Avaya one-X™ Deskphone SIP for 9600 Series IP Telephones Administrator Guide Release 2.6

16-601944
Issue 6
June 2010

Notice

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

Note

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

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

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

Link disclaimer

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

Warranty

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

License

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License Types:

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

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

Copyright

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

Third-party components

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

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

Preventing toll fraud

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

Avaya fraud intervention

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

Trademarks

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Federal Communications Commission (FCC) Interference Statement

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

on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

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

FCC/Industry Canada Radiation Exposure Statement

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

Warning

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

Contents

Chapter 1: Introduction

About This Guide

This guide is for personnel who administer Avaya Communication Manager, DHCP, HTTP/HTTPS servers for 9600 Series IP Deskphones using Session Initiation Protocol (SIP), a Local Area Network (LAN), SIP Enablement Services (SES) or a Network Time server.

The 9600 Series IP Deskphones use Internet Protocol (IP) technology with Ethernet line interfaces and support both SIP and H.323 protocols. The 9600 Series IP Deskphones provide support for DHCP, HTTP, and HTTPS, which enhance the administration and servicing of the deskphones. These deskphones use DHCP to obtain dynamic IP Addresses, and HTTPS or HTTP to download new versions of software or customized settings for the deskphones.

Note:

This document covers SIP administration for 9600 Series IP Deskphones only. For administration for 9600 Series IP Deskphones using the H.323 protocol, see the *Avaya one-X™ 9600 Series IP Deskphones Administrator Guide* (Document Number 16-300698), available at: www.avaya.com/support.

This document does not cover administration for Avaya Aura™ Session Manager. Find full documentation for Avaya Aura™ Session Manager on the Avaya support Web site, www.avaya.com/support, specifically *Installing and Upgrading Avaya Aura™ Session Manager* (Document Number 03-603473) and *Administering Avaya Aura™ Session Manager* (Document Number 03-603324).

This document does not cover administration for Avaya Aura™ System Manager. This document does not cover administration for Avaya Distributed Office.

Full documentation for the above Avaya products is available on the Avaya support Web site, www.avaya.com/support.

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 9600 Series IP and/or SIP Deskphone system. If the servers are not functioning correctly, the 9600 Series IP Deskphones might not operate correctly.

Major Differences Between 9600 Series H.323 and SIP IP Deskphones

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

General IP Telephony - Two major protocols handle Voice over IP (VoIP) signaling, Session Initiation Protocol (SIP) and H.323. The two protocols provide connection control and call progress signaling, but in very different ways. These protocols can be used simultaneously over the same network, but in general, no endpoint supports both protocols at the same time. Neither protocol is necessarily superior, but each offers some unique advantages. SIP deskphones, for example, do not require centralized call servers, and can route calls when a URL identifies the destination. H.323 deskphones leverage the call server's presence into the potential availability of hundreds of telephone-related features that a standalone SIP deskphone cannot provide.

Signaling - 96xx Series IP Deskphones ship from the factory with H.323 signaling. To use the SIP protocol, applicable H.323 96xx Series IP Deskphones must be appropriately converted and configured. See the *Avaya one-X™ 9600 Series SIP Deskphones Installation and Maintenance Guide* for detailed conversion/configuration information.

Avaya Communication Manager (CM) Release - 9600 Series SIP Deskphones are supported only by Communication Manager Release 4.0 and greater. SIP deskphones use Avaya OPS (Outbound SIP Proxy) features on the "trunk" side of Avaya Communication Manager whereas the H.323 (IP) deskphones are supported on the "line" side of the Communication Manager. When a SIP deskphone is running under Communication Manager Release 5.0 and up, an additional feature, Extend Call, is available. The Intercom feature is available only on CM Release 5.1 and later. When using Avaya Aura Session Manager, Communication Manager Release 5.2.1 is required.

Required Servers - SIP deskphones use two [additional] servers that H.323 deskphones do not:

- SIP Proxy server (controller) - provided by SIP Enablement Services (SES) software or Avaya Aura™ Session Manager (SM),
- Network Time server - which controls time-related parameters,
- Presence server - in an SES environment, allows tracking of contacts designated with a presence handle and sharing presence information with compatible software.

These servers are not necessarily separate hardware units. Additional, optional servers may be used to handle survivability but is dependent upon your specific configuration. Depending on your system configuration, the servers listed above may require specific software versions, as described in Avaya Aura™ Communication Manager Administration.

Backup/Restore - 9600 Series (H.323) IP Deskphones use HTTP to store backup files. 9600 Series IP Deskphones with the SIP protocol use the Personal Profile Manager (PPM) functionality within SIP Enablement Services (SES) or Avaya Aura™ Session Manager for backup and restore functions.

Settings File & System Parameters - Both SIP and H.323 9600 Series IP Deskphones (and 4600 Series IP Telephones) use the same settings file. Some of the same system parameters are used, however, numerous SIP-specific parameters support SIP operation only. In H.323 9600 Series IP Deskphones, the parameters OPSTAT and APPSTAT control all user interface functions, whereas SIP deskphones use a separate parameter (for example ENABLE_CONTACTS, ENABLE_CALL_LOG) for each user interface function.

Language Support - SIP deskphones support many of the same languages and fonts as H.323 deskphones but there are some differences. SIP deskphones do not support the English Large Text Font for any language, while H.323 deskphones do not support text entry in Hebrew or Korean. Further, all SIP language files have **.xml** file extensions whereas H.323 language files have **.txt** file extensions.

SNMP & MIBs - Although both SIP and H.323 deskphones support SNMP v2c and have custom Management Information Bases (MIBs) the MIBs for each protocol are formatted somewhat differently.

RSVP & RTCP Monitor Server - SIP deskphones do not use RSVP (Resource ReSerVation Protocol) software to provide real-time monitoring and historical data of audio quality for VoIP calls. 9600 Series (H.323) IP Deskphones do support an RTCP Monitor Server.

QoS - Unlike H.323 deskphones, SIP deskphones do not use Avaya Communication Manager to set Quality of Service (QoS). The SIP deskphones use the parameters L2QAUD, L2QSIG, DSCPAUD, and DSCPSIG (described in Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters).

NAT - SIP deskphones do not support Network Address Translation (NAT); H.323 deskphones do support NAT.

Presence - SIP deskphones support presence for designated contacts but only in conjunction with SES. In addition to appearing on the Phone screen, presence information is shown on the Call Log and for Favorite Features. H.323 deskphone do not support presence tracking.

Direct Media - Deskphone SIP now handles early media and direct media.

Features & Functions Supported by H.323 and Not Supported by SIP

The following features and functions are supported by H.323 but not by SIP software Release 2.6:

- Voice Dialing
- USB Devices
- Calltype Digit Conversion
- RSVP
- NAT (Network Address Translation)
- Multicast pushes

Change History

Issue 1	This document was issued for the first time in May 2007 to support the first release of 9600 Series SIP IP Telephones.
Issue 2	This version of the document was revised and issued in December, 2007 to support SIP IP Software Release 2.0. This release provided the 9600 SIP IP Telephones with similar functionality to their H323 9600 IP Telephone counterparts, despite their signaling protocol differences. Release 2.0 introduced several new functions, new configuration parameters, and added telephone models 9630G and 9640G.
Issue 3	This version of the document was revised and issued in September, 2008 to support programmable hospitality-related features in SIP software Release 2.2.
Issue 4	This version of this document was revised and issued in December, 2008 to support software Release 2.4 for 9600 Series SIP IP Telephones. Note that there was no SIP Software Release 2.3.
Issue 5	This version of this document was revised and issued in November, 2009 to support software Release 2.5 for 9600 Series SIP IP Telephones. In addition to new enhancements that build on SIP software Release 2.4, this release incorporated the features and functionality of SIP software Release (programmable hospitality features). This release also added several 9600 Series IP Telephones to the SIP protocol - 9620C, 9620L, and 9650/9650C.
Issue 6	This is the current version of this document, issued in June, 2010 to support software Release 2.6 for 9600 Series SIP IP Telephones, hereafter referred to as "9600 Series IP Deskphones" in this document. What's New in this Release describes this release in more detail.

What's New in this Release

New material in this issue to support SIP Release 2.6 software includes:

Administration Enhancements - SIP Software Release 2.6 supports additional feature functionality introduced on Avaya Communication Manager and Avaya Aura™ Session Manager Release 6.0+ and SIP Enablement Services (SES) Release 5.2.x. When used with Avaya servers, customers have access to basic SIP features as well as Advanced SIP Telephony (AST) features. New SIP R2.6 features include:

- Enhanced Session Manager inter-operation:
  - Simultaneous Registration with multiple active proxies provides enhanced reliability. A 9600 Series IP Deskphone can continue functioning as long as one of the configured proxies can be reached.
  - Enhanced media preservation allows the audio on a call to continue even if the signaling path is interrupted and to also switch between calls that were signaled between different proxies.
  - 9600 Series IP Deskphones require less media processing infrastructure, which improves scalability and allows the Deskphones to negotiate codecs and encryption more effectively.
  - Registration redirect allows a Deskphone to reregister with another instance of Avaya Session Manager (SM) if the first registration fails because the user has an account of a different instance. This feature provides both mobility and robustness to administration errors.
- Access to additional Avaya Communication Manager (CM) features:
  - Call pickup alerting provides an audible or visual alert when anyone in a call pickup group receives a call (requires CM 6.0). End users set call pickup alerting and an associated ring tone from the Call Settings option on the Avaya menu.
  - Improved call park behavior provides an unpark feature button only when it is administered and allows a user to unpark a call by pressing the same button used to park the call (requires CM 6.0).
  - With Avaya Aura™ System Manager, the voice mail destination can be specified on a per-station basis, making it easier to support multiple voice mail servers (requires CM 6.0).
  - Updated handling for LLDP MED Network Policy TLVs with Application types 1 and 2 or with a zero value improves inter-operation with recent releases of Cisco IOS.

Compatible with Avaya Aura™ Communication Manager - SIP software Release 2.6 is compatible with and supported by Avaya Aura™ Communication Manager releases 4.x and 5.x and greater.

Survivability - The major enhancement for this release involves the ability to maintain deskphone operation in the event of SIP proxy server (controller) failure or network disconnect.

The overall reliability of an Avaya Aura™ system is improved by allowing a deskphone to simultaneously register with one or more Session Managers, reducing the amount of time in failover; a deskphone can switch from one proxy to another much more quickly than the alternate registration required by SES and delivered in SIP software Release 2.4. See the *Avaya one-X™ Deskphone SIP Administrator Guide* and Avaya Aura™ Session Manager (and related) documentation on the Avaya Support Web site for detailed information. An Audiocodes gateway is supported for branch office surviveability for emergency calls during failover. Additional secondary gateways are supported in this release, as described in "SIP Software Releases and Surviveability" in Chapter 10 of the *Avaya one-X™ Deskphone SIP Administrator Guide.*

Compatible with other Avaya products/applications - SIP software Release 2.6 inter-operates with the following Avaya offerings:

- Avaya one-X™ Communicator
- Avaya one-X™ Mobile
- Avaya one-X™ Portal

Find information and documentation for the above products/applications on the Avaya support site http://www.avaya.com/support.

Presence - In addition to appearing on the Phone screen, the Call Log and Favorites screens now display presence information in icon form, but only in conjunction with SES.

Phone number formatting information downloaded from PPM - SIP deskphones now download and use number formatting rules from PPM to format numbers in the display information portion of the P-Asserted-Identity (PAI) or Contact headers of incoming SIP messages in a location-dependent and user-friendly fashion; phone numbers are formatted using traditional dashes or dots. This enhancement improves the user experience by enabling an endpoint to display telephone numbers in more easily readable local formats.

New or Updated Configuration Parameters - Link to each of the following new or updated parameters in "Chapter 8" for details:

- ASTCONFIRMATION
- CONFIG_SERVER_SECURE_MODE
- ENABLE_AVAYA_ENVIRONMENT
- ENFORCE_SIPS_URI
- FAILBACK_POLICY
- FAST_RESPONSE_TIMEOUT
- MSGNUM
- QKLOGINSTAT
- RECOVERYREGISTER WAIT
- REDIRECT_TONE
- SDPCAPNEG

- SIMULTANEOUS_REGISTRATION
- SIPCONFERENCECONTINUE

Document Organization

The guide contains the following sections:

Chapter 1: Introduction	Provides an overview of this document.
Chapter 2: Administration Overview and Requirements	Provides an overview of the administrative process and describes general hardware, software, and operational requirements.
Chapter 3: Network Requirements	Describes administrative requirements for your Local Area Network.
Chapter 4: Avaya Aura™ Communication Manager Administration	Describes how to administer Avaya Communication Manager to operate with 9600 Series SIP deskphones.
Chapter 5: Avaya Aura™ SIP Enablement Services (SES), Session Manager (SM), and System Manager Administration	Covers SIP Enablement Services (SES) configuration for 9600 Series SIP deskphones.
Chapter 6: Server Administration	Describes DHCP and HTTP/HTTPS administration for the 9600 Series SIP deskphones.
Chapter 7: Telephone Software and Binary Files	Describes deskphone software, covers software downloads, and provides information about the configuration file.
Chapter 8: Administering Telephone Options	Describes how to use file parameters and options to administer 9600 Series SIP deskphones. Covers backup and restoration of deskphone data. Also describes how to use local procedures to customize a single deskphone from the dialpad.
Chapter 9: Administering Applications and Options	Describes customizeable application-specific parameters, to provide administrative control of deskphone functions and options.
Chapter 10: System Failover and Survivability	Provides detailed information about survivability, including configuration, parameter setup, and characteristics of each failover state.
Appendix A: Glossary of Terms	Provides a glossary of terms used in this document or which can be applicable to 9600 Series IP Deskphones.
Appendix B: Countries With Specific Network Progress Tones	Provides lists of network progress tones for each country.

Other Documentation

See the Avaya support site at http://www.avaya.com/support for 9600 Series IP Deskphone technical and end user documentation, and documentation for all Avaya products.

See the following Web sites that list related, non-Avaya documents, such as those published by the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU):

- **IETF Documents** - IETF documents provide standards relevant to IP Telephony and are available for free from the IETF Web site: http://www.ietf.org/rfc.html.
- **ITU Documents** - Access the ITU Web site for more information about ITU guidelines and documents, available for a fee from the ITU Web site: http://www.itu.int.
- **ISO/IEC, ANSI/IEEE Documents** - Access the ISO/IEC standards Web site for more information about IP Telephony standards, guidelines, and published documents: http://www.iec.ch.

Chapter 2: Administration Overview and Requirements

9600 Series IP Deskphones

The 9600 Series IP Deskphones currently support the H.323 signaling protocol and the SIP signaling protocol.

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

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

SIP was developed by the IETF. Like H.323, SIP provides for real time audio, video, and data communications transmission over a packet network. SIP uses various messages, or methods, to provide:

- Registration (REGISTER),
- Call signaling (INVITE, BYE)
- Control signaling (SUBSCRIBE, NOTIFY)

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

The 9600 Series IP Deskphones are loaded with either H.323 or SIP software as part of initial 96xxupgrade.txt file administration and initialization during installation. Post-installation, software upgrades automatically download using the proper signaling protocol.

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

- Telephone Administration on the Avaya Aura™ Communication Manager (CM) call server, as covered in Chapter 4: Avaya Aura™ Communication Manager Administration.
- Administration on SIP Enablement Services (SES), or administration on Avaya Aura™ Session Manager (SM). Also, for environments with multiple Session Managers, administer Avaya Aura™ System Manager. See Chapter 5: Avaya Aura™ SIP Enablement Services (SES), Session Manager (SM), and System Manager Administration for information.
- IP Address management for the deskphone, as covered in Chapter 6: Server Administration for dynamic addressing. For static addressing, see the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide*.
- Tagging Control and VLAN administration for the deskphone, if appropriate, as covered in Chapter 8: Administering Telephone Options.
- Quality of Service (QoS) administration for the deskphone, if appropriate. QoS is covered in QoS on page 34 and QoS on page 48.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP).
- Interface administration for the deskphone, as appropriate. Administer the deskphone to LAN interface using the PHY1 parameter described in Chapter 3: Network Requirements. Administer the deskphone to PC interface using the PHY2 parameter described in “Interface Control” in the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide.*
- Application-specific deskphone administration, if appropriate, as described in Chapter 8: Administering Telephone Options. An example of application-specific data is Web-specific information required for the optional Web browser application.

Table 1 indicates that you can administer system configuration parameters in a variety of ways and use the following administrative mechanisms:

- Administering the information on the call server.
- Manually entering the information by means of the deskphone dialpad using Craft (local administrative) procedures. Craft procedures are described in "Chapter 3: Local Administrative Options" in the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide.*
- Administering the DHCP server.
- Editing the configuration file on the applicable HTTP or HTTPS file server.
- User modification of certain parameters, when given administrative permission to do so.

Note:

Not all parameters can be administered on all administrative mechanisms. See the applicable chapters in this guide for specific information.

Table 1: Administration Alternatives and Options for 9600 Series SIP Deskphones

Parameter(s)	Administrative Mechanisms	For More Information See:
Telephone Administration	Avaya Communication Manager and SES/ SM (and System Manager for multiple SMs if applicable)	Chapter 4: Avaya Aura™ Communication Manager Administration, Chapter 6: Server Administration, and Other Documentation. For SES/Session Manager/System Manager administration, see Chapter 5: Avaya Aura™ SIP Enablement Services (SES), Session Manager (SM), and System Manager Administration and the product-related documents available on the Avaya support site.
IP Addresses	DHCP (strongly recommended)	DHCP and File Servers on page 65, and especially DHCP Server Administration on page 66.
	Settings file	Chapter 7: Telephone Software and Binary Files and Chapter 8: Administering Telephone Options.
	Manual administration at the deskphone	"Static Addressing Installation" in the *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide.*
	LLDP	Link Layer Discovery Protocol (LLDP) on page 131.
Tagging and VLAN	LLDP	Link Layer Discovery Protocol (LLDP) on page 131.
	DHCP	DHCP Server Administration on page 66, and Chapter 8: Administering Telephone Options.
	Settings file	DHCP and File Servers on page 65 and Chapter 8: Administering Telephone Options.
	Manual administration at the deskphone	"Static Addressing Installation" in the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide*.
Network Time Server (NTS)	DHCP Settings file	DHCP Server Administration on page 66 and Network Time Protocol (NTP) Server on page 31.
Quality of Service	Settings file	Chapter 8: Administering Telephone Options.
Interface	DHCP	DHCP and File Servers on page 65, and Chapter 7: Telephone Software and Binary Files.
	Settings file (strongly recommended)	DHCP and File Servers on page 65, and Chapter 7: Telephone Software and Binary Files.
	LLDP	Link Layer Discovery Protocol (LLDP) on page 131.
	Manual administration at the deskphone	"Secondary Ethernet Interface Enable/Disable" in the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide*.

Table 1: Administration Alternatives and Options for 9600 Series SIP Deskphones (continued)

Parameter(s)	Administrative Mechanisms	For More Information See:
Application - specific parameters	DHCP	DHCP and File Servers on page 65, and especially DHCP Server Administration on page 66. Also, Chapter 8: Administering Telephone Options.
	Settings file (strongly recommended)	DHCP and File Servers on page 65, and especially HTTP Generic Setup on page 78. Also, Chapter 8: Administering Telephone Options.

General information about administering DHCP servers is covered in DHCP and File Servers on page 65, and more specifically, DHCP Server Administration on page 66. General information about administering HTTP servers is covered in DHCP and File Servers, and more specifically, HTTP Generic Setup. Once you are familiar with that material, you can administer deskphone options as described in Chapter 8: Administering Telephone Options.

Parameter Data Precedence

As shown in Table 1: Administration Alternatives and Options for 9600 Series SIP Deskphones, you can administer a given parameter in a number of ways. The precedence, from lowest to highest, is:

1. LLDP
2. DHCP
3. Settings file

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

4. Personal Profile Manager (PPM) through either SES or SM
5. Manual administration, unless the system parameter USE_DHCP is set to 1 (Get IP Address automatically by DHCP), or backup file data obtained through PPM.

For example, if the SIP outbound proxy server address is defined to have the precedence information so that the value retrieved from DHCP server has a lower precedence than the value retrieved from the settings file, and the value retrieved from the settings file is higher than the value retrieved from PPM, then the following determination occurs:

- If the most recent value the deskphone has is from DHCP and new server address information is retrieved from the settings file, the deskphone will use the new value from the settings file.

- If later on, the deskphone receives a new server address value from PPM, it will not use this value because PPM's precedence as a data source for the server address is lower than the current value (which came from the settings file).
- If the server to which a specific deskphone points is changed manually using the Craft ADDR procedure, that value now takes precedence over the previous value.

Note:

The only exception to this sequence is in the case of VLAN IDs. In the case of VLAN IDs, LLDP settings of VLAN IDs are the absolute authority. Then the usual sequence applies. For the L2QVLAN and L2Q system values, LLDP settings of VLAN IDs are the absolute authority only if the LLDP task receives the VLAN IDs before DHCP, and the DHCP client of the deskphone is activated. If the LLDP task receives the VLAN IDs after DHCP negotiation, several criteria must be successful before the deskphone accepts VLAN IDs from LLDP. For more information, see Link Layer Discovery Protocol (LLDP) on page 131.

The Administrative Process

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

1. Avaya Communication Manager (4.0 or greater) administered for 9600 Series IP Telephones. Administer 9600 Series SIP deskphones running under CM 4.0 with the 4620SIP station type; administer 9600 Series SIP deskphones running later versions of CM as 96*xx*SIP, where *xx* represents the model (for example, 9620SIP, 9630SIP, etc.).
2. SES (SIP Enablement Services; 4.0 or greater) or SM (Session Manager, 5.2 or greater) administered. As of SIP software Release 2.6, Avaya Aura System Manager must also be administered for multiple SM environments. See Supported SIP Environments on page 43 for information.
3. LAN and applicable servers (file servers, Network Time server) administered to accept the deskphones.
4. Telephone software downloaded from the Avaya support site.
5. 46xxsettings file updated with site-specific and SIP-specific information, as applicable.
6. 9600 Series Telephones installed. For more information, see the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide*.
7. Individual SIP deskphones updated using Craft procedures, as applicable. For more information, see "Local Administrative Procedures" in the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide*.
8. Survivability administration to set up the local SIP gateway and administer additional controllers in the settings file as applicable. Note that as of SIP software Release 2.5,

certain gateway configurations require SES 5.2 or SM 5.2 and Avaya Aura Communication Manager 5.2. Additionally, as of SIP software Release 2.6, Avaya Aura Communication Manager 6.0 and Avaya Aura Session Manager 6.0.

Administrative Checklist

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

Note:

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

Table 2: Administrative Checklist

Task	Description	For More Information See:
Network Requirements Assessment	Determine that network hardware is in place and can handle deskphone system requirements.	Chapter 3: Network Requirements.
Administer Avaya 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 CM station form(s).	Chapter 4: Avaya Aura™ Communication Manager Administration. Chapter 4: Avaya Aura™ Communication Manager Administration.
Administer the Proxy Server	Administer for SIP Enablement Services (SES) or Avaya Aura Session Manager (SM).	*Installing, Administering, Maintaining, and Troubleshooting SIP Enablement Services* (Document # 03-600768) or *Administering Avaya Aura™ Session Manager* (Document Number 03-603324), available on the Avaya support Web site, http://www.avaya.com/support. Chapter 5: Avaya Aura™ SIP Enablement Services (SES), Session Manager (SM), and System Manager Administration.

Table 2: Administrative Checklist (continued)

Task	Description	For More Information See:
Administer Avaya Aura System manager	Administer for environments using multiple Session Managers.	Chapter 5: Avaya Aura™ SIP Enablement Services (SES), Session Manager (SM), and System Manager Administration.
DHCP server installation	Install a DHCP application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
Administer DHCP application	Add IP deskphone administration to the DHCP application.	DHCP Server Administration in Chapter 6: Server Administration.
Administer Network Time Server	Set value(s) for Simple Network Time Protocol (SNTP)	Option 42 under DHCP Generic Setup.
HTTP/HTTPS server installation	Install an HTTP/HTTPS application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
Binary file(s), 96xxupgrade.txt file, and settings file installation on HTTP/ HTTPS server	Download the files from the Avaya support site.	http://www.avaya.com/support Chapter 7: Telephone Software and Binary Files.
Modify settings file as needed	Edit the settings file as necessary for your environment, using your own tools.	Chapter 7: Telephone Software and Binary Files.
Administer deskphones locally as applicable	As a Group:	The GROUP System Value on page 90 and the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide.*
	Individually:	The applicable Craft Local Procedures in the *Avaya one-X™ Deskphone Edition SIP Installation and Maintenance Guide.*

Table 2: Administrative Checklist (continued)

Task	Description	For More Information See:
Installation of deskphones in the network		*Avaya one-X™ Deskphone SIP Installation and Maintenance Guide*.
Allow user to modify Options, if applicable	Set the following parameters in the settings file: ENABLE_CALL_LOG ENABLE_CONTACTS ENABLE_MODIFY_CONTACTS ENABLE_PHONE_LOCK ENABLE_PRESENCE PROVIDE_EDITED_DIALING PROVIDE_LOGOUT PROVIDE_NETWORKINFO_SCREEN PROVIDE_OPTIONS_SCREEN USE_EXCHANGE_CALENDAR	SIP 9600 Series IP Deskphones Customizeable System Parameters.

3 of 3

Deskphone Initialization Process

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. This description can help you understand how the 9600 Series SIP Deskphones relate to the routers and servers in your network.

Step 1: Deskphone to Network

The deskphone is appropriately installed and powered. After a short initialization process, the deskphone identifies the LAN speed and sends a message out into the network, identifying itself and requesting further information. A router on the network receives and relays this message to the appropriate DHCP server.

Step 2: Deskphone to LLDP-Enabled Network

An LLDP-enabled network provides information to the deskphone, as described in Link Layer Discovery Protocol (LLDP) on page 131. Among other data passed to the deskphone is the IP Address of the HTTP or HTTPS server.

Step 3: Deskphone to DHCP Server

The DHCP server provides information to the deskphone, as described in DHCP and File Servers on page 65. Among other data passed to the deskphone is the IP Address of the HTTP or HTTPS server.

Step 4: Deskphone and File Server

The 9600 Series IP Deskphones can download upgrade files, binary files, certificates, language files, and settings files from either an HTTP or HTTPS server. The deskphone queries the file server, which transmits an upgrade file to the deskphone. At a minimum, this 96xxupgrade.txt file tells the deskphone which binary file the deskphone must use. The binary file is the software that has the telephony functionality.

The deskphone uses the 96xxupgrade.txt file to determine if it has the proper binary file. If the deskphone determines the proper binary file is missing, the deskphone requests an binary file download from the file server. The file server then downloads the file and conducts some checks to ensure that the file was downloaded properly. If the deskphone determines it already has the proper file, the deskphone proceeds as described in the next paragraph without downloading the binary file again.

The deskphone checks and loads the binary file, then uses the 96xxupgrade.txt file to look for a settings file, if appropriate. The optional settings file can contain settings you have administered for any or all of the 9600 Series SIP IP Telephones in your network. For more information about this download process and settings file, see Chapter 7: Telephone Software and Binary Files.

Step 5: Telephone and SIP Proxy Server

In this step, the deskphone might prompt the user for an extension and password. The deskphone uses that information to exchange a series of messages with SES/SM, which in turn communicates with Avaya Communication Manager (CM). For a new installation and for full service, the user can enter the deskphone extension and the SES/SM password. For a restart of an existing installation, this information is already stored on the deskphone.

Important:

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

The deskphone and SES or SM, and SES/SM and CM exchange more messaging. The expected result is that the deskphone is appropriately registered and call server data such as feature button assignments are downloaded.

For more information about the installation process, see the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide*.

Error Conditions

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

The *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide* 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

Network Assessment

Perform a network assessment to ensure that the network will have the capacity for the expected data and voice traffic, and that it can support for all applications:

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

Also, QoS support is required to run VoIP on your configuration. For more information, see Other Documentation on page 18 and the QoS parameters L2QAUD, L2QSIG, DSCPAUD, and DSCPSIG in Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters.

Hardware Requirements

To operate properly, you need:

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

  Important:

  IP deskphone firmware Release 1.0 or greater requires TN799C V3 or greater C-LAN circuit pack(s). For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya support Web site http://www.avaya.com/support.

To ensure that the appropriate circuit pack(s) are administered on your Communication Manager call server, see Chapter 4: Avaya Aura™ Communication Manager Administration. For more information about hardware requirements in general, see the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide*.

Server Requirements

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

- DHCP server
- HTTP or HTTPS server
- SIP Proxy (controller) or Registration server
- Network Time Protocol server for SNTP
- SES/SM SIP Proxy Server (controller) to be used as a gateway for survivability
- System Manager
- Communication Manager
- WML server (if applicable)

Note:

9600 Series SIP IP Telephones need SIP Enablement Services (SES) or Avaya Aura Session Manager (SM) to work properly. The SIP Proxy and Registration servers reside on the SES/SM server. Avaya Aura Communication Manager (CM) is considered a “feature server” behind SES/SM that provides Outboard Proxy SIP (OPS) features. SIP software Releases 2.0, 2.2 and 2.4 support both SES 4.X and 5.X, but when the corresponding server is running SES 4.X, the deskphones assume only those features compatible with SES 4.X. SIP software Release 2.5 also supports Session Manager 5.2. SIP software Release 2.6 supports Session Manager 6.0 and Communication Manager 6.0.

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

For parameters related to Avaya Communication Manager information, see Chapter 4: Avaya Aura™ Communication Manager Administration. For parameters related to DHCP and file servers, see Chapter 6: Server Administration.

Important:

The deskphones obtain important information from the 96xxupgrade.txt files on the server(s) and depend on the binary file for software upgrades. If these servers are unavailable when the deskphones reset, the deskphones will not operate properly. Some features might not be available. To restore them you need to reset the deskphone(s) when the file server is available.

DHCP Server

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

HTTP/HTTPS Server

Administer the HTTP or HTTPS file server and application as described in HTTP Generic Setup on page 78.

Network Time Protocol (NTP) Server

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

Presence

The deskphone determines the type of primary proxy server during dynamic feature set discovery and sets the PRIMARY_PROXY_ENVIRONMENT parameter accordingly. When the PRIMARY_PROXY_ENVIRONMENT is set to 1 (indicating an SES environment), the deskphone supports any presence server.

For SES environments:

Presence requires SES 4.0 or higher. Avaya Distributed Office is not supported. The following standards and guidelines dictate how presence is processed:

RFC 3856: *A Presence Event Package for the Session Initiation Protocol (SIP)*,

RFC 3857: *A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)*," and

RFC 3858: *An Extensible Markup Language (XML) Based Format for Watcher Information*.

See Presence Notification on page 143 for information on how the deskphone processes presence messages in an SES environment.

Required Network Information

Before you administer DHCP and HTTP/HTTPS, as applicable, complete the information in Table 3. If you have more than one router, HTTP/TLS server and subnetwork mask in your configuration, complete Table 3 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. 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, in accordance with IETF RFCs 1034 and 1035. For more information about DNS, see DHCP Generic Setup on page 68 and DNS Addressing on page 128.

Table 3: Required Network Information Before Installation - Per DHCP Server

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

The default file server file path is the "root" directory used for all transfers by the server. All files are uploaded to or downloaded from this default directory. In configurations where the upgrade (96xxupgrade.txt) and binary files are in the default directory, do not use item 4 in Table 3.

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

- Administering the DHCP server as described in Chapter 6: Server Administration.
- Editing the configuration file on the applicable HTTP or HTTPS file server, as covered in 9600 Series SIP IP Telephone Upgrade and Binary Files.

Other Network Considerations

SNMP

The 9600 Series SIP IP Telephones are fully compatible with SNMPv2c and with Structure of Management Information Version 2 (SMIv2). The deskphones respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. “Fully compatible” means that 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 which IP Addresses the deskphone accepts SNMP queries from. You can also customize your community string with system values SNMPADD and SNMPSTRING, respectively. For more information, see Chapter 6: Server Administration and Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters.

Note:

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

For more information about SNMP and MIBs, see the IETF Web site listed in Other Documentation on page 18. 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 http://www.avaya.com/support.

Registration and Authentication

A 9600 Series SIP IP Telephone requires an outboard proxy SIP (OPS) extension on Avaya Communication Manager and a login and password on the SES/SM Server to register and authenticate it.

Important:

SES and Session Manager have different requirements for assigning a login (user name and password). For SES, the user name is the extension. For Session Manager, the user name takes the canonical address format that uniquely identifies a user across all Enterprise sites; as described in the white paper titled *Avaya Aura™ 6.0 Configuration for Presence and IM* on the Avaya support Web site.

Registration is described in the Initialization process, in Step 5: Telephone and SIP Proxy Server on page 27. For further information, see *Installing, Administering, Maintaining, and Troubleshooting SIP Enablement Services R 4.0* (03-600768) or *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.

Reliability and Performance

All 9600 Series SIP IP Telephones respond to a ping or traceroute message sent from Avaya Communication Manager or any other network source and originate a ping.

If applicable, the deskphones test whether the network Ethernet switch port supports IEEE 802.1D/q tagged frames by ARPing the router with a tagged frame. For more information, see VLAN Considerations on page 124. If your LAN environment includes Virtual LANs (VLANs), your router must respond to ARPs for VLAN tagging to work properly.

QoS

For more information about the extent to which your network can support any or all of the QoS initiatives, see your LAN equipment documentation. See QoS on page 48 for QoS implications for the 9600 Series SIP IP Telephones.

All 9600 Series SIP IP Telephones provide some detail about network audio quality. For more information see, Network Audio Quality Display on 9600 Series SIP IP Telephones on page 35.

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 IEEE 802.1D and 802.1Q on page 48 and VLAN Considerations on page 124. Three bits of the 802.1Q tag are reserved for identifying packet priority to allow any one of eight priorities to be assigned to a specific packet.

- **7:** Network management traffic
- **6:** Voice traffic with less than 10ms latency
- **5:** Voice traffic with less than 100ms latency
- **4:** “Controlled-load” traffic for critical data applications
- **3:** Traffic meriting “extra-effort” by the network for prompt delivery, for example, executive e-mail
- **2:** Reserved for future use
- **0:** The default priority for traffic meriting the “best-effort” for prompt delivery of the network.
- **1:** Background traffic such as bulk data transfers and backups

Note:

Priority 0 is a higher priority than Priority 1.

Network Audio Quality Display on 9600 Series SIP IP Telephones

All 9600 Series SIP IP Telephones give the user an opportunity to monitor network audio performance while on a call using the Avaya menu Network Information option. For more information, see the deskphone user guide.

While on a call, the deskphones display network audio quality parameters in real-time, as shown in Table 4:

Table 4: Parameters in Real-Time

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

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

SIP Station Number Portability

The 9600 Series SIP IP Telephones provide station number portability for visiting users in an SES environment (only) and for mobile users in a Session Manager environment (only). On startup or a reboot, the deskphone attempts to establish communication with its home server based on the User Name and Password. For mobile users, registration redirection occurs automatically. For visiting users, administration is required as covered in Visiting User Administration on page 136.

Assume a situation where the company has multiple locations in London and New York, all sharing a corporate IP network. Users want to take their telephone functionality from their offices in London to their New York office. When users start up their deskphones in the new location and enter their credentials, the local server usually routes them to the local call server. With proper administration of the local server, the deskphone knows to try its home server, the one in London. The user can then be automatically registered with the London server.

TCP/UDP Port Utilization

The 9600 Series SIP IP Telephones use a variety of protocols, particularly TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and TLS (Transport Layer Security) to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP ports each piece of equipment uses to support each protocol and each task within the protocol. For additional TCP/UDP port utilization information as it applies to Avaya Communication Manager, see UDP Port Selection on page 47.

Depending on your network, you might need to know what ports or ranges are used in the operation of 9600 Series IP Telephones. Knowing these ports or ranges helps you administer your networking infrastructure.

Note:

In many cases, the ports used are the ones called for by IETF or other standards bodies.
Some of the explanations in Table 5 and Table 6 refer to configuration parameters or options settings. For more information about parameters and settings, see Administering Options for the 9600 Series SIP Deskphones.

Table 5: Received Packets (Destination = SIP IP Telephone)

Destination Port	Source Port	Use	UDP or TCP?
The number used in the Source Port field of the DNS query sent by the deskphone	Any	Received DNS messages	UDP
The number used in the Source Port field of the packets sent by the deskphone's HTTP client	Any	Packets received by the deskphone's HTTP client	TCP
The number used in the Source Port field of the TLS/ SSL packets sent by the deskphone's HTTP client	Any	TLS/SSL packets received by the deskphone's HTTP client	TCP
68	Any	Received DHCP messages	UDP

1 of 2

Table 5: Received Packets (Destination = SIP IP Telephone) (continued)

Destination Port	Source Port	Use	UDP or TCP?
The number used in the Source Port field of the SNTP query sent by the deskphone	Any	Received SNTP messages	UDP
161	Any	Received SNMP messages	UDP
50000	Any	Received CNA test request messages	UDP
The number used in the Source Port field of registration messages sent by the deskphone's CNA Agent	Any	Received CNA registration messages	TCP
PORTAUD or the port number reserved for CNA RTP tests	Any	Received RTP and SRTP packets	UDP
PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd) or the port number reserved for CNA RTP tests plus or minus one, as for PORTAUD, above	Any	Received RTCP and SRTCP packets	UDP
If signaling is initiated by the deskphone = the number used in the Source Port field of the signaling packets sent by the deskphone If signaling is initiated by the server = System-Specific	Any	Received signaling protocol packets	UDP/TCP

2 of 2

Table 6: Transmitted Packets (Source = SIP IP Telephone)

Destination Port	Source Port	Use	UDP or TCP?
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
80 unless explicitly specified otherwise (i.e. in a URL)	Any unused port number	Packets transmitted by the deskphone's HTTP client	TCP
123	Any unused port number	Transmitted SNTP messages	UDP

1 of 3

Table 6: Transmitted Packets (Source = SIP IP Telephone) (continued)

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

2 of 3

Table 6: Transmitted Packets (Source = SIP IP Telephone) (continued)

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

3 of 3

IP Address Reuse

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

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

Router(s) in Use:

if no responses are received from the router(s) 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 VLAN Detection on page 124 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.

Security

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

9600 Series SIP IP Telephones support Transport Layer Security (TLS) for signaling and for secure communications (SRTP). This standard allows the deskphone to establish a secure connection to a HTTPS server, in which the upgrade and settings file can reside. This setup adds security over another alternative.

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

You also have a variety of optional capabilities to restrict or remove how crucial network information is displayed or used. These capabilities are covered in more detail in Chapter 6: Server Administration and include:

- Depending on the SIGSIGNAL parameter, supporting signaling channel encryption while registering, and when registered, with appropriately administered Avaya Communication Manager.
- Restricting the response of the 9600 Series SIP IP Telephones to SNMP queries to only IP Addresses on a list you specify.
- Specifying an SNMP community string for all SNMP messages the deskphone sends.
- Restricting dialpad access to Craft Local Procedures to experienced installers and technicians and requiring password entry to access Craft procedures.
- Restricting the end user's ability to use a deskphone Options application to view network data.

Chapter 4: Avaya Aura™ Communication Manager Administration

Call Server Requirements

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

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

Supported SIP Environments

SIP software Release 2.6 supports all of the configurations listed below for SIP software Release 2.5 and 2.4, plus:

- Session Manager 6.0 with CM 6.0
- Session Manager 6.1 with CM 6.1 operating as a high availability (for example, multiple SM's) evolution or feature server
- SES 5.2 with CM 5.2 operating as an access server

In addition to the environments supported by SIP software Release 2.4, SIP software Release 2.5 provided support for:

- CM 5.2.1 and Avaya Aura™ Session Manager Release 2.5 (as an alternative to using SES)

With SIP software Release 2.4, 9600 Series IP Telephones could be deployed in non-survivability mode in the following CM/SES enterprise environments:

- CM 4.0, SES 4.0
- CM 4.0, SES 5.0
- CM 5.0, SES 4.0
- CM 5.0, SES 5.0

SIP software Release 2.4 also allowed 9600 Series IP Telephones to be deployed in survivability mode in the following CM/SES enterprise environments:

- CM 4.0 through 5.1, SES 4.0

- CM 4.0 through 5.1, SES 5.0
- CM 4.0 through 5.1, SES 5.1
- CM 5.0/5.1, SES 5.1 and a secondary third-party SIP proxy/gateway, specifically the Audiocodes gateway MP114, MP118 Firmware Version 5.40.

The features available to the deskphones depend on the CM and SES/SM configuration as shown in Table 7. For more information on feature configuration and operation, see the appropriate Communication Manager Feature and Administration guides.

Table 7: Release 2.4+ Feature Compatibility Matrix

Feature	Minimum CM Version Required	Minimum SES Version Required
SBM24 Button Module - feature button assignments & operation	5.0	5.1
SBM24 Button Module - Autodial assignments & operation	5.0	5.1.2
SBM24 Button Module - Bridged Call Appearance (BCA) and Call Appearance operation	5.1.2	5.1
Auto Answer	5.0	5.0

Features from prior SIP phone releases that have dependencies on CM and SES versions are shown in the table below:

Table 8: Prior SIP Release Feature Compatibility Matrix

Feature	Minimum CM/SES Versions Required	Minimum CM/SM Versions Required
Visiting User	5.0/5.0	Not available with SM
Auto Callback	5.0/5.0	Not supported by SM
Extend Call	5.0/5.0	5.2.1/5.2
SRTP	4.0.1/n/a	5.2.1/5.2
All features other than those noted in this and the previous table.	4.0/4.0	5.2.1/5.2

Switch Compatibility

As of SIP software Release S1.0, 9600 Series IP Telephones are supported by Avaya Communication Manager (CM) Release 4.0 and later. For deskphones running a CM Release earlier than 5.2, be sure to administer 9600 Series SIP IP Telephones as 4620SIP deskphones on Avaya Communication Manager; deskphones running CM Release 5.2 and later can be administered as 96*xx*SIP deskphones, where *xx* represents the deskphone model number (for example, 9620, 9630, etc.).

Note:

The 9620 only supports a total of 12 call appearances and administered feature buttons. The 9630/9630G, 9640/9640G, and 9650C can be administered for a total of 24 call appearances and feature buttons. Adding an SBM24 button module provides 24 additional features.

For specific administration instructions about the 9600 Series SIP IP Telephones, see Administering Stations on page 58.

Communication Manager Administrative Requirements for SES

There are several initial CM provisioning tasks that must be performed before administering SIP users. These tasks are described in *SIP Support in Avaya Communication Manager Running on Avaya S8XXX Server*s (Document Number 555-245-206) and related documentation. The tasks to administer Communication Manager for SIP Enablement Services (SES) fall into three categories:

- system-level preparation,
- SIP trunk administration, and
- call routing administration

The sections that follow describe each of these tasks.

System-Level Preparation Tasks

The system-level preparation tasks for SES administration include:

- Setting the SIP Trunk capacity on the System Capacity screen.
- Verifying that the IP Trunks field is set to **y** on the System-Parameters Customer-Options screen page 4.

- Verifying that the Maximum Administered SIP Trunks are set correctly on the System Parameters Customer-Options screen page 2.
- Setting the OPS SIP station capacity on the System Parameters Customer Options screen page 1.
- Setting the IP Node name for SES on the IP Node Names screen.
- Entering the IP Address and host name for the administered SES server on the IP Address Mapping screen.
- Setting the Authoritative Domain on the IP Network Region screen.
- Setting the intra- and inter-region IP-IP Direct Audio to yes on the IP Network Region screen.
- Setting the Signaling Group on the Signaling Group screen page 1.

SIP Trunk Administration

SIP trunk administration tasks for SES include:

- Setting the SIP Intercept Treatment and Trunk-to-Trunk Transfer on the System Parameters Features screen page 1.
- Administering Trunk Groups on the Trunk Group screens (pages 1 through 4).
- Assigning public unknown numbering data on the Numbering - Public/Unknown Numbering screen.
- Assigning a SIP phone Set description on Configuration Set screen.

Call Routing Administration

Call routing administration for SES includes:

- Administering Feature Access Codes (FACs) on the Feature Access Code screen.
- Administering the ARS Digit Analysis Table on the ARS Digit Analysis Table screen.
- Administering the Route Pattern on the Route Pattern screen.
- Adding the Route Pattern to the Numbering - Public/Unknown Numbering screen.
- Administering the Proxy Selection Route Pattern on the Locations screen.
- Allowing the system to identify the location of a caller who dials a 911 emergency call from a SIP endpoint on the IP Network Map screen.

The *Administrator Guide for Avaya Communication Manager* (Document Number 03-300509) provides detailed instructions for administering an IP telephone system on Avaya Communication Manager. See Chapter 3 “Managing Telephones,” which describes the process

of adding new telephones. Also, you can locate pertinent screen illustrations and field descriptions in Chapter 19 “Screen References” of that guide. You can find this document on the Avaya support Web site.

IP Interface and Addresses

Follow these general guidelines for SES administration:

- Define the IP interfaces for each C-LAN and Media processor circuit pack on the switch using the IP Interfaces screen. For more information, see *Administration for Network Connectivity for Avaya Communication Manager* (Document 555-233-504).
- On the Customer Options form, verify that the **IP Stations** field is set to “**y**” (Yes). If it is not, contact your Avaya sales representative.

UDP Port Selection

The 9600 Series SIP IP Telephones use an even-numbered port, selected from the range 4000 to 10000. The deskphones **cannot** be administered from the Avaya Communication Manager Network Region form to support UDP port selection for SES environments.

Communication Manager Administrative Requirements for Session Manager

For information about CM administrative requirements with Session Manager, see the Avaya Aura™ Session Manager and Avaya Aura™ System Manager document libraries on the Avaya support site, as described in Chapter 5: Avaya Aura™ SIP Enablement Services (SES), Session Manager (SM), and System Manager Administration.

Communication Manager Common Administrative Requirements

The sub-sections that follow provide administrative information that is common to both SES and Session Manager.

RSVP and RTCP/SRTCP

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

QoS

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

IEEE 802.1D and 802.1Q

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

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

NAT

9600 Series SIP IP Telephones do not support Network Address Translation (NAT) interworking.

DIFFSERV

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

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

Received DSCP information will be ignored.

Voice Mail Integration

9600 Series SIP IP Telephones use the settings file to configure the **Messages** button by setting the system parameter MSGNUM to any dialable string. MSGNUM examples are:

- a standard telephone number the deskphone should dial to access your voice mail system, such as AUDIX or Octel.
- a Feature Access Code (FAC) that is configured for the Feature "To Voice Mail" will allow the user to transfer the active call directly to voice mail. FACs are supported only for QSIG-integrated voice mail systems like AUDIX or Octel. QSIG is an enhanced signaling system that allows the voice mail system and Avaya Communication Manager Call Processing to exchange information.

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

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

```
SET MSGNUM 1234
```

where ***1234*** is the Voice Mail extension (CM hunt group or VDN). For more information, see Table 14.

To reach the Voice Mail system using the **Messages** button during failover to a non-AST server, administer the parameter PSTN_VM_NUM.

Auto Hold

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

Call Transfer Considerations

Unlike 9600 H.323 IP Telephones, the 9600 Series SIP IP Telephones transfer operation is controlled locally by the deskphone and is not affected by the settings Abort Transfer?, Transfer Upon Hang-up and Toggle Swap, on page 7 of the system-parameters features screen.

Conferencing Call Considerations

Unlike 9600 H.323 IP Telephones, the 9600 Series SIP IP Telephones conference operation is controlled locally by the phone and is not affected by the settings Abort Conference Upon Hang-up, No Dial Tone Conferencing, Select Line Conferencing and Toggle Swap, on page 7 of the system-parameters features screen.

Telephone Administration

Table 9 summarizes the calling features available on 9600 Series SIP IP Telephones. Some features are supported locally at the deskphone, while others are only available with Avaya SIP Enablement Services and Communication Manager with OPS.

The features shown in Table 9 can be invoked at the phone either directly or by selecting a CM-provisioned feature button. Communication Manager automatically handles many other standard calling features such as call coverage, trunk selection using Automatic Alternate Routing (AAR), or Automatic Route Selection (ARS), Class Of Service/Class Of Restriction (COS/COR), and voice messaging. Details on feature operation and administration can be found in the *Feature Description and Implementation for Avaya Communication Manager* (Document Number 555-245-205) and any of the CM administration documents available on the Avaya support site. The Avaya SIP solution configures all SIP deskphones in Communication Manager as OPS.

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

Note:

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

Table 9: Avaya one-X SIP Deskphone Feature Support

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with CM/SES or CM/SM
3-Way Conferencing	Yes	
6-way Conference Bridge		Yes

1 of 4

Table 9: Avaya one-X SIP Deskphone Feature Support

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with CM/SES or CM/SM
Auto Intercom		With SES, requires CM Release 5.1 or later; with SM, requires CM 5.2.1 or later.
Automatic Call Back/ Cancel		Yes but is not supported by SM 6.0/ CM 6.0 operating as a feature server
Call Forward All Calls (on/off)		Yes
Call Forward Busy/ Don’t Answer (on/off)	Yes	Yes
Call Forward Unconditional (on/off)	Yes	
Call Hold	Yes (Consultation Hold)	Yes
Call Management - incoming, outgoing call screening		Yes
Call Park and Unpark		Yes
Call Pick-Up Group		Yes
Call Pickup Directed		Yes
Call Pickup Extended Group		Yes
Calling Party Number Block/Unblock		Yes
Dial Intercom		With SES, requires CM Release 5.1 or later; with SM, requires CM 5.2.1 or later.

2 of 4

Table 9: Avaya one-X SIP Deskphone Feature Support

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with CM/SES or CM/SM
Directed Call Pick-Up		Yes
Distinctive Alerting		Yes
EC500 Enable		Yes
EC500 Disable		Yes
Exclusion		With SES, requires CM Release 5.1 or later; with SM, requires CM 5.2.1 or later.
Extend Call for EC500		With SES, requires CM Release 5.1 or later; with SM, requires CM 5.2.1 or later.
Extended Group Call Pickup		Yes
Find Me		Yes
Group Call Pickup		Yes
Redial	Yes	Yes
Malicious Call Trace		Yes
Message Waiting Indication	Although MWI is not available, user can access their voice mailbox using the Message button if the parameter PSTN_VM_NUM is administered	
Music on Hold		Yes
One Touch Recording		Yes
Priority Call		Yes

3 of 4

Table 9: Avaya one-X SIP Deskphone Feature Support

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with CM/SES or CM/SM
Send All Calls Enable/ Disable		Yes
Third Party Call Forward	Yes	With SES, requires CM Release 5.1 or later; with SM, requires CM 5.2.1 or later.
Third Party Call Forward Busy Don't Answer	Yes	With SES, requires CM Release 5.1 or later; with SM, requires CM 5.2.1 or later.
Third Party Send All Calls	Yes	With SES, requires CM Release 5.1 or later; with SM, requires CM 5.2.1 or later.
Transfer - attended	Yes	Yes
Transfer - unattended	Yes	Yes
Transfer to Voice Mail		Yes
Whisper Page		Yes

4 of 4

CM/SIP IP Telephone Configuration Requirements

This section refers to Communication Manager (CM) administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. The system-wide CM form and the particular page that needs to be administered for each feature are provided. These features, which already exist, are not required but are recommended because they optimize the deskphone user interface. CM 4.0 or greater is required.

Note:

For deskphone configuration requirements for Avaya Aura™ Session Manager, see *Administering Avaya Aura Communication Manager as a Feature Server* (Document Number 03-603479) and related Avaya Aura Session Manager documents, all available on the Avaya support site.

Table 10: CM/SIP Configuration Requirements

Task/Form	Command	Field(s)	Value(s)
IP Network Region		RTCP Report Period (secs)	SIP deskphones have a fixed reporting period. Note that this parameter is only displayed if "Use Default Server Parameters?" is set to "n".
IP Network Region		Authoritative Domain	Make sure that the Authoritative Domain is set to the same value as SIP Domain for Solution.
Off-PBX Telephones Station Mapping	change off-pbx-station mapping xxxx		Bridged call items on this form MUST be “none” or “orig.” In CM Release 5.0, default is “none.”
Feature - Related System Parameters (page 1)	change system-parameters features	Music/Tone on Hold	This CM setting controls the music on hold capability for all endpoints, including SIP deskphones.
Feature - Related System Parameters (page 4)	change system-parameters features	Directed Call Pickup	This CM setting controls the availability of directed call pickup.
Feature - Related System Parameters (page 4)	change system-parameters features	Extended Group Call Pickup	This CM setting allows a user to answer calls that were directed to another call pickup group.
Feature - Related System Parameters (page 17)	change system-parameters features	Whisper Page Tone Given To	This CM setting controls who hears the whisper page.

1 of 5

Table 10: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Define the dial plan formats on the Dialplan Analysis Table form (SES only)	change dialplan analysis	Call Type	Includes all deskphone extensions and OPS Feature Name Extensions (FNEs). To define the FNEs for the OPS features listed in Table 9, a FAC must also be specified for the corresponding feature. In a sample configuration, deskphone extensions are five digits in length and begin with 3 or 4, FNEs are five digits beginning with 7, and the access codes have various formats as indicated with the Call Type of “fac.” Note that for Session Manager environments, dialplan administration is done through Avaya Aura System Manager.
Define the access codes corresponding to the OPS FNEs on the Feature Access Code form	change feature-access-codes	Various fields on pages 1-5 of the form	
After defining the FACs, define the FNEs not provisioned by CM feature buttons using the command	change off-pbx-telephone feature-name-extensions		Used to support both OPS and Extension to Cellular.
Set the appropriate service permissions to support OPS features on the Class of Service form	change cos	Varied	y (Yes) or n (No)
Enable applicable calling features on the Class of Restriction form	change cor	Varied	To use the Call Pickup feature, the Can Use Directed Call Pickup and Can Be Picked Up By Call Pickup fields must be set to "y" for the affected stations. Note that Page 3 can be used to implement a form of centralized call screening for groups of stations and trunks

2 of 5

Table 10: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Add a station for each SIP phone to be supported using the Station form (page 1)	add station ***xxxxxx*** (where ***xxxxxx*** represents the extension number)	Extension	Assign the same extension as the CM call server extension administered in SIP Enablement Services. See Chapter 5: Avaya Aura™ SIP Enablement Services (SES), Session Manager (SM), and System Manager Administration for SES configuration information.
		(Station) Type	Use 9600SIP.
		Port	System-populated.
		Coverage Path	For voice messaging or other hunt group, if available.
		COS and COR	Same values as administered in the previous COS & COR section(s).
		Name	The person associated with the deskphone. This name should match what is entered for name in the Avaya SES proxy configuration.
		Message Lamp Ext	Enter the extension of the station you want to track with the message waiting lamp. (Usually the same extension initially entered on the Station form.)

3 of 5

Table 10: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Continue adding station information for the SIP phone using the Station form (page 2)	add station ***xxxxxx*** (where ***xxxxxx*** represents the extension number)	Bridged Call Alerting	Set to "y" if the extension for this SIP deskphone will have a "bridged" appearance defined on another non-SIP telephone. Note that no other attributes of the bridged appearance feature apply to SIP deskphones (e.g. off-hook indication, bridge-on, etc.).
		Restrict Last Appearance	By default, the last call appearance is reserved for outgoing calls from a phone. On stations with only three (3) call appearances, set the field to "n" for proper SIP conference and transfer operation. In this mode, all call appearances are available for making or receiving calls.
		AUDIX Name	Enter the name of the voice messaging system administered for this system.
		Coverage After Forwarding	This field, with a default of "s" for system, governs whether an unanswered forwarded call is given CM coverage treatment.
		Per Station CPN Send Calling Number?	If CM is configured to always send Caller ID, you can individually block certain stations by setting this field to "n". This field also needs to be set to "n" if you want to use the "Calling Number nblock" FNE.
Continue adding station button assignments for the SIP deskphone using the Station form (page 4)		BUTTON ASSIGNMENTS 1. call-appr 2. call-appr etc.	Fill in the number of call appearances ("call-appr" buttons) to be supported for this deskphone. Use the following guidelines to determine the correct number: To support certain transfer and conference scenarios, the minimum number of "call-appr" buttons should be 3.

Table 10: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Stations With Off-PBX Telephone Integration form (page 1)	change off-pbx-telephone station-mapping ***xxxxxx*** where ***xxxxxx*** represents the extension number of the station being configured	Station Extension Application Dial Prefix Phone Number Trunk Selection Configuration Set	Use to map the Communication Manager extension to the same SIP Enablement Services call server extension. The Application is "OPS." Enter the other appropriate field values, for example, the Trunk Selection value indicates the SIP trunk group. The Configuration Set value can reference a set that has the default settings in Communication Manager.
Stations With Off-PBX Telephone Integration form (page 2)	change off-pbx-telephone station-mapping ***xxxxxx*** where ***xxxxxx*** represents the extension number of the station being configured	Call Limit	Change the call limit to match the number of "call-appr" entries in the Add Station form PLUS one. This setting should always be set to a minimum of three.

Administering Stations

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

Note:

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

Administering Features

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

The following buttons can be administered for a 9600 Series SIP IP Telephone, unless otherwise noted:

Administrable Station Features

Feature	Administration Notes
3-Way Conferencing	
6-Way Conference Bridge	
Audix One-Touch Recording	
Auto Callback/Cancel	This feature is not supported by SM 6.0/CM 6.0 when CM is administered as a feature server.
Auto Intercom	Add an intercom group # (in the Group, add your extension and dial code (DC), then add the other person's extension and DC. Add an auto-icom button, icom group #, DC.
Autodial	
Bridged Call Appearances	
Busy Indicator	
Call Appearances	
Call Forward (all)	
Call Forward Deactivation	
Call Forward Unconditional	
Call Forwarding (busy/ don't answer)	
Call Hold	
Call management (incoming, outgoing call screening)	
Call Park	
Call Unpark	Regardless of CM Station button administration, this feature will show on the Features menu automatically on SES and SM 5.2 configurations.
Call Pickup	
Call Pickup Group	
Call Pickup Extended Group	
Consultation Hold	
CPN Block	
CPN Unblock	

Administrable Station Features (continued)

Feature	Administration Notes
Dial Intercom	On CM: 1. Add an intercom group # (in the group, add your extension and dial code, then add other person's extension and dial code. 2. Add a dial-icom button, icom group #, (no dial code).
Directed Call Pickup	
Distinctive Alerting	
EC500 Enable/Disable	
EC500 Extend Call	
Exclusion	
Extended Call Pickup	Regardless of CM Station button administration, this feature will show on the Features menu automatically.
Find Me	
Last Number Dialed (Redial)	
Malicious Call Trace	
MCT Activation	Regardless of CM Station button administration, this feature will show on the Features menu automatically on SES configurations.
Message Waiting Indication	Not supported in CM5.2.1; supported in CM 6.0.
Music on Hold	
One Touch Recording	
Priority Call	
Send All Calls	
Transfer-to-Voicemail	Regardless of CM Station button administration, this feature will show on the Features menu automatically.
Transfer (Attended)	
Transfer (Unattended - one button transfer)	
Whisper Page	

For additional information about administering Avaya Communication Manager for 9600 Series SIP IP Telephones, see the following Avaya documents, available on the Avaya Support Web site:

- *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: Avaya Aura™ SIP Enablement Services (SES), Session Manager (SM), and System Manager Administration

Introduction

In addition to supporting three Avaya Aura™ Communication Manager configurations (as described in Avaya Aura™ Communication Manager Administration), SIP software Release 2.6 provides administrative flexibility by inter-operating with the following Avaya Aura products:

Avaya Aura™ SIP Enablement Services (SES) software resides on the Converged Communications Server (CCS). SES Release 5.2 works with Avaya Aura Communication Manager Release 5.2 to provide most of the features and functionality to SIP deskphones.

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

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

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

Avaya Aura™ SIP Enablement Services (SES) Administration

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

- I*nstalling the Avaya S8800 Server for Avaya Aura™ SIP Enablement Services* (Document Number 03-603447)
- *Maintaining the Avaya S8800 Server for Avaya Aura™ SIP Enablement Services* (Document Number 03-603448)
- I*nstalling, Administrating, Maintaining, and Troubleshooting Avaya Aura™ SIP Enablement Services* (Document Number 03-600768)
- *SIP Support in Avaya Aura™ Communication Manager* (Document Number 555-245-206)
- *Administering Avaya Aura™ SIP Enablement Services on the Avaya S8300 Server for Co-Residency* (Document Number 03-602508)
- *Avaya Aura™ SIP Enablement Services Implementation guide* (Document Number 16-300140)
- *SIP Personal Information Manager (SIP PIM)* (Document Number 03-300441)
- *Using Avaya Server Availability Management Processor (SAMP)* (Document Number 03-300322)
- SES Release notes

Avaya Aura™ System Manager Administration

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

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

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

Avaya Aura™ Session Manager Administration

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

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

Chapter 6: Server Administration

Software Checklist

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

Note:

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

DHCP and File Servers

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

The DHCP server provides the following information to the 9600 Series SIP IP Telephones:

- IP Address of the 9600 Series SIP IP Telephone(s)
- IP Address of the HTTP or HTTPS server
- IP Address of the NTP (Network Time Protocol) server (using Option 42)
- The subnet mask
- IP Address of the router
- DNS Server IP Address

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

Important:

An IP deskphone cannot function without an IP Address. The failure of a DHCP server at boot time leaves all the affected deskphones unusable. A user can manually assign an IP Address to an IP deskphone. When the DHCP server finally returns, the deskphone never looks for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process.

Avaya recommends that:

- A minimum of two DHCP servers be available for reliability.
- A DHCP server be available when the IP deskphone reboots.

- A DHCP server be available at remote sites if WAN failures isolate IP deskphones from the central site DHCP server(s).

A (HTTP or HTTPS) file server, which may run on the same physical computer as Communication Manager, provides the 9600 Series SIP IP Telephone with a 96xxupgrade.txt file and, if appropriate, new or updated binary software. See Step 4: Deskphone and File Server on page 27. You can edit the settings file (46xxupgrade.txt) to customize deskphone parameters for your specific environment. For more information, see Chapter 8: Administering Telephone Options.

DHCP Server Administration

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

Important:
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 for 9600 Series SIP IP Telephones

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

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

The following parameters for 96xx deskphones can be set in DHCP Option 242. Most of the same parameters can be set in a 46xxsettings.txt file as well, as described in Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters.

Table 11: Parameters Set by DHCP

Parameter	Description
HTTPDIR	Specifies the path to prepend to all configurations and data files the phone might request when starting up, i.e., the path, relative to the root of the HTTP file server, to the directory in which the deskphone configuration and date files are stored. The path may contain no more than 127 characters and may contain no spaces. If an Avaya file server is used to download configuration files over HTTPS, but a different server is used to download software files via HTTP, set the path of the Avaya server in the DHCP site-specific option, and set HTTPDIR again in the 46xxsettings.txt file with the appropriate path for the second server. HTTPDIR is the path for all HTTP operations. The command is "SET HTTPDIR=<path>". In configurations where the upgrade (96xxupgrade.txt) 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.
LOGSRVR	Syslog server IP or DNS address.
MTU_SIZE	Maximum transmission unit size. Used to accommodate older Ethernet switches that cannot support the longer maximum frame length of tagged frames (since 802.1Q adds 4 octets to the frame).
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 (auto-negotiate).
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 (auto-negotiate).
PROCPSWD	Security string used to access local procedures. The default is 27238.
PROCSTAT	Controls whether local procedures are enabled. The default is 0 (enabled).
SIP_CONTROLLER_LIST	SIP proxy/registrar server IP or DNS address(es). (0 to 255 characters; zero or one IP Address in dotted decimal or DNS name format, separated by commas without any intervening spaces.) The default is null.
SNTPSRVR	List of SNTP server IP or DNS address(es) used to retrieve date and time via SNTP
TLSDIR	Used as path name that is prepended to all file names used in HTTPS GET operations during initialization (0-127 character string).

Table 11: Parameters Set by DHCP (continued)

Parameter	Description
TLSPORT	Destination TCP port used for requests to https server (0-65535). The default is 443.
TLSSRVR	IP Address(es) or DNS name(s) of Avaya file server(s) used to download configuration files. **Note:** Transport Layer Security is used to authenticate the server.
VLANTEST	Number of seconds to wait for a DHCPOFFER on a non-zero VLAN. The default is 60 seconds.

DHCP Generic Setup

This section is limited to describing a generic administration that works with 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

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

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 SIP IP Telephones.
   - The following DHCP options:
     - **Option 1 - Subnet mask**.
       As described in Table 3, item 3.
     - **Option 3 - Gateway (router) IP Address(es)**.
       As described in Table 3, item 1. If using more than one address, the total list can contain up to 127 total ASCII characters. You must separate IP Addresses with commas with no intervening spaces.
     - **Option 6 - DNS server(s) address list**.
       If using more than one address, the total list can contain up to 255 total ASCII characters. You must separate IP Addresses with commas with no intervening spaces. At least one address in Option 6 must be a valid, non zero, dotted decimal address.
     - **Option 12 - Host Name**.
       Value is **AV*ohhhhhh***, where: o has one of the following values based on the OID (first three octets) of the deskphone's MAC address: "A" if the OID is 00-04-0D, "B" if the OID is 00-1B-4F, (SIP software Release 2.0+), "E" if the OID is 00-09-6E, "L" if the OID

is 00-60-1D, “T” if the OID is 00-07-3B, (SIP software Release R2.0+) and “X” if the OID is anything else, and where hhhhhh are ASCII characters for the hexadecimal representation of the last three octets of the deskphone’s MAC address.

- **Option 15 - DNS Domain Name**.
  This string contains the domain name to be used when DNS names in system parameters are resolved into IP Addresses. This domain name is appended to the DNS name before the 9600 IP Telephone attempts to resolve the DNS address. Option 15 is necessary if you want to use a DNS name for the HTTP server. Otherwise, you can specify a DOMAIN as part of customizing HTTP as indicated in DNS Addressing on page 128.
- **Option 42 - SNTP Server**.
  This option specifies a list of IP Addresses indicating NTP servers available to the deskphone. List servers in the order of preference.The minimum length is 4, and the length must be a multiple of 4.
- **Option 51 - DHCP lease time**.
  If this option is not received, the DHCPOFFER is not be accepted. Avaya recommends a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the IP Address lease is assumed to be infinite as per RFC 2131, Section 3.3, so that renewal and rebinding procedures are not necessary even if Options 58 and 59 are received. Expired leases cause Avaya IP Telephones to reboot. Avaya recommends providing enough leases so an IP Address for an IP deskphone does not change if it is briefly taken offline.

Note:

Regarding Option 51: The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP Address. If the network has problems and the only DHCP server is centralized, the server is not accessible to the given deskphone. In this case the deskphone is not usable until the server can be reached. 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. As Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters indicates, 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 sends an ARP Request for its own IP Address every five seconds. The request continues either forever, or until the deskphone receives an ARP Reply. After receiving an 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.

- **Option 52 - Overload Option, if desired**.
  If this option is received in a message, the deskphone interprets the **sname** and **file** fields in accordance with IETF RFC 2132,
  Section 9.3, listed in Other Documentation on page 18.

- **Option 53 - DHCP message type**.
  Value is 1 (DHCPDISCOVER) or 3 (DHCPREQUEST). As of Release 2.5, if a DHCPACK is received in response to a DHCPREQUEST sent to renew the deskphone's IP address lease, a log event record is generated with a Log Category of "DHCP". If a DHCPNAK is received in response to a DHCPREQUEST sent to renew the deskphone's IP address lease, the deskphone will immediately cease use of the IP address, a log event record will be generated, IPADD will be set to "0.0.0.0", and the deskphone will enter the DHCP INIT state.
-
- **Option 55 - Parameter Request List**.
  Acceptable values are:
  1 (subnet mask),
  3 (router IP Address[es])
  6 (domain name server IP Address[es])
  7 (log server)
  15 (domain name)
  26 (Interface MTU)
  42 (NTP servers)
  SSON (site-specific option number)
- **Option 57 - Maximum DHCP message size**.
  Release 2.5+ value is 1000; prior to R2.5, value was 576.
- **Option 58 - DHCP lease renew time**.
  If not received or if this value is greater than that for Option 51, the default value of T1 (renewal timer) is used as per IETF RFC 2131, Section 4.5, listed in Other Documentation on page 18.
- **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

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 9600 Series SIP Deskphones on page 93.

Avaya recommends that you administer DHCP servers to deliver only the options specified in this section and Table 11. 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***"

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.

In Table 12, the 9600 Series IP Telephone sets the system values to the DHCPACK message field values shown.

Table 12: DHCPACK Setting of System Values

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

Windows NT 4.0 DHCP Server

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**-->**Settings**-->**Control Panel**.
2. Double-click the **Network** icon.
3. Verify that **Microsoft DHCP Server** is listed as one of the Network Services on the **Services** tab.
4. If it is listed, continue with the next section. If it is not listed, install the DHCP server.

Creating a DHCP Scope for the IP Telephones

Use the following procedure to create a DHCP scope for the IP deskphones.

1. Select **Start**-->**Programs**-->**Admin Tools**-->**DHCP Manager**.
2. Expand **Local Machine** in the DHCP Servers window by double clicking it until the **+** sign changes to a **-** sign.
3. Select **Scope**-->**Create**.
4. Using information recorded in Table 3: Required Network Information Before Installation - Per DHCP Server:

   Define the **Telephone IP Address Range**.

   Set the **Subnet Mask**.

   To ***exclude*** any IP Addresses you do not want assigned to IP deskphones within the **Start** and **End** addresses range:

   a. In the **Exclusion Range Start Address** field, enter the ***first IP Address*** in the range that you want to exclude.

   b. In the **Exclusion Range End Address** field, enter the ***last IP Address*** in the range that you want to exclude.

   c. Click the **Add** button.

   d. Repeat steps a. through c. for each IP Address range to be excluded.

   Note:

   Avaya recommends that you provision the 9600 Series IP Telephones with sequential IP Addresses. Also do not mix 9600 Series IP Telephones and PCs in the same scope.

5. Under **Lease Duration**, select the **Limited To** option and set the ***lease duration*** to the maximum.

6. Enter a ***sensible name*** for the **Name** field, such as “CM IP Telephones," where CM would represent Avaya Communication Manager.
7. Click **OK**.

   A dialog box prompts you: `Activate the new scope now?`
8. Click **No**.

Note:

Activate the scope only after setting all options.

Editing Custom Options

Use the following procedure to edit custom options.

1. Highlight the newly created scope.
2. Select **DHCP Options**-->**Defaults** in the menu.
3. Click the **New** button.
4. In the **Add Option Type** dialog box, enter an appropriate custom option name, for example, “9600OPTION.”
5. Change the **Data Type Byte** value to **String**.
6. Enter **242** in the **Identifier** field.
7. Click the **OK** button.

   The **DHCP Options** menu displays.
8. Select the **Option Name** for 242 and set the *value string*.
9. Click the **OK** button.
10. For the **Option Name** field, select **003 Router** from the drop-down list.
11. Click **Edit Array**.
12. Enter the ***Gateway IP Address*** recorded in Table 3: Required Network Information Before Installation - Per DHCP Server for the **New IP Address** field.
13. Select **Add** and then **OK**.

Adding the DHCP Option

Use the following procedure to add the DHCP option.

1. Highlight the scope you just created.
2. Select **Scope** under **DHCP Options**.
3. Select the **242** option that you created from the **Unused Options** list.
4. Click the **Add** button.

5. Select option **003** from the **Unused Options** list.
6. Click the **Add** button.
7. Click the **OK** button.
8. Select the **Global parameter** under **DHCP Options**.
9. Select the **242** option that you created from the **Unused Options** list.
10. Click the **Add** button.
11. Click the **OK** button.

Activating the Leases

Use the following procedure to activate the leases.

- Click **Activate** under the **Scope** menu.

  The light-bulb icon for the scope lights.

Verifying Your Configuration

This section describes how to verify that the **96XXOPTIONs** are correctly configured for the Windows NT® 4.0 DHCP server.

Verify the Default Option, 242 96XXOPTION

1. Select **Start**-->**Programs**-->**Admin Tools**-->**DHCP Manager**.
2. Expand **Local Machine** in the DHCP servers window by double clicking until the **+** sign changes to a **-** sign.
3. In the DHCP servers frame, click the *scope* for the IP deskphone.
4. Select **Defaults** from the **DHCP_Options** menu.
5. In the **Option Name** pull-down list, select **242 96XXOPTION**.
6. Verify that the **Value String** box contains the correct string from DHCP Server Administration.

   If not, update the string and click the **OK** button twice.

Verify the Scope Option, 242 96XXOPTION

1. Select **Scope** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 96XXOPTION**.
3. Click the **Value** button.

4. Verify that the **Value String** box contains the correct string from DHCP Generic Setup on page 68.

   If not, update the string and click the **OK** button.

Verify the Global Option, 242 96XXOPTION

1. Select **Global** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 96XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct value from DHCP Generic Setup on page 68. If not, update the string and click the **OK** button.

Windows 2000 DHCP Server

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**-->**Program**-->**Administrative Tools**-->**Computer Management**.
2. Under **Services and Applications** in the Computer Management tree, find **DHCP**.
3. If DHCP is not installed, install the DHCP server. Otherwise, proceed directly to Creating and Configuring a DHCP Scope for instructions on server configuration.

Creating and Configuring a DHCP Scope

Use the following procedure to create and configure a DHCP scope.

1. Select **Start**-->**Programs**-->**Administrative Tools**-->**DHCP**.
2. In the console tree, click the *DHCP server* to which you want to add the DHCP scope for the IP deskphones. This is usually the name of your DHCP server machine.
3. Select **Action**-->**New Scope** from the menu.

   Windows displays the **New Scope Wizard** to guide you through rest of the setup.
4. Click the **Next** button.

   The **Scope Name** dialog box displays.
5. In the **Name** field, enter a name for the scope such as “CM IP Telephones” (where CM would represent Avaya Communication Manager), then enter a brief comment in the **Description** field.
6. When you finish Steps 1 - 5, click the **Next** button.

   The **IP Address Range** dialog box displays.
7. Define the range of IP Addresses used by the IP deskphones listed in Table 3: Required Network Information Before Installation - Per DHCP Server. The **Start IP Address** is the first IP Address available to the IP deskphones. The **End IP Address** is the last IP Address available to the IP deskphones.

Note:

Avaya recommends not mixing 9600 Series IP Telephones and PCs in the same scope.

8. Define the **subnet mask** in one of two ways:
   - The number of bits of an IP Address to use for the network/subnet IDs.
   - The subnet mask IP Address.

   Enter only one of these values. When you finish, click the **Next** button.

   The **Add Exclusions** dialog box displays.
9. Exclude any IP Addresses in the range specified in the previous step that you do not want assigned to an IP deskphone.
   a. In the **Start Address** field under **Exclusion Range**, enter the ***first IP Address*** in the range you want to exclude.
   b. In the **End Address** field under **Exclusion Range**, enter the ***last IP Address*** in the range you want to exclude.
   c. Click the **Add** button.
   d. Repeat steps a. through c. for each IP Address range that you want to exclude.

   Note:

   You can add additional exclusion ranges later by right clicking the **Address Pool** under the newly created scope and selecting the **New Exclusion Range** option.

   Click the **Next** button after you enter all the exclusions.

   The **Lease Duration** dialog box displays.
10. For all deskphones that obtain their IP Addresses from the server, enter **30 days** in the **Lease Duration** field. This is the duration after which the IP Address for the device expires and which the device needs to renew.
11. Click the **Next** button.

    The **Configure DHCP Options** dialog box displays.
12. Click the **No, I will activate this scope later** button.

    The **Router** (Default Gateway) dialog box displays.
13. For each router or default gateway, enter the ***IP Address*** and click the **Add** button.

    When you are done, click the **Next** button.

    The **Completing the New Scope Wizard** dialog box displays.
14. Click the **Finish** button.

    The new scope appears under your server in the DHCP tree. The scope is not yet active and does not assign IP Addresses.
15. Highlight the newly created scope and select **Action**-->**Properties** from the menu.

16. Under **Lease duration for DHCP clients**, select **Unlimited** and then click the **OK** button.

    CAUTION:

    IP Address leases are kept active for varying periods of time. To avoid having calls terminated suddenly, make the lease duration unlimited.

Adding DHCP Options

Use the following procedure to add DHCP options to the scope you created in the previous procedure.

1. On the DHCP window, right-click the **Scope Options** folder under the scope you created in the last procedure.

   A drop-down menu displays.

2. In the left pane of the DHCP window, right click the **DHCP Server name**, then click **Set Predefined Options...**.
3. Under **Predefined Options and Values**, click **Add**.
4. In the **Option Type Name** field, enter ***any appropriate name***, for example, “Avaya IP Telephones.”
5. Change the **Data Type** to **String**.
6. In the **Code** field, enter **242**, then click the **OK** button twice.

   The **Predefined Options and Values** dialog box closes, leaving the DHCP dialog box enabled.

7. Expand the newly created scope to reveal its **Scope Options**.
8. Click **Scope Options** and select **Action**-->**Configure Options** from the menu.
9. In the **General** tab page, under the **Available Options**, check the **Option 242** checkbox.
10. In the **Data Entry** box, enter the ***DHCP IP telephone option string*** as described in DHCP Generic Setup on page 68.

    Note:

    You can enter the text string directly on the right side of the **Data Entry** box under the ASCII label.

11. From the list in **Available Options**, check option **003 Router**.
12. Enter the ***gateway (router) IP Address*** from the IP Address field of Table 3: Required Network Information Before Installation - Per DHCP Server.
13. Click the **Add** button.
14. Click the **OK** button.

Activating the New Scope

Use the following procedure to activate the new scope.

1. In the DHCP console tree, click the **IP Telephone Scope** you just created.
2. From the **Action** menu, select **Activate**.

   The small red down arrow over the scope icon disappears, indicating that the scope was activated.

HTTP Generic Setup

You can store the binary file, 96xxupgrade.txt 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 DHCP and File Servers on page 65.

Note:

If you used TFTP to provide the binary, upgrade, and settings files to older Avaya IP telephones, note that 9600 Series IP 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 96xxupgrade.txt file and binary file(s) from the Avaya Web site http://www.avaya.com/support to the HTTP server. For more information, see Chapter 7: Telephone Software and Binary 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 7: Telephone Software and Binary Files

General Download Process

The 9600 Series SIP IP Telephones download upgrade files, settings files, language files, certificate files, and software files from a file server. All of the file types can be downloaded either via HTTP or HTTPS except the software files, which can only be downloaded via HTTP. Avaya recommends HTTPS for downloading the file types because it ensures the integrity of the downloaded file by preventing "man in the middle" attacks. Further, once the trusted certificates are downloaded into the deskphone, HTTPS ensures that the file server itself will be authenticated via a digital certificate. HTTPS is not used for software file downloads because 9600 Series IP Telephone software files are already digitally signed, so there is no need to incur additional processing overhead while downloading these relatively large files. The HTTPS protocol applies only if the server supports Transport Layer Security (TLS) encryption.

Note:

The 96xxupgrade.txt file, binary files, and settings files 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 Telephones might not contain the latest software. When the deskphone is first plugged in, it will attempt to contact a file server, and will download new software if the software version available on the file server is different than the version on the phone. For subsequent software upgrades, the call server provides the capability to remotely reset the deskphone, which then initiates the same process for contacting a file server.

The deskphone queries the file server, which transmits a 96xxupgrade.txt file to the deskphone. The 96xxupgrade.txt file tells the deskphone which binary file the deskphone must use. The binary file is the software that has the telephony functionality, and is easily updated for future enhancements. In a newly installed deskphone, the binary file might be missing. In a previously installed deskphone, the binary file might not be the proper one. In both cases, the deskphone requests a download of the proper binary file from the file server. The file server downloads the file and conducts some checks to ensure that the file was downloaded properly. If the deskphone determines it already has the proper file, the deskphone proceeds to the next step without downloading the binary file again.

After checking and loading the binary file, the 9600 Series SIP IP Telephone, if appropriate, uses the 96xxupgrade.txt file to look for a settings file. The settings file contains options you have administered for any or all of the IP Telephones in your network. For more information about the settings file, see Contents of the Settings File on page 86.

Software

As part of installation, a conversion from H.323 to SIP signaling protocol is done as described in "Converting Software on 9600 Series IP Telephones" of the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide.* When the deskphone is first plugged in, a software download from an HTTP or HTTPS server starts to give the phone its proper functionality.

For software upgrades, SIP Enablement Services (SES)/Session Manager (SM) provides the capability for a remote reboot of the 9600 Series SIP IP Telephones. As a result of a message from SES/SM, the deskphone automatically starts reboot procedures. If new software is available on the file server, the deskphone downloads it as part of the reboot process. The *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide* covers upgrades of a previously installed deskphone and related information.

9600 Series SIP IP Telephone Upgrade and Binary Files

Choosing the Right Binary File and Upgrade File

Every software release contains the files needed to operate the 9600 Series IP Telephones. Two software download "bundles" of files are available for use with 9600 Series IP Telephones. Which bundle you select depends on whether your deskphone environment is primarily SIP-centric or H.323-centric. When all or the majority of your IP deskphones are SIP-based, select the software download bundle for "9600 SIP Telephones" from the Avaya Support Web site. The SIP bundle contains a unique version of the 96xxupgrade.txt file that assumes SIP is the default protocol for your 9600 Series IP Telephones and that H.323 is the exception. For more information on SIP-centric environments, see "Converting Software on 9600 Series IP Telephones" in the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*.

Each SIP software bundle contains:

- An upgrade file, **96xxupgrade.txt**, which allows you to upgrade to the new software release. The 96xxupgrade.txt file tells the deskphone whether a software upgrade is needed. All Avaya IP Deskphones attempt to read this file whenever they reset. The upgrade file also causes the deskphone to download the 46xxsettings.txt file.
- A second upgrade file, **Alternate_96xxupgrade.txt**, which allows you to use both SIP and H.323 IP deskphones in the same environment. You only need this file if you also want some of your 9600 IP Telephones to run H.323 software. If so, use an ASCII text editor to read the directions in the file and to add the file names of the H.323 software files that you want to use. This file must then be saved as "96xxupgrade.txt" and will overwrite the 96xxupgrade.txt file originally provided in the bundle.

- Binary files with the latest SIP binary code for all current 9600 Series SIP IP Telephones.
- Language files that can be downloaded to the deskphones containing the language name (as it should be presented to a user for selection), an indication of the preferred character input method, text string replacements for the built-in English text strings, where each replacement string may contain up to 120 characters, and each has a unique index that associates it with the corresponding built-in English string, an indication as to whether Chinese, Japanese or Korean glyphs should be displayed for the Unicode “Unified Han” character codes, and a Language Identification Tag for the language of the text contained in the file. A downloadable language file may also contain a translation of the language name into any or all of the languages for which a language file is included in the software distribution package.
- Avaya Certificate Authority (CA) certificate files that can be downloaded to the deskphones when the TRUSTCERTS parameter is used to specify the Certificate Authorities that are to be trusted by the deskphones. The Avaya SIP CA certificate file can also be used on an Authentication Server to authenticate the default device certificate built into the deskphones when 802.1X EAP-TLS is being used for network access security.
- Extended Korean ring tones xml files.
- Other useful information such as a ReadMe file.

Each software bundle comes in one or more formats. Download the appropriate software bundle to your file server from the Avaya support Web site at: http://www.avaya.com/support. Note that all files must reside in the same directory on your file server.

Upgrade File (96xxupgrade.txt)

The **96xxupgrade.txt** file tells the IP deskphone whether the deskphone needs to upgrade its software. The 9600 Series SIP IP Telephones attempt to read this file on the file server whenever they reset. This file allows the deskphone to use default settings for customer-definable options. The 96xxupgrade.txt file also points to the Settings File, where you can set provide values to override the default values for any settings you want to customize for your specific environment.

The 96xxupgrade.txt file is part of the software bundle you download from http://www.avaya.com/support.

An "alternate" upgrade file (Alternate_96xxupgrade.txt) is included in the SIP software bundle, designed for environments that will support both the H323 and SIP modes of operation. For such environments, the file needs to be edited in those sections having headings of “H.323 EDIT INSTRUCTIONS.” Specific instructions are provided in the Readme file that accompanies the software bundle. Once these changes are made, the alternate file should be renamed to “96xxupgrade.txt” and placed in the HTTP download directory. The HTTP download directory holds the deskphone backup and application software binaries the deskphone will download. Renaming the alternate file causes any “96xxupgrade.txt” files residing in that directory to be overwritten.

Settings File

The settings file contains the parameters that you can use to customize the Avaya IP Telephones for your enterprise.

Note:

Avaya recommends that the settings file have the extension ***.txt**. The Avaya IP Telephones can use Avaya-provided default values and operate without this file if you have no settings you want to customize. Note that you can also change these settings with DHCP (for information see Configuring DHCP for 9600 Series SIP IP Telephones) or, in some cases, from the dialpad of the deskphone using local administrative (Craft) procedures described in the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*.

Note:

Use one settings file for all your Avaya IP Telephones. The settings file includes the 9600 Series SIP IP Telephones covered in this document. The settings file also includes parameters for 9600 Series (H.323) IP Telephones, 4600 Series IP Telephones, and 1600 Series IP Telephones as covered in their respective administrator guides.

The settings file can include five types of statements, one per line. Any invalid statement is ignored. The statement types are:

- SET statements of the form **SET *parameter_name value***. If the desired value contains a blank or a comma, the entire value must by placed within double quotes.
- GET statements of the form **GET *filename***, which cause the phone to get the named file from the same file server and directory from which it got the current file. If the file is not available, the phone continues to execute the current file.
- GOTO statements, of the form **GOTO *tag***. GOTO statements cause the deskphone to continue interpreting the configuration file after a line that begins with a "**# tag**" statement. If no such line exists in the upgrade or settings file after the GOTO, the phone ignores anything in the file after the GOTO.
- Tags are lines that begin with a # tag; tag is an unquoted string and cannot contain a space or comma.
- IF statements, of the form **IF $*name SEQ string* GOTO *tag***, where name is one of the system parameters shown in table #A#. Conditionals cause the GOTO command to be processed if the (string equivalent) value of name is equal to string. Note that the string comparison ignores case, so "Abc" matches "ABC" or "abc". If no such name exists, the entire conditional is ignored. As for SET statements, the string must be included in double quotes if it includes spaces or commas. Any string may be double quotes, so 1 and "1" are equivalent as are "abc" and abc.

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

Table 13: Settings File System Parameters That Can Be Tested in an IF Statement

Parameter	Description
BOOTNAME	The name of the boot code file in the deskphone.
MACADDR	MAC address of the phone (hh:hh:hh:hh:hh:hh; automatically supplied by a phone).
MODEL	Telephone Model identifier (8 ASCII characters; automatically supplied by a phone).
MODEL4	The first four digits of the model identifier (automatically supplied by a phone).
PWBCC	Avaya identification number for the printed circuit board (automatically supplied by a phone).
GROUP	Group identifier (must be manually set on a phone)
SIG	Signalling protocol identifier (2=SIP, 1=H.323, 0=default; must be manually changed on a phone).

The ***96xxupgrade.txt*** files distributed by Avaya start with a ***GOTO GETSET*** command based on the value of the SIG parameter to preclude loading SIP software into a phone that has been manually designated to run H.323 software (indicated by a SIG value of 1), and to preclude loading H.323 software into a phone that has been manually designated to run SIP software (indicated by a SIG value of 2). The default SIG value of zero indicates that the deskphone should download whatever software is available.

The ***96xxupgrade.txt*** files distributed by Avaya end with the statement ***GET 46xxsettings.txt.*** If you need to redefine the values of any parameters for your installation, do so in the ***46xxsettings.txt*** file and not in the ***96xxupgrade.txt*** file. The reason for using the 46xxsettings.txt file is because each new Avaya release you download will include a new version of ***96xxupgrade.txt***, which will overwrite any changes you have made to your previous copy of that file.

Avaya recommends that you do **not** alter the 96xxupgrade.txt file. If Avaya changes the 96xxupgrade.txt file in the future, any changes you have made will be lost. Avaya recommends that you use the ***46xxsettings*** file to customize your settings instead. However, you can change the settings file name, if desired, as long as you also edit the corresponding **GET** command in the 96xxupgrade.txt file.

For more information on customizing your settings file, see Contents of the Settings File.

Contents of the Settings File

The final step in processing the 96xxupgrade.txt file is to GET the 46xxsettings.txt file. The default 46xxsettings.txt file contains explanatory material and default values on lines that start with ##. A parameter value can be changed and actioned by changing its value and removing the two ##'s at the beginning of the line.

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

```
##
##
## Define the Domain Name Server to be "dns.example.yourco.com"
## Note that quotes are only needed for parameters that contain
  spaces.
##
SET DNSSRVER dnsexample.yourco.com
##
##
## SIP Proxy/Registrar servers list
##  SIP_CONTROLLER_LIST provides ability to configure SIP Proxy/
  Registrar list.
##  The format is host[:port];[transport:xxx]. A comma seperated
  list in this
##  format can be provided. Host can be DNS name or IP address. Port
  is optional.
##  If port is not specified then default value of 5060 for TCP and
  UDP and 5061 for
##  TLS will be used. Transport type is optional. It can be tcp or
  udp or tls.
##  Default value of tls will be used if it is not provided.
SET SIP_CONTROLLER_LIST proxy1,proxy2:5070;transport=udp
##
##
## 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 Telephone LAN
##  Admin Guide for format and setting alternatives.
SET GMTOFFSET "-6:00"
##
##
##  DSTOFFSET sets the daylight savings time adjustment
##  value. The default is 1 but valid values are 0, 1, or 2.
## SET DSTOFFSET "1"
##
##
##  DSTSTART sets the beginning day for daylight savings
##  time. See the 9600 Series
##  SIP Telephone LAN Admin Guide for format and setting
```

```
##  alternatives.
## SET DSTSTART  "2SunMar2L"
##
##  NOTE:
##  The default DSTSTART and DSTSTOP parameters reflect the
##  new 2007 Daylight Savings Time values for North America
##
##  DSTSTOP sets the ending day for daylight savings time.
##  See SIP 9600 Series IP Deskphones Customizeable System
  Parameters for format and setting alternatives.
## SET DSTSTOP   "1SunNov2L"
##
------------------------------
```

See Chapter 8: Administering Telephone Options for details about specific values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

VLAN separation controls whether or not traffic received on the secondary Ethernet interface is forwarded on the voice VLAN and whether network traffic received on the data VLAN is forwarded to the deskphone. Add commands to the 46xxsettings.txt file to enable VLAN separation. The following three lines will enable VLAN separation when the data VLAN ID is "yyy" and the data traffic priority is "z":

- Enable VLAN separation by setting the parameter to 1: `SET VLANSEP "1"`
- Define the data VLAN ID (for any computer connected to the second ethernet port on the phone) to be 'yyy': `SET PHY2VLAN "yyy"`
- Define the priority of the data traffic to be 'z': `SET PHY2PRIO "z"`

Note:

When the configuration parameter VLANSEP is set to "1" you should configure the network switch so that 802.1Q tags are not removed from frames forwarded to the deskphone.

The GROUP System Value

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 system value for this purpose:

1. identify which deskphones are associated with which group, and designate a number for each group. The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group is assigned as Group 0.
2. At each non-default deskphone, instruct the installer or user to invoke the GROUP Craft Local procedure as specified in the *Avaya one-X™ Deskphone Edition for 9600 SIP IP Telephones Installation and Maintenance Guide* and specify which GROUP number to use. The GROUP System value can only be set on a phone-by-phone basis.
3. Once the GROUP assignments are in place, edit the configuration file to allow each deskphone of the appropriate group to download its proper settings.

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

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

##

IF $GROUP SEQ 1 goto GROUP1

##

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

##

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

# GROUP1

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

# GROUP2

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

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

Chapter 8: Administering Telephone Options

Administering Options for the 9600 Series SIP Deskphones

This chapter explains how to change parameters to customize them for your operating environment. In all cases, you are setting a system parameter in the deskphones to a desired value. Table 14 lists:

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

Table 11 is a comprehensive list of all the parameters you can configure. However, you do not have to set every parameter. In most cases, you will include only those parameters in the settings file that are specific to your own environment and let the deskphones use the default values for the remaining ones.

Note:

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

For DHCP, the DHCP Option sets certain parameters to the desired values as discussed in DHCP and File Servers on page 65. For HTTP, the parameters in Table 14 are set to desired values in the script (46xxsettings) file. For more information on working with the settings file, see Contents of the Settings File on page 86.

Avaya recommends that you administer options on the 9600 Series SIP IP Telephones using script files. This is because some DHCP applications have limits on the amount of user-specified information. The administration required can exceed those limits for the more full-featured deskphone models.

Some parameters can be changed using the deskphone dialpad. For example, you might choose to completely disable the capability to enter or change option settings from the dialpad using local administrative (Craft) procedures. You can set the system value, PROCPSWD, as part of standard DHCP/HTTP administration. If PROCPSWD is non-null and consists of 1 to 7 digits, a user cannot invoke any local options without first entering the PROCPSWD value on the Craft Access Code Entry screen. For more information on craft options, see the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*.

Important:

PROCPSWD is likely stored on the server “in the clear” and is sent to the deskphone in the clear. Therefore, do not consider PROCPSWD as a high-security technique to inhibit a sophisticated user from obtaining access to local procedures.

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

Note:

There are several ways to change configuration parameters, for example, using DHCP options, the 46xxsettings file, or using local administrative (manual) procedures, and a specific procedure exists to determine which value the deskphone should use. Parameter Data Precedence on page 22 describes the order in which parameter values are determined.

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters

Parameter Name	Default Value	Description and Value Range
AGCHAND	1	Automatic Gain Control status for handset. Values are 0=disabled, 1=enabled.
AGCHEAD	1	Automatic Gain Control status for headset. Values are 0=disabled, 1=enabled.
AGCSPKR	1	Automatic Gain Control status for speaker. Values are 0=disabled, 1=enabled.
AMADMIN	" " (Null)	URI for obtaining the Avaya (A) menu administration file. If null, a file for administration of A(vaya)-menu will not be downloaded. Otherwise, this parameter defines the URI that points to the location where the A(vaya)-menu administration file can be obtained. Valid values are: zero to one URI in the default length character string.
ASTCONFIRMATION	32	The time in seconds that the phone waits to validate an active subscription when it SUBSCRIBEs to the "avaya-cm-feature-status" package. 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. Values range from 0 through 191.

1 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
AUDIOSTHD	0	Headset sidetone setting. Values are: 0 = Default; no change; 16dB STMR. 1 = Three steps softer than nominal; 24dB STMR. 2 = Off; inaudible; 36dB STMR. 3 = One level softer than nominal;19dB STMR. 4 = Two steps softer than nominal; 21dB STMR. 5 = Four steps softer than nominal; 27dB STMR.
AUDIOSTHS	0	Handset sidetone setting. Values are: 0 = Default; no change; 16dB STMR. 1 = Three steps softer than nominal; 24dB STMR. 2 = Off; inaudible; 36dB STMR. 3 = One level softer than nominal;19dB STMR. 4 = Two steps softer than nominal; 21dB STMR. 5 = Four steps softer than nominal; 27dB STMR.
AUTH	0	Authentication flag for settings file download. Values are: 0=secure setting file download is not required 1=secure setting file download is required
AUTO_SELECT_ANY_IDLE_APPR	0	Automatically select any idle call appearance for conference or transfer. Valid values are: 0 = Active; if CONF_TRANS_ON_PRIMARY_APPR is 0, then if no associated call appearance is selected, the conference or transfer operation will be denied. 1 = Not Active; if CONF_TRANS_ON_PRIMARY_APPR is 0, then if no associated call appearance is selected, the conference or transfer operation will be tried on any available call appearance (primary or bridged).
BAKLIGHTOFF	120	Number of minutes without display activity to wait before turning off the backlight. Values range from zero (never turn off) through 999 minutes (16.65 hours).
CALL_TRANSFER_MODE	0	When ENABLE_AVAYA_ENVIRONMENT=0, this parameter indicates how transfers are performed: 0 = attended transfer 1 = unattended transfer
CALLFWDADDR	" " (Null)	The URI to which calls are forwarded in failover.
CALLFWDDELAY	1	Failover environments only. Specifies the number of ring cycles generated at the phone before the call is forwarded to the Call Forwarding Address, if call forwarding on "No answer" is selected in failover. Valid number of ringing cycles are 0-20.

2 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

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. Valid values are: 0 = no Call Forwarding permitted. 1 = Call Forward Unconditional only permitted. 2 = Call Forward Busy only permitted. 4 = Call Forward No Answer only permitted. Others = sum of Call Forward types permitted.
CNAPORT	50002	Transport-layer port number to be used for registration to CNA server for network analysis. Valid range is 0-65535.
CNASRVR	" " (Null)	List of CNA server IP or DNS address(es). Used to connect to CNA server for network analysis (in case of several entries first address always first, etc.). Format is 0 to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. Currently set to a maximum of 5 servers.
CNGLABEL	1	Indicates whether end user can personalize button labels. Valid values are: 0=User cannot change button labels 1=User has ability to change button labels
CONF_TRANS_ON_ PRIMARY_APPR	0	Conference or Transfer operations will seek to use a primary call appearance only if initiated from a primary appearance. From a bridged appearance, conference or transfer operations will only be made from another idle bridged appearance. If no appearance is available, the operation will be denied. Valid values are: 0 = Active 1 = Not Active; overrides the AUTO_SELECT_ANY_IDLE_APPR parameter
CONFIG_SERVER_ SECURE_MODE	0 (R2.5 & earlier) 1 (Release 2.6+)	Indicates whether or not secure communication via HTTPS is required to access the configuration server. 0 = Use HTTP. 1 = Use HTTPS.
CONTROLLER_SEARCH_ INTERVAL	4	Time in seconds that the phone waits to complete the maintenance check for monitored controllers. Valid values are 4 - 3600 (seconds).

3 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

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.
CNAPORT	50002	Transport-layer port number. Port to be used for registration to CNA server for network analysis. Valid values are 0 – 65535.
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.
CURRENT_CONTENT	" " (Null)	Defines the URL of the customization file for the Home Screen. Range is the default string length of the URL.
CURRENT_LOGO	" " (Null)	Defines the selected background logo on display, if any. Indicates if a custom logo is currently selected (non-empty string) or a built-in default logo is used (empty string or not set). If a custom logo is selected (non-empty string), this value points to the corresponding logo resource definition as defined in LOGOS configuration parameter.
CURRENT_SKIN	" " (Null)	Defines if a custom skin is currently selected (non-empty string) or built-in default skin is used (empty string or not set). If a custom skin is selected (non-empty string), this value points to the corresponding skin resource definition (i.e. contains a label as defined in "SKINS" configuration parameter). Can also be set by the end user via Avaya Menu Screen & Sounds option.
DATEFORMAT	%m/%d/%y	Formatting string defining how to display the date in the top line and the call log.
DAYLIGHT_SAVING_ SETTING_MODE	2	Controls daylight saving setting. Values are: 0=daylight saving time is deactivated (no offset to local time) 1=daylight saving time is activated (offset to local time as configured in "DSTOFFSET") 2=the device switches automatically to daylight saving time and back according to the contents of "DSTSTART" and "DSTSTOP"

4 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DHCPSTD	0	DHCP Standard lease violation flag. Indicates whether to keep the IP Address if there is no response to lease renewal. If set to “1” (No) the deskphone strictly follows the DHCP standard with respect to giving up IP Addresses when the DHCP lease expires. If set to “0” (Yes) the deskphone continues using the IP Address until it detects reset or a conflict (see DHCP Generic Setup).
DIALPLAN	" " (Null)	Dial plan for operation with a secondary controller. The DIALPLAN parameter is used to determine one or more valid dialstrings. Valid value is 0 to 1023 characters that define the dial plan. See Setting the Dial Plan on SIP IP Telephones for more information.
DISCOVER_AVAYA_ ENVIRONMENT	1	Allows the phone to discover whether it is in an Avaya environment where SIP AST features are supported. Valid values are: 0=Non-Avaya environment; do not auto-discover AST support 1 = Avaya environment; auto-discover AST support. The SIP proxy server (controller) may or may not support AST.
DISPLAY_NAME_ NUMBER	0	Indicates whether the calling party’s number will be displayed next to the caller name on an incoming call. If this parameter is not set, only the caller name is shown. Valid values are: 1 = Show caller’s name and number. 0 = Show caller’s name only.
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 system 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 PAE multicast pass-through, but without proxy Logoff. 1= Unicast Supplicant operation only, with PAE multicast pass-through and proxy Logoff. 2= Unicast or multicast Supplicant operation, without PAE multicast pass-through or proxy Logoff.

5 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DOT1XEAPS	MD5	Specifies the EAP authentication method(s) to be used with IEEE 802.1X. Comma-separated list of key words defining EAP methods. In SIP Release 2.0, this value is restricted to a single EAP method. Valid values are either "MD5" or "TLS".
DOT1XSTAT	0	IEEE 802.1X status. Enables/disables IEEE 802.1X function and, if enabled, additionally defines reaction on received multicast or unicast EAPOL messages. Valid values are: 0 = Supplicant operation disabled. 1 = Supplicant operation enabled, but responds only to received unicast EAPOL messages. 2 = Supplicant operation enabled, responds to received unicast and multicast EAPOL messages.
DSCPAUD	46	Differentiated Services Code Point for audio. Values range from 0 to 63.
DSCPSIG	34	Differentiated Services Code Point for signaling. Values range from 0 to 63.
DSTOFFSET	1	Used for daylight saving time calculation in hours. Values range from 0 to 2.
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)

6 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

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_AVAYA_ ENVIRONMENT	1	SIP operational mode. Range is 0-1. Can also be set via local Craft procedure. Valid values are: 0 = Standard SIP proxy mode (3rd party SIP proxy environment). If set to 0, the phone operates in a mode to comply with 3rd party standard SIP proxy (provision of SIPPING 19 feature). 1 = SIP/AST proxy mode (Avaya SES/PPM environment). If set to 1, the phone operates in Avaya environment mode (provision of SIP/AST features and use of PPM for download and backup/restore).
ENABLE_CALL_LOG	1	Enable or disable complete Call Log application. If disabled no calls are logged, screens related to Call Log are not displayed to user, and menu items of User Interface to set Call Log options are not displayed. Values are 0=disabled; 1=enabled.
ENABLE_CONTACTS	1	Enable or disable complete Contact application. If disabled no contacts are downloaded during initialization from PPM, screens related to Contacts application are not displayed to user, and menu items of the User Interface to set Contacts options are hidden. Values are 0=disabled; 1=enabled.

7 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
ENABLE_EARLY_MEDIA	1	Flag that indicates if SIP early is enabled. If enabled and 18x progress message includes early SDP, Spark uses that information to open a VoIP channel to the far-end before the call is answered. Values are 0=disabled; 1=enabled.
ENABLE_EXCHANGE_ REMINDER	0	Enables popup reminder notifications for Microsoft Exchange calendaring. Values are: 0 = No (Off) 1 = Yes (On).
ENABLE_G711A	1	Enable or disable G711A codec capability of the phone. If the parameter is set to 1, the phone includes G711A capability in an outbound INVITE request, and accepts G711A when received in an incoming INVITE request. Values are 0=disabled; 1=enabled.
ENABLE_G711U	1	Enable or disable G711U codec capability of the phone. If the parameter is set to 1, the phone includes G711U capability in an outbound INVITE request, and accepts G711U when received in an incoming INVITE request. Values are 0=disabled; 1=enabled.
ENABLE_G722	0	Enable or disable G722 capability of the deskphone. If the parameter is set to 1, the phone includes G722 capability in an outbound INVITE request, and accepts G722 when received in an incoming INVITE request. If set to 0, processing of G722 as a capability is disabled. Values are 0=disabled, off; 1=enabled, on.
ENABLE_G726	1	Enable or disable G726 capability of the deskphone. If the parameter is set to 1, the deskphone includes G726 capability in an outbound INVITE request, and accepts G726 when received in an incoming INVITE request. Values are 0=disabled, off; 1=enabled, on.

8 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
ENABLE_G729	1	Enable or disable G729A codec capability of the phone. Values are: 0=G.729 disabled. If set to 0, processing of G729A as a capability is disabled. 1 = The phone advertises a preference for "G.729(A) enabled, without Annex B support" in an outbound INVITE request, and accepts either G729A or G729A with annex B support [G.729AB] when received in a 200OK response or an incoming INVITE request. If set to 1, Incoming INVITE request: the phone accepts either G729(A) or G729AB. 2 = The phone advertises a preference for "G.729(A) enabled, with Annex B support [G.729AB]"in an outbound INVITE request, and accepts either G729A or G729AB when received in a 200OK response or an incoming INVITE request. If the parameter is set to 2, Incoming INVITE request: the phone accepts either G729A or G729AB.
ENABLE_MODIFY_ CONTACTS	1	Enable or disable the ability to modify contacts if the Contact application is enabled. Values are 0=disabled; 1=enabled.
ENABLE_PHONE_LOCK	0	Enables the local Phone Lock feature. Values are: 0 = Lock Softkey and Feature Button are not displayed. 1= Lock Softkey and Feature Button are displayed
ENABLE_PRESENCE	0	Enable or disable complete Presence functionality. If disabled, Presence icons do not show in Contacts or Call History Lists, Presence is not displayed to the user, incoming Presence updates are ignored, and menu items of User Interface to set Presence options are not displayed (if available). Values are 0=disabled, off; 1=enabled, on.
ENABLE_PPM_ SOURCED_ SIPPROXYSRVR	1	Enables PPM as a source of SIP proxy server information. Valid values are: 0 = Do not use PPM as a source for SIP proxy server information. 1 = Use PPM for SIP proxy server information.
ENABLE_REDIAL	1	Enable or disable complete Redial functionality. If disabled pressing the redial button has no effect and the redial softkeys and menu items are not displayed. Values are 0=disabled; 1=enabled.

9 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
ENABLE_REDIAL_LIST	1	Enables or disables the capability to redial out of a list of recently dialed numbers instead of performing last number redial. Values are 0=disabled (last number redial only is offered to the user); 1=enabled (user can select either last number redial or redial from a list).
ENABLE_REMOVE_ PSTN_ACCESS_PREFIX	0	Enables the removal of the PSTN access prefix from collected dial strings when the phone is communicating with a non-AST controller.Valid values are: 0 = PSTN access prefix digit is not removed; 1 = PSTN access prefix digit is removed from collected digit string before formulating the INVITE for delivery to the controller. (Enabling this parameter when the phone is communicating with an AST-capable controller has no effect).
ENABLE_SERVER_ BASED_PRESENCE	1	Activates/deactivates server based presence. If set to 1 (Enabled), a subscription to presence list and watcher info is done. If set to 0 (Disabled), individual presence subscriptions are done separately to every contact (buddy) from the contact list.
ENABLE_SIP_USER_ID	0	Activates/deactivates the User ID field on the Login screen. Valid values are: 0=disabled; 1=enabled. If set to 0, user does not see the User ID field on the Login Screen. If set to 1, the user is prompted for the User ID.
ENFORCE_SIPS_URI	1	Controls the enforcement of SIPS URI with SRTP. Valid values are: 0 = Allow either SIP URI or SIPS URI for incoming SRTP media encryption calls and use only SIP URI for outgoing SRTP media encryption calls. 1 = Accept and use only SIPS URI for incoming and outgoing calls with SRTP media encryption.
ENHDIALSTAT	1	Enhanced Dialing Status. Valid range is 0 to 2. If set to “0” the feature is turned off. If set to “1” it is partially enabled (dialing rules do not apply for dialing from Contacts). If set to “2”, the Enhanced Local Dialing feature is fully enabled (dialing rules also apply for dialing from Contacts). Note that If CTDC_SUPPORT is enabled, Enhanced Local Dialing is automatically disabled, independent of the actual setting of ENHDIALSTAT. If CTDC_SUPPORT is disabled, Enhanced Local Dialing is processed as defined by ENHDIALSTAT.

10 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
EXCHANGE_NOTIFY_ SUBSCRIPTION_ PERIOD	3600	Used to administer how long in seconds the phone re-syncs with the Exchange Server. Values are: 0 to 3600 (seconds).
EXCHANGE_REMINDER_ TIME	5	Used to administer how far in advance to remind users of an appointment on their Microsoft Exchange calendar. Values are: 0 to 60 (minutes)
EXCHANGE_REMINDER_ TONE	1	Used to indicate whether a tone should accompany a calendar reminder or not. Values are: 0 = No (Off) or 1 = Yes (On).
EXCHANGE_SERVER_ LIST	" " (Null)	List of Microsoft Exchange™ server IP or DNS addresses. Used to connect to Microsoft Exchange™ server, for example, to access contacts or calendar data (in case of several entries, the first address is always first, etc.). 0 to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.
EXCHANGE_SNOOZE_ TIME	5	Used to administer how long in minutes for the calendar reminder (as set in ENABLE_EXCHANGE_REMINDER and EXCHANGE_REMINDER_TIME to reappear after it has been snoozed (temporally dismissed) by the user. Values are: 0 to 60 (minutes).
EXCHANGE_USER_ DOMAIN	" " (Null)	User domain (URL) for Microsoft Exchange™ Server. Range is the default URL string length.
EXTEND_RINGTONE	" " (Null)	Represents a list of xml files, each representing custom ring tone information. Alternate ring tones to replace the standard Avaya ring tones. As of SIP software Release 2.4, Korean ring tones are available as is the ability to specify custom ring tones, as described in Customizing Ring Tones. A string up to 1023 characters containing up to 8 alternate ring tones in the format *Ringtone1*.xml, *Ringtone2*.xml, or KoreanRT1.xml, KoreanRT2.xml, etc.
FAILBACK_POLICY	"auto"	The policy in effect for recovery from Failover. Valid values are: "admin" = If set to admin, the phone waits for administrative intervention before attempting to failback to a higher priority controller. "auto" = If set to auto, the phone periodically checks the availability of the primary controller and fails back to it if it is available. Note: If set via the settings file this value is given a precedence of 4. If set via PPM in the ListOfMaintenanceData element of the getAllEndpointConfigurationResponse this value is given a precedence of 5.

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
FAILED_SESSION_ REMOVAL_TIMER	30	Timer to automatically remove a failed call session. Range in seconds is 5 to 999.
FAST_RESPONSE_ TIMEOUT	4	The value of the Fast Response Timer for Failover. Valid values are: 0 - 32 (seconds). Note: If set via the settings file this value is given a precedence of 4. If set via PPM in the ListOfMaintenanceData element of the getAllEndpointConfigurationResponse this value is given a precedence of 5.
G726_PAYLOAD_TYPE	110	RTP dynamic payload used for G.726. Range is 96 to 127.
GMTOFFSET	0:00	Offset used to calculate time from GMT reference time. Default string length positive or negative number of hours and minutes less than 13 hours. Consists of 1 to 6 characters, optionally beginning with "+" or "-", followed by one or two number digits whose combined value is from "0" to "12" optionally followed by a ":" and two numeric digits whose combined value is from "00" to "59".
GROUP	0	Specific user group as tested in configuration files. Valid values are 0 to 999.
HEADSYS	1	Headset operational mode. One ASCII numeric digit. Valid values are: 0 or 2=General Operation, where a disconnect message returns the deskphone to an idle state. 1 or 3=Call Center Operation, where a disconnect message does not change the state of the deskphone.
HTTPDIR	" " (Null)	HTTP server directory path. The path name prepended to all file names used in HTTP and HTTPS get operations during initialization/HTTP downloads. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required. The command syntax is “GET HTTPDIR *myhttpdir*” where “myhttpdir” is your HTTP server path. HTTPDIR is the path for all HTTP operations.
HTTPEXCEPTION DOMAINS	" " (Null)	Domains to be excluded for SCEP. String representing zero or one domains in a URL of 0 to 255 characters in dotted decimal or DNS name format with multiple domains delimited by commas.
HTTPPORT	80	Destination TCP port used for requests to the HTTP server during initialization. Range is 0 - 65535.

12 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

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

13 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

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.
LANGUAGES	" " (Null)	List of links to language files to be downloaded. Substrings are delimited by commas. Maximum length is 1023 characters. Each substring shall follow one of the these naming rules: A substring is identical to a file name without any prefix specifying the path or server: The files are downloaded from the same source as the setting file(s). A substring can provide a prefix to the file name, which specifies the relative path ("./" for next higher directory level) from the directory the settings file(s) has been downloaded to the directory the language file shall be download. A substring specifies the completed URL to the language file including protocol identifier ("http://" or "https://"), server and path.
LLDP_ENABLED	2	Flag to enable/disable LLDP (Link Layer Discovery Protocol). Valid values are: 0 = disabled; the deskphone will not support LLDP. 1 = enabled; the deskphone will support LLDP. 2 = auto; the deskphone will support LLDP, but the transmission of LLDP frames will not begin until or unless an LLDP frame is received.
LOCAL_DIAL_AREA_CODE	0	Indicates whether user has to dial the area code for calls within the same area code. Valid values are: 0 = User does not need to dial local area code. 1 = User must dial the area code for local calls.

14 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

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

15 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
MSGNUM	" " (Null)	Voice mail system telephone/extension number. Used for non-failover situations. Specifies the number to be dialed automatically when the deskphone user presses the **Message** button. Note: Set via the following mechanisms in precedence order (highest to lowest); For Release 2.6+- PPM, settings file and DHCP. For Release 2.5 - settings file and DHCP.
MTU_SIZE	1500	Maximum Transmission Unit size. Range is 1496 or 1500 only octets.
MWISRVR	" " (Null)	List of Message Waiting Indicator Event Server IP or DNS address(es). Used to register for MWI event notifications (in case of several entries first address always first, etc.). In some third-party proxy environments the SIP proxy/registrar may be different than the MWI server. In this case, the MWI server is set via this parameter. If both functions are provided by the same server, it is not necessary to set MWISRVR. The SIP proxy server (controller) is then used for MWI indications. Zero to 255 characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. if operating in a non-Avaya environment, this value is set via a SET command in the settings file, otherwise the address of SIP Proxy server (controller) is used.
MYCERTCAID	CAIdentifier	Certificate Authority Identifier. String identifying whether the endpoints can work with another certificate authority.
MYCERTCN	$SERIALNO	Common name (CN) for SUBJECT in SCEP certificate request. Values are: $SERIALNO = the phone's serial number is included as CN parameter in the SUBJECT of a certificate request. $MACADDR = the phone's MAC address is included as CN parameter in the SUBJECT in the certificate request.
MYCERTDN	" " (Null)	Common part of SUBJECT in SCEP certificate request. String which defines the part of SUBJECT in a certificate request (including Organizational Unit, Organization, Location, State, Country), of 0 to 255 characters, starting with / and separating items with /.
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.

16 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

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

17 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
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".
PHNLDLENGTH	10	Length of national telephone number. The number of digits in the longest possible national telephone number. Range: 5 to 15. Needed to for "Enhanced Local Dialing Algorithm".
PHNOL	9	Outside line access code. The character(s) dialed, including # and *, if any, to access public network local trunks. Range: 0-2 dialable numeric digits, including " " (Null).
PHNNUMOFSA	" " (Null)	When ENABLE_AVAYA_ENVIRONMENT=0, this value sets the number of Session Appearances.
PHY1STAT	1	Ethernet line interface setting (1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex, and 6=1000Mbps full-duplex if supported by the hardware). Speed and duplex issues are summarized and the best practice is provided in the *Avaya Application Solutions: IP Telephony Deployment Guide*, Document Number 555-245-600 Issue 6, January 2008 on page 290. This document is available from the Avaya support website.
PHY2PRIO	0	Layer 2 priority value for frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is "1" (enabled). Values are from 0-7 and correspond to the drop-down menu selection.

18 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PHY2STAT	1	Secondary Ethernet interface setting (0=Secondary Ethernet interface off/disabled, 1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex), and, for post-Release S1.0 use, 6=1000Mbps full-duplex (if supported by the hardware). Speed and duplex issues are summarized and the best practice is provided in the *Avaya Application Solutions: IP Telephony Deployment Guide*, Document Number 555-245-600 Issue 6, January 2008 on page 290. This document is available from the Avaya support website.
PHY2VLAN	0	VLAN identifier used by frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is “1” (enabled). Value is 1-4 ASCII numeric digits from “0” to “4094.” Null is not a valid value, nor can the value contain spaces.
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.
PROCPSWD	27238	Text string containing the local (dialpad) procedure password (Null or 1-7 ASCII digits). If set, password must be entered immediately after accessing the Craft Access Code Entry screen, either during initialization or when Mute (or Contacts for the 9610) is pressed to access a craft procedure. Intended to facilitate restricted access to local procedures even when command sequences are known. Password is viewable, not hidden.
PROCSTAT	0	Controls access to Craft local (dialpad) administrative procedures. Values are: 0 = Full access to craft local procedures 1 = restricted access to craft local procedures

19 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PROVIDE_EDITED_ DIALING	2	Controls whether edited dialing is allowed and whether on-hook dialing is disabled. Valid values are: 0 = Disable edit dialing. "Dialing Options" is not displayed to the user so the user cannot change edit dialing; the deskphone defaults to on-hook dialing. 1 = Disable on-hook dialing and do not display "Dialing Options" to the user so the user cannot change edit dialing; the deskphone defaults to edit dialing. 2 = Display "Dialing Options" to allow user to change from on-hook to edit dialing. This is the default. 3 = Display "Dialing Options" to allow user to change from edit dialing to on-hook dialing; the deskphone defaults to edit dialing.
PROVIDE_EXCHANGE_ CALENDAR	1	Flag to define whether or not menu item(s) for Microsoft Exchange® Calendar integration are provided to user. Values are: 0=off; 1=on.
PROVIDE_ LOGOUT	1	Flag to define whether or not logout function is provided to user. If disabled and phone is operating in user mode, hide "Logout" item in option menu. Values are: 0=off; 1=on.
PROVIDE_ NETWORKINFO_ SCREEN	1	Flag to define whether or not "Network Information" menu is provided to user. If disabled and phone is operating in user mode, hide complete "Network Information". Values are: 0=off; 1=on.
PROVIDE_OPTIONS_ SCREEN	1	Flag to define whether or not "Options & Settings" menu is provided to user. If disabled and phone is operating in user mode, hide complete "Option & Settings" menu tree. Values are: 0=off; 1=on.
PROVIDE_TRANSFER_ TYPE	0	Flag to determine whether user can select a Transfer Type (Attended/Unattended). Applies to failover environments only. Value is: 0=user cannot select a transfer type, transfer type not shown.
PSTN_VM_NUM	" " (Null)	Telephone number to be used by the messaging application in a non-Avaya or failover server environment. A "dialable" string representing deskphone number or Feature Access Code. This dialable string is used to call into the messaging system (e.g. when pressing the Message Waiting button).
PUSHCAP	00000	String representing push capabilities. Applies to phones running software Release 2.2 only. Values are: 5 ASCII numeric digits, "00000" to "22222".

20 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PUSHPORT	80	String representing the TCP listening port number used for the deskphone's HTTP server. Applies to phones running software Release 2.2 only. Values are: 2 to 5 ASCII numeric digits, "80" through "65535".
QKLOGINSTAT	1	Quick login status indicator. Specifies whether a password must always be entered manually, when the deskphone is in a "registered and inactive" state (another deskphone is used to take over a primary extension e.g. SIP visiting User). Valid values are: 0 = manual password entry is mandatory. 1 = quick-login is enabled; a "quick-login" is possible by pressing the Continue softkey on the login screen to accept the current password value. Note: If set via the settings file this value is given a precedence of 3. If set via PPM in the ListOfMaintenanceData element of the getAllEndpointConfigurationResponse this value is given a precedence of 4.
RDS_INITIAL_RETRY_ ATTEMPTS	15	Indicates how many times the PPM adaptor should try to download from PPM before giving up on connecting to the PPM server. Values are: 1-30.
RDS_INITIAL_RETRY_ TIME	2	Remote Data Source initial retry time in seconds; indicates the initial delay for a retry to connect to the PPM server. Valid range is 2-60 (seconds).
RDS_MAX_RETRY_TIME	600	Remote data source maximum retry time; indicates the maximum delay interval (in seconds) before giving up on PPM server connection. Values are: 2-3600 (seconds). Software Release 2.5 lowers the minimum value from 300 to 2 seconds to allow the phone to operate in the "older" R2.4 manner by setting the PPM retry parameters to: SET RDS_INITIAL_RETRY_ATTEMPTS 10 SET RDS_INITIAL_RETRY_TIME 2 SET RDS_MAX_RETRY_TIME 2
RECOVERYREGISTER WAIT	60	Reactive monitoring interval in seconds for Failover. Valid values are: 10 - 36000 Note: If set via the settings file this value is given a precedence of 4. If set via PPM in the ListOfMaintenanceData element of the getAllEndpointConfigurationResponse this value is given a precedence of 5.

21 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

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

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
RTCPMONPERIOD	5	RTCP Monitor report period. Valid range = 5 - 30 Interval in seconds for sending out RTCP monitoring reports.
RTCPMONPORT	5005	RTCP monitor port number. TCP/UDP port to be used as destination port for RTCP monitoring. Valid range is 0-65535. Note that this value is only set via SET command in settings file if operating in a NON-Avaya environment, otherwise this value is retrieved via PPM.
RTP_PORT_LOW	5004	Specifies lower limit of a port range to be used by RTP/RTCP or SRTP/SRTCP connections, for example, to adapt to firewall traversal policies. Values: 1024-65503.
RTP_PORT_RANGE	40	Specifies the width of the port range to be used by RTP/RTCP or SRTP/SRTCP connections, for example, to adapt to firewall traversal policies. The upper limit is calculated by the value of RTP_PORT_LOW plus the value of RTP_PORT_RANGE, taking into consideration the overall limit of 65535. Values: 32-64511.
SCREENSAVERON	240	Number of idle time minutes after which the screen saver is turned on. Valid values range from zero (disabled) to 999 minutes (16.65 hours).
SDPCAPNEG	0 (Release 2.5) 1 (Release 2.6+)	Controls SDP capability negotiation; interaction between the SDPCAPNEG and MEDIAENCRYPTION parameters controls INVITE behavior. Valid values are: 1 = SDP capability negotiation is enabled. 0 = SDP capability negotiation is disabled.
SEND_DTMF_ TYPE	2	Defines whether DTMF tones are send in-band (regular audio) or out-band (negotiation and transmission of DTMF according to RFC 2833, with fallback to send in-band DTMF tones, if far end does not support RFC2833). Values are 1=in-band DTMF; 2=RFC2833 procedure.
SIG	0	Parameter to allow to download during start-up the specific configuration sets for H323 or SIP endpoints. Valid values are: 0=Default 1=H323 2=SIP
SIG_PORT_LOW	1024	Lower limit of port range for signaling to support by the phone. Values range from 1024 to 65503.
SIG_PORT_RANGE	64511	Port range for signaling to support by the phone. Values range from 32 to 64511.

23 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SIMULTANEOUS_ REGISTRATION	3	The number of Session Managers in the configuration with which the phone will simultaneously register. Valid range is 1 through 3.
SIP_CONTROLLER_LIST	" " (Null)	The entries in this parameter should be coordinated with those administered in SES or the Primary/Secondary Session Manager and Survivability Server administered in System Manager for users at a particular location. Survivability Servers are typically provisioned in SES or System Manager. List of SIP proxy/registrar server IP or DNS address(es). Server(s) used to address SIP registrations and signaling, if operating in proxy mode (in case of several entries first address always first, etc.). When operating in an Avaya Environment SIP_CONTROLLER_LIST is also used to access Personal Profile Manager (PPM). This parameter is considered 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 Failover; the first element of the list is the highest priority, the last element is the lowest priority. For information on Failover, see Chapter 10: System Failover and Survivability. Format: host[:port][;transport=xxx] where *host* is an IP address in dotted decimal format or DNS name, *port* is the optional port number (if not specified, the default port value of 5060 for UDP and TCP or 5061 for TLS is used), *transport* is the optional transport type (where *xxx* is tls, tcp, or udp) and if not specified, the default value of TLS is used. The first element of this parameter (if applicable) has the highest precedence within the parameter. This parameter can have 0 to 255 characters indicating zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SIP_MODE	0	SIP operational mode. Determines whether the deskphone uses a proxy to receive incoming calls or can receive calls directly from another deskphone. Values are: 0=proxy mode; the phone operates in proxy mode with SIP proxy/registrar, 1=peer-to-peer mode; the phone operates in peer-to-peer mode between SIP endpoints.
SIP_PORT_SECURE	5061	The phone's listening port for inbound connections (for secure message transfer via TLS). Values range from 1024 - 65535.
SIPCONFERENCECONTINUE	0	Conference Continuation on host hang-up mode. When the ENABLE_AVAYA_ENVIRONMENT parameter is 0 (non-Avaya environment; the telephone is registered with a non-Avaya proxy server) and the telephone initiating the conference ends the call, the other parties will be dropped unless SIPCONFERENCECONTINUE is set to 1 (continue conference call without initiator). When this parameter is set to "1" the phone sends a single REFER to the first party referring it to the second party (this in essence "transfers" the first party to the second party). If this parameter is set to 0, the capability is turned off and the phone ends the conference when the initiator hangs up. This parameter has no meaning in Avaya environment. Valid values are: 0 = All conference parties are dropped when conference host drops the conference. 1 = Conference is continued when conference host drops the conference.
SIPDOMAIN	" " (Null)	SIP domain name for registration. 0 to 255 characters: string representing domain name.
SIPPORT	5060	The phone's listening port for inbound connections (for non-secure message transfer only). Values range from 1024 - 65535.
SIPREGPROXYPOLICY	"alternate"	SIP registration proxy policy. A policy to control how the phone treats the list of controllers/servers in the SIP_CONTROLLER_LIST parameter. Valid values are: "alternate" = This is the preferred registration method with SIP proxy controllers. If there is no Active Controller, then all Configured Controllers are Monitored Controllers. If there is an Active Controller, the Monitored Controllers are all controllers whose priority is higher than the current Active Controller. "simultaneous" = All controllers in the configured controller list are Monitored Controllers.

25 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SKINS	" " (Null)	Applicable to the SIP 9640 IP Telephone only. Represents a list of skin information tuples. Each skin information is a pair of {skin label, skin URL} data. Each skin tuple is delimited by commas. Each skin tuple contains skin label (verbatim label displayed on the screen) and skin URL. Skin label and URL are separated by a ' ='. The URL may be specified in an absolute or relative path format (“./” for next higher directory level in relative path format; origin is the directory specified by HTTPDIR or TLSDIR depending on download via http or https). String maximum is 1023 characters. Example: Yankees (Color)=http://svn.avaya.com/drop/skins/yankees_color/boohisscolor.xml
SNMPADD	" " (Null)	Text string containing zero or more allowable source IP Addresses for SNMP queries, in dotted decimal or DNS format, separated by commas, with up to 255 total ASCII characters including commas and no intervening spaces.
SNMPSTRING	" " (Null)	Text string containing the SNMP community name string (up to 32 ASCII characters, no spaces).
SNTPSRVR	" " (Null)	Used to retrieve date and time via SNTP (in case of several entries first address always first, etc.). Zero to 255 characters: zero or more IP Addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.
SPEAKERSTAT	2	Limits the hands-free audio operation mode. Valid values are: 0=no speakerphone allowed 1=one-way speakerphone operation allowed (monitor) 2=two-way speakerphone operation allowed
SUBSCRIBELIST	" " (Null)	String representing the Push subscription list. Applies to phones running software Release 2.2 only. Values are: 0 to 255 ASCII characters: zero or more URLs separated by commas without any intervening spaces.

26 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SUBSCRIBE_SECURITY	2	Controls the use of SIP and SIPS subscriptions. Valid values are 0 - 2: If=0, the phone uses SIP for both the Request URI and the Contact Header regardless of whether SRTP is enabled. If=1, the phone uses SIPS for both the Request URI and the Contact Header if SRTP is enabled (TLS is on and MEDIAENCRYPTION has at least one valid crypto suite). If=2 and the SES/PPM does not show a FS-DeviceData FeatureName with a FeatureVersion of 2 in the response to the getHomeCapabilities request (indicative of SES/PPM 4.0), the phone uses SIP for both the Request URI and the Contact Header. If=2 and the SES/PPM does show a FS-DeviceData FeatureName with a FeatureVersion of 2 or greater in the response to the getHomeCapabilities request, the phone uses SIPS for both the Request URI and the Contact Header if SRTP is enabled (TLS is on and MEDIAENCRYPTION has at least one valid crypto suite).
SUPPORT_GIGABIT	0	Flag indicating whether the deskphone supports GigE (Gigabit Ethernet). Valid values are: 0=Telephone does not support GigE 1=Telephone supports GigE
SYMMETRIC_RTP	1	Enforces RTP on the same port. Values are 0 -1.
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.

27 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

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).
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. Applies to phones running software Release 2.2 only. Values are: 0 to 255 ASCII characters: zero or more domain/path strings, separated by commas without any intervening spaces.
TRUSTCERTS	" " (Null)	File names of certificates to be used for authentication. List of file names separated by commas (0 to 1024 characters).
USE_EXCHANGE_ CALENDAR	0	Flag, that indicates whether calendar data retrieval from Exchange is selected or not. Values are: 0 (Disabled) or 1 (Enabled).
USE_QUAD_ZEROS_ FOR_HOLD	0	Flag that indicates whether a= directional attributes or 0.0.0.0 IP Address is used in the SDP to signal hold operation. 0=use “a= directional attributes”, 1=use quad zeros.

28 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
VLANSEP	1	Enables or disables VLAN separation. Controls whether frames received from the line interface are forwarded to the phone or to the secondary Ethernet interface based on VLANID. Also affects whether frames received on the secondary Ethernet interface are changed before forwarding to the line interface. Values are: 1=On/Enabled, 0= Off/Disabled. This parameter is used with several related parameters. For more information, see VLAN Separation on page 126.
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”).
VU_MODE	0	Visiting User mode. Determines, if and how the deskphone supports Visiting User capabilities: 0 = Off; the deskphone operates "normally" and "Visiting User" has no essential impact for normal operation. 1 = Optional; the deskphone prompts the user at registration time if they are Visiting or Not. 2 = Forced; the deskphone only allows Visiting User registrations.
VU_TIMER	36000	To Be Determined
WAIT_FOR_ REGISTRATION_TIMER	32	Time in seconds the SIP application will wait for a register response message. If no message is received, registration is retried. Range is 4-3600 (seconds).
WAIT_FOR_ UNREGISTRATION_ TIMER	32	Time the SIP application waits before declaring un-registration to be complete. Under normal circumstances un-registration includes termination of all active SIP dialogs, and SIP registration. Range is 4-3600 (seconds).
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.

29 of 30

Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
WMLHOME	" " (Null)	Home page for WML browser. If this parameter is null, the deskphone will not display the browser option under the "A" Avaya Menu. If non-null the URL specified is retrieved via HTTP and rendered in the Web page display area, when the WML browser application is initially accessed. Value is zero or one URL.
WMLIDLETIME	10	Number of minutes of inactivity until the Web browser will display the idle URL. When the Web idle timer reaches the number of minutes equal to this parameter, the deskphone sends an HTTP GET for the URI specified by WMLIDLEURI. Valid value is 1-999. Note that the web idle timer starts only when access to the WML browser is provided by an application line under the "A" Avaya Menu and the parameter WMLIDLEURI is non-null.
WMLIDLEURI	" " (Null)	URL of web page displayed after idle timer expires. Note that the web idle timer will only be started when access to the WML browser is provided by an application line under the "A" Avaya Menu and the parameter WMLIDLEURI is non-null. Value is zero or one URL.
WMLPORT	8080	TCP port number to be used to access the HTTP proxy server by the WML browser application (if defined by WMLPROXY). Valid value is 0 - 65535.
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.

Note:

Table 14 applies to all 9600 Series SIP IP Telephones. Certain 9600 SIP IP Telephones might have additional, optional information that you can administer. For more information, see Chapter 8: Administering Telephone Options.

VLAN Considerations

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

VLAN Tagging

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

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

Regardless of the tagging setting, a 9600 Series SIP IP Telephone will always transmit packets from the deskphone at absolute priority over packets from secondary Ethernet. The priority settings are useful only if the downstream equipment is administered to give the *voice* VLAN priority.

Important:
VLAN tags are always removed from frames that egress (go out of) the secondary Ethernet interface.

VLAN Detection

The Avaya IP Telephones support automatic detection of the condition where the L2QVLAN setting is incorrect. When VLAN tagging is enabled (L2Q= 0 or 1) initially the 9600 Series SIP IP Telephone transmits DHCP messages with IEEE 802.1Q tagging and the VLAN set to L2QVLAN. The deskphones will continue to do this for VLANTEST seconds.

- If the VLANTEST timer expires and L2Q=1, the deskphone sets L2QVLAN=0 and transmits DHCP messages with the default VLAN (0).
- If the VLANTEST timer expires and L2Q=0, 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 Telephone receives a non-zero L2QVLAN value, the deskphone will release the IP Address and send DHCPDISCOVER on that VLAN. Any other release will require a manual reset before the deskphone will attempt to use a VLAN on which VLANTEST has expired. See the Reset procedure in Chapter 3 of the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*.

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

VLAN Default Value and Priority Tagging

The system value **L2QVLAN** is initially set to “0” and identifies the 802.1Q VLAN Identifier. This default value indicates “priority tagging” as defined in IEEE 802.IQ Section 9.3.2.3. Priority tagging specifies that your network closet Ethernet switch automatically insert the switch port default VLAN without changing the user priority of the frame (cf. IEEE 802.1D and 802.1Q).

The VLAN ID = 0 (zero) is used to associate priority-tagged frames to the port/native VLAN of the ingress port of the switch. But some switches do not understand a VLAN ID of zero and require frames tagged with a non-zero VLAN ID.

If you do not want the default VLAN to be used for voice traffic:

- Ensure that the switch configuration lets frames tagged by the 9600 Series SIP IP Telephone through without overwriting or removing them.
- Set the system value **L2QVLAN** to the ***VLAN ID*** appropriate for your voice LAN.

Another system value you can administer is **VLANTEST**. VLANTEST defines the number of seconds the 9600 IP Series Telephone waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is “60” seconds. Using VLANTEST ensures that the deskphone returns to the default VLAN if an invalid VLAN ID is administered or if the phone moves to a port where the L2QVLAN value is invalid. The default value is long, allowing for the scenario that a major power interruption is causing the phones to restart. Always allow time for network routers, the DHCP servers, etc. to be returned to service. If the deskphone restarts for any reason and the VLANTEST time limit expires, the deskphone assumes the administered VLAN ID is invalid. The deskphone then initiates registration with the default VLAN ID.

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

Note:

If the deskphone returns to the default VLAN but must be put back on the L2QVLAN VLAN ID, you must Reset the deskphone. See the Reset procedure in the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*.

Important:

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

VLAN Separation

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

- **VLANSEP** - enables (1) or disables (0) VLAN separation.
- **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.

Table 15 provides several VLAN separation guidelines.

Table 15: VLAN Separation Rules

If		Then
VLANSEP is “1” (On/Enabled)	**AND** the deskphone is tagging frames with a VLAN ID not equal to PHY2VLAN, **AND** the PHY2VLAN value is not zero.	**Tagged Frames received on the secondary Ethernet interface:** All tagged frames received on the secondary Ethernet interface are changed before forwarding to make the VLAN ID equal to the PHY2VLAN value and the priority value equal to the PHY2PRIO value. Untagged frames received on the secondary Ethernet interface are not changed before forwarding to the network. Tagged frames with a VLAN ID of zero (priority-tagged frames) will be changed before they are forwarded such that the VLAN ID of the forwarded frame is equal to the PHY2LAN value and the priority value is equal to the PHY2PRIO value. **Tagged Frames received on the line interface:** Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2VLAN. Tagged frames received on the Ethernet line interface will only be forwarded to the deskphone if the VLAN ID equals the VLAN ID used by the deskphone. Untagged frames are not changed will continue to be forwarded or not forwarded as determined by the Ethernet switch forwarding logic. Tagged frames with a VLAN ID of zero (priority-tagged frames) will be forwarded to the secondary Ethernet interface or to the deskphone as determined by the forwarding logic of the Ethernet switch, but the tag will still be removed from frames that egress from the secondary Ethernet interface.
VLANSEP is “1” (On/Enabled)	**AND** the deskphone is not tagging frames, **OR** if the deskphone is tagging frames with a VLAN ID equal to PHY2VLAN, **OR** if the PHY2VLAN value is zero.	Frames forwarded to the network from the secondary Ethernet interface will not be changed before forwarding. Tagging is not added or removed and the VLAN ID and priority does not change for frames received on the secondary interface. Tags are still removed for frames that egress from the secondary interface. The Ethernet switch forwarding logic determines whether frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the deskphone without regard to specific VLAN IDs or the existence of tags.

1 of 2

Table 15: VLAN Separation Rules (continued)

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

2 of 2

DNS Addressing

The 9600 Series SIP IP Telephones support DNS addresses and dotted decimal addresses. The deskphone attempts to resolve a non-ASCII-encoded dotted decimal IP Address by checking the contents of DHCP Option 6. See DHCP Generic Setup on page 68 for information. At least one address in Option 6 must be a valid, non-zero, dotted decimal address, otherwise, DNS fails. The text string for the **DOMAIN** system parameter (Option 15, Table 14) 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.

IEEE 802.1X

9600 Series IP Deskphones support the IEEE 802.1X standard for pass-through and Supplicant operation but only if the value of the configuration parameter DOT1XSTAT is “1” (the default, meaning supplicant operation is enabled, and the deskphone responds only to received unicast EAPOL messages) or “2” (supplicant operation enabled, and deskphone responds to received unicast and multicast EAPOL messages). If DOT1XSTAT has any other value, supplicant

operation will not be supported. The system parameter DOT1X determines how the deskphones handle 802.1X multicast packets and proxy logoff, as follows:

- When DOT1X = 0 (the default), the deskphone forwards 802.1X multicast packets from the Authenticator to the PC attached to the deskphone and forwards multicast packets from the attached PC to the Authenticator (multicast pass-through). Proxy Logoff is not supported.
- When DOT1X = 1, the deskphone supports the same multicast pass-through as when DOT1X=0. Proxy Logoff is supported.
- 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 MAC address in the packet.

802.1X Pass-Through and Proxy Logoff

9600 Series IP Deskphones with a secondary Ethernet interface support pass-through of 802.1X packets to and from an attached PC. This enables an attached PC running 802.1X supplicant software to be authenticated by an Ethernet data switch.

The SIP IP Telephones support two pass-through modes:

- pass-through and
- pass-through with proxy logoff.

The DOT1X parameter setting controls the pass-through mode. In Proxy Logoff mode (DOT1X=1), when the secondary Ethernet interface loses link integrity, the deskphone sends an 802.1X EAPOL-Logoff message on the Ethernet line interface to the data switch on behalf of the attached PC. The message alerts the switch that the device is no longer present. Proxy logoff occurs only after at least one EAPOL frame with the Port Access Entity (PAE) group multicast address as the destination MAC address was received on the secondary Ethernet interface. The destination MAC address of the proxy EAPOL-Logoff frame is the PAE group multicast address. The source MAC address of the proxy EAPOL-Logoff frame is the same as the source MAC address of the last frame received on the secondary Ethernet interface that had the PAE group multicast address as the destination MAC address.

Note:

When DOT1X = 0 or 2, the Proxy Logoff function is not supported.

802.1X Supplicant Operation

9600 IP Deskphones that support Supplicant operation also support Extensible Authentication Protocol (EAP), but only with the MD5-Challenge authentication method as specified in IETF RFC 3748 [8.5-33a] 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 in effect, the dynamic address process prompts the installer to enter the Supplicant identity and password. See “Dynamic Addressing Process” in the *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide* for information on this process. The deskphone does not accept null value passwords. The default credentials consisting of the values of the DOT1XID and DOT1XPSWD parameters will be used when a new telephone is first plugged in if the EAP method requires an identity and password. In this case, authentication will fail because the password is null, thus the authentication attempt will not actually contain a password (whether or not the default identity is correct). An EAP-Failure message will be received in response, and an 802.1X User Input interrupt screen prompting "Enter Credentials" is then displayed. For all EAP methods, if the Supplicant is unauthenticated, an 802.1X Waiting interrupt screen is displayed when a response is transmitted, unless an 802.1X User Input interrupt screen is already being displayed.

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

The deskphone stores 802.1X credentials when successful authentication is achieved. Post-installation authentication attempts occur using the stored 802.1X credentials, without prompting the user for ID and password entry and the ID and password are not overwritten by deskphone software downloads.

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

These switches support the following three scenarios:

- **Standalone deskphone (Telephone Only Authenticates)** - When the deskphone is configured for Supplicant Mode (DOT1X=2), the deskphone can support authentication from the switch.
- **Deskphone with attached PC (Telephone Only Authenticates)** - When the deskphone is configured for Supplicant Mode (DOT1X=2), the deskphone can support authentication

from the switch. The attached PC in this scenario gains access to the network without being authenticated.

- **Deskphone with attached PC (PC Only Authenticates)** - When the deskphone is configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1), an attached PC running 802.1X supplicant software can be authenticated by the data switch. The deskphone in this scenario gains access to the network without being authenticated.

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

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

Link Layer Discovery Protocol (LLDP)

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

The transmission and reception of LLDP is specified in IEEE 802.1AB-2005. 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 Telephones running SIP Release 2.0 and later software support IEEE 802.1AB if the value of the configuration parameter LLDP_ENABLED is "1" (On) or "2" (Auto). If the value of LLDP_ENABLED is “0” (off), the transmission and reception of Link Layer Discovery Protocol (LLDP) is not supported. When the value of LLDP_ENABLED is “2”, the transmission of LLDP frames will not begin until or unless an LLDP frame is received, and the first LLDP frame will be transmitted within 2 seconds after the first LLDP frame is received. Once transmission begins, an LLDPDU will be transmitted every 30 seconds.

Note:

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

These deskphones:

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

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

Table 16: LLDPDU Transmitted by 9600 Series SIP Deskphones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPADD of deskphone, IANA Address Family Numbers enumeration value for IPv4, or subtype 5:Network address.
Basic Mandatory	Port ID	MAC address of the deskphone.
Basic Mandatory	Time-To-Live	120 seconds.
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.
Basic Optional	System Capabilities	Bit 2 (Bridge) will be set in the System Capabilities if the deskphone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled. Bit 5 (Telephone) will be set in the System Capabilities. If Bit 5 is set in the Enabled Capabilities than the deskphone is registered.
Basic Optional	Management Address	Mgmt IPv4 IP Address of deskphone. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the deskphone.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports autonegotiation status and speed of the uplink port on the deskphone.

1 of 2

Table 16: LLDPDU Transmitted by 9600 Series SIP Deskphones (continued)

Category	TLV Name (Type)	TLV Info String (Value)
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery capabilities = 00-33 (Inventory, Power-via-MDI, Network Policy, MED Caps).
TIA LLDP MED	Network Policy	Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value.
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Firmware Revision	BOOTNAME.
TIA LLDP MED	Inventory – Software Revision	APPNAME.
TIA LLDP MED	Inventory – Serial Number	Telephone serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final D***xxx*** characters removed.
Avaya Proprietary	PoE Conservation Level Support	Provides Power Conservation abilities/settings, Typical and Maximum Power values. OUI = 00-40-0D (hex), Subtype = 1. Current conservation level=POE_CONS_MODE.
Avaya Proprietary	Call Server IP Address	Call Server IP Address. Subtype = 3.
Avaya Proprietary	IP Phone Addresses	Phone IP Address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	CNA Server IP Address	CNA Server IP Address = in-use value from CNASRVR. Subtype = 5.
Avaya Proprietary	File Server	File Server IP Address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not. Subtype = 7.
Basic Mandatory	End-of-LLDPDU	Not applicable.

2 of 2

On receipt of a LLDPDU message the Avaya IP Telephones will act on the TLV elements described in Table 17.

Table 17: Impact of TLVs on System Parameter Values

System Parameter Name	TLV Name	Impact
PHY2VLAN	IEEE 802.1 Port VLAN ID	System value changed to the Port VLAN identifier in the TLV.
L2QVLAN and L2Q	IEEE 802.1 VLAN Name	The system 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.

Table 17: Impact of TLVs on System Parameter Values (continued)

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.

Visiting User Administration

Note:

Visiting user functionality is not available with Avaya Aura™ Session Manager. The deskphone only applies visiting user behavior when the deskphone is not connected to an SM. When a phone is connected to an SM and a user attempts to log into an SM that is not their home SM, the deskphone is redirected with the first register attempt to the local SM community. This is known as Mobile User behavior as opposed to Visiting User.

Note:

Emergency calling is supported regardless of to which controller the phone is connected.

A "visiting user" is anyone who logs into a 9600 Series SIP IP Telephone that is not his or her primary phone at the user’s home location. This could mean that the visiting user can log into a telephone that is across the country from the home location or one in the office adjacent to the home office. When registered as a visiting user:

- After the phone registers with the local SES, the phone is redirected via the PPM GetHomeServer response. From that point on the phone communicates with the local SES and the home PPM.
- An inactivity timer is used to trigger inactivity and thereby un-register a user.The Visiting User Inactivity Timer value is communicated to the telephone via Personal Profile Manager (PPM). The Visiting User Inactivity Timer is a local timer (VUTIMER) in the telephone that has the same value as the EMU timer value that is set in Avaya Communication Manager (CM). The inactivity timer is relevant when users are served through a SIP Enablement Services (SES) that is not their home SES.
- Registration Events with "Q value" of 0 result in a logout. When a new registration is sent from a visiting roaming or non-roaming telephone, the visiting telephone takes priority over the user's home or primary telephone. Outbound calls can be made from either the visiting telephone or the primary telephone. The home SES lowers the q-value of previous registrations to zero and promotes the new registration to ensure that inbound calls will be routed to the most recent telephone registered.
- The telephone will unregister if it is a visiting user telephone. But that telephone will become registered as inactive if it is the primary telephone.

Set the VU_MODE configuration parameter value in the settings file to determine the visiting user login routine. VU_MODE determines whether the phone will support Visiting User capabilities as follows:

- If the VU_MODE value is zero (Off) the telephone is considered a non-VU phone. This is the default value and the value associated with the user's "home" phone. The inactivity timer is not applied when VU_MODE is 0.

- If the VU_MODE value is 1 (Optional), the telephone presents the user with the Login Screen with a Primary Phone yes/no toggle field, for the user to designate whether the telephone is that user's primary phone. If the user selects "yes", then the phone operates as a non-visiting user telephone and the inactivity timer is not applied. If the user selects "no", then the telephone operates in the visiting user mode where an inactivity timer will log the user off after a predetermined time.
- If the value is 2 (Forced), the telephone is always in the visiting user mode and the inactivity timer is always applied.

Emergency Number Administration

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

Note:

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

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

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

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

From: sip:anonymous@avaya.com;tag=-961235f46856f74-5_F135.8.62.174, and Contact: <sip:anonymous@135.8.62.174;transport=tcp>)

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

To: <sip:anonymous@135.8.62.174;transport=tcp>

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

Local Administrative (Craft) Options Using the Telephone Dialpad

The *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide* details how to use Craft local procedures at the deskphone for administration. The local procedures you might use most often as an administrator are:

- **ADDR** - Static address programming.
- **CLEAR** - Remove all administered values, user-specified data, option settings, etc. and return a deskphone to its initial “out of the box” default values.
- **DEBUG** - Enable or disable debug mode for the button module serial port.
- **GROUP** - Set the group identifier on a per-phone basis.
- **INT** - Locally enable or disable the secondary Ethernet hub.
- **RESET** - 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** - Restart the deskphone in response to an error condition, including the option to reset system values.
- **SIG -** Change the default signaling value to/from SIP, or change SIG to/from H.323. Chapter 2 of the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide* also describes how to determine which SIG value is appropriate for your environment.
- **SIP** - Configure SIP call settings.
- **VIEW** - Review the system parameters for the deskphone to verify current values and file versions.

Language Selection

9600 Series IP Telephones are factory-set to display information in the English language. In addition to English, SIP software bundle downloads include the following language files:

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

- Hebrew
- Arabic

Administrators can specify from one to four languages per deskphone to replace English. End users can then select which of those languages they want their deskphone to display. Note that the phone cannot display Japanese, Chinese, and Korean characters at the same time.

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

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

- **LANGUAGES** - the list of languages to be downloaded from which the end user can select a desired display language. Each language is listed in the following format: Mlf_German.xml, Mlf_English.xml, Mlf_CastilianSpanish.xml, and so on.
- **SYSTEM_LANGUAGE** - a string indicating the filename of the default system language. The string indicates which of the available languages to use for display purposes. If this parameter is not set, or if no other language has been set by the user, or if a user language choice cannot be satisfied, the built-in English strings are used.
- **LANG0STAT** - Allows the user to select the built-in English language when other languages are downloaded. If LANG0STAT is "0" and at least one language is downloaded, the user cannot select the built-in English language. If LANG0STAT is "1" (the default) the user can select the built-in English language text strings.

For more information, see SIP 9600 Series IP Deskphones Customizeable System Parameters. To view multiple language strings, see the MLS local procedure in the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*. To download a language file or review pertinent information, go to http://support.avaya.com/unicode.

Note:

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

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

The system values relevant to the Enhanced Dialing Feature are:

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

Note:

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

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

As indicated in Table 14, you can administer the system parameter **ENHDIALSTAT** to turn off the Enhanced Local Dialing feature.

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

Setting the Dial Plan on SIP IP Telephones

Note:

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

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

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

digits 0 through 9, inclusive = Specific dialpad digits
***** = the dialpad character *
# = the dialpad character # (but only if it is the first character in the dialed string – see below)
x = any dialpad digit (i.e., 0-9)
Z or **z** = present dial tone to the user (for example, for Feature Access Code (FAC) entry)
[ ] = any one character within the brackets is a valid match for a dial plan string
- = any one digit between the bounds within the brackets, inclusive, is a match
+ = the character following the + can repeat 0 or more additional times, for a valid match

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

Dial plan example:

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

where:

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

Additional parameters that affect dialing are as follows:

COUNTRY - Country of operation for specific dial tone generation.

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

Example 1. `SET PSTN_VM_NUM 96135550123`

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

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

Example: `SET PHNLAC 617`

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

Example: `SET LOCAL_DIAL_AREA_CODE 1`

Example 1 - Setting the parameter configuration:

```
SET ENHDIALSTAT 2

SET PHNOL 27

SET PHNCC 1

SET PHNDPLENGTH 7

SET PHNLDLENGTH 11

SET PHNLD 0

SET PHNIC 001
```

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

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

See Table 14 for a definition of the DIALPLAN parameter.

Setting the Date and Time on SIP Deskphones

SIP deskphones need a source of date and time information. This typically comes from a network time server running the Simple Network Time Protocol (SNTP). The deskphones use several administrative parameters for this functionality. The parameter SNTPSRVR defines the server's IP Address(es). GMTOFFSET defines the offset from Greenwich Mean Time (GMT). DSTSTART and DSTSTOP define the start and end of Daylight Savings Time, respectively. DSTOFFSET defines the Daylight Savings Time offset from Standard Time. Finally, DATETIMEFORMAT defines the format of the date and time display. See Table 14 for definitions and valid values for SIP Date and Time parameters.

Administering Presence

Presence Notification

Presence notification occurs only if the (internal, non-settable) PRIMARY_PROXY_ENVIRONMENT parameter is 1 (an SES environment) and when the ENABLE_PRESENCE parameter (set using the settings file) is set to 1 (Enabled/On).

For SES environments:

If the deskphone has accepted a subscription to its presence state, it reports the following:

- After the phone completes registration, a NOTIFY message is sent with a presence event header. The presence document in the XML message body shows a status="open" and substatus="online" (Available).
- When the user goes off-hook, a NOTIFY message is sent with a presence event header. The presence document in the XML message body shows a status="inuse" and substatus="onthephone" (On the Phone).
- When the user hangs up and the phone sends a BYE message, it is followed by a NOTIFY message with a presence event header. The presence document in the XML message body shows a status="open" and substatus="online" (Available).
- When the Send All Calls (SAC) feature is enabled, a NOTIFY message is sent with a presence event header. The presence document in the XML message body shows a status="inuse" and substatus="busy" (Busy).
- When SAC is disabled, a NOTIFY message is sent with a presence event header. The presence document in the XML message body shows a status="open" and substatus="online" (Available).
- If the phone has subscribed to the Presence.winfo and Presence.list events, it accepts the following presence information and passes it to the UI for further processing: Available, On the phone, Busy, Away.

Presence User Interface

Presence provides information about other SIP users to the deskphone user when the phone's primary controller is SES.

Primary Presence information is provided through the Contact List view, providing the deskphone user adds "handles" (URI and SIP Domain) for applicable contacts. If a SIP Domain is not provided when the handle is set up, the deskphone software will provide the domain automatically. Primary Presence information is also provided through the Favorite Features on the Phone Screen for Contacts only and in the Call Log, but only for those call log entries that appear in a user’s Contact list.

The Presence icon is used in place of Work, Home, Mobile, Handle icons. During failover, no presence tracking occurs.

For SES environments:

There are two different aspects of presence in an SES environment:

- Sent Presence - The deskphone sends the following presence states:
  - Available: Sent when phone is registered and no other states apply.
  - On the Phone: Sent when the phone is active on a call.
  - Not Registered: The state is not sent when the phone is unregistered. But, the state is rendered at a tracking phone as shown.
  - Busy: Will be sent when "Send All Calls" is activated.
- Received Presence - The phone receives and renders the following presence states:
  - -All those stated above for sent presence.
  - Away: This state is reported by the deskphone.

Presence Administration

Telephone presence is "off" by default. To turn presence on, the following must be included in the 46xxsettings.txt file:

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

Another parameter that controls presence is:

ENABLE_AUTOMATIC_ON_THE_PHONE_PRESENCE - This parameter controls whether "on the phone" presence status is sent out automatically when user whose presence is tracked is on a call (or goes off-hook). Calls on bridged line appearances (that local user has not bridged to) do not affect the trigger of the "on the phone" presence update. The default of "0" indicates this option is disabled; when the person whose presence is being tracked goes off-hook, his or her presence is not reported. A setting of "1" enables automatic on the phone presence. 0When user goes off-hook, no special presence is reported

Integrating Microsoft™ Exchange

SIP software Release 2.5 supports Microsoft Exchange calendaring integration, which allows 9600 Series SIP IP Telephones to download appointment/calendar data containing meeting schedules from an Exchange Server and display this information on a new Appointment screen. End users must specify their credentials (Exchange user account name and password) and calendaring reminder and display preferences using the Avaya (A) Menu’s Options & Settings

Advanced Options option before the Exchange Calendar and the Reminder can be used. User actions regarding exchange integration are described in the applicable deskphone user guide.

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

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

Customizing Ring Tones

End users can select any one of 8 standard ring tones using the A Menu Screen & Sounds option; the ring tone selection is then stored in PPM. Ring tones for external, internal, priority

and intercom calls (distinctive ringing) are combinations of specified frequency, duration and cadence values.

SIP software Release 2.4 provided the EXTEND_RINGTONE parameter to allow you to optionally administer one of two additional sets of 8 ring tones - Korean or customized - to replace the standard Avaya ring tones currently available.

Korean Ring Tones

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

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

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

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

Customized Ring Tones

As of SIP software Release 2.4, 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 Table 18. A sample spreadsheet follows the table for illustration purposes only.

Table 18: Ringtone.XLS Cell Descriptions

Cell Name	Description	Comment
Ringer Name	Name of this custom Ring Tone file, for example, Ringtone1	This filename will be assigned a .XML extension upon completing all required cells and pressing the "Create xml" cell button.
Ringer Index	This numbers the xml file as one of the 8 patterns used in personalized ringing. For example, index 2 will be the second personalized ringing choice a user will have on their phone. Eight xml files with indices 1-8 need to be created to customize all the available personalized ringing choices that will be presented on a phone. If less than 8 indices/files are set in the settings file, Avaya standard ringing patterns will be used for the missing indices.	
Type of Wave	Leave empty; this cell is not currently used.	Reserved for future use.
Number of Active Frequencies	Up to four active frequencies can be set. Valid values are 1, 2, 3, or 4.	
Frequency Values	The range of frequency values is from 0 to 3999Hz.	
Number of Notes	Number of notes in this ring tone, from 1 to 3. A note is an interval in which a frequency is used. Currently, a custom ring tone has a 3 note maximum.	
Note 1, 2, and 3	This value represents a collection of frequency intervals that are grouped together and repeated over and over again as the ring tone.	
Note Pulse State	The pulse state has two possible settings - On or Off	
Note Frequency	The frequency used for a particular note.	
Note Duration	The duration of the note in milliseconds, from 0 to 2^16.	
Next Note	Leave empty; this cell is not currently used.	Reserved for future use.

Table 18: Ringtone.XLS Cell Descriptions

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

Chapter 9: Administering Applications and Options

Customizing Deskphone Applications and Options

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

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

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

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

These parameters have On (1=enabled)/Off (0=disabled) settings, and are described in detail in Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters.

Note:

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

Avaya “A” Menu Administration

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

- Options & Settings
- Browser (only if WMLHOME administered in settings file)
- Network Information
- Log Out
- About Avaya one-X

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

Administering Standard Avaya Menu Entries

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

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

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

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

Administering the WML Browser

SIP software Releases 2.0 and later provide a WML Browser which, if administered, follows the Options and Settings listing on the Avaya (A) Menu.

Note:

WML applications are accessed from the Browser.

Set the configuration parameter WMLHOME in the settings file to link the Browser Home page to the Avaya (A) Menu and to include the Browser option on the Avaya (A) Menu. The Browser application is listed if and only if it is properly administered as specified in *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-600888).

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

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

For detailed information about WML Browser configuration parameters, see Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters.

Chapter 10: System Failover and Survivability

This chapter provides general administrative and detailed information about failover, transition, and failback.

SIP Software Releases and Survivability

SIP Release 2.6

SIP software Release 2.6 provides support for simultaneous calls from multiple servers to accommodate situations that can occur due to network or server failures. This release also ensures that contact data is preserved and actionable during failover transition. Additionally, Release 2.6 adds support for the following secondary gateways:

- Avaya Secure Router 2330 and 4134
- Audiocodes MP-series analog and BRI gateways
- Cisco 2811 ISR
- Juniper SRX 210 and 240
- I55
- Teldat Vyda gateway

In Release 2.6, deskphones fail over to a secondary controller for alternate registration (SES Failover to Session Manager (SM) to a non-AST controller). Simultaneous registration occurs between SMs/BSM (Branch Session Manager) as opposed to alternate registration from SES to SES or SES/SM to a non-AST controller. This arrangement facilitates faster failover/failback transitions than that of the failover solutions offered in previous SIP software releases and provides minimal (if any) disruption from an end user viewpoint.

SIP software Release 2.6 supports Contact caching and caching limits in a Session Manager environment. Multiple operations on a cached contact are not allowed. Release 2.6 also supports preserved media connections/calls. During failover, changes to applications other than Contacts are cached and are updated by the PPM with which the phone successfully registers.

In Release 2.6 with SES and non-AST controllers, contact data is cached until the maximum cache size of 25 contacts is reached; configuration data is cached without limitations. With SM, the PPMs are in sync and the data is sent to the PPM; data is cached only in case of failure.

In SIP software Release 2.6, moving subscriptions to secondary SM/BSM for simultaneous registration has the following effects on call states and transitions:

- Transition from one SM to another SM/BSM is comprised of :
  - Limbo - The phone has lost its connection to its primary controller, but has not yet detected this regardless of whether a user is on a call or not.
  - Moving Subscriptions Interval (MSI) - The phone has detected a lost connection to the primary controller and since it has already registered with a non-primary controller, this is the brief interval between limbo and successful subscription to the non-primary controller. The subscription can be moved regardless of whether a user is on a call or not.
  - Call Preservation - During an active call, the phone has detected a lost connection to the primary controller and exhibits media preservation behavior.
- The Call Preservation Message Box or the Acquiring Services screen are not displayed during the Moving Subscription Interval (MSI).

MSI transition and failback to the primary SM occurs according to the failback behavior described in 3. Select the Active Controller on page 162.

SIP Release 2.5

SIP software Release 2.5 expanded and enhanced survivability capabilities. Release 2.5:

- supported a duplex SES environment running SES versions 4.0, 5.0, 5.1, or 5.2,
- accepted Avaya Communication Manager Versions 4.0, 5.0, 5.1, or 5.2,
- provided for alternate registration,
- expanded the local SIP gateways supported to one of:
  - Audiocodes MP-series using SIP over UDP, TCP or TLS for signaling and RTP or SRTP for media.
  - Cisco ISR using at least one combination of UDP, TCP or TLS for signaling and RTP or SRTP for media.
  - expanded survivability to Avaya Aura Session Manager.
- provided more deskphone functionality during failover, transition, and failback.

SIP Release 2.4

SIP software Release 2.4 gave SIP deskphones the ability to maintain operation during a session controller failure or WAN disconnect when one of the following SIP (CM and SES or SM) environments are in place:

- CM 4.0 through 5.1 and SES 4.0.
- CM 4.0 through 5.1 and SES 5.0.

- CM 5.0/5.1 and SES 5.1 and a secondary third-party SIP proxy/gateway, specifically the Audiocodes gateway MP114, MP118 Firmware Version 5.40.
- CM 5.2.1 and Session Manager 5.2.

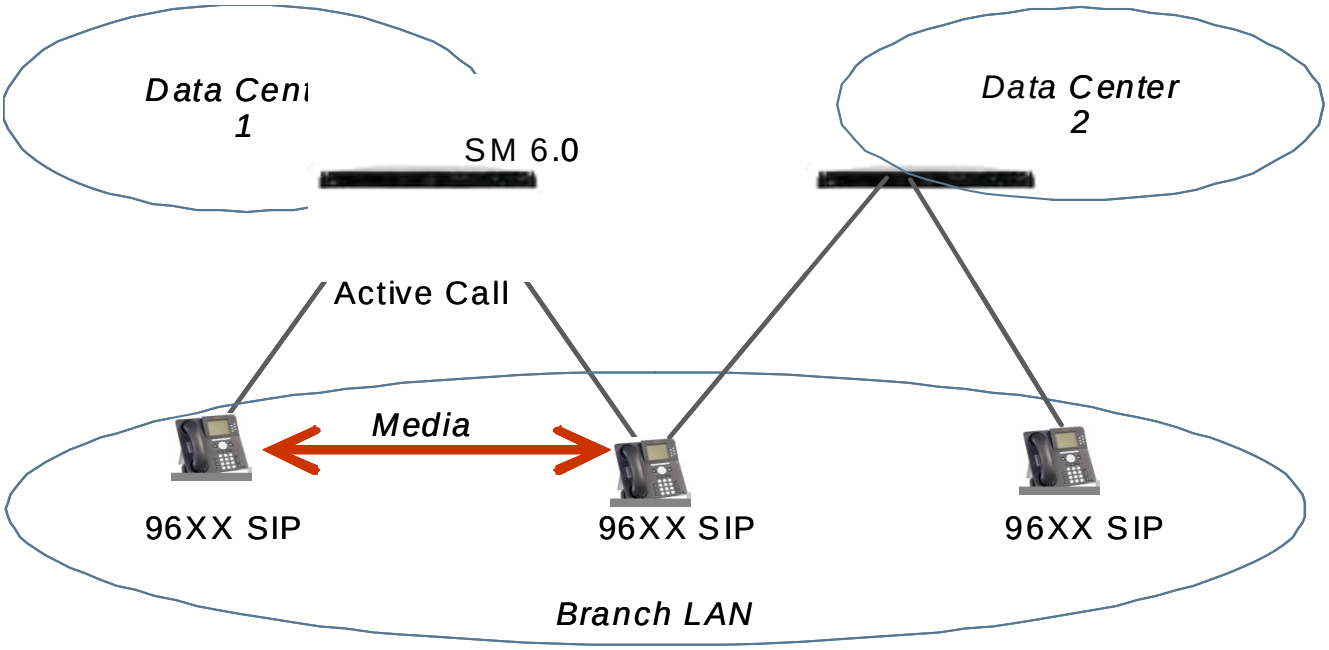
Deskphones in an R2.4 configuration have two controllers - the primary SES controller and a secondary third-party SIP proxy/gateway.

SIP Survivability Configuration Examples

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

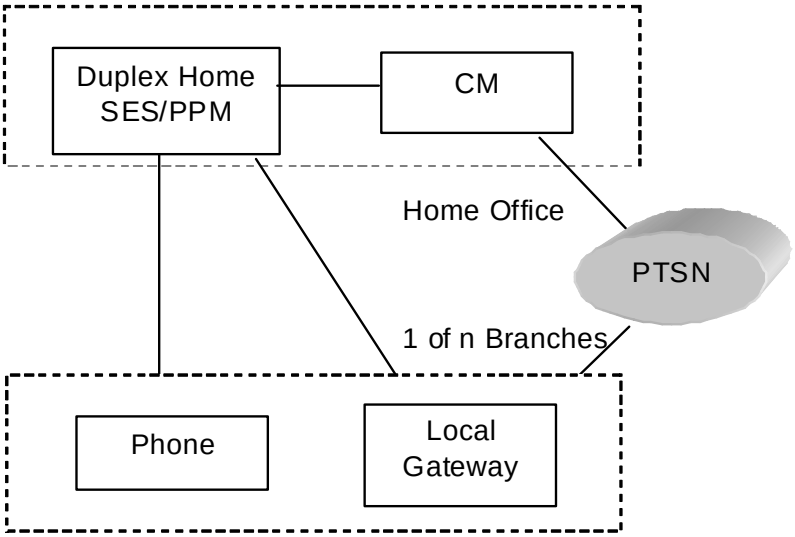
R2.6 Configuration Example:

SIP software Release 2.6 offers simultaneous registration with multiple controllers, and improved feature availability during and after failover to a secondary controller.



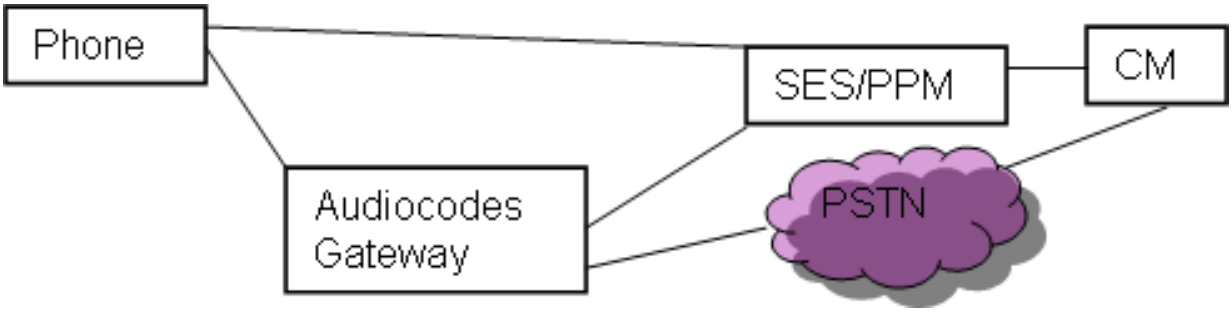
R 2.5 Configuration Example:

SIP software Release 2.5 introduced multiple controllers, improving on survivability.



R 2.4 Configuration Example:

SIP software Release 2.4 provided a single controller for failover.



Hardware/Software Requirements

- Avaya 9600 Series IP Telephones with SIP 2.4+ firmware.
- Supported local (secondary) gateway with Proxy or B2BUA capabilities.

Provisioning Survivability for SIP Deskphones

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

1. Set the applicable failover configuration parameters (described in Survivability Configuration) in the 46xxsettings file.
2. Provision the gateway per the Application Notes, available on the Avaya support Web site.
3. Load the SIP Release 2.6 firmware and associated files on the file server.
4. Reboot all registered phones from SES/SM.
5. Power up other phones.

Survivability Configuration

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

By administering survivability configuration parameters using the 46xxsettings file (or using the default values if applicable), the SIP deskphone(s) can quickly switch to an active controlling server and experience minimal disruption. The failover/failback parameters, described in detail in Table 14: SIP 9600 Series IP Deskphones Customizeable System Parameters, are:

- CONTROLLER_SEARCH_INTERVAL - The time the phone waits to complete the maintenance check for Monitored Controllers.
- DISCOVER_AVAYA_ENVIRONMENT - Determines whether the phone operates in a mode to comply with the Avaya environment mode (provision of SIP/AST features and use of PPM for download and backup/restore).
- ENABLE_REMOVE_PSTN_ACCESS_PREFIX - Enables the removal of the PSTN access prefix from collected dial strings when the phone is communicating with a non-AST controller.
- FAILBACK_POLICY - Failback Policy.
- FAST_RESPONSE_TIMEOUT - Fast Response Timer.
- PSTN_VM_NUM - The number called when the phone is in failover and the Message button is pressed.
- RECOVERYREGISTER 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_REGISTRATION - The number of Session Managers with which the deskphone will simultaneously register.
- SIPREGPROXYPOLICY - Registration Policy.

Note:

With SES 4.0 the survivability parameters are only settable via the 46xxsettings.txt file. They are not settable in the SIP Phone Settings screens of the SES.
With SES 5.0 and up, the survivability parameters can be provisioned in the SES Phone Settings screens; for information see *Installing, Administering, Maintaining, and Troubleshooting SIP Enablement Services* (Document Number 03-600768). With SES 5.0 and up the survivability parameters can also be provisioned in the 46xxsettings.txt file, but Personal Profile Manager values will take precedence over values in the 46xxsettings.txt file.

Setting a Controller via the User Interface

With SES 5.0+ survivability parameters can be provisioned in the SIP Phone Settings screens. 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 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.

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

Controller Determination and Survivability Activity

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

1. Determine Controllers to Monitor

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

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

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

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

2. Determine which Monitored Controllers are Available

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

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

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

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

3. Select the Active Controller

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

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

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

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

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

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

Simultaneous Registration (R2.6)

For SIP software Release 2.6, deskphone behavior for simultaneous registration is based on one of four triggers:

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

Simultaneous registration functions in response to a trigger are:

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

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

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

4. AST Feature Determination

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

If the parameter value is 1, the phone determines if that controller supports the AST (Advanced SIP Telephony) feature set or not. The phone sends a SUBSCRIBE request to the active

controller for the "Feature Status Event Package" (avaya-cm-feature-status). If the request succeeds, the phone proceeds with PPM Synchronization. If the request is either rejected, is proxied back to the phone, or does not receive a response, the deskphone assumes that AST features are not available.

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

As of SIP software Release 2.6 upon receiving a 202 Pending response, the deskphone starts an internal timer of 16 seconds and waits to receive a NOTIFY to determine whether the subscription is active or terminated. If the NOTIFY indicates an "active" state, the phone considers itself in an AST environment and proceeds with PPM Synchronization. If the NOTIFY indicates a "terminated" state, the phone considers itself in a non-AST environment. It periodically retries the subscription to the Feature Status Event Package. If it receives a 202 Pending response, it continues as specified above. If the 16 second timer expires before a NOTIFY is received the phone considers itself in a non-AST environment.

5. PPM Synchronization

As part of PPM 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 - effective with SIP software Release 2.6; applies only when registered to a Session Manager (SM)
- ListOfIdentities - only when registered to a SM
- MWExt - effective with SIP software Release 2.6; applies only when registered to an SM
- VMNumber - effective with SIP software Release 2.6; applies only when registered to an SM

If the getAllEndpointConfiguration request fails, the phone does not continue with the other PPM 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 dependant on the configuration and behaviors of all the SIP network elements such as phones and proxy servers as well as the traditional network elements like routers and DNS servers. The endpoint detects a failure within approximately 90 seconds of the time the failure occurs when TCP or TLS connections are used. Once a failure has been detected, the endpoint completes its selection of an ‘Active’ controller within approximately 5 seconds.

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

Telephone Behavior During Failover

During failover, 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 phone is registered on secondary controller (AudioCodes, Cisco, etc.) and regardless if the phone is active on a call, the phone is in a pushable state, just as if were connected to primary server. The phone is always in a pushable for state for all normal or barge-in Top Line. Display, Audio Receive/Transmit, or phonexml pushes for all transition conditions.

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

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

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

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

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

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

Failover/Failback Administrative Monitoring and Logging

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

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

User Experience for Transitions

SIP software Release 2.6 expanded deskphone reliability during the transition from one controller to another.

Failover to a secondary controller for alternate registration (SES F/O to SM to a non-AST controller)

Transition is comprised of the following conditions:

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

Moving subscriptions from one SM to another SM/BSM (Branch System Manager) due to failover (R2.6+)

Transition is comprised of the following conditions for moving subscriptions:

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

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

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

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

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

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

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

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

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

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

Transition for earlier SIP software releases

For SIP software Release 2.5, transition to a secondary controller is comprised of the following conditions:

- Call attempts which encounter an outage will not succeed.
- “Failover timer” on the SIP INVITE will drive failover to the local gateway after 4 seconds.
- No new calls may be originated during Transition Period.
- Additional call attempts may receive Reorder, until local REGISTER is completed.

- Failover will not happen during an active call. If the media path is still available, calls started via the primary call server will be maintained during failover. Failover/back is deferred until the phone is idle.
- User has no control over failure mode – Failover/back is automatic.
- The telephone display provides an indication of the Failover Operation, by displaying “Link recovery. Limited phone service. Calls may be lost.” No applications are currently available.
- Held calls and transfers are lost during transition.
- Conference calls may be lost during transition.
- Incoming calls during transition may be killed.
- Softkey labels are removed from the display for any feature or operation that is not supportable without the primary call server. (Unavailable softkey features are removed from the display - hold, conference and transfer. The End call softkey remains.) There is a distinction between calls that continue over the transition, and those that originate in failover.
- Any AST feature invocation will fail during transition but once the transition to a new server has occurred, advanced features like Call Park/Unpark, Priority Call, or Automatic Callback are available. Favorite features are not available during failover but will be available after transition to the alternate server.
- Changes to Avaya (A) Menu options can be made/saved. Note that any new or changed settings for these options may be cached and will not become effective until the phone transitions to the alternate server or fails back to its original server.
- The user can press the Phone button to access Home screen Web links/pages during failover, however, any “click to dial” links will not work until the phone transitions to the alternate server.

User Experience During Stable Failover

- A Failover “warning” icon displays on the top line. The Failover icon is shown whenever the primary call server is not active. The Failover icon provides a continuous reminder indicating the deskphone has detected that the primary server is unavailable and that features will be limited until the primary server returns.
- Multiple Call Appearances are consistent with Normal Operation.
- If a call originates using the secondary server, Hold, Conference and Transfer are supported.
- AST features (FNUs and Bridged call appearances) are unavailable when failing over to a secondary gateway.
- Unsupported features and related softkeys are not displayed.

- The dial plan does not remain as it was in normal operation. The dial plan in failover is set with the DIALPLAN parameter which should contain all needed strings while failed over. Calls between sets in the branch are supported, using their usual extensions.
- Outgoing Calls that would normally route to the SES or SM/CM will instead be routed to the local gateway.
- Emergency calls (to the provisioned emergency numbers as defined in the dial plan) will be permitted whether those phones are in failover or normal mode. The Emergency softkey is available when a new controller is found.
- The MWI (Message Waiting Indicator) will be cleared, but voice mail is still available.
- One-button voice mail access will be available if the central voice mail system continues to operate and will make a PSTN call to the voice mail system. Depends on correct provisioning.
- Local deskphone features will be available: audio selection (speaker / headset / handset), mute.
- Local phone applications will be available: local call redial, Call Logs, Volume Control, local contacts, speed-dials, auto-dials, WML browser (WML Browser is dependent on network access to the WML server) but cannot be changed.
- Nothing is saved in PPM when failing over to a secondary (for example, Audiocodes) gateway.
- Basic local features if provisioned (call forwarding) will be available: call hold, consultative hold, Attended Transfer, Unattended Transfer, call forward all, call forward on busy, call forward on no answer, three party conferencing of calls originated in Failover Operation (including drop last party). Additional in-call features will be available if supported by the local proxy - find me, inbound call management and outbound call management.
- Contact or Autodial Favorite Features are displayed on the Phone Screen.
- Presence is not supported.
- "A" (Avaya) Menu Options & Settings are blocked under minimal survivability configurations. Any of the more extensive survivability configurations (for example, moving subscriptions to a secondary SM/BSM for simultaneous registration) allow access to the Avaya Menu and updates to Options & Settings. Likewise, Contacts can be accessed and updated with configurations supported in Software Release 2.5 and up.
- Craft changes may be made and are saved locally on the phone.
- If the phone is logged out during failover, the local phone cache is cleared.

User Experience During Fail Back

For SIP software Release 2.5+, Fail Back (F/B) transition occurs when the Phone detects that the primary server is up, regardless if secondary controller is up.

- Fail back will not happen during an active call. If no calls are in progress, fail back 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.
- Pre-failover Visiting User status maintained after failback.
- In software Release 2.5+ users can access and update Avaya Menu options and the browser, with the exception of activating any click-to-dial links on a Web page.

User Interface Feature Failover Operation

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

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

Appendix A: Glossary of Terms

802.1D **802.1Q**	802.1Q defines a layer 2 frame structure that supports VLAN identification and a QoS mechanism usually referred to as 802.1D.
802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. Applicable 9600 Series IP deskphones support IEEE 802.1X for pass-through and for Supplicant operation with the EAP-MD5 authentication method. SIP Software Releases 2.0 and up support 802.1X.
Active Controller	The SIP Registrar/Proxy server the deskphone believes is the one and only authoritative proxy at a given time. It is the highest priority available controller.
ARP	Address Resolution Protocol, used, for example, to verify that the IP Address provided by the DHCP server is not in use by another IP deskphone.
Available Controller(s)	The subset of Monitored controllers that respond to the 'Maintenance Check' as part of determining available controllers during Failover.
CELP	Code-excited linear-predictive. Voice compression requiring only 16 kbps of bandwidth.
CLAN	Control LAN, a type of circuit pack.
CNA	Converged Network Analyzer, an Avaya product to test and analyze network performance.
Configured Controller(s)	As of SIP software Release 2.4, the list of controllers that the phone will attempt to monitor when Failover occurs. The (list of) elements in the SIP_CONTROLLER_LIST parameter, which can also come from SES/SM and the user interface.
Controller	The new name for a SIP proxy, for example, SES, SM, or a local gateway, or local survivable gateway.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
DNS	Domain Name System, an IETF standard for ASCII strings to represent IP Addresses. The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP Addresses. Avaya 9600 Series IP Telephones can use DNS to resolve names into IP Addresses. In DHCP, TFTP, and HTTP files, DNS names can be used wherever IP Addresses were available as long as a valid DNS server is identified first.

EAP	Extensible Authentication Protocol, or EAP, a universal authentication framework frequently used in wireless networks and Point-to-Point connections defined by RFC 3748. EAP provides some common functions and a negotiation of the desired authentication methods, two of which are EAP-MD5 and EAP-TLS. When EAP is invoked by an 802.1X enabled NAS (Network Access Server) device such as an 802.11 a/b/g Wireless Access Point, modern EAP methods provide a secure authentication mechanism and negotiate a secure PMK (Pair-wise Master Key) between the client and the NAS.
Failover	Selection of a lower priority call controller to become the active controller, when the highest-priority (primary) call controller becomes unavailable.
Failback	Return to normal operation by selection of the highest-priority (primary) call controller as the active controller.
H.323	A TCP/IP-based protocol for VoIP signaling. An alternative to SIP for VoIP signaling. One of the two protocols 9600 Series IP Telephones support.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	A secure version of HTTP.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.
LAN	Local Area Network.
LLDP	Link Layer Discovery Protocol. All IP deskphones with an Ethernet interface support the transmission and reception of LLDP frames on the Ethernet line interface in accordance with IEEE standard 802.1AB. SIP Software Releases 2.0 and up support LLDP.
MAC	Media Access Control, ID of an endpoint.
Media Channel Encryption	Encryption of the audio information exchanged between the IP deskphone and the call server or far end telephone.
Monitored Controller(s)	A SIP Registrar/Proxy server that the deskphone knows about and to which the phone periodically checks IP and SIP connectivity.
NAPT	Network Address Port Translation.
NAT	Network Address Translation.
OPS	Outboard Proxy SIP.
PPM	Personal Profile Manager, part of the SIP Enablement Services (SES) platform. PPM is responsible for maintaining and managing end users' personal information in the system.
Primary Controller	The controller that appears first in the configured controller list.

Proxy Server	An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, meaning its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy, for example, making sure a user is allowed to make a call. A proxy interprets, and if necessary, rewrites specific parts of a request message before forwarding it.
PSTN	Public Switched Telephone Network, the network used for traditional telephony.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks.
RSVP	Resource ReSerVation Protocol, used by hosts to request resource reservations throughout a network.
RTCP	RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service.
RTP	Real-time Transport Protocol. Provides end-to-end services for real-time data such as voice over IP.
SCEP	Simple Certificate Enrollment Protocol, used to obtain a digital certificate.
SDP	Session Description Protocol. A well-defined format for conveying sufficient information to discover and participate in a multi session.
SES	SIP Enablement Services, the Avaya solution for SIP telephony with Avaya Communication Manager.
Session Manager (SM)	Avaya Aura™ Session Manager, the SIP proxy for Avaya Aura™, an alternative to SES as of SIP software Release 2.5.
Signaling Channel Encryption	Encryption of the signaling protocol exchanged between the IP deskphone and the call server. Signaling channel encryption provides additional security to the security provided by channel encryption.
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.
SNTP	Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet.
SRTCP	Secure Real-time Transport Control Protocol.
SRTP	Secure Real-time Transport Protocol.
Surviveable Call Processor	A SES term for the active controller after failover.
Surviveable Gateway	Audiocodes server used as a gateway to survive failover. A supported local gateway with Proxy or B2BUA capabilities.

TCP/IP	Transmission Control Protocol/Internet Protocol, a network-layer protocol used on LANs and internets.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP deskphones. SIP deskphones use HTTP or HTTPS instead of TFTP.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications.
TLV	Type-Length-Value elements transmitted and received as part of Link Layer Discovery Protocol (LLDP).
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
Unnamed Registration	Registration with Avaya Communication Manager by an IP deskphone with no extension. Allows limited outgoing calling.
URI & URL	Uniform Resource Identifier and Uniform Resource Locator. Names for the strings used to reference resources on the Internet (for example, HTTP://....). URI is the newer term.
VLAN	Virtual LAN.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.
WML	Wireless Markup Language, used by the 9600 Series IP Telephone Web Browser to communicate with WML servers.

4 of 4

Appendix B: Countries With Specific Network Progress Tones

Overview

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

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

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

Country List

A:

Abu Dhabi

Albania

Argentina

Australia

Austria

B:

Bahrain
Bangladesh
Belgium
Bolivia
Bosnia
Botswana
Brunei
Bulgaria

C:

China (PRC)
Colombia
Costa Rica
Croatia
Cyprus

D:

Denmark

E:

Ecuador
El Salvador
Egypt

F:

Finland

France

G:

Germany

Ghana

Greece

Guatemala

H:

Honduras

Hong Kong

I:

Iceland

India

Indonesia

Ireland

Israel

J:

Japan

Jordan

K:

Kazakhstan

Korea

Kuwait

L:

Lebanon

Liechtenstein

M:

Macedonia

Malaysia

Mexico

Moldova

Morocco

Myanmar

N:

Netherlands
New Zealand
Nicaragua
Nigeria
Norway

O:

Oman

P:

Pakistan
Panama
Paraguay
Peru
Philippines
Poland
Portugal

Q:

Qatar

R:

Romania
Russia

S:

Saudi Arabia
Serbia
Singapore
Slovakia
Slovenia
Spain
South Africa
Sri Lanka
Swaziland
Sweden
Switzerland
Syria

T:

Taiwan
Tanzania
Thailand
Turkey

U:

Ukraine
United Arab Emirates
United Kingdom
Uruguay
USA

V:

Venezuela
Vietnam

Y:

Yemen

Z:

Zimbabwe

Index

Numerical

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W