



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

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, <https://support.avaya.com/LICENSEINFO> UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

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

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the

documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED

PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

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

Regulatory Statements

Australia Statements

Handset Magnets Statement:



Danger:

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

Industry Canada (IC) Statements

RSS Standards Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage, et
2. L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Radio Transmitter Statement

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Radiation Exposure Statement

This device complies with 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.

Cet appareil est conforme aux limites d'exposition aux rayonnements RF d'Industrie Canada énoncés dans la population générale (environnement non contrôlé) et ne doivent pas être co-situés ou exploités conjointement avec une autre antenne ou émetteur.

Japan Statements

Class B Statement

This is a Class B product based on the standard of the VCCI Council. If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。 VCCI-B

Denan Power Cord Statement



Danger:

Please be careful of the following while installing the equipment:

- Please only use the connecting cables, power cord, and AC adapters shipped with the equipment or specified by Avaya to be used with the equipment. If you use any other equipment, it may cause failures, malfunctioning, or fire.
- Power cords shipped with this equipment must not be used with any other equipment. In case the above guidelines are not followed, it may lead to death or severe injury.



警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

- 接続ケーブル、電源コード、ACアダプタなどの部品は、必ず製品に同梱されております添付品または指定品をご使用ください。添付品指定品以外の部品をご使用になると故障や動作不良、火災の原因となることがあります。
- 同梱されております付属の電源コードを他の機器には使用しないでください。上記注意事項を守らないと、死亡や大怪我など人身事故の原因となることがあります。

México Statement

The operation of this equipment is subject to the following two conditions:

1. It is possible that this equipment or device may not cause harmful interference, and
2. This equipment or device must accept any interference, including interference that may cause undesired operation.

La operación de este equipo está sujeta a las siguientes dos condiciones:

1. Es posible que este equipo o dispositivo no cause interferencia perjudicial y
2. Este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

Power over Ethernet (PoE) Statement

This equipment must be connected to PoE networks without routing to the outside plant.

Taiwan Low Power Radio Waves Radiated Devices Statement

802.11b/802.11g/BT:

Article 12 — Without permission granted by the NCC, any company, enterprise, or user is not allowed to change frequency, enhance transmitting power or alter original characteristic as well as performance to an approved low power radio-frequency devices.

Article 14 — The low power radio-frequency devices shall not influence aircraft security and interfere legal communications; If found, the user shall cease operating immediately until no interference is achieved. The said legal communications means radio communications is operated in compliance with the Telecommunications Act. The low power radio-frequency devices must be susceptible with the interference from legal communications or ISM radio wave radiated devices.

802.11b/802.11g/BT 警語：

第十二條→經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條→低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

U.S. Federal Communications Commission (FCC) Statements

Compliance Statement

The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

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 interferences that may cause undesired operation.

Class B Part 15 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 designated to provide reasonable protection against harmful interferences 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 interferences 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 or more 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.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 8 in or 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

EU Countries

This device complies with the essential requirements and other relevant provisions of Directive 1999/5/EC. A copy of the Declaration may be obtained from <http://support.avaya.com> or Avaya Inc., 211 Mt. Airy Road, Basking Ridge, NJ 07920 USA.

General Safety Warning

- Use only the Avaya approved Limited Power Source power supplies specified for this product.
- There is a risk of explosion if you use an incorrect type of battery in the DECT handset. Replace used batteries with the correct battery type: Nickel Metal Hydride (NiMH), rechargeable, size AAA.
 - This product uses NiMH batteries which are recyclable and must not be disposed of as municipal waste to reduce the risk of releasing substances into the environment. At the end of the battery's useful life, remove the rechargeable batteries and take them to the nearest battery collection location to be recycled.
- Ensure that you:
 - Do not operate the device near water.
 - Do not use the device during a lightning storm.
 - Do not report a gas leak while in the vicinity of the leak.
 - Limit the power to the device over telecommunications wiring to 36-57 volt DC or ≤ 1.3 ampere DC.

To ensure the EMC Class B compliance when using a Collaboration Station with an external HDMI monitor, the monitor must be of a type with an external AC or DC power supply.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction	10
Purpose	10
Chapter 2: 9600 Series IP Deskphones overview	11
9600 Series IP Deskphones overview	11
9600 Series IP Deskphones models	12
New in this release	12
Administrator responsibilities	13
Administrative requirements	13
Administration methods	14
Administration Checklist	15
Administrative checklist	15
Chapter 3: Configuring Avaya Aura® for Avaya Deskphones SIP	18
Supported SIP environments	18
Button modules overview	18
SIP deskphone administration on Communication Manager	19
Feature button for the stations	21
SIP deskphone administration on Session Manager	23
About controllers	24
Chapter 4: Configuration through the DHCP options	25
DHCP configuration overview	25
DHCP Option configurations	25
Codes for Option 43	28
DHCP lease time	28
Parameter configuration through DHCPACK	29
DHCP site-specific option	30
Chapter 5: Configuration through the settings file	32
Settings file	32
Configuring the settings file	32
General parameters	32
Server addresses and ports parameters	32
Protocol-specific parameters	37
Dial plan parameters	44
Audio parameters	44
Logging and debugging parameters	45
Configuration parameters	48
Port ranges parameters	50
Audio operation and quality monitoring parameters	50
General and phone application timer parameters	51
Deskphone interface settings parameters	52

Network parameters.....	57
General network parameters.....	57
Ethernet parameters.....	59
QoS parameters.....	60
VLAN parameters.....	60
IEEE 802.1.x parameters.....	61
Account and password parameters.....	62
Presence parameters.....	62
Microsoft Exchange parameters.....	63
WML browser parameters.....	64
Chapter 6: Configuration through LLDP.....	65
LLDP overview.....	65
LLDPDU transmitted by the deskphones.....	66
TLV impact on system parameter values.....	67
Chapter 7: Security.....	69
Security.....	69
Certificate management.....	70
Parameter configuration for secure installation.....	71
Chapter 8: Administering deskphone options.....	73
Administering a VLAN.....	73
About VLAN Tagging.....	73
The VLAN default value and priority tagging.....	73
Automatic detection of a VLAN.....	74
VLAN separation rules and related parameters.....	75
Administering display language options.....	77
Push server.....	78
SNMP activation.....	78
Registration and authentication.....	78
IP address and settings reuse.....	79
Ping and traceroute.....	80
TCP and UDP ports.....	80
Received packets (destination = SIP deskphone).....	80
Transmitted packets (source = SIP deskphone).....	82
Network audio quality.....	83
About DNS addressing.....	83
About IEEE 802.1X.....	84
Administering emergency numbers.....	85
The Avaya Menu administration file.....	85
GROUP parameter for customized user groups.....	88
Administering settings at the deskphone.....	89
Administering enhanced local dialing.....	90
Setting the dial plan on SIP deskphones.....	91
Setting the date and time on SIP deskphones.....	93

History.....	93
Call treatment in a logged out state and busy Call Appearances.....	94
Customizing ring tones.....	94
Korean ring tones.....	95
Customized ring tones.....	95
Downloadable ring tones.....	97
Administering voice mail.....	98
Administering headset profiles.....	99
Administering Presence.....	99
Presence overview.....	99
Presence profile.....	100
Error conditions.....	101
Chapter 9: Customizing 9600 Series IP Deskphones.....	102
Avaya Aura® Call Center Elite features	102
Applications and features provisioning.....	103
Team Button overview.....	104
Team Button parameters.....	105
Direct Transfer.....	106
Team Button ring.....	106
Team Button override.....	106
Enhanced Call Forward.....	107
Multiple Device Access.....	107
Advanced call conference.....	108
Setting a large font size for the display.....	108
Setting the background logo.....	109
Background logo specifications.....	109
Creating and using localized language files.....	110
Language localization tool field descriptions.....	111
WML browser.....	111
WML browser overview.....	111
Administering the WML browser.....	112
Integrating Microsoft® Exchange.....	113
Network progress tones overview.....	113
Chapter 10: System Failover and Survivability.....	118
Supporting survivability.....	118
Survivability configuration examples.....	119
Survivability requirements.....	121
Provisioning survivability for SIP Deskphones.....	121
Configuring survivability.....	122
Setting a controller via the user interface.....	123
Controller Determination and Survivability Activity.....	123
Determine controllers to monitor.....	124
Determine which monitored controllers are available.....	124

Select the active controller.....	125
AST feature determination.....	126
PPM synchronization.....	127
Failover/failback behavior.....	128
About the user interface/failover experience.....	131
User interface in failover/failback.....	131
User experience during failover transition.....	131
User experience during stable failover.....	134
User experience during failback.....	135
User experience during failover.....	135
Chapter 11: Related resources	137
Documentation.....	137
Finding documents on the Avaya Support website.....	138
Support.....	139

Chapter 1: Introduction

Purpose

This document contains information about how to perform 9600 Series IP Deskphones administration tasks including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks. This document covers administration information for only the following 9600 Series IP Deskphones models:

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

This document is intended for people who perform 9600 Series IP Deskphones system administration tasks such as backing up and restoring data and managing users.

Chapter 2: 9600 Series IP Deskphones overview

9600 Series IP Deskphones overview

9600 Series IP Deskphones is a series of desk handset devices that you can use for unified communication. The series leverages the enterprise IP network and eliminates the need for a separate voice network.

Avaya 9600 Series IP Deskphones offers high audio quality and customizability with low power requirements. With the high-performance models of this series that can operate in both the H.323 and the Session Initiation Protocol (SIP) environment, you can:

- Make conference calls more efficient and enhance customer interactions with high-quality audio.
- Gain access to information quickly through easy-to-read and high-resolution displays.
- Speed completion of common telephony tasks by using prompts on touch screens.
- Improve productivity with context-sensitive graphical interfaces that enhance call control and call management.
- Create a survivable, scalable infrastructure that delivers reliable performance and flexible growth as business needs change.
- Increase performance by deploying Gigabit Ethernet within your infrastructure.
- Reduce energy costs using efficient Power-over-Ethernet (PoE) including sleep mode which lowers energy consumption dramatically.

The 9600 Series IP Deskphones works with the Avaya Aura® environment to provide a flexible architecture that works with your investments and accommodates growth as your business needs change.

Related links

[9600 Series IP Deskphones models](#) on page 12

9600 Series IP Deskphones models

Deskphone model	Description
9601	The 9601 deskphone is SIP-only phone that provides a four-row monochrome display and two lines with dual red and green LEDs. The phone has a built in 10/100 Ethernet switch with a port for your personal computer or a laptop.
9608/9608G	You can use up to eight lines for the deskphone. The deskphone supports a traditional user interface and a graphical monochrome display. The 9608 has a built in 10/100 Ethernet switch, and the 9608G has an integrated Gigabit.
9611G	The 9611G has a traditional user interface and a graphical color display. You can use up to eight lines with the 9611G deskphone. The 9611G deskphone has an integrated Gigabit and a USB interface. The deskphone has a graphical color display with a white backlight.
9621G	The 9621G IP deskphone provides gigabit capability and touch screen functionality. Customers with a need for gigabit connectivity to the desktop prefer the 9621G deskphone.
9641G/9641GS	The 9641G/9641GS deskphone provides advanced capabilities with a color touch screen, wideband speaker, USB interface, Bluetooth® enabled headset support, and gigabit connectivity to the desktop. Customers who require gigabit capability for the desktop and the option to add more advanced capabilities prefer the 9641G/9641GS deskphone.

Related links

[9600 Series IP Deskphones overview](#) on page 11

New in this release

General enhancements

- Improved upgrade process for the deskphones

Administrative features

- Introduced Hunt group busy button to start or stop receiving calls for the hunt group.

Administrator responsibilities

An administrator can perform the following tasks:

- Manage network configurations.
- Provision features.
- Manage accounts.
- Manage app-specific configurations.
- Manage upgrade configurations.
- Manage security configurations.

Related links

[Administrative requirements](#) on page 13

Administrative requirements

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

- IP Address management.
- Tagging Control and VLAN administration.
- Quality of Service (QoS) administration.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP), as applicable.
- Administering the deskphone to LAN interface using the PHY1 parameter.
- Administering the deskphone to PC interface using the PHY2 parameter.
- Application-specific deskphone administration using a text settings file with various deskphone specific parameters. The file resides on an HTTP or HTTPS server and the deskphone retrieves the file when powered on.
- Maintaining the information on the call server.
- Manually entering the information by means of the deskphone dialpad using CRAFT procedures.
- Administering the DHCP server.
- Editing the configuration file on the applicable HTTP or HTTPS file server.
- User modification of certain parameters, when given administrative permission to do so.

Note:

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

Related links

[Administrator responsibilities](#) on page 13

Administration methods

You can use the following methods to administer the devices. The following table lists the parameter categories that you can administer through each of the corresponding methods.

Method	Can administer					
	IP addresses	Ethernet Interface	Tagging and VLAN	Network Time Server	Quality of Service	Application-specific parameters
DHCP	✓	✓	✓	✓	—	✓
LLDP	✓	✓	✓	—	—	—
Settings file	—	✓	✓	✓	✓	✓
Avaya Aura® Session Manager	—	—	✓	—	✓	—
Settings app on the device	✓	✓	✓	—	—	✓

Precedence of the methods

Most of the parameters are configurable through multiple methods. If you configure a parameter through more than one method, the device applies the settings of the method that has a higher precedence. For the parameters that are not backed up through PPM, the non-default value has the highest precedence. The following list shows the precedence of the methods in the highest to lowest order:

1. Settings app on the device. There is an exception of DHCP getting a higher precedence when:
 - IP address is set through DHCP.
 - USE_DHCP parameter is set to 1 to assign a higher priority to DHCP.
2. Avaya Aura® Session Manager.
3. Settings file.
4. DHCP.
5. LLDP. There is an exception of LLDP getting a higher precedence than the settings file and DHCP when the layer 2 parameters, such as L2QVLAN, L2Q, L2QAUD, L2QVID, L2QSIG, DSCPAUD, DSCPSIG, DSCPVID, and PHY2VLAN are set through LLDP.

Note:

The parameter resets to its default value when it is removed from the settings file and is not defined through any other source.

Administration Checklist

No.	Task	Reference	✓
1	Ensure that the device is set-up, assembled, and operating.	<i>Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP</i>	
2	Ensure that the initial configuration parameters are provisioned.	<i>Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP</i>	

Related links

[Administrative checklist](#) on page 15

Administrative checklist

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

No.	Task	Description	Notes	✓
1.	Network requirements assessment.	Determine that network hardware is in place and		

Table continues...

No.	Task	Description	Notes	✓
		can handle deskphone system requirements.		
2.	Administer Avaya Aura® Communication Manager.	Verify that the call server has a valid license file and is administered for Voice over IP (VoIP) Verify the individual deskphones are administered as desired on the Communication Manager station forms.		
3.	Administer the proxy server.	Administration for Session Manager. See <i>Administering Avaya Aura® Session Manager</i> documentation on the Avaya support site.		
4.	Administer Avaya Aura® System Manager.	Administration for System Manager (SMGR). See <i>Avaya Aura® System Manager</i> documentation on the Avaya support site.		
5.	DHCP server installation.	Install a DHCP application on at least one new or existing PC on the LAN.		
6.	Administer DHCP application.	Add IP deskphone administration to the DHCP application.		
7.	Administer Network Time Server.	Set values for Simple Network Time Protocol (SNTP).		
8.	HTTP/HTTPS server installation.	Install an HTTP/HTTPS application on at least one new or existing PC on the LAN.		
9.	Install the deskphone SIP software, the settings file, and the upgrade file onto the HTTP or HTTPS server.	Download the files from the Avaya support site.		
10.	Administer WML servers (Optional).	Add WML content as applicable to new or existing WML servers.		

Table continues...

No.	Task	Description	Notes	✓
		Administer push content as applicable.		
11.	Modify settings file.	Edit the settings file as necessary for your environment, using your own tools.		
12.	Administer deskphones locally.	Use GROUP parameter for group administration or CRAFT for each deskphone.		
13.	Installation of deskphones in the network.	See <i>Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP</i> documentation for more details.		
14.	Allow user to modify Options, if applicable	Set different parameters in the settings file.		

Related links

[Administration Checklist](#) on page 15

Chapter 3: Configuring Avaya Aura® for Avaya Deskphones SIP

Supported SIP environments

The SIP software supports the following configurations for the 9600 Series IP Deskphones :

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

The deskphone features depend on the Communication Manager and Session Manager configuration.

For more information about the configuration and operation of the deskphone features, see the following Communication Manager documents:

- *Avaya Aura® Communication Manager Feature Description and Implementation*
- *Administering Avaya Aura® Communication Manager*

Button modules overview

You can add up to three BM12 or SBM24 button modules to the deskphones. All button modules added to a single deskphone must be the same model. The maximum combined number of features that you can configure on button modules is 48. You can configure all button module lines as long as you do not exceed this maximum number.

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

*** Note:**

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

The following table contains the IEEE switch settings for the button modules:

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

SIP deskphone administration on Communication Manager

The SIP-based calling features in the following table can be invoked directly on 9600 Series IP Deskphones or using a feature button provisioned using Avaya Aura® Communication Manager. Communication Manager automatically processes other 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.

For more information see *Avaya Aura® Communication Manager Feature Description and Implementation* and other Communication Manager administration documents at the Avaya Support website: <http://support.avaya.com/>

The Avaya SIP solution configures all SIP Deskphones in Communication Manager as OPS.

Feature	Survivable operation with third-party proxy	Normal operation with Communication Manager and Session Manager
3-Way Conferencing	Yes	No
Local, on the deskphone		
Conference using conference server	—	Yes
Auto Intercom	—	Yes
Automatic Call Back/Cancel	—	Yes
Call Forward All Calls	Yes	Yes
on/off		
Call Hold	Yes	Yes

Table continues...

Feature	Survivable operation with third-party proxy	Normal operation with Communication Manager and Session Manager
Call Park and Unpark	—	Yes
Call Pick-Up Group	—	Yes
Call Pickup Directed	—	Yes
Calling Party Number Block/Unblock	—	Yes
Dial Intercom	—	Yes
Directed Call Pick-Up	—	Yes
Distinctive Alerting	—	Yes
EC500	—	Yes
Enhanced call forward	—	Yes
Exclusion	—	Yes
Exchange integration	Yes	Yes
Extend Call for EC500	—	Yes
Extended Group Call	—	Yes
Group Call Pickup	—	Yes
Group paging	—	Yes
Hotline	—	Yes
Instant Messaging	—	Yes
LNCC	—	Yes
Malicious Call Trace	—	Yes
Message Waiting Indication	MWI is not available. If the PSTN_VM_NUM parameter is administered, users can gain access to the voice mailbox using the Message button.	Yes
Mute alert	Yes	Yes
One Touch Recording	—	Yes
Presence	—	Yes
Priority Call	—	Yes
Send All Calls Enable/Disable	—	Yes
SSH support	Yes	Yes

Table continues...

Feature	Survivable operation with third-party proxy	Normal operation with Communication Manager and Session Manager
Team button	—	Yes
Team button SAC/ CFWD/ECF override	—	Yes
Third Party Call Forward	—	Yes
Third Party Call Forward Busy Don't Answer	—	Yes
Third Party Send All Calls	—	Yes
Transfer - attended	Yes	Yes
Transfer - unattended	—	Yes
Transfer upon hang-up	—	Yes
URI dialing	Yes	Yes
WML browser	Yes	Yes

Related links

[Feature button for the stations](#) on page 21

Feature button for the stations

The following buttons can be administered for 9600 Series IP Deskphones. Some deskphone models might not support all the features. For more information, see the feature specific details.

Feature	Administration notes
3-Way Conferencing	—
Local, on the deskphone	
Conference using conference server	—
Audix One-Touch Recording	—
Auto Callback/Cancel	—
Auto Intercom	Add an intercom group # (in the Group, add your extension and dial code (DC), then add the other person's extension and DC. Add an auto-icom button, icom group #, DC.
Autodial	—
Bridged Call Appearances	—
Busy Indicator	—
Call Appearances	—
Call Forward (all)	—

Table continues...

Feature	Administration notes
Call Hold	—
Call Park	—
Call Unpark	Regardless of Communication Manager Station button administration, this feature will show on the Features menu automatically on Session Manager 5.2+ configurations. In Session Manager 6.0+ this feature does not appear automatically.
Call Pickup	—
Call Pickup Group	—
Calling Party Number Block/Unblock	—
CPN Block	—
CPN Unblock	—
Dial Intercom	On Communication Manager: 1. Add an intercom group # (in the group, add your extension and dial code, then add other person's extension and dial code. 2. Add a dial-icom button, icom group #, (no dial code).
Directed Call Pickup	—
Distinctive Alerting	—
EC500 Enable/Disable	—
EC500 Extend Call	—
Enhanced call forward	—
Exclusion	—
Extended Call Pickup	Regardless of Communication Manager Station button administration, this feature will show on the Features menu automatically.
LNCC	—
Offline call log	—
Malicious Call Trace	—
MCT Activation	—
Message Waiting Indication	Supported in Communication Manager 6.0.
Music on Hold	—
One Touch Recording	—
Priority Call	—
Send All Calls	—
Team button	—
Team button redirection override	—
Transfer (Attended)	—

Table continues...

Feature	Administration notes
Transfer (Unattended - one button transfer)	—
Transfer upon hung-up	—

For more information about administering Avaya Aura® Communication Manager for 9600 Series IP Deskphones, see the following documents at the Avaya Support website: <http://support.avaya.com/>

- *Administering Avaya Aura® Communication Manager*
- *Avaya Aura® Communication Manager Feature Description and Implementation*
- *Administering Avaya Aura® Communication Manager as a Feature Server*, 7 03-603479, and related Avaya Aura® Session Manager documents.

Related links

[SIP deskphone administration on Communication Manager](#) on page 19

SIP deskphone administration on Session Manager

9600 Series IP Deskphones might display a prompt asking for the extension and password during the administration on Avaya Aura® Session Manager. The deskphones use the extension and password to communicate with Session Manager, which communicates with Avaya Aura® Communication Manager.

For more information, see the following documents at the Avaya Support website: <http://support.avaya.com/>

- For information about the installation process, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*.
- For information about the Communication Manager administration with Session Manager, see the following Session Manager and Avaya Aura® System Manager documents:
 - *Avaya Aura® Session Manager Overview and Specification*
 - *Deploying Avaya Aura® Session Manager*
 - *Upgrading Avaya Aura® Session Manager*
 - *Administering Avaya Aura® Session Manager*
 - *Maintaining Avaya Aura® Session Manager*
 - *Troubleshooting Avaya Aura® Session Manager*
 - *Avaya Aura® Session Manager Case Studies*
 - *Deploying Avaya Aura® System Manager on System Platform*
 - *Deploying Avaya Aura® System Manager*
 - *Upgrading Avaya Aura® System Manager on System Platform*
 - *Upgrading Avaya Aura® System Manager to Release 7.0.1*

- *Administering Avaya Aura® System Manager for Release 7.0.1*
- *Avaya Aura® System Manager Release Notes*

About controllers

A controller is a proxy server that routes the calls. A controller, such as Avaya Aura® Session Manager or IP Office, also works as a registrar and an interface between Communication Manager and phones.

Chapter 4: Configuration through the DHCP options

DHCP configuration overview

The 9600 Series IP Deskphones connect to the DHCP server during the boot up. You can configure the DHCP server to provide the following information to the device:

- IP address
- Subnet mask
- IP address of the router
- IP address of the HTTP or HTTPS file server
- IP address of the SNTP server
- IP address of DNS

DHCP Option configurations

The options that are specified in the following table can be configured in the DHCP server.

Option	Description
Option 1	Specifies the subnet mask of the network.
Option 3	Specifies the gateway IP address list. The list can contain up to 127 total ASCII characters. Separate more than one IP address with commas with no intervening spaces.
Option 6	Specifies the DNS server address list. The list can contain up to 127 total ASCII characters. Separate more than one IP address with commas with no intervening spaces. The deskphone supports DNS and the dotted decimal addresses. The deskphone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the contents of DHCP Option 6. At least one address in option 6 must be a valid, nonzero, dotted decimal address, otherwise the DNS address fails.
Option 12	Specifies the host name.

Table continues...

Option	Description
	AVohhhhhh, where: - o is one of the following values based on Object Unique Identifier (OUI) derived from the first three octets of the deskphone MAC address: - A if OUI is 00-04-0D - B if OUI is 00-1B-4F - E if OUI is 00-09-6E - L if OUI is 00-60-1D - T if the OUI is 00-07-3B - X if the OUI is anything else - hhhhh are the ASCII characters for the hexadecimal representation of the last three octets of the deskphone MAC address.
Option 15	Specifies the domain name. The domain name is required to resolve DNS names into IP addresses. Configure this option if you use a DNS name for the HTTP server. Otherwise, you can specify a domain as part of customizing the HTTP server. This domain name is appended to the DNS addresses specified in option 6 before the deskphone attempts to resolve the DNS address. The deskphone queries the DNS address in the order they are specified in option 6. If there is no response from an address, the deskphone queries the next DNS address. As an alternative to administering DNS by DHCP, you can specify the DNS server and domain name in the HTTP script file. If you use the script file, you must configure the DNSSRV and DOMAIN parameters so that you can use the values of these parameters in the script.  Note: Administer option 6 and option 15 appropriately with DNS servers and domain names respectively.
Option 42	Specifies the SNTP IP address list. List servers in the order of preference. The minimum length is 4 and the length must be a multiple of 4.
Option 43	Specifies the encapsulated vendor-specific options that clients and servers use to exchange the vendor-specific information. Option 43 is processed only if the first code in the Option is 1 with a value of 6889. All values are interpreted as strings of ASCII characters that are accepted with or without a null termination character. Any invalid value is ignored and the corresponding parameter value is not set. For information on codes for this parameter, see Codes for option 43 on page 28.
Option 51	Specifies the DHCP lease time. If this option is not received, the DHCP OFFER is not accepted. Assign 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, so that the renewal and rebinding procedures are not necessary even if options 58 and 59 are received. Expired leases causes the device to reboot.

Table continues...

Option	Description
Option 52	Specifies the overload option. If this option is received in a message, the device interprets the sname and file parameters.
Option 53	Specifies the DHCP message type. The value can be one of the following: • 1 for DHCPDISCOVER • 3 for DHCPREQUEST For DHCPREQUEST sent to renew the device IP address lease: • If a DHCPACK is received in response, a log event record is generated with a Log Category of DHCP. • If a DHCPNAK is received in response, the device immediately ceases IP address usage, generates a log event record, sets IPADD to 0.0.0.0, and enters the DHCP INIT state.
Option 55	Specifies the parameter request list. Acceptable values are: • 1 for subnet mask • 3 for router IP addresses • 6 for domain name server IP addresses • 7 for log server • 15 for domain name • 26 for interface MTU • 42 for NTP servers
Option 57	Specifies the maximum DHCP message size. Set the value to 1500. Set the value to 1000.
Option 58	Specifies the 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.
Option 59	Specifies the 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.
Option 242	Specifies the site-specific option. This option is optional. If you do not configure this option, ensure that one of the following parameters is configured appropriately elsewhere: • FILE_SERVER_URL • HTTPSRVR • TLSSVR

Parameters such as HTTPSRVR and SIP_CONTROLLER_LIST support values with lengths up to 255 octets, but you must set shorter values when you are setting them through DHCP.

Related links

[Codes for Option 43](#) on page 28

[DHCP lease time](#) on page 28

[Parameter configuration through DHCPACK](#) on page 29

Codes for Option 43

The supported codes for Option 43 and the corresponding parameters are as follows:

Code	Parameter
1	Does not set any parameter. The value must be 6889.
2	HTTPSRVR
3	HTTPDIR
4	HTTPPORT
5	TLSSRVR
6	TLSDIR
7	TLSPORT
8	TLSSRVRID
9	L2Q
10	L2QVLAN
11	PHY1STAT
12	PHY2STAT
13	PROCSTAT
14	SIG
15	SIP_CONTROLLER_LIST

Related links

[DHCP Option configurations](#) on page 25

DHCP lease time

The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP address. However, if the network has problems and the only DHCP server is centralized or if the DHCP server itself has problems, the device will not receive responses to its request for a renewal of the lease. In this case the device is not usable until the server can respond. Configure system such that once the IP address is assigned to the device, the device continues using that address after the DHCP lease expires, until a conflict with another device is detected.

The system parameter DHCPSTD allows an administrator to specify that the device will either:

- Comply with the DHCP standard by setting DHCPSTD to 1.
- Continue to use its IP address after the DHCP lease expires by setting DHCPSTD to 0.

The latter case is the default. If the default is invoked, after the DHCP lease expires the deskphone continues to broadcast DHCPREQUEST messages for its current IP address, and it sends an ARP Request for its own IP address every five seconds.

The messages continue to be sent until the device receives a DHCPACK, a DHCPNAK, or an ARP reply. After receiving a DHCPNAK or ARP reply, the device displays an error message, sets its IP address to 0.0.0.0, and attempts to contact the DHCP server again. Log events are generated for either case.

Depending on the DHCP application you choose, the application might not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client a day or more. 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 that there are two IP addresses, therefore two possible DHCP leases. Assume that there are three IP devices in the network, two of which are using the two available IP addresses. When the lease for the first two devices expires, the third device cannot get a lease until the reservation period expires. Even if the other two devices are removed from the network, the third device remains without a lease until the reservation period expires.

Related links

[DHCP Option configurations](#) on page 25

Parameter configuration through DHCPACK

Parameter	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
DNSSRV	Option 6, if received, which might be a list of IP addresses
HTTPSRVR	The siaddr parameter, if that parameter is non-zero
IPADD	The yiaddr parameter
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

Related links

[DHCP Option configurations](#) on page 25

DHCP site-specific option

You can set the values of site-specific configuration parameters through a DHCP option. The default DHCP option to set the site-specific configuration parameters is 242. You can also use any option between 128 to 254. Whichever option you select to specify the site-specific configuration, you must specify that option number in the Site-Specific Option Number (SSON) parameter. You can set the SSON parameter through the device interface.

Following is an example of the DHCP 242 option string that specifies the HTTPSRVR and the Voice VLAN that the device must connect to.

```
HTTPSRVR=10.138.251.67,L2QVLAN=1104
```

The following table lists the site-specific configuration parameters that you can define for the device.

Parameter	Description
FILE_SERVE R_URL	Specifies the list of URL for downloading image and configuration files. This parameter has higher precedence over HTTPSRVR, HTTPPORT, HTTPDIR, TLSSRV, TLS DIR, and TLS PORT.
HTTPDIR	Specifies the path to prepend to all configurations and data files the device might request when starting up, that is, the path, relative to the root of the HTTP file server, to the directory in which the device configuration and data files are stored. The path may contain no more than 127 characters and may contain no spaces. HTTPDIR is the path for all HTTP operations. The command is <code>SET HTTPDIR=<path></code> . In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use the <code>HTTPDIR=<path></code> .
HTTPPORT	Destination port for HTTP requests. The default is 80.
HTTPSRVR	IP addresses or DNS names of HTTP file servers used for downloading settings, language, and firmware files during startup. The firmware 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, that is sends Destination Unreachable messages for closed ports used by traceroute.
ICMPRED	Controls whether ICMP Redirect messages are processed. The default is 0, that is, redirect messages are not processed.
L2Q	802.1Q tagging mode. The default is 0 for automatic.
L2QVLAN	VLAN ID of the voice VLAN. The default is 0.
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 for auto-negotiate.
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 for auto-negotiate.

Table continues...

Parameter	Description
PROCPSWD	Security string used to access local procedures. The default is 27238.
PROCSTAT	Controls whether local procedures are enabled. The default is 0 for enabled.
REUSETIME	Time in seconds for IP address reuse timeout, in seconds. The default is 60 seconds.
SIG	The signaling protocol download flag that indicates the protocol applied as follows: • 0 for Default • 1 for H.323 • 2 for SIP
SIP_CONTR OLLER_LIST	SIP proxy or registrar server IP or DNS addresses that can be 0 to 255 characters, IP address in the dotted decimal name format, separated by commas and without any intervening spaces. The default is null, that is, no controllers.
TLSDIR	Used as path name that is prepended to all file names used in HTTPS GET operations during initialization. The string length can be from 0 to 127.
TLSPORT	Destination TCP port used for requests to https server in the range of 0 to 65535. The default is 443, the standard HTTPS port.
TLSSRVR	IP addresses or DNS names of Avaya file servers used to download configuration files. Firmware files can also be downloaded using HTTPS.  Note: Transport Layer Security is used to authenticate the server.
VLANTEST	Number of seconds to wait for a DHCP OFFER on a non-zero VLAN. The default is 60 seconds.

Chapter 5: Configuration through the settings file

Settings file

You can administer the 9600 Series IP Deskphones centrally through the settings file that Avaya provides with the devices. The settings file is a text file that resides on a file server and contains configuration parameters.

Configuring the settings file

About this task

Modify the settings file with appropriate values to provision the device configuration parameters.

Procedure

1. On the file server, go to the location where you downloaded the settings file.
2. Open the settings file in a text editor.
3. Set the required parameters.
4. Save the settings file.

General parameters

Server addresses and ports parameters

Parameter	Type	Default value	Description
DNSSRV	String	0.0.0.0	Specifies the DNS server IP addresses in dotted-decimal format, separated by commas with no

Table continues...

Parameter	Type	Default value	Description
			intervening spaces. The range is 0 to 255 ASCII characters including commas.
DOMAIN	String	Null	Specifies a text string that contains the domain name to be used when DNS names in parameter values are resolved into IP addresses. The range is 0 to 255 ASCII characters.
FILE_SERVER_URL	String	Null	Specifies the configured file server URLs for downloading firmware and configuration files. If this parameter is set, then the following parameters are ignored: • HTTPSRRV • HTTPPORT • HTTPDIR • TLSSRRV • TLSSRRVDIR • TLSPORT
HTTPSRRV	String	0.0.0.0	Specifies a list of IP or DNS addresses of the HTTP servers for downloading settings file, language files, and firmware during startup procedure. HTTP server addresses can be in dotted decimal or DNS format, and must be separated by commas. The range is from 0 to 255 ASCII characters including commas.
HTTPDIR	String	Null	Specifies the path to prepend to all configurations and data files that the device might request when starting up. The path is relative to the root of the HTTP file server and to the directory in which the configuration and data files are stored. The path can contain no more than 127 characters and must not contain spaces. If an Avaya file server is used to download configuration files over HTTPS, but a different server is used to download software files through HTTP, set the path of the Avaya server in the DHCP site-specific option, and set HTTPDIR again in the <code>46xxsettings.txt</code> file with the appropriate path for the second server. HTTPDIR is the path for all HTTP operations.

Table continues...

Parameter	Type	Default value	Description
			In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use the <code>HTTPTDIR=<path></code> .
HTTPPROXY	String	Null	Specifies a list of IP or DNS addresses of HTTP proxy servers. If this parameter is not null, the proxy transport address assigned in this parameter is used to set up the HTTP connection as transport protocol for SCEP, browser, and Exchange account. This parameter is not a URL and must not begin with the text <code>http://</code>, for example, <code>ca.avaya.com:8000</code>.
HTTPEXCEPTIONDOMAINS	String	Null	Specifies the domains to be excluded for use of HTTP proxy server. An HTTP connection as transport layer for SCEP is only set up through the parameter HTTPPROXY, if the right-most part of the domain portion of the MYCERTURL does not match to one of the values in this parameter.
TLS_VERSION	Numeric	0	Specifies the TLS version for all TLS connections used by the endpoints. Assign one of the following values: • 0: TLS 1.0+ • 1: TLS 1.2+  Note: Ensure that all the components through which the phone communicates are also using the same set version of the TLS.
TLSDIR	String	Null	Specifies the path name for HTTPS downloads. The range is from 0 to 127 characters.
HTTPPORT	Numeric	80	Specifies the destination port for HTTP requests. The range is from 0 to 65535.
TLSPORT	Numeric	443	Specifies the destination port for HTTPS requests. The range is from 0 to 65535.
CONFIG_SERVER	String	Null	Specifies the address of the PPM configuration server. If the SIP environment is set up such that the PPM server is at a different location than the SIP proxy server address, the device uses the configuration server address instead. The device will not use the proxy server for PPM.
SIP_CONTROLLER_LIST	String	Null	Specifies a comma separated list of IP addresses of SIP proxy or registrar server. The range is from 0 to 255.

Table continues...

Parameter	Type	Default value	Description
			The list has the following format. <code>host[:port][;transport=xxx]</code>, where: <code>host</code> is an IP address in dotted-decimal format <code>port</code> is the optional port number. If you do not specify a port number, the system uses the following default values: 5060 for UDP and TCP 5061 for TLS <code>transport</code> is the optional transport type, <code>tls</code>, <code>tcp</code>, or <code>udp</code>. If you do not specify the transport, the system uses TLS as the default type
SIMULTANEOUS_REGISTRATIONS	Numeric	3	Specifies the number of simultaneous Session Manager and Branch Session Manager registrations that the device can maintain. The range is from 1 to 3.
ENABLE_PPM_SOURCED_SIP_PROXYSRVR	Numeric	1	Specifies whether to enable PPM as a source of SIP proxy server information. Assign one of the following values: 0 1
SIPDOMAIN	String	Null	Specifies the SIP domain name for registration. The range is from 0 to 255.
SIPPORT	Numeric	5060	Specifies the port the deskphone opens to receive the SIP signaling messages over TCP. This is the listening port when SIP/TCP is used and dual socket is used with Avaya Aura® Session Manager, that is, the CONNECTION_REUSE parameter is 0. You can set this parameter only if the environment is not an Avaya environment. The range is from 1024 to 65535.
SIP_PORT_SECURE	Numeric	5061	Specifies the default SIP port for secure message transfer through TLS. This is the listening port when SIP/TLS is used and dual socket is used with Avaya Aura® Session Manager, that is, the CONNECTION_REUSE parameter is 0. You can set this parameter only if the environment is not an Avaya environment. The range is from 1024 to 65535.

Table continues...

Parameter	Type	Default value	Description
PRESENCE_SERVER	String	Null	Specifies the address and optional port of a single Presence Presenceserver. The range is from 0 to 255 characters.
MWISVR	String	Null	Specifies a list of IP or DNS addresses for Message Waiting Indicator Event Server. The range is from 0 to 255 characters. You can set this parameter only if the environment is not an Avaya environment
SNTPSRVR	String	Null	Specifies a list of IP or DNS addresses for the SNTP server. The range is from 0 to 255 characters.
LOGSRVR	String	Null	Specifies the IP or DNS addresses for the Syslog server. The range is from 0 to 255 characters.
RTCPMON	String	Null	Specifies the IP or DNS address for the RTCP monitor. You can set this parameter only if the environment is not an Avaya environment. The range is from 0 to 255 characters.
RTCPMONPORT	Numeric	5005	Specifies the RTCP monitor port number. You can set this parameter only if the environment is not an Avaya environment. The range is from 0 to 65535.
EXCHANGE_SERVER_LIST	String	Null	Specifies a list of IP or DNS addresses for the Microsoft Exchange™ server. The range is from 0 to 255 characters.
CONFERENCE_FACTORY_URI	String	Null	Specifies the conference server URI used to start an Avaya Aura® Conferencing conference call.
SIGNAL_P_CONFERENCE_SIP_HEADER	Integer	1	Specifies whether to enable P-Conference header in SIP 200 OK message sent to the Avaya Aura® Conferencing server. Assign one of the following values: • 1: P-Conference header will be sent • 0: P-Conference header will not be sent
P_CONF_OUTDIAL_PROMPT	Integer	0	Specifies whether the value of P-Conference header should contain <code>true</code> or <code>false</code> for "OutdialPrompt=". Assign one of the following values: • 1: P-Conference header should contain <code>true</code> for "OutdialPrompt=" • 0: P-Conference header should contain <code>false</code> for "OutdialPrompt="
P_CONF_FEEDBACK_PROMPTS	Integer	0	Specifies whether the value of P-Conference header should contain <code>true</code> or <code>false</code> for

Table continues...

Parameter	Type	Default value	Description
			"FeedbackPrompts=". Assign one of the following values: • 1: P-Conference header should contain <code>true</code> for "FeedbackPrompts=" • 0: P-Conference header should contain <code>false</code> for "FeedbackPrompts=".

Protocol-specific parameters

SIP

Parameter	Type	Default value	Description
SUBSCRIBE_SECURITY	Integer	2	Specifies the use of SIP and SIPS subscriptions. Applicable values are between 0 to 2.
ENABLE_AVAYA_ENVIRONMENT	Integer	1	Specifies the SIP operational mode. Assign one of the following values: • 0: Operates in a mode to comply with the third-party standard SIP proxy provisioning which includes 19 features. • 1: Operates in Avaya environment mode provisioning SIP and AST features and using PPM to download, back up, and restore operations.
DISCOVER_AVAYA_ENVIRONMENT	Integer	1	Specifies whether the device discovers that it is in an Avaya environment where SIP AST features are supported. Assign one of the following values: • 0: Do not auto discover AST support. • 1: Auto discover AST support. The SIP proxy server might not support AST.
CONFIG_SERVER_SECURE_MODE	Integer	1	Specifies the communication mode for configuration server, that is, whether secure communication through HTTPS is required to access the configuration server. Assign one of the following values: • 0: Use HTTP. • 1: Use HTTPS. • 2: Use HTTPS if the SIP transport type is TLS, otherwise use HTTP.

Table continues...

Parameter	Type	Default value	Description
ENABLE_EARLY_MEDIA	Integer	1	Specifies whether to enable early media. Assign one of the following values: • 0: Disabled • 1: Enabled
RDS_INITIAL_RETRY_ATTEMPTS	Integer	15	Specifies Remote Data Source initial retry attempts. The value indicates the number of times the PPM adaptor tries to download from PPM before giving up the PPM server connection. The range is from 1 to 30.
RDS_INITIAL_RETRY_TIME	Integer	2	Specifies Remote Data Source initial retry time. The value indicates the initial delay for a retry for connecting to the PPM server. The range is 2 to 60 seconds.
RDS_MAX_RETRY_TIME	Integer	600	Specifies Remote Data Source maximum retry time. The value indicates the maximum delay interval before giving up on connecting to the PPM server. The range is 2 to 3600 seconds.
OUTBOUND_SUBSCRIPTION_REQUEST_DURATION	Integer	86400	Specifies outbound subscription request duration. The range is from 60 to 31536000 seconds.
USE_QUAD_ZEROES_FOR_HOLD	Integer	0	Specifies the use of quad zeros to signal Hold operation in SDP. Assign one of the following values: • 0: Use "a= directional attributes". • 1: Use quad zeros.
WAIT_FOR_UNREGISTRATION_TIMER	Integer	32	Specifies the time for which the deskphone waits for before declaring un-registration to be complete. The range is from 4 to 3600.
WAIT_FOR_REGISTRATION_TIMER	Integer	32	Specifies the time for which the deskphone waits for a register response message. If no message is received, registration is retried. The range is from 32 to 3600 seconds.
CONTROLLER_SEARCH_INTERVAL	Integer	16	Specifies the time that the device waits to complete the maintenance check for monitored controllers. The range is from 4 to 3600 seconds.
ASTCONFIRMATION	Integer	60	Specifies the time that the device waits to validate an active subscription when it SUBSCRIBES to the avaya-cm-feature-status package. The range is from 16 to 3600 seconds.

Table continues...

Parameter	Type	Default value	Description
ENABLE_OOD_MSG_TLS_ONLY	Integer	1	Specifies whether a received Out-Of-Dialog (OOD) REFER must have TLS transport. Assign one of the following values: • 0: The OOD REFER must have TCP or TLS transport to be auctioned. • 1: The OOD REFER must have TLS transport to be auctioned.
PHNMUTEALERT_BLOCK	Integer	1	Specifies whether mute alerting is blocked or unblocked. Assign one of the following values: • 0: Unblocks or enables the Mute Alert feature and allows the user to set mute alerting using the Call Settings menu. • 1: Blocks or disables the Mute Alert feature. The setting is not displayed in the Call Settings menu.

TCP

Parameter	Type	Default value	Description
TCP_KEEP_ALIVE_TIME	Integer	60	Specifies the TCP Keep Alive timer. This time interval is the time for which the deskphone waits before sending out TCP keep-alive message to the far-end. The range is from 10 to 3600 seconds.
TCP_KEEP_ALIVE_INTERVAL	Integer	10	Specifies the TCP keep-alive packet re-transmission interval. After this time interval TCP keep-alive packets are re-transmitted. The range is from 5 to 60 seconds.
TCP_KEEP_ALIVE_STATUS	Integer	1	Specifies the TCP keep alive status. Assign one of the following values: • 0: TCP keep alive disabled. • 1: TCP keep alive enabled.
CONNECTION_REUSE	Integer	1	Specifies whether the device uses two TCP/TLS connection, for both outbound and inbound, or one TCP/TLS connection. Assign one of the following values: • 0: Disable. The device opens an outbound connection to the SIP Proxy and listens to the socket for inbound connection from SIP proxy in parallel. • 1: Enable. The deskphone opens a connection to the SIP proxy. The device does not listen to inbound connections from SIP proxies, that is,

Table continues...

Parameter	Type	Default value	Description
			there is only one socket which is used for inbound and outbound.

RTP and RTCP

Parameter	Type	Default value	Description
RTCPCONT	Integer	1	Specifies whether to enable or disable RTCP for audio and video streams between the deskphone and peer. Assign one of the following values: • 0: Disable RTCP. • 1: Enable RTCP.
RTCP-XR	Integer	0	Specifies whether the RTCP-XR Block Type 7 information is transmitted with the RTCP message that is sent to the voice monitoring server. RTCP Block Type 7 is the VoIP Metrics Report Block, which is an extension of the RTCP packet information. Valid values are: • 0: Disabled. RTCP-XR Block Type 7 information is not transmitted. • 1: Enabled: RTCP-XR Block Type 7 information is transmitted.
DTMF_PAYLOAD_TYPE	Integer	120	Specifies the DTMF Payload type. The value from this parameter is used when media offer is sent to the far-end in an INVITE . The range is from 96 to 127.
G726_PAYLOAD_TYPE	Integer	110	Specifies the G.726 Payload type. The value from this parameter is used when media offer is sent to the far-end in an INVITE . The range is from 96 to 127.
SYMMETRIC_RTP	Integer	1	Specifies whether to enforce RTP on the same port. Assign one of the following values: • 0: The device shall accept incoming packets regardless of the UDP source port • 1: The device shall only accept incoming packets if the source port of the incoming UDP datagram matches the destination port used in the UDP datagrams destined for the far-end endpoint. Incoming UDP datagrams that do not satisfy this criterion are discarded.

Table continues...

Parameter	Type	Default value	Description
PLAY_TONE_UNTIL_RTP	Numeric	1	Specifies whether locally-generated ring back tone will stop as soon as SDP is received for an early media session, or whether it will continue until RTP is actually received from the far-end party. Assign one of the following values: • 0: Stop ring back as soon as SDP is received. • 1: Continue ring back tone until RTP is received.

SRTP

Parameter	Type	Default value	Description
MEDIAENCRYPTION	String	9	Specifies the cryptosuite and session parameters for media encryption. You can assign maximum of three comma-separated values from the following list: • 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. • 10: aescm256-hmac80. • 11: aescm256-hmac32.
SDPCAPNEG	Integer	1	Specifies the SDP capability negotiation. Assign one of the following values: • 0: Disables SDP capability negotiation. • 1: Enables SDP capability negotiation.
ENFORCE_SIPS_URI	Integer	1	Specifies the enforcement of SIPS URI with SRTP. Assign one of the following values: • 0: Not enforced • 1: Enforced

Table continues...

Parameter	Type	Default value	Description
100REL_SUPPORT	Integer	1	Specifies whether the 100rel option tag is included in the INVITE header field per RFC 3262. Assign one of the following values: • 0: The tag is not included. • 1: The tag is included.

Trusted certificates and SCEP

Parameter	Type	Default value	Description
TRUSTCERTS	String	Null	Specifies the file names of certificates to be used for authentication.
MYCERTURL	String	Null	Specifies the URL to access Simple Certificate Enrollment Protocol (SCEP) server. The device attempts to contact the server only if this parameter is set to other than its default value.
MYCERTCN	String	\$SERIALNO	Specifies the Common name (CN) for SUBJECT in SCEP certificate request. The values can either be \$SERIALNO or \$MACADDR. If the value includes the string \$SERIALNO, that string will be replaced by the phones serial number. If the value includes the string \$MACADDR, that string will be replaced by the phones MAC address.
MYCERTDN	String	Null	Specifies common part of SUBJECT in SCEP certificate request. This value defines the part of SUBJECT in a certificate request including Organizational Unit, Organization, Location, State, and Country that is common for requests from different devices.
MYCERTKEYLEN	Integer	2048	Specifies the private key length in bits to be created in the device for a certificate enrollment. The range is from 1024 to 2048.
MYCERTRENEW	Integer	90	Specifies the percentage used to calculate the renewal time interval out of the device certificate's Validity Object. If the renewal time interval has elapsed the phone starts to periodically contact the SCEP server again to renew the certificate. The range is from 1 to 99.
MYCERTWAIT	Integer	1	Specifies the behavior of the device when performing certificate enrolment. assign one of the following values: • 0: Periodical check in the background.

Table continues...

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

TLS

Parameter	Type	Default value	Description
TLSSRVRID	Integer	1	Specifies whether the TLS server identification is required. Assign one of the following values: 0: No certificate match necessary. TLS connection will be established. 1: Certificate match required. TLS connection will only be established if the server's identity matches the server's certificate.

LLDP

Parameter	Type	Default value	Description
LLDP_ENABLED	Integer	2	Specifies whether to enable LLDP. Assign one of the following values: 0: Disabled. 1: Enabled. 2: Enabled, but only begin transmitting if an LLDP frame is received.

Dial plan parameters

Parameter	Type	Default value	Description
DIALPLAN	String	Null	Specifies one or more valid dial strings. The range is 0 to 1023 characters.
PHNCC	String	1	Specifies the dial plan country code.
PHNDPLENGTH	Numeric	5	Specifies the dial plan internal extension length. The range is from 3 to 13.
PHNIC	String	011	Specifies the dial plan international access code.
PHNLD	String	1	Specifies the dial plan long distance access code.
PHNLDLENGTH	Numeric	10	Specifies the dial plan national telephone number length. The range is from 5 to 15.
PHNOL	String	9	Specifies the dial plan public network access code.
PHNEMERGNUM	String	Null	Specifies the emergency number.
ENABLE_REMOVE_PSTN_ACCESS_PREFIX	Numeric	0	Specifies whether to enable the removal of the PSTN access prefix. Assign 0 or 1.
LOCAL_DIAL_AREA_CODE	Numeric	0	Specifies whether the user must dial area code for calls within same area code. Assign 0 or 1.
PHNLAC	String	Null	Specifies the local area code.
PHNMOREEMERGNUMS	String	Null	Specifies the list of additional emergency numbers. The range is from 0 to 100.

Audio parameters

Name	Description
Received Coding	G.711, G.722, G.726A, or G.729
Packet Loss	Missing, late, and out-of-sequence packets are counted as lost if they are discarded. Packets are not counted as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.
Packetization Delay	The amount of audio data in each RTP
One-way Network Delay	The number is half the value that RTCP or SRTCP computes for the round-trip delay to the device where the RTP is transmitted. For the calls that have a large geographic distance this number is expected to be larger than for local calls.
Network Jitter Delay	The average delay introduced by the jitter buffer on the deskphone.

Logging and debugging parameters

Parameter	Type	Default value	Description
SYSLOG_ENABLED	Integer	0	Specifies whether the sys log notification is enabled. Assign one of the following values: • 0: Syslog off. • 1: Syslog on.  Note: The Secure call icon is not displayed, if you set the parameter value to 1.
SYSLOG_LEVEL	Integer	3	Specifies the severity level. The device sends a syslog message if an event occurs with a severity level equal or less than the value specified in this parameter. Assign one of the following values: • 3: Error • 4: Warning • 5: Notice • 6: Informational • 7: Debug
LOCAL_LOGS_ENABLED	Integer	1	Specifies whether the local storage of log messages is enabled. Assign one of the following values: • 0: Local log off • 1: Local log on
LOCAL_LOG_LEVEL	Integer	4	Specifies the severity level for storing event logs locally. The device stores entries to a local event log when an event occurs with a severity level equal or less than the value specified in this parameter. Assign one of the following values: • 3: Error • 4: Warning • 5: Notice • 6: Informational • 7: Debug • 8: Stream debug
LOG_CATEGORY	String	All	Specifies a comma-separated list of keywords in standard string format for logging categories.

Table continues...

Parameter	Type	Default value	Description
			Logging implementation blocks all traces at the Warning or lower severity level unless the category corresponding to a given trace is enabled. The device filters all ANDROID and KERNEL syslog or log categories if you do not configure this parameter for these categories or if the value of the parameter is not set to All. If the log level is set to Warning or a lower level, this parameter enables low-level traces from adaptors or manager as indicated. This parameter applies to both syslog and local logging mechanisms. The supported categories are: ALL, ANDROID, 8021X, ADAPMGR, ALSIP, AST, AUDIO, CALENDAR, CCMP, CCSPROFILE, CERTMGMT, CONFERENCE, CONFIG, CONFIG_MULTI, CONTACT, CORE, DATETIME, DAVIDATA, DEVICE, DHCP, DIAL, EEPROMDATA, ENCRYPT, EXTAPP, FAILOVER, FAVORITE, HISTORY, HTTP, KERNEL, LLDP, LOCALDATA, MEDIA, MEDIAAUDIOCODING, MEDIAAUDIODEVICE, MEDIAAUDIOMIXERCLIENT, MEDIAAUDIOMIXERSERVER, MEDIAAUDIOPROCESSING, MEDIAFILE, MEDIARTPRTCP, MEDIASRTP, MEDIATRANSPORT, MEDIAUTILITY, MEDIAVIDEO, MEDIAVIDEOCAPTURE, MEDIAVIDEOCODING, MEDIAVIDEOMIXER, MEDIAVIDEOPROC, MEDIAVIDEORENDERER, MSGMGR, MSG_ROUTING, MSM, MWI, NETADAP, NETMGR, ONEXPAUCDATA, PERSLABELS, PLATFORM_COMP, PPMDATA, PPMMESSAGE, POWER, PRESENCE, QOS, REG, SCRIPT, SCRIPTDATA, SECURITY, SESSION, SESSION_VIDEO, SHARED_CNTRL, SIGADAP, SIGNAL, SIGNAL_VIDEO, SIGNALING_COMP, SIPEVENTS, SIPMESSAGE, SM, SSHDADAP, SUBSCRIBE, THREADWDOG, UI, UPGRADE, VIDEO, VMM, and WEB.
SSH_ALLOWED	Integer	0	Specifies whether and how Secure Shell (SSH) is supported. Assign one of the following values: • 0: Disabled. • 1: Enabled with challenge/response authentication.

Table continues...

Parameter	Type	Default value	Description
SSH_BANNER_FILE	String	Null	Specifies the file name or URL of a file that contains warning banner text that is sent to SSH clients before authentication.
SSH_IDLE_TIMEOUT	Integer	10	Specifies the number of minutes of bidirectional inactivity after which an SSH connection is terminated. The range is from 0 to 32767. Assign one of the following values: • 0: No timeout. • 1–32767: Number of minutes of inactivity after which SSH is disabled.
ENABLE_RECORDING	Integer	0	Specifies whether audio debug recording is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled
QKLOGINSTAT	Integer	0	Specifies the quick login permission flag. Assign one of the following values: • 0: Disabled. Requires an explicit username and password. • 1: Enabled. To see the previous username and password, enter or tap the pound (#) key.
SLMCAP	Integer	0	Specifies whether the SLA Mon™ agent supports packet capture. Assign one of the following values: • 0: Disabled. • 1: Enabled but without RTP payloads. • 2: Enabled with RTP payloads. • 3: Disabled with RTP payloads from the CRAFT menu.  Note: Secure call icon is not displayed, if you set the parameter value to 2.
SLMCTRL	Integer	0	Specifies whether the SLA Mon™ agent supports device control. Assign one of the following values: • 0: Disabled. • 1: Enabled. • 2: Disabled. The feature is enabled from the CRAFT menu.

Table continues...

Parameter	Type	Default value	Description
SLMPERF	Integer	0	Specifies whether the SLA Mon™ agent supports performance monitoring. • 0: Disabled • 1: Enabled
SLMPORT	Integer	50011	Specifies the UDP port used to receive commands from the SLA Mon™ server. The allowed range of values are between 6000 and 65535.
SLMSRVR	Integer	0.0.0.0:0	Specifies the source IP address and, optionally, the source port number of valid discovery messages from an SLA Mon™ server.
SLMSTAT	Integer	0	Specifies whether the SLA Mon™ agent will be enabled. Assign one of the following values: • 0: Disabled • 1: Enabled

Configuration parameters

Generic functionality

Parameter	Type	Default value	Description
ENABLE_PRESENCE	Integer	1	Specifies whether the presence function is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled
SIMULTANEOUS_REGISTRATIONS	Integer	3	Specifies the number of Session Managers for simultaneous registration with the phone. The range is from 1 to 3.
ENABLE_PPM_SOURCED_SIP_PROXYSRVR	Integer	1	Specifies the source of the SIP proxy server information as PPM. The range is from 0 to 1.
ENABLE_G711A	Integer	1	Specifies whether G.711A codec capability of phone is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled
ENABLE_G711U	Integer	1	Specifies whether G.711U codec capability of phone is enabled. Assign one of the following values: • 0: Disabled

Table continues...

Parameter	Type	Default value	Description
			• 1: Enabled
ENABLE_G729	Integer	1	Specifies whether G.729(A) codec capability of phone is enabled. Assign one of the following values: • 0: G.729 disabled. • 1: G.729(A) enabled, without Annex B support. • 2: G.729(A) enabled with Annex B support.
ENABLE_G722	Integer	1	Specifies whether G.722 codec of phone is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled
ENABLE_G726	Integer	1	Specifies whether G.726 capability of phone is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled
BRANDING_VOLUME	Integer	5	Specifies the level of the Avaya audio brand. Assign one of the following values: • 1: 12 db below nominal • 2: 9 db below nominal • 3: 6 db below nominal • 4: 3 db below nominal • 5: nominal • 6: 3 db above nominal • 7: 6 db above nominal • 8: 9 db above nominal

Configuration parameter download

Parameter	Type	Default value	Description
AUTH	Integer	0	Specifies the authentication flag for all files download. Assign of the following values: • 0: Secure files download is not required. • 1: Secure files download is required.

Port ranges parameters

Port ranges parameters

Parameter	Type	Default value	Description
RTP_PORT_LOW	Integer	5004	Specifies the lower limit of a port range to be used by RTP, RTCP, SRTP, or SRTCP connections when the parameter CONNECTION_REUSE is set to 0. The range is from 1024 to 65503.
RTP_PORT_RANGE	Integer	40	Specifies the width of port range to be used by used by RTP, RTCP, SRTP, or SRTCP connections when the parameter CONNECTION_REUSE is set to 0. The range is from 32 to 64511.
SIG_PORT_LOW	Integer	1024	Specifies the lower limit of a port range to be used for SIP signaling independent, if TCP or TLS over TCP. The range is from 1024 to 65503.
SIG_PORT_RANGE	Integer	64511	Specifies the width of port range to be used for SIP signaling independent, if TCP or TLS over TCP. The range is from 32 to 64511.

Audio operation and quality monitoring parameters

Parameter	Type	Default value	Description
QLEVEL_MIN	1 ASCII numeric digit	4	Specifies the minimum quality level for which a low local network quality is not displayed. Assign one of the following values: • 1: Never display icon. • 2: Packet loss is > 5% or round trip network delay is > 720 ms or jitter compensation delay is > 160 ms. • 3: Packet loss is > 4% or round trip network delay is > 640 ms or jitter compensation delay is > 140 ms. • 4: Packet loss is > 3% or round trip network delay is > 560 ms or jitter compensation delay is > 120 ms. • 5: Packet loss is > 2% or round trip network delay is > 480 ms or jitter compensation delay is > 100 ms.

Table continues...

Parameter	Type	Default value	Description
			6: Packet loss is > 1% or round trip network delay is > 400 ms or jitter compensation delay is > 80 ms.
WBCSTAT	1 ASCII numeric digit	1	Specifies whether a wideband codec indication is displayed when used. Assign one of the following values: 0: Wideband codec indication is not displayed. 1: Wideband codec indication is displayed.

General and phone application timer parameters

General and phone application timer

Parameter	Type	Default value	Description
REGISTERWAIT	Integer	900	Specifies the interval in seconds for next reregistration to SIP server. The range is 30 to 86400.
NO_DIGITS_TIMEOUT	Integer	20	Specifies the duration for timeout when no digit is entered. The range is from 1 to 60.
INTER_DIGIT_TIMEOUT	Integer	5	Specifies the duration for timeout between entered digits. The range is from 1 to 10.
FAILED_SESSION_REMOVAL_TIMER	Integer	30	Specifies the timer to remove failed call session. The range is from 5 to 999.
FAST_RESPONSE_TIMEOUT	Integer	4	Specifies the fast response timer. The range is from 0 to 32.
RECOVERYREGISTERWAIT	Integer	60	Specifies the interval for reactive monitoring. The range is from 10 to 36000.
FAILBACK_POLICY	String	auto	Specifies the fail back policy. Assign one of the following values: - admin - auto
WAIT_FOR_INVITE_RESPONSE_TIMEOUT	Integer	60	Specifies the maximum duration in seconds that the phone waits to get a response after receiving 100 Trying. The range is 30 to 180 seconds.

Deskphone interface settings parameters

Common operation

Parameter	Type	Default value	Description
BAKLIGHTOFF	Integer	120	Specifies the idle time in minutes after which the device turns off the backlight. The range is from 0 to 999. * Note: The parameter is only applicable for the registered devices that are currently logged-in.
RINGTONESTYLE	Integer	0	Specifies the style of classic ringtone that the device offers. Assign one of the following values: • 0: For North American ringtones. • 1: For European ringtones.
AUDASYS	Integer	3	Specifies whether the user can set the audible alerting to the lowest level or to zero. Assign one of the following values: • 0: To set the audible alerting to the lowest audible setting. • 1: To set the audible alerting to zero. • 2: To set the audible alerting to the lowest audible setting. • 3: To set the audible alerting to zero.
PHNNUMOFSA	Integer	3	Specifies the number of session appearances that the device supports while operating in a non-Avaya environment. The range is from 1 to 10.
ENHDIALSTAT	Integer	1	Specifies the enhanced local dialing status. Assign one of the following values: • 0: Disables the feature. • 1: Partially enables the feature, that is, the dialing rules do not apply for dialing from Contacts. • 2: Fully enables the feature, that is, the dialing rules also apply for dialing from Contacts.
SEND_DTMF_TYPE	Integer	2	Specifies whether the DTMF tones are send as in-band or out-band. Assign one of the following values: • 1: Send as in-band, that is, as regular audio. • 2: Send as out-band, that is, negotiation and transmission of DTMF occurs according to RFC

Table continues...

Parameter	Type	Default value	Description
			2833. If the far end does not support RFC 2833, send as in-band DTMF tones.
INGRESS_DTMF_VOL_LEVEL	Integer	-12	Specifies the power level of the tone in dBm0 after dropping the sign. The range is from -20 to -7.
SIPCONFERENCECONTINUE	Integer	0	Specifies whether to stop or continue the conference when the host is dropped from the conference. Assign one of the following values: • 0: Conference stops. • 1: Conference continues by transferring the host to the second party.

Audio settings

Parameter	Type	Default value	Description
AGCHAND	Integer	0	Specifies the status of Automatic Gain Control (AGC) for the handset. Assign one of the following values: • 0: AGC off • 1: AGC on
AGCHEAD	Integer	0	Specifies the status of Automatic Gain Control (AGC) for the headset. Assign one of the following values: • 0: AGC off • 1: AGC on
AGCSPKR	Integer	0	Specifies the status of Automatic Gain Control (AGC) for the speaker. Assign one of the following values: • 0: AGC off • 1: AGC on
REDIRECT_TONE	Integer	1	Specifies the single beep of call coverage tone played when at least one of the provisional responses is a 181 Call Forwarded and no RTP packets are received. The range is from 1 to 4.
RINGTONES	String	Null	Specifies the list of audio files to be downloaded as ring tones and offered to the user for selection. The range is from 0 to 1023 octets of UTF-8 characters.
HEADSET_PROFILE_DEFAULT	Integer	1	Specifies the number of the default headset audio profile. The range is from 1 to 20.

Table continues...

Parameter	Type	Default value	Description
HEADSET_PROFILE_NAMES	String	Null	Specifies the names to be displayed for headset audio profile selection. The range is from 0 to 255 octets of UTF-8 characters.
AUDIOSTHS	Integer	0	Specifies the settings for the handset sidetone. Assign one of the following values: • 0: Normal. • 1: Three level softer than normal. • 2: Off. • 3: One level softer than normal. • 4: Two levels softer than normal. • 5: Four levels softer than normal. • 6: Five levels softer than normal. • 7: Six levels softer than normal. • 8: One level louder than normal. • 9: Two levels louder than normal.
AUDIOSTHD	Integer	0	Specifies the settings for the headset sidetone. Assign one of the following values: • 0: Normal. • 1: Three level softer than normal. • 2: Off. • 3: One level softer than normal. • 4: Two levels softer than normal. • 5: Four levels softer than normal. • 6: Five levels softer than normal. • 7: Six levels softer than normal. • 8: One level louder than normal. • 9: Two levels louder than normal.

Display settings

Parameter	Type	Default value	Description
LOCALLY_ENFORCE_PRIVACY_HEADER	Integer	0	Specifies that the display is locally enforced when a Privacy header is included in the INVITE for an incoming call. Assign one of the following values: • 0: Disabled. The responsibility for privacy is with the CM/SM, the endpoint displays any CallerId received in the From or Contact headers as done for a normal, non-private call. • 1: Enabled. The responsibility for privacy is with the endpoint, the endpoint displays the localized string as Restricted.
ENFORCE_DVI	Integer	1	Specifies whether the Digital Visual Interface (DVI) is enforced when the PC display is pass through the phone. Assign one of the following values: • 0: DVI is not enforced. Screen resolution is 720p. • 1: DVI is enforced. Screen resolution is 1080p using DVI. HDMI is not supported.
LOGOS	String	Null	Specifies the list of custom logo definitions for the background display. Each logo tuple contains a label and a full URL.
CURRENT_LOGO	String	Null	Specifies the selected background logo for display. The string is empty for the default logo. In System Manager 6.3.8 or later, you cannot use this parameter if you are using the Expanded Template support for SIP Endpoints feature.

Language and country settings

Parameter	Type	Default value	Description
ISO_SYSTEM_LANGUAGE	String	en-US	Specifies the locale which controls: • Language presented to the user. • Date, time, and numbers format for the relevant locale. Assign one of the following values: • en_CA • en_IN • en_NZ • en_SG • en_GB

Table continues...

Parameter	Type	Default value	Description
			• en_US • fr_BE • fr_CA • fr_FR • fr_CH • ru_RU • pt_BR • zh_CN • ja_JP • ko_KR • ar_EG • iw_IL • es_US  Note: Reboot the phone after you change the system language.
COUNTRY	String	Undefined	Specifies the country of operation for specific dial tone generation, Wi-Fi, DECT, and the default anti flickering frequency for camera – 50 Hz or 60 Hz.

Date and time settings

Parameter	Type	Default value	Description
TIMEFORMAT	Integer	0	Specifies the time format. Assign one of the following values: • 0: For AM and PM format. • 1: For 24-hour format.
GMTOFFSET	String	0:00	Specifies the offset from the Greenwich Mean Time.
DAYLIGHT_SAVING_SETTING_MODE	Integer	2	Specifies the mode for daylight saving time. Assign one of the following values: • 0: No daylight saving time. • 1: Daylight saving time. • 2: Automatic.
DSTOFFSET	Integer	1	Specifies the daylight saving time offset from local time. The range is from 0 to 2.

Table continues...

Parameter	Type	Default value	Description
DSTSTART	String	2SunMar2L	Specifies the daylight saving start date. The formats used are <i>odddmmht</i> and <i>Dmmmht</i> .
DSTSTOP	String	1SunNov2L	Specifies the daylight saving stop date. The formats used are <i>odddmmht</i> and <i>Dmmmht</i> .

Network parameters

General network parameters

Parameter	Type	Default value	Description
DHCPSTD	Integer	0	Specifies the DHCP lease violation flag. Assign one of the following values: • 1: Comply with the DHCP standard, that is, (immediately release IP address, if DHCP lease expires. • 0: Enter proprietary state, that is, continue to use IP address, if DHCP lease expires.
ICMPDU	Integer	1	Specifies whether the ICMP Destination Unreachable messages are generated. Assign one of the following values: • 0: Destination Unreachable messages will not be transmitted. • 1: Destination Unreachable messages will only be transmitted for the UDP port in the range of 33,434 to 33,523. • 2: Destination Unreachable messages will be transmitted.
ICMPRED	Integer	0	Specifies whether the ICMP redirect messages will be processed. Assign one of the following values: • 0: Received Redirect messages will not be processed. • 1: Received Redirect messages will be processed per RFC 1122.

Table continues...

Parameter	Type	Default value	Description
MTU_SIZE	Integer	1500	Specifies the Maximum Transmission Unit size for Ethernet interface only and not for Wi-Fi. Assign one of the following values: • 1496 • 1500
REUSETIME	Integer	60	Specifies the IP address reuse timeout for Ethernet interface only and not for Wi-Fi. The range is from 0 to 20,999.
DECTSTAT	Integer	1	Specifies whether the DECT menu option in the Setting app is enabled for the user. Assign one of the following values: • 0: The DECT and menu option is disabled in the Settings app and the user cannot change it. • 1: The DECT and menu option is enabled in the Settings app and the user can change it to enable or disable the wireless handset.
BLUETOOTHSTAT	Integer	1	Specifies whether Bluetooth is allowed for user configuration. Assign one of the following values: • 0: The Bluetooth and menu option is disabled in the Settings app and the user cannot change it. • 1: The Bluetooth and menu option is enabled in the Settings app and the user can change it to enable or disable Bluetooth.
WIFISTAT	Integer	0	Specifies whether Wi-Fi is allowed for user configuration. Assign one of the following values: • 0: The Wi-Fi and menu option is disabled in the Settings app and the user cannot change it. • 1: The Wi-Fi and menu option is enabled in the Settings app and the user can change it to enable or disable the Wi-Fi.
GRATARP	Integer	0	Specifies whether an existing ARP cache entry is updated with a MAC address received in a gratuitous ARP message. Assign one of the following values: • 0: Gratuitous ARP messages will be ignored. • 1: Gratuitous ARP messages will be processed to update an existing ARP cache entry.
IPADD	String	0.0.0.0	Specifies the IP address of the phone. The range is from 7 to 15 ASCII characters. This is a testable parameter.

Table continues...

Parameter	Type	Default value	Description
CAPTIVE_PORTAL_SERVER	String	Null	Specifies the URL of the captive portal server for HTTP authentication to use the Internet. Use one of the following options for configuration: • [http://]hostname[:port] [/path] • [https://]hostname[:port] [/path]

Ethernet parameters

Parameter	Type	Default value	Description
PHY1STAT	Numeric	1	Specifies the speed and duplex mode of Ethernet line interface. Assign one of the following values: • 1: Auto negotiation speed and duplex. • 2: 10Mbps half-duplex operation. • 3: 10Mbps full-duplex operation. • 4: 100Mbps half-duplex operation. • 5: 100Mbps full-duplex operation.
PHY2STAT	Numeric	1	Specifies the speed and duplex mode of the secondary Ethernet line interface or disables the secondary Ethernet line interface. Assign one of the following values: • 0: Disabled. • 1: Auto negotiation speed and duplex. • 2: 10Mbps half-duplex operation. • 3: 10Mbps full-duplex operation. • 4: 100Mbps half-duplex operation. • 5: 100Mbps full-duplex operation.
PHY2_AUTOMDIX_ENABLED	Numeric	1	Specifies whether Auto-MDIX is enabled on PHY2. Assign one of the following values: • 0: Auto-MDIX will be disabled on PHY2. • 1: Auto-MDIX will be enabled on PHY2.

Table continues...

Parameter	Type	Default value	Description
ASSUME_SP_POE	Numeric	0	Specifies whether Single port PoE injector is connected to the device. Assign one of the following values: • 0: Single port PoE injector is not connected to the device. • 1: Single port PoE injector is connected to the device.
SP_POE_POWER	Numeric	20	Specifies how much power is provided when the device is connected to Single port PoE injector. The range is from 16 to 25.

QoS parameters

Parameter	Type	Default value	Description
L2QAUD	Numeric	6	Specifies the layer 2 audio priority value. The range is from 0 to 7.
L2QVID	Numeric	5	Specifies layer 2 video priority value. The range is from 0 to 7.
L2QSIG	Numeric	6	Specifies the layer 2 signaling priority value. The range is from 0 to 7.
DSCPAUD	Numeric	46	Specifies the differentiated Services Code Point for audio. The range is from 0 to 63.
DSCPSIG	Numeric	34	Specifies the differentiated Services Code Point for signaling. The range is from 0 to 63.
DSCPVID	Numeric	34	Specifies the differentiated Services Code Point for video. The range is from 0 to 63.

VLAN parameters

Parameter	Type	Default value	Description
L2Q	Numeric	0	Specifies 802.1Q tagging mode. Assign one of the following values: • 0: Auto • 1: On • 2: Off

Table continues...

Parameter	Type	Default value	Description
L2QVLAN	Numeric	0	Specifies the 802.1Q VLAN identifier. The range is 0 to 4094.
VLANTEST	Numeric	60	Specifies the timer for DHCPOFFER reception on a non-zero VLAN. The range is 0 to 999.
VLANSEP	Numeric	1	Specifies whether to enable the VLAN separation. Assign one of the following values: • 0: Disabled • 1: Enabled
PHY2VLAN	Numeric	0	Specifies the VLAN ID for tagged frames on the secondary Ethernet Interface. The range is 0 to 4094.
PHY2TAGS	Numeric	0	Specifies whether tags are stripped from frames forwarded to PHY2. Assign one of the following values: • 0: Remove tags from frames forwarded to PHY2. • 1: Do not remove tags from frames forwarded to PHY2.

IEEE 802.1.x parameters

Parameter	Type	Default value	Description
DOT1XSTAT	Numeric	0	Specifies the IEEE 802.1X status for Ethernet interface. Assign one of the following values: • 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.
DOT1X	Numeric	0	Specifies the IEEE 802.1X operational mode for Ethernet interface. Assign one of the following values: • 0: PAE multicast pass-through without proxy Logoff. • 1: PAE multicast pass-through with proxy Logoff. • 2: No PAE multicast pass-through or proxy Logoff.

Table continues...

Parameter	Type	Default value	Description
DOT1XEAPS	String	MD5	Specifies a list of EAP methods for IEEE 802.1x authentication. For now, the values supported are TLS and MD5.

Account and password parameters

Parameter	Type	Default value	Description
PROCPSWD	String	27238	Specifies the password to gain administrator rights for local procedures on the device.

Presence parameters

Parameter	Type	Default value	Description
ENABLE_PRESENCE	Integer	0	Enables presence tracking of users in the Contacts list. Assign one of the following values: • 0: Disabled • 1: Enabled
PRESENCE_SERVER	String	Null	Specifies the an address of the Presence server. The value of PRESENCE_SERVER is obtained from the PPM when the presence profile is downloaded. The PRESENCE_SERVER address obtained from the presence profile takes precedence over the value set in the <code>46xxsettings</code> file. If you do not set this parameter, the deskphone automatically determines the Presence server address, but the Instant Messaging feature will not work.
PRESENCE_ACL_CONFIRM	Integer	0	Specifies the handling of Presence ACL updates. When a watcher list is received (presence.wininfo NOTIFY) which contains one or more watchers with the pending status, the value of this parameter defines the action taken by the device. Assign one of the following values: • 0: Auto Confirm. When a watcher list is received containing “pending” watchers, the phone will

Table continues...

Parameter	Type	Default value	Description
			automatically PUBLISH an approval to allow immediate presence monitoring. • 1: Ignore. The device will not take any action on “pending” watchers.
DND_SAC_LINK	Integer	0	Specifies the link between the DND and SAC buttons. The value of this parameter is used if the ALLOW_DND_SAC_LINK_CHANGE is set to 0. Assign one of the following values: • 0: The behavior of DND and SAC is not linked • 1: The behavior of DND and SAC is linked
ALLOW_DND_SAC_LINK_CHANGE	Integer	0	Specifies whether the user can control the link between Send All Calls (SAC) and Do not Disturb (DND) behaviors. If the features are linked, the deskphone activates SAC when user activates DND. A value of 1 indicates that the user gets the control to link the SAC and DND behaviors. Accordingly, the deskphone displays the appropriate menu to set the link. A value of 0 indicates that the user does not get the control to link the SAC and DND behaviors. Assign one of the following values: • 0: Does not change the default behavior. • 1: Change default behavior, parameter will be included in the A menu.
DND_SAC_LINK_MANUAL	Integer	1	Specifies the link between the DND and SAC buttons. The value of this parameter is used if the ALLOW_DND_SAC_LINK_CHANGE is set to 0. Assign one of the following values: • 0: Enabling DND will not enable SAC • 1: Enabling DND will enable SAC

Microsoft Exchange parameters

Parameter	Type	Default value	Description
EXCHANGE_SERVER_SECURITY_MODE	Integer	1	Specifies whether to use HTTP or HTTPS to contact Microsoft Exchange Server. Assign one of the following values: • 0: Use HTTP.

Table continues...

Parameter	Type	Default value	Description
			1: Use HTTPS.
EXCHANGE_USER_DOMAIN	String	Null	Specifies the user domain for Microsoft Exchange Server.
EXCHANGE_SERVER_LIST	String	Null	Specifies the list containing IP or DNS address of Microsoft Exchange Server. Use the parameter if the automatic synchronization fails.

WML browser parameters

Parameter	Default value	Description
WMLHOME	NULL	Specifies the URL of a WML page to be displayed by default in the WML browser. You can link the browser home page to the Avaya menu to include the browser option.
WMLPROXY	NULL	Specifies a HTTP proxy server address to be used by the WML browser, Weather, and World Clock applications.
WMLPORT	8080	Specifies the TCP port number of the HTTP proxy server set in WMLPROXY. Valid values are 0 to 65535.
WMLEXCEPT	NULL	Specifies the exception list of IP addresses or domains that must not be used by the HTTP proxy server.
WMLIDLETIME	10	Number of minutes of inactivity after which the browser should display the idle URL specified in WMLIDLEURI. Valid values are 1 to 999
WMLIDLEURI	NULL	URL of the web page to be displayed after idle time is reached.

Chapter 6: Configuration through LLDP

LLDP overview

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

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

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

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

LLDPDU transmitted by the 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 device.
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.
Basic Optional	Management Address	Mgmt IPv4 IP address of device. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the device.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports autonegotiation status and speed of the uplink port on the device.
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	Firmware version .
TIA LLDP MED	Inventory – Software Revision	APPNAME.
TIA LLDP MED	Inventory – Serial Number	Device serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final Dxxx characters removed.
Avaya Proprietary	Call Server IP address	Call Server IP Address. Subtype = 3
Avaya Proprietary	IP Phone addresses	Phone IP address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	File Server	File Server IP Address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not.
Basic Mandatory	End-of-LLDPDU	Not applicable.

TLV impact on system parameter values

System parameter name	TLV name	Impact
PHY2VLAN	IEEE 802.1 Port VLAN ID	The value of the PHY2VLAN parameter on the deskphone is configured from the value of the Port VLAN identifier in the TLV.
L2QVLAN and L2Q	IEEE 802.1 VLAN Name	The value is changed to the TLV VLAN Identifier. L2Q is set to 1 (ON). A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. VLAN Name TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The current value of L2QVLAN was set by a TIA LLDP MED Network Policy TLV. • 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 and 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. • The Application Type is not 1 (Voice) or 2 (Voice Signaling). • The Unknown Policy Flag (U) is set to 1.
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.

Table continues...

System parameter name	TLV name	Impact
		This TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The Application Type is not 1 (Voice) or 2 (Voice Signaling). • 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 addresses in this TLV value.  Note: This parameter cannot be used in an environment where both SIP deskphones and H.323 deskphones exist.
TLSSRV and HTTPSRV	Proprietary File Server TLV	TLSSRV and HTTPSRV will be set to the IP addresses 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. • The current L2QVLAN value was set by an IEEE 802.1 VLAN name. • 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.

Chapter 7: Security

Security

SIP-based 9600 Series IP Deskphones provide lock and logout functionalities for security and protection of the privacy of a user. When a user locks the deskphone, no one can unlock the deskphone without the assigned password for the particular user. When the deskphone is in a locked state, a user can receive calls or make emergency calls. The deskphone restricts access to any user data while in locked state.

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

Important:

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

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

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

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

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

The deskphone support SRTP. SRTP is used to encrypt and secure the audio going to and from the endpoint.

In order to correctly use SRTP, there are various components within the network that you must correctly configure. For the deskphones to function properly with SRTP, you must configure the

equivalent parameters in Communication Manager or System Manager. You must configure the following three parameters on the deskphones and the equivalent Communication Manager parameters must match one of the parameters:

- SET ENFORCE_SIPS_URI 1
- SET SDPCAPNEG 1
- SET MEDIAENCRYPTION X,9
- SET MEDIAENCRYPTION X where X is a value from 1 to 8

Certificate management

The applications running in the 9600 Series IP Deskphones setup rely on trusted certificates for secure operation. The trusted certificate repository can be configured through a parameter, which is used by various applications in the following manner:

- SIP/TLS: Uses the trusted certificates if the certificates are configured, else uses the default Avaya SIP Product CA and Avaya Product Root CA certificate.
- PPM/HTTPS/TLS: Uses the trusted certificates if the certificates are configured, else uses the default Avaya SIP Product CA and Avaya Product Root CA certificate.
- Software distribution package and settings file downloaded from the HTTPS server: Uses the trusted certificates if the certificates are configured, else uses the Avaya Product Root CA certificate. The identity certificate generated using SCEP is used if the deskphone identity certificate is requested by the file server for mutual authentication.
- Ethernet 802.1x EAP-TLS: Uses the trusted certificates. The identity certificate generated using SCEP is used as it is required for authentication.

Enterprises can set up their own certificate authority (CA) by replacing the default Avaya root certificates and Avaya Product Root CA certificates with their trusted certificates. The certificates issued by CA must be configured in the settings file when the 9600 Series IP Deskphones is registered with the enterprise. In addition to root certificates, high-security enterprises install a unique identity certificate on each 9600 Series IP Deskphones. Identity certificates are required if the communication setup is using EAP-TLS, or any other server that requires mutual authentication.

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

Note:

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

Parameter configuration for secure installation

For secure installation, configure the following parameters.

Parameter	Set to	Notes
TRUSTCERTS		Provides the file names of certificates to be used for authentication. It supports both root and intermediate certificates and can contain up to six certificate files.
TLSSRVRID	1	Certificates installed on the servers must have the common name that matches the device configuration.
AUTH	1	Ensures usage of HTTPS file servers for configuration and software files download. Once AUTH is set to 1 and the device downloads the trusted certificates, the device can only download files from HTTPS server with certificates that can be validated using trusted certificate repository.
SSH_ALLOWED	0	To keep SSH disabled.

SCEP parameters

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

Parameter	Type	Default value	Description
MYCERTURL	String	Null	Specifies the URL to access Simple Certificate Enrollment Protocol (SCEP) server. The device attempts to contact the server only if this parameter is set to other than its default value.
MYCERTCN	String	\$SERIALNO	Specifies the Common name (CN) for SUBJECT in SCEP certificate request. The values can either be \$SERIALNO or \$MACADDR. If the value includes the string \$SERIALNO, that string will be replaced by the phones serial number. If the value includes the string \$MACADDR, that string will be replaced by the phones MAC address.
MYCERTDN	String	Null	Specifies common part of SUBJECT in SCEP certificate request. This value defines the part of SUBJECT in a certificate request including Organizational Unit, Organization, Location, State, and Country that is common for requests from different devices.
MYCERTKEYLEN	Numeric	2048	Specifies the private key length in bits to be created in the device for a certificate enrollment. The range is from 1024 to 2048.
MYCERTRENEW	Numeric	90	Specifies the percentage used to calculate the renewal time interval out of the device certificate's Validity Object. If the renewal time interval has elapsed the phone starts to

Table continues...

Parameter	Type	Default value	Description
			periodically contact the SCEP server again to renew the certificate. The range is from 1 to 99.
MYCERTWAIT	Numeric	1	Specifies the behavior of the device when performing certificate enrolment. assign one of the following values: • 0: Periodical check in the background • 1: Wait until a certificate or a denial is received or a pending notification is received
MYCERTCAID	String	CAIdentifier	Specifies the Certificate Authority Identifier. Certificate Authority servers may require a specific CA Identifier string in order to accept GetCA requests. If the device works with such a Certificate Authority, the CA identifier string can be set through this parameter.
SCEPPASSWORD	String	\$SERIALNO	Specifies a challenge password to use with SCEP. The value of SCEPPASSWORD, if non-null, is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains \$SERIALNO, \$SERIALNO is replaced by the value of SERIALNO. If the value contains \$MACADDR, \$MACADDR is replaced by the value of MACADDR without the colon separators.

VLAN

Configure the following VLAN parameters.

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

For the above VLAN configuration, there will be a full VLAN separation between the device and computer packets. The device tries to obtain an IP address from the DHCP server on the voice VLAN. If the device gets an IP address, the device sends all the tagged packets on the voice LAN. Set the PHY2VLAN parameter to the data VLAN so that untagged packets from the computer are assigned to the data VLAN or the tagged packets from the computer are forwarded to the data VLAN. Tagged packets from computers on VLANs other than the data VLAN are blocked.

Chapter 8: Administering deskphone options

Administering a VLAN

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

Related links

[About VLAN Tagging](#) on page 73

[The VLAN default value and priority tagging](#) on page 73

[Automatic detection of a VLAN](#) on page 74

[VLAN separation rules and related parameters](#) on page 75

About VLAN Tagging

IEEE 802.1Q tagging (VLAN) is a useful method of managing VoIP traffic in your LAN. You can establish a voice VLAN, set L2QVLAN to the VLAN ID of that VLAN, and provide voice traffic with priority over other traffic. If LLDP was used to set the VLAN for the deskphones, that setting has absolute authority. Otherwise, you can set VLAN tagging manually, by DHCP, or in the 46xxsettings.txt file.

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

Related links

[Administering a VLAN](#) on page 73

The VLAN default value and priority tagging

The parameter L2QVLAN identifies the 802.1Q VLAN Identifier and is initially set to 0. This default value indicates *priority tagging* and specifies that your network Ethernet switch automatically insert the default VLAN ID without changing the user priority of the frame.

But some switches do not process a VLAN ID of zero and require frames tagged with a non-zero VLAN ID.

If you do not want the default VLAN to be used for voice traffic, set the value of L2QVLAN to the VLAN ID appropriate for your voice LAN.

You can also administer another parameter VLANTEST that defines the number of seconds the waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is 60 seconds. If you use VLANTEST, the deskphone returns to the default VLAN if an invalid VLAN ID is administered or if the phone moves to a port where the L2QVLAN value is invalid.

The default value of VLANTEST is long, allowing for the scenario that a major power interruption is causing the phones to restart. Always allow time for network routers, the DHCP servers, and other equipment to be returned to service. If the deskphone restarts for any reason and the VLANTEST time limit expires, the administered VLAN ID becomes invalid. The deskphone then initiates operation with a VLAN ID of 0. Or, if the value of L2Q is 0, that is auto, the deskphone turns off tagging until the L2QVLAN is set to a non-zero value or until the deskphone verifies that the network can support tagged frames.

Setting VLANTEST to "0" causes the phone to use a non-zero VLAN indefinitely to attempt DHCP. In other words, the deskphone does not return to the default VLAN.

Related links

[Administering a VLAN](#) on page 73

Automatic detection of a VLAN

The phones support automatic detection of the L2QVLAN setting that is incorrect. When the value of L2QVLAN is not 0 and VLAN tagging is enabled, L2Q= 0 or 1, initially the transmits DHCP messages with IEEE 802.1Q tagging and sets the VLAN ID to L2QVLAN. The phones will continue to do this for number of seconds configured by VLANTEST.

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

Note:

Regardless of the setting of L2Q, VLANTEST, or L2QVLAN, you must have administer DHCP on the phone so that the phone receives a response to a DHCPDISCOVER on making that request on the default (0) VLAN.

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

The phone ignores any VLAN ID administered on the call server if a non-zero VLAN ID is administered either by LLDP, manually, through DHCP, or through the settings file.

Related links

[Administering a VLAN](#) on page 73

VLAN separation rules and related parameters

VLAN separation is available to control access to the voice VLAN from the secondary Ethernet interface, and to control whether broadcast traffic from the data VLAN is forwarded to the deskphone.

The following system parameters control VLAN separation:

- VLANSEP - enables (1) or disables (0) VLAN separation.
- L2QVLAN - specifies the voice VLAN ID to be used by the deskphone.
- PHY2VLAN - specifies the VLAN ID to be used for frames forwarded to the network from the secondary Ethernet interface.
- PHY2PRIO - the layer 2 priority value to be used for tagged frames forwarded to the network from the secondary Ethernet interface.
- PHY2TAGS - specifies whether tags are stripped from frames forwarded to PHY2.



Note:

The phone does not support more than one data VLAN.

Related links

[Administering a VLAN](#) on page 73

[VLAN separation rules](#) on page 75

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.

Table continues...

If		Then
		- 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. 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.

Table continues...

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. 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.

Related links

[VLAN separation rules and related parameters](#) on page 75

Administering display language options

By default, the phone display information is in English. Administrators can specify up to four languages for each phone to replace English. Users can then select the display language.

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

The actual character input method does not depend on the languages available from the software download. If the phone does not support a character input method, use ASCII instead.

Use the configuration file and the following parameters to customize the settings for up to four languages

- **SYSTEM_LANGUAGE** - Contains the name of the default system language file used in the phone. The filename must be one of the files listed in the **LANGUAGES** parameter. If no filename is specified, or if the filename does not match with one of the **LANGUAGES** values, the deskphone uses its built-in English text strings. Filename must end in .xml
- **LANGUAGES** - Specifies the language files to be installed or downloaded to the phone. Filenames may be full URL, relative path name, or filename. (0 to 1096 ASCII characters, including commas). Filenames must end in .xml. For example, to indicate that and Russian, Parisian French, Latin American Spanish, and Korean are the available languages, the setting is **SET LANGUAGES**
Mlf_Russian.xml,Mlf_ParisianFrench.xml,Mlf_LatinAmericanSpanish.xml,Mlf_Korean.xml

To download a language file or to review pertinent information, go to the [Avaya Support website](#).

*** Note:**

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

Push server

The Push feature requires a trusted push server. The push server administration must conform to the requirements in *9600 Series IP Telephone Application Programmer Interface (API) Guide*.

SNMP activation

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

You can restrict the IP addresses from which the deskphone accepts SNMP queries with the SNMPADD parameter. You can also customize your community string with the SNMPSTRING parameter. For more information, see Chapter 5: Administering DHCP and HTTP servers .

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

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

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

Registration and authentication

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

For the SIP Deskphones to work properly, you must specify the correct domain name on the IP Network Region screen of Communication Manager.

For more information, see the following documents at the Avaya Support website <http://support.avaya.com>:

- For information about the IP Network Region screen, see *Administering Network Connectivity on Avaya Aura® Communication Manager* at the Avaya Support website: <http://support.avaya.com>.
- For information about the registration process, see *Maintaining Avaya Aura® Session Manager* and *Troubleshooting Avaya Aura® Session Manager*. Also, see your call server administration documentation.

IP address and settings reuse

After a successful registration with a call server, the IP address of the deskphone and the parameter values are saved in the non-volatile memory of the deskphone. The deskphone can reuse the saved parameters if the DHCP or HTTP/HTTPS server is not available for any reason after the deskphone restarts.

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

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

- **Routers in Use** - if no responses are received from the routers indicated in the configuration parameter ROUTER (set using DHCP Option 3 or by a local administrative procedure), and if REUSE = 1, then ROUTER_IN_USE will be set to REUSE_ROUTER_IN_USE. With the exception of the ROUTER configuration parameter, the other router-related parameters are internally set system values.
- **VLAN Check** - During the VLAN check, if a reset is to be done and VLAN_IN_USE is not zero, VLAN_IN_USE will be added to VLANLIST if it is not already on VLANLIST.

The VLAN detection process described in Automatically detecting a VLAN on page 52 is followed if tagging is off or if tagging is on and L2QVLAN is > 0, and if REUSETIME > 0, and if REUSE_IPADD is not "0.0.0.0". If VLANTEST expires, the value of VLAN_IN_USE is added to VLANLIST if it is not already on VLANLIST.

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

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

- REUSE_IPADD will be set to the value of IPADD
- REUSE_NETMASK will be set to the value of NETMASK

- REUSE_ROUTERS will be set to the value of ROUTER
- REUSE_ROUTER_IN_USE will be set to the value of ROUTER_IN_USE
- REUSE_TAGGING will be set to the value of TAGGING
- L2QVLAN_INIT will be set to the value of VLAN_IN_USE
- The MIB object endptVLANLIST will be set to the value of VLANLIST and then the value of VLANLIST will be set to null.

Ping and traceroute

All 9600 Series IP Deskphones respond to a ping or traceroute message sent from the call server switch or any other network source.

For more information, see your call server administration documentation.

TCP and UDP ports

9600 Series IP Deskphones use different protocols, such as TCP, TLS, and UDP, to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP ports each piece of equipment uses to support each protocol and each task within the protocol.

Depending on your network, you need to know what ports or ranges are used in the operation of the deskphones.

Related links

[Received packets \(destination = SIP deskphone\)](#) on page 80

[Transmitted packets \(source = SIP deskphone\)](#) on page 82

Received packets (destination = SIP deskphone)

Destination port	Source port	Use	Protocol UDP or TCP
The number used in the Source Port field of the packets that the HTTP client of the deskphone sends	Any	Packets that the HTTP client of the deskphone receives	TCP

Table continues...

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

Related links

[TCP and UDP ports](#) on page 80

Transmitted packets (source = SIP deskphone)

Destination port	Source port	Use	Protocol UDP or TCP
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
80, unless explicitly specified otherwise	Any unused port number	Packets transmitted by the HTTP client of the deskphone	TCP
123	Any unused port number	Transmitted SNTP messages	UDP
The number used in the Source Port field of the SNMP query packet received by the deskphone	161	Transmitted SNMP messages	UDP
443, unless explicitly specified otherwise	Any unused port number	TLS/SSL packets transmitted by the HTTP client of the deskphone.	TCP
514	Any unused port number	Transmitted Syslog messages	UDP
The port number specified in the test request message	50000	Transmitted CNA test results messages	UDP
System-specific	Any unused port number	Transmitted signaling protocol packets	TCP
FEPOR + 1 (if FEPOR is even) or FEPOR - 1 (if FEPOR is odd) or the port number specified in a CNA RTP test request plus or minus one, as with FEPOR	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

Related links

[TCP and UDP ports](#) on page 80

Network audio quality

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

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

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

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

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.

About DNS addressing

support DNS addresses, dotted decimal addresses, and colon-hex addresses. The phone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the contents of DHCP Option 6. At least one address in Option 6 must be a valid, non-zero, dotted decimal address. Otherwise DNS fails. The text string for the DOMAIN system parameter, Option 15 is appended to the addresses in Option 6 before the phone attempts DNS address resolution. If Option 6 contains a list of DNS addresses, those addresses are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS by DHCP, you can specify the DNS server and or the domain name in the HTTP script file. But first SET the DNSSRV and DOMAIN values so that you can use those names later in the script.

 Note:

Administer Options 6 and 15 with DNS servers and domain names respectively.

About IEEE 802.1X

support the IEEE 802.1X standard for Supplicant operation and support pass-through of 802.1X messages to an attached PC. The system parameter DOT1X determines how the phones handle pass-through of 802.1X multicast packets and proxy logoff:

- When DOT1X = 0, the phone forwards 802.1X multicast packets from the Authenticator to the PC attached to the phone and forwards multicast packets from the attached PC to the Authenticator (multicast pass-through). The phone does not support Proxy Logoff. This is the default value.
- When DOT1X = 1, the phone supports the same multicast pass-through as when DOT1X=0, but Proxy Logoff is also supported. When the secondary Ethernet interface loses link integrity, the phone sends an 802.1X EAPOL-Logoff message to the Authenticator with a source MAC address from the previously attached device. This message alerts the Authenticator that the device is no longer connected.
- When DOT1X = 2, the phone forwards multicast packets from the Authenticator only to the phone, ignoring multicast packets from the attached PC (no multicast pass-through). The phone does not support Proxy Logoff.
- Regardless of the DOT1X setting, the phone always properly directs unicast packets from the Authenticator to the phone or its attached PC as specified by the destination MAC address in the packet.

All support Supplicant operation as specified in IEEE 802.1X, only if the value of the parameter DOT1XSTAT is 1 or 2. If DOT1XSTAT has any other value, the phone does not support Supplicant operation.

Unicast 802.1X frames contain the MAC address of the phone as the destination MAC address and a protocol type of 88-8E hex. IP phones respond to unicast 802.1X frames received on the Ethernet line interface if the value of DOT1XSTAT is 1 or 2.

IP phones respond to 802.1X frames that have the PAE group multicast address as the destination MAC address only if the value of DOT1XSTAT is 2. If the value of DOT1XSTAT is changed to 0 from any other value after the Supplicant has been authenticated, an EAPOL-Logoff will be transmitted before the Supplicant is disabled.

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

 Note:

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

Related links

[802.1X Supplicant Operation](#)

Administering emergency numbers

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

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

*** Note:**

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

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

The Avaya Menu administration file

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

To customize Avaya Menu, you need to:

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

The AvayaMenuAdmin.txt file contains the following parameters:

Parameter	Description
AMTYPExx	Specifies the type of Avaya Menu option that you want to configure.

Table continues...

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

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

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

Example

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

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

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

##AMTYPE02=
##AMLBL02=
##AMDATA02=

##AMTYPE03=
##AMLBL03=
##AMDATA03=

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

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

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

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

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

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

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

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

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

GROUP parameter for customized user groups

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

Use the GROUP parameter for this purpose:

- 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.
- At each non-default deskphone, instruct the installer or user to invoke the GROUP from the CRAFT menu and specify which GROUP number to use. The GROUP System value can only be set on a deskphone-by-deskphone basis.

For more information, see *Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*

- Once the GROUP assignments are in place, edit the settings file to allow each deskphone of the appropriate group to download its proper settings.

Example

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

```
## First check if this phone is in group 1.
## If it is, jump to the tag GROUP1
##
IF $GROUP SEQ 1 goto GROUP1
##
## Now check if this phone is in group 2.
## If it is, jump to the tag GROUP2
IF $GROUP SEQ 2 goto GROUP2
##
## The phone is not in either GROUP 1 or 2 so it is in GROUP 0
## {specify settings unique to Group 0}
GOTO END
# GROUP1
## GROUP 1-only settings go here
## {specify settings unique to Group 1}
GOTO END
# GROUP2
```

```
## GROUP 2-only settings go here
## {specify settings unique to Group 2}
# END
## The settings here apply to all three groups
## {specify settings common to all Groups}
```

Administering settings at the deskphone

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

- 802.1X - To set the 802.1X operational mode.
- ADDR - To set the static addresses.
- AGC - To enable or disable Automatic Gain Control.
- CALIBRATION - Applicable to 9621G and 9641G deskphones. To calibrate the touch screen.
- CLEAR - To remove all administered values, user-specified data, option settings, etc. and return a deskphone to its initial "out of the box" default values.
- DEBUG - To enable or disable debug mode for the button module serial port.
- GROUP - To set the group identifier on a per-deskphone basis.
- HANDSET EQ - To set the handset equalization settings of the deskphone.
- INT - To locally enable or disable the secondary Ethernet hub.
- LOG - To enable or disable event logging.
- LOGOUT - To logout the user from the deskphone.
- RESET VALUES - To reset the deskphone to default values including the registration extension and password, any values administered through local procedures, and values previously downloaded using DHCP or a settings file.
- RESTART PHONE - To restart the deskphone in response to an error condition, including the option to reset parameter values.
- SIG - To change the default signaling value from SIP to H.323 or vice versa.
- SIP - To configure SIP call settings.

Warning:

The SIP call settings entered through the CRAFT menu take precedence over other sources for this data, for example- 46xxsettings.txt, or PPM. The only way to override these settings is to go into the CRAFT menu and remove the settings or perform a "Clear" of the deskphone from the CRAFT menu.

- SNTP - To configure the time server settings.
- SSON - To set the site-specific option number.

- VIEW - To review the system parameters for the deskphone to verify current values and file versions.

Administering enhanced local dialing

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

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

The parameters relevant to the Enhanced Dialing Feature are:

- ELD_SYSNUM - Enables enhanced local dialing algorithm for all the system numbers, which include busy indicators and auto dials. To enable enhanced local dialing algorithm, set the parameter to "1" and to disable set it to "0". By default, the parameter is set to "1".
- ENHDIALSTAT - Enhanced dialing status. If set to "1" the enhanced local dialing feature is partially enabled, meaning dialing rules do not apply to dialing from the Contacts list. If set to "2" the enhanced local dialing feature is fully enabled and does apply to dialing from the Contacts list. If set to "0" enhanced local dialing is off.
- PHNCC - The international country code of the Communication Manager call server. For example, "1" for the United States, "44" for the United Kingdom, and so on.
- PHNDPLENGTH - The length of the dial plan on the Communication Manager call server.
- PHNIC - The digits the Communication Manager call server dials to access public network international trunks. For example, "011" for the United States.
- PHNLD - The digit dialed to access public network long distance trunks on the Communication Manager call server.
- PHNLDLENGTH - The maximum length, in digits, of the national telephone number for the country in which the Communication Manager call server is located.
- PHNOL - The character(s) dialed to access public network local trunks on the Communication Manager call server.

Note:

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

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

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

Example: A corporate voice network has a 4-digit dialing plan. The corporate WML Web site lists a 4-digit number as a link on the Human Resources page. A 9621G user taps to select that link. The 9621G deduces the number is a part of the corporate network because the extension matches a dial plan element. The deskphone then dials the number without further processing.

Setting the dial plan on SIP deskphones

Note:

This section only applies to operations with a secondary controller where Communication Manager or Session Manager is not available. In a failover situation, the dial plan is played locally even if a proxy connection is not available. The user might hear a dial tone but cannot make a call.

During manual dialing, a dial plan allows a call to be initiated without using a **Send** button and without waiting for the expiration of a timeout interval. The dial plan consists of one or more format strings. When the dialed digits match a format string in the DIALPLAN configuration parameter, the call is initiated.

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

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

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

Dial plan example:

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

```

where:

- **[2-4]xxx**: Four-digit dial extensions, with valid extensions starting with 2, 3, or 4;
- **[68]xxx**: Four-digit dial extensions, with valid extensions starting with 6 or 8;
- ***xx**: Two-digit Feature Access Codes, preceded by a *;

- **9Z1xxxxxxxxx**: Network Access Code ("9 for an outside line"), followed by dial tone, followed by any string of 10 digits– typical instance of Automatic Route Selection (ARS) for standard US long distance number;
- **9z011x+**: Network Access Code ("9 for an outside line"), followed by dial tone, followed by at least one digit – typical instance of Automatic Route Selection (ARS) for US access to international numbers of unknown, and variable, length.

Additional parameters that affect dialing are as follows:

- **COUNTRY** - Country of operation for specific dial tone generation.
- **PSTN_VM_NUM** (PSTN access number for Voice Mail system) - This parameter specifies the telephone number to be dialed automatically when the deskphone user presses the Messaging button under a non-AST controller. The deskphone places a PSTN call out from the local office and back in to the location that houses the voice mail server. Additional codes necessary to reach a specific user's voice-mail box may also be included. Example 1. SET PSTN_VM_NUM 96135550123
- **ENABLE_REMOVE_PSTN_ACCESS_PREFIX** - When the deskphone is operating with a non-AST controller and the value of the parameter is 0, the PSTN access prefix, defined by the parameter PHNOL, is retained in the outgoing number. If the value is 1, then the PSTN access prefix is stripped from the outgoing number.
- **PHNLAC** - A string representing the deskphone's local area code. When set, this parameter indicates the endpoint's local area code, which along with the parameter LOCAL_DIAL_AREA_CODE, allows users to dial local numbers with more flexibility. Example: SET PHNLAC 617
- **LOCAL_DIAL_AREA_CODE** - A flag indicating whether the user must dial the area code for calls within same area code regions. When the parameter is 0, the user does not need to dial the area code; when this parameter is 1, the user needs to dial the area code. When this parameter is enabled (1), the area code parameter (PHNLAC) should also be configured (i.e., not the empty string). Example: SET LOCAL_DIAL_AREA_CODE 1

Example 1 - Setting the parameter configuration:

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

Table 1: : 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
------------------------	--------------------------------------	-----------------	--------

Table continues...

020	1	Call X from Contacts list	Phone sends an invite message with 2702041018989.
020	1	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.

Setting the date and time on SIP deskphones

9600 Series IP Deskphones need a source of date and time information. This information typically comes from a network time server running the Simple Network Time Protocol (SNTP). The deskphones use several administrative parameters for this functionality. The parameter SNTPSRVR defines the server's IP Address(es). GMTOFFSET defines the offset from Greenwich Mean Time (GMT). DSTSTART and DSTSTOP define the start and end of Daylight Savings Time, respectively. DSTOFFSET defines the Daylight Savings Time offset from Standard Time. Finally, DATETIMEFORMAT defines the format of the date and time display.

History

The History screen displays:

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

The user can select to see at the same time:

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

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

Related links

[Call treatment in a logged out state and busy Call Appearances](#) on page 94

Call treatment in a logged out state and busy Call Appearances

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

If a deskphone gets a call when the user is not logged in, the system saves the incoming call in a database. When the user logs in again, the deskphone displays the previous call log and the calls received in the logged out state.

You need to configure the Call Log feature through System Manager. The Call Log feature has the following limitations:

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

Related links

[History](#) on page 93

Customizing ring tones

End users can select any ring tone from the 14 standard ring tones, 8 classic and 6 rich ring tones. The deskphone then saves the ring tone that the user selected in PPM. Ring tones for external, internal, priority, and intercom calls (distinctive ringing) are combinations of specified frequency, duration and cadence values. You can replace the 8 classic ring tones with the Korean ring tones or the customized ring tones.

Related links

[Korean ring tones](#) on page 95

[Customized ring tones](#) on page 95

[Downloadable ring tones](#) on page 97

Korean ring tones

Korean ring tones are part of the SIP software bundle download. To administer all or any of these tones to replace the existing external, internal, priority and intercom call tones, set the EXTEND_RINGTONE parameter in the settings file with the names of the Korean tones you want available to the user. For example, to replace all the Avaya classic ring tones with the Korean ring tones, set the EXTEND_RINGTONE parameter to Korean ring tone XML files as follows:

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

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

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

* Note:

Do not include space between the XML file names.

Related links

[Customizing ring tones](#) on page 94

Customized ring tones

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

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

! Important:

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

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

Related links

[Customizing ring tones](#) on page 94

[Ring tone XLS cell descriptions](#) on page 96

Ring tone XLS cell descriptions

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

Table continues...

Cell Name	Description	Comment
Next Note	Leave empty; this cell is not currently used.	Reserved for future use.
Cadence Patterns and States	Cadence patterns are set for internal, external, priority, and intercom calls.	
Cadence 1 to 8	The number of available cadences.	
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.
Reserved for future use.	When all applicable cells have been filled in, use this control to create an xml file for this specific tone.	

Related links

[Customized ring tones](#) on page 95

Downloadable ring tones

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

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

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

the display name and the URL. The system treats any subsequent equals signs after the first sign as a part of the URL. Percent encode a comma if you use it in the URL.

Ensure that audio files must:

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

For example,

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

Related links

[Customizing ring tones](#) on page 94

Administering voice mail

Use the settings file to configure the **Messages** button by setting the system parameter MSGNUM to any dialable string. MSGNUM examples are:

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

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

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

```
SET MSGNUM 1234
```

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

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

```
SET PSTN_VM_NUM 913455551234
```

*** Note:**

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

Administering headset profiles

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

Using the headset

- When the deskphone receives a call, the headset produces an audible beep and the user can answer the call by pressing a button on the headset.
- When a call is established, the user can disconnect the call by pressing a button on the headset.
- When a user makes or receives a call using the buttons on the deskphone, the headset automatically connects the speech path without the need for the user to press any buttons on the headset.

*** Note:**

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

Administering Presence

Presence overview

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

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

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

Presence services categorizes users into two types:

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

A user can simultaneously be a watcher and presentity.

Users can manually set their own presence through the deskphone menu. You can configure the deskphone to use the Send All Calls (SAC) feature when the user sets the Do Not Disturb (DND) status.

Access Control List

The Access Control List specifies whether other users on the network can view the presence of another user. By default, users can automatically see the presence of other users. You can disable the automatic viewing by setting the `PRESENCE_ACL_CONFIRM` parameter in the `46xxsettings` file.

Deskphones that are in 1XC Shared Control Mode with a 1XC soft client can control automatic viewing. The 1XC softclient displays a pop-up window to the presentity that prompts whether to allow or to restrict the display of the presence information.

Instant Messaging

Instant Messaging (IM) is available to the user if the Presence feature is operational, and the SIP signaling is set to TLS. Users can communicate through text messages by using this feature. The deskphone stores the IM conversations in the History log. Each deskphone can store IMs up to 2 MB. If a user logs out of a deskphone and logs back into a different deskphone, the IM history is not available.

Note:

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

Presence profile

Presence profile is a part of the communication profile of a user. Presence profile is configured in User Profile Management of Avaya Aura® System Manager. In cluster deployment of multiple presence servers, presence profile explicitly associates a user with a presence server instance. The `46xxsettings` file supports the use of only one presence server address. Using presence profile is an efficient method to ensure that a user is connected to the appropriate presence server. For information about configuring a presence profile, see Administering Avaya Aura® Presence Services.

Error conditions

If deskphones are correctly administered, most issues that deskphone users face are LAN based. Quality of Service (QoS), server administration, and other issues affect user perception of the IP deskphone performance.

Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP contains troubleshooting information about potential issues after the deskphones are installed. User guides of specific deskphone models also contain troubleshooting information about issues with specific IP deskphone applications.

Chapter 9: Customizing 9600 Series IP Deskphones

Avaya Aura® Call Center Elite features

The 9600 SIP software supports Avaya Aura® Call Center Elite features on 9600 Series IP Deskphones models 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS. The Avaya Aura® Call Center Elite features are not supported on the 9601 deskphones. Avaya Aura® Call Center Elite 6.2 is the minimum requirement to support the following Call Center Elite features:

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

For detailed information on all the Call Center features, see *Using Avaya 96X1 SIP Agent Deskphones with Avaya Aura® Call Center Elite*, and *Administering Avaya Aura® Call Center Elite*, available on the Avaya support Website www.avaya.com/support.

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

You can administer the Call Center features through the settings file using the following parameters:

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

Applications and features provisioning

You can configure the following parameters to enable or disable certain applications and general phone features. The following table lists the features and applications and their corresponding parameters that enable

Application or feature	Parameter name	Description
History application	ENABLE_CALL_LOG	If enabled, users can access the list of unanswered and answered calls. If disabled, the History application is not displayed to the user and calls are not logged.
Redial	ENABLE_REDIAL	If enabled, users can redial one to three previously called numbers. If disabled, redialing is not available to the end user.
Redial list	ENABLE_REDIAL_LIST	If enabled, users can select a number to redial from a list. If disabled, only the previously-dialed number can be redialed.
Contacts application	ENABLE_CONTACTS	If enabled, users can access a list of numbers and make calls by selecting a contact name or number. If disabled, the deskphone does not display the Contacts application and users cannot set up or maintain the contact list.
Contacts modification	ENABLE_MODIFY_CONTACTS	If enabled, users can change or update the contact list. If disabled, users cannot change or update the contact list.
Exchange contacts	PROVIDE_EXCHANGE_CONTACTS	If enabled, users can gain access to contacts stored in the Exchange server through the Contact list, by pressing the Exchange contact button. If disabled, users cannot gain access to the Exchange contacts.
Options & Settings menu option	PROVIDE_OPTIONS_SCREEN	If enabled, the deskphone displays the Options & Settings menu option in the Avaya menu or Home Screen. If disabled, the deskphone does not

Table continues...

Application or feature	Parameter name	Description
		display the Options & Settings menu option. Users cannot change any of the features and ppeonfiasscsted with the Options & Settings menu.
Network Information menu option	PROVIDE_NETWORKINFO_SCREEN	If enabled, the deskphone displays the Network Information menu option in the Avaya menu or Home Screen. If disabled, the deskphone does not display the Network Information menu option.
Logout menu option	PROVIDE_LOGOUT	If enabled, the deskphone displays the Logout menu option in the Avaya menu or Home Screen. If disabled, the deskphone does not display the Logout menu option.
Exchange calendar	PROVIDE_EXCHANGE_CALENDAR	If enabled, users can integrate and gain access to the Exchange calendar on the deskphone. If disabled, users cannot gain access to the Exchange calendar on the deskphone.

Team Button overview

The Team Button feature provides the facility to watch or monitor the deskphone of another user. A user can manage the call handling of the deskphone that is being monitored. A user can monitor another deskphone to:

- See if the monitored deskphone redirects calls to any other deskphone.
- See if the monitored deskphone has an active call.
- See and answer if the monitored deskphone has an incoming ringing call.
- Make a speed dial call to the monitored deskphone by pressing the **Team Button** softkey when the monitored deskphone does not have an active call.
- Transfer an active call to the monitored deskphone by pressing the **Team Button** softkey

The Team Button feature is configured on the Avaya Aura® Communication Manager and Avaya Aura® Session Manager. A station is configured to monitor another station.

Team Button override

The monitored deskphone might have a call redirect active through any of the following features:

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

You can configure Communication Manager and Session Manager such that the monitoring deskphone overrides the call redirection active on the monitored deskphone. If the call redirection override is set, the monitored station rings for 30 seconds. If no one answers the call, the call is automatically sent to the redirection number.

Direct Transfer

The Direct Transfer feature facilitates quick transfer of an active call to a monitored station. Team Button must be configured for this feature to be active.

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

Related links

[Team Button parameters](#) on page 105

Team Button parameters

Parameter	Default value	Description
TEAM_BUTTON_REDIRECT_INDICATION	0	Controls if the redirection indication is shown on a Team Button on a monitoring station. Valid values are 0 and 1.
TEAM_BUTTON_REDIRECT_OVERRIDE	0	Specifies whether the monitoring deskphone can override the SAC, CFWD, ECF features set by the monitored deskphone. Valid values are: • 0: Monitoring deskphone cannot override the features. • 1: Monitoring deskphone cannot override the features by placing the call to the monitored deskphone. • 2: Monitoring deskphone displays a message to the user asking if the call should be placed to the monitored deskphone.  Note: The value of this parameter is stored in PPM.
TEAM_BUTTON_RING_TYPE	3	Specifies the default ring tone for all Team Buttons . Valid values are 1 to 8.
TEAM_BUTTON_RING_TYPE_PARAMETER_BUTTON	NULL	Specifies a list of name-value pairs that indicate default ring tones.

Related links

[Team Button overview](#) on page 104

Direct Transfer

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

When a call is answered at a monitoring deskphone, the user can begin the transfer process of transferring the call to the monitored station by pressing the line corresponding to Team button. The monitoring deskphone puts the existing call on hold and places a call to the monitored station. A speech path is established and the monitoring station and monitored station can converse.

To complete the transfer between the original call and the monitored deskphone, the user at the monitoring station can disconnect the call by going on-hook or by pressing the **Complete** softkey.

Direct Transfer is applicable only to the Team Button feature and you need not configure the Direct Transfer feature on Avaya Aura® System Manager.

Team Button ring

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

Team Button override

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

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

You can configure Avaya Aura® Communication Manager and Avaya Aura® Session Manager such that the monitoring deskphone overrides the call redirection active on the monitored deskphone. If the call redirection override is set, the monitored deskphone rings for 30 seconds. If no one answers the call, the call is automatically sent to the redirection number.

Insert a section title

Insert content for the first section.

Insert a section title

Insert content for the first section.

Enhanced Call Forward

The Enhanced Call Forward (ECF) feature provides flexibility to forward incoming calls to different destinations, based on the following different conditions:

- Caller type: Whether the call is coming from internal number or an external number.
- Phone status: Based on the phone status a user can choose to forward the calls in the following scenarios:
 - All incoming calls.
 - When the deskphone is busy.
 - When there is no answer on the deskphone.

You can set the **ECF** feature button for the deskphone to display on the Feature Screen, Quick Touch Panel, SBM24, BM12, Favorite Feature on the Phone Screen, or the Home Screen. Use the **ECF** feature button to access and enable or disable ECF.

Multiple Device Access

The 9600 Series IP Deskphones 6.3 onwards support Multiple Device Access (MDA) with which you can register up to 10 SIP devices with your extension.

With MDA you can do the following:

- Make and receive calls to any of the registered devices.
- Switch to another registered device during an active call.
- Bridge on to calls at multiple registered devices.

Alert all other registered devices for an incoming call to your extension. When you answer a call on any registered device, the alert on all other devices stops. The other devices show indication of an active call on the same call appearance number.

- Be on multiple calls at one time on different devices, but only one call per device.

For example, you can listen to a conference call on one device and answer an incoming call on a second device without putting the conference call on hold. The two calls appear on separate call appearances on all registered devices.

- Use conference and transfer features.

Bridging on to a call at other registered devices and invoking a transfer drops the call from all devices after the transfer completes.

Advanced call conference

In collaboration with the Avaya Aura® Conferencing server and Communication Manager, SIP release 6.5 provides advanced call conference features to the end user. Avaya Aura® Conferencing 7.0 is the minimum requirement to support advanced conferencing. See the following table for a comparison of the advanced call conference features with different conference servers:

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

*** Note:**

The 9601 deskphone does not support the conference details screen.

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

- CONFERENCE_FACTORY_URI
- CONFERENCE_SERVER_ADDRESS
- CONFERENCE_SERVER_PORT
- ENABLE_SECURE_HTTP_FOR_CONFERENCING_SERVICE

*** Note:**

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

Setting a large font size for the display

About this task

Use the following procedure to display the English language text in a larger font on the deskphone display. When you configure the large fonts feature, the deskphone displays the **Text Size** option in the **Options & Settings** menu. The large text size setting applies to the deskphone display as well as any attached button modules.

The 9601 deskphone does not support the large text size feature.

Before you begin

Ensure that the file `Mlf_Enlarge.xml` resides on the web root of the http server.

Procedure

Modify the settings file to set the `LANGLARGEFONT` parameter as follows:

```
SET LANGLARGEFONT "Mlf_Enlarge.xml"
```

Setting the background logo

About this task

Use the following procedure to set a customized background logo. Deskphone models 9601, 9608, and 9608G do not support a background logo.

Before you begin

Ensure that you have set the parameter `LOGOS` in the settings file.

Procedure

Modify the settings file to set the `CURRENT_LOGO` parameter to one of the labels specified in the `LOGOS` parameter.

When the logo file is not configured correctly or the HTTP server containing the logo file is not reachable, the phone might be temporarily unavailable.

In System Manager 6.3.8 or later, you cannot use this parameter if you are using the Expanded Template support for SIP Endpoints feature.

Related links

[Background logo specifications](#) on page 109

Background logo specifications

The following table specifies the information on the maximum size, color depth and format of a logo supported by the deskphone models 9611G, 9621G and 9641G. Deskphone models 9601, 9608, and 9608G do not support a background logo.

Models	Maximum size (pixels)	Color depth (bit)	Format
9611G	217 x 130	16	JPG

Table continues...

Models	Maximum size (pixels)	Color depth (bit)	Format
9621G	232 x 140	16	JPG
9641G	232 x 140	16	JPG

Related links

[Setting the background logo](#) on page 109

Creating and using localized language files

9600 IP Deskphones are shipped with localized interfaces in a defined set of multiple languages. If you want to create a localized interface in a language that is unavailable, use the Language localization tool to create localized language files.

Language localization tool is a MS® Excel file that lists all the text labels displayed on the deskphone. The file includes two macros that generate the localized language file. A user can import these language files to the SIP IP deskphone.

You cannot create new text labels by using the language localization tool. If the language file does not contain the strings for a given text label, the phone uses the built in English language files for display.

Before you begin

- MS® Excel must be installed on your computer.
- You must have administrative rights to store and access the file on the HTTP server.

Procedure

1. Download the Language localization tool file from support.avaya.com.
2. Open the Language localization tool on your computer.
3. Enter the details of the required translation. See Language localization tool field-descriptions for information about the fields.
4. Click **Create language file**.

The output language file is created in a XML format and saved to the same directory where you have stored the tool.

 Note:

Retain the symbol **%s** while creating new strings for localization. For reference, see `Plf_English.xml` file.

5. Copy the output language file to the HTTP server.

- Restart the deskphone. On rebooting, the deskphone downloads the language file from the server.

Related links

[Language localization tool field descriptions](#) on page 111

Language localization tool field descriptions

Field	Description
Name of Language	Specifies the language to which the strings must be translated to.
Filename	Specifies the name of the output language file. You can use a maximum of 20 characters in the filename. The output file will be created as <Filename>.xml
Input method	Specifies whether the user sees an option to enter characters in the requested language. The Abc/123 softkey displays the language options Available options are: • ASCII • Hebrew
Translation	Type the translation of the text label. The translation that you have entered overrides the automatic translation generated by the macros.

Related links

[Creating and using localized language files](#) on page 110

WML browser

WML browser overview

9600 Series IP Deskphones have an built-in WML browser application. Users can see the browser application listed in the **Home** screen of Avaya menu, if the deskphone is administered to include the WML browser.

WML browser feature comparison

The following table shows a comparison of different features of the WML browser across the deskphone models.

Feature	9601	9608/9608G	9611G	9621G	9641G/9641GS
Top line	Yes	Yes	Yes	Yes	Yes
Application lines	2	4	4	4	5
Line buttons	Yes	Yes	Yes	No	No
Selectable objects per line	1	1	1	1	1
Application line height (in pixels)	14	15	31	38	38
Softkeys per screen	3	4	4	5	5
Softkey height (in pixels)	14	14	31	38	38
Navigation buttons	Yes	Yes	Yes	No	No
Text input	Yes	Yes	Yes	Yes	Yes
Color support	No	No	Yes	Yes	Yes
Supported image format	No	JPEG	JPEG	JPEG	JPEG
Max image width (in pixels)	NA	175	300	430	430
Click to dial	Yes	Yes	Yes	Yes	Yes
Add to phonebook	Yes	Yes	Yes	Yes	Yes
Characters per line (normal font)	26	31	40	39	39
Characters per line (large font)	NA	25	22	26	26
Characters per softkey (normal font)	8	8	8	8	8
Characters per softkey (large font)	NA	6	6	8	8

Administering the WML browser

Procedure

To administer the WML browser, configure the WML browser related parameters in the 46xxsettings file.

Related links

[WML browser parameters](#) on page 64

Integrating Microsoft® Exchange

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

- View calendar reminders that users can dismiss or snooze, or use the reminders to make a call.
- Dial into conference calls without entering conference call number and passcode.
- View exchange contacts.

 Note:

Exchange Web Services is supported for Microsoft® Exchange Server 2010 or later.

You can secure the link between the deskphones and Exchange server. The deskphone adds the Exchange contacts of a user to the contact list and displays in the Exchange Contacts screen. Users can save the Exchange contacts to PPM using the +Local key. To gain access to the Exchange contacts, calendar, and reminder information, users must use Avaya Menu to specify the following information:

- Credentials
- Display preferences
- Calendar data

Users can modify or delete contacts that are saved in PPM. Avaya SIP deskphones do not support the presence tracking feature for the Exchange contacts.

Related links

[Microsoft Exchange parameters](#) on page 63

Network progress tones overview

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

- Dialtone
- Ringback
- Busy

- Congestion
- Intercept
- Public Dialtone

All countries listed in this appendix are applicable to the 96xx phones. Some of the dialtone entries have changed from previous releases to be distinctively different than the public dialtone entries.

Alphabetical country list

A:

- Abu Dhabi
- Albania
- Argentina
- Australia
- Austria

B:

- Bahrain
- Bangladesh
- Belgium
- Bolivia
- Bosnia
- Botswana
- Brunei
- Bulgaria

C:

- China (PRC)
- Colombia
- Costa Rica
- Croatia
- Cyprus

D:

- Denmark

E:

- Ecuador
- El Salvador
- Egypt

F:

- Finland

- France

G:

- Germany
- Ghana
- Greece
- Guatemala

H:

- Honduras
- Hong Kong

I:

- Iceland
- India
- Indonesia
- Ireland
- Israel

J:

- Japan
- Jordan

K:

- Kazakhstan
- Korea
- Kuwait

L:

- Lebanon
- Liechtenstein

M:

- Macedonia
- Malaysia
- Mexico
- Moldova
- Morocco
- Myanmar

N:

- Netherlands

- New Zealand
- Nicaragua
- Nigeria Norway

O:

- Oman

P:

- Pakistan
- Panama
- Paraguay
- 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

Chapter 10: System Failover and Survivability

Supporting survivability

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

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

Deskphones fail over to a secondary controller for alternate registration (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.

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

If the SIP connection recovery is in progress due to a brief network outage, the phone will also attempt to recover its XMPP connection to Presence Server automatically by re-logging in to PS. If the PS server is unreachable, Presence will not be available. If the connection recovery fails, the phone will display an appropriate error message.

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.

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

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

Related links

[Survivability configuration examples](#) on page 119

[Survivability requirements](#) on page 121

[Select the active controller](#) on page 125

Survivability configuration examples

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

Related links

[Supporting survivability](#) on page 118

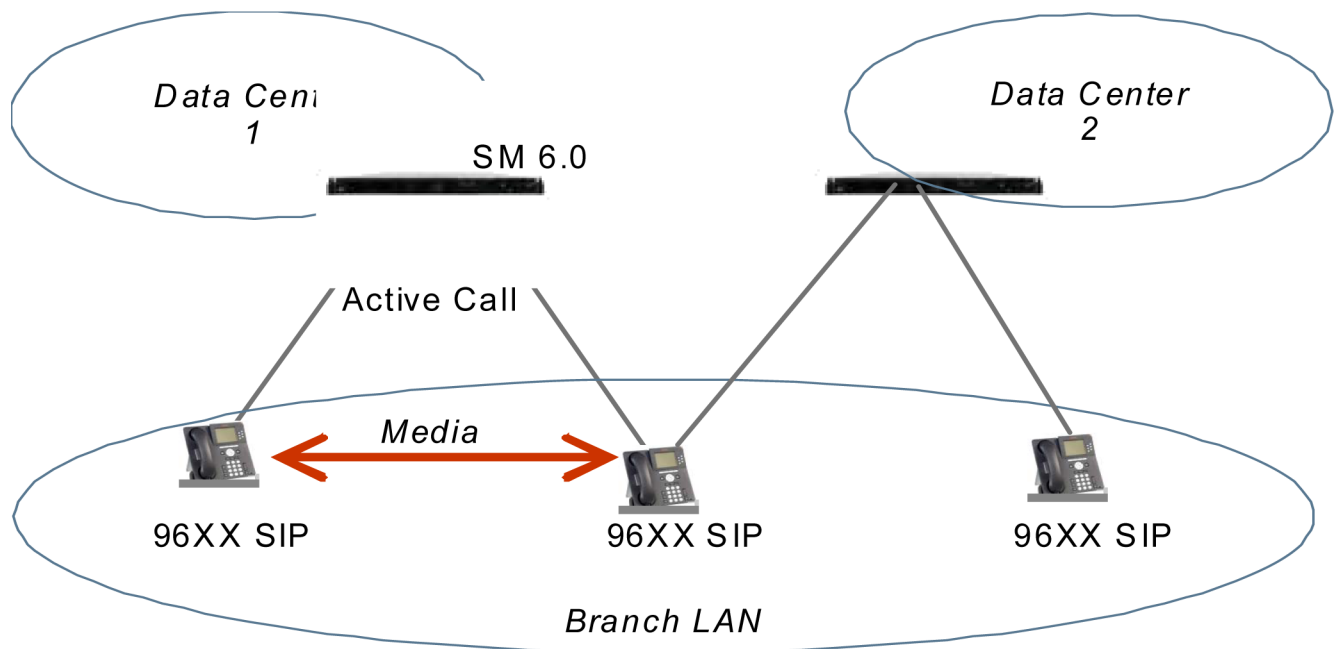
[Configuration Example 1](#) on page 119

[Configuration Example 2](#) on page 120

[Configuration Example 3](#) on page 120

Configuration Example 1

SIP software Release 6.0 and later offers simultaneous registration with multiple controllers, and improved feature availability during and after failover to a secondary controller.

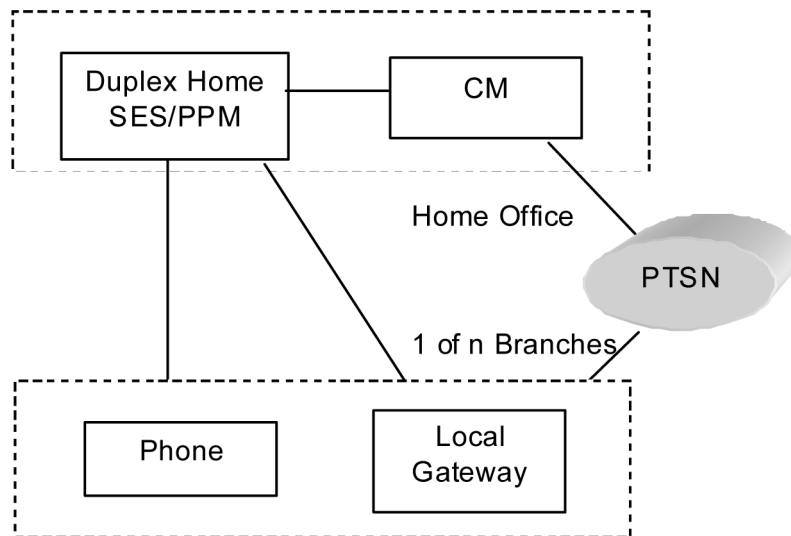


Related links

[Survivability configuration examples](#) on page 119

Configuration Example 2

The use of multiple controllers over a single controller improves survivability configuration.

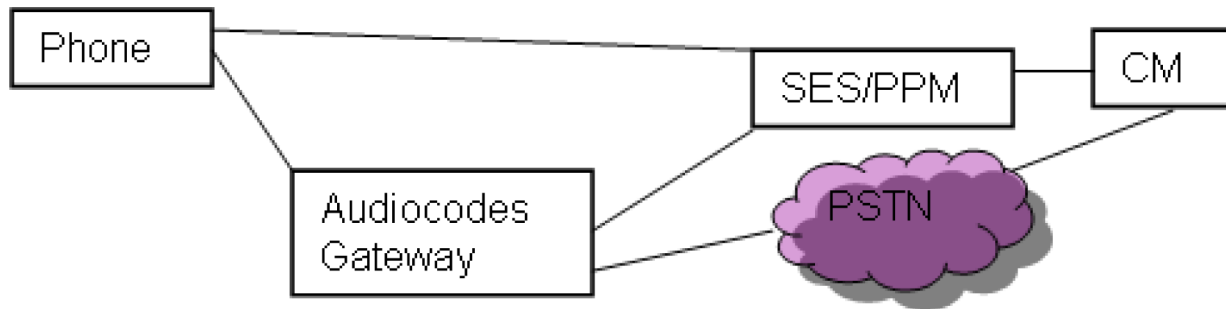


Related links

[Survivability configuration examples](#) on page 119

Configuration Example 3

Minimal survivability using a single controller for failover.

**Related links**

[Survivability configuration examples](#) on page 119

Survivability requirements

- Latest SIP firmware
- Supported local (secondary) gateway with Proxy or back-to-back user agent (B2BUA) capabilities:
 - Audiocodes MP-series analog and BRI gateways
 - Teldat Vyda gateway (Router and PBX)
 - Avaya Secure Router 2330 and 4134
 - Cisco 2811 ISR
 - Juniper SRX 210 and 240
 - I55
- IP Office
- Session Manager

Related links

[Supporting survivability](#) on page 118

Provisioning survivability for SIP Deskphones

About this task

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

Procedure

1. Set the applicable failover configuration parameters (described in [Configuring survivability](#) on page 122) in the 46xxsettings file.
2. Provision the gateway per the Application Notes, available on the Avaya support Web site.
3. Load the latest SIP Release software and associated files on the file server.

4. Reboot all registered phones from SES/SM.
5. Power up other phones.

Configuring survivability

Use the `46xxsettings` file to set these parameters.

By administering survivability configuration parameters using the `46xxsettings` file (or using the default values if applicable), the SIP deskphones can quickly switch to an active controlling server and experience minimal disruption. The failover/failback parameters 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.
- `RECOVERY_REGISTER_WAIT` - Reactive Monitoring Interval in seconds.
- `REGISTERWAIT` - Proactive Monitoring Interval in seconds.
- `SIP_CONTROLLER_LIST` - Configured Controller list. A comma-separated list of SIP URIs, a hostname, or numeric IP address. If null, DHCP/DNS will provide the defaults.
- `SIMULTANEOUS_REGISTRATIONS` - The number of Session Managers with which the deskphone will simultaneously register.
- `SIPREGPROXYPOLICY` - Registration Policy. The default value of this parameter is `simultaneous`.

Related links

[Setting a controller via the user interface](#) on page 123

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 for 9608, 9611G, 9621G, and 9641G Deskphones (Document Number 16-603604)*. The user can log in successfully with a controller at this point.

Related links

[Configuring survivability](#) on page 122

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:

Related links

- [Determine controllers to monitor](#) on page 124
- [Determine which monitored controllers are available](#) on page 124
- [Select the active controller](#) on page 125
- [AST feature determination](#) on page 126
- [PPM synchronization](#) on page 127
- [Failover/failback behavior](#) on page 128

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.

Related links

- [Controller Determination and Survivability Activity](#) on page 123

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.

Related links

[Controller Determination and Survivability Activity](#) on page 123

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:

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.

Related links

[Controller Determination and Survivability Activity](#) on page 123

[Supporting survivability](#) on page 118

AST feature determination

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

If the parameter value is 1, the phone determines if that controller supports the AST (Advanced SIP Telephony) feature set or not. The phone sends a SUBSCRIBE request to the active controller for the "Feature Status Event Package" (avaya-cm-feature-status). If the request succeeds, the phone

proceeds with PPM Synchronization. If the request is either rejected, is proxied back to the phone, or does not receive a response, the deskphone assumes that AST features are not available.

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

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

Related links

[Controller Determination and Survivability Activity](#) on page 123

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 - applies only when registered to a Session Manager (SM)
- ListOfIdentities - only when registered to a SM
- MWExt - applies only when registered to an SM
- VMNumber - applies only when registered to an SM

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.

Related links

[Controller Determination and Survivability Activity](#) on page 123

Failover/failback behavior

Related links

[Controller Determination and Survivability Activity](#) on page 123

[System performance](#) on page 128

[Deskphone behavior during failover](#) on page 128

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.

Related links

[Failover/failback behavior](#) on page 128

Deskphone behavior during failover

During failover, 9600 Series SIP IP Deskphones will:

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

In general, the phone does not attempt to preserve SIP transactions in progress when a controller failure is detected, and some mid-call features like conferencing can fail. However, in some

scenarios the same transaction may succeed if re-attempted once the transition to a new controller has been completed.

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

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

- If the user is active on a call, a failover icon displays when failing over to a non-AST controller and messages like “Link recovery,” “Limited phone service,” and “Calls may be lost,” inform the user of a failover situation. The message “Limited phone service” also displays during failover transition from one Session Manager server to another when the subscriptions have not yet been moved successfully to the secondary SM. The only user options are to navigate to the Phone screen by pressing the OK softkey or the Phone button or hang up the call.
- When failing over to a third party secondary controller, an Acquiring Services screen displays during failover and failback transitions to an active controller and a Call Preservation message window may display for deskphones running SIP software Release 2.6 or greater. Most other screens and applications except for CRAFT screens are unavailable until an active controller is found. However, the user can navigate to the Contacts, Call Forward feature, Avaya (A) Menu or Call Log applications (if administered). Pressing the Phone button causes the user to be redirected to the Home Screen (if one is administered).
- If a call is active when failover occurs, that call will remain active. The user cannot initiate new calls while the phone transitions to the alternate server.
- With SIP software Release 2.6 and later releases for failover to secondary controller for alternate registration, the user can access Contacts, the Call Forward button, Call Log, standard Avaya menu or Home Screen applications if administered. The user cannot make calls in these applications.
- Certain softkeys do not display and their related functions are unavailable.
- Call appearance information does not display while dialing, but does appear when Call is pressed.
- Call connection may take longer than usual.
- Upon failover, any calls in the process of being transferred and any 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 fallback.
- With SIP software Release 6.0 and later, 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., Communication Manager, Communication Manager “knows” about both calls and the user can resume a held call, conference call, or call transfer normally. If both controllers are not connected to the same feature server, the second Feature Server would not have any information about the first call displayed on the phone. In this scenario features that can be applied to the first call would be limited because all the call data is stored in Communication Manager; SM does not store any information related to any call.
- Preserved Media Connections - Applies only to Session Manager configurations when moving a subscription from one SM to another. As of SIP software Release 2.6 in a scenario where the the primary SM fails, any active shuffled or direct media call will be preserved if a new call is received while a preserved call is active. The phone allows the user to manually put the active (media preserved) call on hold or allows the user to switch to the new call and automatically put the preserved call on hold using auto-hold. A media preserved call displays the failover icon in place of a call-associated icon that is left justified on an application line preceding the displayed name or phone number. When active on a media preserved call the softkeys displayed are “Hold, blank, blank, End Call.” Conference and Transfer are not available. When a media preserved call is put on hold, the softkeys displayed are “Resume, blank, blank, blank, blank.” The phone can receive incoming calls at this point but is not available to make outgoing calls or to invoke AST features. The phone supports media preservation sufficient for alternate

registration; if a phone experiences a mid-dialog failure (for example, a timed out or failed SIP request, or a socket-level failure), the phone behaves as if the dialog had been terminated (but does not send a BYE) and preserves the media session until the near-end user hangs up.

Related links

[Failover/failback behavior](#) on page 128

About the user interface/failover experience

The user interface experiences described below expand upon the information provided in [Failover/failback behavior](#) on page 128. User guides for each deskphone model also provide this information in a “user-friendly” format.

Related links

[User interface in failover/failback](#) on page 131

[User experience during failover transition](#) on page 131

[User experience during stable failover](#) on page 134

[User experience during failback](#) on page 135

[User experience during failover](#) on page 135

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.

Related links

[About the user interface/failover experience](#) on page 131

User experience during failover transition

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

Related links

[About the user interface/failover experience](#) on page 131

[Failover to a secondary controller for alternate registration \(SES F/O to SM to a non-AST controller\)](#) on page 132

[Moving subscriptions from one SM to another SM/BSM \(Branch System Manager\) due to failover](#) on page 132

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.

Related links

[User experience during failover transition](#) on page 131

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

Transition is comprised of the following conditions for moving subscriptions:

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

Moving subscriptions occurs immediately after limbo has ended or when there is a graceful socket closure. For an active call scenario, media preservation will only keep shuffled calls or calls using direct media between endpoints up with a direct RTP stream until the call has ended. The user can only put this call on Hold, resume the call, or end the call. The user can also answer any incoming call and the media preserved call is put on hold. During MSI the user can't use call related softkeys (Hold, Conf, Transfer) for call appearances or bridged calls and the softkeys are not removed from

the screen. If the user presses another call appearance or a Favorite Feature an error beep occurs. The Prompt Line displays "Limited phone service". Click to dial links do not work.

All AST features and BCAs are displayed on the phone and SBM24 during MSI regardless if there is an active call. If a user tries to use an AST feature, the feature fails and the phone displays "Feature invocation failed." When the Phone Button is pressed, the Home Screen (if there is one) displays instead of the Phone Screen. The user can press the Phone button to navigate to the Home Screen (if there is one) and all Home Screen sub-screens are accessible. The phone does not block new invites during transition. Changes to applications other than Contacts, for example, Speed Dial, are cached and are updated by whichever PPM with which the phone successfully registers. Any changes made under the Avaya menu Options & Settings take place (including the Home Screen) immediately.

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

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

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

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

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

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

Related links

[User experience during failover transition](#) on page 131

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/Avaya Aura[®] Communication Manager will instead be routed to the local gateway.
- Emergency calls (to the provisioned emergency numbers as defined in the dial plan) will be permitted whether those phones are in failover or normal mode. The Emergency softkey is available when a new controller is found.
- The MWI (Message Waiting Indicator) will be cleared, but voice mail is still available.
- One-button voice mail access will be available if the central voice mail system continues to operate and will make a PSTN call to the voice mail system. Depends on correct provisioning.
- Local deskphone features will be available: audio selection (speaker / headset / handset), mute.
- Local 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 and Home Screen Options & Settings are blocked under minimal survivability configurations. Any of the more extensive survivability configurations (for example, moving subscriptions to a secondary SM/BSM for simultaneous registration) allow access to

the Avaya Menu and updates to Options & Settings. Likewise, Contacts can be accessed and updated.

- CRAFT changes may be made and are saved locally on the phone.
- If the phone is logged out during failover, the local phone cache is cleared.

Related links

[About the user interface/failover experience](#) on page 131

User experience during failback

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

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

Related links

[About the user interface/failover experience](#) on page 131

User experience during failover

Feature	Normal Operation with Communication Manager	Failover Operation with a Generic SIP Gateway
Make call	Yes	Yes
Receive call	Yes	Yes
Call Hold	Yes	Yes
Consultative Hold	Yes	Yes
Ad hoc conferencing	Yes, up to 6 parties	Yes, up to 3 parties
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

Table continues...

Feature	Normal Operation with Communication Manager	Failover Operation with a Generic SIP Gateway
Inbound call management	Yes (Communication Manager COR)	Yes (depends on local proxy capabilities and provisioning)
Outbound call management	Yes (Communication Manager COR)	Yes (proxy)
Calling party block	Yes	No
Calling party unblock	Yes	No
Call park	Yes	No
Call unpark	Yes	No
Call pickup	Yes	No
Directed call pickup	Yes	No
Extended call pickup	Yes	No
Auto callback	Yes	No
Malicious call trace	Yes	No
EC500 on/off	Yes	No
Transfer to voice mail	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

Related links

[About the user interface/failover experience](#) on page 131

Chapter 11: Related resources

Documentation

See the following related documents at <http://support.avaya.com>.

Title	Use this document to:	Audience
Overview		
<i>9600 Series IP Deskphones Overview and Specifications</i>	See characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security and licensing requirements of the 9600 Series IP Deskphones.	For people who want to gain a high-level understanding of the 9600 Series IP Deskphones features, functions, capacities, and limitations.
<i>Avaya Aura® Session Manager Overview and Specification</i>	See characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security and licensing requirements of the Avaya Aura® Session Manager.	For people who want to gain a high-level understanding of the Avaya Aura® Session Manager features, functions, capacities, and limitations.
Implementing		
<i>Deploying Avaya Aura® Session Manager</i>	See the installation procedures and initial administration information for Avaya Aura® Session Manager.	For people who install, configure, and verify Avaya Aura® Session Manager on Avaya Aura® System Platform.
<i>Upgrading Avaya Aura® Session Manager</i>	See upgrading checklists and procedures.	For people who perform upgrades of Avaya Aura® Session Manager.
<i>Deploying Avaya Aura® System Manager on System Platform</i>	See the installation procedures and initial administration information for Avaya Aura® System Manager.	For people who install, configure, and verify Avaya Aura® System Manager on Avaya Aura® System

Table continues...

Title	Use this document to:	Audience
		Platform at a customer site.
Administering		
<i>Administering Avaya Aura® Session Manager</i>	See information about how to perform Avaya Aura® Session Manager administration tasks including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.	For people who perform Avaya Aura® Session Manager system administration tasks.
<i>Administering Avaya Aura® System Manager for Release 7.0.1</i>	See information about how to perform Avaya Aura® System Manager administration tasks including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.	For people who perform Avaya Aura® System Manager administration tasks.
Maintaining		
<i>Maintaining Avaya Aura® Session Manager</i>	See information about the maintenance tasks for Avaya Aura® Session Manager.	For people who maintain Avaya Aura® Session Manager.
<i>Troubleshooting Avaya Aura® Session Manager</i>	See information for troubleshooting Avaya Aura® Session Manager, resolving alarms, replacing hardware, and alarm codes and event ID descriptions.	For people who troubleshoot Avaya Aura® Session Manager.
Installing and Maintaining		
<i>Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP</i>	See information for installing and maintaining 9600 Series IP Deskphones.	For people who install and maintain 9600 Series IP Deskphones.

Related links

[Finding documents on the Avaya Support website](#) on page 138

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at <http://support.avaya.com/>.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.

5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Related links

[Documentation](#) on page 137

Support

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Index

Numerics

802.1X [84](#)

A

account and password parameters [62](#)
active controller
 survivability [125](#)
administering
 VLAN [73](#)
administering emergency numbers [85](#)
administering enhanced local dialing [90](#)
administering voice mail [98](#)
administration methods [14](#)
administration of SIP deskphones
 Communication Manager [19](#)
 Session Manager [23](#)
administrative requirements [13](#)
administrator responsibilities [13](#)
advanced call conference [108](#)
advanced conferencing [108](#)
applications and features provisioning [103](#)
AST Feature Determination, for Failover [126](#)
audio operation and quality monitoring parameters [50](#)
audio quality [83](#)
audio quality field descriptions [44](#)
audio settings [52](#)
authentication [78](#)
Avaya Aura Call Center Elite [102](#)
Avaya Menu administration file [85](#)

B

background logo specifications [109](#)
bridging calls [107](#)
button modules [18](#)

C

Call Appearances [94](#)
Call Center Elite features [102](#)
call conference [108](#)
call conference feature [108](#)
Call Log [94](#)
call redirection [106](#)
call redirection active [106](#)
Call treatment [94](#)
certificate management [70](#)
Checklist
 administration [15](#)
 administrative [15](#)

common operation parameters [52](#)
Communication Manager
 administration of SIP deskphones [19](#)
configuration example 2
 survivability [120](#)
configuration example 3
 survivability [120](#)
configuration examples
 survivability [119](#)
configuration parameters specification [48](#)
Configured Controller(s) [124](#)
configure the settings file [32](#)
Controller Determination and Survivability [123](#)
controllers [24](#)
countries [113](#)
country list [113](#)
customized ring tones [95](#)
customized user groups [88](#)
customizing ring tones [94](#)
customizing ring type [106](#)
customizing Team Button ring [106](#)

D

date and time setting [93](#)
date and time settings [52](#)
deskphone administering settings [89](#)
deskphone interface settings parameters [52](#)
DHCP
 configuration overview [25](#)
 lease time [28](#)
 Option 43 codes [28](#)
 option configurations [25](#)
 site-specific parameters [30](#)
DHCPACK
 parameter configuration [29](#)
dial plan parameters [44](#)
dial plan setting [91](#)
Direct Transfer [106](#)
disabling application [103](#)
disabling feature [103](#)
display settings [52](#)
DNS addressing [83](#)
downloadable ring tones [97](#)

E

Elite features [102](#)
enabling application [103](#)
enabling feature [103](#)
Enhanced Call Forward [107](#)
enhancements, new in this release [12](#)
error conditions [101](#)

Ethernet parameters	59	logging and debugging parameters	45
F		M	
Fail Back, User Experience during	135	Microsoft Exchange parameters	63
Fail Back, User Experience During	135	models	12
Failover, Stable, User Experience During	134	Monitored Controllers	124
Failover, Telephone Behavior	128	multiple device access	107
Failover, User Experience	134		
Failover, User Experience for Transitions	131	N	
Failover/Failback, User Interface in	131	Network progress tones	113
Failover/Failback Behavior	128		
failover and survivability		O	
requirements	121	override	106
supported features	135	overview	11
Failover Experience, User Interface	131		
Failover Transitions	131	P	
feature buttons	21	parameters	
field descriptions		account parameters	62
audio	44	audio operation and quality monitoring	50
		configuration parameters specification	48
G		debugging parameters	45
general and phone application timer parameters	51	deskphone interface settings	52
general network parameters	57	Ethernet parameters	59
GROUP parameter	88	general and phone application	51
		general network parameters	57
H		IEEE 802.1.x parameters	61
headset profile		logging parameters	45
using the headset	99	Microsoft Exchange parameters	63
History	93	password parameters	62
History screen	93	port ranges parameters	50
		presence parameters	62
I		protocol-specific parameters	37
IEEE 802.1.x parameters	61	QoS parameters	60
IP address reuse	79	server addresses and port parameters	32
		VLAN parameters	60
K		ping	80
korean ring tones	95	port ranges parameters	50
		ports	
L		received packets	80
language	77	TCP	80
language and country settings	52	transmitted packets	82
language localization tool		UDP	80
creating and using	110	presence overview	99
language localization tool field descriptions	111	Presence parameters	62
legal notices		presence profile	100
list of countries	113	protocols	
LLDP		received packets	80
overview	65	transmitted packets	82
TLV impact on system parameter values	67	protocol-specific parameters	37
LLDPDU transmitted by the deskphones	66	proxy server	24
		push server	78

Q

QoS parameters [60](#)

R

received packets
 ports [80](#)
 protocols [80](#)
 redirection number [106](#)
 registrar [24](#)
 registration [78](#)
 related documentation [137](#)
 requirements
 failover and survivability [121](#)
 ring tone XLS cell descriptions [96](#)

S

secure installation
 parameters [71](#)
 security [69](#)
 server addresses and ports parameters [32](#)
 Session Manager
 administration of SIP deskphones [23](#)
 set a large font size for the display [108](#)
 set the background logo [109](#)
 settings file [32](#)
 configuring [32](#)
 settings reuse [79](#)
 SIP deskphones
 administration on Communication Manager [19](#)
 administration on Session Manager [23](#)
 SNMP activation [78](#)
 support [139](#)
 supported features
 failover and survivability [135](#)
 supported SIP environments [18](#)
 survivability [118](#)
 active controller [125](#)
 configuration example 2 [120](#)
 configuration example 3 [120](#)
 configuration examples [119](#)
 Survivability [123](#)
 Survivability, Provisioning [121](#)
 Survivability, Setting a Controller for [123](#)
 Survivability Activity and Controller Determination [123](#)
 System Performance during failover/failback [128](#)

T

TCP ports [80](#)
 team button [104](#)
 Team Button [106](#)
 team button, 46xxsettings [105](#)
 Team Button override [106](#)

Team Button ring [106](#)
 TLV impact on system parameter values [67](#)
 traceroute [80](#)
 transmitted packets
 ports [82](#)
 protocols [82](#)

U

UDP ports [80](#)

V

VLAN
 administering [73](#)
 VLAN Default Value [73](#)
 VLAN detection [74](#)
 VLAN parameters [60](#)
 VLAN separation rules [75](#)
 VLAN separation rules and related parameters [75](#)
 VLAN tagging [73](#)

W

WML browser, 46xxsettings [64](#)
 WML browser, administering [111](#), [112](#)
 WML browser, parameters [64](#)