Administering Avaya 9601/9608/ 9608G/9611G/9621G/9641G IP Deskphones SIP

Release 6.5
16-601944
Issue 1
January 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.

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website:

http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

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

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

License Type (s)

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

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

Copyright

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

Third party components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at:

http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise,

any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

Downloading documents

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

Contact Avaya Support

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

Federal Communications Commission (FCC) Interference Statement

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

Note

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

Warning

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

Chapter 1: Introduction

Purpose

This document covers the administration of Avaya Deskphone SIP for the following 9600 Series IP Deskphones models:

- 9601
- 9608
- 9608G
- 9611G
- 9621G
- 9641G

These deskphones use DHCP to obtain dynamic IP addresses, and HTTP or HTTPS to download new software and 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 Deskphone SIP for the following IP deskphones:

- 9601
- 9608
- 9608G
- 9611G
- 9621G
- 9641G

Document changes since last issue

Issue 1 This version of the document, revised and issued in December 2014 to support 9600 Series IP deskphone software release 6.5, for the deskphone models: 9608, 9611G, 9621G, and 9641G.

Major updates:

Chapter 3: Network requirements > Other network considerations > Certificate management.

Chapter 8: Administering applications and options > Presence.

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
Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP	Describes the installation procedures for SIP deskphones.
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.

Title	Description
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	Provides instructions to configure features or applications for deskphones.
Administering Avaya Aura® Presence Services	Provides instructions to configure presence services for a user.

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.

What is new in the 6.5 release

Feature	Description
Presence profile	● Support for Presence Server scalability by supporting Presence Server clusters. ● Support of the Presence Server High Availability architecture enabling the deskphone to automatically reestablish service when presence switches hosts. ● Support for Presence Server resiliency by allowing the phone to immediately log back into the Presence Server after the Presence server has been restarted. ● Ease of Presence management by removing the requirement to explicitly specify the Presence Server IP address in the deskphone's settings file. ● Requires a release of the Presence Server and Avaya Aura® 6.2 FP4.

Chapter 2: Administration overview and requirements

About 9600 Series IP Deskphones

This document covers SIP administration for 9601, 9608, 9608G, 9611G, 9621G, and 9641G deskphones only.

The 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 the IP deskphone models and the SIP software release that these models support.

9600 Series IP Deskphones	Supported SIP software release
9608, 9611G, 9621G, 9641G	6.2
9601, 9608, 9611G, 9621G, 9641G	6.2.2
9601, 9608, 9611G, 9621G, 9641G	6.3
9601, 9608, 9608G, 9611G, 9621G, 9641G	6.3.1
9601, 9608, 9608G, 9611G, 9621G, 9641G	6.4
9601, 9608, 9608G, 9611G, 9621G, 9641G	6.5

Administrative requirements

The conditions under which the 9600 Series SIP deskphones need to operate are summarized as follows:

- IP Address management for the deskphone, as covered in Chapter 5: Administering DHCP and HTTP servers for dynamic addressing. For static addressing, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.

- Tagging Control and VLAN administration for the deskphone, if appropriate, as covered in Chapter 7: Administering deskphone options.
- Quality of Service (QoS) administration for the deskphone, if appropriate. QoS is covered in QoS on page 6.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP), as applicable.
- Interface administration for the deskphone, as appropriate. Administer the deskphone to LAN interface using the PHY1 parameter described in Chapter 3: Network requirements. Administer the deskphone to PC interface using the PHY2 parameter described in “Interface Control” in *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP.*
- Application-specific deskphone administration, if appropriate, as described in Chapter 7: Administering deskphone options. This step consists of creating a text settings file with various deskphone specific parameters. This file resides on an HTTP or HTTPS server and the deskphone retrieves the file when powered on.

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 *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP.*
- 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 by all administrative mechanisms. See the applicable chapters in this guide for specific information.

Administration alternatives and options

Parameters	Administrative Mechanisms	For More Information See:
Telephone Administration	Avaya Communication Manager and System Manager	Chapter 4: Configuring Avaya Aura® for Avaya Deskphone SIP. For Avaya Aura® Session Manager and Avaya Aura® System Manager administration, go to Avaya support website, www.support.avaya.com.
IP Addresses, Interface, Tagging and VLAN		
	Settings file	Chapter 6: Deskphone software and application files and Chapter 7: Administering deskphone options.
	Manual administration of the deskphone	"Static Addressing Installation" in the applicable *Installing and Maintaining Avaya 9601/9608/9608G/ 9611G/9621G/9641G IP Deskphones SIP.*
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 57.
Network Time Server (NTS)	DHCP Settings file	Administering the DHCP Server on page 2 and Simple Network Time Protocol (SNTP) server on page 2.
Quality of Service	Settings file	Chapter 7: Administering deskphone options.
Application - specific parameters	DHCP	Administering the DHCP and File Servers on page 1, and especially Administering the DHCP Server on page 2. Also, Chapter 7: Administering deskphone options.
	Settings file	Administering the DHCP and File Servers on page 1, and especially HTTP Generic Setup on page 9. Also, Chapter 7: Administering deskphone options.

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. IP address parameters that come from the DHCP server, for example, IP address, are used by the deskphone unless the USE_DHCP parameter in the deskphone's CRAFT menu is set to No. If set to No the parameters normally supplied by the DHCP server can be set manually from the CRAFT menu and take precedence over DHCP.

2. Avaya Aura® System Manager.
3. The 46xxsettings.txt settings file.
4. DHCP, except as indicated in DHCPACK setting of parameter values.
5. LLDP.

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 of the highest priority, after which the usual priority sequence applies. For the L2QVLAN and L2Q system values, LLDP settings of VLAN IDs are the highest priority 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 57.

About controllers

A controller is a proxy server that routes the calls. A controller also works like a registrar and an interface between Communication Manager and the deskphone; for example, Avaya Aura® Session Manager.

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.

No.	Task	Description	For more information see
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 as desired on the Communication Manager station forms .	Chapter 4: Configuring Avaya Aura® for Avaya Deskphone SIP.
3.	Administer the Proxy Server	Administration for Session Manager.	*Administering Avaya Aura® Session Manager,* Document Number 03-603324, on the Avaya support website http://www.avaya.com/support.
4.	Administer Avaya Aura® System Manager	Administration for System Manager (SMGR).	Aura® System Manager documentation on Avaya Support website http://www.avaya.com/support.
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 5: Administering DHCP and HTTP servers.
7.	Administer Network Time Server	Set values 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.	Install the deskphone's SIP software, the settings file, and the upgrade file onto the HTTP or HTTPS server.	Download the files from the Avaya support site.	http://www.avaya.com/support Chapter 6: Deskphone software and application files.

1 of 2

No.	Task	Description	For more information see
10.	Administer WML servers (Optional)	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 6: 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 10 and *Installing and Maintaining Avaya 9601/9608/ 9608G/9611G/9621G/9641G IP Deskphones SIP.*
		Individually:	The applicable Craft Local Procedures in the *Installing and Maintaining Avaya 9601/9608/ 9608G/9611G/9621G/9641G IP Deskphones SIP.*
13.	Installation of deskphones in the network		*Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/ 9641G IP Deskphones SIP*.
14.	Allow user to modify Options, if applicable	Set different parameters in the settings file.	Customizable system parameters for SIP-based 9600 Series IP Deskphones on page 2.
			2 of 2

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. *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP* 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 deskphone, the deskphone initiates DHCP, as described in Administering the DHCP and File Servers on page 1. For a list of all the parameters that you can set via DHCP, see Parameters set by DHCP in a site-specific option on page 3.

Step 3: Downloading files

The deskphones can download software, configuration files, certificate files, and language files from either an HTTP or HTTPS server. When the deskphone boots, the deskphone first downloads an upgrade configuration file. The upgrade configuration file specifies the software files to which the deskphone must upgrade. The deskphone then downloads a settings configuration file. Based on the settings in the configuration file, the deskphone may then download language files and/or certificate files. Finally, the deskphone downloads one or two new software files, depending on whether or not the software in the deskphone is the same as that specified in the upgrade file. For more information about this download process and settings file, see. Chapter 6: Deskphone software and application files.

Step 4: Registering with Session Manager

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 Session Manager, which in turn communicates with Communication Manager.

For more information about the installation process, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.

Error conditions

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

Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP 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 has the capacity for the expected data and voice traffic, and that it can support all applications such as following:

- SIP
- DHCP
- HTTP and HTTPS.

Hardware requirements

For LAN powering, you need a Category 5e cables designed to the IEEE 802.3af-2003 standard.

Server requirements

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

- DHCP server
- HTTP or HTTPS server
- Session Manager
- Simple Network Time Protocol (SNTP) server
- Alternate Session Manager for reliability
- System Manager
- Communication Manager
- Presence server
- Avaya Aura® Conferencing
- Branch Session Manager for additional redundancy

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

For parameters related to Avaya Communication Manager information, see Chapter 4: Configuring Avaya Aura® for Avaya Deskphone SIP. For parameters related to DHCP and file servers, see Chapter 5: Administering DHCP and HTTP servers.

DHCP server

Install the DHCP server and application as described in Administering the DHCP and File Servers on page 1.

HTTP/HTTPS server

Administer the HTTP or HTTPS file server as described in HTTP Generic Setup on page 9.

Simple Network Time Protocol (SNTP) server

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

Presence services

The deskphone retrieves presence information of contacts from Avaya Aura® Presence Services. To enable presence, you must set the ENABLE_PRESENCE parameter to 1 in the settings file.

The following standards and guidelines dictate how presence is handled:

- Using the following SIP/SIMPLE RFCs:
    - RFC 3863 *Presence Information Data Format*,
    - RFC 4479 *A Data Model for Presence*, and
    - RFC 4480 *RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)*.
- Using the subscription to the SIP resource list event package, as follows:
    - RFC 4662 - A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists.
    - If the deskphone subscribes to the Presence events, the deskphone accepts the following presence information and passes it to the user interface: Offline, Out of Office, Do Not Disturb, Away, Busy and Available.

- For releases before Avaya Aura® 6.2 FP 4, if the PRESENCE_SERVER parameter is set and contains an IP address, the deskphone will replace the domain on the Request-URI header of any outbound presence-related messages with this IP address. The To header will remain intact in the form user@domain.tld. For Avaya Aura® 6.2 FP 4 and later releases, the deskphones do not use the PRESENCE_SERVER parameter. The presence server address is obtained from PPM.
- Support for configuration of a port number for the presence server.

For information on how the deskphone handles presence messages in an Session Manager environment, see Presence on page 5.

Push server

For "push" functionality, a Trusted Push Server is needed. Your 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 installing a 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.

The 9600 Series SIP IP Telephones 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 4 and About DNS addressing on page 54.

Required network information before installing a 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 5: Administering DHCP and HTTP servers.
- 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

Avaya Deskphone SIP release 6.5 is 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 5: Administering DHCP and HTTP servers.

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 www.ietf.org. The Avaya Custom MIB for the 9600 Series SIP IP Telephones is available for download in *.txt format on the Avaya support Web site at www.avaya.com/support.

Note:

> The SIP software release 2.6 MIB is different than that of release 6.5 MIB. Ensure to download the MIBs applicable to your environment.

Registration and authentication

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

For the SIP Deskphones to work properly, you must specify the correct domain name in the **IP Network Region** screen of Communication Manager. For more information on the IP Network Region screen, see *Administering Network Connectivity on Avaya Aura® Communication Manager* available at www.avaya.com/support.

For more information on the registration process, see *Maintaining and Troubleshooting Avaya Aura® Session Manager* (03-603325), available on the Avaya support Web site, http://www.avaya.com/support and your call server administration manual.

Ping and traceroute

All 9600 Series SIP IP Telephones 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 IP address of the deskphone and the parameter values are saved in the non-volatile memory of the deskphone. The deskphone can reuse the saved parameters if the DHCP or HTTP/HTTPS server is not available for any reason after the deskphone restarts.

IP Address reuse was added to prevent infinite looping when separate DHCP 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 indicated otherwise, 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 - if no responses are received from the routers indicated in the configuration parameter ROUTER (set using DHCP Option 3 or by a local administrative procedure), and if REUSE = 1, then ROUTER_IN_USE will be set to REUSE_ROUTER_IN_USE. With the exception of the ROUTER configuration parameter, the other router-related parameters are internally set system values.

- 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 52 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.

All SIP-based 9600 Series IP Deskphones provide detail about network audio quality. For more information see, Displaying network audio quality on page 7.

IEEE 802.1D and 802.1Q

For more information about IEEE 802.1D and IEEE 802.1Q and the 9600 Series SIP IP Telephones, see VLAN settings on page 50. Three bits of the 802.1Q tag are reserved for identifying packet priority to allow any one of the following 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:

The higher the number, the higher is the priority, except for 0 which has a higher priority than 1.

Displaying network audio quality

Users can view icons on the deskphone that provide information about:

- Audio quality of a call. A Local Network Quality (LNQ) icon appears whenever the audio quality of a call is below a certain threshold. You can define the threshold in the settings file using LNQ and QLEVEL_MIN parameters. The LNQ is based on a combination of jitter, packet loss and delay.
- Use of the wide band codec. An HD icon appears if the deskphone uses the wide band codec. You can enable or disable the icon based on the value you assign to the WBCSTAT parameter in the settings file.

For more information about the settings file parameters, see Customizable system parameters for SIP-based 9600 Series IP Deskphones on page 2.

Users can also monitor network audio performance while on a call. The Network Information screen displays the audio network. Users can gain access to the Network Information screen from the Avaya Menu. On a touchscreen deskphone, users can gain access to the Network Information screen from the Home Screen.

While on a call, the deskphones display network audio quality parameters as shown in the following table.

Audio parameters

Parameter	Possible Values
Received Coding	G.711, G.722, G.726A, or G.729
Packet Loss	Missing, 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.

Parameter	Possible Values
Packetization Delay	The number reflects the amount of audio data in each RTP packet.
One-way Network Delay	The number is half the value RTCP or SRTCP computes for the round-trip delay to the device the RTP is transmitted to. For calls that have a large geographic distance this number is expected to be larger than for local calls.
Network Jitter Delay	The average delay introduced by the jitter buffer on 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.

Administering TCP/UDP port selection

9600Series IP Deskphones use a variety of protocols, particularly Transmission Control Protocol (TCP), Transport Layer Security (TLS), and User Datagram Protocol (UDP) 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 must need to know what ports or ranges are used in the operation of the 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 that the deskphone sends	Any	Received DNS messages	UDP
The number used in the Source Port field of the packets that the HTTP client of the deskphone sends	Any	Packets that the HTTP client of the deskphone receives	TCP
			1 of 2

Destination Port	Source Port	Use	UDP or TCP?
The number used in the Source Port field of the TLS/ SSL packets that the HTTP client of the deskphone sends	Any	TLS/SSL packets that the HTTP client of the deskphone receives	TCP
68	Any	Received DHCP messages	UDP
The number used in the Source Port field of the SNTP query that the deskphone sends	Any	Received SNTP messages	UDP
161	Any	Received SNMP messages	UDP
SIP messages initiated by the call server should be sent to the port number specified by the value of SIPPORT (TCP) or to the port number specified by the value of SIP_PORT_SECURE (TLS over TCP). Responses to SIP messages initiated by the deskphone should be sent to the number used in the Source Port field of the message from the deskphone.	Any	Received signaling protocol packets	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	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	Any unused port number	TLS/SSL packets transmitted by the deskphone's HTTP client	TCP
514	Any unused port number	Transmitted Syslog messages	UDP
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 + 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
			1 of 2

Destination Port	Source Port	Use	UDP or TCP?
System-specific	Any unused port number	Transmitted signaling protocol packets	UDP
			2 of 2

Security

SIP-based 9600 Series IP Deskphones provide lock and logout functionalities for security and protection of the privacy of a user. When a user locks the deskphone, no one can unlock the deskphone without the assigned password for the particular user. When the deskphone is in a locked state, a user can receive calls or make emergency calls. The deskphone restricts access to any user data while in 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 can not access other user's data who have 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 can not access any record of user A, such as contacts and call records, on the deskphone.

> ⚠ **Important:**
> The CRAFT menu provides access to certain administrative procedures from the deskphone. You must change the default password for the CRAFT menu to restrict users from using the administrative procedures to change the deskphone configuration.

For troubleshooting the deskphones, the deskphones support SSH and a secure password assignment mechanism for the Avaya professionals to login to the deskphones remotely and perform the required operations remotely in a secure environment.

SSH users are not given the root access. The access permission is read-only and does not support access to any private data including:

- Digital certificate private keys
- Authentication credentials for SIP, HTTP, 802.1X, VPN, Exchange, and LDAP
- Contact and call log information
- Personal browser information, such as bookmarks, URL history, and cookies

Therefore, an SSH user cannot execute the phone-report script as the script execution requires write-access to some folders as well as read-access to some private data.

The 9600 Series IP Deskphones support Secure Real-time Transport Protocol (SRTP). SRTP is used to encrypt and secure the audio going to and from the endpoint.

In order to correctly use SRTP, there are various components within the network that you must correctly configure. For 9600 Series IP Deskphones to function properly 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)

As well as securing the media (audio) going to and from the phone the signaling that is used to set up the SIP call can also be made secure through the use of TLS (Transport Layer Security). The use of TLS, for signaling, is tied to the SIP proxy that the deskphone registers with.

The deskphones notify you whenever you are in a secure call, using TLS and SRTP. The deskphones display a secure call icon, a small padlock icon, on the call line, to indicate that you are in a secure call and that the call is encrypted.

The support for Transport Layer Security (TLS) allows 9600 Series IP Deskphones to establish a secure connection to a HTTPS server, in which the upgrade and settings file can reside.

Communications between the SIP deskphone and the Personal Profile Manager (PPM) can also be secured by setting the CONFIG_SERVER_SECURE_MODE parameter.

Certificate management

The applications running in the SIP-based 9600 Series IP Deskphones setup rely on trusted certificates for secure operation. The deskphones use certificates to verify the authenticity of servers, such as:

- HTTPS file server
- PPM server
- SIP-TLS server
- Presence server
- Exchange server
- SLAMon server

Enterprises can set up their own certificate authority (CA) and replace the default Avaya root certificates with their trusted certificates. The certificates issued by CA must be configured in `46xxsettings` file when the deskphone is registered with the enterprise.

In addition to root certificates, high-security enterprises install a unique identity certificate on each deskphone. Identity certificates are required if the communication setup is using EAP-TLS, or any other server that requires mutual authentication.

The endpoints support the Simple Certificate Enrollment Protocol (SCEP) to retrieve and load the identity certificates. You can configure SCEP settings in the `46xxsettings` file.

Note:

To remove an identity certificate from the phone, the administrator must use the CLEAR option from the CRAFT menu.

46xxsettings parameter for Certificate Authority configuration

In the `46xxsettings` file, the `TRUSTCERTS` parameter specifies the list of trusted certificates to be downloaded to the deskphone.

`TRUSTCERTS` supports both root and intermediate certificates and can contain up to 6 certificate file names.

The deskphone can use only PEM-formatted certificates. The MIME type associated with the file-extension of the certificate file that is returned by the HTTP server must be plain/text.

Sample `TRUSTCERTS` configuration:

```
SET TRUSTCERTS psstca1.txt,smgrcacert.txt,av_sipca_pem_2027.txt
```

46xxsettings parameters for SCEP configuration

Parameter	**Default value**	**Description**
MYCERTURL	NULL	URL of the SCEP server.
MYCERTCN	$SERIALNO	Common name (CN) to be used in the subject of the SCEP certificate request. The value must be a string that contains either: $SERIALNO: Is replaced by the serial number of the deskphone. $MACADDR: Is replaced by the MAC address of the deskphone.
MYCERTKEYLEN	2048	Length of the private key generated for the certificate request.
SCEPASSWORD	$SERIALNO	0-32 ASCII-character password required for the certificate request.

Parameter	Default value	Description
MYCERTWAIT	1	Specifies what the deskphone must do if the SCEP server indicates that the certificate request is pending approval. Accepted values: 0: Poll the SCEP server. 1: Wait until a certificate is received or the request is rejected.
MYCERTCAID	CAidentifier	0-255 ASCII-character CA identifier, if multiple CAs are used.
MYCERTRENEW	90	Percentage of the validity period elapsed before the deskphone should attempt to renew a certificate.

Chapter 4: Configuring Avaya Aura® for Avaya Deskphone SIP

Call server requirements

Supported SIP environments

SIP software release 6.5 supports the following configurations for the 9601, 9608, 9608G, 9611G, 9621G, and 9641G deskphones:

- Avaya Aura® Session Manager with Avaya Aura® Communication Manager
- Failover and survivable interoperability with the following SIP gateways:
  - Session Manager 6.x for survivable remote gateway
  - Avaya Secure Router 2330 and 4134
  - Audiocodes MP-series analog and BRI gateways
  - IP Office 9.0 and greater

The features available to the deskphones depend on Communication Manager and Session Manager configuration. For more information on feature configuration and operation, see the appropriate Communication Manager Feature and Administration guides.

About button modules

Note:

> The deskphone models 9601 and 9621G do not support button modules and do not have an IEEE power switch.

You can add up to three BM12 or SBM24 button modules to the deskphones. However, multiple button modules attached to a single deskphone must all be the same model type, either BM12 or SBM24.

When you use button modules, you may need to change the power over Ethernet (PoE) settings on the IEEE switch. The IEEE switch is on the back panel of the deskphones and is in low (L) state by default.

Refer the following table for the setting of the IEEE switch while using button modules with the deskphones.

Deskphone model	One BM12 button module	Two BM12 button modules	Three BM12 button modules	One SBM24 button module	Two SBM24 button modules	Three SBM24 button modules
9608/9608G	L	L	H	L	H	H
9611G	H	H	H	H	H	H
9641G	L	L	L	L	L	H

⚠ **Important:**

The maximum combined number of busy indicators, team buttons and bridged appearances, that you can configure on button modules is 48. You can configure all button module lines as long as the specified restriction is met.

Administering Communication Manager with Session Manager

For information about Communication Manager administrative requirements with Session Manager, see the Avaya Aura® Session Manager and Avaya Aura® System Manager documents on the Avaya support website www.avaya.com/support.

The Avaya Aura® Session Manager documents:

- *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)

The Avaya Aura® System Manager documents:

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

Administering SIP Deskphones on Avaya Aura® Communication Manager

SIP feature support summarizes the calling features available on 9600 Series SIP Deskphones.

The features shown in SIP feature support can be invoked at the deskphone either directly or by selecting a Communication Manager-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 Communication Manager administration documents available on the Avaya support site. The Avaya SIP solution configures all SIP Deskphones in Communication Manager as OPS.

SIP feature support

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with Communication Manager + Session Manager
3-way conferencing (Local, on the deskphone)	Yes	No
Conference using conference server		Yes
Auto Intercom		Yes
Automatic Call Back/ Cancel		Yes
Call Forward All Calls (on/off)	Yes	Yes
Call Hold	Yes	Yes
Call Park and Unpark		Yes
Call Pick-Up Group		Yes
Call Pickup Directed		Yes

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with Communication Manager + Session Manager
Calling Party Number Block/Unblock		Yes
Dial Intercom		Yes
Directed Call Pick-Up		Yes
Distinctive Alerting		Yes
EC500		Yes
Enhanced call forward		Yes
Exclusion		Yes
Exchange integration	Yes	Yes
Extend Call for EC500		Yes
Extended Group Call Pickup		Yes
Group Call Pickup		Yes
Group paging		Yes
Hotline		Yes
Instant Messaging		Yes
LNCC		
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
Mute alert	Yes	Yes

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with Communication Manager + Session Manager
One Touch Recording		Yes
Presence		Yes
Priority Call		Yes
Send All Calls Enable/ Disable		Yes
SSH support	Yes	Yes
Team button		Yes
Team button SAC/ CFWD/ECF override		
Third Party Call Forward		Yes
Third Party Call Forward Busy Don't Answer		Yes
Third Party Send All Calls		Yes
Transfer - attended	Yes	Yes
Transfer - unattended		No
Transfer upon hang-up		Yes
URI dialing	Yes	Yes
WML browser	Yes	Yes

Note:

Some of the features may not be applicable to specific phone models. For more information, see the feature specific details provided in this document.

Administering stations

Administering features

The following buttons can be administered for a 9601, 9608, 9608G, 9611G, 9621G, and 9641G SIP deskphone, unless otherwise noted:

Administrable Station Features

Feature	Administration Notes
3-Way Conferencing (Local, on the deskphone)	
Conference using conference server	
Audix One-Touch Recording	
Auto Callback/Cancel	
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 Hold	
Call Park	
Call Unpark	Regardless of Communication Manager Station button administration, this feature will show on the Features menu automatically on Session Manager 5.2+ configurations. In Session Manager 6.0+ this feature does not appear automatically.
Call Pickup	
Call Pickup Group	
Calling Party Number Block/ Unblock	
CPN Block	
CPN Unblock	
Dial Intercom	On Communication Manager: 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	
Distinctive Alerting	
EC500 Enable/Disable	

Administrable Station Features (continued)

Feature	Administration Notes
EC500 Extend Call	
Enhanced call forward	
Exclusion	
Extended Call Pickup	Regardless of Communication Manager Station button administration, this feature will show on the Features menu automatically.
LNCC	
Offline call log	
Malicious Call Trace	
MCT Activation	
Message Waiting Indication	Supported in Communication Manager 6.0.
Music on Hold	
One Touch Recording	
Priority Call	
Send All Calls	
Team button	
Team button redirection override	
Transfer (Attended)	
Transfer (Unattended - one button transfer)	
Transfer upon hung-up	

Note:

> One or more features might not be applicable to specific phone models. For more information, see the feature specific details provided in this document.

For additional information about administering Avaya Aura® Communication Manager for 9600 Series SIP 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: Administering DHCP and HTTP servers

Software Requirements

Ensure that you own licenses to use the Dynamic Host Configuration Protocol (DHCP), HTTP, and HTTPS server software.

Note:

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

⚠ **CAUTION:**

The software in the 9600 Series IP Deskphones reserves IP Addresses of the form 192.168.2.x for internal communications. If you specify addresses in that form, the Deskphones improperly use the addresses.

Administering the DHCP and File Servers

DHCP minimizes maintenance for a 9600 series SIP IP deskphone 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 the 9600 series SIP IP deskphones:

- IP address of the 9600 series SIP IP deskphones
- IP address of the Avaya call server
- IP address of the HTTP or HTTPS file server
- IP address of the Simple Network Time Protocol (SNTP) server using Option 42
- The subnet mask
- IP address of the router
- IP address of DNS

Administer the LAN so that each SIP deskphone can access a DHCP server that contains the IP addresses and subnet mask.

The IP address reuse capability allows the deskphone 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 deskphone. If the user assigns the IP address manually, the deskphone does not search for a DHCP server unless the static IP address is, subsequently, unassigned manually.

Since manual entry of an IP address is an error-prone process, you must ensure the following:

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

A file server, HTTP or HTTPS, provides the deskphone with an upgrade file and, if appropriate, new or updated binary software. See Step 3: Downloading files on page 7. You can further edit the 46xxsettings.txt settings file to customize the deskphone parameters for your specific environment. For more information, see Chapter 7: Administering deskphone options.

Administering the DHCP Server

This section concentrates on the simplest case of a single LAN segment. You can use the information provided here as a basis 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)

For SIP-based 9600 Series IP Deskphones, you can specify the value of some site specific configuration parameters through DHCP option 242, the default Site-Specific Option Number (SSON). Alternatively, you can modify the SSON parameter through the CRAFT menu to use another DHCP option instead of 242.

Following is an example of the DHCP option string that specifies the HTTPSRVR and the VoiceVLAN that the deskphone should join.

HTTPSRVR=10.138.251.67,L2QVLAN=1104

The following section describes the list of parameters that you can define in SSON for SIP-based 9600 Series IP Deskphones.

Parameters set by DHCP in a site-specific option

Parameter	Description
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. The default value is 0 (supplicant disabled).
HTTPDIR	Specifies the path to prepend to all configurations and data files the deskphone 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 (error, critical, alert and emergency events are logged).
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 (auto-negotiate).
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 (auto-negotiate).
PROCPSWD	Security string used to access local procedures. The default is 27238.
PROCSTAT	Controls whether local procedures are enabled. The default is 0 (enabled).
REUSETIME	Time in seconds for IP address reuse timeout, in seconds. The defaut is 60 (second).

Parameter	Description
SIG	The signaling protocol download flag that indicates the protocol applied as follows: ● 0 for Default ● 1 for H.323 ● 2 for SIP Separate upgrade files with different names are used for H.323 and SIP. Default means that the deskphone downloads the upgrade file for the same protocol that the current software on the deskphone supports.
SIP_CONTROLLER_LIST	SIP proxy or registrar server IP or DNS addresses: 0 to 255 characters, IP address in the dotted decimal name format, separated by commas and without any intervening spaces. The default is null, that is, no controllers.
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, the standard HTTPS port.
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 the 9600 Series SIP IP Telephones. 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 the 9600 Series IP Deskphones.

- The following DHCP options:
  - Option 1 - Subnet mask.
    As described in Required network information before installing a DHCP server.
  - Option 3 - Gateway (router) IP Address(es).
    As described in Required network information before installing a 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 deskphone 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 54.
  - 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 43 - Encapsulated vendor-specific options.
    This option is used by clients and servers to exchange vendor-specific information. Option 43 is processed only if the first code is 1 and has a value of 6889. All values are interpreted as strings of ASCII characters that are accepted with or without a null termination character. Any invalid value is ignored, and the corresponding parameter value is not set. Note that since all DHCP options have a maximum length of 255 octets, even though HTTPSRVR, TLSSRVR and SIP_CONTROLLER_LIST can each support values with lengths up to 255 octets when set in a configuration file, shorter values must be used when setting them in DHCP.

    The codes supported and the corresponding parameters are as follows.

Code	Parameter
1	No parameter is set, but the value must be 6889.
2	HTTPSRVR

Code	Parameter
3	HTTPDIR
4	HTTPPORT
5	TLSSRVR
6	TLSDIR
7	TLSPORT
8	TLSSRVRID
9	L2Q
10	L2QVLAN
11	PHY1STAT
12	PHY2STAT
13	PROCSTAT
14	SIG
15	SIP_CONTROLLER_LIST

- 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.

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.

- 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.

- 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***"

The 9600 Series IP Telephones do not support Regular Expression Matching, and therefore, do not use wildcards. For more information, see Administering options for the 9601,9608, 9608G, 9611G, 9621G, and 9641G SIP deskphones on page 1.

As shown in DHCPACK setting of parameter values, the 9600 Series IP deskphone 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).

Parameter Value	Set to
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 3.

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 1.

Note:

If you used TFTP to provide the binary, upgrade, and settings files to older Avaya IP telephones, note that 9600 Series IP Telephones 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 files from the Avaya Web site http://www.avaya.com/support to the HTTP server. For more information, see Chapter 6: 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 6: Deskphone software and application files

About the general download process

The 9600 Series IP Deskphones download upgrade files, settings files, language files, certificate files, and software files from a file server. The deskphones download all file types including software files using HTTP or HTTPS. The deskphones use HTTPS to download software upgrades if you define only an HTTPS server. If you define both HTTP and HTTPS server, deskphones use HTTP for software upgrades. Once trusted certificates are downloaded into the deskphone, HTTPS ensures that the file server itself is authenticated through a digital certificate.

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 a deskphone is first plugged in, the deskphone attempts to connect to a file server, and downloads new software if the software version available on the file server is different than the version on the deskphone. 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.

When a SIP deskphone connects to the file server, the file server sends a 96x1Supgrade.txt file to the deskphone. The upgrade file specifies which software files the deskphone should use.

The 9600 Series IP deskphone then downloads a 46xxsettings.txt file. The settings file contains options you have administered for any or all of the deskphones in your network. For more information about the settings file, see About the settings file on page 2. After downloading the settings file, the deskphone downloads any language or certificate files required by the settings. Finally, if necessary, the deskphone downloads new software files.

Choosing the right application file and upgrade script file

Software files needed to operate the 9600 Series IP Deskphones are packaged together in either a Zip format or 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: www.avaya.com/support based on the protocol that you are using (H.323 or SIP) for all or the majority of your deskphones.

SIP software distribution packages contain:

- One application upgrade file
- One platform upgrade file

- Certificate files
- 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 deskphone software, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.

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 Deskphones 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-deskphone basis using the SIG Craft procedure as described in *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.

About the upgrade file

The upgrade file specifies whether the deskphone needs to upgrade the software or not. The upgrade file is either H.323-specific(96x1Hupgrade.txt) or SIP-specific (96x1Supgrade.txt).

Do not alter the upgrade file and use the 46xxsettings.txt file to customize your settings instead.

About the settings file

The settings file contains the parameters that you can use to customize your enterprise 9600 Series IP Deskphones.

Note:

> You can use one settings file for all your Avaya IP deskphones. The settings file includes configuration parameters for 9600 Series SIP IP Deskphones that are covered in this document, 4600Series IP Deskphones, and 1600 Series IP Deskphones, 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 deskphone 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. In pre-6.0 SIP software releases, BOOTNAME and SIG could also be used. In SIP software release 6.0 and later, SIG_IN_USE can also be used.
- `SET` commands, of the form **SET *parameter_name value***. Invalid values cause the specified value to be ignored for the associated ***parameter_name*** so the default or previously administered value is retained. All values must be text strings, even if the value itself is numeric, a dotted decimal IP Address, 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 deskphone 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 deskphone 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 7: 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 deskphone or read as a comment starts with “##”.

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

Parameter	Description
BOOTNAME	Pre-6.0 software releases only. The name of the Signed Kernel/Root Software package in the deskphone.
MACADDR	MAC address of the deskphone (hh:hh:hh:hh:hh:hh; automatically supplied by a deskphone).
MODEL	Deskphone Model identifier (8 ASCII characters; automatically supplied by a deskphone).
MODEL4	The first four digits of the model identifier (automatically supplied by a deskphone).
GROUP	Group identifier (must be manually set on a deskphone)
SIG	Pre-6.0 software releases only. Signalling protocol identifier (2=SIP, 1=H.323, 0=default).

Parameter	Description
SIG_IN_USE	The signaling protocol in use. For SIP software value is always "SIP" and cannot be changed. 6.0 and later software Releases only. Evaluate configuration files according to value of this parameter (IF…GOTO command) and consider only commands related to the corresponding section of configuration files. 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 or 5061 for TLS.
## 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=tcp
## Presence Enabled
## Determines whether presence functionality is
## enabled on the phone.
## 0 for No
## 1 for Yes
SET ENABLE_PRESENCE 1
## 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 Deskphone 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 Deskphone 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.
## See _ for format and setting alternatives.
## SET DSTSTOP "1SunNov2L"
##
------------------------------
```

About the Avaya Menu administration file

The Avaya Menu administration file contains parameters to customize Avaya Menu and to view Web links on Avaya Menu. You can administer up to eight Web links.

To customize Avaya Menu, you need to:

- Create the Avaya Menu Administration file named AvayaMenuAdmin.txt and configure appropriate parameters.
- Set the AMADMIN parameter in the settings file to point to the HTTP server location where you save the AvayaMenuAdmin.txt file.

The AvayaMenuAdmin.txt file contains the following parameters:

Parameter	Description
AMTYPE*xx*	Specifies the type of Avaya Menu option that you want to configure. For the 9601, 9608, 9608G, and 9611G deskphones, you can assign the following values to this parameter: ● 1 for Web link ● 2 for the Options & Settings option ● 3 for the Network Information option ● 4 for the About Avaya one-X option ● 5 for the Log Out option For the 9621G and 9641G deskphones, you can assign the following values to this parameter: ● 1for Web link ● 2 for the Options & Settings option ● 3 for the Network Information option ● 4 for the Light Off option ● 5 for the Touch Screen Cleaning option ● 6 for the About Avaya one-X option ● 7for the Log Out option where, *xx* is a two-digit integer from 01 to 12. If AMTYPE*xx* is 1 then you must also define the following parameters: ● AMLBL*xx* ● AMDATA*xx* where, *xx* must be the same for each of the three parameters. If AMTYPE*xx* is 2, 3, or 4, the system ignores any value that you specify for AMLBL*xx* or AMDATA*xx*.
AMLBL*xx*	Specifies the label that the deskphone displays for the Web link. The label must not exceed 16 UTF-16 characters.
AMDATA*xx*	Specifies the URI for the Web link. The URI must not exceed 255 ASCII characters.

You can specify 12 Web links, but the deskphone displays only the first eight Web links. If you have also configured the browser, the deskphone displays eight Web links that includes the browser.

The deskphone displays any built-in application for which you set the respective parameter to display the application, even if you do not configure that application in the AvayaMenuAdmin.txt file.

Following is a sample of the AvayaMenuAdmin.txt file.

```
############################################################
##     AVAYA MENU CONFIGURATION FILE TEMPLATE                  ##
```

```
############################################################
## This file is to be used as a template for configuring Avaya Main
## Menu. See the LAN Administrators Guide nd the Avaya one-X™ Deskphone
## Edition for 9600 Series and the Avaya one-X™ Deskphone Edition for
## 9600 Series and the Avaya one-X™ Deskphone Edition for 9600 Series
## IP Telephones Administrator Guide for details.
## Both are available on support.avaya.com
############################################################

## AMLBLxx=Lable   up to 16 unicode character
##
## AMTYPExx=Type   1=WML-Application, 2=local Phone Settings,
## 3=local LogOff Application, 4=local About Avaya Screen
##
## AMDATAxx        URI of up to 255 ASCII-characters
## e.g. http://yy.yy.yy.yy/*.wml
##
## The tags AMLBLxx and AMDATAxx are only used if AMTYPExx = 1
##
## Multiple definitions of local applications (Type 2..4)
## will be supressed. The last tag is valid.
##
## xx describes the sequence in A-Menu and is valid
## from 01 to 12
##

##AMTYPE01=
##AMLBL01=
##AMDATA01=

##AMTYPE02=
##AMLBL02=
##AMDATA02=
##AMTYPE03=
##AMLBL03=
##AMDATA03=

##AMTYPE04=
##AMLBL04=
##AMDATA04=

##AMTYPE05=
##AMLBL05=
##AMDATA05=

##AMTYPE06=
##AMLBL06=
##AMDATA06=

##AMTYPE07=
##AMLBL07=
##AMDATA07=

##AMTYPE08=
##AMLBL08=
##AMDATA08=

##AMTYPE09=
##AMLBL09=
##AMDATA09=

##AMTYPE10=
##AMLBL10=
##AMDATA10=

##AMTYPE11=
##AMLBL11=
##AMDATA11=

##AMTYPE12=
##AMLBL12=
##AMDATA12=
```

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 *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP* and specify which GROUP number to use. The GROUP System value can only be set on a deskphone-by-deskphone 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.

The following 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 7: Administering deskphone options

Administering options for the 9601,9608, 9608G, 9611G, 9621G, and 9641G SIP deskphones

This chapter provides information about changing parameter values to customize your operating environment.

The is a comprehensive list of all parameters that you can configure. This list contains the following:

- Parameter names
- Default values
- Valid ranges for the values
- Description of each parameter

However, you do not have to set every parameter. In most cases, you need to 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:

Ensure that you set the SIP-related parameters: SIP_CONTROLLER_LIST, SIPDOMAIN, SNTPSRVR, ENABLE_PRESENCE, GMTOFFSET, DSTOFFSET, DSTSTART, and DSTSTOP.

You can now also preconfigure some of the user selectable settings through System Manager that could only be configured through the deskphone. Any change by a user overrides these parameters that are set through System Manager. For more information about parameters, see *Administering Avaya Aura® System Manager*.

To restrict the user from entering into the Craft menu, 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 *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP* 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.

This section provides information on parameters that can be set from the 46xxsettings file. You can also set some of these parameters through LLDP, DHCP, the Craft menu, or download them from the Avaya Aura System Manager, that is PPM. A predefined order determines the parameter value that a deskphone uses. For more information about the order in which a deskphone uses parameter values, see Administration alternatives and options on page 3.

Customizable system parameters for SIP-based 9600 Series IP Deskphones

Note:

Depending on your server configuration, some of the parameters mentioned in the table might not work in your environment. Ensure that the configurations in the 46xxsettings.txt file matches with the configurations that you perform through System Manager.VLAN settings.

Parameter Name	Default Value	Description and Value Range
100REL_SUPPORT	1	Used to control the optional tag 100rel in the INVITE header field. The values are: ● 0 when the tag is not included ● 1 when the tag is included
AGCHAND	0	Automatic Gain Control status for handset. Values are 0=disabled, 1=enabled.
AGCHEAD	0	Automatic Gain Control status for headset. Values are 0=disabled, 1=enabled.
AGCSPKR	0	Automatic Gain Control status for speaker. Values are 0=disabled, 1=enabled.
ALLOW_DND_SAC_LINK_ CHANGE	0	Specifies whether the user can control the link between Send All Calls (SAC) and Do not Disturb (DND) behaviors. When the behaviors are linked, the deskphone invokes SAC when the user manually selects DND. You can assign following values to this parameter: ● 0: User gets the control to link the SAC and DND behaviors. Accordingly, the deskphone displays the appropriate menu to set the link. ● 1: User does not get the control to link the SAC and DND behaviors.

Parameter Name	Default Value	Description and Value Range
AMADMIN	Null	Used to display multiple Web links. On button deskphones, the Web links appear as options on Avaya Menu. On touchscreen deskphones, the Web links appear as icons on the Home screen. You can administer the Web links through the Avaya Menu administration file, AvayaMenuAdmin.txt, and assign the location of this file to the AMADMIN parameter. If this parameter is null, the deskphone does not download the AvayaMenuAdmin.txt file. For more information on the AvayaMenuAdmin.txt file, see About the Avaya Menu administration file. For example, ## SET AMADMIN http://192.168.0.28
ASTCONFIRMATION	32	The time that the deskphone waits to validate an active subscription when the deskphone subscribes to the avaya-cm-feature-status package. The valid range is 16 - 3600 seconds.
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. This parameter is used to lower the ambient noise that the deskphone transmits in a call. Values range from 0 through 299. For more information, see the document *Audio Quality Tuning for IP Telephones*, available on the Avaya support website www.avaya.com/support.

Parameter Name	Default Value	Description and Value Range
AUDIOSTHD	0	Headset sidetone setting. Values are: 0 = Default; no change. 1 = Three steps softer than nominal. 2 = Off; inaudible. 3 = One level softer than nominal. 4 = Two steps softer than nominal. 5 = Four steps softer than nominal. 6 = Five steps softer than nominal. 7 = Six steps softer than nominal. 8 = One step louder than nominal. 9 = Two steps louder than nominal.
AUDIOSTHS	0	Handset sidetone setting. Values are: 0 = Default; no change. 1 = Three steps softer than nominal. 2 = Off; inaudible. 3 = One level softer than nominal. 4 = Two steps softer than nominal. 5 = Four steps softer than nominal. 6 = Five steps softer than nominal. 7 = Six steps softer than nominal. 8 = One step louder than nominal. 9 = Two steps louder than nominal.
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

Parameter Name	Default Value	Description and Value Range
AUTO_SELECT_AN_ IDLE_APPR	0	Automatically selects any idle call appearance for conference or transfer. The selection of idle call appearance applies only when the transfer or conference is initiated from a bridged appearance. This parameter is ignored if CONF_TRANS_ON_PRIMARY_APPR is set to 1. Valid values are: ● 0, if an idle bridged call appearance of the same extension is not available, the conference or transfer fails. ● 1, if an idle bridged call appearance of the same extension is not available, an idle call appearance is used.
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 (16.65 hours).
BCA_BUTTON_RING_ TYPE_PER_BUTTON	Each name-value pair has the same value as the PERSONALWAV parameter	Specifies a list of name-value pairs that indicate default ring tones or the ring tones that user selects for each Bridged Call Appearance administered on the deskphone.
BRANDING_VOLUME	5	The volume at which the deskphone plays the Avaya audio clip when the user logs in to the deskphone or unlocks the deskphone. Accepted values are 1 through 8. 1 is the minimum volume and 8 is the maximum volume.

Parameter Name	Default Value	Description and Value Range
BUTTON_MAPPINGS	" " (Null)	A mechanism for a Contact Center environment to disable the Forward, Speaker, Hookswitch/ Switchhook, and Headset buttons and to remap the Speaker button as a Release button. You can assign the following values attributes to this parameter: ● Forward ● Speaker ● Hookswitch ● Headset You can assign the following values to each of these attribute: ● na to disable the button. ● cc-release to remap the button as the Release button. For example, the following setting disables the Forward, Hookswitch/Switchhook, and Headset buttons and remaps the Speaker button as the Release button. SET BUTTON_MAPPINGS "Forward=na,Speaker=cc-release,Hookswitch=na, Headset=na"
CALL_TRANSFER_ MODE	0	Used to specify how transfers are performed when ENABLE_AVAYA_ENVIRONMENT=0. You can assign the following values to this parameter: ● 0 for attended transfer ● 1 for unattended transfer
CALLFWDADDR	" " (Null)	Used to specify the URI to which calls are forwarded in failover.
CALLFWDDELAY	1	Failover environments only. Specifies the number of ring cycles generated at the deskphone 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.

Parameter Name	Default Value	Description and Value Range
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. You can assign the following values to this parameter: ● 0 for no Call Forwarding permitted. ● 1 for Call Forward Unconditional only permitted. ● 2 for Call Forward Busy only permitted. ● 4 for Call Forward No Answer only permitted. ● Others for sum of Call Forward types permitted.
CALL_PICKUP_RING_ TYPE	1	Used to choose between default ringing patterns. Range of values: 1 to 8.
CC_INFO_TIMER	8	Specifies the SIP CC-INFO event package timer in hours. The range is 1 to 24.
CF_RINGTONE	0	Specifies the ring tone that the deskphone plays for an incoming call that is forwarded to the deskphone. The parameter can have the following values: ● 0: The deskphone plays the ring tone that the user assigned to the calling deskphone. ● 1: The deskphone plays the ring tone that the user assigned to the first deskphone that forwarded the call. The deskphone plays the default incoming ring tone if the user did not assign a ring tone to the calling deskphone or the first deskphone that forwarded the call.
CLDISPCONTENT	1	Used to control the display of the called or the calling number on the History screen. You can assign the following values to this parameter: ● 0 to display the called and the calling number. ● 1 to suppress the display of the called and the calling number.

Parameter Name	Default Value	Description and Value Range
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.
CONFERENCE_FACTORY_URI	" " (Null)	This is the adhoc service URI for Avaya Aura Conferencing. Presently, this is supported for use with AAC7. The URI consists of a dial string with domain. For example, 3375000@avaya.com. This must match the routing pattern configured in System Manager for Adhoc Conferencing. Depending on your dialing plan, you might need to prefix this number with an access code, for example- 93375000@avaya.com. The domain portion of the SIP URI can be in the form of an IP address or an FQDN.
CONFERENCE_SERVER_ADDRESS	Null	Specifies the IP address of Avaya Aura Conference Server (AACS) in the dotted decimal format.
CONFIG_SERVER_SECURE_MODE	1	Indicates whether or not secure communication through HTTPS is required to access the configuration server. 0 = Use HTTP. 1 = Use HTTPS. 2 = Use HTTPS if SIP transport mode is TLS, otherwise use HTTP.
CONFERENCE_SERVER_PORT	443	Specifies the AACS destination port.

Parameter Name	Default Value	Description and Value Range
CONF_TRANS_ON_ PRIMARY_APPR	0	Affects the idle line that is selected when initiating a conference or transfer on a call appearance or a bridge appearance. The valid values are: ● 0 - When initiated from a call appearance, an idle call appearance is used if available. If an idle call appearance is not available, an idle bridge appearance is used. - When initiated from a bridge appearance, an idle bridge appearance for the same extension is used if available. If an idle bridge appearance is not available, AUTO_SELECT_ANY_IDLE_APPR defines the behavior. ● 1 - An idle call appearance is always used if available regardless of whether the operation was initiated from a call appearance or bridge appearance. - If an idle call appearance is not available, the conference or transfer fails.
CONNECTION_REUSE	1	Specifies whether the deskphone supports the TLS connection reuse. Valid values are: ● 0: Disables the TLS connection reuse. ● 1: Enables the TLS connection reuse, that is, the deskphone does not open a listening socket and maintains and reuses the sockets that the deskphone creates with the outbound proxies. The SIP messages initiated by the call server are sent to the source port of the origination message from the deskphone. This parameter is only supported on Session Manager and Branch Session Manager and not on other proxy servers such as IP Office and third-party gateways. You must set the parameter to 0 if you are using the third-party gateways.
CONTROLLER_SEARCH_ INTERVAL	16	Time in seconds that the deskphone waits to complete the maintenance check for monitored controllers. Valid values are 4 - 3600 (seconds).

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_LOGO	" " (Null)	Defines the selected background logo on display, if any. The value of this parameter indicates if a custom logo is currently selected (non-empty string) or a built-in default logo is used (empty string or not set). The user can also set the current logo from the deskphone, through the Avaya menu. However, to use a custom logo, the logo must be defined in the LOGOS configuration parameter.
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"
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.

Parameter Name	Default Value	Description and Value Range
DISCOVER_AVAYA_ ENVIRONMENT	1	Allows the deskphone 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, the deskphone displays only the caller name. Valid values are: 0 = Show caller name only. 1 = Show caller name followed by number. 2 = Show caller number only. 3 = Show caller number followed by name. **Note:** For Avaya Aura® CCElite environment, deskphones display the VDN name associated with the call along with the caller name. Use value 1 or 3 so that the deskphone always displays meaningful information even if the caller name is not available.
DND_SAC_LINK	0	The value of this parameter is used only if the ALLOW_DND_SAC_LINK_CHANGE is set to 0. Specifies whether the behavior of Send All Calls (SAC) and Do Not Disturb (DND) features are linked. If the features are linked, the deskphone activates SAC when user activates DND. The parameter can have the following values: ● 0: Does not link the SAC and DND behaviors. ● 1: Links the SAC and DND behaviors.

Parameter Name	Default Value	Description and Value Range
DND_SAC_LINK_MANUAL	0	The value of this parameter is used only if the ALLOW_DND_SAC_LINK_CHANGE is set to 1. Specifies whether the user linked the Send All Calls (SAC) and Do Not Disturb (DND) behaviors. If the features are linked, the deskphone activates SAC when user activates DND. The parameter can have the following values: ● 0: User did not link the SAC and DND behaviors. ● 1: User linked the SAC and DND behaviors.
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.
DOT1X	0	Defines the deskphone's operational mode for IEEE 802.1X.Valid values are: 0 = Unicast Supplicant operation only, with EAP multicast pass-through, but without proxy Logoff. 1= Unicast Supplicant operation only, with EAP multicast pass-through and proxy Logoff. 2= Unicast or multicast Supplicant operation, without EAP 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. 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.

Parameter Name	Default Value	Description and Value Range
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.
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)

Parameter Name	Default Value	Description and Value Range
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.
ENABLE_CALL_LOG	1	Used to enable or disable call logging. You can assign the following values to this parameter: ● 1 to enable call logging. ● 0 to disable call logging. If you disable call logging, the deskphone does not display the screens related to call logs and any menu item that you use to set the call log options.
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.

Parameter Name	Default Value	Description and Value Range
ENABLE_EARLY_MEDIA	1	This parameter enables SIP early media. 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 deskphone. If the parameter is set to 1, the deskphone includes G711A capability in an outbound INVITE request, and accepts G711A when received in an incoming INVITE request. Values are 0=disabled; 1=enabled. **Note:** If the gateway in your network does not support wideband audio codec, you must include codec sets for the Deskphones to work in your network.
ENABLE_G711U	1	Enable or disable G711U codec capability of the deskphone. If the parameter is set to 1, the deskphone includes G711U capability in an outbound INVITE request, and accepts G711U when received in an incoming INVITE request. Values are 0=disabled; 1=enabled.
ENABLE_G722	1	Enable or disable G722 capability of the deskphone. If the parameter is set to 1, the deskphone 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, 1=Enabled.
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.

Parameter Name	Default Value	Description and Value Range
ENABLE_G729	1	Enable or disable G729A codec capability of the deskphone. Values are: 0=G.729 disabled. If set to 0, processing of G729A as a capability is disabled. 1 = The deskphone 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 deskphone accepts either G729(A) or G729AB. 2 = The deskphone 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 deskphone accepts either G729A or G729AB.
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_OOD_MSG_TLS_ ONLY	1	Determines whether a received Out-Of-Dialog (OOD) REFER must have TLS transport. Values are: 1 = The ODD REFER must have TLS. 0 = The ODD REFER must have either TCP or TLS.
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. If you want to enable this feature for a selected number of stations in your network, you can do so by listing those stations under separate groups and by enabling this feature only for the group, which you want this feature to be available for.

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. You must set the value of this parameter to 1.
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 deskphone is communicating with an AST-capable controller has no effect).
ENABLE_SECURE_HTTP_ FOR_CONFERENCING_ SERVICE	1	Specifies the security of the AACS communication. You can assign the following values to this parameter: ● 1 for secure ● 0 for insecure

Parameter Name	Default Value	Description and Value Range
ENFORCE_SIPS_URI	1	Controls the enforcement of SIPS URI with SRTP. Valid values are: 0 = Allow either SIPS URI for incoming SRTP media encryption calls and use only SIPS URI for outgoing SRTP media encryption calls. 1 = Accept and use only SIPS URI for incoming and outgoing calls with SRTP media encryption. The value of this parameter must match with the value of the same parameter on Communication Manager.
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).
ENTRYNAME	0	For an Avaya Aura® Contact Center environment, this parameter sets the entry name as the Calling Party Name or the VDN/Skills Name. Values are: 0 = Use the called party name to populate the Entry Name field in the Contacts List View Screen 1 = Use VDN or Skill name to populate the Entry Name field in the Contacts List View Screen
EVENT_NOTIFY_AVAYA_ MAX_USERS	20	The maximum number of participants returned in the conference event SIP notification. The range is 0 to 1000.
EXCHANGE_EMAIL_ DOMAIN	Null	Specifies the Exchange email domain. The value can contain 0 to 255 characters. You can get the email address of a user if you combine the value of this parameter with the value of EXCHANGE_USER_ACCOUNT. For example, SET EXCHANGE_EMAIL_DOMAIN avaya.com
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).

Parameter Name	Default Value	Description and Value Range
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_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.
EXCHANGE_SERVER_MO DE	3	Specifies the protocol that the deskphone uses to communicate with the Exchange server. You can assign the following values to this parameter: • 1: To use WebDAV. • 2: To use Exchange Web Services (EWS). • 3: To use both. In this case, the deskphone tries to communicate with EWS first. If EWS fails, the deskphone communicates with WebDAV. For example, SET EXCHANGE_SERVER_MODE 1
EXCHANGE_SERVER_SE CURE_MODE	1	Specifies whether the deskphone communicates with the Exchange server over https or http. You can assign the following values to this parameter: • 0: To use HTTP • 1: to use HTTPS For example, SET EXCHANGE_SERVER_SECURE_MODE 0
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.

Parameter Name	Default Value	Description and Value Range
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. The valid values are: ● admin: The deskphone waits for administrative intervention before attempting to failback to a higher priority controller. ● auto: The deskphone periodically checks the availability of the primary controller and fails back to the primary controller if available. When the phone fails over from a core Session Manager to a Branch Session Manager, it temporarily changes the value of the FAILBACK_POLICY parameter to admin. When the deskphone fails back to the core Session Manager, it reverts to the FAILBACK_POLICY value that was set when the active controller was a core Session Manager. **Note:** The value that is set in System Manager overwrites this value.
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. The valid values are 0 - 32 seconds. **Note:** This parameter is mandatory in System Manager and the System Manager value overwrites this value. The default value in System Manager is 2 seconds.
G726_PAYLOAD_TYPE	110	RTP dynamic payload used for G.726. Range is 96 to 127.

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	The conditional parameter with which different groups of deskphones can have different parameter settings within the same 46xxsettings.txt file. This is typically set using the CRAFT menu on the deskphone, and it cannot be set through the 46xxsettings file.
HEADSET_PROFILE	0	Specifies the headset audio profile that the user selects. If the user selects a headset audio profile, the deskphone overrides the default profile and provides the profile specified in this parameter. The parameter can have any value from 0 to 20. The value 0 indicates that the user did not select a headset profile. As Avaya supports only eight headset audio profiles for now, the maximum value that this parameter can have is 8.
HEADSET_PROFILE_ DEFAULT	1	Specifies the default headset audio profile that the deskphone provides to the user. You can assign any value from 1 to 20. As Avaya supports only eight headset audio profiles for now, the maximum value that you can specify to this parameter is 8.

Parameter Name	Default Value	Description and Value Range
HEADSET_PROFILE_NAMES		Specifies an ordered list of names for headset audio profiles. If you set this parameter, the deskphones displays the audio profile name as you specify in this parameter. The list can contain 0 to 255 UTF-8 characters. Provide names of headset audio profiles as comma separated list without any intervening space. Two commas in succession indicate a null name for the corresponding headset audio profile. In such a case, the deskphone displays the default name of the profile. When you name the headset audio profiles, ensure that: ● You do not include a comma or a double quote character in the name. ● Quote the entire list if you include a space in any of the names. ● Specify a name that has the length that your deskphone can display. If the length of the name exceeds the specified limit of your deskphone, the deskphone truncates the name. For example, SET HEADSET_PROFILE_NAMES "Acme Earwigs,,Spinco Ear Horns" In this case, if the deskphone has five profiles, then the deskphone renames only the first and the third headset audio profiles. The deskphone does not rename the second profile or any profile beyond the third profile. Hence, the deskphone displays the names as follows: ● Acme Earwigs ● Profile 2 ● Spinco Ear Horns ● Profile 4 ● Profile 5 The deskphone ignores all names that you specify in the HEADSET_PROFILE_NAMES parameter that do not have corresponding profiles on the deskphone. For example, if a deskphone has five profiles, and you specify a sixth profile name in the parameter, the deskphone will not display the sixth profile name.

Parameter Name	Default Value	Description and Value Range
HEADSET_SIGNALING	0	Specifies the option that the user set for headset behavior. The parameter can have the following values: ● 0: Disabled: User disabled the headset setting. ● 1: Switchhook and Alert: User activated the alert and receive call setting for the headset. ● 2: Switchhook only: User activated only the receive call setting for the headset.
HEADSYS	0	Defines the Headset operational mode. 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.
HOMEIDLETIME	10	Specifies the number of minutes after which the Home screen will be displayed. The accepted values are 0 through 30.
HOTLINE	" " (Null)	Specifies the "hotline" number to dial when the user goes off-hook.
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.

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. The valid values are: ● 0: Redirect messages will neither be transmitted nor processed when received. ● 1: Redirect messages will not be transmitted, but received Redirect messages will be supported according to 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.
INSTANT_MSG_ENABLED	1	Enables or disables the Instant Messaging feature. Values are: 0= Disable, 1 = Enable.
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.

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.
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.
LANGLARGEFONT	" " (Null)	Filename or URL of the file that contains the large language font. For example, Mlf_Englarge.xml. Ensure that the file (Mlf_Englarge.xml) resides in the web root of the http server.
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.

Parameter Name	Default Value	Description and Value Range
LNQ	0	Specifies the current value of the Local Network Quality parameter as determined by the system. The parameter can have any value in teh range of 0 to 6.
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.
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).
LOCALLY_ENFORCE_ PRIVACY_HEADER	0	Locally enforces the display when Privacy header is included in the INVITE for an incoming call. Values are: 0 = Disabled, the responsibility for privacy is with the call server. 1 = Enabled, the responsibility for privacy is with the endpoint.
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.

Parameter Name	Default Value	Description and Value Range
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
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.
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.

Parameter Name	Default Value	Description and Value Range
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 deskphone'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 /.
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.
NO_DIGITS_TIMEOUT	20	Number of seconds of delay after going "off-hook" or getting secondary dial tone before the deskphone 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.

Parameter Name	Default Value	Description and Value Range
PERSONALWAV	1	Specifies the ring tone that the user selects. This parameter can have any of the following values: ● 1-8: Implies that the user selected a classical ring tone. Classical ring tone can be North American or European depending on the value that you assigned to the RINGTONESTYLE parameter. ● 9-14: Implies that user selected a rich ring tone. ● Ring tone name: Implies that the user selected a downloaded ring tone.
PHNEMERGNUM	" " (Null)	The number dialed when the Emerg softkey is pressed, or when a pop-up screen for making an emergency call is confirmed. This parameter can be set through both System Manager and the settings file.
PHNMOREEMERGNUMS	" " (Null)	Specifies 100 emergency numbers. This parameter can be set through both System Manager and the settings file.
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.”
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.
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".

Parameter Name	Default Value	Description and Value Range
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".
PHNMUTEALERT_BLOCK	1	Blocks/unblocks the Mute Alert feature. Valid values are: 0 = Unblocked/Allowed; allows a 9621G/9641G end user to set mute alerting via the Home screen Settings menu. 1 = Blocked; mute alerting not allowed.
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	3	When ENABLE_AVAYA_ENVIRONMENT=0, this value sets the number of Session Appearances. When the deskphone is in AST environment (registered to a proxy with PPM server and Avaya Communication Manager on the background), the deskphone will use the number of call appearances sent by PPM (i.e. call-appearance provisioned on Communication Manager). In case this parameter is set the deskphone 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 Communication Manager in the background, the deskphone is in a non-AST environment); in this case the deskphone used this parameter to set its call-appearance.
PHONE_LOCK_IDLETIME	0	Sets the idle time (in minutes) before the deskphone locks itself. The range is from 0 to 10080. If set to 0, the deskphone never locks.
PHY1STAT	1	Ethernet line interface setting. The values are: 1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex.
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.

Parameter Name	Default Value	Description and Value Range
PHY2STAT	1	Secondary Ethernet interface setting. The values are: 0=Secondary Ethernet interface off or disabled, 1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex.
PHY2TAGS	0	Specifies whether the deskphone removes the tags from frames that the deskphone forwards to the secondary Ethernet interface. You can assign the following values to this parameter: 0: To remove the tags. 1: To not remove the tags. For example, SET PHY2TAGS 1
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.
PLAY_TONE_UNTIL_RTP	1	Determines when to cut through RTP for an early media session. Values are: 0 = Cut through RTP as soon as SDP is received. 1 = Cut through RTP only after RTP is received after received SDP.

Parameter Name	Default Value	Description and Value Range
PLUS_ONE	0	Controls the cycling of symbols, including "+", on the 1 key. 0 = Do not cycle through symbols 1 = Cycle through symbols When the deskphone is in editable dialing mode and: PLUS_ONE=1: The user can use the key 1 to append the "+" as the first digit of a dial string. PLUS_ONE=0: The user can not use the key 1 to append the "+" as the first digit of a dial string. When the user goes off-hook to dial, irrespective of the dial mode or the value of the parameter PLUS_ONE, the user can use the * key to append "+". Alternatively, the user can also use the "+" softkey.
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.

Parameter Name	Default Value	Description and Value Range
PRESENCE_ACL_ CONFIRM	0	Specifies whether the deskphone automatically confirms a request from a watcher to monitor user presence. You can assign following values to this parameter: ● 0: Indicates auto confirm. In this case, the deskphone auto confirms requests from all watchers to monitor user presence. ● 1: Indicates ignore. In this case, the deskphone ignores requests from all watchers to monitor user presence. A shared control client or another device registered with the same AOR as the deskphone displays a prompt to the user. The prompt confirms whether to accept or deny a request from a watcher to monitor user presence. To display the prompt, the shared control client or the device with the same AOR must also subscribe to presence and must have an interface that can display the prompt. **Note:** Note: This parameter has no effect if you configure the Presence server to auto confirm all watchers request to monitor user presence.
PRESENCE_SERVER	" " (Null)	This parameter is used for releases before Avaya Aura® 6.2 FP4. For releases Avaya Aura® 6.2 FP4 and later, the phone retrieves the address of the Presence Server and Instant Messaging Server from PPM. 0 to 255 characters: 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).

Parameter Name	Default Value	Description and Value Range
PROCPSWD	27238	Text string containing the local (dialpad) procedure password (4-7 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. **Note:** You must not use the default value and change the default value at the time of initial installation.
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
PROVIDE_CF_RINGTONE	0	Specifies whether the deskphone displays the call forward ring tone option to users. The call forward ring tone option provides to users the choice to select the ring tone that the users want to hear for a forwarded call. Users can select to hear the ring tone that the users assigned to the: ● Calling deskphone ● First deskphone that forwarded the call You can specify the following values to this parameter: ● 0: The deskphone does not display the call forward ring tone option. ● 1: The deskphone displays the call forward ring tone option
PROVIDE_EXCHANGE_ CALENDAR	1	Defines whether or not menu items for Microsoft Exchange® Calendar integration are provided to user. Values are: 0=Off; 1=On.
PROVIDE_EXCHANGE_ CONTACTS	0	Defines whether or not menu items for Microsoft Exchange® Contact integration are provided to user. Values are: 0=Off; 1=On.

Parameter Name	Default Value	Description and Value Range
PROVIDE_KEY_REPEAT_ DELAY	0	Allows the administrator to set the time interval that invokes a response when a key is pressed. This allows a user to hold down a key and invoke a repetitive action. This parameter can take values from 0 through 9. Values 0, 1, 2, 3, 4 are for "unlocked" and values 5, 6, 7, 8, 9 are for "locked". "Unlocked" allows the user to set the value, while "locked" prevents the user from setting a value for repeat delay. The timer values are: 0 or 5= 500 ms 1 or 6= 250 ms 2 or 7= 1000 ms 3 or 8= 2000 ms 4 or 9= Disable
PROVIDE_ LOGOUT	1	Defines whether or not logout function is provided to user. If disabled and the deskphone is operating in user mode, hide "Logout" item in option menu. Values are: 0=Off; 1=On.
PROVIDE_NETWORKINFO _SCREEN	1	Defines whether or not "Network Information" menu is provided to user. If disabled and the deskphone is operating in user mode, hide complete "Network Information". Values are: 0=Off; 1=On.
PROVIDE_OPTIONS_ SCREEN	1	Defines whether or not "Options & Settings" menu is provided to user. If disabled and the deskphone is operating in user mode, hide complete "Option & Settings" menu tree. Values are: 0=off; 1=on.
PROVIDE_TRANSFER_ TYPE	0	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).

Parameter Name	Default Value	Description and Value Range
PUSHCAP	00000	String representing push capabilities. Consists of five digits abcde, where: • a is to control phonexml pushes and supports only the barge-in priority • b is to control audio transmit pushes • c is to control audio receive pushes and multicast pushes • d is to control display or Web pushes • e is to control top line pushes The valid values for abcde are 0,1,and 2, where: • 0 is to disable • 1 is to support barge-in pushes • 2 is to support normal pushes For example, SET PUSHCAP = 12222 sets barge-in pushfor phonexml and both barge-in and normal pushes for remaining push types.
PUSHPORT	80	String representing the TCP listening port number used for the deskphone's HTTP server. Values are: 2 to 5 ASCII numeric digits, "80" through "65535".
QLEVEL_MIN	4	Specifies the minimum quality level for which the deskphone does not display a low local network quality icon. You can assign any value in the range of 1 to 6.
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).

Parameter Name	Default Value	Description and Value Range

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 deskphone 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	This parameter is used in a failover environment where the deskphone fails over to a non-Aura proxy. If no response is received to a REGISTER request within the number of seconds specified by WAIT_FOR_REGISTRATION_TIMER, the telephone will try again after a randomly selected delay of 50% to 90% of the value of RECOVERYREGISTERWAIT. RECOVERYREGISTERWAIT is configured in SMGR and delivered to the phone via PPM and is a higher priority than the value delivered in the settings file.
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 deskphone 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.

Parameter Name	Default Value	Description and Value Range
REGISTERWAIT	900	The number of seconds for next reregistration to SIP server. The range is 30 to 86400 seconds. The value of this parameter is overridden by the value set in System Manager that the deskphone receives through Personal Profile Manager (PPM).
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.
RINGTONES	Null	Specifies a list of audio files that deskphones download as ring tones. The users can select the required ring tone from the downloaded list. For more information, see Downloadable ring tones.
RINGTONESTYLE	0	Specifies the style of classic ring tones that the deskphone displays. You can provide the following values: ● 0: To display the North American ring tones ● 1: To display the European or extended ring tones
RINGTONES_UPDATE	0	Specifies whether the deskphone at reset or start up sends a query to the file sever to check for the updated version of downloadable ring tones. You can assign the following values to this parameter: ● 0: The deskphone does not check for the updated version of downloadable ring tones, but downloads any new audio file. ● 1: The deskphone checks for the updated version of downloadable ring tones and downloads any audio file that has an updated version.
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.

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	The 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	1	Used for securing voice (SRTP) transmissions. Controls SDP capability negotiation. Interaction between the SDPCAPNEG and MEDIAENCRYPTION parameters controls INVITE behavior. The valid values are: ● 1 to enable SDP capability negotiation. ● 0 to disable SDP capability negotiation.

Parameter Name	Default Value	Description and Value Range
SECURECALL	0	Controls the display of a secure call icon on the user interface. Values are: 0 = The icon is not displayed. 1 = The icon is displayed.
SEND_DTMF_TYPE	2	Defines whether DTMF tones are sent: ● In-band, that is, regular audio, or ● Out-band, that is, negotiation and transmission of DTMF according to RFC 2833. If the far end does not support RFC 2833, send in-band DTMF tones. The valid values are: ● 1 for in-band DTMF ● 2 for RFC 2833 procedure
SIG	0	Indicates the Software Distribution Package to download during start-up or reboot. The valid values are: ● 0 for Default ● 1 for H323 ● 2 for SIP
SIG_PORT_LOW	1024	Lower limit of port range for signaling to support by the deskphone. Values range from 1024 to 65503.
SIG_PORT_RANGE	64511	Port range for signaling to support by the deskphone. Values range from 32 to 64511.
SIMULTANEOUS_ REGISTRATIONS	3	Defines the number of simultaneous Session Manager and Branch Session Manager registrations that the deskphone should maintain. Valid values are 1-3. **Note:** The value of this parameter must not be less than the number of core Session Managers in the SIP_CONTROLLER_LIST.

Parameter Name	Default Value	Description and Value Range
SIP_CONTROLLER_LIST	" " (Null)	List of SIP proxy or registrar server IP addresses. Servers used to address SIP registrations and signaling if operating in proxy mode. In case of several entries, the servers are used in the order they are listed. When operating in an Avaya Environment, SIP_CONTROLLER_LIST is also used to access Personal Profile Manager (PPM). This parameter is considered as the list of configured controllers for failover logic. When this parameter has multiple IP addresses, the ordering of the list defines the priority of the controllers for selection during a failover. The first element of the list is the highest priority, the last element is the lowest priority. For more information about failover, see Chapter 9: System failover and survivability. The following format is used. host[:port][;transport=xxx] where, ● host is an IP address in dotted decimal format. ● port is the optional port number. If not specified, the default port value of 5060 for TCP or 5061 for TLS is used. ● transport is the optional transport type, where *xxx* is tls or tcp. If not specified, the default value of TLS is used. **Note:** Use TCP or TLS for SIP signaling. UDP is not supported. This parameter is unique in that values received from various data sources are combined into an aggregated list. The aggregated list is prioritized by data source and has all duplicates removed. For more information, see Controller Determination and Survivability Activity on page 4.
SIP_PORT_SECURE	5061	The deskphone’s listening port for inbound connections (for secure message transfer via TLS). Values range from 1024 - 65535.

Parameter Name	Default Value	Description and Value Range
SIPCONFERENCECONTINUE	0	When the ENABLE_AVAYA_ENVIRONMENT parameter is 0 (non-Avaya environment) and the deskphone 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 deskphone 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 deskphone's listening port for inbound connections (for non-secure message transfer only). Values range from 1024 - 65535.
SIPREGPROXYPOLICY	"alternate"	SIP registration proxy policy that controls how the deskphone treats the list of controllers/servers in the SIP_CONTROLLER_LIST parameter. The valid values are: ● alternate in which the deskphone registers to only the first controller in the list. If the deskphone cannot reach the first controller, the deskphone registers to the second controller, and so on. ● simultaneous which is the preferred registration method with SIP proxy controllers. The deskphone simultaneously registers to more than one SIP proxy controller at the same time.
SKILLSCREENTIME	5	In an CC Elite environment, this parameter specifies the number of seconds the Skills screen is displayed. The range is from 0 to 60.
SLMCAP	0	Specifies whether the SLA Monitor agent will support packet capture. The values are: 0 = No packet capture 1 = Packet capture with RTP content removed 2 = Packet capture with RTP content
SLMCERTS	" " (NULL)	Specifies the path to the trusted certificate repository.

Parameter Name	Default Value	Description and Value Range
SLMCLIENT	0	Specifies whether the SLA Monitor agent will support a CLI connection. The values are: 0 = CLI connection not supported 1 = CLI connection supported
SLMCTRL	0	Specifies whether the SLA Monitor agent will support device control. The values are: 0 = Device control not supported 1 = Device control supported
SLMFSB	0	Specifies whether the SLA Monitor agent will support file system browsing. The values are: 0 = File system browsing supported 1 = File system browsing not supported
SLMPERF	0	Specifies whether the SLA Monitor agent will support access to deskphone performance data. The values are: 0 = Not supported 1 = Supported
SLMPORT	50011	Specifies the port to use to receive packets from an SLA Monitor server. The values are: 0 through 65535.
SLMSRVR	0.0.0.0: 50011	Specifies the IP address and port number of the SLA Monitor server. Values are 0 to 65535. ⚠ **Important:** SLMSRVR must be configured to a non-default value to activate the SLA monitor agent.
SLMSTAT	0	Specifies whether the SLA Monitor Agent is enabled or disabled. Values are: 0 = Disabled 1 = Enabled
SLMTEST	50012	Specifies the port used for SLA Monitor RTP and traceroute tests. Accepted values are - 0 through 65535.

Parameter Name	Default Value	Description and Value Range
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.
SPEAKERSTAT	2	Limits the hands-free audio operation mode. The valid values are: 0= Speakerphone not allowed. If the value of SPEAKERSTAT is **0**, the default **Audio Path** on the deskphone is set to **Headset**. **Note:** You can use the handset to answer a call when **Audio Path** on the deskphone is **Headset**. 1= One-way speakerphone operation allowed (monitor) 2= Two-way speakerphone operation allowed
SSH_ALLOWED	0	Specifies whether and how Secure Shell (SSH) is supported. Values are: 0 = Disabled. 1 = Enabled with challenge/response authentication.
SSH_BANNER_FILE	" " (Null)	The file name or URL of a file that contains warning banner text to be sent to SSH clients before authentication instead of the built-in default English warning banner text.
SSH_IDLE_TIMEOUT	10	Minutes of inactivity after which SSH will be disabled. 0 = No timeout The range of idle time = 1 to 32767.

Parameter Name	Default Value	Description and Value Range
SUBSCRIBELIST	" " (Null)	String representing the Push subscription list. 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 deskphone uses SIP for both the Request URI and the Contact Header regardless of whether SRTP is enabled. If=1, the deskphone 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 PPM does not show a FS-DeviceData FeatureName with a FeatureVersion of 2 in the response to the getHomeCapabilities request (indicative of PPM 4.0), the deskphone uses SIP for both the Request URI and the Contact Header. If=2 and the PPM does show a FS-DeviceData FeatureName with a FeatureVersion of 2 or greater in the response to the getHomeCapabilities request, the deskphone 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=deskphone does not support GigE 1=deskphone supports GigE
SYMMETRIC_RTP	1	Enforces RTP on the same port. Values are 0 -1.
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.

Parameter Name	Default Value	Description and Value Range
TCP_KEEP_ALIVE_TIME	60	This time interval is the time 9600 Series SIP IP Telephones 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).
TEAM_BUTTON_ REDIRECT_INDICATION	0	Specifies whether the deskphone displays the redirection icon for Team Button on a monitoring deskphone in case the monitoring deskphone is not a redirect destination of the monitored deskphone. You can assign any of the following values: ● 0: The redirect indication is shown only on a monitoring deskphone which is the redirection destination. ● 1: The redirection icon is shown on all monitoring deskphones.
TEAM_BUTTON_ REDIRECT_OVERRIDE	0	Specifies whether the monitoring deskphone can override the SAC/CFWD/ECF set by the monitored deskphone.You can assign the following values to parameter: ● 0: Monitoring deskphone cannot override the SAC/CFWD/ECF set by the monitored deskphone. ● 1: Monitoring deskphone can override the SAC/CFWD/ECF set by the monitored deskphone by placing the call to the monitored deskphone. ● 2: The monitoring deskphone displays a message to the user asking if the call should be placed to the monitored deskphone.
TEAM_BUTTON_RING_ TYPE	1	Specifies the default ring tone that the deskphone plays for all team buttons that the user administered on the deskphone. The default ring tone can be overridden by the user. You can assign any value from 1 to 14 to this parameter.

Parameter Name	Default Value	Description and Value Range
TEAM_BUTTON_RING_TYPE_PER_BUTTON	Each name-value pair has the same value as the TEAM_BUTTON_RING_TYPE parameter	Specifies a list of name-value pairs that indicate default ring tones or the ring tones that user selects for each Team button administered on the deskphone.
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.
TPSLIST	" " (Null)	String representing the Trusted push server list. Values are: 0 to 255 ASCII characters: zero or more domain/path strings, separated by commas without any intervening spaces.

Parameter Name	Default Value	Description and Value Range
TRUSTCERTS	" " (Null)	Specifies a list of comma separated file names of certificates that the deskphone downloads. The deskphone uses these certificates to authenticate the identity certificates presented by server that the deskphone connects to. The list can contain from 0 to 1024 characters. You must install the root certificate of any CA that is used. In case, if the server presents an identity certificate that is issued by an intermediate CA, then you must also install any intermediate CA certificates along with the root certificate. The installation of intermediate CA certificates ensures that the deskphone validates the certificate chain right up to the root.
USE_EXCHANGE_ CALENDAR	0	Indicates whether calendar data retrieval from Exchange is selected or not. Values are: 0 (disabled) or 1 (enabled).
USE_EXCHANGE_ CONTACTS	0	Indicates whether Contacts on Microsoft Exchange Server is available to the user. Values are: 0 (disabled) or 1 (enabled)
USE_QUAD_ZEROES_ FOR_HOLD	0	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.
UUIDISPLAYTIME	10	The number of seconds the UUI Information screen is displayed. The range is 5 to 60.
VLANSEP	1	Enables or disables VLAN separation. Controls whether frames received from the line interface are forwarded to the deskphone 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 52.
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_INVITE_ RESPONSE_TIMEOUT	60	Number of seconds the deskphone should wait to get a response after receiving "100 trying" from the server. Values are - 30 through 180.
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).

Parameter Name	Default Value	Description and Value Range
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).
WBCSTAT	1	Specifies whether the deskphone displays a wide band codec icon when the deskphone uses the wide band codec. You can assign any of the following values: ● 0: The deskphone does not display the icon ● 1: The deskphone displays the icon
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.
WMLHELPSTAT	1	Specifies whether a Web Application Help item is displayed on the Home screen if no WML apps are administered and WMLHOME is null. Values are: 0 = Disabled 1 = Enabled
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.

Parameter Name	Default Value	Description and Value Range
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.
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.

VLAN settings

This section contains information on how to administer SIP-based 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 to ensure correct operation.

VLAN tagging

IEEE 802.1Q tagging (VLAN) is a useful method of managing VoIP traffic in your LAN. For better working of your voice network, establish a voice VLAN, assign the VLAN ID of this voice VLAN to the L2QVLAN parameter , and provide voice traffic with priority over other traffic. You can set VLAN tagging manually, through DHCP, or in the 46xxsettings.txt file.If you enable VLAN tagging, that is, set the L2Q parameter to 0 or 1, the deskphone sets:

- VLAN ID to the L2QVLAN parameter
- VLAN priority for audio packets to L2QAUD. The default value is 6.
- VLAN priority for signaling packets to L2QSIG. The default value is 6.

Regardless of the tagging setting, SIP-based 9600 Series IP Deskphones always transmit packets 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 go out of the secondary Ethernet interface because many PCs will ignore tagged frames.
Perform any changes to the VLAN settings only when the deskphone is non-operational.

The VLAN default value and priority tagging

The L2QVLAN parameter specifies the 802.1Q VLAN Identifier and is initially 0. This default value indicates “priority tagging” and specifies that your network Ethernet switch automatically inserts the switch port default VLAN ID without changing the user priority of the frame.

Some switches do not understand a VLAN ID of 0 and require frames tagged with a value other than 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 specifies the number of seconds 9600 Series IP Deskphones wait 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 deskphone moves to a port where the L2QVLAN value is invalid. The default value is long, allowing for a scenario whena major power interruption causes phones to restart. Always allow time for network routersor the DHCP servers to return to service. If the deskphone restarts for any reason and the VLANTEST time limit expires, the deskphone infersthat the administered VLAN ID is invalid. The deskphone then initiates operation with a VLAN ID.

Setting VLANTEST to 0 indicatesthat the deskphone mustuse a non-zero VLAN indefinitely to attempt DHCP. In other words, the deskphone does not return to the default VLAN.

Important:

If you use DHCP to provision a VLAN ID , then you must also specify L2QVLAN and VLANTEST in all DHCP servers that the deskphone 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 you have enabled VLAN tagging initially, the SIP-based 9600 Series IP Deskphones transmit DHCP messages with IEEE 802.1Q tagging and the VLAN ID set to L2QVLAN. The deskphones 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 a 9600 Series SIP IP deskphone 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 *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*.

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 deskphone. The following system parameters control VLAN separation:

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

VLAN separation rules provide 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.

1 of 2

VLAN separation rules

If		Then
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.
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

The 9600 Series SIP 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 4 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) 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-2004 standard for supplicant operation, and support pass-through of 802.1X messages to an attached PC. 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 feature is inactive in this configuration.
- 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 deskphone 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 Series 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.

When a deskphone is installed for the first time and 802.1x is enabled with EAP-MD5 method, the deskphone prompts the installer to enter the 802.1x supplicant credentials for EAP-MD5 authentication. The default 802.1x supplicant ID is the MAC address of the deskphone.

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 deskphone 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-host mode. These switches typically send multicast 802.1X packets to authenticating devices.

These switches support the following three scenarios:

- Standalone deskphone (Deskphone Only Authenticates) - When the deskphone is configured for Supplicant Mode (DOT1X=2), the deskphone can support authentication from the switch.
- Deskphone with attached PC (Deskphone 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-auth configuration. These switches typically send unicast 802.1X packets to authenticating devices. These switches support the following two scenarios:

- Standalone deskphone (Deskphone 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.

  Note:

  > When you reboot a deskphone to enable 802.1x, enable 802.1x on the switch only when the deskphone completes the rebooting procedure and shows the login prompt or is already logged in.

About Link Layer Discovery Protocol (LLDP)

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

The transmission and reception of LLDP is specified in IEEE 802.1AB-2005. The 9600 Series IP Telephones 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 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.

A 9600 Series IP deskphone initiates 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 (deskphone) 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.

1 of 2

Category	TLV Name (Type)	TLV Info String (Value)
TIA LLDP MED	Inventory – Firmware Revision	BOOTNAME.
TIA LLDP MED	Inventory – Software Revision	APPNAME.
TIA LLDP MED	Inventory – Serial Number	Deskphone 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	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 an LLDPDU message, the Avaya IP Deskphones 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 emergency numbers

Set the PHNEMERGNUM configuration parameter in the settings file or in the Session Manager to assign a default emergency number. The deskphone automatically dials the configured number whenever a user presses the **Emerg** softkey on the Login screen, or the Phone screen, or when the user presses the **Yes** softkey on an Emergency Calling pop-up screen. The deskphone dials the emergency number even if the deskphone is locked or the user is not logged in. You must select the **Allow Unauthenticated Emergency Calls** field in System Manager so that users can dial the emergency number when the deskphone is not registered.

You can set up to 100 emergency numbers for the deskphones to dial. However, you must first configure the additional emergency numbers in System Manager. You can then use the parameter PHNMOREEMERGNUMS to specify these additional emergency numbers in the settings file (46xxsettings.txt) or in the System Manager.

Note:

> 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 deskphone 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 preferred audio path. This means that even if the Speakerphone is disabled, it becomes the default path when the user presses the **Emerg** softkey.

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 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 deskphone number to be dialed automatically when the user presses this button. The command is:

```
SET MSGNUM 1234
```

where ***1234*** is the Voice Mail extension (Communication Manager hunt group or VDN).

However, when the deskphone is in failover mode, the deskphone might need to dial a different number to reach the voice mail system. Administer the parameter PSTN_VM_NUM to access the voice mail system through the Message button, while the deskphone is in failover mode. For example, during failover, the deskphone dials the public access number 345-555-1234 to access the voice mail at 1234. In this case, the command would be:

```
SET PSTN_VM_NUM 913455551234
```

Note:

If you set two different values for the same parameter through PPM and the 46xxsettings.txt file, the PPM settings override the settings in the 46xxsettings.txt file.

Administering settings at the deskphone

The document *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP* explains in details how to use the local administrative procedures on the deskphone for administration. The local procedures that you can administer on 9600 Series IP Deskphones are:

- 802.1X - To set the 802.1X operational mode.
- ADDR - To set the static addresses.
- AGC - To enable or disable Automatic Gain Control.
- CALIBRATION - Applicable to 9621G and 9641G deskphones. To calibrate the touch screen.
- CLEAR - To remove all administered values, user-specified data, option settings, etc. and return a deskphone to its initial “out of the box” default values.
- DEBUG - To enable or disable debug mode for the button module serial port.
- GROUP - To set the group identifier on a per-deskphone basis.
- HANDSET EQ - To set the handset equalization settings of the deskphone.
- INT - To 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 **-** To change the default signaling value from SIP to H.323 or vice versa.
- SIP - To configure SIP call settings.

  ⚠ **WARNING:**

  The SIP call settings entered through the CRAFT menu take precedence over other sources for this data, for example- 46xxsettings.txt, or PPM. The only way to override these settings is to go into the CRAFT menu and remove the settings or perform a “Clear” of the deskphone from the CRAFT menu.
- SNTP - To configure the time server settings.
- SSON - To set the site-specific option number.
- VIEW - To 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. However, the user can change the language of the deskphone and can choose any of the following languages:

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

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 deskphone models 9601, 9608, and 9608G do not support Arabic language. The 9601 deskphone cannot display Korean symbols when the user selects the display language as Chinese, Hebrew, or Japanese. The 9608 and 9608G deskphones cannot display Korean symbols when the user selects the display language as Chinese or Japanese.

For better readability, the deskphones can display the English fonts in a bigger font-size. For information on how to administer this feature, see Setting a larger display font size.

All downloadable language files contain all the information that the deskphone needs 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.

To view multiple language strings, see the MLS local procedure in *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*. 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 Communication Manager settings, values, or text strings.

Administering enhanced local dialing

The 9600 Series SIP 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 number based on administered parameters. The deskphone can automatically prepend the correct digits, saving time and effort of the user. 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 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 Communication Manager call server.
- PHNIC - The digits the Communication Manager 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 Communication Manager call server.
- PHNLDLENGTH - The maximum length, in digits, of the national telephone number for the country in which the Communication Manager call server is located.
- PHNOL - The character(s) dialed to access public network local trunks on the Communication Manager call server.

Note:

In all cases, the values you administer are the values relevant to the location of the Communication Manager call server at which the deskphones are registered. For example, If a deskphone is in Japan, but its Communication Manager 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 Communication Manager 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 , 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 number as a link on the Human Resources page. A 9621G user taps to select that link. The 9621G deduces the number is a part of the corporate network because the extension matches a dial plan element. The deskphone then 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 Communication Manager or Session Manager is not available.
> In a failover situation, the dial plan is played locally even if a proxy connection is not available. The user might 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.

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 deskphone 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 deskphone 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 deskphone'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 for a definition of the DIALPLAN parameter.

Setting the date and time on SIP deskphones

9600 Series IP Deskphones need a source of date and time information. This information 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 for definitions and valid values for SIP Date and Time parameters.

Customizing ring tones

End users can select any ring tone from the14 standard ring tones.8 classic and 6 rich ring tones.The deskphone then saves the ring tone that the user selected in PPM. Ring tones for external, internal, priority, and intercom calls (distinctive ringing) are combinations of specified frequency, duration and cadence values. You can replace the 8 classic ring tones with the Korean ring tones or the customized ring tones

.

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 names of the Korean tones you want available to the user. For example, to replace all the Avaya classic ring tones with the Korean ring tones, , set the EXTEND_RINGTONE parameter to Korean ring tone XML files as follows:

```
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
```

Note:

Do not include space between the XML file names.

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 Ring tone XLS cell descriptions. A sample spreadsheet follows the table for illustration purposes only.

Ring tone 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 deskphone. 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 deskphone. 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	
Note Frequency	The frequency used for a particular note.	
Note Duration	The duration of the note in milliseconds, from 0 to 2^16.	

Cell Name	Description	Comment
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.	

Downloadable ring tones

You can specify list of audio files that deskphones can download as ring tones. The users can select the required ring tone from the downloaded list.

The audio files list can contain 0 to 1023 UTF-8 characters. Provide the list of audio files as name-value pairs separated by commas without any intervening spaces, where:

- name: Is the display name that you assign to the ring tone. Ensure that you:
    - Do not include a comma, an equals sign (=), or a double quote character in the display name.
    - Quote the entire list if you include spaces in any of the display name.
    - Specify the display name that has the length that your deskphone can display. If the length of the display name exceeds the specified limit of your deskphone, the deskphone truncates the name.
    - Do not specify a display name that contains only numbers.
- value: Is the relative or an absolute URL of the audio file. URLs can include an equals sign (=). If you include the equals sign, the system treats the first equals sign as the separator between the display name and the URL. The system treats any subsequent equals signs after the first sign as a part of the URL. Percent encode a comma if you use it in the URL.

Ensure that audio files must:

- Be single-channel WAV files.
- Have encoding as per ITU-T G.711 A-law or u-law PCM with 8-bit samples at 8 kHz or 16-bit samples at 16 kHz.
- Have a maximum size of 512 KB.
- Have the combined size not more than 5 MB.
- Only contain ASCII characters in their file names.

For example,

```
SET RINGTONES "Steam Whistle=tones/swhistle.wav,Car Horn=tones/chorn.wav,Loud Burp=tones/
lburp.wav"
```

Headset profiles

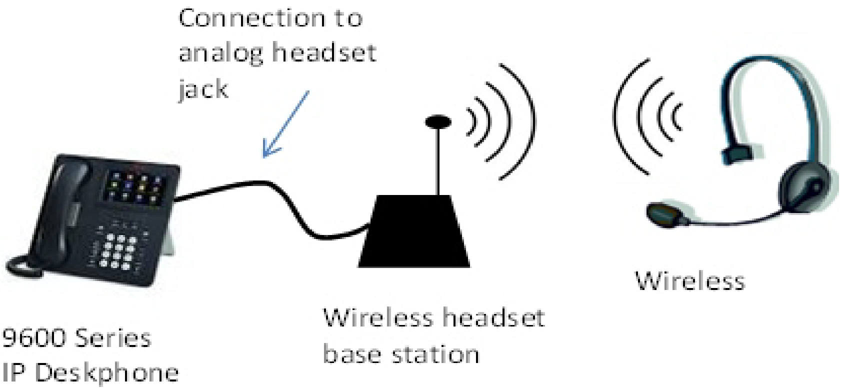
Avaya Deskphone SIP 6.3 introduces headset profiles. To get the best audio quality, a user can select a headset profile that best matches the acoustic performance of the deskphone and the headset.

For more information on headset profiles that Avaya supports, see the document *Avaya one-X® 96X1 Series IP Deskphone Headset Profiles* at the Avaya Support website.

By default, the deskphone displays the name of the headset profiles that Avaya provides. You can use the HEADSET_PROFILE_ NAMES parameter to change the name of the headset profiles.

Wireless Headset Support

The SIP-based 9600 Series IP Deskphones support signaling for wireless headsets that are connected through the analog headset port on the back of the deskphone. With the signaling, users can make, answer, or disconnect calls remotely through controls on the headset. Users call also control the headset through the buttons on their phone.


Connection to analog headset jack
9600 Series IP Deskphone
Wireless headset base station
Wireless

Signaling

When the deskphone receives a call, the headset produces an audible beep and the user can answer the call by pressing a button on the headset.

When a call is established, the user can disconnect the call by pressing a button on the headset.

When a user makes or receives a call using the buttons on the deskphone, the headset automatically connects the speech path without the need for the user to press any buttons on the headset.

Chapter 8: Administering applications and options

Customizing Applications and Options

This chapter covers configuration options for activating or deactivating options and applications. The 9600 Series IP Deskphones offer 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 want to limit the user 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.

SIP deskphones have a 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 or 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, this option allows or prevents the end user from changing or updating the Contact list.
- PROVIDE_EXCHANGE_CONTACTS - If this parameter is disabled, the user can not access the Exchange contacts. If enabled, the user can access the contacts stored in the Exchange server through the Contact list, by pressing the Exchange contact button.
- 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.
- PROVIDE_EXCHANGE_CALENDAR - If this parameter is disabled, the user can not access the Exchange calendar through the deskphone.

Administering the Avaya Menu

The **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:

For the button-based deskphones:

- Options & Settings
- My Presence
- Browser
- Network Information
- About Avaya one-X
- Log Out

However, the touch-based deskphones have a slightly different menu. The touch-based deskphones display the Avaya menu in the following order:

- Options & Settings
- My Presence
- Network Information
- Light Off
- Touch Screen Cleaning
- About Avaya one-X
- Log Out

To access the Avaya menu on the touch-based deskphones, go to HOME>Settings. The touch-based deskphones display the Browser icon under HOME menu.

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.

Setting a larger display font size

Note:

The large text size is not supported on the 9601 deskphone.

When you set the LANGLARGEFONT parameter in the 46xxsettings file, an end user can configure the deskphone to display English language texts in a larger font.

The users of 9600 Series IP Deskphones can activate this feature from - **Options & Settings > Screen & Sounds > Text Size**.

The Large text size setting applies to the deskphone display as well as any attached button modules.

To set the large font, modify the 46xxsettings file as follows:

SET LANGLARGEFONT "Mlf_Englarge.xml"

Ensure that the file (Mlf_Englarge.xml) resides in the web root of the http server.

Setting the background logo

After the deskphone boots up, it displays an Avaya logo by default. The user can change the default logo to any logo from a list of specified logos, from **Options & Settings>Screen & Sound Options>Background Logo**.

To enable the user to change the logo on the deskphone, you must first specify a logo in the 46xxsettings.txt file. For more information, see the parameters CURRENT_LOGO on page 10 and LOGOS on page 26.

Refer the following table for information on the maximum size, color depth and format of a logo supported by the deskphone models 9611G, 9621G and 9641G.

Note:

Deskphone model 9601, 9608, and 9608G do not support a logo.

Models	9611G	9621G	9641G
Max. size (pixels)	217 x 130	232 x 140	232 x 140
Color depth (bit)	16	16	16
Format	JPG	JPG	JPG

History

The History screen displays:

- The calls that the user makes from and receives on the deskphone
- The instant messages that the user sends from and receives on the deskphone

The user can select to see one of the following or all at the same time:

- Answered Calls
- Missed Calls
- Outgoing Calls
- Instant Messages

The user can get information on the Caller ID, the Caller number, the time and date of the call and the call duration.

Call treatment in a logged out state and busy Call Appearances

If a deskphone gets a call when all Call Appearances are busy, the deskphone does not display this call, but the deskphone records this call as a missed call and displays it on the History screen.

If a deskphone gets a call when the user is not logged in, the system saves this call in a database. When the user logs in again, the deskphone displays the previous call log and the calls received in the logged out state. You need to configure this feature through System Manager. The feature has the following limitations.

- This feature is available only when the deskphone is connected to the primary Session Manager.
- When a user logs in multiple devices through the Mulitple Device Access (MDA) configuration, the History screens might not be synchronized between devices. If the user deletes Call Logs from the History screen in one MDA device, the other MDA devices might not clear the Call Logs from the History Screen.
- If the user disables the Call Log feature locally on the deskphone, call logs are stored on the server. When the user enables the Call Log feature, all call logs might show up.
- The deskphone does not display the Group Page calls with the name of the initiator of the Group Page, but with the name Group Page.
- Calls that come to deskphone that were redirected might not show the complete set of History details.

Administering History in the settings file

- ENABLE_CALL_LOG – Specifies enabling or disabling of call logging. 1 indicates enabling and 0 indicates disabling of call logging.
- CLDISPCONTENT – Specifies whether the deskphone displays the called and calling number or suppresses this information on the History screen. 0 indicates displaying and 1 indicates suppressing of the called and the calling numbers.

Presence

Presence is a feature that indicates the availability status of a contact. The deskphone periodically publishes its own presence status and retrieves the presence status of a contact from Avaya Aura® Presence Services.

Presence services facilitates aggregation of presence information collected from the following resources:

- Avaya Aura® Application Enablement Services
- Microsoft Office™ Communicator Server
- eXtensible Messaging and Presence Protocol Server

Presence services categorizes users into two types:

- **Watcher**: A user who is viewing the presence status.
- **Presentity**: A contact whose presence status is being viewed. Presentity is also referred to as Buddy.

A user can simultaneously be a watcher and presentity.

Users can manually set their own presence through the deskphone menu.

SIP-based 9600 Series IP Deskphones support the following presence statuses:

Presence status	Colored icon	Monochrome icon
Available	✅	✔
On a Call	☎	☎
Busy	❗	❗
Away	🕒	🕒

Presence status	Colored icon	Monochrome icon
Do not Disturb	⛔	⊖
Out of Office	◉	◉
Offline	◉	◉
Unknown	?	?

The icon for own presence status is displayed on the top line of the deskphone. The icon for the presence status of a contact is displayed in contacts.

Presence Profile

Presence profile is a part of the communication profile of a user. Presence profile is configured in User Profile Management of Avaya Aura® System Manager.

In cluster deployment of multiple presence servers, presence profile explicitly associates a user with a presence server instance.

The `46xxsettings` file supports the use of only one presence server address. Using presence profile is an efficient method to ensure that a user is connected to the appropriate presence server.

For information about configuring a presence profile, see *Administering Avaya Aura® Presence Services*.

Administering Presence in the settings file

Deskphone presence is disabled by default. To turn presence on, configure the following parameters in the `46xxsettings` file:

- ENABLE_PRESENCE - The value 1 enables presence tracking of users in the Contacts list.
- PRESENCE_SERVER - Specifies the IP address of the presence server. The value of PRESENCE_SERVER is obtained from the PPM when the presence profile is downloaded. The PRESENCE_SERVER address obtained from the presence profile takes precedence over the value set in the `46xxsettings` file. If you do not set this parameter, the deskphone automatically determines the presence server address, but the Instant Messaging feature will not work.
- PRESENCE_ACL_CONFIRM - Specifies whether the deskphone automatically confirms a request from a watcher to monitor the user presence.
- ALLOW_DND_SAC_LINK_CHANGE- Specifies whether the user can control the link between Send All Calls (SAC) and Do not Disturb (DND) behaviors. If the features are linked, the

deskphone activates SAC when user activates DND. A value of 1 indicates that the user gets the control to link the SAC and DND behaviors. Accordingly, the deskphone displays the appropriate menu to set the link. A value of 0 indicates that the user does not get the control to link the SAC and DND behaviors.

- DND_SAC_LINK - The value of this parameter is used only if the ALLOW_DND_SAC_LINK_CHANGE is set to 0. Specifies whether the behavior of SAC and DND features are linked. If the features are linked, the deskphone activates SAC when user activates DND. The value 0 indicates that the SAC and DND behaviors are not linked and the value 1 indicates that the behaviors are linked.
- DND_SAC_LINK_MANUAL - The value of this parameter is used only if the ALLOW_DND_SAC_LINK_CHANGE is set to 1. Specifies whether the user linked the SAC and DND behaviors. If the features are linked, the deskphone activates SAC when user activates DND. The value 0 indicates that the user did not link SAC and DND behaviors and the value 1 indicates that the user linked the behaviors.

Invoking SAC through the DND status

A deskphone can invoke the Send All Calls (SAC) feature when the user sets the Do Not Disturb (DND) status. The linking of SAC and DND behaviors can be automatic or can be under user control. For more information about linking the behaviors, see Administering Presence in the settings file on page 6.

Access Control List

The Access Control List specifies whether other users on the network can monitor the presence of a specific user. By default users can automatically see the presence of other users. You can disable the automatic viewing by setting the PRESENCE_ACL_CONFIRM parameter. If you disable the automatic viewing, user cannot enable it from the deskphone. However, deskphones that are in 1XC Shared Control Mode with a 1XC soft client can control the automatic viewing. When a request comes to the 1XC softclient to watch a user presence, the system displays a pop-up window on 1XC of the user that prompts whether to allow or disallow the presence watching. For more information about setting the parameter, see Administering Presence in the settings file on page 6.

Instant Messaging

Note:

The Instant Messaging feature is not supported on the 9601, 9608, 9608G, and 9611G deskphones.

The Instant Messaging (IM) feature allows a user to communicate through text messages. When user A initiates an IM to user B, user B receives a notification on the Topline of the screen. Then user A and B are able to have an IM conversation. The deskphone stores the IM conversations in the History log. Each deskphone can store IMs up to size 2 MB. If a user logs out of a deskphone and logs back into a different deskphone, the user is not able to see the IM history.

If you configure IM, you must also configure the deskphones with the root CA certificate that issued an identity certificate to the presence server during the server installation. If you used System Manager to issue the identity certificate to the presence server, you can obtain the root CA certificate through System Manager through the following steps:

1. Click **Services** -> **Security** -> **Certificates** -> **Authority**.
2. Click **Download pem file**.
3. Save the pem file on the HTTP server at the same location as 46xxsettings.txt.
4. Set the SET TRUSTCERTS parameter in the 46xxsettings.txt settings to the certificate list as follows. The list must not contain spaces.

   SET TRUSTCERTS av_sipca_pem_2027.txt,smgr_ca.txt

   where smgr_ca.txt is the CA certificate filename.

IM and Presence are not supported if two deskphones are configured with the same extension through Multi Device Access (MDA).

Note:

IM works only if Presence is working. IM requires the SIP signaling be set to TLS.

Integrating Microsoft™ Exchange

9600 Series IP Deskphones can integrate with Microsoft Exchange. With this integration, users can:

- View Calendar reminders that users can dismiss, snoozed, or use the reminders to make a call.
- Dial into conference calls without entering long complex conference call number and passcode.
- View their contacts that are populated in their private exchange contacts

The link between the 9600 Series IP Deskphones and the Exchange server can be secured

9600 Series IP Deskphones models 9601, 9608, 9608G, 9611G, 9621G, and 9641G support Microsoft Exchange calendar integration and Microsoft Exchange contact integration. Using the integration feature deskphones can download the following information from the Exchange server and display this information to the users:

- Contact information
- Appointment
- Calendar data containing meeting schedules.

To gain access to the Exchange contacts, calendar, and reminder information, users must use Avaya Menu to specify their:

- Credentials, that is, the Exchange user account name and the password.
- Calendar reminder and display preferences.

The deskphone automatically adds the Exchange contacts of a user to the contact list under the **Exchange Contacts** screen. Users can save the Exchange contacts to PPM using the **+Local** key.

Note:

Users can modify or delete contacts that are saved in PPM.
Avaya Deskphone SIP does not support the presence tracking feature for the Exchange contacts.
Avaya Deskphone SIP release 6.3 onwards supports integration with Microsoft Exchange Server 2010 and maintains a backward capability with Microsoft Exchange Server 2007.

Configure the following parameters in the settings file so that users can gain access to the Exchange contacts, calendar, and reminder information on their deskphones:

- PROVIDE_EXCHANGE_CALENDAR: A flag to define whether or not menu items 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.
- PROVIDE_EXCHANGE_CONTACTS: A flag to define whether or not menu items for MS Exchange Contacts integration are provided to the end user. If disabled, the menu item in Option & Setting sub-menu to select access to MS Exchange Contacts is hidden. If PROVIDE_EXCHANGE_CALENDAR is also disabled the complete sub-branch for MS Exchange integration is hidden.
- 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 deskphone and is used by the deskphone to access Microsoft Exchange. All servers are tried until the deskphone 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, for example "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 deskphone 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 deskphone. 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 deskphone. Must be saved persistently in device data.
- EXCHANGE_SNOOZE_TIME: Set via the settings file or by the end user at the deskphone. Must be saved persistently in device data.
- EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD: Used to administer how long in seconds the deskphone re-syncs with Exchange Server.
- EXCHANGE_EMAIL_DOMAIN: Specifies the Exchange email domain. The parameter is applicable only if you are connecting to Exchange server 2010.
- EXCHANGE_SERVER_SECURE_MODE: Specifies whether the deskphone communicates with the Exchange server over https or http. The parameter is applicable only if you are connecting to Exchange server 2010.
- EXCHANGE_SERVER_MODE: Specifies the protocol that the deskphone uses to communicate with the Exchange server 2010, 2007, or earlier.

The connection between 9600 Series IP Deskphones and the Microsoft Exchange server can be either a secure connection (TLS) or a non-secure connection. You must use a secure connection. To configure a secure connection, you must download the public root certificate of Microsoft Exchange server.

Note:

Microsoft, by default, only allows a secure connection although it can be made unsecure through configuration on the Exchange server.

The following parameters are relevant to setting up a secure connection:

- TRUSTCERTS - When you use a TLS/SSL connection between the Microsoft Exchange server and 9600 Series IP Deskphones, the deskphone must validate the public root certificate of the Microsoft Exchange server. Use the TRUSTCERTS parameter in the 46xxsettings file to specify the Exchange server public root certificate. For example, SET TRUSTCERTS "ExchangeServer.pem". In case, if the Exchange server presents an identity certificate that is issued by an intermediate CA, then you must also install any intermediate CA certificates along with the root certificate so that the deskphone validates the certificate chain right up to the root.
- TLSSRVID - If this parameter is set to 1, then TLS/SSL connection is established only if the server identity matches the server certificate. You can disable this parameter if the server has multiple FQDN or different FQDN internally and externally such that the single certificate does not have the correct name in all instances.

Administering the WML browser

SIP software release 6.5 provides a WML browser. If administered, the 9601, 9608, 9608G, and 9611G deskphones display the Browser option on the **Avaya (A) Menu**, and 9621G and 9641G deskphones display the Browser option under **Home** screen.

Note:

The WML browser on a 9601 deskphone does not support image rendering.

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:

Parameter	Description
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.

WML browser properties

The following table shows a comparison of different properties of the WML browser across the deskphone models 9601, 9608, 9608G, 9611G, 9621G, and 9641G:

Feature	9601	9608/ 9608G	9611G	9621G	9641G
Top Line	Yes	Yes	Yes	Yes	Yes

Feature	9601	9608/ 9608G	9611G	9621G	9641G
Application Lines	2	4	4	4	5
Line buttons	Yes	Yes	Yes	No	No
Selectable objects per line	1	1	1	1	1
Application line height (pixels)	14	15	31	38	38
Softkeys per screen	3	4	4	5	5
Softkey height (pixels)	14	14	31	38	38
Navigation buttons	Yes	Yes	Yes	No	No
Text input	Yes	Yes	Yes	Yes	Yes
Color support	No	No	Yes	Yes	Yes
Supported image format	No	JPEG	JPEG	JPEG	JPEG
Max image width (pixels)	NA	175	300	430	430
Max image height (pixels)	NA	1440	2976	3648	3168
Click to dial	Yes	Yes	Yes	Yes	Yes
Add to phonebook	Yes	Yes	Yes	Yes	Yes
Characters per line (normal font)	26	31	40	39	39
Characters per line (large font)	NA	25	22	26	26
Characters per softkey (normal font)	8	8	8	8	8

Feature	9601	9608/ 9608G	9611G	9621G	9641G
Characters per softkey (large font)	NA	6	6	8	8

Avaya Aura® Call Center Elite features

The SIP software release 6.5 supports Avaya Aura® Call Center Elite features on 9600 Series IP deskphones models 9608, 9608G, 9611G, 9621G, and 9641G. Avaya Aura® Call Center Elite 6.2 is the minimum requirement to support the Call Center Elite features:

Note:

The Avaya Aura® Call Center Elite features are not supported on the 9601 deskphone.

The supported Call Center Elite features are:

- Agent login/logout
- After call work
- Auxiliary work
- Auto and Manual in
- CC-Info agent event package
- Third party MWI
- Stroke counts
- Call work codes
- Display active VDN name
- VuStats
- Accept and display ASAI UUI information
- Forced logout override
- Supervisor assist
- QStats
- Interruptible AUX work

For detailed information on all the Call Center features, see the Call Center agent for SIP user guide, available on the Avaya support Website www.avaya.com/support.

You can assign the Call Center button features via PPM. The system displays these buttons in the Feature screen, button module, Quick Touch Panel, Phone screen, and the Home screen.

The Call Center features can be administered through the settings file using the following parameters:

- SKILLSCREENTIME - The duration that the deskphone displays the Skills screen.
- ENTRYNAME - This parameters sets the entry name as the calling party name or the VDN/Skills name.
- UUIDISPLAYTIME - Specifies the duration that the deskphone displays the (user to user information (UUI) screen.
- CC_INFO_TIMER - Sets the CC-Info event package timer.
- BUTTON_MAPPINGS - Provides mechanism to disable the Forward, Speaker, Hookswitch/ Switchhook, and Handset buttons to re-map the Speaker button as Release button.

Team Button

The Team Button feature provides the facility to a user to watch or monitor the deskphone of another user. The user can use the Team Button feature to manage call handling of the deskphone that the user monitors. For example, in an office environment where a secretary needs to monitor the deskphone of a boss to answer calls that are ringing on that deskphone of the boss or selectively answer any one of them.

The deskphone of the user who monitors is called the monitoring deskphone and the deskphone that the user monitors is called the monitored deskphone.

Initially, the Team Button feature is configured on the Avaya Aura® Communication Manager and Avaya Aura® Session Manager and in doing so a station is configured to monitor another station. A user can monitor another deskphone to:

- See if the monitored deskphone redirects calls to any other deskphone
- See if the monitored deskphone has an active call
- See if the monitored deskphone has an incoming ringing call
- Answer any of the calls that are ringing on the monitored deskphone
- Make a speed dial call to the monitored deskphone by pressing the Team Button softkey when the monitored deskphone does not have an active call
- Transfer an active call to the monitored deskphone by pressing the Team Button softkey

Team Button override

The monitored deskphone might have call redirection feature active through any of the following features:

- Send All Calls (SAC)
- Call Forward (CFWD)
- ECF (Enhanced Call Forward)

You can configure Avaya Aura® Communication Manager and Avaya Aura® Session Manager such that the monitoring deskphone overrides the call redirection active on the monitored deskphone.

If the call redirection override is set, the monitored station rings for 30 seconds. If no one answers the call, the call is automatically sent to the redirection number.

Direct Transfer

The Direct Transfer feature provides the facility to quickly transfer an active call to the monitored station.

When a call is answered at a monitoring deskphone, the user can begin the transfer process of transferring the call to the monitored station by pressing the Team Button. The monitoring deskphone puts the existing call on hold and places a call to the monitored station. A speech path is established and the monitoring station and monitored station can converse. To complete the transfer between the original call and the monitored deskphone, the monitoring station can disconnect the call by going on-hook or by pressing the Complete softkey.

Direct Transfer is applicable only to the Team Button feature and no configuration is required on Avaya Aura® Session Manager.

Team Button ring

You can customize the ring type for Team Buttons on a monitoring deskphone. Use the TEAM_BUTTON_RING_TYPE parameter to configure the default ring type. The user can override these settings such that a specific Team Button has a specific ring tone.

Administering Team Button in the settings file

The following parameters are used to administer the Team Button feature. Most of these are set in the settings file:

- TEAM_BUTTON_REDIRECT_INDICATION - Specifies whether the deskphone displays the redirection icon for Team Button on a monitoring deskphone in case the monitoring deskphone is not a redirect destination of the monitored deskphone. 0 indicates that the redirect indication is shown only on a monitoring deskphone which is the redirection destination. 1 indicates that the redirection icon is shown on all monitoring deskphones.
- TEAM_BUTTON_REDIRECT_OVERRIDE- Specifies whether the monitoring deskphone can override the SAC/CFWD/ECF set by the monitored deskphone. 0 indicates that a monitoring deskphone cannot override the SAC/CFWD/ECF set by the monitored deskphone. 1 indicates that the monitoring deskphone can override the SAC/CFWD/ECF set by the monitored deskphone by placing the call to the monitored deskphone. 2 specifies that the monitoring deskphone displays a message to the user asking if the call should be placed to the monitored deskphone. The parameter is set through the deskphone and saved in Personal Profile Manager (PPM).
- TEAM_BUTTON_RING_TYPE - Specifies the default ring tone that the deskphone plays for all team buttons that the user administered on the deskphone. The default ring tone can be overridden by the user. You can assign any value from 1 to 14 to this parameter.
- TEAM_BUTTON_RING_TYPE_PER_BUTTON - Specifies a list of name-value pairs that indicate default ring tones or the ring tones that user selects for each Team Button administered on the deskphone.

Enhanced Call Forward

Note:

The Enhanced Call Forward feature is not supported on the 9601 deskphone.

The Enhanced Call Forward (ECF) feature provides flexibility in forwarding incoming calls to different destinations, based on different conditions. These conditions are:

- Caller type: Whether the call is coming from internal number or an external number
- Phone status: A user can choose to forward:
  - All incoming calls
  - When the deskphone is busy, or
  - When there is no answer.

An ECF feature button can be set up for the deskphone to display on the Feature Screen, Quick Touch Panel, SBM24, BM12, Favorite Feature on the Phone Screen, or the Home Screen. ECF can be accessed and enabled or disabled using the feature button.

For more information on ECF, see the user guides for Avaya one-X® Deskphone SIP release 6.5, available on the Avaya support website: www.avaya.com/support.

Advanced call conference

In collaboration with the Avaya Aura® Conferencing server and Communication Manager, SIP release 6.5 provides advanced call conference features to the end user. Avaya Aura® Conferencing 7.0 is the minimum requirement to support advanced conferencing.

See the following table for a comparison of the advanced call conference features with different conference servers:

Feature	AST	AAC7
Participant list	No	Yes
Participant drop	Last party drop	Selective drop
Add participant	Single dial	Dial group
Voicemail	No filter	Voicemail
Number of participants	6	Unlimited
What is displayed	Number of participants, on the call appearance line, or on the Top Line.	The Details screen displays up to 25 participant names and their presence status. The Phone screen or the Top Line displays the total number of participants.
Selective mute	No	Yes.

Note:

The 9601 deskphone does not support the conference details screen.

To enable advanced call conference features, you must first set the following parameters through the settings file:

CONFERENCE_FACTORY_URI

CONFERENCE_SERVER_ADDRESS

CONFERENCE_SERVER_PORT

ENABLE_SECURE_HTTP_FOR_CONFERENCING_SERVICE

Note:

SIP 6.5 does not support non-AST servers as primary controller for conferencing.

For more information on the parameters, see Customizable system parameters for SIP-based 9600 Series IP Deskphones on page 2.

Multiple Device Access

Avaya Deskphone SIP 6.3 onwards supports Multiple Device Access (MDA) with which you can register up to 10 SIP devices with your extension.

With MDA you can:

- Make and receive calls to any of the registered devices.
- Switch to another registered device during an active call.
- Bridge on to calls at multiple registered devices. Alert all other registered devices for an incoming call to your extension. When you answer a call on any registered device, the alert on all other devices stops. The other devices show indication of an active call on the same call appearance number.
- Be on multiple calls at one time on different devices, but only one call per device. For example, you can listen to a conference call on one device and answer an incoming call on a second device without putting the conference call on hold. The two calls appear on separate call appearances on all registered devices.
- Use conference and transfer features. Bridging on to a call at other registered devices and invoking a transfer drops the call from all devices after the transfer completes.

Chapter 9: 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 (UDP is not recommended for signaling) and RTP or SRTP for media
- Expanded survivability to Avaya Aura® Session Manager

  Note:

  > If you are using the third-party gateways, you must set the CONNECTION_REUSE parameter to 0 in the settings file.

The deskphone registers simultaneously to Session Manager and a survivable remote server to facilitate faster failover or failback transitions than that of the failover solutions offered in previous SIP software releases and provides minimal 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 or calls are supported. During failover, changes to applications other than Contacts are cached and are updated by the PPM with which the deskphone successfully registers.

If the SIP connection recovery is in progress due to a brief network outage, the deskphone attempts to recover its XMPP connection to Presence Server automatically by re-logging in to Presence Server. If Presence Server is unreachable, Presence will not be available. If the connection recovery fails, the deskphone displays an error message.

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 Session Manager, 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 Session Manager or BSM for simultaneous registration has the following effects on call states and transitions:

- Transition from one Session Manager to another Session Manager or BSM is comprised of:
  - Limbo - The deskphone 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 deskphone 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 deskphone has detected a lost connection to the primary controller and exhibits media preservation behavior.

- 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 Session Manager occurs according to the failback behavior described in 3. Select the active controller on page 5.

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 as 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 Session Manager.
5. Power up other phones.

Configuring survivability

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

- CONTROLLER_SEARCH_INTERVAL - The time the deskphone waits to complete the maintenance check for Monitored Controllers.
- DISCOVER_AVAYA_ENVIRONMENT - Determines whether the deskphone 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 deskphone is communicating with a non-AST controller.
- FAILBACK_POLICY - The failback policy in effect for recovery from failover. The value can be admin or auto. When the phone fails over from a core Session Manager to a Branch Session Manager, it temporarily changes the value of the FAILBACK_POLICY parameter to admin. When

the deskphone fails back to the core Session Manager, it reverts to the FAILBACK_POLICY value that was set when the active controller was a core Session Manager

- FAST_RESPONSE_TIMEOUT - Fast Response Timer.
- PSTN_VM_NUM - The number called when the deskphone is in failover and the Message button is pressed.
- RECOVERY_REGISTER_WAIT - 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 and Branch Session Managers with which the deskphone will simultaneously register. Do not add Branch Session Managers to this list. The value of this parameter must not be less than the number of core Session Managers in the SIP_CONTROLLER_LIST.
- SIPREGPROXYPOLICY - Registration Policy.

Setting a controller through the user interface

The survivability parameters can be provisioned in the SIP Phone Settings screens. However, any modification that you do through the user interface, can be modified or cleared only through the user interface.

When setting survivability parameters, consider these points:

- 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.
- An entry can be deleted by navigating to the entry and pressing the **Delete** softkey only if the entry was created from this screen. You cannot delete an entry that was not created from this screen.
- 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.

- To clear the values that the deskphone downloads from PPM and displays on the SIP proxy screen, you must clear the values on the deskphone, from Craft.
- 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 *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*. 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 Controllers list using the SIPREGPOLICY parameter setting as a guide. The list of SIP Proxies or Registrars can be obtained from the network DHCP servers, the 46xxsettings file, a PPM, or configured via the deskphone user interface. Similarly, the administrative or the automatic failback parameters and the monitoring intervals can be obtained via the 46xxsettings file, the PPM, or the deskphone user interface.

The priority order (highest to lowest) of the data sources used to construct the controller list is as follows:

1. Deskphone user interface (set using SIP Craft procedure)
2. System Manager
3. Settings file (46xxsettings.txt)
4. DHCP (Option 242)
5. LLDP

The controllers received from these data sources are combined into an aggregated list. The priority of controllers within the aggregated list is based first on the priority of the data source and secondly on the priority of the controller within the list received from that data source. The aggregated list has all duplicates removed. In the case where a controller is included multiple times with different transport types, only one entry for the controller is added using the transport type from the highest priority data source.

The only exception to the above rule is if the deskphone receives a 301 response to a REGISTER request which contains a list of controllers. In this case, the deskphone discards the aggregated controller list and use ONLY the controllers received in the 301 response.

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 deskphone performs a maintenance activity for each Monitored Controller. The deskphone 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. If all the Monitored Controllers are available before the end of the CONTROLLER_SEARCH_INTERVAL, the deskphone continues with selecting the Active Controller. If at least one Monitored Controller is available at the end of the CONTROLLER_SEARCH_INTERVAL, the deskphone 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 deskphone retries the monitoring attempt using the RECOVERYREGISTERWAIT parameter value as a guideline.

The list of controllers that appears in the CRAFT menu is the full list of controllers in effect at the time it is displayed. The list is received in a 301 Moved message in response to a register or an aggregate of the controllers received from the following four sources:

- Deskphone user interface (set using SIP Craft procedure)
- System Manager
- Settings file (46xxsettings.txt)
- DHCP (Option 242)

3. Select the active controller

If the value of the SIPREGPROXYPOLICY parameter is "alternate" and a user is logged in, the deskphone must attempt and maintain a single active SIP registration with the highest priority available controller; the number of available controllers that the deskphone simultaneously registers with is the value of the SIMULTANEOUS_REGISTRATIONS parameter. Any additional controllers are treated as alternate registrations. The deskphone 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 deskphone sets the SIPPROXYSRVR_IN_USE parameter to the IP address of this (Active) controller. The deskphone also performs the other registration tasks.

If the value of the SIPREGPROXYPOLICY parameter is "simultaneous" and a user is logged-in, the deskphone attempts and maintains active SIP registrations with all available controllers.

If the value of the FAILBACK_POLICY parameter is "automatic", the deskphone'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 deskphone 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 deskphone 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

The deskphone behavior for simultaneous registration during failover 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 the deskphone gets a successful response to the REGISTER, the deskphone marks the controller as "available." If the deskphone cannot establish the connection or if the deskphone does not receive a successful response, the deskphone marks the controller as "unavailable".
2. Controller Subscription Refresh - The deskphone sends a refresh SUBSCRIBE to the current controller for all the subscriptions that the deskphone has. If the deskphone gets any failure response for any of the refresh SUBSCRIBE messages, the deskphone removes that particular 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 deskphone determines if that controller supports the AST (Advanced SIP Telephony) feature set or not. The deskphone sends a SUBSCRIBE request to the active controller for the "Feature Status Event Package" (avaya-cm-feature-status). If the request succeeds, the deskphone proceeds with PPM Synchronization. If the request is either rejected, is proxied back to the deskphone, 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 not. If the NOTIFY indicates an "active" state, the deskphone considers itself in an AST environment and proceeds with PPM Synchronization. If the NOTIFY indicates a unreachable state, the deskphone 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 deskphone considers itself in a non-AST environment.

5. Session Manager synchronization

As part of Session Manager synchronization the deskphone performs a getAllEndpointConfiguration request. This request contains the following EndpointConfigurationFields:

- VolumeSettings
- LinePreferenceInfo
- ListOfOneTouchDialData
- ListOfButtonAssignments
- SoftMenuKeyList
- DialPlanData
- ListOfSpeedDialData
- ListOfMaintenanceData
- ListOfTimers

- VMONInfo
- ListOfRingerOnOffData
- ListOfNumberFormatRules
- ListOfIdentities
- MWExt
- VMNumber

If the getAllEndpointConfiguration request fails, the deskphone does not continue with the other Session Manager requests. In this case, the getContactList request doesn't 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 dependent 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 Session Manager environment with SIP software Release 2.6, both failover/failback transition time and behavior is minimized.

Deskphone behavior during failover

During failover, 9600 Series SIP 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 deskphone is registered on secondary controller and regardless if the deskphone is active on a call, the deskphone is in a pushable state, just as if were connected to primary server. The deskphone 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 deskphone 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 corresponding 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 Session Manager. 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, the deskphone displays an "Acquiring Services" screen. The deskphone might also display a Call Preservation message window. Most other screens and applications except for Craft screens are unavailable until the deskphone finds an active controller. However, the user can navigate to the Contacts, Call Forward feature, Avaya (A) Menu or Call Log applications (if administered). The user can go to the Home screen by pressing the Phone button.
- If a call is active when failover occurs, that call will remain active. The user cannot initiate new calls while the deskphone transitions to the alternate server.
- During 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 get diverted 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 deskphone fails back to its original server.
- If the deskphone operates under the latest software, Contacts can be accessed and changed during and after failover to the alternate server.
- If the deskphone operates under the latest software, the end user can access Home Screen Web links/pages during failover, however, any “click to dial” links will not work until the deskphone 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 deskphone is logged out during failover, the local deskphone cache is cleared and the deskphone may become inoperable until it can be reset on the original controller after failback.
- The deskphone accepts calls from any of the proxies it is registered with when the deskphone is simultaneously registered to multiple controllers. There is no visual indication to the user, which indicates that the calls are originating from different feature servers. In the case of Multiple Feature Servers, one feature server can know about one call on the deskphone 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 deskphone 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 deskphone and another controller can know about another call offered to the deskphone. If both controllers are connected to the same feature server. For example, Communication Manager. Communication Manager "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 deskphone. In this scenario features that can be applied to the first call would be limited because all the call data is stored in Communication Manager; Session Manager does not store any information related to any call.
- Preserved Media Connections - Applies only to Session Manager configurations when moving a subscription from one Session Manager to another. In a scenario where the primary Session Manager fails, any active shuffled or direct media call will be preserved if a new call is received while a preserved call is active. The deskphone 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 deskphone 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." The deskphone can

receive incoming calls at this point but is not available to make outgoing calls or to invoke AST features. The deskphone supports media preservation sufficient for alternate registration; if a deskphone experiences a mid-dialog failure (for example, a timed out or failed SIP request, or a socket-level failure), the deskphone 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

The deskphone must be able to identify the active controller from the configured controllers. 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 deskphone 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 Session Manager failed, the deskphone detects F/O and blocks new invites while the deskphone is in transition.
- Stable in F/O where the non-primary proxy is the active controller.
- Fail Back (F/B) transition to normal - The deskphone detects that the primary server is up, regardless if the secondary is up. New invites are blocked while the deskphone is in transition. The deskphone is in a stable Normal mode with Session Manager 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 deskphone is registered back to the primary controller.

User experience during failover transition

SIP software release 6.0 expanded deskphone reliability during the transition from one controller to another.

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

Transition is comprised of the following conditions:

- Limbo - The deskphone 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 deskphone has detected a lost connection to the primary controller and displays an Acquiring Services Screen if the deskphone is idle.
- Call Preservation - During an active call, the deskphone has detected a lost connection to the primary controller and displays a Call Preservation screen.

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

Transition is comprised of the following conditions for moving subscriptions:

- Limbo - The deskphone 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 deskphone 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 deskphone 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 Session Manager to another Session Manager 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 deskphone 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 deskphone 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 deskphone 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 deskphone 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 deskphone 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 deskphone successfully registers.

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

For incoming calls during MSI, the deskphone stops alerting and disconnects the call. If the deskphone is alerting when the deskphone's secondary server goes down (no MSI), the deskphone will keep on ringing. An incoming call will be ended when the link between the Session Manager that routed the call and the deskphone has gone down. For example, if the deskphone has a primary Session Manager (Session Manager 1) and a secondary Session Manager (Session Manager 2), and receives a call directly from the secondary Session Manager but Session Manager 2 goes down, the call that was received from Session Manager 2 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 non-AST 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 Session Manager or Communication Manager 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 deskphone 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.
- Under certain conditions after stable failback, the user might experience issues with self presence or contact presence rendering. For more information, see release notes.
- "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 Session Manager/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 deskphone.
- If the deskphone is logged out during failover, the local deskphone cache is cleared.

User experience during failback

Failback (F/B) transition occurs when the deskphone 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 Communication Manager	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 (Communication Manager COR)	Yes (depends on local proxy capabilities and provisioning)

Feature	Normal Operation with Communication Manager	Failover Operation with a Generic SIP Gateway
Outbound call management	Yes (Communication Manager 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

Term	Description
AAC7	Avaya Aura® Conferencing 7.
Active Controller	The SIP Registrar/Proxy server the Deskphone detects as 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.
Buddy	A contact ("Presentity") for which presence information is to be received.
Configured Controller(s)	The list of controllers that the deskphone will attempt to monitor when Failover occurs. The (list of) elements in the SIP_CONTROLLER_LIST parameter, which can also come from Session Manager and the user interface.
Controller	The new name for a SIP proxy, for example, Session Manager, 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.

1 of 4

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 Telephones support.
Monitored Controller(s)	A SIP Registrar/Proxy server that the deskphone knows about and to which the deskphone periodically checks IP and SIP connectivity.
OPS	Outboard Proxy SIP.
PPM	Personal Profile Manager, part of the System Manager platform. PPM is responsible for maintaining and managing end users' personal information in the system.
Presentity	An entity which publishes its own presence state.
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.
PS	Avaya Aura® Presence server. Performs presence management (event composition, aggregation, ACL enforcement) and XMPP IM routing.

2 of 4

Session Manager	Avaya Aura® Session Manager, the SIP proxy for Avaya Aura®, an alternative to SES.
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 Telephones support.
Surviveable Gateway	Audiocodes server used as a gateway to survive failover. A supported local gateway with Proxy or B2BUA capabilities.

3 of 4

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.
Watcher	A user subscribing for presence notification on a particular Presentity.

4 of 4

AVAYA

Appendix B: Countries with specific network progress tones

About network progress tones

The 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

All countries listed in this appendix are applicable to the 96xx phones. Some of the dialtone entries have changed from previous releases 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
Philippines
Poland
Portugal

Pakistan

Peru

Philippines

Poland

Portugal

Q:

Qatar

R:

Romania

Russia

S:

Saudi Arabia
Serbia
Singapore
Slovakia
Slovenia
Spain
South Africa
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