SPA9xx Set up behind NAT and Experiencing Voice Problem

Document ID: 108951

Contents

Introduction

Why am I experiencing a voice problem when my SPA9xx phone is behind Network Address Translation (NAT)?

Related Information

Introduction

This document is one in a series to assist in the setup, troubleshooting, and maintenance of Cisco Small Business products.

Q. Why am I experiencing a voice problem when my SPA9xx phone is behind Network Address Translation (NAT)?

A. Access the SPA9xx web user interface

Complete these steps:

1. Check your SPA9xx IP address. You can obtain the IP address through the LCD screen on the IP phone. Press the Setup Button, then press 9. The LCD screen displays the current IP address.
2. Launch your browser and type in http://IP_Address_of_your_SPA9xx on the address field, and hit Enter.

Note: You are now ready to configure the SPA9xx for NAT. If the web interface is asking for a username and password, this means that the unit was locked by your Provider. Contact your respective VoIP Provider for assistance.

Enable NAT support settings

Complete these steps:

1. You can set NAT Mapping Enable and NAT Keep Alive Enable to yes under EXT1 tab of the SPA.
Click **Submit All Changes**.

2. Alternatively, if the SIP server registering the SPA9xx supports NAT, you can use Outbound Proxy configuration of the SPA in order to connect to it.

![Outbound Proxy Configuration](image)

3. The SPA product also supports STUN (Simple Traversal of UDP through NAT) protocol. Under the SIP tab, look for NAT Support Parameters. On STUN Server field, place your STUN server address, and set Substitute VIA Addr and STUN Enable to **yes**. Place your WAN IP address on EXT IP, and click **Submit All Changes**.

![STUN Support Parameters](image)

**Note:** STUN will not work if you have a symmetric NAT. If you enable the debug through syslog, and set STUN Test Enable to **yes**, the SPA product will print information about whether or not you have a symmetric NAT.

On your NAT, you need to unblock UDP ports 5060, 5061, and the port range from 16384–16482. You might also need to disable "SPI" if there is such a function in your firewall.