# Administering Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G

Release 6.3
16-300698
Issue 15
August 2013

© 2013 Avaya Inc.

All Rights Reserved.

**Notice**

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

**Note**

Using a cell, mobile, or GSM phone, or a two-way radio in close proximity to an Avaya IP telephone might cause interference.

**Documentation disclaimer**

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

**Link disclaimer**

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

**Warranty**

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

**License types**

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

**Copyright**

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

**Third Party Components**

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

**Preventing Toll Fraud**

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

**Avaya Toll Fraud intervention**

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States

and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

**Trademarks**

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

**Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

**Contact Avaya Support**

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

**Federal Communications Commission (FCC) Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

**FCC/Industry Canada Radiation Exposure Statement**

This device complies with the FCC's and Industry Canada's RF radiation exposure limits set forth for the general population (uncontrolled environment) and must not be co-located or operated in conjunction with any other antenna or transmitter.

**Warning**

The handset receiver contains magnetic devices that can attract small metallic objects. Care should be taken to avoid personal injury.

**Power over Ethernet (PoE) warning**

This equipment must be connected to PoE networks without routing to the outside plant.

根據國家通訊傳播委員會低功率電波輻射性電機管理辦法規定：

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

**VCCI-Class B statement:**

This is a Class B product based on the standard of the VCCI Council. If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

## Contents


**Chapter 1: Introduction** ..... 9
- Intended Audience ..... 9
- Related resources ..... 9
  - Documentation ..... 9
  - Training ..... 10
- Warranty ..... 10
- Support ..... 10

**Chapter 2: Overview** ..... 11
- Overview of the 9600 Series IP deskphones ..... 11
- Document changes since last issue ..... 12
- New in this release ..... 12
- Enhancements in H.323 Release 6.2 Service Pack 4 ..... 14
- Enhancements in H.323 Release 6.2 Service Pack 3 ..... 14
- Enhancements in H.323 Release 6.2 Service Pack 2 ..... 14
- Features introduced in H.323 Release 6.2 Service Pack 1 ..... 15
- Features in Release 6.2 ..... 15
- Features introduced in Release 6.1 ..... 16

**Chapter 3: Administration overview and requirements** ..... 19
- Administrative requirements ..... 19
- Parameter data precedence ..... 22
- Administrative tasks ..... 22
- Administrative checklist ..... 23
- Initialization process overview ..... 24
  - Connection to network ..... 25
  - DHCP processing ..... 25
  - VPN connection ..... 25
  - File downloads ..... 25
  - Registration with the call server ..... 26
- Error conditions ..... 27

**Chapter 4: Network Requirements** ..... 29
- Network Assesment ..... 29
- Hardware requirements ..... 29
- Server requirements ..... 30
- Required network information ..... 31
- Other network considerations ..... 31
  - Enabling SNMP ..... 32
  - Ping and traceroute ..... 32
  - IP address and settings reuse ..... 33
  - QoS ..... 33
  - IEEE 802.1D and 802.1Q ..... 33
  - Network audio quality ..... 34
  - Qtest for audio quality ..... 35
  - IP address lists and station number portability ..... 35
  - TCP/UDP Port utilization ..... 35

Security ... 40
Time-to-Service ... 42
**Chapter 5: Communication Manager Administration ... 45**
Call server requirements ... 45
Aliasing IP deskphones for switch compatibility ... 45
Call server administration ... 47
Administering the IP interface and addresses ... 48
Administering UDP port selection ... 48
Administering RSVP ... 48
Administering QoS ... 49
Administering IEEE 802.1Q ... 49
Administering DIFFSERV ... 49
Administering NAT ... 49
Administering Voice Mail ... 50
Voice mail for deskphones with Communication Manager 4.0+ ... 50
Voice mail for deskphones aliased as 4600 Series IP Telephones ... 50
Call transfer administration ... 51
Call conferencing ... 52
Phone administration on Avaya Aura® Communication Manager ... 53
Feature-related system parameters ... 54
Station administration ... 56
Administering features ... 56
Administering feature buttons and call appearances (CAs) ... 56
Administering 9610 IP deskphone features and CAs ... 56
Administering 9620,9620L,9620C IP deskphone features and CAs ... 57
Administering features and CAs for all other IP deskphones ... 57
Administering enhanced phone screen displays for certain IP deskphones ... 59
Assigning 9650/9650C Aux buttons ... 59
Button module administration on the 9608, 9611G, 9630/9630G, 9640/9640G, 9641G, 9650/9650C, and 9670G ... 60
Administering the Conference Details screen for ad-hoc conferences ... 61
Quick Touch panel for touch screen deskphones ... 61
Shuffling ... 62
Wideband codecs ... 62
**Chapter 6: Server Administration ... 63**
Software Prerequisites ... 63
Administering the DHCP and file Servers ... 63
Configuring DHCP Option 242 ... 64
DHCP Generic Setup ... 67
Setting up the DHCP server ... 67
Setting up a DHCPv6 server ... 70
HTTP Generic Setup ... 71
Backup and restore processing ... 72
About IPv4 and IPv6 operation ... 74
Features not supporting IPv6 ... 75
**Chapter 7: Telephone Software and Application Files ... 77**
Understanding the general download process ... 77

Choosing the right application file and upgrade script file ... 78
Changing the Signaling Protocol ... 79
Using the upgrade file ... 79
About the settings file ... 79
Using the GROUP parameter to set up customized groups ... 81
**Chapter 8: Administering Deskphone Options ... 83**
Administering options for 9600 Series H.323 Deskphones ... 83
9600 Series H.323 customizable system parameters ... 84
Single Sign on for local devices (SSON-LD) ... 109
Administering a VLAN ... 110
About VLAN Tagging ... 110
The VLAN default value and priority tagging ... 111
Automatic detection of a VLAN ... 111
VLAN separation rules and related parameters ... 112
About DNS addressing ... 115
EAP-TLS support for authentication ... 115
Enabling certificate support ... 116
Activating EAP-TLS for authentication ... 117
Scenarios for using EAP-TLS based authentication ... 118
Deploying EAP-TLS based authentication for phones using 802.1x and MD5 ... 118
Deploying EAP-TLS on phones running without any type of 802.1x authentication ... 120
About IEEE 802.1X ... 121
802.1X Supplicant operation ... 122
About Link Layer Discovery Protocol (LLDP) ... 123
Administering settings at the phone ... 128
Administering display language options ... 128
About the gigabit Ethernet (GigE) adapter ... 130
Administering dialing methods ... 131
Understanding log digit or Smart Enbloc dialing ... 131
Using enhanced local dialing ... 131
Enhanced local dialing requirements ... 133
About internal audio parameters ... 134
Managing applications on the Home screen ... 135
Administering features on softkeys ... 137
Administering a custom screen saver ... 145
About administering audio equalization ... 146
Administering deskphones for call center operation ... 147
Administering agent sign in for call centers ... 148
Call Center backup files ... 149
Administering the Vu display button ... 150
Ringing on wireless headset ... 151
Configuring phone based auto-answer ... 152
Administering backup and restore ... 155
Backup file formats ... 156
User data saved during backup ... 157
About restore ... 159
Administering backup and restore for a 9610 ... 160

About the 9610 retrieval process ... 161
General 9610 restore processing ... 162
**Chapter 9: Administering Applications and Options ... 165**
Customizing Applications and Options ... 165
Setting the Application Status flag ... 166
Special Administration for the 9610 ... 168
Special Administration for Touchscreen Deskphones ... 168
Administering the Avaya A Menu ... 168
Administering Phone Settings and Options and Settings ... 170
Administering WML applications on the Avaya Menu ... 171
Main Avaya Menu with Browser (Only) Administered ... 172
Administering the Avaya Menu with WML applications ... 173
How the Home screen displays WML applications ... 174
Sample Avaya Menu Administration File Template ... 177
Administering guest users ... 180
Administering visiting users ... 180
Administering idle timer operation ... 180
Administering the user stopwatch timer ... 182
Requirements for USB Devices ... 183
USB File/Device Support ... 183
Contacts File Format for USB Devices ... 184
Setting up USB logins ... 185
Setting up USB pictures as screensavers ... 185
**Chapter 10: Administering specific 9600 Series IP Deskphones ... 187**
Introduction ... 187
Special Administration for the 9610 IP Telephone ... 187
Overview of the 9610 IP Deskphone ... 187
Key 9610 administration concepts ... 188
Administering the 9610 idle application, screensaver, and WML links ... 192
Accessing 9610 Craft procedures ... 193
Troubleshooting a 9610 IP Telephone ... 194
Sample 9610data.txt file ... 194
Sample idle.wml file ... 197
Sample hotel.wml file ... 197
**Glossary ... 199**
**Index ... 205**

# Chapter 1: Introduction

## Intended Audience

This guide is intended for personnel who administer Avaya Aura® Communication Manager, DHCP, HTTP/HTTPS servers for Avaya 9608, 9611G, 9621G, and 9641G series IP deskphones, a Local Area Network (LAN), or a Web server.

## Related resources

### Documentation

For more information related to the use of the H.323 9600 IP Deskphones refer the following documents:

| Document number | Title | Use this document to: | Audience |
|---|---|---|---|
| Implementing | | | |
| 16–603603 | Avaya IP Deskphone H.323 9608,9611G,9621G, and 9641G | Refer to procedures related to installing and upgrading the deskphone | Administrators |
| Using | | | |
| 16–603593 | Using Avaya IP Deskphone 9621G and 9641G | Refer to tasks related to using the deskphone. | End Users and Administrators |
| 16–603594 | Using Avaya IP Deskphone 9611G and 9621G | Refer to tasks related to using the deskphone. | End Users and Administrators |
| Administering | | | |

| Document number | Title | Use this document to: | Audience |
|---|---|---|---|
| 16-300698 | Administering Avaya IP Deskphone H.323 9608,9611G,9621G, and 9641G | Refer to tasks related to carrying out administrative procedures related to deskphone. | Administrators |

## Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

| Course code | Course title |
|---|---|
| ACIS-6006 | ACIS - Avaya Communication Manager (5.2.1) |
| APSS-1300 | APSS - Avaya Networking |

You can view the training videos at Avaya Training Center - End Points.

## Warranty

Avaya provides a one-year limited warranty on the 9600 Series IP Deskphones. For more information on standard warranty terms and details regarding support, while under warranty, refer the support site at http://support.avaya.com/.

## Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

# Chapter 2: Overview

## Overview of the 9600 Series IP deskphones

Avaya 9608, 9611, 9621 and 9641 Series IP deskphones use Internet Protocol (IP) technology with Ethernet line interfaces and support both H.323 and SIP protocols. These deskphones support DHCP, HTTP, and HTTPS to obtain customized settings and to download new versions of software for the deskphones.

All 9600 Series IP deskphones currently support the H.323 signaling protocol. This document covers only 9600 Series IP deskphones supporting H.323.

The H.323 standard provides real time audio, video, and data communications transmission over a packet network. An H.323 telephone protocol stack comprises several protocols:

- H.225 for registration, admission, status (RAS), and call signaling
- H.245 for control signaling
- Real Time Transfer Protocol (RTP) and Secure Real Time Transfer Protocol (SRTP)
- Real Time Control Protocol (RTCP) and Secure Real Time Control Protocol (SRTCP)

**Caution:**

Avaya does not support many of the products mentioned in this document. Ensure that adequate technical support is available for servers used with any 9600 Series IP deskphone system. If the servers do not function correctly, the deskphones will not operate correctly.

This guide describes the administration of Avaya 9608, 9611, 9621, and 9641 Series IP deskphones using H.323 protocol only. For information about administering these telephones in a Session Initiation Protocol (SIP) environment, see *Administering Avaya IP Deskphone SIP 9608,9611G,9621G, and 9641G*, 16-601944.

This document does not describe how to use the 9600 Series IP deskphones in an IP Office environment.

For more information on using the 9600 Series IP deskphones in an IP Office environment, see the Avaya support site at http://support.avaya.com/css/P8/documents/100150378.

The following terms are used interchangeably in this document as all the terms refer to the same Avaya IP deskphone product line, that is the Avaya 9608, 9611G, 9621G, and 9641G Series IP deskphones:

- 9600 Series IP Telephones
- 9600 Series IP Deskphones
- H.323 deskphone
- Deskphone
- IP telephone
- Phone

# Document changes since last issue

This version of the document released in August 2013 includes the information about the following enhancements:

- Support for EAP-TLS
- Support for SCEP
- SSO logon
- IP redirect feature
- Parameters: SYSAUDIOPATH, CCLOGOUTIDLESTAT, SSO_ENABLED, PHY2_AUTOMDIX_ENABLED, LOCALZIPTONEATT, and LEDMODE
- Support for a configurable headset

# New in this release

Avaya 9600 Series H.323 IP deskphones Release 6.3 has the following enhancements and features.

| Enhancement | Description |
|---|---|
| New parameters<br>**Note:**<br>For more information on the new parameters, see 9600 Series H.323 customizable system parameters on page 84. | SYSAUDIOPATH: To set the default audio path to the speaker or the headset, or allow the call center agent to select the audio path. |
| | CCLOGOUTIDLESTAT: To configure the headset LED to remain on after the call center agent logs out. |
| | SSO_ENABLED: To implement the Single Sign On feature. |

| Enhancement | Description |
|---|---|
| | Additional related parameters added are – SSO_REGISTERED_MODE, SSO_LOCK_SYNC,SSO_DISCONNECT_ACTION, SSO_DISCONNECT_FACS, SSO_CLIENT_CERT. For more information on Single Sign On refer the application note on the Avaya support site. |
| | AGTSPKRSTAT: Modified to allow the call center agent to use the SPEAKER button to release an ongoing call. |
| | LOCALZIPTONEATT: To control the volume of local phone ziptone heard when using AUTOANSSTAT= 1. |
| | PHY2_AUTOMDIX_ENABLED: To configure automatic recognition of crossover or straight Ethernet cables on the deskphone PC port (Auto MDIX). |
| | LEDMODE: To support different LED behaviors. Old behavior is maintained as default (LEDMODE 0). |
| | DOT1XWAIT: To specifiy whether the telephone will wait for 802.1X to complete before proceeding with startup and initiating DHCP. |
| Single Sign on | To allow a PC user to control the login and locked status of a telephone from the PC.<br>**Note:**<br>Contact DevConnect for more information on obtaining the API and developing PC client applications. |
| Identity Certificate (SCEP) support | To perform secure backup of agent greetings. |
| Authentication using EAP-TLS | To authenticate the users using the EAP-TLS mode of secure authentication. |
| IP redirect | The IP redirect feature directs deskphones to download software from the nearest server on the network, thereby reducing download time. |

**Note:**

Voice Initiated Dialing (VID) is no longer supported on the H.323 9600 Series IP deskphones.

# Enhancements in H.323 Release 6.2 Service Pack 4

H.323 Release 6.2 Service Pack 4 has the following enhancements:

- Debug feature is accessible only if you have changed the default password for the craft menu.
- Support for Wireless (Jabra/Plantronics) EHS cable  firmware.

# Enhancements in H.323 Release 6.2 Service Pack 3

H.323 Release 6.2 Service Pack 3 included the following enhancements:

- Agent ID query feature that the deskphone uses to send a query to the CM for the agent ID and use the response from CM accordingly.
- A feature for muting the deskphone when used in shared control configuration with one-X Communicator.

# Enhancements in H.323 Release 6.2 Service Pack 2

This release included the following features and enhancements:

- Bi-directional headset feature configurable by user

  In Release 6.2, only the administrator could switch on the bi-directional feature for the user's headset through the settings file parameter HEADSETBIDIR. In this release onwards, the user can activate or de-activate this feature through the deskphone.

- Phone-based conditional auto-answer

  Using this feature, you can configure the deskphone to automatically answer incoming calls, or a subset of incoming calls, independently of the auto-answer setting on the Communication Manager.

- The AGTIDVUSTAT parameter, introduced in Release 6.2, is renamed in Service Pack 2 to AGTVUSTATID.

# Features introduced in H.323 Release 6.2 Service Pack 1

- A feature to enable ringing on wireless headsets from Jabra and Plantronics and the ability to activate and deactivate the wireless headset from the headset button.
- A new parameter AGTACTIVESK that you can use in the Call center environment to control the softkeys that are available to the agents.
- A new parameter AGTGREETLOGOUTDEL that you can use to keep or remove agent greeting upon agent logout.
- The HEADSYS parameter that you can use to specify whether the deskphone will go on-hook if the headset is active when a *Disconnect* message is received. This feature has been reintroduced.

**Note:**

The default value of HEADSYS is related to the value of CALLCTRSTAT. If the value of CALLCTRSTAT is 1, then the default of HEADSYS is 1.

If value of CALLCTRSTAT is 0, then the default of HEADSYS is also 0.

In either case, the administrator can override defaults by explicitly setting HEADSYS in the 46xxsettings file.

Customers using Call center features without configuring CALLCTRSTAT, must have the HEADSYS parameter set to 1.

# Features in Release 6.2

The following changes that were effected in Release 6.2 software apply only to the 9608, 9611G, 9621G, and 9641G IP deskphones:

- You can use the Debug procedure to send immediate debug reports to specified servers.
- You can download a version of software that disables VPN and media encryption Avaya Support website. The software is identified on the *About Avaya* screen with a *U* appended to the software release.
- This release supports the Secure Shell (SSH) protocol. This protocol is intended to help Avaya Services monitor deskphone performance.
- You can use the AGTIDVUSTAT parameter in Call centers to specify a VuStats format number. This number enables the deskphone to determine the call center agent's Agent ID, which is essential if Agent Greetings are to be used.

- A software application watchdog automatically monitors other software processes to determine whether they have become unresponsive, at which point the watchdog generates a log event, and either kills the process or resets the deskphone. You can enable or disable this application watchdog using the APPLICATIONWD parameter.
- You can disable the Bluetooth functionality from the settings file, using the BLUETOOTHSTAT parameter.
- You can play a recording tone on a call, with the RECORDINGTONE parameter when the call is being recorded. In addition, the interval between tones, and the volume the tones are played, are administrable. This feature is relevant to sites where a recording device is connected to the deskphone and legal requirements mandate warning both parties of the call to that fact.
- Users have a new option under Call Settings called *Audible Headset Alerting* that, when enabled, allows alerting through an attached headset in addition to the speaker on the deskphone.

  This feature is now called Headset Signaling.
- You can control the handset audio equalization through the settings file administration, end user option, and Local Procedure. Equalization is available to optimize the audio for telecoil or T-coil Hearing Aid operation, or for Acoustic Performance.
- Sidetone values for headset and handset administration have been made consistent between intervals.
- Support for Converged Network Analyzer (CNA) has been withdrawn; any applicable administration will be ignored in Release 6.2.
- Call Center agents have their Greetings stored on the deskphone between logins, in addition to storage on a file server.
- The default value of HEADSYS has been changed. The new default is tied to the current value of CALLCTRSTAT. If the value of CALLCTRSTAT is 1, HEADSYS has default value 1. Otherwise, CALLCTRSTAT has value 0, and the default value of HEADSYS is also 0. In either case, though, you can override defaults by explicitly setting HEADSYS in the settings file.

# Features introduced in Release 6.1

The following changes were effected in Release 6.1 as compared to 6.0 for Avaya H.323 IP deskphones. This information is being published in this guide as version 6.1 was a Limited Availability (LA) release.

The information is intended for users who want to migrate directly from version 6.0 to version 6.2.

- The deskphones support a local timer feature. The agent can now select the Local Timer feature to start a stop watch.
- The agent deskphone provides two headset ports for the agent and the supervisor using the standard RJ9.adaptor. Use this feature on the agent deskphone with the dual headset adaptor.
- The agent can manually record a greeting.
- The phones support automatic prompting for greeting.
- The greeting duration can be up to 10 seconds maximum. You can save about 6 greetings.
- Agents can link a greeting to a particular trigger event during the recording process. The trigger events can be manual or automatic.
- The agent can play back greetings when the agent is on a call to both the incoming caller and the agent simultaneously. The agent can manually trigger the play back of the greeting by selecting the greeting during the call. Agent greetings will also be automatically triggered using one of the following events:
    - Answering a call
    - ANI
    - VDN
    - Prompted Digits
- The agent can back up, delete and retrieve greetings from the server automatically.
- The administrator can disable the hook switch by using the Settings file. Administrators thus prevent agents from accidentally going off hook and then on hook with the handset resulting in agents disconnecting from the active call and being logged out.
- Call appearance can be 15 characters of VDN name for touch phones. For button phones, call appearance must be 12 or 24 characters wide depending on the screen width.
- The agent can press the UUI-INFO button to display the UUI information on the phone screen. If this information does not fit on the allocated display area, the agent can scroll down the line to read the content.
- The agent can use the Caller info button to view secondary information about the ongoing call such as collected digits, qcalls, q-time, trk-id, VuStat display, and uui-info.
- The agent can select and control the History backup time as required.
- The administrator can use the new Parameter CLBACKUPTIME to control backup delay.
- The user can see the Logout button displayed on an idle screen.
- Help screen now provides information about how to unlock the phone.
- Agents can now use the Logoff Softkey to log off and logon using another set of credentials.

- The Caller ID displays on the screen in sequential lines if the ID does not fit on one line.
- The capability to assign functions to WML buttons is extended to include the implementation of call control capabilities.
- A user with the visiting user profile can log in to any 9600 series deskphone within the configured network of systems. The user must use a unique user identifier and password.
- The 9600 Series H.323 customizable system parameters now include the following new system parameters. All these parameters are only for use in a Call Center with the exception of TIMERSTAT.
  - AGTCALLINFOSTAT - Automatically invokes the Call-info permission flag.
  - AGTFWDBTNSTAT - Disables or enables the Forward button permission flag.
  - AGTGREETINGSTAT - Sets the agent greeting permission flag.
  - AGTLOGINFAC - Indicates the Feature Access Code to be used by agents when logging in to a Call Center.
  - AGTSPKRSTAT - disables or enables the speakerphone permission flag.
  - AGTTIMESTAT - suppresses the date or time presentation flag.
  - AGTTRANSLTO - Translation for *to* as used on the call server.
  - AGTTRANSCLBK - Translation for *callback* as used on the call server.
  - AGTTRANSLPRI - Translation for *priority* as used on the call server.
  - AGTTRANSLPK - Translation for *park* as used on the call server.
  - AGTTRANSLICOM - Translation for *icom* as used on the call server.
  - CALLCTRSTAT - Call center functionality flag.
  - OPSTATCC - OPSTAT override flag; for Call Center use only.
  - TIMERSTAT - Controls whether the deskphone displays the User Timer Timer On and Timer Off softkeys.
- The Management Information Base (MIB), available on the Avaya Support site, is updated with several new parameters and increase in the number of *syslog* event messages in the *endptRecentLog* and *endptResetLog* parameters.
- The deskphone display now combines the Title line and the Prompt line into one Status line. The phone displays the Status line as the second display line after the Top line.

# Chapter 3: Administration overview and requirements

## Administrative requirements

The operating environment for the 9600 Series IP deskphones is outlined as follows:

- Telephone Administration on the Avaya call server. For more information, see Communication Manager Administration on page 45.
- IP Address management for the deskphone. For more information see, Administering the DHCP and File Servers on page 63 for dynamic addressing.

  For more information on static addressing, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*,16-603603 covering the 9608, 9611G, 9621G, and 9641G deskphones, and *Avaya IP Deskphone Edition for 9600 Series IP Telephones. Installation and Maintenance Guide*, 16-300694 for all other 9600 Series deskphone models.
- Tagging Control and VLAN administration for the phone, if applicable. For more information, see Administering Telephone Options.
- Quality of Service (QoS) administration for the phone, if appropriate. For more information, see QoS on page 33 and Administering QoS on page 49.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP).
- Interface administration for the phone, as appropriate. Administer the phone to LAN interface using the PHY1 parameter. For more information, see Network Requirements on page 29. Administer the deskphone to PC interface using the PHY2 parameter.

  For more information, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*,16-603603 covering the 9608, 9611G, 9621G, and 9641G deskphones, and *Avaya IP Deskphone Edition for 9600 Series IP Telephones. Installation and Maintenance Guide*,16-300694 for all other 9600 Series deskphone models.
- Application-specific phone administration, if applicable. For more information, see Administering Applications and Options on page 165. An example of application-specific data is Web-specific information required for this optional application.

The table on page 20 indicates that you can administer system parameters in a variety of ways and use a variety of delivery mechanisms. For example:

- Maintaining the information on the call server.
- Manually entering the information by means of the phone dial pad.
- Administering the DHCP server.
- Editing the configuration file on the applicable HTTP or HTTPS file server.
- Modifying certain parameters with administrative permission to do so.

**Note:**

You cannot administer all parameters on all delivery mechanisms.

**Table 1: Alternative ways to administer the 9600 Series IP Deskphones**

| Parameter | Administrative mechanisms | Related information |
|---|---|---|
| Phone Administration | Avaya call server | Communication Manager Administration on page 45, Server Administration on page 63, and the applicable call server documentation. |
| IP Addresses | DHCP | Administering The DHCP and File Servers on page 63 and especially Administering the DHCP Server. |
| | Configuration file | Telephone Software and Application Files on page 77 and Administering Telephone Options. |
| | Manual administration at the deskphone | "Static Addressing Installation" in *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G* Guide. |
| | LLDP | About Link Layer Discovery Protocol (LLDP) on page 123 |
| Tagging and VLAN | DHCP | Administering The DHCP Server, and Administering Telephone Options. |
| | Configuration file | Administering The DHCP and File Servers on page 63 and Administering Telephone Options. |
| | LLDP | "Static Addressing Installation" in *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*. |
| | Manual administration at the phone | About Link Layer Discovery Protocol (LLDP) on page 123. |

| Parameter | Administrative mechanisms | Related information |
|---|---|---|
| Quality of Service | Avaya call server | Administering UDP port selection on page 48 and the applicable call server documentation. |
| | DHCP | Administering The DHCP and File Servers on page 63, and Administering Telephone Options. |
| | Configuration file | Administering The DHCP and File Servers on page 63, and Administering Telephone Options. |
| | LLDP | About Link Layer Discovery Protocol (LLDP) on page 123. |
| Interface | DHCP | Administering The DHCP and File Servers on page 63, and Telephone Software and Application Files on page 77. |
| | Configuration file | Administering The DHCP and File Servers on page 63, and Telephone Software and Application Files on page 77. |
| | LLDP | About Link Layer Discovery Protocol (LLDP) on page 123. |
| | Manual administration at the phone | “Secondary Ethernet (Hub) Interface Enable/Disable” in *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*. |
| Application - specific parameters | Configuration file | Administering The DHCP and File Servers on page 63, and especially HTTP Generic Setup on page 71. Also, Administering Applications and Options on page 165. |
| VPN | Configuration file | *VPN Setup Guide for 9600 Series IP Telephones,16-602968.* |

For information about administering DHCP servers, see Administering the DHCP and File Servers on page 63, and more specifically, Administering the DHCP Server. For information on administering HTTP servers, see Administering the DHCP and File Servers on page 63, and more specifically, HTTP Generic Setup on page 71. For administration options, see Administering Telephone Options.

# Parameter data precedence

If a given parameter is administered in multiple places, the last server to provide the parameter takes precedence. The following is a list of precedence, from lowest to highest:

1. Manual administration. Call server or HTTP server or both are two exceptions for the phone parameter STATIC.
2. DHCP, except as indicated in “DHCPACK Setting of Parameter Values” in Setting up the DHCP server on page 67,
3. The 46xxsettings.txt file
4. The Avaya call server.
5. Backup files, if administered and permitted.
6. LLDP: Only the IPv4 mode supports LLDP. Note: Setting the call server and file server IP addresses have the lowest precedence.

# Administrative tasks

Adhere to the following procedure to administer a typical 9600 Series IP deskphone network.

1. Administer the switch for 9600 Series IP deskphones.
2. Administer LAN and applicable servers to accept the deskphones.
3. Download the deskphone software from the Avaya support site.
4. Update the 46xxsettings file with site-specific information, as applicable.
5. Install 9600 Series IP deskphones. For more information, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*,16-603603 covering the 9608, 9611G, 9621G, and 9641G deskphones, and *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694* for all other 9600 Series deskphone models.
6. Update individual 9600 Series IP deskphones using Craft procedures, as applicable. For more information on Local Administrative Procedures, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*.

# Administrative checklist

System and LAN administrators can use the following checklist to ensure that all phone system prerequisites and requirements are met prior to phone installation.

**Table 2: Administrative Checklist**

| Task | Description | Related information |
|---|---|---|
| Network requirements assessment | Determine that network hardware is in place and can handle phone system requirements. | Network Requirements on page 29. |
| Call server administration | Verify that the call server is licensed and is administered for Voice over IP (VoIP). Verify that the individual phones are administered as required. | Communication Manager Administration on page 45. |
| DHCP server installation | Install a DHCP application on at least one new or existing PC on the LAN. | Vendor-provided instructions. |
| DHCP application administration | Add IP deskphone administration to DHCP application. | Administering The DHCP Server in Server Administration on page 63. |
| HTTP/HTTPS server installation | Install an HTTP/HTTPS application on at least one new or existing PC on the LAN. | Vendor-provided instructions. |
| Application files, script file, and settings file installation on the HTTP/HTTPS server. | Download the files from the Avaya support site. | http://www.avaya.com/support Telephone Software and Application Files on page 77. |
| Settings file modification as desired | Edit the settings file as desired, using your own tools. | Telephone Software and Application Files on page 77. |
| WML servers administration | Add WML content as applicable to new or existing WML servers. Administer the content that will be pushed on to the deskphones from WML push servers as applicable. | *Avaya IP Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide, 16-600888*. |
| Local administration of deskphones as applicable | As a Group: | Using the GROUP parameter to set up customized groups on page 81 and the *Installing and Maintaining Avaya IP* |

| Task | Description | Related information |
|---|---|---|
| | | *Deskphone H.323 9608, 9611G, 9621G, and 9641G*, 16-300694 for all but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608, 9611G, 9621G, and 9641G deskphones. |
| | Individually: | The applicable Craft Local Procedures in the *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*, Document Number 16-300694 for all but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608, 9611G, 9621G, and 9641G deskphones. |
| Telephones installation in the network | | *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*, Document Number 16-300694 for all but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608, 9611G, 9621G, and 9641G deskphones) |
| User modification of Options, if applicable | | OPSTAT on page 170 and the respective User Guide for the specific deskphone model. |
| VPN functionality administration if applicable | Enable/disable VPN, provide administration for your particular VPN environment | *VPN Setup Guide for 9600 Series IP Telephones*, 16-602968 |

# Initialization process overview

The deskphone initialization process involves exchange of information that happens when the phone initializes and registers. The process includes the following five steps. This description assumes that all equipment is properly administered ahead of time. For more information, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*, 16-603603 covering the 9608, 9611G, 9621G, and 9641G deskphones, and for a detailed description of initialization, power-up, and reset for all other deskphone models, see *Avaya IP*

*Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*.

**Note:**

When you start a deskphone without access to the HTTP server, the phone reuses parameters from before the reboot. The phone waits for 60 seconds and starts with the old parameters.

**Related topics:**

Connection to network on page 25
DHCP processing on page 25
VPN connection on page 25
File downloads on page 25
Registration with the call server on page 26

## Connection to network

The phone is appropriately installed and powered. After a short initialization process, the phone displays the speed at which it is connected to the network and determines whether to initiate 802.1X network access procedures.

## DHCP processing

If an IP address has not been manually configured in the phone, the phone initiates DHCP, as described in Administering the DHCP and File Servers on page 63. Among other data passed to the phone is the IP address of the HTTP or HTTPS server.

## VPN connection

The process then determines whether the deskphone must establish a Virtual Private Network (VPN) connection. If yes, the deskphone establishes a VPN tunnel as appropriate for its administration.

## File downloads

9600 Series IP deskphones can download configuration files, language files, and certificate files from either an HTTP or HTTPS server, but they can only download software files from an HTTP server. The phone first downloads an upgrade configuration file, which tells the phone

which software files it should use. The phone then downloads a settings configuration file, and based on those settings, it may then download language files and/or certificate files. Finally, the phone will download one or two new software files, depending on whether or not the software in the phone is the same as that specified in the upgrade file. For more information about this download process and settings file, see Telephone Software and Application Files on page 77.

# Registration with the call server

The call server referred to in this section is Avaya Aura Communication Manager.

The phone is registered with the call server in two modes, named registration and unnamed registration.

### Named registration

In this step, the phone might prompt the user for an extension and password. The phone uses that information to exchange a series of messages with the call server. For a new installation and for full service, the user can enter the phone extension and the password configured on the call server for that particular extension. The information required to restart a phone that was previously registered with an extension number is already stored on the phone. The user must confirm the information so that the phone is appropriately registered and can download call server data such as feature button assignments.

### Unnamed registration

Using this feature, you can register a phone with the call server without an extension, provided the call server also supports this feature. To invoke Unnamed Registration, either enter a null (empty) extension or password or take no action. You can also choose to take no action and allow the **`Extension...`** prompt to display for 60 seconds. The phone automatically attempts to register by means of Unnamed Registration. A phone registered with Unnamed Registration has the following characteristics:

- Only one call appearance
- No administrable features
- Outgoing calls only, subject to call server Class of Restriction or Class of Service limitations
- Conversion to normal *named* registration possible by the user entering a valid extension and password.

### Other administrable options using parameters

- MCIPADD

  You can configure the phone to register to a particular call server by listing the IP addresses in the MCIPADD parameter in DHCP or the 46xxsettings.txt file. The standard practice is to list the CLANs on the main call server, followed by any Enterprise Survivable Server (ESS) addresses, followed by any Local Spare Processor (LSP). To deviate from this practice, you can list CLANs for multiple main call servers. In general, the phone will start from the beginning of MCIPADD and attempt to register with each IP address in turn,

one at a time, until the phone gets a positive response. If MCIPADD is administered, users can register to local call servers.

- VUMCIPADD

  When a user from another location wants to register with their home call server using their *home* extension, this type of registration is known as the Visiting User (VU). In H.323 software Release 6.1, the 9600 Series support this scenario using the VUMCIPADD parameter. When this parameter contains one or more IP addresses the user sees a slight change to the Login screen. In that screen the user is asked to specify a Login Mode of either *Default* or *Visiting User*. If the user selects *Default*, the deskphone uses the MCIPADD parameter value whereas if the user selects Visiting User, the deskphone attempts to register with each IP address in VUMCIPADD simultaneously until it gets a positive response.

  For example, if the company has locations in cities A, B, C, and D, you can administer VUMCIPADD with one IP address from each of the main call servers in the four cities. A user from city A is in the city B location but wants to use the city A call server. The user selects Visiting User on the Login screen, the deskphone contacts each of the four main call servers simultaneously and registers with the only call server that gives a positive response for city A.

- UNNAMEDSTAT

  You can also administer the phone to avoid unnamed registration and remain unregistered if no extension and password are provided. For more information, see the UNNAMEDSTAT parameter in the table for 9600 Series H.323 customizable system parameters on page 84.

For more information about the installation process, see *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*. For information on Release 6.2 and later, covering the 9608, 9611G, 9621G, and 9641G deskphones, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*,16-603603.

# Error conditions

Assuming proper administration, most of the problems reported by phone users are likely to be LAN-based, Quality of Service, server administration, and other issues can impact user perception of IP phone performance.

For the likely operational problems after you successfully install 9600 Series IP deskphone, see *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*. You can also see the User Guides for specific deskphone models and applications.

# Chapter 4: Network Requirements

## Network Assesment

Perform a network assessment to ensure that the network has the capacity for the expected data and voice traffic, and can support jitter buffers and the following types of applications as required:

- H.323
- DHCP
- HTTP/HTTPS
- LLDP
- RADIUS

You also need QoS support to run VoIP on your configuration. For more information, see Administering UDP port selection on page 48.

To use the 9600 Series IP deskphones to reach the network through a Virtual Private Network 15 (VPN), see *VPN Setup Guide for 9600 Series IP Telephones*, 16-602968.

## Hardware requirements

- Category 5e cables that conform to the IEEE 802.3af-2003 standards, for LAN powering.
- TN2602 or TN2302 IP Media Processor circuit pack. For increased capacity, install a TN2602 circuit pack even if you have a TN2302 IP Media Processor circuit pack.
- TN799C or D Control-LAN (C-LAN) circuit pack.

**Important:**

IP telephone firmware Release 1.0 or later requires TN799C V3 or greater C-LAN circuit packs. For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya support Web site https://support.avaya.com/CompatibilityMatrix/Index.aspx.

To ensure that the appropriate circuit packs are administered on your server, see Communication Manager Administration on page 45.

For more information about hardware requirements in general, see *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*. For Release 6.0 covering the 9608, 9611G, 9621G, and 9641G deskphones, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*,16-603603.

# Server requirements

You can configure three types of servers for 9600 Series IP deskphones:

- DHCP server: Avaya recommends that you install a DHCP server and do not use static addressing. Install the DHCP server as described in Administering the DHCP and File Servers on page 63.
- HTTP or HTTPS server - Administer the HTTP or HTTPS file server as described in HTTP Generic Setup on page 71.
- Web and Push servers (optional) - If users have access to corporate WML web sites, administer the deskphones as described in Server Administration on page 63. For *push* functionality, you need a Trusted Push Server. The Trusted Push Server can be the same server as your WML server. Avaya recommends that you restrict access to directories on the WML server that contain push content.

**Note:**

Push is supported only in IPv4 mode. Your Web and push server configuration must be compatible with the requirements mentioned in the *9600 Series IP Telephone Application Programmer Interface (API) Guide*.

While the servers listed provide different functions that relate to the 9600 Series IP deskphones, the servers are not necessarily different boxes. For example, DHCP provides file management whereas HTTP provides application management, yet both functions can co-exist on one hardware unit. Use any standards-based server.

For parameters related to Avaya Server information, see Communication Manager Administration on page 45, and the administration documentation for your call server. For parameters related to DHCP and file servers, see Server Administration on page 63.

**Caution:**

The deskphones obtain important information from the script files on the file server and depend on the application file for software upgrades. If the file server is unavailable when the deskphones reset, the deskphones operate based on their default administration and continue with the call server registration process. Not all features are available. To restore them you need to reset the deskphones when the file server is available.

# Required network information

Before you administer DHCP and HTTP/HTTPS, collect the following required network information. If you have more than one Gateway (router), HTTP/HTTPS server, or call server in your configuration, complete the required network information for each DHCP server before phone installation.

The 9600 Series IP deskphones support specifying a list of IP addresses for a gateway/router, HTTP/HTTPS server, and Avaya call servers. Each list can contain up to 255 total ASCII characters, with IP addresses separated by commas with no intervening spaces. Depending on the specific DHCP server, the phone might support only 127 characters.

When you specify IP addresses for the file server or call server, use either dotted decimal format ("*xxx.xxx.xxx.xxx*") or DNS names for IPv4 addresses. If you use DNS, the value of the DOMAIN parameter is appended to the DNS names that you specify. If DOMAIN is null, the DNS names must be fully qualified. For more information about DNS, see DHCP Generic Setup on page 67 and DNS addressing on page 115.

### Required network information before installation (per DHCP server)

- Gateway router IP addresses
- HTTP/HTTPS file server IP addresses, port number, if different from the default, and directory path if files are not located in the root directory
- Subnetwork mask
- Avaya call server IP address(es)
- Phone IP address range (From:/To:)
- DNS server address(es) if applicable

As the LAN or System Administrator, you must also:

- Administer the DHCP server. See Server Administration on page 63.
- Edit the configuration file on the applicable HTTP or HTTPS file server. See Choosing the right application file and upgrade script file on page 78.

# Other network considerations

**Related topics:**

Enabling SNMP on page 32
Ping and traceroute on page 32
IP address and settings reuse on page 33

QoS on page 33
IEEE 802.1D and 802.1Q on page 33
Network audio quality on page 34
Qtest for audio quality on page 35
IP address lists and station number portability on page 35
TCP/UDP Port utilization on page 35
Security on page 40
Time-to-Service on page 42

## Enabling SNMP

The 9600 Series IP deskphones are compatible with SNMPv2c and Structure of Management Information Version 2 (SMIv2). The telephones also respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. The telephones respond to queries directed either at the MIB-II or the read-only Custom MIB. Read-only means that you cannot change the values externally by means of network management tools.

You can restrict the IP addresses from which the phones accepts SNMP queries with the SNMPADD parameter. You can also customize your community string with the SNMPSTRING parameter.

9600 Series IP deskphones support the functionality introduced with Communication Manager Release 4.0 that is, call server administration of SNMPADD and SNMPSTRING. For more information, see Server Administration on page 63 and 9600 Series H.323 customizable system parameters on page 84.

**Note:**

SNMP is disabled by default. Administrators must initiate SNMP by setting the SNMPADD and SNMPSTRING parameters appropriately.

For more information about SNMP and MIBs, see the IETF website. The Avaya Custom MIB for the 9600 Series IP telephones is available for download in *.txt format on the Avaya support Web site at http://www.avaya.com/support.

**Note:**

The H.323 software Release 3.1 MIB differs from the software Release 6.0 and later MIBs. Download the MIBs applicable to your environment.

## Ping and traceroute

All 9600 Series IP deskphones respond to a ping or traceroute message sent from the call server switch or any other network source. The call server can also instruct the telephone to

originate a ping or a traceroute to a specified IP address. The telephone carries out that instruction and sends a message to the call server indicating the results. For more information, see your call server administration documentation.

## IP address and settings reuse

After you successfully register the phone with a call server, the IP address of the phone and parameter values are saved in the non-volatile memory of the phone. The phone can reuse the saved parameters if the DHCP or HTTP/HTTPS server is not available for any reason after a restart. The setting for the DHCPSTD parameter indicates whether to keep the IP address if there is no response to lease renewal. If set to 1 (No) the phone strictly follows the DHCP standard with respect to giving up IP addresses when the DHCP lease expires. If set to 0 (Yes) the phone continues using the IP address until it detects reset or a conflict.

## QoS

For more information about the extent to which your network can support any or all of the QoS initiatives, see your LAN equipment documentation. For information about QoS implications for the 9600 Series IP deskphones, see Administering QoS on page 49.

All 9600 Series IP deskphones provide some detail about network audio quality. For more information, see Network Audio Quality Display on page 34.

## IEEE 802.1D and 802.1Q

For more information about IEEE 802.1D and IEEE 802.1Q and the 9600 Series IP Deskphones, see Administering IEEE 802.1Q on page 49 and Administering a VLAN on page 110. Three bits of the 802.1Q tag are reserved for identifying packet priority to set any one of the following eight priorities to a specific packet.

- 7: Network management traffic
- 6: Voice for traffic with less than 10ms latency and jitter
- 5: Video traffic with less than 100ms latency and jitter
- 4: *Controlled-load* traffic for critical data applications
- 3: Traffic meriting *extra-effort* by the network for prompt delivery, for example, executive email
- 2: Reserved for future use

- 0: The default priority for traffic meriting the *best-effort* for prompt delivery of the network
- 1: Background traffic such as bulk data transfers and backups

**Note:**

Priority 0 is a higher priority than Priority 1.

## Network audio quality

You can monitor network audio performance on the 9600 Series IP deskphones while on a call. You can view this information on the Network Information screen. You can view the Network Information screen on most 9600 Series IP button-based deskphones from the Avaya (A) Menu and select the Network Information option directly if available. You can also select Phone Settings, then select the Network Information option. On touch screen deskphones such as 9621G, 9641G, and 9670G, you can access the Home screen, then select Settings, then Network Information.

While on a call, you can view the network audio quality parameters in real-time. See the following table for the various parameters that you can view:

**Table 3: Parameters in real-time**

| Parameter | Possible values |
|---|---|
| Received Audio Coding | G.711, G.722, G.726, or G.729. |
| Packet Loss | No data or a percentage. Late and out-of-sequence packets are counted as lost if they are discarded. Packets are not counted as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number. |
| Packetization Delay | No data or an integer number of milliseconds. The number reflects the amount of delay in received audio packets, and includes any potential delay associated with the codec. |
| One-way Network Delay | No data or an integer number of milliseconds. The number is one-half the value RTCP or SRTCP computes for the round-trip delay. |
| Network Jitter Compensation Delay | No data or an integer number of milliseconds reporting the average delay introduced by the jitter buffer of the telephone. |

The implication for LAN administration depends on the values the deskphone user reports and the specific nature of your LAN, like topology, loading, and QoS administration. This information gives the administrator an idea of how network conditions affect the audio quality of the current call. Avaya assumes you have more detailed tools available for LAN troubleshooting.

## Qtest for audio quality

### About this task

You can enable the Qtest feature to display network quality information when the deskphone is not on a call. When you set the QTESTRESPONDER parameter to an IP address, the deskphone displays a Qtest softkey on the Network Information screen when a call is not active. For more information on accessing this screen, see Network Audio Quality Display on page 34. When you press the Qtest softkey, UDP packets are sent to the echo port at the IP address specified by QTESTRESPONDER, and statistics are computed and displayed based on the returned packets. A UDP port is opened for Qtest only while the test is active. For information on the UDP port numbers applicable to Qtest, see TCP/UDP Port Utilization on page 35.

## IP address lists and station number portability

You can specify IP address lists on the 9600 Series IP deskphones. On startup or on reboot, the phone attempts to establish communication with these various network elements in turn. The phone starts with the first address on the respective list. If the communication is denied or times out, the phone proceeds to the next address on the appropriate list and tries that IP address. The phone does not report failure unless all the addresses on a given list fail, improving the reliability of IP telephony.

The address list and station portability capability also make station number portability possible. Assume a situation where the company might have multiple locations in London and New York, that share a corporate IP network. Users want to take the phones from the London office to New York office. When the user starts the phones in the new location, the local DHCP server usually routes the user to the local call server. With proper administration of the local DHCP server, the local DHCP server registers the user with call server IP address in London.

For details on administration of DHCP servers for lists of alternate call servers, router/gateways, and HTTP/HTTPS servers, see Server Administration on page 63.

For more information on DNS addresssing, see DNS Addressing on page 115.

## TCP/UDP Port utilization

9600 Series IP deskphones use a variety of protocols, particularly TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and TLS (Transport Layer Security) to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP port each piece of equipment uses to support each protocol and each task within the protocol. For additional TCP/UDP port utilization information related to Communication Manager, see UDP Port Selection on page 48.

Depending on your network, you must know what ports or ranges are used in the phone operation. Knowing these ports or ranges helps you administer your networking infrastructure.

**Note:**

In many cases, the phones use ports defined by IETF or other standards bodies.

For more information about parameters and settings, see Administering Options for 9600 Series H.323 Deskphones on page 83.

**Table 4: Received packets (Destination = 9600 Series IP deskphone)**

| Destination port | Source port | Use | UDP or TCP? |
|---|---|---|---|
| The number used in the Source Port field of Qtest packets sent by the phone | 7 | Received Qtest messages | UDP |
| 22 | Any | Packets received by the SSH server of the phone | TCP |
| The number used in the Source Port field of DNS packets sent by the phone | Any | Received DNS messages | UDP |
| The number used in the Source Port field of the packets sent by the HTTP client on the phone | Any | Packets received by the HTTP client on the phone | TCP |
| Release 2.0+ = PUSHPORT<br>Pre-Release 2.0 = 80 | Any | Packets received by the HTTP server of the phone | TCP |
| 500, 2070, or 4500 | 500 or 4500 | Received IKE or IPsec messages (if NVIKEOVERTCP is 1 or 2) | TCP |
| The number used in the Source Port field of received SSO packet<br>18414 | Any | Received SSO commands | TCP only |
| 546 | Any | Received DHCPv6 messages | UDP |
| The number used in the Source Port field of the TLS/SSL packets sent by the HTTP client on the phone | Any | TLS/SSL packets received by the HTTP client on the phone | TCP |
| 68 | Any | Received DHCP messages | UDP |
| 161 | Any | Received SNMP messages | UDP |

| Destination port | Source port | Use | UDP or TCP? |
|---|---|---|---|
| 500 | Any | Received DHCPv6 messages | UDP |
| 500, 2070, or 4500 | 500 or 4500 | Received IKE or IPsec messages (if NVIKEOVERTCP is 0 or 1) | UDP |
| 50000 | Any | Received CNA test request messages | UDP |
| 50011 | Any | Received SLA discovery and test request messages | UDP |
| 50012 | Any | Received SLA RTP test packets | UDP |
| The number used in the Source Port field of registration messages sent by the CNA test plug on the phone | Any | Received CNA registration messages | TCP |
| 1720 | Any | H.323 signaling messages | TCP |
| The number used in the Source Port field of RAS packets sent by the phone | 1719 | H.323 RAS messages | UDP |
| As specified by CM, or as reserved for CNA RTP tests during CNA registration | Any | Received RTP and SRTP packets | UDP |
| The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd | Any | Received RTCP and SRTCP packets | UDP |
| The number used in the Source Port field of registration messages sent by the SLA agent on the phone | Any | Received SLA registration messages | TCP |

**Table 5: Transmitted packets (Source = 9600 Series IP deskphone)**

| Destination Port | Source Port | Use | UDP or TCP? |
|---|---|---|---|
| 7 | Any unused port number | Transmitted Qtest messages | UDP |
| The number used in the Source Port field of packets received by the SSH server of the phone. | 22 | Packets transmitted by the SSH server of the phone | TCP |

| Destination Port | Source Port | Use | UDP or TCP? |
|---|---|---|---|
| 53 | Any unused port number | Transmitted DNS messages | UDP |
| 67 | 68 | Transmitted DHCP messages | UDP |
| Release 2.0+ = HTTPPORT Pre-Release 2.0 = 80 unless explicitly specified otherwise, for example, use of Port 81 for CM | Any unused port number | Packets transmitted by the HTTP client on the phone during startup | TCP |
| 80 unless explicitly specified otherwise, for example, in a URL or due to use of WMLPORT | Any unused port number | Packets transmitted by the HTTP client of the phone after startup,for example, for backup and restore or push | TCP |
| The number used in the Source Port field of the SNMP query packet received by the phone | 161 | Transmitted SNMP messages | UDP |
| The number used in the Source Port field of packets received by the HTTP server of the phone | Release 2.0+ = PUSHPORT Pre-Release 2.0 = 80 | Packets transmitted by the HTTP server of the phone | TCP |
| Release 2.0+ = TLSPORT Pre-Release 2.0 = 411 | Any unused port number | TLS/SSL packets transmitted by the HTTP client of the phone during startup | TCP |
| 443 unless explicitly specified otherwise, for example in a URL | Any unused port number | TLS/SSL packets transmitted by the HTTP client of the phone after startup, for example for backup or restore | TCP |
| 500 or 4500 | 500, 2070, or 4500 | Transmitted IKE or IPsec messages, if NVIKEOVERTCP is 0 or 1 | TCP |
| 514 | Any unused port number | Transmitted Syslog messages | UDP |
| 547 | Any unused port number | Transmitted DHCPv6 messages | UDP |
| 18414 | Any unused port number | Transmitted SSO status indications | TCP |

| Destination Port | Source Port | Use | UDP or TCP? |
|---|---|---|---|
| 33434 - 33523, starts with 33434, increments by 1 for each message sent, 3 messages per hop, up to 30 hops | Any unused port number | Transmitted traceroute messages | UDP |
| CNAPORT | Any unused port number | Transmitted CNA registration messages | TCP |
| The port number received in the Transport Address field in the RCF message | 1720 | H.323 signaling messages | TCP |
| The port number specified in the test request message | 50000 | Transmitted CNA test results messages | UDP |
| A port number specified in the SLA test request message | 50011 | Transmitted SLA test results messages | UDP |
| A port number specified in the SLA test request message | 50012 | Transmitted SLA RTP test packets | UDP |
| 33434 – 33523,starts with 33434, increments by 1 for each message sent, 3 messages per hop, up to 30 hops | 50013 | Transmitted SLA traceroute messages | UDP |
| System-specific | system - specific | Transmitted signaling protocol packets | TCP |
| As specified by CM, or as specified in a CNA RTP test request | As specified by CM or as reserved for CNA RTP tests | Transmitted RTP and SRTP packets | UDP |
| The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd | The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd | RTCP and SRTCP packets transmitted to the far-end of the audio connection | UDP |
| RTCPMONPORT | The next higher port number if the port used for RTP is even, or the next lower | RTCP packets transmitted to an RTCP monitor | UDP |

| Destination Port | Source Port | Use | UDP or TCP? |
|---|---|---|---|
| | port number if the port used for RTP is odd | | |
| 1719 | An unused port number in the range from 49300 to 49309 | H.323 RAS messages | UDP |
| System-specific | System - specific | Transmitted signaling protocol packets | UDP |
| A port number specified in the SLA discovery message | Any unused port number | Transmitted SLA registration messages | TCP |

# Security

For information about toll fraud, see the respective call server documents on the Avaya support Web site. The 9600 Series IP deskphones cannot guarantee resistance to all Denial of Service (DoS) attacks. However, checks and protections are in place to resist such attacks while maintaining appropriate service to legitimate users.

All 9600 Series IP deskphones that have WML Web applications support Transport Layer Security (TLS). The deskphone uses TLS to establish a secure connection to a HTTP server, in which the upgrade and settings file can reside.

All 9600 Series IP deskphones support HTTP authentication for backup and restore operations. The reprogrammable non-volatile memory stores the authentication credentials and the realm. The reprogrammable non-volatile memory is not overwritten if new phone software is downloaded. The default value of the credentials and the realm are null, set at manufacture and at any other time that user-specific data is removed from the phone or by the local administrative (Craft) CLEAR procedure.

If an HTTP backup or restore operation requires authentication and the realm in the challenge matches the stored realm, the stored credentials are used to respond to the challenge without prompting the user. However, if the realms do not match, or if an authentication attempt using the stored credentials fails, the user is then prompted to input new values for backup/restore credentials.

If an HTTP authentication for a backup or restore operation is successful and if the user ID, password, or realm used is different than those currently stored in the phone, the new values will replace the currently stored values.

You also have the following options to restrict or remove how crucial network information is displayed or used. For more information on these options, see Server Administration on page 63.

- Support signaling channel encryption.

  **Note:**

  Signaling and audio are not encrypted when unnamed registration is effective.

- Restrict the response of the 9600 Series IP deskphones to SNMP queries to only IP addresses on a list you specify.
- Specify an SNMP community string for all SNMP messages the phone sends.
- Restrict dial pad access to Local Administration Procedures, such as specifying IP addresses, with a password.
- Restrict dial pad access to Craft Local Procedures to experienced installers and technicians.
- Restrict the ability of the end user to use a phone *Options* application to view network data.
- Download and use third-party trusted certificates from Release 2.0 onwards.
- Compliant with IETF RFC 1948 *Defending Against Sequence Number Attacks*, May 1996, by S. Bellovin. from Release 1.5 onwards.
- Apply the existing security-related parameters, SNMP community string (SNMPSTRING), SNMP Source IP addresses (SNMPADD), and Craft Access Code (PROCPSWD) to administer on the call server and download with encrypted signaling in addition to unencrypted HTTP or encrypted HTTPS from Release 1.5 onwards.
- From the Avaya Support site, download a version that does not support VPN or media encryption from Release 6.2 onwards.

**Related topics:**

Registration and Authentication on page 41
Secure Shell Support on page 41

## Registration and Authentication

Avaya call servers support using the extension and password to register and authenticate 9600 Series IP deskphones. For more information, see the current version of your call server administration manual.

## Secure Shell Support

Secure Shell (SSH) protocol is a tool that the Avaya Services organization can use to remotely connect to IP deskphones to monitor, diagnose, or debug deskphone performance. Release

6.2 supports only the SSHv2 version. Because of the sensitive nature of remote access, you can disable permission with the SSH_ALLOWED parameter. Even if permission is given, the deskphone has several inbuilt security features. The deskphone displays a security warning message at start of the session. You can specify your own file using SSH_BANNER_FILE, or the deskphone will use the following default file:

```
This system is restricted solely to authorized users for legitimate business purposes
only. The actual or attempted unauthorized access, use, or modification of this
system is strictly prohibited. Unauthorized users are subject to company
disciplinary procedures and or criminal and civil penalties under state, federal, or
other applicable domestic and foreign laws. The use of this system may be monitored
and recorded for administrative and security reasons. Anyone accessing this system
expressly consents to such monitoring and recording, and is advised that if it
reveals possible evidence of criminal activity, the evidence of such activity may be
provided to law enforcement officials. All users must comply with all corporate
instructions regarding the protection of information assets.
```

If you require a custom warning message, you can set SSH_BANNER_FILE to an absolute URL, or the name of the file on the standard file server such as HTTPSRVR.

In addition to the warning message, you can administer the following parameters:

- The amount of inactivity time that will disable SSH with *SSH_IDLE_TIMEOUT*
- The number of failed login attempts that will disable SSH with *SSH_LOCKOUT_ATTEMPTS*
- The number of seconds the deskphone delays between failed login attempts with *SSH_LOGIN_DELAY*
- The user name permitted for SSH logins with *SSH_USERNAME*

## Time-to-Service

The IP Endpoint Time-to-Service (TTS) feature was introduced in Software Release 1.2.1, along with Communication Manager Release 4.0.

TTS changes the way IP phones register with their gatekeeper, reducing the time to come into service.

In the absence of TTS, the system uses a coupled two-step procedure to bring the IP phones into service:

1. H.323 registration
2. TCP socket establishment for call signaling

The TTS feature separates these steps. In Communication Manager Release 4.0, you can enable IP phones for service with just the registration step. TCP sockets are established later, as needed.

The TTS feature also changes the direction of socket establishment. With TTS, Communication Manager, rather than the phone, initiates socket establishment, which further

improves performance. In Communication Manager Release 4, you can enable TTS by default and can also disable TTS for all IP phones in a given IP network region by changing the IP Network form. TTS applies only to IP phones whose firmware has been updated to support this feature. TTS does not apply to the following phones: third party H.323, DCP, BRI, and analog.

From Release 3.0 onwards, 9600 Series IP deskphones can accept an incoming connection request from a server on their gatekeeper list, use this new connection to replace an existing connection, and continue operation without the need to re-register. With this mechanism, Communication Manager starts a new connection to each of these deskphones during a server interchange. These telephones then move quickly to the server and transition from the standby to active state.

The 96x1 Series deskphones support the TTS feature from Release 6.0 onwards.

For more information, see the *Administrator Guide for Avaya Communications Manager*,03-300509.

# Chapter 5: Communication Manager Administration

## Call server requirements

Before you perform administrative tasks, ensure that the proper hardware is in place and your call server software is compatible with 9600 Series IP deskphones. Use the latest PBX software and IP phone firmware.

**Related topics:**

Aliasing IP deskphones for switch compatibility on page 45

## Aliasing IP deskphones for switch compatibility

In Release 1.2, 9600 Series IP deskphones were natively supported by Communication Manager Release 4.0. Although the 9608,9611,9621, and 9641 deskphones are not natively supported on Communication Manager Release 4.0, those phones are natively supported as of Communication Manager 6.2.

Native support means that if you have Communication Manager Release 4.0 or greater, deskphones do not have to be aliased. Administer the deskphones on Communication Manager as follows:

| 9600 Series IP deskphone model | Administer on Communication Manager 3.1 as... | Administer on Communication Manager 4.0+ – 6.1 | Communication Manager 6.2 |
|---|---|---|---|
| 9608 | 4610 | 9650 | 9608 |
| 9610 | 4610 | 9610 | 9610 |
| 9611G | 4620 | 9650 | 9611G |
| 9620/9620L/9620C | 4610 | 9620 | 9620 |
| 9621G | 4620 | 9650 | 9621G |
| 9630/9630G | 4620 | 9630 | 9630 |
| 9640/9640G | 4620 | 9640 | 9640 |

| 9600 Series IP deskphone model | Administer on Communication Manager 3.1 as... | Administer on Communication Manager 4.0+ – 6.1 | Communication Manager 6.2 |
|---|---|---|---|
| 9641G | 4620 | 9650 | 9641G |
| 9650/9650C | 4620 | 9650 | 9650 |
| 9670G | 4620 | 9630 or 9640 | 9630 or 9640 |

**Note:**

Avaya recommends that the 9608, 9611, 9621, and 9641 deskphones be aliased as 9560s, however if you have already aliased these deskphones as 9630s or 9640s, you do not need to change anything; those aliased settings will also work.

You can add up to three SBM24 button modules on each deskphone that supports an SBM24 such as the 9608, 9611G, 9630, 9630G, 9640, 9640G, 9641G, 9650, 9650C, and 9670 IP deskphones.

As of software Release 6.0, you can add up to three BM12 button modules to the 9608, 9611G, and/or 9641G.

**Note:**

Although the 9620, 9620, and the 9620C can be aliased as a 4620SW IP deskphone, some features are not available. For example, the 9620 phones only support a total of 12 call appearances and administered feature buttons. The 4620 can be administered for a total of 24 call appearances and feature buttons.

**Note:**

You cannot configure call appearances for native support of the 9610 in Communication Manager 4.0. Ensure that when you alias the 9610 as a 4610, you must adhere to the unique 9610 administrative guidelines found in Administering 9610 IP Telephone features and CAs on page 56 and Special Administration for the 9610 IP Telephone on page 168.

**Note:**

Softphone is currently not supported using native support of the 96xx phones.

For specific administration instructions about aliasing 9600 Series IP deskphones, see Administering stations on page 56.

When you alias a 9610 IP telephone as a 4610SW IP deskphone, the four administrable call appearances or features should be:

- One primary call appearance
- The Directory, Next, and Make Call feature buttons that are hard-coded with Communication Manager 4.0 or later

**Note:**

The 9610 ignores any other features or call appearances.

When you alias a 9620, 9620L, and 9620C IP deskphone as a 4620SW IP deskphone, do not administer the following:

- A button module (SBM24, EU24, or EU24BL)
- Feature buttons 13 through 24

The 9608, 9611G, 9621G, 9630, 9630G, 9640, 9640G, 9641G, 9650, 9650C, and 9670G IP deskphones support twenty-four administrable telephony call appearances or features. In addition, the 9630, 9630G, 9640, 9640G, 9650, 9650C, and 9670G IP deskphones support the SBM24 button module. These models always support a single SBM24, and in Communication Manager 4.0 or later, support up to three SBM24 button modules per deskphone. From Release 6.0 onwards, the 9608, 9611G, and 9641G can support up to three BM12 button modules or up to three SBM24 button modules. The multiple button modules attached to a single 9608, 9611G or 9641G must all be the same model type.

The SBM24 button module and the BM12 button module provide another 24 administrable call appearances and features. The BM12 displays 12 call appearances or features at a time on each of two pages. You can use either button module as freestanding or attached directly to the applicable deskphone.

# Call server administration

For call server administration information not covered in this chapter, see the following documents on the Avaya support Web site:

- The *Administrator Guide for Avaya Communication Manager*, 03-300509 for more instructions for administering an IP telephone system on Communication Manager.

  . For information on the process of adding new telephones, see the chapter on *Managing Telephones*. For pertinent screen illustrations and field descriptions, see chapter on *Screen References*.

- *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504 for more information about switch administration for your network.

**Related topics:**

Administering the IP interface and addresses on page 48
Administering UDP port selection on page 48
Administering RSVP on page 48
Administering QoS on page 49

Administering IEEE 802.1Q on page 49
Administering DIFFSERV on page 49
Administering NAT on page 49

## Administering the IP interface and addresses

Follow these general guidelines:

- Define the IP interfaces for each CLAN and Media processor circuit pack on the call server that uses the IP Interfaces screen. For more information, see *Administration for Network Connectivity for Avaya Communication Manager* , 555-233-504.
- On the Customer Options form, verify that the IP Stations field is set to **Y** (Yes). If it is not set to (Y), contact your Avaya sales representative. This guideline does not apply to the IP Softphone.

## Administering UDP port selection

You can administer the 9600 Series IP deskphones from the Avaya Communication Manager Network Region form to support UDP port selection. For information on specific port assignment diagrams, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*, 16-603603 for the 9608, 9611G, 9621G, and 9641G deskphones.

Also see *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694* for all other 9600 Series deskphone modules.

For information about Avaya Communication Manager implementation, see *Administration for Network Connectivity for Avaya Communication Manager, 555-233-504* on the Avaya Support Web site.

Administer the switch to use a port within the proper range for the specific LAN, and the IP deskphone(s) copy that port. If no UDP port range is administered on the switch, the IP deskphone uses an even-numbered port, randomly selected from the interval 4000 to 10000.

## Administering RSVP

9600 Series Avaya IP deskphones support the Resource Reservation Protocol (RSVP) for IPv4 audio connections only.

The only way to enable RSVP is by appropriate switch administration. For more information, see your Avaya server administration documentation and *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

## Administering QoS

The 9600 Series IP deskphones support both IEEE 802.1D/Q and DiffServ. Other network-based QoS initiatives such as UDP port selection do not require support by the phones. However, they contribute to improved QoS for the entire network.

## Administering IEEE 802.1Q

The 9600 Series IP deskphones can simultaneously support receipt of packets that are tagged, or not tagged according to the IEEE 802.1Q standard. To support IEEE 802.1Q, you can administer 9600 Series IP deskphones from the network via LLDP, or by appropriate administration of the DHCP or HTTP/HTTPS servers.

You can administer the four IEEE 802.IQ QoS parameters L2Q, L2QVLAN, L2QAUD, and L2QSIG through the IP Network Region form. To set these parameters at the switch, see sections on *Quality of Service (QoS)* and *Voice quality administration* in *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

For information on setting these parameters manually, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*, 16–603603, and *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694* for other 9600 Series deskphone models.

## Administering DIFFSERV

The DiffServ values change to the values administered on the call server as soon as the phone registers. For more information on DiffServ values, see chapter on *Network Quality Administration* in *Administration for Network Connectivity for Avaya Communication Manager, 555-233-504.* Unless there is a specific need in your enterprise LAN, do not change the default values.

## Administering NAT

Network Address Translation (NAT) usage can lead to problems that affect the consistency of addressing throughout your network. All H.323 IP deskphones support NAT interworking.

Support for NAT does not imply support for Network Address Port Translation (NAPT). The phones do not support communication to the PBX through any NAPT device.

NAT requires specific administration on the call server. A direct Avaya IP phone-to-Avaya IP phone call with NAT requires Avaya Communication Manager Release 3.0 or later software. For more information, see *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504 on the Avaya support Web site.

# Administering Voice Mail

## Voice mail for deskphones with Communication Manager 4.0+

Release 1.2 and later provides native support for 9600 Series IP deskphones running on Communication Manager Release 4.0 or later. Although the 9608, 9611, 9621, and 9641 are not natively supported in Communication Manager 4.0, those phones are natively supported as of Communication Manager 6.2. See Aliasing IP deskphones for switch compatibility on page 45.

When native support applies, when you press the **Messages** button, the deskphone first determines if the call server has a dedicated number for retrieving voice mail. If a dedicated number exists, the deskphone proceeds with voice mail retrieval.

## Voice mail for deskphones aliased as 4600 Series IP Telephones

When native support does not apply, 9600 Series IP deskphones are aliased as 4600 Series IP telephones and run under CM Release 3.1 or later. In this case, use the settings file to configure the **Messages** button by setting the system parameter MSGNUM to any dialable string.

Some MSGNUM examples:

- A standard telephone number the telephone should dial to access your voice mail system, such as AUDIX or Octel.
- A Feature Access Code (FAC) that allows users to transfer an active call directly to voice mail. FACs are supported only for QSIG-integrated voice mail systems like AUDIX or Octel. QSIG is an enhanced signaling system with which the voice mail system and Avaya Communication Manager Automated Call Processing (ACP) exchange information.

When the user presses the **Messages** button, the deskphone automatically dials the number or FAC, giving the user one-touch access to voice mail.

On the settings file, specify the number to be dialed automatically when the user presses this button. The command is:

```
SET MSGNUM 1234
```

where *1234* is the Voice Mail extension for the CM hunt group or VDN.

For more information on the SET MSGNUM parameter, see 9600 Series H.323 customizable system parameters on page 84.

**Note:**

You can use MSGNUM only when you aliase the deskphone using non-native support. You must configure messaging for native support. A separate Voice Mail extension can be administered for each station.

# Call transfer administration

This section provides information about call transfer behaviors to consider when you administer the call server. The phone application presents a user interface, based in part on the deduction of the call state. The following server-based features can interact with the user interface resulting in a call state that might need explanation:

- The system parameter Abort Transfer? is set to *Yes*. After you start a transfer, you cannot press a non-idle call appearance until the transfer is complete or the transfer is aborted.
- The system parameter Abort Transfer? is set to *No*: The transfer proceeds normally even if the user presses a non-idle call appearance before the transfer is complete.
- The system parameter Transfer Upon Hang-up is set to *No*: The user must press the **Complete** softkey after dialing the intended destination for the transfer to be completed.
- The system parameter Transfer Upon Hang-up is set to *Yes*: The user can hang up immediately after dialing and the transfer proceeds normally.

The features Abort Transfer and Transfer Upon Hang-up can interact. If a user initiates a transfer, dials the destination, and hangs up without pressing the **Complete** softkey, the three possible outcomes are:

- The transfer is completed. Transfer Upon Hang-up is set to *Yes*, regardless of the Abort Transfer? setting.
- The transfer is aborted. Transfer Upon Hang-up is set to *No* and Abort Transfer? is set to *Yes*.
- The transfer is denied. Transfer Upon Hang-up is set to *No* and Abort Transfer? is set to *No* and the call appearance of the transferee remains on soft hold.

Attempts to transfer an outside call to an outside line are denied. However, the user can drop the denied destination and initiate a transfer to an internal destination.

You can use the *Toggle Swap* feature to swap the soft-held and setup call appearances. That is, the setup call appearance becomes soft-held, and the soft-held call appearance becomes active as the setup call appearance. This feature works only once the setup call appearance is connected on a call. If *Toggle Swap* is pressed while the setup call appearance has ringback, the call server sends a broken flutter to the setup call appearance. If you press *Toggle Swap* while the setup call appearance is still dialing, *Toggle Swap* is ignored without a broken flutter. Toggle swapping the hold status of call appearances can be confusing to the user.

# Call conferencing

This section provides information about conference call behaviors to consider when administering the call server. The deskphone application presents a user interface, based in part on the deduction of the call state. The following call states might result when the server-based features interact with the user interface:

- The system parameter Abort Conference Upon Hang-up is set to *Yes*:

  The user must dial and press the **Complete** softkey for the conference to be completed. If the user hangs up during conference setup before pressing **Complete**, the conference is cancelled with the held party remaining on [hard] hold. When the system parameter Abort Conference Upon Hang-up is set to *No*, the user can hang up immediately after dialing, dial a third party, then press the **Complete** softkey to have the conference proceed normally.

- The system parameter No Dial Tone Conferencing is set to *No* and the **Conference** or **Add** softkey is pressed:

  The call server automatically selects an idle call appearance for the user to dial on. This action allows the next conferee to be added. When the system parameter No Dial Tone Conferencing is set to *Yes*, the user must manually select a call appearance after pressing the **Conference** or **Add** softkey.

Conferencing behavior changes significantly when you set the Select Line Conferencing to *Yes*. Then the No Dial Tone Conferencing is automatically set to *Yes*. Specifically the following scenarios can occur:

- If the user finishes dialing the intended conferee, pressing the initial call appearance completes the conference, as if the **Join** softkey was pressed.
- If the user has not finished dialing the intended conferee, pressing the initial call appearance (placed on soft hold when **Conference** or **Add** was pressed) cancels the conference set up.
- If the user presses the **Conference** or **Add** softkey, then immediately presses a hard-held call appearance, the previously held call appearance is retrieved from hold and joins the existing conference.

When you set the system parameter Select Line Conferencing to *No*, the user can cancel the conference setup by pressing the call appearance on soft hold before pressing **Join**. Selecting a hard-held call appearance during conference setup establishes the held call as the intended conferee.

For either Select Line Conferencing setting, if the user is in conference setup and answers an incoming call, the incoming call is established as the intended conferee. Then the user must press **Join** to add the answered call to the conference. If the user does not want the incoming call to be part of the conference, the call should not be answered, or the call can be answered and then hung up before continuing the conference setup. Pressing an in-use call appearance during conference setup makes that call appearance the intended conferee. The Toggle Swap feature works for Conference setup similar to Transfer Setup.

For more information on call transfers, see Administering call transfers on page 51.

# Phone administration on Avaya Aura® Communication Manager

This section covers Avaya Aura® Communication Manager administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. You must administer Avaya Aura® Communication Manager on SAT or by Avaya Site Administration to optimize the phone user interface. The system-wide CM form and the particular page or screen that needs to be administered for each feature are provided in the SAT. You need Communication Manager 3.1.2 or later.

**Related topics:**

Feature-related system parameters on page 54

# Feature-related system parameters

In Avaya Communication Manager Release 4.0 and later, you can administer three system-wide parameters. When you administer these parameters on CM, the parameters are automatically downloaded to the phone during registration. You do not need to add these parameters using the settings file or sett them locally for each phone. The three system parameters are: SNMP community string, SNMP Source IP addresses, and Craft Access Code (PROCPSWD).

**Note:**

Commenting out SNMPSTRING in the settings file will not prevent a response to an SNMP query unless the CM administration is also changed accordingly. Also, setting the SNMP flag on the IP-Options form in CM to "n" does not disable SNMP. You must enable the download flag and leave the community string value blank so that when the telephone registers, the SNMPSTRING value will remain null.

To administer these three parameters use Page 3 of the *change system-parameters ip-options form*.

| Name | Description |
|---|---|
| **On-Hook Dialing** | Set up CM so that the phone supports on-hook dialing. Use the System Parameters Features form page 10. Use the command **`Change system-parameters features`** to view the form and make the change. |
| **Auto Hold** | Set up CM to enable Auto Hold, so that the phone automatically places an active call on hold when the user answers or resumes a call on another call appearance. Use the System Parameters Features form, page 6. |
| **Coverage Path** | Administer a coverage path for both phone demonstration and normal operations. Use the Coverage Path form and give it a number, for example, Coverage path 1. If Voice Mail is available, administer the hunt group or VDN, depending on the type of VM system being used. |
| **Enhanced Conference Features** | Enable enhanced conference display to support the user experience for conferences. Set Block Enhanced Conference Display on the Class of Restriction (COR) form to No. Use the command **`Change COR`**, followed by a number, to view the form and make the |

| Name | Description |
|---|---|
| | change. This is a sample of the Class of Restriction form. |
| **EC500** | Enable EC500 on the Off-PBX Telephones Station Mapping form if upi have acquired the EC500 licenses. This feature requires trunking to work properly. Use the following command to make the change: **`Change Off-pbx Telephone Mapping`** |
| **Wideband Audio** | Enable Wideband Audio, by using the **`Change IP codec`** command on CM. Ensure that G.722–64K is first on the list of codecs. Note that wide band audio works only for direct-IP calls between two 96xx endpoints, either with both registered to the same server, or registered to different servers when connected by IP trunks. Calls between two 96xx phones connected by an IP trunk do not currently support wide band audio when the call is shuffled so that the media travels directly between the two 96xx IP phones. Calls that involve three or more parties, even if all parties use 96xx IP phones, do not use wide band. Calls between two 96xx IP phones where audio is terminated at a port network/gateway (PN/GW) media resource will not use wideband.<br>Ensure that G.722 is added to all codec-sets that can possibly be used between all regions on the IP-Network Regions form where 96xx IP phones exist. Technically, G722 does not need to be first. What is needed, however, is that all the non media processor-supported codecs (G722, SIREN, etc.) be placed before the media processor-supported codecs (G711, G729, G726, G723).<br>For information on using the wideband codecs with the Communication Manager, see *Administering Avaya Aura® Communication Manager*, 03-300509. |

# Station administration

Administer the following station features on the Station form, which comprises several pages. You must set the features covered in this section to optimize the user interface.

With Avaya Aura Communication Manager Release 4.0 and later, you can perform central call server administration of the GROUP parameter on a station-by-station basis. This parameter is then downloaded to each applicable deskphone starting with the next deskphone boot-up. You can use the GROUP Identifier in conjunction with the 46xxsettings file for administration of specific groups of deskphones. For more information, see Using the GROUP parameter to set up customized groups on page 81. You can administer the GROUP ID parameter on page 3 of the Change Station Form.

If applicable, before administering stations ensure that the deskphones are aliased according to the chart for Aliasing IP Deskphones for switch compatibility on page 45.

**Related topics:**

Administering features on page 56

## Administering features

Administer the following Station Features for maximum user experience:

| Name | Description |
|---|---|
| **Enhanced Conference Features** | Administer **Conf-dsp** (conference display) on the station form as a feature button. Users gain the benefits of enhanced conference features. |
| **Auto select any idle appearance** | Set **Auto select any idle appearance** to N (no) to optimize answering calls. |

# Administering feature buttons and call appearances (CAs)

## Administering 9610 IP deskphone features and CAs

### About this task

You must administer the 9610 as a 4610 on releases earlier than Communication Manager 3.1 as a 4610. Administer the 9610 as a 9610 on Communication Manager 4.0 and later. The

9610 has only one line appearance. Perform the following Communication Manager administration steps:

### Procedure

1. Administer the first call appearance/feature button on the CM Station form as a call appearance.
2. Administer *Directory*, *Next* and Call-disp which is shown as Make Call on the deskphone as the next three feature buttons.

   These features are hard-coded on Communication Manager 4.0 and later.
3. The system will ignore anything administered beyond the first six call appearances.

   On Communication Manager 4.0 and later the call appearance or feature button assignments are hard- coded.

**Important:**

Set *Restrict last appearance* to *n* (no) on the Station form so that incoming calls can be placed and outgoing calls can be answered.

**Note:**

A 9610 IP deskphone does not reflect CM administrative changes until you restart the deskphone. The 9610 does not support the SBM24 button module.

## Administering 9620,9620L,9620C IP deskphone features and CAs

You can administer Feature or Call Appearance Buttons 1 to 12 on the CM Station form, which the deskphone Feature screen then displays in sequence. The deskphone does not display any of the Feature Button labels administered on buttons 13 to 24. The 9620 and its counterpart models do not support button modules.

## Administering features and CAs for all other IP deskphones

You can administer Feature/Call Appearance Buttons 1 to 24 on the CM Station form. The features administered on the Station form appear in the same sequence on the deskphone Feature screen.

Features administered on the Expansion Module (SBM24/BM12) Call Appearance buttons display on the deskphone Features screen following the first 24/12 administered feature buttons.

All administered Button Module Labels, Call Appearances and Feature Buttons, display on the corresponding module buttons.

In the Table 1: Station form administration results on page 58 the term *phone screen* refers to either the call appearance screen or the features screen, as applicable to the button type.

**Table 6: Station form administration results**

| Feature / Call Appearance (CA) / Bridged Call Appearance (BA) buttons on the Station form... | Displayed as: | | | |
|---|---|---|---|---|
| 1 to 3 | 9620/9620C/ 9620L | 9608 9611G 9621G 9630/9630G 9640/9640G 9641G | 9650/9650C | 9670G |
| 4 to 11 | CAs/BAs on Phone screen; must scroll to see more than 3 | CAs/BAs on Phone screen: must scroll to see more than 6 | Aux buttons 1 to 8 CAs/BAs on Phone screen; must scroll to see more than 3 | CAs/BAs on Phone screen; all buttons also appear on the Quick Touch panel (if enabled) and not on the display screen. If Quick Touch panel is disabled, 6 CAs display; switch to Features and scroll to see up to 12 feature buttons |
| 12 to 19 | N/A | Scroll to see CAs/BAs, features on Feature List | Aux buttons 9 to 16 | Scroll to see CAs/BAs, features on Feature List |
| 20 to 24 | N/A | Features on Feature List | Features on Feature List | Features on Feature List |
| 25 to 48 | N/A | 1st SBM24 | 1st SBM24 | 1st SBM24 |
| 49 to 72 | N/A | 2nd SBM24 | 2nd SBM24 | 2nd SBM24 |
| 73 to 96 | N/A | 3rd SBM24 | 3rd SBM24 | 3rd SBM24 |

For additional information about administering the call server for 9600 Series IP deskphones, see the following Avaya documents, available on the Avaya Support Web site:

- *Administrator Guide for Avaya Communication Manager*, 03-300509.
- *Feature Description and Implementation for Avaya Communication Manager*, 555-245-770.

## Administering enhanced phone screen displays for certain IP deskphones

The deskphone determines the total number of call appearances, primary or bridged, and any adjunct button modules, if applicable, that were administered for the deskphone if you set the value of the system parameter FBONCASCREEN to 1. This feature applies to the 9608, 9611G, and 9630/9630G/9640/9640G deskphones.

If the total number of call appearances is less than the number of Application Lines the deskphone supports, then all call appearances, either primary or bridged, that have been administered for the deskphone including any adjunct button modules, if applicable, are displayed in order. The remaining Application Lines display the first administered feature buttons for the deskphone, in order from top to bottom without any gaps.

**Note:**

This feature applies to administered feature buttons for the telephone only, not to administered feature buttons for any adjunct button module.

## Assigning 9650/9650C Aux buttons

### About this task

The 9650/9650C Communication Manager 4.0 Station form assigns buttons 4 to 11 to the Aux Labels 1 to 8, and buttons 12 to 19 to the shifted view of Aux buttons 9 to 16. Communication Manager button assignments 20-24 do not appear on the Aux button labels. Additionally, any call appearances that are assigned to Communication Manager buttons 4 through 24, like all the 96xx phones, appear on the Phone screen in a scrollable list.

Any feature assigned to CM buttons 4 through 24, as in the other 96xx phones, shows on the features list. To reach the features list, press the left or right arrow key while viewing the call appearances screen on the phone.

The 16 Aux button labels display call appearances, bridged call appearances, or features. The deskphone displays eight labels at a time on the bottom two rows of the screen. Users can toggle between the two sets of 8 labels using the Aux shift button to the right of the Aux labels.

### Procedure

1. The Aux button label area can fit 6-7 characters, depending on the width of the characters used. Cluster any call appearances together, bridged call appearances together, or similar features together.

   For example, keep *Directory Next* and *Make Call* adjacent on the same Aux button row. Do not split like labels between the two sets of Aux buttons.
2. Administer features that are not directly usable by the user, such as enhanced conference display, on the Station Form on buttons 20 to 24.
3. Call appearances display 5 digits with a reserved area for a call state icon.
4. In the A menu, you can use the first two Call Settings to set the phone to go to the Phone screen when the phone is ringing using the *Go to Phone Screen on Ringing* features. You can set the phone to go to the Phone screen when the user is dialing by using the *Go to Phone Screen on Dialing* feature.

   Tip: You must set both settings to Yes - except for users covering many bridged appearances who may prefer to set the *Go to Phone Screen on Ringing* option to No. Users can change these settings for themselves using the Call Settings submenu.
5. Group similar types of Aux buttons together on one page (Aux buttons 1-8 or Aux buttons 9-16) if possible.
   - If the user has bridged call appearances on Aux buttons, assign the bridged lines to Aux buttons 1-8 or to Aux buttons 9-16.
   - If the user has AD buttons, put them on the same page, if possible.
   - Keep related features on the same page of Aux buttons. For example, keep *Directory*, *Next*, and *Make call* together on the same row of Aux button labels and do not split between Aux buttons 8 and 9, which represent two different pages.
6. Administer features that the user cannot use directly, such as enhanced conference display on the Station form on buttons 20 to 24.
7. Call appearances display 5 digits with a reserved area for a call state icon.

## Button module administration on the 9608, 9611G, 9630/9630G, 9640/9640G, 9641G, 9650/9650C, and 9670G

Use the applicable Station form to enable the SBM24 or BM12 Expansion button modules and administer Call Appearances as primary appearances, bridged appearances, or busy indicators.

If you cannot see the BM12 or SBM24 Call Appearance corresponding to the CM call-associated display message or dialed-digits string because the user is not on the Phone

screen, the deskphone Top Line displays the call-associated display message or dialed-digits string.

## Administering the Conference Details screen for ad-hoc conferences

### About this task

Using the **Conference Details** softkey, you can view the parties on a conference call and selectively mute or drop individual parties for a conference call setup.

If you administered an Expansion Module button, the BM12 or SBM24 button module must be connected.

### Procedure

1. To enable Conference Details capabilities, on the Class of Restriction (COR) form ensure that **Block Enhanced conference/Transfer Displays** is set to No.
2. Administer the Conference Display Feature Button to a Phone button on the Phone screen. For more information, see Administering feature-related system parameters on page 54.

## Quick Touch panel for touch screen deskphones

The 9621G, 9641G, and 9670G deskphones support the *Quick Touch* panel. You can use the *Quick Touch* panel to gain access to any additional call appearances or switch features programmed on any of eight Quick Touch buttons. The*Quick Touch* panel is located at the bottom of the screen below the application area. The panel is distinguished visibly from the application area and serves as a container for the Quick Touch buttons.

Quick Touch buttons are similar to the Aux buttons on the 9650. Quick Touch buttons are on-screen objects that contain a text label and can have an associated graphic icon to indicate the status of the assigned feature for the button. The space available for the text label is 8-9 characters. If the button is a call appearance, the status icon is on the left side, otherwise the status icon is on the right side.

The basic appearance of a Quick Touch button resembles an actual physical button, and provides appropriate *pressed* or *not pressed* appearances.

The *Quick Touch* panel supports a maximum of eight Quick Touch buttons, arranged in two rows of up to four buttons each. Only buttons with assigned features are displayed, populated from left to right starting in the top row.

The *Quick Touch* panel is displayed on the Phone screen call appearance list and the Personalizing button labels option, when enabled by the associated user option **Home** >

**Settings** > **Options & Settings** > **Screen & Sounds** > **Show Quick-Touch Panel**, even if the *Quick Touch* panel contains 0 buttons. If all or any buttons are empty, you might need to administer the buttons. On the 9670, you can select to display all eight, or no Quick Touch buttons; the 9621G and 9641G provide the option to display all eight, or four, or no Quick touch buttons.

# Shuffling

### About this task

Administer shuffling on the following three forms:

### Procedure

1. Feature-Related Parameters form:
   Set the **Direct IP-IP Audio Connections?** field to y (yes).
2. IP Network Region form:
   Set the **Intra-region IP-IP Direct Audio** field and the **Inter-region IP-IP Direct Audio** field to y (yes).
3. Station form:
   Set the **Direct IP-to-IP Audio Connection** to y (yes). The Station form setting overrides the network region, and the network region overrides the system setting.

# Wideband codecs

### About this task

You must administer wideband codecs for each IP codec set and for IP network regions.

# Chapter 6: Server Administration

## Software Prerequisites

Ensure that you own licenses to use the DHCP, HTTP, and HTTPS server software.

**Note:**

You can install the DHCP and HTTP server software on the same computer.

**Caution:**

The firmware in the 9600 Series IP Deskphones reserves IP addresses of the form 192.168.2.x for internal communications. The phone might not function properly if you configure addresses in that range.

## Administering the DHCP and file Servers

Dynamic Host Configuration Protocol (DHCP) minimizes maintenance for the 9600 Series IP Telephone network. With DHCP, you need not individually assign and maintain IP addresses and other parameters on each IP phone on the network.

Depending on administration, the DHCP server provides the following information to the 9600 Series IP Telephones:

- An IP address of the 9600 Series IP Telephone
- An IP address of the Avaya call server
- An IP address of the HTTP or HTTPS file server
- The subnet mask
- An IP address of the router
- A DNS Server IP address

Administer the LAN so each 9600 Series IP deskphone can reach a DHCP server that contains the IP addresses and subnet mask.

The 9600 Series IP Telephone cannot function without an IP address. Using the IP address reuse capability, the phone can reuse its previous IP address and parameter settings even if

the DHCP server is temporarily unavailable. A user can manually assign a different IP address to an IP deskphone. When the DHCP server finally returns, the 9600 Series IP Telephone does not search for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process.

Ensure that:

- A minimum of two DHCP servers are available for reliability.
- A DHCP server are available when the IP deskphone reboots.
- A DHCP server are available at remote sites if WAN failures isolate IP deskphones from the central site DHCP servers.

The file server provides the 9600 Series IP Telephone with a script file and, if appropriate, new or updated application software.

See Step 3: Establishing a VPN Connection (optional) on page 25 under Deskphone Initialization Process Overview on page 24.

In addition, you can edit an associated settings file to customize phone parameters for your specific environment. For more information, see Administering Telephone Options.

**Related topics:**

Configuring DHCP Option 242 on page 64

# Configuring DHCP Option 242

### About this task

To administer DHCP option 242 for SSON, make a copy of the existing option 176 for your 46xx IP deskphones. Option 242 is specific to the default site and applies to DHCPv4 only. You can then perform one of the following actions:

### Procedure

1. Ignore any parameters the 9600 Series IP Deskphones do not support for setting through DHCP in option 242 to be ignored, or
2. Delete unused or unsupported 9600 Series IP Deskphone parameters to shorten the length of the DHCP message.

### Result

You can set only the following parameters in the DHCP site-specific option for 9600 Series IP Deskphones, although most of them can be set in a 46xxsettings.txt file as well.

**Table 7: Parameters Set by DHCP in a Site-Specific Option**

| Parameter | Description |
|---|---|
| DNSSRVR | Specifies the DNS server IP address or addresses. |
| DOMAIN | Specifies the string that is appended to DNS names in parameter values when they are resolved into IP addresses. |
| DOT1X | Controls the operational mode for 802.1X. The default is 0, for pass-through of multicast EAPOL messages to an attached PC, and enables Supplicant operation for unicast EAPOL messages. |
| DOT1XSTAT | Controls 802.1X Supplicant operation. |
| HTTPDIR | Specifies the path name to prepend to all file names used in HTTP and HTTPS GET operations during startup. (0 to 127 ASCII characters, no spaces.) The command is *SET HTTPDIR myhttpdir*. The path relative to the root of the TLS or HTTP file server where 9600 Series IP Deskphones files are stored. If an Avaya file server is used to download configuration files over TLS, but a different server is used to download software files through HTTP, set the path of the Avaya server in the DHCP site-specific option, and set HTTPDIR again in the 46xxsettings.txt file with the appropriate path for the second server. HTTPDIR is the path for all HTTP operations except for BRURI. |
| HTTPPORT | Specifies the TCP port number to download the HTTP file. |
| HTTPSRVR | Specifies the IP addresses or DNS names of HTTP file servers used to download 9600 Series IP Deskphones software files. The files are digitally signed, so TLS is not required for security. |
| ICMPDU | Controls the extent to which ICMP Destination Unreachable messages are sent in response to messages sent to closed ports so as not to reveal information to potential hackers. The default is 1 which sends Destination Unreachable messages for closed ports used by traceroute. |
| ICMPRED | Controls whether ICMP Redirect messages are processed. The default is 0 which redirects messages that are not processed. |
| L2Q | specifies the 802.1Q tagging mode. The default is 0 which signifies automatic. |
| L2QVLAN | VLAN ID of the voice VLAN. The default is 0. |
| LOGLOCAL | Controls the severity level of events logged in the SNMP MIB. The default is 7. |
| MCIPADD | CM servers IP addresses or DNS names. If there are too many addresses or names to include all of them in the DHCP site-specific option, include at least one from each major system. Then set MCIPADD again in the 46xxsettings.txt file with the complete list of addresses. Providing a subset of the addresses through DHCP improves reliability if the file server is not available due to server or network problems. |

| Parameter | Description |
|---|---|
| NDREDV6 | NDREDV6 IPv6 only. Controls whether IPv6 Neighbor Discovery Redirect messages will be processed. |
| PHY1STAT | Controls the Ethernet line interface speed. The default is 1 which indicates that it is auto-negotiate. |
| PHY2STAT | Controls the secondary Ethernet interface speed. The default is 1 which indicates that it is auto-negotiate. |
| PROCPSWD | Security string used to access local procedures. The default is 27238 (CRAFT). |
| PROCSTAT | Controls whether local Craft procedures are allowed. The default is 0 which indicates that access to all administrative options is allowed. |
| REREGISTER | The number of minutes the phone waits before and between re-registration attempts. |
| REUSETIME | The n umber of seconds to wait for successful completion of DHCP before reusing previous parameters on the default (port) VLAN. The default is 60. |
| SIG | The signaling protocol download flag that indicates which protocol applies (H.323 (1), SIP, (2) or Default (0). For software releases prior to 6.0, SIG can only be set manually on the deskphone and not through DHCP or in the 46xxsettings.txt file. Default means the default protocol supported at that location. A custom upgrade file is required to support both protocols. For software releases 6.0 and later, separate upgrade files with different names are used for H.323 and SIP, and Default means to download the upgrade file for the same protocol that is supported by the software that the deskphone is currently using. |
| SNMPADD | Allowable source IP addresses for SNMP queries. The default is “ ” (Null). |
| SNMPSTRING | SNMP community name string. The default is “ ” (Null). |
| STATIC | Controls whether to use a manually-programmed file server or CM IP address instead of those received through DHCP or a settings file. If a manually programmed file server IP address is to be used, STATIC must be set through DHCP. |
| TLSDIR | Specifies the path name prepended to all file names used in HTTPS GET operations during startup. |
| TLSPORT | Specifies the TCP port number for HTTPS file downloading. |
| TLSSRVR | Specifies the IP addresses or DNS names of Avaya file servers to download configuration files.<br>Specifies that Transport Layer Security is used to authenticate the server. |
| TLSSRVRID | Controls whether the identity of a TLS server is checked against its certificate. |

| Parameter | Description |
|---|---|
| UNNAMEDSTAT | Specifies whether the deskphone will attempt unnamed registration. |
| VLANTEST | Controls the length of time the deskphone tries DHCP with a non-zero VLAN ID. When the interval is exceeded, the deskphone records the VLAN ID so that the VLAN ID is not used again, and DHCP continues on the default VLAN. The default is 60 seconds. |

These parameters are saved in the non-volatile memory of the 9600 Series IP Deskphones. If the DHCP server is not available for any reason during phone restart or reboot, the phone uses these saved parameters.

# DHCP Generic Setup

This document describes the generic DCHPv4 and DHCPv6 administration that works with the 9600 Series IP Deskphones. Windows operating systems include several DHCP software alternatives such as:

- Windows NT® 4.0 DHCP Server
- Windows 2000® DHCP Server
- Windows 2003® DHCP Server

Any other DHCP application might work. It is the responsibility of the customer to install and configure the DHCP server correctly.

# Setting up the DHCP server

### About this task

DHCP server setup involves:

### Procedure

1. Follow vendor instructions to install the DHCP server software.
2. Configure the DHCP server with:
    - IP addresses available for the 9600 Series IP Deskphones.
    - The following DHCP options for using IPv4:
        - **Option 1: Subnet mask**.

- **Option 3: Gateway (router) IP addresses**. If using more than one address, the total list can contain up to 255 total ASCII characters. You must separate IP addresses with commas with no intervening spaces.
- **Option 6: DNS servers address list**. If using more than one address, the total list can contain up to 127 total ASCII characters. You must separate IP addresses with commas with no intervening spaces. At least one address in Option 6 must be a valid, dotted decimal address without a zero.
- **Option 15: DNS Domain Name**. This string contains the domain name that the system uses to resolve DNS names in system parameters into IP addresses. The system appends this domain name to the DNS name before the9600 Series IP Deskphone resolves the DNS address. If you want to use a DNS name for the HTTP server, Option 15 is required. Otherwise, you can specify a DOMAIN as part of customizing HTTP. For more information, see DNS addressing on page 115.
- **Option 51: DHCP lease time**. If this option is not received, the DHCPOFFER is not accepted. Avaya recommends a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the system treats the IP address lease as infinite as per RFC 2131, Section 3.3. In this case, renewal and rebinding procedures are not required even if you receive Options 58 and 59.

  Expired leases cause 9600 Series IP Deskphones to reboot. Avaya recommends providing enough leases so an IP address of an 9600 Series IP Deskphone does not change if it is briefly taken offline.

  **Note:**

  The DHCP standard states that when a DHCP lease expires, the device should immediately cease using the assigned IP address. However, if the network has problems and the only DHCP server is centralized or if the DHCP server itself has problems, the deskphone does not receive responses to its request for a renewal of the lease. In this case the deskphone is unusable until the server can respond. Expired leases do not cause the phone to reboot because you can renew expired leases. However, if the new IP address is different that previous it will cause the phone to reboot. Ensure that once assigned an IP address, the deskphone continues using that address after the DHCP lease expires, until the system detects a conflict with another device. With the system parameter DHCPSTD, an administrator can specify that the telephone will do one of the following: a). Comply with the DHCP standard by setting DHCPSTD to 1. b). Continue to use the IP Address after the DHCP lease expires by setting DHCPSTD to 0. This setting is the default. For more information, see 9600 Series H.323 customizable system parameters on page 84. If the default is invoked, after the DHCP lease expires the phone continues to broadcast DHCPREQUEST messages for its current IP address. The

deskphone sends an ARP Request for its own IP Address every 5 seconds until the phone receives a DHCPACK, a DHCPNAK, or an ARP Reply.. After receiving a DHCPNAK, or ARP Reply, the phone displays an error message, sets its IP address to 0.0.0.0, and attempts to contact the DHCP server again. Depending on the DHCP application you choose, be aware that the application does not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client a day or more. For example, Windows NT® DHCP reserves expired leases for about one day. This reservation period protects a lease for a short time. If the client and the DHCP server are in two different time zones, the clocks of the computers are not synchronized. If the client is not on the network when the lease expires, you have the time to correct the situation.

The following example shows the implication of having a reservation period: Take two IP addresses, therefore two possible DHCP leases. Take three IP deskphones, two of which are using the two available IP addresses. When the lease for the first two deskphones expires, the third deskphone cannot get a lease until the reservation period expires. Even if the other two deskphones are removed from the network, the third deskphone remains without a lease until the reservation period expires.

- **Option 52 - Overload Option**, if required. If this option is received in a message, the 9600 Series IP Deskphone interprets the *sname* and *file* fields in accordance with IETF RFC 2132, Section 9.3.
- **Option 58 - DHCP lease renew time**. If the 9600 Series IP Deskphone does not receive this parameter, or if this value is greater than that for Option 51, the default value of T1 (renewal timer) is used as per IETF RFC 2131, Section 4.5.
- **Option 59 - DHCP lease rebind time**. If the 9600 Series IP Deskphone does not receive this parameter, or if this value is greater than that for Option 51, the default value of T2 (rebinding timer) is used as per RFC 2131, Section 4.5
- **Option 242 - Site-Specific Option Number (SSON)** You do not have to use Option 242. If you do not use this option, you must ensure that the key information, especially HTTPSRVR and MCIPADD, is administered appropriately elsewhere.

  An example of proper DHCP administration is:

  Option 242 for DHCP: **`MCIPADD =`***xxxx.xxx.xxx.xxx*

## Result

In the following table,DHCPACK Setting of Parameter Values on page 70 the 9600 Series IP Deskphone sets the following parameter values to the DHCPACK message field and option.

**Table 8: DHCPACK Setting of Parameter Values**

| Parameter | Set to |
|---|---|
| DOMAIN | If received, Option #15. |
| DHCP lease renew time | Option #58 (if received). |
| DHCP lease rebind time | Option #59 (if received). |
| DHCP lease time | Option #51 (if received). |
| DNSSRVR | Option #6. |
| HTTPSRVR | The siaddr field, if that field is not a zero. |
| TLSSRVR | The siaddr field, if that field is non-zero. |

Since the DHCP site-specific option is processed after the DHCP fields and standard options, the values set in the site-specific option supersede any values set by DHCP fields or standard options, as well as any other previously set values.

You cannot set parameters L2Q, L2QVLAN, and PHY2VLAN from a *site-specific option* if their values were previously set by LLDP. For more information, see About Link Layer Discovery Protocol (LLDP) on page 123.

**Note:**

The 9600 Series IP Deskphones do not support Regular Expression Matching, and therefore, do not use wildcards. For more information, see Administering Options for 9600 Series H.323 deskphones on page 83.

In configurations where the upgrade script and application files are in the default directory on the HTTP server, do not use the command HTTPDIR=<path>.

# Setting up a DHCPv6 server

## About this task

**Important:**

Avaya does not support IPv6 for the general market, and makes the software available to a specific set of customers with known limitations documented in the section Features not supporting IPv6 on page 75. Any additional limitation or bugs discovered within this release will be considered for resolution in future major releases

To set up the DHCPv6 server:

## Procedure

1. Install the DHCP server software according to vendor instructions.

2. Configure the DHCP server to send a Vendor-Specific Information (VSI) option with an enterprise number of 6889 which is the Avaya Enterprise Number.
3. Inclusion of vendor-specific option with an opt-code of 242 within that option.
4. Setting the option-data portion of the vendor-specific option with any or all of the applicable parameters. For information about the parameters, see bullet list in Setting up the DHCP server for the DHCP site-specific option.

   Additionally, the parameters DOMAIN and DNSSRVR can be set in other numbered options by DHCP. These parameters can also be set in the Avaya DHCPv6 vendor-specific option.

### Result

The vendor-specific option is processed after the DHCP fields and standard options. As such, any values set using the VSI will supersede any values that are set using DHCP fields or standard options, as well as any other previously set values.

# HTTP Generic Setup

### About this task

You can store the same application software, script file, and settings file on an HTTP server as you can on a TFTP server. The 9600 Series IP Deskphones do not support TFTP. With proper administration, the 9600 Series IP Deskphone seeks out and uses the application software, script file, and settings file. The 9600 Series IP Deskphone might lose some functionality, if you reset the HTTP server or the HTTP server is unavailable. For more information, see Administering the DHCP and File Servers on page 63.

**Caution:**

Ensure that the files defined by the HTTP server configuration are accessible from all 9600 Series IP Deskphones that need those files. Ensure that the file names match the names in the upgrade script, including case, as UNIX systems are case-sensitive.

**Note:**

Use any HTTP application you want. Commonly used HTTP applications include Apache® and Microsoft® IIS™.

**Important:**

You must use the Avaya Web configuration server to obtain HTTPS so that information is authenticated. The Avaya Web configuration server does not support backup/restore. If you intend to use HTTP for backup and restore purposes, you must use an HTTP server that is independent of the Avaya Web configuration server.

To set up an HTTP server:

### Procedure

1. Install the HTTP server application.
2. Administer the system parameter HTTPSRVR to the addresses of the HTTP server.

   Include the parameter in DHCP Option 242, or the appropriate SSON Option.
3. Download the upgrade script file and application files from the Avaya website http://www.avaya.com/support to the HTTP server.

   For more information, see Telephone Software and Application Files on page 77.

**Note:**

When you download the application file from the Avaya Support Web site, ensure you are downloading the correct version. One version allows VPN and media encryption functionality, while the other disables those functions.

**Note:**

Many LINUX servers distinguish between upper and lower case names. Ensure that you specify the settings file name accurately, as well as the names and values of the data within the file.

### Result

If you choose to enhance the security of your HTTP environment by using Transport Layer Security (TLS), you must:

- Install the TLS server application.
- Administer the system parameter TLSSRVR to the addresses of the Avaya HTTP server.

# Backup and restore processing

9600 Series IP Deskphones support the use of the HTTP client, optionally over TLS to back up and restore user-specific data if initiated by higher-level system procedures. Only one backup or restore attempt is made per request. Retries are the responsibility of the initiating process.

If the BRURI parameter is null, or if the BRURI parameter begins with any character sequence other than http:// or "https://", the initiating process receives a failure indication to the in response to all backup and restore requests.

For backup, the initiating process must supply the backup file and the file name, and the file is sent to the server through an HTTP PUT message. A success or failure indication is returned to the initiating process based on whether or not the file is successfully transferred to the server.

For restore, the initiating process must only supply the file name, and the file is requested from the server through an HTTP GET message. The file is returned to the initiating process if it is successfully obtained from the server, otherwise a failure indication is returned.

For deletion, the initiating process must only supply the file name. The server requests deletion of the file through an HTTP DELETE message. The initiating process receives a success indication, if a 2xx HTTP status code is received, otherwise a failure indication is returned.

For all operations, the URI used in the HTTP message is constructed from the value of BRURI and the file name. If the value of BRURI ends with "/", the file name is appended, otherwise a forward slash is appended to the value of BRURI, then the file name is appended. The BRURI can includes a directory path and a port number or both as specified in IETF RFCs 2396 and 3986.

From Release 6.1 onwards, if the authority component of BRURI contains a DNS name, and if a TCP connection cannot be established to the IP address that was previously used to attempt to establish a connection with the server, the deskphone again attempts to resolve the DNS name. If a new IP address is received, the deskphone attempts to establish a connection to that address. If the deskphone receives the same IP address from the DNS server used previously, or if a TCP connection cannot be established with the new IP address, a failure indication is returned to the initiating process.

With TLS, the phone uses a TLS_RSA_WITH_AES_128_CBC_SHA cipher suite. If TLS is used but no digital certificates have been downloaded based on the TRUSTCERTS value, the IP address of the call server with which the phone is registered and the registration password of the phone will be included as the credentials in an Authorization request-header in each transmitted GET and PUT method. If at least one digital certificate has been downloaded based on TRUSTCERTS, the IP address of the call server with which the phone is registered. The registration password of the phone is included in the credentials in an Authorization request-header in each transmitted GET and PUT method only if the value of BRAUTH is 1.

When the call server IP address and the registration password of the phone are included as the credentials in an Authorization request-header, the call server IP address is included first in dotted-decimal format, followed by a colon (hex 3A), followed by the registration password of the phone. The server is expected to get the extension number of the phone from the backup or restore file name. The server must also protect the user's credentials once they are received via the secure TLS connection.

The phone sends the registration credentials without regard to the BRAUTH setting if no certificates have been downloaded. Only server certificates signed by an Avaya Root CA certificate are authenticated if no certificates have been downloaded.

The9600 Series IP Deskphones support HTTP authentication for backup and restore operations. The phone stores the authentication credentials and the realm in non-volatile memory that will not be overwritten if new phone software is downloaded. The default value of the credentials and the realm is set to null at manufacture and at any other time that user-specific data is removed from the deskphone.

If an HTTP backup or restore operation requires authentication and the realm in the challenge matches the stored realm, the phone uses the stored credentials to respond to the challenge without prompting the user. However, if the stored credentials are null, or if the realms do not match, or if an authentication attempt using the stored credentials fails, the Status Line of the9600 Series IP Deskphones or the Prompt Line for all other 9600 Series IP Deskphones displays an HTTP Authentication or an HTTP Authentication Failure interrupt screen:`Enter backup/restore credentials`.

If HTTP authentication for a backup or restore operation is successful and if the User ID, password or realm used differs from those currently stored in the phone, the new values replace the current values.

# About IPv4 and IPv6 operation

**Important:**

Avaya does not support IPv6 for the general market, and makes the software available to a specific set of customers with known limitations documented in the section Features not supporting IPv6 on page 75. Any additional limitation or bugs discovered within this release will be considered for resolution in future major releases.

From Release 6.0 onwards, Internet Protocol (IP) operation determination follows this order:

- If NVVPNMODE parameter value is set to 1 (Yes) only IPv4 operation is enabled.
- If NVVPNMODE is set to 0 (No), the IPv6 status IPV6STAT parameter is checked to see if IPv6 is allowed; if set to 0 (No) then only IPv4 operation is enabled.
- If IPV6STAT is set to 1 (support IPv6), then the DHCPSTAT parameter is checked:
  - If DHCPSTAT is set to 1 (use DHCPv4 only) then IPv4 only is enabled. But if an IPv6 address was manually programmed, dual-stack operation is enabled.
  - If DHCPSTAT is set to 2 (use DHCPv6 only) then IPv6 only is enabled. But if an IPv4 address was manually programmed, dual-stack operation is enabled.
  - If DHCPSTAT is set to 3 (both IPv4 and IPv6 supported), then dual-stack operation is enabled.

If IPv4-only operation is enabled, the system ignores any IPv6 addresses configured as parameter values and uses the next IPv4 address in the list. If the parameter value does not contain any IPv4 addresses, the system treats the value as null.

If IPv6-only operation is enabled, any IPv4 addresses configured as parameter values are ignored, and the next IPv6 address (if any) in a list of addresses is used. If the parameter value does not contain any IPv6 addresses, the system treats the value as null.

The results of the determination are expressed in table IP Enablement Results.

**Table 9: IP Enablement Results**

| Manually program-med IPv4 address? | IPV6STAT | Manually programmed IPv6 address | DHCPSTAT | Result | Addressing Mode(s) | |
|---|---|---|---|---|---|---|
| | | | | | IPv4 | IPv6 |
| No | 0 | N/A | n/a | IPv4 only | DHCP | n/a |
| | 1 | No<br>Yes | 1<br>2<br>3<br>1 or 3<br>2 | IPv4 only<br>IPv6 only<br>dual-stack<br>dual-stack<br>IPv6 only | DHCP<br>n/a<br>DHCP<br>DHCP<br>n/a | n/a<br>DHCPv6<br>DHCPv6<br>manual<br>manual |
| Yes | 0 | n/a | n/a | IPv4 only | manual | n/a |
| | 1 | No<br>Yes | 1<br>2 or 3<br>n/a | IPv4 only<br>dual-stack<br>dual-stack | manual<br>manual<br>manual | n/a<br>DHCPv6<br>manual |

In general, if dual-stack operation is enabled, whether IPv4 or IPv6 is to be used to contact a server is determined by the value of the parameter that contains the server address(es). However, if the value is a DNS name and if DNS returns both an IPv4 and an IPv6 address, the one that will be used is controlled by the parameter IPPREF.

# Features not supporting IPv6

The features and capabilities detailed in the following table are not available with IPv6 in H.323 software Release 6.0 or later:

**Table 10: Features not supporting IPv6**

| | | | |
|---|---|---|---|
| VPN [IPsec, IKEv1] | LLDP | RSVP [IPv4 audio connections only | RTP |
| RTCP Monitoring | CNA | HTTP Server Push Request | Certificates |

| | | | |
|---|---|---|---|
| Syslog | DHCP | Remote Trace Route, Remote Ping | Audio Push |
| SSH | SNMP | Dynamic VLAN | PTI |
| Many debugging and reporting capabilities available for IPv4 | DOS attack blocker | All secure protocols, including but not limited to https, secure BR, agent greetings | |

**Note:**

Avaya does not support IPv6 for the general market, and makes the software available to a specific set of customers with the understanding that IPv6 is undergoing further refinement. It is strongly recommended that customers planning to deploy IPv6 first thoroughly evaluate it in a test environment that mimics the target live environment. IPv6 environments requiring capabilities detailed in the table above are not supported with this release. Any additional limitation or bugs discovered within this release will be considered for resolution in future major releases.

# Chapter 7: Telephone Software and Application Files

## Understanding the general download process

The 9600 Series IP deskphones download upgrade files, settings files, language files, certificate files, and software files from a file server. 9600 Series IP deskphone downloads all of the file types either through HTTP or HTTPS except the software files, which can only be downloaded through HTTP. Avaya recommends HTTPS for downloading the non-software file types because it ensures the integrity of the downloaded file by preventing *man in the middle* attacks. Further, after the trusted certificates are downloaded into the deskphone, HTTPS ensures that the file server itself will be authenticated through a digital certificate. HTTPS is not used for software file downloads because 9600 Series IP deskphones software files are already digitally signed. You need not incur additional processing overhead while downloading these relatively large files.

**Note:**

The files in the Software Distribution Packages discussed in this chapter are identical for file servers running HTTP and HTTPS. The generic term “file server” refers to a server running either HTTP or HTTPS.

When shipped from the factory, 9600 Series IP deskphones might not contain the latest software. When 9600 Series IP deskphone is first plugged in, the phone attempts to contact a file server, and downloads new software only if the software version available on the file server is different than the version on the phone. For subsequent software upgrades, the call server provides the capability to remotely reset the phone, and the phone initiates the same process for contacting a file server.

The phone queries the file server, which, transmits a 96x1Supgrade.txt file (SIP protocol) or 96x1Hupgrade.txt file (H.323 protocol) to the deskphone based on the SIG parameter setting; software versions prior to Release 6.0 use a 96xxupgrade.txt file, which is not protocol-specific. The software files that the deskphone must use depend on the instructions in the upgrade file.

The 9600 Series IP deskphones then downloads a 46xxsettings.txt file. The settings file contains options that you have administered for any or all of the phones in your network. For more information about the settings file, see About the settings file on page 79. After

downloading the settings file, the phone downloads the language or certificate files required by the settings and then any new software files, if required.

**Related topics:**

Choosing the right application file and upgrade script file on page 78
Changing the Signaling Protocol on page 79
Using the upgrade file on page 79
About the settings file on page 79

# Choosing the right application file and upgrade script file

Software files needed to operate the 9600 Series IP deskphones are packaged together in either a Zip format or RPM/Tar format distribution package. Download the package appropriate to your operating environment to your file server from the Avaya support Web site at: http://www.avaya.com/support.

The choice of the package depends on the protocol you are using, H.323 or SIP, for all or the majority of your deskphones.

H.323 software distribution packages contain:

- One Upgrade file
- All of the Display Text Language Files
- A file named *av_prca_pem_2033.txt* that contains a copy of the Avaya Product Root Certificate Authority certificate in PEM format that may be downloaded to telephones based on the value of the TRUSTCERTS parameter
- A file named *release.xml* that is used by the Avaya Software Update Manager application

Release 6.0 and later software distribution packages in Zip format also contain a signatures directory containing signature files and a certificate file to be used by the Avaya file server application on the Utility server. Customers using a non-Avaya HTTP server can ignore or delete this directory.

For detailed information about downloading files and upgrading telephone software, see *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694* 16-300694 for all releases less than 6.0. For Release 6.1 and later covering the 9608, 9611G, 9621G, and 9641G deskphones, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*, 16-603603.

## Changing the Signaling Protocol

### About this task

Enterprises that require both H.323-based and SIP-based protocols can specify the protocol to be used by all or specific deskphones in the following two ways:

### Procedure

1. Set the SIG parameter in DHCP Option 242, the Site-Specific Option Number, or in the 46xxsettings.txt file for Release 6.0 and later.

   This setting applies to all telephones except the telephones for which SIG was manually configured to a value of H.323 or SIP using the SIG Craft procedure.
2. Set the SIG parameter on a per-phone basis using the SIG Craft procedure. For more information, see *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694* for all releases other than Release 6.0. For Release 6.0 covering the 9608, 9611G, 9621G, and 9641G deskphones, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*, 16-603603.

## Using the upgrade file

The upgrade file indicates to the phone whether it needs to upgrade software. From Release 6.0 onwards, the upgrade file is either H.323-specific or SIP-specific. The deskphones read this file whenever the deskphone is reset. The upgrade script file also directs the phone to the settings file.

Avaya recommends that you do not alter the upgrade script file because if Avaya changes the upgrade script file in the future, any changes you have made will be lost. Avaya recommends that you use the 46xxsettings.txt file to customize your settings instead. However, you can change the settings file name, if desired, as long as you also edit the corresponding **GET** command in the upgrade script file.

## About the settings file

The settings file contains the option settings you need to customize the Avaya IP deskphones for your enterprise.

**Note:**

You can use one settings file for all your Avaya IP deskphones. The settings file includes the 9600 Series IP deskphones covered in this document and 4600 Series IP deskphones.

For more information, see *4600 Series IP Telephone LAN Administrator Guide*, 555-233-507.

The settings file can include any of six types of statements, one on each line:

- Tag lines that begin with a single # (pound) character, followed by a single space character, followed by a text string with no spaces.
- **Goto** commands, of the form `GOTO tag`. **Goto** commands cause the phone to continue interpreting the settings file at the next line after a `#tag` statement. If no such statement exists, the rest of the settings file is ignored.
- Conditionals, of the form `IF $parameter_name SEQ string GOTO tag`. Conditionals cause the **Goto** command to be processed if the value of the parameter named *parameter_name*exactly matches *string*. If no such parameter named *parameter_name* exists, the entire conditional is ignored. You can use only the following parameters in a conditional statement are: GROUP, MACADDR, MODEL and MODEL4. In pre-6.0 software releases, you could use BOOTNAME and SIG. In software release 3.1 and later, you can use VPNACTIVE . In software release 6.0 and later, you can use SIG_IN_USE.
- **SET** commands, of the form `SET parameter_name value`. Invalid values cause the specified value to be ignored for the associated *parameter_name* so the default or previously administered value is retained. All values must be text strings, even if the value itself is numeric, a dotted decimal IP Address, etc.
- Comments, which are statements with a pound (#) character in the first column.

**Note:**

Enclose all data in quotation marks for proper interpretation.

- GET commands, of the form `GET filename`. The phone attempts to download the file named by *filename*, and if the file is successfully downloaded, the downloaded file is interpreted as an additional settings file, and no additional lines are interpreted in the original file. If the file cannot be obtained, the phone continues to interpret the original file.

Download the 46xxsettings.txt template file from the Avaya Support site and edit it to add your own custom settings.

For more information on parameters and valid values, see 9600 Series H.323 customizable system parameters on page 84 .You need only specify settings that vary from defaults, although specifying defaults is harmless.

# Using the GROUP parameter to set up customized groups

### About this task

Different users might have the same phone model but require different administered settings. For example, you might want to restrict Call Center agents from logging off, which might be an essential capability for *hot-desking* associates.

Use the GROUP parameter to set up customized groups:

### Procedure

1. Identify the phones that are associated with which group, and designate a number for each group.

   The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group is assigned as Group 0.

2. The GROUP parameter can only be set either at each individual deskphone or when a you register a phone with Software Release 1.5 or greater to an Avaya Communication Manager server with CM Release 4.0 or greater.

   To set the GROUP parameter on each individual deskphone, use the GROUP Craft (local administrative) procedure. See *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*. To set the GROUP parameter on a phone registered with Communication Manager, administer GROUP on a phone-by-phone basis on the Communication Manager Station Form.

3. After you assign the GROUP assignments, edit the configuration file to allow each phone of the appropriate group to download its proper settings.

### Result

The following is an example of the configuration file for the Call Center agent:

**`IF $GROUP SEQ 1 goto CALLCENTER IF $GROUP SEQ 2 goto HOTDESK`** , {specify settings unique to Group 0} **`goto END`**

**`# CALLCENTER`** {specify settings unique to Group 1} **`goto END`**

**`# HOTDESK`** {specify settings unique to Group 2}

**`# END`** {specify settings common to all Groups}

# Chapter 8: Administering Deskphone Options

## Administering options for 9600 Series H.323 Deskphones

This chapter explains how to change parameter values by using the DHCP or HTTP servers and provides additional information about some related features. For information on the parameter names, values, valid range of the values, and a description of each value, see9600 Series H.323 customizable system parameters on page 84

You can set the parameters for DHCP, DHCP fields and options to the required values. For more information, see Administering the DHCP and File Servers on page 63. For HTTP, the parameters are set to required values in the settings file. For more information, see About the settings file on page 79.

Use the settings file to administer most parameters on the 9600 Series H.323 Deskphones. Some DHCP applications are complicated and require extensive expertise for administration.

You might choose to completely disable the capability to enter or change option settings from the dial pad. You can set the parameter PROCPSWD as part of standard DHCP/HTTP administration. Alternately, you can set PROCPSWD on the system-parameters ip-options form, in Communication Manager Release 4.0. If PROCPSWD is non-null and consists of 1 to 7 digits, a user cannot invoke any local options without first entering the PROCPSWD value on the Craft Access Code Entry screen.

For more information on craft options, see the *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*.

**Note:**

If you configure the minimum length of the password as four digits, the password will be changed to default

**Caution:**

If you administer PROCPSWD as part of DHCP/HTTP administration, the value is stored and transmitted unencrypted. Therefore, PROCPSWD is not a high-security technique to inhibit a sophisticated user from obtaining access to local procedures unless you administer

the parameter using page 3 of the system-parameters IP-options form in Avaya Communication Manager Release 4.0.

If you administer this password, you cannot gain access to all local procedures, including VIEW. VIEW is a read-only Craft option, using which you can review the current phone settings.

**Note:**

For information on the system parameters related to Virtual Private Network (VPN) setup and maintenance, see *VPN Setup Guide for 9600 Series IP Telephones*, 16-602968.

The following table lists the parameters that are described in that document:

| | | |
|---|---|---|
| ALWCLRNOTIFY | NORTELAUTH | NVIKECONFIGMODE |
| NVIKEDHGRP | NVIKEID | NVIKEIDTYPE |
| NVIKEOVERTCP | NVIKEP1AUTHALG | NVIKEP1LIFESEC |
| NVIKEP2AUTHALG | NVIKEP2ENCALG | NVIKEP2LIFESEC |
| NVIKEPSK | NVIKEXCHGMODE | NVIPSECSUBNET |
| NVPFSDHGRP | NVSGIP | NVVPNAUTHTYPE |
| NVVPNCFGPROF | NVVPNCOPYTOS | NVVPNENCAPS |
| NVVPNMODE | NVVPNPSWD | NVVPNPSWDTYPE |
| NVVPNSVENDOR | NVVPNUSER | NVVPNUSERTYPE |
| NVXAUTH | VPNACTIVE | VPNCODE |
| VPNPROC | VPNTTS | |

**Important:**

Some parameters in the table are IPv6-specific.

Avaya does not support IPv6 for the general market, and makes the software available to a specific set of customers with known limitations documented in the section Features not supporting IPv6 on page 75. Any additional limitation or bugs discovered within this release will be considered for resolution in future major releases.

# 9600 Series H.323 customizable system parameters

This table lists the parameters that you can customize in the 46xxsettings file, their default values, parameter descriptions, and valid values.

| Parameter name | Default value | Description and value range |
|---|---|---|
| ADMIN_HSEQUAL | 1 | Handset Equalization alternative permission flag. Valid values are:<br>1 = Use handset equalization that is optimized for acoustic TIA 810/920 performance.<br>2 = Use handset equalization that is optimized for electrical FCC Part 68 HAC telecoil performance. |
| AGCHAND | 1 | Automatic Gain Control status for handset, 0=disabled, 1=enabled. |
| AGCHEAD | 1 | Automatic Gain Control status for headset, 0=disabled, 1=enabled. |
| AGCSPKR | 1 | Automatic Gain Control status for Speaker, 0=disabled, 1=enabled. |
| AGTACTIVESK | 0 | Used to control the softkeys that are available to the agent on the deskphone.<br>If value = 0, Transfer softkey is available on the second row of softkeys, and Release on the first row.<br>If value = 1, Release softkey is available on second row of softkeys, and Transfer on the first row.<br>If value = 2, softkeys available only for Hold, Conference, and Transfer. |
| AGTCALLINFOSTAT | 1 | For Avaya Call Center use only.<br>Automatically invokes Call-info permission when the caller-information button, (buttonType = 141), is administered on the deskphone and AGTCALLINFOSTAT has a value of 1. The deskphone transmits a virtual press of that button to the call server.<br>The call server is expected to respond with a call-associated display message with possible content in Line 2. The Line 2 content, if any, is checked by the call server to see if it contains any strings specified by GREETINGDATAx when the corresponding GREETINGTYPEx begins with *4*. The first such greeting with a match as specified in the Match Criteria is played. 1 ASCII numeric digit. Valid values are: 1 = Invoke the caller information permission to locate a greeting. 0 = Do not automatically invoke Call-info permission. |
| AGTFWDBTNSTAT | 1 | For Avaya Call Center use only. Disables the Forward button permission flag. When the |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | CALLCTRSTAT parameter has a value of 1 and AGTFWDBTNSTAT has a value of *1* and the deskphone has an application button labeled Forward, the deskphone generates an error beep and performs no forwarding action when the **Forward** button is pressed. 1 ASCII numeric digit. Valid values are: 1 = Disable the Forward button. 0 = Do not disable the Forward button. |
| AGTGREETINGSTAT | 1 | For Avaya Call Center use only. Indicates agent Greeting permission and determines whether the deskphone displays the Greeting softkey when the deskphone receives an incoming call. 1 ASCII numeric digit. Valid values are: 1 = Display the Greeting softkey upon alerting. 0 = Do not display the Greeting softkey upon alerting. |
| AGTVUSTATID<br>**Note:**<br>AGTVUSTATID was previously known as AGTIDVUSTAT. | 0 | For Avaya Call Center user only. Specifies the VuStats format number for deriving call center Agent ID. Valid values are 1 or 2 ASCII numeric digits, 0 through 50. |
| AGTLOGINFAC | #94 | For Avaya Call Center use only. Indicates the Feature Access Code agents use to sign in to the call center. Valid values are 1 to 4 ASCII dialable characters 0 through 9 plus star (*) and pound (#). |
| AGTLOGOUTFAC | #95 | For Avaya Call Center use only. Specifies the Feature Access Code agents use to log out. Valid values are 1 to 4 dialable characters 0 through 9 plus star (*) and pound (#) |
| AGTSPKRSTAT | 1 | For Avaya Call Center use only. Disables or enables the speakerphone permission flag. 1 ASCII numeric digit. Valid values are: 0 = Normal speaker operation; agent can activate or deactivate the Speakerphone. 1 = Speaker is disabled; agent cannot activate or deactivate the Speakerphone provided CALLCTRSTAT=1 & non-null Agent ID. 2 = If the deskphone is a 9641G, and other conditions are met (CALLCTRSTAT=1 & Release button is administered & non-null Agent ID), then the Speaker button acts as a Release button. 2 = If the deskphone is NOT a 9641G, and if (CALLCTRSTAT=1 & non-null Agent ID), then the Speaker button is disabled. 3 = If |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | (CALLCTRSTAT=1 & Release button is administered & non-null Agent ID), then the Speaker button acts as a Release button. 4 = If the Release button is administered, then the Speaker button acts as a Release button irrespective of whether the Agent is logged in or not. 4= |
| AGTTIMESTAT | 1 | For Avaya Call Center use only. Suppresses the date/time permission flag and display on the Title line. 1 ASCII numeric digit. Valid values are: 1 = Do not display date and time on the top display line. 0 = Display the date and time on the top display line. |
| AGTTRANSLTO | to | For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters AGTTRANSLCLBK, AGTTRANSLPRI, AGTTRANSLPK, and AGTTRANSLICOM to parse a call-associated display message when a call appearance is in the Alerting call state. Tthe Agent Information line displays the result and provides information about the incoming call. 1 to 6 UTF-8 characters. |
| AGTTRANSCLBK | callback | For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters AGTTRANSLTO, AGTTRANSLPRI, AGTTRANSLPK, and AGTTRANSLICOM to parse a call-associated display message when a call appearance is in the Alerting call state. The result displays on the Agent Information line and provides information about the incoming call. 1 to 6 UTF-8 characters. |
| AGTTRANSLPRI | priority | For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters AGTTRANSLTO, AGTTRANSLCLBK, AGTTRANSLPK, and AGTTRANSLICOM to parse a call-associated display message when a call appearance is in the Alerting call state. The result displays on the Agent Information line and provides information about the incoming call. 1 to 6 UTF-8 characters. |
| AGTTRANSLPK | park | For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters AGTTRANSLTO, |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | AGTTRANSLCLBK, AGTTRANSLPRI, and AGTTRANSLICOM to parse a call-associated display message when a call appearance is in the Alerting call state. The result displays on the Agent Information line and provides information about the incoming call. 1 to 6 UTF-8 characters. |
| AGTTRANSLICOM | ICOM | For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters AGTTRANSLTO, AGTTRANSLCLBK, AGTTRANSLPRI, and AGTTRANSLPK to parse a call-associated display message when a call appearance is in the Alerting call state. The result displays on the Agent Information line and provides information about the incoming call. 1 to 6 UTF-8 characters. |
| AMADMIN | “ ” (Null) | WML-Application URI. The URI used to obtain the AvayaMenuAdmin.txt file for WML-applications under the A (AVAYA) Menu. Specify the HTTP server and directory path to the administration file. Do not specify the administration file name. For more information, see Administering the Avaya A Menu on page 168. |
| APPNAME | “ ” (Null) | The file name of the Signed Application or Library Software Package that the deskphone downloads and installs during power-up or reset if it has not already been downloaded and installed. You should set this parameter only in an upgrade file. |
| APPSTAT | 1 | Controls whether specific applications are enabled, restricted, or disabled. Values are: 1=all applications enabled, 2=Speed Dial (Contacts) changes and Call Log disabled and Redial last number only, 3=Speed Dial (Contacts) changes disabled, 0=Speed Dial (Contacts) changes, Call Log, and Redial disabled. |
| APPLICATIONWD | 1 | Controls whether the application watchdog is enabled 1 or disabled 0. The application watchdog is a software process that, if enabled, monitors other software processes to determine whether the processes have become unresponsive, at which point it generates a log event and either kills the process or resets the deskphone. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| AUDASYS | 3 | Globally controls audible alerting. Possible system settings for audible alerting are 0 through 3 as follows: 0=Audible Alerting is Off; user cannot change this setting. 1=Audible Alerting is On; user cannot change this setting. 2=Audible Alerting is Off; user can change this setting. 3=Audible Alerting is On; user can change this setting. |
| AUDIOENV | 0 | Audio environment selection index. Valid values are 0 through 299. Note that pre-Release 2.0 software has different valid ranges. |
| AUDIOSTHD | 0 | Headset sidetone setting. Valid values for applicable sidetone masking ratings (STMR) are:<br>0= nominal STMR, no change to sidetone level.<br>1= nominal +9 STMR, three steps softer than nominal.<br>2= nominal +21 STMR (off), no sidetone (inaudible).<br>3= nominal +3 STMR, one level softer than nominal.<br>4= nominal +6 STMR, two steps softer than nominal.<br>5= nominal +12 STMR, four steps softer than nominal.<br>6= nominal +15 STMR, five steps softer than nominal.<br>7= nominal +18 STMR, six steps softer than nominal.<br>8= nominal -3 STMR, one step louder than nominal.<br>9= nominal -6 STMR, two steps louder than nominal.<br>Pre-Release 6.2 software has different valid ranges.<br>For more information on fine-tuning your IP phones, see *Audio Quality Tuning for IP Telephones*,100054528 on the Avaya Support site at www.avaya.com/support. |
| AUDIOSTHS | 0 | Handset sidetone setting. Valid values are:<br>0=nominal STMR, no change to sidetone level.<br>1= nominal +9 STMR, three steps softer than nominal.<br>2= nominal +21 STMR (off), no sidetone (inaudible).<br>3= nominal +3 STMR, one level softer than nominal. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | 4= nominal +6 STMR, two steps softer than nominal.<br>5= nominal +12 STMR, four steps softer than nominal.<br>6= nominal +15 STMR, five steps softer than nominal.<br>7= nominal +18 STMR, six steps softer than nominal.<br>8= nominal -3 STMR, one step louder than nominal.<br>9= nominal -6 STMR, two steps louder than nominal.<br>Pre-Release 6.2 software has different valid ranges.<br>For more information on fine-tuning your IP phones, see *Audio Quality Tuning for IP Telephones*, 100054528 on the Avaya Support site at www.avaya.com/support. |
| AUTH | 0 | Script file authentication value (0=HTTP is acceptable, 1=HTTPS is required). |
| BAKLIGHTOFF | 120 | Number of minutes without display activity to wait before setting the backlight to its lowest level. The default is 120 minutes (2 hours). Valid values range from zero to 999 minutes (16.65 hours). |
| BLUETOOTHSTAT | 1 | Bluetooth permission flag. 0=Bluetooth is disabled, 1= Bluetooth is enabled.<br>When Bluetooth is disabled through BLUETOOTHSTAT, the user cannot override this setting locally on the deskphone. |
| BRAUTH | 0 | Backup/restore authentication control. Valid values are:<br>1=If at least one digital certificate is downloaded based on TRUSTCERTS. The IP address of the call server with which the deskphone is registered and the registration password of the deskphone are included as the credentials in an Authorization request-header in each transmitted GET and PUT method if and only if the value of BRAUTH is 1.<br>0=The IP address of the call server and registration password of the deskphone is not included as part of GET or PUT Authorization header, or no digital certificate has been downloaded. |
| BRURI | “ ” (Null) | URL used for backup and retrieval of user data. Specify HTTP or HTTPS server and directory path |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | and/or port number to backup file. Do not specify backup file name. Value: 0-255 ASCII characters. Null is a valid value and you can enter spaces. A subdirectory can be specified, for example: `SET BRURI http://135.8.60.10/backup` This parameter puts the user backup or restore files in a subdirectory away from all other files such as bins, .txts, and others. This parameter turns on authentication for that subdirectory, without turning it on for the root directory. If this value is null or begins with a character sequence other than *http://* or *https://* the Backup or Restore option will not display to the deskphone user. |
| CALCSTAT | 1 | Applies only to deskphones running software Release 6.0 and later. Specifies whether the Calculator application must be displayed or enabled. Valid values are: 1=Yes, enable the Calculator application, 0=No, disable the Calculator application. |
| CALLCTRSTAT | 0 | Applicable only to Call Centers. Call Center functionality flag. 1 ASCII numeric digit. Valid values are: 0 = Call Center functionality does not apply; do not provide access to call center options/functions. 1 = Call Center functionality applies; allow agent access to call center functions like greetings and data backup. |
| CCLOGOUTIDLESTAT | 0 | Specifies whether an agent logging out of a call center will set the Headset LED and audio path to Off, or will leave the Headset LED and audio path On. Valid values are: =0, the deskphone automatically turns the headset LED Off and considers the audio and call states to be Idle. =1, the deskphone does not turn the headset LED Off (if it is On) but still considers the audio and call states to be Idle. If the user is on a call at logout, the deskphone waits for the Disconnect message from the far end. **Note:** When CCLOGOUTIDLESTAT=1, the agent must answer the first call after reboot manually. After the first call the phone returns to headset off-hook idle state. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| CLDELCALLBK | 0 | Call Log Delete Callback Flag. Deletes calls from the Missed Call Log when the user returns the call from the Call Log. Values are 1=No, 0=Yes. |
| CLDISPCONTENT | 1 | Applies only to deskphones running software Release 6.0 and later. Call Log Display Content control; indicates whether call History list includes the caller's number or not. Valid values are: 1=Display caller name but not number. 0=Display both caller name and number. |
| CNAPORT | 50002 | Avaya Converged Network Analyzer (CNA) server registration transport-layer port number (0-65535). Applies to IPv4 only.<br>This parameter is not supported in Release 6.2 and later. |
| CNASRVR | " " (Null) | Text string containing the IP addresses of one or more Avaya Converged Network Analyzer (CNA) servers to be used for registration; applies to IPv4 only. Format is dotted decimal or DNS format, separated by commas, with no spaces Zero to 255 ASCII characters, including commas.<br>This parameter is not supported in Release 6.2 and later. |
| DEFAULTRING | 9 | DEFAULTRING specifies the default ring tone. Valid values are 1 through 14. |
| DHCPPREF | 6 | Applies only to deskphones running software Release 6.0 and later. Specifies whether new values received via DHCPv4 or DHCPv6 are preferred when both are used. Valid values are: 4=DHCPv4 is preferred.<br>6= DHCPv6 is preferred. |
| DHCPSRVR | " " (Null) | Specifies DHCP server address(es). Format is dotted decimal or DNS format, separated by commas, with no spaces. Zero to 255 ACSII characters, including commas. |
| DHCPSTD | 0 | DHCP Standard lease violation flag. Indicates whether to keep the IP address if there is no response to lease renewal. If set to 1, (No) the deskphone strictly follows the DHCP standard with respect to giving up IP addresses when the DHCP lease expires. If set to 0,(Yes) the deskphone continues using the IP address until it detects reset or a conflict. For more information, see DHCP Generic Setup on page 67. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| DIALFEATURES | “ ” (Null) | A list of feature number identifiers for softkey features available in the Dialing call state, for example, Redial. Zero to 255 ASCII characters consisting of zero to five whole numbers separated by commas without any spaces. For more information, see Administering features on softkeys on page 137. |
| DNSSRVR | 0.0.0.0 | Text string containing the IP address of zero or more DNS servers, in dotted-decimal format, separated by commas with no intervening spaces, 0-255 ASCII characters, including commas. |
| DOMAIN | “ ” (Null) | Text string containing the domain name to be used when DNS names in parameter values are resolved into IP addresses. Valid values are 0-255 ASCII characters. If Null, do not leave spaces. |
| DOT1X | 0 | 802.1X Supplicant operation mode. Valid values are: 0= With PAE pass-through, 1= with PAE pass-through and proxy Logoff, 2=without PAE pass-through or proxy Logoff. For more information, see About IEEE 802.1X on page 121. |
| DOT1XEAPS | MD5 | Specifies the EAP method used for 802.1X operation. Valid values are *MD5* and *TLS* . |
| DOT1XSTAT | 0 | Determines how the deskphone handles Supplicants. Valid values are: 0= Supplicant operation is completely disabled. 1=Supplicant operation is enabled, but responds only to received unicast EAPOL messages. 2 = Supplicant operation is enabled and responds to received unicast and multicast EAPOL messages. For more information, see About IEEE 802.1X on page 121. |
| DOT1XWAIT | 0 | Specifies whether the telephone will wait for 802.1X authentication to complete before initiating DHCP<br>Valid values, 0 and 1<br>If DOT1XWAIT = "0" when the 802.1X Supplicant is started, startup will continue without waiting for 802.1X authentication to complete, =1 Startup will not continue., |
| DROPCLEAR | 1 | VPN only. Specifies how clear IPsec packets are processed. One ASCII numeric digit. Valid values |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | are: 0= all other packets will be processed, but not by IPsec, or 1=all other packets will be discarded. |
| ENHDIALSTAT | 1 | Enhanced Dialing Status. If set to 1, the Administering dialing methods feature is turned on for all associated applications. For more information, see Administering dialing methods on page 131. If set to 0, the feature is turned off. |
| FBONCASCREEN | 0 | For the 9630, 9630G, 9640, and 9640G IP deskphones, indicates whether to display feature buttons on available lines on the Call Appearance on the Phone screen. Values are: 1=Yes; 0=No. |
| GRATARP | 0 | Gratuitous ARP flag. Controls whether the deskphone processes gratuitous ARPS or ignores them.<br>If you use Processor Ethernet (PE) duplication and if your phones are on the same subnet as the PE interfaces, set this parameter to 1, to allow the fastest failover to the new PE interface.<br>Valid values are:<br>1 = Yes, process gratuitous ARPS<br>0 = No, ignore gratuitous ARPS |
| GRATNAV6 | 0 | Applies only to deskphones running software Release 6.0 and later. Specifies whether the call server will process gratuitous and unsolicited IPv6 Neighbor Advertisement messages. A received message is considered unsolicited if the deskphone did not send a corresponding Neighbor Solicitation message first; it is not determined by the value of the Solicited flag in the received message. An IPv6 unsolicited Neighbor Advertisement message is similar to a gratuitous ARP message in IPv4. |
| GUESTDURATION | 2 | Guest login duration in hours. One or two ASCII numeric digits. Valid values are 1, through 12. |
| GUESTLOGINSTAT | 0 | Guest login permission flag. If set to 1, the Guest Login option is listed on the Avaya Menu; if set to 0, the Guest Login option is not available. |
| GUESTWARNING | 5 | Guest login warning in minutes to indicate when to notify the user that *GUESTLOGINDURATION* will expire. One or two ASCII numeric digits. Valid values are 1 through 15. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| HEADSYS | 0 if CALLCTRSTAT =0, else 1 | Headset operational mode. Specifies whether the deskphone will go on-hook if the headset is active when a Disconnect message is received. One ASCII numeric digit. Valid values are:<br>0 or 2 = The deskphone will go on-hook if a Disconnect message is received when the headset is active.<br>1 or 3 = Enabled, Disconnect messages are ignored when the headset is active. |
| HEADSETBIDIR | 0 | Specifies the permission flag for enabling or disabling the Headset Bi-directional functionality. Valid values are:<br>0= Default, Bi-directional functionality disabled, 1= Switchhook and Alerting, 2= Switchhook only. |
| HOMEIDLETIME | 10 | For touchscreen deskphones only, the number of minutes after which the Home screen will be displayed. Value is 1 or 2 ASCII numeric digits, 0 through 30. If you prefer an idle Web page as the display instead of the Home screen, set this value to less than the WMLIDLETIME value. |
| HTTPDIR | “ ” (Null) | HTTP server directory path. The path name prepended to all file names used in HTTP *GET* operations during initialization. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required. The command syntax is *SET HTTPDIR myhttpdir*” where *myhttpdir* is your HTTP server path. HTTPDIR is the path for all HTTP operations except for BRURI. |
| HTTPPORT | 80 | TCP port number used for HTTP file downloading. 2 to 5 ASCII numeric digits. Valid values are 80 through 65535. Note that when the file server is on Communication Manager, set this value to 81 that is the port required for HTTP downloads rather than the using the default. |
| HTTPSRVR | “ ” (Null) | IP address(es) or DNS Name(s) of HTTP file servers used to download deskphone files. Dotted decimal or DNS format, separated by commas,0-255 ASCII characters, including commas. |
| ICMPDU | 0 | Controls whether ICMP Destination Unreachable messages will be processed. Values are: 0=No, 1=Send limited Port Unreachable messages, |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | 2=Send Protocol and Port Unreachable messages. |
| ICMPRED | 0 | Controls whether ICMP Redirect messages will be processed. Values are: 0=No, 1=Yes. |
| IDLEFEATURES | “ ” (Null) | A list of feature number identifiers for softkey features potentially available in the Idle call state, for example, Redial. Zero to 255 ASCII characters consisting of zero to six whole numbers separated by commas without any intervening spaces. For more information, see Administering features on softkeys on page 137. |
| IPPREF | 6 | Applies only to deskphones running software Release 6.0 and later. Specifies which type of IP address (IPv4 or IPv6) will be tried first if DNS returns both types. Valid values are: 4= Try IPv4 addresses first over DHCPv6 if DNS returns both types. 6= Try IPv6 addresses first over DHCPv4 if DNS returns both types |
| IPV6STAT | 0 | Applies only to deskphones running software Release 6.0 and later. Specifies whether IPv6 will be enabled. Valid values are: 0 = IPv6 is disabled. 1 = IPv6 is supported/enabled.<br>**Note:**<br>Avaya does not support IPv6 for the general market, and makes the software available to a specific set of customers with known limitations documented in the section Features not supporting IPv6 on page 75. Any additional limitation or bugs discovered within this release will be considered for resolution in future major releases. |
| L2Q | 0 | Controls whether Layer 2 frames have IEEE 802.1Q tags (0=auto, 1=enabled, 2=disabled). |
| L2QVLAN | 0 | 802.1Q VLAN Identifier (0 to 4094). Null (“ ”) is not a valid value and the value cannot contain spaces. VLAN identifier that IP deskphones use. Set this parameter only if IP deskphones use a VLAN that is separate from the default data VLAN.<br>If you must configure the VLAN identifier using H.323 signaling based on Communication Manager administration forms, the VLAN should not be set here. From software Release 2.0, |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | L2QVLAN will always be initialized from the corresponding system initialization value at power-up, but will not be initialized from the system initialization value after a reset. |
| LANG0STAT | 1 | Controls whether the built-in English language text strings can be selected by the user. Valid values are: 0 = User cannot select English language text strings<br>1 = User can select English language text strings.<br>SET LANG0STAT 1 |
| LANGxFILE | “ ” (Null) | Contains the name of the language file *x*, where *x* is 1 through 4. The file name must end in .txt. Example: SET LANG1FILE “`mlf_russian.txt`”<br>LANG1FILE =<br>LANG2FILE =<br>LANG3FILE =<br>LANG4FILE = |
| LANGLARGEFONT | “ ” (Null) | Larger text font file name. A string of up to 32 characters specifies the loadable language file on the HTTP server for the Large Text font. |
| LANGSYS | “ ” (Null) | System-wide language that contains the name of the default system language file, if any. Value is 0 to 32 ASCII characters. The file name must end in .txt. The default is a null string. Example: SET LANGSYS `mlf_german.txt` |
| LEDMODE | 0 | Supports new LED behavior Valid values 0= Old behavior, and would mean that the red led is controlled locally by the phone, 1=New behavior and would mean the buttons red LEDs are controlled by CM .<br>Example: If new behavior is activated, Button module and phone LEDs are aligned and will change according to call state. |
| LLDP_XMIT_SECS | 30 | Specifies the rate in seconds at which LLDP messages will be transmitted.<br>Valid values are 1 to 4 ASCII numeric digits, “1” through “3600”<br>Main usage is for the SSO application to discover the phone faster. |
| LOCALZIPTONEATT | 35 | Controls the local phone ziptone volume when AUTOANSSTAT= 1 Note: If Auto answer is configured on the CM and not using the |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | AUTOANSSTAT setting, this parameter does not influence that zip tone volume.<br>Valid values: 0-95 where 0= Loudest and 95= Lowest |
| LOGBACKUP | 1 | Indicates whether the call log of the user should be backed up. Values are: 1=Yes. The Call Log is backed up to the same backup file as all other user data subject to normal administration of that file. 0=No. |
| LOGLOCAL | 0 | Event Log Severity Level. Valid values are one 0-8 ASCII numeric digit. Controls the level of events logged in the endptRecentLog and endptResetLog objects in the SNMP MIB. Events with the selected level and with a higher severity level are logged. Valid values are: 0=Disabled, 1=emergencies, 2=alerts, 3=critical, 4=errors, 5=warnings, 6=notices, 7=information, 8=debug. |
| LOGMISSEDONCE | 0 | Indicates that only one Call Log entry for multiple Missed calls from the same originating phone number must be maintained. Values are: 1=Yes; each Missed Call Log entry is maintained, along with a Missed Call counter that tracks the number of times (up to 99) the originating number called. 0=No; each Missed Call creates a new Call Log entry. |
| LOGSRVR | “ ” (Null) | Syslog Server IP address. Zero or one IP address in dotted-decimal, colon-hex, or DNS Name format (0-15 ASCII characters). |
| LOGUNSEEN | 0 | Indicates that a Call Log entry should be maintained for calls that are redirected from the deskphone, for example, Call forwarded calls. Values are: 1=Yes; 0=No. CM 5.2 or later is required for this feature to work. |
| LOGTOFILE | 0 | Specifies whether optional debug printf strings will be logged to an internal file.<br>If LOGTOFILE=1, optional debug printf strings are logged to an internal file, =0 not logged. |
| MCIPADD | 0.0.0.0 | Call Server address. Zero or more Avaya Communication Manager server IP addresses. Format is dotted-decimal or DNS name format, separated by commas without intervening spaces (0-255 ASCII characters, including commas). Null is a valid value. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| MSGNUM | “ ” (Null) | Voice mail system deskphone or extension number. Specifies the number to be dialed automatically when the deskphone user presses the **Message** button. MSGNUM is only used when the phone is aliased using non-native support. Messaging must be configured for native support. Value: 0-30 ASCII dialable characters are 0 through 9, star (*) and pound (#) and no spaces. Null is a valid value. |
| MYCERTCAID | “CAIdentifier ” | Certificate Authority Identifier to be used in a certificate request. 0 to 255 ASCII characters. |
| MYCERTCN | “$SERIALNO” | Common Name of the Subject of a certificate request. 0 to 255 ASCII characters that contain the string *$SERIALNO* or *$MACADDR*. |
| MYCERTDN | “ ” (Null) | Additional information for the Subject of a certificate request. 0 to 255 ASCII characters |
| MYCERTKEYLEN | 1024 | Bit length of the private key to be generated for a certificate request. 4 ASCII numeric digits, 1024 through 2048. |
| MYCERTRENEW | 90 | Percentage of a certificate's Validity interval after which renewal procedures will be initiated. 1 or 2 ASCII numeric digits, 1 through 99. |
| MYCERTURL | “ ” (Null) | URL to be used to contact an SCEP server. Zero to 255 ASCII characters, zero or one URL. |
| MYCERTWAIT | 1 | Specifies whether the deskphone will wait until a pending certificate request is complete, or whether it will periodically check in the background. 1 ASCII numeric digit, 0 or 1 as follows:<br>1 = If a connection to the SCEP server is successfully established, SCEP will remain in progress until the request for a certificate is granted or rejected.<br>0 = SCEP will remain in progress until the request for a certificate is granted or rejected or until a response is received indicating that the request is pending for manual approval. |
| NDREDV6 | 0 | Applies only to deskphones running software Release 6.0 and later. Controls whether IPv6 Neighbor Discovery Redirect messages will be processed. Valid values are: 0= Ignore received Redirect messages. 1= Process received Redirect messages. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| NVHTTPSRVR | “ ” (Null) | Applies to both VPN and non-VPN settings. NVHTTPSRVR is the HTTP file server IP addresses used to initialize HTTPSRVR the next time the phone starts up. Zero to 255 ASCII characters: zero or more IP addresses in dotted decimal, colon-hex, or DNS name format, separated by commas without any intervening spaces.<br>NVHTTPSRVR is provided for VPN mode so that a file server IP address can be pre configured and saved in non-volatile memory. For more information, see *VPN Setup Guide for 9600 Series IP Telephones* ,16-602968. |
| NVMCIPADD | “ ” (Null) | Call server IP addresses. Zero to 255 ASCII characters; zero or more IP addresses in dotted-decimal, colon-hex, or DNS name format, separated by commas without any intervening spaces. |
| NVTLSSRVR | “ ” (Null) | VPN and non-VPN. HTTPS file server IP addresses used to initialize TLSSRVR the next time the phone starts up. 0 to 255 ASCII characters: zero or more IP addresses in dotted decimal, colon-hex, or DNS name format, separated by commas without any intervening spaces. For more information, see *VPN Setup Guide for 9600 Series IP Telephones* ,16-602968. |
| OPSTAT | 111 | Option status flag(s) (1 or 3 ASCII numeric digits) indicate which options are user-selectable. The default of 111 grants access to all options and related applications. Single digit valid values are: 1=user can access all options, including Logout, 2= user can access only view-oriented applications. Three-digit valid values are a concatenation of binary values, in the form *abc*, where each letter represents a 0 (disabled/off) or 1 (enabled/on), interpreted as: *a* = base settings for all user options and related applications, except as in *b* or *c*. *b* = setting for view-oriented applications (for example, the Network Information application), as applicable. *c* = setting for Logout application, if applicable. The binary 0 does not allow an end user to see or invoke options and related applications. Setting the flag to binary 1 gives full display and access to all options and related applications. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| OPSTAT2 | 0 | OPSTAT override flag. If set to 0, OPSTAT is not affected. If set to 1, OPSTAT is unaffected with the exception that any changes to customized labels in the backup file are uploaded and used as if OPSTAT permitted this action. |
| OPSTATCC | 0 | Specifies whether Call Center options such as Greetings will be presented to the user even if the value of OPSTAT is set to disable user options. Note that the value of CALLCTRSTAT must be 1 for OPSTATCC to be used.<br>0 = Call Center options will be displayed based on the value of OPSTAT (default).<br>1 = Call Center options will be displayed based on the value of OPSTATCC. |
| PHNCC | 1 | Telephone country code. The administered international country code for the location by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1-3 digits, from 1 to 999. |
| PHNDPLENGTH | 5 | Internal extension deskphone number length. Specifies the number of digits associated with internal extension numbers by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from 3 to 13. |
| PHNEMERGNUM | “ ” (Null) | Emergency deskphone/extension number. Specifies the number to be dialed automatically when the deskphone user presses the **Emerg** button.<br>Value: 0-30 ASCII dialable characters from 0 through 9, star (*), pound (#) and no spaces. Null is a valid value. |
| PHNIC | 011 | Telephone international access code. The maximum number of digits, if any, dialed to access public network international trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-4 digits. |
| PHNLD | 1 | Telephone long distance access code. The digit, if any, dialed to access public network long distance trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 digit or “ ” (Null). |
| PHNLDLENGTH | 10 | Length of national deskphone number. The number of digits in the longest possible national deskphone number by the algorithm that dials |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | calls from the incoming Call Log or from Web pages.<br>Range: 1 or 2 digits, from “3” to “10.” Range: 1 or 2 ASCII numeric characters, from 5 to 15. |
| PHNOL | 9 | Outside line access code. The character(s) dialed, including # and *, if any, to access public network local trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-2 dialable characters, including “ ” (Null). |
| PHNSCRALL | 0 | Applies only to deskphones running software Release 6.0 and later. Phone Screen Consolidation flag. Consolidates call appearances and feature buttons into one scroll-able list, with no separate views. 1 ASCII numeric digit as follows: 0= Do not consolidate call appearances and feature buttons into one scrollable list.<br>1= Consolidate call appearances and feature buttons into one scrollable list. |
| PHY1STAT | 1 | Ethernet line interface setting 1=auto-negotiate, 2=10 Mbps half-duplex, 3=10 Mbps full-duplex, 4=100 Mbps half-duplex, 5=100 Mbps full-duplex, and 6=1000 Mbps full-duplex, if supported by the hardware. |
| PHY2PRIO | 0 | Layer 2 priority value for frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is 1 (enabled). Values are from 0 through 7 and correspond to the drop-down menu selection. |
| PHY2STAT | 1 | Secondary Ethernet interface setting, 0=Secondary Ethernet interface off/disabled, 1=auto-negotiate, 2=10 Mbps half-duplex, 3=10 Mbps full-duplex, 4=100 Mbps half-duplex, 5=100 Mbps full-duplex), and 6=1000 Mbps full-duplex if supported by the hardware. |
| PHY2VLAN | 0 | VLAN identifier used by frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is “1” (enabled).<br>Value is 1-4 ASCII numeric digits from 0 to 4094. Null is not a valid value, nor can the value contain spaces. If this value is set by LLDP using the Port VLAN ID TLV value, the value will not change regardless of settings from other sources. For |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | more information, see About parameter data precedence on page 22. |
| PINGREPLYV6 | 1 | Specifies whether ICMPv6 Echo Reply messages will be sent or not. Valid values are: 0= ICMPv6 Echo Reply messages will not be sent. 1= ICMPv6 Echo Reply messages will be sent only in reply to received Echo Request messages with a Destination address equal to one of the deskphone's unicast IPv6 addresses. 2= ICMPv6 Echo Reply messages will be sent in reply to received Echo Request messages with a Destination address equal to one of the unicast, multicast or anycast IPv6 addresses of the deskphone. |
| PROCPSWD | 27238 | Text string containing the local dial pad procedure password (Null or 1-7 ASCII digits). If set, password must be entered immediately after accessing the Craft Access Code Entry screen, either during initialization or when Mute or the Contacts button for the 9610 is pressed to access a craft procedure. Intended to facilitate restricted access to local procedures even when command sequences are known. Password is viewable, not hidden. |
| PROCSTAT | 0 | Local dial pad Administrative Options status (0=all Administrative (Craft) Options are allowed, 1=only VIEW is allowed). |
| PUSHCAP | 2222 | Push capabilities. Valid values are any three or four digit combination using only the digits 0, 1, or 2.<br>For information on push messaging and administration, see the *Avaya IP Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide, 16-600888*. |
| PUSHPORT | 80 | TCP listening port number used for the deskphone’s HTTP server. 2 to 5 ASCII numeric digits, 80 through 65535. |
| QKLOGINSTAT | 1 | Quick login permission flag. Valid values are:<br>1= Quick login permitted; user must press the pound (#) key to see the previous Extension and Password.<br>0= Quick login not permitted; the user must explicitly enter the extension and password. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| QTESTRESPONDER | “ ” (Null) | Specifies the IP address to which Qtest messages should be sent. The device at this address must support the echo service on UDP port 7, as specified in IETF RFC 862. Format is dotted decimal, colon-hex, or DNS format, separated by commas, with no spaces. Zero to 255 ASCII characters, including commas. |
| RECORDINGTONE | 0 | Recording tone permission flag. (0=Recording tone is disabled, 1= Recording tone is enabled). When recording tone is enabled, when the agent is on an active call or conference call, the deskphone inserts a tone into the audio stream every 15 seconds, so that both the user and the far end hears it. The recording tone has a frequency of 1400 Hz and a duration of 0.2 seconds. |
| RECORDINGTONE_INTERVAL | 15 | Recording tone interval. The number of seconds between recording tones, with a range from 1 to 60. |
| RECORDINGTONE_VOLUME | 0 | Volume of Recording tone played. (1 or 2 ASCII digits from ‘0’ to ‘10’). The default plays the Recording tone at the same volume as the rest of the audio path; each higher number reduces the volume by 5 db. |
| REREGISTER | 20 | Registration timer in minutes. Controls an H.323 protocol timer that should only be changed under very special circumstances by someone who fully understands the system operation impact. Value is 1-120. |
| REUSETIME | 60 | The number of seconds to wait for successful completion of DHCP before reusing previous parameters on the default (port) VLAN. Valid values are 1 to 3 ASCII numeric digits, 0 and 20 through 999. |
| RFSNAME | “ ” (Null) | Applies only to deskphones running software Release 6.0 and later. The file name of the Signed Kernel/Root Software Package that should be downloaded and installed by the deskphone during power-up or reset if it has not already been downloaded and installed. This parameter should only be set in an upgrade file. |
| RINGBKFEATURES | “ ” (Null) | A list of feature number identifiers for softkey features potentially available in the active with far end ringback call state. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | Zero to 255 ASCII characters consisting of zero to three whole numbers separated by commas without any intervening spaces. For more information, see Administering features on softkeys on page 137. |
| RINGTONESTYLE | 0 | The Ring Tone Style Menu initially offered to the user ,0=Classic; 1=Alternate, more modern ringtones. |
| RTCPMON | “ ” (Null) | Text string containing the 4-octet IP address of the RTCP monitor currently in use, in dotted decimal or DNS Name format (0-15 ASCII characters, no spaces). |
| SCEPPASSWORD | “$SERIALNO” | Specifies a challenge password for SCEP. Zero to 32 ASCII characters |
| SCREENSAVER | “ ” (Null) | Filename for a custom screen saver. 0 to 32 ASCII characters. Note that screen saver files must be in .jpg format. Acceptable characters for use in filenames are: 0 through 9<br>A through Z a through z - (dash) . (period)<br>_ (underscore) |
| SCREENSAVERON | 240 | Number of idle time minutes after which the screen saver is turned on. The default is 240 minutes (4 hours). Valid values range from zero (disabled) to 999 minutes (16.65 hours). For 9670G phones, use HOMEIDLETIME instead. |
| SSH_ALLOWED | 1 | Secure Shell (SSH) Protocol permission flag. (0=SSH is not supported, 1= SSH is supported). “Supporting SSH” means the Avaya Services organization can have remote access to the deskphone, using SSHv2, as described in topic Secure Shell Support. |
| SSH_BANNER_FILE | “ ” (Null) | Specifies the file name or URL for a custom SSH banner file. Zero to 255 ASCII characters: zero or one file name or URL. Used to provide a security warning message to the client before SSH authentication is attempted.<br>If the parameters is left at the default value, the default banner message is as stated in the topic Secure Shell Support. |
| SSH_IDLE_TIMEOUT | 10 | Specifies the number of minutes of inactivity after which SSH will be disabled. Valid values are 1 to 5 ASCII numeric digits, zero through 32767. |

| Parameter name | Default value | Description and value range |
|---|---|---|
| SSH_LOCKOUT_ATTEMPTS | 0 | Specifies the number of failed login attempts after which SSH will be disabled. Valid values are 1 to 5 ASCII numeric digits, zero through 32767. |
| SSH_LOGIN_DELAY | 60 | Specifies the number of seconds of delay between login attempts if three or more attempts fail. Valid values are 1 to 5 ASCII numeric digits, zero through 32767. |
| SSH_USERNAME | “craft” | Specifies the user name to be used for SSH logins. Valid values are 0 to 255 ASCII characters. |
| SSO_ENABLED | 0 | Specifies whether Single Sign (SSO) on capability is enabled or disabled. Valid values are:<br>0= Default , SSO disabled. 1=SSO enabled. |
| SSO_CLIENT_CERT | 0 | Specifies whether the telephone will request and authenticate an identity certificate from the desktop computer during the TLS handshake for SSO. Valid values are:<br>0= Default value, specifies that the telephone will not request a certificate from the desktop computer. 1= the telephone will request and authenticate an identity certificate from the desktop computer during the TLS handshake. |
| SSO_DISCONNECT_ACTION | 1 | Specifies what the telephone does if the link is lost on the secondary (PC) Ethernet interface while it is registered with credentials that were provided by, or that are the same as those provided by, an SSO Register command. Valid values are:<br>1= Default, the telephone invokes each FAC contained in the value of SSO_DISCONNECT_FACS and then unregisters. 2 = The telephone locks up. 3 = The telephone remains active.<br>**Note:**<br>If the SSO TCP connection is terminated but the link is not lost, no action is taken based on this parameter. |
| SSO_DISCONNECT_FACS | “null string” | Specifies a list of Feature Access Codes (FACs) to be activated before the deskphone unregisters due to loss of the SSO-LD link. |
| SSO_LOCK_SYNC | 1 | Specifies what the telephone does if the telephone receives a Lock or Unlock command from the SSO application. Valid values are: |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | 1= Default, the telephone attempts to run the LOCK command. 0 = the telephone ignores the LOCK command. |
| SSO_REGISTERED_MODE | 1 | Specifies what the telephone does if the telephone receives a Register command from an SSO application when the telephone is already registered. Valid values are 1,2.<br>1= Default, the telephone unregisters and attempts a normal registration using the received credentials. If the new credentials match the existing credentials, the telephone will not unregister and reregister. 2 = The telephone accepts the received credentials only if the credentials match the existing credentials. |
| SIG | 0 | Signaling protocol download flag. Valid values are:<br>0 = Default. For software releases prior to 6.0, Default means the default protocol as determined by the `96xxupgrade.txt` file, a custom upgrade file is required to support both protocols. For software releases 6.0 and later, Default means to download the upgrade file for the same protocol that is supported by the software that the deskphone is currently using. 1 = Use H.323 protocol 2 = Use SIP protocol |
| SNMPADD | “ ” (Null) | Text string containing zero or more allowable source IP addresses for SNMP queries, in dotted decimal or DNS format, separated by commas, with up to 255 total ASCII characters including commas. Note that from Communication Manager Release 4.0 onwards, SNMP addresses can also be administered on the system-parameters IP-options form. |
| SNMPSTRING | “ ” (Null) | Text string containing the SNMP community name string (up to 32 ASCII characters, no spaces). Note that from Communication Manager Release 4.0 onwards, the SNMP community string can also be administered on the system-parameters IP-options form. |
| SYSAUDIOPATH | 0 | For Avaya Call Center use only<br>Specifies whether the agent can select an option for Audio Path (the Headset or Speaker) or must use the default as configured by the administrator. Valid values are: |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | 0 = Default value. The agent can select the audio path through option & settings -> call settings. The options are Headset or speaker. 1 = The deskphone automatically sets the parameter OPTAUDIOPATH to 1 (speaker) and the agent will not have the option to choose the audio path through call settings. 2 = The deskphone automatically sets parameter OPTAUDIOPATH to 2 (headset) and the agent will not have the option to choose the audio path through call settings.<br>**Note:**<br>By implication, if the 46xx settings file contains a non-default value for SYSAUDIOPATH, the setting for SYSAUDIOPATH overrides any user-specified settings for the audio path. |
| TIMERSTAT | 0 | TIMERSTAT specifies whether Timer On and Timer Off softkeys will be presented to the user. 0 = Timer On and Timer Off softkeys will not be presented to the user (default).<br>1 = Timer On and Timer Off softkeys will be presented to the user. |
| TLSDIR | “ ” (Null) | HTTPS server directory path. The path name prepended to all file names used in HTTPS get operations during initialization. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required. The command syntax is *SET TLSDIR mytlsdir* where *mytlsdir* is your HTTPS server path. TLSDIR is the path for all HTTPS operations except for BRURI. |
| TLSPORT | 80 | TCP port number used for HTTPS file downloading. 2 to 5 ASCII numeric digits. Valid values are 80 through 65535. Note that when the file server is on Communication Manager, set this value to 81 which is the port required for HTTPS downloads rather than the using the default. |
| TLSSRVR | “ ” (Null) | IP addresses or DNS Names of HTTPS file servers used to download deskphone files. Dotted decimal or DNS format, separated by commas. Valid values are 0-255 ASCII characters, including commas. |
| TLSSRVRID | 1 | Controls whether the identity of a TLS server is checked against its certificate. 1 ASCII numeric digit. Valid values are: 1=Provides additional |

| Parameter name | Default value | Description and value range |
|---|---|---|
| | | security by checking to verify that the server certificate's DNS name matches the DNS name used to contact the server. 0=Certificate is not checked against the DNS name used to contact the server. |
| VUMCIPADD | " " (Null) | Specifies a list of H.323 call server IP addresses for the Visiting User feature. addresses can be in dotted-decimal (IPv4) or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters |

**Note:**

The preceding table applies to all 9600 Series IP deskphones. Certain 9600 IP deskphones might have additional, optional information that you can administer. For more information, see Administering Applications and Options on page 165.

# Single Sign on for local devices (SSON-LD)

With the Single Sign On for local devices (SSON-LD) feature, you can log in to your desktop computer and then automatically log in to your deskphone using separate phone login credentials.

When you log out of the desktop computer, the connected deskphone also locks up.

To use this feature:

- Your administrator must enable the SSO-LD feature for your extension.
- Your desktop computer must have an SSO-LD application installed.
- You must connect your desktop computer to your deskphone through the secondary LAN interface on the deskphone.

You can use the SSO-LD feature in the following scenarios:

- Office: When you log in to a computer that you have connected to your office deskphone, or when you reconnect your laptop to your office deskphone, the deskphone automatically unlocks, and logs you in. When you turn off the computer and disconnect the computer the deskphone automatically locks up. The deskphone does not log out and continues to log missed calls.
- Shared public desk: When a user, for example, a guest, connects the office laptop to a deskphone at a public desk, the deskphone automatically registers and the phone is unlocked. When a user disconnects the laptop, the deskphone automatically unregisters

or locks. If the user reconnects to the same deskphone, the deskphone automatically reregisters or unlocks.

- Conference room: This scenario is similar to that at a public desk, but when the user disconnects the laptop, the deskphone reregisters with the room extension.
- Shared desk with shared computer: This scenario is similar to a desktop computer connected to an office phone. However in this case, the desktop computer supports multiple user login accounts as users share the PC and the phone by working on different shifts.
- Contact center: The desktop computer connected to the deskphone runs a contact center program. When an agent logs in to the computer, the phone automatically registers the user to a call server. The agent must log in to the call center separately. The agent also has the option to log in through an agent login Feature Access Code (FAC) to the contact center program. When the agent logs out of the computer, the phone unregisters, and hence, the agent logs out of the call center.

# Administering a VLAN

This section contains information on how to administer 9600 Series IP deskphones to minimize registration time and maximize performance in a Virtual LAN (VLAN) environment. If your LAN environment does not include VLANs, set the system parameter L2Q to 2 (off) to ensure correct operation.

**Related topics:**

[About VLAN Tagging](#) on page 110
[The VLAN default value and priority tagging](#) on page 111
[Automatic detection of a VLAN](#) on page 111
[VLAN separation rules and related parameters](#) on page 112

## About VLAN Tagging

IEEE 802.1Q tagging (VLAN) is a useful method of managing VoIP traffic in your LAN. You can establish a *voice* VLAN, set L2QVLAN to the VLAN ID of that VLAN, and provide voice traffic with priority over other traffic. If LLDP was used to set the VLAN for the deskphones, that setting has absolute authority. Otherwise, you can set VLAN tagging manually, by DHCP, or in the 46xxsettings.txt file.

If VLAN tagging is enabled (L2Q=0 or 1), the9600 Series IP Deskphones set the VLAN ID to L2QVLAN, and VLAN priority for packets from the deskphone to L2QAUD for audio packets and L2QSIG for signalling packets. The default value (6) for these parameters is the recommended value for voice traffic in IEEE 802.1D.

Regardless of the tagging setting, a 9600 Series IP Deskphone will always transmit packets from the deskphone at absolute priority over packets from the secondary Ethernet interface

from an attached PC. The priority settings are useful only if the downstream equipment is administered to give the *voice* VLAN priority.

**Important:**

VLAN tags are always removed from frames that egress or go out of the secondary Ethernet interface because many PCs will ignore tagged frames.

## The VLAN default value and priority tagging

The parameter L2QVLAN identifies the 802.1Q VLAN Identifier and is initially set to 0. This default value indicates *priority tagging* and specifies that your network Ethernet switch automatically insert the default VLAN ID without changing the user priority of the frame.

But some switches do not process a VLAN ID of zero and require frames tagged with a non-zero VLAN ID.

If you do not want the default VLAN to be used for voice traffic, set the value of L2QVLAN to the VLAN ID appropriate for your voice LAN.

You can also administer another parameter VLANTEST that defines the number of seconds the 9600 Series IP Deskphone waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is *60* seconds. If you use VLANTEST, the deskphone returns to the default VLAN if an invalid VLAN ID is administered or if the phone moves to a port where the L2QVLAN value is invalid.

The default value of VLANTEST is long, allowing for the scenario that a major power interruption is causing the phones to restart. Always allow time for network routers, the DHCP servers, and other equipment to be returned to service. If the deskphone restarts for any reason and the VLANTEST time limit expires, the administered VLAN ID becomes invalid. The deskphone then initiates operation with a VLAN ID of 0. Or, if the value of L2Q is 0, that is auto, the deskphone turns off tagging until the L2QVLAN is set to a non-zero value or until the deskphone verifies that the network can support tagged frames.

Setting VLANTEST to “0” causes the phone to use a non-zero VLAN indefinitely to attempt DHCP. In other words, the deskphone does not return to the default VLAN.

## Automatic detection of a VLAN

The deskphones support automatic detection of the L2QVLAN setting that is incorrect. When the value of L2QVLAN is not 0 and VLAN tagging is enabled, L2Q= 0 or 1, initially the 9600 Series IP Deskphone transmits DHCP messages with IEEE 802.1Q tagging and sets the VLAN

ID to L2QVLAN. The deskphones will continue to do this for number of seconds configured by VLANTEST.

- If L2Q=1 and the VLANTEST timer expires because the deskphone has not received a DHCPOFFER, the deskphone sets L2QVLAN=0 and transmits DHCP messages with the default VLAN (0).
- If L2Q=0 and the VLANTEST timer expires because the deskphone has not received a DHCPOFFER, the deskphone sets L2QVLAN=0 and transmits DHCP messages without tagging.
- If VLANTEST is 0, the timer never expires.

**Note:**

Regardless of the setting of L2Q, VLANTEST, or L2QVLAN, you must have administer DHCP on the deskphone so that the deskphone receives a response to a DHCPDISCOVER on making that request on the default (0) VLAN.

After VLANTEST expires, if an Avaya IP deskphone running R1.2 receives a non-zero L2QVLAN value, the deskphone releases the IP address and sends DHCPDISCOVER on that VLAN. Any other release requires you to perform a manual reset before the deskphone attempts to use a VLAN on which VLANTEST has expired. For more information on the Reset procedure, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*.

The deskphone ignores any VLAN ID administered on the call server if a non-zero VLAN ID is administered either by LLDP, manually, through DHCP, or through the settings file.

## VLAN separation rules and related parameters

VLAN separation is available to control access to the voice VLAN from the secondary Ethernet interface, and to control whether broadcast traffic from the data VLAN is forwarded to the phone. The following system parameters control VLAN separation:

- VLANSEP - enables (1) or disables (0) VLAN separation.
- L2QVLAN - specifies the voice VLAN ID to be used by the deskphone.
- PHY2VLAN - specifies the VLAN ID to be used for frames forwarded to the network from the secondary Ethernet interface.
- PHY2PRIO -specifies the layer 2 priority value to be used for tagged frames forwarded to the network from the secondary Ethernet interface.

The table below provides several VLAN separation guidelines.

**Note:**

The 9610 IP deskphone does not support full VLAN separation because the deskphone does not have a secondary Ethernet interface and PHY2VLAN and PHY2PRIO values.

**Table 11: VLAN Separation Rules**

| Condition | | Outcome |
|---|---|---|
| VLANSEP is 1 (On/Enabled) | AND the deskphone is tagging frames with a VLAN ID not equal to PHY2VLAN, AND the PHY2VLAN value is not zero. | **Tagged Frames received on the secondary Ethernet interface:**<br>Tagged frames received on the secondary Ethernet interface are changed/not changed as follows:<br>If a Gigabit Ethernet Adapter is not used, tagged frames with a VLAN ID of zero, prioritytagged frames, are changed and then forwarded such that the VLAN ID of the forwarded frame is equal to the PHY2VLAN value and the priority value is equal to the PHY2PRIO value.<br>If a Gigabit Ethernet Adapter is being used, tagged frames with a VLAN ID of zero will not be changed before they are forwarded.<br>Untagged frames received on the secondary Ethernet interface are not changed before forwarding to the network.<br>**Tagged Frames received on the line interface:**<br>Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2VLAN.<br>Tagged frames received on the Ethernet line interface will only be forwarded to the deskphone if the VLAN ID equals the VLAN ID used by the deskphone.<br>Untagged frames are not changed will continue to be forwarded or not forwarded as determined by the Ethernet switch forwarding logic.<br>Tagged frames with a VLAN ID of zero (priority-tagged frames) will be forwarded to the secondary Ethernet interface or to the deskphone as determined by the forwarding logic of the Ethernet switch, but the tag will still be removed from frames that egress from the secondary Ethernet interface. |
| VLANSEP is 1 (On/Enabled) | AND the deskphone is not tagging frames, OR if the deskphone is tagging frames | Frames forwarded to the network from the secondary Ethernet interface will not be changed before forwarding. Tagging is not added or removed and the VLAN ID and priority does not change for frames received on the |

| Condition | | Outcome |
|---|---|---|
| | with a VLAN ID equal to PHY2VLAN, OR if the PHY2VLAN value is zero. | secondary interface. Tags are still removed for frames that egress from the secondary interface. The Ethernet switch forwarding logic determines whether frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the deskphone regardless of specific VLAN IDs or the existence of tags. |
| VLANSEP is 0, | OR the deskphone is not tagging frames, OR the deskphone is tagging frames with a VLAN ID equal to PHY2VLAN. | Frames forwarded to the network from the secondary Ethernet interface will not be changed before forwarding. Tagging is not added or removed and the VLAN ID and priority does not change for frames received on the secondary interface. Tags are still removed for frames that egress from the secondary interface. The Ethernet switch forwarding logic determines whether frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the deskphone without regard to specific VLAN IDs or the existence of tags. |
| ***VLANSEP is 1 (On/Enabled) | | The deskphone changes all tagged frames that received on the secondary Ethernet interface and then forwards the frames to make the VLAN ID equal to the PHY2VLAN value and the priority value equal to the PHY2PRIO value.<br>The deskphone does not change untagged frames received on the secondary Ethernet interface before forwarding.<br>If the deskphone does not use a Gigabit Ethernet Adapter, priority tagged frames with a VLAN ID of zero are changed before they are forwarded such that the VLAN ID of the forwarded frame is equal to the PHY2VLAN value and the priority value is equal to the PHY2PRIO value. If the deskphone uses the Gigabit Ethernet Adapter, tagged frames with a VLAN ID of zero are not changed before they are forwarded. |
| VLANSEP is 1 (On/Enabled) | AND the deskphone is not tagging frames, OR if the deskphone is tagging frames with a VLAN ID equal to PHY2VLAN, OR if the PHY2VLAN value is zero. | The Ethernet switch forwarding logic determines that frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the deskphone without regard to specific VLAN IDs or the existence of tags. Frames received on the secondary Ethernet interface will not be changed before forwarding. In other words, tagging is not added or removed, and the VLAN ID and priority of tagged frames is not changed. |

| Condition | | Outcome |
|---|---|---|
| VLANSEP is 1 (On/Enabled) | AND the deskphone is tagging frames with a VLAN ID not equal to PHY2VLAN, AND the PHY2VLAN value is not zero. | Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2VLAN.<br>Tagged frames received on the Ethernet line interface will only be forwarded to the deskphone if the VLAN ID equals the VLAN ID used by the deskphone.<br>Untagged frames will continue to be forwarded or not forwarded as determined by the Ethernet switch forwarding logic.<br>Priority tagged frames with a VLAN ID of zero are either be: - forwarded to the secondary Ethernet interface or the deskphone as determined by the forwarding logic of the Ethernet switch preferred, or - dropped. |

# About DNS addressing

The 9600 IP deskphones support DNS addresses, dotted decimal addresses, and as of Release 6.0, colon-hex addresses. The phone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the contents of DHCP Option 6. For more information, see DHCP Generic Setup on page 67. At least one address in Option 6 must be a valid, non-zero, dotted decimal address. Otherwise DNS fails. The text string for the DOMAIN system parameter, Option 15 is appended to the addresses in Option 6 before the phone attempts DNS address resolution. If Option 6 contains a list of DNS addresses, those addresses are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS by DHCP, you can specify the DNS server and/or Domain name in the HTTP script file. But first SET the DNSSRVR and DOMAIN values so that you can use those names later in the script.

**Note:**

Administer Options 6 and 15 appropriately with DNS servers and Domain names respectively.

# EAP-TLS support for authentication

You can use the EAP-TLS as the mode of authentication. To activate this mode, you must add a new parameter DOT1XEAPS, with valid values of `MD5` or `TLS` to the settings file. The default value is `MD5`. The call server supports EAP-TLS as specified in RFC 2716 if and only if an

identity certificate is present in the deskphone and if the value of DOT1XEAPS is `TLS`. If an EAP method requires the authentication of a digital certificate, and if you have enabled the Supplicant on the phone and the value of `DOT1XEAPS` changes, the Supplicant will transmit an EAPOL-Logoff message and return to the CONNECTING state.

**Related topics:**

Enabling certificate support on page 116
Activating EAP-TLS for authentication on page 117
Scenarios for using EAP-TLS based authentication on page 118
Deploying EAP-TLS based authentication for phones using 802.1x and MD5 on page 118
Deploying EAP-TLS on phones running without any type of 802.1x authentication on page 120

# Enabling certificate support

You can use Simple Certificate Enrollment Protocol (SCEP) to provide an identity certificate for use with certificate-based VPN authentication methods. The 802.1x EAP-TLS method also uses the identity certificate for authentication. When you use TLS with HTTPS, you can use the identity certificate to authenticate the phone and save the agent greetings or perform a backup or restore.

The phone stores the identity certificate and the phone uses the identity certificate during the TLS handshake as required when the phone is acting as a server. When the phone is acting as a client, the phone transmits the identity certificate on request. The 9600 Series IP Deskphones support Media Encryption (SRTP) and use built-in Avaya certificates for trust management. Trust management includes downloading certificates and managing policies for additional trusted Certificate Authorities (CA). Simple Certificate Enrollment Protocol (SCEP) handles identity management with phone certificates and private keys. You can apply SCEP to your VPN operation or to standard enterprise network operation.

## Before you begin

For SCEP servers that are outside the corporate firewall, configure the phones that use a VPN connection to establish an SCEP connection through an HTTP proxy server to reach the SCEP server. In this instance, use the WMLPROXY system parameter to configure the HTTP proxy server.

When the phone initiates SCEP, the phone attempts to contact an SCEP server through HTTP, using the value of the configuration parameter MYCERTURL as the URI. SCEP supports an HTTP proxy server. The phone creates a private/public key pair, where the length of each key is equal to the value of the configuration parameter MYCERTKEYLEN. The certificate request uses the public key and the values of the configuration parameters MYCERTCAID, MYCERTCN, MYCERTDN, and SCEPPASSWORD.

## About this task

You must configure the 46xxsettings.txt file on the file server with the specified parameters to use an identity certificate to authenticate the phones.

### Procedure

Configure the following parameters in the 46xxsettings.txt file:

- SET MYCERTURL < URL for enrolling with a SCEP fronted Certificate Authority> for example, http://149.49.44.53/certsrv/mscep/mscep.dll.
- SET MYCERTCN $MACADDR.
- SET MYCERTWAIT 1.
- SET TRUSTCERTS "root_ certificate".

## Activating EAP-TLS for authentication

### Before you begin

To activate the 802.1x EAP-TLS mode, you must “SET DOT1XEAPS TLS on the 46xxsettings.txt file of the file server.

### About this task

You can use the EAP-TLS method to authenticate the phones with the call server. For implementing this type of authentication, you must configure the EAP-TLS parameters in the 46xxsettings file and on the call server.

### Procedure

1. SET MYCERTURL < URL for enrolling with a SCEP fronted Certificate Authority >.

   URL Example: http://149.49.44.53/certsrv/mscep/mscep.dll.
2. SET MYCERTWAIT 1
3. SET MYCERTCN $MACADDR
4. SET DOT1XEAPS `TLS`
5. SET TRUSTCERTS & <Root CA Filename>
6. Connect the phone to a port that does not have 802.1x enabled. The phone receives the settings from 46xxsettings.txt file.
   The phone contacts the call server to activate the SCEP process.
7. Unplug the phone and connect the phone to a port that you have configured for EAP-TLS and enable the supplicant on the phone through the CRAFT procedure. You can also enable the supplicant by configuring the 46xxsettings.txt with `SET DOT1XSTAT 2`.

**Note:**

The MAC option `SET MYCERTCN $MACADDR` supports the `MYCERTCN` parameter in H.323 Release 6.2 Service Pack 1.

For H.323 Release 6.2 Service Pack 1, after the phone starts with EAP-TLS mode, the user does not need to enter device Id or password as in MD5.

## Scenarios for using EAP-TLS based authentication

You can deploy the EAP-TLS method for authentication that requires an identity certificate that is stored in the phone.

The following sections describe the authentication scenarios where you might need to deploy EAP-TLS. Before deploying EAP-TLS, you must set the phones to a default state that can be one of the following:.

- Phones not running any type of 802.1x authentication
- Phones using 802.1x using MD5 as the authentication method

## Deploying EAP-TLS based authentication for phones using 802.1x and MD5

### Before you begin

The administration of EAP-TLS requires the installation of an identity certificate. So, the initial network for phone installation can be a phone, an Ethernet switch, and a computer in the IT department. The computer might need to gain access to the Internet if you use an external CA for signing the certificates. You can configure the settings file on the network to configure DOT1XSTAT to 1 or 2. This change takes effect the next time that the phone resets. The phone must connected to that network without resetting until a certificate is successfully installed. Or, you can enable 802.1x manually by using the 802.1x craft procedure after you install a certificate.

### Procedure

1. Get the Beta files for H.323 Release 6.2 Service Pack 1 from your Avaya contact. Upgrade the phones to H.323 Release 6.2 Service Pack 1 and ensure that the phones still authenticate using MD5.

2. Connect the phones on a network that does not support 802.1X access control (switch and phone), modify the 46xxsettings.txt file, and incorporate the following SCEP parameters:

   a. SET TRUSTCERTS < RootCert >
   b. SET MYCERTURL http:// <IP of CA server > /certsrv/mscep/mscep.dll
   c. SET MYCERTWAIT 0
   d. SET SCEPPASSWORD <password>#### optional
   e. SET DOT1XEAPS TLS
   f. SET DOT1XSTAT 2 #### optional
   g. Clear the phone and then restart the phone, and ensure that the phone upgrades to H.323 Release 6.2 Service Pack 1.
   h. Connect the phone to a network that supports DOT1x.

      The phone starts the process of certificate enrollment automatically, by sending a SCEP request to MYCERTURL. After the boot process completes, the phone obtains the root certificate and the device certificate successfully and changes to the EAP-TLS mode.
   i. Monitor the CA, to check that all phones that you have upgraded, have enrolled their certificates with the CA. If you administer the CA to require manual approval of certificate enrollment requests, then the phone will take a minimum of two minutes to download the enrolled certificate after the CA approves the request. Therefore, do not restart the phones until at least 2 minutes after approving the certificate enrollment request. If the certificate enrollment process is automatic, it takes less time than manual enrollment.

3. Administer the RADIUS server to accept the identity certificates provided by the phones.
4. To turn on 802.1x authentication, change the 46xxsettings.txt file by setting DOT1XSTAT to a value of 1 or 2.
5. Clear the phones and then restart the phones to apply the new settings. The phones start their supplicants with the EAP-TLS authentication method. Configure the Layer 2 switches to which you attach these phones. The switches can then support EAP-TLS on those ports to which you attach the phones.

   If you do not require the phone to connect to a network that does not support DOT1X , reset the phones manually or using the CM and only then, change the switch configuration to support EAP-TLS.

### Result

The switches then prompt the phones to authenticate using EAP-TLS and the phones must authenticate themselves using the enrolled certificates. After you setup the phones, the phones must maintain their configurations across restarts and upgrades. Depending on the value of `MYCERTRENEW`, the phones try to renew their certificates enrollment, periodically. The administrator must monitor pending enrollments.

# Deploying EAP-TLS on phones running without any type of 802.1x authentication

## Before you begin

Configure the Layer 2 switches to which you attach the phones running without any type of 802.1x authentication, so that the switches do not support EAP-TLS on the ports to which the phones are attached.

## Procedure

1. In the 46xxsettings.txt file, turn off the supplicant operation by making the following entry: `SET DOT1XSTAT 0`.
2. Modify the upgrade.txt file to point to location for the H.323 Release 6.2 Service Pack 1 files.
3. Modify the settings file, to incorporate the following SCEP parameters appropriately: `MYCERTURL`, `MYCERTWAIT`, `MYCERTRENEW` and `MYCERTDN` if needed.
4. Reboot the phone, and ensure that the phone upgrades to H.323 Release 6.2 Service Pack 1. The phone starts the process of certificate enrollment automatically, by sending a SCEP request to `MYCERTURL`.
5. Monitor the CA, to check whether all the phones that the system has upgraded, have enrolled their certificates with the CA.

   **Note:**

   If you administer the CA to require manual approval of certificate requests, then the phone takes a minimum of two minutes to download the identity certificate after the CA approves the request. Therefore, do not reboot the phones until at least two minutes after approving the certificate enrollment request. If the certificate enrollment process is automatic, the process takes less time than manual enrollment.
6. Administer the RADIUS server to accept the identity certificates provided by the phones.
7. Change the 46xxsettings.txt file, to turn on 802.1x authentication, by setting `DOT1XSTAT` to a value of 1 or 2.
8. Set the EAPS authentication method to TLS by setting `SET DOT1XEAPS TLS` in the 46xxsettings.txt file.
9. Clear the phones and then restart the phones to apply the new settings. As the phones restart the phones start the supplicants with EAP-TLS authentication method.

10. Configure the Layer 2 switches to which you have attached these phones, to support EAP-TLS on the ports to which you have attached the phones.

### Result

The switches prompt the phones to authenticate using EAP-TLS and the phones authenticate using the enrolled certificates. After setup completes, the phones maintain the configurations across restarts and upgrades. Depending on the value of `MYCERTRENEW`, the phones try to renew their certificates enrollment, periodically. The administrator must monitor pending enrollments.

# About IEEE 802.1X

9600 Series IP phones support the IEEE 802.1X standard for Supplicant operation and support pass-through of 802.1X messages to an attached PC. The system parameter DOT1X determines how the phones handle pass-through of 802.1X multicast packets and proxy logoff:

- When DOT1X = 0, the phone forwards 802.1X multicast packets from the Authenticator to the PC attached to the phone and forwards multicast packets from the attached PC to the Authenticator (multicast pass-through). The phone does not support Proxy Logoff. This is the default value.
- When DOT1X = 1, the phone supports the same multicast pass-through as when DOT1X=0, but Proxy Logoff is also supported. When the secondary Ethernet interface loses link integrity, the phone sends an 802.1X EAPOL-Logoff message to the Authenticator with a source MAC address from the previously attached device. This message alerts the Authenticator that the device is no longer connected.
- When DOT1X = 2, the phone forwards multicast packets from the Authenticator only to the phone, ignoring multicast packets from the attached PC (no multicast pass-through). The phone does not support Proxy Logoff.
- Regardless of the DOT1X setting, the phone always properly directs unicast packets from the Authenticator to the phone or its attached PC as specified by the destination MAC address in the packet.

All 9600 Series IP phones support Supplicant operation as specified in IEEE 802.1X, but, as of software Release 2.0, only if the value of the parameter DOT1XSTAT is *1* or *2*. If DOT1XSTAT has any other value, the phone does not support Supplicant operation.

Unicast 802.1X frames contain the MAC address of the phone as the destination MAC address and a protocol type of 88-8E hex. IP phones respond to unicast 802.1X frames received on the Ethernet line interface if the value of DOT1XSTAT is *1* or *2*.

IP phones respond to 802.1X frames that have the PAE group multicast address as the destination MAC address only if the value of DOT1XSTAT is 2. If the value of DOT1XSTAT is

changed to 0 from any other value after the Supplicant has been authenticated, an EAPOL-Logoff will be transmitted before the Supplicant is disabled.

From Release 2.0 onwards, the system parameter DOT1XSTAT determines how the phone handles Supplicants as follows:

- When DOT1XSTAT = 0, Supplicant operation is completely disabled. This is the default value.
- When DOT1XSTAT = 1, Supplicant operation is enabled, but responds only to received unicast EAPOL messages.
- When DOT1XSTAT = 2, Supplicant operation is enabled and responds to received unicast and multicast EAPOL messages.

**Note:**

If the Ethernet line interface link fails, the 802.1X Supplicant, if enabled, enters the Disconnected state.

**Related topics:**

802.1X Supplicant operation on page 122

# 802.1X Supplicant operation

9600 IP phones that support Supplicant operation also support Extensible Authentication Protocol (EAP), but for software Release 6.1 and earlier, only with the MD5-Challenge authentication method. For more information about the MD5–Challenge authentication, see IETF RFC 3748.

A Supplicant identity (ID) and password of not more than 12 numeric characters are stored in reprogrammable non-volatile memory. The ID and password are not overwritten by phone software downloads. The default ID is the MAC address of the phone, converted to ASCII format without colon separators, and the default password is null. Both the ID and password are set to default values at manufacture. EAP-Response/Identity frames use the ID in the Type-Data field. EAP-Response/MD5-Challenge frames use the password to compute the digest for the Value field, leaving the Name field blank.

When a phone is installed for the first time and 802.1x is in effect, the dynamic address process prompts the installer to enter the Supplicant identity and password. The IP phone does not accept null value passwords.

For more information about Dynamic Addressing Process, see *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*. The IP phone stores 802.1X credentials when successful authentication is achieved. Post-installation authentication attempts occur using the stored 802.1X credentials, without prompting the user for ID and password entry.

An IP phone can support several different 802.1X authentication scenarios, depending on the capabilities of the Ethernet data switch to which it is connected. Some switches may

authenticate only a single device per switch port. This is known as single-supplicant or port-based operation. These switches typically send multicast 802.1X packets to authenticating devices.

These switches support the following three scenarios:

- Standalone phone (Telephone Only Authenticates) - When the IP phone is configured for Supplicant Mode (DOT1XSTAT=2), the phone can support authentication from the switch.
- Phone with attached PC (Telephone Only Authenticates) - When the IP phone is configured for Supplicant Mode (DOT1X=2 and DOT1XSTAT=2), the phone can support authentication from the switch. The attached PC in this scenario gains access to the network without being authenticated.
- Telephone with attached PC (PC Only Authenticates) - When the IP phone is configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1 and DOT1XSTAT=0), an attached PC running 802.1X supplicant software can be authenticated by the data switch. The phone in this scenario gains access to the network without being authenticated.

Some switches support authentication of multiple devices connected through a single switch port. This is known as multi-supplicant or MAC-based operation. These switches typically send unicast 802.1X packets to authenticating devices. These switches support the following two scenarios:

- Standalone phone (Telephone Only Authenticates) - When the IP phone is configured for Supplicant Mode (DOT1XSTAT=2), the phone can support authentication from the switch. When DOT1X is “0” or “1” the phone is unable to authenticate with the switch.
- Phone and PC Dual Authentication - Both the IP phone and the connected PC can support 802.1X authentication from the switch. The IP phone might be configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1 and DOT1XSTAT=1 or 2). The attached PC must be running 802.1X supplicant software.

# About Link Layer Discovery Protocol (LLDP)

Release 1.2 and later 9600 Series IP deskphones support IEEE 802.1AB.

**Note:**

As of software Release 6.0, LLDP is supported only for IPv4 mode.

Link Layer Discovery Protocol (LLDP) is an open standards layer 2 protocol that IP phones use to advertise their identity and capabilities and to receive administration from an LLDP server. LAN equipment can use LLDP to manage power, administer VLANs, and provide some administration.

The transmission and reception of LLDP is specified in IEEE 802.1AB-2005. The 9600 Series IP deskphones use Type-Length-Value (TLV) elements specified in IEEE 802.1AB-2005, TIA TR-41 Committee - Media Endpoint Discovery (LLDP-MED, ANSI/TIA-1057), and Proprietary elements. LLDP Data Units (LLDPDUs) are sent to the LLDP Multicast MAC address (01:80:c2:00:00:0e).

These phones:

- do not support LLDP on the secondary Ethernet interface.
- do not forward frames received with the 802.1AB LLDP group multicast address as the destination MAC address between the Ethernet line interface and the secondary Ethernet interface.

The 9600 Series IP deskphone initiates LLDP after receiving an LLDPDU message from an appropriate system. Once initiated, the phone sends an LLDPDU every 30 seconds with the following contents:

**Table 12: LLDPDU transmitted by the phones**

| Category | TLV Name (Type) | TLV Info String (Value) |
|---|---|---|
| Basic Mandatory | Chassis ID | IPv4 IP Address of phone. |
| Basic Mandatory | Port ID | MAC address of the phone. |
| Basic Mandatory | Time-To-Live | 120 seconds. |
| Basic Optional | System Name | The Host Name sent to the DHCP server in DHCP option 12. |
| Basic Optional | System Capabilities | Bit 2 (Bridge) is set in the System Capabilities if the phone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled.<br>Bit 5 (phone) is set in the System Capabilities. If Bit 5 is set in the Enabled Capabilities than the phone is registered. |
| Basic Optional | Management Address | Mgmt IPv4 IP Address of phone.<br>Interface number subtype = 3 (system port).<br>Interface number = 1.<br>OID = SNMP MIB-II sysObjectID of the phone. |
| IEEE 802.3 Organization Specific | MAC / PHY Configuration / Status | Reports autonegotiation status and speed of the uplink port on the phone. |
| TIA LLDP MED | LLDP-MED Capabilities | Media Endpoint Discovery - Class III - IP Telephone. |
| TIA LLDP MED | Extended Power-Via-MDI | Power Value = 0 if the phone is not currently powered through PoE, else the maximum power usage of the deskphone plus all |

| Category | TLV Name (Type) | TLV Info String (Value) |
|---|---|---|
| | | modules and adjuncts powered by the phone in tenths of a watt. |
| TIA LLDP MED | Network Policy | Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value. |
| TIA LLDP MED | Inventory – Hardware Revision | MODEL - Full Model Name. |
| TIA LLDP MED | Inventory – Firmware Revision | BOOTNAME, or for phones running Software Release 6.0 or later, Firmware Revision = RFSINUSE. |
| TIA LLDP MED | Inventory – Software Revision | APPNAME, or for phones running Software Release 6.0 or later, Software Revision = APPINUSE. |
| TIA LLDP MED | Inventory – Serial Number | Phone serial number. |
| TIA LLDP MED | Inventory – Manufacturer Name | Avaya. |
| TIA LLDP MED | Inventory – Model Name | MODEL with the final D *xxx* characters removed. |
| Avaya Proprietary | PoE Conservation Level Support | Provides power conservation abilities and settings, Typical and Maximum Power values.<br>OUI = 00-40-0D (hex), Subtype = 1. |
| Avaya Proprietary | Call Server IP Address | Call Server IP address.<br>Subtype = 3. |
| Avaya Proprietary | IP Phone Addresses | Phone IP address, Phone address mask, Gateway IP address.<br>Subtype = 4. |
| Avaya Proprietary | CNA Server IP Address | CNA Server IP address = in-use value from CNASRVR.<br>Subtype = 5.<br>This parameter is not supported in Release 6.2 and later. |
| Avaya Proprietary | File Server | File Server IP address.<br>Subtype = 6. |
| Avaya Proprietary | 802.1Q Framing | 802.1Q Framing = 1 if tagging or 2 if not.<br>Subtype = 7. |
| Basic Mandatory | End-of-LLDPDU | Not applicable. |

On receipt of a LLDPDU message, the phones will act on the TLV elements described in the following table:

**Table 13: Impact of TLVs Received by 9600 Series IP deskphones on System Parameter Values**

| System Parameter Name | TLV Name | Impact |
|---|---|---|
| PHY2VLAN | IEEE 802.1 Port VLAN ID | The value is changed to the Port VLAN identifier in the TLV. |
| L2QVLAN and L2Q | IEEE 802.1 VLAN Name | The value is changed to the TLV VLAN Identifier. L2Q will be set to 1 (ON). VLAN Name TLV is only effective if:<br>• The phone is not registered with the call server.<br>• Name begins with VOICE (letters are not case-sensitive).<br>• The VLAN is not zero.<br>• DHCP Client is activated.<br>• The phone is registered but is not tagging layer 2 frames with a non-zero VLAN ID.<br>If VLAN Name causes the phone to change VLAN and the phone already has an IP Address the phone will release the IP Address and reset.<br>If the TLV VLAN ID matches the VLAN ID the phone is using, the VLAN ID is marked as set by LLDP. Otherwise, if already registered, the phone waits until there are no active calls, releases its IP Address, turns on tagging with the TLV VLAN ID, sets L2Q to *on* changes the default L2Q to *on* and resets. If there is no valid IP Address, the phone immediately starts tagging with the new VLAN ID without resetting. |
| L2Q, L2QVLAN, L2QAUD, L2QSIG, DSCPAUD, DSCPSIG | MED Network Policy TLV | L2Q - set to 2 (off) If T (the Tagged Flag) is set to 0; set to 1 (on) if T is set to 1.<br>L2QVLAN - set to the VLAN ID in the TLV.<br>L2QAUD and L2QSIG - set to the Layer 2 Priority value in the TLV.<br>DSCPAUD and DSCPSIG - set to the DSCP value in the TLV.<br>The system checks whether a reset is necessary to obtain a new IP address due to a change in the |

| System Parameter Name | TLV Name | Impact |
|---|---|---|
| | | values of the parameters L2Q or L2QVLAN. This TLV is ignored if:<br>• the value of USE_DHCP is 0 and the value of IPADD is not *0.0.0.0*, or<br>• the Application Type is not 1 (Voice), or<br>• the Unknown Policy Flag (U) is set to 1. |
| MCIPADD | Proprietary Call Server TLV | MCIPADD will be set to this value if it has not already been set. |
| TLSSRVR and HTTPSRVR | Proprietary File Server TLV | TLSSRVR and HTTPSRVR will be set to this value if neither of them have already been set. |
| L2Q | Proprietary 802.1 Q Framing | The default L2Q is set to the value of this TLV. No change is made to the current L2 tagging, but the new default value is used on the next reboot. If TLV = 1, L2Q set to 1 (On). If TLV = 2, L2Q set to 2 (Off). If TLV = 3, L2Q set to 0 (Auto). |
| | Proprietary - PoE Conservation TLV | This proprietary TLV can initiate a power conservation mode. The phones that support this will turn the phone backlight and the backlight of an attached Button Module on or off in response to this TLV. But, the 9670G deskphone puts the display backlight into low-power mode and does not turn off the backlight. |
| | Extended Power-Via-MDI | Power conservation mode is enabled if the received binary Power Source value is 10, and power conservation mode is disabled if the received binary Power Source value is not 10. Power conservation mode is enabled even if the phone is not powered over Ethernet because the phone sends information about the power source that it is using in a TIA LLDP MED Extended Power-Via-MDI TLV. The power management system intends to conserve local power also. |

# Administering settings at the phone

*Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G* describes how to use Craft local procedures at the phone for administration. The local procedures you might use most often as an administrator are:

- 802.1x - Enable or disable the Supplicant and the Pass-thru options.
- ADDR - Add the IP addresses for the call server, HTTP server, HTTPS server, and other network related parameters.
- CLEAR - Remove all administered values, user-specified data, option settings, etc. and return a phone to its initial “out of the box” default values.
- DEBUG - Enable or disable debug mode for the button module serial port.
- GROUP - Set the group identifier on a per-phone basis.
- HSEQUAL - Administer the HAC related parameters.
- INT - Set or change the interface control value(s) of PHY1STAT and/or PHY2STAT.
- RESET - Reset the deskphone to default values including any values administered through local procedures, and values previously downloaded using DHCP or a settings file.
- RESTART - Restart the deskphone in response to an error condition, including the option to reset parameter values.
- SSON - To add site specific options.
- Test - To run a self test on the phone.
- VIEW - Review the 9600 IP deskphone system parameters to verify current values and file versions.

**Note:**

The DEBUG option is available for use only if you change the default password to the craft menu through the PROCPSWD parameter.

The new value of the PROCPSWD parameter must be 4 to 7 numeric digits, "0000" through "9999999". However if value of PROCPSWD is less than 4 digits after you install R6.2.4 or later, the value will be changed back to the default value of 27238.

# Administering display language options

By default, 9600 Series IP deskphones display information in the English language. All software downloads include language files for 13 additional languages. Software Release 1.2

added support for a large font version of English only and Release 1.5 added Arabic to the language file download. Administrators can specify from one to four languages for each phone to replace English. End users can then select the language in which the phone displays messages.

All downloadable language files contain all the information needed for the phone to present the language as part of the user interface.

For touch screen deskphones, this includes an indication of the character to be used as a decimal “point” in numeric values and an indication of the character that should be used as a separator. For example, thousands or millions in numeric values. You cannot use a character or a space character as punctuation marks.

The actual character input method does not depend on the languages available from the software download. If the phone does not support a character input method, ASCII is used instead. Acceptable input methods are as follows:

| | |
|---|---|
| • ASCII | • Croatian, Slovenian |
| • Latin-1 | • Czech, Slovak |
| • German | • Estonian |
| • French | • Hungarian |
| • Italian | • Latvian |
| • Spanish | • Lithuanian |
| • Portuguese | • Polish |
| • Russian | • Romanian |
| • Albanian, Azeri, Turkish | |

Use the configuration file and the following parameters to customize the settings for up to four languages:

- LANGxFILE - The name of a selected language file, for example, *French*. In addition to providing the language name as this value, replace the *x* in this parameter with a 1, 2, 3, or 4 to indicate which of the four languages you are specifying. For example, to indicate that German and French are the available languages, the setting is: **`LANG1FILE=mlf_german.txt`** and **`LANG2FILE=mlf_french.txt`**.
- LANG0STAT - Using this parameter, you can select the built-in English language when other languages are downloaded. If LANG0STAT is 0 and at least one language is downloaded, you cannot select the built-in English language. If LANG0STAT is 1 then you can select the built-in English language text strings.

- LANGSYS - The file name of the system default language file, if any.
- LANGLARGEFONT- The name of the language file you want available for a “large font” display, currently only “English.”

From Release 1.2 onwards, a large text font is available on all 9600 Series IP Telephones but the 9610. You can activate the larger text font only if a language file for this font is available. The Text Size option is presented to the user if the parameter LANGLARGEFONT is not null and if a language file for that value is used as the current user interface language. If neither condition is met, the Text Size option is not available to the user.

For example, if the language in use is English, and a large text font language file for English is specified in LANGLARGEFONT and available, the Text Size option is presented on the **Screen and Sounds Options** screen.

For more information, see 9600 Series H.323 customizable system parameters on page 84. For more information on multiple language strings, see *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*.

To download a language file or review pertinent information, go to support.avaya.com

**Note:**

Specifying a language other than English in the configuration file has no impact on Avaya Communication Manager settings, values, or text strings.

# About the gigabit Ethernet (GigE) adapter

From Release 1.1 onwards, 9600 Series IP deskphones can accommodate a Gigabit Ethernet (GigE) Adapter. Release 1.5 introduced the 9630G and 9640G IP Deskphones that contain a built-in gigabit Ethernet adapter. Release 2.0 introduced the 9670G IP Telephone, which also contains a built-in gigabit Ethernet adapter.

Release 6.0 introduced the 9611G, 9621G, and 9641G IP Deskphones which contain built-in GigE adapters. When connected to an adapter interface, the Gigabit Ethernet Adapter sets the Ethernet line interface operational mode that is built into the deskphone to 1000Mbps full-duplex and deactivates the built-in secondary Ethernet interface.

When a Gigabit Ethernet Adapter is present, any considerations or processing that apply to the *Ethernet line interface* apply only to the Ethernet line interface on that adapter. Likewise, any considerations or processing that apply to the *Secondary Ethernet interface* apply only to the secondary Ethernet interface on the Gigabit Ethernet Adapter.

With an internal or connected Gigabit Ethernet Adapter, system parameters PHY1STAT or the Ethernet line interface and PHY2STAT which is the secondary Ethernet interface activate the respective Ethernet interface in the 1000 Mbps operational mode when supported by the hardware. When the Ethernet interface is not supported by the hardware, the respective Ethernet interface is set to auto-negotiate the speed and duplex.

# Administering dialing methods

9600 Series IP deskphones have a variety of telephony-related applications that might obtain a telephone number during operation. For example, the Call Log/History applications save the number of an incoming caller, but do not account for the fact that the user has to then prepend the saved number with one or more digits to dial an outside line and possibly one or more digits to dial long distance. Two dialing methods are used, depending on which version of Avaya Communication Manager that is running.

**Related topics:**

Understanding log digit or Smart Enbloc dialing on page 131
Using enhanced local dialing on page 131
Enhanced local dialing requirements on page 133

## Understanding log digit or Smart Enbloc dialing

Avaya Aura® Communication Manager Releases 4.0 and later support the feature of a superior level of *enhanced log digit analysis*. This feature is also called smart enbloc dialing and it allows the call server to supplement the number the deskphone dials based on the call server's knowledge of the entire dialing plan. With the server supporting log digit dialing analysis, the deskphone does not attempt to enhance a number as described for enhanced local dialing, and the call server assumes responsibility for analysis and action. Smart enbloc provides a more accurate dialing method because the deskphone signals to the call server that log dialing digit analysis is requested for all calls originated by the Redial buffer(s), the local Call Log/ History applications, and all web-based dialing.

## Using enhanced local dialing

For servers running a CM release earlier than 4.0, 9600 Series IP deskphones evaluate a stored phone number (other than those in the Contacts list) based on parameters administered in the settings file. The phone can then automatically prepend the correct digits, saving the user time and effort. This feature is Enhanced Local Dialing. If you correctly configure several important values, you can successfully implement this feature.

For more information, see 9600 Series H.323 customizable system parameters on page 84.

The parameters relevant to the Enhanced Dialing Feature are:

- ENHDIALSTAT: Enhanced dialing status. If set to 1 which is the default value, the enhanced local dialing feature is turned on. If set to 0, enhanced local dialing is off. However, even when the ENHDIALSTAT parameter is used, Using log digit (Smart

Enbloc) dialing on page 131 takes precedence, regardless of the ENHDIALSTAT setting.

- PHNCC: The international country code of the location of the call server. This value is used in conjunction with the PHNIC value to help identify when a call to be dialed that might be an international number. For example, set PHNCC to 1 when the call server is in the United States, to 44 for the United Kingdom, and so on.
- PHNDPLENGTH: The length of internal extension numbers. Used for identifying whether the number to be called is an outside number or an internal line. To identify whether the number to be called is an outside number, the parameter is combined with PHNOL. As long as PHNDPLENGTH is less than the length of a national number (PHNLDLENGTH), the deskphone can determine the difference between the two types of numbers. However, the deskphone cannot determine the type of number when the extension is at least as long as the national deskphone number
- PHNIC: The maximum number of digits, if any, dialed to access public network international trunks. This value is used in conjunction with the PHNCC value to help identify when a call to be dialed might be an international number. The country code is inserted if the number to be dialed includes a plus sign (+) followed by a country code other than the one identified in PHNCC.However, the plus sign is not presented in calling or called party number data and presented only in Web-based click-to-dial links.
- PHNLD: The long distance access code; the digit dialed to access public network long distance trunks. If the number to be dialed is longer than the extension number length and equal in length to PHNLD, the deskphone treats the number as a national number. The long distance access code must precede the number to be dialed. For example, in the United States, a 10 digit number includes the area code and must be preceded by a 1.
- PHNLDLENGTH: The maximum length, in digits, of the national deskphone number for the country in which the call server is located. If the number to be dialed is longer than the extension number and is not equal to PHNLD, the number is treated to be a subset of the national number and the long distance access code is not used.
- PHNOL: The characters dialed to access public network local trunks on the call server. If the number to be dialed is not an extension number, the deskphone presumes it is an outside number which needs to be preceded by the code to access an outside line, commonly a 9.

**Note:**

As with any parameters, the default values are used unless you explicitly administer different values. Thus, if you do not administer a given parameter or if you comment a given parameter out in the 46xxsettings file, the default value for that parameter is used.

**Important:**

In all cases, the values you administer are the values applicable to the location of the call server, that is, the site of the one Enterprise call server that handles multinational locations. For example, if a deskphone is located in London, England but its call server is in the United States, the PHNCC value needs to be set to 1 for the United States. If the call server is in

London, PHNCC would be set to *44* even if the deskphones it serves are in the United States.

**Note:**

In all cases, the digits the deskphones insert and dial are subject to standard Avaya server features and administration such as, Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), and so on. You can administer the system parameter ENHDIALSTAT to turn off the Enhanced Local Dialing feature.. ,

For more information on using the ENHDIALSTAT parameter, see 9600 Series H.323 customizable system parameters on page 84

Example: A corporate voice network has a 4-digit dialing plan. The corporate WML website lists a 4-digit deskphone number as a link on the Human Resources page. A 9620 user selects that link. The 9620 treats the deskphone number is part of the corporate network because the length of the deskphone number is the same as the corporate dialing plan. The deskphone dials the number without further processing.

Example: A user wants to dial an international deskphone number and initiates the call. The deskphone determines the number to be called is from another country code. The deskphone then prepends the rest of the deskphone number with PHNOL to get an outside line and PHNIC to get an international trunk. The deskphone then dials normally with the call server routing the call appropriately.

## Enhanced local dialing requirements

The enhanced local dialing feature is invoked when all the following conditions are met:

- A user invokes the Redial application, the Missed or Answered Call Log, or any Browser-based click-to-dial link to identify a telephone number to dial.
- The Phone application determines a call appearance is available for an outgoing call.
- The current value of ENHDIALSTAT is “1” (On).
- The call server has not indicated it supports smart enbloc dialing. Smart enbloc dialing is call type digit analysis available with Communication Manager Release 4.0 and later.

The Phone application takes the incoming character string, applies an algorithm, and determines the string of digits to be sent to automated call processing (ACP) for dialing. At this point the Phone application goes off-hook and sends the digits to ACP.

**Note:**

The Enhanced Local Dialing algorithm requires that telephone numbers be presented in a standard format.

For information on administering the parameters for the standard format, see 9600 Series H.323 customizable system parameters on page 84. See also Using enhanced local dialing on page 131.

The algorithm also processes the international telephone numbers that are identified, for example in WML Web sites. An international number is indicated by preceding the number with a plus (+) sign, and a space or some non-digit character following the country code.

# About internal audio parameters

The parameter AUDIOENV provides control of some internal audio parameters. Set these values only if absolutely required. In certain situations, particularly noisy environments, Avaya SSE might recommend you to change the AUDIOENV setting to reduce or eliminate the effects environmental noise can have during deskphone use.

The AUDIOENV parameter has a range of 0 to 299. The Set command:

```
SET AUDIOENV 0
```

is the nominal setting (0,0,0,0).

AUDIOENV impacts four internal variables described in the following table:

**Table 14: Internal Audio Variables**

| Variable | Description | Possible Values |
|---|---|---|
| AGC_Dyn_Range | AGC dynamic range. | 0 for a typical office environment (+/-9dB), 1 for +/-12dB, 2 for +/-15dB, and 3 for +/-18 AGC Dynamic range variation. |
| NR_thresh_Hd | The noise reduction threshold for the headset. | The noise reduction threshold for the headset has a default value of 0 for a typical office environment, 1 for call center applications, 2 and 4 for increasingly noisy audio environments, and 3 where noise reduction is disabled. |
| NR_thresh_Hs | The noise reduction threshold for the handset. | The noise reduction threshold for the handset has a default value of 0 for a typical office environment, 1 for call center applications, 2 and 4 for increasingly noisy audio environments, and 3 where noise reduction is disabled. |
| HD_Tx_Gain | Headset transmit gain. | Headset transmit gain has a default value of 0 for normal transmit gain, 1 for +6dB of gain, and 2 for -6dB of gain. |

For more information, see *Audio Quality Tuning for IP Telephones, Issue 2* on www.avaya.com/support.

# Managing applications on the Home screen

You can control the applications that display on the Home screen by configuring the corresponding parameters in the 46xxsettings.txt file. The following table displays the conditions and or parameters that the deskphone requires for certain applications to be displayed on the Home screen.

| Application | Parameter and value | Dependency |
|---|---|---|
| WML applications | WMLHOME.<br>**Note:**<br>If WMLHOME is null, the deskphone screen displays *WML Applications Help icon* by default, You can suppress the display by setting WMLHELPSTAT to 0. | You administer the WML applications in the AvayaMenuAdmin.txt file. The deskphone displays the local WML browser only if the value of WMLHOME is not null and if you have not administered any WML applications.<br>If WMLHOME is null and the value of WMLHELPSTAT is not 1, the deskphone does not display any WML items . |
| World Clock application | WORLDCLOCKAPP | The **WORLD CLOCK** application displays unless WORLDCLOCKAPP is null. |
| Weather application | WEATHERAPP | The **Weather** application displays sunless WEATHERAPP is null. |
| My Pictures | SCREENSAVERON | **My Pictures** displays if and only if SCREENSAVERON is non-null. |
| Calculator | CALCSTAT | The **deskphone displays the Calculator** application unless CALCSTAT is 0. |
| Settings application | N/A | The **Settings** application always displays unless suppressed by OPSTAT. |

| Application | Parameter and value | Dependency |
|---|---|---|
| Greetings | N/A | The **Greetings** program displays only if you configure the following conditions:<br>• AGTGREETINGSTAT has value 1,<br>• CALLCTRSTAT has value 1,<br>• The deskphone has a non-null call center agent ID if an agent has logged into the call center.<br>• The Agent is not in an Available status. No **Manual-In** or **Auto-In** button has the associated LED On.<br>• All call appearances are in the Idle state. |
| User defined contact favorites | N/A | The user can display up to 16 favorites. If the user has set only one contact as favorite, then an item labeled Favorites Help displays after Contacts Favorite. Favorites Help is unavailable if a temporary contacts list from a USB flash drive is in use.<br>**Note:**<br>If the system suppresses the backups when BRURI is null, then the user loses the Favorites and all other Contacts when the user logs out. If the administrator has set APPSTAT to a value other than 1, the user cannot make changes to Contacts, so the administrator might prepopulate Contacts, and enable or disable entries to display the contacts as Favorites or not. |

# Administering features on softkeys

Release 2.0 onwards, you can administer call server features on softkeys on the deskphhone. The number of features you can place on a set of softkeys depends on the call state the deskphone is presenting to the user.

The chart below lists the call states for which you can administer softkeys, the relevant system parameter associated with a call state, the maximum number of features you can specify in that system parameter, and the softkey numbers that can take administered features.

| Call State | System Parameter | Maximum number of features allowed | Available Softkeys |
|---|---|---|---|
| Idle | IDLEFEATURES | 6 | All softkeys |
| Dialing | DIALFEATURES | 5 | 1, 3, & 4 |
| Active with ringback | RINGBKFEATURES | 3 | 3 |
| Active with talk path | TALKFEATURES | 3 | 4 |

**Note:**

For more information about the system parameters, see 9600 Series H.323 customizable system parameters on page 84.

Administration of softkeys works as follows:

- Administer feature buttons for the deskphone on the call server as you normally would, and the call server sends these button assignments to the deskphone as it always has.
- In the 46xxsettings file, administer any or all of the system parameters indicated in the chart above. Each parameter consists of a list of one or more feature numbers, up to the maximum indicated in that chart, with each feature number corresponding to a specific administrable feature. CM Feature Numbers for Assigning Softkeys on page 139 lists the administrable features and their associated numbers.
- The deskphone compares the list of features administered on the call server with the list of features in the system parameters administered. If a given feature occurs both in call server administration and in a given system parameter, that feature is displayed on a phone application softkey when the highlighted call appearance is in the associated call state. The deskphone displays the feature buttons starting with Softkey 1 and continuing to the right in the order specified in the system parameter, subject to the availability of features and softkeys as listed in this section.

  Example:

  Consider a scenario where call server administration includes the Send All Calls and Directory features. If the system parameter IDLEFEATURES is not administered, the

corresponding softkeys are labeled from left to right as follows when a highlighted call appearance is Idle:

| | | | |
|---|---|---|---|
| Redial | Send All | (blank) | (blank) |

However, when the system parameter IDLEFEATURES is administered to be “26,1000,35” the corresponding softkeys are labeled from left to right as follows when a highlighted call appearance is Idle:

| | | | |
|---|---|---|---|
| Directory | Redial | Send All | (blank) |

Softkeys available to be labeled with feature buttons as indicated under Available Softkeys in the chart are those that are not dedicated to a higher priority function. For example, in the “Active with a talk path” call state, the softkeys for Hold, Conference, and Transfer are dedicated to those functions and cannot be displaced by an administrable feature button, while the softkey normally labeled Drop (softkey #4) can be used for an administrable feature button.

In addition to the administrable feature numbers listed in CM Feature Numbers for Assigning Softkeys on page 139, you can specify three additional *features* on a softkey of your choice or can completely replace the existing features. In the case of the system parameters IDLEFEATURES or DIALFEATURES, if the list of feature numbers includes the value 1000, the corresponding softkey is reserved for the Redial feature local to the deskphone. This means the corresponding softkey is labeled Redial if the deskphone has at least one phone number stored for the Redial feature. Otherwise the softkey is unlabeled. In the case of the system parameter IDLEFEATURES, if the list of feature numbers includes the value 1100, the corresponding softkey is reserved for a *Backlight Off* icon. When you press this softkey, the backlight of the deskphone turns off, saving energy. The backlight is turned on automatically when an phone activity is detected, such as an incoming call or a button press by the user.

If the list of feature numbers includes the value 1200, the corresponding softkey is reserved for a *Log Off* button, regardless of the value of OPSTAT. When pressed, this softkey presents the *Log Out Confirmation Screen*, and the user can either confirm the logout process, or cancel it and return to the Phone Screen.

For IDLEFEATURES or DIALFEATURES, if the system parameter PHNEMERGNUM is administered, the third softkey in the Idle or Dialing call state will always be labeled *Emerg* regardless of the contents of those system parameters.

Features administered only for any SBM24 button module are ignored. The feature must be administered for the deskphone and not the button module.

Primary call appearances, bridged call appearances, and Team Buttons cannot be administered on softkeys.

The feature button softkey labels displayed to the user are those downloaded from the call server. If the user has personalized the labels, the deskphone displays the personalized labels.

If one of the designated parameters contains a Feature number more than once, and that number corresponds to at least one occurrence of a feature button downloaded from the call

server, the designation of softkeys to features is assigned in the order the features are listed. For example, if two Abbreviated Dial (AD) buttons (Feature Number 65) are listed in the DIALFEATURES parameter, the first AD button in that list is associated with the first AD button downloaded from the call server. The second AD button in the DIALFEATURES parameter is associated with the second AD button downloaded from the call server (if any), and so on.

**Note:**

Using the system parameters, you can specify more features than can be displayed on any one deskphone. For example, using the IDLEFEATURES, you can specify up to six features, although any one deskphone can display at most four of them. Using the maximum size of each parameter, you can specify one comprehensive list for that parameter's related call state, but allow your user community to see different feature buttons depending on how you administer their deskphones. Since the deskphone only displays feature button labels for features administered on the call server, you can set the softkey feature system parameters to values that correspond to features for some users, but not others. For example, if TALKFEATURES is administered to "325,50", the users having Conference Display administered would see that label on softkey #3 for the Active with talk path call state, but users with Attendant Release would instead see that label on softkey #3. Because softkey labels display in the order in which they are administered in the system parameter, a user with both Conference Display and Attendant Release would only see a Conference Display softkey.

The Feature Numbers are as follows.

**Table 15: CM Feature Numbers for Assigning Softkeys**

| Feature Name | Default Label | Feature Number |
|---|---|---|
| abr-prog | AbbrvDial Program | 67 |
| abr-spchar | AbrvDial (char) | 68 |
| abrv-dial | AD | 65 |
| abrv-ring | AR | 226 |
| ac-alarm | AC Alarm | 128 |
| aca-halt | Auto-Ckt Assure | 77 |
| account | Acct | 134 |
| act-tr-grp | Cont Act | 46 |
| admin | Admin | 150 |
| after-call | After Call Work | 91 |
| alrt-agchg | Alert Agent | 225 |
| alt-frl | Alt FRL | 162 |
| ani-requst | ANI Request | 146 |

| Feature Name | Default Label | Feature Number |
|---|---|---|
| assist | Assist | 90 |
| asvn-halt | asvn-halt | 214 |
| atd-qcalls | AQC | 89 |
| atd-qtime | AQT | 88 |
| audix-rec | Audix Record | 301 |
| aut-msg-wt | Message (name or ext) | 70 |
| auto-cbk | Auto Callback | 33 |
| auto-icom | Auto (name or ext) | 69 |
| auto-in | Auto In | 92 |
| auto-wkup | Auto Wakeup | 27 |
| autodial | Autodial | 227 |
| aux-work | Auxiliary Work | 52 |
| btn-ring | Button Ring | 258 |
| btn-view | Button View | 151 |
| busy-ind | Busy | 39 |
| call-disp | Make Call | 16 |
| call-fwd | Call Forwarding | 74 |
| call-park | Call Park | 45 |
| call-pkup | Call Pickup | 34 |
| callr-info | Caller Info | 141 |
| call-timer | Ctime | 243 |
| cancel | Cancel | 51 |
| cas-backup | CAS Backup | 76 |
| cdr1-alrm | CDR 1 Failure | 106 |
| cdr2-alrm | CDR 2 Failure | 117 |
| cfwd-bsyda | Call Forwarding bsyda (ext) | 84 |
| cfwd-enh | Call Forwarding Enhanced | 304 |
| check-in | Check In | 29 |
| check-out | Check Out | 28 |
| class-rstr | COR | 59 |
| clk-overid | Clocked Override | 112 |

| Feature Name | Default Label | Feature Number |
|---|---|---|
| conf-dsp | Conference Display | 325 |
| con-stat | Console Status | 185 |
| consult | Consult | 42 |
| cov-cback | Coverage Callback | 17 |
| cov-msg-rt | Cover Msg Retrieve | 12 |
| cpn-blk | CPN Block | 164 |
| cpn-unblk | CPN Unblock | 165 |
| crss-alert | Crisis Alert | 247 |
| cw-ringoff | CW Aud Off | 62 |
| date-time | Date Time | 23 |
| deact-tr-g | Cont Deact | 47 |
| delete-msg | Delete Message | 14 |
| dial-icom | Dial Icom | 32 |
| did-remove | DID Remove | 276 |
| did-view | DID View | 256 |
| directory | Directory | 26 |
| dir-pkup | Directory Pkup | 230 |
| disp-chrg | Display Charge | 232 |
| display | Display | 180 |
| disp-norm | Local/Normal | 124 |
| dn-dst | Do Not Disturb | 99 |
| dont-split | Don’t Split | 176 |
| dtgs-stat | DTGS Status | 181 |
| ec500 | Extension to Cellular | 335 |
| em-acc-att | Emerg Access to Attd | 64 |
| exclusion | Exclusion | 41 |
| ext-dn-dst | Do Not Disturb Ext. | 95 |
| extnd-call | Extend Call | 345 |
| fe-mute | Far End Mute for Conf | 328 |
| flash | Flash | 110 |
| forced-rel | Forced Release | 57 |

| Feature Name | Default Label | Feature Number |
|---|---|---|
| goto-cover | Go To Cover | 36 |
| group-disp | Group Display | 212 |
| group-sel | Group Select | 213 |
| grp-dn-dst | Do Not Disturb Grp | 96 |
| grp-page | GrpPg | 135 |
| headset | Headset | 241 |
| hundrd-sel | Group Select # | 58 |
| hunt-ne | Hunt Group | 101 |
| in-call-id | Coverage (Info) | 30 |
| in-ringoff | In Aud Off | 60 |
| inspect | Inspect Mode | 21 |
| int-aut-an | IntAutoAns | 108 |
| intrusion | Intrusion | 179 |
| last-mess | Last Message | 182 |
| last-numb | Last Number Dialed | 66 |
| last-op | Last Operation | 183 |
| lic-error | License Error | 312 |
| limit-call | LimitInCalls | 302 |
| link-alarm | Link Failure (#) | 103 |
| local-tgs | Local-tgs (#) | 48 |
| lsvn-halt | Login SVN | 144 |
| lwc-cancel | Cancel LWC | 19 |
| lwc-lock | Lock LWC | 18 |
| lwc-store | LWC | 10 |
| maid-stat | Maid Status | 209 |
| major-alrm | Major Hdwe Failure | 104 |
| man-msg-wt | Msg Wait (name or ext.) | 38 |
| man-overid | Immediate Override | 113 |
| manual-in | Manual In | 93 |
| mct-act | MCT Activation | 160 |
| mct-contr | MCT Control | 161 |

| Feature Name | Default Label | Feature Number |
|---|---|---|
| mf-da-intl | Directory Assistance | 246 |
| mf-op-intl | CO Attendant | 229 |
| mj/mn-alrm | Maj/Min Hdwe Failure | 82 |
| mm-basic | MM Basic | 169 |
| mm-call | MM Call | 167 |
| mm-cfwd | MM CallFwd | 244 |
| mm-datacnf | MM Datacnf | 168 |
| mmi-cp-alm | MMI Circuit Pack Alarm | 132 |
| mm-multnbr | MM MultNbr | 170 |
| mm-pcaudio | MM PCAudio | 166 |
| msg-retr | Message Retrieve | 11 |
| mwn-act | Message Waiting Act. | 97 |
| mwn-deact | Message Waiting Deact. | 98 |
| next | Next | 13 |
| night-serv | Night Serv | 53 |
| noans-alrt | RONA | 192 |
| no-hld-cnf | No Hold Conference | 337 |
| normal | Nornal Mode | 15 |
| occ-rooms | Occ-Rooms | 210 |
| off-bd-alm | Offboard Alarm | 126 |
| override | Attndt Override | 178 |
| per-COline | CO Line (#) | 31 |
| pms-alarm | PMS Failure | 105 |
| pos-avail | Position Available | 54 |
| pos-busy | Position Busy | 119 |
| post-msgs | Post Messages | 336 |
| pr-awu-alm | Auto Wakeup Alm | 116 |
| pr-pms-alm | PMS Ptr Alarm | 115 |
| pr-sys-alm | Sys Ptr Alarm | 120 |
| print-msgs | Print Msgs | 71 |
| priority | Priority | 81 |

| Feature Name | Default Label | Feature Number |
|---|---|---|
| q-calls | NQC | 87 |
| q-time | OQT | 86 |
| release | Attendant Release | 50 |
| release | Station Release | 94 |
| remote-tgs | Remote TG (#) | 78 |
| re-ringoff | Ringer Reminder | 61 |
| ringer-off | Ringer Cutoff | 80 |
| rs-alert | System Reset Alert | 109 |
| rsvn-halt | rsvn-halt | 145 |
| scroll | Scroll | 125 |
| send-calls | Send All Calls | 35 |
| send-term | Send All Calls-TEG | 72 |
| serial-cal | Serial Call | 177 |
| serv-obsrv | Service Observing | 85 |
| signal | Signal (name or ext.) | 37 |
| split | Split | 56 |
| split-swap | Split-swap | 191 |
| ssvn-halt | ssvn-halt | 231 |
| sta-lock | Station Lock | 300 |
| start | Start Call | 55 |
| stored-num | Stored Number | 22 |
| stroke-cnt | Stroke Count (#) | 129 |
| term-x-gr | Term Grp (name or ext.) | 40 |
| togle-swap | Conf/Trans Toggle-Swap | 327 |
| trk-ac-alm | FTC Alarm | 121 |
| trk-id | Trunk ID | 63 |
| trunk-name | Trunk Name | 111 |
| trunk-ns | Trunk Group | 102 |
| usr-addbsy | Add Busy Indicator | 239 |
| usr-rembsy | Remove busy Indicator | 240 |
| uui-info | UUI-Info | 228 |

| Feature Name | Default Label | Feature Number |
|---|---|---|
| vc-cp-alm | VC Circuit Pack Alarm | 133 |
| verify | Verify | 75 |
| vip-chkin | VIP Check-in | 277 |
| vip-retry | VIP Retry | 148 |
| vip-wakeup | VIP Wakeup | 147 |
| vis | vis | 184 |
| voa-repeat | VOA Repeat | 208 |
| voice-mail | Message | 326 |
| vu-display | VuStats # | 211 |
| whisp-act | Whisper Page Activation | 136 |
| whisp-anbk | Answerback | 137 |
| whsp-off | Whisper Page Off | 138 |
| work-code | Work Code | 140 |

# Administering a custom screen saver

Avaya provides a standard screen saver. However, you can administer a customized screen saver for 9600 Series IP deskphones with bit-mapped displays. The screen saver displays when the idle timer reaches the value set in the system parameter SCREENSAVERON. The screen saver is removed whenever the idle timer is reset. If the value of SCREENSAVERON is “0”, neither the standard Avaya screen saver nor any customized screen saver you specify in the SCREENSAVER system parameter is displayed.

The deskphones display the screen savers for approximately 5 seconds at a time at random locations on the screen, such that the entire image is always displayed. When the screen saver is removed, the previously displayed screen is restored unless another screen is appropriate due to a specified software operation such as making a call from the Phone screen.

You can administer color images for gray-scale sets or black and white images for color sets. The deskphone will present the images as applicable for their individual displays.

To determine what image to display, the deskphone adheres to this procedure:

1. During boot-up, the deskphone checks for the file named in the system parameter SCREENSAVER. If found, the deskphone checks that file for valid jpeg format, and to verify that the screen saver image height and width do not exceed the specifications: The applicable full screen pixel count is 160x160 for a 9610, 160x320 for a 9620, or 320x240 for a 9630, 9640 or 9650, or 480x640 for a 9670G IP

deskphone. Note that the screen saver should be a smaller size than these pixel values specified so it can move randomly while displaying the entire image.

2. If a valid file was not downloaded, either because no file exists, or because the downloaded file exceeded one or more of the pixel count limits, or because the image is not a valid JPEG image, the deskphone uses the Avaya-specific screen saver.

Use the SCREENSAVER parameter is to administer different file names in the 46xxsettings file, listed under different MODEL4 values, 9620, 9630, and other deskphones. Or use the MODEL4 IF statements to administrator a given deskphone to point to a unique SCREENSAVER value that is appropriate for that deskphone.

# About administering audio equalization

The Federal Communication Commission (a branch of the US Government) in its Part 68 standard, has made Hearing Aid Compatibility (HAC) a mandatory requirement. The HAC feature is an alternative way to provide audio equalization on a handset, from the acoustic standards specified in TIA-810/920 and S004, and may be of benefit to some users of t-coil capable hearing aids.

Release 6.2 onwards, the 9600 Series IP deskphones support the ability to choose either of these standards. Because individual organizations and users differ in how they might want to implement this choice, the deskphone provides 3 ways to specify the desired audio equalization:

- **Settings File**: The administrator can set ADMIN_HSEQUAL. The default value, 1, specifies Handset equalization that is optimized for acoustic TIA 810/920 performance unless otherwise superseded by Local Procedure or User Option. The alternate value, 2, specifies HAC.
- **Local Procedure**: When users are denied access to Options for administrative reasons, but individual users need an equalization value other than the one in the settings file, the HSEQUAL Local Procedure as documented in the *Installing and Maintaining Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G* for 9608, 9611G, 9621G, and 9641G deskphones provides another method to administer the deskphone with the audio equalization value that you require. “Default” uses the settings file value unless superseded by User Option. “Audio Opt.” is optimized for TIA-810/920 acoustic performance, and “HAC Opt.” is optimized for HAC telecoil performance.
- **User Option**: The user can select “Default” by which the deskphone uses the settings file value unless superseded by Local Procedure), “Audio Opt.” which uses Handset equalization that is optimized for acoustic TIA 810/920 performance, or “HAC Opt.” which uses Handset equalization that is optimized for electrical FCC Part 68 HAC telecoil performance.
- Handset equalization options are effected in the following order:

a. The deskphone uses the User Option value if selected and saved.
b. If a Local Procedure value was selected and saved, the deskphone uses the local Procedure value.
c. If a Settings file value is specified and saved the deskphone uses that value.
d. If none of the above options are set, the deskphone uses Handset equalization that is optimized for TIA-810/920 acoustic performance.

**Note:**

The options **Default**, **Audio Opt** and **HAC Opt** that are available for Handset equalization are mutually exclusive, meaning only one can be activated at a time.

# Administering deskphones for call center operation

As of H.323 software Release 6.1, the 9608, 9611G, 9621G, and 9641G H.323 deskphone models can be used in call centers. Perform the appropriate call center administration on the call server. You can administer the agent sign-in using several methods. However, each mode has certain implications for the end user. For more information, see Administering agent sign in for call centers on page 148.

Use the 46xxsettings file to customize any applicable deskphone parameters associated with call center operations. These parameters allow agent access to different options and functions, as follows:

- AGTCALLINFOSTAT - Provides agent access to automatic caller information.
- AGTFWDBTNSTAT - Prevents agents from forwarding calls while signed in.
- AGTGREETINGSTAT - Gives an agent permission to record or select a greeting.
- AGTLOGINFAC - Indicates which Feature Access Code agents must dial to sign in to the call center.
- AGTSPKRSTAT - Allows or disallows agents from disabling the speakerphone.
- AGTTIMESTAT - Displays the time and date on the top display line.
- AGTTRANSLTO -Determines the proper Agent Information message regarding an incoming call.
- AGTTRANSCLBK - Determines the proper Agent Information message regarding an incoming call.
- AGTTRANSLPRI - Determines the proper Agent Information message regarding an incoming call.
- AGTTRANSLPK - Determines the proper Agent Information message regarding an incoming call.

- AGTTRANSLICOM - Determines the proper Agent Information message regarding an incoming call.
- CALLCTRSTAT - Provides agent access to call center features for the phone, including Greetings.
- OPSTATCC - Overrides the OPSTAT parameter setting to allow agent access to related Options & Settings. It specifies whether Call Center options such as Greetings will be presented to the user even if the value of OPSTAT is set to disable user options

For more information about each new parameter, see 9600 Series H.323 customizable system parameters on page 84.

For additional information on agent and call centers using these deskphones with software Release 6.2, see the *Using Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G in the Call Center*, 16-603613.

**Related topics:**

Administering agent sign in for call centers on page 148
Call Center backup files on page 149
Administering the Vu display button on page 150

# Administering agent sign in for call centers

End users access a call center by first logging into the deskphone with their User ID and extension which is the same as normal deskphone login and then entering their Agent ID and optional password to sign in to the call center. You can administer Agent sign in in several ways. Each method has certain implications for the end user as described below.

- Administer a FAC: Administer a Feature Access Code (FAC), for example, FAC #94. The deskphone requires an Agent ID to create and store Greetings on the http server. Thus, entering the Agent ID using an FAC is the most reliable method where the deskphone can display the Agent ID on the Top line and allow station of the agent to retrieve stored greetings or create and backup their own greetings. After administering the FAC on the call server, set the parameter AGTLOGINFAC in the 46xxsettings file to indicate which Feature Access Code you want agents to use to sign in to the call center.
- Administer a Feature button: Administer a Feature button labeled “Sign in”, or “Agent ID,” or another descriptive label that indicates entry of the Agent ID is required. This method might prevent the deskphone from displaying the Agent ID on the Top line. It might also prevent the agent from retrieving or backing up greeting files that are store on the server.
- Configure a Vu display button: For Remote login or CTI login, to utilize the agent greeting functions, administer a FAC for Feature Button Agent login or a CTI login. For more information, see Administering the Vu display button on page 150.

For more information on administering Feature buttons, see Administering features and CAs for all other IP deskphones on page 57.

- Administer a Softkey: Administer a softkey with a descriptive label that indicates Agent ID entry is required. See Administering features on softkeys on page 137 for more information.

The sign in method you administer applies regardless of how you set the AGTGREETINGSTAT parameter.

The *9608/9611G and 9621G/9641G H.323 Call Center User Guide* , 16-603613 includes a description on Agent sign in using a FAC but cautions users that the supervisor might instruct them to use an alternate sign in procedure.

## Call Center backup files

You can use the BRURI parameter to backup and retrieve generic user data as well as specific call center data. If all the following conditions are true, then whenever an agent logs in to the call center, the deskphone automatically attempts to retrieve a file labeled agentID_CCdata.txt with agentID being the Agent ID of the agent. This file is based not on the user extension, like the generic backup file, but on the Agent ID:

- BRURI is non-null
- CALLCTRSTAT has value 1
- AGTGREETINGSTAT has value 1

The first time the agent logs in, this retrieval attempt will fail, because the agent has not recorded any greetings yet. The agent will see an error screen with the message, *No Greetings file found. Press Create to create a greeting now, or press Back to create a greeting later.* After the agent creates, modifies, or deletes a greeting, the data is automatically updated in the location specified by BRURI, subject to standard backup or restore specifications, as indicated in the next section.

When the agent creates, modifies, or deletes a greeting, the following files might be affected:

- agentID_CCdata.txt. This file contains the following data about each greeting:
  - GREETINGLBLx is set to the Label specified by the agent for the x’th greeting
  - GREETINGFILEx is set to “agentID_x.wav” (with agentID and x as applicable)
  - GREETINGDURx is set to the Duration of the recorded greeting
  - GREETINGTYPEx is set to the numerical value of the selected type and match criterion. This is a numerical code used by deskphone software to track the Type and Match Criterion for the greeting.
  - GREETINGDATAx is set to the string that invokes this greeting (which may be non-numeric), if applicable for the greeting Type.

- GREETINGCHKSUMx is set to the checksum of the associated .wav file.

• agentID_x.wav where x is the x'th greeting for the specific agent.

## Administering the Vu display button

Sometimes, even though you carry out the relevant procedures, the deskphone cannot derive the Agent ID of the agent. This scenario occurs when the agent provides a password when logging into the call center, and the deskphone is unable to distinguish the ID from the password. In this environment, you must use the AGTIDVUSTAT parameter.

When AGTIDVUSTAT has its default value of 0, the following procedure is ignored.

When this Vu-display button is administered for your agents, instruct them to press the associated feature button immediately after logging into the call center, if the deskphone does not display their Agent ID in the middle of the Top Line. Pressing the Vu-display button causes the call server to send the Agent ID to the deskphone.

When the agent logs in through abbreviated dial or CTI, the deskphone virtually presses the Vu-display button upon login. If the agent is logged in and the Agent ID is not displayed on the top line, pressing the Vu-display button does not populate the Agent ID at the top of the display when the Agent ID is not present. The agent ID is only populated on the top line through the Vu-display button when the button is virtually pressed upon login.

### Procedure

1. On the Communication Manager, create a unique vustats-display-format.

   Example: Change vustats-display-format *x* where x is an available Vu-stats format number.

2. In the *Change vustats-display-format* form, you must configure the following fields as follows:

   • Next format number: None

   • Data Field: $

   • Number of Intervals: Leave Blank

   • Object Type: agent

   • Update Interval: no-update

   • On Change? N

   • Display Interval: 5

   • Format Discription: ID: $$$$$$$$$$$$ $$$$$$$$$ $$

   • Data Type:

i. agent-extension— Format: Leave Blank— Period: Leave Blank— Threshold: Leave Blank— RC: Leave Blank— Ref: Leave Blank

ii. agent-state— Format: Leave Blank— Period: Leave Blank— Threshold: Leave Blank— RC: Leave Blank— Ref: Top

iii. current-reason-code— Format: Leave Blank— Period: Leave Blank —Threshold: Leave Blank— RC: Leave Blank— Ref: Leave Blank

3. Save the entries.
4. Add a Vu-display button with the format *x* previously created to each station that it going to utilize any type of agent login other than FAC login.

   You can administer the button any available button position on the deskphone.
5. Edit the 46xxxsettings file on the server and add SET AGTIDVUSTAT *x*.
6. Save the 46xxxsettings file.
7. Reboot the phone so the changes made on the settings file are applied to the deskphone.

**Caution:**

Do not use an equal sign as part of the vustats-display. For example, do not use the format "ID=...". If you do so, the deskphone might interpret the Vu-stats message as a call appearance message, and the message might not be displayed properly to the user.

# Ringing on wireless headset

Ringing on wireless headsets from Jabra and Plantronics can be configured by the administrator and is supported as of Release H.323 6.2 Service Pack 2. Using this feature, you can enable ringing on the wireless headset in addition to the speaker. The ringing tone on the speaker may be turned off using the AUDASYS parameter.

**Note:**

By default, this feature is set to 0 and is disabled. For deskphones that are used without wireless headset with the bidirectional interface support this feature must be turned off.

To enable this feature, SET HEADSETBIDIR=1 in the 46xxsettings file.

When the base unit is powered on, either one of the following scenarios might occur:

- When the user goes off-hook with the headset or change from a non-headset device to the headset, the wireless headset is activated.
- When the user goes on-hook on the deskphone with an activated headset or change from wireless headset device to non-headset, the wireless headset is deactivated.

# Configuring phone based auto-answer

You can configure the auto-answer feature through the settings file now. Earlier, you could configure auto-answer through the Communication Manager only. For an incoming call, the auto-answer feature plays a zip tone to alert the agent and automatically activates the headset button and answers the call.

**Note:**

The deskphone plays the zip tone only for the deskphone user and the caller cannot hear it, also, the phone user cannot hear any audio from the caller until the zip tone completes.

For a number having bridged call appearances, you can configure the response of the auto-answer feature for an incoming call based on settings for new parameters AUTOANSSTAT and AUTOANSSTRING. You can also specify whether the deskphone will alert audibly with auto-answering calls using AUTOANSALERT.

You can also configure auto-answer for the incoming call, based on the numbers having a fixed VDN name. You can configure auto-answer not to occur for calls arriving from unidentified numbers or DIDs.

You can configure these parameters in the 46xxsettings file.

### AUTOANSSTAT

Parameter name and default value: AUTOANSSTAT ('0')

Valid values: 1 ASCII numeric digit, '0' through '4'

Usage: Specifies whether the deskphone will auto-answer incoming calls or not.

**Note:**

AUTOANSSTAT is independent of any call center parameter or status, it functions regardless of whether an agent is logged in or not.

### AUTOANSSTRING

Parameter Name and (default value): AUTOANSSTRING('')

Valid Values: 0-15 ASCII characters

Usage: Specifies the VDN to be matched for auto-answering incoming calls.

### AUTOANSALERT

Parameter Name and (default value): AUTOANSALERT ('0')

Valid Values: 1 ASCII numeric digit, '0' and '1'

Usage: Specifies whether the deskphone will audibly alert with auto-answering calls.

**Note:**

If AUTOANSALERT is 0, the deskphone will not provide audible alerting when auto-answering a call, regardless of any other setting (e.g. AUDASYS). Similarly if AUTOANSALERT is 1, the deskphone will provide audible alerting when auto-answering a call, if and only if the phone is administered to provide audible alerting at all, for example by user Volume setting.

## Scenarios addressed using the parameters

You can configure these parameters to address the following scenarios for an incoming call on primary appearance A and a bridged appearance B:

**Note:**

To avoid conflicts when using Phone-based conditional auto-answer, configure auto-answer settings on CM to none.

**Table 16: Parameter values and results**

| Value of AUTOANSSTAT | Value of AUTOANSSTRING | Resulting scenario |
|---|---|---|
| 0 | Specified or null value | The deskphones do not auto-answer the call. |
| 1 | Null value | Auto-answer is attempted on both primary and bridged call appearances (BCAs), and CM will adjudicate any race condition. |
| 1 | Specified and matches the VDN | Auto-answer is attempted on both primary call appearances (PCAs) and BCAs, and CM will adjudicate any race condition. |
| 1 | Specified but does not match VDN | No auto-answer on either PCAs or BCAs. |
| 2 | Null | Auto-answer is attempted on PCAs but not BCAs |
| 2 | Specified and matches the VDN | Auto-answer is attempted on PCAs but not BCAs. |

| | | |
|---|---|---|
| 2 | Specified and does not match VDN | No auto-answer on either PCAs or BCAs. |
| 3 | Not specified | Auto-answer is attempted on both PCAs or BCAs only for deskphones used by an agent logged into a call center (regardless of status such as Ready, Aux Work, etc. |
| 3 | Specified and matches VDN | Auto-answer is attempted on both PCAs or BCAs only for deskphones used by an agent logged into a call center (regardless of status such as Ready, Aux Work, etc.) |
| 3 | Specified and does not match VDN | No auto-answer on either PCAs or BCAs. |
| 4 | Not specified | Auto-answer is attempted on PCAs only and only for deskphones used by an agent logged into a call center (regardless of status such as Ready, Aux Work, etc.) |
| 4 | Specified and matches VDN | Auto-answer is attempted on PCAs only and only for deskphones used by an agent logged into a call center (regardless of status such as Ready, Aux Work, etc.) |
| 4 | Specified and does not match VDN | No auto-answer on either PCAs or BCAs. |

**Note:**

To prevent the condition where both a primary and bridged call appearance (on two separate deskphones) auto-answer an incoming call, you should use either of the following approaches, as applicable to your environment:

- Put the deskphones that you want to auto-answer in a GROUP with AUTOANSSTAT set to 1 (or any other applicable value), and put the other deskphones in a different GROUP with AUTOANSSTAT set to 0. The first Group will auto-answer the call as applicable, and the second Group will never auto-answer the call.
- Set AUTOANSSTAT to 2 for all deskphones so that only the primary call appearances auto-answer calls.

# Administering backup and restore

**Note:**

This section does not apply to the 9610 IP deskphone. For 9610 backup and restore information, see Special Administration for the 9610 IP Telephone on page 168.

9600 Series IP deskphones support the HTTP client to back up and restore the user-specific data indicated in User data saved during backup on page 157. Release 1.5, onwards, HTTP over TLS (HTTPS) is also supported for backup or restore. For backup, the deskphone creates a file with all the user-specific data if a backup file location is specified in system parameter BRURI. The file is sent to the server by an HTTP PUT message, with appropriate success or failure confirmation.

For restore, the initiating process must supply only the backup file name. The file is requested from the server by an HTTP GET message. If successful, the file is returned to the initiating process. Otherwise a failure message is returned.

Backup and restore operations construct the URI used in the HTTP message from the value of the BRURI parameter and from the file name as follows:

- If BRURI ends with a / (a forward slash), the file name is appended.
- Otherwise, a forward slash and the file name is appended to the BRURI value.

**Note:**

BRURI can include a directory path and/or a port number as specified in IETF RFCs 2396 and 3986.

If you use TLS, the call server registration password for the phone must be included in an Authorization request-header in each transmitted GET and PUT method. This is intended for use by the Avaya IP Telephone File Server Application (which can be downloaded from the Avaya support Web site) so that the phone requesting the file transaction can be authenticated.

If no digital certificates are downloaded based on the system parameter TRUSTCERTS, the phone establishes a TLS connection only to a backup/restore file server that has a Avaya-signed certificate, included by default with the Avaya IP Telephone File Server Application, and includes the credentials. However, if at least one digital certificate has been downloaded based on TRUSTCERTS, the credentials are included only if BRAUTH is set to 1. This is a security feature to allow control over whether the credentials are sent to servers with third-party certificates. If the server on which the Avaya IP Telephone File Server Application is installed uses a non-Avaya certificate, set BRAUTH to 1 to enable authentication of the deskphones. The default value of BRAUTH is 0.

When the call server IP address and the registration password of the phone are included as the credentials in an Authorization request-header, the call server IP address is included first

in dotted-decimal format, followed by a colon, hex 3A, followed by the registration password of the phone.

HTTP/HTTPS authentication is supported for both backup and restore operations. The authentication credentials and realm are stored in re-programmable, non-volatile memory, which is not overwritten when new phone software is downloaded. Both the authentication credentials and realm have a default value of null, set at manufacture or at any other time user-specific data is removed from the phone. When TLS is used, the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is used for authentication. If the digital certificate of the server is signed by the Avaya Product Root Certificate Authority certificate, the call server registration password of the phone is included as the credentials in an Authorization request-header for each transmitted PUT (backup) and GET (for restore) method.

New values replace the currently stored authentication and realm values:

- When HTTP authentication for backup or restore succeeds and
- If the userid, password, or realm used differs from those currently stored in the phone

If HTTP authentication fails, the user is prompted to enter new credentials.

**Note:**

Users can request a backup or restore using the Advanced Options Backup/Restore screen, as described in the user guide for their specific deskphone model.

For specific error messages relating to Backup/Restore, see the *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*.

**Related topics:**

Backup file formats on page 156
User data saved during backup on page 157
About restore on page 159

# Backup file formats

When the system parameter BRURI is non-null, user changes are automatically backed up to the file *ext*_96xxdata.txt (where *ext* is the extension number of the deskphone) on the HTTP server to a user-specified directory. The backup formats are as follows:

**Table 17: Backup File Formats**

| Item/Data Value | Format |
|---|---|
| Generic | *name=value* |
| Contacts | ABKNAME*mmm*=ENTRY_NAME<br>ABKNUMBER*mmm*=ENTRY_NUMBER_1<br>ABKTYPE*mmm*=ENTRYT_TYPE |

| Item/Data Value | Format |
|---|---|
| | (where *mmm* is the one-, two-, or three-digit entry ID, with leading zeros for single and double-digit entry IDs) |
| Call Log entries | CLNAME*mmm*=ENTRY_NAME<br>CLNUMBER*mmm*=ENTRY_NUMBER<br>CLTYPE*mmm*=ENTRY_TYPE<br>CLDATE*mmm*=ENTRY_DATE<br>CLTIME*mmm*=ENTRY_TIME<br>CLDURATION*mmm*=ENTRY_DURATION<br>CLBRIDGEDFLAG*mmm*=ENTRY_BRIDGEDFLAG<br>CLMISSEDCNTR*mmm*=ENTRY_COUNTER<br>CLBCALBL*mmm*=ENTRY_BCALBL<br>To be valid, a Call Log entry must have at least a non-null Date and Type, and either Name or Number or both must be non-null. |
| User-generated Call Appearance labels with button identifiers of *mm* where *mm* is the one- or two-digit button number of the entry with a lead zero for single-digit numbers. | PHNLABEL*mm*=CAUSERLABEL |
| User-generated deskphone Feature Button labels with button identifiers of *mm*, where *mm* is the one- or two-digit button number of the entry with a lead zero for single-digit numbers. | PHNLABEL*mm*=FBUSERLABEL |
| User-generated SBM24 Call Appearance or Feature Button labels with button identifiers of *mm*, where *mm* is the one- or two-digit button number of the entry with a lead zero for single-digit numbers. | SBMLABEL*mm*=CAUSERLABEL or FBUSERLABEL, as applicable |

# User data saved during backup

A backup saves the options and non-password parameters. The parameter and the applicable settings are shown in the following table.

**Table 18: Options and non-password parameters saved during backup**

| Parameter Name | Setting |
|---|---|
| HOMEFAV*nn* | Contact Favorites data. Applicable to touchscreen phones only. An entry is backed up |

| Parameter Name | Setting |
|---|---|
| | for each Home screen favorite, where *nn* is the index number for that favorite. The backup file format for a Favorite is: HOMEFAV*nn*=*Fav_Number*<US>*Fav_Caption*<US>*Contact_Name* where Fav_Number is the phone number associated with the Favorite, Fav_Caption is the Favorite's caption text, Contact_Name is the Name for the associated Contact entry, and <US> is the Unit Separator (0x001F Unicode value). Upon Restore, a link must be established between a Favorite and a Contact entry by matching the Contact_Name against a Contact's Name and Fav_Number against one of that Contact's numbers. If no match is found, then the Favorite cannot be restored and is discarded. |
| HEADSETBIDIR | Full support of wireless headset that includes on/off-hook control |
| USER_HSEQUAL | User-specified handset audio equalization standard |
| LANGUSER | Display Language |
| LOGACTIVE | Call Log Active |
| LOGBRIDGED | Log Bridged Calls |
| LOGTDFORMAT | Call Log Data Time/Date Format |
| OPTAGCHAND | Handset Automatic Gain Control |
| OPTAGCHEAD | Headset Automatic Gain Control |
| OPTAGCSPKR | Speaker Automatic Gain Control |
| OPTAUDIOPATH | Audio Path |
| OPTCLICKS | Button Clicks |
| OPTERRORTONE | Error Tones |
| OPTGUESTLOGIN | Guest Login Permitted/Not Permitted |
| OPTHOMEIDLE | Home Screen on idle; 9670G only |
| OPTTEXTSIZE | Text Size |
| PERSONALRING | Personalized Ring. Note: Applicable to the 9670G only. This value is backed up as equal to the PERSONALWAV value when PERSONALWAV is set to one of the 8 standard ring patterns. When PERSONALWAV is greater |

| Parameter Name | Setting |
|---|---|
| | than 8 (meaning it is set to one of the newer ring patterns) and PERSONALRING was set using a backup file value, that backup value is re-saved. If neither of these conditions apply, no PERSONALRING value is backed up. |
| PERSONALWAV | Personalized Ring value - 9670G only |
| PHNABKNAME | Contacts Pairing |
| PHNEDITDIAL | Edit Dialling |
| PHNQUICKPANEL | Quick Touch Panel; 9670G only |
| PHNREDIAL | Redial |
| PHNSCRONANS | Go to Phone Screen on Answer |
| PHNSCRONCALL | Go to Phone Screen on Calling |
| PHNSCRONALERT | Go to Phone Screen on Ringing |
| PHNTIMERS | Call Timer |
| PHNVISUALALERT | Visual Alerting |
| PRINGMENU | Personalized Ring Menu |
| WEATHERLOCID | Weather Location ID; 9670G only |
| WEATHERUNITS | English/Metric; 9670G only |
| WORLDCLOCKLIST | List of World Clock location entries; 9670G only |

## About restore

When automatic or user-requested retrieval of backup data is initiated, user data and option settings are set to values contained in the backup file. The user-requested retrieval of backup data occurs only if the OPSTAT parameter setting allows the user to change those values. Therefore, any restrictions set using OPSTAT are given priority and implemented.

The backup file value is not retrieved, and the current setting remains valid:

- When a value in the backup file has changed and
- That value corresponds to an application that OPSTAT indicates should not be changed.

This prevents a user from bypassing the administration of OPSTAT and changing options settings in the backup file.

**Note:**

If you administered the APPSTAT parameter to suppress changes to one or more applications, the phone backs up and restores data as usual, but ignores data for

"suppressed" applications. This prevents a user from bypassing your APPSTAT restrictions by editing the backup file. For information about APPSTAT, see Setting the Application Status flag (APPSTAT) on page 166.

During backup file restoration, user activity is prohibited until the phone displays a `Retrieval successful` or `Retrieval Failed` . When a restore attempt fails, if a retrieved file has no valid data, or if a retrieved file cannot be successfully stored, the phone displays a `Retrieval Failed` message until the user takes another action.

Important considerations during data retrieval are as follows:

- When you create a backup file rather than edit an existing one, ensure to create the file with UTF-16 LE (little endian) characters, with Byte Order Mark (BOM) for LE of 0xFFFE.
- Backup saves data values using the generic format *name=value*. For specific formats, see Backup file formats on page 156.
- All identifiers, for example, *names*, are interpreted in a case-insensitive manner, except parameter values, Contact names, and numbers.
- Spaces preceding, within, or following a *name* are treated as part of the *name*.
- <CR> and <LF> (UTF-16 characters 0x000D and 0x000A, respectively) are interpreted as line termination characters.
- Blank lines are ignored.
- When an identifier is not recognized or is invalid, the entire line is ignored. Similarly, if an identifier is valid but the data itself is invalid or incomplete, the line is ignored.
- When an identifier is valid with valid and complete data, but the data is not applicable to the current state of the phone, the data is retained for possible use later, and is treated as data to be backed up at the appropriate time.

  For example, if button labels for an SBM24 button module unit are present, but no such module is attached to the deskphone, the button labels are retained.
- When more than one line contains a value for an option, parameter, or Contacts entry, the last value read is retrieved, to allow new values to overwrite previous values as lines are read from the backup file. In all other cases, the line order in the backup file has no bearing on retrieval.
- The existence of invalid data does not constitute a failed retrieval. The success of the retrieval process requires the phone to obtain the backup file and successfully restore valid data.

# Administering backup and restore for a 9610

The 9610 uses its backup and restore functionality differently than other 9600 Series IP Telephones. The deskphone does not have any user-created data or options that need to be

stored in a 9610 backup file. The 9610 uses its backup file as the source for administration of the button labels and associated deskphone numbers in the Contacts application, the Main Menu list, and associated data.

The administrator creates the backup file in accordance with the requirements in this section so that when the 9610 deskphone boots up and registers, the file obtains the appropriate data for user presentation.

The differences in the backup and restore procedures between a 9610 deskphone and the other 9600 Series IP deskphones are as follows:

- The 9610 never *backs up* data, it only retrieves data. Because the user has no mechanism to change any data, there is no need to back up changes. For consistent in terminologies, the 9610 file is referred to as the *backup file*.
- Because the user can never change data, the OPSTAT value is ignored for the purposes of populating the display from the 9610 backup file.
- When the 9610 attempts to retrieve the backup file, the deskphone first attempts to retrieve a file labeled ext_9610data.txt. If the 9610 does not retrieve this file successfully, unlike the other 96xx sets, the 9610 attempts to retrieve a file labeled 9610data.txt. This file does not have an extension designation. This retrieval process has the advantage of allowing all 9610s that are not associated with a specific extension's backup file to share a common backup file. You can have, for example, three unique 9610 backup files; one for a 9610 in the Marketing conference room, one for a 9610 in the Accounting conference room, and one for five 9610 IP Telephones in public areas of the company.

**Related topics:**

[About the 9610 retrieval process](#) on page 161
[General 9610 restore processing](#) on page 162

## About the 9610 retrieval process

When the deskphone initiates an automatic retrieval, the deskphone first attempts to retrieve a file with filename *ext*`_9610data.txt`, where *ext* is the extension number of the deskphone. While in progress, the Top Line displays

```
Retrieval 1
```

. If the file is retrieved successfully, the Top Line of the deskphone displays

```
File obtained
```

while the deskphone validates the data, and stores valid data in memory. All previous corresponding data is replaced, unless the restore fails, as described in the following options. When data storage is completed successfully, the Top Line displays

```
Restore OK
```

for 30 seconds, or until the user selects another Application Line or application, whichever comes first.

If this first retrieval attempt fails for any reason, or if the successfully retrieved file had no valid data, the 9610 deskphone then attempts to retrieve a file with the filename `9610data.txt`. While this retrieval is in progress, the Top Line displays
`Retrieval 2`
If the file is retrieved successfully the remaining steps are identical to those for the `ext_9610data.txt` file.

If the second retrieval attempt fails for any reason, or the file is successfully retrieved but has no valid data, or the successfully-retrieved file was not saved, then the Top Line displays *Restore failed* for 30 second, or until the user selects another Application Line or application, whichever comes first.

After the data storage starts and till the deskphone displays the *Restore OK* or *Restore failed* message, the user cannot perform any action to display another screen. For example, the Avaya Menu button is temporarily locked and you cannot press any press button. After the appropriate result message is displayed, the corresponding 9610 user interface is presented.

## General 9610 restore processing

You must code the characters in UTF-16 LE (little-endian, with Byte Order Mark (BOM) for LE (0xFFFE)), with each item on a separate line terminated by" <CR><LF>" (000D 000A in UTF-16) characters.

**Important:**

If the file is not in this format, the deskphone displays the message "`Restore failed.`".

The generic format for data values is: *name*=*value*.

The format for retrieving a Main Menu entry is:

```
MMLBLxx =entry label MMTYPExx =entry type MMDATAxx =entry data
```

For more information, see Administering a 9610 Main Menu (MM) on page 190.

The format for retrieving a Contacts entry is:

```
CONLABELxxx = entry label CONDATAxxx = entry data
```

For more information, see Administering the 9610 Contacts Application on page 191.

The other parameters in a 9610 backup file are:

IDLEAPP: As described in Administering the 9610 idle application, screensaver, and WML links on page 192.

LISTAPP: When LISTAPP is null or the default, the administrator might not have created an external equivalent to the local Contacts application. The local Contacts application is used unless it too is empty. When the local Contacts application is empty, you can either select **List**

or **Start** . When LISTAPP is non-null, the administrator has populated the parameter with a URI for a WML-based application to be displayed when **List** is selected.

When retrieving data:

- If the Byte Order Mark (BOM) is not 0xFFFE, the entire file is rejected and the retrieval fails.
- All identifiers, for example, names, are interpreted in a case-insensitive manner.
- The case of parameter values and Contacts names and numbers are preserved.
- Spaces preceding, within, or following a *name* or *value* are treated as part of that entity.
- <CR> and <LF> are interpreted as line termination characters.
- Blank lines are ignored.
- If an identifier is not recognized or is invalid, the entire line is ignored.
- If an identifier is valid but the data is invalid or incomplete, the line is ignored. For information on what constitutes a valid value for each data element, see General 9610 Restore Processing on page 162 and 9610 Backup File Format on page 189.
- If more than one line contains a value for a parameter or Contacts entry, the last value read is used (hence, new values overwrite previous values as lines are read from the file). In all other cases, the order of the lines in the file does not matter.

The success of the retrieval process requires the deskphone to obtain the backup file and to successfully store valid data. The existence of invalid data does not constitute a failed retrieval.

**Note:**

Administering Specific 9600 Series IP Deskphones on page 187 describes 9610-specific administration.

# Chapter 9: Administering Applications and Options

## Customizing Applications and Options

The 9600 Series IP deskphones have some unique and powerful capabilities that take advantage of their display and access to LAN facilities. For example, if your LAN has a WML Web site, the deskphone needs key information about the servers providing those facilities. You must provide this information in the 46xxsettings.txt file, depending on the applications you want to make available to your end users.

**Caution:**

For the deskphones to work properly, you must have a *46xxsettings.txt* file in the same directory as the application file. If you do not edit the 46xxsettings.txt file, those deskphones use default settings only. The 46xxsettings file is available as a standalone download. If you already have such a file because you downloaded it for a previous 9600 Series or 4600 Series IP Telephone release, installing the standalone file overwrites the original file.

**Note:**

To facilitate administration, the 9600 Series and 4600 Series IP deskphones use the same `46xxsettings.txt` file.

The following is a list of applications or functions and the parameters that apply to those applications. See 9600 Series H.323 customizable system parameters on page 84 for associated parameter descriptions, default values, and valid values or ranges. Parameters shown as Mandatory must be accurate and non-null for the application to work; other parameters listed are optional. You can change parameters to suit your environment. If you do not include these parameters in the settings file, the default values are used.

Backup/restore parameter - BRURI (Mandatory)

Backlight parameter - BAKLIGHTOFF

Calculator application parameter - CALCSTAT

Call log/history parameters - CLDELCALLBK, LOGBACKUP, LOGMISSEDONCE, LOGUNSEEN

General user parameters - APPSTAT, OPSTAT, OPSTAT2

Guest login parameters - GUESTDURATION, GUESTLOGINSTAT, GUESTWARNING

Options parameter - RINGTONESTYLE

Phone parameter - FBONCASCREEN

User Timer (Stopwatch) — TIMERSTAT

VPN parameters - VPN parameters. For more information on VPN parameters, see *VPN Setup Guide for 9600 Series IP Telephones*,16-602968 as well as 9600 Series H.323 customizable system parameters on page 84.

Weather application parameters that are applicable for the touchscreen phones only - WEATHERAPP, WMLPORT, WMLPROXY

Web access application parameters - SUBSCRIBELIST, TPSLIST, WMLEXCEPT, WMLHELPSTAT, WMLHOME (Mandatory), WMLIDLETIME, WMLIDLEURI, WMLPORT, WMLPROXY, WMLSMALL.

For more information in developing local Web sites. see *Avaya IP Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide, 16-600888*.

World Clock application parameters that are applicable for the touchscreen phones only - WMLPORT, WMLPROXY, WORLDCLOCKAPP

**Related topics:**

Setting the Application Status flag on page 166

# Setting the Application Status flag

9600 Series IP Deskphones offer numerous applications like Contacts, Call Log/History, Redial, and so on to the users. Each of these applications allows the user to add, delete, or in some cases, edit entries. You, as the administrator, might not want the user to use that level of functionality. For example, a user cannot delete the contact number of the concierge from the hotel lobby deskphone. Further, for privacy reasons, that same deskphone must display the Call Log. You can use the Application Status Flag, APPSTAT, to administer specific application functionality permission levels for one or more deskphones.

APPSTAT consists of one number, specifying a certain level of allowed functionality. A Zero, 0, value provides no functionality. Values 2 and 3 provide increasing levels of functionality, and value 1 provides the user complete application functionality.

**Table 19: Application status flags and their meaning of**

| APPSTAT value | Meaning |
|---|---|
| 0 | Redial and Call Logs/History are suppressed. The user cannot change Contacts. |

| APPSTAT value | Meaning |
|---|---|
| 1 | All administered applications are displayed, with full functionality. This is the default value. |
| 2 | Call Log (History) is suppressed. Contact changes are not allowed. Only one-number Redial is allowed. |
| 3 | Contact changes are not allowed. For touch screen phones, this also means that users cannot assign or remove contact Favorites via the Home screen. |

*Suppressed* applications are not displayed to the user. Softkey labels and application tabs are not labeled or displayed. The deskphones continue to display options associated with suppressed applications unless you override them by appropriate OPSTAT parameter administration. Displayed options have no effect while the application is suppressed. The message *Contact changes are not allowed* means the Contacts application displays and the user can make calls as normal. The deskphone does not display any controls using which the user can change any aspect of the Contact application including adding, deleting, or editing any Contact name or number. This restriction includes the ability to add, delete, or edit any Contact name or number. The message *Only one-number Redial is allowed* means the user option that allows a choice between displaying last numbers dialed is suppressed. The Redial buffer stores only one number. The deskphone does not display the Redial application as the user can redial only one number. This restriction allows privacy once a given user has left the deskphone.

You can:

- Set APPSTAT to 1, for example, in a staging area
- Administer a given deskphone with Contact entries of your choice, like the Concierge deskphone number button in the earlier example
- Then move the deskphone to where it will be used, where you have administered APPSTAT to be, for example, 0

When you change the location of the deskphone and the relocated deskphone resets, it retains its Contact entries, like Concierge, but does not allow the user to create new entries.

When you set APPSTAT to any valid value other than 1, the deskphone does not accept any Contact button label changes that might have been made directly on a backup file. Only the existing labels of the deskphone are used. This restriction prevents circumvention of the APPSTAT restrictions. The WML applications are also suppressed by default.

# Special Administration for the 9610

The 9610 IP deskphone is administered using the restore file and not the settings file that all other 9600 Series IP deskphones use. For information, see Administering backup/restore for a 9610 on page 160.

# Special Administration for Touchscreen Deskphones

The 9621G, 9641G, and 9670G are touch-based phones and use a touch-based Home screen instead of the Avaya menu that other 9600 Series IP deskphones use. Using the home screen, users can gain access to deskphone options and settings, special Avaya applications such as a World Clock, Calculator and Weather, Contact Favorites, and any WML applications you might administer. The Home screen can display up to four WML applications. If you have configured more than four applications, users can gain access to all WML applications through **More**. For information about display characteristics and icons, see How the Home screen displays WML applications on page 174. If the deskphone does not have any WML application, the deskphone might show a single WML Browser item, provided the system parameter WMLHOME is set with a value. For more information about Avaya Menu elements like those for WML applications and exceptions for 9670G or other touchscreen deskphone, see Administering the Avaya “A” Menu on page 168.

# Administering the Avaya A Menu

The Avaya A Menu is a list of sub-applications the user can select from to invoke the corresponding functionality. A file called *AvayaMenuAdmin.txt* is available with downloads on which you can specify the menu label, URI, and list order of WML applications on the A Menu.

A Home screen replaces the A Menu for touch screen deskphones only for access to menu options and settings, log out, Bluetooth setup, and touch screen cleaning. The Home screen also displays WML applications, Favorite contact speed dial buttons, Avaya applications such as the World Clock and Weather, and a calculator. For more information on administration of touch screen deskphones, see Special Administration for Touchscreen deskphones on page 168. The addition of touch screen models requires that you use the *AvayaMenuAdmin.txt* file to specify the WML applications you want the deskphone to display on the Home screen. These applications are displayed in order from left to right, going to a second page if necessary.

**Note:**

This section applies to all 9600 Series IP deskphones except the 9610. For information on 9610 IP Telephone menu administration, see Special Administration for the 9610 IP Telephone on page 168 in Chapter 9.

**Important:**

You must set the system parameter AMADMIN in the 46xxsettings file for Avaya A Menu to work with WML applications. The *AvayaMenuAdmin.txt* file must be a Unicode file to be properly processed by the phones. You can create a Unicode version of this file using Notepad or most text editors. Select *Encoding* and *Unicode*.

If WML applications are installed and the system parameter AMADMIN is set in the settings file:

- The WML applications appear in the first-level A Menu as specified in the *AvayaMenuAdmin* file, as shown in Figure 1 on page 171.
- The first level A Menu on all 9600 Series IP deskphones except touch screen deskphones includes a single entry (Phone Settings) that leads to a screen containing choices for Options & Settings and Network Information. For touch screen phones, the Home screen shows a Settings option that leads to an Options & Settings menu.
- The Phone Settings screen is essentially the current Options and Settings menu, with the addition of Network Information, as shown in Figure 2 on page 172.

If WML applications are installed and the system parameter WMLHOME is set in the settings file, the Avaya A Menu is identical to the pre-Release 1.2 A Menu, as shown in the figure on page 172.

If WML applications are not installed, the A Menu is the same as the current Options & Settings menu, with the addition of Network Information, Log Off, and About Avaya IP Deskphone. The figure provides an illustration.

Depending on how you have administered WML applications, you can present the alternatives for sub-applications as follows:

- Set the system parameter AMADMIN to the URL of the *AvayaMenuAdmin.txt* in the 46xxsettings file when you want to display multiple WML applications on the Avaya A Menu. For more information, see Main Avaya Menu with WML Applications Administered on page 171 and Administering the Avaya Menu with WML applications on page 173 in this chapter.
- Set the system parameter WMLHOME in the settings file for all except the 9610 when you want the deskphone to display the Browser instead of individual applications. For more information, see Main Avaya Menu with Browser (Only) Administered on page 172.
- Take no action to administer WML applications.
- The Browser application is listed only if it is properly administered. For more information, see *Avaya IP Deskphone Edition for 9600 IP Telephones Application Programmer*

*Interface (API) Guide, 16-600888*. Administration also includes a non-null value for WMLHOME.

**Related topics:**

[Administering Phone Settings and Options and Settings](#) on page 170
[Administering WML applications on the Avaya Menu](#) on page 171
[Main Avaya Menu with Browser (Only) Administered](#) on page 172
[Administering the Avaya Menu with WML applications](#) on page 173
[How the Home screen displays WML applications](#) on page 174

# Administering Phone Settings and Options and Settings

The Options & Settings application is listed if and only if the OPSTAT value is not 0*xy*, where *x* and *y* can be any value of 0 or 1, if OPSTAT is in 3-bit form, or if and only if the value of OPSTAT is 1, if OPSTAT is in the one-digit form.

The Network Information application is listed if and only if the OPSTAT value is not *x*0*y*, where *x* and *y* can be any value of 0 or 1 if OPSTAT is in 3-bit form, or in any case, if OPSTAT is in the one-digit form.

The Logout function is listed if and only if the OPSTAT value is not *xy*0 , where *x* and *y* can be any value of 0 or 1 if OPSTAT is in 3-bit form, or if, and only if, the OPSTAT value is 1, if OPSTAT is in the one-digit form.

**Note:**

If you administer a Log Out button for a softkey on the Phone Screen, OPSTAT does not prevent that softkey from being labeled and from enabling the user to log out. For more information on administering softkeys, see [Administering features on softkeys](#) on page 137.

If OPSTAT is set to forbid access to Options & Settings, the deskphone ignores changes to the backup file settings of the user. This prevents users from using the backup file to make changes to the settings. This prevents someone from using the backup file as a “back door” for making changes to the settings. However, some customers centralize the customized relabeling of administered features and upload changes to these labels. For this specific case, the OPSTAT2 parameter can override the value of OPSTAT. If you set OPSTAT2 to 1, the deskphone accepts changes to the customized labels stored in the backup file regardless of the OPSTAT value. The parameter OPSTAT2 can override the value of OPSTAT for this specific case - setting OPSTAT2 to 1 allows the telephone to accept changes to the customized labels stored in the backup file regardless of the OPSTAT value.

**Note:**

Software Release 3.0 added the system parameter OPSTAT2. Regardless of the preceding text on OPSTAT settings, if the value of OPSTAT2 has the value 1 then any customized labels in the user's backup file are uploaded and used as if the value of OPSTAT permitted

this action. However, to restore the personalized and customized labels from the backup file to the deskphone, the user must restart the phone by logging out and then logging back in again.

## Administering WML applications on the Avaya Menu

Administering AMADMIN provides direct links to one or more WML applications. As the figure on page 171 shows, the first level Avaya Menu includes entries for three (sample) WML applications, a Phone Settings menu choice for telephone options and settings, and the telephone log out.

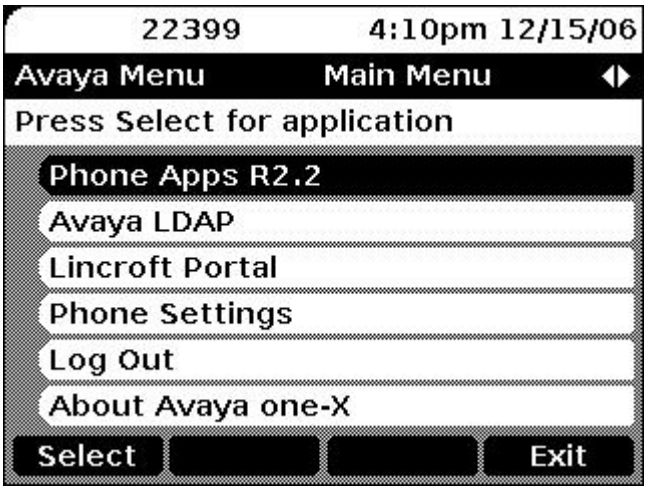



**Figure 1: Avaya Menu with WML applications installed as the first three options**

If at least one WML application is administered, the administrator can choose to specify the order in which the WML applications and the built-in applications are presented. Any built-in applications that are not specifically administered in the WML Administration file are automatically appended to the end of the administered list, in the following order:

- Phone Settings
- Log Out
- About Avaya IP Deskphone

If you select an application and press **Select** or **OK**, the application is run. If the Phone Settings application is listed, the deskphone displays Choice Indicator on the Title Line. If you press the Left or Right Navigation buttons, the deskphone displays the Phone Settings screen. If you select Phone Settings, the deskphone displays the Phone Settings menu as follows.




**Figure 2: Second Level Avaya Menu - Phone Settings Screen**

## Main Avaya Menu with Browser (Only) Administered

If you set the system parameter WMLHOME in the settings file, the deskphone provides a way to link to the Browser Home page by specifying a URL. If you administer WMLHOME, Avaya A Menu is displayed as shown in the figure on page 172.

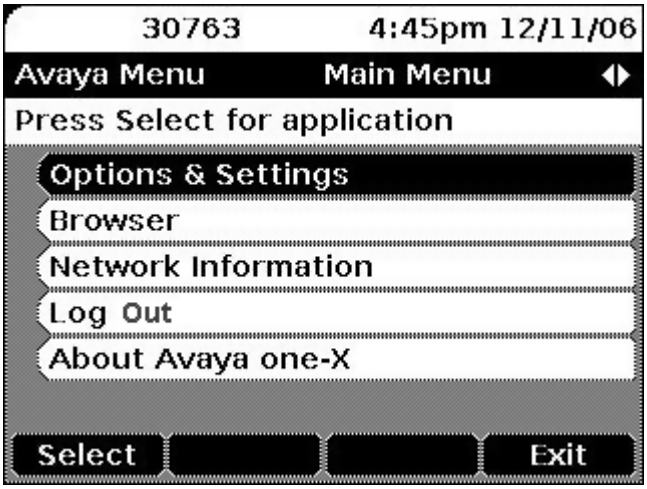



**Figure 3: Avaya Menu with Browser Administered using WMLHOME**

Each individual sub-application is listed left justified on an individual Application Line. From top to bottom, the sub-applications are:

- Options & Settings
- Browser
- Network Information

- Log Out
- About Avaya IP Deskphone

# Administering the Avaya Menu with WML applications

### About this task

Administer the AMADMIN parameter in the 46xxsettings file to point to a URL where the AvayaMenuAdmin.txt file resides.

**Important:**

The `AvayaMenuAdmin.txt` file must be a Unicode file to be properly processed by the phones. You can create a Unicode version of this file using Notepad or most text editors. Select *Encoding* and Unicode.

**Note:**

Use the `AvayaMenuAdmin.txt` file to specify the WML applications to appear on Home screen of the touch screen models.

Then specify objects for the Avaya Menu through the Avaya Menu Administration file, `AvayaMenuAdmin.txt`. Each administered object, up to the maximum of 12, must have valid, non-null parameter data:

**AMTYPExx** One of six options: 01 = URI, 02 = the local “Phone Settings” sub-application, 03 = local Log Off sub-application, 04 = the About Avaya IP Deskphone screen, 05 = Guest Login application, 06 = My Pictures application. Touch screen telephones ignore all AMTYPE values except “1”. If the AMTYPE for an associated administered object is “01”, the additional three parameters must have valid, non-null data for the object to be properly administered:

**AMLBLxx** The label displayed to the user for this object, up to 16 UTF-16 characters, shown left-justified unless spaces precede the label value to center the label.

**AMDATAxx** A URI of up to 255 ASCII characters, without spaces.

**AMICONxx** For touchscreen models only, any number, *N*, from 1 to 25. The touch screen deskphone will use the *Nth* icon presented in the table on page 174 on the Home screen in association with the administered WML application. The labels shown in the table on page 174 are suggestions. The touch screen deskphone uses the label you specify in the AMLBLxx parameter.

The *xx* in these three parameters is a two-digit integer from 01 to 12 inclusive, including a leading zero if applicable. If AMTYPE*xx* is 01, *xx* must be the same for each of the three parameters for an Avaya Menu entry to be displayed and associated with the administered data. If AMTYPE*xx* is 02, 03 or 04, any AMLBL*xx* or AMDATA*xx* data is ignored if provided.

If a given administered object has null or invalid data in any of the required associated parameters, that object is completely ignored. To list an AMTYPE01 entry on the Avaya Menu,

all three associated parameters must be non-null with valid data. For example, an AMTYPE of “00” is considered invalid.

Do not administer more than nine URIs. You cannot specify a telephone number as a TYPE (unlike the 9610).

In case of duplicate data in the settings file, the last entry is retained. For example, if two consecutive lines in the Avaya Menu Administration file are:

```
AMLBL01=ABCD

AMLBL01=WXYZ
```

then the user sees “WXYZ” as the label for the first WML application. This example assumes the rest of the administration is correct.

If no `AvayaMenuAdmin.txt` file is available, or if the file does not contain at least one valid type 1 (URI) object, the deskphone displays Release 1.0/1.1 Avaya Menu shown in**TERRY*x —ref table**is instead.

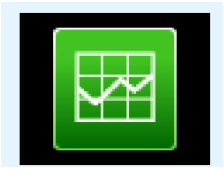
**Note:**

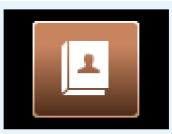
For touchscreen deskphones only, non-WML entries in the AvayaMenuAdmin.txt file are ignored.

## How the Home screen displays WML applications

The following table shows the icons, suggested description(s), and numbering to use to specify the WML applications you want the Home screen to display.

**Table 20: Home Screen WML Application Icons/Labels**

| To Display This Icon: | Set AMICONxx to this Label Number (xx value shown below) | Suggested Label (specify in AMBLxx) |
|---|---|---|
|  | 1 | Alarm Clock/Wakeup Call |
|  | 2 | Business data/Sales/Data Analysis |

| To Display This Icon: | Set AMICONxx to this Label Number (xx value shown below) | Suggested Label (specify in AMBLxx) |
|---|---|---|
|  | 3 | Calendar |
|  | 4 | Communications |
|  | 5 | Control (remote, ...) |
|  | 6 | Directory |
|  | 7 | Document/Folders/Notes |
|  | 8 | Emergency/Assistance |
|  | 9 | Food/Restaurant |
|  | 10 | Financial Information |
|  | 11 | Front Desk |

| To Display This Icon: | Set AMICONxx to this Label Number (xx value shown below) | Suggested Label (specify in AMBLxx) |
|---|---|---|
|  | 12 | Help/Site Help/Feature Help |
|  | 13 | Guard Desk |
|  | 14 | Information |
|  | 15 | Inventory |
|  | 16 | Location/Map |
|  | 17 | Messages |
|  | 18 | Network |
|  | 19 | Person/People information |
|  | 20 | Security/Security Camera |

| To Display This Icon: | Set AMICONxx to this Label Number (xx value shown below) | Suggested Label (specify in AMBLxx) |
|---|---|---|
|  | 21 | Tickets |
|  | 22 | Valet Service |
|  | 23 | Video/TV |
|  | 24 | Slideshow |
|  | 25 | Room Service |

# Sample Avaya Menu Administration File Template

```
############################################################

## ## AVAYA MENU CONFIGURATION FILE TEMPLATE ##

############################################################

## This file is to be used as a template for configuring the ##Avaya
Main Menu. See the Avaya one-X™ Deskphone H.323 ##Administrator Guide
for details. Both are available on ##support.avaya.com ##

##Since the AMICON parameter applies only to touchscreen telephones,
it is not shown in the sample below.

############################################################

##
```

```
## AMLBLxx=Label up to 16 unicode characters
## AMTYPExx=Type 1=WML-Application; 2=local Phone Settings
## 3=local LogOff Application;4=local About Avaya Screen
## 5=Guest Login; 6=My Pictures
## AMDATAxx URI of up to 255 ASCII-characters e.g. http://
yy.yy.yy.yy/*.wml
## The tags AMLBLxx and AMDATAxx are only used if AMTYPExx = 1
## Multiple definitions of local applications (Type 2.4)
## will be suppressed. The last tag is valid.
## xx describes the sequence in the Avaya Menu and is valid
## from 01 to 12.
##
##AMTYPE01=
##AMLBL01=
##AMDATA01=
##
##AMTYPE02=
##AMLBL02=
##AMDATA02=
##
##AMTYPE03=
##AMLBL03=
##AMDATA03=
##
##AMTYPE04=
##AMLBL04=
##AMDATA04=
##
##AMTYPE05=
##AMLBL05=
##AMDATA05=
```

```
##
##AMTYPE06=
##AMLBL06=
##AMDATA06=
##
##AMTYPE07=
##AMLBL07=
##AMDATA07=
##
##AMTYPE08=
##AMLBL08=
##AMDATA08=
##AMTYPE09=
##AMLBL09=
##AMDATA09=
##
##AMTYPE10=
##AMLBL10=
##AMDATA10=
##
##AMTYPE11=
##AMLBL11=
##AMDATA11=
##
##AMTYPE12=
##AMLBL12=
##AMDATA12=
```

# Administering guest users

### About this task

A guest user is a person who logs into a 9600 Series IP deskphone that is not his or her primary phone at the home location of the user.

The guest user can log into a phone that is across the country from the home location or one in the office adjacent to the home office. You administer permission for guest login by setting the system parameter GUESTLOGINSTAT to 1 (permitted), that displays the Guest Login option on the Avaya “A” Menu.

Other related parameters you can administer are GUESTDURATION that can be overridden by a different, user-entered duration during login) and GUESTWARNING. For more information on the parameters, see 9600 Series H.323 customizable system parameters on page 84.

# Administering visiting users

### About this task

A visiting user is anyone who uses a 9600 Series IP deskphone in one location, for example, New York, and intends to register to a call server in some other location. For example in Paris. Typically, this occurs when a user has travelled from his/her home location to another location in the organization, but wants to register with the call server back home. The user might want to get the specific administered feature buttons, etc. provided by the home call server.

To allow this functionality, the parameter VUMCIPADD should be administered in the 46xxsettings file at the current location for the visitor, with the IP addresses of their home call servers. From then on, the deskphone operates as specified in Registration with the call server on page 26.

# Administering idle timer operation

### About this task

When the idle timer in the deskphone expires, you can administer the deskphone to turn the backlight to its lowest power level, put up a screen saver, and/or show a Web page while the deskphone is idle. However, do not set all of these values on the same deskphone. However, you can set a lobby phone to go to a Web page when it is idle and to set a desk phone to go to the screen saver and/or set the backlight to low power mode when idle.

The related system parameters and their defaults are:

### Procedure

1. WMLIDLETIME = 10 minutes
2. BAKLIGHTOFF = 120 minutes
3. SCREENSAVERON = 240 minutes
4. WMLIDLEURI = null

### Result

You must specify WMLIDLEURI only for phones in public areas through the use of a GROUP parameter.

**Table 21: Idle Timer Settings and Results**

| Shortest Timer | Middle Timer | Longest Timer | Operation |
|---|---|---|---|
| WMLIDLETIME and WMLIDLEURI are null | BAKLIGHTOFF is non-zero | SCREENSAVER ON is non-zero | Default operation:<br>After BAKLIGHTOFF minutes, the backlight is set to low power mode.<br>After (SCREENSAVERON – BAKLIGHTOFF) additional minutes, the screen saver is displayed.<br>WMLIDLETIME has no effect. |
| WMLIDLETIME and WMLIDLEURI are null | SCREENSAVER ON is non-zero | BAKLIGHTOFF is non-zero | After SCREENSAVERON minutes, the screen saver is displayed.<br>After (BAKLIGHTOFF-SCREENSAVERON) additional minutes, the backlight is set to low power mode. |
| WMLIDLETIME and WMLIDLEURI are non-null | BAKLIGHTOFF is non-zero | SCREENSAVER ON is non-zero | Every WMLIDLETIME minutes, a GET is sent for WMLIDLEURI, and the browser is displayed. The Web page may contain its own timer to cycle through additional Web pages.<br>The backlight is set to low power mode after the specified time and the screen saver is displayed based on the SCREENSAVERON value. |

For more information, see9600 Series H.323 customizable system parameters on page 84.

**Note:**

The 9610 IP deskphone uses the IDLEAPP value in the 9610data.txt file instead of WMLIDLEURI in the settings file. For more information, see Special Administration for the 9610 on page 168 and Administering backup/restore for a 9610 on page 160.

**Note:**

The Backlight Off icon if administered, allows the end users to bypass the timers in the table on page 181 and set the the backlight to its lowest level automatically. You can administer the Backlight Off icon on a 9600 Series IP deskphone softkey as described in Administering features on softkeys on page 137.

The behavior of backlight for any adjunct button module depends on the backlight of the phone to which the button module is attached.

# Administering the user stopwatch timer

The TIMERSTAT parameter provides user permission to turn a 60 second stopwatch on during a call. The deskphones provide all processes controlling user timer operation. When set to *1* this parameter cannot be turned on or off by the call server.

When the TIMERSTAT parameter is set to *1* a **Timer On** softkey is displayed. For button-based phones it appears as **TimerOn** softkey, with its position determined by the call state, the screen being displayed, and the presence of other softkeys relative to the current screen/activity. For example:

- When the deskphone is in an active call state, the 4th softkey is labeled **Timer On** and the **Drop** softkey is not displayed.
- When the deskphone is In an idle call state and if the **Emerg.** softkey is not administered, the 3rd softkey is labeled **Timer On**. However, if the **Send All** softkey is not administered, the 2nd softkey is labeled **Timer On**.
- Otherwise, the 4th softkey is labeled **More**. If you press **More**, **Timer On/{blank}/ LightOff/More** is displayed on the next set of softkeys. Pressing **More** again displays the original set of softkeys.

When the User Timer is presented it is displayed right justified on the Title Line, overwriting any other displayed content. Once displayed, it remains displayed, even if the user changes screens. If the Title Line changes text, the User Timer remains displayed over the text as applicable. After the User timer is displayed and activated, the timer is removed when:

- The user presses the **TimerOff** softkey.
- The deskphone has displayed 59:59 for 5 seconds.

The user timer begins at 0:00 and increments by one per second until 59:59 is reached, at which point the timer stops but continues to be displayed. Once the User Timer is removed, any overwritten text is displayed normally.

If TIMERSTAT is set to 1, the presence of the **Timer On** softkey or **TimerOn** softkey for button-based models takes priority over other administered features.

# Requirements for USB Devices

A USB device can be used to carry information to support the following usage profiles:

- Mobility/Visiting User: The USB memory stick carries login credentials, contacts and/or digital pictures. If users insert a USB device, the deskphone is registered with a login profile and any 9600 Series IP deskphone can become a personalized extension.
- Deskphone Personalization: A USB memory stick supports import/export of contacts to/from a 9600 Series IP deskphone and/or display of digital pictures.

Users and administrators can use the *Avaya one-X® Deskphone USB Companion,* a PC-based USB management tool that converts Microsoft Office Outlook contacts to a format usable by 9600 Series IP deskphones, and provides an easy way to format other files, like digital pictures that will be used as screensavers. This PC-based tool is available on the Avaya support Web site.

**Related topics:**

USB File/Device Support on page 183
Contacts File Format for USB Devices on page 184
Setting up USB logins on page 185
Setting up USB pictures as screensavers on page 185

## USB File/Device Support

Only FAT or FAT32 file systems are currently supported. The following are not currently supported:

- USB drives with NTFS file systems are not supported.
- USB devices with multiple partitions or multiple LUNS are not supported.
- U3 USB devices are not supported.

# Contacts File Format for USB Devices

As of software Release 2.0, Contacts lists can be imported or exported to or from all 9600 Series IP deskphones except the 9608 and 9610 through a USB device like a Flash drive or memory stick. The user guide provides detailed information on this capability.

Contact files merged or written to the phone's Contacts list must be in a specific format. The user guides provides end users with two ways to ensure that a Contact list is formatted properly.

The rest of this section documents the 9xxxContacts.txt file requirements. Use this information to export contacts from Outlook and other similar software applications without using the Avaya one-X® Deskphone USB Companion tool.

The contacts file must be a little-endian Unicode text file. That is, each character in the file is a 16-bit integer value, stored least significant byte first. The first two bytes of the file are a Byte Order Mark which must be FF followed by FE (hexadecimal). The file name must be "`9xxxContacts.txt`" (without the quotes).

Each contact entry consists of a single line, terminated by <CR><LF> (Carriage Return, 000D hex, and Line Feed, 000A hex). An entry contains one name, one to three phone numbers, and zero to types. Separate the fields within each contact entry with one or more tabs.

The detailed contact entry format is:

```
<name><tab><number1><tab><type1><tab><number2><tab><type2><tab><numb
er3><tab> <type3><CR><LF>
```

Name and Number fields - can start and end with a double quote character ["]). The name and number1 are required, and each must be at least one character (not counting quotes). Limit names and phone numbers to 20 characters for the name, and 30 for the numbers. Values are truncated if the values exceed these maximum sizes.

Types must be three characters, starting and ending with a slash '/' character, with a digit character 0 to 3 in between; e.g. "/1/". Leading and/or trailing spaces are ignored for type fields. The Types are 0 for General, 1 for Work, 2 for Mobile, and 3 for Home. Types are optional and missing types default to 0 (General).

Lines may be at most 255 Unicode characters long, including the <CR><LF>. Blank lines, including lines consisting only of spaces and/or tabs, are ignored. A field other than the first that consists of only spaces is ignored.

Because types can be omitted, if the potential type field is more than three characters or does not start and end with a slash, it is considered the next number field, if any (e.g. "/1" and "/02/" would be considered numbers).

Entries are invalid if:

- The name is null (a non-blank line starts with tab or with “” followed by tab).
- There is no number1 field.
- Any number field is null (for example, just “” for number2).
- A potential type field contains an invalid digit (not 0, 1, 2, or 3) or consists of “/” or “//”.
- More than three numbers are provided.
- The entry contains more types than numbers.

Using the Windows™ XP Notepad program you can create and edite Unicode text files and use the Save As dialog to set the file “Encoding” to “Unicode.”

## Setting up USB logins

### About this task

Release 3.0 onwards, users can log in to their call servers using a USB Login profile. As the administrator, you enable this feature by allowing the parameter USBLOGINSTAT in the settings file to remain at the default value of *1* or you can disable this feature by changing the value to *0*. The advantage of having USB login is that users can go anywhere in the world having sufficient network data connectivity, plug the USB device into a 9600 Series IP deskphone running software Release 3.0 or later and log into their home call server using their own extension and get all their home administered features.

You can use *Avaya IP Deskphone USB Companion*, the Avaya PC-based USB management tool, to create the USB login profile, and specify whether the login password should be encrypted or stored in the clear. For more information on this tool, see the Avaya support Web site, http://www.avaya.com/support.

**Note:**

When users log in using the USB Login feature, the deskphone does not attempt to access the backup file as normal, so normal user-specified data such as Options, or Call Log entries are not available. The reason is that if the user is in a different environment from the usual office the deskphone would attempt to access the local backup file server instead of the remote (home) file server and could obtain a different backup file than that of the user. Additionally, the only contacts a user has access to when registered via USB Login are the contacts available on the USB device (properly formatted as a 9xxxContacts.txt file using the Avaya USB tool or another method).

## Setting up USB pictures as screensavers

### About this task

Software Release 3.0 onwards, you can use one or more pictures from a USB flash drive device as screen savers. The USB device may contain any number of .jpg or .jpeg files that can be

used in place of a default or custom screen saver(s). If multiple files are provided, the phone will present each picture in order, based on the order the pictures were saved, changing to the next image after the number of seconds specified by the timer parameter of a default value of 5 seconds. These pictures also be viewed directly by using the **My Pictures** option on the Avaya **A** Menu or on the Home screen.

Users and administrators can use the *Avaya IP Deskphone USB Companion* to format digital pictures that will be used as screensavers. This PC-based tool is available on the Avaya support Web site.

If you want to set up digital picture files manually without using the *Avaya IP Deskphone USB Companion*, follow these instructions:

### Procedure

1. Create a *\Pictures* directory on the USB device.
2. Add one or more images with an extension of *.jpeg or *.jpg and with a valid JPEG format to the pictures directory.

   The images must not exceed the pixel sizes provided in the following table for the respective deskphone model. Color phones such as the 9620C, 9621G, 9640, and 9650C display a better image quality than 9600 Series IP deskphones that do not have color displays:

| Deskphones Supporting USB | Image Size in Pixels (HxW) |
|---|---|
| 9620/9620C/9620L | 320x160 |
| 9611G/9630/9630G/ 9640G/9650/9650C | 320x240 |
| 9641G | 480x272 |
| 9670G | 640x480 |

**Note:**

If the images are too large to be displayed on the phone, the default screensaver image will be shown instead. The 9608 and 9610 IP deskphones do not have a USB interface and therefore cannot display digital images as screensavers.

**Note:**

The screensaver starts automatically when the phone is idle for the time specified in the SCREENSAVERON parameter for which the default value is 240 minutes. Reduce the default time in order to use the USB Pictures feature. To disable USB picture functionality, set the SCREENSAVERON parameter to *0* in the settings file.

# Chapter 10: Administering specific 9600 Series IP Deskphones

## Introduction

On some 9600 IP deskphone models might have to administer additional features or address special administrative requirements. For example, the 9610 IP deskphone designed as a courtesy, or walk-up, deskphone. The 9610 is not full-featured like other 9600 IP Series deskphones. The 9610 only includes a Contacts application, but you can administer additional features like WML applications and a Directory.

This chapter provides additional or alternate administration details for specific deskphone models.

## Special Administration for the 9610 IP Telephone

### Overview of the 9610 IP Deskphone

The user cannot transfer or place conference calls, or put an active call on hold, because the 9610 is a single line phone.

The 9610 does not have a phone screen, an Avaya Menu, Call Log buttons, or Speaker or Mute buttons like other 9600 Series IP deskphones. The 9610 has two application buttons: **Start** and **Contacts**. The 9610 supports the Web browser application.

The Main Menu (MM) on the Start screen is an list of administrable objects. The user can select a new application that is either local to the deskphone or on an external server, or an outgoing call. The underlying content administration of the Main Menu directs the deskphone to take action applicable to the given selection. The default Main Menu consists of Contacts and Directory, if administered. The Main Menu (MM) on the Start screen is a list of administrable objects that display when the deskphone first starts or resets.

The Contacts application provides functionality that is similar to the other models but only to initiate a call to a contact. You cannot edit, delete, or add contacts.

The deskphone screen displays the Idle Application screen only if you administered both a Web Idle Timer and the Idle application and the timer expires. For example, if the Idle application has been set to *Contacts*, when the Web Idle Timer expires the 9610 display changes to the Contacts application. The Idle application is either one of the existing local applications, Menu or Directory, or a URL, depending on the contents of IDLEAPP.

## Key 9610 administration concepts

Each 9610 seeks a backup or restore file which contains essential administration data in its user interface that enables different capabilities to walk-up users. The administrator must create the backup file, that is common to all phones to specify the required behavior of the deskphone to walk-up users. For more information on backup and retrieval for the 9610, see Backing up and restoring data on a 9610 on page 160.

A group of 9610 phones can share a common backup file, or individual 9610 IP Telephones can have individual customized backup files.

Backup files must be created in an editor. The 9610 cannot store a current configuration to a backup file as other 9600 Series models can do.

Within the backup file format, the configuration is split into the following three portions corresponding to the different applications. SeeGeneral 9610 Functionality on page 187:

- Main Menu administration. See Administering the 9610 Main Menu on page 190.
- Contacts administration. See Administering the 9610 Contacts application on page 191.
- Idle administration. See Administering the 9610 idle application, screensaver, and WML links on page 192.

Create a generic backup and restore file, *9610data.txt*, that you can use as a default to provide basic functionality and serve as a template for any customized 9610 extensions. Create a backup and restore file, *Ext#_9610data.txt*, for the specific extension that you want to customize.

See the Avaya support site http://support.avaya.com to download a 9610 backup file example. You can also see a sample file Sample 9610data.txt file on page 194.

**Note:**

Like other deskphone models, the 9610 looks for a 46xxsettings file at startup. In the 46xxsettings file, you must set the system parameter BRURI to the URI where the *9610data.txt* file is located. This URI consists of the HTTP server IP address and the optional directory.

If the deskphone cannot find the 9610data.txt file or if that file does not exist, the screen displays the default Main Menu (Contacts and Directory).

**Related topics:**

9610 Backup file format on page 189
Administering the 9610 Main Menu on page 190
Administering the 9610 Contacts application on page 191

## 9610 Backup file format

Use a text editor to create the 9610 backup file. Code the characters in UTF-16 LE (little-endian), with Byte Order Mark (BOM) for LE (0xFFFE), each item on a separate line terminated by *<CR><LF> (000D 000A* in UTF-16 characters.

The generic format for data values is: *name*=*value*.

The format for a Main Menu entry is:

`MMLBL`*xx*`=entry label`

`MMTYPE`*xx*`=entry type`

`MMDATA`*xx*=entry data

The format for a Contacts entry is:

`CONLABEL`*xxx*=entry label

`CONDATA`*xxx*`=entry data`

Other parameters that have meaning in a 9610 backup file are:

IDLEAPP

LISTAPP

When retrieving data, the system:

- Rejects the entire file if the BOM is not 0xFFFE and deesm the retrieval to have failed.
- Interprets all identifiers in a case-insensitive manner. For example, names.
- Preserves the case of parameter values and Contacts names and numbers.
- Treats spaces preceding, within, or following a name or value as part of that entity.
- Interprets <CR> and <LF> as line termination characters.
- Ignores blank lines.
- Ignores entire line if an identifier is not recognized or is invalid.

- Ignores line If an identifier is valid but the data itself is invalid or incomplete. The determination of what constitutes a valid value for each data element is specified in the individual requirements in this document.
- Reads the last value if more than one line contains a value for a parameter or Contacts entry. Hence, new values overwrite previous values as lines are read from the file. In all other cases, the order of the lines in the file does not matter.

For the successful retrieval of the process, the deskphone must obtain the backup file and to successfully store valid data. The existence of invalid data does not constitute a failed retrieval.

## Administering the 9610 Main Menu

### About this task

Use the 46xxsettings file to set the system parameter BRURI to point to the URI where the 9610 backup/restore file (9610data.txt) resides. Then specify objects for the Main Menu via the “9610data.txt” backup file. For a sample data file, see Sample 9610data.txt file on page 194.

**Note:**

The 9610 displays a Main Menu only if you set BRURI to point to the 9610data.txt file and specify Main Menu objects.

Each administered object, up to the maximum of 10 objects, must have valid non-null data in each of the three parameters as indicated:

- MMLBLxx: The label that the user can see for this object. The label has up to 16 characters.
- MMTYPExx: One of four choices: 01=URI, 02=telephone number, 03=local Contacts application, 04=local Directory application.
- MMDATAxx: The data used in the parameter. The data depends on the value of MMTYPE*xx*: a URI, if MMTYPE is 01; a dialable string if MMTYPE is 02; the English word Contacts if MMTYPE is 03; the English word Directory if MMTYPE is 04.

**Note:**

If administered as a URI, MMDATA*xx* is up to 255 ASCII characters in length.

In these parameters, *xx* is a two-digit integer from 01 to 10 inclusive, including a leading zero if applicable. If MMTYPE is 01 or 02, *xx* must be the same for each of the three parameters for a Main Menu entry to be displayed and associated with the administered data. If MMTYPE is 03 or 04, *xx* must be the same as a corresponding MMLBL item for a Main Menu entry to be displayed, but no MMDATA need be assigned. The system ignores any MMDATA assigned to that *xx* entry.

The system ignores an object if a given administered object has null or invalid data in any of the required associated parameters. Therefore for a MMTYPE 01 or 02 entry to be listed on

the Main Menu, ensure that all three associated parameters are non-null with valid data. The system considers an MMTYPE*xx* of 00 as invalid.

The default values for Main Menu objects are:

| Parameter | Default Value |
|---|---|
| MMLBL01 | Contacts (automatically translated into the user interface language). |
| MMTYPE01 | 3 (Local Contacts application). |
| MMDATA01 | Contacts (English only) |
| MMLBL02 | Directory (automatically translated into the user interface language). |
| MMTYPE02 | 4 (Local Directory application). |
| MMDATA02 | Directory (English only). |

The *Default tDirectory* will appear as the first Main Menu object whenever *Directory* is not administered in the Main Menu, if there is no 9610 backup file, or if retrieval of the backup file fails.

The DATA terms *Contacts* and *Directory* are always administered in English, and are independent of the user interface (UI) language. The administrator can create labels for the local applications in the UI language if desired. The administrator can use, for example, *Contacts* for a browser-based application, and *List* for the local Contacts application. Instead, the term used presents the appropriate local application, which does present the UI in the user's language.

The Main Menu allows up to 10 administrable objects including two local application objects, Contacts, and Directory. The total number of items must fit on two screens.

## Administering the 9610 Contacts application

The administrator populates the Contacts Application via the backup file. Each administered object, up to the maximum of 250, must have valid, non-null, data in both of the parameters as indicated:

CONLABELxxx (the label displayed to the user for this object)

CONDATAxxx

In the list of parameters above, *xxx* is a three-digit integer from 001 to 250 inclusive. To display and associate with the administered data, the three-digit integer must be the same for both parameters. The *xxx* value includes leading zeroes as applicable.

If a given administered object has null or invalid data in any of the two associated parameters, that object is completely ignored. Hence, to be listed in the Contacts application, both associated parameters must be valid and non-null.

CONLABELxxx data corresponds to ENTRY_NAME. CONDATAxxx maps to the corresponding ENTRY_NUMBER_1.

All contacts are sorted in alphanumeric order on the Phone screen regardless of the order in the backup or restore file.

## Administering the 9610 idle application, screensaver, and WML links

You can configure the following parameters to set the behavior of the 9610 IP deskphone if left idle for a period of time.

WMLIDLETIME: You can configure this parameter in the 46xxsettings file, to specify the number of minutes the phone must be idle before an Idle Application specified by IDLEAPP can be presented on the display.

SCREENSAVERON: You can configure this parameter in the 46xxsettings file, to specify the number of minutes the phone must be idle before the Avaya Screen Saver can be presented on the screen.

**Note:**

In the current firmware version, Avaya recommends that you do not use both WMLIDLETIME and SCREENSAVERON. For example, set one value to 999 and the other to some nominal time, perhaps 30 minutes.

WMLSMALL: You can configure this parameter in the 46xxsettings file. This parameter must be non-null for WML links specified in the Main Menu to be displayed. Set this value to a valid URL, and under certain circumstances, the WML link becomes the Idle Application that is displayed on the phone.

IDLEAPP: You can configure this parameter with “ ” Null, the default value, so that the deskphone displays the URL pointed by that WMLSMALL when the Web Idle Timer expires. However WMLSMALL must be administered. If both IDLEAPP and WMLSMALL are null, the 9610 displays the Avaya IP Deskphone Screen.

If IDLEAPP is administered as:

- Menu: The deskphone displays the Main Menu application if the Main Menu is not empty when the Web Idle Timer expires. If the Main Menu is empty, the Avaya Screen displays instead.
- Directory: The deskphone displays the Directory application. If a Directory does not exist, the deskphone displays the Avaya Screen when the Web Idle Timer expires.

- Contacts: If LISTAPP is non-null, the deskphone launches the Contacts application when the Web Idle Timer expires.
- Contacts: If LISTAPP is null and the local Contacts application is not empty, then the deskphone starts the local Contacts application when the Web Idle Timer expires. If the local Contacts application is empty, the deskphone displays the Avaya Screen.

**Note:**

The terms “Menu,” “Contacts,” and “Directory” are always administered in English. The terms are independent of the user interface language, since the deskphone does not directly present the value of IDLEAPP to the user. Instead, the term is used to present the appropriate local application, which does present the user interface in the user’s language.

If IDLEAPP is administered as “Directory”, and the Directory application is the ACP-based Integrated Directory, then the deskphone will have to reinstate the application approximately every minute, since the feature automatically times out after that interval.

If the screen saver is displayed, the Idle Application is not visible until the screen saver is removed. The screen saver is removed when the user goes off-hook, presses a button, or the deskphone receives an incoming call.

For example:

- To display an IDLEAPP when the deskphone has been idle for 30 minutes, Avaya recommends that you administer IDLEAPP as non-null, WMLIDLETIME to 30 and SCREENSAVERON to 999.
- To display a WMLSMALL URL when the phone has been idle for 30 minutes, Avaya recommends that you administer IDLEAPP as “ ” (null), WMLIDLETIME to 30, SCREENSAVERON 999, and WMLSMALL as a valid URL.
- To display the Avaya Screen Saver after 30 minutes of deskphone idle time, set IDLEAPP to “ ” (null), WMLIDLETIME to 999, WMLSMALL with a URL if Main Menu WML links are to be displayed, or null if you do not want it to display, and SCREENSAVERON to 30.

For examples of generic files to use as templates, seeSample 9610data.txt file on page 194, Sample idle.wml file on page 197, and Sample hotel.wml file on page 197.

## Accessing 9610 Craft procedures

Unlike the other 9600 Series IP Telephones, press the **Contacts** button twice instead of pressing **Mute** to access local procedures.

## Troubleshooting a 9610 IP Telephone

- If the Directory functionality is not present, make sure that you administer *Directory*, *Next*, and *Call-disp*. The *Call-disp* feature is displayed as *Make a call* on the deskphone on the CM station form in the first six call appearances/feature buttons. You can perform this activity only on releases prior to CM 4.0.
- The system will ignore any call appearances/features administered beyond the first six call appearances/feature buttons. You can perform this activity only on releases prior to CM 4.0 only.
- If calls cannot be received on the 9610, check the station administration for a *y* in the *Restrict Last Appearance* field. Change to *n* to allow incoming calls.
- If the *Ext#_9610data.txt* is not set up, the phone will default to the *9610data*.txt file.
- If the *9610data.txt* file is not set up, the deskphone displays the message *Restore Failed* and the default Avaya start screen. In this case, even if CM Directory is administered, the start screen appears and the Directory application will not be available.
- If the deskphone displays a *Restore Failed* message on the screen when you bring up a 9610, this indicates the deskphone could not find or load the backup file.

  Check the following:

  - The availability of file and folders and permissions.
  - The filename matches the required conventions for individual extensions or generic backup for all 9610 IP deskphones.
  - The 46xxsettings.txt file has a “Set BRURI http://xxx.xxx.xxx.xxx” entry, where “xxx.xxx.xxx.xxx” is the IP address of the HTTP server where the 9610data.txt file is stored.
  - There is a byte order mark (BOM) in the 9610data.txt file. The BOM is generated when the 9610data.txt file is saved in Unicode format.
- The WMLSMALL parameter must be non-null for Main Menu WML links to be displayed.

## Sample 9610data.txt file

```
##
## THE FOLLOWING "CON" SECTION IS
## THE DEFAULT 9610 "CONTACTS LIST"
## AND MAY BE POPULATED WITH REAL
## NAMES AND TELEPHONE NUMBERS
```

```
## OR EXTENSIONS FOR YOUR COMPANY.
## THE ITEMS WILL NOT APPEAR IN THE
## ORDER OF THE LABEL NUMBERS BUT
## RATHER, IN ASCII ALPHA ORDER. THE
## CONTACTS LIST MAY BE SELECTED
## USING THE 9610's RIGHT SIDE (BOOK)
## "CONTACTS" BUTTON. THE "CON"
## MENU WILL SCROLL IF MORE THAN 6
## LABEL GROUPS ARE CONFIGURED.
## NOTE: "+" BELOW INDICATES NON WORKING
## TELEPHONE NUMBERS.
##
CONLABEL001=c: Security+
CONDATA001=12345
CONLABEL002=b: Building Svc+
CONDATA002=9155555555555
CONLABEL003=d: Help+
CONDATA003=9155555555555
CONLABEL004=a: Audix+
CONDATA004=12345
CONLABEL005=9610-DEMO-ONLY+
CONDATA005=DUMMY
CONLABEL006=+NOT WORKING#'s
CONDATA006=DUMMY
##
## THE FOLLOWING ""MM" SECTION IS
## THE DEFAULT "MAIN MENU" AND
## NORMALLY APPEARS FOLLOWING
## A 9610 REBOOT OR POWER UP.
## THE ""MM" GROUPS MAY BE
## REPLACED WITH WML LINKS OR
```

```
## TELEPHONE NUMBERS APPROPRIATE
## TO YOUR INSTALLATION, INCLUDING
## THE IP ADDRESS OF YOUR FILE
## SERVER AND WML PATH. NOTE THAT
## WMLSMALL MUST BE A VALID URL FOR
## WML LINKS TO DISPLAY IN THIS MENU.
## THE "MM" MENU WILL SCROLL IF MORE
## THAN 6 LABEL GROUPS ARE CONFIGURED.
##
MMLBL01=ABOUT-9610
MMTYPE01=1
MMDATA01=http://135.8.60.18/WML/about.wml
MMLBL02=MyCo Today
MMTYPE02=1
MMDATA02=http://135.8.60.18/WML/index.wml
MMLBL03=MyCo Directory
MMTYPE03=4
MMDATA03=Directory
MMLBL04=Visitor Info
MMTYPE04=1
MMDATA04=http://135.8.60.18/WML/visit_lz.wml
MMLBL05=Printer Trouble
MMTYPE05=1
MMDATA05=http://135.8.60.18/WML/printer-rooms.wml
MMLBL06=Call Jack+
MMTYPE06=2
MMDATA06=32099
```

Note that the information entered into the backup or restore file is what controls the 9610 Main Menu. The references within the files are to ".wml" files, which are text Web pages and an example is provided for illustration only. The content of these files must be customized for specific phones or sites. The wml files can be placed at the root level or buried in a lower level directory if desired. Modify the Backup or Restore file and 46xxsettings file references accordingly.

## Sample idle.wml file

```
<?xml version="1.0"?>

<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN" "http://
www.wapforum.org/DTD/wml13.dtd">

<wml>
       <card id="splash" title=" ">
       <p align="center">
       <img src="img/IP Deskphone-X_w150_h70.wbmp" alt="Avaya IP Deskphone"/>
       </p>
       </card>
</wml>
```

## Sample hotel.wml file

```
<?xml version="1.0"?>

<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN"

"http://www.wapforum.org/DTD/wml13.dtd">

<wml>

<card id="
hotel"
 title="
Hotels"
>
<p><a href="
hotels/marriott_courtyard.wml"
>Marriott Courtyard</a></p>
<p><a href="
hotels/extended_stay.wml"
>Extended Stay</a></p>
<p><a href="
hotels/molly_pitcher.wml"
>Molly Pitcher</a></p>    <p><a href="
hotels/oyster_point.wml"
>Oyster Point</a></p>   <p><a href="
hotels/holiday_inn.wml"
>Holiday Inn</a></p>
<do type="
prev"
 label="
Back"
><prev/></do>
</card>

</wml>
```

# Glossary

| | |
|---|---|
| **802.1X** | An authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. |
| **ARP** | Address Resolution Protocol, used, for example, to verify that the IP Address provided by the DHCP server is not in use by another IP telephone. |
| **CA** | Certificate Authority, the entity which issues digital certificates for use by other parties. |
| **CELP** | Code-excited linear-predictive. Voice compression requiring only 16 kbps of bandwidth. |
| **CLAN** | Control LAN, a type of Gatekeeper circuit pack. |
| **CNA** | Converged Network Analyzer, an Avaya product to test and analyze network performance. Applies to IPv4 only.<br><br>This feature is not supported in Release 6.2 and later. |
| **DHCP** | Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management. |
| **Diffie -Hellman key exchange** | A key agreement algorithm based on the use of two public parameters p and g that may be used by all users in a system. Parameter p is a prime number and parameter g (usually called a generator) is an integer less than p. |
| **DH Group** | A number that determines the public parameters used by the Diffie-Hellman key exchange. To successfully establish a shared secret key, both parties must use the same DH group. |
| **DiffServ** | Differentiated Services, an IP-based QoS mechanism. |
| **Digital Certificate** | The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by a trusted third party known as a “Certificate Authority” (CA) such as VeriSign (www.verisign.com). The CA verifies that a public key belongs to a specific company or individual (the “Subject”), and the validation process the publick key goes through to determine if the claim of the subject is correct and depends on the level of certification and the CA itself. |

| | |
|---|---|
| **Digital Signature** | A digital signature is an encrypted digest of the file being signed. The file can be a message, a document, or a driver program. The digest is computed from the contents of the file by a one-way hash function such as MD5 or SHA-1 and then encrypted with the private part of a public or private key pair. To prove that the file was not tampered with, the recipient uses the public key to decrypt the signature back into the original digest, recomputes a new digest from the transmitted file and compares the two to see if they match. If they do, the file has not been altered in transit by an attacker. |
| **DNS** | Domain Name System, an IETF standard for ASCII strings to represent IP addresses. The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses. |
| **EAP-TLS** | Extensible Authentication Protocol, or EAP, is an authentication framework frequently used in wireless networks and Point-to-Point connections. EAP is defined in RFC 3748. EAP-Transport Layer Security (EAP-TLS), defined in RFC 5216, is an IETF open standard protocol, with strong security used by wireless vendors. EAP-TLS uses PKI to secure communication to a RADIUS authentication server or another type of authentication server. |
| **Gatekeeper** | An H.323 application that performs essential control, administrative, and managerial functions in the call server. Also known as CLAN in Avaya documents. |
| **H.323** | A TCP/IP-based protocol for VoIP signaling. |
| **HAC** | Hearing Aid Compatibility, an Federal Communications Commission (FCC), part of the United States government Part 68 standard for handset equalization for interoperability with t-coil enabled hearing aid devices. |
| **HTTP** | Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web. |
| **HTTPS** | A secure version of HTTP. |
| **IETF** | Internet Engineering Task Force, the organization that produces standards for communications on the Internet. |
| **IKE** | Internet Key Exchange Protocol, RFC 2409, which is now replaced by IKEv2 in RFC 4306. |
| **IPsec** | A security mechanism for IP that provides encryption, integrity assurance, and authentication of data. Applies only to IPv4. |
| **ISAKMP** | Internet Security Association and Key Management Protocol, RFC 2408, ISAKMP has been replaced by IKEv2 in RFC 4306. ISAKMP defines the |

| | |
|---|---|
| | procedures for authenticating a communicating peer, creation and management of Security Associations (SA), key generation techniques, and threat mitigation. Example: Denial of service and Replay Attacks. ISAKMP defines two phases of negotiation. During Phase 1 negotiation, two entities establish an ISAKMP SA, which is used to protect Phase 2 negotiations establish SAs for other protocols. |
| **LAN** | Local Area Network. |
| **LLDP** | Link Layer Discovery Protocol. All deskphones with an Ethernet interface support the transmission and reception of LLDP frames on the Ethernet line interface in accordance with IEEE standard 802.1AB. |
| **MAC** | Media Access Control, ID of an endpoint. |
| **Media Channel Encryption** | Encryption of the audio information exchanged between the IP deskphone and the call server or far-end telephone. |
| **NAPT** | Network Address Port Translation. |
| **NAT** | Network Address Translation, a mechanism by which IP addresses are mapped from one address space to another, and in which UDP and TCP port numbers are remapped to allow multiple devices to share the same IP address without port number conflicts. |
| **OPS** | Off-PBX Station. |
| **PHP** | Hypertext Preprocessor, software used to assist in the format and display of Web pages. |
| **PSTN** | Public Switched Telephone Network, the network used for traditional telephony. |
| **QoS** | Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks. |
| **Refresh/Rekey** | Use IKE to create a new SA with a new SPI. |
| **RSA** | Rivest-Shamir-Adleman: A highly secure asymmetric cryptography method developed by RSA Security, Inc. that uses a public and private key pair. The private key is kept secret by the owner and the public key is published, usually in a digital certificate. Data is encrypted using the public key of the recipient, which can only be decrypted by the private key of the recipient. RSA is very computation intensive, thus it is often used to encrypt a symmetric session key that is then used by a less computationally-intensive algorithm to encrypt protocol data during a “session”.You can also use RSA for authentication by creating a digital signature, for which the private key of the sender is used for encryption, and the public key of the sender' is used for decryption. |

| | |
|---|---|
| **RSVP** | Resource Reservation Protocol, used by hosts to request resource reservations throughout a network. Applies to IPv4 audio connections only. |
| **RTCP** | RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service. |
| **RTP** | Real-time Transport Protocol. Provides end-to-end services for real-time data such as voice over IP. |
| **SA** | Security Association, a security protocol, for example, IPSEC, TLS, and a specific set of parameters that completely define the services and mechanism necessary to protect security at that security protocol location. These parameters can include algorithm identifiers, modes, cryptographic keys, etc. The SA is referred to by its associated security protocol, for example, ISAKMP SA, ESP SA, and TLS SA. |
| **SCEP** | Simple Certificate Enrollment Protocol, used to obtain a unique digital certificate. |
| **SDP** | Session Description Protocol. A well-defined format for conveying sufficient information to discover and participate in a multimedia session. |
| **Signaling Channel Encryption** | Encryption of the signaling protocol exchanged between the IP telephone and the call server. Signaling channel encryption provides additional security to the security provided by media channel encryption. |
| **SIP** | Session Initiation Protocol. An alternative to H.323 for VoIP signaling. |
| **SLA Monitor Server** | SLA Mon Server is a network monitoring tool that constantly monitors customer network to detect network problems before the network problems affect applications and result in degradation of business critical applications. |
| **SNTP** | Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet. |
| **SOHO** | Small Office Home Office. The environment for which a virtual private network (VPN) is administered. |
| **SPD** | Security Policy Database. Specifies the policies that determine the disposition of all IP traffic inbound or outbound from a host or security gateway IPsec implementation. |
| **SPI** | Security Parameter Index. An identifier for a Security Association, relative to some security protocol. Each security protocol has its own “SPI-space”. |

| | |
|---|---|
| **SRTCP** | Secure Real-time Transport Control Protocol. |
| **SRTP** | Secure Real-time Transport Protocol. |
| **system -specific** | Specific to a particular type of call server. For example, Avaya Communication Manager or SIP Enablement Services (SES). *System-specific signaling* refers to messages specific to the signaling protocol used by the system. For example, H.323 and/or CCMS messages used by CM and IP Office, or SIP messages that possibly include system-specific headers used by SES. *System-specific procedures* refers to procedures in deskphone software that are specific to the call server with which the software is to be used. |
| **SSH** | Secure Shell (SSH) is a network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects through a secure channel over an insecure network. For example, a server running an SSH server program and a client running an SSH client program. |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol, a network-layer protocol used on LANs and internets. |
| **TFTP** | Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP telephones. |
| **TLS** | Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications. |
| **TLV** | Type-Length-Value elements transmitted and received as part of Link Layer Discovery Protocol (LLDP). |
| **UDP** | User Datagram Protocol, a connectionless transport-layer protocol. |
| **Unnamed Registration** | Registration with Avaya Communication Manager by an IP telephone with no extension. Such telephones allow limited outgoing calling. |
| **URI & URL** | Uniform Resource Identifier and Uniform Resource Locator. Names for the strings used to reference resources on the Internet. For example, HTTP://..... URI is the newer term. |
| **VLAN** | Virtual LAN. |
| **VoIP** | Voice over IP, a class of technology for sending audio data and signaling over LANs. |
| **VPN** | Virtual Private Network, a private network constructed across a public network such as the Internet. A VPN can be made secure, even though the network uses using existing Internet connections to carry data communication. Security measures involve encrypting data before |

| | |
|---|---|
| | sending data across the Internet and decrypting the data at the other end. To add an additional level of security, you can encrypt the originating and receiving network address. |
| **VSI** | Vendor Specific Information, used to determine IPv6 information. |
| **WML** | Wireless Markup Language, used by the 9600 Series IP Telephone Web Browser to communicate with WML servers. |

# Index

## Numerics


802.1X ..... 121
9600 Series IP deskphones ..... 165
customizing applications and options ..... 165
9600 Series IP Telephones ..... 11, 19, 83
Administering Options for ..... 83
Administration Alternatives and Options ..... 19
Customizable System Parameters ..... 83
overview ..... 11
9610 Craft Procedures ..... 193
9610 File Retrieval, General Processing ..... 162
9610 IP Telephone, Special Administration for ..... 168
9610 IP Telephone, Troubleshooting ..... 194
9610 Key Administration Concepts ..... 188
9610 Retrieval Procedures ..... 161
9620/9620C/9620L IP Telephone, Feature administration ..... 57


## A


Ad-Hoc Conferences ..... 61
administering ..... 48, 49, 110, 146, 180, 192
DIFFSERV ..... 49
guest user ..... 180
idle application ..... 192
QOS ..... 49
RSVP ..... 48
VLAN ..... 110
Administering ..... 180
Visiting Users ..... 180
Administering agent sign ins for call centers ..... 148
Administering deskphones for call center operation ..... 147
Administering Features ..... 56
Administering the Vu button ..... 150
administration ..... 19, 47, 63
call server ..... 47
DHCP and file servers ..... 63
administrative checklist ..... 23
administrative process ..... 22
Agent sign ins, administering for call centers ..... 148
Aliasing ..... 45
Alternatives, Administration ..... 19
Application File and Upgrade Script, Choosing ..... 78
Application Icons/Labels, for Home Screen ..... 174
Application Status Flag (APPSTAT) ..... 166
Application Status Flags and Their Meaning ..... 166
Application-specific parameters, administering ..... 19
APPSTAT ..... 166
Audio equalization ..... 146
Auto Hold administration ..... 54
Auto select any idle appearance administration ..... 56
Auto-answer ..... 152
Avaya ..... 168
Avaya Menu Administration ..... 173
Avaya Menu Administration File Template ..... 177
Avaya Menu with WML Applications ..... 171


## B


Backup ..... 156
Backup File Format, for the 9610 ..... 189
Backup File Formats ..... 156
Backup, Options and Non-Password Parameters Saved ..... 157
Backup/Restore ..... 155
Backup/restore processing ..... 72
Button Modules (SBM24 and BM12) ..... 60


## C


Call Center operation, administering deskphones for 147
call server ..... 45, 47
administration ..... 47
requirements ..... 45
call servers ..... 48
IP interface and addresses ..... 48
call transfer ..... 51
considerations ..... 51
Calltype Digit Analysis ..... 131
checklist, administrative ..... 23
Codecs, Wide Band ..... 62
Conference/Transfer on Primary Appearance administration ..... 56
Conferencing Call Considerations ..... 52
Contacts Application Administration, for the 9610 ..... 191
Contacts File Format for USB Devices ..... 184
Coverage Path administration ..... 54, 56
Custom Screen Saver, Administering ..... 145
Customizable System Parameters ..... 83

## D


DHCP ..... 33, 67
generic setup ..... 33, 67
DHCP ..... 67
DHCP Generic Setup ..... 64
DHCP options ..... 67, 70
DHCP server ..... 31
DHCP, Parameters Set by ..... 64
Dialing Methods ..... 131
Dialing, Enhanced, Requirements ..... 133
DIFFSERV ..... 49
administering ..... 49
DNS addressing ..... 115
document changes ..... 12


## E


EAP-TLS ..... 116–118, 120
authentication ..... 117
phones using MD5 ..... 118
scenarios ..... 118
without 802.1 authentication ..... 120
EC500 administration ..... 54
enabling ..... 116
SCEP support ..... 116
Enhanced Conference Features administration ... 54, 56
Enhanced Local Dialing ..... 131
Enhanced Local Dialing Requirements ..... 133
Enhanced Phone Screen Display ..... 59
Enhancements ..... 14
error conditions ..... 27


## F


Far End Mute administration ..... 56
Feature administration for all other deskphones (except 9610 and 9620/9620C/9620L) ..... 57
Feature Administration for Avaya Communication Manager ..... 54
Feature Numbers for Assigning Softkeys ..... 137
Feature-Related System Parameters, administering on CM ..... 54
Features, Administering on Softkeys ..... 137
File download ..... 78
Choosing the Right Application and Upgrade Script File ..... 78


## G


General Download Process ..... 77
Gigabit Ethernet Adapter ..... 130
GROUP parameter ..... 81


## H


hardware requirements ..... 29
Home screen ..... 137
managing applications ..... 137
Home Screen WML Application Icons/Labels ..... 174


## I


idle application ..... 192
administering ..... 192
IEEE 802.1D and 802.1Q ..... 33
IEEE 802.1Q ..... 49
IEEE 802.IQ QoS parameters ..... 49
initialization process ..... 24
installation ..... 31
required network information ..... 31
Interface, administering the ..... 19
IP address lists ..... 35
Station Number Portability ..... 35
IP Addresses, administering ..... 19
IP interface and addresses ..... 48
call servers ..... 48
IPv4 and IPv6 operation ..... 74
IPv6 ..... 74
IPv6 Limitations ..... 75


## L


Language Selection ..... 128
legal notices ..... 2
Link Layer Discovery Protocol (LLDP) ..... 123
LLDP Data Units Transmitted ..... 123
local administrative ..... 128
options ..... 128
Log Digit (Smart Enbloc) Dialing ..... 131


## M


Main Menu (MM) Administration, for the 9610 ..... 190


## N


NAT ..... 49
network assessment ..... 29
network audio quality display ..... 34
Network Considerations, Other ..... 31

new features ..... 14

## O

On-Hook Dialing administration ..... 54
OPSTAT ..... 83, 170
options ..... 128
    local administrative ..... 128
options, ..... 83
    administering ..... 83
options, customizing ..... 165
Options, for 9600 Series IP Telephone Administration 19
Other Network Considerations ..... 31
overview ..... 11
    9600 Series IP Telephones ..... 11

## P

Parameter Data Precedence ..... 22
parameters in real-time ..... 34
Parameters Saved During Backup ..... 157
parameters, customizable ..... 85
Parameters, Customizable ..... 83
phone ..... 25, 26, 53
    network initialization ..... 25
    administration ..... 53
    call server initialization ..... 26
    file server initialization ..... 25
    initialization to DHCP server ..... 25
pictures, as screensaver ..... 185
ping ..... 32
port selection ..... 48
    UDP ..... 48
port utilization ..... 35
    TCP/UDP ..... 35
Processing, General, for 9610 Restore ..... 162
Processor Ethernet (PE) ..... 83

## Q

QoS ..... 19, 33, 49
    administering ..... 49
    Administrative Parameters ..... 19
    IEEE 802.1Q ..... 49
Qtest for Audio Quality ..... 35

## R

Realease 6.0 ..... 17
Registration and Authentication ..... 41
related documentation ..... 9
required network information ..... 31
requirements ..... 29, 30, 45
    call server ..... 45
    hardware ..... 29
    server ..... 30
Restore ..... 159
Restore File, for 9610 ..... 160
Restore/Backup ..... 155
Restrict Last Call Appearance administration ..... 56
Retrieval Procedures, for 9610 ..... 161
RSVP ..... 48
    administering ..... 48

## S

SCEP support ..... 116
    enabling ..... 116
Screen Saver, Administering ..... 145
Secure Shell Support ..... 41
security ..... 40
Send All Calls (SAC) administration ..... 56
server ..... 30
    requirements ..... 30
settings file ..... 79
Shuffling ..... 62
signaling protocol, changing ..... 79
Smart Enbloc Dialing ..... 131
SNMP ..... 32
    enabling ..... 32
Softkeys, Administering Features on ..... 137
Software ..... 78
Software prerequisites ..... 63
Software, Telephone ..... 78
SRTP ..... 35
SSO logon ..... 109
SSON, Option 242, configuring ..... 64
station administration ..... 56
Station Form Administration Results Chart ..... 57
Station Number Portability ..... 35
    IP address lists ..... 35
Stopwatch timer, administering ..... 182
Supplicant Operation, 802.1X ..... 122
support ..... 10
    contact ..... 10
Switch Compatibility and Aliasing IP Telephones ..... 45
System Parameter Values, Impact of Received TLVs 123
System Parameters ..... 54
system parameters, customizable ..... 85
System Parameters, Customizable ..... 83

## T


Tagging and VLAN, administering ..... 19
Telephone Administration ..... 19
Time-to-Service (TTS) ..... 42
Timer Operation ..... 180
TLS ..... 35
TLVs Received, Impact on System Parameter Values ..... 123
Touchscreen Deskphones, Special Considerations for ..... 61
traceroute ..... 32
training ..... 10
Troubleshooting a 9610 IP Telephone ..... 194


## U


UDP ..... 48
port selection ..... 48
UDP/TCP Port Utilization ..... 35
Unnamed Registration ..... 26
Upgrade Script and Application File, Choosing the Right ..... 78
upgrading ..... 79
USB Devices, Contacts File Format for ..... 183, 184
USB Devices, requirements for ..... 183
USB pictures ..... 185
User stopwatch timer, administering ..... 182


## V


VLAN ..... 110
administering ..... 110
VLAN Default Value ..... 111
VLAN detection ..... 111
VLAN Separation Rules ..... 112
VLAN Tagging ..... 110


## W


warranty ..... 10
What's changed ..... 17
What’s New ..... 15
Wide Band Codecs ..... 62
Wideband Audio administration ..... 54
Wireless Headset ..... 152
WML Application Display, on Home screen ..... 174