Administering Avaya one-X® Deskphone SIP for 9620/9620C/ 9620L/9630/9630G/9640/9640G/ 9650/9650C IP deskphones

Release 2.6.15
16-604083
Issue 9
Dec 2015

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this 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.

For the most current versions of documentation, go to the Avaya support Web site http://www.avaya.com/support and search for "one-X Deskphone SIP".

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for 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 of the time and we have no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. 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://www.avaya.com/support. Please note that if you acquired the product 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.

License

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE, 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, AND 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). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User’s request (see "Third-party Components" below for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and product(s) 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 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. 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 Avaya’s Web site at: http://www.avaya.com/support/Copyright.

T9 Text Input and other products are covered by one or more of the following patents: U.S. Pat. Nos. 5,187,480,5,818,437, 5,945,928, 5,953,541, 6,011,554, 6,286,064, 6,307,548, 6,307,549, and 6,636,162,6,646,573, 6,970,599; Australia Pat. Nos. 727539, 746674, 747901; Austria Pat. Nos. AT225534, AT221222; Brazil P.I. No. 9609807-4; Canada Pat. Nos. 1,331,057, 2,227,904,2,278,549, 2,302,595; Japan Pat. Nos. 3532780, 3492981; United Kingdom Pat. No. 2238414B; Hong Kong Standard Pat. No. HK1010924; Republic of Singapore Pat. Nos. 51383, 66959, 71979; European Pat. Nos. 1 010 057 (98903671.0), 1 018 069 (98950708.2); Republic of Korea Pat. Nos. KR201211B1, KR226206B1, 402252; People's Republic of China Pat. No. ZL96196739.0; Mexico Pat. Nos. 208141, 216023, 218409; Russian Federation Pat. Nos. 2206118, 2214620, 2221268; additional patent applications are pending.

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 telecommunication services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call the 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 Web site: http://www.avaya.com/support. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support.

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://www.avaya.com/support.

Federal Communications Commission (FCC) Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are assigned 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.

Contents

Contents

Chapter 1: Introduction

Purpose

9600 Series IP Deskphones support either the SIP signaling protocol or the H.323 signaling protocol. This document covers the SIP administration for the following 9600 Series IP Deskphones only:

- 9620, 9620C, and 9620L
- 9630 and 9630G
- 9640 and 9640G
- 9650 and 9650C

These deskphones use DHCP to obtain dynamic IP addresses, HTTP to download new versions of software, and HTTP or HTTPS to download customized settings for the deskphones.

Important:

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

Intended audience

This document is intended for personnel who administer Avaya one-X® Deskphone SIP for 9600 Series IP Deskphones.

Document changes since last issue

Issue 7	This version of the document, revised and issued in February 2015, supports Avaya one-X® Deskphone SIP release 2.6.14 for the deskphone models: 9620C, 9620L, 9640, and 9640G.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at support.avaya.com.

Title	Description
Avaya one-X™ Deskphone SIP Installation and Maintenance Guide Release 2.6	Describes the installation procedures for SIP deskphones.
Avaya one-X® 9600 Series H.323 Deskphones Administrator Guide	Describes how to administer 9600 Series IP Deskphones using the H.323 protocol.
Avaya Aura® Session Manager Overview	Describes features of Avaya Aura® Session Manager.
Implementing Avaya Aura® Session Manager	Describes the installation procedures and initial administration information for Avaya Aura® Session Manager.
Upgrading Avaya Aura® Session Manager	Describes how to upgrade Avaya Aura® Session Manager to a new software release.
Administering Avaya Aura® Session Manager	Describes how to administer Avaya Aura® Session Manager using System Manager.
Maintaining and Troubleshooting Avaya Aura® Session Manager	Describes information for troubleshooting Avaya Aura® Session Manager, resolving alarms, replacing hardware, and alarm codes and event ID descriptions.
Avaya Aura® Session Manager Case Studies	Provides functionality of Avaya Aura® Session Manager in different scenarios.
Installing and Upgrading Avaya Aura® System Manager	Describes the installation procedures and initial administration information for Avaya Aura® System Manager.
Administering Avaya Aura® System Manager	Describes how to administer Aura® System Manager.

Support

Visit the Avaya Support website at support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to help answer questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Major differences between SIP-based and H.323-based 9600 Series IP Deskphones

Review this section if your administrative environment includes both SIP and H.323 signaling protocols for 9600 Series IP Deskphones.

- **General IP Telephony** - Two major protocols handle Voice over IP (VoIP) signaling, Session Initiation Protocol (SIP) and H.323. The two protocols provide connection control and call progress signaling, but in very different ways. These protocols can be used simultaneously over the same network, but in general, no endpoint supports both protocols at the same time. Neither protocol is necessarily superior, but each offers some unique advantages. SIP deskphones, for example, do not require centralized call servers, and can route calls when a URL identifies the destination. H.323 deskphones leverage the call server's presence into the potential availability of hundreds of telephone-related features that a standalone SIP deskphone cannot provide.
- **Signaling** - 9600 Series IP Deskphones ship from the factory with H.323 signaling. To use the SIP protocol, applicable H.323 9600 Series IP Deskphones must be appropriately converted and configured. See the *Avaya one-X ® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694) for detailed conversion/configuration information.
- **Avaya Aura Communication Manager release** - Only Communication Manager release 4.0 and later supports 9600 Series IP Deskphones.

  SIP release 2.6 and later works with Communication Manager release 6.0 and Session Manager release 6.0. SIP software release 2.6 works with Communication Manager 4.x or 5.x.

  SIP-based deskphones connects to Communication Manager on the trunk side through Avaya OSP (Outbound SIP Proxy) whereas H.323-based deskphones connects directly to Communication Manager.

  For a SIP-based deskphone that runs under Communication Manager release 5.0 and later the Extend Call feature is also available. The Intercom feature is available only on

Communication Manager release 5.1 and later. When you use Avaya Aura Session Manager, use Communication Manager release 5.2.1 or later.

- **Required Servers** - SIP-based deskphones use the following additional servers that H.323-based deskphones do not use:
  - SIP Proxy server (controller) - Avaya Aura® Session Manager (SM) provides.
  - Network Time server - That controls time-related parameters.
  - Presence server - That tracks contacts that have presence handle and shares presence information with compatible software in the Session Manager environment.

  These servers are not necessarily separate hardware units. Also, you can use the optional servers to manage survivability depending on the system specific configuration. Depending on your system configuration, these servers might require specific software versions. For more information about software versions, see Avaya Aura® Communication Manager Administration.
- **Backup/Restore** - 9600 Series H.323 IP Deskphones use HTTP to store backup files. 9600 Series IP Deskphones with the SIP protocol use the Personal Profile Manager (PPM) functionality within Avaya Aura® Session Manager for backup and restore functions.
- **Settings File & System Parameters** - Both SIP and H.323 9600 Series IP Deskphones (and 4600 Series IP Telephones) use the same settings file. Some of the same system parameters are used, however numerous SIP-specific parameters support SIP operation only. In H.323 9600 Series IP Deskphones, the parameters OPSTAT and APPSTAT control all user interface functions, whereas SIP deskphones use a separate parameter (for example ENABLE_CONTACTS, ENABLE_CALL_LOG) for each user interface function.
- **Language Support** - SIP deskphones support many of the same languages and fonts as H.323 deskphones but there are some differences. SIP deskphones support text entry in Hebrew or Korean while H.323 deskphones do not. Further, all SIP language files have **.xml** file extensions whereas H.323 language files have **.txt** file extensions.
- **SNMP & MIBs** - Although both SIP and H.323 deskphones support SNMP v2c and have custom Management Information Bases (MIBs) the MIBs for each protocol are formatted somewhat differently.
- **RSVP** - SIP deskphones do not use RSVP (Resource ReSerVation Protocol) software to provide real-time monitoring and historical data of audio quality for VoIP calls.
- **QoS** - Unlike H.323 deskphones, SIP deskphones do not use Avaya Aura® Communication Manager to set Quality of Service (QoS). The SIP deskphones use the parameters L2QAUD, L2QSIG, DSCPAUD, and DSCPSIG (described in SIP-based 9600 Series IP Deskphones customizable system parameters on page 86).
- **NAT** - SIP deskphones do not support Network Address Translation (NAT); H.323 deskphones do support NAT.
- **Direct Media** - Deskphone SIP now handles early direct media when originating a call with direct media over SIP trunks to a "Microsoft" SIP phone connected to Microsoft OCS.

- **Presence** - SIP deskphones support tracking of presence information for designated contacts. H.323 deskphones do not support presence tracking.

Chapter 2: Administration Overview and Requirements

About 9600 Series IP Deskphones

9600 Series IP Deskphones are shipped from the factory with the signaling protocol set to H.323. As a part of initialization during installation, the signaling protocol is changed to SIP. Post-installation, the deskphone automatically downloads the software upgrades using the proper signaling protocol.

The following table lists different SIP software versions that different 9600 Series IP Deskphones supports.

9600 Series IP Deskphones	Latest supported software release
• 9620,9620C, and 9620L • 9630 and 9630G • 9640 and 9640G • 9650 and 9650C	2.6.14
9601, 9608, 9608G, 9611G, 9621G, and 9641G	6.5

9600 Series IP Deskphones support Media Encryption (SRTP) and use built-in Avaya SIP Certificates for trust management. Trust management involves downloading certificates for additional trusted Certificate Authorities (CA) and the policy management of those CAs. Identity management is handled by Simple Certificate Enrollment Protocol (SCEP) with phone certificates and private keys.

9600 Series IP Deskphones Release 2.6.13 and later do not support SIP Enablement Services.

Administrative requirements

The conditions under which 9600 Series IP Deskphones need to operate are summarized as follows:

- Telephone Administration on the Communication Manager (CM) call server, as covered in Chapter 4: Avaya Aura® Communication Manager Administration.

- IP Address management for the deskphone. For static addressing, see the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
- Tagging Control and VLAN administration for the deskphone, if appropriate, as covered in Chapter 9: Administering Deskphone Options.
- Quality of Service (QoS) administration for the deskphone, if appropriate. QoS is covered in QoS on page 38 and Administering QoS on page 48.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP).
- Interface administration for the deskphone, as appropriate. Administer the deskphone to LAN interface using the PHY1STAT parameter described in Chapter 3: Network Requirements. Administer the deskphone to a computer interface using the PHY2STAT parameter described in *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
- Application-specific deskphone administration, if appropriate, as described in Chapter 9: Administering Deskphone Options. An example of application-specific data is Web-specific information required for the optional Web browser application. Note that optional Web browser capabilities are not available for the four deskphone models covered by this release.

Administration alternatives and options indicates that you can administer system configuration parameters in a variety of ways and use the following administrative mechanisms:

- Maintaining the information on the call server.
- Manually entering the information by means of the deskphone dialpad using Craft (local administrative) procedures. Craft procedures are described in "Chapter 3: Local Administrative Options" in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
- 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 administrative mechanisms. See the applicable chapters in this guide for specific information.

Administration alternatives and options

General information about administering DHCP servers is covered in Administering the DHCP

Parameter(s)	Administrative mechanisms	Refer
Telephone Administration	Avaya Communication Manager and SES/ SM (and System Manager for multiple SMs if applicable)	Chapter 4: Avaya Aura® Communication Manager Administration, Chapter 7: Server Administration, and Appendix B: Countries With Specific Network Progress Tones. For SES/Session Manager/System Manager administration, see Chapter 6: Administering Avaya Aura® Session Manager, and System Manager (SM) and the product-related documents available on the Avaya support site.
IP Addresses	DHCP (strongly recommended)	Administering the DHCP and File Servers on page 65, and especially Administering the DHCP Server on page 66.
	Settings file	Chapter 8: Deskphone Software and Application Files and Chapter 9: Administering Deskphone Options.
	Manual administration at the deskphone	“Static Addressing Installation” in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 127.
Tagging and VLAN	LLDP	About Link Layer Discovery Protocol (LLDP) on page 127.
	DHCP	Administering the DHCP Server on page 66, and Chapter 9: Administering Deskphone Options.
	Settings file	Administering the DHCP and File Servers on page 65 and Chapter 9: Administering Deskphone Options.
	Manual administration at the deskphone	“Static Addressing Installation” in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
Network Time Server (NTS)	DHCP Settings file	Administering the DHCP Server on page 66 and Network Time Protocol (NTP) server on page 33.

Parameter(s)	Administrative mechanisms	Refer
Quality of Service	Settings file	Chapter 9: Administering Deskphone Options.
Interface	DHCP	Administering the DHCP and File Servers on page 65, and Chapter 8: Deskphone Software and Application Files.
	Settings file	Administering the DHCP and File Servers on page 65, and Chapter 8: Deskphone Software and Application Files.
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 127.
	Manual administration at the deskphone	"Secondary Ethernet Interface Enable/ Disable" in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
Application - specific parameters	DHCP	Administering the DHCP and File Servers on page 65, and especially Administering the DHCP Server on page 66. Also, Chapter 9: Administering Deskphone Options.
	Settings file (strongly recommended)	Administering the DHCP and File Servers on page 65, and especially HTTP Generic Setup on page 72. Also, Chapter 9: Administering Deskphone Options.

and File Servers on page 65, and more specifically, Administering the DHCP Server on page 66. General information about administering HTTP servers is covered in Administering the DHCP and File Servers, and more specifically, HTTP Generic Setup. Once you are familiar with that material, you can administer deskphone options as described in Chapter 9: Administering Deskphone Options.

About parameter data precedence

As shown in Administration alternatives and options, you can administer a given parameter through various methods. However, deskphones apply the settings based on the precedence of the method. If you apply the same setting through two different methods, the one with the high precedence overwrites the one with the lower precedence Refer the following list to see the order of precedence, from highest to lowest, in which deskphones apply the settings:

1. Manual administration, unless the system parameter USE_DHCP is set to 1 (Get IP Address automatically by DHCP), or backup file data obtained through PPM.

2. Personal Profile Manager (PPM) through SM.
3. 46xxsettings.txt settings file.

   Important:
   Set failover parameters in the settings file and not in SM.

4. DHCP, except as indicated in DHCPACK setting of parameter values
5. LLDP, except for setting the call server and file server IP addresses, for which it has the lowest precedence.

   Note:

   The only exception to this sequence is in the case of VLAN IDs. In the case of VLAN IDs, LLDP settings of VLAN IDs are the absolute authority. Then the usual sequence applies. For the L2QVLAN and L2Q system values, LLDP settings of VLAN IDs are the absolute authority only if the LLDP task receives the VLAN IDs before DHCP, and the DHCP client of the deskphone is activated. If the LLDP task receives the VLAN IDs after DHCP negotiation, several criteria must be successful before the deskphone accepts VLAN IDs from LLDP. For more information, see About Link Layer Discovery Protocol (LLDP) on page 127.

Configured controllers precedence and controller priority

The "list of Configured Controllers" is the aggregation of, in (highest to lowest) precedence order:

1. Controllers entered using a Craft (local administrative) procedure.
2. Controllers delivered by PPM (sipServer in the getHomeServerResponse and proxy "ServiceName" in the getHomeCapabilitiesResponse). SipServer has the highest precedence. The proxy(s) are the next highest precedence. When communicating with a controller delivered by PPM, the phone uses the most secure/reliable transport supported by that controller. The controllers delivered by PPM are ignored if the ENABLE_PPM_SOURCED_SIPPROXYSRVR parameter value is 0.
3. Controllers in the settings file parameter SIP_CONTROLLER_LIST. The first element of the parameter has the highest precedence within the parameter.
4. Controllers in the DHCP option 242 parameter SIP_CONTROLLER_LIST. The first element of the parameter has the highest precedence within the parameter.

The ordering of the list of Configured Controllers defines the priority of the controllers; the first element of the list is the highest priority, the last element is the lowest priority. The phone removes any (duplicate) entries in the list of Configured Controllers that have an identical server IP address or DNS name regardless of the specified transport type and/or port number.

Administrative tasks

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

1. Avaya Communication Manager (4.0 or greater) administered for 9600 Series IP Deskphones. Administer 9600 Series IP Deskphones running under CM 4.0 with the 4620SIP station type; administer 9600 Series IP Deskphones running later versions of CM as 96*xx*SIP, where *xx* represents the model (for example, 9620SIP, 9630SIP, etc.).
2. SM (Session Manager, 5.2 or greater) administered. Avaya Aura® System Manager must also be administered for multiple SM environments. See Supported SIP environments on page 45 for information. SIP software Release has not been tested with CM5.2 and SM 5.2.
3. LAN and applicable servers (file servers, Network Time server) administered to accept the deskphones.
4. Telephone software downloaded from the Avaya support site.
5. 46xxsettings file updated with site-specific and SIP-specific information, as applicable.
6. 9600 Series IP Deskphones installed. For more information, see the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
7. Individual SIP deskphones updated using Craft procedures, as applicable. For more information, see “Local Administrative Procedures” in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
8. Survivability administration to set up the local SIP gateway and administer additional controllers in the settings file as applicable. Certain gateway configurations require Session Manager 6.0 and Avaya Communication Manager 6.0.

Administrative checklist

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

Note:

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

	Task	Description	Refer
1.	Network Requirements Assessment	Determine that network hardware is in place and can handle deskphone system requirements.	Chapter 3: Network Requirements.
2.	Administer Avaya Aura® Communication Manager	Verify that the call server has a valid license file and is administered for Voice over IP (VoIP). Verify the individual deskphones are administered appropriately on the CM station forms.	Chapter 4: Avaya Aura® Communication Manager Administration. Chapter 4: Avaya Aura® Communication Manager Administration.
3.	Administer the Proxy Server	Administer for Avaya Aura® Session Manager (SM).	*Administering Avaya Aura® Session Manager* (Document Number 03-603324), available on the Avaya support website, http://support.avaya.com. Chapter 6: Administering Avaya Aura® Session Manager, and System Manager (SM).
4.	Administer Avaya Aura® System Manager	Administer for environments using multiple Session Managers.	Chapter 6: Administering Avaya Aura® Session Manager, and System Manager (SM).
5.	DHCP server installation	Install a DHCP application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
6.	Administer DHCP application	Add IP deskphone administration to the DHCP application.	Administering the DHCP Server in Chapter 7: Server Administration.
7.	Administer Network Time Server	Set value(s) for Simple Network Time Protocol (SNTP)	Option 42 under DHCP Generic Setup.
8.	HTTP/HTTPS server installation	Install an HTTP/HTTPS application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
9.	SIP Software Distribution Package and 46xxsettings file installation on HTTP/ HTTPS server	Download the files from the Avaya support site.	http://support.avaya.com Chapter 8: Deskphone Software and Application Files.

	Task	Description	Refer
10	Administer WML servers	Add WML content as applicable to new or existing WML servers. Administer push content as applicable.	*Avaya one-X® Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-600888).
11.	Modify settings file as needed	Edit the settings file as necessary for your environment, using your own tools.	Chapter 8: Deskphone Software and Application Files.
12.	Administer deskphones locally as applicable	As a Group:	Using the GROUP parameter to set up customized groups on page 83 and the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
		Individually:	The applicable Craft Local Procedures in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
	Installation of deskphones in the network		*Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).
	Allow user to modify Options, if applicable	Set the following parameters in the settings file: ENABLE_CALL_LOG ENABLE_CONTACTS ENABLE_MODIFY_CONTACTS ENABLE_PHONE_LOCK PROVIDE_EDITED_DIALING PROVIDE_LOGOUT PROVIDE_NETWORKINFO_SCREEN PROVIDE_OPTIONS_SCREEN PROVIDE_EXCHANGE_CALENDAR	

Setting up Primary and Secondary Controllers

The minimal settings required for provisioning SIP Proxies are:

- SIPDOMAIN: The domain name that the phones operate in. All proxies are assumed to support the same domain.
- SIP_CONTROLLER_LIST: Configured Controller list. A comma-separated list of SIP controller designators, without any intervening spaces, where each controller designator has the following format:
  host[:port][;transport=xxx]

where, host is an IP address in dotted-decimal (DNS name format is not supported).

[:port] is an optional port number.

[;transport=xxx] is an optional transport type where xxx can be tls, tcp, or udp.

If a port number is not specified a default value of 5060 for TCP and UDP or 5061 for TLS is used.

If a transport type is not specified, a default value of tls is used.

The value can contain 0 to 255 characters; the default value is null ("").

If null, DHCP/DNS will provide the defaults.

Example:

```
SET SIP_CONTROLLER_LIST
  proxy1:5060;transport=tcp,proxy2:5060;transport=tcp
```

SIP_CONTROLLER_LIST (setting through Windows DHCP server) -

In DHCP scope option set as

```
SIP_CONTROLLER_LIST="Proxy1:<port>;transport=xxx,Proxy2:<port>;tran
  sport=yyy"
```

Where: Proxy1 is the primary SIP server address and Proxy2 is the secondary SIP server address. And xxx and yyy are the transport protocols of respective server.

OR:

```
SIP_CONTROLLER_LIST="Proxy1,Proxy2:<port>;transport=xxx"
```

In the later case, the first controller will take default port (5061) and transport type (TLS) and second controller will take assigned values in the SIP_CONTROLLER_LIST.

SIP_CONTROLLER_LIST (setting through Linux DHCP server (httpd.conf) -

In the following examples Proxy1 is the primary SIP server address and Proxy2 is the secondary SIP server address. And xxx and yyy are the transport protocols of respective server.

For Linux, we would have to use '\' as an escape character for quoting the value inside the already quoted name = value pair.

Example: When using single SIP CONTROLLER

```
"HTTPSRVR=aaa.aaa.aaa.aaa,SIP_CONTROLLER_LIST=\
 "xxx.xxx.xxx.xxx:5060;transport=tcp\"";
```

When using Multiple SIP CONTROLLERs, please follow below examples

```
"HTTPSRVR=aaa.aaa.aaa.aaa,SIP_CONTROLLER_LIST=\
 "xxx.xxx.xxx.xxx:5060;transport=tcp,yyy.yyy.yyy.yyy:5060;transpor
 t=tcp\"";
```

Note:

When viewing the SIP proxy list from the Craft menu, it may contain additional proxies obtained from other data sources which cannot be deleted through the Craft menu. Only proxies entered through the Craft menu can be deleted.

Further settings are optional:

CONFIG_SERVER_SECURE_MODE - When the phone is using HTTPS to communicate with PPM, it reuses the HTTP connection. This parameter applies only to 96xx model phones. The following values specifies the communication mode that the deskphone uses to access the configuration server.

- 0 to use HTTP
- 1 to use HTTPS, which is default
- 2 to use HTTPS if SIP transport mode is TLS, else use HTTP

Note:

Default value is 1 in SIP 2.6 and 0 in SIP 2.5 release.

DISCOVER_AVAYA_ENVIRONMENT - Indicates how server support for Avaya SIP Telephony (AST) capabilities will be determined. The default setting is "1" (AUTO), which means that the support for AST will be determined automatically. Setting DISCOVER_AVAYA_ENVIRONMENT to "0" (NO) means that the SIP proxy server does not support AST.

FAILBACK_POLICY - This is a string 'admin' or 'auto'. When set to 'auto' (the default), if the phones detect that a disabled primary server has recovered, they will attempt to register to the highest priority available controller in the SIP proxy server list, and will stop using the Secondary. If set to 'admin', the phones will never autonomously attempt to leave a working server. Admin failback needs to be invoked from the system manager for that particular user. Please leave this parameter to its default value i.e. 'Auto'.

RDS_INITIAL_RETRY_TIME - Parameter that indicates the initial delay for a retry for connecting to the PPM server. The default value is 2 seconds and provisioning is through the settings file and can be set in the range of 2 to 60 seconds.

RDS_MAX_RETRY_TIME - Parameter that indicates the maximum delay interval before giving up on connecting to the PPM server. The default value is 600 seconds and provisioning is through the settings file and can be set in the range of 2 to 3600 seconds.

RDS_INITIAL_RETRY_ATTEMPT - Parameter that indicates how many times PPM adaptor should try to download from PPM before giving up on connecting to the PPM server. The default value is 15 attempts and provisioning is through the settings file and can be set in the range of 1 to 30 attempts.

SIPREGPROXYPOLICY - This is a string, 'alternate' or 'simultaneous'. If set to 'alternate' (the default), the phones will only register to one server at a time. If set to 'simultaneous', the phones will maintain an active registration on all provisioned servers which is only supported for SM environment.

- For SM environment, use simultaneous.

  Note:

  From 2.6 onwards the default value if CONFIG_SERVER_SECURE_MODE is 1 indicating that PPM download will happen over HTTPS.

100REL_SUPPORT - If we set 100REL_SUPPORT 0 then phone doesn't 100rel in Supported header and so in case of any 18x response phone doesn't respond with PRACK. So this disables the reliable response capability on the phone. When we set it to default value as 1, then phone sends 100rel in Supported header and responds any 18x response with PRACK.

ASTCONFIRMATION - Sets the time that the phone waits to validate an active subscription when it subscribes to the "avaya-cm-feature-status" package. The range is from 16-3600 seconds. The default value for ASTCONFIRMATION is 32 seconds for 2.6 and above.

SIMULTANEOUS_REGISTRATIONS - The number of Session Managers in the configuration that the phone will simultaneously register with. The range is from 1-3. The default value for SIMULTANEOUS_REGISTRATIONS 3 for 2.6 and above.

ENFORCE_SIPS_URI - Controls the enforcement of SIPS URI with SRTP. The range is from 0-1. The default value for ENFORCE SIPS URI is 1 for 2.6 and above releases.

SDPCAPNEG - Controls the SDP capability negotiation. The range is from 0-1. The default value for this SDP CAP NEG is 1 for 2.6 and 0 for 2.5 releases respectively.## SET SDPCAPNEG 1.

CONTROLLER_SEARCH_INTERVAL - For Deskphone SIP 2.6 SP3 and above, we recommend that the value of CONTROLLER_SEARCH_INTERVAL should be set to 16.

Invalid Proxy Settings

If an invalid proxy server address is programmed on the phone (via the administration screen, accessed through Craft procedures, or via the settings file) and a login is attempted and cancelled, rebooting the phone is not sufficient to recover as the phone will continue to attempt to contact the invalid proxy.

Procedure for erasing an invalid proxy server address: During the re-boot sequence, press the "Program" soft key to present the CRAFT menu, select the CLEAR option to clear the phone values and reboot the phone. The valid proxy values can be re-programmed by adding them to

the settings file before the reboot, or through phone programming from the CRAFT menu during the boot.

Deskphone Initialization Process Overview

These steps offer a high-level description of the information exchanged when the deskphone initializes and registers. This description assumes that all equipment is properly administered ahead of time. The *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694) provides a detailed description of initialization (power-up and reset).

Step 1: Accessing the network

The deskphone is appropriately installed and powered. After a short initialization process, the deskphone 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 65. Among other data passed to the deskphone is the IP Address of the HTTP or HTTPS server.

Step 3: Downloading files

9600 Series IP Deskphones can download configuration files, certificate files, and language 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. Chapter 8: Deskphone Software and Application Files.

Note:

The deskphones use the HTTP GET message to download the files from the specified URL. The maximum length allowed for the GET URL file name length is 31 characters.

Step 4: Registering with the SIP proxy server

In this step, the deskphone might prompt the user for an extension and password. The deskphone uses that information to exchange a series of messages with SM, which in turn communicates with Avaya Communication Manager (CM). For a new installation and for full service, the user can enter the deskphone extension and SM password. For a restart of an existing installation, this information is already stored on the deskphone, but the user might have to confirm that information. The expected result is that the deskphone is appropriately registered and call server data such as feature button assignments are downloaded.

Important:

For Session Manager, the user name takes the canonical address format that uniquely identifies a user across all Enterprise sites; see the white paper titled *Avaya Aura® 6.0 Configuration for Presence and IM* on the Avaya support Web site.

For more information about the installation process, see the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).

Error conditions

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

The Avaya one-X™ Deskphone SIP Installation and Maintenance Guide (Document Number 16-601943) covers possible operational problems that might be encountered after successful installation. The User Guides for a specific deskphone model also contain guidance for users having problems with specific IP deskphone 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 for all applications:

- SIP,
- DHCP, and
- HTTP/HTTPS.

Also, QoS support is required to run VoIP on your configuration. For more information, see Administering TCP/UDP port selection on page 39 and the QoS parameters L2QAUD, L2QSIG, DSCPAUD, and DSCPSIG in SIP-based 9600 Series IP Deskphones customizable system parameters on page 86

Hardware requirements

To operate properly, you need:

- Category 5e cables designed to the IEEE 802.3af-2003 standard, for LAN powering,
- TN2602 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 the increased capacity.
- TN799C or D Control-LAN (C-LAN) circuit pack.

Important:

This and earlier software releases require TN799C V3 or greater C-LAN circuit pack(s). For more information, see the *Avaya Aura® Communication Manager Software and Firmware Compatibility Matrix* on the Avaya support Web site http://support.avaya.com.

To ensure that the appropriate circuit pack(s) are administered on your Communication Manager call server, see Chapter 4: Avaya Aura® Communication Manager Administration. For more information about hardware requirements in general, see the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).

Server requirements

The following server types can be configured for the 9600 Series IP Deskphones:

- DHCP server
- HTTP or HTTPS server
- SIP Proxy (controller) or Registration server
- Network Time Protocol server for SNTP
- Alternate Session Manager for reliability
- SM SIP Proxy Server (controller) to be used as a gateway for survivability
- System Manager
- Communication Manager
- Presence server
- Web server (optional)
- Branch Session Manager for Geo redundancy
- Third party gateway, for example, Audiocodes and Teldata

Note:

9600 Series IP Deskphones need Avaya Aura® Session Manager (SM) to work properly. The SIP Proxy and Registration servers reside on the SM server. Avaya Aura® Communication Manager (CM) is considered a “feature server” behind SM that provides Outboard Proxy SIP (OPS) features.

While the servers listed provide different functions that relate to 9600 Series IP Deskphones, they are not necessarily different boxes. For example, DHCP provides network information whereas HTTP provides configuration and application file management, yet both functions can co-exist on one hardware unit. Any standards-based server is recommended.

For parameters related to Avaya Communication Manager information, see Chapter 4: Avaya Aura® Communication Manager Administration. For parameters related to DHCP and file servers, see Chapter 7: Server Administration.

Important:

The deskphones obtain important information from the upgrade files on the server(s) and depend on the application file for software upgrades. If these servers are unavailable when the deskphones reset, the deskphones will not operate properly. Some features might not be available. To restore them you need to reset the deskphones when the file server is available.

DHCP server

Avaya recommends that a DHCP server be installed and that static addressing be avoided. Install the DHCP server and application as described in Administering the DHCP and File Servers on page 65.

HTTP/HTTPS server

Administer the HTTP or HTTPS file server as described in HTTP Generic Setup on page 72.

Network Time Protocol (NTP) server

SIP IP deskphones require NTP server support to set the time and date, used in system log time stamps and other time/date functions. The NTP server is typically needed by one or more servers within the enterprise. Administration of the NTP server is beyond the scope of this document.

Presence server

The connection to the presence server requires Transport Layer Security (TLS).

The following standards and guidelines provide information on how the system manages presence:

- By using the following SIP/SIMPLE RFCs:
  - RFC 3863 *Presence Information Data Format*
  - RFC 4479 *A Data Model for Presence*
  - RFC 4480 *RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)*.
- By using the subscription to the SIP resource list event package, which are as follows:
  - RFC 4662 - A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists.
  - If a deskphone subscribes to the Presence.winfo and Resource.list events, the deskphone accepts the following presence information and then passes this information to the user interface for further processing: unknown, onhook, on-a-call, do-not-disturb, on-a-conference, and Away.

- If you have set the PRESENCE_SERVER parameter to an IP address, the deskphone replaces the domain on the Request-URI header of any outbound presence-related messages with this IP address. The To header remains intact in the form user@domain.tld.
- Support for configuration of a port number for the presence server. If you specify the port number, the presence server can run multiple SIP servers on a single host and can achieve the target scale of 20,000 users (and approximately 60,000 communication addresses, 10 presence changes and 10 messages per user per hour).

For more information on how the deskphone handles presence messages in a Session Manager environment, see About Presence on page 139.

Web and Push servers (optional)

If users have access to corporate WML Web sites, administer the telephones as described in Chapter 7: Server Administration.

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:

The following changes must be done for R2.5 and later for enabling PUSH functionality on the phone.

- The string representing the trusted server list, specified in TPSLIST, should contain a server specification that completely matches the server specified in the push URI.

  Example: If the push URI is: http://192.168.12.63:80/display.wml then the TPSLIST should contain 192.168.12.63:80 that is it includes the port number.

Your Web and push server configuration must be compatible with the requirements covered in the *9600 Series IP Telephone Application Programmer Interface (API) Guide*.

Required network information

Before you administer DHCP and HTTP/HTTPS, as applicable, complete the information in Required network information before installation - per DHCP server. If you have more than one router, HTTP/TLS server and subnetwork mask in your configuration, provide the information for each DHCP server.

9600 Series IP Deskphones support specifying a list of IP Addresses for a gateway/router and the 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 application, only 127 characters might be supported.

When specifying IP Addresses for the file server, use either dotted decimal format (“xxx.xxx.xxx.xxx”) or DNS names. If you use DNS, the system value DOMAIN is appended to the IP Addresses you specify. If DOMAIN is null, the DNS names must be fully qualified. For more information about DNS, see DHCP Generic Setup on page 68 and About DNS addressing on page 124.

Required network information before installation - per DHCP server

1.	Gateway (router) IP Address(es)
2.	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)
3.	Subnetwork mask
4.	HTTP server file path (HTTPDIR)
5.	Telephone IP Address range *From*: *To*:
6.	DNS server address(es) if applicable

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

- Administering the DHCP server as described in Chapter 7: Server Administration.
- Editing the configuration file on the applicable HTTP or HTTPS file server, as covered in Choosing the right application file and upgrade script file.

Other network considerations

Enabling SNMP

9600 Series IP Deskphoness are fully compatible with SNMPv2c and with Structure of Management Information Version 2 (SMIv2). The deskphones respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. The deskphones 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 deskphone accepts SNMP queries with the SNMPADD parameter. You can also customize your community string with the SNMPSTRING parameter. For more information, see Chapter 7: Server Administration.

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: http://www.ietf.org/.

The Avaya Custom MIB for 9600 Series IP Deskphones is available for download in *.txt format on the Avaya support website at http://support.avaya.com.

Note:

Each SIP software release has a different MIB. Ensure that you download the MIB applicable to your environment.

Registration and authentication

9600 Series IP Deskphones require a SIP outbound proxy server (OPS) extension on Avaya Communication Manager and a login and password on the SM server to register and authenticate it.

Important:

For Session Manager, the user name takes the canonical address format that uniquely identifies a user across all Enterprise sites; as described in the white paper titled *Avaya Aura® 6.0 Configuration for Presence and IM* on the Avaya support Web site.

Registration is described in the Initialization process, in Step 4: Registering with the SIP proxy server on page 29. For further information, see *Maintaining and Troubleshooting Avaya Aura® Session Manager* (03-603325), available on the Avaya support website, http://www.avaya.com/support and your call server administration manual.

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. 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 the HTTP/HTTPS server is not available for any reason after a telephone restart.

IP Address reuse was added in SIP software Release 2.5 to prevent infinite looping when separate VLAN servers are used for voice and data VLANs, and a response is received from the DHCP server on the data VLAN, but not on the voice VLAN.

Unless otherwise indicated, the values described here during IP address reuse are internally provisioned or set by the process itself and not by manual administration.

- Routers in Use - The system sets the ROUTER_IN_USE parameter to REUSE_ROUTER_IN_USE if:
  - The routers that you specify in the ROUTER parameter through DHCP Option 3 or through local administrative procedure do not send any response.
  - The value of REUSE parameter is 1.

  The system internally sets the values of all router-related parameters, except for the ROUTER parameter.
- VLAN Check - During the VLAN check, if a reset is to be done and VLAN_IN_USE is not zero, VLAN_IN_USE will be added to VLANLIST if it is not already on VLANLIST.

  The VLAN detection process described in Automatically detecting a VLAN on page 121 is followed if tagging is off or if tagging is on and L2QVLAN is > 0, and if REUSETIME > 0, and if REUSE_IPADD is not “0.0.0.0”. If VLANTEST expires, the value of VLAN_IN_USE is added to VLANLIST if it is not already on VLANLIST.

  If a DHCPOFFER is not received within REUSETIME seconds, or if a DHCPOFFER is received that contains a value of L2QVLAN that is on VLANLIST, REUSE will be set to 1, IPADD will be set to the value of REUSE_IPADD, NETMASK will be set to the value of REUSE_NETMASK, ROUTER will be set to the value of REUSE_ROUTERS, and if the value of REUSE_TAGGING is 1, 802.1Q tagging will be turned on with a VLAN ID equal to the value of L2QVLAN_INIT. DHCP will then enter the “extended” REBINDING state, and operation will proceed as normal.

  After a successful registration, the following system values are set:

- REUSE_IPADD will be set to the value of IPADD
- REUSE_NETMASK will be set to the value of NETMASK
- REUSE_ROUTERS will be set to the value of ROUTER
- REUSE_ROUTER_IN_USE will be set to the value of ROUTER_IN_USE
- REUSE_TAGGING will be set to the value of TAGGING
- L2QVLAN_INIT will be set to the value of VLAN_IN_USE

- the MIB object endptVLANLIST will be set to the value of VLANLIST and then the value of VLANLIST will be set to null

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 48 for QoS implications for 9600 Series IP Deskphones.

All 9600 Series IP Deskphones provide some detail about network audio quality. For more information see, Displaying network audio quality on page 38.

IEEE 802.1D and 802.1Q

For more information about IEEE 802.1D and IEEE 802.1Q and 9600 Series IP Deskphones, see Administering IEEE 802.1D and 802.1Q on page 48 and Administering a VLAN on page 120. 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.

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

Note:

Priority 0 is a higher priority than Priority 1.

Displaying network audio quality

All SIP-based 9600 Series IP Deskphones provides the feature to monitor network audio performance while you are on a call. The Network Information screen displays this information. Gain access to the Network Information screen from the Avaya (A) Menu and select the Network Information option directly. While on a call, the deskphones display network audio quality parameters in real-time, as shown in Parameters in real-time:

Parameters in real-time

Parameter	Possible Values
Received Audio Coding	G.711, G.722, G.726A, 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 audio data in each RTP packet.
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 deskphone.

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.

SIP station number portability

9600 Series IP Deskphones provide station number portability For both SEs and SM environments. With proper administration, upon startup or a reboot at a remote location within a corporate network, the deskphone establishes communication with its home server based on the User Name and Password. For mobile users, registration redirection occurs automatically.

Administering TCP/UDP port selection

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. Depending on your network, you might need to know what ports or ranges are used in the operation of 9600 Series IP Deskphones. 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 Received packets (destination = SIP deskphone) and Transmitted packets (source = SIP Deskphone) refer to configuration parameters or options settings. For more information about parameters and settings, see Administering options for the 9620, 9620C, 9620L, 9630, 9630G, 9640, 9640G, 9650, and 9650C SIP Deskphones.

Received packets (destination = SIP deskphone)

Destination Port	Source Port	Use	UDP or TCP
The number used in the Source Port field of the DNS query sent by the deskphone	Any	Received DNS messages	UDP
The number used in the Source Port field of the packets sent by the deskphone's HTTP client	Any	Packets received by the deskphone's HTTP client	TCP
The number used in the Source Port field of the TLS/SSL packets sent by the deskphone's HTTP client	Any	TLS/SSL packets received by the deskphone's HTTP client	TCP
68	Any	Received DHCP messages	UDP
The number used in the Source Port field of the SNTP query sent by the deskphone	Any	Received SNTP messages	UDP
161	Any	Received SNMP messages	UDP
50000	Any	Received CNA test request messages	UDP
The number used in the Source Port field of registration messages sent by the deskphone's CNA Agent	Any	Received CNA registration messages	TCP
PORTAUD or the port number reserved for CNA RTP tests	Any	Received RTP and SRTP packets	UDP

1 of 2

Destination Port	Source Port	Use	UDP or TCP
PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd) or the port number reserved for CNA RTP tests plus or minus one, as for PORTAUD, above	Any	Received RTCP and SRTCP packets	UDP
If signaling is initiated by the deskphone = the number used in the Source Port field of the signaling packets sent by the deskphone If signaling is initiated by the server = System-Specific	Any	Received signaling protocol packets	UDP/TCP

2 of 2

Transmitted packets (source = SIP Deskphone)

Destination Port	Source Port	Use	UDP or TCP
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
80 unless explicitly specified otherwise (i.e. in a URL)	Any unused port number	Packets transmitted by the deskphone's HTTP client	TCP
123	Any unused port number	Transmitted SNTP messages	UDP
The number used in the Source Port field of the SNMP query packet received by the deskphone	161	Transmitted SNMP messages	UDP
443 unless explicitly specified otherwise (i.e. in a URL)	Any unused port number	TLS/SSL packets transmitted by the deskphone's HTTP client	TCP
514	Any unused port number	Transmitted Syslog messages	UDP
CNAPORT	Any otherwise unused port number	Transmitted CNA registration messages	TCP
The port number specified in the test request message	50000	Transmitted CNA test results messages	UDP
System-specific	Any unused port number	Transmitted signaling protocol packets	TCP
FEPORT or the port number specified in a CNA RTP test request	PORTAUD, which must be in the range specified by the RTP_PORT_LOW and RTP_PORT_RANGE parameters or the port number reserved for CNA RTP tests	Transmitted RTP and SRTP packets	UDP

Destination Port	Source Port	Use	UDP or TCP
FEPORT + 1 (if FEPORT is even) or FEPORT -1 (if FEPORT is odd) or the port number specified in a CNA RTP test request plus or minus one, as with FEPORT above	PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd) or the port number reserved for CNA RTP tests plus or minus one, as for PORTAUD, above	RTCP and SRTCP packets transmitted to the far-end of the audio connection	UDP
RTCPMONPORT	PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd)	RTCP packets transmitted to an RTCP monitor	UDP
System-specific	Any unused port number	Transmitted signaling protocol packets	UDP

2 of 2

Security

For security and protection of the privacy of a user, Avaya one-X® Deskphone SIP provides function to lock a deskphone and to logout from the deskphone. When a user locks the deskphone, no one can unlock the deskphone without the assigned password for the particular user. While in a locked state, a user can only make emergency calls using the deskphone. You cannot gain access to any data when the deskphone is in a locked state.

When a user logs out from the deskphone, the deskphone is available for other users to use. However, when another user logs in to the same deskphone using designated extension and password, the user cannot gain access to the data of any other user who used the same deskphone. For example, suppose user A and user B use the same deskphone. When user A logs out of the deskphone, user B logs in. When user B logs in, user B cannot gain access to any record of user A, for example: contacts, call records, on the deskphone.

Important:

You can gain access to certain administrative procedures from the deskphone through the CRAFT menu. You must change the default password for the CRAFT menu to restrict users from using the administrative procedures to change the deskphone configuration.

To enhance security, Avaya one-X® Deskphone SIP support Transport Layer Security (TLS) for signaling and Secure Real-time Transport Protocol (SRTP) for secure communications. This standard allows the deskphone to establish a secure connection to a HTTPS server, in which the upgrade and settings file can reside. This setup adds security over another alternative.

SRTP provides confidentiality and also message authentication to media traffic going over the LAN infrastructure. This allows the deskphones to encrypt the calls between two or more endpoints, to restrict anyone from eavesdropping. To correctly use SRTP, you must correctly configure the various components within the network. For the 9600 Series IP Deskphones to function with SRTP, you must configure the equivalent parameters in Communication Manager or System Manager. You must configure the following three parameters on 9600 Series IP Deskphones and the equivalent Communication Manager parameters must match:

SET ENFORCE_SIPS_URI 1

SET SDPCAPNEG 1

SET MEDIAENCRYPTION X,9 or

SET MEDIAENCRYPTION X (where X is a value from 1 to 8)

Communications between the SIP deskphone and the Personal Profile Manager (PPM) is secure by default as the default value of the CONFIG_SERVER_SECURE_MODE parameter is 1, which indicates that deskphone downloads PPM over HTTPS.

For information about toll fraud, see the respective call server documents on the Avaya support website. 9600 Series IP Deskphones cannot guarantee resistance to all Denial of Service attacks. However, checks and protections resist such attacks while maintaining appropriate service to legitimate users.

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 Chapter 7: Server Administration and include:

- Depending on the SIP_CONTROLLER_LIST parameter, supporting signaling channel encryption with appropriately administered Avaya Communication Manager.
- Restricting the response of 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 deskphone sends.
- Restricting dialpad access to Craft Local Procedures to experienced installers and technicians and requiring password entry to access Craft procedures.
- Restricting the end user's ability to use a deskphone Options application to view network data.

Chapter 4: Avaya Aura® Communication Manager Administration

Call server requirements

Avaya Communication Manager (CM) extends advanced telephony features to SIP deskphones via Outboard Proxy SIP (OPS) support. This feature set offers enhanced calling features in advance of SIP protocol definitions and deskphone implementations.

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

Supported SIP environments

The table lists the types of survivability configurations for various gateways and protocols, where recommended means minimal latency in the detection of a failover condition.

SIP Proxy/Phone connection Type	UDP	TCP	TLS
SES (as primary controller)	Not recommended	Recommended	Recommended
Avaya Session Manager (as primary controller)	Not recommended	Recommended	Recommended
Avaya Secure Router 2330 and 4134	Not recommended	Recommended	Recommended
Audiocodes MP-series analog and BRI gateways (as secondary controller)	Not recommended	Recommended	Not recommended
Cisco 2811 ISR (as secondary controller)	Not recommended	Recommended	Not supported
I55 (as secondary controller)	Not recommended	Recommended	Not supported
Teldat Vyda gateway	Not recommended	Recommended	Not recommended

- The Audiocodes SIP gateways tested for interoperability are the MP114 and MP118. Use the 5.60A.010.005 firmware or later.
- The Cisco gateways tested for interoperability are the Cisco [ISR]. The minimum firmware revision is c2800nm-ipbasek9-mz.124-20.YA2.bin.
- If deskphones failover to a non-Avaya secondary controller, such as Audiocodes and Cisco, there might be a few call-based issues if the deskphones are using different transport protocols.

For more information on feature configuration and operation, see the appropriate Communication Manager Feature and Administration guides.

The features available on the deskphones depend on the CM and SES/SM configuration/ version. These features are detailed in the Feature Compatibility Matrix in the Release Notes document for the latest 96x0 SIP 2.6 SP which is available on the Avaya Support site at support.avaya.com.

Communication Manager (CM) Compatibility and Encryption

SRTP is not enabled in the 46xxsettings.txt file included with this release. As noted earlier, SRTP is supported, but requires that the gateway software versions also support SRTP (not all do). Once this has been verified SRTP may be provisioned in the following manner.

For SRTP operation, it is recommended that the CM must be provisioned with the SRTP IP codec policy of:

- 1-srtp-aescm128-hmac80
- 9-none

On the 96xx SIP phone, this can be accomplished with the inclusion of the following setting in the 46xxsettings.txt file:

```
SET MEDIAENCRYPTION "1,9"
```

When the ENFORCE_SIPS_URI parameter is 1, the phone accepts and uses only SIPS URI for incoming and outgoing calls with SRTP media encryption. When the ENFORCE_SIPS_URI parameter is 0, the phone allows either SIP URI or SIPS URI for incoming SRTP media encryption calls and uses only SIP URI for outgoing SRTP media encryption calls. This parameter has been introduced in 2.6.

In general, when any encryption is selected, it is necessary to also include '9-none' as a fallback. For more details, see Administering Avaya Aura® Communication Manager Administering Avaya Aura® Communication Manager (Doc. ID 03-300509) at

http://support.avaya.com/css/P8/documents/100059292

Note that, having different Media Encryption settings on different sets requires the union of all the encryption settings in CM. For example, if, in one phone the following media encryption setting is provisioned:

```
SET MEDIAENCRYPTION "1,9"
```

And, in another phone, the following media encryption setting is provisioned:

```
SET MEDIAENCRYPTION "2,9"
```

Then, CM setting must include all unique media encryption values - in this case 1, 2, and 9, or just 9 (if no media encryption is desired).

Aliasing SIP Deskphones for switch compatibility

SIP software Release 2.6.9 supports the 9620, 9620C, 9620L, 9630, 9630G, 9640, 9640G, 9650, and 9650C deskphones using a compatible version of Avaya Communication Manager (CM). These models are not natively supported and must be administered as other 96xx Series models according to the chart below. For deskphones running a CM Release earlier than 5.2, be sure to administer 9600 Series IP Deskphones as 4620SIP deskphones on Avaya Communication Manager. Deskphones running CM Release 5.2 and later can be administered as 96*xx*SIP deskphones, where *xx* represents the deskphone model number (for example, 9620, 9630, etc.). The chart that follows illustrates CM/deskphone compatibility.

9600 Series IP Deskphones model	Administer on CM 6.0+ as...
96020	9620SIP
96020C	9620SIP
9620L	9620SIP
9630	9630SIP
9630G	9630SIP
9640	9640SIP
9640G	9640SIP
9650	9650SIP
9650C	9650SIP

For specific administration instructions about 9600 Series IP Deskphones, see Administering stations on page 53.

Administering Communication Manager for Session Manager

For information about CM administrative requirements with Session Manager, see the Avaya Aura® Session Manager and Avaya Aura® System Manager document libraries on the Avaya support site.

Administering Communication Manager - SM Requirements

Administering RSVP and RTCP/SRTCP

Avaya SIP IP Telephones support the RTP/SRTP Control Protocol (RTCP/SRTCP). 9600 Series IP Deskphones do not support RSVP (Resource ReSerVation Protocol).

Administering QoS

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 deskphones. However, the initiatives contribute to improved QoS for the entire network.

Administering IEEE 802.1D and 802.1Q

9600 Series IP Deskphones can simultaneously support receipt of packets using, or not using, 802.1Q parameters. To support IEEE 802.1D/Q, you can administer 9600 Series IP Deskphones by the value of the following configuration parameters:

- L2Q,
- L2QVLAN,
- L2QAUD, and
- L2QSIG.

Administering DIFFSERV

Type of Service bits 0-5 (also called the Differentiated Services Code Point) are set to the binary equivalent of the decimal number represented by the value of the following configuration parameters:

- DSCPAUD for transmitted audio (RTP, RTCP, SRTP and SRTCP) packets;
- DSCPSIG for transmitted system-specific signaling packets;
- Zero for all other transmitted packets (e.g., DHCP, DNS, HTTP, SNMP, etc.).

Received DSCP information will be ignored.

Administering Voice Mail

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 deskphone should dial to access your voice mail system, such as AUDIX or Octel.
- a Feature Access Code (FAC) that is configured for the Feature "To Voice Mail" will allow the user to transfer the 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 Call Processing to exchange information.

When the user presses the **Messages** button on the deskphone, 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 MSGNUM.

To reach the Voice Mail system using the **Messages** button during failover, administer the parameter PSTN_VM_NUM.

Administering auto hold

The SIP-based 9600 Series IP Deskphones always provide auto hold, regardless of whether or not the Auto Hold parameter is administered on the Avaya Communication Manager IP Network System Parameters form.

Call transfer considerations

Unlike H.323- based 9600 Series IP Deskphones, SIP-based 9600 Series IP Deskphones transfer operation is controlled locally by the deskphone and is not affected by the settings of the system parameters, Abort Transfer, Transfer Upon Hang-up, and Toggle Swap.

Conferencing call considerations

Unlike H.323- based 9600 Series IP Deskphones, SIP-based 9600 Series IP Deskphones conference operation is controlled locally by the phone and is not affected by the settings of the system parameters, Abort Conference Upon Hang-up, No Dial Tone Conferencing, Select Line Conferencing, and Toggle Swap.

Administering SIP Deskphones on Avaya Aura Communication Manager

SIP feature support summarizes the calling features available on 9600 Series IP Deskphones. Some features are supported locally at the deskphone, while others are only available with Communication Manager with OPS.

The features shown in SIP feature support can be invoked at the phone either directly or by selecting a CM-provisioned feature button. Communication Manager automatically handles many other standard calling features such as call coverage, trunk selection using Automatic Alternate Routing (AAR), or Automatic Route Selection (ARS), Class Of Service/Class Of Restriction (COS/COR), and voice messaging. Details on feature operation and administration can be found in the *Feature Description and Implementation for Avaya Communication Manager* (Document Number 555-245-205) and any of the CM administration documents

available on the Avaya support site. The Avaya SIP solution configures all SIP deskphones in Communication Manager as OPS.

For a complete list and comparison of feature availability of Session Manager configurations, see the document titled *Avaya Aura® Services - SIP Handset Features* on the Avaya support Web site: www.avaya.com/support.

Note:

Features activated in CM can only be deactivated via CM; features activated during failover can only be deactivated during the failover period.

SIP feature support

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with CM/SM
3-Way Conferencing	Yes	
6-way Conference Bridge		Yes
Auto Intercom		With SM, requires CM 5.2.1 or later.
Automatic Call Back/ Cancel		Yes but is not supported by SM 6.0/ CM 6.0 operating as a feature server
Call Forward All Calls (on/off)		Yes
Call Forward Busy/ Don’t Answer (on/off)	Yes	Yes
Call Forward Unconditional (on/off)	Yes	
Call Hold	Yes (Consultation Hold)	Yes
Call Management - incoming, outgoing call screening		Yes
Call Park and Unpark		Yes

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with CM/SM
Call Pick-Up Group		Yes
Call Pickup Directed		Yes
Calling Party Number Block/Unblock		Yes
Dial Intercom		With SM, requires CM 5.2.1 or later.
Directed Call Pick-Up		Yes
Distinctive Alerting		Yes
EC500 Enable		Yes
EC500 Disable		Yes
Exclusion		With SM, requires CM 5.2.1 or later.
Extend Call for EC500		With SM, requires CM 5.2.1 or later.
Extended Group Call Pickup		Yes
Group Call Pickup		Yes
Redial	Yes	Yes
Malicious Call Trace		Yes
Message Waiting Indication	Although MWI is not available, users can access their voice mailbox using the Message button if the parameter PSTN_VM_NUM is administered	Yes
Music on Hold		Yes
One Touch Recording		Yes

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with CM/SM
Priority Call		Yes
Send All Calls Enable/ Disable		Yes
Third Party Call Forward	Yes	With SM, requires CM 5.2.1 or later.
Third Party Call Forward Busy Don't Answer	Yes	With SM, requires CM 5.2.1 or later.
Third Party Send All Calls	Yes	With SM, requires CM 5.2.1 or later.
Transfer - attended	Yes	Yes
Transfer - unattended	Yes	Yes
Whisper Page		Yes
More Emergency Numbers	No	CM\SES - No CM\SM - Yes
Presence (optional)	No	Yes

3 of 3

Administering stations

This section refers to Communication Manager (CM) administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. Administer the following items on the Station form. Avaya recommends setting the features covered in this section because they optimize the user interface.

Note:

If you are using Avaya Aura® Session Manager (SM), you can use Avaya Aura® System Manager as an alternative to the SAT to administer the features described in the section that follows, Administering features.

Administering features

The following buttons can be administered for a 9620, 9620C, 9620L, 9630, 9630G, 9640, 9640G, 9650, and 9650C SIP deskphone, unless otherwise noted:

Administrable Station Features

Feature	Administration Notes
3-Way Conferencing	
6-Way Conference Bridge	
Audix One-Touch Recording	
Auto Callback/Cancel	This feature is not supported by SM 6.0/CM 6.0 when CM is administered as a feature server.
Auto Intercom	Add an intercom group # (in the Group, add your extension and dial code (DC), then add the other person's extension and DC. Add an auto-icom button, icom group #, DC.
Autodial	
Bridged Call Appearances	
Busy Indicator	
Call Appearances	
Call Forward (all)	
Call Forward Deactivation	
Call Forward Unconditional	
Call Forwarding (busy/don't answer)	
Call Hold	
Call management (incoming, outgoing call screening)	
Call Park	
Call Unpark	Regardless of CM Station button administration, this feature will show on the Features menu automatically on SM 5.2+ configurations. In SM 6.0+ this feature does not appear automatically.
Call Pickup	
Call Pickup Group	
Calling Party Number Block/ Unblock	
Consultation Hold	
CPN Block	
CPN Unblock	
Dial Intercom	On CM: 1. Add an intercom group # (in the group, add your extension and dial code, then add other person's extension and dial code. 2. Add a dial-icom button, icom group #, (no dial code).
Directed Call Pickup	

Administrable Station Features (continued)

Feature	Administration Notes
Distinctive Alerting	
EC500 Enable/Disable	
EC500 Extend Call	
Exclusion	
Extended Call Pickup	Regardless of CM Station button administration, this feature will show on the Features menu automatically.
Find Me	
Last Number Dialed (Redial)	
Malicious Call Trace	
MCT Activation	
Message Waiting Indication	Supported in CM 6.0.
Music on Hold	
One Touch Recording	
Priority Call	
Send All Calls	
Transfer (Attended)	
Transfer (Unattended - one button transfer)	
Whisper Page	
More Emergency Numbers	
Presence (optional)	

For additional information about administering Avaya Communication Manager for 9600 Series IP Deskphones, see the following Avaya documents, available on the Avaya Support website:

- *Administrator Guide for Avaya Communication Manager* (Document 03-300509).
- *Feature Description and Implementation for Avaya Communication Manager* (Document 555-245-205).
- *Administering Avaya Aura® Communication Manager as a Feature Server* (Document Number 03-603479) and related Avaya Aura® Session Manager documents.

Chapter 5: Security Configuration

Security certificates overview

The applications running on the 9600 Series IP Deskphones setup rely on trusted certificates for secure operation. Enterprises can set up their own certificate authority (CA) or use the Avaya SIP CA. If you are using a non-Avaya CA, you must remove the default Avaya root certificates and install the trusted certificates provided by your CA.

The certificates issued by CA must be configured in the 46xxsettings file when the 9600 Series IP Deskphones is registered with the enterprise. In addition to root certificates, high-security enterprises install a unique identity certificate on each 9600 Series IP Deskphones. Identity certificates are required if the communication setup is using EAP-TLS, or any other server that requires mutual authentication.

The 9600 Series IP Deskphones support the Simple Certificate Enrollment Protocol (SCEP) to retrieve and load the identity certificates. You can configure SCEP settings in the settings file. If the device is preconfigured, you must return to factory defaults before performing the security configurations.

The deskphone use specific certificates during operations.

- SIP/TLS: Uses the trusted certificates if the certificates are configured, else uses the default Avaya SIP Product CA and Avaya Product Root CA certificate.
- PPM/HTTPS/TLS: Uses the trusted certificates if the certificates are configured, else uses the default Avaya SIP Product CA and Avaya Product Root CA certificate.
- Software distribution package and settings file: Uses the trusted certificates if the certificates are configured, else uses the Avaya Product Root CA certificate. Identity certificate generated using SCEP or demo identity certificate.
- Ethernet 802.1x EAP-TLS: Uses the trusted certificates. The identity certificate generated using SCEP is used for authentication.

Secure installation configuration

For secure installation, configure the following parameters:

Parameter	Set to	Notes
TRUSTCERTS	Certificate file names	Provides the file name of certificates to be used for authentication.

Parameter	Set to	Notes
TLSSRVRID	1	Certificates installed on the servers must have the common name that matches the device configuration.
AUTH	1	Ensures usage of HTTPS file servers for configuration and software files download. Once AUTH is set to 1 and the device downloads the trusted certificates, the device can only download files from HTTPS server with certificates that can be validated using trusted certificate repository.

SCEP parameters

Configure the following Simple Certificate Enrollment Protocol (SCEP) parameters.

Parameter	Type	Default value	Description
MYCERTURL	String	Null	Specifies the URL to access Simple Certificate Enrollment Protocol (SCEP) server. The device attempts to contact the server only if this parameter is set to other than its default value.
MYCERTCN	String	$SERIALNO	Specifies the Common name (CN) for SUBJECT in SCEP certificate request. The values can either be **$SERIALNO** or **$MACADDR**. If the value includes the string **$SERIALNO,** that string is replaced by the phones serial number. If the value includes the string **$MACADDR**, that string is replaced by the phones MAC address.

Parameter	Type	Default value	Description
MYCERTDN	String	Null	Specifies common part of SUBJECT in SCEP certificate request. This value defines the part of SUBJECT in a certificate request including Organizational Unit, Organization, Location, State, and Country that is common for requests from different devices.
MYCERTKEYLEN	Numeric	1024	Specifies the private key length in bits to be created in the device for a certificate enrollment. The range is from 1024 to 2048.
MYCERTRENEW	Numeric	90	Specifies the percentage used to calculate the renewal time interval out of the device certificates Validity Object. If the renewal time interval has elapsed, the phone starts to periodically contact the SCEP server again to renew the certificate. The range is from 1 to 99.
MYCERTWAIT	Numeric	1	Specifies the behavior of the device when performing certificate enrolment assigned to one of the following values: l 0: Periodical check in the background l 1: Wait until a certificate or a denial is received or a pending notification is received.

Parameter	Type	Default value	Description
MYCERTCAID	String	CAIdentifier	Specifies the Certificate Authority Identifier. Certificate Authority servers might require a specific CA Identifier string to accept GetCA requests. If the device works with such a Certificate Authority, the CA identifier string can be set through this parameter.
SCEPPASSWORD	String	$SERIALNO	Specifies a challenge password to use with SCEP. The value of SCEPPASSWORD, if non-null, is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains **$SERIALNO**, **$SERIALNO** is replaced by value of SERIALNO. If the value contains **$MACADDR**, **$MACADDR** is replaced by the value of MACADDR without the colon separators.

VLAN

Configure the following VLAN parameters.

Parameter	Set to	Notes
VLANSEP	1	Enables the VLAN separation
L2Q	0, 1, or 2	Specifies 802.1Q tagging mode.
PHY2VLAN	Non-zerovalue	Specifies the data VLAN and must not have the same value as the L2QVLAN parameter.

Parameter	Set to	Notes
L2QVLAN	Non-zerovalue	Specifies the voice VLAN and must not have the same value as the PHY2VLAN parameter.

For VLAN configuration, there is a full VLAN separation between the device and computer packets. The device tries to obtain an IP address from the DHCP server on the voice VLAN. If the device locates an IP address, the device sends all the tagged packets on the voice LAN. You must set the PHY2VLAN parameter to the data VLAN so that untagged packets from the computer are assigned to the data VLAN. Otherwise, the tagged packets from the computer are forwarded to the data VLAN. Other than the data VLAN, tagged packets from computers on VLANs are blocked.

Installing certificate

1. In the 46xx settings file, configure the following parameters:
   a. **SET SIP_CONTROLLER_LIST** `148.147.169.210:5061;transport=tls,148.147.169.216:5061;transport=tls`
   b. **SET SIPDOMAIN** `pssv.com`
   c. **SET TRUSTCERTS** `default7.cacert.pem`
2. Copy the certificate (PEM) file to the HTTP server.
3. In the CRAFT menu go to ADDR -> HTTP Server and enter the IP address.
4. Restart the phone.

Replacing demo certificates on phone

You cannot remove demo certificates from the deskphone. You can configure SCEP on phone to get the Identity certificate from EJBCA server on SMGR to replace the demo certificate installed on phone. The following is an example for SCEP configuration when working with EJBCA server built-in on SGMR.

Note:

The steps for SCEP configuration vary when working with other CA servers, such as standalone EJBCA and Microsoft CA.

Before you begin

1. On SMGR, go to **Home > Services > Security > Certificates > Authority**.
2. Add End Entity, and do the following:

   a. End Entity Profile - INBOUND_OUTBOUND_TLS
   b. Username - phones SN
   c. Common name (CN) - phones SN
   d. Leave other fields as default.
3. Ensure that the HTTP server is saved where 46xxx setting.txt file exist.
4. In the `46xxsettings` file:
   a. **SET MYCERTURL** `http://<SMGR IP address>/ejbca/publicweb/apply/scep/pkiclient.exe`
   b. **SET MYCERTCAID** `default`
   c. **SET MYCERTKEYLEN 2048**
   d. **SET MYCERTWAIT** 1
   e. **SET MYCERTDN /DC=COM/DC=Avaya**
   f. **SET MYCERTCN <phones SN>**
   g. **SET SCEPPASSWORD < End Entity password>**
5. Restart the phone.

The phone configures SCEP to download the certificate generated by EJBCA server on SMGR.

Chapter 6: Administering Avaya Aura® Session Manager, and System Manager (SM)

Avaya product overview

In addition to supporting three Avaya Aura® Communication Manager configurations (as described in Chapter 4: Avaya Aura® Communication Manager Administration), SIP software provides administrative flexibility by inter-operating with the following Avaya Aura® products:

Avaya Aura® System Manager provides centralized administration for multiple instances of Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Avaya Aura® System Manager is a solution-level approach to network administration that manages the elements of Avaya Aura® together as a system. Avaya Aura® System Manager centralizes provisioning, maintenance, and troubleshooting. Avaya Aura® System Manager provides for central administration of dial plans and network routing policy as well as common user provisioning.

Avaya Aura® Session Manager unifies media, modes, networks, devices, applications and real-time, actionable presence across a common infrastructure, creating web-style, on-demand access to services and applications. Third Party PBX support allows connectivity to Avaya equipment as well as Cisco, Nortel, and other third-party PBXs. Dial Plan Allows central enterprise-wide dial plans across multi-vendor PBX environments. Network routing supports creation of system-wide network routing rules to cost effectively route calls using the enterprise's on-net IP network.

This chapter provides references to documents available on the Avaya support Web site www.avaya.com/support for Session Manager, and System Manager. See the appropriate documentation for your system configuration.

Administering Avaya Aura® System Manager

For an administrative overview of Avaya Aura® System Manager and details for administrative requirements and procedures, see the following documents available on the Avaya support Web site www.avaya.com/support:

- *Installing and Upgrading Avaya Aura® System Manager*
- *Administering Avaya Aura® System Manager*
- System Manager Release notes

Because System Manager is used to maintain multiple Avaya Aura® Session Manager installations, also see the Session Manager documents listed in Administering Avaya Aura® Session Manager.

Administering Avaya Aura® Session Manager

For an administrative overview of Session Manager and details for administrative requirements and procedures, see the following documents available on the Avaya support Web site www.avaya.com/support:

- *Avaya Aura® Session Manager Overview* (Document Number 03-603323)
- *Installing and Upgrading Avaya Aura® Session Manager* (Document Number 03-603473)
- *Administering Avaya Aura® Session Manager* (Document Number 03-603324)
- *Maintaining and Troubleshooting Avaya Aura® Session Manager* (Document Number 03-603325)
- *Network Case Study for Avaya Aura® Session Manager* (Document Number 03-603478)

Chapter 7: Server Administration

Software Requirements

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 SIP-based 9600 Series IP Deskphones network by removing the need to individually assign and maintain IP addresses and other parameters for each deskphone on the network.

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

- IP address of 9600 Series IP Deskphones
- IP address of the Avaya call server
- IP address of the HTTP or HTTPS file server
- IP address of the NTP (Network Time Protocol) server (using Option 42)
- The subnet mask
- IP address of the router
- DNS Server IP address

Administer the LAN so each SIP deskphone 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 deskphone reboots.
- A DHCP server be available at remote sites if WAN failures isolate IP deskphones from the central site DHCP server(s).

A (HTTP or HTTPS) file server, which may run on the same physical computer as Communication Manager, provides 9600 Series IP Deskphones with an upgrade file and, if appropriate, new or updated binary software. See Step 3: Downloading files on page 28. In addition, you can edit the settings file (46xxsettings.txt) to customize deskphone parameters for your specific environment. For more information, see Chapter 9: Administering Deskphone Options.

Administering the DHCP Server

This section 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.

Configuring DHCP Option 242 (SSON)

9600 Series IP Deskphones allow you to specify the value of some configuration parameters using DHCP option 242 (the default site-specific option). If you have 46xx phones that use option 176, you can make a copy of an existing option 176. Then, using that copy to administer DHCP option 242, you can either:

- leave any (46xx) parameters 9600 Series IP Deskphoness do not support in Option 242 to be ignored, or
- delete unused or unsupported 9600 Series IP Deskphones parameters to shorten the DHCP message length.

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 as described in .

Parameters set by DHCP in a site-specific option

Parameter	Description
DNSSRVR	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 to prepend to all configurations and data files the phone might request when starting up, i.e., the path, relative to the root of the HTTP file server, to the directory in which the deskphone configuration and date files are stored. The path may contain no more than 127 characters and may contain no spaces. If an Avaya file server is used to download configuration files over HTTPS, 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. The command is "SET HTTPDIR=<path>". In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use the HTTPDIR=<path>.
HTTPPORT	Destination port for HTTP requests (default is 80).
HTTPSRVR	IP Address(es) or DNS name(s) of HTTP file server(s) used for file download (settings file, language files, code) during startup. 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.
LOCAL_LOG_LEVEL	Controls the severity level of events logged in the local event log. The default is 3.
LOGSRVR	Syslog server IP or DNS address.
MTU_SIZE	Maximum transmission unit size. Used to accommodate older Ethernet switches that cannot support the longer maximum frame length of tagged frames (since 802.1Q adds 4 octets to the frame).
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).

Parameter	Description
PROCPSWD	Security string used to access local procedures. The default is 27238.
PROCSTAT	Controls whether local procedures are enabled. The default is 0 (enabled).
SIG	The signaling protocol download flag that indicates which protocol applies (H.323 (1), SIP, (2) or Default (0).
SIP_CONTROLLER_LIST	SIP proxy/registrar server IP or DNS address(es). (0 to 255 characters; zero or one IP Address in dotted decimal or DNS name format, separated by commas without any intervening spaces.) The default is null.
SNTPSRVR	List of SNTP server IP or DNS address(es) used to retrieve date and time via SNTP
TLSDIR	Used as path name that is prepended to all file names used in HTTPS GET operations during initialization (0-127 character string).
TLSPORT	Destination TCP port used for requests to https server (0-65535). The default is 443.
TLSSRVR	IP Address(es) or DNS name(s) of Avaya file server(s) used to download configuration files. **Note:** Transport Layer Security is used to authenticate the server.
VLANTEST	Number of seconds to wait for a DHCPOFFER on a non-zero VLAN. The default is 60 seconds.

DHCP Generic Setup

This section is limited to describing a generic administration that works with 9600 Series IP Deskphones. Three DHCP software alternatives are common to Windows operating systems:

- Windows NT® 4.0 DHCP Server
- Windows 2000® DHCP Server
- Windows 2003® DHCP Server
- Windows 2008® 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

DHCP server setup involves:

1. Installing the DHCP server software according to vendor instructions.
2. Configuring the DHCP server with:
   - IP addresses available for 9600 Series IP Deskphones.

- The following DHCP options:
  - Option 1 - Subnet mask.
    As described in Required network information before installation - per DHCP server.
  - Option 3 - Gateway (router) IP Address(es).
    As described in Required network information before installation - per DHCP server, item . 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.
  - Option 6 - DNS server(s) address list.
    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. At least one address in Option 6 must be a valid, non zero, dotted decimal address.
  - Option 12 - Host Name.
    Value is **AV*ohhhhhh***, where: o has one of the following values based on the OID (first three octets) of the deskphone's MAC address: "A" if the OID is 00-04-0D, "B" if the OID is 00-1B-4F, (SIP software Release 2.0+), "E" if the OID is 00-09-6E, "L" if the OID is 00-60-1D, "T" if the OID is 00-07-3B, (SIP software Release R2.0+) and "X" if the OID is anything else, and where hhhhhh are ASCII characters for the hexadecimal representation of the last three octets of the deskphone's MAC 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 About DNS addressing on page 124.
  - Option 42 - SNTP Server.
    This option specifies a list of IP Addresses indicating NTP servers available to the deskphone. List servers in the order of preference.The minimum length is 4, and the length must be a multiple of 4.
  - 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 Telephones to reboot. Avaya recommends providing enough leases so an IP Address for an IP deskphone does not change if it is briefly taken offline.

Note:

The DHCP standard states that when a DHCP lease expires, the device should immediately cease using 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 deskphone will not receive responses to its request for a renewal of the lease. In this case the deskphone is not usable until the server can respond.

Avaya recommends that once assigned an IP Address, the deskphone continues using that address after the DHCP lease expires, until a conflict with another device is detected. The system parameter DHCPSTD allows an administrator to specify that the deskphone 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 deskphone 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 deskphone receives a DHCPACK, a DHCPNAK, or an ARP Reply. After receiving a DHCPNAK or ARP Reply, the deskphone displays an error message, sets its IP Address to 0.0.0.0, and attempts to contact the DHCP server again. Log events are generated for either case.

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 deskphones expires, the third deskphone cannot get a lease until the reservation period expires. Even if the other two deskphones are removed from the network, the third deskphone remains without a lease until the reservation period expires.

- Option 52 - Overload Option, if desired.
  If this option is received in a message, the deskphone interprets the **sname** and **file** fields in accordance with IETF RFC 2132,
  Section 9.3, listed in Appendix B: Countries With Specific Network Progress Tones.

- Option 53 - DHCP message type.
  Value is 1 (DHCPDISCOVER) or 3 (DHCPREQUEST). As of Release 2.5, if a DHCPACK is received in response to a DHCPREQUEST sent to renew the

deskphone's IP address lease, a log event record is generated with a Log Category of "DHCP". If a DHCPNAK is received in response to a DHCPREQUEST sent to renew the deskphone's IP address lease, the deskphone will immediately cease use of the IP address, a log event record will be generated, IPADD will be set to "0.0.0.0", and the deskphone will enter the DHCP INIT state.

- Option 55 - Parameter Request List.
  Acceptable values are:
  1 (subnet mask),
  3 (router IP Address[es])
  6 (domain name server IP Address[es])
  7 (log server)
  15 (domain name)
  26 (Interface MTU)
  42 (NTP servers)
  SSON (site-specific option number)
- Option 57 - Maximum DHCP message size.
  Release 2.5+ value is 1000; prior to R2.5, value was 576.
- 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, listed in Countries With Specific Network Progress Tones.
- 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 is administered appropriately elsewhere.

  Avaya recommends that you administer DHCP servers to deliver only the options specified in this section and Parameters set by DHCP in a site-specific option. Administering additional, unexpected options might have unexpected results, including causing the IP deskphone to ignore the DHCP server.

  Examples of good DNS administration include:

  - Option 6: “***aaa.aaa.aaa.aaa***”
  - Option 15: “***dnsexample.yourco.com,zzz.zzz.zzz.zzz***”
  - Option 42: "***aaa.aaa.aaa.aaa***"

9600 Series IP Deskphones do not support Regular Expression Matching, and therefore, do not use wildcards. For more information, see Administering options for the 9620, 9620C, 9620L, 9630, 9630G, 9640, 9640G, 9650, and 9650C SIP Deskphones on page 85.

As shown in DHCPACK setting of parameter values, 9600 Series IP Deskphones sets the parameter values to the DHCPACK message field and option contents shown.

DHCPACK setting of parameter values

Parameter Value	Set to
DHCP lease time	Option #51 (if received).
DHCP lease renew time	Option #58 (if received).
DHCP lease rebind time	Option #59 (if received).
DOMAIN	Option #15 (if received).
DNSSRVR	Option #6 (if received, which might be a list of IP Addresses).
HTTPSRVR	The **siaddr** field, if that field is non-zero.
IPADD	The **yiaddr** field.
LOGSRVR	Option #7 (if received).
MTU_SIZE	Option #26.
NETMASK	Option #1 (if received).
ROUTER	Option #3 (if received, which might be a list of IP Addresses).
SNTPSRVR	Option #42.

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 on page 67.

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).

HTTP Generic Setup

You can store the binary file, upgrade file, and settings file on an HTTP server. With proper administration, the deskphone 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 65.

Note:

If you used TFTP to provide the binary, upgrade, and settings files to older Avaya IP telephones, note that 9600 Series IP Deskphones do not support TFTP; you must use HTTP or HTTPS instead.

Important:

The files defined by HTTP server configuration must be accessible from all IP deskphones that might request 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:

To set up an HTTP server:

- Install the HTTP server application.
- Administer the system parameter HTTPSRVR to the address of the HTTP server. Include this parameter in DHCP Option 242 or the appropriate SSON Option.

- Download the upgrade file and software application file(s) from the Avaya website http://support.avaya.com to the HTTP server. For more information, see Chapter 8: Deskphone Software and Application Files.

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.

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.

Chapter 8: Deskphone Software and Application Files

About the general download process

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 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 deskphone, 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 Deskphones 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 deskphone 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 deskphone, which then initiates the same process for contacting a file server.

The deskphone queries the file server, which transmits a 96xxupgrade.txt file (for both SIP and H.323 protocol) to the telephone based on the SIG parameter setting. The upgrade file tells the deskphone which software files the deskphone should use.

9600 Series IP Deskphones 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 77. 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.

Choosing the right application file and upgrade script file

Software files needed to operate 9600 Series IP Deskphones are packaged together in either a Zip format or a RPM/Tar format distribution package. You download the package appropriate to your operating environment to your file server from the Avaya support website at http://

support.avaya.com based on the protocol you are using (H.323 or SIP) for all or the majority of your deskphones.

SIP software distribution packages contain:

- one upgrade file
- all of the display text language files
- all of the ring tone files

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 *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).

Changing the signaling protocol

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:

1. 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 *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).

About the upgrade file

The upgrade file tells the deskphone whether it needs to upgrade software. The upgrade file is either H.323-specific or SIP-specific. The deskphones attempt to read this file on the file server whenever they reset. The upgrade file also points to the About the settings file.

Avaya recommends that you do not alter the upgrade file. If Avaya changes the upgrade 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 file.

About the settings file

The settings file contains the parameters that you can use 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 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 file at the next line after a **# *tag*** statement. If no such statement exists, the rest of the 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, BOOTNAME, SIG, and SIG_IN_USE.
- **SET** commands, of the form **SET *parameter_name value***. Invalid values cause the specified value to be ignored for the associated ***parameter_name*** so the default or previously administered value is retained. All values must be text strings, even if the value itself is numeric, a dotted decimal IP Address, and so on.
- Comments, which are any lines that do not conform to any of the previously described types of statements, including lines that begin with more than one "#" character.

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 Chapter 9: Administering Deskphone Options for details about specific values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

Any line which does not match one of the previous statement types is ignored and, therefore, can be treated as a comment. By convention, in the upgrade and settings files distributed by Avaya, any line intended to be ignored by the phone or read as a comment starts with “##”.

Table 1: Settings File System Parameters That Can Be Tested in an IF Statement

Parameter	Description
BOOTNAME	The name of the Signed Kernel/Root Software package in the deskphone.
MACADDR	MAC address of the phone (hh:hh:hh:hh:hh:hh; automatically supplied by a phone).
MODEL	Deskphone Model identifier (8 ASCII characters; automatically supplied by a phone).
MODEL4	The first four digits of the model identifier (automatically supplied by a phone).
PWBCC	Avaya identification number for the printed circuit board (automatically supplied by a phone).
GROUP	Group identifier (must be manually set on a phone)
SIG	Signaling protocol identifier (2=SIP, 1=H.323, 0=default).
SIG_IN_USE	The signaling protocol in use. For SIP software value is always "SIP" and cannot be changed. Evaluate configuration file(s) according to value of this parameter (IF…GOTO command) and consider only commands related to the corresponding section of configuration file(s). Default=2 (SIP).

A sample settings file follows.

The following are example settings only. Your settings will vary from the settings shown. This sample assumes specification of a DNS Server, identifying SIP-specific settings, and setting the time/date.

```
##
##
## Define the Domain Name Server to be "dns.example.yourco.com"
## Note that quotes are only needed for parameters that contain
  spaces.
##
SET DNSSRVER dnsexample.yourco.com
##
##
## SIP Proxy/Registrar servers list
##  SIP_CONTROLLER_LIST provides ability to configure SIP Proxy/
  Registrar list.
##  The format is host[:port];[transport:xxx]. A comma seperated
  list in this
##  format can be provided. Host can be DNS name or IP address. Port
  is optional.
##  If port is not specified then default value of 5060 for TCP and
  UDP and 5061 for
##  TLS will be used. Transport type is optional. It can be tcp or
  udp or tls.
##  Default value of tls will be used if it is not provided.
SET SIP_CONTROLLER_LIST proxy1,proxy2:5070;transport=udp
##
##
##  SIPDOMAIN sets the domain name to be used during
##  registration.  The default is null ("") but valid values
##  are 0 to 255 ASCII characters with no spaces.
SET SIPDOMAIN   example.com
##
##
##  SNTPSRVR sets the IP address or Fully-Qualified
##  Domain Name (FQDN) of the SNTP server(s) to be used.
```

```
##  The default is null ("") but valid values are zero or
##  more IP addresses in dotted-decimal or DNS format,
##  separated by commas without intervening spaces, to a
##  maximum of 255 ASCII characters.
##  You may also want to use the ntp pool of servers.
##  See http://www.pool.ntp.org/use.html
##
SET SNTPSRVR  192.168.0.5
##
##
##  GMTOFFSET sets the time zone the phone should use. The
##  default is -5:00; see the 9600 Series SIP Telephone LAN
##  Admin Guide for format and setting alternatives.
SET GMTOFFSET "-6:00"
##
##
##  DSTOFFSET sets the daylight savings time adjustment
##  value. The default is 1 but valid values are 0, 1, or 2.
## SET DSTOFFSET "1"
##
##
##  DSTSTART sets the beginning day for daylight savings
##  time. See the 9600 Series
##  SIP Telephone LAN Admin Guide for format and setting
##  alternatives.
## SET DSTSTART  "2SunMar2L"
##
##  NOTE:
##  The default DSTSTART and DSTSTOP parameters reflect the
##  new 2007 Daylight Savings Time values for North America
##
##  DSTSTOP sets the ending day for daylight savings time.
```

```
## SET DSTSTOP   "1SunNov2L"
##
------------------------------
```

Parameters retained during a reboot

During a reboot, if the deskphone is unable to access the settings file, it does not retain the values of all the parameters. For more information on which parameter value is retained, see the following table.

Parameter	Retained
AGCHAND	Y
AGCHEAD	Y
AGCSPKR	Y
APPNAME	N
AUDIOENV	N
AUDIOSTHD	N
AUDIOSTHS	N
AUTH	Y
BAKLIGHTOFF	Y
CNGLABEL	Y
DAYLIGHT_SAVING_SETTING_MODE	Y
DHCPSTD	N
HEADSYS	N
HOMEIDLETIME	N
LOG_CATEGORY	Y
LOGSRVR	N

Parameter	Retained
LOCAL_LOG_LEVEL	Y
LANG0STAT	Y
MSGNUM	N
PROCSTAT	Y
PROCPSWD	Y
PHY1STAT	Y
PHY2STAT	Y
PHNCC	N
PHNDPLENGTH	N
PHNIC	N
PHNLDLENGTH	N
PHNLD	N
PHNLAC	Y
PHNOL	N
RFSNAME	N
SNMPADD	Y
SNMPSTRING	Y
SIG	Y
SCREENSAVERON	N
TEAM_BUTTON_RING_TYPE	Y
TPSLIST	N
VLANTEST	Y
WMLHOME	N
WMLPORT	N
WMLPROXY	N

Using the GROUP parameter to set up customized groups

You might have different communities of users, all of which have the same deskphone model, but which require different administered settings. For example, you might want to group users by time zones or work activities.

Use the GROUP parameter for this purpose:

1. identify which deskphones 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. At each non-default deskphone, instruct the installer or user to invoke the GROUP Craft Local procedure as specified in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694) and specify which GROUP number to use. The GROUP System value can only be set on a phone-by-phone basis.
3. Once the GROUP assignments are in place, edit the settings file to allow each deskphone of the appropriate group to download its proper settings.

Here is an example of a settings file with deskphones in three different groups - group "0" (the default), group "1", and group "2":

```
## First check if this phone is in group 1. If it is, jump to the
  tag GROUP1

##

IF $GROUP SEQ 1 goto GROUP1

##

## Now check if this phone is in group 2. If it is, jump to the tag
  GROUP2
  IF $GROUP SEQ 2 goto GROUP2

##

## The phone is not in either GROUP 1 or 2 so it is in GROUP 0
  {specify settings unique to Group 0}
  goto END

# GROUP1

## GROUP 1-only settings go here
  {specify settings unique to Group 1}
  goto END

# GROUP2

## GROUP 2-only settings go here
  {specify settings unique to Group 2}
  # END

## The settings here apply to all three groups
  {specify settings common to all Groups}
```

Chapter 9: Administering Deskphone Options

Administering options for the 9620, 9620C, 9620L, 9630, 9630G, 9640, 9640G, 9650, and 9650C SIP Deskphones

This chapter explains how to change parameter values to customize them for your operating environment. Table: Customizable parameters on page 86lists:

- The parameter names
- The default values of the parameters
- The valid ranges for those values
- A description of each parameter.

Table: Customizable parameters on page 86 is a comprehensive list of all the parameters you can configure. However, you do not have to set every parameter. In most cases, you will include only those parameters in the settings file that are specific to your own environment and let the deskphones use the default values for the remaining ones.

Note:

At a minimum, be sure to set these important SIP-related parameters: SIP_CONTROLLER_LIST, SIPDOMAIN, SNTPSRVR, GMTOFFSET, ENABLE_PRESENCE, DSTOFFSET, DSTSTART, and DSTSTOP.

For DHCP, DHCP fields and option sets certain parameters to the desired values as discussed in Administering the DHCP and File Servers on page 65. For HTTP, the parameters in Table: Customizable parameters on page 86 are set to desired values in the settings file. For more information on working with the settings file, see About the settings file on page 77.

Avaya recommends that you administer most parameters on 9600 Series IP Deskphones using the settings file as some DHCP applications have limits on the amount of user-specified information. The administration required can exceed those limits for the more full-featured deskphone 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. 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 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694) applicable to the SIP software Release you are using.

Important:

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.

Administering PROCPSWD limits access to all local procedures, including VIEW. VIEW is a read-only Craft option that allows review of the current deskphone settings.

Note:

There are several ways to change configuration parameters, for example, using DHCP options, the 46xxsettings file, or using local administrative (manual) procedures, and a specific procedure exists to determine which value the deskphone should use. About parameter data precedence on page 20 describes the order in which parameter values are determined.

SIP-based 9600 Series IP Deskphones customizable system parameters

Table: Customizable parameters

Parameter name	Default value	Description and value range
ADMIN_HSEQUAL	1	ADMIN_HSEQUAL specifies compliance standards for handset audio equalization. This value affects a deskphone if the the HSEQUAL local procedure or the user has not set the handset equalization. Valid Values are: 1=Use handset equalization that is compliant with TIA 810/920 (default) 2=Use handset equalization that is compliant with FCC Part 68 HAC requirements 96x0 SIP R2.6 SP7 and later software releases supports this parameter.
AGCHAND	1	Automatic Gain Control status for handset. Values are 0=disabled, 1=enabled.
AGCHEAD	1	Automatic Gain Control status for headset. Values are 0=disabled, 1=enabled.

Table: Customizable parameters

Parameter name	Default value	Description and value range
AGCSPKR	1	Automatic Gain Control status for speaker. Values are 0=disabled, 1=enabled.
AMADMIN	" " (Null)	URI for obtaining the Avaya (A) menu administration file. If null, the deskphones does not download the file for administration of A(vaya)-menu. Otherwise, this parameter defines the URI that points to the location from where the deskphone can obtain the A(vaya)-menu administration file. Valid values are: zero to one URI in the default length character string.
ASTCONFIRMATION	32	The time that the deskphone waits to validate an active subscription when it SUBSCRIBEs to the "avaya-cm-feature-status" package. Valid range is 16-3600.
AUDASYS	3	Globally controls audible alerting. Values range from 0 through 3. Value 0 or 2=audible alerting off. Value 1 or 3=audible alerting on.
AUDIOENV	0	Audio environment selection index. Values range from 0 through 191.
AUDIOSTHD	0	Headset sidetone setting. Values are: 0 = Default; no change; 16dB STMR. 1 = Three steps softer than nominal; 24dB STMR. 2 = Off; inaudible; 36dB STMR. 3 = One level softer than nominal;19dB STMR. 4 = Two steps softer than nominal; 21dB STMR. 5 = Four steps softer than nominal; 27dB STMR.
AUDIOSTHS	0	Handset sidetone setting. Values are: 0 = Default; no change; 16dB STMR. 1 = Three steps softer than nominal; 24dB STMR. 2 = Off; inaudible; 36dB STMR. 3 = One level softer than nominal;19dB STMR. 4 = Two steps softer than nominal; 21dB STMR. 5 = Four steps softer than nominal; 27dB STMR.
AUTH	0	Authentication flag for settings file download. Values are: 0 = secure setting file download is not required 1 = secure setting file download is required

Table: Customizable parameters

Parameter name	Default value	Description and value range
AUTO_SELECT_ANY_IDLE_APPR	0	Automatically selects any idle call appearance for conference or transfer. Values are: 0 = Active; If CONF_TRANS_ON_PRIMARY_APPR is 0 and no associated call appearance is selected, then the conference or transfer operation is denied. 1 = Not Active; If CONF_TRANS_ON_PRIMARY_APPR is 0 and no associated call appearance is selected, then the conference or transfer operation is tried on any available call appearance, primary or bridged.
BAKLIGHTOFF	120	Number of minutes without display activity to wait before turning off the backlight. Values range from zero (never turn off) through 999 minutes (16 hours 39 minutes).
CALL_TRANSFER_MODE	0	When ENABLE_AVAYA_ENVIRONMENT=0, this parameter indicates how deskphone performs transfers: 0 = attended transfer 1 = unattended transfer
CALLFWDADDR	" " (Null)	The URI to which calls are forwarded in failover.
CALLFWDDELAY	1	Failover environments only. Specifies the number of ring cycles generated at the phone before the call is forwarded to the Call Forwarding Address, if call forwarding on "No answer" is selected in failover. Valid number of ringing cycles are 0-20.
CALLFWDSTAT	0	Failover environments only. Specifies the sum of the allowed Call Forwarding permissions. This parameter controls which of the Call Forwarding Feature Buttons are made visible and active for the user in 3rd party environments. Valid values are: 0 = no Call Forwarding permitted. 1 = Call Forward Unconditional only permitted. 2 = Call Forward Busy only permitted. 4 = Call Forward No Answer only permitted. Others = sum of Call Forward types permitted.

3 of 35

Table: Customizable parameters

Parameter name	Default value	Description and value range
CALLPICKUPIND	3	Indicates the type of notification for calls received by the phones (None/Audible/Visible/Both). Can also be set by the end user via Screen & Sound options. Valid values are: 0=None (no call pickup alerting) 1=Audible alert on call pickup 2=Visual alert on call pickup 3= Both audible and visual alert on call pickup
CNAPORT	50002	Transport-layer port number to be used for registration to CNA server for network analysis. Valid range is 0-65535.
CNASRVR	" " (Null)	List of CNA server IP or DNS address(es). Used to connect to CNA server for network analysis (in case of several entries first address always first, etc.). Format is 0 to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. Currently set to a maximum of 5 servers.
CNGLABEL	1	Determines if the ability to personalize button labels is displayed to the user. Valid values are: 0=ability to personalize button labels is not displayed to user; 1=ability to personalize button labels is displayed to user.
CONF_TRANS_ON_ PRIMARY_APPR	0	Conference or Transfer operations will seek to use a primary call appearance only if initiated from a primary appearance. From a bridged appearance, conference or transfer operations will only be made from another idle bridged appearance. If no appearance is available, the operation will be denied. Valid values are: 0 = Active 1 = Not Active; overrides the AUTO_SELECT_ANY_IDLE_APPR parameter
CONFIG_SERVER_ SECURE_MODE	1	Indicates whether or not secure communication via HTTPS is required to access the configuration server. 0 = Use HTTP. 1 = Use HTTPS.
CONTROLLER_SEARCH _INTERVAL	4	Time in seconds that the phone waits to complete the maintenance check for monitored controllers. Valid values are 4 - 3600 (seconds).

Table: Customizable parameters

Parameter name	Default value	Description and value range
COUNTRY	USA	Country of operation for specific dial tone generation. This is a specific text string specifying the country in which the device operates (e.g. "USA", "France", "Germany"). See Appendix B: Countries With Specific Network Progress Tones for a list of applicable countries.
COVERAGEADDR	" " (Null)	The URI to which call coverage is sent to in failover (non-Avaya) environments only.
CURRENT_CONTENT	" " (Null)	Defines the URL of the customization file for the Home Screen. Range is the default string length of the URL.
CURRENT_LOGO	" " (Null)	Defines the selected background logo on display, if any. Indicates if a custom logo is currently selected (non-empty string) or a built-in default logo is used (empty string or not set). If a custom logo is selected (non-empty string), this value points to the corresponding logo resource definition as defined in LOGOS configuration parameter.
CURRENT_SKIN	" " (Null)	Defines if a custom skin is currently selected (non-empty string) or built-in default skin is used (empty string or not set). If a custom skin is selected (non-empty string), this value points to the corresponding skin resource definition (i.e. contains a label as defined in "SKINS" configuration parameter). Can also be set by the end user via Avaya Menu Screen & Sounds option.
DATEFORMAT	%m/%d/%y	Formatting string defining how to display the date in the top line and the call log.
DAYLIGHT_SAVING_SETTING_MODE	2	Controls daylight saving setting. Values are: 0=daylight saving time is deactivated (no offset to local time) 1=daylight saving time is activated (offset to local time as configured in "DSTOFFSET") 2=the device switches automatically to daylight saving time and back according to the contents of "DSTSTART" and "DSTSTOP"

Table: Customizable parameters

Parameter name	Default value	Description and value range
DHCPSTD	0	DHCP Standard lease violation flag. Indicates whether to keep the IP Address if there is no response to lease renewal. If set to “1” (No) the deskphone strictly follows the DHCP standard with respect to giving up IP Addresses when the DHCP lease expires. If set to “0” (Yes) the deskphone continues using the IP Address until it detects reset or a conflict (see DHCP Generic Setup).
DIALPLAN	" " (Null)	Dial plan for operation with a secondary controller. The DIALPLAN parameter is used to determine one or more valid dialstrings. Valid value is 0 to 1023 characters that define the dial plan. See Setting the dial plan on SIP Deskphones for more information.
DISCOVER_AVAYA_ ENVIRONMENT	1	Allows the phone to discover whether it is in an Avaya environment where SIP AST features are supported. Valid values are: 0=Non-Avaya environment; do not auto-discover AST support 1 = Avaya environment; auto-discover AST support. The SIP proxy server (controller) may or may not support AST.
DISPLAY_NAME_ NUMBER	0	Indicates whether the calling party’s number will be displayed next to the caller name on an incoming call. If this parameter is not set, only the caller name is shown. Valid values are: 0 = Show caller’s name only. 1 = Show caller’s name followed by number. 2 = Show caller’s number only. 3 = Show caller’s number followed by name.
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.

Table: Customizable parameters

Parameter name	Default value	Description and value range
DOT1X	0	Defines the deskphone's operational mode for IEEE 802.1X.Valid values are: 0 = Unicast Supplicant operation only, with PAE multicast pass-through, but without proxy Logoff. 1= Unicast Supplicant operation only, with PAE multicast pass-through and proxy Logoff. 2= Unicast or multicast Supplicant operation, without PAE multicast pass-through or proxy Logoff.
DOT1XEAPS	MD5	Specifies the EAP authentication method(s) to be used with IEEE 802.1X. Comma-separated list of key words defining EAP methods. In SIP Release 2.0, this value is restricted to a single EAP method. Valid values are either "MD5" or "TLS".
DOT1XSTAT	0	IEEE 802.1X status. Enables/disables IEEE 802.1X function and, if enabled, additionally defines reaction on received multicast or unicast EAPOL messages. Valid values are: 0 = Supplicant operation disabled. 1 = Supplicant operation enabled, but responds only to received unicast EAPOL messages. 2 = Supplicant operation enabled, responds to received unicast and multicast EAPOL messages.
DSCPAUD	46	Differentiated Services Code Point for audio. Values range from 0 to 63.
DSCPSIG	34	Differentiated Services Code Point for signaling. Values range from 0 to 63.
DSTOFFSET	1	Used for daylight saving time calculation in hours. Values range from 0 to 2.

7 of 35

Table: Customizable parameters

Parameter name	Default value	Description and value range
DSTSTART	2Sun Mar2L	Used to identify start date for automatic change to Daylight Saving Time. Default string length with a format of either *odddmmmht* or *Dmmmht*, where: *o* = one character representing an ordinal adjective of "1" (first), "2" (second), "3" (third), "4" (fourth) or "L" (last) *ddd* = 3 characters containing the English abbreviation for the day of the week *mmm* = 3 characters containing the English abbreviation for the month *h* = one numeric digit representing the time to make the adjustment, exactly on the hour at hAM (0h00 in military format), where valid values of h are "0" through "9" *t* = one character representing the time zone relative to the adjustment where "L" is local time and U is universal time *D* = one or two ASCII digits representing the date of the month from "1" or "01" to "31", or the character "L", which means the last day of the month)
DSTSTOP	1SunNov2L	Used to identify stop date for automatic change to Daylight Saving Time. Default string length with a format of either *odddmmmht* or *Dmmmht*, where: *o* = one character representing an ordinal adjective of "1" (first), "2" (second), "3" (third), "4" (fourth) or "L" (last) *ddd* = 3 characters containing the English abbreviation for the day of the week *mmm* = 3 characters containing the English abbreviation for the month *h* = one numeric digit representing the time to make the adjustment, exactly on the hour at hAM (0h00 in military format), where valid values of h are "0" through "9" *t* = one character representing the time zone relative to the adjustment where "L" is local time and U is universal time *D* = one or two ASCII digits representing the date of the month from "1" or "01" to "31", or the character "L", which means the last day of the month)
DTMF_PAYLOAD_TYPE	120	RTP dynamic payload used for RFC 2833 signaling. Range is 96 to 127.

Table: Customizable parameters

Parameter name	Default value	Description and value range
ENABLE_AUTOMATIC_ON_THE_PHONE_PRESENCE	0	This parameter controls whether "on the phone" presence status is sent out automatically when user whose presence is tracked is on a call (or goes off-hook). Calls on bridged line appearances (that local user has not bridged to) do not affect the trigger of the "on the phone" presence update. 0=Disabled: The deskphone does not report presence information. 1=Enabled: The deskphone reports presence information.
ENABLE_CALL_LOG	1	Enable or disable complete Call Log application. If disabled no calls are logged, screens related to Call Log are not displayed to user, and menu items of User Interface to set Call Log options are not displayed. Values are 0=disabled; 1=enabled.
ENABLE_CONTACTS	1	Enable or disable complete Contact application. If disabled no contacts are downloaded during initialization from PPM, screens related to Contacts application are not displayed to user, and menu items of the User Interface to set Contacts options are hidden. Values are 0=disabled; 1=enabled.
ENABLE_EARLY_MEDIA	1	Flag that indicates if SIP early is enabled. If enabled and 18x progress message includes early SDP, Spark uses that information to open a VoIP channel to the far-end before the call is answered. Values are 0=disabled; 1=enabled.
ENABLE_EXCHANGE_REMINDER	0	Enables popup reminder notifications for Microsoft Exchange calendaring. Values are: 0 = No (Off) 1 = Yes (On).
ENABLE_G711A	1	Enable or disable G711A codec capability of the phone. If the parameter is set to 1, the phone includes G711A capability in an outbound INVITE request, and accepts G711A when received in an incoming INVITE request. Values are 0=disabled; 1=enabled.
ENABLE_G711U	1	Enable or disable G711U codec capability of the phone. If the parameter is set to 1, the phone includes G711U capability in an outbound INVITE request, and accepts G711U when received in an incoming INVITE request. Values are 0=disabled; 1=enabled.

Table: Customizable parameters

Parameter name	Default value	Description and value range
ENABLE_G722	0	Enable or disable G722 capability of the deskphone. If the parameter is set to 1, the phone includes G722 capability in an outbound INVITE request, and accepts G722 when received in an incoming INVITE request. If set to 0, processing of G722 as a capability is disabled. Values are 0=disabled, off; 1=enabled, on.
ENABLE_G726	1	Enable or disable G726 capability of the deskphone. If the parameter is set to 1, the deskphone includes G726 capability in an outbound INVITE request, and accepts G726 when received in an incoming INVITE request. Values are 0=disabled, off; 1=enabled, on.
ENABLE_G729	1	Enable or disable G729A codec capability of the phone. Values are: 0=G.729 disabled. If set to 0, processing of G729A as a capability is disabled. 1 = The phone advertises a preference for "G.729(A) enabled, without Annex B support" in an outbound INVITE request, and accepts either G729A or G729A with annex B support [G.729AB] when received in a 200OK response or an incoming INVITE request. If set to 1, Incoming INVITE request: the phone accepts either G729(A) or G729AB. 2 = The phone advertises a preference for "G.729(A) enabled, with Annex B support [G.729AB]"in an outbound INVITE request, and accepts either G729A or G729AB when received in a 200OK response or an incoming INVITE request. If the parameter is set to 2, Incoming INVITE request: the phone accepts either G729A or G729AB.
ENABLE_HOLD_BUTTON	1	Specifies whether a Hold softkey will be displayed during an active call. 0= A Hold softkey will not be displayed 1= A Hold softkey will be displayed (default)
ENABLE_MODIFY_ CONTACTS	1	Enable or disable the ability to modify contacts if the Contact application is enabled. Values are 0=disabled; 1=enabled.
ENABLE_PHONE_LOCK	0	Enables the local Phone Lock feature. Values are: 0 = Lock Softkey and Feature Button are not displayed. 1= Lock Softkey and Feature Button are displayed

Table: Customizable parameters

Parameter name	Default value	Description and value range
ENABLE_PRESENCE	1	Enable or disable complete Presence functionality. If disabled, Presence icons do not show in Contacts or Call History Lists, Presence is not displayed to the user, incoming Presence updates are ignored, and menu items of User Interface to set Presence options are not displayed (if available). Values are 0=disabled, off; 1=enabled, on.
ENABLE_PPM_ SOURCED_ SIPPROXYSRVR	1	Enables PPM as a source of SIP proxy server information. Valid values are: 0 = Do not use PPM as a source for SIP proxy server information. 1 = Use PPM for SIP proxy server information.
ENABLE_REDIAL	1	Enable or disable complete Redial functionality. If disabled pressing the redial button has no effect and the redial softkeys and menu items are not displayed. Values are 0=disabled; 1=enabled.
ENABLE_REDIAL_LIST	1	Enables or disables the capability to redial out of a list of recently dialed numbers instead of performing last number redial. Values are 0=disabled (last number redial only is offered to the user); 1=enabled (user can select either last number redial or redial from a list).
ENABLE_REMOVE_ PSTN_ACCESS_PREFIX	0	Enables the removal of the PSTN access prefix from collected dial strings when the phone is communicating with a non-AST controller.Valid values are: 0 = PSTN access prefix digit is not removed; 1 = PSTN access prefix digit is removed from collected digit string before formulating the INVITE for delivery to the controller. (Enabling this parameter when the phone is communicating with an AST-capable controller has no effect).
ENABLE_SERVER_ BASED_PRESENCE	1	Activates/deactivates server based presence. If set to 1 (Enabled), a subscription to presence list and watcher info is done. If set to 0 (Disabled), individual presence subscriptions are done separately to every contact from the contact list.

Table: Customizable parameters

Parameter name	Default value	Description and value range
ENABLE_SIP_USER_ID	0	Activates/deactivates the User ID field on the Login screen. Valid values are: 0=disabled; 1=enabled. If set to 0, user does not see the User ID field on the Login Screen. If set to 1, the user is prompted for the User ID.
ENFORCE_SIPS_URI	1	Controls the enforcement of SIPS URI with SRTP. Valid values are: 0 = Allow either SIP URI or SIPS URI for incoming SRTP media encryption calls and use only SIP URI for outgoing SRTP media encryption calls. 1 = Accept and use only SIPS URI for incoming and outgoing calls with SRTP media encryption.
ENHDIALSTAT	1	Enhanced Dialing Status. Valid range is 0 to 2. If set to “0” the feature is turned off. If set to “1” it is partially enabled (dialing rules do not apply for dialing from Contacts). If set to “2”, the Administering enhanced local dialing feature is fully enabled (dialing rules also apply for dialing from Contacts). Note that If CTDC_SUPPORT is enabled, Enhanced Local Dialing is automatically disabled, independent of the actual setting of ENHDIALSTAT. If CTDC_SUPPORT is disabled, Enhanced Local Dialing is processed as defined by ENHDIALSTAT.
EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD	180	Used to administer how long in seconds the phone re-syncs with the Exchange Server. Values are: 0 to 3600 (seconds).
EXCHANGE_REMINDER_TIME	1	Used to administer how far in advance to remind users of an appointment on their Microsoft Exchange calendar. Values are: 0 to 60 (minutes)
EXCHANGE_REMINDER_TONE	1	Used to indicate whether a tone should accompany a calendar reminder or not. Values are: 0 = No (Off) or 1 = Yes (On).
EXCHANGE_SERVER_LIST	" " (Null)	List of Microsoft Exchange™ server IP or DNS addresses. Used to connect to Microsoft Exchange™ server, for example, to access contacts or calendar data (in case of several entries, the first address is always first, etc.). 0 to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.

Table: Customizable parameters

Parameter name	Default value	Description and value range
EXCHANGE_SNOOZE_TIME	5	Used to administer how long in minutes for the calendar reminder (as set in ENABLE_EXCHANGE_REMINDER and EXCHANGE_REMINDER_TIME to reappear after it has been snoozed (temporally dismissed) by the user. Values are: 0 to 60 (minutes).
EXCHANGE_USER_DOMAIN	" " (Null)	User domain (URL) for Microsoft Exchange™ Server. Range is the default URL string length.
EXTEND_RINGTONE	" " (Null)	Represents a list of XML files, each representing custom ring tone information. Alternate ring tones to replace the standard Avaya ring tones. As of SIP software Release 2.4, Korean ring tones are available as is the ability to specify custom ring tones, as described in Customizing ring tones. A string up to 1023 characters containing up to 8 alternate ring tones in the format *Ringtone1*.xml, *Ringtone2*.xml, or KoreanRT1.xml, KoreanRT2.xml, etc.
FAILBACK_POLICY	"auto"	The policy in effect for recovery from Failover. Valid values are: "admin" = If set to admin, the phone waits for administrative intervention before attempting to failback to a higher priority controller. "auto" = If set to auto, the phone periodically checks the availability of the primary controller and fails back to it if it is available. Note: If set via the settings file this value is given a precedence of 4. If set via PPM in the ListOfMaintenanceData element of the getAllEndpointConfigurationResponse this value is given a precedence of 5.
FAILED_SESSION_REMOVAL_TIMER	30	Timer to automatically remove a failed call session. Range in seconds is 5 to 999.
FAST_RESPONSE_TIMEOUT	4	The value of the Fast Response Timer for Failover. Valid values are: 0 - 32 (seconds). Note: If set via the settings file this value is given a precedence of 4. If set via PPM in the ListOfMaintenanceData element of the getAllEndpointConfigurationResponse this value is given a precedence of 5.
G726_PAYLOAD_TYPE	110	RTP dynamic payload used for G.726. Range is 96 to 127.

Table: Customizable parameters

Parameter name	Default value	Description and value range
GMTOFFSET	0:00	Offset used to calculate time from GMT reference time. Default string length positive or negative number of hours and minutes less than 13 hours. Consists of 1 to 6 characters, optionally beginning with "+" or "-", followed by one or two number digits whose combined value is from "0" to "12" optionally followed by a ":" and two numeric digits whose combined value is from "00" to "59".
GROUP	0	Specific user group as tested in configuration files. Valid values are 0 to 999.
HEADSYS	1	Headset operational mode. One ASCII numeric digit. Valid values are: 0 or 2=General Operation, where a disconnect message returns the deskphone to an idle state. 1 or 3=Call Center Operation, where a disconnect message does not change the state of the deskphone.
HTTPDIR	" " (Null)	HTTP server directory path. The path name prepended to all file names used in HTTP and HTTPS get operations during initialization/HTTP downloads. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required. The command syntax is “GET HTTPDIR *myhttpdir*” where “myhttpdir” is your HTTP server path. HTTPDIR is the path for all HTTP operations.
HTTPEXCEPTION DOMAINS	" " (Null)	Domains to be excluded for SCEP. String representing zero or one domains in a URL of 0 to 255 characters in dotted decimal or DNS name format with multiple domains delimited by commas.
HTTPPORT	80	Destination TCP port used for requests to the HTTP server during initialization. Range is 0 - 65535.
HTTPPROXY	" " (Null)	Zero or one IP or DNS address of the HTTP server for SCEP. 0 to 255 characters in dotted decimal or DNS name format followed by a colon and port number. The colon and port number are optional. If this parameter is not null, this (proxy) transport address is used to set up the HTTP connection as the transport protocol for SCEP.

Table: Customizable parameters

Parameter name	Default value	Description and value range
HTTPSRVR	0.0.0.0	List of IP Address(es) or DNS Name(s) of HTTP file server(s) used to download deskphone files. HTTP server addresses can be in dotted decimal or DNS format, and must be separated by commas (0-255 ASCII characters, including commas).
ICMPDU	1	Controls whether ICMP Destination Unreachable messages will be processed. Values are: 0=DU messages not transmitted 1= DU messages not transmitted in response to specific events 2= DU message with code 2 will be transmitted in case of specific events
ICMPRED	0	Controls whether ICMP Redirect messages will be processed. Values are: 0 = Redirect messages will neither be transmitted nor received Redirect messages will be supported 1 = Redirect messages will not be transmitted, but received Redirect messages will be supported per RFC 1122
INGRESS_DTMF_VOL_LEVEL	-12	RFC 2833 Digit event "volume" level. The power level of the tone, expressed in dBm0 after dropping the sign. (from RFC 2833 section 3.5 "Payload Format." Values are: -20 to -7.
INTER_DIGIT_TIMEOUT	5	This is the timeout that takes place when user stops inputting digits. The timeout is treated as digit collection completion, and when it occurs, the application sends out an invite. Range in seconds of 1 to 10.
IPADD	0.0.0.0	IP Address of the deskphone. Range is 7 to 15 ASCII characters (less than the default string length) defining one IP Address in dotted-decimal format.
L2Q	0	Requests 802.1Q tagging mode (auto/on/off). Values are: 0 = auto 1 = on 2 = off
L2QAUD	6	Layer 2 audio priority value. Range from 0 to 7.
L2QSIG	6	Layer 2 signaling priority value. Range from 0 to 7.

Table: Customizable parameters

Parameter name	Default value	Description and value range
L2QVLAN	n/a	802.1Q VLAN Identifier (0 to 4094). Null (" ") is not a valid value and the value cannot contain spaces. This parameter is preserved in RAM which survives reset and stored to flash (as L2QVLAN_INIT) only upon successful registration. This value is initialized from L2QVLAN_INIT after power-up. This value will not be initialized from L2QVLAN_INIT after reset, but can be modified using the ADDR craft procedure.
LANGLARGEFONT	" " (Null)	Filename or URL of the file that contains the large language font.
LANG0STAT	1	This flag defines, whether or not the built-in English is offered to the user as selectable item in the language selection UI menu. At least one other language file must be downloaded, before "not offering" built-in English. Values are 0=not offered; 1=selectable.
LANGUAGES	" " (Null)	List of links to language files to be downloaded. Substrings are delimited by commas. Maximum length is 1023 characters. Each substring shall follow one of the these naming rules: A substring is identical to a file name without any prefix specifying the path or server: The files are downloaded from the same source as the setting file(s). A substring can provide a prefix to the file name, which specifies the relative path ("./" for next higher directory level) from the directory the settings file(s) has been downloaded to the directory the language file shall be download. A substring specifies the completed URL to the language file including protocol identifier ("http://" or "https://"), server and path.
LLDP_ENABLED	2	Flag to enable/disable LLDP (Link Layer Discovery Protocol). Valid values are: 0 = disabled; the deskphone will not support LLDP. 1 = enabled; the deskphone will support LLDP. 2 = auto; the deskphone will support LLDP, but the transmission of LLDP frames will not begin until or unless an LLDP frame is received.
LOCAL_DIAL_AREA_CODE	0	Indicates whether user has to dial the area code for calls within the same area code. Valid values are: 0 = User does not need to dial local area code. 1 = User must dial the area code for local calls.

Table: Customizable parameters

Parameter name	Default value	Description and value range
LOCAL_LOG_LEVEL	3	Numerical code of severity level. Store entries to the local event log, if event occurs with a severity level whose numerical code is equal to or less than the LOCAL_LOG_LEVEL value. Values are: 0 (emergencies), 1 (alerts), 2 (critical), 3 (errors), 4 (warning), 5 (notice), 6 (informational), 7 (debug).
LOG_CATEGORY		Comma-separated list of keywords in standard string format representing logging categories (software modules or functions to be included in lower level logging). Logging implementation blocks all traces at level "Warning" or lower, unless the category corresponding to a given trace is enabled. If the LOCAL_LOG_LEVEL is set to "Warning" or lower, this parameter would enable low-level traces from the adaptors or manager as indicated. Applies to all logging mechanisms (syslog and local log). Example: "ALSIP, SESSION" enables debug level traces from the ALSIP adaptor and Session manager.
LOGOS	" " (Null)	List of custom logo definitions used as background on display. Each logo tuple is delimited by commas. Each logo tuple contains logo label (verbatim label displayed on the screen) and logo URL. Logo label and URL are separated from one another by a '='. String maximum of 1023 characters.
LOGSRVR	" " (Null)	Syslog server IP or DNS address. 0 to 255 characters: zero or one IP Addresses in dotted decimal or DNS name format.
MEDIAENCRYPTION	9	This parameter sets the cryptosuite and session parameters for SRTP. The parameter can have one or two of the following nine values (separated by commas without any intervening spaces): 1=aescm128-hmac80 2=aescm128-hmac32 3=aescm128-hmac80-unauth 4=aescm128-hmac32-unauth 5=aescm128-hmac80-unenc 6=aescm128-hmac32-unenc 7=aescm128-hmac80-unenc-unauth 8=aescm128-hmac32-unenc-unauth 9=none

Table: Customizable parameters

Parameter name	Default value	Description and value range
MSGNUM	" " (Null)	Voice mail system telephone/extension number. Used for non-failover situations. Specifies the number to be dialed automatically when the deskphone user presses the **Message** button. Note: Set via the following mechanisms in precedence order (highest to lowest); for Release 2.6+- PPM, settings file and DHCP.
MTU_SIZE	1500	Maximum Transmission Unit size. Range is 1496 or 1500 only octets.
MWISRVR	" " (Null)	List of Message Waiting Indicator Event Server IP or DNS address(es). Used to register for MWI event notifications (in case of several entries first address always first, etc.). In some third-party proxy environments the SIP proxy/registrar may be different than the MWI server. In this case, the MWI server is set via this parameter. If both functions are provided by the same server, it is not necessary to set MWISRVR. The SIP proxy server (controller) is then used for MWI indications. Zero to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. if operating in a non-Avaya environment, this value is set via a SET command in the settings file, otherwise the address of SIP Proxy server (controller) is used.
MYCERTCAID	CAIdentifier	Certificate Authority Identifier. String identifying whether the endpoints can work with another certificate authority.
MYCERTCN	$SERIALNO	Common name (CN) for SUBJECT in SCEP certificate request. Values are: $SERIALNO = the phone's serial number is included as CN parameter in the SUBJECT of a certificate request. $MACADDR = the phone's MAC address is included as CN parameter in the SUBJECT in the certificate request.
MYCERTDN	" " (Null)	Common part of SUBJECT in SCEP certificate request. String which defines the part of SUBJECT in a certificate request (including Organizational Unit, Organization, Location, State, Country), of 0 to 255 characters, starting with / and separating items with /.

Table: Customizable parameters

Parameter name	Default value	Description and value range
MYCERTKEYLEN	1024	Private Key length in range of 1024 to 2048.
MYCERTRENEW	90	Threshold to renew certificate (given as percentage of device certificate's Validity Object). Range is 1 to 99.
MYCERTURL	" " (Null)	URL of SCEP server. String representing zero or one URI starting with "http://", 0 to 255 characters.
MYCERTWAIT	1	Flag defining phone's behavior when performing certificate enrollment. Values are: 0=wait until a certificate or a denial is received or a pending notification is received 1=periodical check in the background
NETMASK	0.0.0.0	IP subnet mask. Range is 7 to 15 ASCII characters defining one IP Address in dotted-decimal format.
NETWORK_PROGRESS_TONE_HANDSET_LEVEL	0	Handset Progress tone level adjust. Values are: 0 = NORMAL level for most users (default) 1 = nominal value 3 Db louder than default value 2 = nominal value 6 Db louder than default value 3 = nominal value 9 Db louder than default value 4 = nominal value 12 Db louder than default value 5 = nominal value 15 Db louder than default value 6 = nominal value 18 Db louder than default value
NETWORK_PROGRESS_TONE_HEADSET_LEVEL	0	Headset Progress tone level adjust. Values are: 0 = NORMAL level for most users (default) 1 = nominal value 3 Db louder than default value 2 = nominal value 6 Db louder than default value 3 = nominal value 9 Db louder than default value 4 = nominal value 12 Db louder than default value 5 = nominal value 15 Db louder than default value 6 = nominal value 18 Db louder than default value
NETWORK_PROGRESS_TONE_SPEAKER_LEVEL	0	Speaker Progress tone level adjust. Values are: 0 = NORMAL level for most users (default) 1 = nominal value 3 Db louder than default value 2 = nominal value 6 Db louder than default value 3 = nominal value 9 Db louder than default value 4 = nominal value 12 Db louder than default value 5 = nominal value 15 Db louder than default value

Table: Customizable parameters

Parameter name	Default value	Description and value range
NO_DIGITS_TIMEOUT	20	Number of seconds of delay after going "off-hook" or getting secondary dial tone before phone automatically plays a warning tone and does not accept dial input any longer. Range in seconds is 1 to 60.
OUTBOUND_ SUBSCRIPTION_ REQUEST_DURATION	86400	Number of seconds used in initial SUBSCRIBE messages. This is the suggested duration value of the deskphone, which might be lowered by the server, depending on the server configuration. Range is 60-31536000. Note that the default value is equal to one day and the maximum value represents one year.
PHONE_LOCK_ IDLETIME	0	Sets the idle time for the Phone Lock feature. Values are: 0 = the phone does not lock. 1-999 - the phone locks after this value (in minutes).
PHNCC	1	Telephone country code. The administered international country code for the location by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1-3 digits, from “1” to “999.”
PHNDPLENGTH	5	Internal extension deskphone number length. Specifies the number of digits associated with internal extension numbers by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from “3” to “13.”
PHNEMERGNUM	" " (Null)	Emergency Number. 0 to 30 dialable characters (0-9, *, and #). This number is dialed when the Emergency softkey is pressed, or when a pop-up screen for making an emergency calls is confirmed.
PHNMOREEMERGNUMS	NULL	Lets you add up to 9 additional emergency numbers separated with a comma. This emergency numbers can be dialed manually even if phone is locked or unregistered.
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.

Table: Customizable parameters

Parameter name	Default value	Description and value range
PHNLAC	" " (Null)	String representing the local area code. When set, this parameter indicates the endpoint's local area code, which, along with the configuration parameter LOCAL_DIAL_AREA_CODE allows users to dial local numbers with more flexibility.
PHNLD	1	Telephone long distance access code. The digit, if any, dialed to access public network long distance trunks. Range: 1 digit (0 to 9) or " " (Null). Needed for "Enhanced Local Dialing Algorithm".
PHNLDLENGTH	10	Length of national telephone number. The number of digits in the longest possible national telephone number. Range: 5 to 15. Needed to for "Enhanced Local Dialing Algorithm".
PHNOL	9	Outside line access code. The character(s) dialed, including # and *, if any, to access public network local trunks. Range: 0-2 dialable numeric digits, including " " (Null).
PHNNUMOFSA	" " (Null)	When ENABLE_AVAYA_ENVIRONMENT=0, this value sets the number of Session Appearances. When the phone is in AST environment (registered to a proxy with PPM server and Avaya CM on the background), the phone will use the number of call appearances sent by PPM (i.e. call-appearance provisioned on the CM). In case this parameter is set the phone updates this parameter and uses it after failover to a secondary proxy. In this case, PPM will have a higher priority than the settings file for this parameter. When the primary controller is set as a non-AST proxy (a proxy without PPM and no CM in the background, the phone is in a non-AST environment); in this case the phone used this parameter to set its call-appearance.

Table: Customizable parameters

Parameter name	Default value	Description and value range
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). Speed and duplex issues are summarized and the best practice is provided in the *Avaya Application Solutions: IP Telephony Deployment Guide*, Document Number 555-245-600 Issue 6, January 2008 on page 290. This document is available from the Avaya support website.
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, for post-Release S1.0 use, 6=1000Mbps full-duplex (if supported by the hardware). Speed and duplex issues are summarized and the best practice is provided in the *Avaya Application Solutions: IP Telephony Deployment Guide*, Document Number 555-245-600 Issue 6, January 2008 on page 290. This document is available from the Avaya support website.
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.

Table: Customizable parameters

Parameter name	Default value	Description and value range
POE_CONS_SUPPORT	1	Flag to activate Power over Ethernet conservation mode. Valid values are: 0 = the deskphone does not support power conservation mode. 1 = the deskphone indicates support of power conservation mode by transmission of LLDP frames with appropriate indication in Avaya/Extreme proprietary PoE Conservation Support Level TLV. The deskphone supports power conservation mode, if requested by reception of an LLDP frame with Avaya/Extreme proprietary PoE Conservation Level Request.
PRESENCE_SERVER	" " (Null)	0 to 255 characters: one IP address in dotted decimal or DNS name format, with an optional port (separated from the address by a colon). Used to access a server for presence indications. In some environments the address of the SIP proxy/registrar may be different than the presence server. In this case the presence server is set via this parameter. If both addresses are the same, it is not necessary to set PRESENCE_SERVER (shall remain null).
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	Controls access to Craft local (dialpad) administrative procedures. Values are: 0 = Full access to craft local procedures 1 = restricted access to craft local procedures

Table: Customizable parameters

Parameter name	Default value	Description and value range
PROVIDE_EDITED_ DIALING	2	Controls whether edited dialing is allowed and whether on-hook dialing is disabled. Valid values are: 0 = Disable edit dialing. "Dialing Options" is not displayed to the user so the user cannot change edit dialing; the deskphone defaults to on-hook dialing. 1 = Disable on-hook dialing and do not display "Dialing Options" to the user so the user cannot change edit dialing; the deskphone defaults to edit dialing. 2 = Display "Dialing Options" to allow user to change from on-hook to edit dialing. This is the default. 3 = Display "Dialing Options" to allow user to change from edit dialing to on-hook dialing; the deskphone defaults to edit dialing.
PROVIDE_EXCHANGE_ CALENDAR	1	Flag to define whether or not menu item(s) for Microsoft Exchange® Calendar integration are provided to user. Values are: 0=off; 1=on.
PROVIDE_ LOGOUT	1	Flag to define whether or not logout function is provided to user. If disabled and phone is operating in user mode, hide "Logout" item in option menu. Values are: 0=off; 1=on.
PROVIDE_ NETWORKINFO_ SCREEN	1	Flag to define whether or not "Network Information" menu is provided to user. If disabled and phone is operating in user mode, hide complete "Network Information". Values are: 0=off; 1=on.
PROVIDE_OPTIONS_ SCREEN	1	Flag to define whether or not "Options & Settings" menu is provided to user. If disabled and phone is operating in user mode, hide complete "Option & Settings" menu tree. Values are: 0=off; 1=on.
PROVIDE_TRANSFER_ TYPE	0	Flag to determine whether user can select a Transfer Type (Attended/Unattended). Applies to failover environments only. Value is: 0=user cannot select a transfer type, transfer type not shown.
PSTN_VM_NUM	" " (Null)	Telephone number to be used by the messaging application in a non-Avaya or failover server environment. A "dialable" string representing deskphone number or Feature Access Code. This dialable string is used to call into the messaging system (e.g. when pressing the Message Waiting button).

Table: Customizable parameters

Parameter name	Default value	Description and value range
PUSHCAP	00000	String representing push capabilities. Applies to phones running software Release 2.2 only. Values are: 5 ASCII numeric digits, "00000" to "22222".
PUSHPORT	80	String representing the TCP listening port number used for the deskphone's HTTP server. Applies to phones running software Release 2.2 only. Values are: 2 to 5 ASCII numeric digits, "80" through "65535".
RDS_INITIAL_RETRY_ ATTEMPTS	15	Indicates how many times the PPM adaptor should try to download from PPM before giving up on connecting to the PPM server. Values are: 1-30.
RDS_INITIAL_RETRY_ TIME	2	Remote Data Source initial retry time in seconds; indicates the initial delay for a retry to connect to the PPM server. Valid range is 2-60 (seconds).
RDS_MAX_RETRY_TIME	600	Remote data source maximum retry time; indicates the maximum delay interval (in seconds) before giving up on PPM server connection. Values are: 2-3600 (seconds). Software Release 2.5 lowers the minimum value from 300 to 2 seconds to allow the phone to operate in the "older" R2.4 manner by setting the PPM retry parameters to: SET RDS_INITIAL_RETRY_ATTEMPTS 10 SET RDS_INITIAL_RETRY_TIME 2 SET RDS_MAX_RETRY_TIME 2
RECOVERYREGISTER WAIT	60	Reactive monitoring interval in seconds for Failover. Valid values are: 10 - 36000 Note: If set via the settings file this value is given a precedence of 4. If set via PPM in the ListOfMaintenanceData element of the getAllEndpointConfigurationResponse this value is given a precedence of 5.

25 of 35

Table: Customizable parameters

Parameter name	Default value	Description and value range
REDIRECT_TONE	1	A single "boop" of call coverage tone played when at least one of the provisional responses is a 181 Call Forwarded and no RTP packets are received; afterwards the deskphone continues playing ringback. If the 181 Call Forwarded response includes early media SDP (implying that an RTP stream is being received) the phone interrupts the RTP stream to play the call coverage tone. This value represents the call coverage tone ID. Valid values are: 1 = Frequency 440 Hz, Cadence 600 ms, then off. 2 = Frequency 425 Hz, Cadence 200 ms, then off. 3 = Frequency 440 + 480 Hz, Cadence 400 ms, then off. 4 = Frequency 1700 Hz, Cadence 2 seconds, then off.
REGISTERWAIT	900	Number of seconds for next re-registration to SIP server. The default value for software Release 2.4+ was originally set to 300 to accommodate UDP, however, TCP/TLS is the recommended arrangement and is the most typical configuration; the default was changed from 300 to 900 seconds for software Release 2.5+. UDP arrangements can be handled by setting the value of the parameter to a lower value in the settings file. Range in seconds: 30 to 86400
REUSETIME	60	IP address reuse timeout, in seconds. Values are: 0, 20-999. Note that this value can also be set via Option# 242 in a DHCPACK message.
ROUTER	0.0.0.0	Address(es) of default router(s) / gateway(s) in the IP network. Range is 7-127 characters defining one or more IP Addresses in dotted decimal format, separated by commas without any intervening spaces.
RTCPCONT	1	Enables/disables the RTCP in parallel to RTP audio streams. Values are 0=RTCP disabled, 1=RTCP enabled.

Table: Customizable parameters

Parameter name	Default value	Description and value range
RTCPMON	" " (Null)	RTCP Monitor IP or DNS address to be used as destination for RTCP monitoring. Zero to 255 characters: zero or one IP addresses in dotted decimal or DNS name format. Note that this value is only set via SET command in settings file if operating in a NON-Avaya environment, otherwise this value is retrieved via PPM.
RTCPMONPERIOD	5	RTCP Monitor report period. Valid range = 5 - 30 Interval in seconds for sending out RTCP monitoring reports.
RTCPMONPORT	5005	RTCP monitor port number. TCP/UDP port to be used as destination port for RTCP monitoring. Valid range is 0-65535. Note that this value is only set via SET command in settings file if operating in a NON-Avaya environment, otherwise this value is retrieved via PPM.
RTP_PORT_LOW	5004	Specifies lower limit of a port range to be used by RTP/RTCP or SRTP/SRTCP connections, for example, to adapt to firewall traversal policies. Values: 1024-65503.
RTP_PORT_RANGE	40	Specifies the width of the port range to be used by RTP/RTCP or SRTP/SRTCP connections, for example, to adapt to firewall traversal policies. The upper limit is calculated by the value of RTP_PORT_LOW plus the value of RTP_PORT_RANGE, taking into consideration the overall limit of 65535. Values: 32-64511.
SCREENSAVERON	240	Number of idle time minutes after which the screen saver is turned on. Valid values range from zero (disabled) to 999 minutes (16.65 hours).
SDPCAPNEG	0 (Release 2.5) 1 (Release 2.6+)	Controls SDP capability negotiation; interaction between the SDPCAPNEG and MEDIAENCRYPTION parameters controls INVITE behavior. Valid values are: 1 = SDP capability negotiation is enabled. 0 = SDP capability negotiation is disabled.

Table: Customizable parameters

Parameter name	Default value	Description and value range
SEND_DTMF_ TYPE	2	Defines whether DTMF tones are send in-band (regular audio) or out-band (negotiation and transmission of DTMF according to RFC 2833, with fallback to send in-band DTMF tones, if far end does not support RFC2833). Values are 1=in-band DTMF; 2=RFC2833 procedure.
SIG	0	Parameter indicating which Software Distribution Package to download during start-up or reboot; indicates which of the specific configuration sets for H323 or SIP endpoints applies. 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=H323 2=SIP
SIG_PORT_LOW	1024	Lower limit of port range for signaling to support by the phone. Values range from 1024 to 65503.
SIG_PORT_RANGE	64511	Port range for signaling to support by the phone. Values range from 32 to 64511.
SIMULTANEOUS_ REGISTRATIONS	3	Defines the number of simultaneous Session Manager registrations that the phone should maintain. Valid values are 1-3.

Table: Customizable parameters

Parameter name	Default value	Description and value range
SIP_CONTROLLER_LIST	" " (Null)	Configured Controller list. A comma-separated list of SIP controller designators, without any intervening spaces, where each controller designator has the following format: host[:port][;transport=xxx] host is an IP address in dotted-decimal format. (DNS name format is not supported). [:port] is an optional port number. [;transport=xxx] is an optional transport type where xxx can be tls, tcp, or udp. If a port number is not specified a default value of 5060 for TCP and UDP or 5061 for TLS is used. If a transport type is not specified, a default value of tls is used. The value can contain 0 to 255 characters; the default value is null (""). If null, DHCP/DNS will provide the defaults.
SIP_MODE	0	SIP operational mode. Determines whether the deskphone uses a proxy to receive incoming calls or can receive calls directly from another deskphone. Values are: 0=proxy mode; the phone operates in proxy mode with SIP proxy/registrar, 1=peer-to-peer mode; the phone operates in peer-to-peer mode between SIP endpoints.
SIP_PORT_SECURE	5061	The phone's listening port for inbound connections (for secure message transfer via TLS). Values range from 1024 - 65535.
SIPCONFERENCECONTINUE	0	When the ENABLE_AVAYA_ENVIRONMENT parameter is 0 (non-Avaya environment) and the telephone initiating the conference ends the call, the other parties will be dropped unless SIPCONFERENCECONTINUE is set to 1 (continue conference call without initiator). If this parameter is set to 0, the capability is turned off and the phone ends the conference when the initiator hangs up.
SIPDOMAIN	" " (Null)	SIP domain name for registration. 0 to 255 characters: string representing domain name.
SIPPORT	5060	The phone's listening port for inbound connections (for non-secure message transfer only). Values range from 1024 - 65535.

Table: Customizable parameters

Parameter name	Default value	Description and value range
SIPREGPROXYPOLICY	"alternate"	SIP registration proxy policy. A policy to control how the phone treats the list of controllers/servers in the SIP_CONTROLLER_LIST parameter. Valid values are: "alternate" = This is the preferred registration method with SIP proxy controllers. If there is no Active Controller, then all Configured Controllers are Monitored Controllers. If there is an Active Controller, the Monitored Controllers are all controllers whose priority is higher than the current Active Controller. "simultaneous" = All controllers in the configured controller list are Monitored Controllers.
SKINS	" " (Null)	Applicable to the SIP 9640 IP Telephone only. Represents a list of skin information tuples. Each skin information is a pair of {skin label, skin URL} data. Each skin tuple is delimited by commas. Each skin tuple contains skin label (verbatim label displayed on the screen) and skin URL. Skin label and URL are separated by a ' ='. The URL may be specified in an absolute or relative path format (“./” for next higher directory level in relative path format; origin is the directory specified by HTTPDIR or TLSDIR depending on download via http or https). String maximum is 1023 characters. Example: Yankees (Color)=http://svn.avaya.com/drop/skins/yankees_color/boohisscolor.xml
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 and no intervening spaces.
SNMPSTRING	" " (Null)	Text string containing the SNMP community name string (up to 32 ASCII characters, no spaces).
SNTPSRVR	" " (Null)	Used to retrieve date and time via SNTP (in case of several entries first address always first, etc.). Zero to 255 characters: zero or more IP Addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.

Table: Customizable parameters

Parameter name	Default value	Description and value range
SPEAKERSTAT	2	Limits the hands-free audio operation mode. Valid values are: 0=no speakerphone allowed 1=one-way speakerphone operation allowed (monitor) 2=two-way speakerphone operation allowed
SUBSCRIBELIST	" " (Null)	String representing the Push subscription list. Applies to phones running software Release 2.2 only. Values are: 0 to 255 ASCII characters: zero or more URLs separated by commas without any intervening spaces.
SUBSCRIBE_SECURITY	2	Controls the use of SIP and SIPS subscriptions. Valid values are 0 - 2: If=0, the phone uses SIP for both the Request URI and the Contact Header regardless of whether SRTP is enabled. If=1, the phone uses SIPS for both the Request URI and the Contact Header if SRTP is enabled (TLS is on and MEDIAENCRYPTION has at least one valid crypto suite). If=2 and the SES/PPM does not show a FS-DeviceData FeatureName with a FeatureVersion of 2 in the response to the getHomeCapabilities request (indicative of SES/PPM 4.0), the phone uses SIP for both the Request URI and the Contact Header. If=2 and the SES/PPM does show a FS-DeviceData FeatureName with a FeatureVersion of 2 or greater in the response to the getHomeCapabilities request, the phone uses SIPS for both the Request URI and the Contact Header if SRTP is enabled (TLS is on and MEDIAENCRYPTION has at least one valid crypto suite).
SUPPORT_GIGABIT	0	Flag indicating whether the deskphone supports GigE (Gigabit Ethernet). Valid values are: 0=Telephone does not support GigE 1=Telephone supports GigE
SYMMETRIC_RTP	1	Enforces RTP on the same port. Values are 0 -1.

Table: Customizable parameters

Parameter name	Default value	Description and value range
SYSTEM_ LANGUAGE	" " (Null)	System Default Language definition. String representing a file name (shall be identical to one of the file names received via LANGUAGES parameter or null).
TCP_KEEP_ALIVE_ INTERVAL	10	Time interval (number of seconds) after which TCP keep-alive packets are re-transmitted. The interval is started by the system TCP/IP stack (when TCP keep-alive is enabled with specified time intervals). Values are 5-60 seconds.
TCP_KEEP_ALIVE_ STATUS	1	Indicates whether TCP/IP keep-alive should be enabled at the system. Values are 0=TCP keep alive disabled, 1=TCP keep alive enabled.
TCP_KEEP_ALIVE_TIME	60	This time interval is the time 9600 Series IP Deskphones will wait before sending out a TCP keep-alive message (TCP ACK message) to the far-end. The time is controlled by the system's TCP/IP stack. The timer is restarted after application level data (for example, a SIP message) is sent over the socket. When the system is idle, this keep-alive time expires and results in sending a TCP ACK (keep-alive) packet. Valid values are 10-3600 (seconds).
TIMEFORMAT	0	Display time according to defined format in the top line and in the call log. Values are: 0=am/pm format 1=24h format
TLSDIR	" " (Null)	Path name for https downloads. Character string of 0 to 127 characters representing a directory name or path to directory.
TLSPORT	443	Destination TCP port used for requests to https server during initialization. Values: 0-65535.
TLSSRVRID	1	Flag to indicate if TLS server identification is required. Valid values are: 0 = no certificate match necessary; TLS/SSL connection will be established anyway. 1 = certificate match required; TLS/SSL connection will only be established if the server's identity matches the server's certificate.

Table: Customizable parameters

Parameter name	Default value	Description and value range
TPSLIST	" " (Null)	String representing the Trusted push server list. Applies to phones running software Release 2.2 only. Values are: 0 to 255 ASCII characters: zero or more domain/path strings, separated by commas without any intervening spaces.
TRUSTCERTS	" " (Null)	File names of certificates to be used for authentication. List of file names separated by commas (0 to 1024 characters).
USE_EXCHANGE_CALENDAR	0	Flag, that indicates whether calendar data retrieval from Exchange is selected or not. Values are: 0 (Disabled) or 1 (Enabled).
USE_QUAD_ZEROS_FOR_HOLD	0	Flag that indicates whether a= directional attributes or 0.0.0.0 IP Address is used in the SDP to signal hold operation. 0=use “a= directional attributes”, 1=use quad zeros.
VLANSEP	1	Enables or disables VLAN separation. Controls whether frames received from the line interface are forwarded to the phone or to the secondary Ethernet interface based on VLANID. Also affects whether frames received on the secondary Ethernet interface are changed before forwarding to the line interface. Values are: 1=On/Enabled, 0= Off/Disabled. This parameter is used with several related parameters. For more information, see VLAN separation rules and related parameters on page 122.
VLANTEST	60	Number of seconds to wait for a DHCPOFFER when using a non-zero VLAN ID (1-3 ASCII digits, from “0” to “999”).
WAIT_FOR_REGISTRATION_TIMER	32	Time in seconds the SIP application will wait for a register response message. If no message is received, registration is retried. Range is 4-3600 (seconds).
WAIT_FOR_UNREGISTRATION_TIMER	32	Time the SIP application waits before declaring un-registration to be complete. Under normal circumstances un-registration includes termination of all active SIP dialogs, and SIP registration. Range is 4-3600 (seconds).

33 of 35

Table: Customizable parameters

Parameter name	Default value	Description and value range
WMLEXCEPT	" " (Null)	Exceptions domains for the WML browser proxy server. If WMLPROXY is resolved and WMLEXCEPT is null, the HTTP proxy server defined by WMLPROXY is used for all transactions of the WML browser application. If WMLEXCEPT is not null, the HTTP proxy server is only used for the URLs whose domains are not on the WMLEXCEPT list. Format is zero or more strings in DNS format, separated by commas without any intervening spaces.
WMLHOME	" " (Null)	Home page for WML browser. If this parameter is null, the deskphone will not display the browser option under the "A" Avaya Menu. If non-null the URL specified is retrieved via HTTP and rendered in the Web page display area, when the WML browser application is initially accessed. Value is zero or one URL.
WMLIDLETIME	10	Number of minutes of inactivity until the Web browser will display the idle URL. When the Web idle timer reaches the number of minutes equal to this parameter, the deskphone sends an HTTP GET for the URI specified by WMLIDLEURI. Valid value is 1-999. Note that the web idle timer starts only when access to the WML browser is provided by an application line under the "A" Avaya Menu and the parameter WMLIDLEURI is non-null.
WMLIDLEURI	" " (Null)	URL of web page displayed after idle timer expires. Note that the web idle timer will only be started when access to the WML browser is provided by an application line under the "A" Avaya Menu and the parameter WMLIDLEURI is non-null. Value is zero or one URL.
WMLPORT	8080	TCP port number to be used to access the HTTP proxy server by the WML browser application (if defined by WMLPROXY). Valid value is 0 - 65535.

Table: Customizable parameters

Parameter name	Default value	Description and value range
WMLPROXY	" " (Null)	Address of WML proxy server. WMLPROXY is used as the HTTP proxy server by the WML browser application. If WMLPROXY is null, or if WMLPROXY cannot be resolved into a valid IP address, an HTTP proxy server is not used. Value is zero or one IP address in dotted decimal or DNS name format. Note that WMLPROXY defines the HTTP proxy server for WML browser application and HTTPPROXY to perform SCEP certificate enrollment.

35 of 35

Note:

Unless otherwise indicated, Table 12 applies to all 9600 Series IP Deskphones. Certain SIP-based 9600 Series IP Deskphones might have additional or optional information that you can administer. For more information, see Chapter 9: Administering Deskphone Options.

Administering a VLAN

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

About VLAN tagging

IEEE 802.1Q tagging (VLAN) is a useful method of managing VoIP traffic in your LAN. Avaya recommends that you establish a *voice* VLAN, set L2QVLAN to the VLANID of that VLAN, and provide voice traffic with priority over other traffic. You can set VLAN tagging manually, by DHCP, or in the 46xxsettings.txt file.

If VLAN tagging is enabled (L2Q= 0 or 1), 9600 Series IP Deskphones set the VLAN ID to L2QVLAN, and the VLAN priority for packets from the deskphone to L2QAUD for audio packets and L2QSIG for signalling packets. The default value (6) for these parameters is the recommended value for voice traffic in IEEE 802.1D.

Regardless of the tagging setting, 9600 Series IP Deskphones will always transmit packets from the deskphone at absolute priority over packets from the secondary Ethernet interface (for example, 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 switch port default VLAN ID without changing the user priority of the frame.

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 deskphone returns to the default VLAN if an invalid VLAN ID is administered or if the phone moves to a port where the L2QVLAN value is invalid. The default value 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 deskphone restarts for any reason and the VLANTEST time limit expires, the deskphone assumes the administered VLAN ID is invalid. The deskphone then initiates operation with a VLAN ID.

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 deskphone does not return to the default VLAN.

Important:
If a VLAN ID is provisioned using DHCP, then L2QVLAN and VLANTEST must be provisioned in all DHCP servers that the phone can potentially use.

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 9600 Series IP Deskphones transmit DHCP messages with IEEE 802.1Q tagging and the VLAN ID set to L2QVLAN. The deskphones will continue to do this for VLANTEST seconds.

- If L2Q=1 and the VLANTEST timer expires because a DHCPOFFER has not been received, the deskphone 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 deskphone 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 deskphone will get a response to a DHCPDISCOVER when it makes that request on the default (0) VLAN.

After VLANTEST expires, if 9600 Series IP Deskphones receives a non-zero L2QVLAN value, the deskphone will release the IP Address and send DHCPDISCOVER on that VLAN. Any other release will require a manual reset before the deskphone will attempt to use a VLAN on which VLANTEST has expired. See the Reset procedure in Chapter 3 of the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694).

The deskphone ignores any VLAN ID administered on the Communication Manager call server.

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.

VLAN separation rules provides several VLAN separation guidelines.

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: 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 to the network. 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 PHY2LAN value and the priority value is equal to the PHY2PRIO value. Tagged Frames received on the line interface: 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 deskphone if the VLAN ID equals the VLAN ID used by the deskphone. Untagged frames are not changed 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 be forwarded to the secondary Ethernet interface or to the deskphone as determined by the forwarding logic of the Ethernet switch, but the tag will still be removed from frames that egress from the secondary Ethernet interface.
VLANSEP is “1” (On/Enabled)	**AND** the deskphone is not tagging frames, **OR** if the deskphone is tagging frames with a VLAN ID equal to PHY2VLAN, **OR** if the PHY2VLAN value is zero.	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.

1 of 2

If		Then
VLANSEP is “0”,	**OR** the deskphone is not tagging frames, **OR** the deskphone is tagging frames with a VLAN ID equal to PHY2VLAN.	Frames forwarded to the network from the secondary Ethernet interface will not be changed before forwarding. Tagging is not added or removed and the VLAN ID and priority does not change for frames received on the secondary interface. Tags are still removed for frames that egress from the secondary interface. The Ethernet switch forwarding logic determines whether frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the deskphone without regard to specific VLAN IDs or the existence of tags.

2 of 2

About DNS addressing

9600 Series IP Deskphones support DNS addresses and dotted decimal addresses. The deskphone 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 68 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, Table: Customizable parameters on page 86) is appended to the address(es) in Option 6 before the deskphone attempts DNS address resolution. If Option 6 contains a list of DNS addresses, those addresses are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS by DHCP, you can specify the DNS server and/or Domain name in the HTTP script file. But first SET the DNSSRVR and DOMAIN values so 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 (except the 9610, which does not have a secondary Ethernet interface). The system parameter DOT1X determines how the deskphones handle pass-through of 802.1X multicast packets and proxy logoff, as follows:

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

802.1X Supplicant Operation

9600 IP Deskphones that support Supplicant operation also support Extensible Authentication Protocol (EAP), but only with the MD5-Challenge authentication method as specified in IETF RFC 3748 or with TLS.

If an EAP method in the configuration parameter DOT1XEAPS requires the authentication of a digital certificate, the standard authentication requirements apply, including matching the TLSSRVRID with that on the certificate.

Note:

When a phone uses EAP-TLS for the 802.1x authentication, the phone provides the MAC address to a switch during an RFI query from the switch. The Microsoft RADIUS server requires that the CN in the certificate of the supplicant to match the 802.1x identity of the supplicant. Therefore, your must set the MYCERTCN parameter in the settings.txt file to the MAC address of the phone. Use the $MACADDR macro to obtain the MAC address of the phone. If you enter any other value of the MYCERTCN parameter, the EAP-TLS for the 802.1x authentication fails because the Microsoft RADIUS server rejects the identity certificate of the phone.

When a deskphone 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. See “Dynamic Addressing Process” in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694) for information on this process. The deskphone does not accept null value passwords. The default credentials consisting of the values of the DOT1XID and DOT1XPSWD parameters will be used when a new telephone is first plugged in if the EAP method requires an identity and password. In this case, authentication will fail because the password is null, thus the authentication attempt will

not actually contain a password (whether or not the default identity is correct). An EAP-Failure message will be received in response, and an 802.1X User Input interrupt screen prompting "Enter Credentials" is then displayed. For all EAP methods, if the Supplicant is unauthenticated, an 802.1X Waiting interrupt screen is displayed when a response is transmitted, unless an 802.1X User Input interrupt screen is already being displayed.

If an EAP-Failure frame is received after transmitting a response that contains an identity or a password, an 802.1X User Input interrupt screen is displayed, unless an 802.1X User Input interrupt screen is already being displayed. If an EAP-Failure frame is received after transmitting a response that did not contain an identity or a password, an 802.1X Failure interrupt screen is displayed.

The deskphone 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 and the ID and password are not overwritten by deskphone software downloads.

An IP deskphone 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 deskphone (Telephone Only Authenticates) - When the deskphone is configured for Supplicant Mode (DOT1X=2), the deskphone can support authentication from the switch.
- Deskphone with attached PC (Telephone Only Authenticates) - When the deskphone is configured for Supplicant Mode (DOT1X=2), the deskphone can support authentication from the switch. The attached PC in this scenario gains access to the network without being authenticated.
- Deskphone with attached PC (PC Only Authenticates) - When the deskphone is configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1), an attached PC running 802.1X supplicant software can be authenticated by the data switch. The deskphone 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 deskphone (Telephone Only Authenticates) - When the deskphone is configured for Supplicant Mode (DOT1X=2), the deskphone can support authentication from the switch. When DOT1X is "0" or "1" the deskphone is unable to authenticate with the switch.
- Deskphone and PC Dual Authentication - Both the deskphone and the connected PC can support 802.1X authentication from the switch. The deskphone may be configured for

Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1). The attached PC must be running 802.1X supplicant software.

About Link Layer Discovery Protocol (LLDP)

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. 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).

9600 Series IP Deskphones running SIP Release 2.0 and later software support IEEE 802.1AB if the value of the configuration parameter LLDP_ENABLED is "1" (On) or "2" (Auto). If the value of LLDP_ENABLED is “0” (off), the transmission and reception of Link Layer Discovery Protocol (LLDP) is not supported. When the value of LLDP_ENABLED is “2”, the transmission of LLDP frames will not begin until or unless an LLDP frame is received, and the first LLDP frame will be transmitted within 2 seconds after the first LLDP frame is received. Once transmission begins, an LLDPDU will be transmitted every 30 seconds.

Note:

There could be a delay of up to 30 seconds in deskphone initialization if the file server address is delivered by LLDP and not by DHCP.

These deskphones:

- 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.

9600 Series IP Deskphones initiate LLDP after receiving an LLDPDU message from an appropriate system. Once initiated, the deskphones send an LLDPDU every 30 seconds with the contents described in LLDPDU transmitted by SIP Deskphones.

LLDPDU transmitted by SIP Deskphones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPADD of deskphone, IANA Address Family Numbers enumeration value for IPv4, or subtype 5:Network address.
Basic Mandatory	Port ID	MAC address of the deskphone.
Basic Mandatory	Time-To-Live	120 seconds.
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.
Basic Optional	System Capabilities	Bit 2 (Bridge) will be set in the System Capabilities if the deskphone 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 than the deskphone is registered.
Basic Optional	Management Address	Mgmt IPv4 IP Address of deskphone. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the deskphone.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports autonegotiation status and speed of the uplink port on the deskphone.
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery capabilities = 00-33 (Inventory, Power-via-MDI, Network Policy, MED Caps).
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.

1 of 2

Category	TLV Name (Type)	TLV Info String (Value)
TIA LLDP MED	Inventory – Software Revision	APPNAME.
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.
Avaya Proprietary	PoE Conservation Level Support	Provides Power Conservation abilities/settings, Typical and Maximum Power values. OUI = 00-40-0D (hex), Subtype = 1. Current conservation level=POE_CONS_MODE.
Avaya Proprietary	Call Server IP Address	Call Server IP Address. Subtype = 3.
Avaya Proprietary	IP Phone Addresses	Phone IP Address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	CNA Server IP Address	CNA Server IP Address = in-use value from CNASRVR. Subtype = 5.
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.

2 of 2

TLV impact on system parameter values

On receipt of a LLDPDU message the Avaya IP Telephones will act on the TLV elements as described in this section.

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 is set to 1 (ON). 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. VLAN Name TLV is ignored if: • the value of USE_DHCP is “0” and the value of IPADD is not “0.0.0.0”, or • the current value of L2QVLAN was set by a TIA LLDP MED Network Policy TLV, or • the VLAN name in the TLV does not contain the substring “voice” in lower-case, upper-case or mixed-case ASCII characters anywhere in the VLAN Name.
L2Q, L2QVLAN, L2QAUD, DSCPAUD,	TIA LLDP MED Network Policy (Voice) 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 - set to the Layer 2 Priority value in the TLV. DSCPAUD - 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: • 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 2 (Voice Signaling), or • the Unknown Policy Flag (U) is set to 1.

System Parameter Name	TLV Name	Impact
VLAN_IN_USE, L2QSIG, DSCPSIG	TIA LLDP MED Network Policy (Voice Signaling)	VLAN_IN_USE - set to the VLAN ID in the TLV. If the Layer 2 Priority value in the TLV is not zero, and if the Application Type is 2 (Voice Signaling), L2QSIG is set to the Layer 2 Priority value in the TLV. If the DSCP value in the TLV is not zero, and if the Application Type is 2 (Voice Signaling), DSCPSIG is set to the DSCP value in the TLV. This TLV is ignored if: • the value of USE_DHCP is “0” and the value of IPADD is not “0.0.0.0”, or • the Application Type is not 1 (Voice) or 2 (Voice Signaling), or • the Unknown Policy Flag (U) is set to 1.
SIP_CONTROLLER_LIST	Proprietary Call Server TLV	SIP_CONTROLLER_LIST will be set to the IP Address(es) in this TLV value.
TLSSRVR and HTTPSRVR	Proprietary File Server TLV	TLSSRVR and HTTPSRVR will be set to the IP Address(es) in this TLV value.
L2Q	Proprietary 802.1 Q Framing	If TLV = 1, L2Q set to "1" (On). If TLV = 2, L2Q set to "2" (Off). If TLV = 3, L2Q set to "0" (Auto). 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: • the value of USE_DHCP is “0” and the value of IPADD is not “0.0.0.0”, or • the current L2QVLAN value was set by an IEEE 802.1 VLAN Name, or • the current L2QVLAN value was set by a TIA LLDP MED Network Policy (Voice) TLV.
POE_CONS_SUPPORT	Proprietary - PoE Conservation Level Request TLV	If the value of POE_CONS_SUPPORT is “1”, POE_CONS_MODE is set to the level requested in the TLV.

Administering an emergency number

Using PHNEMERGNUM to set default emergency number

Set the PHNEMERGNUM configuration parameter in the settings file to assign an emergency telephone number. This telephone number will be automatically dialed whenever the **Emerg** softkey is selected on the Login screen, or the Phone screen, or when the user chooses the **Yes** softkey on an Emergency pop-up screen.

Note:

If SES/SM is not operable, Emergency Number calling is not operable. When using UDP, the Emergency softkey may not work.

When in failover, the Emergency Number must be provisioned on the SIP gateway or the user will not be able to dial it.

The local proxy routes emergency calls from a user at a visited phone so that the local emergency number is called. When PHNEMERGNUM is administered, using the **Emerg** softkey overrides the SPEAKERSTAT parameter setting or a user-selected referred audio path. This means that the even if the Speakerphone is disabled it is the default transducer when the user presses the **Emerg** softkey.

When the telephone is registered with an Avaya server and is in a logged out state, a call to the Emergency number shows a SIP URI username of "anonymous" in the From and Contact headers of the INVITE message. For example:

From: sip:anonymous@avaya.com;tag=-961235f46856f74-5_F135.8.62.174, and Contact: <sip:anonymous@135.8.62.174;transport=tcp>) (Note that anonymous user support must be configured on SM)

The telephone will always accept an incoming INVITE with a SIP URI username of "anonymous" in the To header with the IP address of the telephone.

For example:

To: <sip:anonymous@135.8.62.174;transport=tcp> (Note that anonymous user support must be configured on SM)

This allows for incoming public service access point (PSAP) calls in both the registered inactive state and the registered state.

Using PHNMOREEMERGNUMS for additional emergency numbers

Set the PHNMOREEMERGNUM configuration parameter in PPM to assign upto 10 emergency telephone numbers, separated with a comma. The user can dial any of the numbers specified in PHNMOREEMERGNUM if the phone is locked or in an unregistered state.

Note:

When a user presses the EMERG softkey, the phone automatically dials the number stored in PHNEMERGNUM parameter. The user must manually dial the emergency numbers in PHNMOREEMERGNUMS.

Administering settings at the deskphone

The *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694) details how to use Craft local procedures at the deskphone for administration. The local procedures you might use most often as an administrator are:

- 802.1X - To set the 802.1X operational mode.
- ADDR - Static address programming.
- AGC - To enable or disable Automatic Gain Control.
- CLEAR - Remove all administered values, user-specified data, option settings, etc. and return a deskphone to its initial “out of the box” default values.
- DEBUG - Enable or disable debug mode for the button module serial port.
- GROUP - Set the group identifier on a per-phone basis.
- HSEQUAL - To set the handset equalization settings of the deskphone
- INT - Locally enable or disable the secondary Ethernet hub.
- LOG - To enable or disable event logging.
- LOGOUT - To logout the user from the deskphone.
- RESET VALUES - To reset the deskphone to default values including the registration extension and password, any values administered through local procedures, and values previously downloaded using DHCP or a settings file.
- RESTART PHONE - To restart the deskphone in response to an error condition, including the option to reset parameter values.
- SIG **-** Change the default signaling value to/from SIP, or change SIG to/from H.323. Chapter 2 of the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones*

Installation and Maintenance Guide (Document Number 16-300694) also describes how to determine which SIG value is appropriate for your environment.

- SIP - Configure SIP call settings.
- SNTP - To configure the time server settings.
- SSON - To set the site-specific option number.
- VIEW - Review the system parameters for the deskphone 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. The phones do not allow administrator to customize the English language.In addition to English, SIP software bundle downloads include the following language files:

- Canadian French
- Parisian French
- Latin American Spanish
- German
- Brazilian Portuguese
- Italian
- Dutch
- Castilian Spanish
- Russian
- Simplified Chinese
- Japanese
- Korean
- Hebrew
- Arabic

Administrators can specify from one to four languages per deskphone to replace English. End users can then select which of those languages they want their deskphone to display.

Note:

The phone cannot display Japanese, Chinese, and Korean characters at the same time.

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

Use the configuration file (46xxsettings.txt) and these parameters to customize the settings for up to four languages:

- LANGUAGES - the list of languages to be downloaded from which the end user can select a desired display language. Each language is listed in the following format: Mlf_German.xml, Mlf_English.xml, Mlf_CastilianSpanish.xml, and so on.

- SYSTEM_LANGUAGE - a string indicating the filename of the default system language. The string indicates which of the available languages to use for display purposes. If this parameter is not set, or if no other language has been set by the user, or if a user language choice cannot be satisfied, the built-in English strings are used.
- 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 default) the user can select the built-in English language text strings.

For more information, see *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694). 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 enhanced local dialing

9600 Series IP Deskphones have a variety of telephony-related applications that might obtain a telephone number during operation. For example, the Call Log saves a number of an incoming caller, but does not consider that the user has to then prepend the saved number with a digit to dial an outside line, and possibly a digit to dial long distance.

SIP deskphones can evaluate a raw telephone number, based on administered parameters. The deskphone can automatically prepend the correct digits, saving the user time and effort. This is the Enhanced Local Dialing feature. The key to the success of this feature is accurate administration of several important values, summarized below.

The parameters relevant to the Enhanced Dialing Feature are:

- ENHDIALSTAT - Enhanced dialing status. If set to “1” the enhanced local dialing feature is partially enabled, meaning dialing rules do not apply to dialing from the Contacts list. If set to "2" the enhanced local dialing feature is fully enabled and does apply to dialing from the Contacts list. If set to “0” enhanced local dialing is off.
- PHNCC - the international country code of the Communication Manager (CM) call server. For example, “1” for the United States, “44” for the United Kingdom, and so on.
- PHNDPLENGTH - the length of the dial plan on the CM call server.
- PHNIC - the digits the CM call server dials to access public network international trunks. For example, “011” for the United States.
- PHNLD - the digit dialed to access public network long distance trunks on the CM call server.

- PHNLDLENGTH - the maximum length, in digits, of the national telephone number for the country in which the CM call server is located.
- PHNOL - the character(s) dialed to access public network local trunks on the CM call server.

Note:

In all cases, the values you administer are the values relevant to the location of the CM call server at which the IP deskphones are registered. If a deskphone is in Japan, but its CM call server is in the United States, set the PHNCC parameter value to “1" for the United States.

In all cases, the digits the deskphones insert and dial are subject to standard CM call server features and administration. This includes Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), and so on.

As indicated in Table: Customizable parameters on page 86, 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 extension matches a dial plan element. The deskphone dials the number without further processing.

Setting the dial plan on SIP Deskphones

Note:

This section only applies to operations with a secondary controller where CM/SES/PPM or SM/PPM are not available.
In a failover situation, the dial plan is played locally even if a proxy connection is not available; the user may hear a dial tone but cannot make a call.

During manual dialing, a dial plan allows a call to be initiated without using a **Send** button and without waiting for the expiration of a timeout interval. The dial plan consists of one or more format strings. When the dialed digits match a format string in the DIALPLAN configuration parameter, the call is initiated. (In an Avaya/SES or SM environment, PPM retrieves the equivalent dial plan information in another format, thus the dial plan information from CM).

Valid characters in a format string, and their meanings, are as follows:

digits 0 through 9, inclusive = Specific dialpad digits
* = the dialpad character *
# = the dialpad character # (but only if it is the first character in the dialed string – see below)
x = any dialpad digit (i.e., 0-9)

Z or z = present dial tone to the user (for example, for Feature Access Code (FAC) entry)
[ ] = any one character within the brackets is a valid match for a dial plan string
- = any one digit between the bounds within the brackets, inclusive, is a match
+ = the character following the + can repeat 0 or more additional times, for a valid match

An individual valid dial plan is any combination of the above characters. If there are multiple valid dial plans, separate each one from the next using an OR symbol ("|"). If the dial plan text string begins or ends with an OR symbol, that symbol is ignored. Users cannot modify the dial plan.

Dial plan example:

"[2-4]xxx|[68]xxx|*xx|9Z1xxxxxxxxxx|9z011x+"

where:

[2-4]xxx: Four-digit dial extensions, with valid extensions starting with 2, 3, or 4;
[68]xxx: Four-digit dial extensions, with valid extensions starting with 6 or 8;
***xx**: Two-digit Feature Access Codes, preceded by a *;
9Z1xxxxxxxxxx: Network Access Code ("9 for an outside line"), followed by dial tone, followed by any string of 10 digits– typical instance of Automatic Route Selection (ARS) for standard US long distance number;
9z011x+: Network Access Code ("9 for an outside line"), followed by dial tone, followed by at least one digit – typical instance of Automatic Route Selection (ARS) for US access to international numbers of unknown, and variable, length.

Additional parameters that affect dialing are as follows:

COUNTRY - Country of operation for specific dial tone generation.

PSTN_VM_NUM (PSTN access number for Voice Mail system) - This parameter specifies the telephone number to be dialed automatically when the deskphone user presses the Messaging button under a non-AST controller. The phone places a PSTN call out from the local office and back in to the location that houses the voice mail server. Additional codes necessary to reach a specific user's voice-mail box may also be included.

Example 1. `SET PSTN_VM_NUM 96135550123`

ENABLE_REMOVE_PSTN_ACCESS_PREFIX - When the phone is operating with a non-AST controller and the value of the parameter is 0, the PSTN access prefix, defined by the parameter PHNOL, is retained in the outgoing number. If the value is 1, then the PSTN access prefix is stripped from the outgoing number.

PHNLAC - A string representing the phone's local area code. When set, this parameter indicates the endpoint's local area code, which along with the parameter LOCAL_DIAL_AREA_CODE, allows users to dial local numbers with more flexibility.

Example: `SET PHNLAC 617`

LOCAL_DIAL_AREA_CODE - A flag indicating whether the user must dial the area code for calls within same area code regions. When the parameter is 0, the user does not need to dial the area code; when this parameter is 1, the user needs to dial the area code. When this parameter is enabled (1), the area code parameter (PHNLAC) should also be configured (i.e., not the empty string).

Example: `SET LOCAL_DIAL_AREA_CODE 1`

Example 1 - Setting the parameter configuration:

```
SET ENHDIALSTAT 2
SET PHNOL 27
SET PHNCC 1
SET PHNDPLENGTH 7
SET PHNLDLENGTH 11
SET PHNLD 0
SET PHNIC 001
```

Example 2 - In the Contacts list, save Contact X with the telephone number 41018989:

PHNLAC Parameter Value	LOCAL_DIAL_AREA_CODE Parameter Value	Step to Execute	Result
020	1	Call X from Contacts list	Phone sends an invite message with 2702041018989.
020	0	Call X from Contacts list	Phone sends an invite message with 2741018989 and does not insert the local area code.
Null	1	Call X from Contacts list	Phone sends an invite message with 2741018989 and does not insert the local area code.

See Table: Customizable parameters on page 86 for a definition of the DIALPLAN parameter.

Setting the date and time on SIP Deskphones

SIP deskphones need a source of date and time information. This typically comes from a network time server running the Simple Network Time Protocol (SNTP). The deskphones use several administrative parameters for this functionality. The parameter SNTPSRVR defines the server's IP Address(es). GMTOFFSET defines the offset from Greenwich Mean Time (GMT). DSTSTART and DSTSTOP define the start and end of Daylight Savings Time, respectively. DSTOFFSET defines the Daylight Savings Time offset from Standard Time. Finally, DATETIMEFORMAT defines the format of the date and time display. See Table: Customizable parameters for definitions and valid values for SIP Date and Time parameters.

About Presence

Presence is the ability for the end users to send their availability status to others and to track the availability status of a set of contacts.

Presence tracking is managed by the presence server. Presence administration is dependent on your operating environment, for example, the servers and software. For information about administering presence in specific environments, search on "presence" at http://support.avaya.com.

Presence notification

Presence notification occurs only if the PRIMARY_PROXY_ENVIRONMENT parameter is 1 (an SES environment) or 2 (Session Manager environment) and when the ENABLE_PRESENCE parameter in the 46xxsettings file is set to 1. Additionally, if the address of the SIP proxy is different than the presence server, the IP address of the presence server must be specified using the PRESENCE_SERVER parameter.

The Deskphone tracks and reports the following presence states:

- Contact is logged in (registered) and the line is idle (available)
- Contact is not logged in (offline, or unregistered)
- Contact is sending all calls to another number (busy)
- Contact is currently on a call (busy, online)
- Contact is currently on a conference call
- Contact is away from the phone (the screensaver is on, if administered)
- Contact has locked the phone
- No presence can be tracked for this contact due to system or server differences

Presence icons are associated with each state and are described and illustrated in the respective user guides of the Deskphone models.

About the presence user interface

Presence tracking uses icons to provide information about other SIP users when the primary controller of the Deskphone is SES or Session Manager.

Primary Presence information is provided through the Contact List view, providing the Deskphone user tracking information for applicable contacts. The Deskphone also provides

Primary Presence information through the Favorite features on the Phone screen for contacts and in the **History Log**, but only for those call history entries that appear in a user's Contact list.

The Presence icon is used in place of Work, Home, Mobile icons. During failover, presence tracking does not occur.

"On the phone" presence status is, by default, automatically sent out and displayed. This can be disabled using the ENABLE_AUTOMATIC_ON_THE_PHONE_PRESENCE parameter.

Session Manager presence user interface

The 9620, 9620C, 9620L, 9630, 9630G, 9640, 9640G, 9650, and 9650C SIP Deskphones support rich presence through Avaya Aura® Presence Server (PS). The user guide for the respective Deskphone model illustrates the icons the end user sees depending on the status of the phone and contact for which presence tracking is set up. The user guide also covers presence setup in the "adding a Contact" procedure.

Administering presence in the settings file

Telephone presence is "on" by default. To change the presence information, the following parameters must be configured in the settings file:

ENABLE_PRESENCE - The default of "1" indicates presence tracking is enabled. The default setting tracks the presence of individuals whose handles have been established on the Contact list. The value "0" indicates presence tracking is not enabled.

PRESENCE_SERVER - If the address of the SIP proxy/registrar is different than the presence server, the IP address of the presence server must be specified using the PRESENCE_SERVER parameter.

ENABLE_AUTOMATIC_ON_THE_PHONE_PRESENCE - This parameter controls whether "on the phone" presence status is sent out automatically when user whose presence is tracked is on a call or goes off-hook. This is enabled by default. Calls on bridged line appearances that the local user has not bridged to, do not affect the trigger of the "on the phone" presence update. The default of "0" indicates this option is disabled; when the person whose presence is being tracked goes off-hook, his or her presence is not reported. A setting of "1" (default) enables automatic on the phone presence.

Integrating Microsoft™ Exchange

Microsoft Exchange calendaring integration is supported, which allows the deskphones to download appointment/calendar data containing meeting schedules from an Exchange Server and display this information on an Appointment screen. End users must specify their credentials (Exchange user account name and password) and calendaring reminder and display

preferences using the Avaya (A) Menu's or Home Screen's Options & Settings Advanced Options option before the Exchange Calendar and the Reminder can be used. User actions regarding exchange integration are described in the applicable deskphone user guide.

From an administrative perspective, you must establish several configuration parameters in the settings file before your end users can access and use the calendaring feature on their phones:

- PROVIDE_EXCHANGE_CALENDAR - A flag to define whether or not menu item(s) for MS Exchange® Calendar integration are provided to the end user. If disabled, the Exchange Integration option under the Avaya Menu's Options & Settings, Advanced Options sub-menu is hidden from the user.
- EXCHANGE_SERVER_LIST- A list of up to 5 Microsoft Exchange™ server IP or DNS addresses used to connect to Microsoft Exchange™ server to access calendar data. The list is sent to the phone and is used by the phone to access Microsoft Exchange. All servers are tried until the phone finds the server to use. The EXCHANGE_SERVER_IN_USE is displayed under the Avaya (A) Menu, Network Information, IP Parameters or by accessing the Craft (Local Administrative Procedures) Menu under the View Procedure.
- EXCHANGE_USER_DOMAIN - Domain information (e.g., "avaya.com") used to access an Exchange server to download calendar information. Can be set via a SET command in settings file or at the phone under Exchange Integration (Options and Settings, Advanced Options). Together with EXCHANGE_USER_ACCOUNT (as entered by the end user), provides a full URL. Example: the EXCHANGE_USER_DOMAIN "avaya.com" and the EXCHANGE_USER_ACCOUNT of "userxyz" provides the URL "userxyz @avaya.com".
- ENABLE_EXCHANGE_REMINDER - Set via the settings file or by the end user at the phone. Must be saved persistently in device data. If this value is "Yes" (1), the popup notification is enabled. If this value is "No" (0), popup notification is disabled.
- EXCHANGE_REMINDER_TIME - Time in minutes at which the user is reminded of an appointment or calendar item. Set via the settings file or by the end user at the phone. Must be saved persistently in device data.
- EXCHANGE_SNOOZE_TIME - Set via the settings file or by the end user at the phone. Must be saved persistently in device data.
- EXCHANGE_REMINDER_TONE - Indicates whether a tone should accompany a calendar reminder. Set via the settings file or by the end user at the phone. Must be saved persistently in device data.
- EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD - Used to administer how long in seconds the phone re-syncs with Exchange Server.

Customizing ring tones

End users can select any one of 8 standard ring tones using the A Menu or Home Screen Screen & Sounds option; the ring tone selection is then stored in PPM. Ring tones for external, internal, priority and intercom calls (distinctive ringing) are combinations of specified frequency, duration and cadence values.

The EXTEND_RINGTONE parameter lets you optionally administer one of two additional sets of 8 ring tones - Korean or customized - to replace the standard Avaya ring tones currently available.

About Korean ring tones

Korean ring tones are part of the SIP software bundle download. To administer all or any of these tones to replace the existing external, internal, priority and intercom call tones, set the EXTEND_RINGTONE parameter in the settings file with the name(s) of the Korean tones you want available to the end user. For example, to administer all the Korean ring tones to replace all the Avaya standard ring tones, you would specify (without spaces between entries):

```
SET EXTEND_RINGTONE =
  KoreanRT1.xml,KoreanRT2.xml,KoreanRT3.xml,KoreanRT4.xml,
  KoreanRT5.xml,KoreanRT6.xml,KoreanRT7.xml,KoreanRT8.xml
```

To administer only the second and fourth Korean ring tones to replace the second and fourth Avaya standard tones, you would specify (without spaces between entries):

```
SET EXTEND_RINGTONE = KoreanRT2.xml,KoreanRT4.xml
```

About customized ring tones

An Excel spreadsheet program called Ringtone.XLS is part of the SIP software bundle download. Use this spreadsheet program to create XML files for up to eight custom ring tones as described in this section. Then:

- save the custom ring tones to an HTTP server,
- set the EXTEND_RINGTONE parameter with the name(s) of the XML file(s) you created,
- reboot the deskphone to make the custom tone(s) available to the end user through the Avaya (A) Menu->Options & Settings->Screen & Sound option.

Important:

When setting up multiple ring tone files using the EXTEND_RINGTONE parameter, be sure that there are no spaces before or after the comma separating the filenames.

To create a custom ring tone, open the Ringtone.XLS spreadsheet and provide a value for each of the cells/fields in Ringtone XLS cell descriptions. A sample spreadsheet follows the table for illustration purposes only.

Ringtone XLS cell descriptions

Cell Name	Description	Comment
Ringer Name	Name of this custom Ring Tone file, for example, Ringtone1	This filename will be assigned a .XML extension upon completing all required cells and pressing the "Create xml" cell button.
Ringer Index	This numbers the xml file as one of the 8 patterns used in personalized ringing. For example, index 2 will be the second personalized ringing choice a user will have on their phone. Eight xml files with indices 1-8 need to be created to customize all the available personalized ringing choices that will be presented on a phone. If less than 8 indices/files are set in the settings file, Avaya standard ringing patterns will be used for the missing indices.	
Type of Wave	Leave empty; this cell is not currently used.	Reserved for future use.
Number of Active Frequencies	Up to four active frequencies can be set. Valid values are 1, 2, 3, or 4.	
Frequency Values	The range of frequency values is from 0 to 3999Hz.	
Number of Notes	Number of notes in this ring tone, from 1 to 3. A note is an interval in which a frequency is used. Currently, a custom ring tone has a 3 note maximum.	
Note 1, 2, and 3	This value represents a collection of frequency intervals that are grouped together and repeated over and over again as the ring tone.	
Note Pulse State	The pulse state has two possible settings - On or Off	

Cell Name	Description	Comment
Note Frequency	The frequency used for a particular note.	
Note Duration	The duration of the note in milliseconds, from 0 to 2^16.	
Next Note	Leave empty; this cell is not currently used.	Reserved for future use.
Cadence Patterns and States	Cadence patterns are set for internal, external, priority, and intercom calls.	
Cadence 1 to 8		
Cadence Duration	The duration of the cadence in milliseconds, from 0 to 2^16.	
Next Cadence	The next cadence is executed after the current cadence value is completed. This is used to create a loop of notes. For example, if number 1 is used for cadence state 8, when cadence 8 is completed, cadence 1 will follow.	
Cadence Next Index	Leave empty; this cell is not currently used.	Reserved for future use.
Create xml	When all applicable cells have been filled in, use this control to create an xml file for this specific tone.	

Chapter 10: Administering Applications and Options

Customizing Applications and Options

This chapter covers configuration options for activating/deactivating options and applications. The 9600 Series IP Deskphones offer the user numerous applications like Contacts, a call History log, Redial, and so on. Each of these applications allows the user to add, delete, or in some cases, edit entries. As the administrator, you might not want the user to have that level of functionality.

This chapter also contains information related to administering the Avaya Menu or Home Screen to include the WML browser, and other browser setup information.

In 4600 and 9600 Series H.323 IP Telephones, the parameters APPSTAT (meaning Application permission status) and OPSTAT (meaning Options permission status) control application access and functionality. However, SIP deskphones have a more granular way of assigning functionality, with a specific parameter for each permission, as follows:

- ENABLE_CALL_LOG - Allows end user access to the list of unanswered and answered calls. If disabled, the History application is not displayed to the user and calls are not logged.
- ENABLE_REDIAL - Allows the end user to redial one to three previously called numbers. If disabled, redialing is not available to the end user.
- ENABLE_REDIAL_LIST - Allows the end user to select a number to redial from a list. If disabled, only the previously-dialed number can be redialed.
- ENABLE_CONTACTS - Allows end user access to a list of numbers and to make calls by selecting a Contact Name/Number. If disabled, the Contacts application is not displayed to the user and a Contact list cannot be set up or maintained.
- ENABLE_MODIFY_CONTACTS - If the Contacts application is enabled (ENABLE_CONTACTS=1), this option allows or prevents the end user from changing or updating the Contact list.
- PROVIDE_EDITED_DIALING - Allows the deskphone to mirror cellular phone dialing by capturing, but not sending dialed digits to the dial plan manager until the user presses the Call Softkey.
- PROVIDE_OPTIONS_SCREEN - If disabled, the Options & Settings menu is not displayed on the Avaya menu or Home Screen. The user cannot change any of the features and options associated with the Options & Settings menu.
- PROVIDE_NETWORKINFO_SCREEN - If disabled, the Network Information menu is not displayed on the Avaya menu or Home Screen.
- PROVIDE_LOGOUT - If disabled, Logout is not displayed to the user as an option on the Avaya menu or Home Screen.

These parameters have On (1=enabled)/Off (0=disabled) settings, and are described in detail in SIP-based 9600 Series IP Deskphones customizable system parameters on page 86.

Note:

To facilitate administration of application-related parameters, the 9600 Series IP Deskphones (both SIP and H.323) and 4600 Series IP Telephones use the same 46xxsettings.txt file.

Administering the Avaya “A” Menu

The A (Avaya) Menu is a list of sub-applications the user can select to invoke the corresponding functionality. The Avaya Menu contains these entries in this order:

- Options & Settings
- Browser (only if WMLHOME administered in settings file and if supported by the current SIP software Release.)
- Network Information
- About Avaya one-X
- Log Out

Each individual sub-application is listed left justified on an individual Application Line.

Administering standard Avaya Menu entries

To prevent users from changing Option & Settings, Network Information, or Logging out, set the corresponding configuration parameter to 0 (zero) in the 46xxsettings.txt file.

Options & Settings is listed if and only if the PROVIDE_OPTIONS_SCREEN configuration parameter value is 1.

Network Information is listed if and only if the PROVIDE_NETWORKINFO_SCREEN configuration parameter value is 1.

Logout is listed if and only if the PROVIDE_LOGOUT configuration parameter value is 1. If you wish to prevent users from changing Options & Settings, Network Information, or Logging out, set the corresponding configuration parameter to 0 (zero) in the 46xxsettings.txt file.

Administering the WML Browser

SIP software provides a WML Browser which, if administered, follows the Options and Settings listing on the Avaya (A) Menu.

Note:

WML applications are accessed from the Browser.

Set the configuration parameter WMLHOME in the settings file to link the Browser Home page to the Avaya (A) Menu and to include the Browser option on the Avaya (A) Menu. The Browser application is listed if and 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).

In addition to WMLHOME, other browser-related configuration parameters which can be set using the 46xxsettings.txt file (as applicable to your environment) are:

- WMLEXCEPT - Exception domain for the WML browser proxy server.
- WMLIDLETIME - Number of minutes of inactivity until the Web browser will display the idle URL specified in WMLIDLEURI.
- WMLIDLEURI - URL of web page to be displayed after idle timer (WMLIDLETIME) expires.
- WMLPORT - TCP port number the WML browser application should use to access the HTTP proxy server (if defined by WMLPROXY).
- WMLPROXY - Address of the proxy server to be used by the WML browser application.

The following conditions would apply to the web pages hosting the WML content:

- WML files larger than 250Kbytes will be discarded, they will not be rendered or cached.
- 1 Mbyte of volatile memory will be allocated for storage of the WML deck and any associated images.
- if a WML file is too large, a "Page cannot be rendered" error message will be displayed.

For detailed information about WML Browser configuration parameters, see Chapter 9: Administering Deskphone Options on page 85.

Chapter 11: System Failover and Survivability

Supporting survivability

SIP software provides support for simultaneous calls from multiple servers to accommodate situations that can occur due to network or server failures. This support ensures that contact data is preserved and actionable during failover transition, active calls continue, and that much of the deskphone functionality is available. The following secondary gateways are supported:

- Avaya Secure Router 2330 and 4134
- Audiocodes MP-series analog and BRI gateways; Audiocodes MP-series using SIP over TCP or TLS for signaling and RTP or SRTP for media
- Cisco 2811 ISR; Cisco ISR using at least one combination of TCP or TLS for signaling and RTP or SRTP for media
- Juniper SRX 210 and 240
- I55
- Teldat Vyda gateway
- Expanded survivability to Avaya Aura® Session Manager

Deskphones fail over to a secondary controller for alternate registration. Simultaneous registration occurs between SMs/BSM (Branch Session Manager) as opposed to alternate registration to a non-AST controller. This arrangement facilitates faster failover/failback transitions than that of the failover solutions offered in previous SIP software releases and provides minimal (if any) disruption from an end user viewpoint.

Contact caching and caching limits in a Session Manager environment are supported. Multiple operations on a cached contact are not allowed. Preserved media connections/calls are supported. During failover, changes to applications other than Contacts are cached and are updated by the PPM with which the phone successfully registers.

With non-AST controllers, contact data is cached until the maximum cache size of 25 contacts is reached; configuration data is cached without limitations. With SM, the PPMs are in sync and the data is sent to the PPM; data is cached only in case of failure.

Moving subscriptions to a secondary SM/BSM for simultaneous registration has the following effects on call states and transitions:

- Transition from one SM to another SM/BSM is comprised of :
  - Limbo - The phone has lost its connection to its primary controller, but has not yet detected this regardless of whether a user is on a call or not.
  - Moving Subscriptions Interval (MSI) - The phone has detected a lost connection to the primary controller and since it has already registered with a non-primary controller, this is

the brief interval between limbo and successful subscription to the non-primary controller. The subscription can be moved regardless of whether a user is on a call or not.

- Call Preservation - During an active call, the phone has detected a lost connection to the primary controller and exhibits media preservation behavior.

l The Call Preservation Message Box or the Acquiring Services screen are not displayed during the Moving Subscription Interval (MSI).

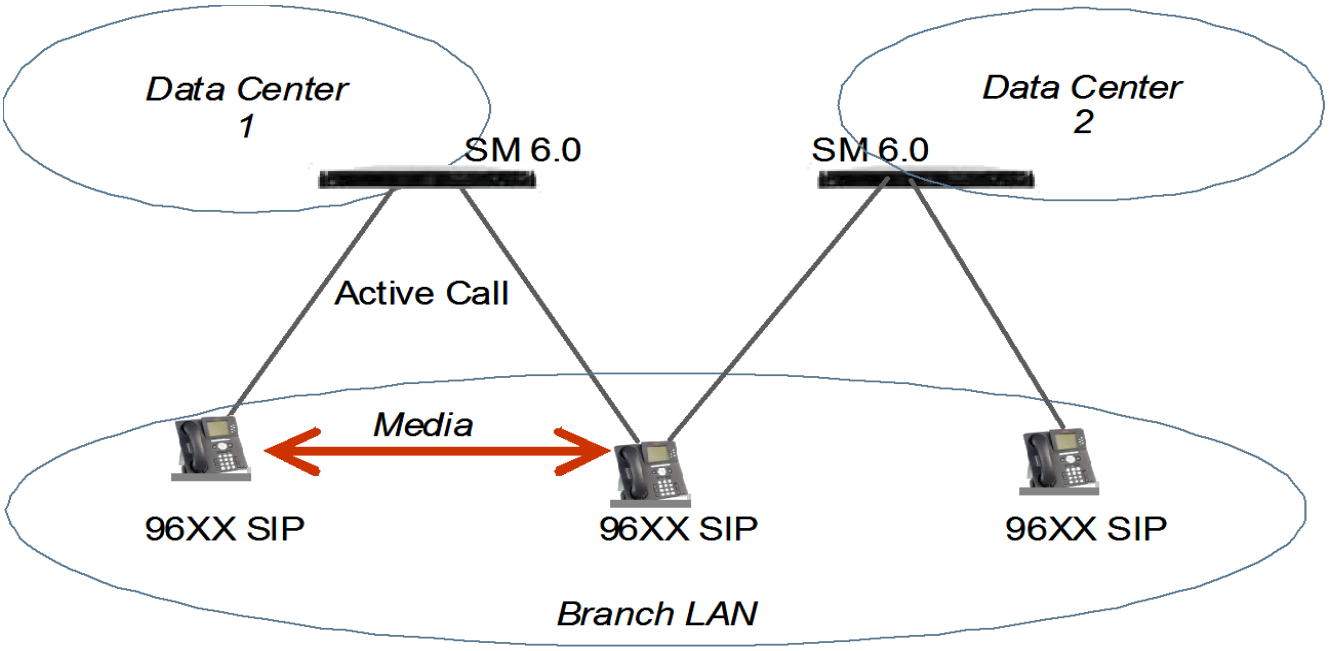
MSI transition and failback to the primary SM occurs according to the failback behavior described in 3. Select the active controller on page 155.

Survivability configuration examples

Several survivability configurations are available, depending on your controller and system management environment, as shown in the illustrations that follow.

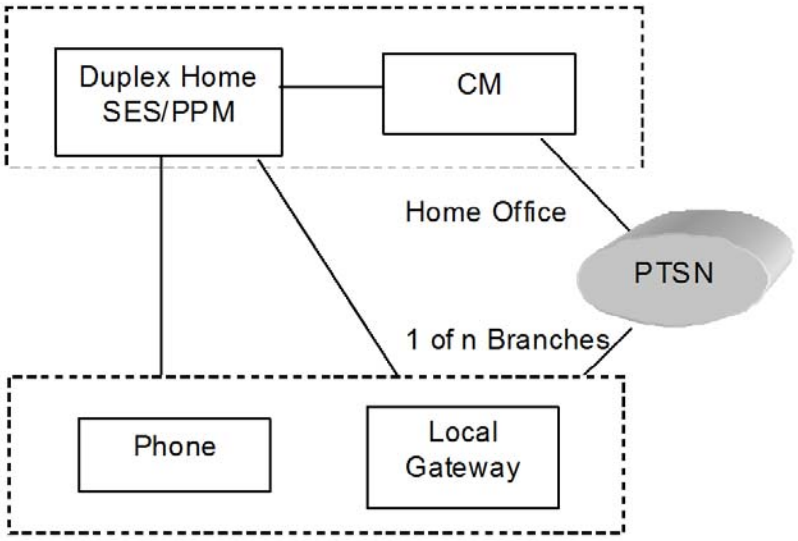
Configuration Example 1

SIP software Release 2.6.9 and later offers simultaneous registration with multiple controllers, and improved feature availability during and after failover to a secondary controller.



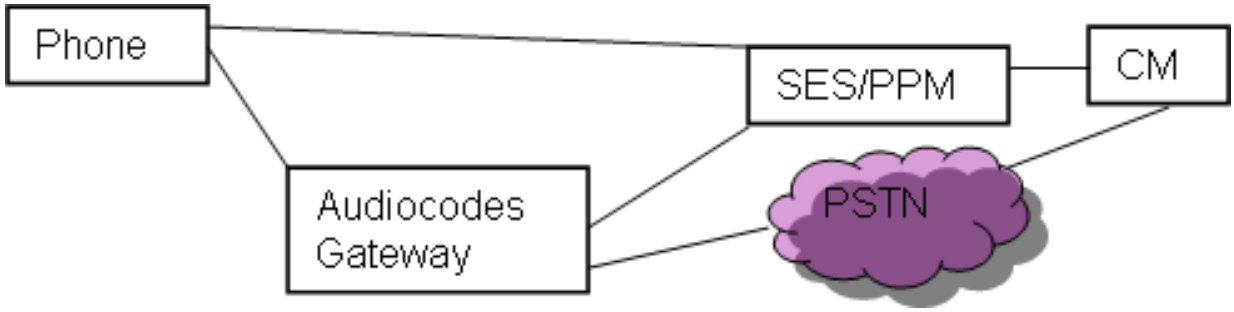
Configuration Example 2

Multiple controllers improve on survivability over a single controller.



Configuration Example 3

Minimal survivability using a single controller for failover.



Survivability hardware/software requirements

- Avaya 9600 Series IP Deskphones with SIP 2.6.10 firmware.
- Supported local (secondary) gateway with Proxy or B2BUA capabilities.

Provisioning survivability for SIP Deskphones

The following steps provide a brief overview of the provisioning process:

1. Set the applicable failover configuration parameters (described in Configuring survivability) in the 46xxsettings file.
2. Provision the gateway per the Application Notes, available on the Avaya support Web site.
3. Load the latest SIP Release software and associated files on the file server.
4. Reboot all registered phones from SM.
5. Power up other phones.

Configuring survivability

Avaya recommends using the 46xxsettings file instead of SM to set these parameters. Avoid mixed sources for configuration of SIP servers.

By administering survivability configuration parameters using the 46xxsettings file (or using the default values if applicable), the SIP deskphone(s) can quickly switch to an active controlling server and experience minimal disruption. The failover/failback parameters, described in detail in the table in SIP-based 9600 Series IP Deskphones customizable system parameters are:

- CONTROLLER_SEARCH_INTERVAL - The time the phone waits to complete the maintenance check for Monitored Controllers.
- DISCOVER_AVAYA_ENVIRONMENT - Determines whether the phone operates in a mode to comply with the Avaya environment mode (provision of SIP/AST features and use of PPM for download and backup/restore).
- ENABLE_REMOVE_PSTN_ACCESS_PREFIX - Enables the removal of the PSTN access prefix from collected dial strings when the phone is communicating with a non-AST controller.
- FAILBACK_POLICY - Failback Policy.
- FAST_RESPONSE_TIMEOUT - Fast Response Timer.

- PSTN_VM_NUM - The number called when the phone is in failover and the Message button is pressed.
- RECOVERYREGISTERWAIT - Reactive Monitoring Interval in seconds.
- REGISTERWAIT - Proactive Monitoring Interval in seconds.
- SIP_CONTROLLER_LIST - Configured Controller list. A comma-separated list of SIP URIs, a hostname, or numeric IP address. If null, DHCP/DNS will provide the defaults.
- SIMULTANEOUS_REGISTRATIONS - The number of Session Managers with which the deskphone will simultaneously register.
- SIPREGPROXYPOLICY - Registration Policy.

Setting a controller via the user interface

Survivability parameters can be provisioned in the SIP Phone Settings screens. Consider the following points when you are setting survivability parameters:

- The SIP proxy settings screen shows the SIP proxy server addresses (or DNS names) from the list of configured controllers in descending priority from top to bottom. Note that duplicate entries are removed from the list of configured controllers.
- You can delete an entry by navigating to that entry and pressing the **Delete** softkey only if you created the entry from the SIP Phone Settings screen.

  WARNING:

  Do not change or delete proxy on the deskphone and in the user profile on the System Manager while the deskphone is in the registered state as it might lead to improper functioning of the deskphone.
- If the **New** softkey is pressed, a new screen is shown which allows the user to enter the parameter's values for server, transport type, and port. The server and port fields are initially blank. The transport type is initially shown as TLS. Once any field is edited the **Save** softkey appears. When the Save softkey is pressed a new entry is inserted into the list of configured controllers at the UI priority. Multiple UI entries are prioritized in the order in which they are entered.
- If an entry is selected (by pressing the **Select** softkey when the entry is highlighted) a new screen is shown which displays the parameter's current values for server, transport type, and port. In this screen all of the values can be edited. Once any of the values are edited the **Save** softkey appears. If the **Save** softkey is pressed, the information is saved as follows.
  - If the selected value originated from user input from the SIP proxy settings screen then the changes will replace that original SIP controller entry.
  - If the selected value originated from any other source, the entire list of configured controllers is copied and saved as if they all originated from the SIP proxy settings screen.

- If the administrator clears the controllers in the setting file, the only way to clear the values that are displayed on the SIP proxy screen that are downloaded from PPM is to clear the values on the phone.
- If the administrator is at the Login screen and no controller has been set, a controller can be set at the Craft (Local Administrative procedures) menu, as described in the *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694). The user can log in successfully with a controller at this point.

Controller Determination and Survivability Activity

The deskphone performs controller determination and verification after a successful user login. The deskphone then periodically performs failover checks. The steps are:

1. Determine controllers to monitor

The list of controllers to monitor is built from the Configured Controller(s) list using the SIPREGPOLICY parameter setting as a guide. The list of SIP Proxies/Registrars can be obtained from the network DHCP servers, retrieved from the 46xxsettings file, retrieved from a PPM (Personal Profile Manager), or configured via the phone's UI (User Interface). Similarly, the administrative/automatic failback parameters and the monitoring intervals might be obtained through the 46xxsettings file, the PPM, or the deskphone's user interface.

The priority order in which the list is obtained is as follows:

1. Deskphone user interface (set using SIP Craft procedure)
2. PPM
3. Settings file
4. DHCP (Option 242)
5. LLDP

Each of these sources might provide a list of controllers (servers). The contents of each one of these lists is assumed to be in priority order.

2. Determine which monitored controllers are available

Using the Monitored Controllers list, the deskphone performs DNS queries to resolve hostnames and the signaling protocol (TLS, TCP, UDP in that order when no DNS NAPTR or SIP URI parameter is located). To determine which of the Monitored Controllers is actually available to provide service, the phone performs a maintenance activity for each Monitored Controller. The phone starts the controller search timer and sends a SIP REGISTER (adding

bindings) message to each controller, which may necessitate establishing a TLS or TCP connection to the controller.

The controller is considered available once a 200 OK response is received in response to the REGISTER request. Once a controller has been marked as available, the phone unregisters from the controller. If all the Monitored Controllers are available before the end of the CONTROLLER_SEARCH_INTERVAL the phone continues with selecting the Active Controller. If at least one Monitored Controller is available at the end of the CONTROLLER_SEARCH_INTERVAL, the phone continues determining which controllers are available.

If a failure response to the REGISTER request is received, the controller is considered unavailable and depending on the failure code, either retries the query, provides the requested credentials, abandons the query, or stops monitoring this specific controller entirely.

If no response to the REGISTER request is received within the timeout period, the phone retries the monitoring attempt using the RECOVERYREGISTERWAIT parameter value as a guideline.

3. Select the active controller

If the value of the SIPREGPROXYPOLICY parameter is "alternate" and a user is logged in, the phone must attempt and maintain a single active SIP registration with the highest priority Available Controller; the number of Available Controllers that the phone simultaneously registers with is the value of the SIMULTANEOUS_REGISTRATIONS parameter. Any additional controllers are treated as alternate registrations. The phone attempts to register using the username and password provided during the login process. It also uses the SIPDOMAIN parameter. The deskphone uses a SIP URI unless SRTP is enabled where a SIPS URI is used. When registration is successful, the phone sets the SIPPROXYSRVR_IN_USE parameter to the IP address of this (Active) Controller. The phone also performs the other registration tasks.

If the value of the SIPREGPROXYPOLICY parameter is "simultaneous" and a user is logged-in, the phone attempts and maintains active SIP registrations with all Available Controller(s).

If the value of the FAILBACK_POLICY parameter is "automatic", the phone's active controller will always be the highest priority available controller. If the value of the FAILBACK_POLICY parameter is "admin", then a controller lower down the priority list may be active.

The phone initiates a search for a new Active Controller whenever one of the following triggers is encountered:

- Fast Response Timer Expiry,
- TCP keep-alive failure (or other socket error),
- The phone receives an administrative failback trigger,
- An incoming INVITE is received from a non-Active controller,
- A re-registration with the Active Controller times out, or

Whenever one of these triggers is encountered and a user is logged in, the deskphone initiates parallel REGISTER transactions with every controller in its configured list, including the currently active controller.

Simultaneous Registration

For SIP software Release 2.6.9, deskphone behavior for simultaneous registration is based on one of four triggers:

- Trigger 1: The TCP socket closes.
- Trigger 2: A TCP Keep-alive timeout occurs.
- Trigger 3: The deskphone receives an administrative failback trigger from a Configured Controller.
- Trigger 4: "Fast Response Timer"

Simultaneous registration functions in response to a trigger are:

1. Controller search (maintenance check) - The deskphone tries to establish a connection (if needed) and then register (or refresh registration) with each of the controllers. If it gets a successful response to the REGISTER, it marks the controller as "available." If the deskphone cannot establish the connection or if it does not receive a successful response, it marks the controller as "unavailable".
2. Controller Subscription Refresh - The deskphone sends a refresh SUBSCRIBE to the current controller for all the subscriptions that it has. If it gets any failure response other than "489 Bad Event" for any of the refresh SUBSCRIBE messages, it removes that subscription and re-establishes a subscription for that event package.
3. Controller Failover - The deskphone removes all the existing subscriptions and establishes subscriptions with the highest priority controller that is available.
4. Controller Failback - If the failback policy is "auto" or if the failback policy is "admin" and the trigger is a message, the deskphone unsubscribes from the current controller and subscribes with the highest priority controller available. Otherwise (for example, the failback policy is "admin" and the trigger is Trigger 1 or Trigger 2), the deskphone executes a "controller subscription refresh."

When one of the triggers occurs, the deskphone follows this algorithm:

1. If there is no active call, the controller search is performed immediately.
   - If the current controller is available and it is the highest priority available controller, the "Controller Subscription Refresh" function is performed.
   - If the current controller is available, but there is a higher priority controller available, the "Controller Failback" function is performed.
   - If the current controller is not available, the "Controller Failover" function is performed.
2. If there is an active call, the controller search (Step 1) is performed when the call is over.

4. AST feature determination

After the Active controller has been selected, the deskphone examines the value of the DISCOVER_AVAYA_ENVIRONMENT parameter.

If the parameter value is 1, the phone determines if that controller supports the AST (Advanced SIP Telephony) feature set or not. The phone sends a SUBSCRIBE request to the active controller for the "Feature Status Event Package" (avaya-cm-feature-status). If the request succeeds, the phone proceeds with PPM Synchronization. If the request is either rejected, is proxied back to the phone, or does not receive a response, the deskphone assumes that AST features are not available.

If the parameter value is 0, the deskphone operates in a mode where AST features are not available.

Upon receiving a 202 Pending response, the deskphone starts an internal timer of 16 seconds and waits to receive a NOTIFY to determine whether the subscription is active or terminated. If the NOTIFY indicates an "active" state, the phone considers itself in an AST environment and proceeds with PPM Synchronization. If the NOTIFY indicates a "terminated" state, the phone considers itself in a non-AST environment. It periodically retries the subscription to the Feature Status Event Package. If it receives a 202 Pending response, it continues as specified above. If the 16 second timer expires before a NOTIFY is received the phone considers itself in a non-AST environment.

5. Session Manager synchronization

As part of Session Manager synchronization the deskphone sends a getAllEndpointConfiguration request. The request contains the following configuration fields in the EndpointConfigurationFields parameter:

- VolumeSettings
- LinePreferenceInfo
- ListOfOneTouchDialData
- ListOfButtonAssignments
- SoftMenuKeyList
- DialPlanData
- ListOfSpeedDialData
- ListOfMaintenanceData
- ListOfTimers
- VMONInfo
- ListOfRingerOnOffData
- ListOfNumberFormatRules - applies only when registered to a Session Manager (SM)
- ListOfIdentities - only when registered to a SM
- MWExt - applies only when registered to an SM
- VMNumber - applies only when registered to an SM
- ListOfEmmergencyNumbers

If the getAllEndpointConfiguration request fails, the phone does not continue with the other Session Manager requests. In this case the getContactList request does not occur causing no contacts and no "New" softkey to be displayed in the Contact list.

Failover/failback behavior

System performance

The survivability characteristics of the system as a whole are dependant on the configuration and behaviors of all the SIP network elements such as phones and proxy servers as well as the traditional network elements like routers and DNS servers. The endpoint detects a failure within approximately 90 seconds of the time the failure occurs when TCP or TLS connections are used. Once a failure has been detected, the endpoint completes its selection of an ‘Active’ controller within approximately 5 seconds.

With simultaneous registration, available in a multiple SM environment with SIP software Release 2.6, both failover/failback transition time and behavior is minimized.

Telephone behavior during failover

During failover, SIP-based 9600 Series IP Deskphones will:

- Locate multiple controller addresses in priority order,
- Detect the availability of each controller,
- Transition automatically to lower priority controllers whenever a high priority controller fails or becomes unreachable (automatic failover),
- Transition from lower priority controllers to a high priority controller (failback) either automatically or as a result of explicit administrator activity,
- Preserve active calls to the greatest extent possible in the event of a transition, and
- Preserve as many call and system features as possible when operating under failure conditions.
- Be in a pushable state during transition, when the primary controller is lost and the deskphone is not connected to a secondary controller. Once the phone is registered on secondary controller (AudioCodes, Cisco, etc.) and regardless if the phone is active on a call, the phone is in a pushable state, just as if were connected to primary server. The phone is always in a pushable for state for all normal or barge-in Top Line. Display, Audio Receive/Transmit, or phonexml pushes for all transition conditions.

In general, the phone does not attempt to preserve SIP transactions in progress when a controller failure is detected, and some mid-call features like conferencing can fail. However, in some scenarios the same transaction may succeed if re-attempted once the transition to a new controller has been completed.

The deskphone always registers to a configured controller with the credentials (username/password) of the user who is currently logged-in, even if the deskphone transitions from one controller to another.

As described in the respective deskphone user guide, certain features may not be available and functionality may be limited or work differently during any stage of failover, "limbo," transition, or failback. Calls can still be placed and received, and other deskphone functions remain active. The following apply when a deskphone is in failover mode:

- If the user is active on a call, a failover icon displays when failing over to a non-AST controller and messages like "Link recovery." "Limited phone service." and "Calls may be lost." inform the user of a failover situation. The message "Limited phone service" also displays during failover transition from one Session Manager server to another when the subscriptions have not yet been moved successfully to the secondary SM. The only user options are to navigate to the Phone screen by pressing the OK softkey or the Phone button or hang up the call.
- When failing over to a third party secondary controller, an Acquiring Services screen displays during failover and failback transitions to an active controller and a Call Preservation message window may display for deskphones running SIP software Release 2.6 or greater. Most other screens and applications except for Craft screens are unavailable until an active controller is found. However, the user can navigate to the Contacts, Call Forward feature, Avaya (A) Menu or Call Log applications (if administered). Pressing the Phone button causes the user to be redirected to the Home Screen (if one is administered).
- If a call is active when failover occurs, that call will remain active. The user cannot initiate new calls while the phone transitions to the alternate server.
- With SIP software Release 2.6 and later releases for failover to secondary controller for alternate registration, the user can access Contacts, the Call Forward button, Call Log, standard Avaya menu or Home Screen applications if administered. The user cannot make calls in these applications.
- Certain softkeys do not display and their related functions are unavailable.
- Call appearance information does not display while dialing, but does appear when Call is pressed.
- Call connection may take longer than usual.
- Upon failover, any active conference calls, call transfers, and held calls will be dropped.
- Emergency calls may or may not work, depending on the stage of failover and the functionality available on the alternate server.
- Bridged call appearances are not available. Despite a "Log Bridged Calls" option setting of yes, bridged calls are not logged during failover.
- During the transition stage, incoming calls may not be received and may go to voice mail.
- Call forwarding may not be available unless the extension to which calls are being forwarded is on the same server as the forwarding extension.

- The Message Waiting Indicator is cleared, but voice mail may still be available, if the voice mail server to which calls are being sent is not in failover.
- Advanced features like Call Park/Unpark, Priority Call, or Automatic Callback are not available. Most features on the Feature menu will not be available. Favorite features are not available during failover.
- Once the transition to a new server has occurred, changes to Avaya (A) Menu options can be made/saved during failover. Note that any new or changed settings for these options will become effective when the phone fails back to its original server.
- If the phone operates under the latest software (Release 2.5 or greater), Contacts can be accessed and changed during and after failover to the alternate server.
- If the phone operates under the latest software (Release 2.5 or greater), the end user can access Home Screen Web links/pages during failover, however, any “click to dial” links will not work until the phone transitions to the alternate server.
- If users are part of a corporate Directory or database, access may be limited to local contacts only.
- If the phone is logged out during failover, the local phone cache is cleared and the phone may become inoperable until it can be reset on the original controller after failback.
- The phone accepts calls from any of the proxies it is registered with when the phone is simultaneously registered to multiple controllers. There is no visual indication to the user differentiating calls from different feature servers. In the case of Multiple Feature Servers, one feature server can know about one call on the phone and another feature server or controller can know about another call on another call appearance. The second Feature Server does not have any information about the first call displayed on the phone and there will be limitation in the features that can be applied to the first call. When there are multiple controllers, one controller may know about one call on the phone and another controller can know about another call offered to the phone. If both controllers are connected to the same feature server e.g., CM, CM "knows" about both calls and the user can resume a held call, conference call, or call transfer normally. If both controllers are not connected to the same feature server, the second Feature Server would not have any information about the first call displayed on the phone. In this scenario features that can be applied to the first call would be limited because all the call data is stored in CM; SM does not store any information related to any call.
- Preserved Media Connections - Applies only to Session Manager configurations when moving a subscription from one SM to another. As of SIP software Release 2.6 in a scenario where the the primary SM fails, any active shuffled or direct media call will be preserved if a new call is received while a preserved call is active. The phone allows the user to manually put the active (media preserved) call on hold or allows the user to switch to the new call and automatically put the preserved call on hold using auto-hold. A media preserved call displays the failover icon in place of a call-associated icon that is left justified on an application line preceding the displayed name or phone number. When active on a media preserved call the softkeys displayed are "Hold, blank, blank, End Call." Conference and Transfer are not available. When a media preserved call is put on hold, the softkeys displayed are "Resume, blank, blank, blank, blank." The phone can receive

incoming calls at this point but is not available to make outgoing calls or to invoke AST features. The phone supports media preservation sufficient for alternate registration; if a phone experiences a mid-dialog failure (for example, a timed out or failed SIP request, or a socket-level failure), the phone behaves as if the dialog had been terminated (but does not send a BYE) and preserves the media session until the near-end user hangs up.

Failover/failback administrative monitoring and logging

It is ultimately up to the deskphone to determine which of its configured controllers is the Active Controller. This information is available in the SNMP MIB, which the network administrator can view; the Active Controller is the SIPPROXYSRVR_IN_USE value. The deskphone sends an SNMP notification whenever a transition occurs. In addition, whenever the appropriate level of logging is enabled, the phone logs its transitions from one server to another.

About the user interface/failover experience

The user interface experiences described below expand upon the information provided in Failover/failback behavior. User guides for each deskphone model also provide this information in a "user-friendly" format.

User interface in failover/failback

- Failover (F/O) transition - Connection to SM failed, the phone detects F/O and blocks new invites while the phone is in transition.
- Stable in F/O where the non-primary proxy is the active controller.
- Fail Back (F/B) transition to normal - The phone detects that the primary server is up, regardless if the secondary is up. New invites are blocked while the phone is in transition. The phone is in a stable Normal mode with SM as the active controller. Any cached changes (for example, to Contacts or other Avaya Menu options and settings) are updated to the PPM once the phone is registered back to the primary controller.

User experience during failover transition

SIP software Release 2.6.9 expanded deskphone reliability during the transition from one controller to another.

Failover to a secondary controller for alternate registration (SM to a non-AST controller)

Transition is comprised of the following conditions:

- Limbo - The phone has lost its connection to its primary controller, but has not yet detected this condition regardless of whether a user is on a call or not.
- Acquiring Services - The phone has detected a lost connection to the primary controller and displays an Acquiring Services Screen if the phone is idle.
- Call Preservation - During an active call, the phone has detected a lost connection to the primary controller and displays a Call Preservation screen.

Moving subscriptions from one SM to another SM/BSM (Branch System Manager) due to failover

Transition is comprised of the following conditions for moving subscriptions:

- Limbo - The phone has lost its connection to its primary controller, but has not yet detected this condition, regardless of whether a user is on a call or not.
- Moving Subscriptions Interval (MSI) - The phone has detected a lost connection to the primary controller and since it has already registered with a non-primary controller, this is the interval between limbo and successful subscription to the non-primary controller. The subscription can be moved regardless of whether a user is on a call or not. The Call Preservation Message Box or the Acquiring Services screen are not displayed during MSI.
- Call Preservation - During an active call, the phone has detected a lost connection to the primary controller and exhibits media preservation behavior.
- The failover icon displays on the Top Line when failing over to a non-AST controller (for example, Audiocodes) or in the very short interval after limbo and before a successful subscription from one SM to another (or BSM) in the same community.
- When transition to the secondary server (or back to the primary server) occurs, all deskphone functionality is restored to normal.

Moving subscriptions occurs immediately after limbo has ended or when there is a graceful socket closure. For an active call scenario, media preservation will only keep shuffled calls or calls using direct media between endpoints up with a direct RTP stream until the call has ended. The user can only put this call on Hold, resume the call, or end the call. The user can also answer any incoming call and the media preserved call is put on hold. During MSI the user can't use call related softkeys (Hold, Conf, Transfer) for call appearances or bridged calls and the softkeys are not removed from the screen. If the user presses another call appearance or a Favorite Feature an error beep occurs. The Prompt Line displays "Limited phone service". Click to dial links do not work.

All AST features and BCAs are displayed on the phone and SBM24 during MSI regardless if there is an active call. If a user tries to use an AST feature, the feature fails and the phone displays "Feature invocation failed." When the Phone Button is pressed, the Home Screen (if

there is one) displays instead of the Phone Screen. The user can press the Phone button to navigate to the Home Screen (if there is one) and all Home Screen sub-screens are accessible. The phone does not block new invites during transition. Changes to applications other than Contacts, for example, Speed Dial, are cached and are updated by whichever PPM with which the phone successfully registers. Any changes made under the Avaya menu Options & Settings take place (including the Home Screen) immediately.

If the deskphone is idle when failover occurs and the user presses a call appearance or Favorite Feature, the phone plays an error beep. Going off hook produces no dial tone. The Prompt Line displays "Limited phone service" and no digits are displayed on the screen. All Home Screen sub-screens are accessible. The user can access all the web links from any of the Home Screen options except for a "Click to Dial Link," which produces an error beep if selected. The Prompt Line displays "Limited phone service" in this case.

During MSI the Contacts button remains activated and the user can view the Contacts Screen. Contacts can be changed during failover transition up to the maximum cache size regardless of which primary controller is used. The New, Edit, or Delete softkeys display during failover. During MSI transition, the +AddtoContact function on a web page will fail and the Prompt Line will display "Contact cannot be saved." Selecting a contact or pressing the Call softkey produces an error beep and the Prompt Line displays "Limited phone service."

All screens are visible. Any changes made under the Avaya menu Options & Settings take place on all screens (including the Home Screen) immediately. All changes other than Contacts are cached and are updated to the PPM with which the phone successfully registers.

All Audio Receive, Transmit, Top Line, Web Push, or phoneXML pushes operate normally.

For incoming calls during MSI, the phone stops alerting and disconnects the call. If the phone is alerting when the phone's secondary server goes down (no MSI), the phone will keep on ringing. An incoming call will be ended when the link between the Session Manager that routed the call and the phone has gone down. For example, if the deskphone has a primary SM (SM1) and a secondary SM (SM2), and receives a call directly from the secondary SM but SM2 goes down, the call that was received from SM2 is terminated.

Media preservation only keeps shuffled calls or calls using direct media between endpoints up with a direct RTP stream until the call has ended. The user can only put this call on Hold, resume the call, or end the call. The user can also answer any incoming call and the media preserved call will be put on hold.

User experience during stable failover

- A Failover “warning” icon displays on the top line. The Failover icon is shown whenever the primary call server is not active. The Failover icon provides a continuous reminder indicating the deskphone has detected that the primary server is unavailable and that features will be limited until the primary server returns.
- Multiple Call Appearances are consistent with Normal Operation.

- If a call originates using the secondary server, Hold, Conference and Transfer are supported.
- AST features (FNUs and Bridged call appearances) are unavailable when failing over to a secondary gateway.
- Unsupported features and related softkeys are not displayed.
- The dial plan does not remain as it was in normal operation. The dial plan in failover is set with the DIALPLAN parameter which should contain all needed strings while failed over. Calls between sets in the branch are supported, using their usual extensions.
- Outgoing Calls that would normally route to the SM/CM will instead be routed to the local gateway.
- Emergency calls (to the provisioned emergency numbers as defined in the dial plan) will be permitted whether those phones are in failover or normal mode. The Emergency softkey is available when a new controller is found.
- The MWI (Message Waiting Indicator) will be cleared, but voice mail is still available.
- One-button voice mail access will be available if the central voice mail system continues to operate and will make a PSTN call to the voice mail system. Depends on correct provisioning.
- Local deskphone features will be available: audio selection (speaker / headset / handset), mute.
- Local phone applications will be available: local call redial, Call Logs, Volume Control, local contacts, speed-dials, auto-dials, WML browser (WML Browser is dependent on network access to the WML server) but cannot be changed.
- Nothing is saved in PPM when failing over to a secondary (for example, Audiocodes) gateway.
- Basic local features if provisioned (call forwarding) will be available: call hold, consultative hold, Attended Transfer, Unattended Transfer, call forward all, call forward on busy, call forward on no answer, three party conferencing of calls originated in Failover Operation (including drop last party). Additional in-call features will be available if supported by the local proxy - find me, inbound call management and outbound call management.
- Contact or Autodial Favorite Features are displayed on the Phone Screen.
- "A" (Avaya) Menu and Home Screen Options & Settings are blocked under minimal survivability configurations. Any of the more extensive survivability configurations (for example, moving subscriptions to a secondary SM/BSM for simultaneous registration) allow access to the Avaya Menu and updates to Options & Settings. Likewise, Contacts can be accessed and updated.
- Craft changes may be made and are saved locally on the phone.
- If the phone is logged out during failover, the local phone cache is cleared.

User experience during failback

Failback (F/B) transition occurs when the Phone detects that the primary server is up, regardless if secondary controller is up.

- Failback will not happen during an active call. If no calls are in progress, failback occurs and the user interface returns to its normal appearance.
- While switching from one server to another (including while waiting for an active call to end) reject any new inbound calls (including emergency callbacks) or outbound call requests.
- AST features return.
- Users can access and update Avaya Menu/Home Screen options.

User interface failover operation for features

Feature	Normal Operation with CM	Failover Operation with a Generic SIP Gateway
Make call	Yes	Yes
Receive call	Yes	Yes
Call Hold	Yes	Yes
Consultative Hold	Yes	Yes
Ad hoc conferencing	Yes, up to 6 parties	Yes, up to 3 parties
Last party drop	Yes	No
Forward all my calls/SAC	Yes	Yes
Forward my calls when busy/no answer	Yes	Yes
Attended call transfer	Yes	Yes
Unattended call transfer	Yes	Yes
Hunt groups	Yes	Find me (proxy)
Inbound call management	Yes (CM COR)	Yes (depends on local proxy capabilities and provisioning)

Feature	Normal Operation with CM	Failover Operation with a Generic SIP Gateway
Outbound call management	Yes (CM COR)	Yes (proxy)
Calling party block	Yes	No
Calling party unblock	Yes	No
Call park	Yes	No
Call unpark	Yes	No
Call pickup	Yes	No
Directed call pickup	Yes	No
Extended call pickup	Yes	No
Priority call	Yes	No
Auto callback	Yes	No
Malicious call trace	Yes	No
EC500 on/off	Yes	No
Transfer to voice mail	Yes	No
Whisper page	Yes	No
Recording voice call to messaging	Yes	No
Bridge line and call appearances	Yes	No
Extend-call	Yes	No
Hold recall	Yes	No
Transfer recall	Yes	No
Busy indicator	Yes	One-button dial - Yes Busy indicator - No
Message waiting indicator	Yes	No

Appendix A: Glossary of Terms

Active Controller	The SIP Registrar/Proxy server the deskphone believes is the one and only authoritative proxy at a given time. It is the highest priority available controller.
Available Controller(s)	The subset of Monitored controllers that respond to the 'Maintenance Check' as part of determining available controllers during Failover.
Configured Controller(s)	The list of controllers that the phone will attempt to monitor when Failover occurs. The (list of) elements in the SIP_CONTROLLER_LIST parameter, which can also come from SM and the user interface.
Controller	The new name for a SIP proxy, for example, SM, or a local gateway, or local survivable gateway.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
EAP	Extensible Authentication Protocol, or EAP, a universal authentication framework frequently used in wireless networks and Point-to-Point connections defined by RFC 3748. EAP provides some common functions and a negotiation of the desired authentication methods, two of which are EAP-MD5 and EAP-TLS. When EAP is invoked by an 802.1X enabled NAS (Network Access Server) device such as an 802.11 a/b/g Wireless Access Point, modern EAP methods provide a secure authentication mechanism and negotiate a secure PMK (Pair-wise Master Key) between the client and the NAS.
Failover	Selection of a lower priority call controller to become the active controller, when the highest-priority (primary) call controller becomes unavailable.
Failback	Return to normal operation by selection of the highest-priority (primary) call controller as the active controller.

H.323	A TCP/IP-based protocol for VoIP signaling. An alternative to SIP for VoIP signaling. One of the two protocols 9600 Series IP Deskphones support.
Monitored Controller(s)	A SIP Registrar/Proxy server that the deskphone knows about and to which the phone periodically checks IP and SIP connectivity.
OPS	Outboard Proxy SIP.
PPM	Personal Profile Manager, part of the SM. PPM is responsible for maintaining and managing end users' personal information in the system.
Primary Controller	The controller that appears first in the configured controller list.
Proxy Server	An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, meaning its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy, for example, making sure a user is allowed to make a call. A proxy interprets, and if necessary, rewrites specific parts of a request message before forwarding it.
Session Manager (SM)	Avaya Aura® Session Manager, the SIP proxy for Avaya Aura®.
SIP	Session Initiation Protocol, an open standard defined initially by IETF RFC 3261. SIP is an alternative to H.323 for VoIP signaling, both of which 9600 Series IP Deskphones support.
Surviveable Call Processor	A term for the active controller after failover.

Surviveable Gateway	Audiocodes server used as a gateway to survive failover. A supported local gateway with Proxy or B2BUA capabilities.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP deskphones. SIP deskphones use HTTP or HTTPS instead of TFTP.

3 of 3

Appendix B: Countries With Specific Network Progress Tones

About network progress tones

SIP-based 9600 Series IP Deskphones provide country-specific network progress tones which are presented to the user at appropriate times. The tones are controlled by administering the COUNTRY parameter for the country in which the deskphone will operate. Each Network Progress Tone has six components, as follows:

- Dialtone
- Ringback
- Busy
- Congestion
- Intercept
- Public Dialtone

As of software Release 2.5, all countries listed in this appendix are applicable to the 96xx phones. Some of the dialtone entries have changed from previous releaSIP_CONTROLLER_LIST ses to be distinctively different than the Public dialtone entries.

Alphabetical country list

A:

Abu Dhabi

Albania

Argentina

Australia

Austria

B:

Bahrain
Bangladesh
Belgium
Bolivia
Bosnia
Botswana
Brunei
Bulgaria

C:

China (PRC)
Colombia
Costa Rica
Croatia
Cyprus

D:

Denmark

E:

Ecuador

El Salvador

Egypt

F:

Finland

France

G:

Germany

Ghana

Greece

Guatemala

H:

Honduras

Hong Kong

I:

Iceland

India

Indonesia

Ireland

Israel

J:

Japan

Jordan

K:

Kazakhstan

Korea

Kuwait

L:

Lebanon

Liechtenstein

M:

Macedonia
Malaysia
Mexico
Moldova
Morocco
Myanmar

N:

Netherlands
New Zealand
Nicaragua
Nigeria
Norway

O:

Oman

P:

Pakistan
Panama
Paraguay
Peru
Philippines
Poland
Portugal

Q:

Qatar

R:

Romania
Russia

S:

Saudi Arabia
Serbia
Singapore
Slovakia
Slovenia
Spain
South Africa

Saudi Arabia
Sri Lanka
Swaziland
Sweden
Switzerland
Syria

T:

Taiwan
Tanzania
Thailand
Turkey

U:

Ukraine
United Arab Emirates
United Kingdom
Uruguay
USA

V:

Venezuela
Vietnam

Y:

Yemen

Z:

Zimbabwe

INDEX

Numerical

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W