed, the Power LED indicates the status of the mobile network connection. Continuous flashing orange means the router failed to connect to the Internet through the mobile network connection and is trying again. One possible explanation is that the router cannot get a strong signal from the mobile network. Consider moving the router to a location where you have a stronger signal. The Power LED shines steady orange upon a successful mobile network connection,

Q. Q. I am unable to connect to the mobile network. What do I do?

a. Make sure that you have the latest mobile-support firmware loaded on your WRP400. To download the latest firmware, go to the WRP400 product page on www.cisco.com/en/US/products/ps10028/index.html

b. Make sure that your USB device is on the list of supported Mobile Broadband USB Modems. For more information, visit the WRP400 product page on www.cisco.com/en/US/products/ps10028/index.html

c. If you're installing a Mobile Broadband USB modem, make sure that your modem is activated with a data service, and verify that it can be used on your computer.

d. Some mobile network service providers require that you enter specific information such as APN, Dial Number, User Name, and Password. This information can be obtained from your service provider, if required. Log on to the WRP400 administration web server and input the correct settings on the Setup > Mobile Network page, the Mobile Network Setup section.

e. Make sure that you input the correct SIM PIN if you lock your SIM with a PIN code.

Q. How do I disconnect from the mobile broadband network, when not in use?

Disconnecting from your mobile broadband service when not in use may provide savings on usage costs or prevent unnecessary downloads. To disconnect, you can use one of the following methods:

- Option 1: Physically remove and reinsert your Mobile Broadband USB modem from the WRP400.
- Option 2: Log on to the WRP400 web-based utility. Click Setup tab > Mobile Network page. Click the **Disconnect** button.

NOTE The Disconnect button appears only when Connect mode is set on Manual. For more information, see **"Setup > Connection Recovery," on page 46**.

Q. Why does my WRP400 always use my Ethernet connection instead of my mobile network connection?

By default, the WRP400 connects to the Internet through the Ethernet interface, if available. The mobile network connection may be used as a failover when an Ethernet connection is unavailable. If you wish to connect to mobile network only, simply unplug your Ethernet cable. Alternatively, change the Priority setting so that the mobile network connection is used even when the Ethernet cable is connected. To change these settings, log on to the WRP400 web-based utility and use the Setup tab > Mobile Network page and the Setup tab > Ethernet Recovery page. For more information, see **"Setup > Mobile Network," on page 43** and **"Setup > Connection Recovery," on page 46**.

Q. How do you know which mobile network you are using?

Follow these instructions:

a. Open a web browser.

b. Enter the IP address of the WRP400 in the Address field (the default IP address is 192.168.15.1). Then press **Enter**.

c. When prompted, complete the User name and Password fields (the default user name and password is **admin**). Click **OK**.

d. Click the **Status** tab.

e. Click the **Mobile Network** tab. In the Mobile Network Status section, on the Carrier line, you will see the name of the network that you are currently using.

Q. Can I make a VoIP call over the mobile broadband network?

If the WRP400 is configured to use a Mobile Broadband USB modem and voice services with an Internet telephony service provider, the WRP400 can send and receive voice traffic over the mobile broadband network. However, because a voice service is more sensitive to latency and network congestion compared to data services, your voice quality over the mobile network cannot be guaranteed.

Q. What if my Mobile Broadband USB modem is not supported on the WRP400?

Cisco is continuously adding support for more Mobile Broadband USB modems and works closely with mobile broadband providers and manufacturers to stay current with the latest devices available. For a current list of supported Mobile Broadband USB Modems, visit the WRP400 product page at www.cisco.com/en/US/products/ps10028/index.html

B

Specifications

Data Networking	MAC Address (IEEE 802.3)
	IPv4 - Internet Protocol v4 (RFC 791) upgradeable to v6 (RFC 1883)
	ARP - Address Resolution Protocol
	DNS - A Record (RFC 1706), SRV Record (RFC 2782)
	DHCP Client - Dynamic Host Configuration Protocol (RFC 2131)
	DHCP Server - Dynamic Host Configuration Protocol (RFC 2131)
	PPPoE Client - Point to Point Protocol over Ethernet (RFC 2516)
	ICMP - Internet Control Message Protocol (RFC792)
	TCP - Transmission Control Protocol (RFC793)
	UDP - User Datagram Protocol (RFC768)
	RTP - Real Time Protocol (RFC 1889) (RFC 1890)
	RTCP - Real Time Control Protocol (RFC 1889)
	TFTP
	RTSP
	HTTP
	NAT (RFC 1631)
	Reverse NAT
	SDP
	Type of Service - TOS (RFC 791/1349)
	SNTP - Simple Network Time Protocol (RFC 2030)
	QoS - Packet Prioritization by Type
	MAC Address Cloning
	Port Forwarding
	IP Multicast / IGMP v1/v2/v3 / IGMP proxy / IGMP Immediate Leave

Voice Features	Voice Algorithms ▪ G.711 (a-law and µ-Law) ▪ G.726 (16/24/32/40 kbps) ▪ G.729 AB Call Forwarding: No Answer/Busy/Unconditional Support for two simultaneous calls, including G.729 SIP TLS (Transport Layer Security) Call Transfer Call Waiting/Hold/Retrieve Three-way Conferencing Call ID number & name (primary line & on Call waiting) Caller ID Block (prevent sending of caller ID) Anonymous Call Blocking Distinctive ringing Do not Disturb Setting Repeat Dialing on Busy Call Return Emergency Call Support Dial plan Speed Dial In-Band/ SIP-INFO DTMF Translation
Voice RFCs Compliance	RFC 3261 (SIP: Session Initiation Protocol) RFC 3262 (PRACK : Provisional Response ACK) RFC 3263 (Locating SIP Servers) RFC 3264 (SDP Answer and Offer) RFC 3265 (SIP Specific Event Notification) RFC 3550 (RTP: Real Time Protocol) RFC 3551 (RTP: Real Time Protocol for AVP) RFC 2327 (SDP: Session Description Protocol) RFC 3428 (SIP Extensions for Instant Messaging) RFC 3261 (SIP: Session Initiation Protocol) RFC 3262 (PRACK : Provisional Response ACK) RFC 3263 (Locating SIP Servers)

Voice RFCs Compliance continued	RFC 3264 (SDP Answer and Offer) RFC 3265 (SIP Specific Event Notification) RFC 3550 (RTP: Real Time Protocol) RFC 3551 (RTP: Real Time Protocol for AVP) RFC 2327 (SDP: Session Description Protocol) RFC 3428 (SIP Extensions for Instant Messaging) RFC 3515 (SIP Refer) RFC 3581 (SIP Extensions for Symmetric Response Routing) RFC 3842 (SIP Message Summary and Message Waiting Indication) RFC 3856 (SIP Presence Event Package) RFC 3891 (SIP "Replaces" Header) RFC 4028 (SIP Session Timers) RFC 2976 (SIP INFO) RFC 2617 (HTTP Authentication : Basic and Digest Access Authentication) RFC 3325 (Private Extensions to the SIP for Asserted Identity within Trusted Network) RFC 3489 (STUN) RFC 3863 (Presence Event Package for SIP) RFC 3428 (SIP Extension for Instant Messaging (Message Method)) RFC 3665 (SIP Basic Call Flow Example) RFC 4235 (An Invite - Initiated Dialog Event Package for SIP) RFC 3339 (Date and Time on the Internet : Timestamps) RFC 3362 (Support of T.38 in SIP) Only sdPv2 RFC 3892 (SIP Referred-By Mechanism) RFC 3555 (MIME Type Registration of RTP Payload Formats) RFC 2782 (A DNS RR for specifying the location of services (DNS SRV)) RFC 4235 (An INVITE-Initiated Dialog Event Package for SIP) RFC 3455 (Private Header (P-Header) Extensions to SIP for 3GPP) RFC 3323 (A Privacy Mechanism for SIP) RFC 3420 (Internet Media Type Message/Sipfrag) RFC 2833 (RTP Payload for DTMF, Telephone Tone and Signals) RFC 3711 (SRTP)

Voice RFCs Compliance continued	RFC 2396 (URI : Generic Identifier) Draft-ieft-mmusic-media-loopback-04.txt (Media Loopback) Draft-ietf-sip-privacy-04.txt (Remote-party ID)
Provisioning, Administration and Maintenance:	Web Browser Administration & Configuration via Integral Web Server Telephone Key Pad Configuration with Interactive Voice Prompts Provisioning/Configuration/Authentication via HTTPS, HTTP, TFTP Provisioning Support for Configuring Router/Data and Voice Parameters Asynchronous Notification of Upgrade Availability via NOTIFY Non-intrusive, In-Service Upgrades Report Generation & Event Logging Stats in BYE Message Syslog & Debug Server Records Per Line and Purpose Configurable Syslog and Debug Options
Physical Interfaces:	4 100baseT RJ-45 Ethernet LAN Port (IEEE 802.3u) 1 100baseT RJ-45 Ethernet WAN Port (IEEE 802.3u) 2 RJ-11 FXS Phone Ports - For Analog Circuit Telephone Device USB 2.0 for Mobile Broadband Connection modems (available separately)
Buttons	Reset, WPS
Subscriber Line Interface Circuit (SLIC)	Ring Voltage: 40-55 Vrms Ring Frequency: 10 Hz ~ 40Hz Ring Waveform: Trapezoidal and Sinosoidal Maximum Ringer Load: 3 REN On-hook/off-hook Characteristics: ▪ On-hook voltage (tip/ring): - 46 ~ -56V ▪ Off-hook current: 18 ~ 20mA Frequency Response: 300 – 3400Hz Terminating Impedance : 8 Configurable Settings including North America 600 ohms, European CTR21
Regulatory Compliance:	FCC (Part 15 Class B), CE, ICES-003, RoHS, UL, A-Tick, NZ Telepermit, CB
Number of Antennas	1
Connector Type	Fixed

Detachable Antenna	No
RF Pwr (EIRP) in dBm	Average, not including antenna: 802.11g: Typ. 18 dBm @ Normal Temp Range(with PA) 802.11b: Typ: 20 dBm @ Normal Temp Range (with PA)"
Antenna Gain in dBi	2 dBi
UPnP able/cert	Yes
Power Supply	Switching Type (100-240v) Automatic DC Input Voltage: +5 VDC at 2.0 A Max. Power Consumption: 7.9 WATTs (Average) Power Adapter: 100-240v - 50-60Hz (26-34VA) AC Input, 1.8m cord
Indicator Lights/LED	Power, Ethernet 1-4, Wireless, Phone 1, Phone 2, Internet, WPS
Documentation	Quick Installation and User Guide are downloaded from www.cisco.com/go/smallbiz SPA ATA Administration Guide - Service Providers Only Provisioning Guide - Service Providers Only
Security features	"Password protected configuration for web & voice access Stateful Packet Inspection (SPI) Firewall Protection Denial of Service (DoS) Prevention URL filtering, and keyword, Java, ActiveX, Proxy, Cookie blocking VPN Passthrough for IPSec, PPTP, and L2TP Protocols Access restriction by MAC and IP addresses MAC Filtering Security Feature SSID Broadcast Disable 64, 128 bits WEP with Passphrase WEP key generation Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2) Wi-Fi Protected Setup (WPS)"
Security key bits	64, 128
Environmental	
Device Dimensions	WidthHeightDepthWeight Metric14014027mm0.285 kg English5.515.511.06inches0.63 lbs or 10.05 oz
Power	External, Switching 5VDC 2A
Certification	FCC, CE, CB, IC, UL, Wi-Fi (802.11b + WPA2, 802.11g + WPA2, WMM, WPS)

Operating Temperature	0° C to 40° C (32° F to 104° F)
Storage Temperature	-20° C to 60° C (-4° F to 140° F)
Operating Humidity	10% to 85% relative humidity, Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

NOTE Many specifications are programmable within a defined range or list of options. Please see the *ATA Administration Guide* for details. The target configuration profile is uploaded to the WRP400 at the time of provisioning.

NOTE Specifications are subject to change without notice.

C

Regulatory Information

This appendix includes the following regulatory statements:

Federal Communications Commission Interference Statement

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

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 25 cm between the radiator and your body.

This device has been tested and passed co-located EMC / RF exposure test with the following three 3G cards, as described in this filing. Other 3G cards with substantially similar physical dimensions, construction, and electrical and RF characteristics may or may not comply with FCC rule, please consult manufacture before purchase.

Item	Brand Name	Model Name	FCC ID
1	Sierra Wireless, Inc.	AirCard 595U	N7N-MC5725U
2	Novatel Wireless, Inc.	U720	PKRNVWMCD3000
3	Novatel Wireless, Inc.	U727	PKRNVWMCD727

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. IEEE 802.11b or 802.11g operation of this product in the USA is firmware-limited to channels 1 through 11.

Safety Notices and Information

CAUTION:

- To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

WARNING: This product contains lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

WARNING: This equipment will be inoperable when main power fails.

WARNING: Many Internet phone service providers do not support calls to emergency service numbers (000 in Australia or 111 in New Zealand). An alternative phone should be used to make emergency calls.

Regulatory Information

C

WARNING: To ensure compliance with explosure limits to radiofrequency fields, the antenna of the WRP400 should be no closer than 20 cm from the body during use.

Industry Canada Statement

This device complies with Industry Canada ICES-003 rule.

Operation is subject to the following two conditions:

1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Industry Canada Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 25 cm between the radiator & your body.

This device has been tested and passed co-located EMC / RF exposure test with the following three 3G cards, as described in this filing. Other 3G cards with substantially similar physical dimensions, construction, and electrical and RF characteristics may or may not comply with FCC rule, please consult manufacture before purchase.

Item	Brand Name	Model Name	FCC ID
1	Sierra Wireless, Inc.	COMPASS 597	N7NC597
2	Novatel Wireless, Inc.	U720	PKRNVWMCD3000
3	Novatel Wireless, Inc.	U727	PKRNVWMC727

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Avis d’Industrie Canada

Cet appareil numérique de la classe B est conforme aux normes NMB-003 et RSS210 du Canada.

L’utilisation de ce dispositif est autorisée seulement aux conditions suivantes :

1. il ne doit pas produire de brouillage et
2. il doit accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.
   Afin de réduire le risque d’interférence aux autres utilisateurs, le type d’antenne et son gain doivent être choisis de façon à ce que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne soit pas supérieure au niveau requis pour obtenir une communication satisfaisante.

Avis d’Industrie Canada concernant l’exposition aux radiofréquences :

Ce matériel est conforme aux limites établies par IC en matière d’exposition aux radiofréquences dans un environnement non contrôlé. Ce matériel doit être installé et utilisé à une distance d’au moins 25 cm entre l’antenne et le corps de l’utilisateur.

L’émetteur ne doit pas être placé près d’une autre antenne ou d’un autre émetteur, ou fonctionner avec une autre antenne ou un autre émetteur.

Wireless Disclaimer

The maximum performance for wireless is derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

Avis de non-responsabilité concernant les appareils sans fil

Les performances maximales pour les réseaux sans fil sont tirées des spécifications de la norme IEEE 802.11. Les performances réelles peuvent varier, notamment en fonction de la capacité du réseau sans fil, du débit de la transmission de données, de la portée et de la couverture. Les performances dépendent de facteurs, conditions et variables multiples, en particulier de la distance par rapport au point d'accès, du volume du trafic réseau, des matériaux utilisés dans le bâtiment et du type de construction, du système d'exploitation et de la combinaison de produits sans fil utilisés, des interférences et de toute autre condition défavorable.

Telepermit Statement

The cabling between the phone port and the phone shall not exceed 100 metres.

Statement 287—Declaration of Conformity to R&TTE Directive 1999/5/EC for the European Community, Switzerland, Norway, Iceland and Liechtenstein

English: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Български: [Bulgarian]: Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/EC.

Česky [Czech]: Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.

Dansk [Danish]: Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.

Deutsch [German]: Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.

Eesti [Estonian]: See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.

Español [Spanish]: Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.

Ελληνική [Greek]: Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.

Français [French]: Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.

Íslenska [Icelandic]: Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.

Italiano [Italian]: Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.

Latviski [Latvian]: Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

Lietuvių [Lithuanian]: Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.

Nederlands [Dutch]: Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.

Malti [Maltese]: Dan l-apparat huwa konformi mal-htigiet essenzjali u l-provedimenti l-ohra rilevanti tad-Direttiva 1999/5/EC.

Magyar [Hungarian]: Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.

Norsk [Norwegian]: Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.

Polski [Polish]: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.

Português [Portuguese]: Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.

Română [Romanian]: Acest echipament este in conformitate cu cerintele esentiale si cu alte prevederi relevante ale Directivei 1999/5/EC.

Slovensko [Slovenian]: Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.

Slovensky [Slovak]: Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.

Suomi [Finnish]: Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.

Svenska [Swedish]: Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

Ελληνική Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις υσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.

Български: Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/EC.

Česky Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.

Ελληνική Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις υσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.

Latviski Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

Lietuvių Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.

Malti Dan l-apparat huwa konformi mal-htigiet essenzjali u l-provedimenti l-ohra rilevanti tad-Direttiva 1999/5/EC.

Magyar Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.

Polski Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.

Română	**Acest echipament este in conformitate cu cerintele esentiale si cu alte prevederi relevante ale Directivei 1999/5/EC.**
Suomi	**Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.**
Svenska	**Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.**

For all products, the Declaration of Conformity (DofC) is available through one or more of these options:

- A pdf file is included on the product's CD.
- A print copy is included with the product.
- A pdf file is available on the product's webpage. Visit www.cisco.com/go/smallbusiness.

If you need any other technical documentation, see **Appendix E, "Additional Information."**.

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 300 328 and/or EN 301 893 as applicable
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950 and either EN 50385 or EN 50371

Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) are required for operation in the 5 GHz band.

DFS: The equipment meets the DFS requirements as defined in ETSI EN 301 893. This feature is required by the regulations to avoid interference with Radio Location Services (radars).

TPC: For operation in the 5 GHz band, the maximum power level is 3 dB or more below the applicable limit. As such, TPC is not required.

CE Marking

For the Wireless-N, -G, -B, and/or -A products, the following CE mark, notified body number (where applicable), and class 2 identifier are added to the equipment.

CE 0560 (!)

or

CE 0678 (!)

or

CE 0336 (!)

or

CE (!)

Check the CE label on the product to find out which notified body was involved during the assessment.

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1999/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2,4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). The table labeled "Overview of Regulatory Requirements for Wireless LANs" provides an overview of the regulatory requirements applicable for the 2,4- and 5-GHz bands.

Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

C

The requirements for any country may evolve. Cisco recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

Table 1 Overview of Regulatory Requirements for Wireless LANs

Frequency Band (MHz)	Max Power Level (EIRP) (mW)	Indoor ONLY	Indoor & Outdoor
2400-2483.5	100		X
5150-5350*	200	X	
5470-5725*	1000		X

*Dynamic Frequency Selection and Transmit Power Control are required in the frequency ranges of 5250-5350 MHz and 5470-5725 MHz.

The following countries have restrictions and/or requirements in addition to those given in the **"Overview of Regulatory Requirements for Wireless LANs"** table:

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

France

For 2,4 GHz, the product should not be used outdoors in the band 2454 - 2483,5 MHz. There are no restrictions when used in other parts of the 2,4 GHz band when used indoors. Check http://www.arcep.fr/ for more details.

Pour la bande 2,4 GHz, l' équipement ne doit pas être utilisé en extérieur dans la bande 2454 - 2483,5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur dans d'autres parties de la bande 2,4GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

Table 2 Applicable Power Levels in France

Location	Frequency Range (MHz)	Power (EIRP)
Indoor (No restrictions)	2400-2483.5	100 mW (20 dBm)
Outdoor	2400-2454 2454-2483.5	100 mW (20 dBm) 10 mW (10 dBm)

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this 2,4-GHz wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.comunicazioni.it/it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2,4 GHz richiede una "Autorizzazione Generale". Consultare http://www.comunicazioni.it/it/ *per maggiori dettagli.*

Latvia

The outdoor usage of the 2,4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2,4 GHz frekveu joslas izmantošanai rpus telpm nepieciešama atauja no Elektronisko sakaru direkcijas. Vairk informcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

Product Usage Restrictions

This product is designed for indoor usage only. Outdoor usage is not recommended, unless otherwise noted.

2,4 GHz Restrictions

This product is designed for use with the standard, integral or dedicated (external) antenna(s) that is/are shipped together with the equipment. However, some applications may require the antenna(s), if removable, to be separated from the product and installed remotely from the device by using extension cables. For these applications, Cisco offers an R-SMA extension cable (AC9SMA) and an R-TNC extension cable (AC9TNC). Both of these cables are 9 meters long and have a cable loss (attenuation) of 5 dB. To compensate for the attenuation, Cisco also offers higher gain antennas, the HGA7S (with R-SMA connector) and HGA7T (with R-TNC connector). These antennas have a gain of 7 dBi and may only be used with either the R-SMA or R-TNC extension cable.

Combinations of extension cables and antennas resulting in a radiated power level exceeding 100 mW EIRP are illegal.

Third-Party Software or Firmware

The use of software or firmware not supported/provided by Cisco may result that the equipment is no longer compliant with the regulatory requirements.

User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

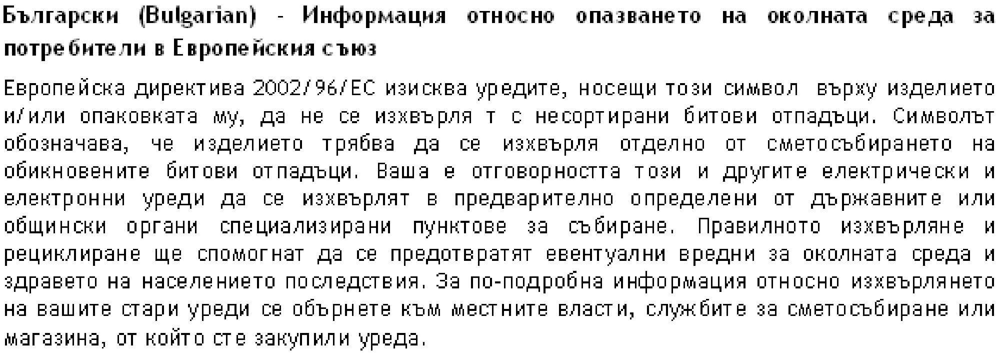
This document contains important information for users with regards to the proper disposal and recycling of Cisco products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:

Regulatory Information

C

English - Environmental Information for Customers in the European Union

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.



Български (Bulgarian) - Информация относно опазването на околната среда за потребители в Европейския съюз

Европейска директива 2002/96/EC изисква уредите, носещи този символ върху изделието и/или опаковката му, да не се изхвърля т с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от сметосъбирането на обикновените битови отпадъци. Ваша е отговорността този и другите електрически и електронни уреди да се изхвърлят в предварително определени от държавните или общински органи специализирани пунктове за събиране. Правилното изхвърляне и рециклиране ще спомогнат да се предотвратят евентуални вредни за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обърнете към местните власти, службите за сметосъбиране или магазина, от който сте закупили уреда.

Ceština (Czech) - Informace o ochran životního prostedí pro zákazníky v zemích Evropské unie

Evropská smrnice 2002/96/ES zakazuje, aby zaízení oznaené tímto symbolem na produktu anebo na obalu bylo likvidováno s netídným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován oddlen od bžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zaízení prostednictvím urených sbrných míst stanovených vládou nebo místními úady. Správná likvidace a recyklace pomáhá pedcházet potenciálním negativním dopadm na životní prostedí a lidské zdraví. Podrobnjší informace o likvidaci starého vybavení si laskav vyžádejte od místních úad, podniku zabývajícího se likvidací komunálních odpad nebo obchodu, kde jste produkt zakoupili.

Dansk (Danish) - Miljøinformation for kunder i EU

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Deutsch (German) - Umweltinformation für Kunden innerhalb der Europäischen Union

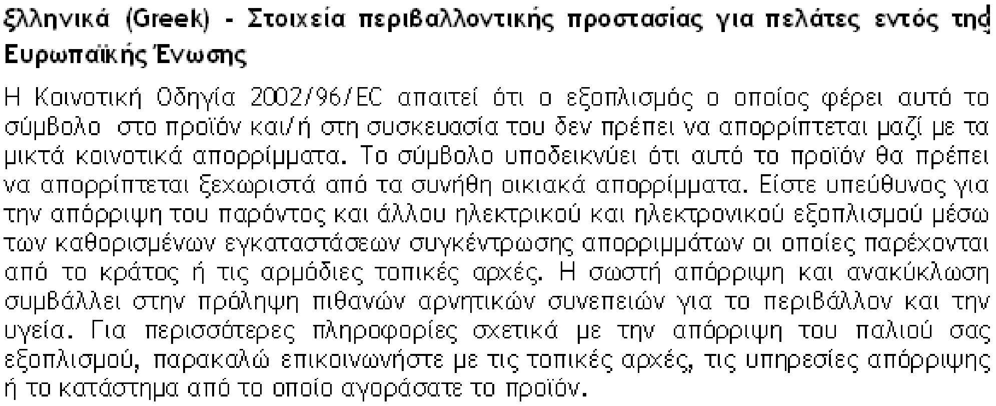
Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist , nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben**.**

Eesti (Estonian) - Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol , keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español (Spanish) - Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.



ξλληνικά (Greek) - Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινοτικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français (French) - Informations environnementales pour les clients de l’Union européenne

La directive européenne 2002/96/CE exige que l’équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L’élimination et le recyclage en bonne et due forme ont pour but de lutter contre l’impact néfaste potentiel de ce type de produits sur l’environnement et la santé publique. Pour plus d’informations sur le mode d’élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l’endroit où vous avez acheté le produit.

Italiano (Italian) - Informazioni relative all’ambiente per i clienti residenti nell’Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull’imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l’ambiente e per la salute dell’essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda (Latvian) - Ekoloiska informcija klientiem Eiropas Savienbas jurisdikcij

Direktv 2002/96/EK ir prasba, ka aprkojumu, kam pievienota zme uz paša izstrdjuma vai uz t iesaiojuma, nedrkst izmest neširot veid kop ar komunlajiem atkritumiem (tiem, ko rada vietji iedzvotji un uzmumi). Š zme nozm to, ka š ierce ir jizmet atkritumos t, lai t nenonktu kop ar parastiem mjsaimniecbas atkritumiem. Jsu pienkums ir šo un citas elektriskas un elektroniskas ierces izmest atkritumos, izmantojot pašus atkritumu savkšanas veidus un ldzekus, ko nodrošina valsts un pašvaldbu iestdes. Ja izmešana atkritumos un prstrde tiek veikta pareizi, tad mazins iespjamais kaitjums dabai un cilvku veselbai. Skkas zias par novecojuša aprkojuma izmešanu atkritumos js varat saemt vietj pašvaldb, atkritumu savkšanas dienest, k ar veikal, kur iegdjties šo izstrdjumu.

Lietuvškai (Lithuanian) - Aplinkosaugos informacija, skirta Europos Sjungos vartotojams

Europos direktyva 2002/96/EC numato, kad rangos, kuri ir kurios pakuot yra pažymta šiuo simboliu (veskite simbol), negalima šalinti kartu su neršiuotomis komunalinmis atliekomis. Šis simbolis rodo, kad gamin reikia šalinti atskirai nuo bendro buitini atliek srauto. Js privalote užtikrinti, kad ši ir kita elektros ar elektronin ranga bt šalinama per tam tikras nacionalins ar vietins valdžios nustatytas atliek rinkimo sistemas. Tinkamai šalinant ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmoni sveikatai. Daugiau informacijos apie js senos rangos šalinim gali pateikti vietins valdžios institucijos, atliek šalinimo tarnybos arba parduotuvs, kuriose sigijote t gamin.

Malti (Maltese) - Informazzjoni Ambjentali gal Klijenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart muniipali li ma iex isseparat. Is-simbolu jindika li dan il-prodott gandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegek li tarmi dan it-tagmir u kull tagmir ieor ta' l-elettriku u elettroniku permezz ta' failitajiet ta' bir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riikla jgin jipprevjeni konsegwenzi negattivi potenzjali gall-ambjent u gas-saa tal-bniedem. Gal aktar informazzjoni dettaljata dwar ir-rimi tat-tagmir antik tiegek, jekk jogbok ikkuntattja lill-awtoritajiet lokali tiegek, is-servizzi gar-rimi ta' l-iskart, jew il-anut minn fejn xtrajt il-prodott.

Magyar (Hungarian) - Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektõl elkülönített eljárást kell alkalmazni. Az Ön felelõssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyjtõredszereken keresztül számolja fel. A megfelelõ hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelõzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

Nederlands (Dutch) - Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk (Norwegian) - Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski (Polish) - Informacja dla klientów w Unii Europejskiej o przepisach dotyczcych ochrony rodowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzt oznaczony symbolem znajdujcym si na produkcie i/lub jego opakowaniu nie by wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, e produkt nie powinien by usuwany razem ze zwykymi odpadami z gospodarstw domowych. Na Pastwu spoczywa obowizek wyrzucania tego i innych urzdze elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez wadze krajowe lub lokalne. Pozbywanie si sprztu we waciwy sposób i jego recykling pomog zapobiec potencjalnie negatywnym konsekwencjom dla rodowiska i zdrowia ludzkiego. W celu uzyskania szczegóowych informacji o usuwaniu starego sprztu, prosimy zwróci si do lokalnych wadz, sub oczyszczania miasta lub sklepu, w którym produkt zosta nabyty.

Português (Portuguese) - Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através das instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Român (Romanian) - Informaii de mediu pentru clienii din Uniunea European

Directiva european 2002/96/CE impune ca echipamentele care prezint acest simbol pe produs i/sau pe ambalajul acestuia s nu fie casate împreun cu gunoiul menajer municipal. Simbolul indic faptul c acest produs trebuie s fie casat separat de gunoiul menajer obinuit. Este responsabilitatea dvs. s casai acest produs i alte echipamente electrice i electronice prin intermediul unitilor de colectare special desemnate de guvern sau de autoritile locale. Casarea i reciclarea corecte vor ajuta la prevenirea potenialelor consecine negative asupra sntii mediului i a oamenilor. Pentru mai multe informaii detaliate cu privire la casarea acestui echipament vechi, contactai autoritile locale, serviciul de salubrizare sau magazinul de la care ai achiziionat produsul.

Slovenina (Slovak) - Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Poda európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie by likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidova oddelene od bežného odpadu z domácností. Je vašou povinnosou likvidova toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení urených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabráni prípadným negatívnym dopadom na životné prostredie a zdravie udí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenina (Slovene) - Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, oznaene s tem simbolom – na izdelku in/ali na embalaži – med obiajne, nerazvršene odpadke. Ta simbol opozarja, da je treba izdelek odvrei loeno od preostalih gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo elektrino in elektronsko opremo odnesete na posebna zbirališa, ki jih doloijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste prepreili morebitne škodljive vplive na okolje in zdravje ljudi. e želite izvedeti ve o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi (Finnish) - Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Svenska (Swedish) - Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall. Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

D

Where to Go From Here

This appendix describes additional resources that are available to help you and your customer obtain the full benefits of the SPA9000 Voice System.

Resource	Location
Technical Documentation	www.cisco.com/en/US/products/ps10024/tsd_products_support_series_home.html
Firmware Downloads	www.cisco.com/en/US/products/ps10024/index.html
Customer Support	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Warranty and End User License Agreement	www.cisco.com/go/warranty
Open Source License Notices	www.cisco.com/go/osln
Regulatory Compliance and Safety Information	www.cisco.com/en/US/products/ps10024/tsd_products_support_series_home.html
Cisco Partner Central site for Small Business	www.cisco.com/web/partners/sell/smb