Product Overview and Deployment Guidelines

This chapter describes the features and benefits of the WRP500, describes deployment scenarios, and offers guidelines to help you plan your network.

WRP500 Features and Benefits

With a variety of features, the WRP500 offers the benefits of five devices in one:

- **Router:** The WRP500 is a broadband router with a robust security firewall to protect your network.
- **Switch:** The WRP500 includes a built-in, 4-port, full-duplex, 10/100/1000M Ethernet switch to connect computers, printers, and other equipment directly or to attach additional hubs and switches. Advanced Quality of Service functionality ensures that you can prioritize traffic for data, voice, and video applications.
- **Analog Telephone Adapter:** The WRP500 includes a two-port Analog Telephone Adapter (ATA) that allows you to connect your analog phones or fax machines to your configured Internet telephone service. Two traditional phone lines also can be connected for support of legacy phone numbers and fax numbers.
- **Wireless Access Point:** The WRP500 has an integrated 802.11ac/b/g/n wireless access point that secures your communications with WEP, WPA, and WPA2 security protocols. It is preconfigured to support two wireless networks: one for transferring general data, such as data from a connected PC; and another for transferring data from voice devices, such as audio or fax data.
- **Mobile Broadband Router:** When you attach a compatible Mobile Broadband Modem to the USB port, the WRP500 allows multiple Wi-Fi and Ethernet devices to share a mobile broadband connection. This feature also can be used to provide continuous Internet service by providing automatic failover to the mobile network when the primary Internet connection is unavailable. For the latest copy of the USB Modem Compatibility List, visit the following URL: http://www.cisco.com/c/en/us/products/unified-communications/wrp500-wireless-g-broadband-router-2-phone-ports/index.html

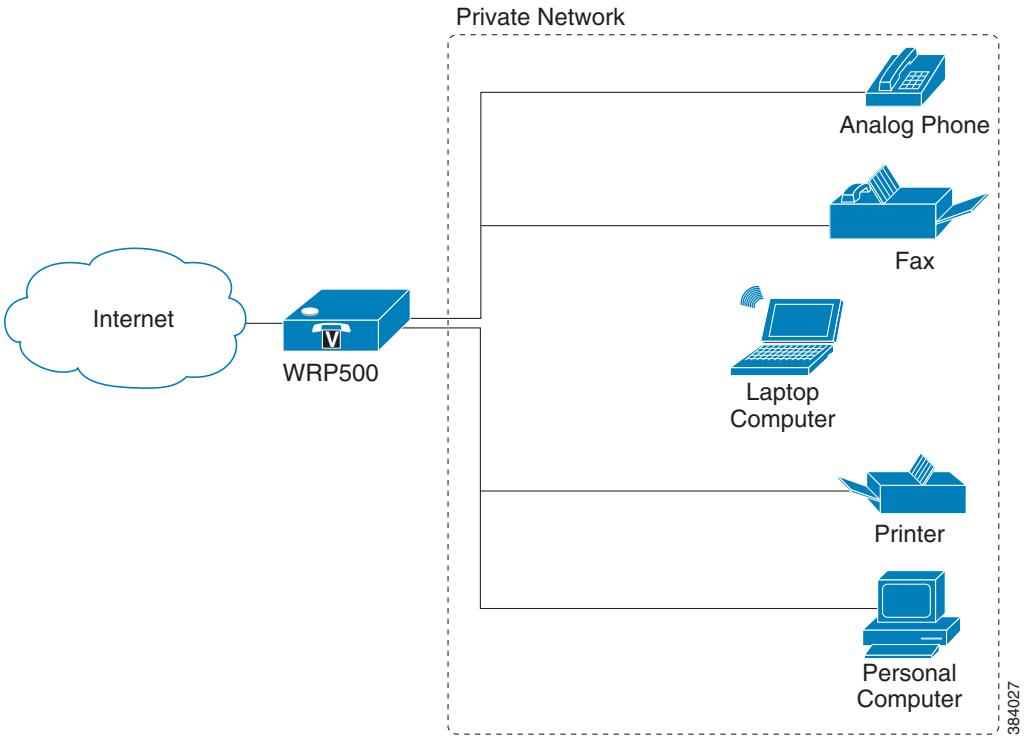
Note Because this device has many unique functions, the administrative tasks for the WRP500 may be different from corresponding tasks on other Cisco Small Business routers, switches, and ATAs. Administrators should refer to this guide for the proper procedures for installation, configuration, and management of the WRP500.

Deployment Models

The versatility of the WRP500 makes it useful for a variety of deployments:

- WRP500 Deployment in a Basic Network, page 1-3
- WRP500 Deployment with a Wireless Guest Network, page 1-4
- WRP500 Deployment with Mobile Broadband, page 1-5

WRP500 Deployment in a Basic Network



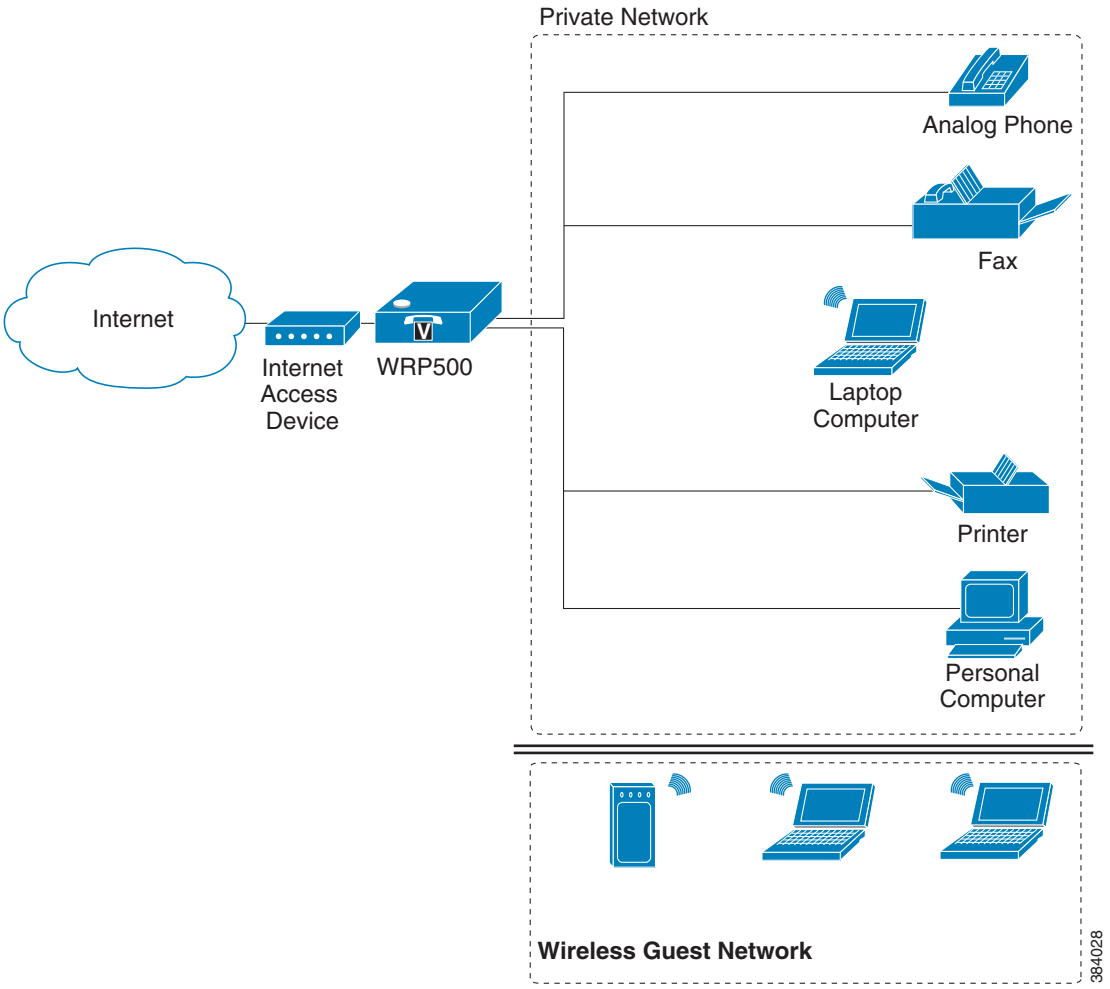
In this scenario, the WRP500 is deployed in a small business that has a basic network configuration.

- The WRP500 is preconfigured by the Service Provider to act as the edge device that routes traffic between the small business network and the Service Provider network.

Note The WRP500 may be configured as an edge device or can be connected to another device that provides access to the Service Provider network.

- The WRP500 connects computers to the Internet. Computers may be connected by network cables or may operate wirelessly. All computers have access to the printer on the local network.
- An analog phone and a fax machine are connected to the WRP500 phone ports and have access to the configured Voice over IP services.

WRP500 Deployment with a Wireless Guest Network



In this example, the WRP500 is deployed in an Internet cafe.

- The WRP500 is connected to a cable modem that provides Internet access.

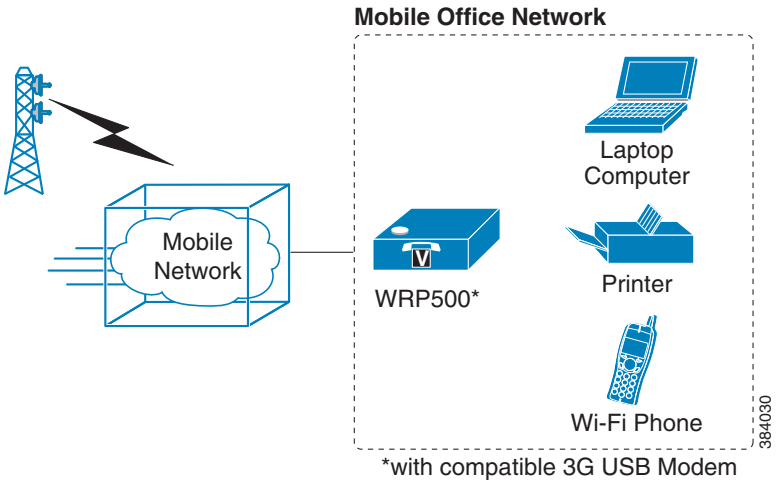
Note The WRP500 may be configured as an edge device or can be connected to another device that provides access to the Service Provider network.

- In the private network, a computer is connected to the WRP500 by an Ethernet cable. The manager also has a laptop computer that can be used wirelessly from anywhere on the premises through the main wireless network, SSID1. The manager and employees who use SSID1 have access to the printer. If desired, a wireless phone can also connect to this network for business use.
- An analog phone and a fax machine are in the private network. The WRP500 is configured for Internet telephone service.
- The WRP500 is configured with a guest network, SSID2, that enables the business to provide its customers with a free wireless hotspot for their laptop computers and other mobile devices. Because this network is separate from the main wireless network, customers have no access to the manager's computer, printer, or telephone service.

WRP500 Deployment with Mobile Broadband

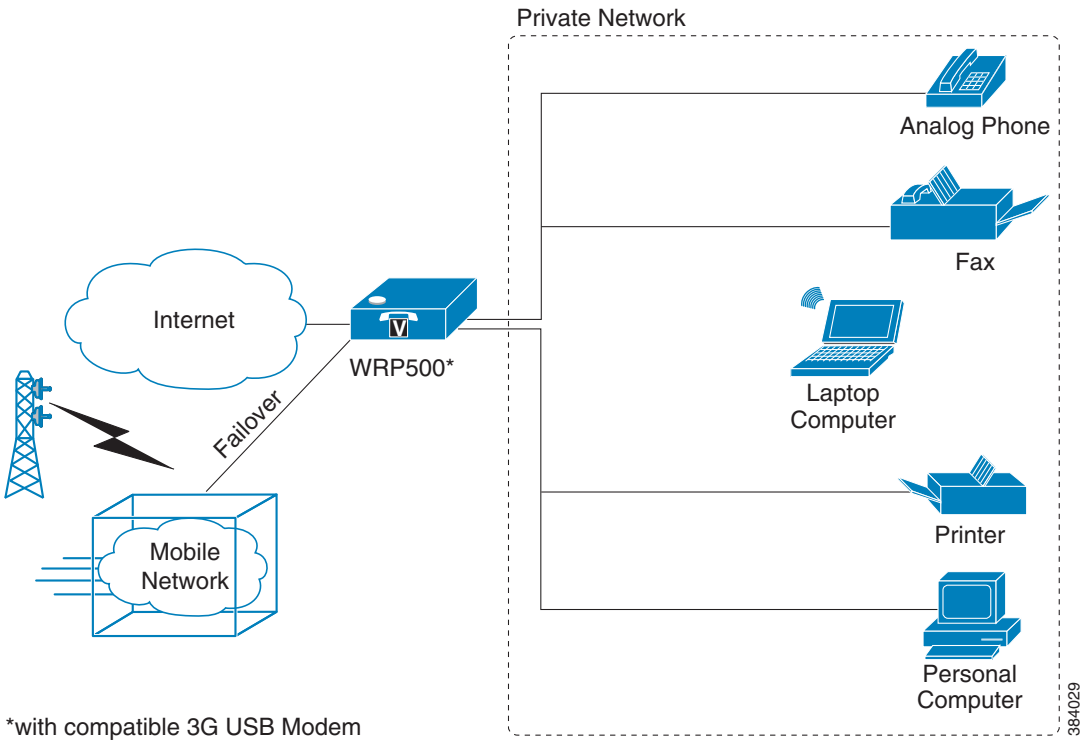
When a compatible mobile broadband modem connects to the USB port, the WRP500 can connect to a mobile broadband network. The mobile network can be the primary network or can serve as a backup network to ensure continuous Internet connectivity. Consider the scenarios that follow.

Mobile Office That Uses the Mobile Network for Internet Access



In this example, a team has set up a temporary network at a construction site. Team members have laptop computers and Wi-Fi phones that share a mobile broadband connection for Internet access. All computers can connect to the printer on the local network. If a Virtual Private Network (VPN) tunnel is configured on the laptop computer, team members also can securely connect to resources at the main office (not illustrated).

Basic Office Deployment That Uses the Mobile Network as a Backup Connection



In this example, the business has the same network as illustrated in the "WRP500 Deployment in a Basic Network" section on page 1-3. However, this business has the added benefit of using the mobile broadband network as a backup network to ensure continuous Internet connectivity. In the event that the Internet connection fails, the WRP500 fails over to the configured mobile network. When the Internet connection becomes available, the WRP500 recovers the connection.

Local Area Network Guidelines

This section offers guidelines for setting up your Local Area Network (LAN).

Note As you design your network, be aware that the WRP500 is intended for deployment in a very small business. The router is designed to handle the data, voice, and video traffic that is expected by office personnel who use the Internet to find data, conduct phone conversations, transmit email, and participate in videoconferences. For large-scale operations with heavy data, voice, and video requirements, consider other models of Cisco Small Business routers.

Power, Cabling, and Telephone Lines

- **AC outlets:** Ensure that an AC outlet is available for every network device that requires AC power.
  - The WRP500 requires power, and Ethernet switches (optional) require power.
  - Some analog telephones require AC power.

- **Ethernet cabling:** If an Internet access device is present, you need to connect it to the WRP500 with an Ethernet cable. You also need Ethernet cable for any devices that do not have wireless connectivity. Ethernet cables that are UTP Cat5e or better are recommended.
- **UPS:** It is strongly recommended that you included an Uninterrupted Power Supply (UPS) mechanism in your network to ensure continuous operation during a power failure. Connect all essential devices, including the Internet access device, the WRP500, and the Ethernet switch (if present).

Basic Services and Equipment

The following basic services and equipment are required:

- An integrated access device or modem for broadband access to the Internet
- Business grade Internet service
- Internet Telephony Service Provider (ITSP) for Voice over IP (VoIP) telephone service that supports a “bring your own device” model
- A computer with Microsoft Windows for system configuration

Special Requirements for Voice Deployments

Voice deployments have special requirements that you must meet to ensure voice quality.

- Bandwidth for Voice Deployments, page 1-7
- NAT Mapping for Voice over IP Deployments, page 1-8
- Local Area Network Design for Voice Deployments, page 1-9

Bandwidth for Voice Deployments

You can choose from several types of broadband access technologies to provide symmetric or asymmetric connectivity to a small business. These technologies vary on the available bandwidth and on the quality of service. For voice deployments, it is generally recommended that you use broadband access with a Service Level Agreement that provides quality of service. If a Service Level Agreement with regard to the broadband connection quality of service is not in place, the downstream audio quality may be affected negatively under heavy load conditions (bandwidth utilization beyond 80%).

To eliminate or minimize this effect, Cisco recommends one of the following actions:

- For broadband connections with a bandwidth lower than 2 Mbps, perform the call capacity calculations by assuming a bandwidth value of 50% of the existing broadband bandwidth. For example, in the case of a 2 Mbps uplink broadband connection, assume 1 Mbps. Limit the uplink bandwidth in the Integrated Access Device to this value. This setting helps to maintain utilization levels below 60%, and thus reduces jitter and packet loss.
- Use an additional broadband connection for voice services only. A separate connection is required when the broadband connection services do not offer quality of service and when it is not possible to apply the above mentioned utilization mechanism.

The available connection bandwidth determines the maximum number of simultaneous calls that the system can support with the appropriate audio quality. Use this information to determine the maximum number of simultaneous VoIP connections that the system can support.

Note Some ITSP SIP trunk services limit the maximum number of simultaneous calls. Please check with your Service Provider to understand the maximum number of simultaneous calls that each SIP trunk supports.

The following table provides the approximate bandwidth budget for different codecs.

Note The Cisco WRP500 supports only the G.711 and G.729 codecs.

Codec	Approximate Bandwidth Budget for Each Side of Conversation	2 Calls	4 Calls	6 Calls	8 Calls
G.711	128 kbps	256 kbps	512 kbps	768 kbps	1024 kbps
G.729	16 kbps	32 kbps	64 kbps	96 kbps	128 kbps

For more information about bandwidth calculation, refer to the following web sites:

www.erlang.com/calculator/lipb/

www.bandcalc.com/

NAT Mapping for Voice over IP Deployments

Network Address Translation (NAT) is the function that allows multiple devices in your small business network to share one external (public) IP address that you receive from your Internet Service Provider. Voice over IP can co-exist with NAT only when some form of NAT traversal is provided.

Some Internet Telephone Service Providers (ITSPs) provide NAT traversal, but some do not. **For voice deployments, it is strongly recommended that you choose an ITSP that supports NAT mapping through a Session Border Controller.**

If your ITSP does not provide NAT mapping through a Session Border Controller (the preferred method), you have these options for providing NAT traversal on your WRP500:

- Deploy an edge device that has a SIP ALG (Application Layer Gateway). The Cisco Small Business WRV200 is suited for this purpose, but other SIP-ALG routers can be used. If your Internet Service Provider provides the edge device, check with your provider to determine whether the router has a SIP ALG.
- Configure NAT mapping with the EXT IP setting. This option requires that you have (1) a static external (public) IP address from your Internet Service Provider and (2) an edge device with a symmetric NAT mechanism. If the WRP500 is the edge device, the second requirement is met. For more information about the EXT IP setting, see the "NAT Support Parameters section" section on page A-10.
- Configure Simple Traversal of UDP through NAT (STUN). This option requires that you have (1) a dynamic external (public) IP address from your service provider, (2) a computer that is running STUN server software, and (3) an edge device with an asymmetric NAT mechanism. If the WRP500 is the edge device, the third requirement *is not* met. For more information about the STUN Enable setting and the STUN Test Enable setting, see the "NAT Support Parameters section" section on page A-10.

Local Area Network Design for Voice Deployments

Use these guidelines to manage the LAN setup for voice deployments:

- Ensure that all telephones are located in the same local area network subnet.
- Configure your WRP500 as a DHCP server for the purpose of easily adding network devices to the system. Ensure that the DHCP server can assign enough IP addresses to serve the devices that you need to connect to your network.
- Use stable DNS server addresses for URL name resolution. Your Internet Service Provider can provide the primary and secondary DNS server IP addresses.
- If you need to connect more than four network devices directly (other than wireless devices), you need to connect an Ethernet switch to the WRP500. For voice deployments, Cisco recommends use of the SLMxxxP, SRWxxxP and SRWxxxMP switch product families. The SLM224P is a popular choice. For more information about these switches, visit the following URL: www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/index.html
- If you use an Ethernet switch, configure it to ensure voice quality. These settings are recommended:
  - Enable Port Fast and Spanning Tree Protocol on the ports to which your voice devices are connected. Cisco phones are capable of rebooting in a few seconds and will attempt to locate network services while a switch port is being blocked by STP after it senses a device reboot. If you enable Port Fast, the network will be available to the phones when it is needed. If the switch does not provide a way to enable Port Fast, you must disable Spanning Tree Protocol.
  - In the administrative web pages for the switch, enable QoS and choose DSCP as the Trust Mode.

WRP500 Maintenance Operations

Due to its unique functions, the WRP500 has unique maintenance operations as compared to other Cisco Small Business IP telephony devices.

- **Remote Management:** For security purposes, remote management is disabled by default.
  - When you first configure the WRP500, connect your administrative computer directly to one of the LAN ports and enter the default static IP address into your web browser to log on to the configuration utility.

    Note The default LAN IP address of the WRP500 is 192.168.15.1. If another device on the network has the same IP address, the WRP500 takes the address 192.168.16.1. To modify the Local IP Address, go to the Interface Setup tab > LAN > DHCP Server section.

    If you are using the IVR, be aware that this address is NOT the address that the 110 option of the IVR reports. The device does not respond to the 110 option address.
  - To enable web access and wireless access to the configuration utility, use the Administration tab > Web Access Management section.
- **DHCP Server:** The DCHP server on LAN ports is enabled by default. This setting is on the Interface Setup tab > LAN > DHCP Server section.
- **System Logging:** To enable system logging, be aware that two sets of system logs exist: one for the data (router) functions and another for the voice functions.

  - **Data (router) logging:** See the Administration tab > Log page.
  - **Voice logging:** See the Voice tab > System page, Miscellaneous Settings section.
- **Factory Reset:** To reset your WRP500 to the factory default settings, reset the data (router) settings and the voice settings separately.

Factory Reset of Data (Router) Settings

Use one of the following methods:

- **Option 1:** Log on to the configuration utility, then click **Administration > Factory Defaults**. Next to **Restore Router Factory Defaults**, click **Yes**. Then click **Submit** to begin the operation.
- **Option 2:** Press and hold the reset button located on the rear panel for approximately ten seconds.

Factory Reset of Voice Settings

Use one of the following methods:

- **Option 1:** Log on to the configuration utility, then click Administration tab > Factory Defaults. Next to **Restore Voice Factory Defaults**, click **Yes**. Then click **Submit** to begin the operation.
- **Option 2:** Connect an analog phone to the Phone 1 or Phone 2 port. Press **** to access the Interactive Voice Response menu. After you hear the greeting, press 73738 for factory reset. Listen to the prompts, then press 1 to confirm or * to cancel.

Remote Provisioning

Like other Cisco Small Business IP Telephony Devices, the WRP500 provides for secure provisioning and remote upgrade. Provisioning is achieved through configuration profiles that are transferred to the device via TFTP, HTTP, or HTTPS. To configure Provisioning, go to the Provisioning tab in the Configuration Utility.

For complete details, see the *Provisioning Guide* at the following URL:

http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/csbpvga/ata/provisioning/guide/Provisioning.pdf

Upgrade URL

Remote firmware upgrade is achieved via TFTP or HTTP/HTTPS. Remote upgrades are initiated by causing the WRP500 to request the upgrade firmware image by providing a URL for the WRP500 to retrieve the firmware.

Note The Upgrade/Resync/Reboot URL works only after the administrator logs in to the web GUI.

Note If the value of the *Upgrade Enable* parameter in the Provisioning page is **No**, you cannot upgrade the WRP500 even if the web page indicates otherwise.

The syntax of the Upgrade URL is as follows:

http://*WRP500_ip_address*/admin/upgrade?[protocol://][server-name[:port]][/firmware-pathname]

HTTP, HTTPS, and TFTP are supported for the upgrade operation.

If no *protocol* is specified, TFTP is assumed.

If no port specified, the default port of the protocol is used (69 for TFTP, 80 for HTTP, or 443 for HTTPS).

The *firmware-pathname* is typically the file name of the binary that is located in a directory on the TFTP, HTTP, or HTTPS server. If no *firmware-pathname* is specified, */spa.bin* is assumed, as in the following example:

http://192.168.2.217/amin/upgrade?tftp://192.168.2.251/spa.bin

Resync URL

The WRP500 can be configured to automatically resync its internal configuration state to a remote profile periodically and on power up. The automatic resyncs are controlled by configuring the desired profile URL into the device.

Note The Upgrade/Resync/Reboot URL works only after the administrator logs in to the web GUI.

The Resync URL lets you force the WRP500 to do a resync to a profile specified in the URL, which can identify either a TFTP, HTTP, or HTTPS server. The syntax of the Resync URL is as follows:

http://*WRP500_ip_address*/admin/resync?[[protocol://][server-name[:port]]/profile-pathname]

Note The WRP500 resyncs only when it is idle.

If no port is specified, the default port is used (69 for TFTP, 80 for HTTP, and 443 for HTTPS).

The profile-path is the path to the new profile with which to resync, for example:

http://192.168.2.217/admin/resync?tftp://192.168.2.251/spaconf.xml

Reboot URL

The Reboot URL lets you reboot the WRP500. The Reboot URL is as follows:

http://*WRP500_ip_address***/admin/reboot**

Note The Upgrade/Resync/Reboot URL works only after the administrator logs in to the web GUI.

Configuration Profile

Because the WRP500 has two sets of parameters, one set for data and one set for voice, the requirements vary from the provisioning of other Cisco Small Business IP Telephony Devices. You will have two profiles: one for the data (router) parameters and one for the voice parameters. One benefit of having separate profiles for voice parameters and data parameters is that you can deploy the common data parameters to all of your customer sites and deploy the custom voice parameters to each site individually.

- **Data (router) parameters:** Use the XML format only, as described in the *Provisioning Guide*
- **Voice parameters:** Use the XML format. The binary format is generated by a profile compiler tool available from Cisco. Find the correct SPA Profiler Compiler (SPC) for the firmware that you have installed on your WRP500. For more information about the data parameters, see Appendix A, "Advanced Voice Fields."

Note You can download the SPC tools at the following URL: http://www.cisco.com/c/en/us/products/unifiedcommunications/wrp500-wireless-ac-broadband-router-2-phone-ports/index.html

XML Format

Use the XML format for data (router) parameters. The XML file consists of a series of elements (one per configuration parameter), encapsulated within the element tags <flat-profile> … </flat-profile>. The encapsulated elements specify values for individual parameters. Here is an example of a valid XML profile:

```
<flat-profile>

<Web_Remote_Management>0</Web_Remote_Management>

<Web_Remote_Upgrade>0</Web_Remote_Upgrade>

</flat-profile>
```

The names of parameters in XML profiles can generally be inferred from the WRP500 Configuration Utility, by substituting underscores (_) for spaces and other control characters. To distinguish between Lines 1, 2, 3, and 4, corresponding parameter names are augmented by the strings _1_, _2_, _3_, and _4_. For example, Line 1 Proxy is named Proxy_1_ in XML profiles.

Binary Format

The WRP500 does not support binary format files.