



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**.

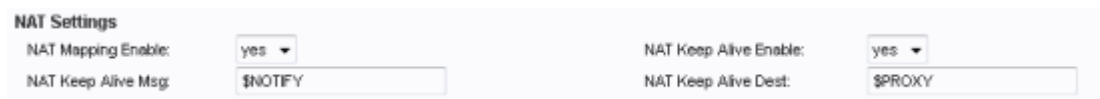
- Step 3** In the *NAT Support Parameters* section, enter the following settings:
- **Substitute VIA Addr:** Choose **yes**.
 - **EXT IP:** Enter the public IP address that was assigned by your ISP.

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



NAT Settings	
NAT Mapping Enable:	yes
NAT Keep Alive Enable:	yes
NAT Keep Alive Msg:	\$NOTIFY
NAT Keep Alive Dest:	\$PROXY

- 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

NAT Settings			
NAT Mapping Enable:	yes ▾	NAT Keep Alive Enable:	yes ▾
NAT Keep Alive Msg:	\$NOTIFY	NAT Keep Alive Dest:	\$PROXY



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:
- Under the **Voice** menu, click **System**.
 - 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.
 - From the *Debug level* drop-down list, choose **3**.
 - From the Debug option drop-down list, choose **dbg_all**.

Figure 2-5 Voice tab > System

Miscellaneous Settings	
Syslog Server:	10.74.1.1
Debug Level:	3
Debug Server:	10.74.1.1
Debug Option:	dbg_all

- Step 4** To collect information about the type of NAT that your router is using, complete the following tasks:
- Under the **Voice** menu, click **SIP**.
 - Scroll down to the *NAT Support Parameters* section.
 - From the *STUN Test Enable* field, choose **yes**.
- Step 5** To enable SIP signaling, complete the following task:
- Under the **Voice** menu, click **Line 1** or **Line 2** to choose the line interface that you want to modify.
 - 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](#).

