Cisco WRP500 Administration Guide

Wireless-AC Broadband Router with 2 Phone Ports and Built-In Analog Telephone Adapter

Published: January 30, 2015
Revised: April 29, 2015

Cisco Systems, Inc.
www.cisco.com

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

CHAPTER 1 **Product Overview and Deployment Guidelines** 1-1

- WRP500 Features and Benefits 1-1
- Deployment Models 1-2
  - WRP500 Deployment in a Basic Network 1-3
  - WRP500 Deployment with a Wireless Guest Network 1-4
  - WRP500 Deployment with Mobile Broadband 1-5
    - Mobile Office That Uses the Mobile Network for Internet Access 1-5
    - Basic Office Deployment That Uses the Mobile Network as a Backup Connection 1-6
- Local Area Network Guidelines 1-6
  - Power, Cabling, and Telephone Lines 1-6
  - Basic Services and Equipment 1-7
- Special Requirements for Voice Deployments 1-7
  - Bandwidth for Voice Deployments 1-7
  - NAT Mapping for Voice over IP Deployments 1-8
  - Local Area Network Design for Voice Deployments 1-9
- WRP500 Maintenance Operations 1-9
- Remote Provisioning 1-10
  - Upgrade URL 1-10
  - Resync URL 1-11
  - Reboot URL 1-11
  - Configuration Profile 1-12
    - XML Format 1-12
    - Binary Format 1-12

CHAPTER 2 **Configure Your System for ITSP Interoperability** 2-1

- Configure NAT Mapping 2-1
  - Configure NAT Mapping with a Static IP Address 2-1
  - Configure NAT Mapping with STUN 2-2
  - Determine Whether the Router Uses Symmetric or Asymmetric NAT 2-4
- Firewalls and SIP 2-5
- Configure SIP Timer Values 2-5

CHAPTER 3 **Configure Voice Services** 3-1

Analog Telephone Adapter Operations 3-1

ATA Software Features 3-2

Supported Codecs 3-2

SIP Proxy Redundancy 3-2

Other ATA Software Features 3-3

Register to the Service Provider 3-5

Manage Caller ID Service 3-7

Optimize Fax Completion Rates 3-8

Fax Troubleshooting 3-9

Silence Suppression and Comfort Noise Generation 3-10

Configure Dial Plans 3-10

About Dial Plans 3-10

Digit Sequences 3-11

Digit Sequence Examples 3-12

Acceptance and Transmission of Dialed Digits 3-13

Dial Plan Timer (Off-Hook Timer) 3-14

Interdigit Long Timer (Incomplete Entry Timer) 3-15

Interdigit Short Timer (Complete Entry Timer) 3-15

Edit Dial Plans 3-16

Enter the Line Interface Dial Plan 3-16

Reset the Control Timers 3-16

Secure Call Implementation 3-17

Enable Secure Calls 3-17

APPENDIX A **Advanced Voice Fields** A-1

Info page A-1

Product Information section A-1

System Status section A-2

Line Status section A-2

System page A-4

System Configuration section A-4

Miscellaneous Settings section A-5

SIP page A-5

SIP Parameters section A-5

SIP Timer Values (sec) section A-7

Response Status Code Handling section A-8

RTP Parameters section A-8

SDP Payload Types section A-9
NAT Support Parameters section A-10
Regional page A-11
Call Progress Tones section A-12
Distinctive Ring Patterns section A-13
Distinctive Call Waiting Tone Patterns section A-14
Distinctive Ring/CWT Pattern Names section A-15
Control Timer Values (sec) section A-16
Vertical Service Activation Codes section A-17
Outbound Call Codec Selection Codes section A-22
Miscellaneous section A-23
Line page A-24
Line Enable section A-25
Streaming Audio Server (SAS) section A-25
NAT Settings section A-26
Network Settings section A-27
SIP Settings section A-28
Call Feature Settings section A-30
Proxy and Registration section A-31
Subscriber Information section A-32
Supplementary Service Subscription section A-32
Audio Configuration section A-34
Dial Plan section A-36
FXS Port Polarity Configuration section A-38
User page A-38
Call Forward Settings section A-38
Selective Call Forward Settings section A-39
Speed Dial Settings section A-39
Supplementary Service Settings section A-40
Distinctive Ring Settings section A-41
Ring Settings section A-41

APPENDIX B **Data Fields** B-1
Interface Setup module B-1
Interface Setup > WAN page B-1
Interface Setup > WAN > Internet Setup B-1
Interface Setup > WAN > Internet Option B-3
Internet Setup > WAN > Mobile Network B-4
Internet Setup > WAN > Multi-WAN Config B-6

Interface Setup > LAN page B-7
Interface Setup > LAN > DHCP Server B-7
Interface Setup > LAN > VLAN Settings B-9
Interface Setup > LAN > Port Settings B-11
Interface Setup > LAN > STP B-12
Interface Setup > Wi-Fi Settings B-13
Interface Setup > Wi-Fi Settings > Basic Wireless Settings B-13
Interface Setup > Wi-Fi Settings > Wi-Fi Protected Setup B-14
Interface Setup > Wi-Fi Settings > Advanced Wireless Settings B-15
Interface Setup > Wi-Fi Settings > WMM Setting B-16
Interface Setup > Management Interface B-16
Network Setup module B-16
Network Setup > Routing page B-17
Network Setup > Routing > Static Routes > IPv4 B-17
Network Setup > Routing > RIP > IPv4 B-18
Network Setup > Routing > Intervlan Routing B-19
Network Setup > Routing > Policy Routing B-19
Network Setup > NAT B-20
Network Setup > NAT > NAT Setting B-20
Network Setup > NAT > NAT Bypass B-20
Network Setup > NAT > Port Forwarding B-22
Network Setup > NAT > Port Range Triggering B-24
Network Setup > QoS B-25
Network Setup > QoS > QoS Bandwidth Control B-25
Network Setup > QoS > QoS Policy B-25
Network Setup > QoS > CoS To Queue B-29
Network Setup > QoS > DSCP To Queue B-29
Network Setup > Firewall B-29
Network Setup > Firewall > Firewall Filter B-29
Network Setup > Firewall > Firewall Filter B-30
Network Setup > Firewall > IPV4 > Internet Access Control B-30
Network Setup > Firewall > IPV4 > Inbound Access Control B-32
Network Setup > PPPoE Relay B-34
Network Setup > DDNS B-34
Network Setup > DMZ B-35
Network Setup > DMZ > Software DMZ B-35
Network Setup > DMZ > Hardware DMZ B-36
Network Setup > IGMP B-36
Network Setup > UPnP B-36
Network Setup > CDP B-37

Network Setup > DNS Spoofing **B-37**

VPN module **B-38**

VPN > Site to Site IPSec VPN **B-38**

VPN > Site to Site IPSec VPN > NAT Traversal **B-38**

VPN > Site to Site IPSec VPN > IKE Policy **B-38**

VPN > Site to Site IPSec VPN > IPSec Policy **B-39**

VPN > GRE Tunnel **B-41**

VPN > VPN Passthrough **B-42**

VPN > Cisco VPN Server **B-42**

VPN > Cisco VPN Server > Group **B-42**

VPN > Cisco VPN Server > User **B-43**

Administration module **B-44**

Administration > Web Access Management **B-44**

Administration > Remote Support **B-45**

Administration > Remote Management **B-45**

Administration > Remote Management > TR-069 **B-45**

Administration > Remote Management > SNMP **B-46**

Administration > Remote Management > Local TFTP **B-47**

Administration > Time Setup **B-48**

Administration > Certificate Management **B-48**

Administration > User Management **B-49**

Administration > User Management > Password Complexity Settings **B-49**

Administration > User Management > User List **B-50**

Administration > User Privilege Control **B-50**

Administration > Log **B-50**

Administration > Log > Log Setting **B-50**

Administration > Log > Log Module **B-52**

Administration > Log > Log Viewer **B-52**

Administration > Log > Firewall Log **B-52**

Administration > Factory Defaults **B-53**

Administration > Firmware Upgrade **B-54**

Administration > Backup & Restore **B-54**

Administration > Backup & Restore > Default Configuration **B-54**

Administration > Backup & Restore > Backup Configuration **B-54**

Administration > Backup & Restore > Restore Configuration **B-55**

Administration > Reboot **B-55**

Administration > Switch Setting **B-55**

Administration > Switch Setting > Port Status **B-55**

Administration > Switch Setting > Bind MAC to Port **B-55**

Administration > Status **B-57**

APPENDIX C **Troubleshooting** C-1

APPENDIX D **Environmental Specifications for the WRP500** D-1

APPENDIX E **Where to Go From Here** E-1

CHAPTER 1

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, page 1-1
- Deployment Models, page 1-2
- Local Area Network Guidelines, page 1-6
- Special Requirements for Voice Deployments, page 1-7
- WRP500 Maintenance Operations, page 1-9
- Remote Provisioning, page 1-10

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

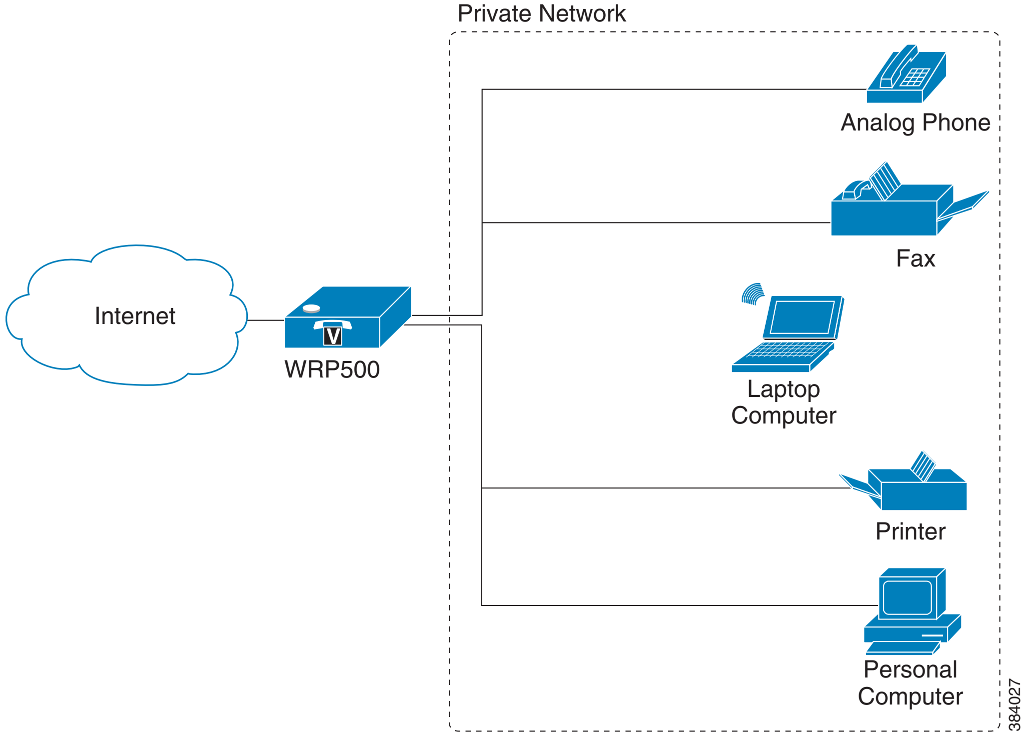
Note Because this device has many unique functions, the administrative tasks for the WRP500 may be different from corresponding tasks on other Cisco Small Business routers, switches, and ATAs. Administrators should refer to this guide for the proper procedures for installation, configuration, and management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



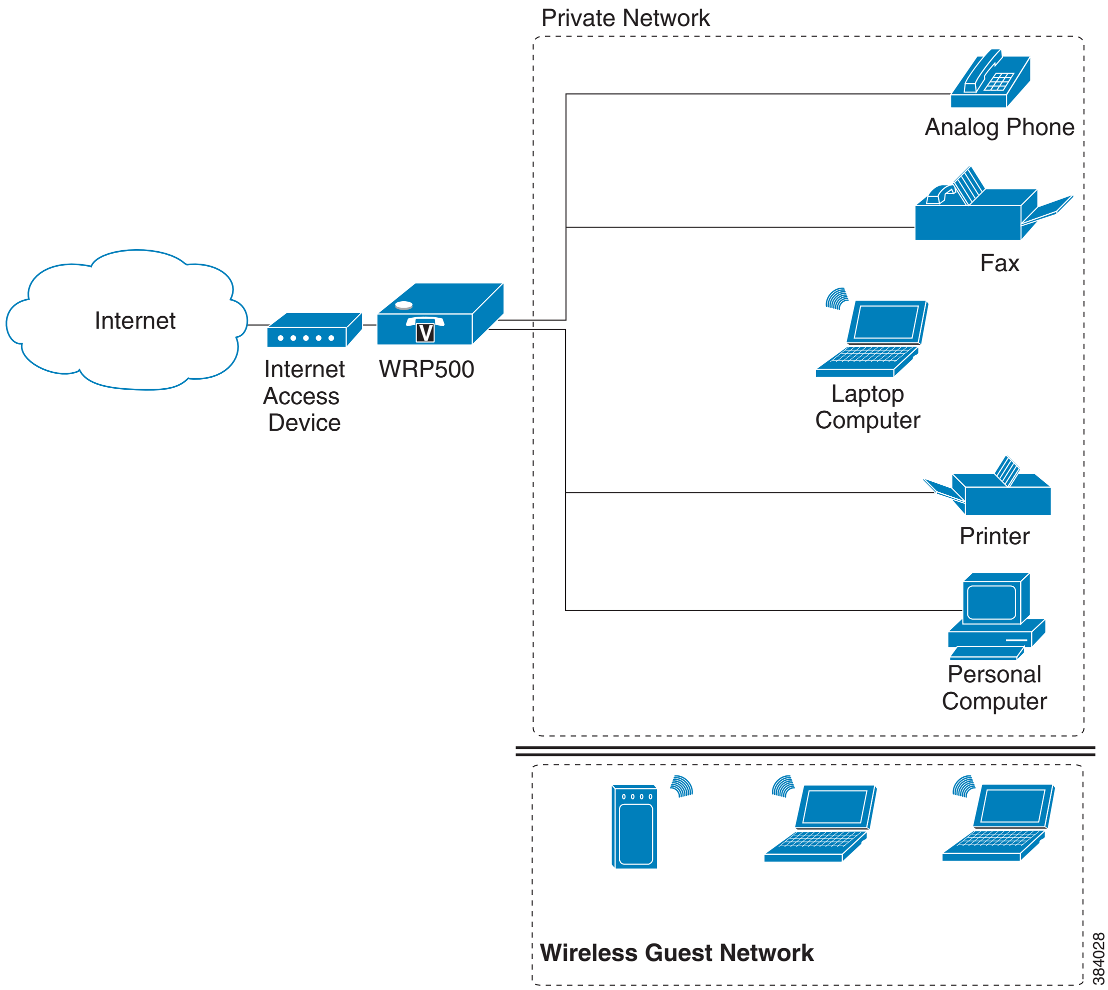
In this scenario, the WRP500 is deployed in a small business that has a basic network configuration.

- 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.

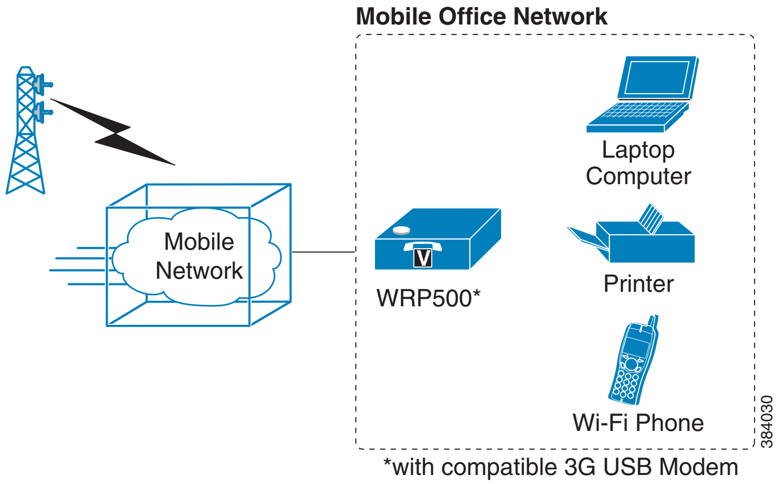
Note The WRP500 may be configured as an edge device or can be connected to another device that provides access to the Service Provider network.

- 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

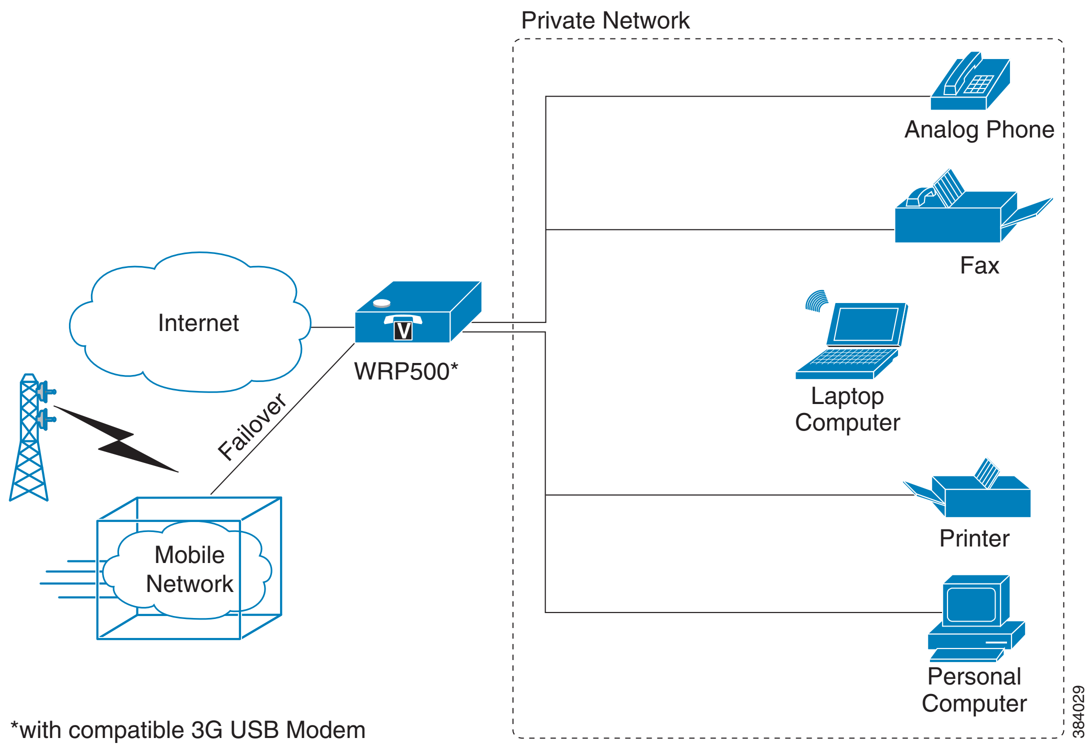
When a compatible mobile broadband modem connects to the USB port, the WRP500 can connect to a mobile broadband network. The mobile network can be the primary network or can serve as a backup network to ensure continuous Internet connectivity. Consider the scenarios that follow.

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.

Configure Your System for ITSP Interoperability

This chapter provides configuration details to help you to ensure that your infrastructure properly supports voice services.

- Configure NAT Mapping, page 2-1
- Firewalls and SIP, page 2-5
- Configure SIP Timer Values, page 2-5

Configure NAT Mapping

As discussed in Chapter 1, "Product Overview and Deployment Guidelines," some form of Network Address Translation (NAT) mapping is needed to support VoIP. If your ITSP does not support NAT mapping through a Session Border Controller, and if your edge device is not a SIP-ALG router, you can address this issue through one of the following methods:

- Configure NAT Mapping with a Static IP Address, page 2-1
- Configure NAT Mapping with STUN, page 2-2

Configure NAT Mapping with a Static IP Address

This option can be used if the following requirements are met:

- You must have a static external (public) IP address from your ISP.
- The edge device—that is, the router between your local area network and your ISP network—must have a symmetric NAT mechanism. If the WRP500 is the edge device, this requirement is met. If another device is used as the edge device, see the "Determine Whether the Router Uses Symmetric or Asymmetric NAT" section on page 2-4.
- If the WRP500 is connected to an Ethernet switch, the switch must be configured to enable Spanning Tree Protocol and Port Fast on the port to which the WRP500 is connected.

Note Use NAT mapping only if the ITSP network does not provide a Session Border Controller functionality.

Step 1 Log in as administrator.

Step 2 Under the **Voice** menu, click **SIP.**

Step 3 In the *NAT Support Parameters* section, enter the following settings:

- **Substitute VIA Addr:** Choose **yes.**
- **EXT IP:** Enter the public IP address that was assigned by your ISP.

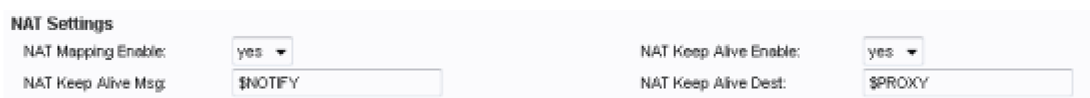
Figure 2-1 Voice tab > SIP: NAT Support Parameters

Step 4 Under the **Voice** menu, click **Line 1** or **Line 2** to choose the line interface that you want to modify.

Step 5 In the *NAT Settings* section, enter the following settings:

- **NAT Mapping Enable:** Choose **yes.**
- **NAT Keep Alive Enable:** Choose **yes.**

Figure 2-2 Voice tab > Line N > NAT Settings



Step 6 Click **Submit.**

Note You also need to configure the firewall settings on your router to allow SIP traffic. See "Firewalls and SIP," on page 5.

Configure NAT Mapping with STUN

This option is considered a practice of last resort and should be used only if the other methods are unavailable. This option can be used if the following requirements are met:

- You have a dynamically assigned external (public) IP address from your ISP.
- You must have a computer running STUN server software.
- The edge device uses an asymmetric NAT mechanism. If the WRP500 is the edge device, this requirement *is not met*. For more information, see the "Determine Whether the Router Uses Symmetric or Asymmetric NAT" section on page 2-4.
- If the WRP500 is connected to an Ethernet switch, the switch must be configured to enable Spanning Tree Protocol and Port Fast on the port to which the WRP500 is connected.

Note Use NAT mapping only if the ITSP network does not provide a Session Border Controller functionality.

Step 1 Log in as administrator.

Step 2 Under the **Voice** menu, click **SIP.**

Step 3 In the *NAT Support Parameters* section, enter the following settings:

- **Substitute VIA Addr:** yes
- **STUN Enable**: Choose **yes.**
- **STUN Test Enable:** Choose **yes.**
- **STUN Server:** Enter the IP address for your STUN server.

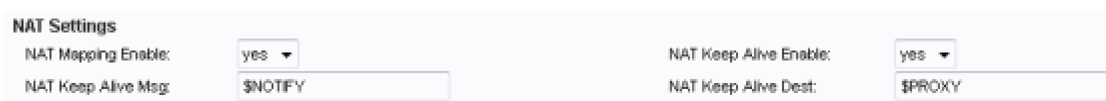
Figure 2-3 Voice tab > SIP > NAT Support Parameters

Step 4 Under the **Voice** menu, click **Line 1** or **Line 2** to choose the line interface that you want to modify.

Step 5 In the *NAT Settings* section, enter the following settings:

- **NAT Mapping Enable:** Choose **yes.**
- **NAT Keep Alive Enable:** Choose **yes** (optional).

Figure 2-4 Voice tab > Line N > NAT Settings



Note Your ITSP may require the WRP500 to send NAT keep alive messages to keep the NAT ports open permanently. Check with your ITSP to determine the requirements.

Step 6 Click **Submit.**

Note You also need to configure the firewall settings on your router to allow SIP traffic. See the "Firewalls and SIP" section on page 2-5.

Determine Whether the Router Uses Symmetric or Asymmetric NAT

To use a STUN server, the edge device—that is, the device that routes traffic between your private network and your ISP network—must have an asymmetric NAT mechanism. You need to determine which type of NAT mechanism is available on that device.

STUN does not work on routers with symmetric NAT. With symmetric NAT, IP addresses are mapped from one internal IP address and port to one external, routable destination IP address and port. If another packet is sent from the same source IP address and port to a different destination, a different IP address and port number combination is used. This method is restrictive because an external host can send a packet to a particular port on the internal host *only if* the internal host first sent a packet from that port to the external host.

Note This procedure assumes that a syslog server is configured and is ready to receive syslog messages.

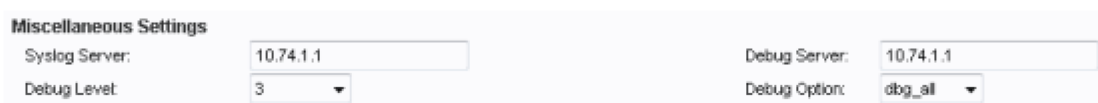
Step 1 Make sure that no firewall is running on your computer that could block the syslog port (port 514 by default).

Step 2 Log in as administrator.

Step 3 To enable debugging, complete the following tasks:

- **a.** Under the **Voice** menu, click **System**.
- **b.** In the *Syslog Server* and *Debug Server* fields, enter the IP address of your syslog server. This address and port number must be reachable from the WRP500.
- **c.** From the *Debug level* drop-down list, choose **3.**
- **d.** From the Debug option drop-down list, choose **dbg_all.**

Figure 2-5 Voice tab > System



Step 4 To collect information about the type of NAT that your router is using, complete the following tasks:

- **a.** Under the **Voice** menu, click **SIP.**
- **b.** Scroll down to the *NAT Support Parameters* section.
- **c.** From the *STUN Test Enable* field, choose **yes.**

Step 5 To enable SIP signaling, complete the following task:

- **a.** Under the **Voice** menu, click **Line 1** or **Line 2** to choose the line interface that you want to modify.
- **b.** In the *SIP Settings* section, choose **full** from the *SIP Debug Option* field.

Step 6 Click **Submit**.

Step 7 View the syslog messages to determine whether your network uses symmetric NAT. Look for a warning header in the REGISTER messages, such as Warning: 399 spa "Full Cone NAT Detected."

Firewalls and SIP

To enable SIP requests and responses to be exchanged with the SIP proxy at the ITSP, you must ensure that your firewall allows both SIP and RTP unimpeded access to the Internet.

- Make sure that the following ports are not blocked:
  - SIP ports—UDP port 5060 through 5061, which are used for the ITSP line interfaces
  - RTP ports—16384 to 16482
- Also disable SPI (Stateful Packet Inspection) if this function exists on your firewall.

Configure SIP Timer Values

The default timer values should be adequate in most circumstances. However, you can adjust the SIP timer values as needed to ensure interoperability with your ITSP. For example, if SIP requests are returned with an "invalid certificate" message, you may need to enter a longer SIP T1 retry value.

For more information, see the "SIP Timer Values (sec) section" section on page A-7.

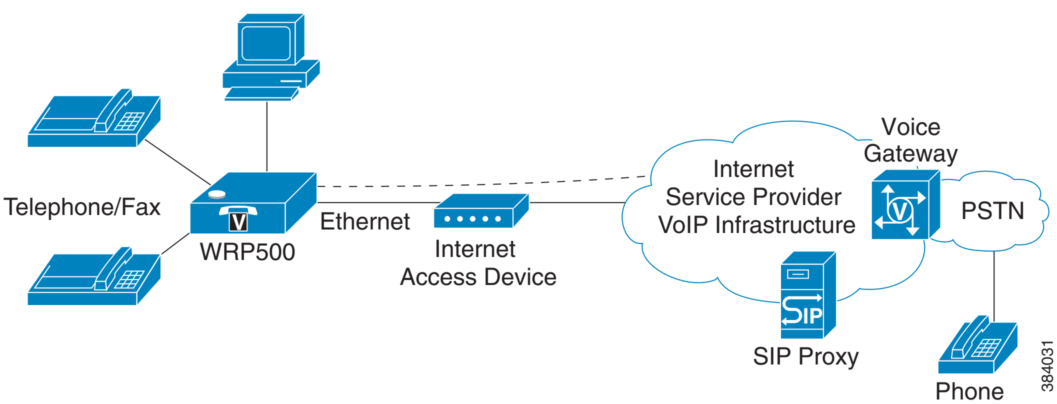
Configure Voice Services

This chapter describes how to configure your WRP500 to meet customer requirements for voice services.

- Analog Telephone Adapter Operations, page 3-1
- ATA Software Features, page 3-2
- Register to the Service Provider, page 3-5
- Manage Caller ID Service, page 3-7
- Optimize Fax Completion Rates, page 3-8
- Silence Suppression and Comfort Noise Generation, page 3-10
- Configure Dial Plans, page 3-10
- Secure Call Implementation, page 3-17

Analog Telephone Adapter Operations

The WRP500 is equipped with a built-in Analog Telephone Adapter (ATA). An ATA is an intelligent low-density Voice over IP (VoIP) gateway that enables carrier-class residential and business IP Telephony services that are delivered over broadband or high-speed Internet connections. Users can access Internet phone services through standard analog telephone equipment.



The WRP500 maintains the state of each call it terminates and reacts properly to user input events (such as on/off hook or hook flash). The WRP500 uses the Session Initiation Protocol (SIP) open standard, so little or no involvement by a "middle-man" server or media gateway controller occurs. SIP allows interoperation with all Internet telephony service providers (ITSPs) that support SIP.

ATA Software Features

The WRP500 is equipped with a full featured, fully programmable ATA that can be custom provisioned within a wide range of configuration parameters. These sections describe the factors that contribute to voice quality:

- Supported Codecs, page 3-2
- SIP Proxy Redundancy, page 3-2
- Other ATA Software Features, page 3-3

Supported Codecs

The WRP500 supports the following codecs:

- G.711u (configured by default) and G.711a

  G.711 (A-law and mu-law) are very low complexity codecs that support uncompressed 64 kbps digitized voice transmissions at one through ten 5-millisecond voice frames per packet. This codec provides the highest voice quality and uses the most bandwidth of any of the available codecs.

- G.729a

  The ITU G.729 voice coding algorithm is used to compress digitized speech. G.729a is a reduced complexity version of G.729. It requires about half the processing power as compared to G.729. The G.729 and G.729a bit streams are compatible and interoperable, but not identical.

The administrator can select the preferred codecs to be used for each line. See the "Audio Configuration section" section on page A-34.

In addition, negotiation of the optimal voice codec sometimes depends on the ability of an ATA to match a codec name with the codec that the far-end device uses. You can individually name the various codecs so that the WRP500 can successfully negotiate the codec with the far-end equipment. For more information, see the "Audio Configuration section," on page 34.

SIP Proxy Redundancy

In typical commercial IP Telephony deployments, all calls are established through a SIP proxy server. An average SIP proxy server may handle thousands of subscribers. It is important that a backup server be available so that an active server can be temporarily switched out for maintenance. The WRP500 supports the use of backup SIP proxy servers (via DNS SRV) so that service disruption should be nearly eliminated.

A relatively simple way to support proxy redundancy is to configure your DNS server with a list of SIP proxy addresses. The WRP500 can be instructed to contact a SIP proxy server in a domain named in the SIP message. The WRP500 consults the DNS server to get a list of hosts in the given domain that provides SIP services. If an entry exists, the DNS server returns an SRV record that contains a list of SIP proxy servers for the domain, with their host names, priority, listening ports, and so on. The WRP500 tries to contact the list of hosts in the order of their stated priority.

If the WRP500 is currently using a lower priority proxy server, it periodically probes the higher priority proxy to check whether it is back on line, and switches back to the higher priority proxy when possible. SIP Proxy Redundancy is configured in the Line and PSTN Line pages in the Configuration Utility.

Other ATA Software Features

Table 3-1 summarizes other features that the WRP500 provides.

Table 3-1 ATA Software Features

Feature	Description
Silence Suppression	See "Silence Suppression and Comfort Noise Generation" section on page 3-10.
Modem and Fax Pass-Through	• Modem pass-through mode can be triggered only by predialing the number that is set in the Modem Line Toggle Code. (Set in the Regional tab.) • FAX pass-through mode is triggered by a CED/CNG tone or by an NSE event. • Echo canceler is automatically disabled for Modem pass-through mode.
Adaptive Jitter Buffer	The WRP500 can buffer incoming voice packets to minimize out-of-order packet arrival. This process is known as jitter buffering. The jitter buffer size proactively adjusts or adapts in size, depending on changing network conditions. The WRP500 has a Network Jitter Level control setting for each line of service. The jitter level determines how aggressively the WRP500 tries to shrink the jitter buffer over time to achieve a lower overall delay. If the jitter level is higher, it shrinks more gradually. If jitter level is lower, it shrinks more quickly. Adaptive Jitter Buffer is configured in the Line and PSTN Line tabs. See Appendix A, "Advanced Voice Fields."
International Caller ID Delivery	In addition to support of the Bellcore (FSK) and Swedish/Danish (DTMF) methods of Caller ID (CID) delivery, ATAs provide a large subset of ETSI-compliant methods to support international CID equipment. International CID is configured in the Line and PSTN Line tabs. See Appendix A, "Advanced Voice Fields."
Secure Calls	A user (if enabled by service provider or administrator) has the option to make an outbound call secure in the sense that the audio packets in both directions are encrypted. See the "Secure Call Implementation" section on page 3-17.
Adjustable Audio Frames Per Packet	This feature allows the user to set the number of audio frames that are contained in one RTP packet. Packets can be adjusted to contain audio frames of 10ms to 30ms in length. Increasing the time of packets decreases the bandwidth utilized, but it also increases delay and may affect voice quality. See the RTP Packet Size parameter found in the SIP tab in Appendix A, "Advanced Voice Fields."
DTMF	The WRP500 may relay DTMF digits as out-of-band events to preserve the fidelity of the digits. This can enhance the reliability of DTMF transmission that many IVR applications, such as dial-up banking and airline information, require. DTMF is configured in the *DTMF Tx Mode* parameter that is found in the Line tabs. See Appendix A, "Advanced Voice Fields."

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>Call Progress Tone Generation</td><td>The WRP500 has configurable call progress tones. Call progress tones are generated locally on the WRP500 so an end user is advised of status (such as ringback). Parameters for each type of tone (for instance, a dial tone that is played back to an end user) may include frequency and amplitude of each component, and cadence information. See the Regional tab in Appendix A, “Advanced Voice Fields.”</td></tr>
<tr><td>Call Progress Tone Pass Through</td><td>This feature allows the user to hear the call progress tones (such as ringing) that are generated from the far-end network. See the Regional tab in Appendix A, “Advanced Voice Fields.”</td></tr>
<tr><td>Echo Cancellation</td><td>Impedance mismatch between the telephone and the IP Telephony gateway phone port can lead to near-end echo. The WRP500 has a near-end echo canceler that compensates for impedance match. The WRP500 also implements an echo suppressor with comfort noise generator (CNG) so that any residual echo is not noticeable. Echo Cancellation is configured in the Regional, Line, and PSTN Line tabs. See Appendix A, “Advanced Voice Fields.”</td></tr>
<tr><td>Signaling Hook Flash Event</td><td>The WRP500 can signal hook flash events to the remote party on a connected call. This feature can be used to provide advanced mid-call services with third-party-call-control. Depending on the features that the service provider offers using third-party-call-control, the following ATA features may be disabled to correctly signal a hook-flash event to the softswitch:
• Call Waiting Service (parameter call waiting serv set in the Line tab)
• Three Way Conference Service (parameter three-way conf serv set in the Line tab)
• Three Way Call Service (parameter three-way call serv set in the Line tab)
You can configure the length of time allowed for detection of a hook flash using the Hook Flash Timer parameter on the Regional tab of the Configuration Utility. See Appendix A, “Advanced Voice Fields.”</td></tr>
<tr><td>Configurable Dial Plan with Interdigit Timers</td><td>The WRP500 has three configurable interdigit timers:
• Initial timeout (T)—Signals that the handset is off the hook and that no digit has been pressed yet.
• Long timeout (L)—Signals the end of a dial string; that is, no more digits are expected.
• Short timeout (S)—Used between digits; that is, after a digit is pressed, a short timeout prevents the digit from being recognized a second time.
See “Configure Dial Plans” section on page 3-10 for more information.</td></tr>
<tr><td>Polarity Control</td><td>The WRP500 allows the polarity to be set when a call is connected and when a call is disconnected. This feature is required to support some pay phone system and answering machines. Polarity Control is configured in the Line and PSTN Line tabs. See Appendix A, “Advanced Voice Fields.”</td></tr>
</table>

Feature	Description
Calling Party Control	Calling Party Control (CPC) signals to the called party equipment that the calling party has hung up during a connected call by removing the voltage between the tip and ring momentarily. This feature is useful for auto-answer equipment, which then knows when to disengage. CPC is configured in the Regional, Line, and PSTN Line tabs. See Appendix A, "Advanced Voice Fields."
Syslog and Debug Server Records	Syslog and Debug Sever Records log more details than Report Generation and Event Logging. Using the configuration parameters, the WRP500 allows you to select which type of activity/events should be logged. Syslog and Debug Server allow the information to be sent to a Syslog Server. Syslog and Debug Server Records are configured in the System, Line, and PSTN Line tabs. See Appendix A, "Advanced Voice Fields."
SIP Over TLS	The WRP500 allows the use of SIP over Transport Layer Security (TLS). SIP over TLS is designed to eliminate the possibility of malicious activity by encrypting the SIP messages of the service provider and the end user. SIP over TLS relies on the widely deployed and standardized TLS protocol. SIP Over TLS encrypts only the signaling messages and not the media. A separate secure protocol, such as Secure Real-Time Transport Protocol (SRTP), can be used to encrypt voice packets. SIP over TLS is configured in the SIP Transport parameter configured in the Line tab(s). See Appendix A, "Advanced Voice Fields."

Register to the Service Provider

To use VoIP phone service, you must configure your WRP500 to the Internet Telephony Service Provider (ITSP).

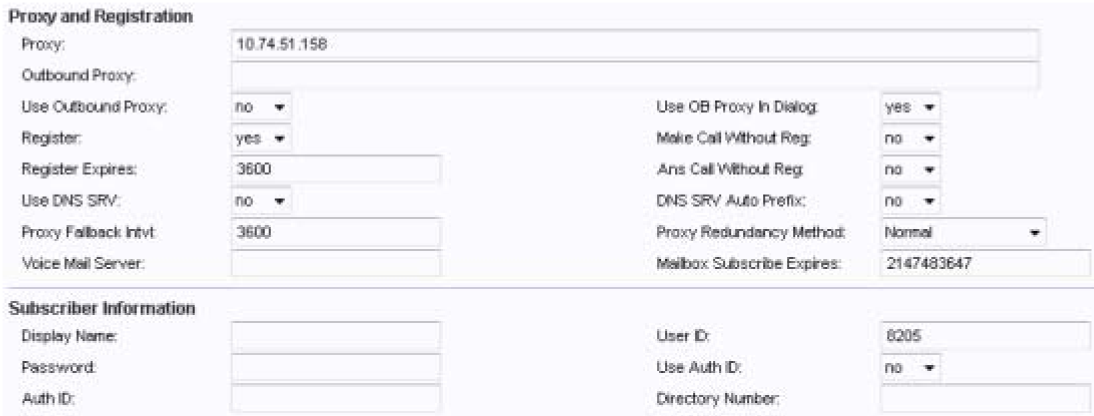
Note Each line tab must be configured separately. Each line tab can be configured for a different ITSP.

Step 1 Log in as administrator.

Step 2 Under the **Voice** menu, click **Line 1** or **Line 2** to choose the line interface that you want to modify.

Step 3 In the **Proxy and Registration** section, enter the **Proxy.**

Step 4 In the **Subscriber Information** section, enter the **User ID** and **Password.**

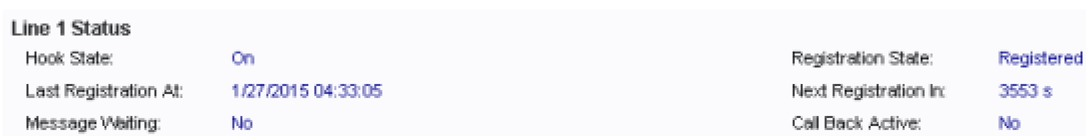


Note These are the minimum settings for most ITSP connections. Enter the account information as required by your ITSP.

Step 5 Click **Submit.** The devices reboot.

Step 6 To verify your progress, perform the following tasks:

- Under the **Voice** menu, click **Info**. Scroll down to the **Line 1 Status** or **Line 2 Status** section of the page, depending on which line you configured. Verify that the line is registered. Refer to the following example.



- Use an external phone to place an inbound call to the telephone number that was assigned by your ITSP. Assuming that you have left the default settings in place, the phone should ring and you can pick up the phone to get two-way audio.
- If the line is not registered, you may need to refresh the browser several times because it can take a few seconds for the registration to succeed. Also verify that your DNS is configured properly.

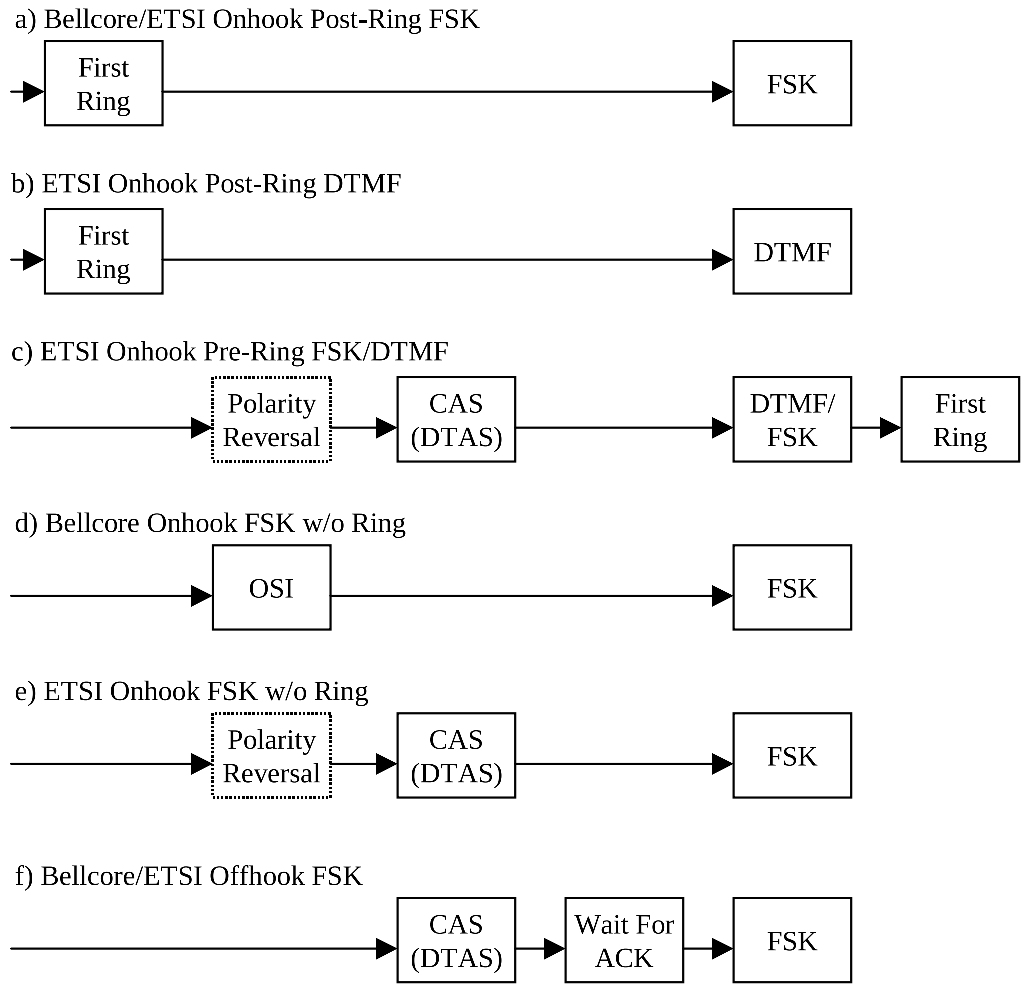
Manage Caller ID Service

The choice of caller ID (CID) method is dependent on your area/region. To configure CID, use the following parameters:

Parameter	Tab	Description and Value
Caller ID Method	Regional	The following choices are available: • **Bellcore (N.Amer,China)**—CID, CIDCW, and VMWI. FSK sent after first ring (same as ETSI FSK sent after first ring) (no polarity reversal or DTAS). • **DTMF (Finland, Sweden)**—CID only. DTMF sent after polarity reversal (and no DTAS) and before first ring. • **DTMF (Denmark)**—CID only. DTMF sent before first ring with no polarity reversal and no DTAS. • **ETSI DTMF**—CID only. DTMF sent after DTAS (and no polarity reversal) and before first ring. • **ETSI DTMF With PR**—CID only. DTMF sent after polarity reversal and DTAS and before first ring. • **ETSI DTMF After Ring—**CID only. DTMF sent after first ring (no polarity reversal or DTAS). • **ETSI FSK—**CID, CIDCW, and VMWI. FSK sent after DTAS (but no polarity reversal) and before first ring. Waits for ACK from CPE after DTAS for CIDCW. • **ETSI FSK With PR (UK)**—CID, CIDCW, and VMWI. FSK is sent after polarity reversal and DTAS and before first ring. Waits for ACK from CPE after DTAS for CIDCW. Polarity reversal is applied only if equipment is on hook. The default is Bellcore (N.Amer, China).
Caller ID FSK Standard	Regional	The WRP500 supports bell 202 and v.23 standards for caller ID generation. Select the FSK standard you want to use, **bell 202** or **v.23.** The default is **bell 202.**

Three types of Caller ID exist:

- On Hook Caller ID Associated with Ringing — This type of Caller ID is used for incoming calls when the attached phone is on hook. See the following figure (a) – (c). All CID methods can be applied for this type of CID.
- On Hook Caller ID Not Associated with Ringing — This feature is used to send VMWI signal to the phone to turn the message waiting light on and off. See the following figure (d) and (e). This is available only for FSK-based CID methods: Bellcore, ETSI FSK, and ETSI FSK With PR.
- Off Hook Caller ID — This is used to delivery caller-id on incoming calls when the attached phone is off hook. (See the following figure.) This can be call waiting caller ID (CIDCW) or to notify the user that the far-end party identity has changed or updated (such as due to a call transfer). This is available only for FSK-based CID methods: Bellcore, ETSI FSK, and ETSI FSK With PR.



Optimize Fax Completion Rates

Issues can occur with fax transmissions over IP networks, even with the T.38 standard, which is supported by the WRP500. You can adjust several settings on your WRP500 to optimize your fax completion rates.

Note Only T.38 Fax is supported. The WRP500 supports one connection.

Step 1 Ensure that you have enough bandwidth for the uplink and the downlink:

- For G.711 fallback, approximately 100 kbps are recommended.
- For T.38, allocate at least 50 kbps.

Step 2 To optimize G.711 fallback fax completion rates, set the following on the Line tab of your ATA device:

- **Call Waiting Serv:** no
- **Three Way Call Serv:** no

- **Preferred Codec:** G.711
- **Use pref. codec only:** yes

Step 3 If you are using a Cisco media gateway for PSTN termination, disable T.38 (fax relay) and enable fax using modem passthrough.

For example:

```
modem passthrough nse payload-type 110 codec g711ulaw
fax rate disable
fax protocol pass-through g711ulaw
```

Step 4 Enable T.38 fax on the WRP500 by configuring the following parameter on the Line tab for the FXS port to which the FAX machine is connected:

FAX_Enable T38: **Yes**

Note If a T.38 call cannot be set up, the call automatically reverts to G.711 fallback.

Step 5 If you are using a Cisco media gateway, use the following settings:

Make sure the Cisco gateway is correctly configured for T.38 with the SPA dial peer. For example:

```
fax protocol T38
fax rate voice
fax-relay ecm disable
fax nsf 000000
no vad
```

Fax Troubleshooting

If you have problems sending or receiving faxes, complete the following steps:

Step 1 Verify that your fax machine is set to a speed between 7200 and 14400.

Step 2 Send a test fax in a controlled environment between two ATAs.

Step 3 Determine the success rate.

Step 4 Monitor the network and record the following statistics:

- Jitter
- Loss
- Delay

Step 5 If faxes fail consistently, capture a copy of the voice settings by selecting **Save As** > **Web page, complete** from the administration web server page. You can send this configuration file to Technical Support.

Step 6 Enable and capture the debug log. For instructions, refer to Appendix C, “Troubleshooting.”

Note You may also capture data by using a sniffer trace.

Step 7 Identify the type of fax machine that is connected to the ATA device.

Step 8 Contact technical support:

- If you are an end user of VoIP products, contact the reseller or Internet telephony service provider (ITSP) that supplied the equipment.
- If you are an authorized Cisco partner, contact Cisco technical support.

Silence Suppression and Comfort Noise Generation

Voice Activity Detection (VAD) with Silence Suppression is a means of increasing the number of calls that the network supports by reducing the required bandwidth for a single call. VAD uses a sophisticated algorithm to distinguish between speech and non-speech signals. Based on the current and past statistics, the VAD algorithm decides whether speech is present. If the VAD algorithm decides speech is not present, silence suppression and comfort noise generation is activated. This is accomplished by removing and not transmitting the natural silence that occurs in a normal two-way connection. The IP bandwidth is used only when someone is speaking. During the silent periods of a telephone call, additional bandwidth is available for other voice calls or data traffic because the silence packets are not being transmitted across the network.

Comfort Noise Generation provides artificially-generated background white noise (sounds), designed to reassure callers that their calls are still connected during silent periods. If Comfort Noise Generation is not used, the caller may think the call has been disconnected because of the "dead silence" periods that the VAD and Silence Suppression feature creates.

Silence suppression is configured in the Line tab.

Configure Dial Plans

Dial plans determine how the digits are interpreted and transmitted. They also determine whether the dialed number is accepted or rejected. You can use a dial plan to facilitate dialing or to block certain types of calls, such as long distance or international.

This section includes information that you need to understand dial plans, as well as procedures for configuring your own dial plans. This section includes the following topics:

- About Dial Plans, page 3-10
- Edit Dial Plans, page 3-16

About Dial Plans

This section provides information to help you understand how dial plans are implemented.

Refer to the following topics:

- Digit Sequences, page 3-11
- Digit Sequence Examples, page 3-12
- Acceptance and Transmission of Dialed Digits, page 3-13
- Dial Plan Timer (Off-Hook Timer), page 3-14

- Interdigit Long Timer (Incomplete Entry Timer), page 3-15
- Interdigit Short Timer (Complete Entry Timer), page 3-15

Digit Sequences

A dial plan contains a series of digit sequences, separated by the | character. The entire collection of sequences is enclosed within parentheses. Each digit sequence within the dial plan consists of a series of elements, which are individually matched to the keys that the user presses.

Note White space is ignored, but may be used for readability.

Digit Sequence	Function
0 1 2 3 4 5 6 7 8 9 0 * #	Enter any of these characters to represent a key that the user must press on the phone keypad.
x	Enter x to represent any character on the phone keypad.
[sequence]	Enter characters within square brackets to create a list of accepted key presses. The user can press any one of the keys in the list. • Numeric range For example, enter [2-9] to allow the user to press any one digit from 2 through 9. • Numeric range with other characters For example, enter [35-8*] to allow the user to press 3, 5, 6, 7, 8, or *.
. (period)	Enter a period for element repetition. The dial plan accepts 0 or more entries of the digit. For example, 01. allows users to enter 0, 01, 011, 0111, and so on.
<dialed:substituted>	Use this format to indicate that certain dialed digits are replaced by other characters when the sequence is transmitted. The dialed digits can be zero or more characters. **EXAMPLE 1:** <8:1650>xxxxxxx When the user presses 8 followed by a seven-digit number, the system automatically replaces the dialed 8 with 1650. If the user dials **85550112**, the system transmits **16505550112**. **EXAMPLE 2:** <:1>xxxxxxxxxx In this example, no digits are replaced. When the user enters a 10-digit string of numbers, the number 1 is added at the beginning of the sequence. If the user dials **9725550112**, the system transmits **19725550112**
, (comma)	Enter a comma between digits to play an “outside line” dial tone after a user-entered sequence. **EXAMPLE:** 9, 1xxxxxxxxxx An “outside line” dial tone is sounded after the user presses 9, and the tone continues until the user presses 1.

Digit Sequence	Function
! (exclamation point)	Enter an exclamation point to prohibit a dial sequence pattern. **EXAMPLE:** 1900xxxxxxx! The system rejects any 11-digit sequence that begins with 1900.
*xx	Enter an asterisk to allow the user to enter a 2-digit star code.
S0 or L0	Enter S0 to reduce the short inter-digit timer to 0 seconds, or enter L0 to reduce the long inter-digit timer to 0 seconds.

Digit Sequence Examples

The following examples show digit sequences that you can enter in a dial plan.

In a complete dial plan entry, sequences are separated by a pipe character (|), and the entire set of sequences is enclosed within parentheses.

EXAMPLE: ([1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11)

- Extensions on your system

  EXAMPLE: (**[1-8]xx** | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11)

  [1-8]xx Allows a user to dial any three-digit number that starts with the digits 1 through 8. If your system uses four-digit extensions, you would instead enter the following string: **[1-8]xxx**

- Local dialing with seven-digit number

  EXAMPLE: ([1-8]xx | **9, xxxxxxx** | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]111)

  9, xxxxxxx After a user presses 9, an external dial tone sounds. The user can enter any seven-digit number, as in a local call.

- Local dialing with 3-digit area code and a 7-digit local number

  EXAMPLE: ([1-8]xx | 9, xxxxxxx | **9, <:1>[2-9]xxxxxxxxx** | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11)

  9, <:1>[2-9]xxxxxxxxx This example is useful where a local area code is required. After a user presses 9, an external dial tone sounds. The user must enter a 10-digit number that begins with a digit 2 through 9. The system automatically inserts the 1 prefix before transmitting the number to the carrier.

- Local dialing with an automatically inserted 3-digit area code

  EXAMPLE: ([1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | **8, <:1212>xxxxxxx** | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11)

  8, <:1212>xxxxxxx This example is useful where a local area code is required by the carrier but the majority of calls go to one area code. After the user presses 8, an external dial tone sounds. The user can enter any seven-digit number. The system automatically inserts the 1 prefix and the 212 area code before transmitting the number to the carrier.

- U.S. long distance dialing

  EXAMPLE: ([1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | **9, 1 [2-9] xxxxxxxxx** | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11)

9, 1 [2-9] xxxxxxxxx After the user presses 9, an external dial tone sounds. The user can enter any 11-digit number that starts with 1 and is followed by a digit 2 through 9.

- Blocked number

  EXAMPLE: ([1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | **9, 1 900 xxxxxxx !** | 9, 011xxxxxx. | 0 | [49]11)

  9, 1 900 xxxxxxx ! This digit sequence is useful if you want to prevent users from dialing numbers that are associated with high tolls or inappropriate content, such as 1-900 numbers in the U.S. After the user presses 9, an external dial tone sounds. If the user enters an 11-digit number that starts with the digits 1900, the call is rejected.

- U.S. international dialing

  EXAMPLE: ([1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | **9, 011xxxxxx.** | 0 | [49]11)

  9, 011xxxxxx. After the user presses 9, an external dial tone sounds. The user can enter any number that starts with 011, as in an international call from the U.S.

- Informational numbers

  EXAMPLE: ([1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | **0 | [49]11**)

  0 | [49]11 This example includes two digit sequences, separated by the pipe character. The first sequence allows a user to dial 0 for an operator. The second sequence allows the user to enter 411 for local information or 911 for emergency services.

Acceptance and Transmission of Dialed Digits

When a user dials a series of digits, each sequence in the dial plan is tested as a possible match. The matching sequences form a set of candidate digit sequences. As the user enters more digits, the set of candidates diminishes until only one or none are valid. When a terminating event occurs, the WRP500 either accepts the user-dialed sequence and initiates a call, or rejects the sequence as invalid. The user hears the reorder (fast busy) tone if the dialed sequence is invalid.

The following table explains how terminating events are processed.

Terminating Event	Processing
The dialed digits do not match any sequence in the dial plan.	The number is rejected.
The dialed digits exactly match one sequence in the dial plan.	If the sequence is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan. If the sequence is blocked by the dial plan, the number is rejected.

Terminating Event	Processing
A timeout occurs.	The number is rejected if the dialed digits are not matched to a digit sequence in the dial plan within the time specified by the applicable interdigit timer. • The Interdigit Long Timer applies when the dialed digits do not match any digit sequence in the dial plan. The default value is 10 seconds. • The Interdigit Short Timer applies when the dialed digits match one or more candidate sequences in the dial plan. The default value is 3 seconds.
The user presses the # key or the **dial** softkey on the phone display.	If the sequence is complete and is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan. If the sequence is incomplete or is blocked by the dial plan, the number is rejected.

Dial Plan Timer (Off-Hook Timer)

You can think of the Dial Plan Timer as "the off-hook timer." This timer starts counting when the phone goes off hook. If no digits are dialed within the specified number of seconds, the timer expires and the null entry is evaluated. Unless you have a special dial plan string to allow a null entry, the call is rejected. The default value is 5.

Syntax for the Dial Plan Timer

SYNTAX: (P*s*<:*n*> | *dial plan*)

- **s:** The number of seconds; if no number is entered after P, the default timer of 5 seconds applies.
- **n:** (optional): The number to transmit automatically when the timer expires; you can enter an extension number or a DID number. No wildcard characters are allowed because the number will be transmitted as shown. If you omit the number substitution, <:n>, the user hears a reorder (fast busy) tone after the specified number of seconds.

Examples for the Dial Plan Timer

- Allow more time for users to start dialing after taking a phone off hook.

  EXAMPLE: (**P9** | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)

  P9 After taking a phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the user hears a reorder (fast busy) tone. By setting a longer timer, you allow more time for users to enter the digits.

- Create a hotline for all sequences on the System Dial Plan

  EXAMPLE: (**P9<:23>** | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)

  P9<:23> After taking the phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the call is transmitted automatically to extension 23.

- Create a hotline on a line button for an extension

  EXAMPLE: **(P0 <:1000>)**

  With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook. Enter this sequence in the Phone Dial Plan for Ext 2 or higher on a client station.

Interdigit Long Timer (Incomplete Entry Timer)

You can think of this timer as the "incomplete entry" timer. This timer measures the interval between dialed digits. It applies as long as the dialed digits do not match any digit sequences in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated as incomplete, and the call is rejected. The default value is 10 seconds.

Note This section explains how to edit a timer as part of a dial plan. Alternatively, you can modify the Control Timer that controls the default interdigit timers for all calls. See the "Reset the Control Timers" section on page 3-16.

Syntax for the Interdigit Long Timer

SYNTAX: L:*s*, (*dial plan*)

- **s:** The number of seconds; if no number is entered after L:, the default timer of 5 seconds applies.
- Note that the timer sequence appears to the left of the initial parenthesis for the dial plan.

Example for the Interdigit Long Timer

EXAMPLE: **L:15,** (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)

L:15, This dial plan allows the user to pause for up to 15 seconds between digits before the Interdigit Long Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

Interdigit Short Timer (Complete Entry Timer)

You can think of this timer as the "complete entry" timer. This timer measures the interval between dialed digits. It applies when the dialed digits match at least one digit sequence in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated. If it is valid, the call proceeds. If it is invalid, the call is rejected. The default value is 3 seconds.

Syntax for the Interdigit Short Timer

- **SYNTAX 1:** S:*s*, (*dial plan*)

  Use this syntax to apply the new setting to the entire dial plan within the parentheses.

- **SYNTAX 2:** *sequence* Ss

  Use this syntax to apply the new setting to a particular dialing sequence.

  s: The number of seconds; if no number is entered after S, the default timer of 5 seconds applies.

Examples for the Interdigit Short Timer

- Set the timer for the entire dial plan.

  EXAMPLE: **S:6,** (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)

  S:6, While entering a number with the phone off hook, a user can pause for up to 15 seconds between digits before the Interdigit Short Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

- Set an instant timer for a particular sequence within the dial plan.

  EXAMPLE: (9,8<:1408>[2-9]xxxxxx | **9,8,1[2-9]xxxxxxxxxS0** | 9,8,011xx. | 9,8,xx.|[1-8]xx)

  9,8,1[2-9]xxxxxxxxxS0 With the timer set to 0, the call is transmitted automatically when the user dials the final digit in the sequence.

Edit Dial Plans

You can edit dial plans and can modify the control timers.

Enter the Line Interface Dial Plan

This dial plan is used to strip steering digits from a dialed number before it is transmitted out to the carrier.

Step 1 Start Internet Explorer, connect to the Configuration Utility, choose **Voice**. If prompted, enter the administrative login provided by the Service Provider. (The default username and password are both **admin**.)

Step 2 Under the **Voice** menu, click **Line 1** or **Line 2**, depending on the line interface that you want to configure.

Step 3 Scroll down to the *Dial Plan* section.

Step 4 Enter the digit sequences in the *Dial Plan* field. For more information, see the "About Dial Plans" section on page 3-10.

Step 5 Click **Submit.**

Reset the Control Timers

You can use the following procedure to reset the default timer settings for all calls.

Note If you need to edit a timer setting only for a particular digit sequence or type of call, you can edit the dial plan. See the "About Dial Plans" section on page 3-10.

Step 1 Start Internet Explorer, connect to the Configuration Utility, choose **Voice**. If prompted, enter the administrative login provided by the Service Provider. (The default username and password are both **admin**.)

Step 2 Under the **Voice** menu, click **Regional.**

Step 3 Scroll down to the *Control Timer Values* section.

Step 4 Enter the desired values in the *Interdigit Long Timer* field and the *Interdigit Short Timer* field. Refer to the definitions at the beginning of this section.

Secure Call Implementation

This section describes secure call implementation with the WRP500. It includes the following topics:

- Enable Secure Calls, page 3-17

Note This is an advanced topic meant for experience installers. Also 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

Enable Secure Calls

WRP500 does not support establishing secure call by "mini certificate" as WRP400 did. The only method to enable a secure call requires use of SRTP, while the SRTP key parameters are transferred in SIP messages that are encrypted by TLS.

To enable SRTP on Line 1:

- Voice > Line 1 > Secure Call Serv, set to Yes
- Voice > User 1 > Secure Call Setting, set to Yes

To enable SIP over TLS on Line:

- Voice > Line 1 > SIP Transport, set to TLS

Advanced Voice Fields

This appendix describes the Advanced settings that are available after you log in as administrator.

After you click the *Voice* tab, you can choose the following pages:

- Info page, page A-1
- System page, page A-4
- SIP page, page A-5
- Regional page, page A-11
- Line page, page A-24
- User page, page A-38

Info page

You can use the *Voice tab* > *Info* page to view information about the WRP500. This page includes the following sections:

- Product Information section, page A-1
- System Status section, page A-2
- Line Status section, page A-2

Note The fields on the Info page are read-only and cannot be edited.

Product Information section

This table describes the fields in the Product Information section of the Voice tab > Info page.

Field	Description
Product Name	Model number/name.
Serial Number	Serial number.
Software Version	Software version number.
Hardware Version	Hardware version number.

Field	Description
MAC Address	MAC address.
Client Certificate	Status of the client certificate, which can indicate whether the WRP500 has been authorized by your ITSP.
Customization	For a Remote Configuration (RC) unit, this field indicates whether the unit has been customized or not. Pending indicates a new RC unit that is ready for provisioning. If the unit has already retrieved its customized profile, this field displays the name of the company that provisioned the unit.
Voice Module Version	Voice module number.

System Status section

This table describes the fields in the System Status section of the Voice tab > Info page.

Field	Description
Current Time	Current date and time of the system; for example, 10/3/2003 16:43:00.
Elapsed Time	Total time elapsed since the last reboot of the system; for example, 25 days and 18:12:36.
RTP Packets Sent	Total number of RTP packets sent (including redundant packets).
RTP Bytes Sent	Total number of RTP bytes sent.
RTP Packets Recv	Total number of RTP packets received (including redundant packets).
RTP Bytes Recv	Total number of RTP bytes received.
SIP Messages Sent	Total number of SIP messages sent (including retransmissions).
SIP Bytes Sent	Total number of bytes of SIP messages sent (including retransmissions).
SIP Messages Recv	Total number of SIP messages received (including retransmissions).
SIP Bytes Recv	Total number of bytes of SIP messages received (including retransmissions).
External IP	External IP address used for NAT mapping.

Line Status section

This table describes the fields in the Line Status section of the Voice tab > Info page.

Field	Description
Hook State	Hook state of the FXS port. Options are either On or Off.
Registration State	Indicates if the line has registered with the SIP proxy.
Last Registration At	Last date and time the line was registered.
Next Registration In	Number of seconds before the next registration renewal.

Field	Description
Message Waiting	Indicates whether you have new voice mail waiting. Options are either Yes or No. The value automatically is set to Yes when a message is received. You also can clear or set the flag manually. Setting this value to Yes can activate stutter tone and VMWI signal. This parameter is stored in long term memory and survives after reboot or power cycle.
Call Back Active	Indicates whether a call back request is in progress. Options are either Yes or No.
Last Called Number	The last number called from the FXS line.
Last Caller Number	Number of the last caller.
Mapped SIP Port	Port number of the SIP port mapped by NAT.
Call 1 and 2 State	May take one of the following values: • Idle • Dialing • Stunning • Calling • Proceeding • Ringing • Invalid • Connected • Hold • Holding • Resuming • Transit
Call 1 and 2 Tone	Type of tone used by the call.
Call 1 and 2 Encoder	Codec used for encoding.
Call 1 and 2 Decoder	Codec used for decoding.
Call 1 and 2 FAX	Status of the fax mode.
Call 1 and 2 Type	Direction of the call. May take one of the following values: • Inbound • Outbound • Transferred
Call 1 and 2 Remote Hold	Indicates whether the far end has placed the call on hold.
Call 1 and 2 Callback	Indicates whether the call was triggered by a call back request.
Call 1 and 2 Peer Name	Name of the internal phone.
Call 1 and 2 Peer Phone	Phone number of the internal phone.
Call 1 and 2 Call Duration	Duration of the call.

Field	Description
Call 1 and 2 Packets Sent	Number of packets sent.
Call 1 and 2 Packets Recv	Number of packets received.
Call 1 and 2 Bytes Sent	Number of bytes sent.
Call 1 and 2 Bytes Recv	Number of bytes received.
Call 1 and 2 Decode Latency	Number of milliseconds for decoder latency.
Call 1 and 2 Jitter	Number of milliseconds for receiver jitter.
Call 1 and 2 Packets Lost	Number of packets lost.
Call 1 and 2 Packet Error	Number of invalid packets received.
Call 1 and 2 Mapped RTP Port	The port mapped for Real Time Protocol traffic for Call 1/2.
Call 1 and 2 Media Loopback	Media loopback is used to quantitatively and qualitatively measure the voice quality that the end user experiences.

System page

You can use the *Voice tab* > *System* page to configure your system and network connections. This page includes the following sections:

- System Configuration section, page A-4
- Miscellaneous Settings section, page A-5

System Configuration section

This table describes the fields in the System Configuration section of the Voice tab > System page.

Field	Description
Restricted Access Domains	This feature is used when implementing software customization.
IVR Admin Passwd	Password for entering IVR menu.

Miscellaneous Settings section

This table describes the fields in the Miscellaneous section of the Voice tab > System page.

Field	Description
Syslog Server	Specifies the IP address of the syslog server.
Debug Server	Specifies the IP address of the debug server, which logs debug information. The level of detailed output depends on the debug level parameter setting.
Debug Level	Determines the level of debug information that is generated. Select 0, 1, 2, or 3 from the drop-down menu. The higher the debug level, the more debug information is generated. The default is 0, which indicates that no debug information is generated.
Debug Option	Specifies what debug information is expected. Generally can be set to *dbg_all.*

SIP page

You can use the *Voice tab > SIP* page to configure the SIP settings. This page includes the following sections:

- SIP Parameters section, page A-5
- SIP Timer Values (sec) section, page A-7
- Response Status Code Handling section, page A-8
- RTP Parameters section, page A-8
- SDP Payload Types section, page A-9
- NAT Support Parameters section, page A-10

SIP Parameters section

This table describes the fields in the SIP Parameters section of the Voice tab > SIP page.

Field	Description
Max Forward	SIP Max Forward value, which can range from 1 to 255. The default is **70.**
Max Redirection	Number of times an invite can be redirected to avoid an infinite loop. The default is **5.**
Max Auth	Maximum number of times (from 0 to 255) a request may be challenged. The default is **2.**
SIP User Agent Name	User-Agent header used in outbound requests. The default is **$VERSION**. If empty, the header is not included. Macro expansion of $A to $D corresponding to GPP_A to GPP_D allowed.

Field	Description
SIP Server Name	Server header used in responses to inbound responses. The default is **$VERSION**.
SIP Reg User Agent Name	User-Agent name to be used in a REGISTER request. If this value is not specified, the *SIP User Agent Name* parameter is also used for the REGISTER request. The default is blank.
SIP Accept Language	Accept-Language header used. There is no default (this indicates the WRP500 does not include this header). If empty, the header is not included.
DTMF Relay MIME Type	MIME Type used in a SIP INFO message to signal a DTMF event. The default is **application/dtmf-relay.**
Remove Last Reg	Lets you remove the last registration before registering a new one if the value is different. Select yes or no from the drop-down menu. The default is **no.**
Use Compact Header	Lets you use compact SIP headers in outbound SIP messages. Select yes or no from the drop-down menu. If set to yes, the WRP500 uses compact SIP headers in outbound SIP messages. If set to no, the WRP500 uses normal SIP headers. If inbound SIP requests contain compact headers, the WRP500 reuses the same compact headers when generating the response regardless the settings of the *Use Compact Header* parameter. If inbound SIP requests contain normal headers, the WRP500 substitutes those headers with compact headers (if defined by RFC 261) if *Use Compact Header* parameter is set to yes. The default is **no.**
Escape Display Name	Lets you keep the Display Name private. Select yes if you want the WRP500 to enclose the string (configured in the Display Name) in a pair of double quotes for outbound SIP messages. Any occurrences of or \ in the string is escaped with \ and \\ inside the pair of double quotes. Otherwise, select no. The default is **no.**
RFC 2543 Call Hold	Configures the type of call hold: a:sendonly or 0.0.0.0. The default is **no;** do not use the 0.0.0.0 syntax in a HOLD SDP; use the a:sendonly syntax.
Mark All AVT Packets	If set to yes, all AVT tone packets (encoded for redundancy) have the marker bit set. If set to no, only the first packet has the marker bit set for each DTMF event. The default is **yes.**
SIP TCP Port Min	Specifies the lowest TCP port number that can be used for SIP sessions. The default Port Min is 5060.
SIP TCP Port Max	Specifies the highest TCP port number that can be used for SIP sessions. The default Port Max is 5080.

SIP Timer Values (sec) section

This table describes the fields in the SIP Timer Values section of the Voice tab > SIP page.

Field	Description
SIP T1	RFC 3261 T1 value (RTT estimate), which can range from 0 to 64 seconds. The default is 5.
SIP T2	RFC 3261 T2 value (maximum retransmit interval for non-INVITE requests and INVITE responses), which can range from 0 to 64 seconds. The default is 4.
SIP T4	RFC 3261 T4 value (maximum duration a message remains in the network), which can range from 0 to 64 seconds. The default is 5.
SIP Timer B	INVITE time-out value, which can range from 0 to 64 seconds. The default is 32.
SIP Timer F	Non-INVITE time-out value, which can range from 0 to 64 seconds. The default is 32.
SIP Timer H	INVITE final response, time-out value, which can range from 0 to 64 seconds. The default is 32.
SIP Timer D	ACK hang-around time, which can range from 0 to 64 seconds. The default is 32.
SIP Timer J	Non-INVITE response hang-around time, which can range from 0 to 64 seconds. The default is 32.
INVITE Expires	INVITE request Expires header value. If you enter 0, the Expires header is not included in the request. The default is 240. Range: 0–(2^{31}–1).
ReINVITE Expires	ReINVITE request Expires header value. If you enter 0, the Expires header is not included in the request. The default is 30. Range: 0–(2^{31}–1).
Reg Min Expires	Minimum registration expiration time allowed from the proxy in the Expires header or as a Contact header parameter. If the proxy returns a value less than this setting, the minimum value is used. The default is 1.
Reg Max Expires	Maximum registration expiration time allowed from the proxy in the Min-Expires header. If the value is larger than this setting, the maximum value is used. The default is 7200.

Field	Description
Reg Retry Intvl	Interval to wait before the WRP500 retries registration after failing during the last registration. The default is 30.
Reg Retry Long Intvl	When registration fails with a SIP response code that does not match *Retry Reg RSC*, the WRP500 waits for the specified length of time before retrying. If this interval is 0, the WRP500 stops trying. This value should be much larger than the Reg Retry Intvl value, which should not be 0. The default is 1200.

Response Status Code Handling section

This table describes the fields in the Response Status Code Handling section of the Voice tab > SIP page.

Field	Description
SIT1 RSC	SIP response status code for the appropriate Special Information Tone (SIT). For example, if you set the SIT1 RSC to 404, when the user makes a call and a failure code of 404 is returned, the SIT1 tone is played. **Reorder** or **Busy** tone is played by default for all unsuccessful response status code for SIT 1 RSC through SIT 4 RSC.
SIT2 RSC	SIP response status code to INVITE on which to play the SIT2 Tone.
SIT3 RSC	SIP response status code to INVITE on which to play the SIT3 Tone.
SIT4 RSC	SIP response status code to INVITE on which to play the SIT4 Tone.
Try Backup RSC	SIP response code that retries a backup server for the current request.
Retry Reg RSC	Interval to wait before the WRP500 retries registration after failing during the last registration. The default is 30.

RTP Parameters section

This table describes the fields in the RTP Parameters section of the Voice tab > SIP page.

Field	Description
RTP Port Min	Minimum port number for RTP transmission and reception. The *RTP Port Min* and *RTP Port Max* parameters should define a range that contains at least 4 even number ports, such as 100 – 106. The default is 16384.
RTP Port Max	Maximum port number for RTP transmission and reception. The default is 16482.

Field	Description
RTP Packet Size	Packet size in seconds, which can range from 0.01 to 0.16. Valid values must be a multiple of 0.01 seconds. The default is 0.030.
Stats In BYE	Determines whether the WRP500 includes the P-RTP-Stat header or response to a BYE message. The header contains the RTP statistics of the current call. Select yes or no from the drop-down menu. The format of the P-RTP-Stat header is: P-RTP-State: PS=<packets sent>,OS=<octets sent>,PR=<packets received>,OR=<octets received>,PL=<packets lost>,JI=<jitter in ms>,LA=<delay in ms>,DU=<call duration in s>,EN=<encoder>,DE=<decoder>. The default is **no.**

SDP Payload Types section

This table describes the fields in the SDP Payload Types section of the Voice tab > SIP page.

Field	Description
NSE Dynamic Payload	NSE dynamic payload type. The valid range is 96-127. The default is 100.
AVT Dynamic Payload	AVT dynamic payload type. The valid range is 96-127. The default is 101.
INFOREQ Dynamic Payload	INFOREQ dynamic payload type. There is no default.
NSE Codec Name	NSE codec name used in SDP. The default is NSE.
AVT Codec Name	AVT codec name used in SDP. The default is telephone-event.
G711u Codec Name	G.711u codec name used in SDP. The default is PCMU.
G711a Codec Name	G.711a codec name used in SDP. The default is PCMA.
G729a Codec Name	G.729a codec name used in SDP. The default is G729a.
G729b Codec Name	G.729b codec name used in SDP. The default is G729ab.

Field	Description
EncapRTP Codec Name	EncapRTP codec name used in SDP. The default is EncapRTP.
EncapRTP Dynamic Payload	EncapRTP dynamic payload type.

NAT Support Parameters section

This table describes the fields in the NAT Support Parameters section of the Voice tab > SIP page.

Field	Description
Handle VIA received	If you select yes, the WRP500 processes the received parameter in the VIA header (this value is inserted by the server in a response to anyone of its requests). If you select no, the parameter is ignored. Select **yes** or **no** from the drop-down menu. The default is **no.**
Handle VIA rport	If you select yes, the WRP500 processes the rport parameter in the VIA header (this value is inserted by the server in a response to anyone of its requests). If you select no, the parameter is ignored. Select **yes** or **no** from the drop-down menu. The default is **no.**
Insert VIA received	Inserts the received parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. Select yes or no from the drop-down menu. The default is **no.**
Insert VIA rport	Inserts the parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. Select yes or no from the drop-down menu. The default is **no.**
Substitute VIA Addr	Lets you use NAT-mapped IP:port values in the VIA header. Select yes or no from the drop-down menu. The default is **no.**
Send Resp To Src Port	Sends responses to the request source port instead of the VIA sent-by port. Select yes or no from the drop-down menu. The default is **no.**
STUN Enable	Enables the use of STUN to discover NAT mapping. Select yes or no from the drop-down menu. The default is **no.**

Field	Description
STUN Test Enable	If the STUN Enable feature is enabled and a valid STUN server is available, the WRP500 can perform a NAT-type discovery operation when it powers on. It contacts the configured STUN server, and the result of the discovery is reported in a Warning header in all subsequent REGISTER requests. If the WRP500 detects symmetric NAT or a symmetric firewall, NAT mapping is disabled. The default is **no.**
STUN Server	IP address or fully-qualified domain name of the STUN server to contact for NAT mapping discovery.
EXT IP	External IP address to substitute for the actual IP address of the WRP500 in all outgoing SIP messages. If 0.0.0.0 is specified, no IP address substitution is performed. If this parameter is specified, the WRP500 assumes this IP address when generating SIP messages and SDP (if NAT Mapping is enabled for that line). However, the results of STUN and VIA received parameter processing, if available, supersede this statically configured value. **Note** This option requires that you have (1) a static 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. The default is **0.0.0.0**.
EXT RTP Port Min	External port mapping number of the RTP Port Min. number. If this value is not zero, the RTP port number in all outgoing SIP messages is substituted for the corresponding port value in the external RTP port range. The default is **0.**
NAT Keep Alive Intvl	Interval between NAT-mapping keep alive messages. The default is **15.**

Regional page

You can use the *Voice tab > Regional* page to localize your system with the appropriate regional settings. This page includes the following sections:

- Call Progress Tones section, page A-12
- Distinctive Ring Patterns section, page A-13
- Distinctive Call Waiting Tone Patterns section, page A-14
- Distinctive Ring/CWT Pattern Names section, page A-15
- Control Timer Values (sec) section, page A-16
- Vertical Service Activation Codes section, page A-17
- Outbound Call Codec Selection Codes section, page A-22
- Miscellaneous section, page A-23

Call Progress Tones section

This table describes the fields in the Call Progress Tones section of the Voice tab > Regional page.

Field	Description
Dial Tone	Prompts the user to enter a phone number. Reorder Tone is played automatically when *Dial Tone* or any of its alternatives times out. The default is 350@-19,440@-19;10(*/0/1+2).
Second Dial Tone	Alternative to the Dial Tone when the user dials a three-way call. The default is 420@-19,520@-19;10(*/0/1+2).
Outside Dial Tone	Alternative to the Dial Tone. It prompts the user to enter an external phone number, as opposed to an internal extension. It is triggered by a, (comma) character encountered in the dial plan. The default is 420@-19;10(*/0/1).
Prompt Tone	Prompts the user to enter a call forwarding phone number. The default is 520@-19,620@-19;10(*/0/1+2).
Busy Tone	Played when a 486 RSC is received for an outbound call. The default is 480@-19,620@-19;10(.5/.5/1+2).
Reorder Tone	Played when an outbound call has failed or after the far end hangs up during an established call. Reorder Tone is played automatically when *Dial Tone* or any of its alternatives times out. The default is 480@-19,620@-19;10(.25/.25/1+2).
Off Hook Warning Tone	Played when the caller has not properly placed the handset on the cradle. Off Hook Warning Tone is played when Reorder Tone times out. The default is 480@10,620@0;10(.125/.125/1+2)
Ring Back Tone	Played during an outbound call when the far end is ringing. The default is 440@-19,480@-19;*(2/4/1+2).
Ring Back 2 Tone	Your WRP500 plays this ringback tone instead of *Ring Back Tone* if the called party replies with a SIP 182 response without SDP to its outbound INVITE request. The default value is the same as *Ring Back Tone*, except the cadence is 1s on and 1s off. The default is 440@-19,480@-19;*(1/1/1+2).
Confirm Tone	Brief tone to notify the user that the last input value has been accepted. The default is 600@-16; 1(.25/.25/1).
SIT1 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. The default is 985@-16,1428@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0).

Field	Description
SIT2 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. The default is 914@-16,1371@-16,1777@-16;20(.274/0/1,.274/0/2,.380/0/3,0/4/0).
SIT3 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. The default is 914@-16,1371@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0).
SIT4 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. The default is 985@-16,1371@-16,1777@-16;20(.380/0/1,.274/0/2,.380/0/3,0/4/0).
MWI Dial Tone	Played instead of the Dial Tone when there are unheard messages in the caller's mailbox. The default is 350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2).
Cfwd Dial Tone	Played when all calls are forwarded. The default is 350@-19,440@-19;2(.2/.2/1+2);10(*/0/1+2).
Holding Tone	Informs the local caller that the far end has placed the call on hold. The default is 600@-19*(.1/.1/1,.1/.1/1,.1/9.5/1).
Conference Tone	Played to all parties when a three-way conference call is in progress. The default is 350@-19;20(.1/.1/1,.1/9.7/1).
Secure Call Indication Tone	Played when a call has been successfully switched to secure mode. It should be played only for a short while (less than 30 seconds) and at a reduced level (less than -19 dBm) so it does not interfere with the conversation. The default is 397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2).
Feature Invocation Tone	Played when a feature is implemented. The default is 350@-16;*(.1/.1/1).

Distinctive Ring Patterns section

This table describes the fields in the Distinctive Ring Patterns section of the Voice tab > Regional page.

Field	Description
Ring1 Cadence	Cadence script for distinctive ring 1. The default is 60(2/4).
Ring2 Cadence	Cadence script for distinctive ring 2. The default is 60(.8/.4,.8/4).

Field	Description
Ring3 Cadence	Cadence script for distinctive ring 3. The default is 60(.4/.2,.4/.2,.8/4).
Ring4 Cadence	Cadence script for distinctive ring 4. The default is 60(.3/.2,1/.2,.3/4).
Ring5 Cadence	Cadence script for distinctive ring 5. The default is 1(.5/.5).
Ring6 Cadence	Cadence script for distinctive ring 6. The default is 60(.2/.4,.2/.4,.2/4).
Ring7 Cadence	Cadence script for distinctive ring 7. The default is 60(.4/.2,.4/.2,.4/4).
Ring8 Cadence	Cadence script for distinctive ring 8. The default is 60(0.25/9.75).

Distinctive Call Waiting Tone Patterns section

This table describes the fields in the Distinctive Call Waiting Tone Patterns section of the Voice tab > Regional page.

Field	Description
CWT1 Cadence	Cadence script for distinctive CWT 1. The default is 30(.3/9.7).
CWT2 Cadence	Cadence script for distinctive CWT 2. The default is 30(.1/.1,.1/9.7).
CWT3 Cadence	Cadence script for distinctive CWT 3. The default is 30(.1/.1,.1/.1,.1/9.7).
CWT4 Cadence	Cadence script for distinctive CWT 4. The default is 30(.1/.1,.3/.1,.1/9.3).
CWT5 Cadence	Cadence script for distinctive CWT 5. The default is 1(.5/.5).
CWT6 Cadence	Cadence script for distinctive CWT 6. The default is 30(.1/.1,.3/.2,.3/9.1).
CWT7 Cadence	Cadence script for distinctive CWT 7. The default is 30(.3/.1,.3/.1,.1/9.1).
CWT8 Cadence	Cadence script for distinctive CWT 8. The default is 2.3(.3/2).

Distinctive Ring/CWT Pattern Names section

This table describes the fields in the Distinctive Ring/CWT Pattern Names section of the Voice tab > Regional page.

Field	Description
Ring1 Name	Name in an INVITE Alert-Info Header to pick distinctive ring/CWT 1 for the inbound call. The default is Bellcore-r1.
Ring2 Name	Name in an INVITE Alert-Info Header to pick distinctive ring/CWT 2 for the inbound call. The default is Bellcore-r2.
Ring3 Name	Name in an INVITE Alert-Info Header to pick distinctive ring/CWT 3 for the inbound call. The default is Bellcore-r3.
Ring4 Name	Name in an INVITE Alert-Info Header to pick distinctive ring/CWT 4 for the inbound call. The default is Bellcore-r4.
Ring5 Name	Name in an INVITE Alert-Info Header to pick distinctive ring/CWT 5 for the inbound call. The default is Bellcore-r5.
Ring6 Name	Name in an INVITE Alert-Info Header to pick distinctive ring/CWT 6 for the inbound call. The default is Bellcore-r6.
Ring7 Name	Name in an INVITE Alert-Info Header to pick distinctive ring/CWT 7 for the inbound call. The default is Bellcore-r7.
Ring8 Name	Name in an INVITE Alert-Info Header to pick distinctive ring/CWT 8 for the inbound call. The default is Bellcore-r8.

IMPORTANT: Ring and Call Waiting tones do not work the same way on all phones. When setting ring tones, consider the following recommendations:

- Begin with the default Ring Waveform, Ring Frequency, and Ring Voltage.
- If your ring cadence does not sound right, or your phone does not ring, change your Ring Waveform, Ring Frequency, and Ring Voltage to the following:
  - Ring Waveform: Sinusoid
  - Ring Frequency: 25
  - Ring Voltage: 80V

Field	Description
Ring Waveform	Waveform for the ringing signal. Choices are **Sinusoid** or **Trapezoid**. The default is **Trapezoid**.
Ring Frequency	Frequency of the ringing signal. Valid values are 10–100 (Hz). The default is **20**.
Ring Voltage	Ringing voltage. Choices are **60–90** (V). The default is **85**.
CWT Frequency	Frequency script of the call waiting tone. All distinctive CWTs are based on this tone. The default is **440@-10**.

Control Timer Values (sec) section

This table describes the fields in the Control Timer Values (sec) section of the Voice tab > Regional page.

Field	Description
Hook Flash Timer Min	Minimum on-hook time before off-hook qualifies as hook-flash. For values, less than this, the on-hook event is ignored. Range: 0.1–0.4 seconds. The default is **0.1**.
Hook Flash Timer Max	Maximum on-hook time before off-hook qualifies as hook-flash. For values greater than this, the on-hook event is treated as on-hook (no hook-flash event). Range: 0.4–1.6 seconds. The default is **0.9**.
Callee On Hook Delay	Phone must be on-hook for at least this length of time in sec before the WRP500 tears down the current inbound call. This does not apply to outbound calls. Range: 0–255 seconds. The default is **0**.
Reorder Delay	Delay after far end hangs up before reorder tone is played. 0 = plays immediately, inf = never plays. Range: 0–255 seconds. The default is **5**.
Call Back Expires	Expiration time in seconds of a call back activation. Range: 0–65535 seconds. The default is **1800**.
Call Back Retry Intvl	Call back retry interval in seconds. Range: 0–255 seconds. The default is **30**.
Call Back Delay	Delay after receiving the first SIP 18x response before declaring the remote end is ringing. If a busy response is received during this time, the WRP500 still considers the call as failed and keeps on retrying. The default is **0.5**.
VMWI Refresh Intvl	Interval between VMWI refresh to the CPE. The default is **0.**

Field	Description
Interdigit Long Timer	Long timeout between entering digits when dialing. The interdigit timer values are used as defaults when dialing. The Interdigit_Long_Timer is used after any one digit, if all valid matching sequences in the dial plan are incomplete as dialed. Range: 0–64 seconds. The default is **10**.
Interdigit Short Timer	Short timeout between entering digits when dialing. The Interdigit_Short_Timer is used after any one digit, if at least one matching sequence is complete as dialed, but more dialed digits would match other as yet incomplete sequences. Range: 0–64 seconds. The default is **3**.
CPC Delay	Delay in seconds after caller hangs up when the WRP500 starts removing the tip-and-ring voltage to the attached equipment of the called party. Range: 0–255 seconds. This feature is generally used for answer supervision on the caller side to signal to the attached equipment when the call has been connected (remote end has answered) or disconnected (remote end has hung up). This feature should be disabled for the called party (in other words, by using the same polarity for connected and idle state) and the CPC feature should be used instead. Without CPC enabled, reorder tone will is played after a configurable delay. If CPC is enabled, dial tone will be played when tip-to-ring voltage is restored Resolution is 1 second. The default is **2**.
CPC Duration	Duration in seconds for which the tip-to-ring voltage is removed after the caller hangs up. After that, tip-to-ring voltage is restored and dial tone applies if the attached equipment is still off-hook. CPC is disabled if this value is set to 0. Range: 0 to 1.000 second. Resolution is 0.001 second. The default is **0** (CPC disabled).

Vertical Service Activation Codes section

Vertical Service Activation Codes are automatically appended to the dial plan. There is no need to include them in the dial plan, but no harm is done if they are included.

This table describes the fields in the Vertical Service Activation Codes section of the Voice tab > Regional page.

Field	Description
Call Return Code	This code calls the last caller. The default is *69.
Call Redial Code	Redials the last number called. The default is *07.
Blind Transfer Code	Begins a blind transfer of the current call to the extension specified after the activation code. The default is *98.

Field	Description
Call Back Act Code	Starts a callback when the last outbound call is not busy. The default is *66.
Call Back Deact Code	Cancels a callback. The default is *86.
Call Back Busy Act Code	Starts a callback when the last outbound call is busy. The default is *05
Cfwd All Act Code	Forwards all calls to the extension specified after the activation code. The default is *72.
Cfwd All Deact Code	Cancels call forwarding of all calls. The default is *73.
Cfwd Busy Act Code	Forwards busy calls to the extension specified after the activation code. The default is *90.
Cfwd Busy Deact Code	Cancels call forwarding of busy calls. The default is *91.
Cfwd No Ans Act Code	Forwards no-answer calls to the extension specified after the activation code. The default is *92.
Cfwd No Ans Deact Code	Cancels call forwarding of no-answer calls. The default is *93.
Cfwd Last Act Code	Forwards the last inbound or outbound calls to the extension specified after the activation code. The default is *63.
Cfwd Last Deact Code	Cancels call forwarding of the last inbound or outbound calls. The default is *83.
Block Last Act Code	Blocks the last inbound call. The default is *60.
Block Last Deact Code	Cancels blocking of the last inbound call. The default is *80.
Accept Last Act Code	Accepts the last outbound call. It lets the call ring through when do not disturb or call forwarding of all calls are enabled. The default is *64.
Accept Last Deact Code	Cancels the code to accept the last outbound call. The default is *84.
CW Act Code	Enables call waiting on all calls. The default is *56.
CW Deact Code	Disables call waiting on all calls. The default is *57.

Field	Description
CW Per Call Act Code	Enables call waiting for the next call. The default is *71.
CW Per Call Deact Code	Disables call waiting for the next call. The default is *70.
Block CID Act Code	Blocks caller ID on all outbound calls. The default is *67.
Block CID Deact Code	Removes caller ID blocking on all outbound calls. The default is *68.
Block CID Per Call Act Code	Blocks caller ID on the next outbound call. The default is *81.
Block CID Per Call Deact Code	Removes caller ID blocking on the next inbound call. The default is *82.
Block ANC Act Code	Blocks all anonymous calls. The default is *77.
Block ANC Deact Code	Removes blocking of all anonymous calls. The default is *87.
DND Act Code	Enables the do not disturb feature. The default is *78.
DND Deact Code	Disables the do not disturb feature. The default is *79.
CID Act Code	Enables caller ID generation. The default is *65.
CID Deact Code	Disables caller ID generation. The default is *85.
CWCID Act Code	Enables call waiting, caller ID generation. The default is *25.
CWCID Deact Code	Disables call waiting, caller ID generation. The default is *45.
Dist Ring Act Code	Enables the distinctive ringing feature. The default is *26
Dist Ring Deact Code	Disables the distinctive ringing feature. The default is *46.
Speed Dial Act Code	Assigns a speed dial number. The default is *74.
Secure All Call Act Code	Makes all outbound calls secure. The default is *16.

Field	Description
Secure No Call Act Code	Makes all outbound calls not secure. The default is *17.
Secure One Call Act Code	Makes the next outbound call secure. (It is redundant if all outbound calls are secure by default.) The default is *18.
Secure One Call Deact Code	Makes the next outbound call not secure. (It is redundant if all outbound calls are not secure by default.) The default is *19.
Conference Act Code	If this code is specified, the user must enter it before dialing the third party for a conference call. Enter the code for a conference call.
Attn-Xfer Act Code	If the code is specified, the user must enter it before dialing the third party for a call transfer. Enter the code for a call transfer.
Modem Line Toggle Code	Toggles the line to a modem. The default is *99. Modem pass-through mode can be triggered only by pre-dialing this code.
FAX Line Toggle Code	Toggles the line to a fax machine. The default is #99.

Field	Description
Referral Services Codes	These codes tell the WRP500 what to do when the user places the current call on hold and is listening to the second dial tone. One or more *code can be configured into this parameter, such as *98, or *97|*98|*123, etc. Max total length is 79 chars. This parameter applies when the user places the current call on hold (by Hook Flash) and is listening to second dial tone. Each *code (and the following valid target number according to current dial plan) entered on the second dial-tone triggers the WRP500 to perform a blind transfer to a target number that is preceded by the service *code. For example, after the user dials *98, the WRP500 plays a special dial tone called the Prompt Tone while waiting for the user the enter a target number (which is checked according to dial plan as in normal dialing). When a complete number is entered, the WRP500 sends a blind REFER to the holding party with the Refer-To target equals to *98 *target_number*. This feature allows the WRP500 to hand off a call to an application server to perform further processing, such as call park. The *codes should not conflict with any of the other vertical service codes internally processed by the WRP500. You can empty the corresponding *code that you do not want the WRP500 to process.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Feature Dial Services Codes</td><td>These codes tell the WRP500 what to do when the user is listening to the first or second dial tone.

One or more *code can be configured into this parameter, such as *72, or *72|*74|*67|*82, etc. Max total length is 79 chars. This parameter applies when the user has a dial tone (first or second dial tone). Enter *code (and the following target number according to current dial plan) entered at the dial tone triggers the WRP500 to call the target number preceded by the *code. For example, after user dials *72, the WRP500 plays a special tone called a Prompt tone while awaiting the user to enter a valid target number. When a complete number is entered, the WRP500 sends a INVITE to *72 target_number as in a normal call. This feature allows the proxy to process features like call forward (*72) or Block Caller ID (*67).

The *codes should not conflict with any of the other vertical service codes internally processed by the WRP500. You can empty the corresponding *code that you do not want to the WRP500 to process.

You can add a parameter to each *code in Features Dial Services Codes to indicate what tone to play after the *code is entered, such as *72‘c‘|*67‘p‘. Below are a list of allowed tone parameters (note the use of back quotes surrounding the parameter w/o spaces)

‘c‘ = <Cfwd Dial Tone>
‘d‘ = <Dial Tone>
‘m‘ = <MWI Dial Tone>
‘o‘ = <Outside Dial Tone>
‘p‘ = <Prompt Dial Tone>
‘s‘ = <Second Dial Tone>
‘x‘ = No tones are place, x is any digit not used above

If no tone parameter is specified, the WRP500 plays Prompt tone by default.

If the *code is not to be followed by a phone number, such as *73 to cancel call forwarding, do not include it in this parameter. In that case, simple add that *code in the dial plan and the WRP500 send INVITE *73@..... as usual when user dials *73.</td></tr>
</table>

Outbound Call Codec Selection Codes section

These codes are automatically appended to the dial plan. Thus, they do not need to be included in the dial plan, but there is no harm in doing so.

This table describes the fields in the Outbound Call Codec Section Codes section of the Voice tab > Regional page.

Field	Description
Prefer G711u Code	Makes this codec the preferred codec for the associated call. The default is *017110.
Force G711u Code	Makes this codec the only codec that can be used for the associated call. The default is *027110.
Prefer G711a Code	Makes this codec the preferred codec for the associated call. The default is *017111
Force G711a Code	Makes this codec the only codec that can be used for the associated call. The default is *027111.
Prefer G729a Code	Makes this codec the preferred codec for the associated call. The default is *01729.
Force G729a Code	Makes this codec the only codec that can be used for the associated call. The default is *02729.

Miscellaneous section

This table describes the fields in the Miscellaneous section of the Voice tab > Regional page.

Field	Description
Set Local Date (mm/dd)	Sets the local date (mm stands for months and dd stands for days). The year is optional and uses two or four digits.
Set Local Time (HH/mm)	Sets the local time (hh stands for hours and mm stands for minutes). Seconds are optional.
FXS Port Impedance	Sets the electrical impedance of the FXS port. Choices are 600, 900, 600+2.16uF, 900+2.16uF, 270+750||150nF, 220+850||120nF, 220+820||115nF, or 200+600||100nF. The default is 600.
FXS Port Input Gain	Input gain in dB, up to three decimal places. The range is 6.000 to -12.000. The default is -3.
FXS Port Output Gain	Output gain in dB, up to three decimal places. The range is 6.000 to -12.000. The Call Progress Tones and DTMF playback level are not affected by the *FXS Port Output Gain* parameter. The default is -3.
DTMF Playback Level	Local DTMF playback level in dBm, up to one decimal place. The default is -7.3.

Field	Description
DTMF Playback Length	Local DTMF playback duration in milliseconds. The default is .1.
DTMF Playback Twist	Local DTMF playback duration. The default is 1.3.
Caller ID Method	The following choices are available: • **Bellcore (N.Amer,China)**—CID, CIDCW, and VMWI. FSK sent after first ring (same as ETSI FSK sent after first ring) (no polarity reversal or DTAS). • **DTMF (Finland, Sweden)**—CID only. DTMF sent after polarity reversal (and no DTAS) and before first ring. • **DTMF (Denmark)**—CID only. DTMF sent before first ring with no polarity reversal and no DTAS. • **ETSI DTMF**—CID only. DTMF sent after DTAS (and no polarity reversal) and before first ring. • **ETSI DTMF With PR**—CID only. DTMF sent after polarity reversal and DTAS and before first ring. • **ETSI DTMF After Ring**—CID only. DTMF sent after first ring (no polarity reversal or DTAS). • **ETSI FSK**—CID, CIDCW, and VMWI. FSK sent after DTAS (but no polarity reversal) and before first ring. Waits for ACK from CPE after DTAS for CIDCW. • **ETSI FSK With PR (UK)**—CID, CIDCW, and VMWI. FSK is sent after polarity reversal and DTAS and before first ring. Waits for ACK from CPE after DTAS for CIDCW. Polarity reversal is applied only if equipment is on hook. The default is Bellcore(N.Amer, China).
Caller ID FSK Standard	The WRP500 supports bell 202 and v.23 standards for caller ID generation. Select the FSK standard you want to use, bell 202 or v.23. The default is bell 202.
Feature Invocation Method	Select the method you want to use, Default or Sweden default. The default is Default.

Line page

You can use the *Voice tab* > *Line* page to configure the lines for voice service. This page includes the following sections:

- Line Enable section, page A-25
- Streaming Audio Server (SAS) section, page A-25
- NAT Settings section, page A-26
- Network Settings section, page A-27
- SIP Settings section, page A-28

- Call Feature Settings section, page A-30
- Proxy and Registration section, page A-31
- Subscriber Information section, page A-32
- Supplementary Service Subscription section, page A-32
- Audio Configuration section, page A-34
- Dial Plan section, page A-36
- FXS Port Polarity Configuration section, page A-38

In a configuration profile, the Line parameters must be appended with the appropriate numeral (for example, [1] or [2]) to identify the line to which the setting applies.

Line Enable section

This table describes the fields in the Line Enable section of the Voice tab > Line page.

Field	Description
Line Enable	To enable this line for service, select yes. Otherwise, select no. The default is **yes**.

Streaming Audio Server (SAS) section

This table describes the fields in the Streaming Audio Server (SAS) section of the Voice tab > Line page.

Field	Description
SAS Enable	To enable the use of the line as a streaming audio source, select yes. Otherwise, select no. If enabled, the line cannot be used for outgoing calls. Instead, it auto-answers incoming calls and streams audio RTP packets to the caller. The default is **no**.

Field	Description
SAS DLG Refresh Intvl	If this value is not zero, it is the interval at which the streaming audio server sends out session refresh (SIP re-INVITE) messages to determine whether the connection to the caller is still active. If the caller does not respond to the refresh message, the WRP500 ends this call with a SIP BYE message. The range is 0 to 255 seconds (0 means that the session refresh is disabled). The default is 30.
SAS Inbound RTP Sink	This setting works around devices that do not play inbound RTP if the streaming audio server line declares itself as a send-only device and tells the client not to stream out audio. Enter a Fully Qualified Domain Name (FQDN) or IP address of an RTP sink; this value is used by the streaming audio server line in the SDP of its 200 response to an inbound INVITE message from a client. The purpose of this parameter is to work around devices that do not play inbound RTP if the SAS line declares itself as a send-only device and tells the client not to stream out audio. This parameter is a FQDN or IP address of a RTP sink to be used by the SAS line in the SDP of its 200 response to inbound INVITE from a client. It will appear in the c = line and the port number and, if specified, in the m = line of the SDP. If this value is not specified or equal to 0, then c = 0.0.0.0 and a=sendonly will be used in the SDP to tell the SAS client to not to send any RTP to this SAS line. If a non-zero value is specified, then a=sendrecv and the SAS client will stream audio to the given address. Special case: If the value is $IP, then the SAS line's own IP address is used in the c = line and a=sendrecv. In that case the SAS client will stream RTP packets to the SAS line. The default value is empty.

NAT Settings section

This table describes the fields in the NAT Settings section of the Voice tab > Line page.

Field	Description
NAT Mapping Enable	To use externally mapped IP addresses and SIP/RTP ports in SIP messages, select yes. Otherwise, select no. The default is **no**.
NAT Keep Alive Enable	To send the configured NAT keep alive message periodically, select yes. Otherwise, select no. The default is **no**.

Field	Description
NAT Keep Alive Msg	Enter the keep alive message that should be sent periodically to maintain the current NAT mapping. If the value is $NOTIFY, a NOTIFY message is sent. If the value is $REGISTER, a REGISTER message without contact is sent. The default is $**NOTIFY**.
NAT Keep Alive Dest	Destination that should receive NAT keep alive messages. If the value is $PROXY, the messages are sent to the current proxy server or outbound proxy server. The default is $**PROXY**.

Network Settings section

This table describes the fields in the Network Settings section of the Voice tab > Line page.

Field	Description
SIP ToS/DiffServ Value	TOS/DiffServ field value in UDP IP packets carrying a SIP message. The default is **0x68**.
SIP CoS Value [0-7]	CoS value for SIP messages. The default is **3**.
RTP ToS/DiffServ Value	ToS/DiffServ field value in UDP IP packets carrying RTP data. The default is **0xb8**.
RTP CoS Value [0-7]	CoS value for RTP data. The default is **6**.
Network Jitter Min/Max	Determines how jitter buffer range of WRP500 when Network Jitter Mode is adaptive. Jitter buffer size is adjusted dynamically. The default value of Network Jitter Min is **10ms**. The default value of Network Jitter Max is **200ms**.
Network Jitter Mode	Specify whether the jitter buffer should be adjusted or use some constant interval value. Select the appropriate setting: **adaptive**, **static**. The default is **adaptive**.

SIP Settings section

This table describes the fields in the SIP Settings section of the Voice tab > Line page.

Field	Description
SIP Transport	The TCP choice provides “guaranteed delivery”, which assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent. As a result, TCP overcomes the main disadvantages of UDP. In addition, for security reasons, most corporate firewalls block UDP ports. With TCP, new ports do not need to be opened or packets dropped, because TCP is already in use for basic activities such as Internet browsing or e-commerce. Options are: **UDP**, **TCP**, **TLS**. The default is **UDP**.
SIP Port	Port number of the SIP message listening and transmission port. The default is **5060**.
SIP 100REL Enable	To enable the support of 100REL SIP extension for reliable transmission of provisional responses (18x) and use of PRACK requests, select yes. Otherwise, select no. The default is **no**.
EXT SIP Port	The external SIP port number.
Auth Resync-Reboot	If this feature is enabled, the WRP500 authenticates the sender when it receives the NOTIFY resync reboot (RFC 2617) message. To use this feature, select yes. Otherwise, select no. The default is **yes**.
SIP Proxy-Require	The SIP proxy can support a specific extension or behavior when it sees this header from the user agent. If this field is configured and the proxy does not support it, it responds with the message, unsupported. Enter the appropriate header in the field provided.
SIP Remote-Party-ID	To use the Remote-Party-ID header instead of the From header, select yes. Otherwise, select no. The default is **yes**.
SIP GUID	The Global Unique ID is generated for each line for each device. When it is enabled, the WRP500 adds a GUID header in the SIP request. The GUID is generated the first time the unit boots up and stays with the unit through rebooting and even factory reset. This feature was requested by Bell Canada (Nortel) to limit the registration of SIP accounts. The default is **no**.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SIP Debug Option</td><td>SIP messages are received at or sent from the proxy listen port. This feature controls which SIP messages to log. Choices are as follows:
none—No logging.
1-line—Logs the start-line only for all messages.
1-line excl. OPT—Logs the start-line only for all messages except OPTIONS requests/responses.
1-line excl. NTFY—Logs the start-line only for all messages except NOTIFY requests/responses.
1-line excl. REG—Logs the start-line only for all messages except REGISTER requests/responses.
1-line excl. OPT|NTFY|REG—Logs the start-line only for all messages except OPTIONS, NOTIFY, and REGISTER requests/responses.
full—Logs all SIP messages in full text.
full excl. OPT—Logs all SIP messages in full text except OPTIONS requests/responses.
full excl. NTFY—Logs all SIP messages in full text except NOTIFY requests/responses.
full excl. REG—Logs all SIP messages in full text except REGISTER requests/responses.
full excl. OPT|NTFY|REG—Logs all SIP messages in full text except for OPTIONS, NOTIFY, and REGISTER requests/responses.
The default is none.</td></tr>
<tr><td>RTP Log Intvl</td><td>The interval for the RTP log. The default value is 0.</td></tr>
<tr><td>Restrict Source IP</td><td>If Lines 1 and 2 use the same SIP Port value and the Restrict Source IP feature is enabled, the proxy IP address for Lines 1 and 2 is treated as an acceptable IP address for both lines. To enable the Restrict Source IP feature, select yes. Otherwise, select no. If configured, the WRP500 will drop all packets sent to its SIP Ports originated from an untrusted IP address. A source IP address is untrusted if it does not match any of the IP addresses resolved from the configured Proxy (or Outbound Proxy if Use Outbound Proxy is yes).

The default is no.</td></tr>
<tr><td>Referor Bye Delay</td><td>Controls when the WRP500 sends BYE to terminate stale call legs upon completion of call transfers. Multiple delay settings (Referor, Refer Target, Referee, and Refer-To Target) are configured on this screen. For the Referor Bye Delay, enter the appropriate period of time in seconds.

The default is 4.</td></tr>
<tr><td>Refer Target Bye Delay</td><td>For the Refer Target Bye Delay, enter the appropriate period of time in seconds.

The default is 0.</td></tr>
</table>

Field	Description
Referee Bye Delay	For the Referee Bye Delay, enter the appropriate period of time in seconds. The default is **0**.
Refer-To Target Contact	To contact the refer-to target, select yes. Otherwise, select no. The default is **no**.
Sticky 183	If this feature is enabled, the IP telephony ignores further 180 SIP responses after receiving the first 183 SIP response for an outbound INVITE. To enable this feature, select yes. Otherwise, select no. The default is **no**.
Auth INVITE	When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy.
Use Anonymous With RPID	Set value of Remote Party ID to “anonymous, yes”
Use Local Addr in FROM	Use IP address in From header, no
Reply 182 On Call Waiting	Send 182 response when enter call waiting, no

Call Feature Settings section

This table describes the fields in the Call Feature Settings section of the Voice tab > Line page.

Field	Description
Blind Attn-Xfer Enable	Enables the WRP500 to perform an attended transfer operation by ending the current call leg and performing a blind transfer of the other call leg. If this feature is disabled, the WRP500 performs an attended transfer operation by referring the other call leg to the current call leg while maintaining both call legs. To use this feature, select yes. Otherwise, select no. The default is **no**.
Xfer When Hangup Conf	Makes the ATA perform a transfer when a conference call has ended. Select yes or no from the drop-down menu. The default is **yes**.
MoH server	Address of music on hold server
Conference Bridge URL	URL of Conference server

Proxy and Registration section

This table describes the fields in the Proxy and Registration section of the Voice tab > Line page.

Field	Description
Proxy	SIP proxy server for all outbound requests.
Outbound Proxy	SIP Outbound Proxy Server where all outbound requests are sent as the first hop.
Use Outbound Proxy	Enables the use of an *Outbound Proxy*. If set to no, the *Outbound Proxy* and *Use OB Proxy in Dialog* parameters are ignored. The default is **no**.
Use OB Proxy In Dialog	Whether to force SIP requests to be sent to the outbound proxy within a dialog. Ignored if the parameter *Use Outbound Proxy* is no, or the *Outbound Proxy* parameter is empty. The default is **yes**.
Register	Enable periodic registration with the *Proxy* parameter. This parameter is ignored if *Proxy* is not specified. The default is **yes**.
Make Call Without Reg	Allow making outbound calls without successful (dynamic) registration by the unit. If No, dial tone will not play unless registration is successful. The default is **no**.
Register Expires	Allow answering inbound calls without successful (dynamic) registration by the unit. If proxy responded to REGISTER with a smaller Expires value, the WRP500 will renew registration based on this smaller value instead of the configured value. If registration failed with an Expires too brief error response, the WRP500 will retry with the value given in the Min-Expires header in the error response. The default is **3600**.
Ans Call Without Reg	Expires value in sec in a REGISTER request. The WRP500 will periodically renew registration shortly before the current registration expired. This parameter is ignored if the *Register* parameter is no. Range: 0 – (231 – 1) sec
Use DNS SRV	Whether to use DNS SRV lookup for Proxy and Outbound Proxy. The default is **no**.
DNS SRV Auto Prefix	If enabled, the WRP500 will automatically prefix the Proxy or Outbound Proxy name with _sip._udp when performing a DNS SRV lookup on that name. The default is **no**.

Field	Description
Proxy Fallback Intvl	This parameter sets the delay (sec) after which the WRP500 will retry from the highest priority proxy (or outbound proxy) servers after it has failed over to a lower priority server. This parameter is useful only if the primary and backup proxy server list is provided to the WRP500 via DNS SRV record lookup on the server name. (Using multiple DNS A record per server name does not allow the notion of priority and so all hosts will be considered at the same priority and the WRP500 will not attempt to fall back after a fail over). The default is **3600**
Proxy Redundancy Method	The WRP500 will make an internal list of proxies returned in DNS SRV records. In normal mode, this list will contain proxies ranked by weight and priority. if Based on SRV port is configured the WRP500 does normal first, and also inspect the port number based on 1st proxy's port on the list. The default is **Normal**.
Voice Mail Server	Enter the URL or IP address of the server.
Mailbox Subscribe Expires	Expiry time to the voice mail server. The time to send another subscribe message to the voice mail server. The default is 2147483647.

Subscriber Information section

This table describes the fields in the Subscriber Information section of the Voice tab > Line page.

Field	Description
Display Name	Display name for caller ID.
User ID	Extension number for this line.
Password	Password for this line.
Use Auth ID	To use the authentication ID and password for SIP authentication, select yes. Otherwise, select no to use the user ID and password. The default is **no**.
Auth ID	Authentication ID for SIP authentication.
Directory Number	Enter the number for this line.

Supplementary Service Subscription section

The WRP500 provides native support of a large set of enhanced or supplementary services. All of these services are optional. The parameters listed in the following table are used to enable or disable a specific supplementary service. A supplementary service should be disabled if a) the user has not subscribed for it, or b) the Service Provider intends to support similar service using other means than relying on the WRP500.

This table describes the fields in the Supplementary Service Subscription section of the Voice tab > Line page.

Field	Description
Call Waiting Serv	Enable Call Waiting Service. The default is **yes**.
Block CID Serv	Enable Block Caller ID Service. The default is **yes**.
Block ANC Serv	Enable Block Anonymous Calls Service The default is **yes**.
Dist Ring Serv	Enable Distinctive Ringing Service The default is **yes**.
Cfwd All Serv	Enable Call Forward All Service The default is **yes**.
Cfwd Busy Serv	Enable Call Forward Busy Service The default is **yes**.
Cfwd No Ans Serv	Enable Call Forward No Answer Service The default is **yes**.
Cfwd Sel Serv	Enable Call Forward Selective Service The default is **yes**.
Cfwd Last Serv	Enable Forward Last Call Service The default is **yes**.
Block Last Serv	Enable Block Last Call Service The default is **yes**.
Accept Last Serv	Enable Accept Last Call Service The default is **yes**.
DND Serv	Enable Do Not Disturb Service The default is **yes**.
CID_Serv	Enable Caller ID Service The default is **yes**.
CWCID Serv	Enable Call Waiting Caller ID Service The default is **yes**.
Call Return Serv	Enable Call Return Service The default is **yes**.
Call Redial Serv	Enable Call Redial Service.
Call Back Serv	Enable Call Back Service.

Field	Description
Three Way Call Serv	Enable Three Way Calling Service. Three Way Calling is required for Three Way Conference and Attended Transfer. The default is **yes**.
Three Way Conf Serv	Enable Three Way Conference Service. Three Way Conference is required for Attended Transfer. The default is **yes**.
Attn Transfer Serv	Enable Attended Call Transfer Service. Three Way Conference is required for Attended Transfer. The default is **yes**.
Unattn Transfer Serv	Enable Unattended (Blind) Call Transfer Service. The default is **yes**.
MWI Serv	Enable MWI Service. MWI is available only if a Voice Mail Service is set-up in the deployment. The default is **yes**.
VMWI Serv	Enable VMWI Service (FSK). The default is **yes**.
Speed Dial Serv	Enable Speed Dial Service. The default is **yes**.
Secure Call Serv	Enable Secure Call Service. The default is **yes**.
Referral Serv	Enable Referral Service. See the *Referral Services Codes* parameter for more details. The default is **yes**.
Feature Dial Serv	Enable Feature Dial Service. See the *Feature Dial Services Codes* parameter for more details. The default is **yes**.
Service Announcement Serv	Enable Service Announcement Service. The default is **no**.

Audio Configuration section

A codec resource is considered as allocated if it has been included in the SDP codec list of an active call, even though it eventually may not be the one chosen for the connection. So, if the G.729a codec is enabled and included in the codec list, that resource is tied up until the end of the call whether or not the call actually uses G.729a. If the G.729a resource is already allocated and since only one G.729a resource is allowed per device, no other low-bit-rate codec may be allocated for subsequent calls; the only choices are G711a and G711u.

This table describes the fields in the Audio Configuration section of the Voice tab > Line page.

Field	Description
Preferred Codec	Preferred codec for all calls. (The actual codec used in a call still depends on the outcome of the codec negotiation protocol.) Select one of the following: **G711u**, **G711a**, **G729a.** The default is **G711u.**
Second Preferred Codec	Second preferred codec for all calls. (The actual codec used in a call still depends on the outcome of the codec negotiation protocol.) Select one of the following: **Unspecified**, **G711u, G711a, G729a.** The default is **Unspecified.**
Third Preferred Codec	Third preferred codec for all calls. (The actual codec used in a call still depends on the outcome of the codec negotiation protocol.) Select one of the following: **Unspecified, G711u, G711a, G729a.** The default is **Unspecified.**
Use Pref Codec Only	To use only the preferred codec for all calls, select yes. (The call fails if the far end does not support this codec.) Otherwise, select no. The default is **no**.
Silence Supp Enable	To enable silence suppression so that silent audio frames are not transmitted, select yes. Otherwise, select no. The default is **no**.
G729a Enable	To enable the use of the G.729a codec at 8 kbps, select yes. Otherwise, select no. The default is **yes**.
Echo Canc Enable	To enable the use of the echo canceler, select yes. Otherwise, select no. The default is **yes**.
Echo Supp Enable	To enable the use of the echo suppressor, select yes. Otherwise, select no. The default is **yes**.
FAX CED Detect Enable	To enable detection of the fax Caller-Entered Digits (CED) tone, select yes. Otherwise, select no. The default is **yes**.
FAX V21 Detect Enable	To enable detection of the fax v.21 signal, select yes. Otherwise, select no. The default is **yes**.
FAX Passthru Codec	Select the codec for fax passthrough, G711u or G711a. The default is **G711u**.
DTMF Process INFO	To use the DTMF process info feature, select yes. Otherwise, select no. The default is **yes**.
FAX Codec Symmetric	To force the ATA to use a symmetric codec during fax passthrough, select yes. Otherwise, select no. The default is **yes**.

Field	Description
FAX Passthru Method	Select the fax passthrough method: None, NSE, or ReINVITE. The default is **NSE**.
DTMF Tx Method	Select the method to transmit DTMF signals to the far end: **InBand, AVT, INFO, Auto.** InBand sends DTMF using the audio path. AVT sends DTMF as events. INFO uses the SIP INFO method. Auto uses InBand or AVT based on the outcome of codec negotiation. The default is **Auto**.
FAX Process NSE	To use the fax process NSE feature, select yes. Otherwise, select no. The default is **yes**.
Hook Flash Tx Method	Select the method for signaling hook flash events: None, AVT, or INFO. None does not signal hook flash events. AVT uses RFC2833 AVT (event = 16). INFO uses SIP INFO with the single line signal=hf in the message body. The MIME type for this message body is taken from the Hook Flash MIME Type setting. The default is **None**.
Release Unused Codec	This feature allows the release of codecs not used after codec negotiation on the first call, so that other codecs can be used for the second line. To use this feature, select yes. Otherwise, select no. The default is **yes**.
FAX T38 Redundancy	Select the appropriate number to indicate the number of previous packet payloads to repeat with each packet. Choose 0 for no payload redundancy. The higher the number, the larger the packet size and the more bandwidth consumed. The default is **1**.
FAX Tone Detect Mode	If you want the Gateway to detect the fax tone whether the Gateway is a caller or callee, select caller or callee. If you want the Gateway to detect the fax tone only if the Gateway is the caller, select caller only. If you want the Gateway to detect the fax tone only if the Gateway is the callee, select callee only. This parameter has three possible values: caller or callee - The WRP500 will detect FAX tone whether it is callee or caller caller only - The WRP500 will detect FAX tone only if it is the caller callee only - The WRP500 will detect FAX tone only if it is the callee The default is **caller or callee**.
FAX Enable T38	Set to yes to enable fax T.38 mode
FAX T38 ECM Enable	Set to yes to enable T38 error correction mode

Dial Plan section

The default dial plan script for each line is as follows:

(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxx|xxxxxxxxxxxx.).

These tables describe the fields in the Dial Plan section of the Voice tab > Line page, which provide the syntax for a dial plan expression.

Dial Plan Entry	Functionality
*xx	Allow arbitrary 2 digit star code
[3469]11	Allow x11 sequences
0	Operator
00	International Operator
[2-9]xxxxxx	US local number
1xxx[2-9]xxxxxx	US 1 + 10-digit long distance number
xxxxxxxxxxxx.	Everything else (International long distance, FWD, ...)

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Dial Plan</td><td>Dial plan script for this line.

The default is
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxxx.)

Each parameter is separated by a semi-colon (;).

Example 1:

<code>*1xxxxxxxxxx<:@fwdnat.pulver.com:5082;uid=jsmith;pwd=xyz</code>

Example 2:

<code>*1xxxxxxxxxx<:@fwd.pulver.com;nat;uid=jsmith;pwd=xyz</code>

Example 3:

<code>[39]11<:@gw0></code></td></tr>
<tr><td>Enable IP Dialing</td><td>Enable or disable IP dialing.

If IP dialing is enabled, one can dial [user-id@]a.b.c.d[:port], where ‘@’, ‘.’, and ‘:’ are dialed by entering *, user-id must be numeric (like a phone number) and a, b, c, d must be between 0 and 255, and port must be larger than 255. If port is not given, 5060 is used. Port and User-Id are optional. If the user-id portion matches a pattern in the dial plan, then it is interpreted as a regular phone number according to the dial plan. The INVITE message, however, is still sent to the outbound proxy if it is enabled.

The default is no.</td></tr>
<tr><td>Emergency Number</td><td>Comma separated list of emergency number patterns. If outbound call matches one of the pattern, the WRP500 will disable hook flash event handling. The condition is restored to normal after the phone is on-hook. Blank signifies no emergency number. Maximum number length is 63 characters.

The default is blank.</td></tr>
</table>

FXS Port Polarity Configuration section

This table describes the fields in the FXS Port Polarity Configuration section of the Voice tab > Line page.

Field	Description
Idle Polarity	Polarity before a call is connected: Forward or Reverse. The default is **Forward**.
Caller Conn Polarity	Polarity after an outbound call is connected: Forward or Reverse. The default is **Forward**.
Callee Conn Polarity	Polarity after an inbound call is connected: Forward or Reverse. The default is **Forward**.

User page

You can use this page to configure the user settings. This page includes the following sections:

- Call Forward Settings section, page A-38
- Selective Call Forward Settings section, page A-39
- Speed Dial Settings section, page A-39
- Supplementary Service Settings section, page A-40
- Distinctive Ring Settings section, page A-41
- Ring Settings section, page A-41

When a call is made from Line 1 or Line 2, the WRP500 uses the user and line settings for that line; there is no user login support. Per user parameter tags must be appended with [1] or [2] (corresponding to line 1 or 2) in the configuration profile. It is omitted below for readability.

Call Forward Settings section

This table describes the fields in the Call Forward Settings section of the Voice tab > User page.

Field	Description
Cfwd All Dest	Forward number for Call Forward All Service The default is blank.
Cfwd Busy Dest	Forward number for Call Forward Busy Service. Same as Cfwd All Dest. The default is blank.

Field	Description
Cfwd No Ans Dest	Forward number for Call Forward No Answer Service. Same as Cfwd All Dest. The default is blank.
Cfwd No Ans Delay	Delay in sec before Call Forward No Answer triggers. Same as Cfwd All Dest. The default is **20**.

Selective Call Forward Settings section

This table describes the fields in the Selective Call Forward Settings section of the Voice tab > User page.

Field	Description
Cfwd Sel1- 8 Caller	Caller number pattern to trigger Call Forward Selective 1, 2, 3, 4, 5, 6, 7, or 8. The default is blank.
Cfwd Sel1 - 8 Dest	Forward number for Call Forward Selective 1, 2, 3, 4, 5, 6, 7, or 8. Same as Cfwd All Dest. The default is blank.
Block Last Caller	ID of caller blocked via the Block Last Caller service. The default is blank.
Accept Last Caller	ID of caller accepted via the Accept Last Caller service. The default is blank.
Cfwd Last Caller	The Caller number that is actively forwarded to *Cfwd Last Dest* by using the Call Forward Last activation code The default is blank.
Cfwd Last Dest	Forward number for the *Cfwd Last Caller* parameter. Same as Cfwd All Dest. The default is blank.

Speed Dial Settings section

This table describes the fields in the Speed Dial Settings section of the Voice tab > User page.

Field	Description
Speed Dial 2-9	Target phone number (or URL) assigned to speed dial 2, 3, 4, 5, 6, 7, 8, or 9. The default is blank.

Supplementary Service Settings section

The WRP500 provides native support of a large set of enhanced or supplementary services. All of these services are optional. The parameters listed in the following table are used to enable or disable a specific supplementary service. A supplementary service should be disabled if a) the user has not subscribed for it, or b) the Service Provider intends to support similar service using other means than relying on the WRP500.

This table describes the fields in the Supplementary Service Settings section of the Voice tab > User page.

Field	Description
CW Setting	Call Waiting on/off for all calls. The default is **yes**.
Block CID Setting	Block Caller ID on/off for all calls. The default is **no**.
Block ANC Setting	Block Anonymous Calls on or off. The default is **no**.
DND Setting	DND on or off. The default is **no**.
CID Setting	Caller ID Generation on or off. The default is **yes**.
CWCID Setting	Call Waiting Caller ID Generation on or off. The default is **yes**.
Dist Ring Setting	Distinctive Ring on or off. The default is **yes**.
Secure Call Setting	If yes, all outbound calls are secure calls by default. The default is **no**.
Message Waiting	This value is updated when there is voice mail notification received by the WRP500. The user can also manually modify it to clear or set the flag. Setting this value to yes can activate stutter tone and VMWI signal. This parameter is stored in long term memory and will survive after reboot or power cycle. The default is **no**.
Accept Media Loopback Request	Controls how to handle incoming requests for loopback operation. Choices are: **Never**, **Automatic**, and **Manual**, where: • **never**—never accepts loopback calls; reply 486 to the caller • **automatic—**automatically accepts the call without ringing • **manual** —rings the phone first, and the call must be picked up manually before loopback starts. The default is **Automatic**.

Field	Description
Media Loopback Mode	The loopback mode to assume locally when making call to request media loopback. Choices are: **Source** and **Mirror.** Default is **Source**. Note that if the WRP500 answers the call, the mode is determined by the caller.
Media Loopback Type	The loopback type to use when making call to request media loopback operation. Choices are Media and Packet. Default is **Media**. Note that if the WRP500 answers the call, then the loopback type is determined by the caller (the WRP500 always picks the first loopback type in the offer if it contains multiple types.)

Distinctive Ring Settings section

Caller number patterns are matched from Ring 1 to Ring 8. The first match (not the closest match) will be used for alerting the subscriber.

This table describes the fields in the Distinctive Ring Settings section of the Voice tab > User page.

Field	Description
Ring1 - 8 Caller	Caller number pattern to play Distinctive Ring/CWT 1, 2, 3, 4, 5, 6, 7, 8. The default is **blank**.

Ring Settings section

This table describes the fields in the Ring Settings section of the Voice tab > User page.

Field	Description
Default Ring	Default ringing pattern, 1 – 8, for all callers. The default is **1**.
Default CWT	Default CWT pattern, 1 – 8, for all callers. The default is **1**.
Hold Reminder Ring	Ring pattern for reminder of a holding call when the phone is on-hook. The default is **8**.
Call Back Ring	Ring pattern for call back notification. The default is **7**.

Data Fields

This appendix describes the fields for the data parameters. After you log in, you can view or perform configuration from these tabs in the GUI:

- Quick Setup
- Interface Setup
- Network Setup
- Voice
- VPN
- Administration
- Diagnostics
- Status

Interface Setup module

The Interface Setup module includes these pages:

- Interface Setup > WAN
- Interface Setup > LAN
- Interface Setup > Wi-Fi Settings
- Interface Setup > Management Interface

Interface Setup > WAN page

Interface Setup > WAN > Internet Setup

From the **Interface Setup > WAN > Internet Setup** page, you can perform this configuration:

- Add a new WAN interface
- Edit an existing AN interface
- Configure a WAN interface

Add a New WAN Interface

Click the plus symbol to the right of the Ethernet WAN1 link.

Edit an Existing WAN Interface

Click the pen symbol to the right of the existing interface.

Configure WAN Interface

Either add or edit a WAN interface, The user sees a window with the fields that are described in the table that follows.

To save your settings, click the **Submit** button.

Field	Description
WAN	The interface ID (not applicable). This value cannot be changed.
VLAN ID	The ID for the VLAN (not applicable). VLAN 0, is used for the WAN interface, and this value cannot be changed.
Connection Type	Choose the connection type as required by your Internet Service Provider (ISP): • Automatic Configuration - DHCP • Static IP • PPPoE (for ADSLuser) • PPTP • L2TP
Automatic Configuration - DHCP	This type of connection is often used with cable modems. Select this option if your ISP did not assign a static IP address to your account and instead uses Dynamic Host Control Protocol (DHCP) to assign an IP address dynamically. No other information is required for this selection.
Static IP	Select this option if your ISP provides you with a static IP address. Enter the following required information as provided by your ISP: Internet IP Address, Subnet Mask, and Default Gateway IP address. Optionally, you can enter the IP addresses of up to three Domain Name System (DNS) servers, or leave the fields blank to allow a DNS server to be chosen dynamically. DNS servers translate website names such as www.cisco.com into routable IP addresses. • **Internet IP Address and Subnet Mask**–This is the router IP address and subnet mask as seen by external users on the Internet (including your ISP). If your Internet connection requires a static IP address, then your ISP will provide you with a Static IP Address and Subnet Mask. • **Default Gateway**–Your ISP will provide you with the Gateway IP Address. • **DNS 1-3**–The Domain Name System (DNS) is the method by which the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, type that IP Address in one of these fields. You can enter up to three DNS Server IP Addresses here. The router will use these for quicker access to functioning DNS servers.

Field	Description
PPPoE (for ADSLuser)	Select this option if your ISP uses PPPoE (commonly with DSL services). Enter the User Name and Password for your ISP account. If required by your ISP, also enter the Service Name. Finally, choose either the Keep Alive or Connect On Demand option. With Connect on Demand, the router opens a connection only when a user attempts to connect to the Internet. The connection is automatically terminated if there is a period of inactivity longer than the specified Max Idle Time (in minutes). This option is recommended if your billing is based on the time that you are connected. Alternatively, the Keep Alive option enables the router to send messages to keep the connection permanently open, regardless of the level of Internet activity by your users. • **User Name and Password**–Enter the User Name and Password you use when you log on to your ISP through a PPPoE connection. • **Service Name**–If provided by your ISP, enter the Service Name. • **Connect on Demand**–You can configure the Router to terminate the Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain active at all times, click the radio button next to Keep Alive. Otherwise, enter the number of minutes you want to elapse before your Internet connection terminates. • **Keep Alive**–This option keeps you connected to the Internet indefinitely, even when your connection sits idle. To use this option, click the radio button next to Keep Alive. The default Redial Period is 30 seconds (that is, the router checks the Internet connection every 30 seconds).
MTU	Size, in bytes, of the largest packet that can be sent through the network. This value is typically 1500 bytes, however it might need to be lower for some broadband services. Check with your service provider for specific requirements.

Interface Setup > WAN > Internet Option

Some ISPs may require the following information. Enter this information only if your ISP instructs you to do so.

Field	Description
Host Name	A host name for the WRP500. Some service providers, usually cable service providers, require a host name and a domain name as identification. In most cases, these fields can be left blank.
Domain Name	A domain name for the WRP500. Some service providers, usually cable service providers, require a host name and a domain name as identification. In most cases, these fields can be left blank.

Field	Description
IPv4 Static DNS 1 - 3	Optionally, enter the IP addresses for up to three Domain Name System (DNS) servers.
Scheduled WAN Reconnect	Enabled this feature will cause all WAN connections to be restarted at the specified Reconnect Time.
Reconnect Time	Set the reconnect time by hour and minute for Scheduled WAN Reconnect feature.

Internet Setup > WAN > Mobile Network

Field	Description
Global Settings	
Connect Mode	Select Auto to enable your 3G USB modem to establish a connection automatically. Select Manual to connect or disconnect your mobile connection manually. Please note that Ethernet Connection Recovery and Interface Connection Failover will work only if the Connection Mode is set to Auto. If you select Auto, you must select either Connect on Demand and Keep Alive. • Auto/Manual Select Auto to enable your modem to establish connection automatically. Select Manual to connect or disconnect your modem connection manually. Please note that Ethernet Connection Recovery and Interface Connection Failover will work only if the Connection Mode is set to Auto. • Connect on Demand Select this option to enable the router to terminate the Internet connection after it is inactive for a specified period of time (Max Idle Time). If your Internet connection is 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. In the Max Idle Time field, enter the number of minutes of idle time that can elapse before your Internet connection terminates. The default Max Idle Time is 5 minutes. • Keep Alive Select this option to enable the router to check your Internet connection at the specified interval (Redial Period). If you are disconnected, then the router will automatically re-establish your connection. In the Redial Period field, specify how often you want the router to check the Internet connection. The default Redial Period is 30 seconds.

Field	Description
Tunnel Protocol	The Tunnel Protocol (PPTP/L2TP) could be supported via 3G USB modem by these simple instructions. • None Select this option to disable the Tunnel Protocol support. The option is used by default. • PPTP/L2TP Select one of the options to enable the PPTP or L2TP service you want to use. You will need to provide the server IP address, user name, and password. If you select 'None', the service would not be applied.
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.
Mobile Network Setup	
Configure Mode	Select Auto to allow the router to automatically detect which card model was inserted and which carrier is available. Select Manual to set up the connection manually. To allow the router to automatically configure modem and mobile network settings, use the default setting, Auto.
Card Model	The data card model that is inserted in the USB drive. The mobile network service provider for Internet connection. This setting is required when you are using HSDPA/UMTS/GPRS Internet service.
Access Point Name (APN)	The Internet network to which the mobile device is connecting. 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.
User Name/ Password	Enter the user name and password provided by your mobile network service provider.
SIM PIN	The PIN code associated with your SIM card. Enter your SIM PIN number here.
Server Name	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, use 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 enhanced build up connection. The first selection will always search for HSPDA/3G/UMTS service or switch to GPRS automatically only when it is available.
LTE Service	LTE (Long-Term Evolution), commonly marketed as 4G LTE, is a standard for wireless communication of high-speed data for mobile phones and data terminals.Select your LTE service. If you do not know which service to use, use the default setting, Auto

Internet Setup > WAN > Multi-WAN Config

Field	Description
Failover	
Connection Failover	This feature ensures that the Internet connection is always connected through a stable WAN link. When this option is enabled, the WRP500 will first bring up the highest priority WAN interface. If the validation site associated with the WAN is unreachable, WRP500 will try to bring up the next priority WAN if available, and change system default route to that WAN. Once the validation site associated with higher priority WAN interface is reachable, WRP500 will change system default route back to the higher priority WAN interface and stop lower priority WAN connection. When this option is disabled, all WAN interfaces will try to establish the connection, and system default route will set to the highest priority WAN interface. Load balance feature is available at this time.
Failover Check Interval	Specify the time interval at which the WRP500 detects the status of the Internet connection. The default timeout interval is 60 seconds.
Failover Ping timeout	Specify the timeout value that WRP500 wait validation site response the ping request. The default timeout interval is 5 seconds.
Failover Ping Retries	Specify the retry value that validation site not respond the ping request. The default retry value is 1.
Failback after N Check Interval Successes	Specify how many successful responses from validation site the WRP500 recovery back to the high priority WAN.
Connection Validation Site	An IP address to use as a ping target to detect the status of the Internet connection. By default the WRP500 pings the gateway associated with the binding priority WAN. You may specify a different IP address as a target here.
WAN Interface	This summary provides information on the current status of the Ethernet Internet connection and the Mobile Network connection. You can click the hyperlink in the Status column to view the interface details. You may also configure the interface priority by using the Priority pull-down menu. If USB_Modem is the priority one and shows status **"Connected: Validation site unreachable,"** configure a valid IP address in the Priority 1 WAN field.
WAN Interface Detail	List WAN information related to WAN Interfaces table. The information includes WAN interface ID, IP address, net mask and gateway address.
Load Balance	
WAN Load Balancing	Enable or disable load balance. This feature is only available when Failover is disabled.
Weight	Specify the weight value associated with each WAN interface while running load balance. The valid value is between 0~99. 0 means the WAN interface will not join load balance.

Interface Setup > LAN page

Interface Setup > LAN > DHCP Server

Field	Description
DHCP Server	
Add Entry	After clicking the Add Entry button, you can create another DHCP Server Pool. To edit the settings for an existing DHCP server pool, click the pencil icon.
DHCP List	Name DHCP Name, Default is DHCPRule_1(Default LAN) and DHCPRule_voice. VLAN VLAN ID, The default is **1** and **100**.
DHCP Details	Click an entry in the DHCP List to see the details in the DHCP table
Router IP	
DHCP Name	Label which identifies this DHCP Server configuration and is used to assign the service to a VLAN interface.
Local IP Address/Subnet Mask	IP address and subnet mask used to configure the VLAN interface to which this DHCP rule is applied.
DHCP Server Setting	
DHCP Mode	To select this DHCP pool run as **DHCP Server** or **DHCP Relay** agent. Please note, DHCP Relay only works when the NAT function is disabled.
DHCP Server	
Show DHCP Reservation	Click this button to review and modify the DHCP reservations. Click the button again to hide the reservation tables.
Select Clients from DHCP Tables	Shows the clients that are currently receiving IP addresses from the DHCP server. If you want to reserve the currently assigned IP address for exclusive use by a client, check the Select box and click Add. The client appears in the Clients Already Reserved table.
Manually Adding Client	To reserve an IP address for a client, enter a client name and an IP address that you want to reserve for the client. Then enter the MAC address of the client and click Add. The client appears in the Clients Already Reserved table.
WAN Interface	Choose the WAN Interface from which the related DHCP information, specifically DNS, is obtained.
Default Gateway	Enter the IP address of the default gateway to be used by clients of this pool. If the field is 0.0.0.0. the VLAN Local IP Address is used as the default gateway.

Field	Description
Option 66	Provides provisioning server address information to hosts requesting this option. Server information can be defined in one of three ways: • Local TFTP Server: The WRP500 uses its own TFTP server to source provisioning files so it returns its own local IP address to the client. • Remote TFTP Server: If the WRP500 was configured by using this method, it uses the server information it received through option 66 on its WAN interface in response to local client requests. • Manual TFTP Server: Allows the manual configuration of a configuration server address. While this option is typically used to provide either an IP address or a fully qualified hostname, the WRP500 will also accept and offer a full URL including protocol, path and filename to meet to requirements of specific clients.
Option 67	Provides a configuration/bootstrap filename to hosts requesting this option. This is used in conjunction with option 66 to allow the client to form an appropriate TFTP request for the file.
Option 159	Provides a configuration URL to clients requesting this option. An option 159 URL defines the protocol and path information by using an IP address for clients that cannot use DNS. For example: **https://10.1.1.1:888/configs/bootstrap.cfg**
Option 160	Provides a configuration URL to clients requesting this option. An option 160 URL defines the protocol and path information by using a fully qualified domain name for clients that can use DNS. For example: **https://myconfigs.cisco.com:888/configs/bootstrap.cfg**
DNS Proxy	If DNS proxy is enabled, local clients are offered the WRP500 Local IP Address to use for DNS requests. The WRP500 then proxies these requests to the DNS servers it was configured with. If DNS proxy is disabled, then DHCP clients will be offered DNS server information based on the following: If the Static DNS field is configured, then that server alone will be offered to clients. If the Static DNS field is not configured up to three servers are offered, first from the global Internet Options static configuration and then from the WAN interface nominated above.
Starting IP Address	Enter an IP address of the first address in this pool.
Maximum DHCP Users	Enter the maximum number of devices that you want the DHCP server to assign IP addresses to.This number cannot be greater than 256.
Client Lease Time	Amount of time an address is leased to a client. Enter the amount of time, in minutes, for the lease. The default is 0 minutes, which means one day. Enter 9999 to assign an infinite lease.
WINS	The Window Internet Naming Service (WINS) manages the window's host name to address resolution. If you use a WINS server, enter the IP address of the server here. Otherwise, leave this field blank.
DHCP Relay	
Remote DHCP Server	Set the DHCP server IP address that DHCP message will be relayed to.

Interface Setup > LAN > VLAN Settings

Field	Description
VLAN Settings	
Add Entry	Click the **Add Entry** button to create another VLAN.
VLAN List	• Name—VLAN Name. The default is data_Lan and voice_Lan. • ID—VLAN ID, The default is data_Lan : 1 and voice_Lan : 100. • Address Type—LAN Address Type. The default is data_Lan and voice_Lan : DHCP Server Pool. • Voice—Voice, The default is data_Lan: disabled and voice_Lan : enabled. • Membership—Membership, The default is data_Lan: LAN Port 1-4 and SSID1, voice_Lan : LAN Port 1-4 and SSID2.
VLAN Details	Select one item the VLAN List, the Detail of VLAN table will show all VLAN information.
VLAN – Add	
VLAN Name	Enter your VLAN Name.
VLAN ID	Enter an identification number for the VLAN. Note that VLAN ID **0~2**, and **4080~4095** are reserved for internal interfaces, and cannot be set as the manual VLAN ID.
Voice VLAN	Click this box if you want voice applications to use this VLAN. **Note** All traffic from a voice VLAN follows the voice default route specified in WAN interface configuration unless there is policy based routing configured for the voice VLAN. Policy based routing takes precedence over the default route. There are no implicit QoS settings for voice VLAN. You will need to change these accordingly.
Role	When bridging LAN ports with a WAN interface, the VLAN role will control how the associated IP interface is created. • Select the WAN role to create the IP interface as a subinterface of the selected Ethernet WAN. The resulting VLAN will be a layer 2 broadcast domain on the outside of the firewall. • Select the LAN role to create the IP interface, if required, as a LAN VLAN. VLANs created without WAN interfaces are automatically created with the LAN role.

Field	Description
IPv4 Address Type	Address type determines the way in which the VLAN IP interface is configured. • Choose **None** if an IP interface is not required. This would typically be the case when bridging ports only. • Choose **Static IP Address** to manually define an address for the interface. • Choose **Dynamic IP Address** to request an address from a DHCP server on the local network. • Choose **DHCP server** to enable a previously configured DHCP Server service on this interface. In this case, the VLAN IP address will be derived from the DHCP Server configuration.
Available Interface	The interfaces that are available to be added to the VLAN. To move an interface to the Added Interface list, click the interface, and then click the right-arrow button (>). To move all of the interfaces at once, click the double right arrow button (>>).
Added Interface	The interfaces that were selected as members of the VLAN bridge. If you want to remove an interface from this list, click the interface and then click the left arrow button (<). To remove all of the interfaces at once, click the double left-arrow button (<<).

Interface Setup > LAN > Port Settings

Field	Description
Port Settings	
Port List	• Interface Show Port Interface. • Mode Describes the currently configured behavior of the port. • Desktop mode: Provides attached devices with access to a single data VLAN for which the WRP500 provides DHCP services. Incoming traffic from the host can be tagged or untagged. Outgoing traffic to the host will be untagged. • IP Phone + Desktop mode: The port is configured with a data VLAN for native access and a voice VLAN for use with an attached IP Phone. CDP is used to communicate voice VLAN information to the phone. • Switch/AP mode: The port is configured to be part of multiple VLANs (any combination other than 1 data and 1 voice VLAN) for the purposes of trunking to either a switch or wireless access point. • Generic: The port is configured for layer 2 bridging mode only. • Enabled Flow Control Mechanism for temporarily stopping the transmission of data on this physical interface. For example: A situation might arise where a sending station (computer) is transmitting data faster than some other part of the network (including the receiving station) can accept. The overwhelmed network element will send a PAUSE frame, which halts the transmission of the sender for a specified period of time. To enable this feature, check the box. The default setting is Enabled. • Speed Duplex (Ethernet Port 1~4) Choose the duplex mode. You can select from Autonegotiate, 10 Half, 10 Full, 100 Half,100 Full,1000 Half and 1000 Full. The default is Auto-negotiate.
Port	Defines the quality of service trust settings for the port. The default setting is untrusted. • If the port is not trusted, the queuing priority for incoming traffic is defined by the port priority setting. • If the port is trusted, the queuing priority for the traffic is determined by 802.1p priority (CoS to Queue) if present, or IP priority (DSCP to Queue) if not. If neither priority is available, the queuing priority is set based on the port setting.
Port/Access VLAN	Select the native VLAN (PVID) for this port. The dropdown list includes all VLAN IDs that were configured on the VLAN Settings page.

Field	Description
Voice VLAN	When the VLAN mode is IP Phone + Desktop, the voice VLAN ID is shown. This value is informational only.
Priority	Set a priority for unmarked, or untrusted traffic received on this port. By default, the priority is set to 0. A higher number indicates a higher priority.

Interface Setup > LAN > STP

Field	Description
STP	
Bridge Priority	Bridge priority is used to influence what bridge becomes the STP root. The bridge with the lowest value in the network will be elected as the root. Valid Bridge Priorities **range from 0 through 61440, in steps of 4096.** The default value is 32768.
Forward Delay	**Note** Forward Delay, Hello Time, and Max Age are configuration settings sent by the root bridge to all other bridges to define the current STP configuration. If the WRP500 is not elected as the root, the active timer values might be different to those configured here. Forward Delay is the time spent in the listening and learning state. This time is equal to **15** seconds by default, but you can adjust the time to be between **4** and **30** seconds. Base IEEE 802.1D Standard, to support interoperability with legacy Bridges, a Bridge shall enforce the following relationship: **2 x (Forward_Delay - 1.0 seconds) >= Max_Age** **Max_Age >= 2 x (Hello_Time + 1.0 seconds)**
Hello Time	The Hello Time is the time between each Bridge Protocol Data Unit (BPDU) that is sent by a bridge. This time is equal to **2** seconds by default, but you can adjust the time to be between **1** and **10** seconds. Base IEEE 802.1D Standard, to support interoperability with legacy Bridges, a Bridge shall enforce the following relationship: **2 x (Forward_Delay - 1.0 seconds) >= Max_Age** **Max_Age >= 2 x (Hello_Time + 1.0 seconds)**
Max Age	The Max Age timer defines how long bridges will wait after receiving the last hello message before assuming that the layer 2 topology has changed. At this point the current spanning tree configuration is discarded and the new topology is discovered. This time is **20** seconds by default, but you can adjust the time to be between **6** and **40** seconds. Base IEEE 802.1D Standard, to support interoperability with legacy Bridges, a Bridge shall enforce the following relationship: **2 x (Forward_Delay - 1.0 seconds) >= Max_Age** **Max_Age >= 2 x (Hello_Time + 1.0 seconds)**

Interface Setup > Wi-Fi Settings

Interface Setup > Wi-Fi Settings > Basic Wireless Settings

Field	Description
Wireless Network	
Operating Radio	Select Radio 1 (2.4 GHz) or Radio 2 (5 GHz) to specify which radio to configure. The rest of the settings on this tab apply to the radio you select in this field. Be sure to configure settings for both radios.
Wireless Table	
Wireless Network Name (SSID)	The default wireless network uses this name: “cisco-radio1-data” To rename the default wireless network, enter a unique Wireless Network Name, which is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). To create a second wireless network, enter a unique Wireless Network Name in the SSID2 setting. (To activate this network, select Network Enabled.) Note: Your ISP or ITSP may control the SSID2 settings. Contact your ISP or ITSP for more information.
Broadcast Network Name	When wireless clients survey the local area for wireless networks to associate with, they detect the SSID broadcast by the Router. If you want to broadcast the SSID, leave the check box selected. If you do not want to broadcast the SSID, deselect the check box.
Enabled Network	To enable the wireless network, select the check box. To disable the wireless network, deselect the check box.
WPS Hardware Button	
Security	These settings configure the security of your wireless network.
Click “Edit” to configure SSID security	

Wireless Security	
Security Mode	Select the security method for your wireless network. Proceed to the appropriate instructions. If you do not want to use wireless security, use the default, Disabled. • **WEP** • **WPA2 Personal** • **WPA/WPA2-Mixed Personal** • **WPA2 Enterprise** • **WPA/WPA2 Enterprise**

Interface Setup > Wi-Fi Settings > Wi-Fi Protected Setup

Field	Description
Select a SSID	From this drop-down menu, you can decide the WPS settings apply to which SSID. The default is SSID1.
Wi-Fi Protected Setup™	Select disabled if you don't want to use the Wi-Fi Protected Setup. The default is Disabled. There are three methods available. Use the method that applies to the client device; you are configuring. • Method 1 Use this method if your client device has a Wi-Fi Protected Setup button. a. Click or press the **Wi-Fi Protected Setup** button on the client device. b. Click the Wi-Fi Protected Setup button on this screen. c. After the client device has been configured, click d. **OK.** Then refer back to your client device or its documentation for further instructions. • Method 2 Use this method if your client device has a Wi-Fi Protected Setup PIN number. a. Enter the PIN number in the field on this screen. b. Click c. **Register.** d. After the client device has been configured, click e. **OK**. Then refer back to your client device or its documentation for further instructions. • Method 3 Use this method if your client device asks for the Router's PIN number. a. Enter the PIN number listed on this screen. (IT is also listed on the label on the bottom of the Router.) b. After the client device has been configured, click c. **OK**. Then refer back to your client device or its documentation for further instructions. The Wi-Fi Protected Setup Status, Network Name (SSID), Security are displayed at the bottom of the screen.

Interface Setup > Wi-Fi Settings > Advanced Wireless Settings

Field	Description
Operating Radio	Radio 1 and Radio 2 can be selected, after configure radio 1, you can select radio 2 to continue configuration.
RTS Threshold	The router sends Request to Send (RTS) frames to a 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. If you encounter inconsistent data flow, you can adjust this threshold. 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 RTS Threshold value should remain at its default value of **2347**.
AP Isolation	This feature isolates all wireless clients and wireless devices from one another. Wireless devices will be able to communicate with the router but not with other wireless devices on the network. To use this function, select Enabled. AP Isolation is disabled by default.
Basic Rate	The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is Default, which allows the Router to transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are 1-2Mbps, for use with older wireless technology, and All, which allows the Router to transmit at all wireless rates.
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 Router 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**
Fragmentation Threshold	This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most case, it should remain at its default value of **2346**.
Beacon Interval	Enter a value between 20 and 1,024 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router to synchronize the wireless network. The default value is 100.
Power Control	Form this drop-down menu, you can choose **high**, **middle**, or **low** value to specify the range of the wireless network. This option will determine the available distance. The default is **high** which is a normal power level.

Field	Description
PMF Capable	The 802.11w protocol applies only to a set of robust management frames that are protected by the Management Frame Protection (**PMF**) service. These include Disassociation, Deauthentication, and Robust Action frames. When PMF capable enabled, it is to be used if the client supports 802.11w.
PMF Required	Enabled PMF required will ensure that the clients that do not support 802.11w cannot associate with the WLAN.
PMF SHA256	Enable or Disable SHA-256 key derivation functionality.
Multicast Power Save	Enable or Disable Multicast Power Save.

Interface Setup > Wi-Fi Settings > WMM Setting

Field	Description
Wireless	
Operating Radio	Radio 1 and Radio 2 can be selected, after configure radio 1, you can select radio 2 to continue configuration.
WMM Support	WMM provides Quality of Service features to support voice and video applications. To enable WMM, keep the default setting, **Enabled**. Otherwise, choose **Disabled.**
No Acknowledgement	When this option is enabled, the router does not resend data if an error occurs. To enable this feature, keep the default setting, **Disabled**. Otherwise, choose **Enabled**.

Interface Setup > Management Interface

Field	Description
List of Management Interface	
IP Address	Enter the IP Address to use for the loopback test. If IP Address and WAN IP Address or LAN IP Address are the same, it is unavailable.

Network Setup module

The Network Setup module includes these pages:

- Network Setup > Routing
- Network Setup > NAT
- Network Setup > QoS
- Network Setup > Firewall
- Network Setup > PPPoE Relay
- Network Setup > DDNS
- Network Setup > DMZ

- Network Setup > IGMP
- Network Setup > UPnP
- Network Setup > CDP
- Network Setup > LLDP
- Network Setup > DNS Spoofing

Network Setup > Routing page

Network Setup > Routing > Static Routes > IPv4

Field	Description
Add Entry	After clicking the **Add Entry** button, it will create another Static Route.
Static Routing list	• Name Show all routes of name. • Interface Show all routes of interface.
Static Routing Details	Select one entry of Static Routing list, Defaults of Static Routing Details will show all Information. (Link Route Name, Destination IP Address, Subnet Mask, Gateway, Interface).
Enter Route Name	Enter a net Static Routing Name.
Destination	The Destination IP Address is the address of the network or host to which you want to assign a static route.
Subnet Mask	The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
Gateway	The IP address of the gateway device that allows for contact between the Router and the network or host.
Routing Table	• Destination LAN IP The Destination IP Address is the address of the network or host to which the static route is assigned. • Subnet Mask The Subnet Mask determines which portion of an 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 Router and the network or host. • Interface This interface tells you whether the Destination IP Address is on the **LAN** (internal wired and wireless networks), the **Internet (WAN)**.

Network Setup > Routing > RIP > IPv4

Field	Description
RIP	Routing Information Protocol is used for dynamic routing. You can enable this protocol to allow the specified interfaces to automatically adjust to physical changes in the network's layout and to exchange routing tables with other router. The router determines the network packets' route based on the fewest number of hops between the source and destination. To enable the Dynamic Routing feature, select Enabled then enter the RIP settings, and enable RIP on the interfaces where you want to use this feature. To disable the Dynamic Routing feature for all data transmissions, use the default setting, **Disabled**.
RIP Version	To limit the types of packets that can be transmitted, choose Version 1 or Version 2. Alternatively, choose RIP v1/v2 to allow both Version 1 and Version 2 packets to be transmitted.
RIP Timer	RIP uses timers to regulate its performance. These include a routing-update timer, a route-timeout timer, and a route-flush timer. • Update Specify the rate at which the router sends routing updates. The default is 30 seconds • Timeout Specify the rate at which the router expects to receive routing updates from each router in the routing table. If this value is exceeded, the route is declared unreachable. The route is not removed from the routing table until the route flush timer expires. • Flush Specify the maximum period that the router will wait for an update before removing a route from the routing table.
RIP List	This list displays the RIP settings for the WAN interface (WAN1) and each VLAN. To edit the settings, click the pencil icon. • Interface Show RIP default interface. • RIP Enable • Passive • Authentication
RIP Network	• Network Address Specifies the IP Address and Subnet mask for the entry.

Network Setup > Routing > Intervlan Routing

Field	Description
Intervlan Routing	Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local. However, when an end station in one VLAN needs to communicate with an end station in another VLAN, Intervlan communication is required. This communication is supported by Intervlan routing. To enable this feature, keep the default setting, **Enabled**. To disable this feature, choose **Disabled**.

Network Setup > Routing > Policy Routing

Field	Description
Add Entry	
Name	Specify the name for this policy route rule
Incoming Interface	Select LAN interface to apply for a rule. Any means the OUT Interface for this rule applied for all LAN interfaces
Source IP Address	Matches the source IP address from which packets are addressed to this rule.
Subnet Mask	Defines the source IP address wildcard mask. Masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that all the bits are important. A mask of 0.0.0.0 indicates that all the bits will be ignored. Therefore, if an Source IP Address is specified but source subnet mask specified to 0.0.0.0, the rule will regards it as 0.0.0.0/0 (all) address.
Destination IP Address	Matches the destination IP address to which packets are addressed to this rule.
Subnet Mask	Defines the destination IP address wildcard mask. Masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that all the bits are important. A mask of 0.0.0.0 indicates that all the bits will be ignored. Therefore, if a destination IP address is specified but destination subnet mask specified to 0.0.0.0, the rule will regards it as 0.0.0.0/0 (all) address.
Port	Defines the TCP/UDP destination port to match. "Any" means port field will not be inspected. "Single" means a port is specified. "Range" means that port range are specified
Protocol	Specify the interested protocol for this rule. Default is "Any", which, means protocol filed filter will be disabled and all kind of protocol are going to inspect. Beside, user can specify UDP, TCP

Field	Description
DSCP	Specify the DSCP number to match for this rule.
Route	Two possible output categories can be selected. One is existed VPN tunnel, and the other is existed WAN interface. When select WAN interface as output interface, an additional option can be checked: "Disable this rule if the interface is down". When this option is checked, the policy route rule will take no effect while the output interface is down (got no IP). The traffic will then fall through to match other policy route rules, or obey system's route (typically system default route).

Network Setup > NAT

Network Setup > NAT > NAT Setting

Field	Description
Address Translation	
NAT	Choose the correct working mode. Use the default setting, Enabled, if the Router is hosting your network's connection to the Internet (Enabled mode is recommended for most users). Select Disabled if the Router exists on a network with other routers
Application Layer Gateways	
SIP	SIP ALG can help to establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls. The default is Enabled.
NetMeeting	NetMeeting ALG can modify RAS, Fast Start, H.245 Tunneling, Call Forwarding, RTP/RTCP and T.120 based audio, video, fax, chat, whiteboard, file transfer. Besides, it only support connected way from LAN hosts to WAN hosts at present. If you want to connected way from WAN to LAN, you need to set DMZ. The default is Enabled.
RTSP	RTSP ALG allows UDP transports to be setup properly, including RTP and RDT. The default is Enabled.
IRC	IRC ALG can allow users to send files to each other and user need connect to IRC server. The default is Enabled.

Network Setup > NAT > NAT Bypass

Field	Description
NAT Bypass	NAT Bypass Policy Setting which addressed a flexible and configurable rule matching criteria to set the matched traffic to perform pure routing while global NAT option is enabled.
Add Policy	Click the Add Policy button to create a NAT bypass rule

Field	Description
Policy List	• Policy Name User specified NAT bypass rule name • Inside Interface This field presents user specified inside interface, which will be VLAN interface, Host IP address or Indirect Network • Outside Interface This field presents user specified outside interface • Status This field presents this NAT bypass rule is enabled or disabled
Policy Details	All detailed information will be shown by selecting one entry from the list of NAT bypass rule.
Policy Name	Specify the rule name for this rule.
Enable	Enable/disable this rule.
Inside interface	Specify the traffic source rule • VLAN interface Specify the VLAN that to become the NAT bypass VLAN domain. The pull down menu contain all LAN (VLAN) collection. This is the either one option between Host and Indirect Network Domain options. • Host IP Address Specify a host IP address that to become a routed host. This is the either one option between VLAN and Indirect Network Domain options • Indirect Network Specify an indirect network domain (non-VLAN) to be a routed domain. This is the either one option between VLAN and Host options. • IP Address Specify source IP address associated with the indirect network domain when indirect network domain option selected. • Subnet Mask Specify the subnet mask associated with the source IP address when indirect network domain option is selected.
Outside Interface	Specify the traffic destination rule. • WAN interface Select the out interface. The pull down menu contains all WAN collection. • IP Address Specify destination IP address • Subnet Mask Specify the subnet mask associated with the destination IP address.

Network Setup > NAT > Port Forwarding

Port Forwarding	Use the Port Forwarding page if your network hosts network services (Internet applications) such as World Wide Web, email, FTP, videoconferencing or gaming. For each service, you need to configure the settings to forward Internet traffic to the servers that host these services. After clicking the Add Entry button, you can create another entry for another network service. To edit an entry, click the pencil icon. Before you perform this procedure, you should reserve a DHCP addresses for each server that hosts an Internet application. Use the Interface Setup > LAN > DHCP Server page. Click Add Entry, and then click Show DHCP Reservation. You can add the server from the Select Clients table, or manually enter the client information.
Add Entry	Click the **Add Entry** button to create another Single Port Forwarding or Port Range Forwarding
List of Port Forwarding	• Number • Type Show Port Forwarding entry type is Single Port Forwarding or Port Range Forwarding. • Status Show Enable or Disable the entry. • Application Show Entry Name.
Port Forwarding Details	Select one entry from the List of Port Forwarding Details of Port Forwarding will show all Information. (like Wan Interface Name, External Port, Internal Port, Protocol, IP Address).
Port Forwarding Type	Choose Single Port Forwarding to forward traffic to a single port on the specified server, or choose Port Range Forwarding to forward traffic to a range of ports.

	Single Port Forwarding • Application Name: Choose a standard application from the drop-down list. To enter an application that is not on the list, choose Add a new name, and then enter the name of a new application. • Enter a Name: Enter the name of the Internet application. • WAN Interface Name: Choose the WAN interface through which the traffic is transmitted • External Port: For single port forwarding, enter the external port number that is used by the server or Internet application. Check the Internet application's documentation for more information • Internal Port: For single port forwarding, enter the internal port number used by the server or Internet application. Check the Internet application's documentation for more information. • Protocol: Select the protocol TCP or UDP. • IP Address: Enter the IP address of the server that hosts this Internet application. The server must have a static IP address, which you can set on the Interface Setup > LAN > DHCP Server page. • Enabled: Check the box to enable the application you have defined. The default setting is unchecked (Disabled)
	Port Range Forwarding • Enter a Name: Enter the name of the Internet application • WAN Interface Name: Choose the WAN interface through which the traffic is transmitted • Start ~ End Port: For port range forwarding, specify the range of ports used by the server or Internet application. Enter the first port in the first box, and enter the final port in the second box to specify the range. Check the Internet application's documentation for more information. • Protocol: Select the protocol TCP or UDP. • IP Address: Enter the IP address of the server that hosts this Internet application. The server must have a static IP address, which you can set on the Interface Setup > LAN > DHCP Server page. • Enabled: Check the box to enable the application you have defined. The default setting is unchecked (Disabled).

Network Setup > NAT > Port Range Triggering

Field	Description
Port Range Triggering	Use the Port Range Triggering page to allow the router to dynamically open ports for network services (Internet applications) that are hosted by individual computers. When this feature is enabled, an outbound connection from specified ports triggers the router to open other specified ports for incoming traffic. Port Range Triggering does not require you to reserve an IP address (static IP address) for the computer that hosts the specified application. However, Port Range Triggering allows only one computer to host a service on the specified ports at one time.
Add Entry/Edit	After clicking **Add Entry** button, it can create another Port Range Triggering.
Port Range Triggering List	• Status Show Enable or Disable the entry. • Application Show Entry Name.
Port Range Triggering Details	Select one entry of Port Range Triggering List, Details of Port Triggering will show all Information, such as WAN Interface, LAN Interface, Triggered Range, Forwarded Range, Protocol.
Application Name	Enter a name to identify the application in the Port Range Triggering List
WAN	Choose the WAN Interface for the Internet traffic
LAN	Choose the LAN where the host computer is located
Triggered Range	Enter the starting and ending port numbers of the triggered port range. When a computer makes an outbound connection from these ports, the router will open the ports that are specified in the Forwarded Range fields. Check with the Internet application's documentation for the port number(s) needed.
Forwarded Range	Enter the starting and ending port numbers of the forwarded port range. These ports will be opened when an outbound connection is made from the ports that are specified in the Triggered Range fields. Check with the Internet application documentation for the port number(s) needed.
Protocol	Select the protocol TCP or UDP.
Enabled	Click the Enabled check box to enable the applications you have defined. This is disabled (unchecked) by default.

Network Setup > QoS

Network Setup > QoS > QoS Bandwidth Control

Field	Description
QoS Bandwidth Control	Set the bandwidth priority rule for a variety of interface.
Name	Show the interface name
Enabled	To use the QoS policies you have set, select the check box. Otherwise, deselect the check box.
Upstream Bandwidth	Show the maximum bandwidth for upstream data transmissions
Strict High/ High / Medium / Normal / Low	Show the bandwidth guarantees for each priority queues
Upstream Bandwidth	Set the maximum bandwidth for upstream data transmissions.
Priority	Set the bandwidth guarantees for the priority queues. • Strict High Enter the guaranteed bandwidth for the Strict High Priority queue. • High, Medium, Normal, Low Increase the rate and bandwidth for each queue by clicking the plus (+) button, or reduce the rate and bandwidth by clicking the minus (-) button.

Network Setup > QoS > QoS Policy

Field	Description
QoS Policy	Configures the Quality of Service (QoS) settings for specified applications, devices, ports, or VLANs. Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as video conferencing. 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.
Add Entry	Click the **Add Entry** button to create another QoS Policy.New create rule will have high priority than old one
List of QoS Policy	• Priority Show the priority of entry. • Name Show the name of entry
QoS Details	Select one entry of List of QoS Policy, Details of QoS will show all information about QoS

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Category</td><td>There are five categories available. Select one of the following: Application, MAC Address, Ethernet Port, VLAN and IP Address, then complete the fields that appear, based on your selection.</td></tr>
<tr><td></td><td>Application

Applications: Choose a standard application from the drop-down list. To enter an application that is not on the list, choose Add a New Application, and then enter the name.
Name: For most categories and applications, this field displays the name of the selected category or application. If you chose Add a New Application, enter the name of the application.
LAN: Choose the VLAN that is used for this traffic
Port Range:

Port Range: Enter the number or range of port(s) used by the server or Internet application. Check the Internet application's documentation for more information. Also select the protocol TCP or UDP, or select Both.
Protocol: Select the protocol TCP or UDP, or select Both

Priority: Choose the bandwidth priority for this traffic: Strict, High, Medium, Normal, or Low, Medium is recommended
Marking: Marking modifies the DiffServ or CoS field of the packet according to QoS Policy Rule (by Application port range, Mac, Ethernet port, VLAN and IP Address).
Note: CoS value only valid when output interface is subwan (with 802.1Q tagging).
CoS and DiffServ: Setting Network Setup/QoS/Qos policy, this will classify the LAN to WAN packet. If traffic doesn't match these policy rules, it will use default priority setting by each Ethernet port if it is untrust mode, or classify by packet COS or DiffServ priority setting if it is trust mode.
</td></tr>
</table>

Field	Description
	MAC Address • Name: Enter a name to describe this rule. • LAN: Choose the VLAN that is used for this traffic • MAC Address: Enter the MAC address of the device in the following format: xx:xx:xx:xx:xx:xx • Priority: Choose the bandwidth priority for this traffic: **Strict**, **High**, **Medium**, **Normal**, or **Low**, **Medium** is recommended. • Marking: Marking modifies the DiffServ or CoS field of the packet according to QoS Policy Rule (by Application port range, Mac, Ethernet port, VLAN and IP Address). **Note** CoS value only valid when output interface is subwan (with 802.1Q tagging). • CoS and DiffServ: Setting Network Setup/QoS/Qos policy, this will classify the LAN to WAN packet. If traffic doesn't match these policy rules, it will use default priority setting by each Ethernet port if it is untrust mode, or classify
	Ethernet Port • Name: Enter a name to describe this rule. • LAN: Choose the VLAN that is used for this traffic • Ethernet Choose the Ethernet port. • Priority: Choose the bandwidth priority for this traffic: **Strict**, **High**, **Medium**, **Normal**, or **Low**, **Medium** is recommended. • Marking: Marking modifies the DiffServ or CoS field of the packet according to QoS Policy Rule (by Application port range, Mac, Ethernet port, VLAN and IP Address). **Note** CoS value only valid when output interface is subwan (with 802.1Q tagging). • CoS and DiffServ: Setting Network Setup/QoS/Qos policy, this will classify the LAN to WAN packet. If traffic doesn't match these policy rules, it will use default priority setting by each Ethernet port if it is untrust mode, or classify by packet's COS or DiffServ priority setting if it is trust mode.

Field	Description
	VLAN • Name: Enter a name to describe this rule. • LAN: Choose the VLAN that is used for this traffic • Priority: Choose the bandwidth priority for this traffic: **Strict**, **High**, **Medium**, **Normal**, or **Low**, **Medium** is recommended. • Marking: Marking modifies the DiffServ or CoS field of the packet according to QoS Policy Rule (by Application port range, Mac, Ethernet port, VLAN and IP Address). **Note** CoS value only valid when output interface is subwan (with 802.1Q tagging). • CoS and DiffServ: Setting Network Setup/QoS/Qos policy, this will classify the LAN to WAN packet. If traffic doesn't match these policy rules, it will use default priority setting by each Ethernet port if it is untrust mode, or classify by packet's COS or DiffServ priority setting if it is trust mode.
	IP Address • Name: Enter a name to describe this rule. • Destination IP Address: Set the destination IP address of traffic flow that would apply QoS. • Destination Mask: Set the subnet mask to decide the destination IP address range. • Priority: Choose the bandwidth priority for this traffic: **Strict**, **High**, **Medium**, **Normal**, or **Low**, **Medium** is recommended. • Marking: Marking modifies the DiffServ or CoS field of the packet according to QoS Policy Rule (by Application port range, Mac, Ethernet port, VLAN and IP Address). **Note** CoS value only valid when output interface is subwan (with 802.1Q tagging). • CoS and DiffServ: Setting Network Setup/QoS/Qos policy, this will classify the LAN to WAN packet. If traffic doesn't match these policy rules, it will use default priority setting by each Ethernet port if it is untrust mode, or classify by packet's COS or DiffServ priority setting if it is trust mode.

Network Setup > QoS > CoS To Queue

Field	Description
VLAN CoS	Specifies the VLAN (CoS) priority tag values, where zero is the lowest and 7 is the highest.
Priority	Defines the traffic forwarding queue to which the CoS priority is mapped. Where five kinds of traffic priority queues are supported.

Network Setup > QoS > DSCP To Queue

Field	Description
DiffServ	Indicates the Differentiated Services Code Point (DSCP) value in the incoming packet
Priority	Defines the traffic forwarding queue to which the DSCP priority is mapped

Network Setup > Firewall

Network Setup > Firewall > Firewall Filter

Field	Description
SPI Firewall Protection	A firewall enhances network security and uses Stateful Packet Inspection (SPI) for more review of data packets entering your network. Select **Enabled** to use a firewall, or **Disabled** to disable it.
Filter Anonymous Internet Requests	When enabled, this feature keeps your network from being "pinged," or detected, by other Internet users. It also hides your network ports. Both to make it more difficult for outside users to enter your network. This filter is enabled by default. Select **Disabled** to allow anonymous Internet requests.
Filter Internet NAT Redirection	This feature uses port forwarding to block access to local servers from local networked computers. This filter is disabled by default. Select **Enabled** to filter Internet NAT redirection, or **Disabled** to disable this feature.
Filter IDENT (Port 113)	This feature keeps port 113 from being scanned by devices outside of your local network. This filter is enabled by default. Select **Enabled** to filter port 113, or **Disabled** to disable this feature.
Filter DoS Attack	When enabled, this feature wards off ICMP Ping flood (ICMP echo request) and TCP SYN flood (tcp_syn cookies) attacks. The default is disabled. Check the box to enable it. The maximum rate limit for both types of flood attacks is 50 packets per second Note: If an IP packet is destined to an IP broadcast or IP multicast destination address, your network can be used to execute a flooding DoS attack to other hosts.

Field	Description
Proxy	Use of WAN proxy servers may compromise your network security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, check the box.
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. To enable Java filtering, check the box.
ActiveX	ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites that use this programming language. To enable ActiveX filtering, check the box.
Cookies	A cookie is data stored on your computer and used by Internet sites when you interact with them. To prevent the storage of cookies, check the box.
Filter Port	Set the Web service port for filtering Proxy/Java/ActiveX/Cookies, port 80 is used by default

Network Setup > Firewall > Firewall Filter

Field	Description
Internet Filter	• Filter Anonymous Internet Requests • Filter Internet NAT Redirection • Filter IDENT (Port 113 • Filter DoS Attack
Web Filter	• Proxy • Java • ActiveX • Cookies

Network Setup > Firewall > IPV4 > Internet Access Control

Field	Description
Internet Access Control	Configures rules controlling users' access to the Internet
Add Entry	Click the **Add Entry** button to create another Internet Access Control

Field	Description
Internet Access Policy list	• PolicyName Show the entry of name. • Status Show the entry of status. • From LAN Interface Show the entry of LAN interface. • To WAN Interface Show the entry of WAN interface.
Policy Details	Select an entry from the Internet Access Policy list, Details of Policy will show all information about Internet Access Policy.
Policy Name	Add Policy Name
Status	To enable this policy, click Enabled. To disable this policy, click **Disabled**. The default is **Disabled**
From LAN, To WAN	You can apply the rule to all traffic by choosing From All, To All, or you can limit the rule to apply only to particular interfaces, such as From VLAN1 to Ether_WAN1
Applied PCs	If you want the policy to apply only to specified PCs, click the Show Edit List button. Then you can specify individual PCs by entering the MAC address or the IP address. You can specify groups of PCs by entering up to two ranges of IP addresses
Days/Times	Choose the days and times when you want this policy to be enforced. Select the individual days, or select **Everyday**. Enter a range of hours by specifying the start time (From) and the end time (To), or select **24 Hours**.
Blocking Everything	Check this box to block all Internet traffic that meets the criteria that you specified on this page. Uncheck this box to choose one or more of the other filtering options.
Blocking by URL and Keyword	Check this box to prevent users from accessing specified URLs or URLs that contain specified keywords in HTTP session only, but HTTPS session is not supported. Enter up to four URLs and up to six keywords.

Field	Description
Blocking by destination IP address	Check this box to prevent users from accessing specified IP addresses. Enter up to four IP addresses.
Blocking by Services	Check this box to prevent users from accessing specified Internet services, such as FTP or telnet. (You can block up to three applications per policy.) From the Applications list, click the application that you want to block. Then click the right-arrow button to move the application to the Blocked List. To remove an application from the Blocked List, click it and then click the button left-arrow button. Application List: •DNS(53 - 53) •FTP(21 - 21) •HTTP(80 - 80) •HTTPS(443 - 443) •TFTP(69 - 69) •IMAP(143 - 143) •NNTP(119 - 119) •POP3(110 - 110) •SMTP(25 - 25) •SNMP(161 - 161) •TELNET(23 - 23)

Network Setup > Firewall > IPV4 > Inbound Access Control

Field	Description
Inbound Access Control	Configure rules controlling your users' access from the Internet (WAN to LAN).
Add Entry	Click the **Add Entry** button to create another Advanced Firewall Policy entry
Advanced Firewall Policy List	• Policy Name Show the entry of Policy Name • Status Show the entry of Status • IN Interface(WAN) Show the entry of IN Interface(WAN) • OUT Interface(LAN) Show the entry of OUT Interface(LAN) • Priority Show the entry of Priority

Field	Description
Rule Name	User specified rule name. Up to 31 characters are allowed to key-in.
Status	Enabled or disabled this rule entry.
IN Interface(WAN)	Select WAN interface to apply for a rule. ALL WAN means the IN Interface for this rule applied for all WAN interfaces.
OUT Interface(LAN)	Select LAN interface to apply for a rule. ALL LAN means the OUT Interface for this rule applied for all LAN interfaces.
Source IP Address	Matches the Source IP address to which packets are addressed to this rule.
Source Subnet Mask	Defines the source IP address wildcard mask. Masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that all the bits are important. A mask of 0.0.0.0 indicates that all the bits will be ignored. Therefore, if an Source IP Address is specified but source subnet mask specified to 0.0.0.0, the rule will regards it as 0.0.0.0/0 (all) address
Destination IP Address	Matches the destination IP address to which packets are addressed to this rule.
Destination Subnet Mask	Defines the destination IP address wildcard mask. Masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that all the bits are important. A mask of 0.0.0.0 indicates that all the bits will be ignored. Therefore, if an destination IP address is specified but destination subnet mask specified to 0.0.0.0, the rule will regards it as 0.0.0.0/0 (all) address.
Protocol	Specify the interested protocol for this rule. Default is "Any", which, means protocol filed filter will be disabled and all kind of protocol are going to inspect. Beside, user can specify UDP, TCP, or ICMP protocol
Source Port	Defines the TCP/UDP source port that this rule to match. “Any” means port field will not be inspected. “Single” means a port is specified. “Range” means that port range are specified.
Destination Port	Defines the TCP/UDP destination port that this rule to match. “Any” means port field will not be inspected. “Single” means a port is specified. “Range” means that port range are specified
Action	Deny or Permit the traffic associated with this rule.
Schedule	Selective week day schedule that this rule is going to apply.
Times	Specified time period that this rule is going to apply.

Network Setup > PPPoE Relay

Field	Description
Add Entry	Click the **Add Entry** button to create another PPPoE Relay
PPPoE Relay list	• Wan option Show the entry of wan option. • Lan option Show the entry of lan option. • PPPoE Relay Show the entry of status.
PPPoE Relay	Enable or Disable PPPoE Relay
WAN Interface	Select the WAN Interface for this rule
LAN Interface	Select the LAN Interface for this rule

Network Setup > DDNS

Field	Description
DDNS	Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. If your ISP has not provided you with a static IP, and your WAN connection is configured to use DHCP to get an IP address dynamically, then DDNS allows you to have a virtual static address for your website. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.com or TZO.com Use the DDNS page to activate your service on the router.
DynDNS.org	
DynDNS.org	You must sign up for an account with DynDNS.org before you can use this service.
User Name	Enter the user name from DynDNS.org.
Password	Enter the password from DynDNS.org.
Host Name	Enter your host name. This should be in the format of name.dyndns.org.
System	Select the DynDNS service you use: **Dynamic**, **Static**, or **Custom**.
Mail Exchange (Optional)	Enter the address of your mail exchange server, so the email to your DynDNS address go to your mail server.
Mail Exchange (Backup MX)	This feature allows the mail exchange server to be a backup. To enable this feature, use the default setting, **Enabled**. To disable this feature, select **Disabled**. If you are not sure, which setting to select, use the default setting, **Enabled**.

Field	Description
Wildcard	This feature allows you to use a wildcard value in the DDNS address. For example, if your DDNS address is myplace.dyndns.org and you enable wildcard, then the x.myplace.dyndns.org will work as well (x is the wildcard). To enable wild cards, use the default setting, **Enabled**. To disable wildcard, select Disabled. If you are not sure which to select, use the default setting, **Enabled**.
Internet IP Address	Your current IP address.
Status	Your DDNS status.
Update	To manually trigger an update, click this button.
TZO.com	
TZO	You must sign up for an account with TZO before you can use this service.
E-Mail Address	Enter the email address for your TZO account.
TZO Key	Enter the key for your TZO account.
Domain Name	Enter your host name. This should be in the format of name.dyndns.org.
Internet IP Address	Your current IP address.
Status	TZO DDNS status.
Update	To manually trigger an update, click this button.

Network Setup > DMZ

Network Setup > DMZ > Software DMZ

Field	Description
Software DMZ	A DMZ (Demarcation Zone or Demilitarized Zone) is a sub-network that is behind the firewall but that is open to the public. By placing your public services on a DMZ, you can add an additional layer of security to the LAN. The public can connect to the services on the DMZ but cannot penetrate the LAN. You should configure your DMZ to include any hosts that must be exposed to the WAN (such as web or email servers)
Add Entry	Click the Add Entry button to create a software DMZ entry
Status	Select enable to activate this entry, or disable to deactivate it.
Public IP	Input an public IP address that this DMZ server will expose to the Internet
Private IP	The Subnet Mask Server's private IP address behind LAN corresponding to the Public IP address

Network Setup > DMZ > Hardware DMZ

Field	Description
Hardware DMZ	This feature will use new LAN port 4 as can be used for DMZ purposes for public access to the customer's web and other servers that are accessible from the Internet. The rest LAN network ports will continue to be used for private internal traffic.Please note that this feature only supported while WAN in static or DHCP mode. Hardware DMZ site can't be applied for a VPN connection site.
Hardware DMZ	When select enabled, LAN port 4 will act as DMZ port, or it acts as a normal LAN port for private internal traffic.
Add Entry	Click the Add Entry button to create a hardware DMZ IP matching.
Hardware DMZ Details	
Status	Select enable to activate this entry, or disable to deactivate it.
Public IP	Input an public IP address that equal to the server IP address that attached behind hardware DMZ port

Network Setup > IGMP

Field	Description
IGMP	Internet Group Management Protocol (IGMP) is a signaling protocol that supports IP multicasting for IPTV.
IGMP Proxy	Keep the default setting, **Enabled**, if you want to allow multicast traffic through the router for your multimedia application devices. Otherwise, select **Disabled**.
Support IGMP Version	Select the version you want to support, **IGMP v1**, **IGMP v2**,or **IGMP v3**. If you are not sure which version to select, keep the default setting, **IGMP v2**.
WAN Interface	Select WAN interface you want to forward, you can check **Internet Setup** to check its type. If you are not sure which WAN interface to select, keep the default setting [**AUTO**] to follow system default route interface.
Immediate Leave	Select **Enabled**, if you use IPTV applications and want to allow immediate channel swapping or flipping without lag or delays. Otherwise, use the default setting, **Disabled**.

Network Setup > UPnP

Field	Description
UPnP	UPnP (Universal Plug and Play) is a feature that allows for automatic discovery of devices that can communicate with the router.
UPnP	If you want to use UPnP, use the default setting, **Enabled**. Otherwise, select **Disabled**.

Field	Description
Allow Users to Configure	When this feature is enabled (the default setting), you can make manual changes while using the UPnP feature. Select Disabled, if you don't want to be able to make manual changes.
Keep UPnP Configurations After System Reboot	When this feature is enabled, the router saves UPnP configuration after a system reboot. The default is **Disabled**. When this feature is disabled, the router does not save UPnP configuration, but it does not remove the previous UPnP configuration.

Network Setup > CDP

Field	Description
CDP	Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco equipment. Each CDP-enabled device sends periodic messages to a multicast address and also listens to the periodic messages sent by others in order to learn about neighboring devices. Use the CDP page to choose the CDP settings for your network.
CDP Setting	
CDP	You can enable CDP on all ports, disable CDP on all ports, or configure CDP per port. Cisco recommends the default setting, Per Port. Enabling CDP is not recommended on the WAN port because it is connected to an insecure network.
CDP Timer	Specify the interval at which successive CDP packets can be sent. Valid values are from 5-900. The default is 60.
CDP Hold Timer	Specify the amount of time that the information sent in the CDP packet is cached by the device that receives the CDP packet. Valid values are from 10-255. The default is 180.
Interface List	Checked the enable check box to enable the interface.

Network Setup > DNS Spoofing

Field	Description
Enable	Enable DNS spoofing
Add Entry	Add DNS spoofing entry
DNS Spoofing Add Entry Setting	
Host Name	Enter one domain name field to spoofing.
IP Address	Enter one mapping IP address.

VPN module

The VPN module includes these pages:

- VPN > Site to Site IPSec VPN
- VPN > GRE Tunnel
- VPN > VPN Passthrough
- VPN > Cisco VPN Server

VPN > Site to Site IPSec VPN

VPN > Site to Site IPSec VPN > NAT Traversal

Field	Description
NAT Traversal	
NAT Traversal	IPSec NAT Traversal can support detecting the presence of NAT. The detecting packet not only detects the presence of NAT between the two IKE peers, but also detects where the NAT is. The location of the NAT device is important, as the keepalives have to initiate from the peer behind the NAT. Please refer RFC3947.To enable this feature, choose **Enabled**. To disable this feature, choose **Disabled**.

VPN > Site to Site IPSec VPN > IKE Policy

Field	Description
IKE Policy	
Add Entry	Click the **Add Entry** button to create another IKE policy.
List of IKE Policies	• Name Show entry of name.
IKE Details	Select an entry from the List of IKE Policies, Details of IKE will show all information about IKE Policy.
General	
Policy Name	Use a unique name which will be displayed in the list of VPN policies for the selection.
Exchange Mode	Choose the exchange mode based on your requirements for security and speed. Main: Choose this mode if you want higher security, but with a slower connection. Main Mode relies upon two-way key exchanges between the initiator and the receiver. The key-exchange process slows down the connection but increases security. Aggressive: Choose this mode if you want a faster connection, but with lowered security. In Aggressive Mode there are fewer key exchanges between the initiator and the receiver. Both sides exchange information even before there is a secure channel. This feature creates a faster connection but with less security than Main Mode.

Field	Description
Remote ID/Local ID	To set up remote and local identity, keep empty to remove identity setting. This can be an IP address (specified as dotted quad or as a Fully Qualified Domain Name, **which will be resolved immediately**) or as a Fully Qualified Domain Name itself (prefixed by "@" to signify that **it should not be resolved**)
IKE SA Parameters	
Encryption Algorithm	The available encryption algorithms are, **DES**, **3DES**, **AES128**, **AES192**, and **AES256**.
Authentication Algorithm	The available authentication algorithms are **MD5** and **SHA1**.
Diffie-Hellman (DH) Group	Choose a DH group to set the strength of the algorithm in bits: Group 1 (768 bits) and Group 2 (1024bits).
Pre Shared Key	Enter an alpha-numeric key to be shared with IKE peer.
Enable Dead Peer (DPD) Detection	This function is not necessary for an IKE rule, but it will help to keep the connection alive during periods when there is no traffic.
DPD Interval	DPD packet is sent periodically in interval seconds during no data traffic.
DPD Timeout	The connection will be disconnected if there is no DPD response after DPD timeout. Unit is second.
Extended Authentication	
XAUTH Client Enable	When this feature is enabled, the router can authenticate users from an external authentication server such as a RADIUS server. Enable this function only if the router is connected to a XAUTH server.
User Name/Password	Enter the credentials that the router uses to connect to the XAUTH server.

VPN > Site to Site IPSec VPN > IPSec Policy

Field	Description
IPSec Policy	A VPN policy contains IPSec Security Association parameters, which define the connection type and key type. Click the Add Entry button to add another VPN policy. To edit an existing policy, click the pencil icon.
Add Entry	Click the **Add Entry** button to create another IPSec policy.
List of VPN Policies	• Enable Select the enable check box to enable the VPN entry. • Number Show Entry of number. • NAME Show Entry of name
VPN Details	Select one entry of List of VPN Policies, Details of VPN will show all information about VPN Policy.
General	
Enable	Check to Enable IPSec Policy.

Field	Description
Policy Number	Enter an identification number for the policy.
Policy Name	Enter a unique name to be used to bring up the tunnel.
Policy Type	Choose Auto Policy or Manual Policy. The Auto Policy uses the IKE protocol to negotiate random keys for more security. You also must set an IKE policy on the Site to Site IPSec VPN > IKE Policy page The Manual Policy does not use IKE, which makes this policy more simple, but less secure.
Remote Endpoint	Choose how you want to identify the remote gateway for this site-to-site VPN tunnel. Choose IP Address to enter an IP address, choose FQDN to enter a Fully Qualified Domain Name, or choose Any (available only for an Auto Policy). Be aware that an FQDN requires that the router can connect to a DNS server to resolve the address before establishing the VPN tunnel.
Encryption Algorithm	Choose DES, 3DES, AES128, AES192, or AES256.
Integrity Algorithm	Choose MD5 or SHA1.
WAN Interface Name	Choose System Default Route, Ether_WAN1, USB_Modem.
Auto Policy Parameters	
PFS	When used in the memo Perfect Forward Secrecy (PFS) refers to the notion that compromise of a single key will permit access to only data protected by a single key. For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.
SA Lifetime	Enter the IPSec SA life time in seconds. The default value is 7800, which is 130 minutes.
Local Traffic Selection	
Local IP	Choose the type of identifier that you want to use (IP Address or IP Address and Subnet Mask) for the local group that is allowed to pass through this tunnel then enter the identifier(s).
IP Address	Enter the IP Address.
Subnet Mask	
Remote Traffic Selection	
Remote IP	Choose the type of identifier that you want to use (IP Address or IP Address and Subnet Mask) for the local group that is allowed to pass through this tunnel then enter the identifier(s).
IP Address	Enter the IP Address.
Select IKE Policy	Choose an IKE policy to associate with this IPSec Policy. To view all IKE policies in a table, click the View IKE Table button.

VPN > GRE Tunnel

Field	Description
GRE Tunnel	Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of network layer protocol packet type inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP Internet network.
Add Entry	Click the **Add Entry** button to create another GRE tunnel
Summary GRE Tunnel	• Number Displayed here is the number which you selected. • Status Displayed here is the status of the tunnel. Tunnel Name Displayed here is the name of the tunnel.
GRE Details	Select one GRE tunnel of Summary GRE tunnel, GRE Details will show all Information about GRE. (like Status, Checksum, Sequence, Key, Key Value, Tunnel Name, Destination IP or HostName and Remote IP Address / Subnet mask)
GRE IP Tunnel	
Tunnel Number	Choose an identification number for this tunnel.
Tunnel Name	Enter a name to describe this tunnel.
Enable	Check the box to enable the tunnel, or uncheck the box to disable the tunnel.
Checksum	Choose **Input**, **Output**, **Both**, or **None**. **Input** requires that all inbound packets have the correct checksum. **Output** requires the checksums for outbound packets. **Both** require the checksum for all inbound and outbound packets. The default is **None**.
Sequence	Choose **None**, **Both**, **Input**, or **Output**. **Output** requires a sequence number for outbound packets. **Input** requires a sequence number for inbound packets. **Both** require a sequence number for inbound and outbound packets. The default is **None**. If sequence number check is set as **Input** or **Both** in receiver side, when sender side GRE session restart, the connection will be resumed after the sequence number reach the amount that record in previous session.
Key	Choose **Input**, **Output**, **Both**, or **None**. **Output** requires a key for outbound packets. **Input** requires a key for inbound packets. **Both** require a key for inbound and outbound packets. The default is **None**.
Key Value	If you chose **Input**, **Output**, or **Both** for the Key, specify the key by entering a number between 1 and 4294967295.
WAN Interface Name	Choose the WAN interface that is used to create the GRE Tunnel with the remote host.
Destination IP or HostName	Enter the Destination IP is the address of the remote network or host to which you want to build a tunnel with it.

Field	Description
Remote IP Address/Subnet Mask	Select the Remote IP Address/Subnet Mask for the remote host. You can use the below Add/Delete button to add/delete the pair
Modify Remote IP Address/Subnet Mask	You can input the pair of Remote IP Address and Subnet mask in this field. And then use the **Add** button to add it into the list of Remote IP Address/Subnet Mask. The following is example for this field: 192.168.2.0/24 or 192.168.3.0/32.

VPN > VPN Passthrough

Field	Description
VPN Passthrough	Configure IPSec passthrough if there are devices behind the router that need to set up IPSec tunnels independently, for example, to connect to another router on the WAN.
IPSec Passthrough	Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Passthrough is enabled by default. To disable IPSec Passthrough, select **Disabled**.
PPTP Passthrough	Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Pass-Through is enabled by default. To disable PPTP Passthrough, select **Disabled**.
L2TP Passthrough	Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Pass-Through is enabled by default. To disable L2TP Passthrough, select **Disabled**.

VPN > Cisco VPN Server

VPN > Cisco VPN Server > Group

Field	Description
Group	The Cisco VPN Server allows mobile users to access Intranet resource via an encrypted (IPSec) VPN tunnel by Cisco Systems VPN Client. The default values of IKE phase 1 and 2 are accepted by Cisco VPN client. Due to system restriction, “Cisco VPN Server” and “Site to Site VPN” are mutually exclusive.
Enable	Click Enable to activate the VPN server. The default is Disable. Enabling the VPN Server will deactivate any site-to-site VPN tunnels that have been defined.
Identify	
Group Name	Cisco VPN Group name used as an identifier for the VPN server. This name must match the group name specified the VPN Client profile. The length can contain up to 32 characters.

Field	Description
Password	Cisco VPN Group password. This password must match the group password specified the VPN Client profile. The length can contain up to 32 characters.
IKE Phase 1	
Exchange Mode	Aggressive mode is applied by default and cannot be changed. This mode is used for negotiating phase one ISAKMP Security Associations (SAs) when using preshared keys for authentication.
ESP Algorithm	Enter an encryption algorithm for the ISAKMP SA.Choices are AES, DES, and 3DES. The default is AES.
AH Algorithm	Hash algorithm for the ISAKMP SA. Choices are MD5 and SHA1. The default is MD5.
Auth Method	Method used to authenticate the remote user. Choices are PSK or PSK+XAUTH. If PSK is selected, then the client will be authenticated if it specifies the correct group name and password. If PSK+XAUTH is selected, then an additional username and password is required.
DH Group	Diffie-Hellman group options. Only 2 [modp 1024], The default is 2 [modp 1024]
IKE Phase 2	
PFS Group	Diffie-Hellman exponentiation group. Choices are: 1 [modp 768], 2 [modp 1024], 5 [modp 1536], 14 [modp 2048], or 15 [modp 3072].
SA Life Time	Defines how long an IPSec SA (security association) will be used. The default is 30 minutes.
Mode Configuration	
Starting IP Address	Starting IP address of the range of addresses that are assigned to the remote client. This range must not be in the same subnet as any VLAN.
Subnet Mask	Subnet mask for the address range assigned to remote clients.
DNS1	Primary DNS server to be used by remote clients.
DNS2	Secondary DNS server to be used by remote clients.
WINS1	Primary WINS server to be used by remote clients.
WINS2	Secondary WINS server to be used by remote clients
Banner	Message displayed to the remote user after they log on. The banner allows up to 500 printable ASCII characters on 1 line.

VPN > Cisco VPN Server > User

Field	Description
VPN Server Users	The Users page contains a list of usernames and passwords that can login to the Cisco VPN Server. Up to 15 unique users can be defined
Add Entry	Add User
List of VPN Server Users	List all the VPN users

Field	Description
User Account	
Username	Username to be provided by the VPN client when using PSK+XAUTH as the authentication method.
Password	Password to be provided by the VPN client when using PSK+XAUTH as the authentication method.
Confirm password	The contents of this field must match the Password field.

Administration module

The Administration module includes these pages:

- Administration > Web Access Management
- Administration > Remote Support
- Administration > Remote Management
- Administration > Time Setup
- Administration > Certificate Management
- Administration > User Management
- Administration > User Privilege Control
- Administration > Log
- Administration > Factory Defaults
- Administration > Firmware Upgrade
- Administration > Backup & Restore
- Administration > Reboot
- Administration > Switch Setting
- Administration > Status

Administration > Web Access Management

Field	Description
Web Access Management	Allows you to change the Router's access settings.
Web Utility Access	To access this web utility, you can use no security by selecting **HTTP** or security by selecting HTTPS. If you select **HTTPS**, be aware that you will need to include https in the address when you connect to the utility. Refer to the following example: https://xxx.xxx.xxx.xxx (the x's represent the Gateway's Internet IP address).
Web Utility Access via Wireless	This feature allows the administrator to access web utility from a wireless device.

Field	Description
Login Banner	
Banner Text	Input the Banner Text, the 1024 character left limitation
Remote Access	
Remote Management	This feature allows you to manage your Gateway from a remote location, via the Internet. If you enable this option and have not changed the router password from the default value, you will be prompted to change the password for security purposes.
Web Utility Access	To access this web utility, you can have no security **HTTP** or security **HTTPS**. For **HTTPS**, enter https://xxx.xxx.xxx.xxx (the x's represent the Gateway's Internet IP address) in your web browser's Address field.
Remote Upgrade	If enabled, the router firmware can be upgraded from Internet.
Allowed Remote IP Address	If you want to access the Router from any external IP address, select **Any 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

Administration > Remote Support

Field	Description
Remote Support Access	
Collect Device Status Information	Click this button will collect system configuration and useful routing information that can help to debug this system.
Enable Remote Support	Turn on remote debug shell.
Access Port	The debug shell's port number. Default is port 22.

Administration > Remote Management

Administration > Remote Management > TR-069

Field	Description
TR-069	Some service providers can automatically provision your customer premises equipment from a central server. Use the TR-069 page to set up communication with an Auto Configuration Server (ACS).
Status	Click **Enabled** to allow auto-configuration of your router from a central server. Otherwise, click **Disabled**.

Field	Description
ACS URL	Enter the address and port of the ACS server. The format should be http(s)://xxx.xxx.xxx.xxx:port or xxx.xxx.xxx.xxx:port or http(s)://xxx.xxx.xxx.xxx:port/zzzz or xxx.xxx.xxx.xxx/zzz. The X's represent the IP address or domain name. The Z's represent the URL location. After the colon, enter the port number.
ACS UserName	The default username is OUI-Serial Number; this value should be the same as configured at ACS side and must be filled.
ACS Password	This value should be the same as configured at ACS side and must be filled.
Connection Request Port	This port receives the Connection Request notification from the ACS
Connection Request Username	This value should be the same as configured at ACS side.
Connection Request Password	This value should be the same as configured at ACS side.
Periodic Inform Enable	Choose Enabled to allow the router to periodically initiate connections to the ACS. Otherwise, choose Disabled.
Periodic Inform Interval	Specify the interval (in seconds) at which the router will initiate connections to the ACS. The default value is 86400 seconds, which is 24 hours.
Binding with Loopback Interface	To check the Binding with Loopback Interface box and select a Loopback Interface to bind IP of the interface with TR-069 Connection request URL. The default is unchecked, which is to bind default WAN IP with Connection request URL.
Request Download	Click the Apply button if you want to immediately initiate a connection to the ACS. The ACS may call the Download RPC when it receives the request.
Provisioning Code	This value could be used by ACS to determine service provider-specific customization and provisioning parameters.

Administration > Remote Management > SNMP

Field	Description
SNMP	Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol that lets you monitor and manage your network from an SNMP manager. SNMP provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SNMP Setting	
SNMP	To enable SNMP identification, click **Enabled**. To disable SNMP, click **Disabled**.
Trusted IP	Choose Any to allow access from any IP address (not recommended) or enter the IP address and subnet mask of a single SNMP manager or trap agent that can access this router via SNMP.
Get Community	Enter the password that allows read-only access to the Gateway's SNMP information.

Field	Description
Set Community	Enter the password that allows read/write access to the Gateway's SNMP information.
SNMPV3	To enable SNMPV3 function, click **Enabled**. To disable SNMPV3, click **Disabled**.
R/W User	Enter the user name for SNMPV3
Auth-Protocol	Choose SNMPV3 auth protocol, available protocol is “HMAC-MD5” and “HMAC-SHA”
Auth-Password	Enter password for Auth check.
PrivProtocol	Authentication is performed by using a users **privKey** to encrypt the data portion the message being sent.
Privacy Password	Enter the privKey for PrivProtocol to use.
SNMP Trap	To enable SNMP Trap, click **Enabled**. To disable SNMP Trap, click **Disabled**. SNMP Trap can be enabled only when SNMP is enabled
Trap Server	Enter the IP address that trap will be sent to.
Trap Community	Enter the password that allow read access to the SNMP Trap message.
Trap User	Enter the user name for SNMPV3 Trap
Trap Auth- Protocol	Choose SNMPV3 Trap auth protocol, available protocol is "HMAC-MD5" and “HMAC-SHA”.
Trap Auth- Password	Enter SNMPV3 Trap password for Auth check
Trap PrivProtocol	SNMPV3 Trap authentication is performed by using a users **privKey** to encrypt the data portion the message being sent.
Trap Privacy Password	Enter SNMPV3 Trap privKey for PrivProtocol to use.

Administration > Remote Management > Local TFTP

Field	Description
Local TFTP Control	
TFTP	Control TFTP enabled or disabled. Default Enabled.
Get Remote File	
URL	This shows where can get remote file.
Save As	Specify the file name to save
Session Timeout	Maximum time allowed for a connection session. A connection timeout for HTTP and FTP session will be 3 seconds, TFTP will be 1 seconds. For HTTP and FTP, a TCP reset response message will terminate a session.
Retry Sessions	Specify how many sessions are going to retry if transient problem occurred in a session

Field	Description
Status	The status of processing get remote file
File List	• Name This is the name of local file. • Size This is the size of local file.

Administration > Time Setup

Field	Description
Time Zone	Setup the time zone and configure the system time by synchronizing with time server (NTP) or set time manually (Manual Setting).
Time Zone	Select the time zone in which your network functions from this drop-down menu.Time zone is a region of the earth that has uniform standard time, usually referred to as the local time.
NTP	
Time Server Address	If you want to use the device's default Network Time Protocol (NTP) server, use the default setting, Auto. If you want to specify the NTP server, select Manual, and enter the URL or IP address of the NTP server you want to use.
Resync Timer	The timer controls how often the Device resyncs with the NTP server. Enter the number of seconds you want the interval to be, or use the default setting, 3600 seconds.
Enable Daylight Saving	Select this option if you want the device to automatically adjust for daylight saving time. This option is enabled by default
Manual Setting	
Date	date in format “Year/Month/Day”
Time	time in format “Hour:Min:Sec”
Auto Recovery After Reboot	
Auto Recovery After Reboot	When this feature is enabled, the device will recover system time after system reboot.

Administration > Certificate Management

Field	Description
Certificate Management	To support uploading certificate authority file through WEB GUI for TR069 and Provision. Up to 3 certificate authority files can be uploaded for T069 and 1 certificate authority file can be uploaded for Provision.

Field	Description
TR069 - Root CA File List	
Enabled	After uploading certificate authority file, click the check box to allow TR069 using the file in certification. Deselect all check boxes to disable all certificate authority file used by TR069. Please note, only one certificate authority file can be selected in the same time.
CA Name	To set the certificate authority file name in the system.
Select Certificate	To select a certificate authority file in client PC, and click Upload button to uploading the file. After uploading, you can click Enabled check box or click icon to delete the file.
Provision File List	
Enabled	After uploading certificate authority file, click the check box to allow Provision using the file in certification. Deselect all check boxes to disable all certificate authority file used by Provision.
CA Name	To set the certificate authority file name in the system.
Select Certificate	To select a certificate authority file in client PC, and click Upload button to uploading the file. After uploading, you can click Enabled check box or client icon to delete the file.

Administration > User Management

Administration > User Management > Password Complexity Settings

Field	Description
Password Complexity Settings	
Password Complexity	Click **Enabled** to activate the User Password Complexity. The default is **Disabled**. Password Complexity check Level: • Low - Too Short Password • Low - Passwords cannot be repeated consecutively for three times • Low - Weak Password, use letters & numbers. • Medium - Medium Password, Use special charecters • High - Strong Password • Password is the same as username.

Administration > User Management > User List

Field	Description
User List	Use the User List page to manage the users who have access to the router configuration utility. There are two default accounts. The account with the default username of admin has administrator-level access. The account with the default username of cisco has guest-level access.
User Account	
Username	This is the name to login router.
Level	This shows user's level.
User List	
Username	Enter a new Username. The two default usernames cannot be changed.
Old Password	To ensure the device's security, you will be asked for your old password when you want to change the password. The default administrator password is admin. The default guest password is cisco. Cisco strongly recommends changing the password.
New Password	To ensure the device's security or WRP500's security, you will be asked for your password when you access the device's configuration utility. The default administrator password is admin. The default guest password is cisco. Cisco strongly recommends changing the password
Confirm New Password	Enter the new password again to confirm.
Level	The level of permission for this user: Admin or User. Admin has access to all settings as specified on the Privilege Control page. User has read-only access.

Administration > User Privilege Control

The privilege control provides three access types for all webpages: Read/Write, Read Only and Hidden. The Read/Write means to allow view and configure the items of the webpage. The Read Only means only allow view the webpage. The Hidden means the no any hyperlink to the webpage.

Administration > Log

Administration > Log > Log Setting

Field	Description
Local	
Local	To save log message in memory of router, after reboot, all the logs will disappear.
Log size	Up limit to save log message in memory, the allowed range is 128~1024KB.

Field	Description
USB	
USB	To save log message in external USB storage, if no USB storage plugs in, only “USB disconnect” shows. If USB storage is connected to, user can set
File Name	Filename to be saved into USB disk
Log size	Up limit to save log message in USB storage, the allowed range is 1~512MB
Syslog Server	
Syslog Server	Send out log message to remote syslog server.
IP Address	Enter IP address of remote syslog server
Port	Enter port number that syslog server listen on. Port 514 is chosen by default.
E-Mail	
E-Mail	Send out log message to specific E-Mail address.
Sender	Specify sender's E-Mail address.
Receiver	Specify receiver's E-Mail address.
SMTP Server	Enter mail server address.
SMTP Port	Enter port number that mail server listen on. Port 25 is chosen by default.
Subject	Specify mail subject to send log.
Number of logs	Enter a number to specify how many logs are collected in an E-Mail.
Interval	Enter a time interval to force send out E-Mail if the amount of logs doesn't reach Number of logs
User Name	Enter a user name for mail server authentication.
Password	Enter a password for mail server authentication.

Administration > Log > Log Module

Field	Description
Log Module Settings	
Status	To enable the collection of activity logs, select **Enabled**, and then click Submit. With logging enabled, you can choose to view temporary logs. Click the **Disabled** radio button to disable this function
Log	This drop-down list becomes available if you enable logging and choose log target to decide where the log save to. • Local Save log to system memory • USB Save log to USB disk, only work when USB disk is plugged in. • E-Mail Send log through E-Mail, please setup E-Mail related information in Log Setting page. • Syslog Server Send log to specific log server, please setup log server address in Log Setting page

Administration > Log > Log Viewer

Field	Description
Log Viewer	Allow user to see, download or clean log message save in system memory
Download All Log	Click to download log message in a file to local PC
Clear Log	Click to clean all log message saved in memory.
Display	Choose module to see related log message.
Filter	To filter log message with specific pattern.

Administration > Log > Firewall Log

Field	Description
Firewall Log	Firewall Log provides a functionality that can log certain specified traffic according to the current system firewall, such as SPI and DoS attacking. The traffic that matches the specified firewall rules will be logged. Firewall Log configuration page is shown as below. The description of each configured fields are explained as below.

Field	Description
Firewall Log Settings	
Firewall Log	Enable or disable firewall logging.
Log Level	Level of logging by using the specified syslog level: • 0 Emergency: system is unusable • 1 Alert: action must be taken immediately • 2 Critical: critical conditions • 3 Error: error conditions • 4 Warning: warning conditions • 5 Notice: normal but significant condition • 6 Info: Info messages • 7 Debug: debug-level messages
Log Category	Select which firewall module that is going to be logged and set how many events that generate one log.

Administration > Factory Defaults

Field	Description
Factory Defaults	The *Factory Defaults* screen allows you to restore the Router's Configuration to its Router and/or voice factory default settings. **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 ITSP for more information.
Factory Defaults	
Restore Router Factory Defaults	To reset the data (router) settings to the default values, select Yes, then click Submit. Any custom data (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 Submit. Any custom voice settings you have saved will be lost when the default settings are restored.

Administration > Firmware Upgrade

Field	Description
Firmware Upgrade	The *Firmware Upgrade* screen allows you to upgrade the Router's firmware. You do not need to upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use. Before upgrading the firmware, download the Router's firmware upgrade file from the Cisco website, *www.cisco.com*. Then extract the file. **Note** The Router may lose the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade the firmware, you will have to re-enter all of your configuration settings.
Firmware Upgrade Settings	
Please select a file to upgrade.	In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.
Upgrade	After you have selected the appropriate file, click this button, and follow the on-screen instructions.

Administration > Backup & Restore

Administration > Backup & Restore > Default Configuration

Field	Description
Default Configuration	Specifies the Default Configuration settings.
Load Service Provider Default Configuration	Select **Yes** to load Service Provider default configure when do system factory default, select **No** to load Cisco factory default.

Administration > Backup & Restore > Backup Configuration

Field	Description
Backup Configuration	To back up the router's configuration settings
Backup	To back up the Router's configuration settings, click this button and follow the on-screen instructions.

Administration > Backup & Restore > Restore Configuration

Field	Description
Restore Configuration	To backup current configuration in case you need to reset the router back to its factory default settings.
Please select a file to restore	To restore the Router's configuration settings, click this button and follow the on-screen instructions. (You must have previously backed up the Router's configuration settings.)

Administration > Reboot

Click **Reboot** to power cycle the router.

Administration > Switch Setting

Administration > Switch Setting > Port Status

Field	Description
Port Status	Active/Inactive switch wire port. When deactivated, this port cannot do any network function until it is reactivated.
Port Status Setting	
Interface	The wire physical port that support on/off by administrator, don't include wireless or pvc interface.
Enabled	Click to allow network traffic input/output from this physical port. When administrator unclicks this port, LED will be off and traffic cannot pass.

Administration > Switch Setting > Bind MAC to Port

Field	Description
Bind MAC to Port	Enable this function will bind the assigned mac address to one of the LAN ports, and only allow this mac address can access this assigned LAN port but not others port.

Field	Description
Bind MAC to Port Setting	
Adding MAC address	Administrator add new entry to allow network traffic which source MAC come from which physical wire port. • LAN Port The physical wire port that support will bind to this mac address, not include wireless or PVC port. • MAC Address DUT will allow network traffic which source MACs (amount of 16) to match this setting. • Add Button that add this bind LAN Port/MAC address into filter table.
Enable Bind MAC to LAN Port 1	All MAC address entries that LAN Port 1 is relative • Enable click button to on/off Bind MAC address to LAN Port 1 function. • MAC Address address lists that administrator setting at LAN Port 1.
Enable Bind MAC to LAN Port 2	All MAC address entries that LAN Port 2 is relative. • Enable click button to on/off Bind MAC address to LAN Port 2 function. • MAC Address address lists that administrator setting at LAN Port 2.
Enable Bind MAC to LAN Port 3	All MAC address entries that LAN Port 3 is relative. • Enable click button to on/off Bind MAC address to LAN Port 3 function. • MAC Address address lists that administrator setting at LAN Port 3.
Enable Bind MAC to LAN Port 4	All MAC address entries that LAN Port 4 is relative. • Enable click button to on/off Bind MAC address to LAN Port 4 function. • MAC Address address lists that administrator setting at LAN Port 4.

Administration > Status

Field	Description
Status	
CPU	This shows CPU's MIPS, Loads and Uptime • Loads This shows CPU's Loads. • Uptime This shows CPU's Uptime.
Memory	This shows Memory's Total size(%), Free size(%), Used size(%), Buffer size(%), Cached size(%), active size and inactive size(%). • Total This shows Memory's total size(%). • Free This shows Memory's free size(%). • Used This shows Memory's used size(%). • Buffers This shows Memory's buffer size(%). • Cached This shows Memory's cached size(%). • Active This shows Memory's active size(%). • Inactive This shows Memory's inactive size(%).

Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the WRP500s.

Note If you can't find an answer here, visit Cisco Community Central > Small Business Support Community at the following URL:
www.myciscocommunity.com/community/smallbizsupport/voiceandconferencing/ata

Q. I want to access the Configuration Utility, but the address I entered did not work.

A. If the device has ever been configured to allow access from the WAN interface, use the Interactive Voice Response Menu to find the Internet IP address. Follow these steps:

1. Use a telephone that is connected to the Phone 1 port of the WRP500.
2. Press **** (in other words, press the star key four times).
3. After the greeting plays, press **110#**.
4. Write down the IP address as it is announced.
5. Open a web browser on a networked computer.
6. Start Internet Explorer and enter the IP address of the WRP500.

A. If the device has never been configured (that is, it still has the factory default configuration):

1. Connect PC to the LAN port. The PC should obtain the IP address through DHCP; the gateway is the IP address of the WRP500. For example, if the PC receives IP address 192.168.15.100, the WRP500 IP address is 192.168.15.1.
2. Enter web page.
3. Use default account admin: admin to login.
4. Navigate to **Administration > Web Access Management.**
5. Set *remote management* to *enabled* and *remote management port* to *80*.
6. Follow the steps from the previous Answer (if the device has ever been configured) to access the device web page through the WAN interface.

Q. I am trying to access the Configuration Utility, but I do not see the login screen. Instead, I see a *404 Forbidden* screen.

A. If you are using Windows Explorer, perform the following steps until you see the Configuration Utility login screen. (Mozilla requires similar steps.)

1. Click **File.** Make sure *Work Offline* is NOT checked.
2. Press **CTRL + F5**. This is a hard refresh, which forces Windows Explorer to load new web pages instead of cached ones.
3. Click **Tools.**
4. Click **Internet Options.**
5. Click the **Security** tab.
6. Click the **Default level** button.
7. Ensure that the security level is Medium or lower.
8. Click the **OK** button.

Q. How do I save the voice configuration for my WRP500?

1. Log in as admin.
2. Navigate to **Administration > Backup & Restore > Backup Configuration.**
3. Click the **Backup** button. The configuration is downloaded to your PC.
4. This .cfg file is helpful to provide to the support team when you have a problem or technical question.

Q. How do I debug the WRP500? Is there a syslog?

A. The WRP500 provides the option to send messages to both a syslog and debug server. The ports can be configured (by default, the port is 514).

1. Make sure you do not have a firewall running on your computer that can block port 514.
2. Start Internet Explorer, connect to the Configuration Utility.
3. Login as admin.The default username and password are both **admin**.
4. Under the **Voice > System** menu, set *Syslog Server* and *Debug Server* as the IP address and port number of your syslog server. Note that this address has to be reachable from the WRP500. For example, if the WRP500 is at 192.168.15.1, reachable addresses are in the range of 192.168.15.x, for example 192.168.15.100:514.
5. Set *Debug level* to **3.** You do not need to change the value of the *syslog server* parameter.
6. Set *Debug Option* to **dbg.all**.
7. To capture SIP signaling messages, under the **Voice > Line** page, set *SIP Debug Option* to **Full**. The file output is syslog.<portnum>.log (for the default port setting, syslog.514.log).

Q. How do I access the WRP500 if I forget my password?

A. By default, the User and Admin accounts have no password. If the ITSP sets the password for either account and you do not know it, you need to contact the ITSP.

If the password for the user account was configured after you received the WRP500, you can reset the device to the user factory default, which preserves any provisioning that the ITSP completed.

If the Admin account needs to be reset, you have to perform a full factory reset, which also erases any provisioning.

To reset the WRP500 to the factory defaults, perform the following steps:

1. Connect an analog phone to the WRP500 and access the IVR by pressing ****.
2. Press the appropriate code to reset the unit:
   - Press **73738#** to perform a full reset of the unit to the factory default settings. The Admin account password will be reset to the default of blank.
3. Press **1** to confirm the operation, or press * to cancel the operation.
4. Log in to the unit by using the User or Admin account without a password.
5. Reconfigure the unit as necessary.

Q. The WRP500 is behind a NAT device or firewall. I am unable to make a call or I am only receiving a one-way connection. What should I do?

A. Complete the following steps:

1. Configure your router to port forward *TCP port 80* to the IP address of the WRP500. You should use a static IP address. (For help with port forwarding, consult the documentation for the NAT device or firewall.)
2. On the Line tab of the Configuration Utility, change the value of *Nat Mapping Enable* to **yes**. On the SIP tab, change *Substitute VIA Addr* to **yes**, and the *EXT IP* parameter to the IP address of your router.
3. Make sure you are not blocking the UDP PORT 5060,5061 and port for UDP packets in the range of 16384-16482.
4. Disable SPI if this feature is provided by your firewall.
5. Identify the SIP server to which the WRP500 is registering. If it supports NAT, using the *Outbound Proxy* parameter.
6. Add a STUN server to allow traversal of UDP packets through the NAT device. On the SIP tab of the Configuration Utility, set *STUN Enable* to **yes**, and enter the IP address of the STUN server in *STUN Server*.

   STUN (Simple Traversal of UDP through NATs) is a protocol defined by RFC 3489. STUN allows a client behind a NAT device to find out its public address, the type of NAT it is behind, and the port associated on the Internet connection with a particular local port. This information is used to set up UDP communication between two hosts that are both behind NAT routers. Open source STUN software can be obtained at the following address: http://www.voip-info.org/wiki-Open+Source+VOIP+Software

Note STUN does not work with a symmetric NAT router. Enable debug through syslog (see FAQ#10), and set *STUN Test Enable* to **yes**. The messages indicate whether you have symmetric NAT or not.

Q. My computer cannot connect to the Internet. What should I do?

A. Follow this procedure:

1. Ensure that the Unified Communications Platform is powered on. The Power/Sys LED should be solid green and not flashing.

2. If the Power LED is flashing, power off all of your network devices, including the modem, the Unified Communications Platform, and the computers.
3. Wait for 30 seconds.
4. Power on each device in the following order:
   – Cable or DSL modem
   – Unified Communications Platform
   – Computer
5. Check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the Unified Communications Platform. The modem must be connected to the WAN (Internet) port on the Unified Communications Platform. For those ADSL devices that do not come with a modem, connect the ADSL line (normally, the digital phone line) to the WAN (Internet) port on the Unified Communications Platform.

Q. The computer cannot connect wirelessly to the network. What should I do?

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

Q. I upgraded my firmware and now the Unified Communications Platform is not working properly. Why?

A. If the Unified Communications Platform is not working properly after an upgrade, you may need to perform a factory reset. To perform a factory reset, use a ball pen point or a paper clip to poke through the hole labeled **reset** on the side of the Unified Communications Platform.

Q. There is no dial tone, and the Phone 1 or 2 LED is not solid green. What should I do?

A. Follow this procedure:

1. Make sure the telephone is plugged into the appropriate port, Phone 1 or 2.
2. Disconnect and re-connect the RJ-11 telephone cable between the Unified Communications Platform and telephone.
3. Ensure your telephone is set to its tone setting (not pulse).
4. Ensure your network has an active Internet connection. Try to access the Internet, and check to see whether the Unified Communications Platform WAN LED flashes green.
   a. If you do not have a connection, power off all of your network devices, including the modem, the Unified Communications Platform, and the computers.
   b. Wait 30 seconds.
   c. Power on each device in the following order:
   – Cable or DSL modem
   – Unified Communications Platform
   – Computers and other devices
5. 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. Why?

A. Consider the following possible causes and solutions:

- Cordless phone

  If you are using the Unified Communications Platform wireless function and a cordless phone, they may be using the same radio frequency and may interfere with each other. Move the cordless phone farther away from the Unified Communications Platform.

- 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 be sure to exit the program before you make 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 that are 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 DSL telephone line does not fit into the Unified Communications Platform WAN (Internet) port. Why?

A. The Unified Communications Platform does not replace your modem. You still need your DSL modem in order to use the Unified Communications Platform. Connect the telephone line to the DSL modem, re-run the setup wizard, then follow the on-screen instructions.

Q. The modem does not have an Ethernet port.

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

Q. The Unified Communications Platform does not have a coaxial port for the cable connection.

A. The Unified Communications Platform does not replace your modem. You still need your cable modem in order to use the Unified Communications Platform. Connect your cable connection to the cable modem, re-run the setup wizard, then follow the on-screen instructions.

APPENDIX D

Environmental Specifications for the WRP500

Device Dimensions	6.69 x 6.69 x 1.30 in. (170 x 170 x 33 mm) (includes foot)
Unit Weight	15.52 oz (440g)
Power	External, switching 12 VDC 1.67A
Certification	FCC, CE, CB,IC, UL Wi-Fi (802.11ac/b/g/n, WPA2, WMM, WMM Power Save, and WPS2.0)
Operating Temperature	32 to 104°F (0 to 40°C)
Storage Temperature	-22 to 140°F (-30 to 60°C)
Operating Humidity	5 to 95%, noncondensing
Storage Humidity	5 to 95%, noncondensing

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 Cisco WRP500.

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Downloads (Login Required)	www.cisco.com/support
Small Business Support Center (SBSC) Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Cisco Small Business Firmware Downloads	www.cisco.com/go/software
Product Documentation	
Product Documentation for Cisco Small Business Voice Gateways and ATAs	http://www.cisco.com/c/en/us/support/unified-communications/small-business-voice-gateways-ata/tsd-products-support-series-home.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb