Administering 9608/9608G/9611G/9621G/ 9641G IP Deskphones H.323

Release 6.4
16-300698
Issue 19
June 2014

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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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 or such successor site as designated by Avaya. 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN 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 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, with the exception of Heritage Nortel Software, 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. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance 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, Instance, 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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 or Hosted Service 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”). As required, 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 or such successor site as designated by Avaya. 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 or such successor site as designated by Avaya. 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, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), 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

Intended Audience

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

Related resources

Documentation

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

See the following related documents at support.avaya.com.

Document number	Title	Use this document to:	Audience
Overview			
16-604299	Avaya 9600 Series H.323 IP Deskphones Overview and Specifications	Refer to the overview and specifications.	People who want to gain a high-level understanding of the product features, functions, capacities, and limitations.
Using			
16–603593	Using Avaya IP Deskphone 9608, 9608G, and 9611G	Refer to tasks related to using the deskphone.	End users and administrators
16–603594	Using Avaya IP Deskphone 9621G and 9641G	Refer to tasks related to using the deskphone.	End users and administrators

Document number	Title	Use this document to:	Audience
16-603613	Using Avaya IP Deskphone H. 323 9608, 9608G, 9611G, 9621G, and 9641G in the Call Center	Refer to tasks related to using the deskphone in a call center environment.	End users and administrators
Implementing			
16–603603	Installing and maintaining Avaya IP Deskphone H.323 9608, 9608G, 9611G, 9621G, and 9641G	Refer to procedures related to installing and upgrading the 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

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, 9608G, 9611G, 9621G, and 9641G 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, 9608G, 9611G, 9621G, and 9641G 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, 9608G, 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, 9608G, 9611G, 9621G, and 9641G Series IP deskphones:

- 9600 Series IP Telephones
- 9600 Series IP Deskphones

- H.323 deskphone
- Deskphone
- IP telephone
- Phone

New in this release

With H.323 Release 6.4, the following features have been introduced:

- New media quality indication on the top line of the phone for the following conditions:
  - Call uses wide band codecs
  - Phone detects poor network quality which impacts audio quality.
- Added support for French on-screen keyboard. This feature is enabled when French locale is configured.
- Addition of missed calls to call log for calls received when phone is offline. With this feature enabled, after a user logs in, the user is able to see call history even for up to 10 calls that the phone received after the user logged out. The phone call log can be synchronized with the call log of a Avaya one-x communicator (H323). This feature requires administration on Communication Manager.
- Support for the new global (Icons Only) version of the 9611 phone.
- Added support for Service Level Agreement (SLA) monitor. This feature requires the installation of the Avaya Diagnostic Server (ADS).
- Support for querying the phone Hardware revision through SNMP.
- IDLEFEATURES parameter settings now saved in a non-volatile memory thus retaining the information after power down or reboot.
- SSH remote debug capability has been extended and includes now a wider commands set. In addition, there is a new option in the phone's DEBUG menu to enable the SSH on the fly, without performing a reboot. Note: This works only when the value of SSH_ALLOWED parameter is set to 2 in the 46xxsettings file.
- Added a new soft keys layout that can be configured in the settings file by setting the existing parameter AGTACTIVESK to a value of 3. The soft keys would be labeled as an active call in a -call center environment from left to right: Hold, Conf, Transfer, Drop.
- Addition of the following new parameters:
  - CALL_LOG_JOURNAL -To trigger restore of offline call log journal
  - PHNSCRCOLUMNS - To set column width for phone
  - QLEVEL_MIN - To specify the minimum quality level below which the LNQ icon is not displayed.

- WBCSTAT - To indicate the use of a wideband codec.
- AGENTGREETINGSDELAY - To specify the delay time for playing the agent greeting.
- SLMCAP - To specify whether the SLA monitor agent supports packet capture.
- SLMCTRL - To specify whether the SLA monitor agent supports device control.
- SLMPERF - To specify whether the SLA monitor supports performance monitoring.
- SLMPORT - To specify the UDP port used to receive commands from SLA monitor server.
- SMMSRVR - To specify source IP address and source port number for messages from the SLA monitor server.
- SLMSTAT - To specify whether the SLA monitor agent would be enabled.
- SLMTEST - To specify the UDP ports used for the RTP and traceroute tests.

Changes in Release 6.3.1

With Release 6.3.1, Avaya introduced the 9608G Gigabit IP Deskphone. The 9608G offers all of the features of the 9608 IP deskphone, and adds Gigabit network connectivity and an Ethernet activity LED.

Changes in Release 6.3

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

Enhancement	Description
New parameters **Note:** For more information on the new parameters, see 9600 Series H.323 customizable system parameters on page 68.	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. 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.

Enhancement	Description
	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. **Note:** 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.
HTTP redirect	The HTTP redirect feature directs IP phones to download software from the nearest server on the network, thereby reducing download time. See HTTP Redirect feature on page 50.

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 delivered 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.

Chapter 3: Administration overview and requirements

Administrative requirements

This topic outlines the operating environment for the 9600 Series IP deskphones as follows:

- Telephone Administration on the Avaya call server. For more information, see Communication Manager Administration on page 39.
- IP Address management for the deskphone. For more information see, Administering the DHCP and File Servers on page 49 for dynamic addressing.

  For more information about static addressing, see *Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*,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 About VLAN Tagging on page 91 and Administering a VLAN on page 91.
- Quality of Service (QoS) administration for the phone, if appropriate. For more information, see QoS on page 29 and Administering QoS on page 40.
- 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 26.

  Administer the deskphone to computer interface using the PHY2 parameter.

  For more information, see, *Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*,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 128. An example of application-specific data is Web-specific information required for this optional application.

The table on page 16 indicates that you can administer system parameters in many ways and use many delivery mechanisms. For example:

- Maintaining the information on the call server.
- Manually entering the information with 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.

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 39, Server Administration on page 49, and the applicable call server documentation.
IP Addresses	DHCP	Administering the DHCP and file servers on page 49 and especially Administering the DHCP server on page 53.
	Configuration file	Understanding the general download process on page 63 and Administering options for IP phones on page 67.
	Manual administration at the deskphone	“Static Addressing Installation” in *Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323* Guide.
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 100
Tagging and VLAN	DHCP	Administering The DHCP Server on page 53, and Administering options for IP phones on page 67.
	Configuration file	Administering The DHCP and File Servers on page 49 and Administering options for IP phones on page 67.
	LLDP	“Static Addressing Installation” in *Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*.
	Manual administration at the phone	About Link Layer Discovery Protocol (LLDP) on page 100.
Quality of Service	Avaya call server	Administering UDP port selection on page 40 and the applicable call server documentation.
	DHCP	Administering The DHCP and File Servers on page 49, and Administering options for IP phones on page 67.
	Configuration file	Administering The DHCP and File Servers on page 49, and Administering options for IP phones on page 67.
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 100.

Parameter	Administrative mechanisms	Related information
Interface	DHCP	Administering The DHCP and File Servers on page 49, and Telephone Software and Application Files on page 63.
	Configuration file	Administering The DHCP and File Servers on page 49, and Telephone Software and Application Files on page 63.
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 100.
	Manual administration at the phone	“Secondary Ethernet (Hub) Interface Enable or Disable” in*Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*.
Application - specific parameters	Configuration file	Administering The DHCP and File Servers on page 49, and especially HTTP Generic Setup on page 57. Also, Administering Applications and Options on page 128.
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 49, and more specifically, Administering the DHCP Server on page 53. For information on administering HTTP servers, see Administering the DHCP and File Servers on page 49, and more specifically, HTTP Generic Setup on page 57. For administration options, see Administering options for IP phones on page 67.

Parameter data precedence

If you administer a parameter 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 54.
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

To administer the 9600 Series IP deskphone, complete the tasks in the order shown.

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 9608, 9608G, 9611G, 9621G, and 9641G H.323*,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 each 9600 Series IP deskphones using Craft procedures, as applicable. For more information about Local Administrative Procedures, see *Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*.

Administrative checklist

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

Table 2: Administrative Checklist

Task	Description	Related information
Network requirements assessment	Determine that network engineers have installed the network hardware and the network hardware can handle phone system requirements.	Network Requirements on page 26.
Call server administration	Verify that the administrator has installed the license of the call server and administered the system for Voice over IP (VoIP). Verify that the administrator has administered each phone as required.	Communication Manager Administration on page 39.
DHCP server installation	Install a DHCP application on at least one new or existing computer on the LAN.	Vendor-provided instructions.
DHCP application administration	Add IP deskphone administration to DHCP application.	Administering The DHCP Server on page 53 in Server Administration on page 49.

Task	Description	Related information
HTTP/HTTPS server installation	Install an HTTP or HTTPS application on at least one new or existing computer on the LAN.	Vendor-provided instructions.
Application files, script file, and settings file installation on the HTTP or HTTPS server.	Download the files from the Avaya support site.	www.avaya.com/support Telephone Software and Application Files on page 63.
Settings file modification as you want.	Edit the settings file as required, using your own tools.	Telephone Software and Application Files on page 63.
WML servers administration	Add WML content as applicable to new or existing WML servers. Administer the content that the WML push servers push on to the deskphones 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 66 and the *Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*, 16-300694 for all, but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608,9608G, 9611G, 9621G, and 9641G deskphones.
	Individually:	The applicable Craft Local Procedures in the *Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*, Document Number 16-300694 for all, but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608,9608G, 9611G, 9621G, and 9641G deskphones.
Phones installation in the network		*Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*, Document Number 16-300694 for all, but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608, 9608G, 9611G, 9621G, and 9641G deskphones)
User modification of Options, if applicable		OPSTAT and the respective User Guide for the specific deskphone model.

Task	Description	Related information
VPN functionality administration if applicable	Enable or 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 includes exchange of information that happens when the phone initializes and registers. The process includes the following five steps. This description assumes that you have properly administered all equipment ahead of time. See *Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*, 16-603603 covering the 9608, 9608G, 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*.

You must administer all equipment properly prior to initialization.

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.

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 49. Among other data passed to the phone is the IP address of the HTTP or HTTPS server.

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 63.

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 68.

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 9608, 9608G, 9611G, 9621G, and 9641G H.323*,16-603603.

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
9641G	4620	9650	9641G

9600 Series IP deskphone model	Administer on Communication Manager 3.1 as...	Administer on Communication Manager 4.0+ – 6.1	Communication Manager 6.2
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:

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 46.

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.

SLA Monitor Server

Release 6.4 includes support for using the SLA. monitor. This feature requires the installation of an ADS (Avaya Diagnostic server).

SLA Mon™ technology is a patented Avaya technology embedded in Avaya products to facilitate advanced diagnostics. The technology works in a server-agent model where an SLA Mon server controls the actions of SLA Mon agents to execute advanced diagnostic functions consisting of the following:

- Endpoint Diagnostics
  - The ability to remotely control IP phones, to assist end users with IP Phone configuration and troubleshooting.
  - The ability to remotely generate single and bulk test calls between IP phones.
  - The ability to remotely execute limited packet captures on IP phones to troubleshoot and diagnose IP phone network traffic.
- Network Monitoring
  - The ability to monitor multiple network segments for performance in terms of packet loss, jitter, and delay.
  - The ability to monitor hop-by-hop QoS markings for voice and video traffic.

Note:

In case the settings file already includes the trust certificates list in the TRUSTCERT setting file parameter, then the SLA monitor root certificate must also be added to the list and placed as the first certificate.

For example: SET TRUSTCERTS *slamonRootCA.crt, rootCertRNAAD.cer*

In case the ADS Server is installed with the default Avaya certificate, then the phone must use the default Avaya root certificate which is included as part of the phone package and is called *slamonRootCA.crt*.

Note that Avaya does not recommend the use of default certificate for ADS server as it is non-unique certificate and can expose the equipment to security risk. In order to avoid this risk, obtain and install unique certificates on both ADS server and relevant trusted certificate on the phone.

Error conditions

Assuming proper administration, most of the problems reported by phone users are likely to be LAN-based or 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 traffic 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 40.

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 site https://support.avaya.com/CompatibilityMatrix/Index.aspx.

To ensure that you administer the appropriate circuit packs on your server, see Communication Manager Administration on page 39.

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 9608, 9608G, 9611G, 9621G, and 9641G H.323*,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 49.
- HTTP or HTTPS server:Administer the HTTP or HTTPS file server as described in HTTP Generic Setup on page 57.
- Web and Push servers (optional): If users have access to corporate WML web sites, administer the deskphones as described in Server Administration on page 49. 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 folders on the WML server that contain push content.

  Note:

  The system supports Push 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 coexist on one hardware unit. Use any standards-based server.

For parameters related to Avaya Server information, see Communication Manager Administration on page 39, and the administration documentation for your call server. For parameters related to DHCP and file servers, see Server Administration on page 49.

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 the default administration and continue with the call server registration process. Not all features are available. To restore the features, you must reset the deskphones when the file server is available.

Required network information

Before you administer DHCP, HTTP, and the HTTPS servers, collect the following 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 you install the phones.

The 9600 Series IP deskphones support specifying a list of IP addresses for a gateway/router, HTTP or 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, you must use DNS names that are fully qualified. For more information about DNS, see DHCP Generic Setup on page 53 and DNS addressing on page 93.

Required network information before installation for each DHCP server

- Gateway router IP addresses
- If the HTTP or the HTTPS file server IP addresses, port number, are different from the default, and the directory path if files are not located in the root directory
- Subnetwork mask
- Avaya call server IP address or addresses
- Phone IP address range
- DNS server address or addresses if applicable

As the LAN or System Administrator, you must also:

- Administer the DHCP server. See Server Administration on page 49.
- Edit the configuration file on the applicable HTTP or HTTPS file server. See Choosing the right application file and upgrade script file on page 64.

Other network considerations

Enabling SNMP

The 9600 Series IP deskphones support SNMPv2c and Structure of Management Information Version 2 (SMIv2). The phones also respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. The phones 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 with network management tools. H.323 Release 6.4 onwards, SNMP can be used to query the hardware revisions on the phone.

You can restrict the IP addresses from which the phones accepts SNMP queries using 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 49 and 9600 Series H.323 customizable system parameters on page 68.

Note:

SNMP is disabled by default. Administrators must start 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 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 phone to originate a ping or a traceroute to a specified IP address. The phone carries out that instruction and sends a message to the call server indicating the results. For more information about administering an IP telephone system on Communication Manager, see *Administrator Guide for Avaya Communication Manager*, 03-300509.

IP address and settings reuse

After you successfully register the phone with a call server, the phone saves the IP address and the parameter values 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 no response is received for 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 the QoS initiatives, see your LAN equipment documentation. For information about QoS implications for the 9600 Series IP deskphones, see Administering QoS on page 40.

All 9600 Series IP deskphones provide some detail about network audio quality. For more information, see Network Audio Quality Display on page 30.

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 40 and Administering a VLAN on page 91. 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 10 ms latency and jitter
- 5: Video traffic with less than 100 ms 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 gain access to 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. The system counts late and out-of-sequence packets as lost if the packets are discarded. The system does not count the packets as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.

Parameter	Possible values
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 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 that is introduced by the jitter buffer of the phone.

The implication for LAN administration depends on the values the deskphone user reports and the topology, loading, and QoS administration for the LAN. 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.

IP address list and station number portability

You can specify IP address lists on the 9600 Series IP deskphones. On startup or on restart, 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 call server denies communication with the phone or the session times out, the phone continues to the next address on the appropriate list and tries that IP address. The phone does not report failure unless all addresses on a specified 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 has 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. The local DHCP server if configured correctly, 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 49.

For more information on DNS addressing, see DNS Addressing on page 93.

TCP/UDP Port utilization

9600 Series IP deskphones use many 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 more TCP/UDP port utilization information related to Communication Manager, see UDP Port Selection on page 40.

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

Note:

Often, 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 67.

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 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 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 that are sent by the HTTP client on the phone	Any	TLS/SSL packets that the HTTP client receives on the phone	TCP
68	Any	Received DHCP messages	UDP
161	Any	Received SNMP messages	UDP
500	Any	Received DHCPv6 messages	UDP
1024 – 5000 (ephemeral port selected by O/S)	Any	Received Traceroute, HTTPS, HTTP messages	UDP
1720	Any	Received H.323 signaling messages	TCP
49,300 – 49,309	Any	Received RAS messages	UDP
2048 – 3029	Any	Received RTP, RTSP, SRTP, and SRTCP messages	UDP

Destination port	Source port	Use	UDP or TCP?
500, 2070, or 4500	500 or 4500	Received IKE or IPsec messages (if NVIKEOVERTCP is 0 or 1)	UDP
1720	Any	H.323 signaling messages	TCP
The number used in the Source Port field of RAS packets that are 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 that are sent by the SLA agent on the phone	Any	Received SLA registration messages	TCP

Note:

SLA and CNA not supported in H323 Release 6.3 and later.

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 that are received by the SSH server of the phone.	22	Packets that are transmitted by the SSH server of the phone	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 that the HTTP client transmits on the phone during startup	TCP
80 unless explicitly specified otherwise, for example, in a URL or because of use of WMLPORT	Any unused port number	Packets that the HTTP client of the phone transmits after startup, for example, for backup and restore or push	TCP

Destination Port	Source Port	Use	UDP or TCP?
The number used in the Source Port field of the SNMP query packet that the phone receives	161	Transmitted SNMP messages	UDP
The number used in the Source Port field of packets that are received by the HTTP server of the phone	Release 2.0+ = PUSHPORT Pre-Release 2.0 = 80	Packets that the HTTP server of the phone transmits	TCP
Release 2.0+ = TLSPORT Pre-Release 2.0 = 411	Any unused port number	TLS/SSL packets that the HTTP client of the phone transmits during startup	TCP
443 unless explicitly specified otherwise, for example in a URL	Any unused port number	TLS/SSL packets that the HTTP client of the phone transmits 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
Specified by CM (default is 5005)	Any unused port number	Transmitted RTCP messages	UDP
18414	Any unused port number	Transmitted SSO status indications	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
1719		Transmitted H.323 RAS messages	UDP
2048 – 3029		Transmitted RTP, RTCP, SRTP, and SRTCP messages	UDP
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

Destination Port	Source Port	Use	UDP or TCP?
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 for each 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 port number if the port used for RTP is odd	RTCP packets transmitted to an RTCP monitor	UDP
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
Determined by SNMP mgmt app	Any unused port number	Transmitted SNMP messages	UDP
Determined by the SSH client or the O/S of the client	Any unused port number	Transmitted SSH messages	TCP

Security

For information about toll fraud, see the respective call server documents on the Avaya Support website. The 9600 Series IP deskphones cannot guarantee resistance to all Denial of Service (DoS) attacks. However, checks and protections are in-built 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 nonvolatile 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 the values 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 the deskphone displays crucial network information or uses the information. For more information on these options, see Server Administration on page 49.

- 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 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 security-related parameters, SNMP community string (SNMPSTRING), SNMP Source IP addresses (SNMPADD), and Craft Access Code (PROCPSWD) that is administered on the call server. Download the file 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.

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.

You can also administer the *SSH_IDLE_TIMEOUT*parameter to configure the duration of inactivity that will disable SSH.

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 the gatekeeper list, use this new connection to replace an existing connection, and continue operation without the need to reregister. With this mechanism, Communication Manager starts a new connection to each deskphone during a server interchange. These phones then move quickly to the server and transition from the standby to active state.

The 9600 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 you have installed the proper hardware and your call server software is compatible with 9600 Series IP deskphones. Use the latest PBX software and IP phone firmware.

Call server administration

For call server administration information not covered in this chapter, see the following documents on the Avaya Support website :

- *Administering Avaya Aura Communication Manager*, 03-300509 for more instructions for administering an IP phone system on Communication Manager.

  For information on the process of adding new phones, see chapter 6,*Managing Telephones*. For related 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.

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 9608, 9608G, 9611G, 9621G, and 9641G H.323*, 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 website.

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.

You can fully enable RSVP by provisioning CM ip-network-region.

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 through LLDP, or by appropriate administration of the DHCP or HTTP/HTTPS servers.

You can administer the IEEE 802.IQ QoS parameters 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 9608, 9608G, 9611G, 9621G, and 9641G H.323*, 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 website.

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 22.

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 68.

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 **Join** softkey for the conference to be completed. If the user hangs up during conference setup before pressing **Join**, 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, and then press the **Join** 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 user to add the next conferee. 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 cancels the conference set up. Note: The initial conference is placed on soft hold when **Conference** or **Add** button is pressed.
- 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 user must not answer the call, or the user must answer the call and then hang 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 about call transfers, see Administering call transfers on page 42.

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 SAT provides the system-wide CM form and the particular page or screen that you need to administer for each feature. You need Communication Manager 3.1.2 or later.

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 set 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 change. This is a sample of the Class of Restriction form.
EC500	Enable EC500 on the Off-PBX Telephones Station Mapping form if you 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

Name	Description
	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. 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). 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. The Station form comprises of 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 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 66. 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 22.

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 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 47 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 9630/9630G 9640/9640G	9650/9650C	9670G/9621G/ 9641G
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 BM12/SBM24	1st BM12/ SBM24	1st BM12/SBM24

Feature / Call Appearance (CA) / Bridged Call Appearance (BA) buttons on the Station form...	Displayed as:			
49 to 72	N/A	2nd BM12/SBM24	2nd BM12/ SBM24	2nd BM12/SBM24
73 to 96	N/A	3rd BM12/SBM24	3rd BM12/ SBM24	3rd BM12/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.

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 the HTTP server software on the same computer.

Caution:

The firmware in the 9600 Series IP Deskphones reserves the 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 the 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 the 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 is available when the IP deskphone restarts.
- A DHCP server is 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) under Deskphone initialization process overview on page 20.

In addition, you can edit the settings file to customize phone parameters for your specific environment. For more information, see Administering options for IP phones on page 67.

HTTP Redirect feature

HTTP redirection allows you to configure and use multiple servers to download files to IP phones without the need to configure different values of HTTPSRVR (or TLSSRVR) for different groups of phones.

You do not any special configuration on the phone. The phone responds automatically to HTTP redirection requests from the HTTP server.

Using this feature you can:

- Spread the load across multiple servers. This feature allows local file servers to be used to avoid bottlenecks caused by low bandwidth WAN links to remote locations.
- Use this capability for firmware upgrades, backup or restore and agent greeting download.

The feature supports the following HTTP Redirection response codes:

- 301 (Moved Permanently)
- 302 (Found)
- 303 (See Other)
- 307 (Moved Temporarily)

To be able to use this feature, you must configure the central file server to support HTTP Redirection to an appropriate alternate server. See the Microsoft website for more information and examples on configuring HTTP Redirection on IIS7 server.

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 which the 9600 Series IP Deskphones do not support for setting through DHCP in option 242, 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.

Parameter	Description
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.
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.

Parameter	Description
	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.
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.

Administering the DHCP server

This document describes how to administer a single LAN segment, which is the simplest configuration. But you can use the same information for more complex LAN configurations.

Caution:

Before you start, understand your current network configuration. An improper installation might cause network failures or reduce the reliability and performance of your network.

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 DHCP application might work if the DHCP server is correctly configured.

Note:

Avaya does not assume responsibility for configuring your DHCP server. Contact your vendor or supplier for configuring 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 the 9600 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 93.
     - **Option 51: DHCP lease time**. If the deskphone does not receive this option, the deskphone does not accept the DHCPOFFER. 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 required by RFC 2131, Section 3.3. In this case, the deskphone does not require renewal and rebinding procedures even if you receive Options 58 and 59.

       Expired leases cause 9600 Series IP Deskphones to restart. Avaya recommends providing enough leases so the IP address of a 9600 Series IP Deskphone does not change if you briefly take the phone offline.

       Note:

       The DHCP standard states that when a DHCP lease expires, the device must immediately cease using the assigned IP address. However, if the network has problems and the you centralize the DHCP server, or if the DHCP server 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 restart because you can renew expired leases. However, if the new IP address is different than the previous, the phone

restarts. Ensure that after an IP address is assigned, 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 68.If you invoke the default after the DHCP lease expires, the phone continues to broadcast DHCPREQUEST messages for the 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 the 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 for one day or more. For example, Windows NT® DHCP reserves expired leases for about 1 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 you remove the other two deskphones from the network, the third deskphone remains without a lease until the reservation period expires.

- **Option 52: Overload Option**, if required. If the 9600 Series IP Deskphone receives this option in a message and 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 phone uses the default value of T1 (renewal timer) according to 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 phone uses the default value of T2 (rebinding timer) according to 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 you administer the key information, especially HTTPSRVR and MCIPADD 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 56 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.

Because 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 the parameter values were previously set by LLDP. For more information, see About Link Layer Discovery Protocol (LLDP) on page 100.

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 67.

In configurations where the upgrade script and the 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 62. 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.

Administering the DHCP server

This document describes how to administer a single LAN segment, which is the simplest configuration. But you can use the same information for more complex LAN configurations.

Caution:

Before you start, understand your current network configuration. An improper installation might cause network failures or reduce the reliability and performance of your network.

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 49.

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 suitable HTTP application. Commonly used HTTP applications include Apache® and Microsoft® IIS™.

Important:

You must use the Avaya Web configuration server to get HTTPS so that information is authenticated. The Avaya Web configuration server does not support backup or 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 Support website to the HTTP server.

   For more information, see Telephone Software and Application Files on page 63.

   Note:

   When you download the application file from the Avaya Support website, 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 and also 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 HTTP client to back up and restore the user-specific data indicated in User data saved during backup on page 124. Release 1.5 and later support HTTP over TLS (HTTPS) for backup or restore. For backup, the deskphone creates a file with all 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 a failure confirmation.

The phone stores the authentication credentials and the realm in non-volatile memory that is not 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.

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.

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.

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 method is intended for use by the Avaya IP Telephone File Server Application so that the phone requesting the file transaction can be authenticated. You can downloaded the Avaya IP Telephone File Server Application from the Avaya Support website.

If no digital certificates are downloaded based on the system parameter TRUSTCERTS, the phone establishes a TLS connection only to a backup and restore file server that has a Avaya-signed certificate. The Avaya certificate is 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 method 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.

Both backup and restore operations support HTTP/HTTPS authentication. 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.

With TLS, the phone uses a TLS_RSA_WITH_AES_128_CBC_SHA cipher suite. If TLS is used but no digital certificates are 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 gets 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 through the secure TLS connection.

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

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 the 9600 Series IP Deskphones or the Prompt Line for all other 9600 Series IP Deskphones display an HTTP Authentication or an HTTP Authentication Failure interrupt screen: `Enter backup/restore credentials`.

New values replace the stored authentication and realm values:

- When HTTP authentication for backup or restore succeeds and
- If the userid, password, or realm used differs from those values that are 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 or restore, see the *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*.

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 62. 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 programmed 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	1	IPv4 only	DHCP	n/a
		Yes	2	IPv6 only	n/a	DHCPv6
			3	dual-stack	DHCP	DHCPv6
			1 or 3	dual-stack	DHCP	manual
			2	IPv6 only	n/a	manual
Yes	0	n/a	n/a	IPv4 only	manual	n/a

Manually program-med IPv4 address?	IPV6STAT	Manually programmed IPv6 address	DHCPSTAT	Result	Addressing Mode(s)	
	1	No Yes	1 2 or 3 n/a	IPv4 only dual-stack dual-stack	manual manual manual	n/a DHCPv6 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

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 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 deskphone downloads the trusted certificates, HTTPS ensures that the file server is authenticated through a digital certificate. The deskphone does not use HTTPS 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 you first plug in the 9600 Series IP deskphone, 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 can 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 before 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 the phones in your network. For more information about the settings file, see About the settings file on page 64. After downloading the settings file, the phone downloads the language or the certificate files and then any new software files that the settings require.

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 website.

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

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 9608, 9608G, 9611G, 9621G, and 9641G H.323*, 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 website 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 68 .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 and the groups the phones belong to, 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. You can only set the GROUP parameter either at each individual deskphone or when a you register a phone with Software Release 1.5 or greater to an Avaya Aura® Communication Manager Release 4.0 or greater.

   To set the GROUP parameter on each deskphone, use the GROUP procedure from the local administrative options. 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 the GROUP parameter on a phone-by-phone basis on the Communication Manager Station Form.

3. After you assign the GROUP assignments, edit the configuration file to enable each phone of the appropriate group to download the 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, see 9600 Series H.323 customizable system parameters on page 68

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 49. For HTTP, set the parameters to required values in the settings file. For more information, see About the settings file on page 64.

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 not null and consists of one to seven 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 is 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 getting access to local procedures unless you administer the parameter using page 3 of the system-parameters IP-options form in 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 62. 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: 1 = Use handset equalization that is optimized for acoustic TIA 810/920 performance. 2 = Use handset equalization that is optimized for electrical FCC Part 68 HAC telecoil performance.

Parameter name	Default value	Description and value range
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.
AGENTGREETINGSDELAY	700	Valid values: 0 – 3000 where the value specifies the delay time (milli seconds) between call autoanswer and playing of an agent greeting.
AGTACTIVESK	0	Used to control the softkeys that are available to the agent on the deskphone. If value = 0, Transfer softkey is available on the second row of softkeys, and Release on the first row. If value = 1, Release softkey is available on second row of softkeys, and Transfer on the first row. If value = 2, Release softkey is not available on first/ second row of softkeys, because there can be more softkeys with value 2 other than mentioned. If value =3, On an active call, the soft keys are labeled from left to right: Hold, Conf, Transfer, Drop in a non-call center environment.
AGTCALLINFOSTAT	1	For Avaya Call Center use only. 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. 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 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:

Parameter name	Default value	Description and value range
		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 **Note:** 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 (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

Parameter name	Default value	Description and value range
		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, 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.
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.

Parameter name	Default value	Description and value range
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.
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: 0= nominal STMR, no change to sidetone level. 1= nominal +9 STMR, three steps softer than nominal. 2= nominal +21 STMR (off), no sidetone (inaudible). 3= nominal +3 STMR, one level softer than nominal. 4= nominal +6 STMR, two steps softer than nominal. 5= nominal +12 STMR, four steps softer than nominal. 6= nominal +15 STMR, five steps softer than nominal. 7= nominal +18 STMR, six steps softer than nominal. 8= nominal -3 STMR, one step louder than nominal. 9= nominal -6 STMR, two steps louder than nominal. Pre-Release 6.2 software has different valid ranges. 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: 0=nominal STMR, no change to sidetone level. 1= nominal +9 STMR, three steps softer than nominal.

Parameter name	Default value	Description and value range
		2= nominal +21 STMR (off), no sidetone (inaudible). 3= nominal +3 STMR, one level softer than nominal. 4= nominal +6 STMR, two steps softer than nominal. 5= nominal +12 STMR, four steps softer than nominal. 6= nominal +15 STMR, five steps softer than nominal. 7= nominal +18 STMR, six steps softer than nominal. 8= nominal -3 STMR, one step louder than nominal. 9= nominal -6 STMR, two steps louder than nominal. Pre-Release 6.2 software has different valid ranges. 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. 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: 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. 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 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:

Parameter name	Default value	Description and value range
		`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.
CALL_LOG_JOURNAL	0	Valid values are 0 or 1 Value = 1 triggers restore of call log journal.
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.
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.

Parameter name	Default value	Description and value range
CNAPORT	50002	Avaya Converged Network Analyzer (CNA) server registration transport-layer port number (0-65535). Applies to IPv4 only. 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. 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. 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 53.
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 109.
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.

Parameter name	Default value	Description and value range
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 98.
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 98.
DOT1XWAIT	0	Specifies whether the telephone will wait for 802.1X authentication to complete before initiating DHCP Valid values, 0 and 1 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 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 106. If set to 0, the feature is turned off.
FBONCASCREEN	0	Specifies whether the Feature buttons are displayed on the same screen as Call Appearance when the value of PHNSCRALL is 0. Applies only to 9608, 9608G, and 9611G deskphones. • 0: Deskphone does not display Feature buttons on the Call Appearance screen. • 1: Deskphone displays Feature buttons that can adjust on the Call Appearance screen. In addition, the deskphone has a separate screen for Features.
GRATARP	0	Gratuitous ARP flag. Controls whether the deskphone processes gratuitous ARPS or ignores them. 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.

Parameter name	Default value	Description and value range
		Valid values are: 1 = Yes, process gratuitous ARPS 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.
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: 0 or 2 = The deskphone will go on-hook if a Disconnect message is received when the headset is active. 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: 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.

Parameter name	Default value	Description and value range
		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, 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 109. **Note:** H.323 Release 6.4 onwards, information of the parameter is saved in a non-volatile memor, thus retaining the information even after power down or reboot.
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. **Note:** 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 62. Any additional limitation or bugs discovered within this

Parameter name	Default value	Description and value range
		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. 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, 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 1 = User can select English language text strings. 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`” LANG1FILE = LANG2FILE = LANG3FILE = 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 . Example: If new behavior is activated, Button module and phone LEDs are aligned and will change according to call state.

Parameter name	Default value	Description and value range
LLDP_XMIT_SECS	30	Specifies the rate in seconds at which LLDP messages will be transmitted. Valid values are 1 to 4 ASCII numeric digits, “1” through “3600” 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 AUTOANSSTAT setting, this parameter does not influence that zip tone volume. 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. 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

Parameter name	Default value	Description and value range
		intervening spaces (0-255 ASCII characters, including commas). Null is a valid value.
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: 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. 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.
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

Parameter name	Default value	Description and value range
		in dotted decimal, colon-hex, or DNS name format, separated by commas without any intervening spaces. 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.
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. 0 = Call Center options will be displayed based on the value of OPSTAT (default). 1 = Call Center options will be displayed based on the value of OPSTATCC.

Parameter name	Default value	Description and value range
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. 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 calls from the incoming Call Log or from Web pages. 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	Specifies whether the deskphone displays separate screens for Call Appearance and Feature buttons. • 0: Separate screens for Call Appearance and Feature buttons. • 1: Consolidated screen for Call Appearance and Feature buttons.
PHNSCRCOLUMNS	0	Valid values are 0 or 1 Specifies whether the Phone Screen is presented with one (full-width) or two (each half-width) columns.

Parameter name	Default value	Description and value range
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). 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 more information, see About parameter data precedence on page 17.
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.

Parameter name	Default value	Description and value range
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: 1= Quick login permitted; user must press the pound (#) key to see the previous Extension and Password. 0= Quick login not permitted; the user must explicitly enter the extension and password.
QLEVEL_MIN	4	Valid values are 1 to 6 Specifies the minimum quality level in which a low local network quality indication will not be displayed.
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.

Parameter name	Default value	Description and value range
RINGBKFEATURES	“ ” (Null)	A list of feature number identifiers for softkey features potentially available in the active with far end ringback call state. 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 109.
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 A through Z a through z - (dash) . (period) _ (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.
SLMCAP	0	Valid values are 0, 1 or 2 Specifies whether the SLA Monitor agent supports packet capture.
SLMCTRL	0	Valid values are 0 or 1 Specifies whether the SLA Monitor agent supports device control.
SLMPERF	0	Valid values are 0 or 1 Specifies whether the SLA Monitor agent supports performance monitoring.
SLMPORT	50011	Valid values are 6000 - 65535 Specifies the UDP port used to receive commands from the SLA Monitor server.
SLMSRVR	0.0.0.0:0	Valid values, any Specifies the source IP address and, optionally, the source port number of valid discovery messages from an SLA Monitor server.
SLMSTAT	0	0 or 1

Parameter name	Default value	Description and value range
		Specifies whether the SLA Monitor agent will be enabled.
SLMTEST	50012	Valid values are 6000 - 65535 Specifies the UDP ports used for RTP and traceroute tests.
SSH_ALLOWED	2	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. When value =2, SSH will still be disabled by default (i.e., the SSH server listen port will be closed), but SSH will be able to be manually enabled (or disabled if it was previously manually enabled) from the Craft Debug procedure.
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. 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.
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: 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: 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.

Parameter name	Default value	Description and value range
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: 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. **Note:** 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: 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. 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: 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

Parameter name	Default value	Description and value range
		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 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: 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. **Note:** 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). 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.

Parameter name	Default value	Description and value range
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 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
WBCSTAT	1	Valid values are 1 to 6 Specifies whether a wideband codec indication will be displayed when a wideband codec is being used.

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 128.

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.

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 signaling 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 phones 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 phones will continue to do this for number of seconds configured by VLANTEST.

- If L2Q=1 and the VLANTEST timer expires because the phone has not received a DHCPOFFER, the phone sets L2QVLAN=0 and transmits DHCP messages with the default VLAN (0).
- If L2Q=0 and the VLANTEST timer expires because the phone has not received a DHCPOFFER, the phone 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 phone so that the phone receives a response to a DHCPDISCOVER on making that request on the default (0) VLAN.

After VLANTEST expires, if the phone receives a non-zero L2QVLAN value, the phone releases the IP address and sends DHCPDISCOVER on that VLAN. Any other release requires you to perform a manual reset before the phone attempts to use a VLAN on which VLANTEST has expired.

For more information on the Reset procedure, see *Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*.

The phone 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.

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 53. 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 the 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 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.

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.

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 phone software downloads do not overwrite the ID and password. 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 you install a phone 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 the phone achieves successful authentication. 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 the deskphone is connected. Some switches might authenticate only a single device per switch port. This operation is known as single-supplicant or port-based operation. These switches usually send multicast 802.1X packets to authenticating devices.

These switches support the following three scenarios:

- Standalone phone (Telephone Only Authenticates) - When you configure the IP phone for supplicant mode (DOT1XSTAT=2), the phone can support authentication from the switch.
- Phone with attached PC (Telephone Only Authenticates) - When you configure the IP phone for supplicant mode (DOT1X=2 and DOT1XSTAT=2), the phone can support authentication from the switch. The attached computer in this scenario gains access to the network without being authenticated.
- Telephone with attached computer (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 authentication.

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

- Standalone phone (Telephone Only Authenticates) - When you configure the IP phone for supplicant mode (DOT1XSTAT=2), the phone can support authentication from the switch. When DOT1X is “0” or “1” the phone cannot authenticate with the switch.
- Phone and computer Dual Authentication - Both the IP phone and the connected computer can support 802.1X authentication from the switch. You can configure the IP phone for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1 and DOT1XSTAT=1 or 2). The attached computer 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 1.0, LLDP is supported only for IPv4 mode.

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.

IEEE 802.1AB-2005 specifies the transmission and reception of LLDP. 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. After the phone is initiated, the phone sends an LLDPDU every 30 seconds or as specified by LLDP_XMIT_SECS parameter with the following contents:

Table 11: 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. Bit 5 (phone) 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. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the phone.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports auto-negotiation 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 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.

Category	TLV Name (Type)	TLV Info String (Value)
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. OUI = 00-40-0D (hex), Subtype = 1.
Avaya Proprietary	Call Server IP Address	Call Server IP address. Subtype = 3.
Avaya Proprietary	IP Phone Addresses	Phone IP address, Phone address mask, Gateway IP address. Subtype = 4.
Avaya Proprietary	CNA Server IP Address	CNA Server IP address = in-use value from CNASRVR. Subtype = 5. Release 6.2 and later do not support this parameter.
Avaya Proprietary	File Server	File Server IP address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not. 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 12: 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 the following conditions are met: • The phone is not registered with the call server. • Name begins with VOICE (letters are not case-sensitive). • The VLAN is not zero. • DHCP Client is activated.

System Parameter Name	TLV Name	Impact
		• The phone is registered but is not tagging layer 2 frames with a non-zero VLAN ID. 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. 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. L2QVLAN - set to the VLAN ID in the TLV. L2QAUD and L2QSIG - set to the Layer 2 Priority value in the TLV. DSCPAUD and DSCPSIG - set to the DSCP value in the TLV. The system checks whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • the value of USE_DHCP is 0 and the value of IPADD is not *0.0.0.0*, or • the Application Type is not 1 (Voice), or • 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.

System Parameter Name	TLV Name	Impact
	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 9608, 9608G, 9611G, 9621G, and 9641G H.323 describes how to use Craft local procedures at the phone for administration. The local procedures you might use 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 the phone's 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 the 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 the current parameter values and file versions.

Note:

If you have not changed the default password, the Debug option is available in a Read-Only mode.

You can use the DEBUG option only if you change the default password to the Craft local procedures 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 Release 6.2.4 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 more 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. Users can then select the language in which the phone displays messages.

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

For touch screen deskphones, this information includes an indication of the character that you can use as a decimal “point” in numeric values and an indication of the character that you should use 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, use ASCII 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 - Use this parameter to 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 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, except 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 visible on the **Screen and Sounds Options** screen.

For more information, see 9600 Series H.323 customizable system parameters on page 68. For more information on multiple language strings, see *Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, and 9641G H.323*.

To download a language file or to review pertinent information, go to the Avaya Support website.

Note:

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

Administering dialing methods

9600 Series IP deskphones have a variety of telephony-related applications that might obtain a telephone number during operation. Two dialing methods are used, depending on which version of Avaya Aura® Communication Manager that is running.

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 13: 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. **Note:** 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. If WMLHOME is null and the value of WMLHELPSTAT is not 1, the

Application	Parameter and value	Dependency
		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.
Greetings	N/A	The **Greetings** program displays only if you configure the following conditions: • AGTGREETINGSTAT has value 1, • CALLCTRSTAT has value 1, • The deskphone has a non-null call center agent ID if an agent has logged into the call center. • The Agent is not in an Available status. No **Manual-In** or **Auto-In** button has the associated LED On. • 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. **Note:** If the system suppresses the backups when BRURI is null, then the user loses the Favorites and all other Contacts when the user logs

Application	Parameter and value	Dependency
		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 68.

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 111 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 111, 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 14: 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
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

Feature Name	Default Label	Feature Number
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
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

Feature Name	Default Label	Feature Number
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
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

Feature Name	Default Label	Feature Number
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
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

Feature Name	Default Label	Feature Number
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
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 phone removes the screen saver whenever you reset the idle timer. If the value of SCREENSAVERON is “0”, the phone does not display either the standard Avaya screen saver or any customized screen saver you specify in the SCREENSAVER system parameter.

The deskphones display the screen savers for approximately 5 seconds at a time at random locations on the screen, so that the entire image is always displayed. When the phone removes the

screen saver, the phone restores the previously displayed screen unless a specified software operation such as making a call from the Phone screen displays some other 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 displays.

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

1. During start-up, the deskphone checks for the file named in the system parameter SCREENSAVER. If the deskphone finds a file, the deskphone checks that file for valid jpeg format, and to verify that the screen saver image height and screen saver image width do not exceed the specifications.

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

2. If the deskphone does not download a valid file, 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.

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 9608, 9608G, 9611G, 9621G, and 9641G H.323* 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:
  1. The deskphone uses the User Option value if selected and saved.
  2. If a Local Procedure value was selected and saved, the deskphone uses the local Procedure value.
  3. If a Settings file value is specified and saved the deskphone uses that value.
  4. 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.

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 68.

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

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 name that must match with the incoming VDN name to auto-answer. The incoming VDN name can be longer but the vector matches only the first 15 characters.

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 15: 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

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 124. 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*.

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 folder. The backup formats are as follows:

Table 16: Backup File Formats

Item/Data Value	Format
Generic	*name=value*
Contacts	ABKNAME*mmm*=ENTRY_NAME ABKNUMBER*mmm*=ENTRY_NUMBER_1 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 CLNUMBER*mmm*=ENTRY_NUMBER CLTYPE*mmm*=ENTRY_TYPE CLDATE*mmm*=ENTRY_DATE CLTIME*mmm*=ENTRY_TIME CLDURATION*mmm*=ENTRY_DURATION CLBRIDGEDFLAG*mmm*=ENTRY_BRIDGEDFLAG CLMISSEDCNTR*mmm*=ENTRY_COUNTER CLBCALBL*mmm*=ENTRY_BCALBL 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 17: 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 for each Home screen favorite, where *nn* is the index number for that favorite. The backup file format for a Favorite is:

Parameter Name	Setting
	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; 9621G/9641G/9670G only
OPTTEXTSIZE	Text Size
PERSONALRING	Personalized Ring. Note: 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 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
PHNABKNAME	Contacts Pairing
PHNEDITDIAL	Edit Dialling
PHNQUICKPANEL	Quick Touch Panel; 9621G/9641G/9670G only

Parameter Name	Setting
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; 9621G/9641G/9670G only
WEATHERUNITS	English/Metric; 9621G/9641G/ 9670G only
WORLDCLOCKLIST	List of World Clock location entries; 9621G/9641G/ 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 method 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 method prevents a user from bypassing your APPSTAT restrictions by editing the backup file.

For information about APPSTAT, see Setting the Application Status flag (APPSTAT).

During backup file restoration, do not perform any user activity 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 instead of editing 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 123.
- 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 get the backup file and successfully restore valid data.

Chapter 9: Administering Applications and Options

Administering guest users

About this task

A guest user is a person who logs into a 9600 Series IP deskphone other than the primary phone at the home location of the user.

The guest user can log in to a phone that is across the country from the home location or one in the office near 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 that you can administer are GUESTDURATION and GUESTWARNING. For more information on the parameters, see 9600 Series H.323 customizable system parameters on page 68.

Idle timer configuration

When the idle timer in the deskphone expires, you can administer the deskphone to turn the backlight to the lowest power level, put up a screen saver, or show a Web page while the deskphone is idle. However, do not set all these values on the same deskphone. However, you can set a lobby phone to go to a Web page when the phone is idle. You can also set a desk phone to go to the screen saver or set the backlight to low power mode when idle.

The related system parameters and their default values are:

System parameter	Default value
WMLIDLETIME	10 minutes
WMLIDLEURI	Null
BAKLIGHTOFF	120 minutes
SCREENSAVERON	240 minutes

You must specify WMLIDLEURI only for phones installed in public areas through the use of a GROUP parameter.

Table 18: Idle Timer Settings and Results

Shortest Timer	Middle Timer	Longest Timer	Operation
WMLIDLETIME and WMLIDLEURI are null	BAKLIGHTOFF is non-zero	SCREENSAVERON is non-zero	Default operation: After BAKLIGHTOFF minutes, the backlight is set to low power mode. After (SCREENSAVERON – BAKLIGHTOFF) additional minutes, the screen saver is displayed. WMLIDLETIME has no effect.
WMLIDLETIME and WMLIDLEURI are null	SCREENSAVERON is non-zero	BAKLIGHTOFF is non-zero	After SCREENSAVERON minutes, the phone displays the screen saver. After (BAKLIGHTOFF-SCREENSAVERON) additional minutes, the backlight is set to low power mode.
WMLIDLETIME and WMLIDLEURI are non-null	BAKLIGHTOFF is non-zero	SCREENSAVERON is non-zero	Every WMLIDLETIME minutes, a GET is sent for WMLIDLEURI, and the the phone displays a browser. The Web page may contain a timer to cycle through additional Web pages. The backlight is set to low power mode after the specified time and the phone displays a screen saver on the SCREENSAVERON value.

For more information, see 9600 Series H.323 customizable system parameters on page 68.

Note:

The Backlight Off icon if administered, allows the users to bypass the timers in the table 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 109.

The behavior of backlight for any adjunct button module depends on the backlight of the phone to which you attach the button module.

802.1X

An authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access.

CA

Certificate Authority, the entity which issues digital certificates for use by other parties.

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.

This feature is not supported in Release 6.2 and later.

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 public key goes through to determine if the claim of the subject is correct and depends on the level of certification and the CA.

DHCP

Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.

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.

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.

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.

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.

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.

MAC

Media Access Control, ID of an endpoint.

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.

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.

RTCP

RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service.

SCEP

Simple Certificate Enrollment Protocol, used to obtain a unique digital certificate.

SIP

Session Initiation Protocol. An alternative to H.323 for VoIP signaling.

SNTP

Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet.

TFTP

Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP telephones.

WML

Wireless Markup Language, used by the IP phones Web Browser to communicate with WML servers.

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.

Index

Numerics

A

B

C

D

E

F

G

H

I

L

N

O

P

Q

R

S

T

U

V

W