



Avaya one-X[®] Deskphone H.323 9608, 9611G, 9621G, and 9641G Administrator Guide

Release 6.2
16-300698
Issue 10
February 2012

Notice

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

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; 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 End User a license within the scope of the license types described below. 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 End User. “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. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

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

Shrinkwrap License (SR). Customer 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”). (see “Third-party Components” for more information).

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

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 Web site: <http://support.avaya.com>. Suspected security

vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://support.avaya.com>.

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: About this Guide	9
About this guide.....	9
Change History.....	10
What's New in This Release.....	11
Changes from Release 6.0 to Release 6.1.....	12
Chapter 2: Administration Overview and Requirements	15
About 9600 Series IP deskphones.....	15
Administrative requirements.....	16
About parameter data precedence.....	18
Administrative tasks.....	19
Administrative checklist.....	19
Deskphone Initialization Process Overview.....	21
Step 1: Accessing the network.....	22
Step 2: DHCP processing.....	22
Step 3: Establishing a VPN Connection (optional).....	22
Step 4: Downloading files.....	22
Step 5: Registering with the call server.....	22
Error conditions.....	24
Chapter 3: Network Requirements	25
Performing a network assessment.....	25
Hardware requirements.....	25
Server requirements.....	26
Required network information.....	27
Other network considerations.....	27
Enabling SNMP.....	28
Ping and traceroute.....	28
IP address and settings reuse.....	29
QoS.....	29
IEEE 802.1D and 802.1Q.....	29
Displaying network audio quality.....	30
Enabling Qtest for audio quality.....	31
IP address lists and station number portability.....	31
TCP/UDP Port Utilization.....	31
Security.....	36
Time-to-Service (TTS).....	38
Chapter 4: Communication Manager Administration	39
Call server requirements.....	39
Aliasing IP Deskphones for switch compatibility.....	39
Administering the call server (switch).....	41
Administering the IP interface and addresses.....	42
Administering UDP port selection.....	42
Administering RSVP.....	42
Administering QoS.....	43
Administering IEEE 802.1Q.....	43

Administering DIFFSERV.....	43
Administering NAT.....	43
Administering Voice Mail.....	44
Administering voice mail for deskphones with CM 4.0+ Native support.....	44
Administering voice mail for deskphones aliased as 4600 Series IP Telephones.....	44
Administering call transfers.....	45
Administering call conferencing.....	46
Administering Deskphones on Avaya Aura Communication Manager (CM).....	47
Administering feature-related system parameters.....	47
Administering stations.....	49
Administering features.....	49
Administering feature buttons and call appearances (CAs).....	50
Administering 9610 IP Telephone features and CAs.....	50
Administering 9620/9620L/9620C IP Telephone features and CAs.....	51
Administering features and CAs for all other IP Deskphones.....	51
Administering enhanced Phone screen displays for certain IP Deskphones.....	53
Assigning 9650/9650C Aux Buttons.....	53
Administering button module(s) on the 9608, 9611G, 9630/9630G, 9640/9640G, 9641G, 9650/9650C, and 9670G.....	54
Administering the Conference Details screen for ad-hoc conferences.....	55
Administering the Quick Touch panel for touchscreen deskphones.....	55
Administering shuffling.....	56
Administering wide band codecs.....	56
Chapter 5: Server Administration.....	57
Software Prerequisites.....	57
Administering the DHCP and File Servers.....	57
Administering the DHCP Server.....	58
Configuring DHCP Option 242 (SSON).....	58
DHCP Generic Setup.....	61
Setting up the DHCP server.....	61
Setting up a DHCPv6 server.....	64
HTTP Generic Setup.....	65
Backup/restore processing.....	66
About IPv4 and/or IPv6 Operation.....	68
Features not supporting IPv6.....	69
Chapter 6: Telephone Software and Application Files.....	71
About the general download process.....	71
Choosing the right application file and upgrade script file.....	72
Changing the Signaling Protocol.....	72
About the upgrade file.....	73
About the settings file.....	73
Using the GROUP parameter to set up customized groups.....	74
Chapter 7: Administering Telephone Options.....	77
Administering Options for 9600 Series H.323 Deskphones.....	77
9600 Series H.323 Customizable System Parameters.....	78
Administering a VLAN.....	100
About VLAN Tagging.....	100

The VLAN default value and priority tagging.....	100
Automatically detecting a VLAN.....	101
VLAN separation rules and related parameters.....	102
About DNS addressing.....	105
About IEEE 802.1X.....	105
802.1X Supplicant Operation.....	106
About Link Layer Discovery Protocol (LLDP).....	108
Administering settings at the deskphone.....	112
Administering display language options.....	112
Administering voice-initiated dialing.....	114
About the gigabit Ethernet (GigE) adapter.....	115
Administering dialing methods.....	116
About log digit (Smart Enbloc) dialing.....	116
Using enhanced local dialing.....	116
Enhanced local dialing requirements.....	118
About internal audio parameters.....	119
Administering features on softkeys.....	120
Administering a custom screen saver.....	128
About administering audio equalization.....	129
Administering deskphones for call center operation.....	130
Administering agent sign ins for call centers.....	131
Call Center backup files.....	132
Administering the Vu display button.....	133
Administering backup/restore.....	134
Backup file formats.....	136
User data saved during backup.....	137
About restore.....	139
Administering backup/restore for a 9610.....	140
About the 9610 retrieval process.....	141
General 9610 restore processing.....	142
Chapter 8: Administering Applications and Options.....	145
Customizing Applications and Options.....	145
Setting the Application Status flag (APPSTAT).....	146
Special Administration for the 9610.....	147
Special Administration for Touchscreen Deskphones.....	148
Administering the Avaya "A" Menu.....	148
Administering Phone Settings and Options and Settings (OPSTAT and OPSTAT2).....	150
Administering WML applications on the Avaya Menu.....	150
Main Avaya Menu with Browser (Only) Administered.....	152
Administering the Avaya Menu with WML applications.....	153
How the Home screen displays WML applications.....	154
Sample Avaya Menu Administration File Template.....	157
Administering guest users.....	160
Administering visiting users.....	160
Administering idle timer operation.....	160
Administering the user stopwatch timer.....	162
Requirements for USB Devices.....	163

USB File/Device Support.....	163
Contacts File Format for USB Devices.....	163
Setting up USB logins.....	165
Setting up USB pictures as screensavers.....	165
Chapter 9: Administering Specific 9600 Series IP Deskphones.....	167
Introduction.....	167
Special Administration for the 9610 IP Telephone.....	167
General 9610 Functionality.....	167
Key 9610 Administration Concepts.....	168
Administering the 9610 idle application, screensaver, and WML links.....	172
Accessing 9610 Craft procedures.....	173
Troubleshooting a 9610 IP Telephone.....	173
Sample 9610data.txt file.....	174
Sample idle.wml file.....	176
Sample hotel.wml file.....	177
Glossary.....	179
Index.....	185

Chapter 1: About this Guide

About this guide

This guide is for personnel who administer Avaya Aura™ Communication Manager, DHCP, HTTP/HTTPS servers for 9600 Series IP deskphones, a Local Area Network (LAN), or a Web server.

The 9600 Series IP deskphones use Internet Protocol (IP) technology with Ethernet line interfaces and support both H.323 and SIP protocols. The 9600 Series IP deskphones provide support for DHCP, HTTP, and HTTPS to obtain customized settings and to download new versions of software for the telephones.

Caution:

Avaya does not support many of the products mentioned in this document. Take care to ensure that there is adequate technical support available for servers used with any 9600 Series IP Deskphone system. If the servers are not functioning correctly, the deskphones might not operate correctly.

Note:

This guide covers administration of 9600 Series IP deskphones using H.323 protocol only. For information about administering these telephones in a Session Initiation Protocol (SIP) environment, see *Avaya one-X® Deskphone SIP Administrator Guide* (Document Number 16-601944).

This document does not cover using the 9600 Series IP deskphones in an IP Office environment; for information on doing so, see the Avaya support site at <http://support.avaya.com/css/P8/documents/100150378>.

Important:

IP Telephone Software Release 3.1 does not support Avaya Communication Manager (CM) releases prior to 3.1.

Tip:

For a quick reference to Avaya Communication Manager settings for 9600 Series IP deskphones and related telephone interface information, see *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Read This First* (Document Number 16-601533), available at: www.avaya.com/support.

*** Note:**

The terms “9600 Series IP Telephone(s),” “9600 Series IP Deskphone(s),” “H.323 deskphone,” “deskphone,” and “IP telephone” all refer to the same Avaya one-X® product line and are used interchangeably in this document.

Change History

Issue 1	This document was issued for the first time in July 2006 to support the first release of 9600 Series IP telephones.
Issue 2	This version of the document, revised and issued in September 2006, supports 9600 Series IP Telephone Software Release 1.1.
Issue 3	This version of the document was revised in January, 2007 to support 9600 Series IP Telephone Software Release 1.2.
Issue 4	This version of the document was revised and issued in May, 2007 to support Software Release 1.5.
Issue 5	This version of the document was revised and issued in May, 2008 to support 9600 Series IP Telephone Software Release 2.0.
Issue 6	This version of the document was revised and issued in February, 2009 to support 9600 Series IP Telephone Software Release 3.0 and the addition of three new telephone models: 9620L, 9620C, and 9650C.
Issue 6	This version of the document was revised and issued in May, 2009 to support the addition of the 9670G telephone model, running on 9600 Series IP Telephone Software Release 2.0; this 9670-specific issue was concurrent with Issue 6 for Software Release 3.0.
Issue 7	This version of this document was revised and issued in November, 2009 to support 9600 Series IP Telephone Software Release 3.1. In addition to software enhancements, this version incorporates the 9670G IP telephone’s administration requirements and information, previously issued separately in May, 2009.
Issue 8	This version was revised and issued in August, 2010 to support 9600 Series IP Deskphone Software Release 6.0 and the addition of four new deskphone models: 9608, 9611G, 9621G, and 9641G; this release also supports the BM12 Button Module. Release 6.0 was numbered to be compatible with Release 6.0 of Avaya Aura Communication Manager and Release 6.0 of Avaya Aura™ System Manager.
Issue 9	This version of the document, revised and issued in March, 2011 to support 9600 Series IP Deskphone Software Release 6.1, which applies to four deskphone models: 9608, 9611G, 9621G, and 9641G. Most updates expand the Call Center functionality for these deskphones.

Issue 10	This version of the document was revised and issued in February 2012 to support 9600 Series IP Deskphone Software Release 6.2. The section <i>What's New in This Release</i> on page 11 describes Release 6.2 in more detail. Note that for 9600 Series IP deskphones other than the 9608, 9611, 9621G, and 9641G models, Software Release 3.1, issued in November, 2009 still applies.
----------	---

What's New in This Release

New material in this issue to support Release 6.2 software includes the following features and functionality that apply only to the 9608, 9611G, 9621G, and 9641G IP deskphones:

- The Debug procedure has been expanded to allow technicians to send immediate debug reports to specified servers.
- A version of software that disables VPN and media encryption can be downloaded from the Support website; it is identified on the About Avaya one-X® screen with a “U” appended to the software release.
- Secure Shell (SSH) protocol is supported. This protocol is intended to help Avaya Services monitor telephone performance.
- EAP-TLS (Extensible Authentication Protocol with TLS authentication) is supported, in part as enabled or disabled with the DOT1XEAPS parameter.
- For call centers, the AGTIDVUSTAT parameter can be used to specify a VuStats format number to enable the telephone 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 it generates a log event and either kills the process or resets the telephone. This application watchdog can be disabled or re-enabled with the APPLICATIONWD parameter.
- Bluetooth functionality can be disabled from the settings file, with the BLUETOOTHSTAT parameter.
- A recording tone can be played when the user is on a call, with the RECORDINGTONE parameter. In addition, the interval between tones, and the volume the tones are played, are administrable. This would be relevant to sites where a recording device is connected to the telephone 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 telephone's speaker.
- Support for control of handset audio equalization has been made available 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 as of Release 6.2.
- Call Center agents have their Greetings stored on the telephone 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 CALLCTRSTAT has value "1", HEADSYS has default value "1". Otherwise, CALLCTRSTAT has value "0", and the default value of HEADSYS is likewise 0. In either case, though, you have the normal ability to override defaults by explicitly setting HEADSYS in the settings file.

Changes from Release 6.0 to Release 6.1

The following section describes what has changed from the version 6.0 to 6.1 of the H.323 Release for Avaya deskphones. This information is being published in this guide as version 6.1 was a Limited Availability (LA) release.

The information is targeted at the group of users who are migrating directly from version 6.0 to version 6.2

- The deskphones now support a local timer (Stop watch) feature. The agent is able to select the Local Timer Feature and start a stop watch.
- The agent deskphone, with the dual headset adapter box, will provide 2 headset ports for the agent and the supervisor using the standard RJ9.adaptor.
- Agent can manually recording a greeting.
- Automatic prompting for greeting.
- Greeting size of 10 secs supported, and about 16 greetings can be saved.
- Agents can link a greeting to a particular trigger event during the recording process. The trigger events could be manual or automatic.
- The agent can now play back greetings when on a call to both the incoming caller and the agent simultaneously. The agent can manually trigger the play back of the greeting by selecting the greeting during the call. Agent greetings will also be automatically triggered using one of the following events:
 - Time of day
 - Answering a call

- ANI
- VDN
- Skills
- Prompted Digits
- Greetings can be backed up, deleted and retrieved from server automatically.
- Administrator can disable the hook switch via the settings file to prevent agents accidentally going off hook and then on hook with the handset resulting in them disconnecting the active call and being logged out.
- Call appearance is now 15 characters wide of VDN name for touch phones, for button phones it must be 12 or 24 char wide depending on screen width.
- The agent can press the UUI-INFO button to get the UUI information displayed. If this information does not fit on the allocated display area the content will scroll on the line.
- Agent can use the Caller info button to view secondary information about the ongoing call (collected digits, qcalls, q-time, trk-id, VuStat display, and uui-info).
- History backup time controlled by agent selection.
- New Parameter CLBACKUPTIME can be defined to control backup delay.
- Logout button displayed in idle screen.
- Help screen now provided that states how to unlock the phone.
- Logoff Softkey provided for agent to log off and logon using another set of credentials.
- Caller ID to be displayed on screen sequential lines if it does not fit in one line.
- Capability to define WML buttons with functions will be extended to allow the implementation of call control capabilities
- Using the visiting user profile, a user will be able to log into any 9600 series Deskphone within the configured network of systems using their unique user identifier and password.
- The following new system parameters have been added to the list of 9600 Series H.323 Customizable System Parameters:
 - AGTCALLINFOSTAT - Automatically invokes the Call-info permission flag; for Call Center use only.
 - AGTFWDBTNSTAT - Disables/enables the Forward button permission flag; for Call Center use only.
 - AGTGREETINGSTAT - Sets the agent greeting permission flag; for Call Center use only.
 - AGTLOGINFAC - Indicates the Feature Access Code to be used by agents when logging in to a Call Center; for Call Center use only.
 - AGTSPKRSTAT - disables/enables the speakerphone permission flag; for Call Center use only.

- AGTTIMESTAT - suppresses the date/time presentation flag; for Call Center use only.
 - AGTTRANSLTO - Translation for "to" as used on the call server; for Call Center use only.
 - AGTTRANSCLBK - Translation for "callback" as used on the call server; for Call Center use only.
 - AGTTRANSLPRI - Translation for "priority" as used on the call server; for Call Center use only.
 - AGTTRANSLPK - Translation for "park" as used on the call server; for Call Center use only.
 - AGTTRANSLICOM - Translation for "icom" as used on the call server; for Call Center use only.
 - CALLCTRSTAT - Call center functionality flag; for Call Center use only.
 - OPSTATCC - OPSTAT override flag; for Call Center use only.
 - TIMERSTAT - Controls whether the User Timer Timer On and Timer Off softkeys display on the deskphone or not.
- The Management Information Base (MIB), available on the Avaya support site has been updated for several new parameters and to increase the number of syslog event messages in the *endptRecentLog* and *endptResetLog* parameters.
 - The deskphone display now combines the Title line and the Prompt line shown on other 9600 Series IP deskphones into one Status line. The Status line appears as the second display line, under the Top line.

Chapter 2: Administration Overview and Requirements

About 9600 Series IP deskphones

All 9600 Series IP deskphones currently support the H.323 signaling protocol. The 9608, 9611G, 9620, 9621G, 9630/9630G, 9640/9640G, 9641G, and 9650/9650C can alternately be configured to support Session Initiation Protocol (SIP), as covered in the *Avaya one-X® Deskphone SIP Administrator Guide (Document Number 16–603813 for the 9608, 9611G, 9621G, and 9641G models, and Document Number 16-601944 for all other 9600 Series deskphone models)*. This document covers only 9600 Series IP deskphones supporting H.323.

As of H.323 software Release 6.0, different software versions support different 9600 Series IP deskphones, as shown:

9600 Series Deskphone Model	Latest Supported Software Release
9610, 9620/9620C/9620L, 9630/9630G, 9640/9640G, 9650/9650C, 9670G	3.1
9608, 9611G, 9621G, 9641G	6.0 and later

The H.323 standard provides for 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)

Administrative requirements

The parameters under which the 9600 Series IP deskphones need to operate are summarized as follows:

- Telephone Administration on the Avaya call server, as covered in [Communication Manager Administration](#) on page 39.
- IP Address management for the telephone, as covered in [Administering the DHCP and File Servers](#) on page 57 for dynamic addressing. For static addressing, see the *Avaya one-X® Deskphone H.323 Installation and Maintenance Guide* (Document Number 16-603603 covering the 9608, 9611G, 9621G, and 9641G deskphones, and Document Number 16-300694 for all other 9600 Series deskphone models).
- Tagging Control and VLAN administration for the telephone, if appropriate, as covered in [Administering Telephone Options](#) on page 77.
- Quality of Service (QoS) administration for the telephone, if appropriate. QoS is covered in [QoS](#) on page 29 and [Administering QoS](#) on page 43.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP).
- Interface administration for the telephone, as appropriate. Administer the telephone to LAN interface using the PHY1 parameter described in [Network Requirements](#) on page 25. Administer the telephone to PC interface using the PHY2 parameter described in “Interface Control” in the *Avaya one-X® Deskphone H.323 Installation and Maintenance Guide* (Document Number 16-603603 covering the 9608, 9611G, 9621G, and 9641G deskphones, and Document Number 16-300694 for all other 9600 Series deskphone models)
- Application-specific telephone administration, if appropriate, as described in [Administering Applications and Options](#) on page 145. An example of application-specific data is Web-specific information required for this optional application.

[The table](#) on page 17 indicates that you can administer system parameters in a variety of ways and use a variety of delivery mechanisms like:

- Maintaining the information on the call server.
- Manually entering the information by means of the telephone dialpad.
- Administering the DHCP server.
- Editing the configuration file on the applicable HTTP or HTTPS file server.
- User modification of certain parameters, when given administrative permission to do so.

*** Note:**

Not all parameters can be administered on all delivery mechanisms.

Table 1: Administration Alternatives and Options for 9600 Series IP Telephones

Parameter(s)	Administrative mechanisms	For more information see:
Telephone Administration	Avaya call server	Communication Manager Administration on page 39, Server Administration on page 57 and the applicable call server documentation.
IP Addresses	DHCP (strongly recommended)	Administering The DHCP and File Servers on page 57, and especially Administering the DHCP Server on page 58.
	Configuration file	Telephone Software and Application Files on page 71 and Administering Telephone Options on page 77.
	Manual administration at the telephone	“Static Addressing Installation” in the appropriate <i>Avaya one-X® Deskphone H.323 Installation and Maintenance Guide</i> .
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 108
Tagging and VLAN	DHCP	Administering The DHCP Server on page 58, and Administering Telephone Options on page 77.
	Configuration file	Administering The DHCP and File Servers on page 57 and Administering Telephone Options on page 77.
	LLDP	“Static Addressing Installation” in the appropriate <i>Avaya one-X® Deskphone H.323 Installation and Maintenance Guide</i> .
	Manual administration at the telephone	About Link Layer Discovery Protocol (LLDP) on page 108.
Quality of Service	Avaya call server	Administering UDP port selection on page 42 and the applicable call server documentation.
	DHCP	Administering The DHCP and File Servers on page 57, and Administering Telephone Options on page 77.
	Configuration file	Administering The DHCP and File Servers on page 57, and Administering Telephone Options on page 77.
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 108.

Parameter(s)	Administrative mechanisms	For more information see:
Interface	DHCP	Administering The DHCP and File Servers on page 57, and Telephone Software and Application Files on page 71.
	Configuration file	Administering The DHCP and File Servers on page 57, and Telephone Software and Application Files on page 71.
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 108.
	Manual administration at the telephone	“Secondary Ethernet (Hub) Interface Enable/Disable” in the appropriate <i>Avaya one-X® Deskphone H.323 Installation and Maintenance Guide</i> .
Application - specific parameters	Configuration file	Administering The DHCP and File Servers on page 57, and especially HTTP Generic Setup on page 65. Also, Administering Applications and Options on page 145.
VPN	Configuration file	<i>VPN Setup Guide for 9600 Series IP Telephones (Document 16-602968)</i> .

General information about administering DHCP servers is covered in [Administering the DHCP and File Servers](#) on page 57, and more specifically, [Administering the DHCP Server](#) on page 58. General information about administering HTTP servers is covered in [Administering the DHCP and File Servers](#) on page 57, and more specifically, [HTTP Generic Setup](#) on page 65. Once you are familiar with that material, you can administer telephone options as described in [Administering Telephone Options](#) on page 77.

About parameter data precedence

If a given parameter is administered in multiple places, the last server to provide the parameter usually has precedence. The precedence, from lowest to highest, is:

1. Manual administration, with the two exceptions of call server or HTTP server or both for the phone parameter STATIC,
2. DHCP, except as indicated in “DHCPACK Setting of Parameter Values” in [Setting up the DHCP server](#) on page 61,
3. the 46xxsettings.txt file,
4. the Avaya call server,

5. Backup files, if administered and if permitted, and finally,
6. LLDP, except for setting the call server and file server IP addresses, for which it has the lowest precedence (LLDP is only supported in IPv4 mode).

Administrative tasks

The following list depicts administration for a typical 9600 Series IP telephone network. Your own configuration might differ depending on the servers and system you have in place.

1. Switch administered for 9600 Series IP deskphones.
2. LAN and applicable servers administered to accept the telephones.
3. Telephone software downloaded from the Avaya support site.
4. 46xxsettings file updated with site-specific information, as applicable.
5. 9600 Series IP deskphones installed. For more information, see the appropriate *Avaya one-X® Deskphone H.323 Installation and Maintenance Guide* (Document Number 16-603603 covering the 9608, 9611G, 9621G, and 9641G deskphones, and Document Number 16-300694 for all other 9600 Series deskphone models)
6. Individual 9600 Series IP Deskphones updated using Craft procedures, as applicable. For more information, see “Local Administrative Procedures” in the appropriate *Avaya one-X® Deskphone H.323 Installation and Maintenance Guide*.

Administrative checklist

Use the following checklist as a guide to system and LAN administrator responsibilities. This high-level list helps ensure that all telephone system prerequisites and requirements are met prior to telephone installation.

*** Note:**

One person might function as both the system administrator and the LAN administrator in some environments.

Table 2: Administrative Checklist

Task	Description	For more information see:
Network Requirements Assessment	Determine that network hardware is in place and can handle telephone system requirements.	Network Requirements on page 25.

Task	Description	For more information see:
Administer the call server	Verify that the call server is licensed and is administered for Voice over IP (VoIP). Verify the individual telephones are administered as desired.	Communication Manager Administration on page 39.
DHCP server installation	Install a DHCP application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
Administer DHCP application	Add IP telephone administration to DHCP application.	Administering The DHCP Server on page 58 in Server Administration on page 57.
HTTP/HTTPS server installation	Install an HTTP/HTTPS application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
Application file(s), script file, and settings file installation on HTTP/HTTPS server	Download the files from the Avaya support site.	http://www.avaya.com/support/Telephone Software and Application Files on page 71.
Modify settings file as desired	Edit the settings file as desired, using your own tools.	Telephone Software and Application Files on page 71.
Administer WML servers	Add WML content as applicable to new or existing WML servers. Administer push content as applicable.	<i>Avaya one-X® Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide</i> (Document Number 16-600888).
Administer telephones locally as applicable	As a Group:	Using the GROUP parameter to set up customized groups on page 74 and the <i>Avaya one-X® Deskphone H.323 Installation and Maintenance Guide</i> . (Document Number 16-300694 for all but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608, 9611G, 9621G, and 9641G deskphones).
	Individually:	The applicable Craft Local Procedures in the <i>Avaya one-X® Deskphone H.323 Installation and Maintenance Guide</i> (Document Number 16-300694 for all but Release

Task	Description	For more information see:
		6.2 and Document Number 16-603603 for Release 6.2 covering the 9608, 9611G, 9621G, and 9641G deskphones).
Installation of telephones in the network		Avaya one-X® Deskphone H.323 Installation and Maintenance Guide (Document Number 16-300694 for all but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608, 9611G, 9621G, and 9641G deskphones).
Allow user to modify Options, if applicable		OPSTAT on page 150 and the respective User Guide for the specific telephone model.
Administer VPN functionality if applicable	Enable/disable VPN, provide administration for your particular VPN environment	VPN Setup Guide for 9600 Series IP Telephones (Document 16-602968)

Deskphone Initialization Process Overview

These steps offer a high-level description of the information exchanged when the telephone initializes and registers. This description assumes that all equipment is properly administered ahead of time. The *Avaya one-X® Deskphone H.323 Installation and Maintenance Guide* (Document Number 16-603603 covering the 9608, 9611G, 9621G, and 9641G deskphones, and Document Number 16-300694 for all other 9600 Series deskphone models) provides a detailed description of initialization (power-up and reset).

*** Note:**

When a phone starts without access to the HTTP server, the phone re-use parameters known before reboot. The phone waits 60 seconds and starts with old parameters.

Related topics:

[Step 1: Accessing the network](#) on page 22

[Step 2: DHCP processing](#) on page 22

[Step 3: Establishing a VPN Connection \(optional\)](#) on page 22

[Step 4: Downloading files](#) on page 22

[Step 5: Registering with the call server](#) on page 22

Step 1: Accessing the network

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

Step 2: DHCP processing

If an IP address has not been manually configured in the telephone, the telephone initiates DHCP, as described in [Administering the DHCP and File Servers](#) on page 57. Among other data passed to the telephone is the IP Address of the HTTP or HTTPS server.

Step 3: Establishing a VPN Connection (optional)

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

Step 4: Downloading files

The 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 telephone first downloads an upgrade configuration file, which tells the telephone which software files it should use. The telephone then downloads a settings configuration file, and based on those settings, it may then download language files and/or certificate files. Finally, the telephone will download one or two new software files, depending on whether or not the software in the telephone 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 71.

Step 5: Registering with the call server

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

In this step, the telephone might prompt the user for an extension and password. The telephone 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 telephone extension and the password

configured on the call server for that particular extension. For a restart of a telephone that was previously registered with an extension number, this information is already stored on the telephone, but the user might have to confirm the information. The expected result is that the telephone is appropriately registered and call server data such as feature button assignments are downloaded.

The 9600 Series IP Deskphones support a feature called Unnamed Registration. Unnamed Registration allows a telephone to register with the call server without an extension, assuming the call server also supports this feature (i.e., unnamed registration is enabled through Avaya Communication Manager administration). To invoke Unnamed Registration, either enter a null (empty) extension or password or take no action. In the latter case, allow the **Extension...** prompt display for 60 seconds without making an entry. The telephone automatically attempts to register by means of Unnamed Registration. A telephone registered with Unnamed Registration has the following characteristics:

- only one call appearance,
- no administrable features,
- can make only outgoing calls, subject to call server Class of Restriction/Class of Service limitations, and
- can be converted to normal “named” registration by the user entering a valid extension and password.

You can also administer the telephone to avoid unnamed registration and remain unregistered if no extension and password are provided. For more information, see the UNNAMEDSTAT parameter in the [9600 Series H.323 Customizable System Parameters](#) on page 78 table.

In general, you tell the deskphone where to register by listing IP Addresses in the MCIPADD parameter in DHCP or the 46xxsettings.txt file. Standard practice is to list the CLANs on the main call server, followed by any Enterprise Survivable Server (ESS) address(es), followed by any Local Spare Processor (LSP). You can depart from this practice, for example, you can list CLANs for multiple main call servers. In general, the deskphone will start from the beginning of MCIPADD and attempt to register with each IP address in turn, one at a time, until it gets a positive response. MCIPADD is generally administered to allow users to register to local call servers.

However, sometimes a user from another location wants to register with their home call server using their “home” extension; this is known as the “Visiting User” (VU) scenario. As of 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 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, VUMCIPADD could be administered then 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.

For more information about the installation process, see the appropriate *Avaya one-X® Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide (Document Number 16-300694 for all but Release 6.2 and later, and Document Number 16-603603 for Release 6.2 and later, covering the 9608, 9611G, 9621G, and 9641G deskphones)*.

Error conditions

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

The *Avaya one-X® Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide* covers possible operational problems that might be encountered after successful 9600 Series IP deskphone installation. The User Guides for a specific telephone model also contain guidance for users having problems with specific applications.

Chapter 3: Network Requirements

Performing a network assessment

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

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

Also, QoS support is required to run VoIP on your configuration. For more information, see [Administering UDP port selection](#) on page 42.

If you want any of your users to be able to use their 9600 Series IP Deskphones to access your network through a Virtual Private Network (VPN), see the *VPN Setup Guide for 9600 Series IP Telephones (Document 16-602968)*.

Hardware requirements

To operate properly, you need:

- Category 5e cables designed to the IEEE 802.3af-2003 standard, for LAN powering,
- TN2602 or TN2302 IP Media Processor circuit pack. Sites with a TN2302 IP Media Processor circuit pack are strongly encouraged to install a TN2602 circuit pack to benefit from increased capacity.
- TN799C or D Control-LAN (C-LAN) circuit pack.

! **Important:**

IP telephone firmware Release 1.0 or greater requires TN799C V3 or greater C-LAN circuit pack(s). For more information, see the *Communication Manager Software and*

Firmware Compatibility Matrix on the Avaya support Web site <http://www.avaya.com/support>.

To ensure that the appropriate circuit pack(s) are administered on your server, see [Communication Manager Administration](#) on page 39. For more information about hardware requirements in general, see the appropriate *Avaya one-X® Deskphone H.323 Installation and Maintenance Guide (Document Number 16-300694 for all but Release 6.0. For Release 6.0 covering the 9608, 9611G, 9621G, and 9641G deskphones, use Document Number 16-603603)*.

Server requirements

Three server types can be configured for the 9600 Series IP deskphones:

- DHCP server - Avaya recommends that a DHCP server be installed and that static addressing be avoided. Install the DHCP server as described in [Administering the DHCP and File Servers](#) on page 57.
- HTTP or HTTPS server - Administer the HTTP or HTTPS file server as described in [HTTP Generic Setup](#) on page 65.
- Web and Push servers (optional) - If users have access to corporate WML Web sites, administer the telephones as described in [Server Administration](#) on page 57. For “push” functionality, a Trusted Push Server is needed. The Trusted Push Server can be the same server as your WML server. Avaya recommends that you restrict access to directories on the WML server that contain push content.

*** Note:**

Push is supported only in IPv4 mode. Your Web and push server configuration must be compatible with the requirements covered 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, they are not necessarily different boxes. For example, DHCP provides file management whereas HTTP provides application management, yet both functions can co-exist on one hardware unit. Any standards-based server is recommended.

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 57.

⚠ Caution:

The telephones 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 telephones reset, the telephones operate based on their default administration and continue on to register with the call server. Some features might not be available. To restore them you need to reset the telephone(s) when the file server is available.

Required network information

Before you administer DHCP and HTTP/HTTPS, complete the information listed below in this section. 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 deskphone installation.

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

When specifying IP Addresses for the file server or call server, use either dotted decimal format (“xxx.xxx.xxx.xxx”) or DNS names for IPv4 addresses, or colon-hex format or DNS names for IPv6 entries. If you use DNS, the value of the DOMAIN parameter is appended to the DNS names that you specify. If DOMAIN is null, the DNS names must be fully qualified. For more information about DNS, see [DHCP Generic Setup](#) on page 61 and [DNS Addressing](#) on page 105.

Required network information before installation (per DHCP server)

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

As the LAN or System Administrator, you are also responsible for:

- Administering the DHCP server as described in [Server Administration](#) on page 57.
- Editing the configuration file on the applicable HTTP or HTTPS file server, as covered in [Choosing the right application file and upgrade script file](#) on page 72.

Other network considerations

Related topics:

[Enabling SNMP](#) on page 28

[Ping and traceroute](#) on page 28

- [IP address and settings reuse](#) on page 29
- [QoS](#) on page 29
- [IEEE 802.1D and 802.1Q](#) on page 29
- [Displaying network audio quality](#) on page 30
- [Enabling Qtest for audio quality](#) on page 31
- [IP address lists and station number portability](#) on page 31
- [TCP/UDP Port Utilization](#) on page 31
- [Security](#) on page 36
- [Time-to-Service \(TTS\)](#) on page 38

Enabling SNMP

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

You can restrict the IP addresses from which the telephone accepts SNMP queries with the SNMPADD parameter. You can also customize your community string with the SNMPSTRING parameter. 9600 Series IP deskphones support the functionality introduced with Avaya Communication Manager Release 4.0 that allows call server administration of SNMPADD and SNMPSTRING. For more information, see [Server Administration](#) on page 57 and [9600 Series H.323 Customizable System Parameters](#) on page 78.

*** Note:**

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

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

*** Note:**

The H.323 software Release 3.1 MIB differs from the software Release 6.0 and later MIBs. Be sure to download the MIB(s) applicable to your environment.

Ping and traceroute

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

instruction and sends a message to the call server indicating the results. For more information, see your call server administration documentation.

IP address and settings reuse

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

QoS

For more information about the extent to which your network can support any or all of the QoS initiatives, see your LAN equipment documentation. See [Administering QoS](#) on page 43 about QoS implications for the 9600 Series IP deskphones.

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 43 and [Administering a VLAN](#) on page 100. Three bits of the 802.1Q tag are reserved for identifying packet priority to allow any one of eight priorities to be assigned to a specific packet.

- 7: Network management traffic
- 6: Voice (traffic with less than 10ms latency and jitter)
- 5: Video (traffic with less than 100ms latency and jitter)
- 4: "Controlled-load" traffic for critical data applications
- 3: Traffic meriting "extra-effort" by the network for prompt delivery, for example, executive E-mail
- 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.

Displaying network audio quality

All 9600 Series IP deskphones give the user an opportunity to monitor network audio performance while on a call. The Network Information screen displays this information. 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 shown, or (if not shown) first select Phone Settings, then select the Network Information option. On touchscreen deskphones (9621G, 9641G, and 9670G), access the Home screen, then select Settings, then Network Information.

While on a call, the telephones display network audio quality parameters in real-time, as shown in [the table](#) on page 30.

Table 3: Parameters in real-time

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

The implication for LAN administration depends on the values the user reports and the specific nature of your LAN, like topology, loading, and QoS administration. This information gives the user 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.

Enabling Qtest for audio quality

About this task

A Qtest capability can be enabled that allows network quality information to be displayed when the deskphone is not on a call. When the QTESTRESPONDER parameter is set to an IP Address, a Qtest softkey displays on the Network Information screen when a call is not active; see [Network Audio Quality Display](#) on page 30 for information on accessing this screen. When the Qtest softkey is pressed, UDP packets are sent to the echo port at the IP Address specified by QTESTRESPONDER, and statistics are computed and displayed based on the returned packets. A UDP port is opened for Qtest only while it is active; see [TCP/UDP Port Utilization](#) on page 31 for the UDP port numbers applicable to Qtest.

IP address lists and station number portability

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

This capability also has the advantage of making station number portability easier. Assume a situation where the company has multiple locations in London and New York, all sharing a corporate IP network. Users want to take their telephones from their offices in London and bring them to New York. When users start up their telephones in the new location, the local DHCP server usually routes them to the local call server. With proper administration of the local DHCP server, the telephone knows to try a second call server IP address, this one in London. The user can then be automatically registered with the London call server.

[Server Administration](#) on page 57 contains details on administration of DHCP servers for lists of alternate call servers, router/gateways, and HTTP/HTTPS servers. For more information, see [DNS Addressing](#) on page 105.

TCP/UDP Port Utilization

The 9600 Series IP deskphones use a variety of protocols, particularly TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and TLS (Transport Layer Security) to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP ports each piece of equipment uses to support each protocol and each task within the protocol. For additional TCP/UDP port utilization information as it applies to Avaya Communication Manager, see [UDP Port Selection](#) on page 42.

Depending on your network, you might need to know what ports or ranges are used in the deskphone operation. Knowing these ports or ranges helps you administer your networking infrastructure.

*** Note:**

In many cases, the ports used are the ones called for by IETF or other standards bodies. Some of the explanations in [the table](#) on page 32 and [the table](#) on page 33 refer to configuration parameters or options settings. For more information about parameters and settings, see [Administering Options for 9600 Series H.323 Deskphones](#) on page 77.

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

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 phone's SSH server	TCP
The number used in the Source Port field of DNS packets sent by the telephone	Any	Received DNS messages	UDP
The number used in the Source Port field of the packets sent by the telephone's HTTP client	Any	Packets received by the telephone's HTTP client	TCP
Release 2.0+ = PUSHPORT Pre-Release 2.0 = 80	Any	Packets received by the telephone's HTTP server	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 the TLS/SSL packets sent by the telephone's HTTP client	Any	TLS/SSL packets received by the telephone's HTTP client	TCP
68	Any	Received DHCP messages	UDP
161	Any	Received SNMP messages	UDP
500	Any	Received DHCPv6 messages	UDP
500, 2070, or 4500	500 or 4500	Received IKE or IPsec messages (if NVIKEOVERTCP is 0 or 1)	UDP
50000	Any	Received CNA test request messages	UDP

Destination Port	Source Port	Use	UDP or TCP?
50011	Any	Received SLA discovery and test request messages	UDP
50012	Any	Received SLA RTP test packets	UDP
The number used in the Source Port field of registration messages sent by the telephone's CNA test plug	Any	Received CNA registration messages	TCP
1720	Any	H.323 signaling messages	TCP
The number used in the Source Port field of RAS packets sent by the phone	1719	H.323 RAS messages	UDP
As specified by CM, or as reserved for CNA RTP tests during CNA registration	Any	Received RTP and SRTP packets	UDP
The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd.	Any	Received RTCP and SRTCP packets	UDP
The number used in the Source Port field of registration messages sent by the telephone's SLA agent.	Any	Received SLA registration messages	TCP

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

Destination Port	Source Port	Use	UDP or TCP?
7	Any unused port number	Transmitted Qtest messages	UDP
The number used in the Source Port field of packets received by the phone's SSH server.	22	Packets transmitted by the phone's SSH server	TCP
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
Release 2.0+ = HTTPPORT	Any unused port number	Packets transmitted by the telephone's HTTP client during startup	TCP

Network Requirements

Destination Port	Source Port	Use	UDP or TCP?
Pre-Release 2.0 = 80 unless explicitly specified otherwise (i.e. use of Port 81 for CM)			
80 unless explicitly specified otherwise (e.g., in a URL or due to use of WMLPORT)	Any unused port number	Packets transmitted by the telephone's HTTP client after startup (for example, for backup/restore or push)	TCP
The number used in the Source Port field of the SNMP query packet received by the telephone	161	Transmitted SNMP messages	UDP
The number used in the Source Port field of packets received by the telephone's HTTP server	Release 2.0+ = PUSHPORT Pre-Release 2.0 = 80	Packets transmitted by the telephone's HTTP server	TCP
Release 2.0+ = TLSPORT Pre-Release 2.0 = 411	Any unused port number	TLS/SSL packets transmitted by the telephone's HTTP client during startup	TCP
443 unless explicitly specified otherwise (i.e. in a URL)	Any unused port number	TLS/SSL packets transmitted by the telephone's HTTP client after startup (for example, for backup/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
33434 - 33523 (starts with 33434, increments by 1 for each message sent, 3 messages per hop, up to 30 hops)	Any unused port number	Transmitted traceroute messages	UDP
CNAPORT	Any unused port number	Transmitted CNA registration messages	TCP
The port number received in the Transport Address field in the RCF message	1720	H.323 signaling messages	TCP

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

Destination Port	Source Port	Use	UDP or TCP?
A port number specified in the SLA discovery message	Any unused port number	Transmitted SLA registration messages	TCP

Security

For information about toll fraud, see the respective call server documents on the Avaya support Web site. The 9600 Series IP deskphones cannot guarantee resistance to all DoS (Denial of Service) attacks. However, there are checks and protections 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). This standard allows the telephone to establish a secure connection to a HTTP server, in which the upgrade and settings file can reside. This setup adds security over another alternative.

HTTP authentication is supported for backup and restore operations. The authentication credentials and the realm are stored in reprogrammable non-volatile memory that is not overwritten if new telephone 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 telephone 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 userid, password or realm used is different than those currently stored in the telephone, the new value(s) will replace the currently stored value(s).

You also have a variety of optional capabilities to restrict or remove how crucial network information is displayed or used. These capabilities are covered in more detail in [Server Administration](#) on page 57.

- Support signaling channel encryption.

*** Note:**

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

- Restricting the response of the 9600 Series IP Deskphones to SNMP queries to only IP Addresses on a list you specify.
- Specifying an SNMP community string for all SNMP messages the telephone sends.
- Restricting dialpad access to Local Administration Procedures, such as specifying IP Addresses, with a password.

- Restricting dialpad access to Craft Local Procedures to experienced installers and technicians.
- Restricting the end user's ability to use a telephone Options application to view network data.
- As of Release 2.0, 9600 Series IP Telephones can download and use third-party trusted certificates.
- As of Release 1.5, 9600 Series IP Telephones are fully compliant with IETF RFC 1948 *Defending Against Sequence Number Attacks*, May 1996, by S. Bellovin.
- As of Release 1.5, three existing security-related parameters can be administered on the call server and downloaded with encrypted signaling, in addition to unencrypted HTTP or encrypted HTTPS. Those parameters are SNMP community string (SNMPSTRING), SNMP Source IP Addresses (SNMPADD), and Craft Access Code (PROCPSWD).
- As of Release 6.2, you can download an application file from the Avaya Support Web site that does not support VPN or media encryption.

Related topics:

[Registration and Authentication](#) on page 37

[Secure Shell Support](#) on page 37

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 telephones to monitor, diagnose, or debug telephone performance. Only the SSHv2 version is supported. Because of the sensitive nature of remote access, you can disable permission with the SSH_ALLOWED parameter. Even if permission is given, the telephone takes several security precautions. First, a security warning message is displayed. You can specify your own file using SSH_BANNER_FILE, or the following default file will be used:

```
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 want to use a custom warning message, `SSH_BANNER_FILE` can be set to an absolute URL, or alternatively the name of the file on the standard file server (e.g. `HTTPSRVR`).

In addition to the warning message, you can administer the amount of inactivity time that will disable SSH (with `SSH_IDLE_TIMEOUT`), the number of failed login attempts that will disable SSH (with `SSH_LOCKOUT_ATTEMPTS`), the number of seconds the telephone delays between failed login attempts (with `SSH_LOGIN_DELAY`), or the user name permitted for SSH logins `SSH_USERNAME`.

Time-to-Service (TTS)

The IP Endpoint Time-to-Service (TTS) feature was introduced in Software Release 1.2.1, along with Avaya Communication Manager (CM) Release 4.0. TTS changes the way IP endpoints register with their gatekeeper, reducing the time to come into service. Without TTS, IP endpoints are brought into service in two steps, which are coupled: (1) H.323 registration and (2) TCP socket establishment for call signaling. The TTS feature de-couples these steps. In CM 4.0, IP endpoints can be enabled 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 endpoint, initiates socket establishment, which further improves performance. In CM 4.0, TTS is enabled by default, but can be disabled for all IP endpoints in a given IP network region by changing the IP Network form. TTS applies only to IP endpoints whose firmware has been updated to support this feature. It does not apply to the following endpoints: third party H.323, DCP, BRI, and analog.

As of software Release 3.0, 9600 Series IP deskphones will accept an incoming connection request from a server on their gatekeeper list, use this new connection to replace an existing connection, and continue operation without the need to re-register. This mechanism allows CM to quickly originate a new connection to each of these telephones during a server interchange, causing the telephones to move quickly to the server and transitioning from the standby to active state.

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

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

Chapter 4: Communication Manager Administration

Call server requirements

Before you perform administration tasks, ensure that the proper hardware is in place, and your call server software is compatible with the 9600 Series IP Deskphones. Avaya recommends the latest PBX software and the latest IP telephone firmware.

Related topics:

[Aliasing IP Deskphones for switch compatibility](#) on page 39

Aliasing IP Deskphones for switch compatibility

As of Release 1.2, 9600 Series IP telephones were natively supported by Avaya Communication Manager (CM) Release 4.0. Although the 9608, 9611, 9621, and 9641 phones are not natively supported on CM 4.0, those phones are natively supported as of CM 6.2.

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

9600 Series IP Deskphone Model	Administer on CM 3.1 as...	Administer on CM 4.0+ – CM 6.1	CM 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
9650/9650C	4620	9650	9650

9600 Series IP Deskphone Model	Administer on CM 3.1 as...	Administer on CM 4.0+ – CM 6.1	CM 6.2
9670G	4620	9630 or 9640	9630 or 9640

*** Note:**

Avaya recommends that the 9608, 9611, 9621, and 9641 telephones be aliased as 9560s, however if you have already aliased these telephones 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 (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 9620/9620L/9620C can be aliased as a 4620SW IP telephone, 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:**

Call appearances are not configurable for native support of the 9610 in CM 4.0. Care should be taken when aliasing the 9610 as a 4610, since the call appearances are configurable but must adhere to the unique 9610 administrative guidelines found in [Administering 9610 IP Telephone features and CAs](#) on page 50 and [Special Administration for the 9610 IP Telephone](#) on page 147.

*** Note:**

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

For specific administration instructions about aliasing 9600 Series IP telephones, see [Administering stations](#) on page 49.

When a 9610 IP telephone is aliased as a 4610SW IP telephone, its four administrable call appearances/features should be:

- one primary call appearance
- the Directory, Next, and Make Call feature buttons (hard-coded with CM 4.0 or later)

The 9610 ignores any other features or call appearances.

When a 9620/9620L/9620C IP Telephone is aliased as a 4620SW IP telephone, do not administer:

- a button module (SBM24, EU24, or EU24BL), or
- 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 within CM 4.0 or later, support up to three SBM24 Button Modules per telephone. As of software Release 6.0, the 9608, 9611G, and 9641G can support up to three BM12 Button Modules or up to three SBM24 Button Modules; 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 twenty-four administrable call appearances and features; the BM12 displays twelve call appearances/features at a time on each of two pages. Either button module can be used freestanding or attached directly to the applicable deskphone.

Administering the call server (switch)

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

- The *Administrator Guide for Avaya Communication Manager* (Document Number 03-300509) provides detailed instructions for administering an IP telephone system on Avaya Communication Manager. See Chapter 3 “Managing Telephones,” which describes the process of adding new telephones. Also, you can locate pertinent screen illustrations and field descriptions in Chapter 19 “Screen References” of that guide.
- *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504) provides detailed information about switch administration for your network.

Related topics:

[Administering the IP interface and addresses](#) on page 42

[Administering UDP port selection](#) on page 42

[Administering RSVP](#) on page 42

[Administering QoS](#) on page 43

[Administering IEEE 802.1Q](#) on page 43

[Administering DIFFSERV](#) on page 43

[Administering NAT](#) on page 43

Administering the IP interface and addresses

Follow these general guidelines:

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

Administering UDP port selection

The 9600 Series IP deskphones can be administered from the Avaya Communication Manager Network Region form to support UDP port selection. Locate specific port assignment diagrams in the appropriate *Avaya one-X® Deskphone H.323 Installation and Maintenance Guide* (Document Number 16-603603 for the 9608, 9611G, 9621G, and 9641G deskphones, and Document Number 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* (Document Number 555-233-504) on the *Avaya support Web site*.

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

Administering RSVP

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

The only way to enable RSVP is by appropriate switch administration. For more information, see your Avaya server administration documentation and *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 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 telephones. 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, per the IEEE 802.1Q standard. To support IEEE 802.1Q, you can administer 9600 Series IP deskphones from the network via LLDP, or by appropriate administration of the DHCP or HTTP/HTTPS servers.

The four IEEE 802.1Q QoS parameters in the telephones that can be administered on the IP Network Region form are L2Q, L2QVLAN, L2QAUD, and L2QSIG. To set these parameters at the switch, see “About Quality of Service (QoS) and voice quality administration” in *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504). To set these parameters manually see the *applicable Avaya one-X® Deskphone H.323 Installation and Maintenance Guide* (Document Number 16–603603 for the 9608, 9611G, 9621G, and 9641G deskphone models, and Document Number 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 telephone registers. For more information, see Chapter 4 “Network Quality Administration” in *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504). Unless there is a specific need in your enterprise LAN, Avaya recommends that you 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 telephones do not support communication to the PBX through any NAPT device.

NAT requires specific administration on the call server. A direct Avaya IP telephone-to-Avaya IP telephone call with NAT requires Avaya Communication Manager Release 3.0 or greater

software. For more information, see *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504) on the Avaya support Web site.

Administering Voice Mail

Administering voice mail for deskphones with CM 4.0+ Native support

Release 1.2 and later provides native support for 9600 Series IP deskphones running on Avaya Communication Manager (CM) Release 4.0 or later. Although the 9608, 9611, 9621, and 9641 are not natively supported on CM 4.0, those phones are natively supported as of CM 6.2 as indicated in [Aliasing IP Deskphones for switch compatibility](#) on page 39. When native support applies, pressing the **Messages** button causes the telephone to first determine if the call server has a dedicated number for retrieving voice mail and when found, to proceed with voice mail retrieval.

Administering 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. MSGNUM examples are:

- 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 that allows the voice mail system and Avaya Communication Manager Automated Call Processing (ACP) to exchange information.

When the user presses the **Messages** button on the telephone, that number or FAC is automatically dialed, giving the user one-touch access to voice mail.

The settings file specifies the telephone number to be dialed automatically when the user presses this button. The command is:

```
SET MSGNUM 1234
```

where 1234 is the Voice Mail extension (CM hunt group or VDN). For more information, see [9600 Series H.323 Customizable System Parameters](#) on page 78.

*** Note:**

MSGNUM is only used when the telephone is aliased using non-native support. Messaging must be configured for native support. A separate Voice Mail extension can be administered for each station.

Administering call transfers

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

- When the system parameter *Abort Transfer?* is set to *Yes*, once a transfer has been started the user cannot press a non-idle call appearance until the transfer is complete or the transfer is aborted.
- When 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.
- When 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.
- When 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. This is the case when *Transfer Upon Hang-up* is set to *Yes*, regardless of the *Abort Transfer?* setting.
- The transfer is aborted. This is the case when *Transfer Upon Hang-up* is set to *No* and *Abort Transfer?* is set to *Yes*.
- The transfer is denied. This is the case when *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.

The call server feature, *Toggle Swap* allows the user 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 only works 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. Toggle Swap is ignored without a broken flutter if pressed while the setup call appearance is still dialing. Toggle swapping the hold status of call appearances can be confusing to the user.

Administering call conferencing

This section provides information about conference call behaviors to consider when administering the call server. The telephone application presents a user interface, based in part on the deduction of the call state. But, as the administrator, be aware that the following server-based features can interact with the user interface resulting in a call state that might need explanation:

- When the system parameter Abort Conference Upon Hang-up is set to *Yes*, the user must dial and press the **Complete** softkey for the conference to be completed. If the user hangs up during conference setup before pressing **Complete**, the conference is cancelled with the held party remaining on [hard] hold. When the system parameter Abort Conference Upon Hang-up is set to *No*, the user can hang up immediately after dialing, dial a third party, then press the **Complete** softkey to have the conference proceed normally.
- When the system parameter No Dial Tone Conferencing is set to *No*, and the **Conference** or **Add** softkey is pressed, the call server automatically selects an idle call appearance for the user to dial on. This action allows the next conferee to be added. When the system parameter No Dial Tone Conferencing is set to *Yes*, the user must manually select a call appearance after pressing the **Conference** or **Add** softkey.

Conferencing behavior changes significantly when Select Line Conferencing is set to *Yes*, which automatically sets No Dial Tone Conferencing to *Yes*. Specifically:

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

When the system parameter Select Line Conferencing is set to *No*, the user cancels 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; the user must press **Join** to add the answered call to the conference. If the user does not want the incoming call

to be part of the conference, the call should not be answered, or the call can be answered and then hung up before continuing the conference setup. Pressing an in-use call appearance during conference setup makes that call appearance the intended conferee. The Toggle Swap feature works for Conference setup just like it does for Transfer Setup. For more information, see the last paragraph of [Administering call transfers](#) on page 45.

Administering Deskphones on Avaya Aura Communication Manager (CM)

This section covers Avaya Aura Communication Manager (CM) administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. The system-wide CM form and the particular page (screen) that needs to be administered for each feature are provided. These features are not required but are recommended because they optimize the telephone user interface. CM 3.1.2 or greater is required.

Related topics:

[Administering feature-related system parameters](#) on page 47

Administering feature-related system parameters

Avaya Communication Manager Release 4.0 and later allows call server administration of three system-wide parameters. By administering these parameters on CM, they can be automatically downloaded to the telephone during registration, instead of or in addition to using the settings file or setting them locally for each telephone. The three system parameters are: SNMP community string, SNMP Source IP addresses, and Craft Access Code (PROCPSWD). Administer these three parameters using 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.

Name	Description
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, this is also where you 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. Block Enhanced Conference Display on the Class of Restriction (COR) form must be set to No. Use the command Change COR , followed by a number, to view the form and make the change. a sample of the Class of Restriction form.
EC500	If EC500 licenses have been acquired, enable EC500 on the Off-PBX Telephones Station Mapping form. This feature requires trunking to work properly. Use the following command to make the change: Change Off-pbx Telephone Mapping
Wideband Audio	<p>To enable Wideband Audio, use 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 such that the media travels directly between the two 96xx IP deskphones. Calls involving three or more parties, even if they are all 96xx IP deskphones, will not use wide band. Calls between two 96xx IP deskphones where audio is terminated at a port network/gateway (PN/GW) media resource will not use wideband.</p> <p>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 deskphones exist. Technically, G722 does not need to be first. What is needed, however, is that all the non media processor-supported codecs (G722,</p>

Name	Description
	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.

Administering stations

Administer the following items on the Station form, which comprises several pages. Avaya recommends setting the features covered in this section because they optimize the user interface.

Avaya Aura Communication Manager Release 4.0 and later allows central call server administration of the GROUP parameter on a station-by-station basis, which is then downloaded to each applicable telephone starting with the next telephone boot-up. As covered in [Using the GROUP parameter to set up customized groups](#) on page 74, the GROUP Identifier can be used in conjunction with the 46xxsettings file to allow administration to apply to specific “groups” of telephones. The GROUP ID parameter is administered on page 3 of the Change Station Form.

If applicable, before administering stations be sure the deskphones are aliased according to the chart for [Aliasing IP Deskphones for switch compatibility](#) on page 39.

Related topics:

[Administering features](#) on page 49

Administering features

The following are administrable Station Features that Avaya recommends for maximum user experience.

Name	Description
Enhanced Conference Features	Administer Conf-dsp (conference display) on the station form as a feature button. Doing so turns on enhanced conference features and gives users advanced conference features.
Far End Mute	Administer fe-mute (far end mute). When this is enabled the phone shows a “Silence”

Name	Description
	softkey on the Conference details screen. This feature works only for trunk calls.
Send All Calls (SAC)	On the Station form, administer SAC (send-calls) as a feature button. On the Station form to the right of where send all calls is administered, leave the extension box empty. This feature requires a coverage path to be administered on the station form.
Coverage Path	For normal operation, you must set up a coverage path for each telephone. Administer the Station form to point to the appropriate system coverage path, for example, coverage path 1.
Auto select any idle appearance	Set Auto select any idle appearance to N (no) to optimize answering calls.
Restrict Last Call Appearance	Set Restrict Last Call Appearance to Y (yes).
Conference/Transfer on Primary Appearance	Set Conference/Transfer on Primary Appearance to Y (yes) to ensure that conference/transfer of a bridged appearance works properly.

*** Note:**

If you are administering the agent sign in method for a call center, see [Administering agent sign ins for call centers](#) on page 131 for guidance.

Administering feature buttons and call appearances (CAs)

Administering 9610 IP Telephone features and CAs

About this task

The 9610 must be administered on releases earlier than CM3.1 as a 4610. On Release CM4.0 and later, administer the 9610 as a 9610. The 9610 has only one line appearance. As a consequence, you must follow these CM administration steps:

Procedure

1. Administer the first call appearance/feature button on the CM Station form as a call appearance.
2. Administer “Directory,” “Next,” and “Call-disp (the latter being shown as “Make Call” on the telephone) as the next three feature buttons.
This is hard-coded on CM 4.0 and later.
3. Anything administered beyond the first six call appearances will be ignored.
On CM4.0 and later the call appearance/feature button assignments are hard-coded.

! Important:

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

*** Note:**

A 9610 IP telephone does not reflect CM administrative changes until the telephone is reset/restarted. The 9610 does not support the SBM24 button module.

Administering 9620/9620L/9620C IP Telephone features and CAs

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

Administering features and CAs for all other IP Deskphones

You can administer Feature/Call Appearance Buttons 1 – 24 on the CM Station form. The features administered on the Station form appear in the same sequence on the telephone Feature screen. Features administered on the Expansion Module SBM24/BM12 Call Appearance buttons display on the telephone 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](#) on page 52 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...	are displayed on this deskphone as:			
1 to 3	9620/9620C/ 9620L	9608 9611G 9621G 9630/9630G 9640/9640G 9641G	9650/9650C	9670G
4 to 11	CAs/BAs on Phone screen; must scroll to see more than 3	CAs/BAs on Phone screen: must scroll to see more than 6	Aux buttons 1 to 8 CAs/BAs on Phone screen; must scroll to see more than 3	CAs/BAs on Phone screen; all buttons also appear on the Quick Touch panel (if enabled) and not on the display screen. If Quick Touch panel is disabled, 6 CAs display; switch to Features and scroll to see up to 12 feature buttons
12 to 19	N/A	Scroll to see CAs/BAs, features on Feature List	Aux buttons 9 to 16	Scroll to see CAs/BAs, features on Feature List
20 to 24	N/A	Features on Feature List	Features on Feature List	Features on Feature List
25 to 48	N/A	1st SBM24	1st SBM24	1st SBM24
49 to 72	N/A	2nd SBM24	2nd SBM24	2nd SBM24
73 to 96	N/A	3rd SBM24	3rd SBM24	3rd SBM24

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

- *Administrator Guide for Avaya Communication Manager* (Document Number 03-300509).
- *Feature Description and Implementation for Avaya Communication Manager* (Document Number 555-245-770).

Administering enhanced Phone screen displays for certain IP Deskphones

For the 9608, 9611G, and 9630/9630G/9640/9640G deskphones, if the system parameter FBONCASCSCREEN has value "1" the telephone determines the total number of call appearances (primary or bridged) that have been administered for the telephone (plus any adjunct button modules, if applicable).

If the total number of call appearances is less than the number of Application Lines the deskphone supports, then all call appearances (primary or bridged) that have been administered for the telephone (including any adjunct button modules, if applicable) are displayed in order. The remaining Application Lines display the first administered feature buttons for the telephone, in order from top to bottom without any gaps. Note that this applies to administered feature buttons for the telephone only; administered feature buttons for any adjunct button module are not displayed on this list.

Assigning 9650/9650C Aux Buttons

About this task

The 9650/9650C CM 4.0 Station form assigns buttons 4 to 11 to the Aux Labels 1 to 8, and buttons 12 to 19 to the shifted view of Aux buttons 9 to 16. CM button assignments 20-24 do not appear on the Aux button labels. Additionally, any call appearances that are assigned to CM buttons 4 through 24, like all the 96xx phones, appear on the Phone screen in a scrollable list. Any feature assigned to CM buttons 4 through 24, like the other 96xx phones, appears on the features list (reached by pressing the left or right arrow key while viewing the call appearances screen on the phone).

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

Procedure

1. The Aux button label area can fit 6-7 characters, depending on the width of the characters used.

2. Cluster any call appearances together, bridged call appearances together, or similar features together.
For example, keep “Directory” “Next” and “Make Call” adjacent on the same Aux button row. Do not split like labels between the two sets of Aux buttons.
 3. Administer features that are not directly usable by the user, such as enhanced conference display, on the Station Form on buttons 20 to 24.
 4. Call appearances display 5 digits with a reserved area for a call state icon.
 5. Under the A menu, the first two Call Settings items allow the users to set the phone to go to the Phone screen when the phone is ringing (Go to Phone Screen on Ringing) and/or when the user is dialing (Go to Phone Screen on Dialing).
In general, Avaya recommends that you set both to Yes - except for users covering many bridged appearances who may prefer to set the Go to Phone Screen on Ringing option to No. Users can change these settings for themselves using the Call Settings submenu.
 6. Group similar types of Aux buttons together on one page (Aux buttons 1-8 or Aux buttons 9-16) if possible.
 - If the user has bridged call appearances on Aux buttons, assign the bridged lines to Aux buttons 1-8 or to Aux buttons 9-16.
 - If the user has AD buttons, put them on the same page, if possible.
 - Keep related features on the same page of Aux buttons. For example, keep “Directory,” “Next,” and “Make call” together on the same row of Aux button labels and do not split between Aux buttons 8 and 9, which represent two different “pages.”
 7. Administer features that are not directly usable by the user, such as enhanced conference display on the Station form on buttons 20 to 24.
 8. Call appearances display 5 digits with a reserved area for a call state icon.
-

Administering button module(s) on the 9608, 9611G, 9630/9630G, 9640/9640G, 9641G, 9650/9650C, and 9670G

Use the applicable Station form to enable the SBM24 or BM12 Button (Expansion) Module(s) and administer Call Appearances as primary appearances, bridged appearances, or busy indicators.

If the BM12 or SBM24 Call Appearance corresponding to the CM call-associated display message or dialed-digits string is not visible because the user is not on the Phone screen, the telephone Top Line displays the call-associated display message or dialed-digits string.

Administering the Conference Details screen for ad-hoc conferences

About this task

Conference Details allows the user to view parties on a conference call and selectively mute or drop individual parties for a conference call setup.

If administered on an Expansion Module button, the BM12 or SBM24 Button Module must be connected.

Procedure

1. To enable Conference Details capabilities, on the Class of Restriction (COR) form make sure that **Block Enhanced conference/Transfer Displays** is set to No .
 2. As described in [Administering feature-related system parameters](#) on page 47, administer the Conference Display Feature Button to a Phone button on the Phone screen.
-

Administering the Quick Touch panel for touchscreen deskphones

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

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

The basic appearance of a Quick Touch button resembles an actual physical button, and provides appropriate “pressed” (down) and “not pressed” (up) appearances.

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

The Quick Touch Panel is displayed on the Phone screen call appearance list and the Personalizing button labels option, when enabled by the associated user option (Home-> Settings-> Options & Settings-> Screen & Sounds-> Show Quick-Touch Panel), even if it contains 0 buttons. If all or any buttons are empty, that should indicate to the user that some configuration or administration needs to be done. For the 9670, the user can select to display

all eight, or no Quick Touch buttons; the 9621G and 9641G provide the option to display all eight, or four, or no Quick touch buttons.

Administering shuffling

About this task

Administer shuffling on three forms:

Procedure

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

Administering wide band codecs

About this task

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

Chapter 5: Server Administration

Software Prerequisites

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

 **Note:**

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

 **Caution:**

The firmware in the 9600 Series IP Deskphones reserves IP Addresses of the form 192.168.2.x for internal communications. The telephone(s) improperly use addresses you specify if they are of that form.

Administering the DHCP and File Servers

Dynamic Host Configuration Protocol (DHCP) minimizes maintenance for a 9600 Series IP Telephone network by removing the need to individually assign and maintain IP Addresses and other parameters for each IP telephone on the network.

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

- IP Address of the 9600 Series IP Telephone(s)
- IP Address of the Avaya call server
- IP Address of the HTTP or HTTPS file server
- The subnet mask
- IP Address of the router
- DNS Server IP Address

Administer the LAN so each IP telephone can access a DHCP server that contains the IP Addresses and subnet mask.

The IP telephone cannot function without an IP Address. The IP Address reuse capability allows the phone to reuse its previous IP Address and parameter settings even if the DHCP server is temporarily unavailable. A user can manually assign a different IP Address to an IP

telephone. When the DHCP server finally returns, the telephone never looks for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process.

Avaya recommends that:

- A minimum of two DHCP servers be available for reliability.
- A DHCP server be available when the IP telephone reboots.
- A DHCP server be available at remote sites if WAN failures isolate IP Deskphones from the central site DHCP server(s).

The file server provides the 9600 Series IP Telephone with a script file and, if appropriate, new or updated application software. See [Step 3: Establishing a VPN Connection \(optional\)](#) on page 22 under [Deskphone Initialization Process Overview](#) on page 21. In addition, you can edit an associated settings file to customize telephone parameters for your specific environment. For more information, see [Administering Telephone Options](#) on page 77.

Administering the DHCP Server

This document concentrates on the simplest case of a single LAN segment. Information provided here can be used for more complex LAN configurations.

 **Caution:**

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

Related topics:

[Configuring DHCP Option 242 \(SSON\)](#) on page 58

Configuring DHCP Option 242 (SSON)

About this task

To administer DHCP option 242 (the default site-specific option, which applies to DHCPv4 only), make a copy of an existing option 176 for your 46xx IP Telephones. You can then either:

Procedure

1. Leave any parameters the 9600 Series IP Deskphones do not support for setting via DHCP in option 242 to be ignored, or

2. Delete unused or unsupported 9600 IP Series Telephone parameters to shorten the DHCP message length.

Result

Only the following parameters can be set in the DHCP site-specific option for 96xx telephones, 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
DNSSVR	DNS server IP address(es).
DOMAIN	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 (pass-through of multicast EAPOL messages to an attached PC, and enable 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 96xx telephone 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 via 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 be used for HTTP file downloading.
HTTPSRVR	IP Address(es) or DNS name(s) of HTTP file server(s) used to download 96xx telephone 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 (sends Destination Unreachable messages for closed ports used by traceroute).
ICMPRED	Controls whether ICMP Redirect messages are processed. The default is 0 (redirect messages are not processed).
L2Q	802.1Q tagging mode. The default is 0 (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.

Parameter	Description
MCIPADD	CM server(s) IP Address(es) or DNS name(s). 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 via DHCP improves reliability if the file server is not available due to server or network problems.
NDREDV6	IPv6 only. Controls whether IPv6 Neighbor Discovery Redirect messages will be processed.
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 (auto-negotiate).
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 (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 (access to all administrative options is allowed).
REREGISTER	The number of minutes the telephone waits before., and between, re-registration attempts
REUSETIME	The number 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 telephone (not via DHCP or in the 46xxsettings.txt file), and 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 telephone is currently using.
SNMPADD	Allowable source IP Address(es) 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 via DHCP or a settings file. If a manually-programmed file server IP Address is to be used, STATIC must be set via DHCP.
TLSDIR	Specifies the path name prepended to all file names used in HTTPS GET operations during startup.
TLSPORT	Specifies the TCP port number used for HTTPS file downloading.

Parameter	Description
TLSSRVR	IP Address(es) or DNS name(s) of Avaya file server(s) used to download configuration files. 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 telephone will attempt unnamed registration.
VLANTEST	Controls the length of time the telephone tries DHCP with a non-zero VLAN ID. When the interval is exceeded, the telephone records the VLAN ID so that it is not used again, and DHCP continues on the default VLAN. The default is 60 seconds.

These parameters are saved in a 9600 Series IP Telephone's non-volatile memory. If the DHCP server is not available for any reason during telephone restart or reboot, the telephone uses these saved parameters.

DHCP Generic Setup

This document is limited to describing generic DHCPv4 and DHCPv6 administration that works with the 9600 Series IP Deskphones. Several DHCP software alternatives are common to Windows operating systems including:

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

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

Setting up the DHCP server

About this task

DHCP server setup involves:

Procedure

1. Installing the DHCP server software according to vendor instructions.
2. Configuring the DHCP server with:

- IP Addresses available for the 9600 Series IP deskphones.
- The following DHCP options if IPv4 will be used:
 - **Option 1 - Subnet mask.**
 - **Option 3 - Gateway (router) IP Address(es).** 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 server(s) 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, non zero, dotted decimal address.
 - **Option 15 - DNS Domain Name.** This string contains the domain name to be used when DNS names in system parameters are resolved into IP Addresses. This domain name is appended to the DNS name before the 9600 IP Telephone attempts to resolve the DNS address. Option 15 is necessary if you want to use a DNS name for the HTTP server. Otherwise, you can specify a DOMAIN as part of customizing HTTP as indicated in [DNS Addressing](#) on page 105.
 - **Option 51 - DHCP lease time.** If this option is not received, the DHCPOFFER is not be accepted. Avaya recommends a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the IP Address lease is assumed to be infinite as per RFC 2131, Section 3.3, so that renewal and rebinding procedures are not necessary even if Options 58 and 59 are received. Expired leases cause Avaya IP deskphones to reboot. Avaya recommends providing enough leases so an IP Address for an IP telephone does not change if it is briefly taken offline.

*** Note:**

The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP Address. However, if the network has problems and the only DHCP server is centralized or if the DHCP server itself has problems, the telephone will not receive responses to its request for a renewal of the lease. In this case the telephone will not be usable until the server can respond. Expired leases do not cause the phone to reboot - it can be renewed. However, if the new IP address is different that previous it will cause the phone to reboot. Ensure that once assigned an IP Address, the telephone continues using that address after the DHCP lease expires, until a conflict with another device is detected. As [9600 Series H.323 Customizable System Parameters](#) on page 78 indicates, the system parameter DHCPSTD allows an administrator to specify that the telephone will either: a). Comply with the DHCP standard by setting DHCPSTD to "1", or b). Continue to use its IP Address after the DHCP lease expires by setting DHCPSTD to "0." The latter case is the default. If the default is invoked, after the DHCP lease expires the telephone continues to broadcast DHCPREQUEST messages for its current IP

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

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

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

An example of good DHCP administration is:

- Option 242 for DHCP: "MCIPADD =xxxx.xxx.xxx.xxx"

Result

In the table that follows, the 9600 Series IP Telephone sets the parameter values to the DHCPACK message field and option contents shown.

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).
DNSSVR	Option #6.
HTTPSRVR	The siaddr field, if that field is non-zero.
TLSSVR	The siaddr field, if that field is non-zero.

Since the DHCP site-specific option is processed after the DHCP fields and standard options, any values set in the site-specific option will supersede any values set via DHCP fields or standard options, as well as any other previously set values. Values that can be set using the DHCP site-specific option are listed in [Parameters Set by DHCP in a Site-Specific Option](#).

Parameters L2Q, L2QVLAN, and PHY2VLAN are not set from a *site-specific option* if their values were previously set by LLDP. For more information, see [About Link Layer Discovery Protocol \(LLDP\)](#) on page 108.

*** 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 77.

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

Setting up a DHCPv6 server

About this task

! Important:

IPv6 operation is limited to a specific customer set and is not for general use.

DHCPv6 server setup involves:

Procedure

1. Installing the DHCP server software according to vendor instructions.
2. Configuring the DHCP server to send a Vendor-Specific Information (VSI) option with an enterprise number of 6889 (the Avaya Enterprise Number).

3. Within that Vendor-Specific Information option, including a vendor-specific option with an opt-code of 242.
4. Setting the option-data portion of the vendor-specific option with any or all of the applicable parameters listed in the bullet list that precedes this section for the DHCP site-specific option.

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

Result

Since the vendor-specific option is processed after the DHCP fields and standard options, any values set via the VSI will supersede any values set via DHCP fields or standard options, as well as any other previously set values.

HTTP Generic Setup

About this task

You can store the same application software, script file, and settings file on an HTTP server as you can on a TFTP server. TFTP is not supported for 9600 Series IP deskphones. With proper administration, the telephone seeks out and uses that material. Some functionality might be lost by a reset if the HTTP server is unavailable. For more information, see [Administering the DHCP and File Servers](#) on page 57.

Caution:

The files defined by HTTP server configuration must be accessible from all IP deskphones invoking those files. Ensure that the file names match the names in the upgrade script, including case, since UNIX systems are case-sensitive.

Note:

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

Important:

You must use the Avaya Web configuration server to obtain HTTPS so information is authenticated. The Avaya Web configuration server does not support backup/restore. If you intend to use HTTP for backup/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 address(es) of the HTTP server.
Include the parameter in DHCP Option 242, or the appropriate SSON Option.
3. Download the upgrade script file and application file(s) from the Avaya Web site <http://www.avaya.com/support> to the HTTP server.
For more information, see [Telephone Software and Application Files](#) on page 71.

*** Note:**

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

*** Note:**

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

Result

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

- Install the TLS server application.
- Administer the system parameter TLSSRVR to the address(es) of the Avaya HTTP server.

Backup/restore processing

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

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

For backup, the initiating process must supply the backup file and the file name, and the file is sent to the server via 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 via 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. Deletion of the file is requested from the server via an HTTP DELETE message. A success indication is returned to the initiating process if a 2xx HTTP status code is received, otherwise a failure indication is returned.

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

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

If TLS is used, the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is used. If TLS is used but no digital certificates have been downloaded based on the TRUSTCERTS value, the IP address of the call server with which the telephone is registered and the telephone's registration password 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 telephone is registered and the telephone's registration password will be 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".

When the call server IP address and the telephone's registration password 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 telephone's registration password. The server is expected to get the telephone's extension number from the backup/restore file name. The server must also protect the user's credentials once they are received via the secure TLS connection.

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

HTTP authentication is supported for backup and restore operations. The authentication credentials and the realm are stored in non-volatile memory that will not be overwritten if new telephone software is downloaded. The default value of the credentials and the realm will be null, set at manufacture and at any other time that user-specific data is removed from the telephone.

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 stored credentials are null, or if the realms do not match, or if an authentication attempt using the stored credentials fails, an HTTP Authentication or an HTTP Authentication Failure interrupt screen is displayed on the Status Line (for 9608, 9611G, 9621G, and 9641G deskphones) or the Prompt Line (for all other 9600 Series IP Deskphones):
`Enter backup/restore credentials.`

If HTTP authentication for a backup or restore operation is successful and if the userid, password or realm used differs from those currently stored in the telephone, the new value(s) replace the currently stored value(s).

About IPv4 and/or IPv6 Operation

Important:

IPv6 operation is limited to a specific customer set and is not for general use.

As of software Release 6.0 (and later), Internet Protocol (IP) operation determination follows this order:

- If NVVPMODE parameter value is set to “1” (Yes) only IPv4 operation is enabled.
- If NVVPMODE 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, any IPv6 address(es) configured as parameter values are ignored, and the next IPv4 address (if any) in a list of addresses is used. If the parameter value does not contain any IPv4 addresses, the value is treated as if it was null.

If IPv6-only operation is enabled, any IPv4 address(es) 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 value is treated as if it was null.

The results of the determination are expressed in [the table](#) on page 69.

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

Related topics:

[Features not supporting IPv6](#) on page 69

Features not supporting IPv6

The following features do not support IPv6 in H.323 software Release 6.0 or later:

- VPN (IPsec, IKEv1)
- LLDP
- RSVP (for IPv4 audio connections only)
- HTTP server Push request
- RTCP monitoring
- Remote traceroute, Remote Ping
- CNA

Chapter 6: Telephone Software and Application Files

About the general download process

The 9600 Series IP deskphones download upgrade files, settings files, language files, certificate files, and software files from a file server. All of the file types can be downloaded either via HTTP or HTTPS except the software files, which can only be downloaded via 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, once trusted certificates are downloaded into the telephone, HTTPS ensures that the file server itself will be authenticated via a digital certificate. HTTPS is not used for software file downloads because 9600 Series IP telephone software files are already digitally signed, so there is no need to 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 the telephone is first plugged in, it will attempt to contact a file server, and will download new software if the software version available on the file server is different than the version on the phone. For subsequent software upgrades, the call server provides the capability to remotely reset the telephone, which then initiates the same process for contacting a file server.

The telephone queries the file server, which, as of Software Release 6.0, transmits a 96x1Supgrade.txt file (SIP protocol) or 96x1Hupgrade.txt file (H.323 protocol) to the telephone based on the SIG parameter setting; software versions prior to Release 6.0 use a 96xxupgrade.txt file, which is not protocol-specific. The upgrade file tells the telephone which software files the telephone should use.

The 9600 Series IP deskphone then downloads a 46xxsettings.txt file. The settings file contains options you have administered for any or all of the IP deskphones in your network. For more information about the settings file, see [About the settings file](#) on page 73. After the settings file has been downloaded, any language or certificate files required by the settings will be downloaded. Finally, any new software files will be downloaded, if necessary.

Related topics:

[Choosing the right application file and upgrade script file](#) on page 72

[Changing the Signaling Protocol](#) on page 72

[About the upgrade file](#) on page 73

[About the settings file](#) on page 73

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. You download the package appropriate to your operating environment to your file server from the Avaya support Web site at: <http://www.avaya.com/support> based on the protocol you are using (H.323 or SIP) for all or the majority of your deskphones.

H.323 software distribution packages contain:

- one Upgrade file;
- all of the Display Text Language Files;
- all of the Voice Input Language Files (for 9600 Series IP deskphone software releases earlier than Release 6.0);
- 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 their own (non-Avaya) HTTP server can ignore or delete this directory.

For detailed information about downloading files and upgrading telephone software, see the appropriate *Avaya one-X[®] Deskphone H.323 Installation and Maintenance Guide (Document Number 16-300694 for all but Release 6.0+; for Release 6.1 covering the 9608, 9611G, 9621G, and 9641G deskphones, see Document Number 16-603603).*

Changing the Signaling Protocol

About this task

For enterprises requiring both H.323- and SIP-based protocols, there are two ways to specify the protocol to be used by all or specific deskphones:

Procedure

1. As of Release 6.0, the SIG parameter can be set in DHCP Option 242 (Site-Specific Option Number) or in the 46xxsettings.txt file.
This setting will apply to all telephones except those for which SIG has been manually configured to a value of H.323 or SIP using the SIG Craft procedure.
 2. The SIG parameter can be set on a per-phone basis using the SIG Craft procedure as described in the appropriate *Avaya one-X™ Deskphone H.323 Installation and Maintenance Guide (Document Number 16-300694 for all but Release 6.0; for Release 6.0 covering the 9608, 9611G, 9621G, and 9641G deskphones, see Document Number 16-603603)*.
-

About the upgrade file

The upgrade file tells the deskphone whether it needs to upgrade software. As of software Release 6.0, the upgrade file is either H.323-specific or SIP-specific. The deskphones attempt to read this file whenever they reset. The upgrade script file also points to the settings file.

Avaya recommends that you do not alter the upgrade script file. 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 telephones. The settings file includes the 9600 Series IP deskphones covered in this document and 4600 Series IP telephones, as covered in the *4600 Series IP Telephone LAN Administrator Guide (Document Number 555-233-507)*.

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

- Tags, which are lines that begin with a single “#” 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 telephone 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. The only parameters that can be used in a conditional statement are: GROUP, MACADDR, MODEL and MODEL4. In pre-6.0 software releases, BOOTNAME and SIG could also be used. In software release 3.1 and later, VPNACTIVE can also be used. In software release 6.0 and later, SIG_IN_USE can also be used.
- **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 “#” character in the first column.

 **Note:**

Enclose all data in quotation marks for proper interpretation.

- **GET** commands, of the form `GET filename`. The telephone will attempt to download the file named by *filename*, and if it is successfully obtained, it will be interpreted as an additional settings file, and no additional lines will be interpreted in the original file. If the file cannot be obtained, the telephone will continue to interpret the original file.

Download the 46xxsettings.txt template file from support.avaya.com and edit it to add your own custom settings. See [9600 Series H.323 Customizable System Parameters](#) on page 78 for details about specific values. 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

You might have different communities of users, all of which have the same telephone model, but which require different administered settings. For example, you might want to restrict Call Center agents from being able to Logoff, which might be an essential capability for “hot-desking” associates. We provide examples of the group settings for each of these situations later in this section.

Use the GROUP parameter for this purpose:

Procedure

1. Identify which telephones are associated with which group, and designate a number for each group.
The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group is assigned as Group 0.
2. The GROUP parameter can only be set either at each individual telephone or when a telephone with Software Release 1.5 or greater is registered to an Avaya Communication Manager (CM) server with CM Release 4.0 or greater.
In the former case, the GROUP Craft (local administrative) procedure must be invoked as specified in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*. In the latter case, GROUP is administrable on a phone-by-phone basis on the CM Station Form.
3. Once the GROUP assignments are in place, edit the configuration file to allow each telephone of the appropriate group to download its proper settings.

Result

Here 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 7: Administering Telephone Options

Administering Options for 9600 Series H.323 Deskphones

This chapter explains how to change parameter values by means of the DHCP or HTTP servers and provides additional topic-specific information for some related features. The [9600 Series H.323 Customizable System Parameters](#) on page 78 table lists:

- the parameter names,
- their default values,
- the valid ranges for those values, and
- a description of each one.

For DHCP, DHCP fields and options set these parameters to the desired values as discussed in [Administering the DHCP and File Servers](#) on page 57. For HTTP, the parameters are set to desired values in the settings file. For more information, see [About the settings file](#) on page 73.

Avaya recommends that you administer most parameters on the 9600 Series IP deskphones using the settings file. Some DHCP applications have limits on the amount of user-specified information. The administration required can exceed those limits for the more full-featured telephone models.

You might choose to completely disable the capability to enter or change option settings from the dialpad. 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, as of Communication Manager Release 4.0. If PROCPSWD is non-null and consists of 1 to 7 digits, a user cannot invoke any local options without first entering the PROCPSWD value on the Craft Access Code Entry screen. For more information on craft options, see the *Avaya one-X® Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

 **Caution:**

If you administer PROCPSWD as part of DHCP/HTTP administration, the value is stored and transmitted unencrypted. Therefore, do not consider PROCPSWD as a high-security technique to inhibit a sophisticated user from obtaining access to local procedures unless you administer it using page 3 of the system-parameters IP-options form, as of Avaya Communication Manager Release 4.0. Administering this password limits access to all local

procedures, including VIEW. VIEW is a read-only Craft option that allows review of the current telephone settings.

*** Note:**

All system parameters related to Virtual Private Network (VPN) setup and maintenance are described in the *VPN Setup Guide for 9600 Series IP Telephones* (Document # 16-602968).

The list of parameters that are described in that document include:

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. IPv6 operation is limited to a specific customer set and is not for general use.

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).
AGTCALLINFOSTAT	1	For Avaya Call Center use only. Automatically invokes Call-info permission when the telephone has a caller-information button administered (buttonType = 141), and AGTCALLINFOSTAT has a value of "1", the telephone sends 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 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 telephone has an application button labeled Forward, the deskphone generates an error beep and takes no forwarding action when the Forward button is pressed. 1 ASCII numeric digit. Valid values are: 1 = Disable the Forward button. 0 = Do not disable the Forward button.
AGTGREETINGSTAT	1	For Avaya Call Center use only. Indicates agent Greeting permission and determines whether the Greeting softkey displays when an incoming call is received. 1 ASCII numeric digit. Valid values are: 1 = Display the Greeting softkey upon alerting. 0 = Do not display the Greeting softkey upon alerting.
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"

Parameter Name	Default Value	Description and Value Range
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 "*" and "#").
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 (0-9, * and #)
AGTSPKRSTAT	1	For Avaya Call Center use only. Disables the speakerphone permission flag. 1 ASCII numeric digit. Valid values are: 0 = Normal speaker operation; agent can activate/deactivate the Speakerphone. 1 = Speaker is disabled; agent cannot activate/deactivate the Speakerphone. 2 = If the telephone is a 9641G, and other conditions are met (CALLCTRSTAT=1 & Release button administered & non-null Agent ID), then the Speaker button acts as a Release button.
AGTTIMESTAT	1	For Avaya Call Center use only. Suppresses the date/time permission flag and display on the Title line. 1 ASCII numeric digit. Valid values are: 1 = Do not display date and time on the top display line. 0 = Display the date and time on the top display line.
AGTTRANSLTO	to	For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters (AGTTRANSLCLBK, AGTTRANSLPRI, AGTTRANSLPK, and AGTTRANSLICOM) to parse a call-associated display message when a call appearance is in the Alerting call state. The result displays on the Agent Information line and provides information about the incoming call. 1 to 6 UTF-8 characters.
AGTTRANSLCLBK	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.

Parameter Name	Default Value	Description and Value Range
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 on page 148.
APPNAME	“ ” (Null)	The file name of the Signed Application/Library Software Package that should be downloaded and installed by the telephone during power-up or reset if it has not already been downloaded and installed. This parameter should only be set in an upgrade file.
APPSTAT	1	Controls whether specific applications are enabled, restricted, or disabled. Values are: 1=all

Parameter Name	Default Value	Description and Value Range
		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 they have become unresponsive, at which point it generates a log event and either kills the process or resets the telephone.
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.

Parameter Name	Default Value	Description and Value Range
		For more information on fine-tuning your IP phones, refer the white paper titled <i>Audio Quality Tuning for IP Telephones</i> (Document 100054528) on the Avaya Support site.
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. 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, refer the white paper titled <i>Audio Quality Tuning for IP Telephones</i> (Document 100054528) on the Avaya Support site.
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 (never turn off) to 999 minutes (16.65 hours).
BLUETOOTHSTAT	1	Bluetooth permission flag. (0=Bluetooth is disabled, 1= Bluetooth is enabled). When Bluetooth is disabled via BLUETOOTHSTAT, the user cannot override this setting locally on the telephone.
BRAUTH	0	Backup/restore authentication control. Valid values are:

Parameter Name	Default Value	Description and Value Range
		<p>1=If at least one digital certificate has been downloaded based on TRUSTCERTS, the IP address of the call server with which the telephone is registered and the telephone's registration password will be 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=telephone's call server IP Address and registration password is not included as part of GET or PUT Authorization header, or no digital certificate has been downloaded.</p>
BRURI	" " (Null)	<p>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 spaces are allowed. A subdirectory can be specified, for example: <pre>SET BRURI http://135.8.60.10/backup</pre> This puts the user backup/restore files in a subdirectory away from all other files (.bins, .txts, etc.) and permits authentication to be turned on for that subdirectory, without turning it on for the root directory. If this value is null or begins with a character sequence other than <i>http://</i> or <i>https://</i> the Backup/Restore option will not display to the telephone user.</p>
CALCSTAT	1	<p>Applies only to deskphones running software Release 6.0 and later. Specifies whether the Calculator application should be displayed/enabled. Valid values are: 1=Yes, enable the Calculator application, 0=No, disable the Calculator application.</p>
CALLCTRSTAT	0	<p>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.</p>
CLDELCALLBK	0	<p>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.</p>

Parameter Name	Default Value	Description and Value Range
CLDISPCONTENT	1	Applies only to deskphones running software Release 6.0 and later. Call Log Display Content control; indicates whether call History list includes the caller's number or not. Valid values are: 1=Display caller name but not number. 0=Display both caller name and number.
CNAPORT	50002	Avaya Converged Network Analyzer (CNA) server registration transport-layer port number (0-65535). Applies to IPv4 only. 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 ASCII characters, including commas.
DHCPSTAT	1	Applies only to deskphones running software Release 6.0 and later. Specifies whether DHCPv4, DHCPv6, or both will be used. Valid values are: 1= Use DHCPv4 only. 2= Use DHCPv6 only. 3= Use both DHCPv4 and DHCPv6. Even though “0” is not a valid value for DHCPSTAT to disable both DHCPv4 and DHCPv6, either DHCP client will be disabled if a corresponding IP address is manually programmed. This setting ensures that both DHCP clients cannot be disabled if at least one IP address was not manually programmed, because if IPV6STAT is set to “0” (preventing even an IPv6

Parameter Name	Default Value	Description and Value Range
		link-local address from being created), the telephone could be left with no network connectivity.
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 telephone strictly follows the DHCP standard with respect to giving up IP Addresses when the DHCP lease expires. If set to "0" (Yes) the telephone continues using the IP Address until it detects reset or a conflict (see DHCP Generic Setup on page 61).
DIALFEATURES	" " (Null)	A list of feature number identifiers for softkey features potentially 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 intervening spaces. For more information, see Administering features on softkeys on page 120.
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, no spaces allowed.
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 105.
DOT1XEAPS	MD5	Specifies the EAP method used for 802.1X operation. Valid values are "MD5" and "TLS" .
DOT1XSTAT	0	Determines how the telephone 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

Parameter Name	Default Value	Description and Value Range
		messages. For more information, see About IEEE 802.1X on page 105.
DROPCLEAR	1	VPN only. Specifies the treatment of clear IPsec packets. 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 on page 116 feature is turned on for all associated applications. If set to "0" the feature is turned off.
FBONCASCREEEN	0	For the 9630/9630G/9640/9640G IP deskphones, indicates whether to display feature buttons on available lines on the Call Appearance (Phone) screen. Values are: 1=Yes; 0=No.
GRATARP	0	Gratuitous ARP flag. Controls whether the telephone will process gratuitous ARPS or ignore 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. 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 gratuitous (unsolicited) IPv6 Neighbor Advertisement messages will be processed. A received message is considered unsolicited if the telephone 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. Valid values are: 0= Do not process received unsolicited Neighbor Advertisement messages. 1=Process received unsolicited Neighbor Advertisement messages if an entry already exists for the target address in the Neighbor Cache.
GUESTDURATION	2	Guest login duration in hours. One or two ASCII numeric digits. Valid values are "1" through "12".

Parameter Name	Default Value	Description and Value Range
GUESTLOGINSTAT	0	Guest login permission flag. If "1" the Guest Login option is listed on the Avaya Menu; if "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 CALLCTRS TAT =0, else 1	Headset operational mode. Specifies whether the telephone 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 telephone will go on-hook if a Disconnect message is received when the headset is active. 1 or 3 = Disconnect messages are ignored when the headset is active.
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 to 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 <i>myhttpdir</i> " where "myhttpdir" is your HTTP server path. HTTPDIR is the path for all HTTP operations except for BRURI.
HTTPPORT	80	TCP port number used for HTTP file downloading. 2 to 5 ASCII numeric digits. Valid values are "80" through "65535". Note that when the file server is on Communication Manager, set this value to "81" (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 telephone files. Dotted decimal or DNS format, separated by commas (0-255 ASCII characters, including commas).
ICMPDU	0	Controls whether ICMP Destination Unreachable messages will be processed. Values are: 0=No, 1=Send limited Port Unreachable messages,

Parameter Name	Default Value	Description and Value Range
		2=Send Protocol and Port Unreachable messages.
ICMPRED	0	Controls whether ICMP Redirect messages will be processed. Values are: 0=No, 1=Yes.
IDLEFEATURES	“ ” (Null)	A list of feature number identifiers for softkey features potentially available in the Idle call state, for example, Redial. Zero to 255 ASCII characters consisting of zero to six whole numbers separated by commas without any intervening spaces. For more information, see Administering features on softkeys on page 120.
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 supported. Valid values are: 0 = IPv6 is not supported. 1 = Support/enable IPv6.
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 used by IP deskphones. Set this parameter only when IP deskphones are to use a VLAN that is separate from the default data VLAN. If the VLAN identifier is to be configured via H.323 signaling based on Communication Manager administration forms, it should not be set here. As of 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.

Parameter Name	Default Value	Description and Value Range
		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”
LOGBACKUP	1	Indicates whether the user’s Call Log 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 (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 will be 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 should 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

Parameter Name	Default Value	Description and Value Range
		telephone, for example, Call forwarded calls. Values are: 1=Yes; 0=No. CM 5.2 or later is required for this feature to work.
MCIPADD	0.0.0.0	Call Server Address. Zero or more Avaya Communication Manager server IP Addresses. Format is dotted-decimal or DNS name format, separated by commas without intervening spaces (0-255 ASCII characters, including commas). Null is a valid value.
MSGNUM	“ ” (Null)	Voice mail system telephone/extension number. Specifies the number to be dialed automatically when the telephone 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 (0-9, * and #) 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. 0 to 255 ASCII characters, zero or one URL.
MYCERTWAIT	1	Specifies whether the telephone 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

Parameter Name	Default Value	Description and Value Range
		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.
NVHTTPSRRV	“ ” (Null)	Applies to both VPN and non-VPN settings. This is the HTTP file server IP addresses used to initialize HTTPSRRV 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. NVHTTPSRRV is provided for VPN mode so that a file server IP address can be pre configured and saved in non-volatile memory. See the <i>VPN Setup Guide for 9600 Series IP Telephones</i> (Document # 16-602968) for VPN use.
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.
NVTLSSRRV	“ ” (Null)	VPN and non-VPN. HTTPS file server IP addresses used to initialize TLSSRRV 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 VPN use, see the <i>VPN Setup Guide for 9600 Series IP Telephones</i> (Document # 16-602968).
OPSTAT	111	Options 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 <i>abc</i> , where each letter represents a 0 (disabled/off) or 1 (enabled/on), interpreted as: <i>a</i> = base settings for all user options and related applications,

Parameter Name	Default Value	Description and Value Range
		except as noted in <i>b</i> or <i>c</i> . <i>b</i> = setting for view-oriented applications (for example, the Network Information application), as applicable. <i>c</i> = setting for Logout application, if applicable. The binary "0" does not allow an end user to see or invoke options and related applications. The binary "1" allows 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.
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 telephone 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."
PHNEMERGNM	" " (Null)	Emergency telephone/extension number. Specifies the number to be dialed automatically when the telephone user presses the Emerg button. Value: 0-30 ASCII dialable characters (0-9, * and #) 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.

Parameter Name	Default Value	Description and Value Range
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 telephone number. The number of digits in the longest possible national telephone 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	Applies only to deskphones running software Release 6.0 and later. Phone Screen Consolidation flag. Consolidates call appearances and feature buttons into one scrollable list, with no separate views). 1 ASCII numeric digit as follows: 0= Do not consolidate call appearances and feature buttons into one scrollable list. 1= Consolidate call appearances and feature buttons into one scrollable list.
PHY1STAT	1	Ethernet line interface setting (1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex, and 6=1000Mbps 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 0-7 and correspond to the drop-down menu selection.
PHY2STAT	1	Secondary Ethernet interface setting (0=Secondary Ethernet interface off/disabled, 1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex), and 6=1000Mbps full-duplex if supported by the hardware).

Parameter Name	Default Value	Description and Value Range
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, it will not change regardless of settings from other sources. For more information, see About parameter data precedence on page 18.
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 telephone'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 telephone's unicast, multicast or anycast IPv6 addresses.
PROCPSWD	27238	Text string containing the local (dialpad) 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 Contacts 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 (dialpad) 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". For information on push messaging and administration, see the <i>Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Application Programmer Interface (API) Guide</i> (Document Number 16-600888).
PUSHPORT	80	TCP listening port number used for the telephone's HTTP server. 2 to 5 ASCII numeric digits, "80" through "65535".

Parameter Name	Default Value	Description and Value Range
QKLOGINSTAT	1	Quick login permission flag. Valid values are: 1= Quick login permitted; user must press the # key to see the previous Extension and Password. 0= Quick login not permitted; the user must explicitly enter the Extension and Password.
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 telephone 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 telephone during

Parameter Name	Default Value	Description and Value Range
		power-up or reset if it has not already been downloaded and installed. This parameter should only be set in an upgrade file.
RINGBKFEATURES	“ ” (Null)	A list of feature number identifiers for softkey features potentially available in the active (with far end ringback) call state. 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 120.
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.
SSH_ALLOWED	1	Secure Shell (SSH) Protocol permission flag. (0=SSH is not supported, 1= SSH is supported). “Supporting SSH” means the Avaya Services organization can have remote access to the telephone, using SSHv2, as described in topic Secure Shell Support.
SSH_BANNER_FILE	“ ” (Null)	Specifies the file name or URL for a custom SSH banner file. Zero to 255 ASCII characters: zero or one file name or URL. Used to provide a security warning message to the client before SSH authentication is attempted. If left at the default

Parameter Name	Default Value	Description and Value Range
		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, "0" 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, "0" through "32767".
SSH_LOGIN_DELAY	60	Specifies the number of seconds of delay between login attempts if 3 or more attempts fail. Valid values are 1 to 5 ASCII numeric digits, "0" through "32767".
SSH_USERNAME	"craft"	Specifies the user name to be used for SSH logins. Valid values are 0 to 255 ASCII characters.
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 telephone 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 as of Communication Manager Release 4.0, 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 as of Communication Manager Release 4.0, the SNMP community string can also be administered on the system-parameters IP-options form.
TIMERSTAT	0	TIMERSTAT specifies whether Timer On and Timer Off softkeys will be presented to the user.

Parameter Name	Default Value	Description and Value Range
		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” (port required for HTTPS downloads) rather than the using the default.
TLSSRVR	“ ” (Null)	IP Address(es) or DNS Name(s) of HTTPS file servers used to download telephone files. Dotted decimal or DNS format, separated by commas (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

*** Note:**

The table above 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 145.

Administering a VLAN

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

Related topics:

[About VLAN Tagging](#) on page 100

[The VLAN default value and priority tagging](#) on page 100

[Automatically detecting a VLAN](#) on page 101

[VLAN separation rules and related parameters](#) on page 102

About VLAN Tagging

IEEE 802.1Q tagging (VLAN) is a useful method of managing VoIP traffic in your LAN. Avaya recommends that you 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 set the telephones' VLAN, 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), the 9600 Series IP deskphones set the VLAN ID to L2QVLAN, and VLAN priority for packets from the telephone to L2QAUD for audio packets and L2QSIG for signalling packets. The default value (6) for these parameters is the recommended value for voice traffic in IEEE 802.1D.

Regardless of the tagging setting, a 9600 Series IP telephone will always transmit packets from the telephone at absolute priority over packets from the secondary Ethernet interface (i.e., 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 (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 understand 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.

Another parameter you can administer is VLANTEST. VLANTEST defines the number of seconds the 9600 IP Series Telephone waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is “60” seconds. Using VLANTEST ensures that the telephone 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 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, etc. to be returned to service. If the telephone restarts for any reason and the VLANTEST time limit expires, the telephone assumes the administered VLAN ID is invalid. The telephone then initiates operation with a VLAN ID of 0 or, if the value of L2Q is “0” (auto), tagging will be turned off until the L2QVLAN is set to a non-zero value, or until the telephone verifies that the network can support tagged frames..

Setting VLANTEST to “0” has the special meaning of telling the phone to use a non-zero VLAN indefinitely to attempt DHCP. In other words, the telephone does not return to the default VLAN.

Automatically detecting a VLAN

The deskphones support automatic detection of the condition where the L2QVLAN setting is incorrect. When the value of L2QVLAN is not 0 and VLAN tagging is enabled (L2Q= 0 or 1) initially the 9600 Series IP Telephone transmits DHCP messages with IEEE 802.1Q tagging and the VLAN ID is set to L2QVLAN. The telephones will continue to do this for VLANTEST seconds.

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

*** Note:**

Regardless of the setting of L2Q, VLANTEST, or L2QVLAN, you must have DHCP administered so that the telephone will get a response to a DHCPDISCOVER when it makes that request on the default (0) VLAN.

After VLANTEST expires, if an Avaya IP telephone running R1.2 receives a non-zero L2QVLAN value, the telephone will release the IP Address and send DHCPDISCOVER on that VLAN. Any other release will require a manual reset before the telephone will

attempt to use a VLAN on which VLANTEST has expired. See the Reset procedure in Chapter 3 of the *Avaya one-X® Deskphone H.323 Installation and Maintenance Guide*.

The telephone ignores any VLAN ID administered on the call server if a non-zero VLAN ID is administered either:

- by LLDP,
- manually,
- through DHCP, and/or
- in the settings file.

VLAN separation rules and related parameters

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

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

The table below provides several VLAN separation guidelines.

*** Note:**

The 9610 IP telephone does not support full VLAN separation because it has no secondary Ethernet interface and therefore never has PHY2VLAN and PHY2PRIO values.

Table 10: VLAN Separation Rules

If		Then
VLANSEP is "1" (On/Enabled)	AND the deskphone is tagging frames with a VLAN ID not equal to PHY2VLAN, AND the PHY2VLAN value is not zero.	Tagged Frames received on the secondary Ethernet interface: Tagged frames received on the secondary Ethernet interface are changed/not changed as follows: If a Gigabit Ethernet Adapter is not being used, tagged frames with a VLAN ID of zero (priority-tagged frames) will be changed before they are forwarded such that the VLAN ID of the forwarded frame is equal to the PHY2VLAN

If		Then
		<p>value and the priority value is equal to the PHY2PRIO value.</p> <p>If a Gigabit Ethernet Adapter is being used, tagged frames with a VLAN ID of zero will not be changed before they are forwarded.</p> <p>Untagged frames received on the secondary Ethernet interface are not changed before forwarding to the network.</p> <p>Tagged Frames received on the line interface:</p> <p>Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2VLAN.</p> <p>Tagged frames received on the Ethernet line interface will only be forwarded to the deskphone if the VLAN ID equals the VLAN ID used by the deskphone.</p> <p>Untagged frames are not changed will continue to be forwarded or not forwarded as determined by the Ethernet switch forwarding logic.</p> <p>Tagged frames with a VLAN ID of zero (priority-tagged frames) will be forwarded to the secondary Ethernet interface or to the deskphone as determined by the forwarding logic of the Ethernet switch, but the tag will still be removed from frames that egress from the secondary Ethernet interface.</p>
VLANSEP is "1" (On/Enabled)	<p>AND the deskphone is not tagging frames,</p> <p>OR if the deskphone is tagging frames with a VLAN ID equal to PHY2VLAN,</p> <p>OR if the PHY2VLAN value is zero.</p>	<p>Frames forwarded to the network from the secondary Ethernet interface will not be changed before forwarding. Tagging is not added or removed and the VLAN ID and priority does not change for frames received on the secondary interface. Tags are still removed for frames that egress from the secondary interface. The Ethernet switch forwarding logic determines whether frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the deskphone without regard to specific VLAN IDs or the existence of tags.</p>
VLANSEP is "0",	<p>OR the deskphone is not tagging frames,</p> <p>OR the deskphone is tagging frames with a VLAN ID equal to PHY2VLAN.</p>	<p>Frames forwarded to the network from the secondary Ethernet interface will not be changed before forwarding. Tagging is not added or removed and the VLAN ID and priority does not change for frames received on the secondary interface. Tags are still removed for frames that egress from the secondary interface.</p>

If		Then
		<p>The Ethernet switch forwarding logic determines whether frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the deskphone without regard to specific VLAN IDs or the existence of tags.</p>
<p>***VLANSEP is "1" (On/Enabled)</p>		<p>All tagged frames received on the secondary Ethernet interface are changed before forwarding to make the VLAN ID equal to the PHY2VLAN value and the priority value equal to the PHY2PRIO value. Untagged frames received on the secondary Ethernet interface are not changed before forwarding. If a Gigabit Ethernet Adapter is not being used, tagged frames with a VLAN ID of zero (priority-tagged frames) will be changed before they are forwarded such that the VLAN ID of the forwarded frame is equal to the PHY2VLAN value and the priority value is equal to the PHY2PRIO value. If a Gigabit Ethernet Adapter is being used, tagged frames with a VLAN ID of zero will not be changed before they are forwarded.</p>
<p>VLANSEP is "1" (On/Enabled)</p>	<p>AND the telephone is not tagging frames, OR if the telephone is tagging frames with a VLAN ID equal to PHY2VLAN, OR if the PHY2VLAN value is zero.</p>	<p>The Ethernet switch forwarding logic determines that frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the telephone without regard to specific VLAN IDs or the existence of tags. Frames received on the secondary Ethernet interface will not be changed before forwarding. In other words, tagging is not added or removed, and the VLAN ID and priority of tagged frames is not changed.</p>
<p>VLANSEP is "1" (On/Enabled)</p>	<p>AND the telephone is tagging frames with a VLAN ID not equal to PHY2VLAN, AND the PHY2VLAN value is not zero.</p>	<p>Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2VLAN. Tagged frames received on the Ethernet line interface will only be forwarded to the telephone if the VLAN ID equals the VLAN ID used by the telephone. Untagged frames will continue to be forwarded or not forwarded as determined by the Ethernet switch forwarding logic. Tagged frames with a VLAN ID of zero (priority-tagged frames) will either be: - forwarded to the secondary Ethernet interface or the telephone</p>

If		Then
		as determined by the forwarding logic of the Ethernet switch (preferred), or - dropped.

About DNS addressing

The 9600 IP deskphones support DNS addresses, dotted decimal addresses, and as of Release 6.0, colon-hex addresses. The telephone attempts to resolve a non-ASCII-encoded dotted decimal IP Address by checking the contents of DHCP Option 6. See [DHCP Generic Setup](#) on page 61 for information. 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 address(es) in Option 6 before the telephone attempts DNS address resolution. If Option 6 contains a list of DNS addresses, those addresses are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS by DHCP, you can specify the DNS server and/or Domain name in the HTTP script file. But first SET the DNSSRV and DOMAIN values so you can use those names later in the script.

*** Note:**

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

About IEEE 802.1X

9600 Series IP deskphones support the IEEE 802.1X standard for Supplicant operation, and support pass-through of 802.1X messages to an attached PC; one exception is the 9610, which does not have a secondary Ethernet interface. The system parameter DOT1X determines how the telephones handle pass-through of 802.1X multicast packets and proxy logoff, as follows:

- When DOT1X = 0, the telephone forwards 802.1X multicast packets from the Authenticator to the PC attached to the telephone and forwards multicast packets from the attached PC to the Authenticator (multicast pass-through). Proxy Logoff is not supported. This is the default value.
- When DOT1X = 1, the telephone 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 telephone 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 telephone forwards multicast packets from the Authenticator only to the telephone, ignoring multicast packets from the attached PC (no multicast pass-through). Proxy Logoff is not supported.
- Regardless of the DOT1X setting, the telephone always properly directs unicast packets from the Authenticator to the telephone or its attached PC, as dictated by the destination MAC address in the packet.

All 96xx telephones 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, Supplicant operation is not supported.

IP telephones will respond to unicast 802.1X frames (frames with the telephone's MAC address as the destination MAC address, and a protocol type of 88-8E hex) received on the Ethernet line interface if the value of DOT1XSTAT is "1" or "2", but will only respond to 802.1X frames that have the PAE group multicast address as the destination MAC address 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.

As of software Release 2.0, the system parameter DOT1XSTAT determines how the telephone handles Supplicants as follows:

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

*** Note:**

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

Related topics:

[802.1X Supplicant Operation](#) on page 106

802.1X Supplicant Operation

9600 IP deskphones 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 as specified in IETF RFC 3748. As of Release 6.2, telephones also support EAP-TLS as specified in IETF RFC 2716.

! Important:

EAP-TLS operation requires an identity certificate that is stored in the telephone and requires that the value of DOT1XEAPS is administered in the 46xxsettings file as "TLS". In addition, all other requirements for TLS and digital certificates apply for EAP-TLS.

A Supplicant identity (ID) and password of no more than 12 numeric characters are stored in reprogrammable non-volatile memory. The ID and password are not overwritten by telephone software downloads. The default ID is the MAC address of the telephone, converted to ASCII format without colon separators, and the default password is null. Both the ID and password are set to defaults at manufacture. EAP-Response/Identity frames use the ID in the Type-Data field. EAP-Response/MD5-Challenge frames use the password to compute the digest for the Value field, leaving the Name field blank.

When a telephone is installed for the first time and 802.1x is in effect, the dynamic address process prompts the installer to enter the Supplicant identity and password. The IP telephone does not accept null value passwords. See "Dynamic Addressing Process" in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*. The IP telephone stores 802.1X credentials when successful authentication is achieved. Post-installation authentication attempts occur using the stored 802.1X credentials, without prompting the user for ID and password entry.

An IP telephone can support several different 802.1X authentication scenarios, depending on the capabilities of the Ethernet data switch to which it is connected. Some switches may authenticate only a single device per switch port. This is known as single-supplicant or port-based operation. These switches typically send multicast 802.1X packets to authenticating devices.

These switches support the following three scenarios:

- Standalone telephone (Telephone Only Authenticates) - When the IP telephone is configured for Supplicant Mode (DOT1XSTAT=2), the telephone can support authentication from the switch.
- Telephone with attached PC (Telephone Only Authenticates) - When the IP telephone is configured for Supplicant Mode (DOT1X=2 and DOT1XSTAT=2), the telephone can support authentication from the switch. The attached PC in this scenario gains access to the network without being authenticated.
- Telephone with attached PC (PC Only Authenticates) - When the IP telephone 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 telephone in this scenario gains access to the network without being authenticated.

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

- Standalone telephone (Telephone Only Authenticates) - When the IP telephone is configured for Supplicant Mode (DOT1XSTAT=2), the telephone can support

authentication from the switch. When DOT1X is “0” or “1” the telephone is unable to authenticate with the switch.

- Telephone and PC Dual Authentication - Both the IP telephone and the connected PC can support 802.1X authentication from the switch. The IP telephone may be configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1 and DOT1XSTAT=1 or 2). The attached PC must be running 802.1X supplicant software.

About Link Layer Discovery Protocol (LLDP)

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

*** Note:**

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

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

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

These telephones:

- do not support LLDP on the secondary Ethernet interface.
- will 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.

A 9600 Series IP telephone initiates LLDP after receiving an LLDPDU message from an appropriate system. Once initiated, the telephones send an LLDPDU every 30 seconds with the following contents:

Table 11: LLDPDU Transmitted by the 9600 Series IP Deskphones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPv4 IP Address of telephone.
Basic Mandatory	Port ID	MAC address of the telephone.
Basic Mandatory	Time-To-Live	120 seconds.

Category	TLV Name (Type)	TLV Info String (Value)
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.
Basic Optional	System Capabilities	Bit 2 (Bridge) will be set in the System Capabilities if the telephone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled. Bit 5 (Telephone) will be set in the System Capabilities. If Bit 5 is set in the Enabled Capabilities then the telephone is registered.
Basic Optional	Management Address	Mgmt IPv4 IP Address of telephone. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the telephone.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports autonegotiation status and speed of the uplink port on the telephone.
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 telephone is not currently powered via PoE, else the maximum power usage of the telephone plus all modules and adjuncts powered by the telephone 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 deskphones running Software Release 6.0 or later, Firmware Revision = RFSINUSE.
TIA LLDP MED	Inventory – Software Revision	APPNAME, or for deskphones running Software Release 6.0 or later, Software Revision = APPINUSE.
TIA LLDP MED	Inventory – Serial Number	Telephone serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final D xxx characters removed.

Category	TLV Name (Type)	TLV Info String (Value)
Avaya Proprietary	PoE Conservation Level Support	Provides Power Conservation abilities/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 CNASVR. Subtype = 5. This parameter is not supported in Release 6.2 and later.
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 deskphones will act on the TLV elements described in [the table](#) on page 110:

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: <ul style="list-style-type: none"> • The telephone is not registered with the Call Server. • Name begins with VOICE (case does not matter). • The VLAN is not zero. • DHCP Client is activated. • The telephone is registered but is not tagging layer 2 frames with a non-zero VLAN ID. If VLAN Name causes the telephone to change VLAN and the telephone already has an IP

System Parameter Name	TLV Name	Impact
		Address the telephone will release the IP Address and reset. If the TLV VLAN ID matches the VLAN ID the telephone is using, the VLAN ID is marked as set by LLDP. Otherwise, if already registered, the telephone 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 telephone 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. A check is made as to 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: <ul style="list-style-type: none"> • 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 telephones that support this will turn on/off the telephone backlight and the backlight of an attached Button Module in response to this TLV. Exception: the 9670G display backlight is put into low-power mode rather than being turned off.

System Parameter Name	TLV Name	Impact
	Extended Power-Via-MDI	Power conservation mode will be enabled if the received binary Power Source value is 10, and power conservation mode will be disabled if the received binary Power Source value is not 10. Power conservation mode is enabled even if the telephone is not powered over Ethernet because the telephone sends information about the power source that it is using in a TIA LLDP MED Extended Power-Via-MDI TLV; it is assumed that the power management system intends to conserve local power as well.

Administering settings at the deskphone

The *Avaya one-X® Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide* details how to use Craft local procedures at the telephone for administration. The local procedures you might use most often as an administrator are:

- CLEAR - Remove all administered values, user-specified data, option settings, etc. and return a telephone to its initial “out of the box” default values.
- DEBUG - Enable or disable debug mode for the button module serial port.
- GROUP - Set the group identifier on a per-phone basis.
- INT - Set or change the interface control value(s) of PHY1STAT and/or PHY2STAT.
- RESET - Reset the telephone to default values including any values administered through local procedures, and values previously downloaded using DHCP or a settings file.
- RESTART - Restart the telephone in response to an error condition, including the option to reset parameter values.
- VIEW - Review the 9600 IP telephone system parameters to verify current values and file versions.

Administering display language options

9600 Series IP deskphones are factory-set to display information in the English language. All software downloads include language files for 13 additional languages. Software Release 1.2 added support for a large font version of English only and Release 1.5 added Arabic to the language file download. Administrators can specify from one to four languages per telephone

to replace English. End users can then select which of those languages they want their telephone to display.

All downloadable language files contain all the information needed for the telephone to present the language as part of the user interface. For touchscreen deskphones, this includes an indication of the character to be used as a decimal “point” in numeric values and an indication of the character, if any, to be used as a separator (thousands, millions, etc.) in numeric values (no character or a space character must be usable as well as punctuation characters).

There are no dependencies between the languages available from the software download and the actual character input method. If a character input method is not supported, ASCII is used instead. Acceptable input methods are as follows:

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

Use the configuration file and these 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 four languages you are specifying. For example, to indicate German and French are the available languages, the setting is:
LANG1FILE=mlf_german.txt and **LANG2FILE=mlf_french.txt**.
- **LANG0STAT** - Allows the user to select the built-in English language when other languages are downloaded. If LANG0STAT is “0” and at least one language is downloaded, the user cannot select the built-in English language. If LANG0STAT is “1” the user can select the built-in English language text strings.
- **LANGSYS** - The file name of the system default language file, if any.
- **LANGLARGEFONT**- The name of the language file you want available for a “large font” display, currently only “English.”

As of Release 1.2, a large text font is available for user selection on all 9600 Series IP Telephones but the 9610. The larger text font can only be activated if a language file for this

font is available. The Text Size option is presented to the telephone user if and only if the parameter LANGLARGEFONT is not null and if a language file for that value is being used as the current user interface language. If neither condition is met, the Text Size option is not presented to the user.

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

For more information, see [9600 Series H.323 Customizable System Parameters](#) on page 78. To view multiple language strings, see the MLS local procedure in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*. To download a language file or review pertinent information, go to <http://support.avaya.com/unicode>

*** Note:**

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

Administering voice-initiated dialing

As of software Release 2.0, all 9600 Series IP deskphones with a speakerphone microphone (all except the 9610) are capable of voice-initiated dialing.

*** Note:**

Telephones introduced in software Release 6.0 (9608, 9611G, 9621G, and 9641G) do not support the voice dialing feature.

The telephone software distribution packages include a voice language file for each of the supported languages. Administer the system parameter VOXFILES to identify the voice language file(s) you want available to your end users. All downloadable VOX language files contain data files that allow the telephone to perform the following tasks for the associated language:

- Accept a user's verbal input of keywords and Names.
- Search the local Contacts list of Names.
- Return zero, one, or more prospective matching Contacts entries.

Each voice language file has a file name beginning with three characters that indicate the language supported and ending with “.tar”. The available languages and corresponding three-character filename designations are as follows:

Language	Initial Characters of the Filename
----------	------------------------------------

Brazilian Portuguese	PTB
European Spanish	SPE
Dutch	DUN
German	GED
Italian	ITI
Parisian French	FRF
U.K. English	ENG
U.S. English	ENU

Two voice-initiated dialing settings are available to end users by the Avaya Menu -> Call Settings option. They are Voice Dialing and Voice Dialing Language, which allow the end user to enable/disable voice-initiated dialing and select one of the voice languages you administered using the VOXFILES parameter for voice dialing, respectively. The user guide for each applicable telephone model describes the voice-initiated dialing user interface.

About the gigabit Ethernet (GigE) adapter

As of Release 1.1, 9600 Series IP telephones can accommodate a Gigabit Ethernet (GigE) Adapter. Release 1.5 introduced the 9630G and 9640G IP Telephones, which contain a built-in gigabit Ethernet adapter. Release 2.0 introduced the 9670G IP Telephone, which also contains a built-in gigabit Ethernet adapter. Release 6.0 introduced the 9611G, 9621G, and 9641G IP Deskphones which contain built-in GigE adapters. When connected to an adapter interface, the Gigabit Ethernet Adapter sets the Ethernet line interface operational mode that is built into the telephone to 1000Mbps full-duplex and deactivates the built-in secondary Ethernet interface. When a Gigabit Ethernet Adapter is present, any considerations or processing that apply to the “Ethernet line interface” apply only to the Ethernet line interface on that adapter. Likewise, any considerations or processing that apply to the “secondary Ethernet interface” apply only to the secondary Ethernet interface on the Gigabit Ethernet Adapter.

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

Administering dialing methods

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

Related topics:

[About log digit \(Smart Enbloc\) dialing](#) on page 116

[Using enhanced local dialing](#) on page 116

[Enhanced local dialing requirements](#) on page 118

About log digit (Smart Enbloc) dialing

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

Using enhanced local dialing

For servers running a CM release earlier than 4.0, the 9600 Series IP deskphones evaluate a stored telephone number (other than those in the Contacts list) based on parameters administered in the settings file. The telephone can then automatically prepend the correct digits, saving the user time and effort. This is Enhanced Local Dialing. The key to the success of this feature is accurate administration of several important values, described in [9600 Series H.323 Customizable System Parameters](#) on page 78 and summarized below.

The parameters relevant to the Enhanced Dialing Feature are:

- ENHDIALSTAT - Enhanced dialing status. If set to “1” (the default) the enhanced local dialing feature is turned on. If set to “0” enhanced local dialing is off. However, when in

effect, [Using log digit \(Smart Enbloc\) dialing](#) on page 116 takes precedence, regardless of the ENHDIALSTAT setting.

- PHNCC - the international country code of the call server's location. This value is used in conjunction with the PHNIC value to help identify when a call to be dialed might be an international number. For example, set PHNCC to "1" when the call server is in the United States, to "44" for the United Kingdom, and so on.
- PHNDPLENGTH - the length of internal extension numbers. Used to help the telephone identify whether the number to be called is an outside number (which requires combining with PHNOL to get an outside line) or an internal line. As long as PHNDPLENGTH is less than the length of a national number (PHNLDLENGTH), the telephone can determine the difference between the two types of numbers. However, the telephone cannot determine the type of number when the extension is at least as long as the national telephone number
- PHNIC - the maximum number of digits, if any, dialed to access public network international trunks. This value is used in conjunction with the PHNCC value to help identify when a call to be dialed might be an international number. The country code is inserted if the number to be dialed includes a plus sign (+) followed by a country code other than the one identified in PHNCC. However, the plus sign is almost never presented in calling or called party number data and usually only in Web-based click-to-dial links.
- PHNLD - the long distance access code; the digit dialed to access public network long distance trunks. If the number to be dialed is longer than the extension number length and equal in length to PHNLD, the telephone presumes it is a national number, and should be preceded by the long distance access code. For example, in the United States a 10 digit number includes the area code and must be preceded by a "1."
- PHNLDLENGTH - the maximum length, in digits, of the national telephone number for the country in which the call server is located. If the number to be dialed is longer than the extension number and is not equal to PHNLD, the number is presumed to be a subset of the national number and the long distance access code is not used.
- PHNOL - the character(s) dialed to access public network local trunks on the call server. If the number to be dialed is not an extension number, the telephone presumes it is an outside number which needs to be preceded by the code to access an outside line, commonly a "9".

 **Note:**

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

 **Important:**

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

States. If the call server is in London, PHNCC would be set to “44” even if the telephones it serves are in the United States.

*** Note:**

In all cases, the digits the telephones insert and dial are subject to standard Avaya server features and administration. This includes Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), and so on. As indicated in [9600 Series H.323 Customizable System Parameters](#) on page 78, you can administer the system parameter ENHDIALSTAT to turn off the Enhanced Local Dialing feature.

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

Example: A user notes a Web site contains an international telephone number that needs to be called and initiates the call. The telephone determines the number to be called is from another country code. The telephone then prepends the rest of the telephone number with PHNOL to get an outside line and PHNIC to get an international trunk. The telephone then dials normally, with the call server routing the call appropriately.

Enhanced local dialing requirements

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

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

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

*** Note:**

The Enhanced Local Dialing algorithm requires that telephone numbers be presented in a standard format. The standard format depends on how you administer the parameters indicated in [9600 Series H.323 Customizable System Parameters](#) on page 78. also described in [Using enhanced local dialing](#) on page 116. The algorithm also assumes that international telephone numbers are identified as such in, for example, WML Web sites. This is indicated by preceding that type of number with a plus (+) sign, and a space or some non-digit character following the country code.

About internal audio parameters

The parameter AUDIOENV provides control of some internal audio parameters. Avaya does not recommend that customers set these values. In certain situations, particularly noisy environments, Avaya SSE may recommend a change in the AUDIOENV setting to reduce/eliminate the effects environmental noise can have during telephone 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 is an index into a table that impacts four internal variables:

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.

Administering features on softkeys

As of software Release 2.0, you can administer call server features on softkeys in the Phone application. The number of features you can place on a set of softkeys depends on the call state the telephone 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 # 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:**

The system parameters are described in more detail in [9600 Series H.323 Customizable System Parameters](#) on page 78.

This capability works as follows:

- You administer feature buttons for the telephone on the call server as you normally would, and the call server sends these button assignments to the telephone as it always has.
- In the 46xxsettings file, you 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 122 lists the administrable features and their associated numbers.
- The telephone compares the list of features you administered on the call server with the list of features in the system parameters you administered. Assuming 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 telephone displays the feature buttons starting with Softkey 1 and continuing to the right in the order specified in the system parameter, subject to the considerations listed in this section.

Example:

Assume 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 122, three additional "features" can be specified on a softkey of your choice or can be completely replaced. 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 telephone. This means the corresponding softkey is labeled Redial if the telephone 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 pressed, this softkey turns the telephone's backlight off, saving energy. The backlight comes back 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.

Another consideration for IDLEFEATURES or DIALFEATURES is that 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 telephone itself 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 personalized labels are presented instead.

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:**

The system parameters allow you to specify more features than can be displayed on any one telephone. For example, IDLEFEATURES allows you to specify up to six features, although any one telephone can display at most four of them. The maximum size of each parameter allows you to specify one comprehensive list for that parameter’s related call state, but allows your user community to see different feature buttons depending on how you administer their telephones. Since the telephone only displays feature button labels for features administered on the call server, you can set the softkey feature system parameters to values that will 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. Since 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	AbbrvDial (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-requist	ANI Request	146
assist	Assist	90

Feature Name	Default Label	Feature Number
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-alm	CDR 1 Failure	106
cdr2-alm	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

Feature Name	Default Label	Feature Number
con-stat	Console Status	185
consult	Consult	42
cov-cback	Coverage Callback	17
cov-msg-rt	Cover Msg Retrieve	12
cpn-blk	CPN Block	164
cpn-unblk	CPN Unblock	165
crss-alert	Crisis Alert	247
cw-ringoff	CW Aud Off	62
date-time	Date Time	23
deact-tr-g	Cont Deact	47
delete-msg	Delete Message	14
dial-icom	Dial Icom	32
did-remove	DID Remove	276
did-view	DID View	256
directory	Directory	26
dir-pkup	Directory Pkup	230
disp-chrg	Display Charge	232
display	Display	180
disp-norm	Local/Normal	124
dn-dst	Do Not Disturb	99
dont-split	Don't Split	176
dtgs-stat	DTGS Status	181
ec500	Extension to Cellular	335
em-acc-att	Emerg Access to Attd	64
exclusion	Exclusion	41
ext-dn-dst	Do Not Disturb Ext.	95
extnd-call	Extend Call	345
fe-mute	Far End Mute for Conf	328
flash	Flash	110
forced-rel	Forced Release	57
goto-cover	Go To Cover	36

Feature Name	Default Label	Feature Number
group-disp	Group Display	212
group-sel	Group Select	213
grp-dn-dst	Do Not Disturb Grp	96
grp-page	GrpPg	135
headset	Headset	241
hundrd-sel	Group Select #	58
hunt-ne	Hunt Group	101
in-call-id	Coverage (Info)	30
in-ringoff	In Aud Off	60
inspect	Inspect Mode	21
int-aut-an	IntAutoAns	108
intrusion	Intrusion	179
last-mess	Last Message	182
last-numb	Last Number Dialed	66
last-op	Last Operation	183
lic-error	License Error	312
limit-call	LimitInCalls	302
link-alarm	Link Failure (#)	103
local-tgs	Local-tgs (#)	48
lsvn-halt	Login SVN	144
lwc-cancel	Cancel LWC	19
lwc-lock	Lock LWC	18
lwc-store	LWC	10
maid-stat	Maid Status	209
major-alm	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

Feature Name	Default Label	Feature Number
mf-op-intl	CO Attendant	229
mj/mn-alm	Maj/Min Hdwe Failure	82
mm-basic	MM Basic	169
mm-call	MM Call	167
mm-cfwd	MM CallFwd	244
mm-datacnf	MM Datacnf	168
mmi-cp-alm	MMI Circuit Pack Alarm	132
mm-multnbr	MM MultNbr	170
mm-pcaudio	MM PCAudio	166
msg-retr	Message Retrieve	11
mwn-act	Message Waiting Act.	97
mwn-deact	Message Waiting Deact.	98
next	Next	13
night-serv	Night Serv	53
noans-ahrt	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

Feature Name	Default Label	Feature Number
q-time	OQT	86
release	Attendant Release	50
release	Station Release	94
remote-tgs	Remote TG (#)	78
re-ringoff	Ringer Reminder	61
ringer-off	Ringer Cutoff	80
rs-alert	System Reset Alert	109
rsvn-halt	rsvn-halt	145
scroll	Scroll	125
send-calls	Send All Calls	35
send-term	Send All Calls-TEG	72
serial-cal	Serial Call	177
serv-obsrv	Service Observing	85
signal	Signal (name or ext.)	37
split	Split	56
split-swap	Split-swap	191
ssvn-halt	ssvn-halt	231
sta-lock	Station Lock	300
start	Start Call	55
stored-num	Stored Number	22
stroke-cnt	Stroke Count (#)	129
term-x-gr	Term Grp (name or ext.)	40
togle-swap	Conf/Trans Toggle-Swap	327
trk-ac-alm	FTC Alarm	121
trk-id	Trunk ID	63
trunk-name	Trunk Name	111
trunk-ns	Trunk Group	102
usr-addbsy	Add Busy Indicator	239
usr-rembsy	Remove busy Indicator	240
uui-info	UUI-Info	228
vc-cp-alm	VC Circuit Pack Alarm	133

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

Administering a custom screen saver

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

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

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

To determine what image to display, the telephone follows this procedure:

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

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

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

The best way to use the SCREENSAVER parameter is to administer different file names in the 46xxsettings file, listed under different MODEL4 values (9620, 9630, etc.). In other words, using the MODEL4 IF statements, you can administrator a given telephone to point to a unique SCREENSAVER value that is appropriate for that telephone.

About administering audio equalization

The Federal Communication Commission (a branch of the US Government) in its Part 68 standard, requires support for Hearing Aid Compatibility (HAC). This 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.

As of Release 6.2, 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 telephone 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 Avaya one-X® Deskphone H.323 Installation and Maintenance Guide for 9608, 9611G, 9621G, and 9641G Deskphones) provides a “backdoor” to allow the telephone to be administered with the desired audio equalization value. “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” (which uses the settings file value unless superseded by Local Procedure), “Audio Opt.” which uses Handset equalization that is optimized for acoustic TIA 810/920 .performance, or “HAC Opt.” which uses Handset equalization that is optimized for electrical FCC Part 68 HAC telecoil performance.
- Handset equalization options are effected in the following order:
 - a. The telephone will use the User Option value if one was selected and saved.

- b. Otherwise, if a Local Procedure value was selected and saved, the telephone will use the local Procedure value.
- c. Otherwise, if a Settings file value is specified and saved the telephone will use that value.
- d. If none of the above options have been set, the telephone will use 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. First perform the appropriate call center administration on the call server. There are several modes by which you can administer the Agent sign-in. However, each mode has certain implications for the end user. For more information, see [Administering agent sign ins for call centers](#) on page 131.

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 - Give an agent permission to record/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 - Used to determine the proper Agent Information message regarding an incoming call.
- AGTTRANSLCLBK - Used to determine the proper Agent Information message regarding an incoming call.
- AGTTRANSLPRI - Used to determine the proper Agent Information message regarding an incoming call.
- AGTTRANSLPK - Used to determine the proper Agent Information message regarding an incoming call.

- AGTTRANSLICOM - Used to determine 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

See [9600 Series H.323 Customizable System Parameters](#) on page 78 in Chapter 7 for details about each new parameter:

In addition to agent call center documentation available for your Call Center, the 9608, 9611G, 9621G and 9641G H.323 Call Center User Guide (Document Number 16-603613) describes using these deskphones with software Release 6.2 functionality.

Related topics:

[Administering agent sign ins for call centers](#) on page 131

[Call Center backup files](#) on page 132

[Administering the Vu display button](#) on page 133

Administering agent sign ins for call centers

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

- Administer a FAC — Administer a Feature Access Code (FAC), for example, FAC #94. The deskphone requires an Agent ID to create and store Greetings on the http server. Thus, entering the Agent ID using a FAC is the most reliable method where the deskphone can display the Agent ID on the Top line and allow agent's station to retrieve stored Greetings or create and backup their own Greetings. After administering the FAC on the call server, set the parameter AGTLOGINFAC in the 46xxsettings file to indicate which Feature Access Code you want agents to use to sign in to the call center.
- Administer a Feature button — Administer a Feature button labeled “Sign in”, or “Agent ID,” or another descriptive label that indicates entry of the Agent ID is required. This method might prevent the deskphone from displaying the Agent ID on the Top line and more importantly, it might also prevent the agent from retrieving or backing up Greeting files that are store on the server.
- Configure a Vu display button— For Remote login or CTI login, to utilize the agent greeting functions, administer a FAC for Feature Button Agent login or a CTI login. For more information, see [Administering the Vu display button](#) on page 133.

For more information on administering Feature buttons, see [Administering features and CAs for all other IP deskphones](#) on page 51.

- Administer a Softkey — Administer a softkey with a descriptive label that indicates Agent ID entry is required. See [Administering features on softkeys](#) on page 120 for more information.

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

The *9608/9611G and 9621G/9641G H.323 Call Center User Guide* (Document Number 16-603613) describes Agent sign in using a FAC but cautions users that their supervisor may instruct them to use an alternate sign in procedure.

Call Center backup files

The BRURI parameter is used to backup and retrieve generic user data, as explained in the next section, but can also be used to back and retrieve specific call center data. If all the following conditions are true, then whenever an agent logs in to the call center, the telephone will automatically attempt to retrieve a file labeled agentID_CCdata.txt with agentID being the agent's Agent ID. Note that this file is based not on the user extension, like the generic backup file, but on the Agent ID:

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

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

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

- agentID_CCdata.txt. This file contains data about each greeting. Specifically, for each greeting, it contains:
 - GREETINGLBLx is set to the Label specified by the agent for the x'th greeting
 - GREETINGFILEx is set to "agentID_x.wav" (with agentID and x as applicable)
 - GREETINGDURx is set to the Duration of the recorded greeting
 - GREETINGTYPEx is set to the numerical value of the selected type and match criterion. This is a numerical code used by telephone software to track the Type and Match Criterion for the greeting.

- GREETINGDATAx is set to the string that invokes this greeting (which may be non-numeric), if applicable for the greeting Type.
- GREETINGCHKSUMx is set to the checksum of the associated .wav file.
- agentID_x.wav where x is the x'th greeting for the specific agent.

Administering the Vu display button

Sometimes, even though the relevant procedures are carried out, it might be that the telephone cannot derive the agent's Agent ID. This typically happens when the agent must also provide a password when logging into the call center, and the telephone is unable to distinguish the ID from the password. In this environment, the AGTIDVUSTAT parameter should be considered.

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

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

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

Procedure

1. In CM, create a unique vustats-display-format.
(Example: change vustats-display-format "x" where x is an available Vu-stats format number)
2. In the change vustats-display-format form the following fields need to be configured exactly as follows:
 - Next format number: None
 - Data Field: \$
 - Number of Intervals: Leave Blank
 - Object Type: agent
 - Update Interval: no-update
 - On Change? N
 - Display Interval: 5
 - Format Discription: ID: \$\$\$\$\$\$\$\$\$\$\$\$ \$\$\$\$\$\$\$\$ \$

- Data Type:
 - i. agent-extension— Format: Leave Blank— Period: Leave Blank— Threshold: Leave Blank— RC: Leave Blank— Ref: Leave Blank
 - ii. agent-state— Format: Leave Blank— Period: Leave Blank— Threshold: Leave Blank— RC: Leave Blank— Ref: Top
 - iii. current-reason-code— Format: Leave Blank— Period: Leave Blank— Threshold: Leave Blank— RC: Leave Blank— Ref: Leave Blank
 - 3. Save the Entries made.
 - 4. Add a vu-display button with the format “x” previously created to each station that it going to utilize any type of agent login other than FAC login.
The button can be administered on any available button position on the phone.
 - 5. Go to the 46xxxsettings file on the server and add or change to: SET AGTGREETINGSTAT “x”.
 - 6. Save the 46xxxsettings file.
 - 7. Reboot the phone so the changes made on the settings file are applied to the phone.
-

Administering backup/restore

*** Note:**

This section does not apply to the 9610 IP telephone. For 9610 backup/restore information, see [Special Administration for the 9610 IP Telephone](#) on page 147.

The 9600 Series IP deskphones support the HTTP client to back up and restore the user-specific data indicated in [User data saved during backup](#). As of Software Release 1.5, HTTP over TLS (HTTPS) is also supported for backup/restore. For backup, the telephone 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 forward slash), the file name is appended.

- Otherwise, a forward slash is appended to the BRURI value, then the file name is appended to that.

*** Note:**

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

If TLS is used, the telephone's call server registration password can 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 telephone requesting the file transaction can be authenticated.

If no digital certificates have been downloaded based on the system parameter TRUSTCERTS, the telephone establishes a TLS connection only to a backup/restore file server that has a Avaya-signed certificate (which is included by default with the Avaya IP Telephone File Server Application), and the credentials are always included. 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 a non-Avaya certificate is used by the server on which the Avaya IP Telephone File Server Application is installed, set BRAUTH to "1" to enable authentication of the telephones. The default value of BRAUTH is "0".

When the call server IP address and the telephone's registration password 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 telephone's registration password.

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 telephone 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 telephone. 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 telephone's call server registration password is included as the credentials in an Authorization request-header for each transmitted PUT (backup) and GET (for restore) method.

New value(s) 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 telephone.

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 detailed in the user guide for their specific telephone model. For specific error messages

relating to Backup/Restore, see the *Avaya one-X® Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

Related topics:

[Backup file formats](#) on page 136

[User data saved during backup](#) on page 137

[About restore](#) on page 139

Backup file formats

When the system parameter BRURI is non-null, user changes are automatically backed up to the file `ext_96xxdata.txt` (where `ext` is the extension number of the deskphone) on the HTTP server to a user-specified directory. Backup formats are as follows:

Table 15: Backup File Formats

Item/Data Value	Format
Generic	<code>name=value</code>
Contacts	<code>ABKNAMEmmm=ENTRY_NAME</code> <code>ABKNUMBERmmm=ENTRY_NUMBER_1</code> <code>ABKTYPEmmm=ENTRYT_TYPE</code> (where <code>mmm</code> is the one-, two-, or three-digit entry ID, with leading zeros for single and double-digit entry IDs)
Call Log entries	<code>CLNAMEmmm=ENTRY_NAME</code> <code>CLNUMBERmmm=ENTRY_NUMBER</code> <code>CLTYPEmmm=ENTRY_TYPE</code> <code>CLDATEmmm=ENTRY_DATE</code> <code>CLTIMEmmm=ENTRY_TIME</code> <code>CLDURATIONmmm=ENTRY_DURATION</code> <code>CLBRIDGEDFLAGmmm=ENTRY_BRIDGEDFLAG</code> <code>CLMISSEDCNTRmmm=ENTRY_COUNTER</code> <code>CLBCALBLmmm=ENTRY_BCALBL</code> 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 <code>mm</code> (the one- or two-digit button number of the entry with a lead zero for single-digit numbers)	<code>PHNLABELmm=CAUSERLABEL</code>
User-generated telephone Feature Button labels with button identifiers of <code>mm</code> (the one- or two-digit button	<code>PHNLABELmm=FBUSERLABEL</code>

Item/Data Value	Format
number of the entry with a lead zero for single-digit numbers)	
User-generated SBM24 Call Appearance or Feature Button labels with button identifiers of <i>mm</i> (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 16: Options and Non-Password Parameters Saved During Backup

Parameter Name	Setting
HOMEFAV nn	Contact Favorites data; 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: 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	Audible Headset Alerting
USER_HSEQUAL	User-specified handset audio equalization standard
LANGUSER	Display Language
LOGACTIVE	Call Log Active
LOGBRIDGED	Log Bridged Calls

Parameter Name	Setting
LOGTDFORMAT	Call Log Data Time/Date Format
OPTAGCHAND	Handset Automatic Gain Control
OPTAGCHEAD	Headset Automatic Gain Control
OPTAGCSPKR	Speaker Automatic Gain Control
OPTAUDIOPATH	Audio Path
OPTCLICKS	Button Clicks
OPTERRORTONE	Error Tones
OPTGUESTLOGIN	Guest Login Permitted/Not Permitted
OPTHOMEIDLE	Home Screen on idle; 9670G only
OPTTEXTSIZE	Text Size
PERSONALRING	Personalized Ring Note for the 9670G only: this value is backed up as equal to the PERSONALWAV value when PERSONALWAV is set to one of the 8 standard ring patterns. When PERSONALWAV is greater than 8 (meaning it is set to one of the newer ring patterns) and PERSONALRING was set using a backup file value, that backup value is re-saved. If neither of these conditions apply, no PERSONALRING value is backed up.
PERSONALWAV	Personalized Ring value - 9670G only
PHNABKNAME	Contacts Pairing
PHNEDITDIAL	Edit Dialling
PHNQUICKPANEL	Quick Touch Panel; 9670G only
PHNREDIAL	Redial
PHNSCRONANS	Go to Phone Screen on Answer
PHNSCRONCALL	Go to Phone Screen on Calling
PHNSCRONALERT	Go to Phone Screen on Ringing
PHNTIMERS	Call Timer
PHNVBDIALSTAT	Voice Initiated Dialing
PHNVBDIALLANG	Voice Initiated Dialing Language
PHNVISUALALERT	Visual Alerting
PRINGMENU	Personalized Ring Menu
VIDHELP	Voice Initiated Dialing Help Counter

Parameter Name	Setting
WEATHERLOCID	Weather Location ID; 9670G only
WEATHERUNITS	English/Metric; 9670G only
WORLD CLOCKLIST	List of World Clock location entries; 9670G only

About restore

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

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

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

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

* Note:

If you administered the APPSTAT parameter to suppress changes to one or more applications, the telephone backs up and restores data as usual, but ignores data for “suppressed” applications. This prevents a user from bypassing your APPSTAT restrictions by editing the backup file. For information about APPSTAT, see [Setting the Application Status flag \(APPSTAT\)](#) on page 146.

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

Data retrieval considerations are as follows:

- When you create a backup file rather than edit an existing one, be sure 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 136.
- All identifiers, for example, *names*, are interpreted in a case-insensitive manner, but the case of parameter values, Contact names, and numbers is preserved.
- 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. Likewise, 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 telephone, the data is retained for possible use later, and is considered 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 telephone, 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 telephone to obtain the backup file and successfully restore valid data.

Administering backup/restore for a 9610

The 9610 uses its backup/restore functionality differently than other 9600 Series IP Telephones. There is no user-created data nor are there options that need to be stored in a 9610 backup file. The 9610 uses its backup file as the source for administration of the button labels and associated telephone numbers in the Contacts application, the Main Menu list, and associated data, etc.

The administrator is expected to build the backup file in accordance with the requirements in this section, so that when the 9610 boots up and registers, it will obtain the appropriate data for user presentation.

Differences with the backup/restore procedures used on the other 9600 Series IP Telephones include:

- The 9610 never “backs up” data, it only retrieves data. Since the user has no mechanism to change any data, there is no need to back up changes. For consistent terminology with other 9600 Series IP Telephones, we use the term “backup file” here for the 9610 file.
- Because the user can never change data, the OPSTAT value is ignored for the purposes of populating the display from the 9610 backup file.
- When the 9610 attempts to retrieve the backup file, the telephone first attempts to retrieve a file labeled ext_9610data.txt. If the 9610 does not retrieve this file successfully, unlike the other 96xx sets, the 9610 attempts to retrieve a file labeled 9610data.txt. This file does not have an extension designation. This retrieval process has the advantage of allowing

all 9610s that are not associated with a specific extension's backup file to share a common backup file. You can have, for example, three unique 9610 backup files - one for a 9610 in the Marketing conference room, one for a 9610 in the Accounting conference room, and one for five 9610 IP Telephones in public areas of the company.

Related topics:

[About the 9610 retrieval process](#) on page 141

[General 9610 restore processing](#) on page 142

About the 9610 retrieval process

When the telephone initiates an automatic retrieval, the telephone first attempts to retrieve a file with filename `ext_9610data.txt`, where `ext` is the extension number of the telephone.

While in progress, the Top Line displays

Retrieval 1

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

File obtained

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

Restore OK

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

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

Retrieval 2

If the file is retrieved successfully the remaining steps are identical to those for the `ext_9610data.txt` file.

If:

- this second retrieval attempt fails for any reason, or
- the file is successfully retrieved but has no valid data, or
- either successfully-retrieved file was not successfully stored, then

the Top Line displays

Restore failed

for 30 seconds, or until the user selects another Application Line or application, whichever comes first. Once the data storage starts and until the

Restore OK

or

Restore failed

message displays, the user cannot perform any action to display another screen, for example, the Avaya Menu button is temporarily locked out and any press of it is ignored. Once the

appropriate result message is displayed, the corresponding 9610 user interface is presented.

General 9610 restore processing

Characters are assumed to be coded in UTF-16 LE (little-endian, with Byte Order Mark (BOM) for LE (0xFFFE)), with each item on a separate line terminated by" <CR><LF>" (000D 000A in UTF-16) characters.

Important:

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

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

The format for retrieving a Main Menu entry is:

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

For more information, see [Administering a 9610 Main Menu \(MM\)](#) on page 170.

The format for retrieving a Contacts entry is:

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

For more information, see [Administering the 9610 Contacts Application](#) on page 171.

The other parameters that have meaning in a 9610 backup file are:

IDLEAPP- as described in [Administering the 9610 idle application, screensaver, and WML links](#) on page 172.

LISTAPP - when LISTAPP is null (the default), the assumption is the administrator has not created an external equivalent to the local Contacts application. The local Contacts application is used unless it too is empty. When the local Contacts application is empty, selecting **List** is the same as pressing the **Start** button. When LISTAPP is non-null, the assumption is the administrator has populated it with a URI for a WML-based application to be displayed when **List** is selected.

When retrieving data, the following applies:

- If the Byte Order Mark (BOM) is not 0xFFFE, the entire file is rejected and the retrieval fails.
- All identifiers, for example, names, are interpreted in a case-insensitive manner.
- The case of parameter values and Contacts names and numbers are preserved.
- Spaces preceding, within, or following a *name* or *value* are treated as part of that entity.
- <CR> and <LF> are interpreted as line termination characters.
- Blank lines are ignored.

- If an identifier is not recognized or is invalid, the entire line is ignored.
- If an identifier is valid but the data itself is invalid or incomplete, the line is ignored. The determination of what constitutes a valid value for each data element is specified in [General 9610 Restore Processing](#) and [9610 Backup File Format](#) on page 169.
- If more than one line contains a value for a parameter or Contacts entry, the last value read is used (hence, new values overwrite previous values as lines are read from the file). In all other cases, the order of the lines in the file does not matter.

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

 **Note:**

[Administering Specific 9600 Series IP Deskphones](#) on page 167 describes 9610-specific administration.

Chapter 8: Administering Applications and Options

Customizing Applications and Options

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

 **Caution:**

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

 **Note:**

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

Following is a list of applications or functions and the parameters that apply to those applications. See [9600 Series H.323 Customizable System Parameters](#) on page 78 for associated parameter descriptions, default values, and valid values or ranges. Parameters shown as Mandatory must be accurate and non-null for the application to work; other parameters listed are optional. You can change parameters to suit your environment. If you do not include these parameters in the settings file, the defaults are used.

Backup/restore parameter - BRURI (Mandatory)

Backlight parameter - BAKLIGHTOFF

Calculator application parameter - CALCSTAT

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

General user parameters - APPSTAT, OPSTAT, OPSTAT2

Guest login parameters - GUESTDURATION, GUESTLOGINSTAT, GUESTWARNING

Options parameter - RINGTONESTYLE

Phone parameter - FBONCASCREEN

User Timer (Stopwatch) — TIMERSTAT

VPN parameters - VPN parameters are listed in the *VPN Setup Guide for 9600 Series IP Telephones* (Document 16-602968) as well as in [9600 Series H.323 Customizable System Parameters](#) on page 78 in this document.

Weather application parameters (touchscreen phones only) - WEATHERAPP, WMLPORT, WMLPROXY

Web access application parameters - SUBSCRIBELIST, TPSSLIST, WMLEXCEPT, WMLHELPSTAT, WMLHOME (Mandatory), WMLIDLETIME, WMLIDLEURI, WMLPORT, WMLPROXY, WMLSMALL. The *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-600888) provides assistance in developing local Web sites.

World Clock application parameters (touchscreen phones only) - WMLPORT, WMLPROXY, WORLDCLOCKAPP

Related topics:

[Setting the Application Status flag \(APPSTAT\)](#) on page 146

Setting the Application Status flag (APPSTAT)

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

APPSTAT consists of one number, specifying a certain level of allowed functionality. A Zero (“0”) value is the most limiting setting. Values “2” and “3” allow increasing levels of functionality, and “1” allows the user complete application functionality.

Table 17: Application Status Flags and Their Meaning of

APPSTAT Value	Meaning
0	Redial and Call Logs/History are suppressed. Contact changes are not allowed.
1	All administered applications are displayed, with full functionality. This is the default value.

APPSTAT Value	Meaning
2	Call Log (History) is suppressed. Contact changes are not allowed. Only one-number Redial is allowed.
3	Contact changes are not allowed. For touchscreen deskphones, this also means that users cannot assign or remove contact Favorites via the Home screen.

“Suppressed” applications are not displayed to the user. Softkey labels, application tabs, and so on are not labeled or displayed. Options associated with suppressed applications can continue to display unless you override them by appropriate OPSTAT parameter administration. Displayed options have no effect while the application is suppressed. “Contact changes are not allowed” means the Contacts application displays and the user can make calls as normal. Any controls that allow the user to change any aspect of the Contact application do not display. This restriction includes the ability to add, delete, or edit any Contact name or number. “Only one-number Redial is allowed” means the user option that allows a choice between displaying last numbers dialed is suppressed. The Redial buffer stores only one number. The Redial application does not display since the user can redial only one number. This restriction allows privacy once a given user has left the telephone.

You can:

- set APPSTAT to “1”, for example, in a staging area,
- administer a given telephone with Contact entries of your choice, like the Concierge telephone number button in the earlier example,
- then move the telephone to where it will be used, where you have administered APPSTAT to be, for example, 0 (zero).

When the relocated telephone resets, it retains its Contact entries, like Concierge, but does not allow the user to create new entries.

When you set APPSTAT to any valid value other than 1, the telephone does not accept any Contact button label changes that might have been made directly on a backup file. Only the existing labels of the telephone are used. This restriction prevents circumvention of the APPSTAT restrictions. The WML applications are also suppressed by default.

Special Administration for the 9610

Administration of the 9610 IP Telephone is handled using the restore file rather than the settings file which is used by all other 9600 Series IP Telephones. For information, see [Administering backup/restore for a 9610](#) on page 140.

Special Administration for Touchscreen Deskphones

The 9621G, 9641G, and 9670G are touch-based phones, and as such, use a touch-based Home Screen in place of the Avaya Menu that other 9600 Series IP deskphones use. The Home Screen provides access to telephone options and settings, special Avaya applications like a World Clock, Calculator and Weather, Contact Favorites, and any WML applications you may administer. The Home screen can display up to four WML applications, but if you have configured more than four applications, the softkey **More** displays to provide access to all WML applications. See [How the Home screen displays WML applications](#) on page 154 for information about display characteristics and icons. If there are no WML applications, there may be a single WML Browser item shown, providing the system parameter WMLHOME is set with a value. Most Avaya Menu elements like those for WML applications do apply, and any 9670G or other touchscreen deskphone exceptions are noted where applicable in the appropriate sections under [Administering the Avaya “A” Menu](#) on page 148.

Administering the Avaya “A” Menu

The A (Avaya) Menu is a list of sub-applications the user can select from to invoke the corresponding functionality. A file called AvayaMenuAdmin.txt is available with downloads on which you can specify the menu label, URI, and list order of WML applications on the “A” Menu.

A Home screen replaces the A Menu for touchscreen deskphones only for access to menu options and settings, log out, Bluetooth setup, and touch screen cleaning. The Home screen also displays WML applications, Favorite contact speed dial buttons, Avaya applications (World Clock and Weather), and a calculator; for more information see [Special Administration for Touchscreen deskphones](#) on page 148. The addition of touchscreen models requires that the AvayaMenuAdmin.txt file be used to specify the WML applications you want displayed on the Home screen. These applications are displayed in order from left to right, going to a second page if necessary.

*** Note:**

This section applies to all 9600 Series IP deskphones except the 9610. For information on 9610 IP Telephone menu administration, see [Special Administration for the 9610 IP Telephone](#) on page 147 in Chapter 9.

! Important:

You must set the system parameter AMADMIN in the 46xxsettings file for Avaya “A” Menu administration with WML applications to work. The AvayaMenuAdmin.txt file must be a Unicode file to be properly processed by the phones. You can create a Unicode version of this file using Notepad or most text editors (select “Encoding” and “Unicode”).

If WML applications are installed and the system parameter AMADMIN is set in the settings file:

- the WML applications appear in the first-level A Menu as specified in the AvayaMenuAdmin file, as shown in [Figure 1](#).
- the first level A Menu on all 9600 Series IP deskphones except touchscreen deskphones includes a single entry (Phone Settings) that leads to a screen containing choices for Options & Settings and Network Information. For touchscreen phones, the Home screen shows a Settings option that leads to an Options & Settings menu.
- the Phone Settings screen is essentially the current Options and Settings menu, with the addition of Network Information, as shown in [Figure 2](#).

If WML applications are installed and the system parameter WMLHOME is set in the settings file, the Avaya “A” Menu is identical to the pre-Release 1.2 “A” Menu, as shown in [the figure](#).

If WML applications are not installed, the A Menu is essentially the same as the current Options & Settings menu, with the addition of Network Information, Log Off, and About Avaya one-X. [The figure](#) provides an illustration.

There are alternatives for how the sub-applications are presented, depending on whether you have administered WML applications or not, as follows:

- Set the system parameter AMADMIN to the URL of the AvayaMenuAdmin.txt in the 46xxsettings file when you have multiple WML applications you want to display on the Avaya “A” Menu. For more information, see [Main Avaya Menu with WML Applications Administered](#) on page 150 and [Administering the Avaya Menu with WML applications](#) on page 153 in this chapter.
- Set the system parameter WMLHOME in the settings file for all but the 9610 when you want “Browser” to show instead of individual applications. For more information, see [Main Avaya Menu with Browser \(Only\) Administered](#) on page 152.
- Take no action to administer WML applications. For more information, see [Main Menu – No WML Applications Administered](#).
- The Browser application is listed only if it is properly administered as specified in *Avaya one-X® Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-600888). Administration also includes a non-null value for WMLHOME.

Related topics:

[Administering Phone Settings and Options and Settings \(OPSTAT and OPSTAT2\)](#) on page 150

[Administering WML applications on the Avaya Menu](#) on page 150

[Main Avaya Menu with Browser \(Only\) Administered](#) on page 152

[Administering the Avaya Menu with WML applications](#) on page 153

[How the Home screen displays WML applications](#) on page 154

Administering Phone Settings and Options and Settings (OPSTAT and OPSTAT2)

The Options & Settings application is listed if and only if the OPSTAT value is not 0xy, where x and y can be any value of 0 or 1, if OPSTAT is in 3-bit form, or if and only if the value of OPSTAT is 1, if OPSTAT is in the one-digit form.

The Network Information application is listed if and only if the OPSTAT value is not x0y, where x and y can be any value of 0 or 1 if OPSTAT is in 3-bit form, or in any case, if OPSTAT is in the one-digit form.

The Logout function is listed if and only if the OPSTAT value is not xy0, where x and y can be any value of 0 or 1 if OPSTAT is in 3-bit form, or if, and only if, the OPSTAT value is 1, if OPSTAT is in the one-digit form.

*** Note:**

If you administer a Log Out button for a softkey on the Phone Screen (as indicated in [Administering features on softkeys](#)), OPSTAT will not prevent that softkey from being labeled and enabling the user to log out.

In general, if OPSTAT is set to forbid access to Options & Settings, changes to the user's backup file settings are ignored. This prevents someone from using the backup file as a "back door" for making changes to the settings. However, some customers centralize the customized relabeling of administered features, and want to be able to upload changes to these labels despite forbidding end users to change settings. The parameter OPSTAT2 can override the value of OPSTAT for this specific case - setting OPSTAT2 to "1" allows the telephone to accept changes to the customized labels stored in the backup file regardless of the OPSTAT value.

*** Note:**

Software Release 3.0 added the system parameter OPSTAT2. Regardless of the preceding text on OPSTAT settings, if the value of OPSTAT2 has the value "1" then any customized labels in the user's backup file are uploaded and used as if the value of OPSTAT permitted this action. However, in order to restore the personalized/customized labels from the backup file to the telephone, the user needs to restart the phone by logging out and then logging back in again.

Administering WML applications on the Avaya Menu

Administering AMADMIN provides direct links to one or more WML applications. As [the figure](#) on page 151 shows, the first level Avaya Menu includes entries for three (sample) WML

applications, a Phone Settings menu choice for telephone options and settings, and the telephone log out.

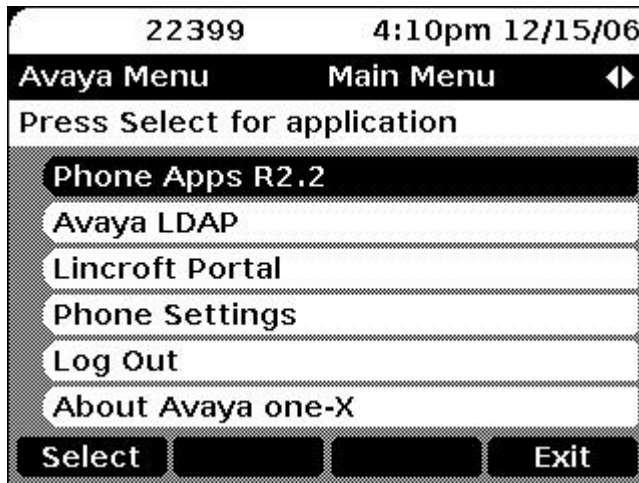


Figure 1: Avaya Menu with WML Applications Installed as the first three Menu options

Given that at least one WML application is administered, the administrator can choose to specify the order in which not only the WML applications are presented, but also the order in which the built-in applications are presented. Any built-in applications that are not specifically administered in the WML Administration file are automatically appended to the end of the administered list, in the following order:

- Phone Settings
- Log Out
- About Avaya one-X

Selecting (highlighting) an application and pressing **Select** or **OK** launches the application. When the Phone Settings application is listed, the Choice Indicator is also displayed on the Title Line. Pressing the Left or Right Navigation buttons displays the Phone Settings Screen. Selecting Phone Settings brings up the Phone Settings menu, shown below.

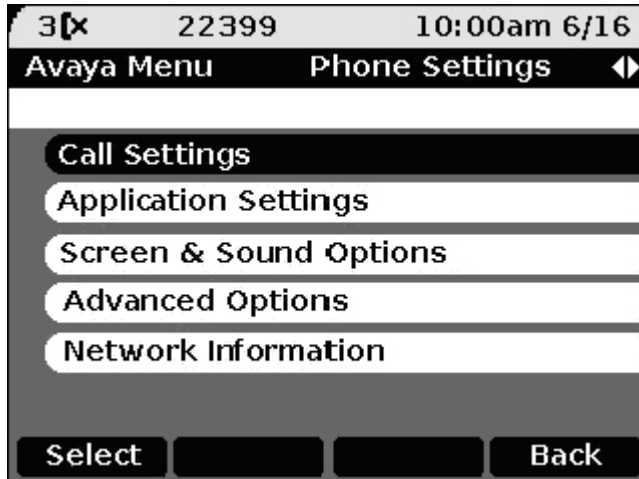


Figure 2: Second Level Avaya Menu - Phone Settings Screen

Main Avaya Menu with Browser (Only) Administered

Setting the system parameter WMLHOME in the settings file provides a way to link to the Browser Home page by specifying a URL. Administering WMLHOME produces the Avaya “A” Menu shown in [the figure](#) on page 152.

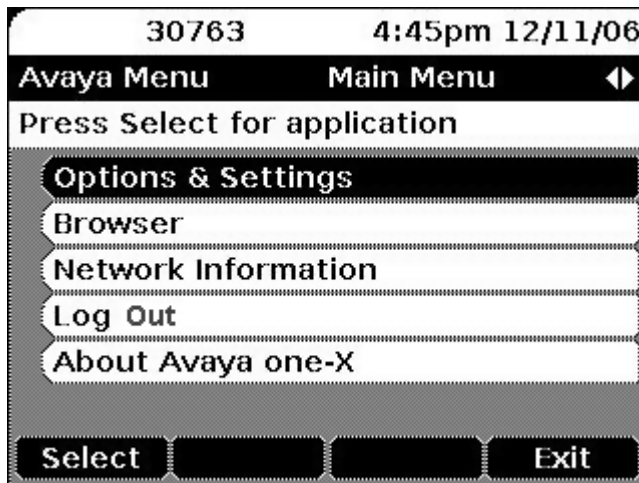


Figure 3: Avaya Menu with Browser Administered using WMLHOME

Each individual sub-application is listed left justified on an individual Application Line. From top to bottom, the sub-applications are:

- Options & Settings
- Browser
- Network Information

- Log Out
- About Avaya one-X

Administering the Avaya Menu with WML applications

About this task

Administer the AMADMIN parameter in the 46xxsettings file to point to a URL where the AvayaMenuAdmin.txt file resides.

! Important:

The AvayaMenuAdmin.txt file must be a Unicode file to be properly processed by the phones. You can create a Unicode version of this file using Notepad or most text editors (select “Encoding” and “Unicode”).

* Note:

Use the AvayaMenuAdmin.txt file to specify the WML applications to appear on touchscreen models’ Home screen.

Then specify objects for the Avaya Menu through the Avaya Menu Administration file, AvayaMenuAdmin.txt. Each administered object, up to the maximum of 12, must have valid, non-null parameter data:

AMTYPExx One of six choices: 01 = URI, 02 = the local “Phone Settings” sub-application, 03 = local Log Off sub-application, 04 = the About Avaya one-X screen, 05 = Guest Login application, 06 = My Pictures application. Touchscreen telephones ignore all AMTYPE values except “1”. If the AMTYPE for an associated administered object is “01”, an additional three parameters must have valid, non-null data for the object to be properly administered:

AMLBLxx The label displayed to the user for this object, up to 16 UTF-16 characters, shown left-justified unless spaces precede the label value to center the label.

AMDATAxx A URI of up to 255 ASCII characters, without spaces.

AMICONxx For touchscreen models only, any number, *N*, from 1 to 25. The touchscreen deskphone will use the *N*th icon presented in [the table](#) on the Home screen in association with the administered WML application. The labels shown in [the table](#) are merely suggestions; the touchscreen deskphone uses the label you specify in the AMLBLxx parameter.

The xx in these three parameters is a two-digit integer from 01 to 12 inclusive, including a leading zero if applicable. If AMTYPExx is 01, xx must be the same for each of the three parameters for an Avaya Menu entry to be displayed and associated with the administered data. If AMTYPExx is 02, 03 or 04, any AMLBLxx or AMDATAxx data is ignored if provided.

If a given administered object has null or invalid data in any of the required associated parameters, that object is completely ignored. To list an AMTYPE01 entry on the Avaya Menu,

all three associated parameters must be non-null with valid data. For example, an AMTYPE of “00” is considered invalid.

Do not administer more than nine URIs. By implication, there is no way to specify a telephone number as a TYPE (unlike the 9610).

In case of duplicate data in the settings file, the last entry is retained. For example, if two consecutive lines in the Avaya Menu Administration file are:

```
AMLBL01=ABCD
```

```
AMLBL01=WXYZ
```

then the user sees “WXYZ” as the label for the first WML application. This example assumes the rest of the administration is correct.

If no AvayaMenuAdmin.txt file is available, or if the file does not contain at least one valid type 1 (URI) object, the Release 1.0/1.1 Avaya Menu shown in ****TERRY*x—ref table**** is presented instead.



*** Note:**

For touchscreen deskphones only, non-WML entries in the AvayaMenuAdmin.txt file are ignored.

How the Home screen displays WML applications






[The table](#) on page 154 shows the icons, suggested description(s), and numbering to use to specify the WML applications you want the Home screen to display.

Table 18: Home Screen WML Application Icons/Labels

To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMLBxx)
	1	Alarm Clock/Wakeup Call
	2	Business data/Sales/Data Analysis

To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMBLxx)
	3	Calendar
	4	Communications
	5	Control (remote, ...)
	6	Directory
	7	Document/Folders/Notes
	8	Emergency/Assistance
	9	Food/Restaurant
	10	Financial Information
	11	Front Desk

To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMBLxx)
	12	Help/Site Help/Feature Help
	13	Guard Desk
	14	Information
	15	Inventory
	16	Location/Map
	17	Messages
	18	Network
	19	Person/People information
	20	Security/Security Camera

To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMLBxx)
	21	Tickets
	22	Valet Service
	23	Video/TV
	24	Slideshow
	25	Room Service

Sample Avaya Menu Administration File Template

```
#####
## ## AVAYA MENU CONFIGURATION FILE TEMPLATE ##
#####
## This file is to be used as a template for configuring the ##Avaya
Main Menu. See the Avaya one-X™ Deskphone H.323 ##Administrator Guide
for details. Both are available on ##support.avaya.com ##
##Since the AMICON parameter applies only to touchscreen telephones,
it is not shown in the sample below.
#####
##
## AMLBLxx=Label up to 16 unicode characters
```

Administering Applications and Options

```
## AMTYPExx=Type 1=WML-Application; 2=local Phone Settings
## 3=local LogOff Application;4=local About Avaya Screen
## 5=Guest Login; 6=My Pictures
## AMDATAxx URI of up to 255 ASCII-characters e.g. http://
YY.YY.YY.YY/*.wml
## The tags AMLBLxx and AMDATAxx are only used if AMTYPExx = 1
## Multiple definitions of local applications (Type 2.4)
## will be suppressed. The last tag is valid.
## xx describes the sequence in the Avaya Menu and is valid
## from 01 to 12.
##
##AMTYPE01=
##AMLBL01=
##AMDATA01=
##
##AMTYPE02=
##AMLBL02=
##AMDATA02=
##
##AMTYPE03=
##AMLBL03=
##AMDATA03=
##
##AMTYPE04=
##AMLBL04=
##AMDATA04=
##
##AMTYPE05=
##AMLBL05=
##AMDATA05=
##
```

```
##AMTYPE06=  
##AMLBL06=  
##AMDATA06=  
##  
##AMTYPE07=  
##AMLBL07=  
##AMDATA07=  
##  
##AMTYPE08=  
##AMLBL08=  
##AMDATA08=  
##AMTYPE09=  
##AMLBL09=  
##AMDATA09=  
##  
##AMTYPE10=  
##AMLBL10=  
##AMDATA10=  
##  
##AMTYPE11=  
##AMLBL11=  
##AMDATA11=  
##  
##AMTYPE12=  
##AMLBL12=  
##AMDATA12=
```

Administering guest users

About this task

A “guest user” is anyone who logs into a 9600 Series IP Telephone that is not his or her primary phone at the user’s home location. This could mean that the guest user can log into a telephone that is across the country from the home location or one in the office adjacent to the home office. You administer permission for guest login by setting the system parameter GUESTLOGINSTAT to “1” (permitted), which in turn displays the Guest Login option on the Avaya “A” Menu. Other related parameters you can administer are GUESTDURATION (which can be overridden by a different, user-entered duration during login) and GUESTWARNING. All parameters are described in [9600 Series H.323 Customizable System Parameters](#) on page 78.

Administering visiting users

About this task

A “visiting user” is anyone who uses a 9600 Series IP telephone in one location (e.g. New York), and intends to register to a call server in some other location (e.g. Paris). Typically, this occurs when a user has travelled from his/her home location to another location in the organization, but wants to register with the call server back home (perhaps to get the specific administered feature buttons, etc. provided by the home call server).

To allow this functionality, the parameter VUMCIPADD should be administered in the 46xxsettings file at the current location for the visitor(s), with the IP address(es) of their home call servers. From then on, the telephone operates as specified in [Step 5: Registering with the call server](#) on page 22.

Administering idle timer operation

About this task

When the idle timer in the telephone expires you can administer the telephone to turn the backlight to its lowest power level, put up a screen saver, and/or show a Web page while the telephone is idle. However, Avaya does not recommend setting all of these values on the same telephone. Avaya does recommend, for instance, that you set a lobby phone to go to a Web page when it is idle and to set a desk phone to go to the screen saver and/or set the backlight to low power mode when idle.

The related system parameters and their default values, further described in [9600 Series H.323 Customizable System Parameters](#) on page 78, are:

Procedure

1. WMLIDLETIME = 10 minutes
2. BAKLIGHTOFF = 120 minutes
3. SCREENSAVERON = 240 minutes
4. WMLIDLEURI = null

Result

WMLIDLEURI is expected to be specified only for phones in public areas through the use of a GROUP parameter.

Table 19: 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 screen saver is displayed. 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 browser is displayed. The Web page may contain its own timer to cycle through additional Web pages. The backlight is set to low power mode after the specified time and the screen saver is displayed based on the SCREENSAVERON value.

*** Note:**

The 9610 IP Telephone uses the IDLEAPP value in the 9610data.txt file instead of WMLIDLEURI in the settings file. For more information, see [Special Administration for the 9610](#) on page 147 and [Administering backup/restore for a 9610](#) on page 140.

*** Note:**

The Backlight Off icon allows the end users to bypass the timers in [the table](#) on page 161 and set the the backlight to its lowest level automatically. You can administer the Backlight Off icon on a 9600 Series IP Telephone softkey as described in [Administering features on softkeys](#) on page 120. The backlight for any adjunct button module will follow the behavior of the backlight of the telephone to which the button module is attached.

Administering the user stopwatch timer

The TIMERSTAT parameter provides user permission to turn a 60 second stopwatch on during a call. The deskphones rather than the call server provide all processes controlling user timer operation. When set to "1" this parameter cannot be turned on or off by the call server.

When the TIMERSTAT parameter is set to "1" a **Timer On** (shown as **TimerOn** for button-based deskphone models) softkey displays, with its position determined by the call state, the screen being displayed, and the presence of other softkeys relative to the current screen/activity. For example:

- When the deskphone is in an active call state, the 4th softkey is labeled **Timer On** and the **Drop** softkey is not presented.
- When the deskphone is in an idle call state, if the **Emerg.** softkey is not administered, the 3rd softkey is labeled **Timer On**. However, if the **Send All** softkey is not administered, the 2nd softkey is labeled **Timer On**.
- Otherwise, the 4th softkey is labeled **More**, and pressing **More** displays **Timer On/ {blank}/ LightOff/More** on the next set of softkeys. Pressing **More** again displays the original set of softkeys.

When the User Timer is presented it is displayed right justified on the Title Line, overwriting any other displayed content. Once displayed, it remains displayed, even if the user changes screens. If the Title Line changes text, the User Timer remains displayed over the text as applicable. Once displayed and activated, the timer is removed when:

- The user presses the **TimerOff** softkey.
- The telephone has displayed 59:59 for 5 seconds.

The user timer begins at 0:00 and increments one second per second until 59:59 is reached, at which point the timer stops but continues being displayed. Once the User Timer is removed, any overwritten text is displayed normally.

If TIMERSTAT is set to 1, the presence of the **Timer On** (or **TimerOn** for button-based models) softkey take priority over other administered features.

Requirements for USB Devices

A USB device can be used to carry information to support the following usage profiles:

- **Mobility/Visiting User:** The USB memory stick carries login credentials, contacts and/or digital pictures. Inserting a USB device will cause the phone to register with a login profile, allowing any 9600 Series IP telephone to become a personalized extension.
- **Deskphone Personalization:** A USB memory stick supports import/export of contacts to/from a 9600 Series IP Telephone and/or display of digital pictures.

Users and administrators can use the *Avaya one-X[®] Deskphone USB Companion*, a PC-based USB management tool that converts Microsoft Office Outlook contacts to a format usable by 9600 Series IP deskphones, and provides an easy way to format other files, like digital pictures that will be used as screensavers. This pc-based tool is available on the Avaya support Web site.

Related topics:

[USB File/Device Support](#) on page 163

[Contacts File Format for USB Devices](#) on page 163

[Setting up USB logins](#) on page 165

[Setting up USB pictures as screensavers](#) on page 165

USB File/Device Support

Only FAT or FAT32 file systems are currently supported. The following are not currently supported:

- USB drives with NTFS file systems are not supported.
- USB devices with multiple partitions or multiple LUNS are not supported.
- U3 USB devices are not supported.

Contacts File Format for USB Devices

As of software Release 2.0, Contacts lists can be imported or exported to or from all 9600 Series IP telephones (except the 9608 and 9610) via a USB device like a Flash drive or memory stick. The telephone user guide provides detailed information on this capability.

Contact files merged or written to the phone's Contacts list must be in a specific format. The user guides advise end users of two ways to ensure that a Contact list is formatted properly.

The rest of this section documents the 9xxxContacts.txt file requirements. Use this information as a guide to export contacts from Outlook and other similar software applications without using the Avaya one-X® Deskphone USB Companion tool.

The contacts file must be a little-endian Unicode text file. That is, each 'character' in the file is a 16-bit integer value, stored least significant byte first. The first two bytes of the file are a Byte Order Mark which must be FF followed by FE (hexadecimal). The file name must be "9xxxContacts.txt" (without the quotes).

Each contact entry consists of a single line, terminated by <CR><LF> (Carriage Return, 000D hex, and Line Feed, 000A hex). An entry contains 1 name, 1 to 3 phone numbers, and 0 to 3 types. Separate the fields within each contact entry with one or more tabs.

The detailed contact entry format is:

```
<name><tab><number1><tab><type1><tab><number2><tab><type2><tab><number3><tab> <type3><CR><LF>
```

Name and Number fields - can start and end with a double quote character ["]]. The name and number1 are required, and each must be at least one character (not counting quotes). Limit names and phone numbers to 20 characters for the name, 30 for the numbers. Values are truncated if they exceed these maximum sizes.

Types - must be 3 characters, starting and ending with a slash '/' character, with a digit character 0 to 3 in between; e.g. "/1/". Leading and/or trailing spaces are ignored for type fields. The Types are 0 for General, 1 for Work, 2 for Mobile, and 3 for Home. Types are optional and missing types default to 0 (General).

Lines may be at most 255 Unicode characters long, including the <CR><LF>. Blank lines, including lines consisting only of spaces and/or tabs, are ignored. A field other than the first that consists of only spaces is ignored.

Because types can be omitted, if the potential type field is more than 3 characters or does not start and end with a slash, it is considered the next number field, if any (e.g. "/1" and "/02/" would be considered numbers).

Entries are invalid if:

- the name is null (a non-blank line starts with tab or with "" followed by tab).
- there is no number1 field.
- any number field is null (for example, just "" for number2).
- a potential type field contains an invalid digit (not 0, 1, 2, or 3) or consists of "/" or "/".
- more than three numbers are provided.
- the entry contains more types than numbers.

The Windows™ XP Notepad program allows Unicode text files to be created and edited. Use the Save As dialog to set the file “Encoding” to “Unicode.”

Setting up USB logins

About this task

As of software Release 3.0, users can be allowed to log in to their call servers via a USB Login profile. As the administrator, you enable this feature by allowing the parameter USBLOGINSTAT in the settings file to remain at the default value of “1” or you can disable this feature by changing the value to “0”. The advantage of having USB login is that users can go anywhere in the world having sufficient network data connectivity, plug the USB device into a 9600 Series IP telephone running software Release 3.0 or later and log into their home call server using their own extension and get all their home administered features.

You can use *Avaya one-X® Deskphone USB Companion*, the Avaya PC-based USB management tool, to create the USB login profile and specify whether the login password should be encrypted or stored in the clear. For more information on this tool, see the Avaya support Web site, <http://www.avaya.com/support>.

* Note:

When users log in via the USB Login feature, the telephone does not attempt to access the backup file as normal, so normal user-specified data such as Options, or Call Log entries are not available. The reason is that if the user is in a different environment from the usual office the telephone would attempt to access the local backup file server instead of the remote (home) file server and could obtain a different backup file than that of the user. Additionally, the only contacts a user has access to when registered via USB Login are the contacts available on the USB device (properly formatted as a 9xxxContacts.txt file using the Avaya USB tool or another method).

Setting up USB pictures as screensavers

About this task

As of Software Release 3.0, one or more pictures from a USB flash drive device can be used as screen savers. The USB device may contain any number of .jpg or .jpeg files that can be used in place of a default or custom screen saver(s). If multiple files are provided, the telephone will present each picture in order, based on the order the pictures were saved, changing to the next image after the number of seconds specified by the timer parameter, which has a default of 5 seconds. These pictures also be viewed directly by using the “My Pictures” option on the Avaya “A” Menu or on the Home screen.

Users and administrators can use the *Avaya one-X® Deskphone USB Companion* to format digital pictures that will be used as screensavers. This pc-based tool is available on the Avaya support Web site.

If you want to set up digital picture files manually without using the *Avaya one-X® Deskphone USB Companion*, follow these instructions:

Procedure

1. Create a “Pictures” directory on the USB device.
2. Add one or more images with an extension of *.jpeg or *.jpg, and with a valid JPEG format to the pictures directory.

The images should not exceed the pixel sizes below for the respective telephone model. Color phones such as the 9620C, 9621G, 9640, and 9650C display a better image quality than those 9600 Series IP Deskphones that do not have color displays:

Deskphones Supporting USB	Image Size in Pixels (HxW)
9620/9620C/9620L	320x160
9611G/9630/9630G/ 9640G/9650/9650C	320x240
9641G	480x272
9670G	640x480

*** Note:**

Images that are too large to be displayed on the phone will not be displayed; in this case, the default screensaver image will be shown instead. The 9608 and 9610 IP deskphones do not have a USB interface and therefore cannot display digital images as screensavers.

*** Note:**

The screensaver will start automatically when the phone is idle for the time specified in the SCREENSAVERON parameter (default is 240 minutes). In practice, it is useful to reduce this time in order to use the USB Pictures feature. To disable USB picture functionality, set the SCREENSAVERON parameter to “0” in the settings file.

Chapter 9: Administering Specific 9600 Series IP Deskphones

Introduction

Some 9600 IP telephone models may require that you administer additional features or have special administrative requirements. For example, the 9610 IP telephone is a one-line telephone designed as a courtesy, or walk-up, telephone. The 9610 is not full-featured like other 9600 IP Series telephones, with just a Contacts application, but additional features like WML applications and a Directory can be administered for a 9610.

This chapter provides additional or alternate administration details for specific telephone models.

Special Administration for the 9610 IP Telephone

General 9610 Functionality

Because the 9610 is a single line phone, the user cannot transfer or conference calls, or put an active call on hold.

The 9610 does not have a phone screen like other 9600 Series IP deskphones. There are two application buttons - **Start** and **Contacts**. There are no “A” (Avaya Menu) or Call Log buttons, Speaker or Mute buttons. The Web browser application is supported.

The Main Menu (MM) on the Start screen is an administrable list of “objects” from which a user can select a new application that is either local to the telephone or on an external server, or an outgoing call. Underlying Main Menu content administration directs the telephone to take action applicable to the given selection. The default Main Menu consists of Contacts and Directory, assuming they have been appropriately administered. The Main Menu displays when the telephone first powers up or resets.

The Contacts Application provides functionality similar to the other models but only to launch a call to a contact. Contacts cannot be edited, deleted or added.

The Idle Application displays when both a Web Idle Timer and the Idle application have been administered and the timer expires. For example, if the Idle application has been set to “Contacts,” when the Web Idle Timer expires the 9610 display changes to the Contacts application. The Idle application is either one of the existing local applications (Menu or Directory) or a URL, depending on the contents of IDLEAPP.

Key 9610 Administration Concepts

Each 9610 seeks a backup/restore file which contains essential administration data in its user interface that enables different capabilities to walk-up users. The backup file concept is common to all phones, but in the case of the 9610, must be created by an administrator to specify the required behavior of the telephone to walk-up users. Backup and retrieval for the 9610 is covered in more detail in [Backing up and restoring data on a 9610](#) on page 140.

A group of 9610 phones can share a common backup file, or individual 9610 IP Telephones can have individual customized backup files.

Backup files must be created in an editor. There is no capability to store a current configuration from the phone to a backup file as there is for other 9600 Series models.

Within the backup file format, the configuration is split into three portions corresponding to the applications mentioned in [General 9610 Functionality](#) on page 167:

- Main Menu administration as described on [Administering a 9610 Main Menu \(MM\)](#) on page 170.
- Contacts administration as described on [Administering the 9610 Contacts Application](#) on page 171.
- Idle administration as described on [Administering the 9610 idle application, screensaver, and WML links](#) on page 172.

Create a generic backup/restore file named “9610data.txt” that can be used as a default to provide basic functionality and serve as a template for any customized 9610 extensions. Create a backup/restore file named “Ext#_9610data.txt” for the specific extension you want to customize.

See the Avaya support site <http://support.avaya.com> to download a 9610 backup file example. A sample file also appears on [Sample 9610data.txt file](#) on page 174.

*** Note:**

Like other telephone models, the 9610 looks for a 46xxsettings file at startup. In the 46xxsettings file, the system parameter BRURI must be set to the URI where the 9610data.txt file is located. This consists of the HTTP server IP Address and (optional) directory.

If the telephone cannot find the 9610data.txt file or if that file does not exist, the screen displays the default Main Menu (Contacts and Directory).

Related topics:

[9610 Backup File Format](#) on page 169

[Administering a 9610 Main Menu \(MM\)](#) on page 170

[Administering the 9610 Contacts Application](#) on page 171

9610 Backup File Format

Use a text editor to create the 9610 backup file. Characters are assumed to be coded in UTF-16 LE (little-endian), with Byte Order Mark (BOM) for LE (0xFFFE)), with each item on a separate line terminated by” <CR><LF>” (000D 000A in UTF-16) characters.

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

The format for a Main Menu entry is:

MMLBLxx=entry label

MMTYPExx=entry type

MMDATAxx=entry data

The format for a Contacts entry is:

CONLABELxxx=entry label

CONDATAxxx=entry data

Other parameters that have meaning in a 9610 backup file are:

IDLEAPP

LISTAPP

When retrieving data, the following applies:

- If the BOM is not 0xFFFE, the entire file is rejected and the retrieval is considered to have failed.
- All identifiers (for example, names) are interpreted in a case-insensitive manner.
- The case of parameter values and Contacts names and numbers is preserved.
- Spaces preceding, within, or following a name or value are treated as part of that entity.
- <CR> and <LF> are interpreted as line termination characters.
- Blank lines are ignored.
- If an identifier is not recognized or is invalid, the entire line is ignored.

- If an identifier is valid but the data itself is invalid or incomplete, the line is ignored. The determination of what constitutes a valid value for each data element is specified in the individual requirements in this document.
- If more than one line contains a value for a parameter or Contacts entry, the last value read is used. Hence, new values overwrite previous values as lines are read from the file. In all other cases, the order of the lines in the file does not matter.

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

Administering a 9610 Main Menu (MM)

About this task

Use the 46xxsettings file to set the system parameter BRURI to point to the URI where the 9610 backup/restore file (9610data.txt) resides. Then specify objects for the Main Menu via the “9610data.txt” backup file. A [Sample 9610data.txt file](#) on page 174 is provided at the end of this chapter.

* Note:

The 9610 will not display a Main Menu unless you set BRURI to point to the 9610data.txt file and specify Main Menu objects.

Each administered object, up to the maximum of 10, must have valid, non-null data in each of the three parameters as indicated:

- MMLBLxx - the label displayed to the user for this object, up to 16 characters.
- MMTYPExx - one of four choices: 01=URI, 02=telephone number, 03=local Contacts application, 04=local Directory application.
- MMDATAxx - the data used depends on the value of MMTYPExx: a URI, if MMTYPE is 01; a dialable string if MMTYPE is 02; the English word Contacts if MMTYPE is 03; the English word Directory if MMTYPE is 04.

* Note:

If administered as a URI, MMDATAxx is up to 255 ASCII characters in length.

In these parameters, xx is a two-digit integer from 01 to 10 inclusive, including a leading zero if applicable. If MMTYPE is 01 or 02, xx must be the same for each of the three parameters for a Main Menu entry to be displayed and associated with the administered data. If MMTYPE is 03 or 04, xx must be the same as a corresponding MMLBL item for a Main Menu entry to be displayed, but no MMDATA need be assigned. Any MMDATA assigned to that xx entry is ignored.

If a given administered object has null or invalid data in any of the required associated parameters, that object is completely ignored. Therefore for a MMTYPE 01 or 02 entry to be listed on the Main Menu, all three associated parameters must be non-null with valid data. An MMTYPExx of “00” is considered invalid.

The default values for Main Menu (MM) objects are:

Parameter	Default Value
MMLBL01	Contacts (automatically translated into the user interface language).
MMTYPE01	3 (Local Contacts application).
MMDATA01	Contacts (English only)
MMLBL02	Directory (automatically translated into the user interface language).
MMTYPE02	4 (Local Directory application).
MMDATA02	Directory (English only).

The default “Directory” will appear as the first Main Menu object whenever it is not administered in the Main Menu, if there is no 9610 backup file, or if retrieval of the backup file fails.

The DATA terms “Contacts” and “Directory” are always administered in English, and are independent of the user interface (UI) language. The administrator can create labels for the local applications in the UI language if desired. The administrator can use, for example, “Contacts” for a browser-based application, and “List” for the local Contacts application. Instead, the term used presents the appropriate local application, which does present the UI in the user’s language.

The Main Menu allows up to 10 administrable objects including the two local application objects, Contacts, and Directory so that the total number of items fit on two screens.

Administering the 9610 Contacts Application

The administrator populates the Contacts Application via the backup file. Each administered object, up to the maximum of 250, must have valid, non-null, data in both of the parameters as indicated:

CONLABELxxx (the label displayed to the user for this object)

CONDATAxxx

In the list of parameters above, xxx is a three-digit integer from 001 to 250 inclusive. To display and associate with the administered data, the three-digit integer must be the same for both parameters. The xxx value includes leading zeroes as applicable.

If a given administered object has null or invalid data in any of the two associated parameters, that object is completely ignored. Hence, to be listed in the Contacts application, both associated parameters must be valid and non-null.

CONLABELxxx data maps to the corresponding ENTRY_NAME. CONDATAxxx maps to the corresponding ENTRY_NUMBER_1.

All contacts are sorted in alphanumeric order on the Phone screen regardless of the order put in the backup/restore file.

Administering the 9610 idle application, screensaver, and WML links

The 9610 IP Telephone can present a variety of behaviors if the telephone is left idle for a period of time.

WMLIDLETIME - This parameter (set in the 46xxsettings file, if administered) specifies the number of minutes the phone must be idle before an Idle Application specified by **IDLEAPP** can be presented on the display.

SCREENSAVERON - This parameter (set in the 46xxsettings file, if administered) specifies the number of minutes the phone must be idle before the Avaya Screen Saver can be presented on the screen.

*** Note:**

In the current firmware version, it is not advisable to use both **WMLIDLETIME** and **SCREENSAVERON**. For example, one value should be set to 999 and the other to some nominal time, perhaps 30 minutes.

WMLSMALL - This parameter (set in the 46xxsettings file, if administered) is required to be non-null for WML links specified in the Main Menu to be displayed. Set this value to a valid URL, and under certain circumstances, it will become the Idle Application displayed on the phone.

IDLEAPP - If the **IDLEAPP** parameter is administered as " " (Null, the default value), when the Web Idle Timer expires, the URL that **WMLSMALL** points to is presented, if **WMLSMALL** is administered. If both **IDLEAPP** and **WMLSMALL** are null, the 9610 displays the Avaya one-X Screen.

If **IDLEAPP** is administered as:

- **Menu** - when the Web Idle Timer expires, the telephone displays the Main Menu application if the Main Menu is not empty. If the Main Menu is empty, the Avaya Screen displays instead.
- **Directory** - when the Web Idle Timer expires, the telephone displays the Directory application. If a Directory does not exist, the telephone displays the Avaya Screen.
- **Contacts and LISTAPP is non-null** - when the Web Idle Timer expires, the telephone launches the Contacts application.
- **Contacts and LISTAPP is null** - and the local Contacts application is not empty when the Web Idle Timer expires, the telephone launches the local Contacts application. If the local Contacts application is empty, the telephone displays the Avaya Screen.

Note:

The terms “Menu,” “Contacts,” and “Directory” are always administered in English. The terms are independent of the user interface language, since the telephone does not directly present the value of IDLEAPP to the user. Instead, the term is used to present the appropriate local application, which does present the user interface in the user’s language.

If IDLEAPP is administered as “Directory”, and the Directory application is the ACP-based Integrated Directory, then the telephone will have to reinstate the application approximately every minute, since the feature automatically times out after that interval.

If the screen saver is displayed, the Idle Application is not visible until the screen saver is removed. The screen saver is removed when the user goes off-hook, presses a button, or the telephone receives an incoming call.

For example:

- if an IDLEAPP display is desired when the telephone has been idle for 30 minutes, Avaya recommends that IDLEAPP be administered as non-null, that WMLIDLETIME be set to “30” and SCREENSAVERON be set to “999.”
- If a WMLSMALL URL display is desired when the phone has been idle for 30 minutes, Avaya recommends that IDLEAPP be administered as “ ” (null), that WMLIDLETIME be set to “30,” that SCREENSAVERON be set to “999,” and that WMLSMALL be administered as a valid URL.
- To display the Avaya Screen Saver after 30 minutes of telephone idle time, set IDLEAPP to “ ” (null), set WMLIDLETIME to “999,” set WMLSMALL as desired (with a URL if Main Menu WML links are to be displayed, or null if not), and set SCREENSAVERON to “30.”

See [Sample 9610data.txt file](#) on page 174, [Sample idle.wml file](#) on page 176, and [Sample hotel.wml file](#) on page 177 for examples of generic files to use as templates. Also see the Avaya 9600 Series IP Telephones support Web site for a downloadable example of typical 9610 setup files.

Accessing 9610 Craft procedures

Unlike the other 9600 Series IP Telephones, press the **Contacts** button twice instead of pressing **Mute** to access local procedures.

Troubleshooting a 9610 IP Telephone

- If the Directory functionality is not present, make sure that you administer “Directory,” “Next,” and “Call-disp” (the latter which shows as “Make call” on the telephone) on the

CM station form in the first six call appearances/feature buttons. (Applies to pre-CM4.0 only.)

- Any call appearances/features administered beyond the first six call appearances/feature buttons will be ignored. (Applies to pre-CM4.0 only.)
- If calls cannot be received on the 9610, check the station administration for a “y” in the “Restrict Last Appearance” field. Change to “n” to allow incoming calls.
- If the “Ext#_9610data.txt” is not set up, the phone will default to the “9610data.txt” file.
- If the “9610data.txt” file is not set up, the telephone displays the message “Restore Failed.” and the default Avaya start screen. In this case, even if CM Directory is administered, the start screen appears and the Directory application will not be available.
- If “Restore Failed” appears on the screen when you bring up a 9610, this indicates the telephone could not find or load the backup file.
 - Check folder and file availability and permissions.
 - Check to be sure the filename matches the required conventions for individual extensions or generic backup for all 9610 IP Telephones.
 - Check to be sure the 46xxsettings.txt file has a “Set BRURI http://xxx.xxx.xxx.xxx” entry, where “xxx.xxx.xxx.xxx” is the IP Address of the HTTP server where the 9610data.txt file is stored.
 - Check to be sure there is a byte order mark (BOM) in the 9610data.txt file. The BOM is generated when the 9610data.txt file is saved in Unicode format.
- The WMLSMALL parameter must be non-null for Main Menu WML links to be displayed.

Sample 9610data.txt file

```
##
## THE FOLLOWING "CON" SECTION IS
## THE DEFAULT 9610 "CONTACTS LIST"
## AND MAY BE POPULATED WITH REAL
## NAMES AND TELEPHONE NUMBERS
## OR EXTENSIONS FOR YOUR COMPANY.
## THE ITEMS WILL NOT APPEAR IN THE
## ORDER OF THE LABEL NUMBERS BUT
## RATHER, IN ASCII ALPHA ORDER. THE
## CONTACTS LIST MAY BE SELECTED
```

```

## USING THE 9610's RIGHT SIDE (BOOK)
## "CONTACTS" BUTTON. THE "CON"
## MENU WILL SCROLL IF MORE THAN 6
## LABEL GROUPS ARE CONFIGURED.
## NOTE: "+" BELOW INDICATES NON WORKING
## TELEPHONE NUMBERS.
##
CONLABEL001=c: Security+
CONDATA001=12345
CONLABEL002=b: Building Svc+
CONDATA002=91555555555555
CONLABEL003=d: Help+
CONDATA003=91555555555555
CONLABEL004=a: Audix+
CONDATA004=12345
CONLABEL005=9610-DEMO-ONLY+
CONDATA005=DUMMY
CONLABEL006=+NOT WORKING#'s
CONDATA006=DUMMY
##
## THE FOLLOWING ""MM" SECTION IS
## THE DEFAULT "MAIN MENU" AND
## NORMALLY APPEARS FOLLOWING
## A 9610 REBOOT OR POWER UP.
## THE ""MM" GROUPS MAY BE
## REPLACED WITH WML LINKS OR
## TELEPHONE NUMBERS APPROPRIATE
## TO YOUR INSTALLATION, INCLUDING
## THE IP ADDRESS OF YOUR FILE
## SERVER AND WML PATH. NOTE THAT
## WMLSMALL MUST BE A VALID URL FOR

```

```
## WML LINKS TO DISPLAY IN THIS MENU.  
## THE "MM" MENU WILL SCROLL IF MORE  
## THAN 6 LABEL GROUPS ARE CONFIGURED.  
##  
MMLBL01=ABOUT-9610  
MMTYPE01=1  
MMDATA01=http://135.8.60.18/WML/about.wml  
MMLBL02=MyCo Today  
MMTYPE02=1  
MMDATA02=http://135.8.60.18/WML/index.wml  
MMLBL03=MyCo Directory  
MMTYPE03=4  
MMDATA03=Directory  
MMLBL04=Visitor Info  
MMTYPE04=1  
MMDATA04=http://135.8.60.18/WML/visit_lz.wml  
MMLBL05=Printer Trouble  
MMTYPE05=1  
MMDATA05=http://135.8.60.18/WML/printer-rooms.wml  
MMLBL06=Call Jack+  
MMTYPE06=2  
MMDATA06=32099
```

Note that the information entered into the backup/restore file is what controls the 9610 Main Menu. The references within the files are to ".wml" files, which are text Web pages and an example is provided for illustration only. The content of these files must be customized for specific phones/sites. The wml files can be placed at the root level or buried in a lower level directory if desired. Modify the Backup/Restore and 46xxsettings file references accordingly.

Sample idle.wml file

```
<?xml version="1.0"?>
```



```
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN" "http://
www.wapforum.org/DTD/wml13.dtd">
```

```
<wml>
  <card id="splash" title=" ">
    <p align="center">
      
    </p>
  </card>
</wml>
```

Sample hotel.wml file

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN"
"http://www.wapforum.org/DTD/wml13.dtd">
<wml>
  <card id="
hotel"
  title="
Hotels"
  >
    <p><a href="
hotels/marriott_courtyard.wml"
>Marriott Courtyard</a></p>
    <p><a href="
hotels/extended_stay.wml"
>Extended Stay</a></p>
    <p><a href="
hotels/molly_pitcher.wml"
>Molly Pitcher</a></p>    <p><a href="
hotels/oyster_point.wml"
>Oyster Point</a></p>    <p><a href="
hotels/holiday_inn.wml"
>Holiday Inn</a></p>
    <do type="
prev"
  label="
Back"
  ><prev/></do>
  </card>
</wml>
```


Glossary

802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. Applicable 9600 Series IP Deskphones support IEEE 802.1X for pass-through and for Supplicant operation with the EAP-MD5 authentication method.
ARP	Address Resolution Protocol, used, for example, to verify that the IP Address provided by the DHCP server is not in use by another IP telephone.
CA	Certificate Authority; the entity which issues digital certificates for use by other parties.
CELP	Code-excited linear-predictive. Voice compression requiring only 16 kbps of bandwidth.
CLAN	Control LAN, 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.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.
Diffie -Hellman key exchange	A key agreement algorithm based on the use of two public parameters p and g that may be used by all users in a system. Parameter p is a prime number and parameter g (usually called a generator) is an integer less than p .
DH Group	A number that determines the public parameters used by the Diffie-Hellman key exchange. To successfully establish a shared secret key, the same DH group must be used by both parties.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
Digital Certificate	The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by a trusted third party known as a "Certificate Authority" (CA) such as VeriSign (www.verisign.com). The CA verifies that a public key belongs to a specific company or individual (the "Subject"), and the validation process

it goes through to determine if the subject is who it claims to be depends on the level of certification and the CA itself.

Digital Signature

A digital signature is an encrypted digest of the file (message, document, driver, program) being signed. 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/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. Avaya 9600 Series IP Deskphones can use DNS to resolve names into IP Addresses. In DHCP, TFTP, and HTTP files, DNS names can be used wherever IP Addresses were available as long as a valid DNS server is identified first.

EAP-TLS

Extensible Authentication Protocol, or EAP, is an authentication framework frequently used in wireless networks and Point-to-Point connections. It 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. It uses PKI to secure communication to a RADIUS authentication server or another type of authentication server.

Gatekeeper

H.323 application that performs essential control, administrative, and managerial functions in the call server. Sometimes called CLAN in Avaya documents.

H.323

A TCP/IP-based protocol for VoIP signaling.

HAC

Hearing Aid Compatibility, an FCC (Federal Communications Commission, part of the United States government) Part 68 standard for handset equalization for interoperability with t-coil enabled hearing aids devices.

HTTP

Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.

HTTPS

A secure version of HTTP.

IETF

Internet Engineering Task Force, the organization that produces standards for communications on the internet.

IKE	Internet Key Exchange Protocol, RFC 2409, which has been obsoleted by IKEv2 in RFC 4306.
IPsec	A security mechanism for IP that provides encryption, integrity assurance, and authentication of data; applies only to IPv4.
ISAKMP	Internet Security Association and Key Management Protocol, RFC 2408, which has been obsoleted by IKEv2 in RFC 4306, defines the procedures for authenticating a communicating peer, creation and management of security associations, key generation techniques, and threat mitigation e.g. Denial of service and Replay Attacks. ISAKMP defines two phases of negotiation. During Phase 1 negotiation, two entities establish an ISAKMP SA, which is used to protect Phase 2 negotiations, in which SAs are established for other protocols.
LAN	Local Area Network.
LLDP	Link Layer Discovery Protocol. All deskphones with an Ethernet interface support the transmission and reception of LLDP frames on the Ethernet line interface in accordance with IEEE standard 802.1AB.
MAC	Media Access Control, ID of an endpoint.
Media Channel Encryption	Encryption of the audio information exchanged between the IP telephone and the call server or far end telephone.
NAPT	Network Address Port Translation.
NAT	Network Address Translation, a mechanism by which IP addresses are mapped from one address space to another, and in which UDP and TCP port numbers may be remapped to allow multiple devices to share the same IP address without port number conflicts.
OPS	Off-PBX Station.
PHP	Hypertext Preprocessor, software used to assist in the format and display of Web pages.
PSTN	Public Switched Telephone Network, the network used for traditional telephony.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks.
Refresh/Rekey	Use IKE to create a new SA with a new SPI.
RSA	Rivest-Shamir-Adleman; a highly secure asymmetric cryptography method developed by RSA Security, Inc. that uses a public/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

RSVP

recipient's public key, which can only be decrypted by the recipient's private key. 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". RSA can also be used for authentication by creating a digital signature, for which the sender's private key is used for encryption, and the sender's public key is used for decryption.

RSVP

Resource ReSerVation Protocol, used by hosts to request resource reservations throughout a network; applies to IPv4 audio connections only.

RTCP

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

RTP

Real-time Transport Protocol. Provides end-to-end services for real-time data such as voice over IP.

SA

Security Association, a security protocol (e.g., IPSEC, TLS) and a specific set of parameters that completely define the services and mechanism necessary to protect security at that security protocol location. These parameters can include algorithm identifiers, modes, cryptographic keys, etc. The SA is referred to by its associated security protocol (for example "ISAKMP SA", "ESP SA", "TLS SA").

SCEP

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

SDP

Session Description Protocol. A well-defined format for conveying sufficient information to discover and participate in a multimedia session.

Signaling Channel Encryption

Encryption of the signaling protocol exchanged between the IP telephone and the call server. Signaling channel encryption provides additional security to the security provided by media channel encryption.

SIP

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

SLA Monitor Server

SLA Mon Server is a network monitoring tool that constantly monitors customer network to detect network problems before they affect applications and result in degradation of business critical applications.

SNTP

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

SOHO

Small Office Home Office. The environment for which a virtual private network (VPN) would be administered.

SPD	Security Policy Database. Specifies the policies that determine the disposition of all IP traffic inbound or outbound from a host or security gateway IPsec implementation.
SPI	Security Parameter Index. An identifier for a Security Association, relative to some security protocol. Each security protocol has its own “SPI-space”.
SRTCP	Secure Real-time Transport Control Protocol.
SRTP	Secure Real-time Transport Protocol.
system -specific	Specific to a particular type of call server, e.g., Avaya Communication Manager (CM) or SIP Enablement Services (SES). “System-specific signaling” refers to messages specific to the signaling protocol used by the system, e.g., H.323 and/or CCMS messages used by CM and IP Office, or SIP messages (possibly including system-specific headers) used by SES. “System-specific procedures” refers to procedures in telephone software that are specific to the call server with which the software is intended to be used.
SSH	Secure Shell (SSH) is a network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network: a server (running an SSH server program) and a client (running an SSH client program).
TCP/IP	Transmission Control Protocol/Internet Protocol, a network-layer protocol used on LANs and internets.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP telephones.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications.
TLV	Type-Length-Value elements transmitted and received as part of Link Layer Discovery Protocol (LLDP).
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
Unnamed Registration	Registration with Avaya Communication Manager by an IP telephone with no extension. Allows limited outgoing calling.
URI & URL	Uniform Resource Identifier and Uniform Resource Locator. Names for the strings used to reference resources on the Internet (for example, HTTP://...). URI is the newer term.

VLAN

VLAN

Virtual LAN.

VoIP

Voice over IP, a class of technology for sending audio data and signaling over LANs.

VPN

Virtual Private Network; a private network constructed across a public network such as the Internet. A VPN can be made secure, even though it is using existing Internet connections to carry data communication. Security measures involve encrypting data before sending it across the Internet and decrypting the data at the other end. An additional level of security can be added by encrypting the originating and receiving network address.

VSI

Vendor Specific Information; used in determining IPv6 information.

WML

Wireless Markup Language, used by the 9600 Series IP Telephone Web Browser to communicate with WML servers.

Index

Numerics

802.1X	105
9600 Series IP telephones	145
Customizing Applications and Options	145
9600 Series IP Telephones	15 , 16 , 21 , 72 , 77
Administering Options for	77
Administration Alternatives and Options	16
Customizable System Parameters	77
General	15
Initialization Process	21
Scripts and Application Files	72
9610 Craft Procedures	173
9610 File Retrieval, General Processing	142
9610 IP Telephone, Special Administration for	147
9610 IP Telephone, Troubleshooting	173
9610 Key Administration Concepts	168
9610 Retrieval Procedures	141
9620/9620C/9620L IP Telephone, Feature administration	51

A

About This Guide	9
Ad-Hoc Conferences	55
administering	129
Administering	160
Visiting Users	160
Administering agent sign ins for call centers	131
Administering deskphones for call center operation ..	130
Administering Features	49
Administering the Vu button	133
Administration Alternatives and Options for 9600 Series IP Telephones	16
Administration Overview and Requirements	15
Administrative Checklist	19
Administrative Process, The	19
Agent sign ins, administering for call centers	131
Aliasing	39
Alternatives, Administration	16
Application File and Upgrade Script, Choosing	72
Application Icons/Labels, for Home Screen	154
Application Status Flag (APPSTAT)	146
Application Status Flags and Their Meaning	146
Application-specific parameters, administering	16
APPSTAT	146
Assessment, of Network	25

Audio equalization	129
Auto Hold administration	47
Auto select any idle appearance administration	49
Avaya	148
Avaya Menu Administration	153
Avaya Menu Administration File Template	157
Avaya Menu with WML Applications	150

B

Backup	136
Backup File Format, for the 9610	169
Backup File Formats	136
Backup, Options and Non-Password Parameters Saved	137
Backup/Restore	134
Backup/restore processing	66
Button Modules (SBM24 and BM12)	54

C

Call Center operation, administering deskphones for ..	130
Call Server (Switch) Administration	41
Call Server Requirements	39
Call Transfer Considerations	45
Calltype Digit Analysis	116
Checklist, Administrative	19
Codecs, Wide Band	56
Conference/Transfer on Primary Appearance administration	49
Conferencing Call Considerations	46
Contacts Application Administration, for the 9610	171
Contacts File Format for USB Devices	163
Coverage Path administration	47 , 49
Custom Screen Saver, Administering	128
Customizable System Parameters	77
Customizing 9600 Series IP Telephone Applications and Options	145

D

DHCP and File Servers	57
DHCP Generic Setup	29 , 58
DHCP options	61 , 64
DHCP Server	27
DHCP Server Administration	58

DHCP Server Setup	58	IEEE 802.1Q	43
DHCP Server to Telephone initialization	22	IEEE 802.1Q QoS parameters	43
DHCP, Configuring for 9600 Series IP Deskphones ..	58	Initialization Process, for 9600 Series IP Telephones	21
DHCP, Parameters Set by	58	Installation, Network Information Required before	
Dialing Methods	116	installing	27
Dialing, Enhanced, Requirements	118	Interface, administering the	16
DNS Addressing	105	IP Address Lists and Station Number Portability	31
<hr/>		IP Addresses, administering	16
E		IP Interface and Addresses, for call servers	42
EC500 administration	47	IPv4 and/or IPv6 Operation	68
Enhanced Conference Features administration ..	47, 49	<hr/>	
Enhanced Local Dialing	116	L	
Enhanced Local Dialing Requirements	118	Language Selection	112
Enhanced Phone Screen Display	53	legal notices	2
Error Conditions	24	Link Layer Discovery Protocol (LLDP)	108
<hr/>		LLDP Data Units Transmitted	108
F		Local Administrative Options	112
Far End Mute administration	49	Log Digit (Smart Enbloc) Dialing	116
Feature administration for all other deskphones (except		<hr/>	
9610 and 9620/9620C/9620L)	51	M	
Feature Administration for Avaya Communication		Main Menu (MM) Administration, for the 9610	170
Manager	47	<hr/>	
Feature Numbers for Assigning Softkeys	120	N	
Feature-Related System Parameters, administering on		NAT	43
CM	47	Network Assessment	25
Features, Administering on Softkeys	120	Network Audio Quality Display	30
File download	72, 73	Network Considerations, Other	27
Choosing the Right Application and Upgrade Script		Network Information, Required	27
File	72	<hr/>	
Download File Content	73	O	
<hr/>		On-Hook Dialing administration	47
G		OPSTAT	77, 150
General Download Process	71	Options, Administering	77
Generic Setup, for DHCP	61	Options, Customizing	145
Gigabit Ethernet Adapter	115	Options, for 9600 Series IP Telephone Administration	16
GROUP parameter	74	Other Network Considerations	27
Guest User Administration	160	<hr/>	
<hr/>		P	
H		Parameter Data Precedence	18
Hardware Requirements	25	Parameters in Real-Time	30
Home Screen WML Application Icons/Labels	154	Parameters Saved During Backup	137
<hr/>		Parameters, customizable	78
I		Parameters, Customizable	77
Idle Application	172	Pictures, as screensaver	165
IEEE 802.1D and 802.1Q	29	Ping and Traceroute	28

Port Utilization	42
Selection	42
Processing, General, for 9610 Restore	142
Processor Ethernet (PE)	77

Q

QoS	16, 29, 43
Administrative Parameters	16
IEEE 802.1Q	43
Qtest for Audio Quality	31

R

Realease 6.0	12
Registration and Authentication	37
Requirements	25, 26, 39
Call Server	39
Hardware	25
Server	26
Restore	139
Restore File, for 9610	140
Restore/Backup	134
Restrict Last Call Appearance administration	49
Retrieval Procedures, for 9610	141
RSVP	42

S

Screen Saver, Administering	128
Secure Shell Support	37
Security	36
Send All Calls (SAC) administration	49
Server Administration, DHCP	58
Server Requirements	26
Settings File	73
Shuffling	56
Signaling Protocol, changing	72
Smart Enbloc Dialing	116
SNMP	28
Softkeys, Administering Features on	120
Software	72
Software prerequisites	57
Software, Telephone	72
SRTP	31
SSON, Option 242, configuring	58
Station Form Administration Results Chart	51
Station Number Portability and IP Address Lists	31
Stopwatch timer, administering	162
Supplicant Operation, 802.1X	106
Switch Administration	41

Switch Compatibility and Aliasing IP Telephones	39
System Parameter Values, Impact of Received TLVs	108
System Parameters	47
System parameters, customizable	78
System Parameters, Customizable	77

T

Tagging and VLAN, administering	16
TCP/UDP Port Utilization	31
Telephone Administration	16, 47
Telephone and Call Server initialization	22
Telephone and File Server initialization	22
Telephone Initialization Process	21
Telephone to Network initialization	22
Time-to-Service (TTS)	38
Timer Operation	160
TLS	31
TLVs Received, Impact on System Parameter Values	108
Touchscreen Deskphones, Special Considerations for	55
Troubleshooting a 9610 IP Telephone	173

U

UDP Port Selection	42
UDP/TCP Port Utilization	31
Unnamed Registration	22
Upgrade Script and Application File, Choosing the Right	72
Upgrade Script File	73
USB Devices, Contacts File Format for	163
USB Devices, requirements for	163
USB Pictures	165
User stopwatch timer, administering	162

V

VLAN Considerations	100
VLAN Default Value	100
VLAN Detection	101
VLAN Separation Rules	102
VLAN Tagging	100
Voice-Initiated Dialing, Administering	114

W

What's changed	12
What's New	11
Wide Band Codecs	56
Wideband Audio administration	47
WML Application Display, on Home screen	154

