ADMINISTRATION GUIDE

Cisco Small Business

IP Phones Models SPA301, SPA303, SPA501G, SPA502G, SPA504G, SPA508G, SPA509G, SPA512G, SPA514G, SPA525G, SPA525G2, and WIP310

Contents

Chapter 1: Getting Started 11

Overview of the Phones 12

Cisco Attendant Console 12

Changing the Cisco SPA500DS Attendant Console Display 12

Network Configurations 14

Cisco SPA9000 Voice System 15

Cisco Unified Communications 500 Series for Small Business 15

Other SIP IP PBX Call Control Systems 15

Updating Firmware 16

Determining the Firmware Version 17

Determining the IP Address of the Phone 18

Downloading the Firmware 19

Installing the Firmware 19

Using the Web-Based Configuration Utility 20

Allowing Web Access to the IP Phone 21

Saving the Configuration Profile 23

Understanding Administrator and User Views 23

Restricting User Access to the Phone Interface Menus (Cisco SPA300 and Cisco SPA500 Series) 24

Accessing Administrative Options 24

Using the Web Administration Tabs 24

Viewing Phone Information 25

Viewing Reboot Reasons 25

Viewing the Reboot History on the Phone Web User Interface 27

Viewing the Reboot History on the IP Phone Screen 27

Viewing the Reboot History in the SPA Status Dump File 27

Using IVR on IP Phones Without Screens 27

Ensuring Voice Quality 31

Supported Codecs 31

Bandwidth Requirements 32

Factors Affecting Voice Quality 33

SIP Publish Signaling Improvements 35

Chapter 2: Configuring Lines 37

Configuring a Line Key 38

Configuring Shared–Line Appearance 38

Configuring Call Appearance Per Line 41

Expand Call Appearance Per Line 42

Configuring Unused Line Keys to Access Services 42

Configuring Call Park on the Cisco SPA525G or Cisco SPA525G2 (MetaSwitch) 43

Assigning Busy Lamp Field, Call Pickup, or Speed Dial Functions to Unused Lines 44

Configuring Call Pickup and Busy Lamp Field 45

Configuring Speed Dial 46

Configuring Audio Indication for Call Pickup Event 47

Chapter 3: Customizing Standard Features 48

Configuring Phone Information and Display Settings 49

Configuring the Phone Name 49

Configuring Voice Mail 49

Configuring Internal Voice Mail for Each Extension (Using a Cisco SPA400) 49

Customizing the Startup Screen 50

Changing the Display Background 51

Configuring the Screen Saver 52

Configuring the LCD Contrast 54

Configuring Back Light Settings (Cisco SPA525G or Cisco SPA525G2) 54

Configuring Linksys Key System Parameters 55

Enabling Call Features 56

Enabling Anonymous Call and Caller ID Blocking Services 56

Enabling ACD Service 56

Enabling Call Back Service 56

Enabling Call Park and Call Pickup Services 57

Enabling Call Transfer and Call Forwarding Services 57

Enabling Conferencing 58

Enabling Do Not Disturb 58
Enabling the Missed Call Shortcut 58
Logging Missed Calls 58
Enabling Paging (Intercom) 59
Configuring Paging Groups 59
Enabling Service Announcements 61
Customizing Phone Softkeys 61
Programmable Softkeys 66
Configuring the Message Waiting Indicator 68
Configuring Ring Tones 69
Configuring On-Demand Ring Tones (Cisco SPA525G or Cisco SPA525G2) 70
User-Created MP3 Ring Tones (Cisco SPA525G or Cisco SPA525G2) 71
Creating and Uploading Ring Tones Using the Ring Tone Utility (Cisco SPA300 Series and Cisco SPA500 Series only) 71
Assigning a Ring Tone to an Extension 73
Configuring RSS Newsfeeds (Cisco SPA525G or Cisco SPA525G2) 74
Configuring Audio Settings 75
Configuring Audio Input Gain (Cisco SPA300 Series and Cisco SPA500 Series) 76
Enabling Wireless (Cisco SPA525G or Cisco SPA525G2 only) 76
Configuring Bluetooth (Cisco SPA525G or Cisco SPA525G2 only) 77
Enabling Bluetooth from the Web Interface 77
Enabling Bluetooth from the Phone 77
Pairing a Bluetooth Headset 78
Pairing Your Cisco SPA525G2 with a Bluetooth-Enabled Mobile Phone 79
Initiating Pairing from the Cisco SPA525G2 80
Initiating Pairing from Your Bluetooth-Enabled Mobile Phone 81
Enabling SMS Messaging 82
Enabling and Configuring the Phone Web Server 83
Configure the Web Server from the Phone Web Interface 83
Configure the Web Server from the Phone Screen Interface 84

Configuring LDAP for the Cisco SPA300 Series and Cisco SPA500 Series IP Phones 84

Configuring BroadSoft Settings (Cisco SPA300 Series and Cisco SPA500 Series) 89

Configuring BroadSoft Directory 89

Configuring Synchronization of Do Not Disturb and Call Forward on a Per Line Basis (Applicable to Broadsoft) 90

Configuring Synchronization of DND and CEWD 90

Configuring Synchronization of DND and CEWD by Using the Configuration File 91

Configuring Broadsoft ACD Support 91

Configuring Broadsoft ACD Support 92

Configuring XML Services 92

Configuring Music On Hold 95

Configuring Extension Mobility 95

Configuring Video Surveillance (Cisco SPA525G or Cisco SPA525G2) 96

Configuring the User Name and Account on the Camera 97

Entering Camera Information Into the Cisco SPA525G or Cisco SPA525G2 Configuration Utility 97

Viewing the Video 98

Chapter 4: Configuring SIP, SPCP, and NAT 99

SIP and Cisco IP Phones 99

SIP Over TCP 101

SIP Proxy Redundancy 101

Configuring Survivable Remote Site Telephony (SRST) Support 101

RFC3311 Support 102

Support for SIP NOTIFY XML-Service 102

Configuring SIP 103

Configuring Basic SIP Parameters 103

Configuring SIP Timer Values 107

Configuring Response Status Code Handling 110

Configuring RTP Parameters 110

Configuring SDP Payload Types 112
Configuring SIP Settings for Extensions 115
Configuring a SIP Proxy Server 121
Configuring Subscriber Information Parameters 123
Configuring the IP Phone Communications Protocol 124
Configuring the Protocol on a Cisco SPA525G or Cisco SPA525G2 125
Configuring the Protocol on a Cisco SPA300 Series or Cisco SPA500 Series IP Phone 125
Managing NAT Transversal with Cisco IP Phones 125
NAT Mapping with Session Border Controller 126
NAT Mapping with SIP-ALG Router 126
NAT Mapping with a Static IP Address 126
NAT Mapping with STUN 127
Determining Whether the Router Uses Symmetric or Asymmetric NAT 128

Chapter 5: Configuring Security, Quality, and Network Features 130

Setting Security Features 131
Challenging SIP Initial INVITE and MWI Messages 131
Encrypting Signaling with SIP Over TLS 131
Securing Voice Traffic with SRTP 132
Authorizing Secure Calls with a Mini-certification 132
Secure Call Indication Tone 133
Configuring Voice Codecs 133
Configuring Domain and Internet Settings 137
Configuring Restricted Access Domains 137
Configuring DHCP, Static IP, or PPPoE Connection Type 137
Configuring Power Settings 139
Setting Optional Network Servers 139
Configuring VLAN Settings 141
Configuring Cisco Discovery Protocol (CDP) 141
Configuring LLDP-MED 141
TLV Information 143
Configuring the VLAN Settings 149

Configuring SSL VPN on the Cisco SPA525G or Cisco SPA525G2 151
Configuring the VPN on the Security Appliance 152
Configuring the VPN on the Cisco SPA525G or Cisco SPA525G2 152

Chapter 6: Provisioning 155

Redundant Provisioning Servers 156
Retail Provisioning 156
Automatic In-House Preprovisioning 157
Using HTTPS 158
Server Certificates 158
Client Certificates 159
Obtaining a Server Certificate 159
Manually Provisioning a Phone from the Keypad 160
Sample Configuration File 161
Updating Profiles and Firmware 162
Launch a Firmware Update by using a Browser Command 168
Launch a Profile Update by using a Browser Command 168
Rebooting a Phone by using a Browser Command 169
Configuring a Custom Certificate Authority 169
General Purpose Parameters 170
Using TR-069 170

Chapter 7: Configuring Regional Parameters and Supplementary Services 174

Scripting for Cadences, Call Progress Tones, and Ring Tones 175
Cadence Script 175
Example: Normal Ring 175
Example 2: Distinctive Ring (short, short, short, long) 176
Tone Script 176
Example: Dial Tone 176
Example: SIT Tone 177
Ring Script 178
Call Progress Tones 179

Distinctive Ring Patterns 179
Example 1: Normal Ring 179
Example 2: Distinctive Ring (short, short, short, long) 180
Distinctive Call Waiting Tone 180
Control Timer Values (sec) 181
Configuring Supplementary Services (Star Codes) 182
Entering Star Code Values 182
Activating or Deactivating Supplementary Services 186
Vertical Service Announcement Codes (Cisco SPA300 Series and Cisco SPA500 Series) 187
Bonus Services Announcement Description 187
Outbound Call Codec Selection Codes 189
Miscellaneous Parameters 189
DTMF Parameters 189
Localizing Your IP Phone 190
Managing the Time and Date 191
Configuring Daylight Saving Time 192
Daylight Saving Time Examples 193
Selecting a Display Language 194
Creating a Dictionary Server Script 194

Chapter 8: Configuring Dial Plans 196

About Dial Plans 196
Digit Sequences 197
Digit Sequence Examples 200
Acceptance and Transmission of the Dialed Digits 202
Dial Plan Timer (Off-Hook Timer) 203
Syntax for the Dial Plan Timer 203
Interdigit Long Timer (Incomplete Entry Timer) 204
Syntax for the Interdigit Long Timer 204
Interdigit Short Timer (Complete Entry Timer) 205
Syntax for the Interdigit Short Timer 205
Editing Dial Plans on the IP Phone 206

Resetting the Control Timers 207

Chapter 9: Configuring LED Patterns 208

LED Script Examples 211
LED Pattern 211

Appendix A: Cisco SPA IP Phone Field Reference 213

Info Tab 214
System Information 214
Network Configuration (SPCP) 217
VPN Status (Cisco SPA525G or Cisco SPA525G2 Only) 218
Product Information 218
Phone Status 219
Ext Status 220
Line/Call Status 221
Downloaded Ring Tone 223
System Tab 224
System Configuration 224
Internet Connection Type and Static IP Settings 226
Power Settings (Cisco SPA500 Series or Cisco SPA300 Series Only) 227
PPPoE Settings (Cisco SPA525G or Cisco SPA525G2 Only) 227
Optional Network Configuration 228
VLAN Settings 229
Wi-Fi Settings (Cisco SPA525G or Cisco SPA525G2 Only) 231
Bluetooth Settings (Cisco SPA525G or Cisco SPA525G2 Only) 231
VPN Settings (Cisco SPA525G or Cisco SPA525G2 Only) 231
SIP Tab 232
SIP Parameters 232
SIP Timer Values (sec) 237
Response Status Code Handling 240
RTP Parameters 241
SDP Payload Types 243

NAT Support Parameters 246
Linksys Key System Parameters 249
Provisioning Tab 250
Regional Tab 250
Call Progress Tone Description 250
Distinctive Ring Patterns 254
Control Timer Values (sec) 256
Vertical Service Activation Codes 257
Vertical Service Announcement Codes 262
Outbound Call Codec Selection Codes 263
Time (Cisco SPA525G or Cisco SPA525G2 Only) 266
Language (Cisco SPA525G or Cisco SPA525G2 Only) 267
Miscellaneous 267
Phone Tab 272
General 272
Line Key 275
Miscellaneous Line Key Settings 277
Line Key LED Pattern 278
Supplementary Services 280
Ring Tone (Cisco SPA300 Series and Cisco SPA500 Series) 282
Ring Tone (Cisco WIP310) 283
Auto Input Gain (dB) 284
Multiple Paging Group Parameters 285
BroadSoft Settings 286
LDAP Corporate Directory Search 287
XML Service 291
Extension Mobility 291
Programmable Softkeys 292
Ext Tab 293
General 294
Share Line Appearance 294
NAT Settings 295

Network Settings 296
SIP Settings 297
Call Feature Settings 301
Proxy and Registration 304
Subscriber Information 307
Audio Configuration 308
Dial Plan Script 312
User Tab 314
Call Forward 314
Speed Dial 314
Supplementary Services 315
Camera Settings (Cisco SPA525G or Cisco SPA525G2) 315
Web Information Service Settings (Cisco SPA525G or Cisco SPA525G2) 315
Audio (SPA5XX)/Audio Volume (SPA525G/525G2) 315
Screen (Cisco SPA525G or Cisco SPA525G2) 317
Attendant Console Tab (Cisco SPA500 Series) 319
General 319
Attendant Console Status 321
Cisco SPA525G or Cisco SPA525G2-Specific Tabs 322
Wi-Fi 322
Bluetooth 322
Personal Address Book 324
Call History 324
Speed Dials 324
Firmware Upgrade 324

Appendix B: Where to Go From Here 325

1

Getting Started

This chapter contains basic information on Cisco SPA300 Series, Cisco SPA500 Series, and Cisco Wireless-G IP phones. This chapter contains the following sections:

- Overview of the Phones
- Network Configurations
- Updating Firmware
- Using the Web-Based Configuration Utility
- Viewing Phone Information
- Using IVR on IP Phones Without Screens

Overview of the Phones

The Cisco SPA IP Phone family is a line of full-featured VoIP (Voice-over-Internet Protocol) phones that provide voice communication over an IP network. They provide all the features of traditional business phones, such as call forwarding, redialing, speed dialing, transferring calls, conference calling, and accessing voice mail. Calls can be made or received with a handset, a headset, or a speaker.

For more information on phone features, see the data sheets for each product.

Cisco Attendant Console

The Cisco Attendant Consoles are accessory consoles for the Cisco SPA500 Series IP phones. The Cisco SPA500S provides 32 three-color (red, green, and orange) programmable line buttons, and the Cisco SPA500DS provides 30 buttons. The Cisco Attendant Console attaches to the IP phone with the attachment arm provided. It obtains power directly from the IP phone; it does not require a separate power supply. Two Cisco Attendant Console units can be attached to a single IP phone to monitor a total of 64 (SPA500S) or 60 (SPA500DS) separate lines.

Detailed information on the installation of the Cisco Attendant Consoles are provided in the *Cisco Small Business SPA500S Attendant Console Quick Start Guide* and the *Cisco Small Business SPA500DS 15-Button Digital Attendant Console for SPA500 Family Phones Quick Start Guide*.

Changing the Cisco SPA500DS Attendant Console Display

The Cisco SPA500DS provides a backlit LCD display. The backlight is controlled by the backlight settings of the phone display and is not separately configurable; that is, the Cisco SPA500DS display is lit when the phone display is lit, and is off when the phone display is off.

You can choose the font size (10 or 12 point) of the text displayed on the Cisco SPA500DS. You can also configure the text contrast, or how dark the text appears on the display.

To configure these options from the phone:

Cisco SPA5XX:

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Att. Cons. Preferences** and press **select**.

STEP 3 Choose **Font Size** or **Contrast** from the menu and press **edit**:

- To change the font size, press **option** to switch between 10 and 12 point font. Press **ok** to save.
- To change the display contrast, use the keypad to enter a number value from 1 to 30. The higher the number, the greater the contrast on the display. Press **ok** to save.

STEP 4 Press **save** to save your changes.

Cisco SPA525G/525G2:

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **User Preferences** and press **Select**.

STEP 3 Scroll to **Att. Console Preferences** and press **Select**.

STEP 4 Choose **Font Size** or **Contrast** from the menu.

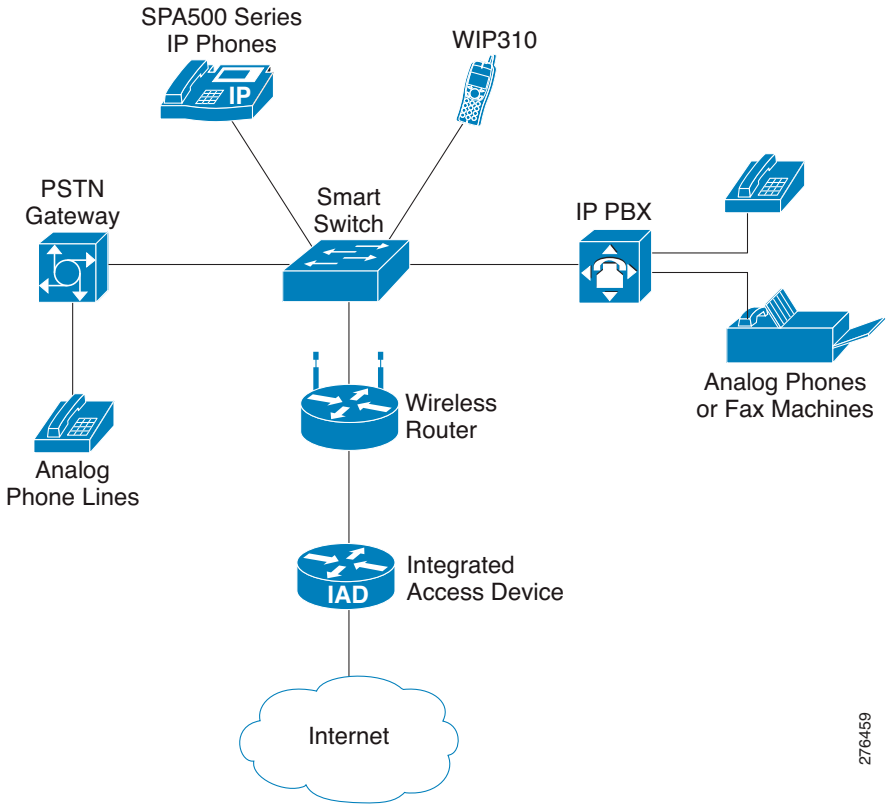
- To change the font size, press the **Right Arrow** button to switch between 10 and 12 point font. Press **Set** to save.
- To change the display contrast, use the keypad to enter a number value from 1 to 30. The higher the number, the greater the contrast on the display. Press **Set** to save.

To configure these options from the web interface, navigate to **Admin Login** > **advanced** > **Voice** > **Attendant Console.** In the General section, configure the following parameters:

- **Attendant Console Font Size**—Choose 10 or 12 point font.
- **Attendant Console LCD Contrast**—Enter a number value from 1 to 30. The higher the number, the greater the contrast on the display.

Network Configurations

The Cisco SPA IP phones can be used as part of a Cisco SPA9000 Voice System phone network, any vendor SIP network, or Cisco Unified Communications 500. The Cisco SPA IP phones support Session Initiation Protocol (SIP). The Cisco SPA300 Series or the Cisco SPA500 Series IP phones also support Smart Phone Control Protocol (SPCP).



This document describes some common network configurations; however, your configuration can vary, depending on the type of equipment used by your service provider.

Cisco SPA9000 Voice System

The Cisco SPA9000 Voice System is an affordable and feature-rich voice-over-IP (VoIP) telephone system that is designed for small businesses. The Cisco SPA9000 Voice System uses standard TCP/IP protocols and can provide global connectivity through any Internet Telephony Service Provider (ITSP) that supports SIP.

At minimum, the Cisco SPA9000 Voice System includes a Cisco IP PBX and one or more Cisco SPA IP phones. These devices are connected through a switch to a local area network (LAN). With an Internet connection, the Cisco SPA9000 Voice System can subscribe to ITSP services to take advantage of low calling rates. With the optional Cisco SPA400, the Cisco SPA9000 Voice System can connect to the Public Switched Telephone Network (PSTN) to support legacy phone lines and provide local voice mail service.

You can configure and manage the Cisco SPA IP phones by using the Interactive Voice Response (IVR) system, the Cisco SPA9000 Voice System Setup Wizard, or a built-in web server.

The phone web user interface is limited when the phone is connected to a Cisco UC320W. For information on configuring the network phone system, refer to the Cisco UC320W Administration Guide.

Cisco Unified Communications 500 Series for Small Business

The Cisco Unified Communications 500 Series for Small Business is an affordable SPCP appliance that provides voice, data, video, network security, and wireless communications capabilities while integrating with existing desktop applications, such as calendar, e-mail, and customer relationship management (CRM) programs. The Cisco SPA300 Series and Cisco SPA500 Series IP phones can be configured to work with this system.

Other SIP IP PBX Call Control Systems

Cisco SPA IP phones are compatible with other SIP IP PBX call control systems, such as BroadSoft and Asterisk. Configuration of these systems is not described in this document. For more information, see the documentation for the SIP PBX system to where you are connecting the Cisco SPA IP phones.

Updating Firmware

Phones should be updated to the latest firmware before using any administration features. There are several ways to update your firmware:

SIP Phones

- Cisco SPA9000 Voice System Setup Wizard—If you are using the Cisco SPA IP phones with a Cisco SPA9000 Voice System, see the *Cisco SPA9000 Voice System Setup Wizard User Guide* for instructions. (The Setup Wizard does not support Cisco SPA300 Series IP phones; you must use a different process to upgrade that firmware.)
- Autoprovisioning—A configuration file that includes firmware upgrade information is downloaded by a phone when it is powered on or configured to do so. The configuration file (also referred to as a profile) includes parameters that direct how and when the phone firmware is to be updated. See the **"Updating Profiles and Firmware" section on page 162** for more information.

Cisco SPA300 Series, Cisco SPA500 Series, and Cisco WIP310 Executable

- Firmware Update Executable File—Download the firmware update utility from the related product page on Cisco.com to your PC. Run the update by double-clicking the executable file. Your computer must be on the same subnetwork as the Cisco SPA IP phones.

Cisco SPA525G and Cisco SPA525G2

- Configuration Utility—You can download the latest phone firmware configuration utility from Cisco.com onto your PC and use that utility to upgrade your firmware.

Cisco WIP310

- TFTP or HTTP server—The latest firmware image file is loaded onto an HTTP/TFTP server and is accessed by a web browser. See the *Cisco WIP310 User Guide* for more information.

Determining the Firmware Version

To determine the current firmware version:

Cisco SPA301G

STEP 1 Quickly press the asterisk (*) button four times to enter the IVR menu.

STEP 2 Enter **150#**. The firmware version is recited.

Cisco SPA501G

STEP 1 Press the **Setup** button. The IVR configuration menu is announced.

STEP 2 Enter **150#**. The firmware version is recited.

Cisco SPA303, Cisco SPA500 Series

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Product Info** and press **Select**. The current firmware is displayed under *Software Version*.

Cisco SPA525G or Cisco SPA525G2

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Status** and press **Select**.

STEP 3 Select **Product Information**. The firmware version is displayed under **Software Version**.

Cisco WIP310

STEP 1 In the **Home** screen, press **Options**, highlight **Phone Info**, and press **Select**.

STEP 2 Scroll to **Software Version**. The firmware is displayed.

Determining the IP Address of the Phone

Before you update the device, you must know the IP address of the phone you are upgrading. Often an IP address is assigned by a DHCP server, so the phone must be booted up and connected to the subnetwork.

To display your IP address:

Cisco SPA301

STEP 1 Quickly press the asterisk (*) button four times to enter the IVR menu.

STEP 2 Enter **110#**. The IP address is recited.

Cisco SPA501G

STEP 1 Press the **Setup** button. The IVR configuration menu is announced.

STEP 2 Enter **110**, then press **#**. The IP address is recited.

Cisco SPA500 Series

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Network** and press **Select**. The IP Address is displayed under Current IP.

Cisco SPA525G or Cisco SPA525G2

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Status** and press **Select**.

STEP 3 Scroll to **Network Status** and press **Select**. The IP address is displayed.

Cisco WIP310

STEP 1 In the Home window, press **Select** and navigate to **Settings**.

STEP 2 Press **Select** and navigate to **Phone Info**.

STEP 3 The **IP Address** field displays the IP address.

Downloading the Firmware

To download firmware from Cisco.com to your PC:

STEP 1 Direct your browser to the URL http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm.

STEP 2 Follow the instructions on the page to locate your product and download the firmware file.

STEP 3 If the firmware file you download is in zip format, double-click the file and extract its contents to a single folder or to the desktop.

Installing the Firmware

Your computer must be on the same subnetwork as the phone you are upgrading.

Cisco SPA300 Series and Cisco SPA500 Series

STEP 1 With your PC attached to the same subnetwork as the phone, run the executable file for the firmware update.

STEP 2 Click **Continue** after reading the message regarding updating and your service provider information.

STEP 3 Enter the IP address of the phone.

STEP 4 Follow the on-screen directions.

Cisco SPA525G or Cisco SPA525G2

STEP 1 Log in to the configuration utility for the phone.

STEP 2 Choose the **Firmware Upgrade** tab.

STEP 3 Click **Firmware Upgrade Window**.

STEP 4 Browse to select the firmware file from your PC. Click **Submit**. The firmware is installed and your phone reboots.

Cisco WIP310

STEP 1 Turn off your Cisco WIP310 and connect it to your computer by using a USB cable.

STEP 2 Double-click the executable file for the firmware upgrade (for example, double-click **wip310-5-0-11.exe**).

STEP 3 Follow the on-screen instructions.

STEP 4 When the upgrade is complete, disconnect the phone from your PC and power it on.

Using the Web-Based Configuration Utility

Your phone system administrator can allow you to view the phone statistics and modify some or all of the parameters by using the phone web user interface. The features of the Cisco SPA phones that can be modified by the user by using the phone web user interfaceare described in this document; however, not all features are available on all phones.

If you are using the Cisco SPA IP phones with the Cisco Unified Communications 500 Series for Small Business for Call Control, use Cisco Unified Communication Manager Express or Cisco Configuration Assistant (CCA) for phone administration. For more information, refer to the *Cisco Unified Communications 500 Office Administrator Guide* or the *Cisco Configuration Assistant Smart Business Communications System Administrator Guide*.

To access the IP phone configuration utility, launch a web browser on a computer that can reach the phone on the subnetwork and enter the IP address of the phone in your web browser address bar. For example, `http://192.168.1.8`. To get the IP address of your phone, see **Determining the IP Address of the Phone**. If you are connected to a VPN, you must first exit the VPN.

NOTE If your service provider disabled access to the configuration utility, you must contact the service provider to proceed.

Allowing Web Access to the IP Phone

To view the phone parameters by using the phone web user interface, the configuration profile must be enabled. To make changes to any of the parameters by using the phone web user interface, the configuration profile must be writable. Your system administrator might have disabled the phone option to make the phone web user interface viewable or writable.

Cisco SPA303, Cisco SPA500 Series

To allow or disallow from the phone viewing of the phone web user interface:

STEP 1 Press the **Setup** button.

STEP 2 To display the Web Server Writable option either:

- Select **Network** > **Enable Web Server**.
- Select **Settings** > **Security Configuration** > **Web Access Enabled**.

STEP 3 Press **Edit** to change the status of the Web Access Enabled parameter.

If the option to edit the parameter is not displayed, press **# to display the option. If the edit option still does not display, it might be set by your phone system administrator such that you cannot modify this parameter.

STEP 4 Press **Y/N** to toggle the parameter and press **ok** to set the parameter.

STEP 5 To save your change, press **save**.

Making the Profile Writeable

On some models you can enable modifying the configuration profile by using the phone web user interface or disable the ability to modify the profile making the phone web user interface read only.

To toggle the write access:

STEP 1 Press the **Setup** button.

STEP 2 To display the Web Server Writable option, select **Settings** > **Security Configuration** > **Web Server Writable**.

STEP 3 To change the status of the Web Server Writable, press **Edit**.

STEP 4 Press **Y/N** to toggle the parameter and press **OK** to set the parameter.

STEP 5 To save your change, press **Save**.

Cisco SPA501G

To allow or disallow from the phone viewing of the phone web user interface by using the IVR:

STEP 1 Press the **Setup** button on the phone. The configuration menu is announced.

STEP 2 In the IVR menu, enter **7932**.

STEP 3 Press **1** to enable the web server, then press **#**.

STEP 4 To save the configuration, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press ***.**

Cisco SPA525G or Cisco SPA525G2

To view the phone parameters by using the phone web user interface, the phone web server must be enabled. Your system administrator might have disabled the phone option to make the phone web user interface viewable or writable.

To allow or disallow from the phone viewing of the phone web user interface:

STEP 1 Press **Setup**.

STEP 2 To display the Web Server Writable option, select **Settings** > **Network Configuration** > **Web Server**.

STEP 3 To change the status of the Web Server parameter, press the **Right Arrow** key to toggle the feature enabled (checked) or disabled (unchecked).

STEP 4 To save your change, press **Set**.

Cisco WIP310

To allow or disallow from the phone viewing of the phone web user interface:

STEP 1 In the **Home** screen, press **Select** to choose **Settings**.

STEP 2 Press **Select** again to reach the **Settings** menu.

STEP 3 Scroll to highlight **Misc Settings** and press **Select** .

STEP 4 Press the left arrow to ensure that **Enable Web Server** is set to **On**.

STEP 5 Press **Select** to save this setting.

Saving the Configuration Profile

Click **Submit All Changes** when you have finished modifying the fields in the phone web user interface to update the configuration profile. The phone is rebooted and the changes are applied.

Click **Undo All Changes** if you want to clear all changes made this session and return to the parameter values set before the session began or since the last time you clicked **Submit All Changes**.

Understanding Administrator and User Views

The Cisco IP phone firmware provides specific privileges for login to a user account and an administrator account. The Administrator account name is **admin**, and the User account name is **user**. These account names cannot be changed. The Admin account is designed to give the service provider or VAR configuration access to the Cisco IP phone, while the User account is designed to give limited and configurable control to the end user of the device.

The User and Admin accounts can be independently password protected. If the service provider set an Administrator account password, you are prompted for it when you click **Admin Login**. If it does not yet exist, the screen is refreshed, displaying the administration parameters. No default passwords are assigned to either the Administrator or the User accounts. Only the Administrator account can assign or change passwords.

The Administrator account can view and modify all web profile parameters, including web parameters available to the user login. The phone system administrator can further restrict the parameters that a User account can view and modify by using a *provisioning profile*.

The configuration parameters available to the User account are configurable in the Cisco IP phone. User access to the Cisco IP phone web user interface can be disabled.

Restricting User Access to the Phone Interface Menus (Cisco SPA300 and Cisco SPA500 Series)

The Admin account can set the phone web user interface to allow or disable access by the User account. Allowing User account access gives a user the option of setting parameters, such as speed dial numbers and caller ID blocking through the phone web user interface.

The ability to configure individual parameters can be restricted by using phone profile provisioning. For more information on provisioning, see the *Cisco Small Business IP Telephony Devices Provisioning Guide* on cisco.com.

To change User account access to the web administration interface, navigate to **Admin Login** > **advanced** > **Voice** > **System.** Under **System Configuration** in the Phone-UI-user-mode field, choose **yes**.

Accessing Administrative Options

To access administrative options, either:

- Log in to the configuration utility, then click **Admin Login**.
- Enter the IP address of the phone in a Web browser and include the **admin/** extension. For example: http://192.168.1.220/admin/

Using the Web Administration Tabs

Each tab contains parameters related to that feature. Some tasks require that you set multiple parameters in different tabs.

Appendix A, "Cisco SPA IP Phone Field Reference," briefly describes each parameter available on the phone web user interface.

Viewing Phone Information

You can check the current status of the Cisco SPA IP phones by clicking the **Info** tab. The Info tab shows information about all phone extensions, including phone statistics and the registration status.

Viewing Reboot Reasons

The phone stores the most recent five reasons the phone was refreshed or rebooted. When the phone is reset to factory defaults, this information is deleted.

The list describes the reboot and refresh reasons (Cisco SPA300 Series and Cisco SPA500 Series IP phones).

Reason	Description
DHCP Failed	The reboot was the result of a DHCP error caused when the lease expired, or when the renewal or verification failed.
Upgrade	The reboot was a result of an upgrade operation (regardless whether the upgrade completed or failed).
Provisioning	The reboot was the result of changes made to parameter values by using the IP phone screen or phone web user interface, or as a result of synchronization.
SIP Triggered	The reboot was triggered by a SIP request.
Link Down	The reboot was triggered when the link to the network went down.
VLAN Changed	The reboot was triggered when the VLAN was changed.
RC	The reboot was triggered as a result of remote customization.
User Triggered	The user manually triggered a warm reboot.
Software Req	The warm reboot was triggered by a remote server.

Reason	Description
System *n*	The reboot was triggered by system events (for example, running out of resources).
IP Changed	The reboot was triggered after the phone IP address was changed.

The following is a list of the supported reboot/refresh reasons (Cisco SPA525G or Cisco SPA525G2):

Reason	Description
Upgrade	The reboot was a result of an upgrade operation (regardless whether the upgrade completed or failed).
Provisioning	The reboot was the result of changes made to parameter values via the IP phone screen or phone web user interface, or as a result of synchronization.
SIP Triggered	The reboot was triggered by a SIP request.
RC	The reboot was triggered as a result of remote customization.
User Triggered	The user manually triggered a warm reboot.
Software Req	The warm reboot was triggered by a remote server.
System *n*	The reboot was triggered by system events (for example, running out of resources).
IP Changed	The reboot was triggered after the phone IP address was changed.

You can view the reboot history from the phone web user interface, the IP phone screen, and the phone SPA Status Dump file (http://*phoneIP*/status.xml or http://*phoneIP*/admin/status.xml).

Viewing the Reboot History on the Phone Web User Interface

The **Info** > **System Information** > **Reboot History** page displays the device reboot history, the five most recent reboot dates and times and a reason for the reboot. Each field displays the reason for the reboot and a time stamp indicating when the reboot took place. For example:

```
Reboot Reason 1: Provisioning(06/22/2011 13:29:33)
Reboot Reason 2: Upgrade(06/22/2011 13:01:43)
Reboot Reason 3: Provisioning(06/22/2011 10:40:12)
```

The reboot history is displayed in reverse chronological order; the reason for the most recent reboot is displayed in **Reboot Reason 1**.

Viewing the Reboot History on the IP Phone Screen

Reboot History is located under the **Setup menu**. On the **Reboot History** Page, the reboot entries are displayed in reverse chronological order, similar to the sequence displayed on the phone web user interface.

Viewing the Reboot History in the SPA Status Dump File

The reboot history is stored in the SPA Status Dump file (http://*<phone_IP_address>*/admin/status.xml). In this file, tags **Reboot_Reason_1** to **Reboot_Reason_5** store the reboot history, as shown in this example:

```
<Reboot_History><Reboot_String/>
<Reboot_Reason_1>Provisioning(06/13/2011 14:03:43)</Reboot_Reason_1>
<Reboot_Reason_2>Provisioning(06/13/2011 13:58:15)</Reboot_Reason_2>
<Reboot_Reason_3>Provisioning(06/13/2011 12:08:58)</Reboot_Reason_3>
<Reboot_Reason_4>Provisioning(05/26/2011 15:26:49)</Reboot_Reason_4>
<Reboot_Reason_5>System 4(05/24/2011 10:20:06)</Reboot_Reason_5>
<Reboot_History/>
```

Using IVR on IP Phones Without Screens

The Cisco SPA301 and Cisco SPA501G provides an IVR menu to perform configuration tasks and obtain information about the phone.

To access the IVR menu:

- **Cisco SPA301**: Press the asterisk (*) four times. Enter the number of the option and press **#**.
- **Cisco SPA501G**: Press **Settings**. Enter the number of the option and press **#**.

Some menus require entering of more information or numbers.

Press **9** on the IVR menu to be guided through a list of commonly used tasks or enter the number of the desired menu to go directly to that feature.

Enter the number of the settings you want to change:

- 1—Network
  - 1—Connection Type—Recites the connection type.
    Press **1** to change the connection type, then press **0** for DHCP or press **1** for static IP.
    To save, press **1**.
    To review, press **2**.
    To reenter, press **3**.
    To exit, press *.
  - 2—IP Address—Recites the IP address
  - 3—Netmask—Recites the network mask.
  - 4—Gateway Address—Recites the gateway IP address.
  - 5—MAC Address—Recites the MAC (hardware) address.
  - 6—DNS—Recites the primary DNS server address.
- 2—Protocol
  - 1—Call Control Protocol—Recites the current call control protocol.
    Press **1** to change, or * to go back.
  - 2—Multicast Address—Recites the multicast address.
    Press **1** to change, or * to go back.
  - 3—CDP—Tells you if CDP is enabled.
    Press **1** to change, or * to go back.
  - 4—SPCP Auto Detection—Indicates that SPCP auto detection is enabled.
    Press **1** to change, or * to go back.
- 3— Other Options
  - 1—Software Version—Recites the software version.
  - 2—Primary Extension—Recites the primary extension.
  - 3—Reboot—Reboots the phone. Hang up to exit.

- 4—Factory Reset—Restores the phone to the factory default software and settings. Enter **1** to confirm or ***** to cancel.
- 5—Debug Server—Recites the address of the debug server. Press **1** to change, or * to go back.

The following table lists the IVR options that you can enter immediately after accessing the IVR system.

Number	Option
100	Indicates that Dynamic Host Configuration Protocol (DHCP) is enabled.
110	Recites the IP address of the phone.
120	Recites the netmask of the phone.
130	Recites the gateway address.
140	Recites the MAC (hardware) address of the phone.
150	Recites the phone software version.
160	Recites the primary DNS server address.
170	Recites the HTTP port on which the web server listens. Defaults to 80.
180	Recites the IP multicast address (used by the Cisco SPA 9000 to communicate with the IP phone).
220	Recites the method of call control (SIP or SPCP).
221	Set call control—enter the value for the call control method and press #: ▪ 0: SIP ▪ 1: SPCP To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press *****.
73738	Restores the phone to the factory default software and settings. Enter **1** to confirm, or ***** to exit. If you chose to reset, hang up to exit and begin the restore process.

Number	Option
87778 (Cisco SPA501G)	Restore the phone user settings to the default. (Clears all user settings such as speed dials.) Enter **1** to confirm, or * to exit. If you chose to reset, hang up to exit and begin the restore process.
732668	Reboot the phone. Enter **#** and hang up to begin rebooting.
111	Set a static IP address. Enter the IP address (use * to enter the decimal (.)), then press #. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press *. **NOTE** DHCP must be disabled to use this option; if DHCP is not disabled, you receive an error message.
121	Set a netmask. Enter the address (use * to enter the decimal (.)), then press #. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press *. **NOTE** DHCP must be disabled to use this option; if DHCP is not disabled, you receive an error message.
131	Set a gateway. Enter the address (use * to enter the decimal (.)), then press #. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press *. **NOTE** DHCP must be disabled to use this option; if DHCP is not disabled, you receive an error message.
161	Set the address of the primary Domain Name Server (DNS). Enter the address (use * to enter the decimal (.)), then press #. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press *.
181	Set the IP multicast address (used by the Cisco SPA 9000 to communicate with the IP phone). Enter the address (use * to enter the decimal (.)), then press #. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press *.
7932	Enable or disable the web-based configuration utility. Press **1** to enable or **0** to disable, then press **#**. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press *.

Number	Option
723646	Enable or disables access to the administrative (admin) login on the configuration utility. Press **1** to enable or **0** to disable, then press **#**. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press ***.**

Ensuring Voice Quality

Voice quality perceived by the subscribers of the IP Telephony service should be indistinguishable from that of a PSTN.

Supported Codecs

The table shows the codecs (voice compression algorithms) supported by Cisco SPA IP phones. The Mean Opinion Score (MOS) measures the voice quality by using a scale of 1–5, where 1 is the lowest quality and 5 is the highest quality.

Codec	Complexity and Description	MOS
G.711 (A-law and u-law)	Very low complexity. Supports uncompressed 64 kbps digitized voice transmission at one to ten 5ms voice frames-per-packet. This codec provides the highest voice quality and uses the most bandwidth of any of the available codecs.	4.5
G.726	Low complexity. Supports compressed 16, 24, 32, or 64 kbps digitized voice transmission at one to ten 10ms voice frames per packet. When no static payload value is assigned per RFC-1890, Cisco SPA IP phones can support dynamic payloads for G.726. G.726 is supported only for 32 kbps on the Cisco SPA525G or Cisco SPA525G2.	4.1 (32 kbps)

Codec	Complexity and Description	MOS
G.729 and G.729A	G.729A low-medium complexity. G.729 medium complexity. G.729A requires about half the processing power of G.729. The G.729 and G.729A bit streams are compatible and interoperable, but not identical.	4
G.723.1	High complexity. Cisco SPA IP phones support the use of ITU G.723.1 audio codec at 6.4 kbps. Up to two channels of G.723.1 can be used simultaneously. For example, Line 1 and Line 2 can use G.723.1 simultaneously, or Line 1 or Line 2 can initiate a three-way conference with both call legs using G.723.1. G.723.1 is not supported on the Cisco SPA525G or Cisco SPA525G2 or Cisco WIP310 phones.	3.8
G.722	Only one G.722 call at a time is allowed. If a conference call is placed, a SIP re-invite message is sent to switch the calls to narrowband audio. Not supported on the Cisco WIP310.	4.3 (approx)

Bandwidth Requirements

Depending on how you have your IP phones configured, each call requires 55 to 110 kbps of the bandwidth in each direction. For example, using G.729 with an average business-grade broadband Internet connection supporting 1.5 Mbps downstream and 384 kbps upstream, a total of seven (7) simultaneous conversations can be reliably supported with adequate bandwidth available for file downloads.

We recommend using Cisco SPA IP phones with QoS-capable networking equipment that can prioritize the VoIP traffic. A QoS-enabled device prioritizes the packets going upstream to the ISP.

The table approximates the bandwidth budget for each side of the conversation (in each direction) using different codecs and the number of calls the network might support. The table is based on the following assumptions:

- Bandwidth calculated with no silence suppression, as the use of silence suppression can reduce the average bandwidth budget by 30 percent or more.
- 20 millisecond of payload per RTP packet

Codec	Estimated Bandwidth	2 Calls	4 Calls	6 Calls	8 Calls
G.711	110 kbps	220 kbps	440 kbps	660 kbps	880 kbps
G.722	110 kbps	220 kbps	440 kbps	660 kbps	880 kbps
G.726-40	87 kbps	174 kbps	348 kbps	522 kbps	696 kbps
G.726-32	79 kbps	158 kbps	316 kbps	474 kbps	632 kbps
G.726-24	71 kbps	142 kbps	284 kbps	426 kbps	568 kbps
G.726-16	63 kbps	126 kbps	252 kbps	378 kbps	504 kbps
G.729	55 kbps	110 kbps	220 kbps	330 kbps	440 kbps

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

http://www.erlang.com/calculator/lipb/

http://www.packetizer.com/voip/diagnostics/bandcalc.html

Factors Affecting Voice Quality

The following factors contribute to voice quality:

- Audio compression algorithm—Speech signals are sampled, quantized, and compressed before they are packetized and transmitted to the other end. For IP Telephony, speech signals are usually sampled at 8000 samples per second with 12–16 bits per sample. The compression algorithm plays a large role in determining the voice quality of the reconstructed speech signal at the other end. Cisco SPA IP phones support popular audio compression algorithms for IP Telephony: G.711 a-law and u-law, G.726, G.729a, G.722 (not supported on Cisco WIP310) and G.723.1. (not supported on the Cisco SPA525G or Cisco SPA525G2 or Cisco WIP310.)

- The encoder and decoder pair in a compression algorithm is known as a codec. The compression ratio of a codec is expressed in terms of the bit rate of the compressed speech. The lower the bit rate, the smaller the bandwidth required to transmit the audio packets. Although voice quality is usually lower with a lower bit rate, it is usually higher as the complexity of the codec gets higher at the same bit rate.
- Silence suppression—Cisco SPA IP phones apply *silence suppression* so that silence packets are not sent to the other end to conserve more transmission bandwidth. IP bandwidth is used only when someone is speaking. Voice activity detection (VAD) with silence suppression is a means of increasing the number of calls supported by the network by reducing the required bidirectional bandwidth for a single call. A noise level measurement is sent periodically during silence suppressed intervals so that the other end can generate artificial comfort noise by using a comfort noise generator (CNG).
- Packet loss—Audio packets are transported by UDP. Packets might be lost or contain errors that can lead to audio sample drop-outs and distortions and lower the perceived voice quality. The Cisco SPA IP phones apply an error concealment algorithm to alleviate the effect of packet loss.
- Network jitter—The IP network can induce varying delays of received packets. The RTP receiver in Cisco SPA IP phones keep a reserve of samples to absorb the network jitter, instead of playing out all the samples as soon as they arrive. This reserve is known as a jitter buffer. The bigger the jitter buffer, the more jitter it can absorb, but this also introduces bigger delay.
  - Jitter buffer size should be kept to a relatively small size whenever possible. If jitter buffer size is too small, many late packets might be considered lost and thus lower the voice quality. Cisco SPA IP phones dynamically adjust the size of the jitter buffer according to the network conditions that exist during a call.
  - The minimum jitter buffer size is 30 ms or 10 ms plus the current RTP frame size, whichever is larger, for all jitter level settings. However, the starting jitter buffer size value is larger for higher jitter levels. This setting controls the rate at which the jitter buffer size is adjusted to reach the minimum.
  - Jitter Buffer Adjustment—Controls how the jitter buffer should be adjusted.

- Echo—Impedance mismatch between the telephone and the IP telephony gateway phone port can lead to near-end echo. Cisco SPA IP phones have a near-end echo canceller with at least 8 ms tail length to compensate for impedance mismatch. Cisco SPA IP phones implement an echo suppressor with CNG so that any residual echo is not noticeable.
- Hardware noise—Certain levels of noise can be coupled into the conversational audio signals because of the hardware design. The source can be ambient noise or 60 Hz noise from the power adaptor. The Cisco hardware design minimizes noise coupling.
- End-to-end delay—End-to-end delay does not affect voice quality directly, but is an important factor in determining whether IP phone subscribers can interact normally in a conversation. A reasonable delay should be 50 to 100 ms. End-to-end delay larger than 300 ms is unacceptable to most callers. Cisco SPA IP phones support end-to-end delays well within acceptable thresholds.
- Adjustable Audio Frames Per Packet—Allows you to set the number of audio frames contained in one RTP packet. Packets can be adjusted to contain from 1–10 audio frames. Increasing the number of frames decreases the bandwidth utilized, but it also increases delay and can affect voice quality.

SIP Publish Signaling Improvements

The Cisco SPA IP phones resend the SIP PUBLISH messages with the voice quality report once per 5xx response with a valid Retry-After header.

A valid time value in seconds is a positive integer from 0 to 65536. A SIP message with a Retry-After time value of 0 is treated as a `500 Server Internal Error` message. A time value less than 0 is ignored.

The following is a summary of the 5xx messages with Retry-After header that the phone supports:

5xx SIP Response	Description
500 Server Internal Error	An unexpected server condition prevents the fulfillment of request.
503 Service Unavailable	The server is unavailable due to a temporary overload or maintenance.

2

Configuring Lines

The Cisco SPA IP phones provide different numbers of lines depending on the phone model. Each line corresponds to a phone number (or extension) used for calls. Each line can support two calls. For example, a four-line phone can handle eight calls. One call can be active (in conversation) and seven can be on hold.

This chapter contains the following sections:

- **Configuring a Line Key**
- **Assigning Busy Lamp Field, Call Pickup, or Speed Dial Functions to Unused Lines**
- **Configuring Audio Indication for Call Pickup Event**

Configuring a Line Key

Each line key can be assigned multiple extensions, a short name, and share call appearance. The number of line keys depends on the model of the IP phone (does not apply to the Cisco WIP310). Generally you should reserve **Line Key 1** on the IP phone as the primary and private extension of the designated user.

To configure a phone line:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

STEP 2 Under each line key for the phone, configure the following:

- Extension—Assign an extension number to the line key. Defaults to 1.
- Short Name—Enter a short name or a number to display on the IP phone screen.
- Share Call Appearance—Select **shared** to share incoming call appearances with other phones. See **Configuring Shared–Line Appearance**. If you select **private**, the call appearance is not shared with any other phone. Defaults to private.
- Extended Function—See **Assigning Busy Lamp Field, Call Pickup, or Speed Dial Functions to Unused Lines**.

STEP 3 Click **Submit All Changes**.

Configuring Shared–Line Appearance

You create a shared-line appearance by assigning the same directory number to different devices. A Cisco system considers a directory number to be a shared line if it appears on more than one device. In a shared-call appearance, for example, you can set up a shared line, so a directory number appears on line 1 of a manager phone and on line 2 of an assistant phone. Another example of a shared line involves a single incoming 800 number that is set up to appear as line 2 on every sales representative phone in an office.

Most devices with a shared-line appearance can make or receive new calls or resume held calls at the same time. Incoming calls display on all devices that share a line, and anyone can answer the call. Only one call remains active at a time on a device.

Call information (such as calling party or called party) displays on all devices that are sharing a line. If one of the devices turns on the Privacy feature, other devices that share the line will not see outbound calls that are made from the device that turned on privacy. All devices will still see inbound calls to the shared line.

Devices with shared-call appearances can initiate independent transfer or conference transactions.

When a call is made to the extension number for the shared-call, all sharing Cisco SPA IP phones ring. Any IP phone can answer the call. If the active phone places the shared call on hold, the call can be resumed from any of the sharing Cisco SPA IP phones by pressing the corresponding line key (except for the Cisco SPA502G) or the **Select** button when the **Resume** icon is displayed (Cisco WIP310).

The Cisco SPA300 Series and Cisco SPA500 Series IP phones support the *private hold* feature for MetaSwitch and BroadSoft. Users who have a shared line can press **PrivHold**, and the call can only be resumed by the user who placed the call on hold.

Each IP phone can be configured independently. Although the account information is usually the same for all of the Cisco SPA IP phones, settings such as the dial plan or the preferred codec can vary between phones and continue to support shared-line appearance.

To configure the line:

STEP 1 Click **Admin Login** > **advanced** > **Voice**.

STEP 2 Click the **Ext_n** tab of the extension that is shared (do not use Ext 1).

STEP 3 Under **General** in the Line Enable list, choose **yes**.

STEP 4 Under **Share Line Appearance** in the Share Ext list, select **shared**. If you set this extension to **private** (not shared), the extension does not share calls, regardless of the **Share Call Appearance** setting on the **Phone** tab. If you set this extension to **shared**, calls follow the **Share Call Appearance** setting on the **Phone** tab. On the Cisco SPA500 Series phones that have line buttons, a hollow telephone icon is displayed next to the shared line button. For the Cisco SPA525G or Cisco SPA525G2, a telephone icon is displayed.

STEP 5 In the Shared User ID field, enter the user ID (name) of the phone with the extension that is being shared.

STEP 6 In the Subscription Expires field, enter the number of seconds before the SIP subscription expires. Until the subscription expires, the phone gets NOTIFY messages from the SIP server on the status of the shared phone extension. The default is 60 seconds.

STEP 7 In the **Restrict MWI** (message waiting indicator) field, choose **yes** to set the message waiting indicator to light only for messages on private lines (SIP). Choose **no** to set the message waiting indicator to light for all messages.

STEP 8 Under **Proxy and Registration**, in the **Proxy** field, enter the IP address of the proxy server (for example, the IP address of the Cisco SPA9000).

STEP 9 Under **Subscriber Information**, enter a **Display Name** and **User ID** (extension number) for the shared extension. These are shown on the IP phone screen.

STEP 10 (Optional) In the **Phone** tab, under **Miscellaneous Line Key Settings**, configure line mapping. Each LED (line/extension) can hold two calls. You can assign an extension to two LEDs. The first call always causes the assigned LED to flash. Choose one of the following:

- Vertical first—The next LED on the phone flashes with the second incoming call.
- Horizontal first—The same LED to flashes with the second incoming call.

STEP 11 (Optional) In the **Phone** tab, under **Miscellaneous Line Key Settings**, configure **SCA Barge-In Enable**. Choose **yes** to allow users sharing call appearances to take over the call on a shared line. Choose **no** to prevent users from taking over the call on a shared line.

For example, Bob and Chris share the extension 401. Adam, calls extension 401. Bob answers the call. Adam and Bob are connected. If Chris has the SCA Barge-In Enable field on her phone set to **yes**, she can press the line button for extension 401. Chris and Adam are connected in a call and Bob is dropped from the call.

The Cisco SPA525G or Cisco SPA525G2 support the *private hold* feature for MetaSwitch and Broadsoft. Users who have a shared line can press **PrivHold**, and the call can only be resumed by the user who placed the call on hold; no barge-in can be performed on these calls.

STEP 12 Click **Submit All Changes**.

Configuring Call Appearance Per Line

In the **Phone** tab, **Call Appearance Per Line** (under **Miscellaneous Line Key Settings**) lets you choose the number of calls per line button. The default value is **2**.

This option is not supported on the Cisco SPA501G and Cisco SPA301 phones. Also, this feature is only supported when the phones are operating in SIP mode.

When you increase the number of calls per line to a value greater than 2, you *must* set the following:

- **Line ID Mapping** (under **Miscellaneous Line Key Settings**) to **Horizontal First**.
- **Line Navigation** (under **Miscellaneous Line Key Settings**) to **Per Call**.
- **Programmable Softkey Enable** (under **Programmable Softkeys**) to **Yes**.

When the maximum numbers of calls per phone is reached, the phone does not allow you to make a new call and rejects incoming calls. Table 1 lists the maximum number of calls per phone for each model.

Table 1 Maximum Number of Allowed Calls Per Phone

Phone	Maximum Number of Calls
Cisco SPA303, SPA502G, SPA504G	10
Cisco_SPA508G	16
Cisco SPA509G	24
Cisco SPA512G and Cisco SPA514G	10
Cisco SPA525G or Cisco SPA525G2	10

Expand Call Appearance Per Line

To expand the call appearances per line:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone.**

STEP 2 In the **Miscellaneous Line Key Settings** section in the Call Appearance Per Line field, choose how many calls per line to allow from the drop-down.

Configuring Unused Line Keys to Access Services

On the Cisco SPA300 Series and Cisco SPA500 Series IP phones, unused or idle phone lines can also be configured to access services, such as:

- XML services
- MP3 player (Cisco SPA525G or Cisco SPA525G2)
- Weather (RSS)
- News (RSS)

To configure line keys to access services:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**

STEP 2 In the Line Key to configure (line 4 in this example):

a. From the **Extension** drop down list, choose **Disabled.**

b. Enter the following string in the Extended Function field:

```
fnc=type
```

where:

- fnc: function

- type:
  - xml: pressing the line button accesses XML services. The XML service configured on the Phone tab under the launches the page identified in the XML Service field (see **Configuring XML Services**). You can specify a different XML service to connect to by using the syntax `fnc=xml;URL=http://xxx.xx.xxx/entry.html` where `xxx.xx.xxx` is the URL of the XML service.
  - mp3: pressing the line button starts the mp3 player.
  - weather: pressing the line button accesses weather information.
  - news: pressing the line button accesses news.

For example, to configure line 4 for the mp3 player:

```
fnc=mp3
```

STEP 3 Click **Submit All Changes**. After the phone reboots, configured lines glow orange and display the following icons next to the extension label:

- xml: XML icon
- mp3: mp3 player icon (Cisco SPA525G or Cisco SPA525G2)
- news: RSS icon
- weather: thermometer icon

Configuring Call Park on the Cisco SPA525G or Cisco SPA525G2 (MetaSwitch)

Unused line keys can be enabled to allow call park (for the MetaSwitch soft switch) on the Cisco SPA525G or Cisco SPA525G2. Users can press this line button to park a call or retrieve a parked call.

To configure unused line keys for call park and retrieval:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Att(endant) Console**.

STEP 2 In the **General** section under Server Type, choose **RFC3265_4236**.

STEP 3 Click the **Phone** tab.

STEP 4 Choose the line key to configure (line 5 in this example):

a. From the **Extension** drop down list, choose **Disabled**.

b. From the **Share Call Appearance** drop-down list, choose **private**.

c. Enter the following string in the Extended Function field:

```
fnc=prk;sub=05@domain.com
```

where:

- fnc: function
- prk: call park
- sub: call park orbit, or location where the call is parked. Valid value range is from **01** through **10**. In this example, 5 is used.
- domain.com: phone domain, usually the same as the *proxy* value in the Ext 1 tab. You can also use fnc=prk;sub=05@$PROXY to set this value.

STEP 5 Click **Submit All Changes**.

Assigning Busy Lamp Field, Call Pickup, or Speed Dial Functions to Unused Lines

You can configure unused or idle lines on a Cisco SPA300 Series or Cisco SPA500 Series IP phones to interact with another line in the system. For example, if you have two idle lines on an assistant's phone, you can configure those lines to show the status of a supervisor's phone (Busy Lamp Field [BLF]). You can also configure the idle lines so that they can be used to speed dial the supervisor's phone, or pick up calls that are ringing on the supervisor's phone.

A monitored extension must be private, not shared. Additionally, if using the Cisco SPA9000 for call control, an extension can only be monitored by one other extension.

For detailed instructions on configuring the phones with the BroadSoft Busy Lamp Field (BLF) feature, see *Configuring SPA303 and 5xxG IP Phones with Broadsoft's BLF*, available on the Cisco Support Community at https://supportforums.cisco.com/docs/DOC-9977

Configuring Call Pickup and Busy Lamp Field

You must enable BLF to configure call pickup.

In this example, the assistant Bob (extension 200) has an idle line (line 4) on his Cisco SPA508G. He would like to be able to see if his supervisor Stephanie (extension 300) is on the phone, and pick up calls that are ringing at her extension.

To configure this feature for Bob:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone.**

STEP 2 In the Line Key to configure (line 4 in this example):

a. From the **Extension** drop down list, choose **Disabled**.

b. From the Share Call Appearance drop-down list, choose **private.**

c. Enter the following string in the Extended Function field:

```
fnc=blf+cp;sub=Stephanie@$PROXY;ext=300@$PROXY
```

Using the following syntax:

```
fnc=type;sub=stationname@$PROXY;ext=extension#@$PROXY
```

where:

- fnc: function
- blf: busy lamp field
- cp: call pickup
- sub: station name
- ext or usr: extension or user (the **usr** and **ext** keywords are interchangeable)

STEP 3 Click **Submit All Changes.** After the phone reboots, the phone in this example displays the following color LEDs for the monitored lines:

- Green: Available
- Red: Busy
- Red Fast Blink: Ringing

If the phone LEDs display orange or slow blinking orange, there is a problem: Orange indicates that the phone failed to subscribe (received a 4xx response) and slow-blinking orange denotes an undefined problem (there might be no response to the subscribe request, or the BLF).

When the phone is successfully configured, Bob can monitor Stephanie's line. When a call is ringing at Stephanie's line, he can press line button 4 to pick it up.

Configuring Speed Dial

In this example, the assistant, Bob (extension 200), has another idle line (line 5) on his Cisco SPA508G. He wants to speed dial his supervisor Mark (extension 400) from that line.

To configure this feature for Bob:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone.**

STEP 2 In the Line Key to configure (line 5 in this example):

a. From the **Extension** drop down list, choose **Disabled**.

b. From the Share Call Appearance drop-down list, choose **private**.

c. Enter the following string in the Extended Function field:

```
fnc=sd;ext=400@$PROXY
```

Using the following syntax:

```
fnc=type;ext=extension#@$PROXY
```

where:

- fnc: function
- sd: speed dial
- ext or usr: extension or user (the **usr** and **ext** keywords are interchangeable)

STEP 3 Click **Submit All Changes.**

When the phone is successfully configured, Bob can press line button 5 to dial Mark's line.

Configuring Audio Indication for Call Pickup Event

You can configure the phone to play the Call Pickup tone when there are incoming calls to any of the lines that the user is monitoring with the Call Pickup function.

To configure Audio Indication:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Att(endant) Console**.

STEP 2 In the **General** section under Call Pickup Audio Notification, select **Yes**,

To configure this parameter by using the configuration file, configure the following line to the profile:

```
<Call_Pickup_Audio_Notification ua="na">Yes
</Call_Pickup_Audio_Notification>
```

STEP 3 Click the **Regional** tab.

STEP 4 In the **Call Progress Tones** section under the **Call Pickup Tone** parameter.

The default value is `440@-10;30(.3/9.7/1)`, same as the call waiting tone.

To configure this parameter by using the configuration file, configure the following line the profile:

```
<Call_Pickup_Tone ua="na">440@-10;30(.3/9.7/1)</Call_Pickup_Tone>
```

STEP 5 Click **Submit All Changes**.

3

Customizing Standard Features

This chapter describes customizing the Cisco SPA IP phones and contains the following sections:

- Configuring Phone Information and Display Settings
- Configuring Linksys Key System Parameters
- Enabling Call Features
- Customizing Phone Softkeys
- Configuring the Message Waiting Indicator
- Configuring Ring Tones
- Configuring RSS Newsfeeds (Cisco SPA525G or Cisco SPA525G2)
- Configuring Audio Settings
- Enabling Wireless (Cisco SPA525G or Cisco SPA525G2 only)
- Configuring Bluetooth (Cisco SPA525G or Cisco SPA525G2 only)
- Enabling SMS Messaging
- Enabling and Configuring the Phone Web Server
- Configuring LDAP for the Cisco SPA300 Series and Cisco SPA500 Series IP Phones
- Configuring BroadSoft Settings (Cisco SPA300 Series and Cisco SPA500 Series)
- Configuring XML Services
- Configuring Music On Hold
- Configuring Extension Mobility
- Configuring Video Surveillance (Cisco SPA525G or Cisco SPA525G2)

Configuring Phone Information and Display Settings

The phone web user interface allows you to customize settings such as the phone name, background photo, logo, and screen saver.

Configuring the Phone Name

Navigate to **Admin Login** > **advanced** > **Voice** > **Phone.**

Under **General**, enter the Station Name for the phone. This name displays in the corporate directory.

Configuring Voice Mail

This configures the internal or external phone number or URL for the the voice mail system. If you are using an external voice-mail service, the number must include any digits required to dial out and any required area code.

To configure the phone to connect to voice mail:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**

STEP 2 Under **General**, enter the Voice Mail Number.

STEP 3 (Optional) Enter the Voice Mail Subscribe Interval; the expiration time in seconds, of a subscription to a voice mail server.

STEP 4 Click **Submit All Changes**. The phone reboots.

Configuring Internal Voice Mail for Each Extension (Using a Cisco SPA400)

To configure internal voice mail, navigate to **Admin Login** > **advanced** > **Voice** > **Ext** n. Under **Call Feature Settings**, enter the voice mail line number and phone extension in the Mailbox ID field. For example, 2101 indicates that the Cisco SPA400 voice mail server is configured on the Cisco SPA9000 Line 2, phone extension 101.

Customizing the Startup Screen

You can create a text or 128-by-48 pixel by 1-bit deep image logo to display when the IP phone boots up. (Not applicable to Cisco WIP310 or the Cisco SPA501G.) A logo displays during the boot sequence for a short period after the Cisco logo displays.

To configure a custom logo:

STEP 1 For the Cisco SPA303 and Cisco SPA5XXG, click **Admin Login** > **advanced** > **Voice** > **Phone.**

For the Cisco SPA525G or Cisco SPA525G2, click **Admin Login** > **advanced** > **Voice** > **User.**

STEP 2 To display a text logo, in the Text Logo field enter text as follows:

- Up to two lines of text
- Each line must be less than 32 characters
- Insert a new line character (\n) and escape code (%0a) between the two lines

  For example, `Super\n%0aTelecom` displays:

  ```
  Super
  Telecom
  ```

- Use the **+** character to add spaces for formatting. You can add multiple **+** characters before and after the text to center it.

STEP 3 To display a picture logo:

a. In the BMP Picture Download URL field, enter the path, for example:

   `http://192.168.2.244/pictures/image04_128x48.bmp`
   (you can also use a TFTP server)

b. Change **Select Logo** to **BMP Picture.**

STEP 4 Click **Submit All Changes.** The phone reboots, retrieves the .bmp file, and displays the picture when it next boots.

Changing the Display Background

You can use a picture to customize the background on your IP phone screen. (Not applicable to Cisco WIP310 or the Cisco SPA501G.) Phone models and acceptable image file types are:

- Cisco SPA303 and Cisco SPA500 Series: Bitmap format, 1 bit-per-pixel color, size 128-by-48 pixels.
- Cisco SPA525G or Cisco SPA525G2: Either .jpg format (recommended) or bitmap (1, 2, 4, 8, or 24 bits-per-pixel). Recommended image size is 320-by-240 pixels. Other image sizes are scaled to fit, which can cause distortion.

When the *BMP Picture Download URL* is changed, the phone compares the URL to the previous image URL. (If the URLs are the same, the phone does not perform the download.) If the URLs are different, the phone downloads the new image and displays it (providing the *Select Background Picture* field is set to **BMP Picture)**.

The phone does not reboot after you change the background image URL.

Cisco SPA303 and Cisco SPA500 Series

A background image is displayed while the phone is running. To display a logo during the phone boot sequence.

STEP 1 Copy the image to a TFTP or HTTP server that is accessible from the phone.

STEP 2 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

STEP 3 Select the background picture in the Select Background Picture menu:

- None–Does not display a background picture.
- BMP Picture–Displays the **BMP Picture Download URL** picture.
- Text Logo–Displays the text string in the Text Logo field.

STEP 4 If you selected None, in **STEP 3**, go to **STEP 6**. If you selected **Text Logo** in **STEP 3**, go to Otherwise, enter the URL of the image file you want in **BMP Picture Download URL**. The URL must include the TFTP or HTTP server name (or IP address), directory, and filename, for example:

`tftp://myserver.mydomain.com/images/downloadablepicture.bmp`

or

`http://myserver.mydomain.com/images/downloadablepicture.bmp`

If the HTTP Refresh Timer is set in the server response to **BMP Picture Download URL**, the phone downloads the picture from the link and displays it on the IP phone screen. The phone automatically retrieves the picture after the specified number of seconds.

STEP 5 If you selected **Text Logo**, enter a text string in the Text Logo field.

STEP 6 Click **Submit All Changes**.

Cisco SPA525G or Cisco SPA525G2

STEP 1 Copy the image to an HTTP server that is accessible from the phone. (TFTP is not supported.)

STEP 2 Click **Admin Login** > **advanced** > **User**.

STEP 3 In the Screen section, Background Picture Type field, select **Download BMP Picture**.

STEP 4 Enter the URL of the .bmp file you want in the *BMP Picture Download URL* field. The URL must include the HTTP server name (or IP address), directory, and filename, for example:

`http://myserver.mydomain.com/images/downloadablepicture.jpg`

If the HTTP Refresh Timer is set in the server response to **BMP Picture Download URL**, the phone downloads the picture from the link and displays it on the IP phone screen. The phone automatically retrieves the picture after the specified number of seconds.

STEP 5 Click **Submit All Changes**.

Configuring the Screen Saver

You can configure a screen saver for the Cisco SPA300 Series and Cisco SPA500 Series IP phones. (Not applicable to Cisco WIP310 or the Cisco SPA501G.) When the phone is idle for a specified time, it enters screen saver mode. (Users can set up screen savers directly by using phone **Setup** button.)

Any button press or on/off hook event triggers the phone to return to normal mode. If a user password is set, the user must enter it to exit screen saver mode.

To configure the screen saver:

Cisco SPA303 or Cisco SPA5XXG

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

STEP 2 In the **General** section, in the Screen Saver Enable field, choose **yes** to enable.

STEP 3 In the **Screen Saver Wait** field, enter the number of seconds of idle time to elapse before the screen saver starts.

STEP 4 In the **Screen Saver Icon** field, choose the display type:

- A background picture.
- The station time in the middle of the IP phone screen.
- A moving padlock icon. When the phone is locked, the status line displays a scrolling message “Press any key to unlock your phone.”
- A moving phone icon.
- The station date and time in the middle of the IP phone screen.
- A blank *power save* screen.”

STEP 5 Click **Submit All Changes**.

Cisco SPA525G or Cisco SPA525G2:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **User**.

STEP 2 Under **Screen**, in the Screen Saver Enable field, choose **yes** to enable.

STEP 3 In the **Screen Saver Type** field, choose the display type:

- **Black Background**—Displays a black screen.
- **Gray Background**—Displays a gray screen.
- **Black/Gray Rotation**—The screen incrementally cycles from black to gray.
- **Picture Rotation**—The screen rotates through available pictures on the phone.
- **Digital Frame**—Shows the background picture.

STEP 4 In the **Screen Saver Trigger Time** field, enter the number of seconds that the phone remains idle before the screen saver turns on.

STEP 5 In the **Screen Saver Refresh Time** field, enter the number of seconds before the screen saver should refresh (if, for example, you chose a rotation of pictures).

STEP 6 Click **Submit All Changes**.

Configuring the LCD Contrast

You can configure the LCD contrast on the Cisco SPA300 Series and Cisco SPA500 Series IP phones. (Not applicable to the Cisco WIP310.)

To configure the contrast for the IP phone screen on the phone:

Cisco SPA303 and Cisco SPA5XXG

STEP 1 Click **Admin Login** > **advanced** > **User**.

STEP 2 Under **LCD**, in the LCD Contrast field, enter a number value from 1 to 30. The higher the number, the greater the contrast on the IP phone screen.

STEP 3 Click **Submit All Changes**.

Cisco SPA525G or Cisco SPA525G2:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **User**.

STEP 2 Under **Screen**, in the **LCD Contrast** field, enter a number value from 1 to 30. The higher the number, the greater the contrast on the IP phone screen.

STEP 3 Click **Submit All Changes**.

Configuring Back Light Settings (Cisco SPA525G or Cisco SPA525G2)

To configure the back light settings for the IP phone screen on the phone:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **User**.

STEP 2 Under **Screen** in the Back Light Enable field, choose **yes** to enable the screen back light.

STEP 3 In the **Back Light Timer** field, enter the number of seconds of idle time that can elapse before the back light turns off.

STEP 4 Click **Submit All Changes**.

Configuring Linksys Key System Parameters

To configure the phone as part of a Linksys Key System (for use with the Cisco SPA9000):

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **SIP**.

STEP 2 Under **Linksys Key System Parameters**, configure the following fields:

- **Linksys Key System**—Enables or disables the Linksys Key System for use with the Cisco SPA9000. Defaults to yes. See the *Cisco SPA9000 System Administration Guide* for more details.
- **Multicast Address**—Used by the Cisco SPA9000 to communicate with Cisco SPA IP phones. Defaults to 224.168.168.168:6061. (The Cisco SPA501G, can be configured by using the IVR. See the **"Using IVR on IP Phones Without Screens" section on page 27**.)
- **Key System Auto Discovery**—Enables or disables auto discovery of the call control server (for example, the Cisco SPA9000). Disable this feature for teleworkers or other scenarios where multicast does not work.
- **Key System IP Address**—IP address of the call control server IP. Enter the IP address for teleworkers or other scenarios where multicast does not work.
- **Force LAN Codec**—Used with the Cisco SPA9000. Choices are **none**, **G.711u**, or **G.711a**. Defaults to none.

STEP 3 Click **Submit All Changes**.

Enabling Call Features

This section describes how to enable and disable call features on the phone.

Enabling Anonymous Call and Caller ID Blocking Services

To enable Anonymous Call and Caller ID Blocking navigate to **Admin Login** > **advanced** > **Voice** > **User**. Under **Supplementary Services** under the type of call blocking, choose **yes** to enable or **no** to disable:

- **Block ANC Serv**—Blocks anonymous calls.
- **Block CID Serv**—Blocks outbound caller ID.

Enabling ACD Service

Typically used for call centers, Automatic Call Distribution (ACD) handles incoming calls and manages them based on a database of instructions. You can enable this with the SIP B parameter (**"Configuring SIP" section on page 103**).

To enable ACD

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **User**.

STEP 2 Under **Supplementary Services** from the ACD Login Serv list, choose **yes** to enable. (Defaults to no (disabled).)

STEP 3 In the **ACD Ext** field, choose the extension used for handling ACD calls. Select 1-6 (depending on your phone model). Defaults to 1.

STEP 4 Click **Submit All Changes**.

Enabling Call Back Service

Call back forces the phone to repeatedly try a number that received a busy response. The busy number is tried until the call goes through and the target phone rings.

To enable call back service, navigate to **Admin Login** > **advanced** > **Voice** > **Phone**. Under **Supplementary Services** in the Call Back Serv field, choose **yes** to enable.

Enabling Call Park and Call Pickup Services

Call park allows users to put a call on a line and make it available for another user to pick up. Call pickup allows a user to pick up a phone that is ringing at another user phone. Call park and call pickup are available on IP phones when used with a Cisco SPA9000 system.

To enable call park and call pickup, navigate to **Admin Login** > **advanced** > **Voice** > **Phone**. Under **Supplementary Services**, under the type of call feature to enable, choose **yes** to enable or **no** to disable:

- **Call Park Serv**—Enables call parking.
- **Call Pickup Serv**—Enables call pickup.

Enabling Call Transfer and Call Forwarding Services

You can transfer or forward a call when the service is enabled.

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

STEP 2 Under **Supplementary Services**, under the transfer type you want to enable, choose **yes**:

- **Attn Transfer Serv**—Attended call transfer service. The user answers the call before transferring it.
- **Blind Transfer Serv**—Blind call transfer service. The user transfers the call without speaking to the caller.

You can also enable or disable call forwarding:

- **Cfwd All**—Forwards all calls.
- **Cfwd Busy**—Forwards calls only if the line is busy.
- **Cfwd No Ans**—Forwards calls only if the line is not answered.

STEP 3 Click **Submit All Changes**.

Enabling Conferencing

To allow the user to perform call conferencing, navigate to **Admin Login** > **advanced** > **Voice** > **Phone**. Under **Supplementary Services** in the Conference Serv field, choose **yes** to enable.

Enabling Do Not Disturb

You can allow users to turn the Do Not Disturb feature on or off. This feature directs all incoming calls to voice mail or, if voice mail is not configured, plays a message to the caller saying the user is unavailable. On the Cisco SPA300 Series and Cisco SPA500 Series IP phones, users can press the **Ignore** softkey to divert a ringing call to another destination.

To allow users to use Do Not Disturb (enabled by default), navigate to **Admin Login** > **advanced** > **Voice** > **Phone**. Under **Supplementary Services** under DND Serv, choose **yes** to enable. (This feature can also be configured from the **User** tab, under **Supplementary Services**.)

Enabling the Missed Call Shortcut

The IP phones can display a notification that a call has been missed. (Not applicable to Cisco WIP310.) To enable this notification, navigate to **Admin Login** > **advanced** > **Voice** > **User**. Under **Supplementary Services** in the Miss Call Shortcut list, choose **yes** to enable.

Logging Missed Calls

You can disable or enable missed call logging per extension. For example, if you have set up a line to monitor another user line, you can disable missed call logging for the monitored line.

To enable logging, navigate to **Admin Login** > **advanced** > **Voice** > **User**. Under **Supplementary Services** in the Log Missed Calls for Ext <nu*mber*> field, choose **yes** to enable.

Enabling Paging (Intercom)

The paging, or intercom feature, allows two types of paging, single page and group paging. When paging occurs, the speaker on the paged IP phone is automatically activated unless the handset or headset is being used.

A user can directly contact another user by phone. If the person being paged has configured their phone to automatically accept pages, the phone does not ring; a direct connection between the two phones is automatically established when paging is initiated.

Group Paging lets the user page all the client Cisco SPA IP phones at once, or *page groups* of phones. If the client phone is on an active call while a group page starts, the incoming page is ignored. Group page is one-way; the paged client IP phones can only listen to the call from the originator.

To enable paging, navigate to **Admin Login** > **advanced** > **Voice** > **Phone**. Under **Supplementary Services** in the Paging Serv list, choose **yes** to enable.

To configure a phone to automatically accept pages, navigate to **Admin Login** > **advanced** > **Voice** > **User**. Under **Supplementary Services** in the **Auto Answer Page** list, choose **yes** to enable.

Configuring Paging Groups

You can configure a phone to be a member of a paging group. Users can then direct pages to specific groups of phones.

Limitations:

- A phone can be a listening member of no more than two paging groups.
- No more than five paging groups can be configured on a phone.

To configure a phone as part of a paging group:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

STEP 2 Under **Multiple Paging Group Parameters**, enter the paging commands into the **Group Paging Script** field. The syntax is as follows:

```
pggrp=ip-address:port;[name=xxx;]num=xxx;[listen={yes|no}]];
```

Where:

- IP address: Multicast IP address of the phone that listens for and receives pages.
- port: Port on which to page; use different ports for each paging group. All phones in the same paging group must use the same port number.
- name (optional): The name of the paging group. In this name, do not use the `pggrp` string because it is reserved. Using it causes the script not to work, as in these examples:

  ```
  pggrp=224.168.168.168:3141;name=ITGPgGrp;num=800;listen=yes;
  ```

  ```
  pggrp=224.168.168.168:3141;name=PgGrp;num=800;listen=yes;
  ```

- num: The number users will dial to access the paging group; must be unique to the group.
- listen: If the phone being configured is a listening member of the page group. A phone can be a listening member of a maximum of two groups. If no value is entered, the default is to **not listen** as a member of this group.

STEP 3 Click **Submit All Changes**.

Paging Group Example

This example sets up four paging groups: *All*, *Sales*, *Support*, and *Engineering*. Users will press 801 to send pages to all phones, 802 to send pages to phones configured as part of the Sales group, 803 to send pages to phones configured as part of the Support group, and 804 to send pages to phones configured as part of the Engineering group.

A phone that is configured with this example is a listening member of the “All” and “Sales” paging groups. That phone will automatically receive pages sent to those two paging groups. For each Sales phone, enter the following in the **Phone** > **Multiple Paging Groups Parameters** > **Group Paging Script** field:

```
pggrp=224.123.123.121:43210;name=All; num=801;listen=yes;
pggrp=224.123.123.121:43211;name=Sales;num=802; listen=yes;
pggrp=224.123.123.121:43212;name=Support;num=803;
pggrp=224.123.123.121:43213;name=Engineering;num=804;
```

Enabling Service Announcements

Service Announcements allows a user to send announcement requests to a customer-supplied announcement server. (Not applicable to the Cisco WIP310.)

To configure Service Announcements, navigate to **Admin Login** > **advanced** > **Voice** > **Phone**. Under Supplementary Services, in the **Service Annc Serv** list, choose **yes** to enable.

Customizing Phone Softkeys

You can customize the softkeys displayed on the phone. The default softkeys (when the phone is in an idle state) are Redial, Directory, Call Forward, and Do Not Disturb. Other softkeys are available during specific call states (for example, if a call is on hold, the Resume softkey displays).

This feature is not available on the IP phones that are using SPCP.

To program softkeys:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

STEP 2 (Cisco SPA525G or Cisco SPA525G2 only) Under Programmable Softkey Enable, choose **yes** to enable.

STEP 3 Edit the softkeys depending on the call state that you want the softkey to display. Refer to the table for information about softkeys.

In the Programmable Softkeys section, each phone state is displayed and the softkeys that are available to display during that state are listed. Each softkey is separated by a semicolon. Softkeys are shown in the format:

softkeyname|[*position*]

where *softkeyname* is the name of the key and *position* is where the key is displayed on the IP phone screen. Positions are numbered, with position one displayed on the lower left of the IP phone screen, followed by positions two through four. Additional positions are accessed by pressing the right arrow key on the phone. If no position is given for a softkey, the key will *float* and appears in the first available empty position on the IP phone screen.

NOTE On a Cisco SPA525G or Cisco SPA525G2 in the Off Hook state, the **More** softkey is fixed in position 4 and cannot be changed.

The table below lists each softkey and the phone state under which the softkey displays. You can have a maximum of 16 softkeys for each call state field.

Keyword	Key Label	Definition	Available Phone States
acd_login	Login	Logs user in to Automatic Call Distribution (ACD).	Idle
acd_logout	Logout	Logs user out of ACD.	Idle
alpha	Alpha	Enter alphabetic characters in a data entry field.	Off-Hook, Dialing Input
answer	Answer	Answers an incoming call.	Ringing
avail	Avail	Denotes that a user who is logged in to an ACD server has set his status as available.	Idle
barge	Barge	Allows another user to interrupt a shared call.	Shared-Active, Shared-Held
bxfer	BlindXfer/ bxfer	Performs a blind call transfer (transfers a call without speaking to the party to whom the call is transferred). Requires that Blind Xfer Serv is enabled.	Connected, Connected
cancel	Cancel	Cancels a call (for example, when conferencing a call and the second party is not answering).	Dialing Input
cfwd	Forward	Forwards all calls to a specified number.	Idle, Off-Hook, Hold, Shared-Active, Shared-Held
chkcfwd	Clr Fwd/-cfwd	Deactivates call forwarding.	Idle
chkdnd	Clr DND/-dnd	Deactivates Do Not Disturb.	Idle

Keyword	Key Label	Definition	Available Phone States
clear	Clear	Clears an entire text/number field.	Input
conf	Conf	Initiates a conference call. Requires that Conf Serv is enabled and there are two or more calls that are active or on hold.	Connected, Start-Conf
confLx	Conf Line	Conferences active lines on the phone. Requires that Conf Serv is enabled and there are two or more calls that are active or on hold.	Connected
delchar	delChar	Deletes a character when entering text.	Dialing (input)
dial	Dial	Dials a number.	Dialing (input)
dir	Dir	Provides access to phone directories.	Idle, Connected, Start-Conf, Start-Xfer, Off-Hook (no input), Redial
dnd	DND	Sets Do Not Disturb to prevent calls from ringing the phone.	Idle, Off-Hook (no input), Hold, Shared-Active, Shared-Held
em_login	Login	Logs user in to Extension Mobility.	Idle
em_logout	Logout	Logs user out of Extension Mobility.	Idle

Keyword	Key Label	Definition	Available Phone States
endcall	End Call	Ends a call.	Connected, Off-hook, Progressing, Start-Xfer, Start-Conf, Conferencing, Releasing, Resume
gpickup	GrPickup/ grPick	Allows user to answer a call ringing on an extension by discovering the number of the ringing extension.	Idle, Off-Hook (no input)
hold	Hold	Put a call on hold.	Connected, Start-Xfer, Start-Conf, Conferencing
ignore	Ignore	Ignores an incoming call.	Ringing
join	Join	Connects a conference call.	Conferencing
lcr	Call Rtn/lcr	Returns the last missed call.	Idle, Missed-Call, Off-Hook (no input)
left	Left	Moves the cursor to the left.	Dialing Input
miss	Miss	Displays the list of missed calls.	Missed-Call
newcall	New Call	Begins a new call.	Hold, Shared-Active
option	Option	Opens a menu of input options.	Off-Hook (no input), Dialing (input)
park	Park	Puts a call on hold at a designated “park” number.	Connected
phold	PrivHold	Puts a call on hold on an active shared line.	Connected

Keyword	Key Label	Definition	Available Phone States
pickup	Pickup	Allows user to answer a call ringing on another extension by entering the extension number.	Idle, Off-Hook (no input)
redial	Redial	Displays the redial list.	Idle, Connected, Start-Conf, Start-Xfer, Off-Hook (no input), Hold
resume	Resume	Resumes a call that is on hold.	Idle, Hold, Shared-Held
right	Right	Moves the cursor to the right.	Dialing (input)
starcode	Input Star Code/ *code	Displays a list of star codes that can be selected.	Off-Hook, Dialing (input)
toggle	Toggle	Switches between two calls that are active or on hold. (Cisco SPA502)	Connected
unavail	Unavail	Denotes that a user who is logged in to an ACD server has set his status as unavailable.	Idle
unpark	Unpark	Resumes a parked call.	Idle, Off-Hook (no input)
xfer	Transfer/ xfer	Performs a call transfer. Requires that Attn Xfer Serv is enabled and there is at least one connected call and one idle call.	Connected, Start-Xfer
xferLx	Xfer Line/ xferLx	Transfers an active line on the phone to a called number. Requires that Attn Xfer Serv is enabled and there are two or more calls that are active or on hold.	Connected

STEP 4 Click **Submit All Changes**.

Programmable Softkeys

The Cisco SPA300 Series and Cisco SPA500 Series IP Phones provide six programmable softkeys (fields PSK 1 through PSK 6). These keys can be defined by either a speed dial script or an XML service script.

To configure programmable softkeys:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

STEP 2 (Cisco SPA525G or Cisco SPA525G2 only) Under Programmable Softkey Enable, choose **yes** to enable.

To configure a speed dial script, enter the following in the PSK field:

```
fnc=sd;ext=extensionname@$PROXY;vid=outboundextnum;nme=name
```

where *fnc* is the function of the key (speed dial), ext (*extensionname*) is the extension being dialed, *vid* is the extension on the calling phone from which the outbound call is sent, and *name* is the name of the speed dial being configured.

Vertical service activation codes (* codes) are supported in speed dial configurations.

The *name* field displays on the softkey on the IP phone screen. Cisco recommends a maximum of 8 characters for a Cisco SPA30X or Cisco SPA50X phone and 10 characters for a Cisco SPA525G or Cisco SPA525G2 phone. If more characters are used, the label can be truncated on the IP phone screen.

To configure an XML script, enter the following in the PSK field:

```
fnc=xml;url=http://scriptURL.xml;nme=scriptname
```

where *fnc* is the function of the key (an XML script), *scriptURL.xml* is the URL where the script is located, and *scriptname* is the name of the script.

The *scriptname* field displays on the softkey on the IP phone screen. Cisco recommends a maximum of 8 characters for a Cisco SPA300 Series or Cisco SPA500 Series phone and 10 characters for a Cisco SPA525G or Cisco SPA525G2 phone. If more characters are used, the label can be truncated on the IP phone screen.

You can use macro variables in XML URLs. The following macro variables are supported:

- User ID—UID1, UID2
- Display name—DISPLAYNAME1, DISPLAYNAME2
- Auth ID—AUTHID1, AUTHID2
- Proxy—PROXY1, PROXY2
- MAC Address—MA
- Product Name—PN
- Product Series Number—PSN
- Serial Number—SERIAL_NUMBER

STEP 3 Click **Submit All Changes**.

Softkey Example

Configure the Cisco SPA525G or Cisco SPA525G2 phone with softkey that, when pressed, dials the Sales Department extension (200). You want this button to display on the far lower left of the IP phone screen when the phone is idle, when the phone is off hook, or when the phone is connected on a call. You want the outbound call (that is going to the speed dial) to originate from the second extension on the user phone, not the primary extension.

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

STEP 2 Under Programmable Softkey Enable, choose **yes** to enable.

STEP 3 In the Programmable Softkeys section, edit the following:

- Programmable Softkey Enable: yes
- PSK1: fnc=sd;ext=200@$PROXY;vid=2;nme=Sales
- Idle Key List: Edit the field to add psk1|1 to the beginning of the string; for example:

```
psk1|1;em_login;acd_login;acd_logout;avail;unavail;
redial;dir;cfwd;dnd;lcr;pickup;gpickup;unpark;em_logout;
```

- Off Hook Key List: Edit the field to add psk1|1 to the beginning of the string; for example:

  ```
  psk1|1;option;redial;dir;cfwd;dnd;lcr;unpark;pickup;
  gpickup;
  ```

- Connected Key List: Edit the field to add psk1|1 to the string, editing the existing *softkeyname*|1 to PSK1. For example, the original string:

  ```
  hold|1;endcall|2;conf|3;xfer|4;bxfer;confLx;xferLx;park;p
  hold;flash;
  ```

  becomes:

  ```
  psk|1;hold|2;endcall|3;conf|4;xfer;bxfer;confLx;xferLx;
  park;phold;flash
  ```

STEP 4 Click **Submit All Changes**. The **Sales** speed dial softkey is displayed in the lower left of the IP phone screen when the phone is idle, when the phone is connected on a call, and when the phone is off hook.

Configuring the Message Waiting Indicator

You can configure the message waiting indicator (MWI) for separate extensions on the phone. The MWI lights based on the presence of new voicemail messages in the mailbox.

To enable the indicator at the top of your Cisco SPA300 Series or Cisco SPA500 Series IP phone to light when voice mail is left, or on a Cisco WIP310 display a seeing message waiting notification, navigate to **Admin Login** > **advanced** > **Voice** > **Ext_n**. Under **Call Feature Settings** in the **Message Waiting** list, choose **yes** to enable.

Configuring Ring Tones

You can define up to 12 ring tones for a Cisco SPA300 Series or Cisco SPA500 Series IP phone. In addition to these 12 ring tones, 4 user-configurable ring tones can be used in place of some of the default ring tones. See **Appendix A, "Ring Tone (Cisco SPA300 Series and Cisco SPA500 Series),"** for more information about ring tones.

Cisco WIP310 ring tones are not configurable from the phone web user interface.

You can define:

- The default ring tone for the extension
- Specific ring tones assigned to individual callers in the personal directory. These override the default ring tone.

To configure ring tones:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone** and scroll to the **Ring Tone** section.

Configure the characteristics of each ring tone by using a Ring Tone script. Specify:

- Name (n)—Ring tone name, such as Classic, Simple, or Office
- Waveform (w):
  - (Not supported on the Cisco SPA300 Series or Cisco SPA5XXG.)
  - (Cisco SPA525G or Cisco SPA525G2) 1, 2, 3, 4, file://Pulse1.raw, file://Ring7.raw, file://Warble.raw, w=file://Low.raw, file://Floor.raw, file://Reverb.raw
- Cadence (c)—1, 2, 3, 4, or 5 (Not supported on the Cisco SPA300 Series or Cisco SPA5XXG.)

You can also use the configuration file to configure a ring tone. For example, to configure Ring1 to play the Warble ring tone, change the Ring1 parameter as follows

- Cisco SPA300 Series or Cisco SPA5XXG

```
<Ring1 ua="na">n=warble;w=7;c=1</Ring1>
```

- (Cisco SPA525G or Cisco SPA525G2)

```
<Ring1 ua="na">n=warble;w=file://Warble.raw;c=1</Ring1>
```

You can also download one of two available ring tones (user ring tone 1 or 2) by using TFTP:

```
http://phone_ip_addr/ringtone1?[url]
```

The `[url]` syntax is `tftp://host[:port]/path`.

- The default host is the TFTP host.
- Port is optional. The default port is 69.
- The link is case sensitive.

On the IP phones, user-downloaded ring tones are labeled User 1 and User 2 in the choices for the Default Ring. On the phone ring tone menu, the User 1 and User 2 choices are replaced by the corresponding name of the ring tone. **Not Installed** appears if the user ring tone slots are not used.

For ring tone User 1 and User 2, the cadence is fixed with the on-time equals to the duration of the ring tone file and off-time equals to four seconds. The total ring duration is fixed at 60 seconds. The user ring tone names displayed on the IP phone screen are derived from the ring tone file header file.

The phone does not require rebooting after downloading a ring tone.

To remove the User 1 ring tone from the phone, set the *path* to delete, as follows:

```
http://phone_ip_addr/ringtone1?/delete
```

STEP 2 Click **Submit All Changes**.

Configuring On-Demand Ring Tones (Cisco SPA525G or Cisco SPA525G2)

The Cisco SPA525G or Cisco SPA525G2 support on-demand ring tones; ring tones are downloaded from a TFTP server and played when a call comes in. To configure:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

STEP 2 Scroll to the **Ring Tone** section.

STEP 3 In one or more of the ten ring tone fields, enter the following:

```
n=office;w=[tftp://]host[:port]/path;c=0
```

Specify the URL to download in the `host/port/path` field. If the connection cannot be established, a default ring tone is played.

STEP 4 Click **Submit All Changes**.

User-Created MP3 Ring Tones (Cisco SPA525G or Cisco SPA525G2)

A Cisco SPA525G or Cisco SPA525G2 user can create up to two ring tones from an MP3 audio file stored on a USB memory device. For instructions, see the *Cisco Small Business SPA525G and SPA525G2 SIP IP Phones User Guide*, located on Cisco.com.

Creating and Uploading Ring Tones Using the Ring Tone Utility (Cisco SPA300 Series and Cisco SPA500 Series only)

To convert a file for use as a ring tone, use the Ring Tone Utility, available at:

https://supportforums.cisco.com/docs/DOC-9944

You must have a .wav file of less than 8 seconds in length saved to your computer. You can also use a sound editor to create the file with the following restrictions:

- 16-bit PCM mono
- 8000 samples per second
- Less than 6000 ms in length

To create a ring tone and upload it to a phone:

STEP 1 Open the Ring Tone Utility.

STEP 2 Enter the IP address of the phone.

STEP 3 Click **Browse** and navigate to the directory on your computer where the source .wav file is stored. Select the wav file and click **Open**.

STEP 4 Click **Load Source File**.

STEP 5 Enter a name for the ring tone. This name will appear in the display on the phone. You choose the file name later.

STEP 6 Enter the target. You can have up to two customized ring tones uploaded to the phone.

STEP 7 (Optional) Click **Preview** to preview the ring tone. Click **Options** to change the start or end positions, or to squeeze or stretch the audio.

STEP 8 Click **Upload to Phone** to upload the ring tone to the phone. Click **OK** when the success status message appears.

STEP 9 Close the open Ring Tone Utility windows.

To create a ring tone and save it to a file:

STEP 1 Open the Ring Tone Utility.

STEP 2 Enter the IP address of the user phone or press **Skip** to create the ring tone and save it as a file.

STEP 3 Click **Browse** and navigate to the directory on your computer where the source wav file is stored. Select the wav file and click **Open**.

STEP 4 Click **Load**.

STEP 5 Enter a name for the ring tone. This name will appear in the IP phone screen. You choose the file name later.

STEP 6 (Optional) Click **Preview** to preview the ring tone. Click **Options** to change the start or end positions, or to squeeze or stretch the audio.

STEP 7 Click **Save As** to save the file to your computer. Enter the file name and press **Save**.

STEP 8 Close the open Ring Tone Utility windows.

To delete a ring tone from a phone:

STEP 1 Open the Ring Tone Utility.

STEP 2 Enter the IP address of the phone.

STEP 3 Click the **Delete** button next to the ring tone you want to delete.

STEP 4 Click **OK**.

STEP 5 Close the Ring Tone Utility windows.

Assigning a Ring Tone to an Extension

To assign a ring tone to an extension:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Ext Ext** <*number*> tab.

STEP 2 Under **Call Feature Settings** in the **Default Ring** field, choose from the following:

- No Ring
- 1 through 12
- User 1
- User 2

STEP 3 Click **Submit All Changes**.

Configuring RSS Newsfeeds (Cisco SPA525G or Cisco SPA525G2)

The Cisco SPA525G or Cisco SPA525G2 provides the option to view RSS newsfeeds for news in the categories of local, world, finance, sports, and politics. Newsfeeds provided by Yahoo are supported for U.S. customers only.

To configure newsfeeds:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **User**.

STEP 2 Under **Web Information Service Settings**, you can edit the following fields:

Parameter	Description
RSS Feed URLs 1-5	URLs for Local and World news, Finance, Sports, and Politics. Default values are: ▪ 1—Local News (defaults to URL http://rss.cnn.com/rss/cnn_us.rss) ▪ 2—World News (defaults to URL http://newsrss.bbc.co.uk/rss/newsonline_uk_edition/world/rss.xml) ▪ 3—Finance News (defaults to URL http://finance.yahoo.com/rss/topstories) ▪ 4—Sports News (defaults to URL http://rss.news.yahoo.com/rss/sports ▪ 5—Politics News (defaults to URL http://rss.news.yahoo.com/rss/politics)
Weather Temperature Unit	Choose which unit to display for weather information (Fahrenheit or Celsius).

STEP 3 Click **Submit All Changes**. The phone reboots.

Configuring Audio Settings

You can configure default audio settings for the phone. The volume settings can be modified by the user by pressing the volume control button on the phone, then pressing the **Save** soft button. (Not applicable to the Cisco WIP310.)

To configure the audio volume settings:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **User**.

STEP 2 In the Audio Volume section, configure a volume level between 1 and 10, with 1 being the lowest level:

Parameter	Description
Ringer Volume	Sets the volume for the ringer.
Speaker Volume	Sets the volume for the full-duplex speakerphone.
Handset Volume	Sets the volume for the handset.
Headset Volume	Sets the volume for the headset.
Bluetooth Volume	Sets the volume for the Bluetooth device (Cisco SPA525G or Cisco SPA525G2 only).
Handset Version	Handset Version—Change the handset version manually. Auto—Phone automatically sets the handset version based on the hardware version and model. (Default) Original—Handset set to Version 2 and below. V3—Handset set to Version 3.
Deep Bass	Sets a standard tone or an enhanced bass tone.

STEP 3 Click **Submit All Changes**.

Configuring Audio Input Gain (Cisco SPA300 Series and Cisco SPA500 Series)

The value on the handset, headset, or speakerphone parameters default to zero, indicating that the volume is set to a base level. This does not mean that the sound is turned off; it is set to a level the average person can hear in a normal office environment.

To amplify or reduce the sound level, navigate to **Admin Login** > **advanced** > **Voice** > **Phone**. Under Audio Input Gain (dB), choose the item to configure:

- A positive value increases amplification (sound is louder).
- A negative value decreases amplification (sound is quieter).
- Set a value that is loud enough to hear clearly without producing echo (an indication that the input gain is too high).

Enabling Wireless (Cisco SPA525G or Cisco SPA525G2 only)

The Cisco SPA525G or Cisco SPA525G2 provides a Wireless-G interface. If a wired link is connected to the phone, the wireless connection is automatically disabled.

To enable wireless communications, navigate to **Admin Login** > **advanced** > **Voice** > **System**. Under **Wi-Fi Settings**, in the **SPA525-wifi-on** field, choose **yes** to enable or **no** to disable.

Configuring Bluetooth (Cisco SPA525G or Cisco SPA525G2 only)

The Cisco SPA525G or Cisco SPA525G2 supports Bluetooth to allow use of the phone with a wireless Bluetooth-enabled headset. The Cisco SPA525G2 also supports Bluetooth communications with a Bluetooth-enabled mobile phone. You can do the following:

- Pair your Bluetooth-enabled mobile phone and Cisco SPA525G2. Your mobile phone is assigned a line button on your Cisco SPA525G2. You can make and receive mobile network calls by using the Cisco SPA525G2.
- Switch audio for in-progress calls between your mobile phone and the Cisco SPA525G2.
- Import your mobile phone address book to your Cisco SPA525G2 personal address book.
- Use your Cisco SPA525G2 as a *handsfree device* for your mobile phone.

For a list of supported Bluetooth headsets, see https://supportforums.cisco.com/docs/DOC-9926.

Enabling Bluetooth from the Web Interface

To enable Bluetooth from the phone web user interface:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **System**.

STEP 2 Under **Bluetooth Settings** in the **Enable BT** field, choose **yes** to enable or **no** to disable.

STEP 3 Click **Submit All Changes**.

Enabling Bluetooth from the Phone

To enable Bluetooth from the IP phone screen:

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **User Preferences** and press **Select**.

STEP 3 Scroll to **Bluetooth Configuration** and press **Select**.

STEP 4 With **Bluetooth** selected, press the **Right Arrow** key until a blue check mark appears indicating that the feature is enabled.

STEP 5 Press **Save**.

Pairing a Bluetooth Headset

To enable a Bluetooth headset from the phone web user interface:

STEP 1 Click **Admin Login** > **advanced** > **Bluetooth**.

STEP 2 Under **Bluetooth Device**, choose **On**.

STEP 3 Under **Bluetooth Device List**, press **Scan for Bluetooth Devices**.

STEP 4 In the **Bluetooth Device List**, click the name of the Bluetooth headset.

STEP 5 Enter the PIN for the Bluetooth headset.

STEP 6 Press **Submit All Changes**.

To enable a Bluetooth headset from the IP phone screen:

STEP 1 Enable Bluetooth as described in **"Enabling Bluetooth from the Web Interface."**

STEP 2 Press the **Setup** button.

STEP 3 Scroll to **User Preferences** and press **Select**.

STEP 4 Scroll to **Bluetooth Configuration** and press **Select**.

STEP 5 Scroll to **Bluetooth Mode** and press the **Right Arrow** key to choose one of the following:

- **Phone**—Configures a Cisco SPA525G2 with a Bluetooth-enabled mobile phone. (The Cisco SPA525G pairs with headsets only; it does not pair with mobile phones.)

- **Both**—The Cisco SPA525G2 uses a Bluetooth headset or operates with a Bluetooth-enabled mobile phone (see **Pairing Your Cisco SPA525G2 with a Bluetooth-Enabled Mobile Phone**). The Cisco SPA525G2 connects to only one device at a time (either a Bluetooth headset or a Bluetooth-enabled mobile phone).

  If multiple Bluetooth devices are in range of the Cisco SPA525G2, the order of devices in the **Bluetooth Configuration** > **Bluetooth Profiles** list is used, and the device with a higher priority is activated first.

STEP 6 Scroll to **Bluetooth Profiles** and press the **Right Arrow** key to enter the profile screen.

STEP 7 Press **Scan** to scan for your headset.

NOTE Depending on the network environment (such as the number of Bluetooth devices and noise level), your Bluetooth headset might not appear on the found devices list. Ensure the headset is powered on and has Bluetooth activated, and retry the scan.

STEP 8 In the list of found devices, select your headset and press **Select** to edit the profile.

STEP 9 Scroll to **PIN** and enter the PIN for your Bluetooth headset.

STEP 10 Scroll to **Connect Automatically** and press the **Right Arrow** key to turn to **On**.

STEP 11 Press **Connect**. The profile screen displays and a check mark appears next to the headset if the connection was successful.

Pairing Your Cisco SPA525G2 with a Bluetooth-Enabled Mobile Phone

This feature is based on the following standard Bluetooth profiles:

- Phone Book Access Profile 1.0
- Handsfree Profile 1.5
- Handset Profile 1.1

Make sure your mobile phone provides support for one of the above profiles. Cisco provides a reference list of Bluetooth-enabled mobile phones supported with the Cisco SPA525G2. See the Cisco support community at http://www.cisco.com/go/smallbizsupport and consult the latest Cisco SPA525G2 release notes, available at cisco.com.

For more detailed instructions, see the *Cisco Small Business Cisco SPA525G or Cisco SPA525G2 IP Phone User Guides*.

To pair your Cisco SPA525G2 with your Bluetooth-enabled mobile phone, you can either initiate pairing from the Cisco SPA525G2, or from your mobile phone.

Initiating Pairing from the Cisco SPA525G2

STEP 1 Enable Bluetooth as described in **Enabling Bluetooth from the Web Interface**.

STEP 2 Press the **Setup** button.

STEP 3 Scroll to **User Preferences** and press **Select**.

STEP 4 Scroll to **Bluetooth Configuration** and press **Select**.

STEP 5 Scroll to **Bluetooth Mode** and press the **Right Arrow** key to choose one of the following:

- **Handsfree**—Your Cisco SPA525G2 operates as a handsfree device with a Bluetooth-enabled mobile phone.
- **Both**—Your Cisco SPA525G2 operates with your Bluetooth-enabled mobile phone **or** operate with a Bluetooth headset. The Cisco SPA525G2 connects to only one device at a time (either the Bluetooth headset or the Bluetooth-enabled mobile phone.)

  If multiple Bluetooth devices are in range of the Cisco SPA525G2, the order of devices in the **Bluetooth Configuration** > **Bluetooth Profiles** list is used, and the device with a higher priority is activated first.

STEP 6 Scroll to **Bluetooth Profiles** and press the **Right Arrow** key to enter the profile screen.

STEP 7 Press **Scan** to scan for your mobile phone.

Depending on the network environment (such as the number of Bluetooth devices and the noise level), your Bluetooth headset might not appear on the found devices list. Ensure the headset is powered on and has Bluetooth activated, and retry the Scan.

STEP 8 In the Select a Bluetooth Device to Pair list, select the mobile phone to which you want to pair and press **Connect**.

Initiating Pairing from Your Bluetooth-Enabled Mobile Phone

The procedure varies depending on your phone model. The example in this section uses an Apple iPhone.

Before starting, it is helpful to find the MAC address of your Cisco SPA525G2 IP phone. From your IP phone, go to the Setup menu and select **Status**. Select **Product Information**. The MAC address is displayed.

STEP 1 On your iPhone, click **Settings**.

STEP 2 Under **General**, choose **Bluetooth**. Ensure Bluetooth is turned on.

STEP 3 In the Bluetooth Window, under Devices, find the MAC address of your Cisco SPA525G2 IP phone.

STEP 4 Select the MAC address of the Cisco SPA525G2.

STEP 5 Enter the PIN (the default is 0000) and press **Connect**.

When paired with your mobile phone, the Cisco SPA525G2 IP phone screen assigns one of your line buttons to the mobile phone. A mobile phone icon with a flashing lightning bolt icon is displayed next to the mobile phone number.

To verify the mobile phone configuration:

STEP 1 On the Cisco SPA525G2, press the **Setup** Button.

STEP 2 Scroll to User Preferences and press **Select**.

STEP 3 Scroll to Bluetooth Configuration and press **Select**.

STEP 4 Scroll to Bluetooth Profiles and press the **Right Arrow** key.

The mobile phone appears in the list of Bluetooth devices.

Enabling SMS Messaging

The Cisco SPA IP phones can receive and display text messages by using SIP (RFC-3428). Cisco WIP310 users can send *and* receive text messages.

When this feature is enabled, the IP phone screen displays messages up to 255 characters in length. The message appears on the IP phone screen along with the date and time.

Service providers could use text messages to:

- Send billing information, calling minutes consumed, minutes available.
- Include additional text with a call to facilitate call processing.

Cisco SPA303 and Cisco SPA5XXG

To enable text message receipt on the Cisco SPA303 or Cisco SPA500 Series phones:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **User**.

STEP 2 Under **Supplementary Services** in the **Text Message** field, choose **yes** to enable.

STEP 3 (Optional) To enable receipt of text messages from a third party directly without proxy involvement, in the **Text Message from 3rd Party** field, choose **yes** to enable.

STEP 4 Click **Submit All Changes**.

Cisco SPA525G or Cisco SPA525G2

To enable text messaging on Cisco SPA525G or Cisco SPA525G2 phones:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **User**.

STEP 2 Under **Supplementary Services** in the **Display Text Message on Recv** field, choose **yes** to enable.

STEP 3 (Optional) To enable receipt of text messages from a third party directly without proxy involvement, in the **Text Message from 3rd Party** field, choose **yes** to enable.

STEP 4 Click **Submit All Changes**.

Cisco WIP310

STEP 1 Click **Admin Login** > **advanced** > **Phone**.

STEP 2 Under **SMS Enable**, choose **yes** to enable.

STEP 3 Click **Submit All Changes**.

Enabling and Configuring the Phone Web Server

The web server allows administrators and users to log in to the phone by using a phone web user interface. Administrators and users have different privileges and see different options for the phone based on their role.

Configure the Web Server from the Phone Web Interface

To enable the web server:

STEP 1 Click **Admin Login** > **advanced** > **System**.

STEP 2 Under the **System Configuration** section in the **Enable Web Server** field, verify that the parameter is set to **yes** to enable the web administration server. (For the Cisco 301 and Cisco SPA501G, this can be configured by using the IVR. See the **"Using IVR on IP Phones Without Screens" section on page 27**.)

STEP 3 In the **Web Server Port** field, enter the port to access the web server. The default is port 80.

STEP 4 In the **Enable Web Admin Access** field, you can enable or disable local access to the **Admin Login** of the phone web user interface. Defaults to **yes** (enabled). (For the Cisco SPA301 and Cisco SPA501G, can be configured using the IVR. See the **"Using IVR on IP Phones Without Screens" section on page 27**.)

STEP 5 In the **Admin Passwd** field, enter a password if you want the system administrator to log in to the phone web user interface with a password. The password prompt appears when an administrator clicks **Admin Login**. The maximum password length is 32 characters.

STEP 6 In the **User Password** field, enter a password if you want users to log in to the phone web user interface with a password. The password prompt appears when users click **User Login**. The maximum password length is 32 characters

STEP 7 Click **Submit All Changes**.

Configure the Web Server from the Phone Screen Interface

To enable the phone web user interface from the **Phone** tab (does not apply to the Cisco WIP310):

STEP 1 Press menu.

STEP 2 Select **Network** and **Enable Web Server**.

STEP 3 Select the **Edit**.

STEP 4 Press y/n to toggle the selection to **Yes** and enable.

STEP 5 Click **OK** > **Save**.

Configuring LDAP for the Cisco SPA300 Series and Cisco SPA500 Series IP Phones

The Cisco SPA300 Series and Cisco SPA500 Series IP phones support Lightweight Directory Access Protocol (LDAP) v3. LDAP Corporate Directory Search allows a user to search a specified LDAP directory for a name, phone number, or both. LDAP-based directories, such as Microsoft Active Directory 2003 and OpenLDAP-based databases, are supported. (LDAP is not supported on the Cisco WIP310.)

Users access LDAP from the **Directory** menu on their IP phone. There is a limit of 20 records returned from a LDAP search.

The instructions in this section assume you have the following equipment and services:

- A LDAP server, such as OpenLDAP or Microsoft Active Directory Server 2003
- A Cisco SPA300 Series or Cisco SPA500 Series IP phone running firmware version 6.1.3a or higher

To prepare the LDAP Corporate Directory Search:

STEP 1 Click **Admin Login** > **advanced** > **System**.

STEP 2 In the **Optional Network Configuration** section, under **Primary DNS**, enter the IP address of the DNS server. (Only required if using Active Directory with authentication set to MD5.)

STEP 3 In the **Optional Network Configuration** section, under **Domain**, enter the LDAP domain. (Only required if using Active Directory with authentication set to MD5.)

Some sites might not deploy DNS internally and instead use Active Directory 2003. In this case, it is not necessary to enter a Primary DNS address and an LDAP Domain. However, with Active Directory 2003, the authentication method is restricted to Simple.

STEP 4 Click the **Phone** tab.

STEP 5 Under **LDAP**, in the **LDAP Dir Enable** field, choose **yes** to enable LDAP and cause the name defined in **LDAP Corp Dir Name** to appear in the phone directory.

STEP 6 Configure values for the fields in the following table and click **Submit All Changes**.

Parameter	Description
LDAP Corp Dir Name	Enter a free-form text name, such as *Corporate Directory*.
LDAP Server	Enter a fully qualified domain name or IP address of LDAP server, in the format `nnn.nnn.nnn.nnn`. Enter the host name of the LDAP server if the MD5 authentication method is used.

Parameter	Description
LDAP Auth Method	Select the authentication method that the LDAP server requires: None—No authentication is used between the client and the server. Simple—The client sends its fully-qualified domain name and password to the LDAP server. Might create security issues. Digest-MD5—The LDAP server sends authentication options and a token to the client. The client returns an encrypted response that is decrypted and verified by the server.
LDAP Client DN	Enter the distinguished name domain components [dc] ; for example: `dc=cv2bu,dc=com` If using the default Active Directory schema (Name(cn)->Users->Domain), example of the client DN: `cn="David Lee",dc=users,dc=cv2bu,dc=com`
LDAP Username	Enter the username for a credentialed user on the LDAP server.
LDAP Password	Enter the password for the LDAP username.
LDAP Search Base	Specify a starting point in the directory tree from which to search. Separate domain components [dc] with a comma. For example: `dc=cv2bu,dc=com`
LDAP Last Name Filter	Define the search for surnames [sn], known as last name in some parts of the world. For example, `sn:(sn=*$VALUE*)`. This searches for the text string anywhere in the beginning, middle, or at the end of a name. You must enter a value in both the last name and first name fields so that the LDAP corporate directory option displays on the phone. If both fields are empty, the directory does not display.

Parameter	Description
LDAP First Name Filter	Define the search for the common name `[cn]`. For example, `cn:(cn=*$VALUE*)`. This searches for the text string anywhere in the beginning, middle, or at the end of a name. You must enter a value in both the last name and first name fields so that the LDAP corporate directory option displays on the phone. If both fields are empty, the directory does not display.
LDAP Search Item 3	Enter a customized search item. Can be blank if not needed.
LDAP Item 3 Filter	Enter a customized filter for the searched item. Can be blank if not needed.
LDAP Search Item 4	Enter a customized search item. Can be blank if not needed.
LDAP Item 4 Filter	Enter a customized filter for the searched item. Can be blank if not needed.

Parameter	Description
LDAP Display Attrs	Enter the format of LDAP results display on phone where: ▪ a—Attribute name ▪ cn—Common name ▪ sn—Surname (last name) ▪ telephoneNumber—Phone number ▪ n—Display name For example, `n=Phone` causes `Phone:` to be displayed in front of the phone number of an LDAP query result when the detail soft button is pressed. t—type When `t=p`, **t** is of type phone number and the retrieved number can be dialed. Only one number can be made dialable. If two numbers are defined as dialable, only the first number is used. For example, `a=ipPhone, t=p; a=mobile, t=p;` This example results in only the `ipPhone` number being dialable and the mobile number is ignored. ▪ p—phone number When **p** is assigned to a type attribute, example `t=p`, the the retrieved number is dialable.
LDAP Number Mapping	With the LDAP number mapping you can manipulate the number that was retrieved from the LDAP server. For example, you can append **9** to the number if your dial plan requires a user to enter 9 before dialing. Add the 9 prefix by adding `(<:9>xx.>)` to the LDAP Number Mapping field. For example, 555 1212 will become 9555 1212. Can be blank if not needed. If you do not manipulate the number in this fashion, a user can use the **Edit Dial** feature to edit the number before dialing out.

For more information on LDAP, including troubleshooting information, see the *Configuring LDAP Directory Search on SPA SIP IP Phones* Application Note, available from http://www.cisco.com/web/partners/sell/smb/products/voice_and_conferencing.html#~vc_technical_resources (partner log on required).

Configuring BroadSoft Settings (Cisco SPA300 Series and Cisco SPA500 Series)

Configuring BroadSoft Directory

The BroadSoft directory service enables users to search and view their personal, group, or enterprise contacts. This application feature uses BroadSoft's Extended Services Interface (XSI).

To configure the BroadSoft Directory service:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

STEP 2 Under **Broadsoft Settings**, configure the following:

- Directory Enable: Set to **yes**.
- XSI Host Server: Enter the name of the server; for example, **xsp.xdp.broadsoft.com**.
- Directory Name: Name of the directory. Displays on the user phone as a directory choice (for example, **John's Personal Directory**).
- Directory Type: Select the type of BroadSoft directory:
  - Enterprise (default): Allows users to search on last name, first name, user or group ID, phone number, extension, department, or email address.
  - Group: Allows users to search on last name, first name, user ID, phone number, extension, department, or email address.
  - Personal: Allows users to search on last name, first name, or telephone number.
- Directory UserID: BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com.
- Directory Password: Alphanumeric password associated with the User ID.

To improve security, the SPA phone firmware places access restrictions on the host server and directory name entry fields.

Field	Access Restriction
Dir. Name	Admin password required (if set)
Host Server	Admin password required (if set)
Type	None
User ID	None
Password	None

STEP 3 Click **Submit All Changes**.

Configuring Synchronization of Do Not Disturb and Call Forward on a Per Line Basis (Applicable to Broadsoft)

Enabling synchronization of Do Not Disturb (DND) and Call Forward (CFWD) allows the phone to synchronize with the call server (for example, the BroadSoft server) so that if Do Not Disturb or Call Forwarding settings are changed on the phone, changes are also made on the server; if changes are made on the server, they are propagated to the phone. You can enable DND/CFWD per extension.

This feature is disabled by default.

Limitations:

- Cisco SPA301 or Cisco SPA501G—The softkey and phone menu settings are not available.
- Cisco SPA509—Lines 9–12 cannot be set by using the SoftKeys or Menu settings.

Configuring Synchronization of DND and CEWD

To enable synchronization:

STEP 1 Click **Admin Login** > **advanced** > **Voice**.

STEP 2 Click the **Ext n** tab.

STEP 3 Under **Call Feature Settings** in the **Device Feature Sync** field, choose **yes** to enable DND/CFWD.

STEP 4 Under **SIP**, enable the relevant event package (Talk Package, Hold Package, and Conference Package).

STEP 5 Click **Submit All Changes**.

Configuring Synchronization of DND and CEWD by Using the Configuration File

You can also configure broadsoft DND and CFWD on a per line basis by modifying your configuration. For example, to configure this feature on line 1, add the following line to the configuration file:

```
<Device_Feature_Sync_1_ ua="na">Yes</Device_Feature_Sync_1_>
```

Configuring Broadsoft ACD Support

To support basic Broadsoft Automatic Call Distribution (ACD), enable the relevant **Broadsoft ACD** option. This option is available for each extension under **Call Feature Settings**.

The supported values for this option are **Yes** and **No** (default).

If you set **Broadsoft ACD** to **Yes**, the phone sends a Subscribe message according to the Broadsoft specification.

If you set **Broadsoft ACD** to **No**, the phone may still send out a Subscribe message because another feature is using ACD, but the phone ignores any Notify message from the Broadsoft server related to ACD.

Limitations:

- Cisco SPA301 or Cisco SPA501G—ACD is not supported. The ACD Login and Status keys are not visible.
- Cisco SPA509—Lines 9–12 cannot be used as ACD Agents since the Lines cannot be selected for Login/Logout and Agent status.

Configuring Broadsoft ACD Support

To enable broadsoft ACD support, navigate to **Admin Login** > **advanced** > **Voice** > **Ext n**. Under **Call Feature Settings**, in the **Broadsoft ACD** list, choose **yes** to enable broadsoft ACD support.

You can also configure broadsoft ACD support by adding the following line to your configuration file to configure this feature on line 1:

```
<Broadsoft_ACD_1_ ua="na">Yes</Broadsoft_ACD_1_>
```

Configuring XML Services

The Cisco SPA300 Series and Cisco SPA500 Series IP phones provide support for XML services, such as an XML Directory Service or other XML applications.

The following table shows some Cisco XML objects that are supported:

Cisco XML Object	Supported Phone
CiscoIPPhoneMenu	Cisco SPA5XXG, Cisco SPA30X, Cisco SPA525G or Cisco SPA525G2
CiscoIPPhoneText	
CiscoIPPhoneInput	
CiscoIPPhoneDirectory	
CiscoIPPhoneIconMenu	
CiscoIPPhoneStatus	
CiscoIPPhoneExecute	

Cisco XML Object	Supported Phone
CiscoIPPhoneImage	Cisco SPA525G or Cisco SPA525G2
CiscoIPPhoneImageFile	
CiscoIPPhoneGraphicMenu	
CiscoIPPhoneFileMenu	
CiscoIPPhoneStatusFile	
CiscoIPPhoneResponse	
CiscoIPPhoneErrror	
CiscoIPPhoneGraphicFileMenu	
Init:CallHistory	Cisco SPA5XXG
Key:Headset	
EditDial:n	

You can use macro variables in XML URLs. The following macro variables are supported:

- User ID—UID1, UID2
- Display name—DISPLAYNAME1, DISPLAYNAME2
- Auth ID—AUTHID1, AUTHID2
- Proxy—PROXY1, PROXY2
- MAC Address—MA
- Product Name—PN
- Product Series Number—PSN
- Serial Number—SERIAL_NUMBER

For more information on XML support, see the Cisco Small Business Support community. The URL is given in **Appendix B, "Where to Go From Here."**

To configure the phone to connect to an XML Directory service:

STEP 1 Click **Admin Login** > **advanced** > **Voice > Phone**.

STEP 2 Enter the following information:

- **XML Directory Service Name**: Name of the XML Directory. Displays on the user phone as a directory choice.
- **XML Directory Service URL**: URL where the XML Directory is located.

STEP 3 Click **Submit All Changes**.

To configure the phone to connect to an XML application:

STEP 1 Click **Admin Login** > **advanced** > **Voice > Phone**.

STEP 2 Enter the following information:

- **XML Application Service Name**: Name of the XML application. Displays on the user phone as a menu item.
- **XML Application Service URL**: URL where the XML application is located.

If you have configured an unused line button to connect to an XML application, the button connects to the URL configured here, unless you enter a different URL when configuring the line button. See the **"Configuring Unused Line Keys to Access Services" section on page 42**.

STEP 3 Click **Submit All Changes**.

Configuring Music On Hold

Your phone can play music on hold if it is part of a system that has a music-on-hold (MOH) server. To configure music on hold:

STEP 1 Click **Admin Login** > **advanced** > **Voice > Ext_n**.

STEP 2 Under **Call Feature Settings** in the **MOH Server** field, enter the user ID or the URL of the MOH streaming audio server. If you enter a user ID (no server), the current or outbound proxy is contacted. Defaults to blank (no MOH). If used with a Cisco SPA9000, it defaults to *imusic*. For more information, see the *Cisco SPA9000 Administration Guide*.

STEP 3 Click **Submit All Changes**.

Configuring Extension Mobility

Extension mobility allows mobile users to access their personalized phone settings, such as the personal extensions, shared lines, and speed dials, from other phones. For example, people who work different shifts or who work at different desks during the week can share an extension, yet have their own personalized settings. EM is supported for BroadSoft and other servers. EM dynamically configures a phone according to the current user.

A Login prompt appears on the IP phone screen when EM is enabled on a phone (for example, a conference room phone). A user can either enter their User ID and Password to access their personal phone settings, or ignore the login and use the phone as a guest. After logging on, users have access to personal directory numbers, services, speed dials, and other properties on the phone. When a user logs out, the phone reverts to a basic profile with limited features enabled.

This feature is not available on the Cisco WIP310.

To configure extension mobility:

STEP 1 Click **Admin Login** > **advanced** > **Voice > Phone**.

STEP 2 Under **Extension Mobility**, in the **EM Enable** field, choose **yes** to enable.

STEP 3 In the **EM User Domain** field, enter the domain for the phone, or the authentication server. For example, `@domain.com`, which is appended to the user ID (userID@domain.com) for authentication to the HTTP server.

STEP 4 Click **Submit All Changes**. The phone reboots.

You must also configure the Extension Mobility parameters in the profile rule field in the Provisioning tab. See the *Provisioning Parameters for Extension Mobility on Cisco SPA500 Series IP Phones* application note at:

https://www.myciscocommunity.com/docs/DOC-11277

For more information on extension mobility and BroadSoft, see http://www.broadsoft.com.

Configuring Video Surveillance (Cisco SPA525G or Cisco SPA525G2)

The Cisco SPA525G or Cisco SPA525G2 provides a simple video surveillance solution for a small business office. It works with the Cisco WVC2300 Wireless-G Business Internet Video Camera and the Cisco PVC2300 Business Internet Video Camera to provide simple video monitoring from your IP phone of a location such as a lobby entrance or doorway. Up to four cameras can be monitored from one IP phone.

Camera audio is not supported.

The Cisco SPA525G or Cisco SPA525G2 connects to the videocamera and provides a real-time video stream display from the camera. Storage and manipulation of video and physical camera control are not available from the IP phone.

The IP phone supports the camera display at a rate of two to three frames per second with good video quality. However, video quality can degrade if the camera is processing multiple streaming sessions, there is heavy Wi-Fi network traffic, or the IP phone is performing other processing. To avoid degrading voice audio quality on a call, the frame rate decreases to one frame per second if a codec other than G.711 is used for a call or when the user accesses the video monitoring page during a call.

Configuring the User Name and Account on the Camera

To configure the username and account:

STEP 1 Download and install the software release for the camera that provides video monitoring support. For more information, consult the release notes for the camera software.

STEP 2 Use the phone web user interface to create a user ID and password that are used by the phone to connect to the camera. The IP phone user account that you create should have viewer privileges.

Entering Camera Information Into the Cisco SPA525G or Cisco SPA525G2 Configuration Utility

To add camera information:

STEP 1 Click **Admin Login** > **advanced** > **Voice > User**.

STEP 2 Under Camera Settings in the **Enable Video VLAN** field, choose **yes** to enable. This option sends the camera traffic to a separate VLAN.

STEP 3 (Optional) If configuring Virtual LAN (VLAN) support, in the Enable Video VLAN field, choose **yes** to enable. The default Video VLAN ID is 1, the data VLAN. To separate traffic onto another VLAN (for example, a VLAN for video traffic only), enter the ID for that VLAN. (Video VLAN parameters do not apply to Wi-Fi or VPN.)

STEP 4 Under Camera Profile 1, enter the settings for the first camera. Enter the camera name (for example, **Lobby**). This name is displayed on the IP phone screen to identify the camera.

STEP 5 In the Access URL field, enter the URL to access the camera, in the following format:

`rtsp://`***XXX.XXX.X.XXX***`/img/jpgvideo.sav`

where *xxx.xxx.x.xxx* is the IP address of the camera.

STEP 6 In the **Access User Name** field, enter the username for the phone that you created by using the camera phone web user interface.

STEP 7 In the **Access Password** field, enter the password for the phone username that you created by using the camera phone web user interface.

STEP 8 (Optional) In the **Associated Caller ID** field, enter the phone number of the phone associated with the camera. For example, if the camera is located in the lobby, you can enter the extension of the lobby phone if one is installed there. People monitoring that camera from their phone can press **Call** to dial the number of the phone associated with the camera. For example, someone monitoring the lobby could call the receptionist to identify a visitor.

STEP 9 Repeat **STEP 3** through **STEP 7** for each camera.

STEP 10 Click **Submit All Changes**.

Viewing the Video

To view video from the phone:

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Video Monitoring** and press **Select**.

STEP 3 Scroll to the camera from which you want to view and press **Monitor** or **Select**.

Pressing **Call** dials the number associated with the camera (see **Entering Camera Information Into the Cisco SPA525G or Cisco SPA525G2 Configuration Utility**).

4

Configuring SIP, SPCP, and NAT

The Cisco SPA IP phones use the following protocols:

- Session Initiation Protocol (SIP)—Cisco SPA300 Series, Cisco SPA500 Series, Cisco WIP310
- Cisco Smart Phone Control Protocol (SPCP)—Cisco SPA300 Series, Cisco SPA500 Series

This chapter describes how to configure the phone protocols:

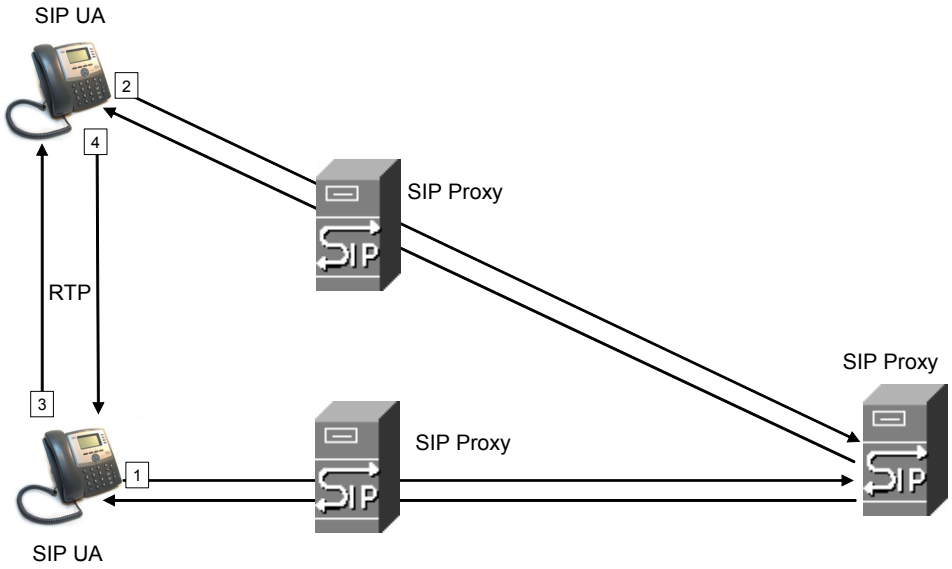
- **SIP and Cisco IP Phones**
- **Configuring SIP**
- **Configuring the IP Phone Communications Protocol**
- **Configuring the Protocol on a Cisco SPA300 Series or Cisco SPA500 Series IP Phone**
- **Managing NAT Transversal with Cisco IP Phones**

SIP and Cisco IP Phones

Cisco IP phones use Session Initiation Protocol (SIP), allowing interoperation with all IT service providers supporting SIP.

SIP handles signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* controls the attributes of an end-to-end call.

The diagram shows a SIP request for connection to another subscriber in the network.



In typical commercial IP telephony deployments, all calls go through a SIP proxy server. The requesting phone is called the SIP user agent server (UAS), while the receiving phone is called the user agent client (UAC).

SIP message routing is dynamic. If a SIP proxy receives a request from a UAS for a connection but cannot locate the UAC, the proxy forwards the message to another SIP proxy in the network. When the UAC is located, the response is routed back to the UAS, and a direct peer-to-peer session is established between the two UAs. Voice traffic is transmitted between UAs over dynamically-assigned ports using Real-time Protocol (RTP).

RTP transmits real-time data such as audio and video; it does not guarantee real-time delivery of data. RTP provides mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of UDP. See **NAT Mapping with STUN**.

SIP Over TCP

To guarantee state-oriented communications, Cisco IP phones can use TCP as the transport protocol for SIP. This protocol provides *guaranteed delivery* that assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent.

TCP overcomes the problem UDP ports have of being blocked by corporate firewalls. 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.

SIP Proxy Redundancy

An average SIP proxy server can handle tens of thousands of subscribers. A backup server allows an active server to be temporarily switched out for maintenance. Cisco phones support the use of backup SIP proxy servers to minimize or eliminate service disruption.

A static list of proxy servers is not always adequate. If your user agents are served by different domains, for example, you would not want to configure a static list of proxy servers for each domain into every Cisco IP phone.

A simple way to support proxy redundancy is to configure a SIP proxy server in the Cisco IP phone configuration profile. The DNS SRV records instruct the phones to contact a SIP proxy server in a domain named in SIP messages. The phone consults the DNS server. If configured, 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 forth. The Cisco IP phone tries to contact the hosts in the order of their priority.

If the Cisco IP phone currently uses a lower-priority proxy server, the phone periodically probes the higher-priority proxy and switches to the higher-priority proxy when available.

Configuring Survivable Remote Site Telephony (SRST) Support

The *proxy* and *outbound proxy* fields in the **Ext** tab can be configured with an extension that includes a statically-configured DNS SRV record or DNS A record. This allows for failover and fallback functionality with a secondary proxy server. The format for the parameter value is:

```
FQDN format: hostname[:port][:SRV=host-list OR :A=ip-list]
host-list:  srv[|srv[|srv…]]
srv: hostname[:port][:p=priority][:weight][:A=ip-list]
ip-list: ip-addr[,ip-addr[,ip-addr…]]
```

The default priority is 0 and default weight is 1. The default port is 0, and the application substitutes the proper port value (for example, port 5060 for SIP).

RFC3311 Support

The Cisco SPA525G or Cisco SPA525G2 support RFC-3311, the SIP UPDATE Method.

Support for SIP NOTIFY XML-Service

The Cisco SPA300 Series and Cisco SPA500 Series IP phones support the SIP NOTIFY XML-Service event. On receipt of a SIP NOTIFY message with an XML-Service event, the IP phone challenges the NOTIFY with a 401 response if the message does not contain correct credentials. The client must be furnish the correct credentials using MD5 digest with the SIP account password for the corresponding line of the IP phone.

The body of the message can contain the XML event Message. For example:

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>
</CiscoIPPhoneExecute>
```

Authentication:

```
challenge  = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
where A1 = username ":" realm ":" passwd
and A2 = Method ":" digest-uri
```

Configuring SIP

SIP settings for the Cisco SPA IP phones are configured for the phone in general and for individual extensions.

Configuring Basic SIP Parameters

To configure general SIP parameters, navigate to **Admin Login** > **advanced** > **Voice** > **SIP.** Under **SIP Parameters**, make these changes:

Parameter	Description
Max Forward	The number of proxies or gateways that can forward the request to the next downstream server. The Max-Forwards value is an integer in the range of 0 to 255 indicating the remaining number of times the request message is allowed to be forwarded. This count is decremented by each server that forwards the request. The initial value 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 might 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 $D corresponding to GPP_A to GPP_D allowed.
SIP Server Name	Server header used in responses to inbound responses. The default is **$VERSION**.
SIP Reg User Agent Name	User-Agent name used in a REGISTER request. If not specified, the SIP User Agent Name is used for the REGISTER request.
SIP Accept Language	The preferred languages for reason phrases, session descriptions, or status responses carried as message bodies in the response. If blank, the header is not included and the server assumes that all languages are acceptable to the client. Defaults to blank.

Parameter	Description
DTMF Relay MIME Type	MIME Type used in a SIP INFO message to signal a DTMF event. This parameter must match that of the service provider. Defaults to application/dtmf-relay.
Hook Flash MIME Type	MIME Type used in a SIPINFO message to signal a hook flash event.
Remove Last Reg	If set to **yes**, removes the previous registration before re-registering (if the value is different). Defaults to no.
Use Compact Header	If set to **yes**, the Cisco IP phone uses compact SIP headers in outbound SIP messages. If inbound SIP requests contain normal (non-compact) headers, the phone substitutes incoming headers with compact headers. If set to **no**, Cisco SPA IP phones use normal SIP headers. If inbound SIP requests contain compact headers, the phones reuse the same compact headers when generating the response, regardless of this setting. Defaults to no.
Escape Display Name	If set to **yes**, encloses the configured Display Name string 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. Defaults to yes.
SIP-B Enable	If set to **yes**, enables SIP for Business (supports Sylantro call flows) call features. See www.broadsoft.com for more information. Defaults to no.
Talk Package	If set to **yes**, enables support for the BroadSoft Talk Package that lets users answer or resume a call by clicking a button in an external application. Defaults to no.
Hold Package	If set to **yes**, enables support for the BroadSoft Hold Package, which lets users place a call on hold by clicking a button in an external application. Defaults to no.
Conference Package	If set to **yes**, enables support for the BroadSoft Conference Package that enables users to start a conference call by clicking a button in an external application. Defaults to no.

Parameter	Description
Notify Conference	If set to **yes**, Cisco SPA IP phones send out a NOTIFY with event=conference when starting a conference call (with the BroadSoft Conference Package). Defaults to no.
RFC 2543 Call Hold	If set to **yes**, Cisco SPA IP phones include Session Description Protocol (SDP) syntax c=0.0.0.0 when sending a SIP re-INVITE to a peer to hold the call. If set to no, Cisco SPA IP phones do not include the c=0.0.0.0 syntax in the SDP. With either setting, the phone includes a=sendonly syntax in the SDP. Defaults to yes.
Random REG CID On Reboot	If set to **yes**, Cisco SPA IP phones use a different random call-ID for registration after the next software reboot. If set to no, the phone tries to use the same call-ID for registration after the next software reboot. With either setting the phone uses a new random call-ID for registration after a power-cycle. Defaults to no. Not applicable to the Cisco WIP310.
Mark All AVT packets	If set to **yes**, all audio video transport (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. Defaults to yes.
SIP TCP Port Min	Lowest TCP port number that can be used for SIP sessions. Defaults to 5060.
SIP TCP Port Max	Highest TCP port number that can be used for SIP sessions. Defaults to 5080.
Keep Referee When REFER Failed	When set to **yes**, the phone immediately handles NOTIFY sipfrag messages.

Parameter	Description
CTI Enable	If set to **yes**, enables the computer telephony integration (CTI), where a computer can act as a call center handling all sorts of incoming and outgoing communications., including phone calls, faxes, and text messages. The CTI interface allows a third-party application to control and monitor the state of a Cisco IP phone and, for example, initiate or answer a call by clicking a mouse on a PC, CTI must be enabled on the Cisco SPA300 Series or Cisco SPA500 Series IP phones for an attached Cisco Attendant Console to properly monitor the IP phone line status. Defaults to no.
Caller ID Header	Select from where the IP phone gets the caller ID: PAID-RPID-FROM P-ASSERTED-IDENTITY REMOTE-PARTY-ID FROM header Defaults to PAID-RPID-FROM. Not applicable to the Cisco WIP310.
SRTP Method	The method to use for Secure Real-time Transport Protocol (SRTP): x-sipura—legacy SRPT method s-descriptor—compliant with RFC-3711 and RFC-4568 The default value is **x-sipura**. Not applicable to Cisco WIP310.
Hold Target Before REFER	Controls whether to hold call leg with transfer target before sending REFER to the transferee when initiating a fully-attended call transfer (where the transfer target has answered). Default value is “no,” where the call leg is not held. Not applicable to Cisco WIP310.

Parameter	Description
Dialog SDP Enable	When enabled and the Notify message body is too big causing fragmentation, the Notify message xml dialog is simplified; Session Description Protocol (SDP) is not included in the dialog xml content.
Display Diversion Info	Parses Diversion Header information in an incoming SIP Invite and displays it as the Caller ID.

Configuring SIP Timer Values

All SIP timer values are in seconds. To configure SIP timer values, navigate to **Admin Login** > **advanced** > **Voice** > **SIP.** Under **SIP Timer Values (sec)**, make these changes:

Parameter	Description
SIP T1	RFC-3261 T1 value (RTT estimate). Ranges from 0 to 64 seconds. Defaults to .5 seconds.
SIP T2	RFC-3261 T2 value, the maximum retransmit interval for non-INVITE requests and INVITE responses. Ranges from 0 to 64 seconds. Defaults to 4 seconds.
SIP T4	RFC-3261 T4 value, which is the maximum duration a message remains in the network. Ranges from 0 to 64 seconds. Defaults to 5 seconds.
SIP Timer B	RFC-3261 INVITE transaction time-out value. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer F	RFC-3261 Non-INVITE transaction time-out value. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer H	RFC-3261 INVITE final response time-out value for ACK receipt. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer D	RFC-3261 wait time for response retransmits. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer J	RFC-3261 Wait time for Non-INVITE request retransmits. Ranges from 0 to 64 seconds. Defaults to 16 seconds.

Parameter	Description
INVITE Expires	The length of time the INVITE is valid. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 19999999999999999999999999999999. Defaults to 240 seconds.
RelNVITE Expires	RelNVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 19999999999999999999999999999999. Defaults to 30
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 smallest of the two values is used. Defaults to 1 second.
Reg Max Expires	Maximum registration expiration time allowed from the proxy in the Min-Expires header. If the value is greater than this setting, the largest of the two values is used. Defaults to 7200 seconds.
Reg Retry Intvl[1]	Interval to wait before the Cisco IP phone retries registration after failing during the previous registration. The range is from 1 to 268435455. Do not enter 0. Defaults to 30 seconds.
Reg Retry Long Intvl 1	When registration fails with a SIP response code that does not match the Retry Reg response status code (RSC) value (see next table), the IP phone waits for this length of time before retrying. If this interval is 0, the Cisco IP phone stops trying. This value should be much larger than the Reg Retry Intvl value. The range is from 0 to 268435455. Defaults to 1200 seconds.
Reg Retry Random Delay	Random delay added to the Register Retry Intvl value when retrying REGISTER after a failure. Minimum and maximum random delay to be added to the short timer. The range is from 0 to 268435455. Defaults to 0, which disables this feature.

Parameter	Description
Reg Retry Long Random Delay	Random delay added to Register Retry Long Intvl value when retrying REGISTER after a failure. Minimum and maximum random delay to be added to the long timer. Random delay range (in seconds) to add to the Register Retry Long Intvl when retrying REGISTER after a failure. Defaults to 0, which disables this feature. Not applicable to Cisco WIP310.
Reg Retry Intvl Cap	Reg_Retry_Intvl_Cap—Maximum value of the exponential delay. The maximum value to cap the exponential backoff retry delay (which starts at the Register Retry Intvl and doubles every retry). Defaults to 0, which disables the exponential backoff (that is, the error retry interval is always at the Register Retry Intvl). When this feature is enabled, the Reg Retry Random Delay is added to the exponential backoff delay value. The range is from 0 to 268435455. Not applicable to Cisco WIP310.
Sub Min Expires	Lower limit of the REGISTER (subscribe) expires value returned from the proxy server. The range is from 0 to 268435455. Defaults to 10 seconds.
Sub Max Expires	Upper limit of the REGISTER (subscribe) min-expires value returned from the proxy server in the Min-Expires header. The range is from 0 to 268435455. Defaults to 7200 seconds.
Sub Retry Intvl	The retry interval when the last Subscribe request fails. The range is from 0 to 268435455. Defaults to 10 seconds.

1. Cisco IP phones can use a RETRY-AFTER value when it is received from a SIP proxy server that is too busy to process a request (503 Service Unavailable message). If the response message includes a RETRY-AFTER header, the phone waits for the specified length of time before to REGISTER again. If a RETRY-AFTER header is not present, the phone waits for the value specified in the Reg Retry Interval or the Reg Retry Long Interval.

Configuring Response Status Code Handling

To configure response status code handling , under **Response Status Code Handling** make these changes:

- **SIT1 through SIT4 RSC**—SIP response status code for the appropriate Special Information Tone (SIT). 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. The Reorder or Busy tone is played by default for all unsuccessful response status code for SIT 1 RSC through SIT 4 RSC. Defaults to blank.
- **Try Backup RSC**—SIP response code that retries a backup server for the current request. Defaults to blank.
- **Retry Reg RSC**—Interval the device waits before re-trying registration after a failed registration. Defaults to blank.

Configuring RTP Parameters

To configure Real-time Transport Protocol (RTP), navigate to **Admin Login** > **advanced** > **Voice** > **SIP.** Under **RTP Parameters**, configure these fields:

- **RTP Port Min**—Minimum port number for RTP transmission and reception. <RTP Port Min> and <RTP Port Max> defines a range that contains at least 10 even number ports (twice the number of lines); for example, 100–106. Defaults to 16384.
- **RTP Port Max**—Maximum port number for RTP transmission and reception. <RTP Port Min> and <RTP Port Max> should define a range that contains at least 10 even number ports (twice the number of lines); for example, 100–106. Defaults to 16482.
- **RTP Packet Size**—Packet size in seconds. The range is from 0.01 to 0.16. Valid values must be a multiple of 0.01 seconds. Defaults to 0.030.
- **Max RTP ICMP Err**—Number of successive ICMP errors allowed when transmitting RTP packets to the peer before the Cisco IP phone terminates the call. If the value is set to 0 (the default), the Cisco IP phone ignores the limit on ICMP errors, disabling the feature.

- **RTCP Tx Interval**—Interval for sending out Real-Time Transport Control Protocol (RTCP) sender reports on an active connection. During an active connection, the Cisco SPA IP phones send out compound RTCP packets. Each compound RTP packet, except the last one, contains a sender report (SR) and a source description (SDES). The last RTCP packet contains an additional BYE packet. Each SR, except the last one, contains one receiver report (RR); the last SR carries no RR.

  The SDES contains CNAME, NAME, and TOOL identifiers:

  - **CNAME**—*User ID@Proxy*
  - **NAME**—*Display Name* (or *Anonymous* if user blocks caller ID)
  - **TOOL**—Vendor/Hardware-platform-software-version (such as Cisco SPA9000-5.2.2(SCb)).

  The NTP timestamp used in the SR is a snapshot of the Cisco IP phone local time, not the time reported by an NTP server.

  If the Cisco IP phone receives a RR from a peer, it tries to compute the round trip delay and show it as the *Call Round Trip Delay* value in the Info section of the phone web user interface administration page. The range is from 0 to 255 seconds. Defaults to 0.

- **No UDP Checksum**—Select **yes** to enable the Cisco IP phone to calculate the UDP header checksum for SIP messages. Since this adds to the computation load, we recommend the default value, no (disabled).

- **Symmetric RTP**—Select **yes** to enable Symmetric RTP operation. When enabled, it sends RTP packets to the source address and the port of the last received valid inbound RTP packet. If disabled (or before the first RTP packet arrives) it sends RTP to the destination as indicated in the inbound SDP. Defaults to no.

- **Stats in BYE**—Select **yes** to send the P-RTP-Stat header in response to a BYE message. The header contains the RTP statistics on the current call. Defaults to no.

  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>
  ```

Configuring SDP Payload Types

Configured dynamic payloads are used for outbound calls only when the Cisco IP phone presents a Session Description Protocol (SDP) offer. For inbound calls with a SDP offer, the phone follows the caller's assigned dynamic payload type.

Cisco IP phones use the configured codec names in outbound SDP. For incoming SDP with standard payload types of 0-95, the Cisco IP phone ignores the codec names. For dynamic payload types, the Cisco IP phone identifies the codec by the configured codec names (comparison is case-sensitive).

To configure SDP payload types, navigate to **Admin Login** > **advanced** > **Voice** > **SIP.** Under **SDP Payload Types**, configure these parameters:

Parameter	Description
AVT Dynamic Payload	Any non-standard data. Both sender and receiver must agree on a number. Ranges from 96 to 127. Defaults to 101.
INFOREQ Dynamic Payload	Codec number used in the SIP messaging for the Dynamic Payload size mechanism. This number should match the number configured in the network/other party to enable the use of Dynamic Payload. The best range is 96 to 27 for any dynamic payload type. Defaults to blank.
G726r16 Dynamic Payload	RTP Payload Type Number that indicates the transmitted packet is using the G.726 codec. Other codecs have preassigned payload numbers that you do not have to be set, but G.726 does not.. Ranges from 96 to 127. Defaults to 98. Not applicable to Cisco SPA525G or Cisco SPA525G2.
G726r24 Dynamic Payload	RTP Payload Type Number that indicates the transmitted packet is using the G.726-24 codec. Ranges from 96 to 127. Defaults to 97. Not applicable to Cisco SPA525G or Cisco SPA525G2.

Parameter	Description
G726r32 Dynamic Payload	RTP Payload Type Number that indicates the transmitted packet is using the G726r32 codec. The range is from 0 to 268435455. Defaults to 2.
G726r40 Dynamic Payload	RTP Payload Type Number that indicates the transmitted packet is using the G.726-40 codec Ranges from 96 to 27. Defaults to 96. Not applicable to Cisco SPA525G or Cisco SPA525G2.
G729b Dynamic Payload	RTP Payload Type Number that indicates the transmitted packet is using the G729b codec. The range is from 0 to 268435455. Defaults to 99.
EncapRTP Dynamic Payload	EncapRTP Dynamic Payload type. The range is from 0 to 268435455. Defaults to 112.
RTP-Start-Loopback Dynamic	RTP-Start-Loopback Dynamic Payload. Defaults to 113.
RTP-Start-Loopback Codec	RTP-Start-Loopback codec. Select one of following: G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a, or G723. Defaults to G711u.
AVT Codec Name	AVT codec name used in SDP. Defaults to `telephone-event`.
G711u Codec Name	G.711u codec name used in SDP. Defaults to Pulse Code Modulation mu-law (PCMU).
G711a Codec Name	G.711a codec name used in SDP. Defaults to Pulse Code Modulation A-Law (PCMA).
G726r16 Codec Name	G.726-16 codec name used in SDP. Defaults to G726-16. Not applicable to Cisco SPA525G or Cisco SPA525G2.

Parameter	Description
G726r24 Codec Name	G.726-24 codec name used in SDP. Defaults to G726-24. Not applicable to Cisco SPA525G or Cisco SPA525G2.
G726r32 Codec Name	G.726-32 codec name used in SDP. Defaults to G726-32.
G726r40 Codec Name	G.726-40 codec name used in SDP. Defaults to G726-40. Not applicable to Cisco SPA525G or Cisco SPA525G2.
G729a Codec Name	G.729a codec name used in SDP. Defaults to G729a.
G729b Codec Name	G.729b codec name used in SDP. Defaults to G729ab.
G723 Codec Name	G.723 codec name used in SDP. Defaults to G723. Not applicable to the Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
EncapRTP Codec Name	EncapRTP codec name used in SDP. Defaults to encaprtp.

Configuring SIP Settings for Extensions

To configure the network settings for SIP extensions, navigate to **Admin Login** > **advanced** > **Voice** > **Ext_n.** Under **Network Settings**, configure the following fields:

Parameter	Description
SIP ToS/DiffServ Value	Time of service (ToS)/differentiated services (DiffServ) field value in UDP IP packets carrying a SIP message. Defaults to 0x68.
SIP CoS Value [0-7]	Class of service (CoS) value for SIP messages. Ranges from 0 to 7. Defaults to 3.
RTP ToS/DiffServ Value	ToS/DiffServ field value in UDP IP packets carrying RTP data. Defaults to 0xb8.
RTP CoS Value [0-7]	CoS value for RTP data. Ranges from 0 to 7. Defaults to 6.
Network Jitter Level	The jitter buffer size as it is adjusted by a device. Jitter buffer size is adjusted dynamically. The minimum jitter buffer size is 30 milliseconds or (10 milliseconds plus the current RTP frame size), whichever is larger, for all jitter level settings. However, the starting jitter buffer size value is larger for higher jitter levels. This setting controls the rate at which the jitter buffer size is adjusted to reach the minimum milliseconds. Select: **low (30 ms)**, **medium (40 ms)**, **high (60 ms)**, **very high** (80 ms), or **extremely high (180 ms)**. Defaults to high.
Jitter Buffer Adjustment	How the jitter buffer is adjusted. Select: **up and down**, **up only**, **down only**, or **disable**. Defaults to up and down.

To configure SIP settings, navigate to **Admin Login** > **advanced** > **Voice** > **Ext_n.** Under **SIP Settings**, configure the following fields:

Parameter	Description
SIP Transport	Select from **UDP**, **TCP** or **TLS**. Defaults to UDP.
SIP Port	Port number of the SIP message listening and transmission port. Defaults to 5060.

Parameter	Description
SIP 100REL Enable	Support of 100REL SIP extension for reliable transmission of provisional responses (18x) and use of PRACK requests. Select **yes** to enable. Otherwise, select **no**. Defaults to no.
EXT SIP Port	The external SIP port number substituted for the actual SIP port in all outgoing SIP messages. If 0 is specified, no SIP port substitution is performed. Defaults to blank. The range is from 0 to 65535.
Auth Resync-Reboot	The Cisco IP phone authenticates the sender when it receives a NOTIFY message with the following requests: resync reboot report restart XML-service Select **yes** to enable. Otherwise, select **no**. Defaults to yes.
SIP Proxy-Require	SIP proxy for each extension or behavior when an extension 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. For example, `com.nortel.networks.firewall`.
SIP Remote-Party-ID	The Remote-Party-ID header to use instead of the From header. Select **yes** to enable. Otherwise, select **no**. Defaults to yes.
Referor Bye Delay	Time when the Cisco IP phone sends BYE to terminate stale call legs upon completion of call transfers. Multiple delay settings (Referor, Refer Target, Referee, and Refer-To Target). Enter the appropriate period of time in seconds. Defaults to 4.
Refer-To Target Contact	Indicates the refer-to target. Select **yes** to send the **SIP Refer** to the contact. Otherwise, select **no**. Defaults to no.

Parameter	Description
Referee Bye Delay	Delay time for the Referee Bye Delay. Enter the appropriate period of time in seconds. Defaults to 0.
SIP Debug Option	How SIP messages are received at or sent from the proxy listen port to the log. Select: ▪ 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. Defaults to none.
Refer Target Bye Delay	Delay time for the Refer Target Bye Delay. Enter the appropriate period of time in seconds. Defaults to 0.

Parameter	Description
Sticky 183	When 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**. Defaults to no.
Auth INVITE	When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no. Not applicable to the Cisco WIP310.
Ntfy Refer On 1xx-To-Inv	When enabled as a transferee, the phone sends a NOTIFY with Event:Refer to the transferor for any 1xx response returned by the transfer target, on the transfer call leg. To enable this feature, select **yes**. If set to **no**, the phone only sends a NOTIFY for final responses (200 and higher). Not applicable to the Cisco WIP310.
Use Anonymous with RPID	When enabled and the caller blocks his caller-id, the FROM header display-name and user-id fields are set to **anonymous**. This parameter applies only if <SIP Remote-Party-ID> is set to yes; otherwise, it is ignored. When disabled, the FROM header display-name and user-id are not masked. The Remote-Party-ID header indicates privacy=full when the caller tries to block his caller-id. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to yes. Not applicable to the Cisco WIP310.

Parameter	Description
Set G729 annexb	G.729 Annex B (G.729b) that provides silence compression by enabling a voice activity detection (VAD) module. It uses 2-byte Silence Insertion Descriptor (SID) frames transmitted to initiate comfort noise generation (CNG). If transmission is stopped and the link goes quiet because of there is no speech transmitted, the receiving side might assume that the link has been cut. By inserting comfort noise, analog hiss is simulated digitally during the silence to assure the receiver that the link is active and operational. **none**—do not enable. **no**—turn on but do not silence the VAD. **yes**—enable. Not applicable to the Cisco SPA525G or Cisco SPA525G2.

Parameter	Description

Voice Quality Report Address	The name of the collector that collects the statistics from SIP PUBLISH events. For example, **collector@*fully-qualified-domain-name*** (collector@reports.cisco.com) or ***collector@IP-address*** (collector@192.168.5.1). The SIP event package, SIP PUBLISH, enables the collection and reporting of metrics that measure the quality for VoIP sessions. Voice call quality information derived from RTCP-XR and call information from SIP is conveyed from a User Agent in a session to the third party in SIP PUBLISH method.
	
	RTCP-XR must be configured first (see **Configuring RTP Parameters**). After RTCP-XR is enabled, the call status information is updated on the **Voice** > **Info** page during an active call. Additionally, RTCP-XR packets containing a voice metrics block report are sent with the interval specified in the RTCP Tx Interval. When the call session is ended, a SIP PUBLISH with voice metrics info is sent to the collector endpoint.
	
	This parameter supports a full SIP URI. Examples of valid addresses:
	▪ collector@domain.com
	▪ 123.collect@123.123.123.123:5555
	▪ 5678@domain.com:5656
	
	For example if extension 1 was configured by using the phone profile:
	
	`<Voice_Quality_Report_Address_1_ ua="na">`
	`collector@domain.com`
	`</Voice_Quality_Report_Address_1_>`
	
	or
	
	`<Voice_Quality_Report_Address_1_ ua="na">`
	`123.collect@123.123.123.123:5555`
	`</Voice_Quality_Report_Address_1_>`
	
	or
	
	`<Voice_Quality_Report_Address_1_ ua="na">`
	`5678@domain.com:5656`
	`</Voice_Quality_Report_Address_1_>`

Configuring a SIP Proxy Server

To configure SIP proxy and registration parameters, navigate to **Admin Login** > **advanced** > **Voice** > **Ext_n.** Under **Proxy and Registration**, configure the following fields:

Parameter	Description
Proxy	SIP proxy server and port number set by the service provider for all outbound requests. For example: 192.168.2.100:6060. The port number is optional. The default is port 5060.

Use Outbound Proxy	The outbound proxy (for example, 172.20.2.1:5060—port is optional) or a domain name, such as *sip.server.com*, as long as this name is a fully-qualified domain name. When set to **no**, the **Outbound Proxy** and **Use OB Proxy in Dialog** parameters are ignored. Defaults to no.
	
	Optionally, the proxy can be configured (Cisco SPA300 or Cisco SPA500 Series only) for Survivable Remote Site Telephony (SRST) support. The proxy is configured with an extension that includes a statically-configured DNS SRV record or DNS A record. Configuring the proxy allows for failover and fallback functionality with a secondary proxy server. For example:
	
	For SRV Record:
	`sip.server.com:SRV=node1.sip.server.com:5060:p=1:w=50|node2.sip.server.com:5060:p=2:w=50`
	
	For A Record:
	`sip.server.com:A=172.20.2.1,172.20.2.2`
	
	In both examples **Use DNS SRV** to **no** and **DNS SRV Auto Prefix** are set to **no**.

Outbound Proxy	All outbound requests are sent as the first hop. Enter an IP address or domain name.

Parameter	Description
Use OB Proxy In Dialog	SIP requests are sent to the outbound proxy within a dialog. This field is ignored if **Use Outbound Proxy** is set to **no**, or **Outbound Proxy** is blank. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to yes.
Register	Enables periodic registration with the proxy. This parameter is ignored if a proxy is not specified. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to yes.
Make Call Without Reg	Enables making outbound calls without successful (dynamic) registration by the phone. If set to no, the dial tone plays only when registration is successful. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.
Register Expires	Defines how often the phone renews registration with the proxy. If the proxy responds to a REGISTER with a lower expires value, the phone renews registration based on that lower value instead of the configured value. If registration fails with an "Expires too brief" error response, the phone retries with the value specified in the Min-Expires header of the error. The range is from 0 to 268435455. Defaults to 3600 seconds.
Ans Call Without Reg	The user does not have to be registered with the proxy to answer calls. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.
Use DNS SRV	Enables DNS SRV lookup for the proxy and outbound proxy. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.
DNS SRV Auto Prefix	The phone automatically prepends the proxy or outbound proxy name with _sip._udp when performing a DNS SRV lookup on that name. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.

Parameter	Description
Proxy Fallback Intvl	Sets the delay after which the phone retries from the highest priority proxy (or outbound proxy) after it has failed over to a lower priority server. The phone should have the primary and backup proxy server list from a DNS SRV record lookup on the server name. It needs to know the proxy priority; otherwise, it does not retry. The range is from 0 to 65535. Defaults to 3600 seconds.
Proxy Redundancy Method	The phone creates an internal list of proxies returned in the DNS SRV records. Select **Normal** to create a list that contains proxies ranked by weight and priority. Select **Based on SRV** and the phone creates a Normal list, then inspects the port numbers based on the first-listed proxy port. When the weight and priority match, the device selects the first port in the list. Defaults to Normal.

STEP 1 Click **Submit All Changes**.

Configuring Subscriber Information Parameters

To configure subscriber information parameters for each extension, navigate to **Admin Login** > **advanced** > **Voice** > **Ext_n.** Under **Subscriber Information**, configure the following fields:

Parameter	Description
Display Name	Name displayed as the caller ID.
User ID	Extension number for this line.
Password	Password for this line. Defaults to blank (no password required).

Parameter	Description
Use Auth ID	Enables the authentication ID and password for SIP authentication. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.
Auth ID	Authentication ID for SIP authentication. Defaults to blank.
Mini Certificate	Base64 encoding of a mini-certificate concatenated with the 1024-bit public key of the certificate authority (CA) signing the mini-certificate of all subscribers in the group. Defaults to blank.
SRTP Private Key	Base64 encoding of the 512-bit private key per subscriber for establishment of a secure call. Defaults to blank.

Reversed Authentication Realm	The IP address for an authentication realm other than the proxy IP address. The default value is blank; the proxy IP address is used as the authentication realm.
	
	The parameter for extension 1 appears as follows in the phone configuration file:
	
	`<Reversed_Auth_Realm_1_ ua="na">`
	`</Reversed_Auth_Realm_1_>`

Configuring the IP Phone Communications Protocol

By default, the phone automatically detects the protocol and the Unified Communications device.

Cisco SPA500 Series IP Phones can be used as part of a Cisco Unified Communications System that uses Smart Phone Control Protocol (SPCP), also known as Skinny Call Control Protocol (SCCP), to manage a voice network. Or the phones can be configured to use Session Initiation Protocol (SIP), an IETF-defined signaling protocol that controls voice communication sessions in an IP network.

Configuring the Protocol on a Cisco SPA525G or Cisco SPA525G2

To configure the protocol on the Cisco SPA525G or Cisco SPA525G2, navigate to **Admin Login** > **advanced** > **Voice** > **System.** Under **System Configuration** in the **SPA525-protocol** field, choose **SCCP or SIP**.

To configure the phone to automatically detect the protocol being used on the network that it is connected to, in the **SPA525-auto-detect-sccp** field, choose **yes**.

Configuring the Protocol on a Cisco SPA300 Series or Cisco SPA500 Series IP Phone

To configure the protocol on a Cisco SPA300 Series or Cisco SPA500 Series IP phone, navigate to **Admin Login** > **advanced** > **Voice** > **System.** Under **System Configuration** in the **Signaling Protocol** field, choose **SCCP or SIP**.

To configure the phone to automatically detect the protocol being used on the network that it is connected to, in the **SPCP Auto-detect** field, choose **yes**. The phone defaults to SIP unless it detects a Cisco Unified Communications device. When set to no, the phone uses the protocol set in the **Signaling Protocol** field.

The Cisco SPA301 or the Cisco SPA501G can be configured by using the IVR. See **Using IVR on IP Phones Without Screens** for more information.

Managing NAT Transversal with Cisco IP Phones

Network Address Translation (NAT) allows multiple devices to share a single, public, routable, IP address to establish connections over the Internet. NAT is present in many broadband access devices to translate public and private IP addresses. For VoIP to co-exist with NAT, NAT traversal is required.

Not all service providers provide NAT traversal. If your service provider does not provide NAT traversal, you have several options:

- **NAT Mapping with Session Border Controller**
- **NAT Mapping with SIP-ALG Router**
- **NAT Mapping with a Static IP Address**
- **NAT Mapping with STUN**

NAT Mapping with Session Border Controller

We recommend that you choose an service provider that supports NAT mapping through a Session Border Controller. With NAT mapping provided by the service provider, you have more choices in selecting a router.

NAT Mapping with SIP-ALG Router

NAT mapping can be achieved by using a router that has a SIP Application Layer Gateway (ALG). By using a SIP-ALG router, you have more choices in selecting an service provider.

NAT Mapping with a Static IP Address

You can configure NAT mapping on the phone to ensure interoperability with the service provider.

- You must have an external (public) IP address that is static.
- The NAT mechanism used in the router must be symmetric. See **Determining Whether the Router Uses Symmetric or Asymmetric NAT**.

Use NAT mapping only if the service provider network does not provide a Session Border Controller functionality. To configure NAT mapping on the phone:

STEP 1 Click **Voice** > **SIP** and navigate to **NAT Support Parameters**.

STEP 2 Set the following parameters to **yes**:

- **Handle VIA received**
- **Insert VIA received**,
- **Substitute VIA Addr**
- **Handle VIA rport**
- **Insert VIA rport**
- **Send Resp To Src Port**

STEP 3 Enter the public IP address for your router **EXT IP** field.

STEP 4 Click the **Ext_n** tab and navigate to **NAT Settings**.

STEP 5 Set **NAT Mapping Enable** to **yes**.

STEP 6 (Optional) Set **NAT Keep Alive Enable** to **yes**.

The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open. Check with your service provider to determine the requirements.

STEP 7 Click **Submit All Changes**.

STEP 8 Configure the firewall settings on your router to allow SIP traffic. See **Configuring SIP**.

NAT Mapping with STUN

If the service provider network does not provide a Session Border Controller functionality and if the other requirements are met, it is possible to use Session Traversal Utilities for NAT (STUN) to discover the NAT mapping. The STUN protocol allows applications operating behind a network address translator (NAT) to discover the presence of the network address translator and to obtain the mapped (public) IP address (NAT addresses) and the port number that the NAT has allocated for the User Datagram Protocol (UDP) connections to remote hosts. The protocol requires assistance from a third-party network server (STUN server) located on the opposing (public) side of the NAT, usually the public Internet. This option is considered a last resort and should be used only if the other methods are not available. To use STUN

- The router must use asymmetric NAT. See **Determining Whether the Router Uses Symmetric or Asymmetric NAT**.
- A computer running STUN server software is available on the network. You can also use a public STUN server or set up your own STUN server.

STEP 1 Click **Voice** > **SIP** and navigate to **NAT Support Parameters**.

STEP 2 Set the following parameters to **yes**:

- **Handle VIA received**
- **Insert VIA received**,
- **Substitute VIA Addr**
- **Handle VIA rport**
- **Insert VIA rport**

- **Send Resp To Src Port**
- **STUN Enable**

STEP 3 Enter the IP address for your STUN server in the **STUN Server** field.

STEP 4 Click **Ext_n.**

STEP 5 Set **NAT Mapping Enable** to **yes**.

STEP 6 (Optional) Set **NAT Keep Alive Enable** to **yes**.

The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open. Check with your service provider to determine the requirements.

STEP 7 Click **Submit All Changes**.

STEP 8 Configure the firewall settings on your router to allow SIP traffic. See **Configuring SIP**.

Determining Whether the Router Uses Symmetric or Asymmetric NAT

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.

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

To Determine Whether the Router Uses Symmetric or Asymmetric NAT:

STEP 1 Verify that the firewall is not running on your PC. (It can block the syslog port.) By default, the syslog port is 514.)

STEP 2 Click **Voice** > **System** and navigate to **Optional Network Configuration**.

STEP 3 Enter the IP address for the **Debug Server** and port number of your syslog server, if the port number is anything other than the default, 514. It is not necessary to include the port number if it is the default.

The address and port number must be reachable from the Cisco IP phone. The port number appears on the output log file name. The default output file is `syslog.514.log` (if port number was not specified).

STEP 4 Set the **Debug Level** to **3.**

STEP 5 To capture SIP signaling messages, click the **Ext** tab and navigate to SIP Settings. Set the **SIP Debug Option** to **Full**.

STEP 6 To collect information about what type of NAT your router uses click the **SIP** tab and navigate to NAT Support Parameters.

STEP 7 Click **Voice** > **SIP** and navigate to NAT Support Parameters.

STEP 8 Set **STUN Test Enable** to **yes**.

STEP 9 Determine the type of NAT by viewing the debug messages in the log file. If the messages indicate that the device is using symmetric NAT, you cannot use STUN.

STEP 10 Click **Submit All Changes**.

5

Configuring Security, Quality, and Network Features

This chapter describes how to configure security, voice quality, and optional network features for the phone:

- **Setting Security Features**
- **Configuring Voice Codecs**
- **Configuring Domain and Internet Settings**
- **Setting Optional Network Servers**
- **Configuring VLAN Settings**
- **Configuring SSL VPN on the Cisco SPA525G or Cisco SPA525G2**

Setting Security Features

The security features ensure that calls are secure and authenticated.

Challenging SIP Initial INVITE and MWI Messages

The SIP INVITE (initial) and Message Waiting Indication (MWI) messages in a session can be challenged by the endpoint. The challenge restricts the SIP servers that are permitted to interact with the devices on a service provider network. This significantly increases the security of the VoIP network by preventing malicious attacks against the device.

To configure SIP INVITE challenge, navigate to **Admin Login** > **advanced** > **Voice** > **Ext_n.** Under **SIP Settings** in the Auth INVITE field, choose **yes**.

Encrypting Signaling with SIP Over TLS

Transport Layer Security (TLS) is a standard protocol for securing and authenticating communications over the Internet. SIP Over TLS encrypts the SIP messages between the service provider SIP proxy and the end user. SIP Over TLS encrypts only the signaling messages, not the media. A protocol such as Secure Real-Time Transport Protocol (SRTP) can be used to encrypt voice packets (see **Securing Voice Traffic with SRTP**).

TLS has two layers:

- TLS Record Protocol--layered on a reliable transport protocol, such as SIP or TCH, it ensures that the connection is private by using symmetric data encryption and it ensures that the connection is reliable.
- TLS Handshake Protocol--authenticates the server and client, and negotiates the encryption algorithm and cryptographic keys before the application protocol transmits or receives data.

Cisco SPA IP phones use UDP as a standard for SIP transport, but they also support SIP over TLS for added security.

To enable TLS for the phone, navigate to **Admin Login** > **advanced** > **Voice** > **Ext_n.** Under **SIP Settings,** select **TLS** from the SIP Transport list.

Securing Voice Traffic with SRTP

Secure Real-Time Transport Protocol (SRTP) is a secure protocol for transporting real-time data over networks. It provides media encryption to ensure that media streams between devices are secure and that only the intended devices receive and read the data. Cisco SPA IP phones use SRTP to securely send and receive voice traffic to and from phones and gateways that support SRTP. (Security Description (RFC-4568) is supported.)

When a call is secured with SRTP, the voice conversation is encrypted so that others cannot eavesdrop on the conversation. To enable this feature, Cisco SPA IP phones must have a mini-certificate installed.

Defaults to prefer to use encrypted media (voice codecs). Audio packets in both directions of outbound calls are encrypted by using SRTP.

Authorizing Secure Calls with a Mini-certification

The phone can encrypt calls to protect them from eavesdroppers. The dial pad codes for encrypting calls are:

- *16—Secures all calls.
- *17—Disable the call security the user enabled by dialing *16.
- *18—Secures an individual call when dialed before or during a call. Using this star code is redundant if all outbound calls are already secure by default or from having dialed *16.

To enable call encryption on the phone web user interface:

STEP 1 Obtain the Generate Mini-Cert tool from your service provider.

STEP 2 Navigate to **Admin Login** > **advanced** > **Voice** > **Ext_n.**

STEP 3 Under **Subscriber Information**, enter the **Mini Certificate** and the **SRTP Private Key** that provide secure encryption of RTP streams between two endpoints on an extension.

STEP 4 To enable the secure call service, navigate to **Admin Login** > **advanced** > **Voice** > **Phone.**

STEP 5 Under **Supplementary Services** verify that **Secure Call Serv** is set to **yes**. (This feature can also be configured in the **User** tab under **Supplementary Services**.)

Secure Call Indication Tone

This tone is played when a call that 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.

To configure the tone, navigate to **Admin Login** > **advanced** > **Voice** > **Regional.** Under **Call Progress Tones**, enter the tone string in the Secure Call Indication Tone field. Defaults to 397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2). See **Scripting for Cadences, Call Progress Tones, and Ring Tones** for syntax information.

Configuring Voice Codecs

A codec resource is considered allocated if it has been included in the SDP codec list of an active call, even though it eventually might not be chosen for the connection. 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 G729a resource is already allocated (and since only one G.729a resource is allowed per IP phone), no other low-bit-rate codec can be allocated for subsequent calls. The only choices are G711a and G711u.

Since two G.723.1/G.726 resources are available per IP phone, you should disable the use of G.729a to guarantee support for two simultaneous G.723/G.726 codecs.

Negotiation of the optimal voice codec sometimes depends on the ability of the Cisco SPA IP phones to match a codec name with the far-end device or gateway codec name. Cisco SPA IP phones allow the network administrator to individually name the various codecs that are supported such that the correct codec successfully negotiates with the far-end equipment.

Note that Cisco SPA IP phones support voice codec priority. You can select up to three preferred codecs. The administrator can select the low-bit-rate codec used for each line. G.711a and G.711u are always enabled.

To configure the voice codecs on each extension, navigate to **Admin Login** > **advanced** > **Voice** > **Ext_n.** Under **Audio Configuration**, configure the following parameters:

Parameter	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 (all models) ▪ G711a (all models) ▪ G726-16 (not supported on Cisco WIP310, Cisco SPA525G or Cisco SPA525G2) ▪ G726-24 (not supported on Cisco WIP310, Cisco SPA525G or Cisco SPA525G2) ▪ G726-32 (all models) ▪ G726-40 (not supported on Cisco WIP310, Cisco SPA525G or Cisco SPA525G2) ▪ G729a (all models) ▪ G723 (not supported on Cisco WIP310, Cisco SPA525G or Cisco SPA525G2) ▪ G722 (not supported on Cisco WIP310) Defaults to G711u.
Use Pref Codec Only	To use only the preferred codecs for all calls, select **yes**. (The call fails if the far end does not support these codecs.) Otherwise, select **no**. Defaults to no.
Second Preferred Codec	If the first codec fails, this codec is tried. Defaults to **unspecified**. Not applicable to the Cisco WIP310.
Third Preferred Codec	If the second codec fails, this codec is tried. Defaults to **unspecified**. Not applicable to the Cisco WIP310.

Parameter	Description
G729a Enable	To enable the use of the G.729a codec at 8 kbps, select **yes**. Otherwise, select **no**. Defaults to yes.
G722 Enable	Enables use of the G.722 codec. Defaults to yes. Not applicable to the Cisco WIP310.
G723 Enable	To enable the use of the G.723a codec at 6.3 kbps, select yes. Otherwise, select no. Defaults to yes. Not applicable to the Cisco WIP310, Cisco SPA300 Series, Cisco SPA525G or Cisco SPA525G2.
G726-16 Enable	To enable the use of the G.726 codec at 16 kbps, select **yes**. Otherwise, select **no**. Defaults to yes. Not applicable to the Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
G726-24 Enable	To enable the use of the G.726 codec at 24 kbps, select **yes**. Otherwise, select **no**. Defaults to yes. Not applicable to the Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
G726-32 Enable	To enable the use of the G.726 codec at 32 kbps, select **yes**. Otherwise, select **no**. Defaults to yes.
G726-40 Enable	To enable the use of the G.726 codec at 40 kbps, select **yes**. Otherwise, select **no**. Defaults to yes. Not applicable to the Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
Release Unused Codec	To enable the release of codecs not used after codec negotiation on the first call so that other codecs can be used for the second line, select **yes**. Otherwise, select **no**. Defaults to yes.
DTMF Process AVT	Processes RTP DTMF events. When **yes** DTMF is relayed by using Named Telephony Events (NTEs) in Real-Time Transport Protocol (RTP) packets (RFC-2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals). Defaults to yes.

Parameter	Description
Silence Supp Enable	To enable silence suppression so that silent audio frames are not transmitted, select **yes**. Otherwise, select **no**. Defaults to no.
DTMF Tx Method	The method for transmitting DTMF signals to the far end. The options are: InBand, audio video transport (AVT), INFO, Auto, InBand+INFO, or AVT+INFO. ▪ InBand sends DTMF by using the audio path. ▪ AVT sends DTMF as AVT events. ▪ INFO uses the SIP INFO method. ▪ Auto uses InBand or AVT based on the outcome of codec negotiation. Defaults to Auto.
DTMF Tx Volume for AVT Packet	Allows you to manually configure the AVT Tx volume. The value of this parameter is inserted into the volume field of the payload in the AVT packet. Values are based on the AVT specification as described in RFC-2833, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*. According to RFC-2833, the volume field is represented by 6 bits, and describes the power level of the tone, expressed in dBm0 after dropping the sign. Valid range for this parameter is 0 to 63. If the provisioned value is negative, it is negated first. Thereafter, if the value is beyond the high limit of 63, it is clipped to 63. The default value is 0 and the recommended setting. However, some gateways do not accept this volume setting. If the gateway does not accept a value of 0, the DTMF tone is not relayed to the remote end. As a workaround for the phone to interoperate with those gateways, you can change the value to a value greater than 0.

Parameter	Description
Use Remote Pref Codec	To set the phone to communicate by using the remote phone-preferred codec, select **yes**. If set to **no**, the Cisco IP phone communicates by using its own preferred codec (as indicated in the **Preferred Codec** field and in the SDP by order of preferences). The default vale is no.
Codec Negotiation	When set to **Default**, the Cisco IP phone responds to an Invite with a 200 OK response advertising the preferred codec only. When set to **List All**, the Cisco IP phone responds listing all the codecs that the phone supports. The default value is Default.

Configuring Domain and Internet Settings

Configuring Restricted Access Domains

If you enter domains, the Cisco IP phones respond to SIP messages only from the identified servers.

To configure restricted access domains, navigate to **Admin Login** > **advanced** > **Voice** > **System.** Under **System Configuration** in the Restricted Access Domains field. Enter fully-qualified domain names (FQDNs) for each SIP server you want the phone to respond to. Separate FQDNs with semicolons. For example, `voiceip.com;voiceip1.com`.

Configuring DHCP, Static IP, or PPPoE Connection Type

You can set the connection type to one of the following:

- Dynamic Host Configuration Protocol (DHCP) receives an IP address from the network DHCP server. Cisco SPA IP phones typically operate in a network where a DHCP server assigns the devices their IP addresses. Because IP addresses are a limited resource, the DHCP server periodically renews the device lease on the IP address. If a phone loses its IP address for any reason, or if some other device on the network is assigned its IP address, the communication between the SIP proxy and the phone is either severed or degraded. Whenever an expected SIP response is not received within a programmable amount of time after the corresponding SIP command is sent, the *DHCP Timeout on Renewal* parameter causes the device to request a renewal of its IP address. If the DHCP server returns the IP address that it originally assigned to the phone, the DHCP assignment is presumed to be operating correctly. Otherwise, the phone resets to try to fix the issue.
- Static IP—A static IP address for the phone.
- PPPoE—Point-to-Point Protocol over Ethernet (PPPoE) connects users on an Ethernet network to the Internet through a common broadband medium, such as DSL line, wireless device, or cable modem. All users on an Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP that apply to serial connections.

To set the connection type, navigate to **Admin Login** > **advanced** > **Voice** > **System.** Under **Internet Connection Type** choose the Connection Type:

- Dynamic Host Configuration Protocol (DHCP)
- Static IP, and configure the following:
  - **Static IP Address** of the phone.
  - **Netmask** of the phone.
  - **Gateway** IP address

  If you are configuring a Cisco SPA525G or Cisco SPA525G2, also configure:
  - LAN MTU—LAN Maximum Transmission Unit size. Default value: 1500.
  - Duplex Mode—Choose the speed/duplex for the phone Ethernet ports: Auto, 10MBps/Duplex, 10MBps/Half, 100Mbps/Duplex, 100MBps/Half
- PPPoE (PPPoE is only available on the Cisco SPA525G or Cisco SPA525G2), and configure the following:

- PPPoE Login Name—The account name assigned by the ISP for connecting on a PPPoE link.
- PPPoE Login Password—The password assigned by the ISP.
- PPPoE Service Name—The service name assigned by the ISP.

The Cisco SPA301 or Cisco SPA501G can be configured by using the IVR. See **Using IVR on IP Phones Without Screens**.

Configuring Power Settings

The Power-over-Ethernet (PoE) requirements requested of a PoE switch by the phone can be Normal (default) or Maximum.

When one or more attendant consoles are attached to the phone, use Maximum to advertise to a PoE switch that the phone might consume up to 12 W.

When no attendant consoles are attached, use Normal to advertise a required power budget of 6.5 Watts.

To configure the (PoE) requirements, navigate to **Admin Login** > **advanced** > **Voice** > **System.** Under Power Setting select Normal or Maximum.

Setting Optional Network Servers

Optional network servers provide resources such as DNS lookup, network time, logging, and device discovery.

To configure the (PoE) requirements, navigate to **Admin Login** > **advanced** > **Voice** > **System.** Under **Optional Network Configuration** configure the following fields:

- Host Name—The host name of the phone.
- Domain—The network domain of the phone. If using LDAP see **Configuring LDAP for the Cisco SPA300 Series and Cisco SPA500 Series IP Phones**.
- Primary DNS—DNS server used by the phone in addition to the DHCP-supplied DNS servers (if DHCP is enabled), When DHCP is disabled, this is the primary DNS server. Defaults to 0.0.0.0. If using LDAP see **Configuring LDAP for the Cisco SPA300 Series and Cisco SPA500 Series IP Phones**.
- Secondary DNS—DNS server used by the phone in addition to the DHCP-supplied DNS servers (if DHCP is enabled), When DHCP is disabled, this is the secondary DNS server. Defaults to 0.0.0.0.

- DNS Server Order—Method for selecting the DNS server. The options are:
  - Manual—Enter the IP address of the DNS server manually; do not use the DHCP-supplied DNS table.
  - Manual/DHCP—Look for a manual entry of the IP address of the DNS server. Use the DHCP-supplied DNS table if it is not found.
  - DHCP/Manual—Use the DHCP-supplied DNS table. If not found, look for a manual entry of the IP address of the DNS server.

DNS Query Mode—Parallel or Sequential DNS query. A parallel DNS query sends the same DNS lookup request to all of the DNS servers at the same time. The first incoming reply is accepted by the phone. A sequential query polls the DNS servers in sequence. Defaults to parallel. Not available on Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.

Syslog Server—Syslog server name and port for logging system information and critical events. If both Debug Server and Syslog Server are specified, Syslog messages are also logged to the Debug Server.

Debug Server—Debug server name and port for logging debug information. The level of detailed output depends on the Debug Level.

Debug Level—The debug level ranges from 0 to 3. The higher the level, the more debug information is generated. Zero (0) means no debug information is generated. To log SIP messages, you must set the Debug Level to at least 2. Defaults to 0.

NTP Enable—Enables the Network Time Protocol (NTP). Applies to the Cisco SPA525G or Cisco SPA525G2 only.

Primary NTP Server—IP address or name of the primary NTP server used to synchronize its time. Defaults to blank.

Secondary NTP Server—IP address or name of the secondary NTP server used to synchronize its time. Defaults to blank.

Enable Bonjour—Bonjour is used by Office Manager and Cisco Configuration Assistant to discover the Cisco IP phones. Choose **yes** to enable or **no** to disable. Applies to the Cisco SPA525G or Cisco SPA525G2 only.

Configuring VLAN Settings

If you use a VLAN, your IP phone voice packets are tagged with the VLAN ID. (This section does not apply to the Cisco WIP310.)

Configuring Cisco Discovery Protocol (CDP)

CDP is negotiation-based and determines which VLAN the IP phone resides in. If you are using a Cisco switch, Cisco discovery protocol (CDP) is available and enabled by default. CDP:

- Obtains the protocol addresses of neighboring devices and discovers the platform of those devices.
- Shows information about the interfaces your router uses.
- Is media and protocol-independent.

If you are using a VLAN without CDP, you must enter a VLAN ID for the IP phone.

Configuring LLDP-MED

The Cisco SPA300 Series and Cisco SPA500 Series IP phones support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) for deployment with Cisco or other third-party network connectivity devices that use a Layer 2 auto-discovery mechanism. Implementation of LLDP-MED is done in accordance with IEEE 802.1AB (LLDP) Specification of May 2005, and ANSI TIA-1057 of April 2006.

Cisco SPA IP phones operate as LLDP-MED Media End Point Class III devices with direct LLDP-MED links to Network Connectivity Devices, according to the Media Endpoint Discovery Reference Model and Definition (ANSI TIA-1057 Section 6).

Cisco SPA IP phones support only the following limited set of TLVs as LLDP-MED Media Endpoint device class III:

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- Port Description TLV
- System Name TLV
- System Capabilities TLV

- IEEE 802.3 MAC/PHY Configuration/Status TLV (for wired network only)
- LLDP-MED Capabilities TLV
- LLDP-MED Network Policy TLV (for application type=Voice only)
- LLDP-MED Extended Power-Via-MDI TLV (for wired network only)
- LLDP-MED Firmware Revision TLV
- End of LLDPDU TLV

The outgoing LLDPDU contains all the above TLVs when if applicable. For the incoming LLDPDU, the LLDPDU is discarded if any of the following TLVs are missing. All other TLVs are not validated and ignored.

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- LLDP-MED Capabilities TLV
- LLDP-MED Network Policy TLV (for application type=Voice only)
- End of LLDPDU TLV

The phone sends out the shutdown LLDPDU if applicable. The LLDPDU frame contains the following TLVs:

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- End of LLDPDU TLV

There are some restrictions in the implementation of LLDP-MED on the Cisco IP Phones:

- Storage and retrieval of neighbor information is not supported.
- SNMP and corresponding MIBs are not supported.
- Recording and retrieval of statistical counters are not supported.

- There is no full validation of all TLVs; TLVs that do not apply to the phones are ignored.
- Protocol state machines as stated in the standards are only used for reference.

TLV Information

These sections provide the TLV information.

Chassis ID TLV

For the outgoing LLDPDU, the TLV supports sub-type=5 (Network Address). When IP address is known, the value of Chassis ID is an octet of the INAN address family number followed by the octet string for the IPv4 address used for voice communication. If the IP address is unknown, the value for Chassis ID is 0.0.0.0. The only INAN address family supported is IPv4. Currently, IPv6 address for the Chassis ID is not supported. For the incoming LLDPDU, the Chassis ID is treated as an opaque value to form MSAP identifier. The value is not validated against its sub-type. The Chassis ID TLV is mandatory as the first TLV. Only one Chassis ID TLV is allowed for the outgoing and incoming LLDPDUs.

Port ID TLV

For the outgoing LLDPDU, the TLV supports sub-type=3 (MAC address). The 6 octet MAC address for the Ethernet port is used for the value of Port ID in wired or wireless mode. For the incoming LLDPDU, the Port ID TLV is treated as an opaque value to form the MSAP identifier. The value is not validated against its sub-type. The Port ID TLV is mandatory as the second TLV. Only one Port ID TLV is allowed for the outgoing and incoming LLDPDUs.

Time to Live TLV

For the outgoing LLDPDU, the Time to live TTL value is 180 seconds. This is different from 120 seconds as recommended by the standard. For the shutdown LLDPDU, the TTL value is always 0. The Time to Live TLV is mandatory as the third TLV. Only one Time to Live TLV is allowed for the outgoing and incoming LLDPDUs.

End of LLDPDU TLV

The value is 2-octet, all zero. This TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs.

Port Description TLV

For the outgoing LLDPDU, in the Port Description TLV, the value for the port description is the same as “Port ID TLV” for CDP. The incoming LLDPDU, the Port Description TLV, is ignored and not validated. Only one Port Description TLV is allowed for outgoing and incoming LLDPDUs.

System Name TLV

For the outgoing LLDPDU, in the System Name TLV, the value is the same as ‘Platform TLV” for CDP. For the Cisco SPA525G2, the name is “SPA525G2.” The incoming LLDPDU, the System Name TLV, is ignored and not validated. Only one System Name TLV is allowed for the outgoing and incoming LLDPDUs.

System Capabilities TLV

For the outgoing LLDPDU, in the System Capabilities TLV, the bit values for the 2 octet system capabilities field should be set for Bit 2 (Bridge) and Bit 5 (Phone) for a phone with a PC port. If the phone does not have a PC port, only Bit 5 should be set. The same system capability value should be set for the enabled capability field. For the incoming LLDPDU, the System Capabilities TLV is ignored. The TLV is not validated semantically against the MED device type. The System Capabilities TLV is mandatory for outgoing LLDPDUs. Only one System Capabilities TLV is allowed.

IEEE 802.3 MAC/PHY Configuration/Status TLV

The TLV is not for auto-negotiation, but for troubleshooting purposes. For the incoming LLDPDU, the TLV is ignored and not validated. For the outgoing LLDPDU, for the TLV, the octet value auto-negotiation support/status should be:

- Bit 0—Set to 1 to indicate the auto-negotiation support feature is supported.
- Bit 1—Set to 1 to indicate auto-negotiation status is enabled.
- Bit 2-7—Set to 0.

The bit values for the 2 octets PMD auto-negotiation advertised capability field should be set to:

- Bit 13—10BASE-T half duplex mode
- Bit 14—10BASE-T full duplex mode
- Bit 11—100BASE-TX half duplex mode
- Bit 10—100BASE-TX full duplex mode
- Bit 15—Unknown

Bit 10, 11, 13 and 14 should be set.

The value for 2 octets operational MAU type should be set to reflect the real operational MAU type:

- 16—100BASE-TX full duplex
- 15—100BASE-TX half duplex
- 11—10BASE-T full duplex
- 10—10BASE-T half duplex

For example, in most cases, the phone is set to 100BASE-TX full duplex. The value 16 should then be set. The TLV is optional for a wired network and not applicable for a wireless network. The phone will send out this TLV only when in wired mode. When the phone is not set for auto-negotiation but specific speed/duplexity, for the outgoing LLDPDU TLV, bit 1 for the octet value auto-negotiation support/status should be clear (0) to indicate auto-negotiation is disabled. The 2 octets PMD auto-negotiation advertised capability field should be set to 0x8000 to indicate unknown. The Cisco SPA525G/525G2 allows the administrator to set the switch operational mode to auto-negotiation or to a specific speed/duplexity.

LLDP-MED Capabilities TLV

For the outgoing LLDPDU, the TLV should have the device type 3 (End Point Class III) and with the following bits set for 2-octet Capability field:

Bit Position	Capability
0	LLDP-MED Capabilities
1	Network Policy
4	Extended Power via MDI-PD
5	Inventory

For the incoming TLV, if the LLDP-MED TLV is not present, the LLDPDU is discarded. The LLDP-MED Capabilities TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs. Any other LLDP-MED TLVs will be ignored if they present before the LLDP-MED Capabilities TLV.

Network Policy TLV

Outgoing LLDPDU—The phone will send out only one Network Policy TLV with the Application Type Value set to 1 (Voice). Before the VLAN or DSCP is determined, the Unknown Policy Flag (U) is set to 1. If the VLAN setting or DSCP is known, the value is set to 0. When the policy is unknown, all other values are set to 0. Before the VLAN is determined or used, the Tagged Flag (T) is set to 0. If the tagged VLAN (VLAN ID > 1) is used for the phone, the Tagged Flag (T) is set to 1. Reserved (X) is always set to 0. If the VLAN is used, the corresponding VLAN ID and L2 Priority will be set accordingly. VLAN ID valid value is range from 1-4094. However, VLAN ID=1 will never be used (limitation). If DSCP is used, the value range from 0-63 is set accordingly.

Incoming LLDPDU—Multiple Network Policy TLVs for different application types are allowed. The phone will only support and interpret the TLV with the application type=1 (Voice). TLVs for other application types are ignored and not validated.

LLDP-MED Extended Power-Via-MDI TLV

In the TLV for the outgoing LLDPDU, the binary value for Power Type is set to “0 1” to indicate the power type for phone is PD Device. The Power source for the phone is set “PSE and local” with binary value “1 1”. The Power Priority is set to binary “0 0 0 0” to indicate unknown priority while the Power Value is set to maximum power value based on phone type:

Phone Type	Power Value
Cisco SPA525G or Cisco SPA525G2	125
Cisco SPA500 Series	120
Cisco SPA300 Series	100

For the incoming LLDPDU, the TLV is ignored and not validated. Only one TLV is allowed in the outgoing and incoming LLDPDUs. The phone will send out the TLV for wired network only.

The LLDP-MED standard was originally drafted in the context of Ethernet. Discussion is ongoing for LLDP-MED for Wireless Networks. Refer to ANSI-TIA 1057, Annex C, C.3 Applicable TLV for VoWLAN, table 24. It is recommended that the TLV is not applicable in the context of the wireless network. This TLV is targeted for use in the context of PoE and Ethernet. The TLV, if added, will not provide any value for network management or power policy adjustment at the switch.

LLDP-MED Inventory Management TLV

This TLV is optional for Device Class III. For the outgoing LLDPDU, we support only Firmware Revision TLV. The value for the firmware revision is the firmware version. For the incoming LLDPDU, the TLVs are all ignored and not validated. Only one Firmware Revision TLV is allowed for the outgoing and incoming LLDPDUs.

Final Network Policy Resolution and QoS For the Phone

The following sections describe network policy and QoS for the IP phones.

Special VLANs

VLAN=0, VLAN=1 and VLAN=4095 are treated the same way as an untagged VLAN. As the VLAN is untagged, CoS is not applicable.

Default QoS for SIP Mode

If there is no network policy from CDP or LLDP-MED, the default network policy is used. CoS is based on configuration for the specific extension. It is applicable only if the manual VLAN is enabled and manual VLAN ID is not equal to 0, 1, or 4095. ToS is based on configuration for the specific extension.

Default QoS for SPCP Mode

If there is no network policy from CDP or LLDP-MED, the default network policy is used. CoS is based on a pre-defined value of 5. It is applicable only if the manual VLAN is enabled and manual VLAN ID is not equal to 0, 1, or 4095. ToS is based on precedence value from the StartMediaTransmission Message from the Unified Communications 500 Series for the Cisco SPA525G/525G2. However, ToS is based on the value specified for the specific extension in the web administration interface for the Cisco SPA50X IP phone.

QoS Resolution for CDP

If there is a valid network policy from CDP:

- If the VLAN=0, 1 or 4095, the VLAN will not be set, or the VLAN is untagged. CoS is not applicable, but DSCP is applicable. ToS is based on the default as previously described.
- If the VLAN > 1 and VLAN< 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.
- For the Cisco SPA525G/525G2, when the VLAN is changed, the user sees the voice component refreshed when the IP address is changed. For the Cisco SPA50X, the phone reboots and restarts the fast start sequence.

QoS Resolution for LLDP-MED

If CoS is applicable and if CoS=0, the default will be used for the specific extension as previously described. But the value shown on L2 Priority for TLV for outgoing LLDPDU is based on value used for extension 1. If CoS is applicable and if CoS != 0, CoS will be used for all extensions.

If DSCP (mapped to ToS) is applicable and if DSCP=0, the default will be used for the specific extension as previously described. But the value show on DSCP for TLV for outgoing LLDPDU is based on value used for the extension 1. If DSCP is applicable and if DSCP != 0, DSCP will be used for all extensions.

If the VLAN > 1 and VLAN < 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.

If there is a valid network policy for voice application from LLDP-MED PDU and if the tagged flag is set, the VLAN, L2 Priority (CoS) and DSCP (mapped to ToS) are all applicable.

If there is a valid network policy for voice application from LLDP-MED PDU and if the tagged flag is not set, only the DPSC (mapped to ToS) is applicable.

For the Cisco SPA525G/525G2, when the VLAN is changed, the user sees the voice component refreshed when IP address is changed. For the Cisco SPA50X, the phone reboots and restarts the fast start sequence.

Co-Existence with CDP

If both CDP and LLDP-MED are enabled, the network policy for the VLAN is determined by the last policy set or changed with either one of the discovery modes. If both LLDP-MED and CDP are enabled, during startup, the phone sends both CDP and LLDP-MED PDUs at the same time.

Inconsistent configuration and behavior for network connectivity devices for CDP and LLDP-MED modes could result in an oscillating rebooting behavior for the phone due to switching to different VLANs.

If the VLAN is not set via CDP and LLDP-MED, the VLAN ID that is configured manually is used. If the VLAN ID is not configured manually, no VLAN will be supported. DSCP is used and the network policy is determined by LLDP-MED if applicable.

Wireless LAN Environments

Network policy for the VLAN feature is not supported for wireless networks. The Wireless AP or Wireless router must be enabled for LLDP-MED as the Network Connectivity Device. The DSCP portion for network policy from Wireless AP/ Router will be supported if enabled.

LLDP-MED and Multiple Network Devices

If the same application type is used for network policy but different Layer 2 or Layer 3 QoS Network policies are received by the phones from multiple network connectivity devices, the last valid network policy is honored. To ensure deterministic and consistent of Network Policy, multiple network connectivity devices should not send out conflicting network policies for the same application type.

LLDP-MED and IEEE 802.X

The phones do not support IEEE 802.X and will not work in a 802.1X wired environment. However, IEEE 802.1X or Spanning Tree Protocols on network devices could result in delay of fast start response from switches.

Configuring the VLAN Settings

To configure VLAN settings, navigate to **Admin Login** > **advanced** > **Voice** > **System.** Under **VLAN Settings**, configure the following parameters:

Parameter	Description
Enable VLAN	Choose **Yes** to enable VLAN. Choose **no** to disable.
VLAN ID	If you use a VLAN without Cisco Discovery Protocol (CDP) (VLAN enabled and CDP disabled), enter a *VLAN ID* for the IP phone. Note that only voice packets are tagged with the VLAN ID. Do not use **1** for the VLAN ID.
PC Port VLAN Highest Priority	Choose **No Limit**, or **0**-**7** (default 0). The highest priority is 7. The priority applied to all frames, tagged and untagged. The phone modifies the frame priority only if the incoming frame priority is higher than this value.

Parameter	Description
Enable PC Port VLAN Tagging	Enables VLAN and priority tagging on the phone data port (802.1p/q). This feature facilities tagging of the VLAN ID (802.1Q) and priority bits (802.1p) of the traffic coming from the PC port of the IP phone. Choose **Yes** to enable the tagging algorithm. Defaults to No.
PC Port VLAN ID	The phone tags all of the untagged frames coming from the PC. (It does not tag frames with existing tags). Ranges from 0 to 4095. Defaults to 0.
Enable CDP	Enable CDP only if you are using a switch that has CDP. CDP is negotiation-based and determines on which VLAN the IP phone resides.
Enable LLDP-MED	Choose **yes** to enable LLDP-MED for the phone to advertise itself to devices that use that discovery protocol. (By default, this setting is enabled.) When the LLDP-MED feature is enabled, after the phone has initialized and Layer 2 connectivity is established, the phone sends out LLDP-MED PDU frames. If the phone receives no acknowledgment, the manually configured VLAN or default VLAN is used if applicable. If CDP is used concurrently, a waiting period of 6 seconds is used. The waiting period increases the overall startup time for the phone.
Network Startup Delay	Enter the delay in seconds for the switch to get to the forwarding state before the phone sends out the first LLDP-MED packet. The default delay is 3 seconds. For configuration of some switches, it might be necessary to increase this value to a higher value for LLDP-MED to work. Configuring a delay can be important for networks that use Spanning Tree Protocol.

Configuring SSL VPN on the Cisco SPA525G or Cisco SPA525G2

The Cisco SPA525G or Cisco SPA525G2 can be used in a virtual private network (VPN) to allow users secure access to the office phone network from remote locations or to connect the Internet and use VPN to access the company phone network. This feature works on the Cisco SPA525G or Cisco SPA525G2 using either SIP or SPCP.

The phone works with the Cisco AnyConnect VPN client and the following VPN devices:

- Cisco 500 Series Secure Router
- Cisco 5500 Series Adaptive Security Appliance
- Cisco Unified Communications 520 Series

You must configure the SSL VPN device to ensure proper routing of voice data by using VLAN and QoS at the end of the SSL VPN server. The following restrictions apply:

- HTTP proxy is not supported.
- SSL client certificate verification is not supported.
- CDP and VLAN tagging and QoS for the voice and PC port are not supported on the SSL VPN tunnel.

Because using VPN requires internal phone resources, performance can suffer if using memory-intensive applications or configurations on the phone when the phone is connected to the VPN. The following restrictions apply:

- Only the G.711 Audio Codec is supported.
- SRTP for secured audio is not supported.
- Video monitoring is not supported.

To configure and use the Cisco SPA525G or Cisco SPA525G2 on a VPN, you must do the following:

1. Configure the VPN on the VPN server by using Cisco AnyConnect VPN client software.
2. Configure the VPN administrative settings on the IP phone by using the phone web user interface.

3. Configure the VPN user settings using the phone web user interface or on the IP phone by using the IP phone screen.

Configuring the VPN on the Security Appliance

This configuration is for example purposes. Specific configuration instructions are not presented in this document. For detailed instructions for your particular device, see the application notes in the Cisco Small Business Support Community.

STEP 1 Download the Cisco AnyConnect VPN client software from Cisco.com and install it on the VPN server.

STEP 2 Download a Cisco IOS version that supports this feature and install it on the VPN server.

STEP 3 Configure SSL VPN on the VPN server.

STEP 4 Ensure the VPN is functional and you can connect to the VPN by using the Cisco AnyConnect VPN client.

Configuring the VPN on the Cisco SPA525G or Cisco SPA525G2

The phone obtains its software load from a TFTP server when the phone either boots in SPCP mode (if the **Connect on Bootup** field on the phone is set to **yes**), or connects to the VPN manually (as a result of a user pressing **Connect** on the phone under the **Network Configuration** > **VPN** menu).

Administrator Settings

If the phone will be connecting to the VPN by using SPCP:

STEP 1 Navigate to **Admin Login** > **advanced** > **Voice** > **System.**

STEP 2 Under **Optional Network Configuration,** from the Alternate TFTP list choose **yes**.

STEP 3 In the TFTP Server field, enter the IP address of the Cisco Unified Communications 500 Series server.

STEP 4 Click **Submit All Changes**.

User Settings

Enter the user settings for the phone, using either the phone web user interface or the phone itself:

STEP 1 Navigate to **Admin Login** > **advanced** > **Voice** > **System.** (Not applicable to the Cisco SPA525G or Cisco SPA525G2 in SPCP mode.)

STEP 2 Under VPN Settings, enter the following:

- In the VPN Server field, enter the IP address of the VPN server.
- In the VPN User Name and Password fields, enter the username and password to log in to the VPN server. These were created when you set up the VPN on the server.
- (Optional) Enter the VPN tunnel group, if required by your VPN server.
- (Optional) To connect to the VPN when the phone is powered on, in the **Connect on Bootup** field, choose **yes**.

STEP 3 Click **Submit All Changes**. If you did not choose **yes** in the **Connect on Bootup** field, connect to the VPN on the phone by pressing the **Setup** button and choosing **Network Configuration** > **VPN** > **Connect**.

To use the phone interface:

STEP 1 On the phone, press the **Setup** button.

STEP 2 Scroll to **Network Configuration** and press **Select**.

STEP 3 Scroll to **Web Server** and ensure that it is enabled. Press the right arrow key if it is not enabled.

If the option to edit the parameter is not displayed, press **# to display the option. If the edit option still does not display, it might be set by your phone system administrator such that you cannot modify this parameter.

STEP 4 Scroll to VPN and press the right arrow key.

STEP 5 Under VPN server, enter the IP address of the VPN server.

STEP 6 Enter the username to log in to the VPN server.

STEP 7 Enter the password for the user.

STEP 8 (Optional) Enter the tunnel group, if this is required by the VPN server.

STEP 9 (Optional) To connect to the VPN when the phone is powered on, ensure that **Connect on Bootup** is enabled.

STEP 10 To connect to the VPN, ensure that **Connect** is enabled.

STEP 11 Press **Save**. After the VPN connection is established, a VPN icon appears in the upper right of the IP phone screen.

To view the VPN status, either:

- Use the phone web user interface:
  - Click **Admin Login** and **advanced**. (Not applicable to the Cisco SPA525G or Cisco SPA525G2 in SPCP mode.) Click the **Info** tab.
- Use the phone menu:
  - Press the **Setup** button. Scroll to **Status** and press **Select**. Scroll to **VPN Status** and press **Select**.

6

Provisioning

Phones can be *provisioned* to download configuration profiles or updated firmware from a remote server when they are connected to a network, when they are powered up, and at set intervals. Provisioning is typically part of high-volume, Voice-over-IP (VoIP) deployments and limited to service providers. Configuration profiles or updated firmware are transferred to the device by using TFTP, HTTP, or HTTPS.

The Cisco IP phones accept configuration profiles in XML format, or in a proprietary binary format generated by the SIP Profile Compiler (SPC) available from Cisco. The Cisco IP phones support 256-bit symmetric key encryption to secure the XML content of the profiles. SPC compiled binary profiles can be encrypted when they are complied. Since firmware does not contain sensitive personal information, typically it is not encrypted.

Provisioning is described in detail in the *Cisco Small Business IP Telephony Devices Provisioning Guide*.

This chapter describes:

- **Redundant Provisioning Servers**
- **Retail Provisioning**
- **Automatic In-House Preprovisioning**
- **Using HTTPS**
- **Manually Provisioning a Phone from the Keypad**
- **Updating Profiles and Firmware**
- **Configuring a Custom Certificate Authority**
- **General Purpose Parameters**

Additional information is available in:

- *Cisco SPA3xx, SPA50xG, and SPA525G SPC Templates for Configuration Files*, available on the Cisco Support Community at:

  https://supportforums.cisco.com/docs/DOC-10008

- Cisco SPA9000 Administration Guide

Redundant Provisioning Servers

The provisioning server may be specified as an IP address or as a fully qualified domain name (FQDN). The use of a FQDN facilitates the deployment of redundant provisioning servers. When the provisioning server is identified through a FQDN, the Cisco IP phone attempts to resolve the FQDN to an IP address through DNS. Only DNS A-records are supported for provisioning; DNS SRV address resolution is not available for provisioning. The Cisco IP phone continues to process A-records until the first server responds. If no server associated with the A-records responds, the Cisco IP phone logs an error to the syslog server.

Retail Provisioning

The Cisco IP phone includes the web-based phone web user interface that displays internal configuration and accepts new configuration parameter values. The server also accepts a special URL command syntax for performing remote profile resync and firmware upgrade operations.

In a retail distribution model, a customer purchases a Cisco voice endpoint device, and subsequently subscribes to a particular service. The customer first signs on to the service and establishes a VoIP account, possibly through an online portal. Subsequently, the customer binds the particular device to the assigned service account.

To do so, the unprovisioned Cisco IP phone is instructed to resync with a specific provisioning server through a resync URL command. The URL command typically includes an account PIN number or alphanumeric code to associate the device with the new account.

In the following example, a device at the DHCP-assigned IP address 192.168.1.102 is instructed to provision itself to the SuperVoIP service:

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/
1234abcd
```

In this example, 1234abcd is the PIN number of the new account. The remote provisioning server is configured to associate the Cisco IP phone that is performing the resync request with the new account, based on the URL and the supplied PIN. Through this initial resync operation, the Cisco IP phone is configured in a single step, and is automatically directed to resync thereafter to a permanent URL on the server. For example:

```
https://prov.supervoip.com/cisco-init
```

For both initial and permanent access, the provisioning server relies on the Cisco IP phone client certificate for authentication and supplies correct configuration parameter values based on the associated service account.

Automatic In-House Preprovisioning

Using the phone web user interface and issuing a resync URL is convenient for a customer in the retail deployment model, but it is not as convenient for preprovisioning a large number of units.

The Cisco IP phone supports a more convenient mechanism for in-house preprovisioning. With the factory default configuration, a Cisco IP phone automatically tries to resync to a specific file on a TFTP server, whose IP address is offered as one of the DHCP-provided parameters. This lets a service provider connect each new Cisco IP phone to a LAN environment configured to preprovision phones. Any new Cisco IP phone connected to this LAN automatically resyncs to the local TFTP server, initializing its internal state in preparation for deployment. Among other parameters, this preprovisioning step configures the URL of the Cisco IP phone provisioning server.

Subsequently, when a new customer signs up for service, the preprovisioned Cisco IP phone can be simply bar-code scanned, to record its MAC address or serial number, before being shipped to the customer. Upon receiving the unit, the customer connects the unit to the broadband link. On power-up the Cisco IP phone already knows the server to contact for its periodic resync update.

Using HTTPS

The Cisco IP phone provides a reliable and secure provisioning strategy based on HTTPS requests from the Cisco IP phone to the provisioning server, using both server and client certificates for authenticating the client to the server and the server to the client.

To use HTTPS with Cisco IP phones, you must generate a Certificate Signing Request (CSR) and submit it to Cisco. The Cisco IP phone generates a certificate for installation on the provisioning server that is accepted by Cisco IP phones when they seek to establish an HTTPS connection with the provisioning server.

The Cisco IP phone implements up to 256-bit symmetric encryption, using the American Encryption Standard (AES), in addition to 128-bit RC4. The Cisco IP phone supports the Rivest, Shamir, and Adelman (RSA) algorithm for public/private key cryptography.

Server Certificates

Each secure provisioning server is issued an secure sockets layer (SSL) server certificate, directly signed by Cisco. The firmware running on the Cisco IP phone clients recognizes only these certificates as valid. The clients try to authenticate the server certificate when connecting via HTTPS, and reject any server certificate not signed by Cisco.

This mechanism protects the service provider from unauthorized access to the Cisco IP phone endpoint, or any attempt to spoof the provisioning server. This might allow the attacker to reprovision the Cisco IP phone to gain configuration information, or to use a different VoIP service. Without the private key corresponding to a valid server certificate, the attacker is unable to establish communication with a Cisco IP phone.

Client Certificates

In addition to a direct attack on the Cisco IP phone, an attacker might attempt to contact a provisioning server using a standard web browser, or other HTTPS client, to obtain the Cisco IP phone configuration profile from the provisioning server. To prevent this kind of attack, each Cisco IP phone also carries a unique client certificate, also signed by Cisco, including identifying information about each individual endpoint. A certificate authority root certificate capable of authenticating the device client certificate is given to each service provider. This authentication path allows the provisioning server to reject unauthorized requests for configuration profiles.

Obtaining a Server Certificate

To obtain a server certificate:

STEP 1 Contact a Cisco support person who will work with you on the certificate process. If you are not working with a specific support person, you can email your request to ciscosb-certadmin@cisco.com.)

STEP 2 Generate a private key that will be used in a CSR (Certificate Signing Request). This key is private and you do not need to provide this key to Cisco support. Use open source “openssl” to generate the key. For example:

```
openssl genrsa -out <file.key> 1024
```

STEP 3 Generate CSR a that contains fields that identify your organization, and location. For example:

```
openssl req -new -key <file.key> -out <file.csr>
```

You must have the following information:

- Subject field—Enter the Common Name (CN) that must be a FQDN (Fully Qualified Domain Name) syntax. During SSL authentication handshake, the SPA 9000 verifies that the certificate it receives is from the machine that presented it.
- Server's hostname—For example, provserv.domain.com.
- Email address—Enter an email address so that customer support can contact you if needed. This email address is visible in the CSR.

STEP 4 Email the CSR (in zip file format) to the Cisco support person or to ciscosb-certadmin@cisco.com. The certificate is signed by Cisco and given to you.

Manually Provisioning a Phone from the Keypad

Typically Cisco SPA IP phones are configured to be provisioned when first connected to the network and at configured intervals that are set when the phone is preprovisioned (configured) by the service provider or the VAR. Service providers can authorize VARs or advanced users to manually provision Cisco SPA IP phones by using the phone keypad.

The status of the provisioning process is indicated by the phone mute button blinking in the following patterns:

- Red/orange slow blink (1.0 seconds on, 1.0 seconds off): Contacting server, server not resolvable, not reachable, or down.
- Red/orange fast blink (0.2 seconds on, 0.2 seconds off, 0.2 seconds on, 1.4 seconds off): Server responded with file not found or corrupt file.

To manually provision the phone by using the keypad:

Cisco SPA303 and Cisco SPA5XXG

STEP 1 Press **Setup**, then scroll to **Profile Rule**.

STEP 2 Enter the profile rule by using the following format:

protocol://server[:port]/profile_pathname

For example:

`tftp://192.168.1.5/spa504.cfg`

If no protocol is specified, TFTP is assumed. If no server-name is specified, the host that requests the URL is used as the server name. If no port is specified, the default port is used (69 for TFTP, 80 for HTTP, or 443 for HTTPS).

STEP 3 Press the **Resync** softkey.

Cisco WIP310

STEP 1 Press **Select** to choose Settings and press **Select** again.

STEP 2 Navigate to Misc Settings.

STEP 3 Navigate to profile rule. Enter the profile rule in the following format:

protocol://server[:port]/profile_pathname

For example, to have the Cisco WIP310 provisioning done by a Cisco SPA9000, enter:

```
192.168.2.64/cfg/generic.xml
```

STEP 4 Press the **Resync** softkey.

Cisco SPA525G or Cisco SPA525G2

STEP 1 Press the **Setup** button.

STEP 2 Navigate to Device Administration and press **Select**.

STEP 3 Scroll to Profile Rule and press **Select**.

STEP 4 Enter the profile rule by using the following format.

protocol://server[:port]/profile_pathname

For example:

```
tftp://192.168.1.5/spa525.cfg
```

STEP 5 Press the **Resync** softkey.

Sample Configuration File

Following is a sample configuration file:

```
Set_Local_Date_(mm/dd) "" ;
Set_Local_Time_(HH/mm) "" ;
Time_Zone "GMT-07:00" ; # options: GMT-12:00/GMT-11:00/GMT-10:00/GMT-09:00/
GMT-08:00/GMT-07:00/GMT-06:00/GMT-05:00/GMT-04:00/GMT-03:30/GMT-03:00/GMT-
02:00/GMT-01:00/GMT/GMT+01:00/GMT+02:00/GMT+03:00/GMT+03:30/GMT+04:00/
GMT+05:00/GMT+05:30/GMT+05:45/GMT+06:00/GMT+06:30/GMT+07:00/GMT+08:00/
GMT+09:00/GMT+09:30/GMT+10:00/GMT+11:00/GMT+12:00/GMT+13:00
```

```
FXS_Port_Impedance "600" ; # options: 600/900/600+2.16uF/900+2.16uF/
270+750||150nF/220+820||120nF/220+820||115nF/370+620||310nF
FXS_Port_Input_Gain "-3" ;
FXS_Port_Output_Gain "-3" ;
DTMF_Playback_Level "-16" ;
DTMF_Playback_Length ".1" ;
Detect_ABCD "Yes" ;
Playback_ABCD "Yes" ;
Caller_ID_Method "Bellcore(N.Amer,China)" ; # options:
Bellcore(N.Amer,China)/DTMF(Finland,Sweden)/DTMF(Denmark)/ETSI DTMF/ETSI
DTMF With PR/ETSI DTMF After Ring/ETSI FSK/ETSI FSK With PR(UK)
FXS_Port_Power_Limit "3" ; # options: 1/2/3/4/5/6/7/8
Protect_IVR_FactoryReset “No” ;
```

Updating Profiles and Firmware

Cisco IP phones support secure remote provisioning (configuration) and firmware upgrades. An unprovisioned Cisco IP phone can receive an encrypted profile specifically targeted for that device without requiring an explicit key by using a secure first-time provisioning mechanism using SSL functionality.

User intervention is not required to initiate or complete a profile update or firmware upgrade. If intermediate upgrades are required to reach a future upgrade state from an older release, the Cisco IP phone upgrade logic is capable of automating multi-stage upgrades. A profile resync is only attempted when the Cisco IP phone is idle, because this might trigger a software reboot and disconnect a call.

General purpose parameters manage the provisioning process. Each Cisco IP phone can be configured to periodically contact a normal provisioning server (NPS). Communication with the NPS does not require the use of a secure protocol because the updated profile is encrypted by a shared secret key. The NPS can be a standard TFTP, HTTP or HTTPS server with client certificates.

The administrator can upgrade, reboot, restart, or resync Cisco IP phones by using the phone web user interface. The administrator can also perform these tasks by using a SIP notify message.

Configuration profiles are generated by using common, open-source tools that integrate with service provider provisioning systems. (Provisioning is described in detail in the *Cisco Small Business IP Telephony Devices Provisioning Guide*.)

Allow and Configure Profile Updates

The profile updates can be allowed at specified intervals. Updated profiles are sent from a server to the phone by using a TFTP or HTTP.

To configure a profile update:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Provisioning**.

STEP 2 Under **Configuration Profile** in the Provision Enable field, choose **yes**.

STEP 3 Enter the parameters defined in the table:

Parameter	Description
Provision Enable	Allows or denies resync actions. Defaults to **yes**.
Resync On Reset	The device performs a resync operation after power-up and after each upgrade attempt when set to **yes**.
Resync Random Delay	A random delay following the boot-up sequence before performing the reset, specified in seconds. In a pool of IP Telephony devices that are scheduled to simultaneously powered up, this introduces a spread in the times at which each unit sends a resync request to the provisioning server. This feature can be useful in a large residential deployment, in the case of a regional power failures.
Resync At (HHmm)	Time in 24-hour format (hhmm) to resync the device.
Resync At Random Delay	To avoid flooding the server with simultaneously resync requests from multiple phones set to resync at the same time, the phone triggers the resync up to ten minutes after the specified time. If this parameter is provisioned, the Resync Periodic parameter is ignored.
Resync Periodic	Time in seconds between periodic resynchs. If this value is empty or zero, the device does not resync periodically.

Parameter	Description
Resync Error Retry Delay	If a resync operation fails because the IP Telephony device was unable to retrieve a profile from the server, if the downloaded file is corrupt, or an internal error occurs, the device tries to resync again after a time specified in seconds. If the delay is set to 0, the device does not try to resync again following a failed resync attempt.
Forced Resync Delay	The resync typically takes place when the voice lines are idle. When a voice line is active and a resync is due, the IP Telephony device delays the resync procedure until the line becomes idle. However, it waits no longer than the Forced Resync Delay (seconds). A resync might cause configuration parameter values to change. This causes a firmware reboot and terminates any voice connection active at the time of the resync.
Resync From SIP	Controls requests for resync operations by using a SIP NOTIFY event sent from the service provider proxy server to the device. When set to **yes**, the proxy can request a resync by sending a SIP NOTIFY message containing the `Event: resync` header to the device.
Resync After Upgrade Attempt	Requests a resync of the device after a failed upgrade attempt.
Resync Trigger 1 Resync Trigger 2	A conditional expression (that undergoes macro expansion). If the condition in one of these triggers evaluates to true, a resync operation is initiated as though the periodic resync timer had expired.
Resync Fails On FNF	A resync is considered unsuccessful if a requested profile is not received from the server. This can be overridden by this parameter. When it is set to **no**, the device accepts a `file-not-found` response from the server as a successful resync.

Parameter	Description
Profile Rule Profile Rule B Profile Rule C Profile Rule D	Remote configuration profile rules evaluated in sequence. Each resync operation can retrieve multiple files, potentially managed by different servers.
DHCP Option To Use	DHCP options, delimited by commas, used to retrieve firmware and profiles.
Transport Protocol	The transport protocol used to retrieve firmware and profiles. If none is selected, TFTP is assumed and the IP address of the TFTP server is obtained from the DHCP server.
Log Resync Request Msg	The message sent to the syslog server at the start of a resync attempt. The default value is: `$PN $MAC –Requesting resync $SCHEME:// $SERVIP:$PORT$PATH`
Log Resync Success Msg	The syslog message issued upon successful completion of a resync attempt. The default value is: `$PN $MAC –Successful resync $SCHEME:// $SERVIP:$PORT$PATH -- $ERR.`
Log Resync Failure Msg	The syslog message that is issued after a failed resync attempt. The default value is: `$PN $MAC – Resyncfailed: $ERR.`
Report Rule	The device provides a mechanism for reporting its current internal configuration to the provisioning server. The URL in this field specifies the destination for a report and can include an encryption key.
User Configurable Resync	Allows a user resynch the phone from the IP phone screen.

Allow and Configure Firmware Updates

The firmware updates can be allowed at specified intervals. Updated firmware is sent from a server to the phone by using a TFTP or HTTP. Security is less of an issue with a firmware upgrade, because firmware does not contain personal information.

To configure a firmware update:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Provisioning**.

STEP 2 Under **Firmware Upgrade** in the Upgrade Enable field, choose **yes**.

STEP 3 Enter the parameters defined in the table:

Parameter	Description
Upgrade Enable	Allows firmware update operations independent of resync actions. Defaults to yes.
Upgrade Error Retry Delay	The interval applied in the event of an upgrade failure. The firmware upgrade error timer activates after a failed firmware upgrade attempt and is initialized with this value. The next firmware upgrade attempt occurs when this timer counts down to zero. The default is 3600 seconds.
Downgrade Rev Limit	Enforces a lower limit on the acceptable firmware version number during an upgrade or downgrade. The device does not complete a firmware upgrade operation unless the firmware version is greater than or equal to this parameter. For example: `7.4.8` The default is (empty).
Upgrade Rule	A firmware upgrade script that defines upgrade conditions and associated firmware URLs. It uses the same syntax as Profile Rule. (See **Manually Provisioning a Phone from the Keypad** for the Upgrade Rule syntax.) The default is (empty).
Log Upgrade Request Msg	Syslog message issued at the start of a firmware upgrade attempt. The default is `$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH`
Log Upgrade Success Msg	Syslog message issued after a firmware upgrade attempt completes successfully. The default is `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
Log Upgrade Failure Msg	Syslog message issued after a failed firmware upgrade attempt. The default is `$PN $MAC -- Upgrade failed: $ERR.`
License Keys	This field is not used.

Launch a Firmware Update by using a Browser Command

An upgrade command entered into the browser address bar can be used to upgrade firmware on a phone. The phone updates only when it is idle. The update is attempted automatically after the call is complete.

To update the phone firmware, enter this command:

`http://`*`phone-ip-address`*`/`**`admin`**`/`**`upgrade?`***`protocol`*`://`*`server-name`*`[:`*`port`*`]]/`*`firmware-path`*

- `protocol` defaults to TFTP.
- `server-name` defaults to the host requesting the URL.
- `port` defaults to:
  - 69 for TFTP
  - 80 for HTTP
  - 443 for HTTPS
- `firmware-path` defaults to /spa.bin (The firmware-pathname typically includes the file name of the binary located in a directory on the TFTP or HTTP server. For example, `http://192.168.2.217/admin/upgrade?tftp://192.168.2.251/spa.bin`) for SPA phones, and `/wip310.img` for the Cisco WIP310.)

Launch a Profile Update by using a Browser Command

Cisco SPA IP phones can synchronize to specific profiles stored on a remote server. The phone resyncs only when it is idle. The update is attempted automatically after the call is complete.

To update the phone profile, enter this command:

`http://`*`phone-ip-addr`*`/admin/resync?`*`protocol`*`://`*`server-name[:port]/profile-pathname`*

- `phone-ip-addr` is the IP address of the phone.
- Parameter following `resync?` defaults to the Profile Rule setting on the web server Provisioning page.
- `protocol` defaults to TFTP.
- `server-name` defaults to the host requesting the URL.

- `port` defaults to:
  - 69 for TFTP
  - 80 for HTTP
  - 443 for HTTPS
- `profile-pathname` defaults to the path for the new synchronization profile (for example, `http://192.168.2.217admin/resync?tftp://192.168.2.251/spaconf.cfg`).

Rebooting a Phone by using a Browser Command

You can remotely reboot a Cisco IP phone by entering a command in a web browser URL field.

To reboot a phone, enter the following command:

`http://`*`phone-ip-address`*`/`**`admin`**`/`**`reboot`**

- `phone-ip-addr` is the IP address of the phone.

Configuring a Custom Certificate Authority

Digital certificates can be used to authenticate network devices and users on the network. They can be used to negotiate IPSec sessions between network nodes.

A third party uses a Certificate Authority Certificate to validate and authenticate two or more nodes that are attempting to communicate. Each node has a public and private key. The public key encrypts data. The private key decrypts data. Because the nodes have obtained their certificates from the same source, they are assured of their respective identities.

The device can use digital certificates provided by a third-party Certificate Authority (CA) to authenticate IPSec connections.

To enable and configure a custom certificate of authority:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Provisioning**.

STEP 2 In the **CA Settings section** in Custom CA Check Enable, select **yes**.

STEP 3 In Custom CA RULE, enter the rule in the following format:

STEP 4 Click **Submit All Changes**.

General Purpose Parameters

The general purpose parameters GPP_* are used as free string registers when configuring the Cisco IP phones to interact with a particular provisioning server solution. The GPP_* parameters are empty by default. They can be configured to contain diverse values, including the following:

- Encryption keys
- URLs
- Multistage provisioning status information
- Post request templates
- Parameter name alias maps
- Partial string values, eventually combined into complete parameter values.

The GPP_* parameters are available for macro expansion within other provisioning parameters. For this purpose, single-letter upper-case macro names (A through P) are sufficient to identify the contents of GPP_A through GPP_P. Also, the two-letter upper-case macro names SA through SD identify GPP_SA through GPP_SD as a special case when used as arguments of the **key** URL option.

These parameters can be used as variables in provisioning and upgrade rules. They are referenced by prepending the variable name with a '$' character, such as $GPP_A.

To configure general purpose parameters, navigate to **Admin Login** > **advanced** > **Voice** > **Provisioning**.

Using TR-069

TR-069 (Technical Report 069) provides Service Providers with a common platform to manage all voice devices and other customer-premises equipment (CPE) in large-scale deployments, no matter neither the device type nor the manufacturer.

As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. The protocol allows the automatic configuration of Internet access devices, such as modems, routers, gateways, set-top box, and VoIP-phones. The technical specifications are managed and published by the Broadband Forum.

Cisco IP phones can be managed by using the protocols and standards defined in TR-069. The ACS enables bulk configuration changes and firmware updates for CPEs (IP phones). TR-069 inter operates with any ACS that will inter operate with a MOTIVE client.

To configure the TR-069 client, navigate to **Admin Login** > **advanced** > **Voice** > **TR-069**:

Field	Description
Enable TR-069	From the drop-down menu, select **yes** to enable TR-069. or **no** to disable TR-069.
ACS URL	Enter the URL of the ACS using the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when using SSL or TLS.
ACS Username	Enter the username that authenticates the CPE to the ACS by using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Enter the password grants access to the ACS for this user. This password is used only for HTTP-based authentication of the CPE.
ACS URL In Use	Displays the ACS URL.
Connection Request URL	Displays the ACS making the connection request to the CPE.
Connection Request Username	Enter the username that authenticates the ACS making the connection request to the CPE.

Field	Description
Connection Request Password	Enter the password used to authenticate the ACS making a connection request to the CPE.
Periodic Inform Interval	The duration in seconds of the interval between CPE attempts to connect to the ACS when Periodic Inform Enable is set to **yes**.
Periodic Inform Enable	From the drop-down menu, select **yes** to enable CPE connection requests. Enter **no** to disable connection requests.
TR-069 Traceability	From the drop-down menu, select **yes** to enable TR-069 transaction traceability. Enter **no** to disable traceability.
CWMP V1.2 Support	From the drop-down menu, select **yes** to enable CPE WAN Management Protocol (CWMP) support. Enter **no** to disable CWMP support such that the device does not send any Inform messages to the ACS or accept any connection requests from the ACS.
TR-069 VoiceObject Init	From the drop-down menu, select **yes** to initialize all voice objects to factory default values. Enter **no** to retain the current values.
TR-069 DHCP Option Init	From the drop-down menu, select **yes** to initialize the DHCP settings from the ACS. Enter **no** to leave the settings unchanged.
TR-069 IGD Support	From the drop-down menu, select **yes** to enable TR-069 on the Internet Gateway Device (IGD). Enter **no** to disable traceability. (This is used for debugging purposes.)
TR-069 Fallback Support	From the drop-down menu, select **yes** to enable TR-069 fallback support. Enter **no** to disable fallback support. If the SPA phone first attempt to discover the ACS by using DHCP, it attempts to use DNS to resolve ACS IP address.
TR-069 DHCP Inform Timer	Enter the interval in seconds that the phone should poll the DHCP server.

Field	Description
BACKUP ACS URL	Enter the backup URL of the ACS using the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when using SSL or TLS.
BACKUP ACS User	Enter the backup username that authenticates the CPE to the ACS by using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
BACKUP ACS Password	Enter the backup password grants access to the ACS for the backup user. This password is used only for HTTP-based authentication of the CPE.

7

Configuring Regional Parameters and Supplementary Services

Use the *Regional* tab to configure regional and local settings, such as Vertical Service Activation codes (star codes), Vertical Service Announcement codes, and local language and dictionary.

- **Scripting for Cadences, Call Progress Tones, and Ring Tones**
- **Call Progress Tones**
- **Distinctive Ring Patterns**
- **Control Timer Values (sec)**
- **Vertical Service Announcement Codes (Cisco SPA300 Series and Cisco SPA500 Series)**
- **Miscellaneous Parameters**
- **Localizing Your IP Phone**
- **Selecting a Display Language**

Call progress tone pass-through lets a user hear call progress tones (such as ringing) that are generated by the far-end network.

Scripting for Cadences, Call Progress Tones, and Ring Tones

Cisco SPA IP phones have configurable call progress tones. Parameters for each type of tone can include a number of components, defining frequency, amplitude and cadence.

Cadence Script

A CadScript is a mini-script that specifies the cadence parameters of a signal up to 127 characters in length. Syntax:

$S_1[;S_2]$

where:

`Si=Di(oni,1/offi,1[,oni,2/offi,2[,oni,3/offi,3[,oni,4/offi,4[,oni,5/offi,5[,oni,6/offi,6]]]]])` and is known as a *section*

`oni,j` and `offi,j` are the on/off durations in seconds of a *segment.* The subscript ranges are: i = 1 or 2, j = 1 to 6.

D_i is the total duration of the section in seconds. All durations can have up to three decimal places to provide 1 ms resolution. The wildcard character "*" indicates infinite duration.

The segments within a section are played in order and repeated until the total duration is played.

Example: Normal Ring

`60(2/4)`

where:

- Number of Cadence Sections = 1
- Cadence Section 1: Section Length = 60 s
- Number of Segments = 1
- Segment 1: On=2s, Off=4s
- Total Ring Length = 60s

Example 2: Distinctive Ring (short, short, short, long)

```
60(.2/.2,.2/.2,.2/.2,1/4)
```

Where:

- Number of Cadence Sections = 1
- Cadence Section 1: Section Length = 60s
- Number of Segments = 4
- Segment 1: On=0.2s, Off=0.2s
- Segment 2: On=0.2s, Off=0.2s
- Segment 3: On=0.2s, Off=0.2s
- Segment 4: On=1.0s, Off=4.0s
- Total Ring Length=60s

Tone Script

A ToneScript is a mini-script that specifies the frequency, level, and cadence of a call progress tone. It can contain up to 127 characters. Syntax:

```
FreqScript;Z1[;Z2]
```

Section Zi is similar to the Si section in a CadScript except that each on/off segment is followed by a frequency parameter: `Zi = Di(oni,1/offi,1/fi,1[,oni,2/offi,2/fi,2 [,oni,3/offi,3/fi,3 [,oni,4/offi,4/fi,4 [,oni,5/offi,5/fi,5 [,oni,6/offi,6/fi,6]]]]])`

where `fi,j = n1[+n2]+n3[+n4[+n5[+n6]]]] 1< nk < 6` indicates which of the frequency components given in the FreqScript are used in that segment; if more than one frequency component is used in a segment, the components are summed together.

Example: Dial Tone

```
350@-19,440@-19;10(*/0/1+2)
```

- Number of Frequencies = 2
- Frequency 1 = 350 Hz at –19 dBm
- Frequency 2 = 440 Hz at –19 dBm

- Number of Cadence Sections = 1
- Cadence Section 1: Section Length = 10 s
- Number of Segments = 1
- Segment 1: On=forever, with Frequencies 1 and 2
- Total Tone Length = 10s
- Example 2: Stutter Tone
- 350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)
- Number of Frequencies = 2
- Frequency 1 = 350 Hz at –19 dBm
- Frequency 2 = 440 Hz at –19 dBm
- Number of Cadence Sections = 2
- Cadence Section 1: Section Length = 2s
- Number of Segments = 1
- Segment 1: On=0.1s, Off=0.1s with Frequencies 1 and 2
- Cadence Section 2: Section Length = 10s
- Number of Segments = 1
- Segment 1: On=forever, with Frequencies 1 and 2
- Total Tone Length = 12s

Example: SIT Tone

```
985@-16,1428@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/
0)
```

- Number of Frequencies = 3
- Frequency 1 = 985 Hz at –16 dBm
- Frequency 2 = 1428 Hz at –16 dBm
- Frequency 3 = 1777 Hz at –16 dBm
- Number of Cadence Sections = 1
- Cadence Section 1: Section Length = 20s

- Number of Segments = 4
- Segment 1: On=0.38s, Off=0s, with Frequency 1
- Segment 2: On=0.38s, Off=0s, with Frequency 2
- Segment 3: On=0.38s, Off=0s, with Frequency 3
- Segment 4: On=0s, Off=4s, with no frequency components
- Total Tone Length = 20s

Ring Script

A RingScript is a mini-script that describes a ring tone. Syntax:

`n=ring-tone-name;w=waveform-id-or-path;c=cadence-id;b=break-time;t=total-time`

`ring-tone-name` identifies this ring tone. This name appears on the Ring Tone menu of the phone. The same name can be used in a SIP Alert-Info header in an inbound INVITE request to tell the phone to play the corresponding ring tone. The name should contain the same characters allowed in a URL only.

`waveform-id-or-path` is the index of the desired waveform to use in this ring tone. The built-in waveforms are:

- 1 = Classic phone with mechanical bell
- 2 = Typical phone ring
- 3 = Classic ring tone
- 4 = Wide-band frequency sweep signal

This field can also be a network path (url) to download a ring tone data file from a server on-the-fly. In this case, the syntax of the field is:

`w=[tftp://]hostname[:port]/path`

`cadence-id` is the index of the desired cadence to play the given waveform. 8 cadences (1–8) as defined in <Cadence 1> through <Cadence 8>. Cadence-id can be 0 If w=3,4, or an url. Setting c=0 implies the on-time is the natural length of the ring tone file.

`break-time` specifies the number of seconds to break between two bursts of ring tone, such as b=2.5.

`total-time` specifies the total number of seconds to play the ring tone before it times out.

Call Progress Tones

For definitions of all call progress tones, see **Call Progress Tone Description**.

Distinctive Ring Patterns

Ring cadence defines the ringing pattern that announces a telephone call. The Cisco WIP310 has only eight distinctive ring pattern fields.

The pattern is:

```
length(on/off)
```

where:

- Length: The total length of the ring
- On: The number of on seconds the ring is heard.
- Off: The number of seconds the ring is silent.

Example 1: Normal Ring

```
60(2/4)
```

where:

- Number of Cadence Sections = 1
- Cadence Section 1: Section Length = 60 s
- Number of Segments = 1
- Segment 1: On=2s, Off=4s
- Total Ring Length = 60s

Example 2: Distinctive Ring (short, short, short, long)

```
60(.2/.2,.2/.2,.2/.2,1/4)
```

where:

- Number of Cadence Sections = 1
- Cadence Section 1: Section Length = 60s
- Number of Segments = 4
- Segment 1: On=0.2s, Off=0.2s
- Segment 2: On=0.2s, Off=0.2s
- Segment 3: On=0.2s, Off=0.2s
- Segment 4: On=1.0s, Off=4.0s
- Total Ring Length=60s

Distinctive Call Waiting Tone

When the phone is off-hook on a call, the call waiting tone plays. Support for Distinctive Ring is based on the Alert-Info header that supports the Distinctive Call Waiting tone. The distinctive call waiting tone is generated based on the phone call waiting tone frequency and gain values, and the cadence value of the matched ring tone.

The cadence value (following the `c=` element) of the matched ring tone must be an integer from 1 to 9 that specifies the ring cadence under the **Regional** tab of the phone web user interface.

If there is no matching ring tone name, or an invalid cadence value is specified, the configured Call Waiting Tone is used.

Control Timer Values (sec)

The table describes Control Timer parameters.

Field	Description
Reorder Delay	Delay after far end hangs up before reorder (busy) tone is played. Ranges from 0 to 255 seconds. 0 = play immediately inf = never play 255 = return the phone immediately to on-hook status and do not play the tone. Defaults to 5.
Call Back Expires	Expiration time of a call back activation request. Ranges from 0 to 65535 seconds. Defaults to 1800.
Call Back Retry Intvl	The interval between call back retry requests. Ranges from 0 to 255 seconds. Defaults to 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 Cisco SPA IP phones still consider the call as failed and continues to retry. Defaults to 0.5.
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. Ranges from 0 to 64 seconds. Setting this value high can result in a longer post dialing delay (PDD), which is the time between the start of a call and the time the phone starts ringing. A value that is too low can result in dialed digits not being correctly recognized. Defaults to 10.

Field	Description
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. Ranges from 0 to 64 seconds. Defaults to 3.

Configuring Supplementary Services (Star Codes)

The Cisco IP phones provide native support of a large set of enhanced or supplementary services (also known as star codes). A user can enter star codes (such as *21 for call forward, followed by the target number) to perform call features such as call return, blind call transfers, call pickup, and so on. These codes can be handled locally by the phone or to be sent to the network as an INVITE to the service provider.

Some service providers choose to disable star codes. See **Configuring Supplementary Services (Star Codes)** for more information.

Entering Star Code Values

The phone provides default values for star codes. To change star code values, navigate to **Admin Login** > **advanced** > **Regional**. Under **Vertical Service Activation Codes**, enter the values you want to change for the codes.

The codes are:

- Call Return (*69)—Calls the last caller, regardless which extension.
- Blind Transfer (*98)—Allows the user to transfer a call to another number without waiting for the other party to pick up.
- Call Back Act (*66)—Periodically redials the last busy number (every 30 seconds by default) until it rings or until the attempt expires (30 min by default), regardless which extension. Only one call back operation can be ordered at a time. A new order automatically cancels the previous order.
- Call Back Deact (*86)—Cancels the last call back operation.

- Call Forward All Act (*72)—Call forwards all inbound calls. Applies to primary extension only.
- Call Forward All Deact (*73)—Cancels call forward all. Applies to primary extension only.
- Call Forward Busy Act (*90)—Call forwards on busy. Applies to primary extension only.
- Call Forward Busy Deact (*91)—Cancels call forward on busy. Applies to primary extension only.
- Call Forward No Answer Act (*92)—Call forwards if no answer. Applies to primary extension only.
- Call Forward No Answer Deact (*93)—Cancels call forward no answer. Applies to primary extension only.
- CW Act (*56)—Enables call waiting. For example, if call waiting is turned off globally, this star code will turn on call waiting until the CW Deact code is entered.
- CW Deact (*57)—Deactivates call waiting. For example, if call waiting is turned on globally, this star code deactivates call waiting until the CW Act code is entered.
- CW Per Call Act (*71)—Enables call waiting for a single call. For example, if call waiting is turned off globally, this star code will turn on call waiting for that call.
- CW Per Call Deact (*70)—Deactivates call waiting for a single call. For example, if call waiting is turned on globally, this star code deactivates call waiting for that call.
- Block CID Act (*67)—Blocks caller ID on all outbound calls. Applies to all extensions.
- Block CID Deact (*68)—Deactivates caller ID blocking on outbound calls. Applies to all extensions.
- Block CID Per Call (*81)—Blocks caller ID on the next outbound call (on the current call appearance only).
- Block CID Per Call Deact (*82)—Deactivates caller ID blocking on the next outbound call (on the current call appearance only).
- Block ANC Act—Blocks anonymous calls. Applies to all extensions.

- Block ANC Deact—Deactivates anonymous call blocking. Applies to all extensions.
- DND Act (*78)—Activates Do Not Disturb. Applies to all extensions.
- DND Deact (*79)—Deactivates Do Not Disturb. Applies to all extensions.
- Secure All Call Act (*16)—Defaults to prefer to use encrypted media (voice codecs).
- Secure No Call Act (*17)—Defaults to prefer to use unencrypted media for all outbound calls. Applies to all extensions.
- Secure One Call Act (*18)—Prefers to use encrypted media for the outbound call (on this call appearance only).
- Secure One Call Deact (*19)—Prefers to use unencrypted media for the outbound call (on this call appearance only).
- Paging (*96)—Pages the number called.
- Call Park (*38)—Parks a call on an entered line number.
- Call UnPark Code (*39)—Retrieves a call from an entered line number.
- Call Pickup (*36)—Picks up a call at an entered extension.
- Group Call Pickup (*37)—Picks up a ringing call at a group of extensions.
- Media Loopback Code (*03)—A service provider can set up a test call from an IP media loopback server (the source) to a subscriber VoIP device (the mirror). The test call provides statistical reporting on network performance and audio quality.

  Depending on the source capabilities, a service provider can see packet jitter, loss, and delay (although Media Loopback cannot identify an offending hop). This helps the service provider identify an offending hop that could be causing issues in VoIP calls to a subscriber. The test results can also provide audio quality scoring, that lets a service provider better understand the subscriber's experience.

- Referral Services Codes—One or more * codes can be configured into this parameter, such as *98, or *97|*98|*123, and so forth. The maximum total length is 79 characters.

  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 Cisco IP phone to perform a blind transfer to a target number that is prepended by the service * code. For example:

  - After the user dials *98, the Cisco IP phone plays a special prompt tone while waiting for the user the enter a target number (which is validated according to the dial plan as in normal dialing).
  - When a complete number is entered, the Cisco IP phone sends a blind REFER to the holding party with the Refer-To target equals to *98 *target_number*. This feature allows the Cisco IP phone 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 Cisco IP phone. You can delete any * code that you do not want the call server to process.

  Feature Dial Services Codes: Tells the Cisco IP phone what to do when the user is listening to the first or second dial tone.

  You can configure one or more * codes into this parameter, such as *72, or *72|*74|*67|*82, and so on. The maximum total length is 79 characters. When the user has a dial tone (first or second dial tone), they can enter a * code (and the following target number according to current dial plan) to trigger the Cisco IP phone to call the target number prepended by the * code. For example:

  - After the user dials *72, the Cisco IP phone plays a special prompt tone while waiting for the user the enter a target number (which is validated according to the dial plan as in normal dialing).
  - When a complete number is entered, the Cisco IP phone sends an INVITE to *72 *target_number* as in a normal call. This feature allows the proxy to process features such as call forward (*72) or BLock Caller ID (*67).

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‘. Following is a list of allowed dial tone parameters (note the use of back quotes surrounding the parameter without 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 Cisco IP phone plays the 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, add that * code in the dial plan.

Activating or Deactivating Supplementary Services

You can disable services handled locally by the phone in one of two ways:

- Delete the star code in the *Vertical Service Activation* section in the **Regional** tab.
- Disable the service in the ***Phone*** tab. See **Configuring Supplementary Services (Star Codes), page 182**.

If a service is enabled in the Phone tab but cleared in the Regional tab, the service can still be enabled/disabled from the IP phone screen or the phone web user interface. If a service is disabled, the soft button associated with that service is hidden on the IP phone screen. Also, any menu item associated with a disabled service is preceded with an exclamation mark (!).

A supplementary service should be disabled if

- the user has not subscribed to it
- the service provider intends to support similar service by using means other than relying on the Cisco IP phone.

Vertical Service Announcement Codes (Cisco SPA300 Series and Cisco SPA500 Series)

The Cisco SPA300 Series and Cisco SPA500 Series IP phones support all services that can be activated on a phone (call forward, do not disturb, and so on). Vertical service announcement codes apply only when the user dials the corresponding star code.

Following is an example of how you can use these fields:

```
<Service Annc Base Number> = 1234
<Service Annc Extension Codes>=
"CWT:00;CWF:01;FAT:02;FAF:05;FBT:03;FBF:05;FNT:04;FNF:05;"
Here CWT: Call waiting service enabled;
CWF: Call waiting service disabled;
FAT: Call forward all service enabled;
FAF: Call forward all service disabled;
FBT: Call forward busy service enabled;
FBF: Call forward busy service disabled;
FNT: Call forward no answer enabled;
FNF: Call forward no answer disabled;
```

When the user enables call waiting service, the IP phone automatically calls `123400@$proxy`.

When the user *disables* the call waiting service, IP phone connects to `123401@$proxy`.

If the <Service Annc Extension Codes> do not define CWT/CWF extension codes, the IP phone defaults to normal.

Bonus Services Announcement Description

When the user enables the callback service using the *code, the IP phone automatically calls `123400@$proxy`.

When the user disables the callback service using the *code, the IP phone automatically connects to the `123401@$proxy`.

If the *Service Annc Extension Codes* do not define CBT/CBF extension codes, the IP phone does not use this feature.

```
[Line1/2]<Service Announcement Serv> = Yes
[Regional]<Service Annc Base Number> = {announcement server base number}
[Regional]<Service Annc Extension Codes> = {SAEC Script}
SAEC Script format:{SA_map;}*    Here * means 0 or multiple
SA_map syntax:
      SA_serv=SA_extcode
```

```
      SA_serv is the name of service plus the current condition;
      SA_extcode is the extension code which the ANNC server will route to.
Appendix: SA_serv list
    1) Call Back
    CBT: Call back enabled
    CBF: Call back disabled
    CBB: Call back busy enabled
2) Call Forward
    FAT: Call forward all enabled
    FAF: Call forward all disabled
    FBT: Call forward busy enabled
    FBF: Call forward busy disabled
    FNT: Call forward no answer enabled
    FNF: Call forward no answer disabled
    FLT: Call forward last enabled
    FLF: Call forward last disabled
3) Call Waiting
    CWT: Call waiting enabled
    CWF: Call waiting disabled
4) Block Last Call
    BLT: Block last call enabled
    BLF: Block last call disabled
5) Accept Last Call
    ALT: Accept last call enabled
    ALF: Accept last call disabled
6) Block Caller ID
    BCT: Block caller id enabled
    BCF: Block caller id disabled
7) Distinctive Ringing
    DRT: Distinctive ringing enabled
    DRF: Distinctive ringing disabled
8) Speed Dial
    SDT: Speed dial enabled
    SDF: Speed dial disabled
9) Secure Call
    SCT: Secure call enabled
    SCF: Secure call disabled
10) Do Not Disturb
    DDT: DND enabled
    DDF: DND disabled
11) Caller ID
    CDT: Caller ID enabled
    CDF: Caller ID disabled
12) CW CID
    WDT: CWCID enabled
    WDF: CWCID disabled
13) Block Anonymous call
    BAT: Block anonymous call enabled
    BAF: Block anonymous call disabled
```

Outbound Call Codec Selection Codes

Codec call selection codes affect voice quality. For more information about voice codecs, see the **Configuring Voice Codecs**. You can choose a *preferred* codec for a call or *force* a call to use a specific codec:

- Prefer *G.711u (*017110)* through *G.729a (*01729)*—Sets the preferred codec for next outbound call. If the preferred codec is unavailable, the second, then the third preferred codec is used, if specified.
- Force *G.711u (*027110)* through *G.729a (*02729)* —Forces the specified codec for next outbound call. If the specified codec is unavailable, the preferred codecs are used in order, if specified.

See **Configuring Voice Codecs** for more information.

Miscellaneous Parameters

This section describes Dual Tone Multi-Frequency (DTMF) and localization parameters:

DTMF Parameters

DTMF is used by touch-tone phones to assign a specific frequency (consisting of two separate tones) to each key so that it can easily be identified by a microprocessor.

In-Band and Out-of-Band (RFC-2833): IP phones can relay DTMF digits as out-of-band events to preserve the fidelity of the digits. This can enhance the reliability of DTMF transmission required by many IVR applications such as dial-up banking and airline information.

The following parameters can either reduce false detection or get better detection by the IVR. In general, the default values are recommended for both IVR functions.

- *DTMF Playback Level*: Local DTMF playback level in decibels per minute, up to one decimal place. Applicable locally when a user presses a digit or when the phone receives an out-of-band (OOB) DTMF signal from the network side. Does not affect DTMF transmission. Defaults to -16.
- *DTMF Playback Length*: Local DTMF playback duration in milliseconds. Affects only OOB. Defaults to .1.

- *Inband DTMF Boost*: Controls the amount of amplification applied to DTMF signals. Affects only tones sent by inband method. Choices are 0, 3, 6, 9, 12, 15, and 18 decibels. Defaults to 12 dB.

To support false detection, avoid inband and use OOB. With OOB, the DTMF Playback Length does not matter. If you use inband, use a smaller DTMF Boost value.

To get better detection by the IVR, avoid inband and use OOB. This way, the DTMF tone is reconstructed by the PSTN gateway or the remote endpoint, and the quality is not subject to distortion from the audio codec. If you use OOB, use a slightly longer DTMF Playback Length.

If you use inband, use a higher Inband DTMF boost.

NOTE On the Cisco SPA525G2, when using the Mobile Link line (through the Bluetooth-enabled mobile phone), the local user can hear a double tone (echo) when pressing digits (DTMF tones) and engaged on a call. This can happen with certain mobile phones that have the option to play locally the local tone (which is also played by the Cisco SPA525G2). This does not affect operation with interactive voice response applications, as the tone is audible only on the local device. See the Cisco support community at http://www.cisco.com/go/smallbizsupport for phone compatibility information, and also consult the latest Cisco SPA525G2 release notes, available at cisco.com.

Localizing Your IP Phone

The following table describes the localization parameters in the Miscellaneous section.

Field	Description
Set Local Date (mm/dd)	Enter the local date (*mm* represents the month and *dd* represents the day). The year is optional and uses two or four digits. For example, May 1, 2008, can be entered as: **05/01** or **05/01/08** or **05/01/2008**.
Set Local Time (HH/mm)	Enter the local time (*hh* represents hours and *mm* represents minutes). Seconds are optional.

Field	Description
Time Zone	Selects the number of hours to add to GMT to generate the local time for caller ID generation. Choices are GMT-12:00, GMT-11:00,..., GMT, GMT+01:00, GMT+02:00, ..., GMT+13:00. Defaults to GMT-08:00.
Time Offset (HH/mm)	Enter the offset from GMT to use for the local system time.
Daylight Saving Time Rule	Enter the rule for calculating daylight saving time. See **Configuring Daylight Saving Time**.
Daylight Saving Enable	Select **yes** to enable or **no** to disable DST on the phone. This setting affects all lines (extensions) on the phone.
Dictionary Server Script	Defines the location of the dictionary server, the languages available, and the associated dictionary. See **Creating a Dictionary Server Script**.

Language Selection	Specifies the default language. The value must match one of the languages supported by the dictionary server. The script (dx value) is:
	
	`<Language_Selection ua="na">`
	`</Language_Selection>`
	
	Defaults to blank; the maximum number of characters is 512. For example:
	
	`<Language_Selection ua="na"> Spanish`
	`</Language_Selection>`

Managing the Time and Date

Cisco IP phones obtain the time settings in one of three ways:

- NTP Server—When the phone boots up, it tries to contact the first Network Time Protocol (NTP) server to get the time. The phone periodically synchronizes its time with the NTP server. The synchronization period is fixed at 1 hour. Between updates the phone tracks time with its internal clock.
- SIP Messages—Each SIP message (request or response) sent to the phone could contain a Date header with the current time information. If the header is present, the phone uses it to set its clock.

- Manual Setup—The time and date can be entered manually by using the IP phone screen or the phone web user interface. However, this value is overwritten by the NTP time or SIP Message Date whenever they are available to the phone. Manual setup requires that you enter the time in 24-hour format only.

The time served by the NTP Server and the SIP Date Header are expressed in GMT time. The local time is obtained by offsetting the GMT according to the time zone of the region.

The *Time Zone* parameter can be configured by using the phone web user interface or through provisioning. This time can be further offset by the *Time Offset (HH/mm)* parameter. This parameter must be entered in 24-hour format and can also be configured from the IP phone screen.

The *Time Zone* and *Time Offset (HH/mm)* offset values are *not* applied to manual time and date setup.

Configuring Daylight Saving Time

The phone supports auto adjustment for daylight saving time. You must set *Daylight Savings Time Enable* to **yes** and enter the DST rule. This option affects the time stamp on the *CallerID*.

To enter the rule for calculating DST, include the start, end, and save values separated by semi-colons (;) as follows:

```
Start = start-time; end=end-time; save = save-time
```

For example, the default DST rule is:

```
start=4/1/7;end=10/-1/7;save=1.
```

The *start-time* and *end-time* values specify the start and end dates and times of daylight saving time. The format is:

```
month/day/weekday[/HH:mm:ss]
```

The *month* value equals any value in the range 1-12 (January-December).

The *day* value equals any + or - value in the range 1-31. If value is -1, the time will change on the weekday on or before the end of the month; the last occurrence of a weekday in that month.

The *weekday* value equals any value in the range -7 to 7 (Monday to Sunday). If the weekday value is 0, the date to start or end daylight saving is exactly the *month* and *day*. If the weekday value is -7 to 7, daylight saving starts or ends on the weekday value on or *after* the month and day. If the weekday value is not 0 and the day value is negative, then daylight saving starts or ends on the weekday value on or *before* the month and day.

Optional time values: *HH* represents hours (0-23), *mm* represents minutes (0-59). and *ss* represents seconds (0-59). Optional values inside brackets [ ] are assumed to be 0 if not specified. Midnight is represented by 0:0:0.

The *save-time* value is the number of hours, minutes, and/or seconds to add to the current time during DST. The *save-time* value cannot be a minus (-) in version 7.5.1 and higher. Earlier firmware versions support a negative value.

Daylight Saving Time Examples

The following example configures daylight saving time for the U.S, adding one hour starting at midnight on the first Sunday in April and ending at midnight on the last Sunday of October; add 1 hour (USA, North America):

```
start=4/1/7/0:0:0;end=10/31/7/0:0:0;save=1
start=4/1/7;end=10/-1/7;save=1
start=4/1/7/0;end=10/-1/7/0;save=1
```

The following example configures daylight saving time for Egypt, starting at midnight on the last Sunday in April and ending at midnight on the last Sunday of September:

```
start=4/-1/7;end=9/-1/7;save=1 (Egypt)
```

The following example configures daylight saving time for New Zealand (in version 7.5.1 and higher), starting at midnight on the first Sunday of October and ending at midnight on the third Sunday of March.

```
start=10/1/7;end=3/22/7;save=1 (New Zealand)
```

The following example reflects the new change starting March 2007. DST starts on the second Sunday in March and ends on the first Sunday in November:

```
start=3/8/7/02:0:0;end=11/1/7/02:0:0;save=1
```

Selecting a Display Language

This section describes how to localize the Cisco SPA300 Series and Cisco SPA500 Series IP Phone display language. You can define up to nine languages, in addition to English, to be available and host the dictionaries for each of the languages on the HTTP or TFTP provisioning server. Language support follows Cisco dictionary principles.

NOTE The Cisco WIP310 does not support localization.

Use the Language Selection parameter to select the phone default display language. The value must match one of the languages supported by the dictionary server. The script (dx value) is as follows:

- <Language_Selection ua="na">
- </Language_Selection>

Defaults to blank; the maximum number of characters is 512. For example:

```
<Language_Selection ua="na"> Spanish
</Language_Selection>
```

During startup, the phone checks the selected language and downloads the dictionary from the TFTP/HTTP provisioning server indicated in the phone configuration. The dictionaries are available at the support website. See **Appendix B, "Where to Go From Here,"** for the website location.

The end user can change the language of the phone on the phone by following these steps:

STEP 1 Press the **Setup** button.

STEP 2 Select **Language**, then press the **Select** soft button.

STEP 3 Select **Option** to change the language.

STEP 4 With the desired language highlighted, press **Save**.

Creating a Dictionary Server Script

The Dictionary Server Script defines the location of the dictionary server, the languages available and the associated dictionary. The syntax is:

```
Dictionary_Server_Script ua="na"/Dictionary_Server_Script
```

Defaults to blank; the maximum number of characters is 512. The detailed format is as follows:

```
serv={server ip port and root path};
d0=language0;x0=dictionary0 filename;
d1=language1;x1=dictionary1 filename;
d2=language2;x2=dictionary2 filename;
d3=language3;x3=dictionary3 filename;
d4=language4;x4=dictionary4 filename;
d5=language5;x5=dictionary5 filename;
d6=language6;x6=dictionary6 filename;
d7=language3;x7=dictionary7 filename;
d8=language8;x8=dictionary8 filename;
d9=language5;x9=dictionary9 filename;
```

For example:

```
Dictionary_Server_Script ua="na"
serv=tftp://192.168.1.119/
;d0=English;x0=enS_v101.xml;d1=Spanish;x1=esS_v101.xml /
Dictionary_Server_Script
```

8

Configuring 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.

If the Cisco SPA IP phones are part of the Cisco SPA9000, dial plans are configured on the Cisco SPA9000. In installations where a Cisco SPA9000 is not present (such as IP Centrex installations), installations where the phones are removed from the Cisco SPA9000 (such as by a VPN), or other situations, dial plans can be configured on the IP phone by using the phone web user interface.

For more information on using dial plans on the Cisco SPA9000, see the *Cisco SPA9000 Administration Guide*. See the **Appendix B, "Where to Go From Here,"** for the location of the document.

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

- **About Dial Plans**
- **Editing Dial Plans on the IP Phone**
- **Resetting the Control Timers**

About Dial Plans

The Cisco SPA IP phones and the Cisco SPA9000 are involved in applying various levels of the dial plans and process the digits sequence in the same manner.

When a user lifts a handset or presses a speaker button on the IP phone, the following sequence of events begins:

1. The phone begins collecting the dialed digits. The inter-digit timers starts tracking the time that elapses between digits.
2. If the inter-digit timer value is reached, or if another terminating event occurs, the phone compares the dialed digits with the IP phone dial plan. (This dial plan is configured in the phone web user interface in the **Voice** tab, on the tab for each extension (**Ext N**), under the **Dial Plan** section.)

   If the phone is part of a Cisco SPA9000:

3. If the phone dial plan allows the call to process, the dialed numbers are sent to the Cisco SPA9000.
4. The Cisco SPA9000 compares the dialed digits to the CALL ROUTING RULE (on SPA9000 Voice > SIP page in the PBX Parameters section).
5. If the call routing rule allows the call to process, then the Cisco SPA9000 compares the dialed digits to the LINE INTERFACE dial plan (on the Cisco SPA9000 Voice > Line N page, Dial Plan).
6. The Cisco SPA9000 uses the information in the line dial plan to manipulate the number (for example, to remove steering digits) and then transmits the number.

NOTE The dial plan feature (digit sequences and timers) is not used with the Cisco SPA525G2 phone line associated to Mobile Link (a Bluetooth-enabled mobile phone). Mobile phone dial plan rules continue to apply in this scenario.

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 that are individually matched to the keys that the user presses.

White space is ignored, but can be used for readability.

Digit Sequence	Function
0 1 2 3 4 5 6 7 8 9 0 * #	Characters that represent a key that the user must press on the phone keypad.
x	Any character on the phone keypad.

Digit Sequence	Function
[sequence]	Characters within square brackets create a list of accepted key presses. The user can press any one of the keys in the list. A numeric range, for example, `[2-9]` allows a user to press any one digit from `2` through `9`. A numeric range can include other characters. For example, `[35-8*]` allows a user to press 3, 5, 6, 7, 8, or *.
. (period)	A period indicates 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 forth.

<dialed:substituted>	This format indicates that certain *dialed* digits are replaced by the *substituted* characters when the sequence is transmitted. The *dialed* digits can be zero to 9. For example:
	
	`<8:1650>xxxxxxx`
	
	When the user presses `8` followed by a seven-digit number, the system automatically replaces the dialed `8` with the sequence `1650`. If the user dials **85550112**, the system transmits **16505550112**.
	
	If the *dialed* parameter is empty and there is a value in the *substituted* field, no digits are replaced and the *substituted* value is always prepended to the transmitted string. For example:
	
	`<:1>xxxxxxxxxx`
	
	When the user dials **9725550112**, the number `1` is added at the beginning of the sequence; the system transmits **19725550112**.

Digit Sequence	Function
, (comma)	An intersequence tone played (and placed) between digits plays an **outside line** dial tone. For example: `9, 1xxxxxxxxxx` An outside line dial tone is sounded after the user presses `9`. The tone continues until the user presses `1`.
! (exclamation point)	Prohibits a dial sequence pattern. For example: `1900xxxxxxx!` Rejects any 11-digit sequence that begins with 1900.
*xx	Allows a user to enter a 2-digit star code.
S0 or L0	For Interdigit Timer Master Override, 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.
P	To pause, enter `P`, the number of seconds to pause, and a space. This feature is typically used for implementation of a hot line and warm line, with a 0 delay for the hot line and a non-zero delay for a warm line. For example: **EXAMPLE:** `P5` A pause of 5 seconds is introduced.

NOTE The Cisco SPA9000 and the Cisco IP phones implicitly append the vertical code sequences entered in the regional parameter settings to the end of the dial plan. Likewise, if Enable_IP_Dialing is enabled, IP dialing is also accepted on the associated line.

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:

```
( [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:

```
( [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 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:

```
( [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:

```
( [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 is 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 press 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 the 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 more digits are entered by the user, the set of candidates diminishes until only one or none are valid. When a terminating event occurs, the IP PBX either accepts the user-dialed sequence and initiates a call, or else 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
Dialed digits do not match any sequence in the dial plan.	The number is rejected.
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.
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.
A user presses the # key or the **dial** softkey on the IP phone screen.	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 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: `(Ps<:n> | dial plan )`

- **s:** The number of seconds; if no number is entered after `P`, the default timer of 5 seconds applies. With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook.
- **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>, then 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 phone.

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.

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 **Resetting the Control Timers**.

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 is 5 seconds. With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook.
- 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]xxxxxxxxS0** `| 9,8,011xx. | 9,8,xx.|[1-8]xx)`

9,8,1[2-9]xxxxxxxxS0 With the timer set to 0, the call is transmitted automatically when the user dials the final digit in the sequence.

Editing Dial Plans on the IP Phone

You can edit dial plans and modify the control timers. To edit the dial plans on the IP phone:

STEP 1 Navigate to **Admin Login** > **advanced** > **Voice**.

STEP 2 Click the **Ext *N*** tab, where *N* is the extension being configured.

STEP 3 In the Dial Plan section, enter the digit sequences in the Dial Plan field. For more information and examples, see **Digit Sequences**.

The default (US-based) system-wide dial plan appears automatically in the field. You can delete digit sequences, add digit sequences, or replace the entire dial plan with a new dial plan. For more information and examples, see **Digit Sequences**.

Separate each digit sequence with a pipe character, and enclose the entire set of digit sequences within parentheses. Refer to the following example:

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

STEP 4 (Optional) Enter the Caller ID Map—Inbound caller ID numbers can be mapped to a different string. For example, a number that begins with +44xxxxxx can be mapped to 0xxxxxx. This feature has the same syntax as the Dial Plan parameter. With this parameter, you can specify how to map a caller ID number for display on screen and recorded into call logs. (Not applicable to Cisco WIP310.)

STEP 5 (Optional) Enable IP dialing—Enable or disable IP dialing. Defaults to no.

STEP 6 (Optional) Emergency Number—Enter a comma-separated list of emergency numbers. When one of these numbers is dialed, the unit disables processing of *CONF*, *HOLD*, and other similar softkeys or buttons to avoid accidentally putting the current call on hold. The phone also disables hook flash event handling. Only the far end can terminate an emergency call. The phone is restored to normal after the call is terminated and the phone is back on-hook.

Maximum number length is 63 characters. Defaults to blank (no emergency number). (Not applicable to Cisco WIP310.)

STEP 7 Click **Submit All Changes**. The phone reboots.

STEP 8 If you need to configure a dial plan for any other extensions on the phone (depending on the model), click the appropriate *Extension* tab, enter the dial plan, and submit the changes.

STEP 9 Verify that you can successfully complete a call using each digit sequence that you entered in the dial plan.

NOTE If you hear a reorder (fast busy) tone, you need to review your entries and modify the dial plan appropriately. See **Digit Sequences**.

Resetting the Control Timers

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

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 **About Dial Plans**.

STEP 1 Log in to the phone web user interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click **Voice > Regional**.

STEP 4 Scroll down to the *Control Timer Values* section.

STEP 5 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.

9

Configuring LED Patterns

You can customize the LED patterns for the line keys.

To configure Line Key LED patterns:

STEP 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**

STEP 2 Under **Line Key LED Pattern**, use the following letters to customize the fields shown in the following table:

- **p** indicates **pattern**: the blinking pattern of the LED
- **c** indicates **color**: the color setting of the LED
- **r** indicates **red**: a red-colored LED
- **g** indicates **green**: a green-colored LED

Parameters	Description
Idle LED	The line is idle. Defaults to blank (c=r).
Remote Undefined LED	The Remote Undefined state pattern, where the shared call state is undefined (the phone is still waiting for the state information from the application server). Not applicable if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Seized LED	This phone seized the call appearance in preparation for a new outbound call. Defaults to blank (c=r).

Parameters	Description
Remote Seized LED (applicable only to shared call appearance)	The shared call appearance was seized by another phone. Defaults to blank (c=r; p=d).
Local Progressing LED	This phone attempts an outgoing call on this call appearance (the called number is ringing). Defaults to blank (c=r).
Remote Progressing LED (applicable only to shared call appearance)	Another phone attempts an outbound call on this shared call appearance. Defaults to blank (c=r; p=d).
Local Ringing LED	The call appearance is ringing. Defaults to blank (c=r;p=f).
Remote Ringing LED (applicable only to shared call appearance)	The shared call appearance is in ringing on another phone. Defaults to blank (c=r;p=d).
Local Active LED	The call appearance is engaged in an active call. Defaults to blank (c=r).
Remote Active LED (applicable only to shared call appearance)	Another phone is engaged in an active call on this shared call appearance. Defaults to blank (c=r;p=d).
Local Held LED	The call appearance is held by this phone. Defaults to blank (c=r;p=s).
Remote Held LED (applicable only to shared call appearance)	Another phone placed this call appearance on hold. Defaults to blank (c=r,p=s).
Register Failed LED	The corresponding extension has failed to register with the proxy server. Leaving this entry blank defaults to c=a.

Parameters	Description
Disabled LED	Call Appearance is disabled (not available for any incoming or outgoing call). Leaving this entry blank defaults to c=o.
Registering LED	The corresponding extension tries to register with the proxy server. Defaults to blanks (c=r;p=s).
Call Back Active LED	Call Back operation is currently active on this call. Defaults to blank (c=r;p=s).

STEP 3 Click **Submit All Changes**.

LED Script

The LED script describes the color and blinking pattern of a Line Key LED. Each script contains a number of fields separated by a semicolon(;). White spaces are ignored. Each field has the syntax *<field-name>* = *<field-value>*. The allowed *field-name* and corresponding *field-values* are listed below:

c=o|r|g|a

This field sets the **color** of the LED. The 4 choices are:

- o = off
- r = red
- g = green
- a = amber (orange)

p=n[b]|s[b]|f[b]|d[b]|u[d]

This field sets the blinking **pattern** of the LED. The 4 choices are:

- nb = no blink (steady on or off)
- sb = slow blink (1s on and 1s off)
- fb = fast blink (100ms on and 100ms off)
- ud = user-defined (according to the contents of the u field)

`u=on/off/on/off/etc.`

This is a user-defined blinking pattern used only when p = ud. It consists of up to 4 pairs of on/off duration in seconds with up to 2 decimal places; each value is separated by a forward slash (/).

LED Script Examples

`c=r;p=sb`

Color is red and pattern is slow blink.

`c=o`

LED is off.

`c=g`

Color is green and pattern is steady on (default).

`c=a;p=ud;u=.1/.1/.1/.1/.1/.9`

Color is amber (orange) and the blink pattern is: 100ms on, 100ms off, 100ms on, 100ms off, 100ms on, 900ms off

LED Pattern

The administrator can also specify a different color and pattern for each of the following states of the call appearance.

- Idle: This call appearance is not in use. It can be used to make outbound call on this phone
- Local Seized: This call appearance has been seized by this phone to prepare for an outbound call
- Local Progressing: This phone is making an outbound call that is progressing
- Local Active: This phone is engaged in a connected call on this call appearance
- Local Ringing: This phone is ringing for an incoming call on this call appearance
- Local Held: This phone has placed this call appearance on hold

- Remote Seized: This call appearance has been seized by another phone to prepare for an outbound call
- Remote Progressing: Another phone is making a call on this call appearance and is progressing
- Remote Active: Another phone is engaged in a connected call on this call appearance
- Remote Ringing: Another phone is ringing for an incoming call to this call appearance
- Remote Held: Another phone has placed this call appearance on hold
- Remote Undefined: The share call state is not known (this phone is waiting for a notification from the application server)
- Registration Failed: This phone has failed to register with the proxy server for the corresponding extension
- Registering: The phone is attempting registration with the proxy server for the corresponding extension.
- Disabled: This line key on this phone is disabled
- Call Back: A call back (repeat dialing) operation is currently active on this call appearance

A

Cisco SPA IP Phone Field Reference

This appendix describes the fields within the following sections of the phone web user interface:

- Info Tab
- System Tab
- SIP Tab
- Provisioning Tab
- Regional Tab
- Phone Tab
- Ext Tab
- User Tab
- Attendant Console Tab (Cisco SPA500 Series)
- Attendant Console Status
- Cisco SPA525G or Cisco SPA525G2-Specific Tabs

Info Tab

The fields on this tab are read-only and cannot be edited.

System Information

Parameter	Description
Connection Type	Indicates the type of internet connection for the phone: ▪ DHCP ▪ Static IP ▪ PPPoE (only applicable to Cisco SPA525G or Cisco SPA525G2)
Current IP	Displays the current IP address assigned to the IP phone.
Host Name	Displays the current host name assigned to the SPA9000 (defaults to SipuraSPA).
Domain	Displays the network domain name of the SPA9000.
Current Netmask	Displays the network mask assigned to the SPA9000.
Current Gateway	Displays the default router assigned to the SPA9000.
Primary DNS	Displays the primary DNS server assigned to the SPA9000.
Secondary DNS	Displays the secondary DNS server assigned to the SPA9000.
Reboot History	Stores information about the last reboot/refresh reasons. When the phone is reset to factory defaults, this information is deleted. For each reboot, this parameter provides a reason and a time stamp.

Parameter	Description
NTP Enable (Cisco SPA525G or Cisco SPA525G2 only)	Shows if Network Time Protocol is enabled.
Primary NTP Server (Cisco SPA525G or Cisco SPA525G2 only)	IP Address of the primary NTP server.
Secondary NTP Server (Cisco SPA525G or Cisco SPA525G2 only)	IP Address of the secondary NTP server.
TFTP Server (Cisco SPA525G or Cisco SPA525G2 only)	Address of the TFTP server for provisioning.
Bluetooth Enabled (Cisco SPA525G or Cisco SPA525G2 only)	Shows if Bluetooth is enabled.
Bluetooth Firmware Version (Cisco SPA525G or Cisco SPA525G2 only)	Displays the Bluetooth firmware version.
Bluetooth Connected (Cisco SPA525G or Cisco SPA525G2 only)	Shows if a Bluetooth device is connected to the phone.
Bluetooth MAC (Cisco SPA525G or Cisco SPA525G2 only)	Shows the hardware address of the Bluetooth device.
Connected Device ID (Cisco SPA525G or Cisco SPA525G2 only)	Shows the name of the connected Bluetooth device.
Wireless Enabled (Cisco SPA525G or Cisco SPA525G2 only)	Shows if Wireless-G is enabled on the phone.
Wireless Connected (Cisco SPA525G or Cisco SPA525G2 only)	Shows if the phone is connected to the wireless network.

Parameter	Description
Wireless MAC (Cisco SPA525G or Cisco SPA525G2 only)	Shows the hardware address of the Wireless-G controller.
SSID (Cisco SPA525G or Cisco SPA525G2 only)	Shows the SSID, or name of the wireless router to which the phone is connected.
Standard Channel (Cisco SPA525G or Cisco SPA525G2 only)	Shows the wireless channel being used in the wireless connection.
Security Mode (Cisco SPA525G or Cisco SPA525G2 only)	Shows if wireless security is configured on the phone (yes or no).

Cisco SPA525G or Cisco SPA525G2-Specific Parameters:

Parameter	Description
NTP Enable	Shows if Network Time Protocol is enabled.
Primary NTP Server	IP Address of the primary NTP server.
Secondary NTP Server	IP Address of the secondary NTP server.
TFTP Server	Address of the TFTP server for provisioning.
Bluetooth Enabled	Shows if Bluetooth is enabled.
Bluetooth Firmware Version	Displays the Bluetooth firmware version.
Bluetooth Connected	Shows if a Bluetooth device is connected to the phone.
Bluetooth MAC	Shows the hardware address of the Bluetooth device.
Connected Device ID	Shows the name of the connected Bluetooth device.
Wireless Enabled	Shows if Wireless-G is enabled on the phone.

Parameter	Description
Wireless Connected	Shows if the phone is connected to the wireless network.
Wireless MAC	Shows the hardware address of the Wireless-G controller.
SSID	Shows the SSID, or name of the wireless router to which the phone is connected.
Standard Channel	Shows the wireless channel being used in the wireless connection.
Security Mode	Shows if wireless security is configured on the phone (yes or no).

Network Configuration (SPCP)

Parameter	Description
TFTP Server	Address of the TFTP server for provisioning.
Call Manager	IP address of the Unified Communications server.
Directories URL	Populated by the Unified Communications Server; points to the directory application server.
Services URL	Populated by the Unified Communications Server; points to the Cisco XML application server.
Authentication URL	Populated by the Unified Communications Server; points to the authentication server.
DHCP Address Released	Populated by the Unified Communications Server; indicates if the DHCP address has been released.

VPN Status (Cisco SPA525G or Cisco SPA525G2 Only)

Parameter	Description
VPN Connected	Indicates if the phone is connected to a VPN.
Client Address	IP address given to the phone from the VPN server.
Client Netmask	Netmask given to the phone from the VPN server.
Bytes Sent	Size of data sent from the phone.
Bytes Recv	Size of data received by the phone.

Product Information

Parameter	Description
Product Name	Model number of the IP phone.
Serial Number	Serial number of the IP phone.
Software Version	Version number of the IP phone software.
Hardware Version	Version number of the IP phone hardware.
MAC Address	Hardware address of the IP phone.
Client Certificate	Status of the client certificate, which authenticates the IP phone for use in the ITSP network. This field indicates if the client certificate is properly installed in the IP phone.
Customization	For an 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.
Licenses	Indicates any additional licenses that you have installed in the IP phone.

Phone Status

Parameter	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.
Broadcast Pkts Sent	Total number of broadcast packets sent.
Broadcast Bytes Sent	Total number of broadcast packets received.
Broadcast Pkts Recv	Total number of broadcast bytes sent.
Broadcast Bytes Recv	Total number of broadcast bytes received and processed.
Broadcast Pkts Dropped	Total number of broadcast packets received but not processed. Most codecs can handle up to 5% random packet drops as long as the packets are random and not in groups of two or more. Concurrent packet drops result in voice quality issues.
Broadcast Bytes Dropped	Total number of broadcast bytes received but not processed.
RTP Packets Sent	Total number of RTP packets sent (including redundant packets).
RTP Bytes Sent	Total number of RTP packets received (including redundant packets).
RTP Packets Recv	Total number of RTP bytes sent.
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 SIP messages received (including retransmissions).
SIP Messages Recv	Total number of bytes of SIP messages sent (including retransmissions).

Parameter	Description
SIP Bytes Recv	Total number of bytes of SIP messages received (including retransmissions).
External IP	External IP address used for NAT mapping.
Operational VLAN ID	ID of the VLAN currently in use if applicable. **NOTE** Not applicable to Cisco WIP310.
SW Port (Cisco SPA300 Series and Cisco SPA500 Series)	Displays the type of Ethernet connection from the IP phone to the switch.
PC Port (Cisco SPA303 and Cisco SPA500 Series)	Indicates whether the link from the IP phone to a device plugged into the PC port on the phone is up or down.

Ext Status

The following parameters show for each extension on the phone.

Parameter	Description
Registration State	Shows “Registered” if the phone is registered, “Not Registered” if the phone is not registered to the ITSP.
Last Registration At	Last date and time the line was registered.
Next Registration In	Number of seconds before the next registration renewal.
Message Waiting	Indicates whether the phone user has a new voice mail waiting: Yes or No. This is updated when voice mail notification is received.
Mapped SIP Port	Port number of the SIP port mapped by NAT.

Line/Call Status

The following parameters show for each line and call on the phone.

Parameter	Description
Call State	Status of the call.
Tone	Type of tone used by the call.
Encoder	Codec used for encoding.
Decoder	Codec used for decoding.
Type	Direction of the call.
Remote Hold	Indicates whether the far end has placed the call on hold.
Callback	Indicates whether the call was triggered by a call back request.
Peer Name	Name of the internal phone.
Peer Phone	Phone number of the internal phone.
Duration	Duration of the call.
Packets Sent	Number of packets sent.
Packets Recv	Number of packets received.
Bytes Sent	Number of bytes sent.
Bytes Recv	Number of bytes received.
Mapped RTP Port	The port mapped for Real Time Protocol traffic for the call.
Media Loopback	If the call is a loopback call, displays the loopback mode (source or mirror) and type (media or packet). If the call is not loopback, the field appears blank.
Decode Latency	Number of milliseconds for decoder latency.
Jitter	Number of milliseconds for receiver jitter.

Parameter	Description
Round Trip Delay	Number of milliseconds for delay in the RTP-to-RTP interface round trip.
End System Delay	Number of milliseconds for delay in the internal round trip within the reporting endpoint.
Packets Lost	Number of packets lost.
Packet Error	Number of invalid packets received.
Loss Rate	The fraction of RTP data packets from the source lost since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
Discard Rate	The fraction of RTP data packets from the source that have been discarded since the beginning of reception, due to late or early arrival, under-run or overflow at the receiving jitter buffer. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
Burst Duration	The mean duration, expressed in milliseconds, of the burst periods that have occurred since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
Gap Duration	The mean duration, expressed in milliseconds, of the gap periods that have occurred since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).

Parameter	Description
R Factor	Voice quality metric describing the segment of the call that is carried over this RTP session. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
MOS-LQ/MOS Listening	The estimated mean opinion score for listening quality (MOS-LQ) is a voice quality metric on a scale from 1 to 5, in which 5 represents excellent and 1 represents unacceptable. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
MOS-CQ/MOS Conversational	The estimated mean opinion score for conversational quality (MOS-CQ) is defined as including the effects of delay and other effects that would affect conversational quality. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).

Downloaded Ring Tone

Parameter	Description
Status	Indicates whether the phone is downloading a ring tone (and from where) or if it is idle.
Ring Tone 1	Information about the user downloaded ring tone 1: name, size, and time-stamp of the tone.
Ring Tone 2	Information about the user downloaded ring tone 2: name, size, and time-stamp of the tone.

System Tab

System Configuration

Parameter	Description
Restricted Access Domains (SIP)	This feature is used when implementing software customization.
Enable Web Server	Enable/disable web server of the IP phone. Defaults to yes.
Web Server Port	Port number of the phone web user interface. Defaults to 80.
SPA525-http-write (Cisco SPA525G or Cisco SPA525G2 SPCP only)	Allow Cisco Configuration Assistant (CCA) or other application to write XML file parameters directly to the phone using HTTP. Choose **yes** to allow this feature, or no to disable this feature.
Enable Web Admin Access	Lets you enable or disable local access to the phone web user interface. Select yes or no from the drop-down menu. Defaults to yes.
Admin Passwd	Password for the administrator. Defaults to no password.
User Password	Password for the user. Defaults to no password.

Parameter	Description
SPA525-protocol (Cisco SPA525G or Cisco SPA525G2 only)	Allows you to choose the type of protocol for the phone: ▪ SIP—Session Initiation Protocol. Choose if the phone is used with a SIP call control system, such as the Cisco SPA9000 or a SIP call control system from another provider such as BroadSoft or Asterisk. ▪ SPCP—Smart Phone Control Protocol. Choose if the phone is used with a Cisco Unified Communications Series server, such as the Cisco Unified Communications 500 Series for Small Business.
SPA525-auto-detect-sccp (Cisco SPA525G or Cisco SPA525G2 only)	Choose if the phone should automatically detect the type of protocol used on the network to which it is connected. If set to yes, the phone automatically discovers if it is connected to a call control system using SPCP.
SPA525-readonly (Cisco SPA525G or Cisco SPA525G2 only)	If set to **yes**, the Signaling Protocol and Auto Detect SCCP Settings on the phone are read only. If set to **no**, the above settings on the phone can be changed by the end user.
Phone-UI-user-mode	Allows you to restrict the menus and options that phone users see when they use the phone interface. Choose **yes** to enable this parameter and restrict access. The default is no. Specific parameters are then designated as “na” or “ro” using provisioning files. Parameters designated as “na” will not appear on the phone interface. Parameters designated as “ro” will not be editable by the user.

Internet Connection Type and Static IP Settings

Parameter	Description
Internet Connection Type	Choose the type of internet connection: ▪ DHCP ▪ Static IP ▪ PPPoE (not applicable to Cisco WIP310)
Static IP	If static IP was chosen as the type of internet connection, displays the static IP address assigned to the phone.
Netmask	If static IP was chosen as the type
Gateway	Default router IP address. Blank if DHCP assigned.
LAN MTU	LAN Maximum Transmission Unit size. Default value: 1500.
Ethernet MTU (Cisco SPA525G or Cisco SPA525G2 SPCP only)	Ethernet Maximum Transmission Unit size. Default value: 1500.
Duplex Mode	Duplex Mode—Choose one of the following to configure the speed/duplex for the phone Ethernet ports: ▪ Auto ▪ 10MBps/Duplex ▪ 10MBps/Half ▪ 100Mbps/Duplex ▪ 100MBps/Half

Power Settings (Cisco SPA500 Series or Cisco SPA300 Series Only)

Parameter	Description
PoE Power Required	Specifies the PoE power setting: Normal (default) or Maximum. When one or more attendant consoles are attached to the phone, use Maximum to advertise to a PoE switch that the phone will consume up to 12 watts. When no attendant consoles are attached, use Minimum to advertise a required power budget of 6.5 watts. This parameter is not applicable to Cisco SPA301 or SPA303 as they do not have Cisco Attendant Console support.

PPPoE Settings (Cisco SPA525G or Cisco SPA525G2 Only)

Parameter	Description
PPPoE Login Name	Specifies the account name assigned by the ISP for connecting on a Point-to-Point Protocol over Ethernet (PPPoE) link.
PPPoE Login Password	Specifies the password assigned by the ISP for connecting on a Point-to-Point Protocol over Ethernet (PPPoE) link.
PPPoE Service Name	Specifies the service name assigned by the ISP for connecting on a Point-to-Point Protocol over Ethernet (PPPoE) link.

Optional Network Configuration

Parameter	Description
Host Name	The host name of the SPA9000.
Domain	The network domain of the SPA9000.
Primary DNS	DNS server used by SPA9000 in addition to DHCP supplied DNS servers if DHCP is enabled; when DHCP is disabled, this is the primary DNS server. Defaults to 0.0.0.0.
Secondary DNS	DNS server used by SPA9000 in addition to DHCP supplied DNS servers if DHCP is enabled; when DHCP is disabled, this is the secondary DNS server. Defaults to 0.0.0.0.
DNS Server Order	Specifies the method for selecting the DNS server. The options are Manual, Manual/DHCP, and DHCP/Manual.
DNS Query Mode	Do parallel or sequential DNS Query. With parallel DNS query mode, the SPA9000 sends the same request to all the DNS servers at the same time when doing a DNS lookup, the first incoming reply is accepted by the SPA9000. Defaults to parallel.
Syslog Server	Specify the syslog server name and port. This feature specifies the server for logging IP phone system information and critical events. If both Debug Server and Syslog Server are specified, Syslog messages are also logged to the Debug Server.
Debug Server	The debug server name and port. This feature specifies the server for logging IP phone debug information. The level of detailed output depends on the debug level parameter setting.

Parameter	Description
Debug Level	The debug level from 0-3. The higher the level, the more debug information is generated. Zero (0) means no debug information is generated. To log SIP messages, you must set the Debug Level to at least 2. Defaults to 0.
Primary NTP Server	IP address or name of primary NTP server.
Secondary NTP Server	IP address or name of secondary NTP server.
Enable Bonjour (Cisco SPA525G or Cisco SPA525G2 only)	Enable Bonjour networking that is used by Office Manager and Cisco Configuration Assistant to discover the Cisco IP phones. Choose **yes** to enable or **no** to disable.

VLAN Settings

Not applicable to the Cisco WIP310.

Parameter	Description
Enable VLAN	Choose **Yes** to enable VLAN. Choose **no** to disable.
VLAN ID	If you use a VLAN without CDP (VLAN enabled and CDP disabled), enter a *VLAN ID* for the IP phone. Note that only voice packets are tagged with the VLAN ID. Do not use 1 for the VLAN ID.
Enable PC Port VLAN Tagging	Enables VLAN and priority tagging on the phone data port (802.1p/q). This feature facilities tagging of the VLAN ID (802.1Q) and priority bits (802.1p) of the traffic coming from the PC port of the IP phone. Defaults to No. Choose **Yes** to enable the tagging algorithm.

Parameter	Description
PC Port VLAN Highest Priority	0-7 (default 0). The priority applied to all frames, tagged and untagged. The phone modifies the frame priority only if the incoming frame priority is higher than this value.
PC Port VLAN ID	0-4095 (default 0). Value of the VLAN ID. The phone tags all the untagged frames coming from the PC (it will not tag frames with an existing tag).
Enable CDP	Enable CDP only if you are using a switch that has Cisco Discovery Protocol. CDP is negotiation based and determines which VLAN the IP phone resides in.
Enable LLDP-MED	Choose **yes** to enable LLDP-MED for the phone to advertise itself to devices that use that discovery protocol. When the LLDP-MED feature is enabled, after the phone has initialized and Layer 2 connectivity is established, the phone sends out LLDP-MED PDU frames. If the phone receives no acknowledgment, the manually configured VLAN or default VLAN will be used if applicable. If the CDP is used concurrently, the waiting period of 6 seconds is used. The waiting period will increase the overall startup time for the phone.
Network Startup Delay	Setting this value causes a delay for the switch to get to the forwarding state before the phone will send out the first LLDP-MED packet. The default delay is 3 seconds. For configuration of some switches, you might need to increase this value to a higher value for LLDP-MED to work. Configuring a delay can be important for networks that use Spanning Tree Protocol.

Wi-Fi Settings (Cisco SPA525G or Cisco SPA525G2 Only)

Parameter	Description
SPA525-wifi-on	Set to yes to enable Wireless-G service.

Bluetooth Settings (Cisco SPA525G or Cisco SPA525G2 Only)

Parameter	Description
Enable BT	Set to yes to enable support for Bluetooth devices.

VPN Settings (Cisco SPA525G or Cisco SPA525G2 Only)

Parameter	Description
VPN Server	The IP address of the VPN server to which the phone connects.
VPN User Name	Username configured on the VPN server for the phone.
VPN Password	Password associated with the username configured on the VPN for the phone.
VPN Tunnel Group	(Optional) The tunnel group, if required by the VPN server.
Connect on Bootup	If the phone should attempt to connect to the VPN each time it is powered on. Choose **yes** to have the phone try to automatically connect, or no to keep the default behavior.

SIP Tab

This section describes the fields for the SIP tab.

SIP Parameters

Parameter	Description
Max Forward	SIP Max Forward value, which can range from 1 to 255. Defaults to 70.
Max Redirection	Number of times an invite can be redirected to avoid an infinite loop. Defaults to 5.
Max Auth	Maximum number of times (from 0 to 255) a request may be challenged. Defaults to 2.
SIP User Agent Name	Used in outbound REGISTER requests. Defaults to $VERSION. If empty, the header is not included. Macro expansion of $A to $D corresponding to GPP_A to GPP_D allowed.
SIP Server Name	Server header used in responses to inbound responses. Defaults to $VERSION.
SIP Reg User Agent Name	User-Agent name to be used in a REGISTER request. If this is not specified, the <SIP User Agent Name> is also used for the REGISTER request. Defaults to blank.

Parameter	Description
SIP Accept Language	Accept-Language header used. To access, click the SIP tab, and fill in the SIP Accept Language field. There is no default (this indicates SPA9000 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. This field must match that of the Service Provider. Defaults to application/dtmf-relay.
Hook Flash MIME Type	MIME Type used in a SIP INFO message to signal a hook flash event. The default is application/hook-flash.
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. Defaults to 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 phone uses compact SIP headers in outbound SIP messages. If set to no, the phone uses normal SIP headers. If inbound SIP requests contain compact headers, the phone 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 phone substitutes those headers with compact headers (if defined by RFC-261) if <Use Compact Header> parameter is set to yes. Default: no

Parameter	Description
Escape Display Name	Lets you keep the Display Name private. Select yes if you want the IP phone 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. Defaults to yes.
SIP-B Enable	Enables SIP for Business (supports Sylantro call flows) call features.
Talk Package	Enables support for the BroadSoft Talk Package, which enables a user to answer or resume a call by clicking a button in an external application.
Hold Package	Enables support for the BroadSoft Hold Package, which enables a user to place a call on hold by clicking a button in an external application.
Conference Package	Enables support for the BroadSoft Conference Package, which enables a user to start a conference by clicking a button in an external application.
Notify Conference	If enabled, the unit will send out a NOTIFY with event=conference when starting a conference.
RFC 2543 Call Hold	If set to yes, unit will include c=0.0.0.0 syntax in SDP when sending a SIP re-INVITE to the peer to hold the call. If set to no, unit will not include the c=0.0.0.0 syntax in the SDP. The unit will always include a=sendonly syntax in the SDP in either case. Defaults to yes.

Parameter	Description
Random REG CID On Reboot	If set to yes, the Cisco IP phone uses a different random call-ID for registration after the next software reboot. If set to no, the Cisco IP phone tries to use the same call-ID for registration after the next software reboot. The Cisco IP phone always uses a new random Call-ID for registration after a power-cycle, regardless of this setting. Defaults to no.
Mark All AVT packets	If set to yes, all audio video transport (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. Defaults to yes.
SIP TCP Port Min	Specifies the lowest TCP port number that can be used for SIP sessions. Defaults to 5060.
SIP TCP Port Max	Specifies the highest TCP port number that can be used for SIP sessions. Defaults to 5080.
CTI Enable	The CTI interface allows a third-party application to control and monitor the state of a phone that has registered with the Cisco SPA9000. With this interface, an application can control a phone to initiate an outgoing call or answer an incoming call with a mouse click from a PC.
Caller ID Header	Provides the option to take the caller ID from PAID-RPID-FROM, P-ASSERTEDIDENTITY, REMOTE-PARTY-ID, or FROM header.

Parameter	Description
SRTP Method	Selects the method to use for SRTP. Two choices are available: ▪ x-sipura—legacy SRPT method ▪ s-descriptor—new method compliant with RFC-3711 and RFC-4568 The default value is "x-sipura." **NOTE** Not applicable to Cisco WIP310.
Hold Target Before REFER	Controls whether to hold call leg with transfer target before sending REFER to the transferee when initiating a fully-attended call transfer (where the transfer target has answered). Default value is "no," where the call leg is not held. **NOTE** Not applicable to Cisco WIP310.
Keep Referee When REFER Failed	Set this parameters to yes to configure the phone to immediately handle NOTIFY sipfrag messages. You can also configure this parameter in the configuration file: `<Keep_Referee_When_REFER_Failed ua="na">Yes</Keep_Referee_When_REFER_Failed>`

SIP Timer Values (sec)

Parameter	Description
SIP T1	RFC 3261 T1 value (RTT estimate) that can range from 0 to 64 seconds. Defaults to .5 seconds.
SIP T2	RFC 3261 T2 value (maximum retransmit interval for non-INVITE requests and INVITE responses) that can range from 0 to 64 seconds. Defaults to 4 seconds.
SIP T4	RFC 3261 T4 value (maximum duration a message remains in the network) that can range from 0 to 64 seconds. Defaults to 5 seconds.
SIP Timer B	INVITE time-out value that can range from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer F	Non-INVITE time-out value that can range from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer H	INVITE final response, time-out value that can range from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer D	ACK hang-around time that can range from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer J	Non-INVITE response hang-around time that can range from 0 to 64 seconds. Defaults to 16 seconds.
INVITE Expires	INVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 19999999999999999999999999999999. Defaults to 240 seconds.

Parameter	Description
RelNVITE Expires	RelNVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 199999999999999999999999999999. Defaults to 30
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. Defaults to 1 second.
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. Defaults to 7200.
Reg Retry Intvl (See note below)	Interval to wait before the SPA9000 retries registration after failing during the last registration. Defaults to 30.
Reg Retry Long Intvl (See note below)	When registration fails with a SIP response code that does not match<Retry Reg RSC>, the SPA9000 waits for the specified length of time before retrying. If this interval is 0, the SPA9000 stops trying. This value should be much larger than the Reg Retry Intvl value, which should not be 0. Defaults to 1200.
Reg Retry Random Delay	Random delay range (in seconds) to add to <Register Retry Intvl> when retrying REGISTER after a failure. This feature was added in Release 5.1. Defaults to blank, which disables this feature.

Parameter	Description
Reg Retry Long Random Delay	Random delay range (in seconds) to add to <Register Retry Long Intvl> when retrying REGISTER after a failure. This feature was added in Release 5.1. Defaults to blank, which disables this feature.
Reg Retry Intvl Cap	The maximum value to cap the exponential back-off retry delay (which starts at <Register Retry Intvl> and doubles on every REGISTER retry after a failure). In other words, the retry interval is always at <Register Retry Intvl> seconds after a failure. If this feature is enabled, <Reg Retry Random Delay> is added on top of the exponential back-off adjusted delay value. This feature was added in Release 5.1. Defaults to blank, which disables the exponential back-off feature.
Sub Min Expires	This value sets the lower limit of the REGISTER expires value returned from the Proxy server.
Sub Max Expires	This value sets the upper limit of the REGISTER min-expires value returned from the Proxy server in the Min-Expires header. Defaults to 7200.
Sub Retry Intvl	This value (in seconds) determines the retry interval when the last Subscribe request fails. Defaults to 10.

NOTE Cisco IP phones can use a RETRY-AFTER value when received from a SIP proxy server that is too busy to process a request (503 Service Unavailable message). If the response message includes a RETRY-AFTER header, the phone waits for the specified length of time before retrying to REGISTER again. If a RETRY-AFTER header is not present, the phone waits for the value specified in the *Reg Retry Interval* or the *Reg Retry Long Interval* parameter.

Response Status Code Handling

Parameter	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. Defaults to blank.
SIT2 RSC	SIP response status code to INVITE on which to play the SIT2 Tone. Defaults to blank.
SIT3 RSC	SIP response status code to INVITE on which to play the SIT3 Tone. Defaults to blank.
SIT4 RSC	SIP response status code to INVITE on which to play the SIT4 Tone. Defaults to blank.
Try Backup RSC	SIP response code that retries a backup server for the current request. Defaults to blank.
Retry Reg RSC	Interval to wait before the SPA9000 retries registration after failing during the last registration. Defaults to blank.

RTP Parameters

Parameter	Description
RTP Port Min	Minimum port number for RTP transmission and reception. Minimum port number for RTP transmission and reception. Should define a range that contains at least 10 even number ports (twice the number of lines); for example, configure RTP port min to 16384 and RTP port max to 16402. Defaults to 16384.
RTP Port Max	Maximum port number for RTP transmission and reception. Should define a range that contains at least 10 even number ports (twice the number of lines); for example, configure RTP port min to 16384 and RTP port max to 16402. Defaults to 16482.
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. Defaults to 0.030.
Max RTP ICMP Err	Number of successive ICMP errors allowed when transmitting RTP packets to the peer before the SPA9000 terminates the call. If value is set to 0, the SPA9000 ignores the limit on ICMP errors. Defaults to 0.

Parameter	Description
RTCP Tx Interval	Interval for sending out RTCP sender reports on an active connection. It can range from 0 to 255 seconds. During an active connection, the SPA9000 can be programmed to send out compound RTCP packet on the connection. Each compound RTP packet except the last one contains a SR (Sender Report) and a SDES (Source Description). The last RTCP packet contains an additional BYE packet. Each SR except the last one contains exactly 1 RR (Receiver Report); the last SR carries no RR. The SDES contains CNAME, NAME, and TOOL identifiers. The CNAME is set to <User ID>@<Proxy>, NAME is set to <Display Name> (or Anonymous if user blocks caller ID), and TOOL is set to the Vendor/Hardware-platform-software-version (such as Cisco/SPA9000-1.0.31(b)). The NTP timestamp used in the SR is a snapshot of the SPA9000 local time, not the time reported by an NTP server. If the SPA9000 receives a RR from the peer, it attempts to compute the round trip delay and show it as the <Call Round Trip Delay> value (ms) in the Info section of SPA9000 web page. Defaults to 0.

Parameter	Description
No UDP Checksum	Select yes if you want the SPA9000 to calculate the UDP header checksum for SIP messages. Otherwise, select no. Defaults to no.
Symmetric RTP	Enable symmetric RTP operation. If enabled, sends RTP packets to the source address and port of the last received valid inbound RTP packet. If disabled (or before the first RTP packet arrives) sends RTP to the destination as indicated in the inbound SDP. Defaults to no.
Stats In BYE	Determines whether the IP phone 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>. Defaults to no.

SDP Payload Types

The configured dynamic payloads are used for outbound calls only where the Cisco SPA9000 presents the SDP offer. For inbound calls with a SDP offer, the Cisco SPA9000 follows the caller dynamic payload type assignments.

The Cisco SPA9000 uses the configured codec names in its outbound SDP. The SPA9000 ignores the codec names in incoming SDP for standard payload types (0-95). For dynamic payload types, the Cisco SPA9000 identifies the codec by the configured codec names. Comparison is case-insensitive.

Parameter	Description
AVT Dynamic Payload	AVT dynamic payload type. Ranges from 96-127. Defaults to 101.
INFOREQ Dynamic Payload	INFOREQ dynamic payload type. Defaults to blank.
G726r16 Dynamic Payload	G.726-16 dynamic payload type. Ranges from 96-127. Defaults to 98. **NOTE** Not applicable to Cisco SPA525G or Cisco SPA525G2 or Cisco WIP310.
G726r24 Dynamic Payload	G.726-24 dynamic payload type. Ranges from 96-127. Defaults to 97. **NOTE** Not applicable to Cisco SPA525G or Cisco SPA525G2 or Cisco WIP310.
G726r40 Dynamic Payload	G.726-40 dynamic payload type. Ranges from 96-127. Defaults to 96. **NOTE** Not applicable to Cisco SPA525G or Cisco SPA525G2 or Cisco WIP310.
G729b Dynamic Payload	G729b Dynamic Payload type. Defaults to 99.
EncapRTP Dynamic Payload	EncapRTP Dynamic Payload type. Defaults to 112.
RTP-Start-Loopback Dynamic	RTP-Start-Loopback Dynamic Payload. Defaults to 113.

Parameter	Description
RTP-Start-Loopback Codec	RTP-Start-Loopback Codec. Select one of following: G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a, or G723. Cisco SPA525G or Cisco SPA525G2: G711u, G711a, G726-32, G729a, G722. Defaults to G711u.
AVT Codec Name	AVT codec name used in SDP. Defaults to telephone-event.
G711u Codec Name	G.711u codec name used in SDP. Defaults to PCMU.
G711a Codec Name	G.711a codec name used in SDP. Defaults to PCMA.
G726r16 Codec Name	G.726-16 codec name used in SDP. Defaults to G726-16. **NOTE** Not applicable to Cisco SPA525G or Cisco SPA525G2 or Cisco WIP310.
G726r24 Codec Name	G.726-24 codec name used in SDP. Defaults to G726-24. **NOTE** Not applicable to Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
G726r32 Codec Name	G.726-32 codec name used in SDP. Defaults to G726-32.
G726r40 Codec Name	G.726-40 codec name used in SDP. Defaults to G726-40. **NOTE** Not applicable to Cisco SPA525G or Cisco SPA525G2 or Cisco WIP310.
G729a Codec Name	G.729a codec name used in SDP. Defaults to G729a.

Parameter	Description
G729b Codec Name	G.729b codec name used in SDP. Defaults to G729ab.
G722 Codec Name	G.722 codec name used in SDP. Defaults to G722. **NOTE** Not supported on the Cisco WIP310.
EncapRTP Codec Name	EncapRTP codec name used in SDP. Defaults to encaprtp.

NAT Support Parameters

Parameter	Description
Handle VIA received	If you select yes, the phone processes the received parameter in the VIA header (this is inserted by the server in a response to any of its requests). If you select no, the parameter is ignored. Select yes or no from the drop-down menu. Defaults to no.
Handle VIA rport	If you select yes, the SPA9000 processes the rport parameter in the VIA header (this is inserted by the server in a response to any of its requests). If you select no, the parameter is ignored. Select yes or no from the drop-down menu. Defaults to 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. Defaults to no.

Parameter	Description
Insert VIA rport	Inserts the rport 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. Defaults to 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. Defaults to 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. Defaults to no.
STUN Enable	Enables the use of STUN to discover NAT mapping. Select yes or no from the drop-down menu. Defaults to no.
STUN Test Enable	If the STUN Enable feature is enabled and a valid STUN server is available, the SPA9000 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 SPA9000 detects symmetric NAT or a symmetric firewall, NAT mapping is disabled. Defaults to no.
STUN Server	IP address or fully-qualified domain name of the STUN server to contact for NAT mapping discovery. You can use a public STUN server or set up your own STUN server.

Parameter	Description
EXT IP	External IP address to substitute for the actual IP address of the SPA9000 in all outgoing SIP messages. If 0.0.0.0 is specified, no IP address substitution is performed. If this parameter is specified, the SPA9000 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. Defaults to blank.
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. Defaults to blank.
NAT Keep Alive Intvl	Interval between NAT-mapping keep alive messages. Defaults to 15.

Linksys Key System Parameters

Parameter	Description
Linksys Key System	Enable or disable the Linksys Key System on the IP phone. Defaults to yes.
Multicast Address	The multicast address is used by the Cisco SPA9000 to communicate with the Cisco SPA IP phones. Defaults to 224.168.168.168:6061.
Key System Auto Discovery	Enables or disables auto discovery of the call control server (for example, the Cisco SPA9000). Disable this feature for teleworkers or other scenarios where multicast does not work.
Key System IP Address	IP address of the call control server IP. Enter the IP address for teleworkers or other scenarios where multicast does not work.
Force LAN Codec	The choices are: none, G.711u, or G.711a. Defaults to none.

Provisioning Tab

For information about the Provisioning page, see the *Cisco Small Business IP Telephony Devices Provisioning Guide*.

Regional Tab

This section describes the fields for the Regional tab.

Call Progress Tone Description

Parameter	Description
Dial Tone	Prompts the user to enter a phone number. Defaults to 350@-19,440@-19;10(*/0/1+2).
Bluetooth Dial Tone (Cisco SPA525G or Cisco SPA525G2 only)	Indicates a bluetooth headset is paired and the user can make a call. Defaults to 350@-19,440@-19;1(0/*/0);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. Defaults to 420@-16;10(*/0/1).
Prompt Tone	Prompts the user to enter a call forwarding phone number. Defaults to 520@-19,620@-19;10(*/0/1+2).
Busy Tone	Played when a 486 RSC is received for an outbound call. Defaults to 480@-19,620@-19;10(.5/.5/1+2).

Parameter	Description
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. Defaults to 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. Defaults to 480@10,620@0;10(.125/.125/1+2).
Ring Back Tone	Played during an outbound call when the far end is ringing. Defaults to 440@-19,480@-19;*(2/4/1+2).
Call Waiting Tone	Played when a call is waiting. Defaults to 440@-10;30(.3/9.7/1)
Call Pickup Tone	The default value for this parameter is 440@-10;30(.3/9.7/1), which is the same as the call waiting tone. This feature appears as follows in the phone configuration file: `<Call_Pickup_Tone ua="na">440@-10;30(.3/9.7/1)</Call_Pickup_Tone>`
Confirm Tone	Brief tone to notify the user that the last input value has been accepted. Defaults to 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 theIP phone screen. Defaults to 985@-16,1428@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0).

Parameter	Description
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. Defaults to 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. Defaults to 480@10,620@0;10(.125/.125/1+2).
Ring Back Tone	Played during an outbound call when the far end is ringing. Defaults to 440@-19,480@-19;*(2/4/1+2).
Call Waiting Tone	Played when a call is waiting. Defaults to 440@-10;30(.3/9.7/1)
Call Pickup Tone	The default value for this parameter is 440@-10;30(.3/9.7/1), which is the same as the call waiting tone. This feature appears as follows in the phone configuration file: `<Call_Pickup_Tone ua="na">440@-10;30(.3/9.7/1)</Call_Pickup_Tone>`
Confirm Tone	Brief tone to notify the user that the last input value has been accepted. Defaults to 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 theIP phone screen. Defaults to 985@-16,1428@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0).

Parameter	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 IP phone screen. Defaults to 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 IP phone screen. Defaults to 914@-16,1371@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0)
SIT4 Tone	This is an 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 IP phone screen. Defaults to 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. Defaults to 350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2).
Cfwd Dial Tone	Played when all calls are forwarded. Defaults to 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. Defaults to 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. Defaults to 350@-19;20(.1/.1/1,.1/9.7/1).

Parameter	Description
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. Defaults to 397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2).
Page Tone	Specifies the tone transmitted when the paging feature is enabled. Defaults to 600@-16;.3(.05/0.05/1).
Alert Tone	Played when an alert occurs. Defaults to 600@-19;.2(.05/0.05/1).
System Beep	Audible notification tone played when a system error occurs. Defaults to 600@-16;.1(.05/0.05/1). **NOTE** Applies to Cisco SPA525G or Cisco SPA525G2 or Cisco WIP310 only.

Distinctive Ring Patterns

Parameter	Description
Cadence 1	Cadence script for distinctive ring 1. Defaults to 60(2/4).
Cadence 2	Cadence script for distinctive ring 2. Defaults to 60(.3/.2, 1/.2,.3/4).
Cadence 3	Cadence script for distinctive ring 3. Defaults to 60(.8/.4,.8/4).

Parameter	Description
Cadence 4	Cadence script for distinctive ring 4. Defaults to 60(.4/.2,.3/.2,.8/4).
Cadence 5	Cadence script for distinctive ring 5. Defaults to 60(.2/.2,.2/.2,.2/.2,1/4)
Cadence 6	Cadence script for distinctive ring 6. Defaults to 60(.2/.4,.2/.4,.2/4).
Cadence 7	Cadence script for distinctive ring 7. Defaults to 60(4.5/4).
Cadence 8	Cadence script for distinctive ring 8. Defaults to 60(0.25/9.75)
Cadence 9	Cadence script for distinctive ring 9. Defaults to 60(.4/.2,.4/2).

Control Timer Values (sec)

Parameter	Description
Reorder Delay	Delay after far end hangs up before reorder (busy) tone is played. 0 = plays immediately, inf = never plays. Range: 0–255 seconds. Set to 255 to return the phone immediately to on-hook status and to not play the tone. Defaults to 5.
Call Back Expires	Expiration time in seconds of a call back activation. Range: 0–65535 seconds. Defaults to 1800.
Call Back Retry Intvl	Call back retry interval in seconds. Range: 0–255 seconds. Defaults to 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 SPA9000 still considers the call as failed and keeps on retrying. Defaults to 0.5.
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. Defaults to 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. Defaults to 3.

Vertical Service Activation Codes

The following Vertical Service Activation Codes are automatically appended to the dial plan.

Parameter	Description
Call Return Code	This code calls the last caller. Defaults to *69.
Blind Transfer Code	Begins a blind transfer of the current call to the extension specified after the activation code. Defaults to *98.
Call Back Act Code	Starts a callback when the last outbound call is not busy. Defaults to *66.
Call Back Deact Code	Cancels a callback. Defaults to *86.
Cfwd All Act Code	Forwards all calls to the extension specified after the activation code. Defaults to *72.
Cfwd All Deact Code	Cancels call forwarding of all calls. Defaults to *73.
Cfwd Busy Act Code	Forwards busy calls to the extension specified after the activation code. Defaults to *90.
Cfwd Busy Deact Code	Cancels call forwarding of busy calls. Defaults to *91.
Cfwd No Ans Act Code	Forwards no-answer calls to the extension specified after the activation code. Defaults to *92.

Parameter	Description
Cfwd No Ans Deact Code	Cancels call forwarding of no-answer calls. Defaults to *93.
CW Act Code	Enables call waiting on all calls. Defaults to *56.
CW Deact Code	Disables call waiting on all calls. Defaults to *57.
CW Per Call Act Code	Enables call waiting for the next call. Defaults to *71.
CW Per Call Deact Code	Disables call waiting for the next call. Defaults to *70.
Block CID Act Code	Blocks caller ID on all outbound calls. Defaults to *67.
Block CID Deact Code	Removes caller ID blocking on all outbound calls. Defaults to *68.
Block CID Per Call Act Code	Blocks caller ID on the next outbound call. Defaults to *81.
Block CID Per Call Deact Code	Removes caller ID blocking on the next inbound call. Defaults to *82.
Block ANC Act Code	Blocks all anonymous calls. Defaults to *77.
Block ANC Deact Code	Removes blocking of all anonymous calls. Defaults to *87.
DND Act Code	Enables the do not disturb feature. Defaults to *78.

Parameter	Description
DND Deact Code	Disables the do not disturb feature. Defaults to *79.
Secure All Call Act Code	Makes all outbound calls secure. Defaults to *16.
Secure No Call Act Code	Makes all outbound calls not secure. Defaults to *17.
Secure One Call Act Code	Makes the next outbound call secure. (It is redundant if all outbound calls are secure by default.) Defaults to *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.) Defaults to *19.
Paging Code	The star code used for paging the other clients in the group. Defaults to *96.
Call Park Code	The star code used for parking the current call. Defaults to *38.
Call Pickup Code	The star code used for picking up a ringing call. Defaults to *36.
Call UnPark Code	The star code used for picking up a call from the call park. Defaults to *39.
Group Call Pickup Code	The star code used for picking up a group call. Defaults to *37.
Media Loopback Code	The star code used for media loopback. Defaults to *03.

Parameter	Description
Referral Services Codes	These codes tell the SPA9000 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 SPA9000 to perform a blind transfer to a target number that is prepended by the service *code. For example, after the user dials *98, the SPA9000 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 SPA9000 sends a blind REFER to the holding party with the Refer-To target equals to *98<target_number>. This feature allows the Cisco SPA9000 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 Cisco SPA9000. You can empty the corresponding *code that you do not want to Cisco SPA9000 to process.

Parameter	Description
Feature Dial Services Codes	These codes tell the Cisco SPA9000 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, and so forth. The maximum total length is 79 characters. 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 Cisco SPA9000 to call the target number prepended by the *code. For example, after user dials *72, the Cisco SPA9000 plays a prompt tone awaiting the user to enter a valid target number. When a complete number is entered, the Cisco SPA9000 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).

Parameter	Description
Feature Dial Services Codes (continued	The *codes should not conflict with any of the other vertical service codes internally processed by the Cisco SPA9000. You can empty the corresponding *code that you do not want to Cisco SPA9000 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 without 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 Cisco SPA9000 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 SPA9000 send INVITE *73@..... as usual when user dials *73.

Vertical Service Announcement Codes

- Service Annc (Announcement) Base Number: Defaults to blank.
- Service Annc (Announcement) Extension Codes: Defaults to blank.

Outbound Call Codec Selection Codes

These codes automatically appended to the dial plan. You do not need to include them in the dial plan.

Parameter	Description
Prefer G711u Code	Makes this codec the preferred codec for the associated call. Defaults to *017110.
Force G711u Code	Makes this codec the only codec that can be used for the associated call. Defaults to *027110.
Prefer G711a Code	Makes this codec the preferred codec for the associated call. Defaults to *017111
Force G711a Code	Makes this codec the only codec that can be used for the associated call. Defaults to *027111.
Prefer G722 Code	Makes this codec the preferred codec for the associated call. Defaults to *01722. Only one G.722 call at a time is allowed. If a conference call is placed, a SIP re-invite message is sent to switch the calls to narrowband audio. **NOTE** Not supported on the Cisco WIP310.

Parameter	Description
Force G722 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02722. Only one G.722 call at a time is allowed. If a conference call is placed, a SIP re-invite message is sent to switch the calls to narrowband audio. **NOTE** Not supported on the Cisco WIP310.
Prefer L16 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *01016.
Force L16 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02016.
Prefer G723 Code	Makes this codec the preferred codec for the associated call. Defaults to *01723. **NOTE** Not applicable to Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
Force G723 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02723. **NOTE** Not applicable to Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
Prefer G726r16 Code	Makes this codec the preferred codec for the associated call. Defaults to *0172616. **NOTE** Not applicable to Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.

Parameter	Description
Force G726r16 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *0272616. **NOTE** Not applicable to Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
Prefer G726r24 Code	Makes this codec the preferred codec for the associated call. Defaults to *0172624. **NOTE** Not applicable to Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
Force G726r24 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *0272624. **NOTE** Not applicable to Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
Prefer G726r32 Code	Makes this codec the preferred codec for the associated call. Defaults to *0172632.
Force G726r32 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *0272632.
Prefer G726r40 Code	Makes this codec the preferred codec for the associated call. Defaults to *0172640. **NOTE** Not applicable to Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.

Parameter	Description
Force G726r40 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *0272640. **NOTE** Not applicable to Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
Prefer G729a Code	Makes this codec the preferred codec for the associated call. Defaults to *01729.
Force G729a Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02729.

Time (Cisco SPA525G or Cisco SPA525G2 Only)

Parameter	Description
Time Zone	Selects the number of hours to add to GMT to generate the local time for caller ID generation. Choices are GMT-12:00, GMT-11:00,..., GMT, GMT+01:00, GMT+02:00, ..., GMT+13:00. Defaults to GMT-08:00.
Time Offset	This specifies the offset from GMT to use for the local system time.
Daylight Saving Time Rule	See **Daylight Saving Time Rule** in **Miscellaneous**.
Daylight Saving Time Enable	Select **yes** to enable Daylight Saving Time.

Language (Cisco SPA525G or Cisco SPA525G2 Only)

Parameter	Description
Dictionary Server Script.	See **Dictionary Server Script** in **Miscellaneous**.
Language Selection	See **Language Selection** in **Miscellaneous**.

Miscellaneous

Parameter	Description
Set Local Date (mm/dd)	Sets the local date (mm represents the month and dd represents the day). The year is optional and uses two or four digits. **NOTE** Not applicable to the Cisco SPA525G or Cisco SPA525G2.
Set Local Time (HH/mm)	Sets the local time (hh represents hours and mm represents minutes). Seconds are optional. **NOTE** Not applicable to the Cisco SPA525G or Cisco SPA525G2.
Time Zone	Selects the number of hours to add to GMT to generate the local time for caller ID generation. Choices are GMT-12:00, GMT-11:00,..., GMT, GMT+01:00, GMT+02:00, ..., GMT+13:00. Defaults to GMT-08:00. **NOTE** Found in the **Time** section for the Cisco SPA525G or Cisco SPA525G2.
Time Offset (HH/mm)	This specifies the offset from GMT to use for the local system time. **NOTE** Found in the **Time** section for the Cisco SPA525G or Cisco SPA525G2.

Parameter	Description
Daylight Saving Time Rule	Enter the rule for calculating daylight saving time; it should include the start, end, and save values. This rule is comprised of three fields. Each field is separated by ; (a semicolon) as shown below. Optional values inside [ ] (the brackets) are assumed to be 0 if they are not specified. Midnight is represented by 0:0:0 of the given date. This is the format of the rule: Start = <start-time>; end=<end-time>; save = <save-time>. The <start-time> and <end-time> values specify the start and end dates and times of daylight saving time. Each value is in this format: <month> /<day> / <weekday>[/HH:[mm[:ss]]] The <save-time> value is the number of hours, minutes, and/or seconds to add to the current time during daylight saving time. The <save-time> value can be preceded by a negative (-) sign if subtraction is desired instead of addition. The <save-time> value is in this format: [/[+|-]HH:[mm[:ss]]] The <month> value equals any value in the range 1-12 (January-December). The <day> value equals [+|-] any value in the range 1-31. If <day> is 1, it means the <weekday> on or before the end of the month (in other words the last occurrence of < weekday> in that month).

Parameter	Description
Daylight Saving Time Rule (continued)	The <weekday> value equals any value in the range 1-7 (Monday-Sunday). It can also equal 0. If the <weekday> value is 0, this means that the date to start or end daylight saving is exactly the date given. In that case, the <day> value must not be negative. If the <weekday> value is not 0 and the <day> value is positive, then daylight saving starts or ends on the <weekday> value on or after the date given. If the <weekday> value is not 0 and the <day> value is negative, then daylight saving starts or ends on the <weekday> value on or before the date given. Where: HH stands for hours (0-23). mm stands for minutes (0-59). ss stands for seconds (0-59). The default Daylight Saving Time Rule is start=4/1/7;end=10/-1/7;save=1. **NOTE** Found in the **Time** section for the Cisco SPA525G or Cisco SPA525G2.
Daylight Saving Time Enable	Select yes to enable Daylight Saving Time. **NOTE** Found in the **Time** section for the Cisco SPA525G or Cisco SPA525G2.
DTMF Playback Level	Local DTMF playback level in dBm, up to one decimal place. Defaults to -16.
DTMF Playback Length	Local DTMF playback duration in milliseconds. Defaults to .1.
Inband DTMF Boost	Controls the amount of amplification applied DTMF signals. Choices are OdB, 3dB, 6dB, 9dB, 12dB, 15dB, or 18dB. Defaults to 12dB.

Parameter	Description

Dictionary Server Script/SCCP Dictionary Server Script (Cisco SPA525G or Cisco SPA525G2 SCCP only)	Defines the location of the dictionary server, the languages available and the associated dictionary. The syntax is as follows:
	`<Dictionary_Server_Script ua="na">`
	`</Dictionary_Server_Script>`
	Defaults to blank and the maximum number of characters is 512. The detailed format is as follows:
	`serv={server ip port and root path};`
	`d0=<language0>;x0=<dictionary0 filename>;`
	`d1=<language1>;x1=<dictionary1 filename>;`
	`d2=<language2>;x2=<dictionary2 filename>;`
	`d3=<language3>;x3=<dictionary3 filename>;`
	`d4=<language4>;x4=<dictionary4 filename>;`
	`d5=<language5>;x5=<dictionary5 filename>;`
	`d6=<language6>;x6=<dictionary6 filename>;`
	`d7=<language3>;x7=<dictionary7 filename>;`
	`d8=<language8>;x8=<dictionary8 filename>;`
	`d9=<language5>;x9=<dictionary9 filename>;`

Parameter	Description
	The following is an example value: <Dictionary_Server_Script ua="na"> serv=tftp://192.168.1.119/ ;d0=English;x0=enS_v101.xml;d1=Spanish;x1 =esS_v101.xml </Dictionary_Server_Script> **NOTE** Not applicable to the Cisco WIP310.
Language Selection/ SCCP Language Selection (Cisco SPA525G or Cisco SPA525G2 SCCP Only)	Specifies the default language. The value needs to match one of the languages supported by the dictionary server. The script (dx value) is as follows: <Language_Selection ua="na"> </Language_Selection> Defaults to blank and the maximum number of characters is 512. The following is an example: <Language_Selection ua="na"> Spanish </Language_Selection> **NOTE** Not applicable to the Cisco WIP310.
Default Character Encoding (Cisco SPA303, Cisco SPA500 Series)	The default is ISO-8859-1 for backward compatibility with Cisco SPA900 series phones. If set to UTF-8, line keys and other labels entered by using the phone web user interface containing UTF-8 characters are displayed correctly on the phone. (SIP only)

Phone Tab

This section describes the fields for the Phone tab.

General

Parameter	Description
Station Display Name	Name to identify the IP phone; appears on the IP phone screen on models that have a display. You can use spaces in this field and the name does not have to be unique. If both the Station Display Name and Station Name fields are populated, the Station Display Name field takes precedence and is displayed on the phone.
Station Name	Name to identify this IP phone; appears on the IP phone screen on models that have a display. No spaces are allowed and the name must be unique.
Voice Mail Number	Phone number or URL to check voice mail. The service provider often hosts a voice mail service. The advantages of hosted voice mail include: ▪ Advanced features such as voice mail to email conversion. ▪ Calls can go to voice mail when the broadband connection is down.

Parameter	Description

Text Logo	Text logo to display when the phone boots up. A service provider, for example, can enter logo text as follows:
	▪ Up to 2 lines of text
	▪ Each line must be fewer than 32 characters
	▪ Insert a new line character (\n) between lines
	▪ Insert escape code %0a
	For example, `Super\n%0aTelecom` displays:
	`Super`
	`Telecom`
	Use the + character to add spaces for formatting. For example, you can add multiple + characters before and after the text to center it.
	NOTE Not applicable to the Cisco WIP310, Cisco SPA301, or Cisco SPA501G. On the Cisco SPA525G or Cisco SPA525G2, this setting is located on the **User** tab.

BMP Picture Download URL	URL locating the bitmap (.BMP) file to display on the IP phone screen background. For more information, see **Configuring Phone Information and Display Settings**. **NOTE** Not applicable to the Cisco WIP310, Cisco SPA301, or Cisco SPA501G. On the Cisco SPA525G or Cisco SPA525G2, this setting is located on the **User** tab.
Select Logo	Select from Default, BMP Picture, Text Logo, or None. Defaults to Default. **NOTE** Not applicable to the Cisco WIP310, Cisco SPA301, or Cisco SPA501G. On the Cisco SPA525G or Cisco SPA525G2, this setting is located on the **User** tab.

Parameter	Description
Select Background Picture	Select from Default, BMP Picture, or None. Defaults to Default. **NOTE** Not applicable to the Cisco WIP310, Cisco SPA301, or Cisco SPA501G. On the Cisco SPA525G or Cisco SPA525G2, this setting is located on the **User** tab.
Softkey Labels Font	Choose the font width for the softkey labels to display on your phone. See **Customizing Phone Softkeys**. **NOTE** Not applicable to the Cisco WIP310, Cisco SPA301, or Cisco SPA501G.
Screen Saver Enable	Enables a screen saver on the IP phone screen. When the phone is idle for a specified time, it enters screen saver mode. (Users can set up screen savers directly using phone Setup button.) Any button press or on/off hook event triggers the phone to return to its normal mode. (The screen shows `Press any key to unlock your phone`.) If a user password is set, the user must enter it to exit screen saver mode. **NOTE** Not applicable to the Cisco WIP310, Cisco SPA301, or Cisco SPA501G. On the Cisco SPA525G or Cisco SPA525G2, this setting is located on the **User** tab.
Screen Saver Wait	Amount of idle time before screen saver displays. **NOTE** Not applicable to the Cisco WIP310, Cisco SPA301, or Cisco SPA501G. On the Cisco SPA525G or Cisco SPA525G2, this setting is located on the **User** tab.

Parameter	Description
Screen Saver Icon	In screen saver mode, the IP phone screen can display: ▪ A background picture. ▪ The station time in the middle of the screen. ▪ A moving padlock icon. When the phone is locked, the status line displays a scrolling message “Press any key to unlock your phone.” ▪ A moving phone icon. ▪ The station date and time in the middle of the screen. **NOTE** Not applicable to the Cisco WIP310, Cisco SPA301, or Cisco SPA501G. On the Cisco SPA525G or Cisco SPA525G2, this setting is located on the **User** tab.
JPEG Logo Download URL (Cisco SPA525G or Cisco SPA525G2)	URL from which to download a .jpg file for the phone logo display.
JPEG Wallpaper Download URL (Cisco SPA525G or Cisco SPA525G2)	URL from which to download a .jpg file for the phone wallpaper.
Enable SMS	Enables sending and receiving of SMS text messages on the phone. **NOTE** Cisco WIP310 only.

Line Key

When used in the configuration profile, parameters in this section must be appended with *n*, where *n* represents line 1, 2, 3, 4, 5 or 6. For more information on these parameters, see **Configuring Lines**.

NOTE Does not apply to the Cisco WIP310.

Parameter	Description
Extension	Extension number of the line key.
Short Name	A short label shown on the IP phone screen for Line Key 1 through Line Key 6.
Share Call Appearance	**Yes** indicates that Line Key 1/2/3/4/5/6 is a shared call appearance. Otherwise this call appearance is not shared (it is private). Defaults to no.
Extended Function	Use to assign Busy Lamp Field, Call Pickup, and Speed Dial Functions to Idle Lines on the IP phone. Syntax is: `fnc=type;sub=stationname@$PROXY;ext=extension#@$PROXY` where: ▪ fnc: function ▪ blf: busy lamp field ▪ cp: call pickup ▪ sub: station name (not needed for speed dial) ▪ ext or usr: extension or user (the usr and ext keywords are interchangeable) **NOTE** Not applicable to the Cisco WIP310, Cisco SPA301, or Cisco SPA501G.

Miscellaneous Line Key Settings

Does not apply to the Cisco WIP310.

Parameter	Description
SCA Line ID Mapping	Specifies the shared call appearance line ID mapping. Choose Vertical First or Horizontal First. Each LED can hold multiple calls and the first call on an LED makes it light up. Horizontal first means the second call makes the same LED flash. Vertical first means the second call lights up the next LED. For example, if Extension 101 is assigned to two LEDs, and Vertical First is selected, the second call on Extension 101 lights up the second LED. The third call makes the first LED flash, and the fourth call makes the second LED flash. If Horizontal First is selected, the second call on Extension 101 makes the first LED flash. The third call lights up the second LED, and the fourth call makes the second LED flash.
SCA Barge-In Enable	Enables the SCA Barge-In. Defaults to no.
SCA Sticky Auto Line Seize	When enabled, taking the phone off-hook will not automatically pick up an incoming call on a shared line.
Call Appearance Per Line	Specifies how many calls per line to allow. You can choose a value from 2 (default) to the maximum value of 10. This parameter is not supported on the Cisco SPA501G and Cisco SPA301 phones. Also, this parameter is only supported when the phones are operating in the SIP mode.

Line Key LED Pattern

Does not apply to the Cisco WIP310.

Parameter	Description
Idle LED	The call appearance is not is in use and is available to make a new call. Leaving this entry blank indicates the default value of c=g.
Remote Undefined LED	The shared call state is undefined (the phone is still waiting for the state information from the application server). Not applicable if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Seized LED	This phone has seized the call appearance to prepare for a new outbound call. Leaving this entry blank indicates the default value of c=r.
Remote Seized LED	The shared call appearance is seized by another phone. Not application if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Progressing LED	This phone is attempting on this call appearance an outgoing call that is in proceeding (i.e. the called number is ringing). Leaving this entry blank indicates the default value of c=r.
Remote Progressing LED	Another phone is attempting on this shared call appearance an outbound call that is progressing. Not applicable if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Ringing LED	The call appearance is ringing. Leaving this entry blank indicates the default value of c=r;p=f.
Remote Ringing LED	The shared call appearance is in ringing on another phone. Not applicable if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.

Parameter	Description
Local Active LED	The call appearance is engaged in an active call. Leaving this entry blank indicates the default value of c=r.
Remote Active LED	Another station is engaged in an active call on this shared call appearance. Not applicable is this call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Held LED	The call appearance is held by this phone. Leaving this entry blank indicates the default value of c=r;p=s.
Remote Held LED	Another phone has placed this call appearance on hold. Not applicable if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r,p=s.
Register Failed LED	The corresponding extension has failed to register with the proxy server. Leaving this entry blank indicates the default value of c=a.
Disabled LED	The Call Appearance is disabled (not available for any incoming or outgoing call). Leaving this entry blank indicates the default value of c=o.
Registering LED	The corresponding extension is trying to register with the proxy server. Leaving this entry blank indicates the default value of c=r;p=s.
Call Back Active LED	Call Back operation is currently active on and this call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=s.
Trunk In-Use LED	A shared trunk is in use.
Trunk No Service LED	A shared trunk is not in service.
Trunk Reserved LED	A shared trunk has been reserved.

Supplementary Services

Enable or disable the corresponding supplementary services on the phone. A value of **yes** indicates enabled; **no** indicates disabled.

Parameter	Description
Conference Serv	Enable/disable Three way conference service. Defaults to yes.
Attn Transfer Serv	Enable/disable attended-call-transfer service. Defaults to yes.
Blind Transfer Serv	Enable/disable blind-call-transfer service. Defaults to yes.
DND Serv	Enable/disable do-not-disturb service. Defaults to yes.
Block ANC Serv	Enable/disable block-anonymous-call service. Defaults to yes.
Call Back Serv	Enable/disable call-back (aka. repeating dialing) service. Defaults to yes.
Block CID Serv	Enable/disable blocking outbound Caller-ID service. Defaults to yes.
Secure Call Serv	Enable/disable secure-call service. Defaults to yes.
Cfwd All Serv	Enable/disable call-forward-all service. Defaults to yes.
Cfwd Busy Serv	Enable/disable call-forward-on-busy service. Defaults to yes.

Parameter	Description
Cfwd On No Ans Serv	Enable/disable call-forward-on-no-answer service. Defaults to yes.
Paging Serv	Enable/disable the paging service. Defaults to yes.
Call Park Serv	Enable/disable the call park service. Defaults to yes.
Call Pick Up Serv	Enable/disable the call pickup service. Defaults to yes.
ACD Login Serv	Enable/disable the ACD Login Service, used for call centers. Typically enabled with the <SIP-B> parameter. Defaults to no.
Group Call Pick Up Serv	Enable/disable the group call pickup service. Defaults to yes.
Group Call Pick Up Serv	Enable/disable the group call pickup service. Defaults to yes.
ACD Ext	The extension used for handling ACD calls. Select from 1, 2, 3, 4, 5, or 6. Defaults to 1.
Service Annc Serv	Enable/disable sending announcement requests to a customer-supplied announcement server. Defaults to no.
Web Serv (Cisco SPA525G or Cisco SPA525G2 only)	Enable/disable the web server. Defaults to yes.
SMS Serv (Cisco SPA525G or Cisco SPA525G2 only)	Enable/disable the SMS text messaging server.

Ring Tone (Cisco SPA300 Series and Cisco SPA500 Series)

Each entry defines a ring tone to be used on the phone, with an ID between 1 and 12. The ID can be used in a DirEntry to indicate which ring tone to use when the corresponding caller calls.

Parameter	Description
Ring1	Ring tone script for ring 1. Defaults to n=Classic-1;w=3;c=1.
Ring2	Ring tone script for ring 2. Defaults to n=Classic-2;w=3;c=2.
Ring3	Ring tone script for ring 3. Defaults to n=Classic-3;w=3;c=3.
Ring4	Ring tone script for ring 4. Defaults to n=Classic-4;w=3;c=4.
Ring5	Ring tone script for ring 5. Defaults to n=Simple-1;w=2;c=1.
Ring6	Ring tone script for ring 6. Defaults to n=Simple-2;w=2;c=2.
Ring7	Ring tone script for ring 7. Defaults to n=Simple-3;w=2;c=3.
Ring8	Ring tone script for ring 8. Defaults to n=Simple-4;w=2;c=4.
Ring9	Ring tone script for ring 9. Defaults to n=Simple-5;w=2;c=5.
Ring10	Ring tone script for ring 10. Defaults to n=Office;w=4;c=1.
Ring11	(Cisco SPA300 Series and Cisco SPA500 Series) Ring tone script for ring 11. Defaults to n=Pulse;w=5;c=1. (Cisco SPA525G or Cisco SPA525G2) Ring tone script for ring 11. Defaults to n=Pulse;w=file://Pulse1.raw;c=1.
Ring12	(Cisco SPA300 Series and Cisco SPA500 Series) Ring tone script for ring 12. Defaults to n=Du-dut;w=6;c=1. (Cisco SPA525G or Cisco SPA525G2) Ring tone script for ring 11. Defaults to n=Du-dut;w=file://Ring7.raw;c=1.

In addition to these two ring tones, four user-configurable ring tones were added:

Label	Value of the w Parameter
Warble	(Cisco SPA300 Series and Cisco SPA500 Series) w=7 ((Cisco SPA525G or Cisco SPA525G2)) w=file://Warble.raw
Low	(Cisco SPA300 Series and Cisco SPA500 Series) w=8 ((Cisco SPA525G or Cisco SPA525G2)) w=file://Low.raw
Floor	(Cisco SPA300 Series and Cisco SPA500 Series) w=9 ((Cisco SPA525G or Cisco SPA525G2)) w=file://Floor.raw
Reverb	(Cisco SPA300 Series and Cisco SPA500 Series) w=10 ((Cisco SPA525G or Cisco SPA525G2)) w=file://Reverb.raw

These four ring tones must be provisioned or configured by using the phone web user interface.

Ring Tone (Cisco WIP310)

Parameter	Description
Keypad Tone	Select **yes** to enable the keypad tone to be played when a key on the keypad is pressed. Select no to silence the keypad.
Keypad Tone Volume	Corresponds to the volume of the keypad tone. Default is 5.

Auto Input Gain (dB)

NOTE Does not apply to the Cisco WIP310.

Parameter	Description
Handset Input Gain	The amount of amplification to apply to the audio input signal for the handset. Defaults to zero.
Headset Input Gain	The amount of amplification to apply to the audio input signal for the headset. Defaults to zero. **NOTE** Not applicable to the Cisco SPA301 or the Cisco SPA501G.
Speakerphone Input Gain	The amount of amplification to apply to the audio input signal for the speakerphone. Defaults to zero. **NOTE** Not applicable to the Cisco SPA301 or the Cisco SPA501G.
Bluetooth Input Gain (Cisco SPA525G or Cisco SPA525G2 only)	The amount of amplification to apply to the audio input signal for the Bluetooth device. Defaults to zero.
Handset Additional Input Gain	Applies additional input gain to the handset. **NOTE** Does not apply to the Cisco SPA525G or Cisco SPA525G2.
Headset Additional Input Gain	Applies additional input gain to the headset. **NOTE** Does not apply to the Cisco SPA525G or Cisco SPA525G2, or the Cisco SPA501G.
Speakerphone Additional Input Gain	Applies additional input gain to the speakerphone. **NOTE** Does not apply to the Cisco SPA301 or Cisco SPA525G or Cisco SPA525G2 or Cisco SPA501G.

Multiple Paging Group Parameters

You can configure a phone as part of a paging group by using a Group Paging Script. Users can then direct pages to specific groups of phones. A phone can be part of no more than two paging groups, and user can page a maximum of five paging groups.

Syntax:

```
pggrp=ip-address:port;[name=xxx;]num=xxx;
[listen={yes|no}]];
```

Where:

IP address: Multicast IP address of the phone that listens for and receives pages.

port: Port on which to page; you must use different ports for each paging group.

name (optional): The name of the paging group. In this name, do not use the pggrp string because it is reserved. Using it causes the script not to work, as in these examples:

```
pggrp=224.168.168.168:3141;name=ITGPgGrp;
num=800;listen=yes;
```

```
pggrp=224.168.168.168:3141;name=PgGrp;num=800;listen=yes;
```

num: The number users dial to access the paging group; must be unique to the group.

listen: If the phone should listen on the page group. Only the first two groups with listen set to yes will listen to group pages. If the field is not defined, the default value is no, so you must set this field to listen to the group pages.

BroadSoft Settings

The Cisco SPA300 Series and Cisco SPA500 Series supports the BroadSoft directory feature and synchronization of Do Not Disturb and Call Forward.

Parameter	Description
Directory Enable	Set to **yes** to enable BroadSoft directory for the phone user. Defaults to no. **NOTE** Not applicable to the Cisco SPA301 or Cisco SPA501G.
XSI Host Server	Enter the name of the server; for example, xsp.xdp.broadsoft.com. **NOTE** Not applicable to the Cisco SPA301 or Cisco SPA501G.
Directory Name	Name of the directory. Displays on the user phone as a directory choice. **NOTE** Not applicable to the Cisco SPA301 or Cisco SPA501G.

Parameter	Description
Directory Type	Select the type of BroadSoft directory: Enterprise (default): Allows users to search on last name, first name, user or group ID, phone number, extension, department, or email address. Group: Allows users to search on last name, first name, user ID, phone number, extension, department, or email address. Personal: Allows users to search on last name, first name, or telephone number. **NOTE** Not applicable to the Cisco SPA301 or Cisco SPA501G.
Directory UserID	BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com. **NOTE** Not applicable to the Cisco SPA301 or Cisco SPA501G.
Directory Password	Alphanumeric password associated with the User ID. **NOTE** Not applicable to the Cisco SPA301 or Cisco SPA501G.

LDAP Corporate Directory Search

If using Active Directory with authentication set to MD5, you must first configure the following:

- Click the **System** tab. In the **Optional Network Configuration** section, under **Primary DNS**, enter the IP address of the DNS server.
- In the **Optional Network Configuration** section, under **Domain**, enter the Lightweight Directory Access Protocol (LDAP) domain.

NOTE Does not apply to the Cisco WIP310, Cisco SPA301, or Cisco SPA501G.

Parameter	Description
LDAP Dir Enable	Choose **yes** to enable LDAP.
LDAP Corp Dir Name	Enter a free-form text name, such as “Corporate Directory.”
LDAP Server	Enter a fully qualified domain name or IP address of LDAP server, in the following format: `nnn.nnn.nnn.nnn`
LDAP Auth Method	Select the authentication method that the LDAP server requires. Choices are: None—No authentication is used between the client and the server. Simple—The client sends its fully-qualified domain name and password to the LDAP server. Might present security issues. Digest-MD5—The LDAP server sends authentication options and a token to the client. The client returns an encrypted response that is decrypted and verified by the server.

LDAP Client DN	Enter the distinguished name domain components [dc] ; for example:
	`dc=cv2bu,dc=com`
	If using the default Active Directory schema (Name(cn)->Users->Domain), an example of the client DN follows:
	`cn="David Lee",dc=users,dc=cv2bu,dc=com`

LDAP Username	Enter the username for a credentialed user on the LDAP server.
LDAP Password	Enter the password for the LDAP username.

Parameter	Description
LDAP Search Base	Specify a starting point in the directory tree from which to search. Separate domain components [dc] with a comma. For example: `dc=cv2bu,dc=com`
LDAP Last Name Filter	This defines the search for surnames [sn], known as last name in some parts of the world. For example, sn:(sn=*$VALUE*). This search allows the provided text to appear anywhere in a name, beginning, middle, or end.
LDAP First Name Filter	This defines the search for the common name [cn]. For example, cn:(cn=*$VALUE*). This search allows the provided text to appear anywhere in a name, beginning, middle, or end.
LDAP Search Item 3	Additional customized search item. Can be blank if not needed.
LDAP Item 3 Filter	Customized filter for the searched item. Can be blank if not needed.
LDAP Search Item 4	Additional customized search item. Can be blank if not needed.
LDAP Item 4 Filter	Customized filter for the searched item. Can be blank if not needed.

Parameter	Description
LDAP Display Attrs	Format of LDAP results display on phone where: ▪ a—Attribute name ▪ cn—Common name ▪ sn—Surname (last name) ▪ telephoneNumber—Phone number ▪ n—Display name For example, n=Phone causes "Phone:" to be displayed in front of the phone number of an LDAP query result when the detail soft button is pressed. ▪ t—type When t=p, that is, t is of type phone number, then the retrieved number can be dialed. Only one number can be made dialable. If two numbers are defined as dialable, only the first number is used. For example, a=ipPhone, t=p; a=mobile, t=p; This example results in only the IP Phone number being dialable and the mobile number will be ignored. ▪ p—phone number When p is assigned to a type attribute, example t=p, then the retrieved number is dialable by the phone.
LDAP Number Mapping	Can be blank if not needed. **NOTE** With the LDAP number mapping you can manipulate the number that was retrieved from the LDAP server. For example, you can append 9 to the number if your dial plan requires a user to enter 9 before dialing. Add the 9 prefix by adding (<:9xx.>) to the LDAP Number Mapping field. For example, 555 1212 would become 9555 1212. If you do not manipulate the number in this fashion, a user can use the **Edit Dial** feature to edit the number before dialing out.

XML Service

The Cisco SPA300 Series and Cisco SPA500 Series IP phones support XML services, such as an XML Directory Service or other XML applications. (Not applicable to the Cisco SPA301 or the Cisco SPA501G.)

Parameter	Description
XML Directory Service Name	Name of the XML Directory. Displays on the user's phone as a directory choice.
XML Directory Service URL	URL where the XML Directory is located.
XML Application Service	Name of the XML application. Displays on the user's phone as a web application choice.
XML Application Service URL	URL where the XML application is located.

Extension Mobility

For more information, see **Configuring Extension Mobility**.

NOTE Does not apply to the Cisco WIP310.

Parameter	Description
Extension Mobility	Enable or disable extension mobility. Defaults to no (disabled).
EM User Domain	The user domain for extension mobility. Defaults to blank.

Programmable Softkeys

The Cisco SPA300 Series and Cisco SPA500 Series IP phones (models with display screens) have four softkeys on the screen that, when pressed, perform certain actions.

You can customize the softkeys displayed on the phone, and create your own softkeys for speed dials or XML scripts. Customized softkey information is entered in the PSK1 through PSK6 fields. (See **Customizing Phone Softkeys** for more information.)

Parameter	Description
Programmable Softkey Enable	Enables programmable softkeys (Cisco SPA525G or Cisco SPA525G2 only).
Idle Key List	Softkeys that display when the phone is idle.
Missed Call Key List	Softkeys that display when a call has been missed.
Off Hook Key List	Softkeys that display when the receiver is lifted, or the headphone or speakerphone buttons are pressed.
Dialing Input Key List	Softkeys that display when the user must enter dialing data.
Progressing Key List	Softkeys that display when a call is attempting to connect. (Cisco SPA525G or Cisco SPA525G2 only)
Connected Key List	Softkeys that display when a call is connected.
Start-Xfer Key List	Softkeys that display when a call transfer has been initiated.
Start-Conf Key List	Softkeys that display when a conference call has been initiated.
Conferencing Key List	Softkeys that display when a conference call is in progress.
Releasing Key List	Softkeys that display when a call is disconnecting. (Cisco SPA525G or Cisco SPA525G2 only)
Hold Key List	Softkeys that display when one or more calls are on hold. (Cisco SPA525G or Cisco SPA525G2only)
Ringing Key List	Softkeys that display when a call is incoming.

Parameter	Description
Shared Active Key List	Softkeys that display when a call is active on a shared line. (Cisco SPA525G or Cisco SPA525G2 only)
Shared Held Key List	Softkeys that display when a call is on hold on a shared line. (Cisco SPA525G or Cisco SPA525G2 only)
PSK1 through PSK6	To configure a speed dial script, enter the following in the PSK field: `fnc=sd;ext=`*`extensionname`*`@$PROXY;vid=`*`outboundextnum`*`;nme=`*`name`* where `fnc` is the function of the key (speed dial), `ext` (*`extensionname`*) is the extension being dialed, `vid` is the extension on the calling phone from which the outbound call is sent, and *`name`* is the name of the speed dial being configured. To configure an XML script, enter the following in the PSK field: `fnc=xml;url=http://`*`scriptURL.xml`*`;nme=`*`scriptname`* where `fnc` is the function of the key (an XML script), *`scriptURL.xml`* is the URL where the script is located, and *`scriptname`* is the name of the script.

Ext Tab

The Ext tabs vary by phone and depend on the number of extensions the phone model supports. In a configuration profile, the Line parameters must be appended with the appropriate numeral to indicate the line to which the setting applies. For example:

```
[1] to specify line one
[2] to specify line two
```

General

Line Enable: To enable this line for service, select **yes**. Otherwise, select **no**.

Defaults to yes.

Share Line Appearance

Parameter	Description
Share Ext	Indicates whether this extension is to be shared with other Cisco SPA IP phones or private. If the extension is not shared, then a call appearance assigned to this extension is not shared, regardless the setting of `<Share Call Appearance>` for that call appearance. If the extension is shared, then whether or not a call appearance assigned to this extension is shared follows the setting of `<Share Call Appearance>` for that call appearance. The choices are shared or private. Defaults to shared.
Shared User ID	The user identified assigned to the shared line appearance.
Subscription Expires	Number of seconds before the SIP subscription expires. Before the subscription expiration, the phone gets NOTIFY messages from the SIP server on the status of the shared phone extension. Defaults to 60 seconds.
Restrict MWI	When enabled, the message waiting indicator lights only for messages on private lines.
Monitor User ID (Cisco SPA300 Series, Cisco SPA500 Series)	This field is for future use.

NAT Settings

Parameter	Description
NAT Mapping Enable	To use externally mapped IP addresses and SIP/RTP ports in SIP messages, select **yes**. Otherwise, select **no**. Defaults to no.
NAT Keep Alive Enable	To send the configured NAT keep alive message periodically, select **yes**. Otherwise, select **no**. Defaults to no.
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. Defaults to $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 or outbound proxy. Defaults to $PROXY.

Network Settings

Parameter	Description
SIP TOS/DiffServ Value	TOS/DiffServ field value in UDP IP packets carrying a SIP message. Defaults to 0x68.
SIP CoS Value	CoS value for SIP messages. Defaults to 3.
RTP TOS/DiffServ Value	ToS/DiffServ field value in UDP IP packets carrying RTP data. Defaults to 0xb8.
RTP CoS Value	CoS value for RTP data. Defaults to 6.
Network Jitter Level	Determines how jitter buffer size is adjusted by the Cisco SPA9000. Jitter buffer size is adjusted dynamically. The minimum jitter buffer size is 30 milliseconds or (10 milliseconds + current RTP frame size), whichever is larger, for all jitter level settings. However, the starting jitter buffer size value is larger for higher jitter levels. This setting controls the rate at which the jitter buffer size is adjusted to reach the minimum. Select the appropriate setting: low, medium, high, very high, or extremely high. Defaults to high.
Jitter Buffer Adjustment	Controls how the jitter buffer should be adjusted. Select the appropriate setting: up and down, up only, down only, or disable. Defaults to up and down.

SIP Settings

Parameter	Description
SIP Transport	Select from UDP, TCP, or TLS. Defaults to UDP.
SIP Port	Port number of the SIP message listening and transmission port. Defaults to 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**. Defaults to no.
EXT SIP Port	The external SIP port number.
Auth Resync-Reboot	If this feature is enabled, the Cisco SPA9000 authenticates the sender when it receives the NOTIFY resync reboot (RFC 2617) message. To use this feature, select **yes**. Otherwise, select **no**. Defaults to 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**. Defaults to yes.
Referor Bye Delay	Controls when the SPA9000 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. Defaults to 4.

Parameter	Description
Refer-To Target Contact	To contact the refer-to target, select **yes**. Otherwise, select **no**. Defaults to no.
Referee Bye Delay	For the Referee Bye Delay, enter the appropriate period of time in seconds. Defaults to 0.
SIP Debug Option	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. Defaults to none.

Parameter	Description
Refer Target Bye Delay	For the Refer Target Bye Delay, enter the appropriate period of time in seconds. Defaults to 0.
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**. Defaults to no.
Auth INVITE	When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy.
Ntfy Refer On 1xx-To-Inv	If set to **yes**, as a transferee, the phone will send a NOTIFY with Event:Refer to the transferor for any 1xx response returned by the transfer target, on the transfer call leg. If set to **no**, the phone will only send a NOTIFY for final responses (200 and higher). **NOTE** Not applicable to the Cisco WIP310.
Use Anonymous With RPID	This parameter applies only if <SIP Remote-Party-ID> is set to **yes**; otherwise, it is ignored. If the parameter is set to **yes**, the FROM header's display-name and user-id fields are set to anonymous when the caller blocks his caller-id. If the parameter is set to **no**, the FROM header's display-name and user-id are not masked. The Remote-Party-ID header indicates privacy=full when the caller wishes to block his caller-id. Defaults to yes. **NOTE** Not applicable to the Cisco WIP310.
Set G729annexb	Configure G.729 Annex B settings. **NOTE** Not applicable to Cisco SPA525G or Cisco SPA525G2.

Parameter	Description

Voice Quality Report Address	For configuration of a SIP event package, SIP PUBLISH, that enables the collection and reporting of metrics that measure the quality for VoIP sessions. Voice call quality information derived from RTCP-XR and call information from SIP is conveyed from a User Agent in a session to the third party in SIP PUBLISH method.
	
	To configure, first configure RTCP-XR (see **RTP Parameters**). Configure the RTCP Tx Interval. In the Voice Quality Report Address field, enter the name of the collector that collects the statistics from the SIP PUBLISH events. For example, enter **collector@*fully-qualified-domain-name*** (collector@reports.cisco.com) or ***collector@IP-address*** (collector@192.168.5.1).
	
	After RTCP-XR feature is enabled, the call status information is updated on **Voice** > **Info** during an active call. Additionally, RTCP-XR packets containing a voice metrics block report are sent with the interval specified in the RTCP Tx Interval. When the call session is ended, a SIP PUBLISH with voice metrics information is sent to the collector endpoint. This parameter supports a full SIP URI. Examples of valid addresses are:
	▪ collector@domain.com
	▪ 123.collect@123.123.123.123:5555
	▪ 5678@domain.com:5656
	
	For example to configure for extension 1, edit the phone configuration file as follows:
	
	`<Voice_Quality_Report_Address_1_ ua="na">collector@domain.com </Voice_Quality_Report_Address_1_>`
	
	`<Voice_Quality_Report_Address_1_ ua="na">123.collect@123.123.123.123:5555 </Voice_Quality_Report_Address_1_>`
	
	`<Voice_Quality_Report_Address_1_ ua="na">5678@domain.com:5656 </Voice_Quality_Report_Address_1_>`

Call Feature Settings

Parameter	Description
Blind Attn-Xfer Enable	Enables the IP phone 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 IP phone 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**. Defaults to no.
MOH Server	User ID or URL of the auto-answering streaming audio server. When only a user ID is specified, the current or outbound proxy is contacted. Music-on-hold is disabled if the MOH Server is not specified. Defaults to imusic when used with a Cisco SPA9000 IP PBX.
Message Waiting	Indicates whether the Message Waiting Indicator on the phone is lit. This parameter is toggled by a message from the SIP proxy to indicate if a message is waiting. You can manually modify it to clear or set the flag in the Ext 1-6 tab. 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. Defaults to No.
Auth Page	Specifies whether to authenticate the invite before auto answering a page. Defaults to No.

Parameter	Description
Default Ring	Type of ring heard. This corresponds to the Ring Tone on the Phone tab. Choose from No Ring, 1 through 10, User 1, or User 2. Defaults to 1.
Auth Page Realm	Identifies the Realm part of the Auth that is accepted when the Auth Page parameter is set to **yes**. This parameter accepts alphanumeric characters. Defaults to blank.
Conference Bridge URL	This is the URL used to join into a conference call, generally in the form of the word **conference** or **user@IPaddress:port**. Defaults to blank.
Auth Page Password	Identifies the password used when the Auth Page parameter is set to **yes**. This parameter accepts alphanumeric characters. Defaults to blank.
Mailbox ID	Identifies the voice mailbox number/ID for the phone. Defaults to blank.
Voice Mail Server	Identifies the SpecVM server for the phone, generally the IP address and port number of the VM server.
Voice Mail Subscribe Interval	The expiration time, in seconds, of a subscription to a voice mail server.
State Agent	Reserved feature.
CFWD Notify Serv	Specifies whether to enable a SIP-B feature regarding the sending of a Notify to the phone when a call is forwarded elsewhere. Defaults to No.

Parameter	Description
CFWD Notifier	Typically, this field is configured with the SIP proxy information.
User ID with Domain (Cisco SPA300 Series)	When this field is set to **yes**, the IP phone will show the Caller ID followed by domain name, and the domain name is also shown in the received calls list. This parameter is used when calls are made between different branches of the same phone system. For example, if user John@domain1.com receives a call from Mary@domain2.com, by default the phone only shows the call as being from Mary, so John is not able to pick up or call back Mary from the received call list. With this parameter set to **yes**, the phone logs the call as being from Mary@domain2.com, and John can dial Mary from the received call list.
Device Feature Sync	Set this parameter to yes to enable DND/CFWD synchronization per extension.

Proxy and Registration

Parameter	Description
Proxy	SIP proxy server and port number set by the Service Provider for all outbound requests. For example: 192.168.2.100:6060.
Outbound Proxy	SIP Outbound Proxy Server where all outbound requests are sent as the first hop.

Use Outbound Proxy	Enables an outbound proxy (for example, 172.20.2.1:5060—port is optional) or a domain name such as sip.server.com as long as this name is a fully-qualified domain name. If set to no, the Outbound Proxy and Use OB Proxy in Dialog fields are ignored.
	
	Defaults to no.
	
	Optionally, the proxy can be configured (Cisco SPA500 Series only) for Survivable Remote Site Telephony (SRST) support. The proxy is configured with an extension that includes a statically-configured DNS SRV record or DNS A record. Configuring the proxy allows for failover and fallback functionality with a secondary proxy server. For example:
	
	For SRV Record:
	
	`sip.server.com:SRV=node1.sip.server.com:5060:p=1:w=50|node2.sip.server.com:5060:p=2:w=50`
	
	Set Use DNS SRV to **no** and DNS SRV Auto Prefix to **no**.
	
	For A Record:
	
	`sip.server.com:A=172.20.2.1,172.20.2.2`
	
	Set Use DNS SRV to **no** and DNS SRV Auto Prefix to **no**.

Parameter	Description
Use OB Proxy In Dialog	Whether to force SIP requests to be sent to the outbound proxy within a dialog. Ignored if <Use Outbound Proxy> is no or <Outbound Proxy> is empty. Defaults to yes.
Register	Enable periodic registration with the <Proxy>. This parameter is ignored if <Proxy> is not specified. Defaults to yes.
Make Call Without Reg	Allow making outbound calls without successful (dynamic) registration by the unit. If no, the dial tone will not play unless registration is successful. Defaults to 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 phone will renew registration based on this smaller value instead of the configured value. If registration failed with an Expires too brief error response, the phone will retry with the value given in the Min-Expires header in the error response. Defaults to 60.
Ans Call Without Reg	If enabled, the user does not have to be registered with the proxy to answer calls. Defaults to no.
Use DNS SRV	Whether to use DNS SRV lookup for Proxy and Outbound Proxy. Defaults to no.

Parameter	Description
DNS SRV Auto Prefix	If enabled, the phone will automatically prepend the Proxy or Outbound Proxy name with _sip._udp when performing a DNS SRV lookup on that name. Defaults to no.
Proxy Fallback Intvl	This parameter sets the delay (sec) after which the phone 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 phone 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 phone will not attempt to fall back after a fail over). Defaults to 3600
Proxy Redundancy Method	Select Normal or Based on SRV port. The phone creates an internal list of proxies returned in the DNS SRV records. If you select Normal, the list contains proxies ranked by weight and priority. If you select Based on SRV, the phone uses normal, then inspects the port number based on the first listed proxy port. Defaults to Normal.

Subscriber Information

Parameter	Description
Display Name	Display name for caller ID.
User ID	Extension number for this line.
Password	Password for this line. Defaults to blank.
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. Defaults to no.
Auth ID	Authentication ID for SIP authentication. Defaults to blank.
Mini Certificate	Base64 encoded of Mini-Certificate concatenated with the 1024-bit public key of the certificate authority (CA) signing the mini-certificate of all subscribers in the group. Defaults to blank.
SRTP Private Key	Base64 encoded of the 512-bit private key per subscriber for establishment of a secure call. Defaults to blank.

Audio Configuration

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 might 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 might be allocated for subsequent calls; the only choices are G711a and G711u. On the other hand, two G.723.1/G.726 resources are available per device.

Therefore it is important to disable the use of G.729a in order to guarantee the support of two simultaneous uses of the G.723/G.726 codecs.

Parameter	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, G722, G726-16, G726-24, G726-32, G726-40, G729a, or G723. Cisco SPA525G or Cisco SPA525G2: G711u, G711a, G726-32, G729a, and G722. G.723 (not available on Cisco SPA300 Series or Cisco SPA500 Series). G722 not available on Cisco WIP310. Defaults to G711u.
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. Defaults to no.
Second Preferred Codec	The second preferred codec when the preferred codec cannot be used. If *Use Pref Codec Only* is enabled (set to **yes**), this parameter is not used. Defaults to Unspecified.

Parameter	Description
Third Preferred Codec	The third preferred codec when the preferred codec and second preferred codec cannot be used. If *Use Pref Codec Only* is enabled (set to **yes**), this parameter is not used. Defaults to Unspecified.
G729a Enable	To enable the use of the G.729a codec at 8 kbps, select yes. Otherwise, select no. Defaults to yes.
G722 Enable	Enables use of the G.722 codec. Defaults to yes. **NOTE** Not applicable to the Cisco WIP310.
G723 Enable	To enable the use of the G.723a codec at 6.3 kbps, select **yes**. Otherwise, select **no**. Defaults to yes. **NOTE** G.723 is not supported on the Cisco SPA300 Series, Cisco SPA500 Series, or Cisco WIP310.
G726-16 Enable	To enable the use of the G.726 codec at 16 kbps, select **yes**. Otherwise, select **no**. Defaults to yes. **NOTE** Not supported on the Cisco SPA525G or Cisco SPA525G2.
G726-24 Enable	To enable the use of the G.726 codec at 24 kbps, select **yes**. Otherwise, select **no**. Defaults to yes. **NOTE** Not supported on the Cisco SPA525G or Cisco SPA525G2 or Cisco WIP310.
L16 Enable	To enable the use of the L16 codec, select **yes**. Otherwise, select **no**. Defaults to yes. **NOTE** Cisco SPA525G or Cisco SPA525G2 only.

Parameter	Description
G726-32 Enable	To enable the use of the G.726 codec at 32 kbps, select **yes**. Otherwise, select **no**. Defaults to yes.
G726-40 Enable	To enable the use of the G.726 codec at 40 kbps, select **yes**. Otherwise, select **no**. Defaults to yes. **NOTE** Not applicable to the Cisco SPA525G or Cisco SPA525G2.
Release Unused Codec	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. Defaults to yes.
DTMF Process AVT	Select **yes** to process RTP DTMF events. Otherwise, select **no**. If this parameter is set to no, the AVT payload type is not included in outbound SDP. Defaults to yes.
Silence Supp Enable	To enable silence suppression so that silent audio frames are not transmitted, select **yes**. Otherwise, select no. Defaults to **no**.
DTMF Tx Method	Select the method to transmit DTMF signals to the far end: InBand, AVT, INFO, Auto, InBand+INFO, or AVT+INFO. InBand sends DTMF using the audio path. AVT sends DTMF as AVT events. INFO uses the SIP INFO method. Auto uses InBand or AVT based on the outcome of codec negotiation. Defaults to Auto.

Parameter	Description
DTMF Tx Volume for AVT Packet	Allows you to manually configure the AVT Tx volume. The value of this parameter is inserted into the volume field of the payload in the AVT packet. Values are based on the AVT specification as described in RFC 2833, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*. According to RFC 2833, the volume field is represented by 6 bits, and describes the power level of the tone, expressed in dBm0 after dropping the sign. Valid range for this parameter is 0 to 63. If the provisioned value is negative, it will be negated first. Thereafter, if the value is beyond the high limit of 63, it will be clipped to 63. The default value is 0, and is the recommended setting. However, some gateways do not accept this volume setting. If the gateway does not accept the value of 0, the DTMF tone is not relayed to the remote end. As a workaround for the phone to interoperate with those gateways, you can change the value to a value greater than 0.
Use Remote Pref Codec	If set to **yes**, the phone communicates using the remote phone preferred codec. If set to **no**, the Cisco IP phone communicates using its own preferred codec (as indicated in the **Preferred Codec** field and in the SDP by order of preferences). The default vale is no.
Codec Negotiation	When set to **Default**, the Cisco IP phone responds to an Invite with a 200 OK response advertising the preferred codec only. When set to **List All**, the Cisco IP phone responds listing all the codecs that the phone supports. The default value is **Default**, or to respond with the preferred codec only.

A codec resource is considered allocated if it has been included in the SDP codec list of an active call, even though it eventually might not be chosen for the connection. 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 G729a resource is already allocated (and since only one G.729a resource is allowed per phone), no other low-bit-rate codec can be allocated for subsequent calls. The only choices are G711a and G711u.

Since two G.723.1/G.726 resources are available per IP phone, you should disable the use of G.729a to guarantee support for two simultaneous G.723/G.726 codecs.

Dial Plan Script

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

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

Parameter	Description
Dial Plan	Dial plan script for this line. The default is `(<9:>xx.)` `(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxxx.)` The dial plan syntax is expanded in the Cisco SPA IP phones to allow the designation of three parameters to be used with a specific gateway: ▪ uid— authentication user-id ▪ pwd—authentication password ▪ nat— if this parameter is present, use NAT mapping Each parameter is separated by a semi-colon (;).
Caller ID Map	Inbound caller ID numbers can be mapped to a different string. For example, a number that begins with +44xxxxxx can be mapped to 0xxxxxx. This feature has the same syntax as the Dial Plan parameter. With this parameter, you can specify how to map a caller ID number for display on screen and recorded into call logs. (Not applicable to Cisco WIP310.)
Enable IP Dialing	Enable or disable IP dialing. Defaults to no.

User Tab

This section describes the fields for the User tab.

Call Forward

Parameter	Description
Cfwd All Dest	Enter the extensions to forward calls to.
Cfwd Busy Dest	Enter the extensions to forward calls to when the line is busy. Defaults to voice mail.
Cfwd No Ans Dest	Enter the extension to forward calls to when the call is not answered. Defaults to voice mail.
Cfwd No Ans Delay	Enter the time delay in seconds to wait before forwarding a call that is not answered. Defaults to 20 seconds.

See **Vertical Service Activation Codes** for more information on call forwarding parameters.

Speed Dial

You can configure speed dials on the Cisco SPA300 Series and Cisco SPA500 Series IP phones. Speed dial configuration is on a separate tab on the Cisco SPA525G or Cisco SPA525G2. It is not configurable from the phone web user interface on the Cisco WIP310. Speed dial configuration for the Cisco WIP310 is done on the IP phone screen.

Speed Dial 2 through 9: Target phone number (or URL) assigned to speed dial 2, 3, 4, 5, 6, 7, 8, or 9.

Defaults to blank.

See the respective phone user guides for the phone for more information.

Supplementary Services

The Cisco SPA9000 provides native support of a large set of enhanced or supplementary services. All of these services are optional. A supplementary service should be disabled if the user has not subscribed to it or the service provider intends to support similar service by using other means. Most supplementary service parameters are listed in **Supplementary Services**.

The user can enable or disable supplementary services and the other settings in this section. For more star code or supplementary service information, see **Configuring Supplementary Services (Star Codes)**.

Camera Settings (Cisco SPA525G or Cisco SPA525G2)

The Cisco SPA525G or Cisco SPA525G2 works with the Cisco WVC2300 Wireless-G Business Internet Video Camera and the Cisco PVC2300 Business Internet Video Camera to provide simple video monitoring from your IP phone. See **Entering Camera Information Into the Cisco SPA525G or Cisco SPA525G2 Configuration Utility**.

Web Information Service Settings (Cisco SPA525G or Cisco SPA525G2)

These parameters apply only to the Cisco SPA525G or Cisco SPA525G2. For configuration information, see **Configuring RSS Newsfeeds (Cisco SPA525G or Cisco SPA525G2)**.

Audio (SPA5XX)/Audio Volume (SPA525G/525G2)

NOTE Does not apply to the Cisco WIP310.

Parameter	Description
Ringer Volume	Sets the default volume for the ringer.
Speaker Volume	Sets the default volume for the full-duplex speakerphone.
Handset Volume	Sets the default volume for the handset.
Headset Volume	Sets the default volume for the headset.

Handset Version	Change the handset version manually. **Auto**—Phone automatically sets the handset version based on the hardware version and model. (Default) **Original**—Handset set to Version 2 and below. **V3**—Handset set to Version 3.
Deep Bass	Sets a standard tone or an enhanced bass tone.
Bluetooth Volume	Volume of the Bluetooth device. **NOTE** Applies to the Cisco SPA525G or Cisco SPA525G2 only.
Speakerphone Enable	Enables or disables the speakerphone. If the parameter is set to **yes** (the default setting), the speakerphone is enabled. If the parameter is set to **no**, the speakerphone is disabled, and pressing the Speakerphone button on the phone sends the audio to the phone handset instead of the speaker.

Screen (Cisco SPA525G or Cisco SPA525G2)

Parameter	Description
Screen Saver Enable	Enables a screen saver on the IP phone screen. When the phone is idle for a specified time, it enters screen saver mode. (Users can set up screen savers directly using phone Setup button.) Any button press or on/off hook event triggers the phone to return to its normal mode. (The screen shows "Press any key to unlock your phone.") If a user password is set, the user must enter it to exit screen saver mode.
Screen Saver Type	Choose the type of screen saver: ▪ **Black Background**—Displays a black screen. ▪ **Gray Background**—Displays a gray screen. ▪ **Black/Gray Rotation**—The screen incrementally cycles from black to gray. ▪ **Picture Rotation**—The screen rotates through available pictures on the phone. ▪ **Digital Frame**—Shows the background picture.
Screen Saver Trigger Time	Number of seconds that the phone remains idle before the screen saver turns on.
Screen Saver Refresh Time	Number of seconds before the screen saver should refresh (if, for example, you chose a rotation of pictures).

Parameter	Description

Text Logo	Text logo to display when the phone boots up. A service provider, for example, can enter logo text as follows:
	▪ Up to 2 lines of text
	▪ Each line must be fewer than 32 characters
	▪ Insert a new line character (\n) between lines
	▪ Insert escape code %0a
	For example, “Super\n%0aTelecom” will display:
	`Super`
	`Telecom`
	For more information, see the **“Configuring Phone Information and Display Settings” section on page 49.**

BMP Picture Download URL	URL locating the bitmap (.BMP) or .jpg file to display on the IP phone screen background. For more information, see the **“Configuring Phone Information and Display Settings” section on page 49.**
Logo Type	Select from Default, Download BMP Picture, or Text Logo. Defaults to Default. For more information, see the **“Configuring Phone Information and Display Settings” section on page 49.**
Background Picture Type	Select from Default, Download BMP Picture, or None. Defaults to Default. For more information, see the **“Configuring Phone Information and Display Settings” section on page 49.**

Parameter	Description
LCD Contrast	Enter a number value from 1 to 30. The higher the number, the greater the contrast on the IP phone screen.
Back Light Enable	Select yes to enable the IP phone screen back light.
Back Light Timer (sec)	Enter the number of seconds before the back light should turn off.

Attendant Console Tab (Cisco SPA500 Series)

General

Parameter	Description
Subscribe Expires	Specifies how long the subscription remains valid. After the specified period of time, elapses, the Cisco Attendant Console initiates a new subscription. Defaults to 1800.
Subscribe Retry Interval	Specifies the length of time to wait to try again if subscription fails.
Unit 1 Enable	Enables or disables the first Cisco Attendant Console unit (each IP phone can have up to two Cisco Attendant Consoles attached).
Subscribe Delay	Length of delay before attempting to subscribe. Defaults to 1.
Unit 2 Enable	Enables or disables the second Cisco Attendant Console unit (each IP phone can have up to two Cisco Attendant Consoles attached).
Server Type	Selects the type of server used (Cisco SPA9000, BroadSoft, or Asterisk).

Parameter	Description
Test Mode Enable	Enables or disables test mode. When test mode is enabled, the LEDs are turned on when keys are pressed, going from off to green to red, and back to off. In test mode, when all the buttons on the Cisco Attendant Console are returned to off, all the keys become orange. The IP phone must be rebooted after the test is completed.
Attendant Console Call Pickup Code	The star code used for picking up a ringing call. Defaults to *98.
Attendant Console Call Park Code	The star code used for parking a call. Defaults to *68.
Attendant Console Call unPark Code	The star code used for retrieving a parked call. Defaults to *88.
BLF List URI	Automatically configures Busy Lamp Field (BLF) subscriptions for all users on a monitored list.
Call Pickup Audio Notification	By default, this parameter is set to **no**. If you set it to **yes**, the phone plays the Call Pickup tone when there are incoming calls to any of the lines that the user is monitoring with the Call Pickup function. Use the following in your configuration file: `<Call_Pickup_Audio_Notification ua="na">Yes </Call_Pickup_Audio_Notification>`
Attendant Console LCD Contrast (SPA500DS)	The contrast between the text, lines, and background on the attendant console display. Enter a number value from 1 to 30. The higher the number, the greater the contrast on the display.
Attendant Console Font Size (SPA500DS)	Font size of the text on the attendant console display. Choose 10 or 12 point font.
Unit 1/2 Key 1-32 (SPA500S) Unit 1/2 Key 1-30 (SPA500DS)	Enter a strings that define the extension and other parameters associated with each lighted button on the first Cisco Attendant Console. Keywords and values are case-sensitive.

Attendant Console Status

This page provides two tabs to display the status of up to two Cisco Attendant Consoles that are supported by a single IP phone:

- Unit 1—Displays information about the first Cisco Attendant Console.
- Unit 2—Displays information about the second Cisco Attendant Console.

Each tab provides the read-only fields described in the following table:

Parameter	Description
Unit Enable	Indicates that the Cisco Attendant Console is enabled or disabled.
Subscribe Expires	When the current subscription expires. After the subscription expires, the Cisco Attendant Console automatically requests a new subscription.
HW Version	Version of the hardware.
Unit Online	Indicates that the Cisco Attendant Console is powered on and connected.
Subscribe Retry Interval	Length of time the Cisco Attendant Console waits to try again if subscription fails.
SW Version	Version of the software.
Key	Key number on the attendant console.
Name	Name assigned to each key.
Type	Function enabled for each key.
Line	Extension assigned to each key.
Station	Displays the subscribe URI configured for each key.
Subscribed	Subscription status of the unit/key. The value can be Yes, Fail, or N/A. N/A indicates that the feature/function (fnc) of that line does not require a subscription (such as a speed dial).

Cisco SPA525G or Cisco SPA525G2-Specific Tabs

The tabs described in this section appear on the Cisco SPA525G or Cisco SPA525G2.

Wi-Fi

Enable or disable the Wireless-G service on the phone from this tab.

Parameter	Description
Wireless Enable	Click **on** to enable the wireless controller.
Wi-Fi Device	Choose the method of wireless setup: ▪ Wi-Fi Profile—Create a wireless profile by manually entering the information. ▪ Wi-Fi Protected Setup—If your router has a WPS button, you can use Wi-Fi Protected Setup to add a new wireless network profile.
Wireless Status	Information about the wireless network.
Wi-Fi Profile	Contains up to 3 wireless profiles for the phone. Includes a wireless profile for the Cisco Unified Communications Server.

Bluetooth

For more information on configuring Bluetooth, see **Configuring Bluetooth (Cisco SPA525G or Cisco SPA525G2 only)**.

Parameter	Description
Bluetooth Device	Click **on** to enable Bluetooth.
Bluetooth Status (Cisco SPA525G2 only)	Name and status of any connected Bluetooth devices.

Parameter	Description
Bluetooth Mode (Cisco SPA525G2 only)	Shows the method of Bluetooth connection chosen: ▪ **Phone**—Pairs with a Bluetooth headset only. ▪ **Handsfree**—Operates as a handsfree device with a Bluetooth-enabled mobile phone. ▪ **Both**—Uses a Bluetooth headset, or operates with a Bluetooth-enabled mobile phone (see **Configuring Bluetooth (Cisco SPA525G or Cisco SPA525G2 only)**. The Cisco SPA525G2 connects to only one Bluetooth device at a time.
Bluetooth Profiles (Cisco SPA525G2 only)	This table shows the MAC (hardware) address, device name, and other information for the Bluetooth device that is associated with a Cisco SPA525G or Cisco SPA525G2. If multiple Bluetooth devices are in range of a Cisco SPA525G or Cisco SPA525G2, the phone attempts to pair with the devices in order the shown in the list. Highlight an entry and click the arrow keys to move devices up and down the list, changing the priority. You can choose **yes** or **no** to indicate if the phone should connect to a Bluetooth device automatically. You can also remove devices from the list.
Bluetooth Device List (Cisco SPA525G2 only)	Click **Scan for Bluetooth Devices** to locate Bluetooth devices in the area. Found devices are shown with the type of device, MAC address, and device name.

Personal Address Book

Address book for the phone. For more information, see the respective Cisco Small Business IP Phone User Guide.

Call History

Displays the call history for the phone. To change the information displayed, select the type of call history from the drop-down list:

- All Calls
- Received Calls
- Placed Calls
- Missed Calls

Speed Dials

See **Speed Dial**.

Firmware Upgrade

Used to upgrade the firmware for the Cisco SPA525G or Cisco SPA525G2. See **Updating Firmware**.

B

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco SPA IP phone.

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business Firmware Downloads	www.cisco.com/cisco/web/download/ index.html Select a link to download firmware for Cisco Small Business Products. No login is required.
Product Documentation	
Cisco SPA300 Series IP Phones	www.cisco.com/go/300phones
Cisco SPA500 Series IP Phones	www.cisco.com/go/spa500phones
Cisco Cisco WIP310	www.cisco.com/en/US/partner/products/ps10033/tsd_products_support_series_home.html
IP Phone Accessories	www.cisco.com/en/US/products/ps10042/tsd_products_support_series_home.html
Cisco SPA9000 Voice System	www.cisco.com/en/US/products/ps10030/tsd_products_support_series_home.html
Cisco Unified Communications 500 Series for Small Business	www.cisco.com/en/US/products/ps7293/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

NOTE For older Cisco IP phone models, such as the Cisco SPA9XX, see the *Cisco SPA9XX Phone Administration Guide* on cisco.com. This guide covers only the Cisco SPA300 Series IP phones, Cisco SPA500 Series IP phones, and the Cisco Cisco WIP310.

Document revised July 2012

OL-19749-07