Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323

Release 6.6
Issue 1
June 2015

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Avaya grants You a license within the scope of the license types described below, 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”).

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.

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Downloading Documentation

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

Contact Avaya Support

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

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.

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 to 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.

Trademarks

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

Intended Audience

This guide is intended for personnel who install, administer, and maintain Avaya Aura® Communication Manager, DHCP, HTTP/HTTPS servers for Avaya 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS IP Deskphones H.323, and a Local Area Network (LAN). Before deploying the product, ensure that you have the following knowledge, skills, and tools:

Knowledge

- Networking
- H.323 protocol

Skills

How to configure:

- Avaya Aura® Communication Manager
- DHCP server
- HTTP or HTTPS server

Tools

- Avaya Aura® Communication Manager
- Avaya Aura® System Manager

Related resources

Documentation

For more information related to the use of the H.323 9600 IP Deskphones refer the following documents:

See the following related documents at support.avaya.com.

Document number	Title	Use this document to:	Audience
Overview			
16-604299	Avaya 9600 Series H.323 IP Deskphones Overview and Specifications	Refer to the overview and specifications.	People who want to gain a high-level understanding of the product features, functions, capacities, and limitations.
Using			
16–603593	Using Avaya IP Deskphone 9608, 9608G, and 9611G	Refer to tasks related to using the deskphone.	End users and administrators
16–603594	Using Avaya IP Deskphone 9621G, 9641G and 9641GS	Refer to tasks related to using the deskphone.	End users and administrators
16-603613	Using Avaya IP Deskphone H. 323 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS in the Call Center	Refer to tasks related to using the deskphone in a call center environment.	End users and administrators
Implementing			
16–603603	Installing and maintaining Avaya IP Deskphone 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS H.323	Refer to procedures related to installing and upgrading the deskphone.	Administrators

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com .

After logging in to the website, enter the course code or the course title in the Search field and click Go to search for the course.

Course Code	Course Title
ACIS-6006 ACIS	Avaya Communication Manager (5.2.1)
APSS-1300 APSS	Avaya Networking

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.

Chapter 2: Overview

Deskphone models relevant to this guide

This guide describes the following deskphone models: 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS.

All models except the 9608 have a Gigabit Ethernet switch with which the phone and a PC can share the same LAN connection. Thus, these models do not work with the 30A switched hub interface. The 9641G and 9641GS deskphones also have an integrated Bluetooth™ interface. For information about setting up a Bluetooth device, see *Using Avaya 9621G/9641G/9641GS IP Deskphone H.323*.

This document describes the installation and maintenance procedures for the deskphones. For information about using the deskphone features, see the user documentation. For information about desk mounting or wall mounting, see the instructions boxed with the phone or the Avaya Support website at http://www.avaya.com/support.

New in this release

General enhancements

- Introduced the 9641GS deskphone to the 9600 Series IP Deskphones portfolio. 9641GS has a 5.0 inch TFT capacitive touch screen, which provides better touch response to the users.
- Added support for Bluetooth® secure simple pairing and an easier interface for connecting to Bluetooth® devices.
- Added support for Russian and Korean keyboards.
- Added support for Thai keyboard and language file.
- Enhanced local dialing rules for contacts.
- Added support for DHCP option 43.
- Added support for sending unmodified packets to the PC port based on the PHY2TAGS parameter configuration.
- Added support for automatic labelling for line and bridge appearance through the CADISPMODE parameter.
- Added the feature retain the highlight on the active or on-hold call appearance when there is an incoming call, which is configurable through the CALLAPPRSELMODE parameter.

- Added the feature to hide Drop, Transfer, Conference and Hold softkeys. These softkeys use the HOLDSTAT, XFERSTAT, CONFSTAT, DROPSTAT and CCBTNSTAT parameter configurations.
- Support for sending + to Ccommunication Manager.
- Added support for four layer 2 queues on the internal switch instead of two.
- Ability to control display of the information associated with a call, in the agent information line. This feature uses the AGTCAINFOLINE parameter.
- VLAN separation scheme. Added new parameter VLANSEPMODE to enforce separation of the PC port and deskphone.
-

Security enhancements

- Periodic tests of certificate expiration or revocation for ongoing TLS connections according to SERVER_CERT_RECHECK_HOURS
- Validation of the server identity, as presented in subjectAltName/common name in the Subject field with the server IP or host name configuration. The TLSSRVRVERIFYID parameter is used for the server identity validation.
- Configurable timer for checking the expiration of trusted certificates, identity certificate, and OCSP certificates.
- Certificate signature validation for certificates with sha256WithRSAEncryption signature.
- 2048 bits asymmetric key length for SSH server.
- Download of intermediate certificates for cases where servers do not provided the full chain up to the root CA.
- Ability to view the SSH fingerprint in the SSH CRAFT menu.
- Support for downloading identity certificate using PKCS12 format.
- Secure renegotiation as specified in IETF RFC 5746.
- Added support for Online Certificate Status Protocol (OCSP) for checking whether certificates presented to the phone by servers are good, revoked, or unknown.
- Disabled SSLv3 because of POODLE vulnerability, as defined in CVE-2014-3566.
- Added support for key usage with SCEP certificate requests.
- Added support for FIPS 140-2 cryptographic libraries.
- Added support for 802.1Q tagging with VPN packets.
- Enhanced SLA agent security.
- Added support for SHA-256 on agent greetings files.

Administrative features

- CALCSTAT retains its configuration when a file server is not reachable
- Configurable duration of Unsuccessful Discovery Timer using the UDT parameter.
- Increased the character limit of SCEPPASSWORD to 50 characters.

Interoperability

The 9600 Series IP Deskphones support interoperability with IP Office 9.1. The following features are available in an IP Office environment:

- H.323 Signaling encryption using Annex-H
- Support for SRTP and SRTCP
- Support for Korean keyboard and language files
- Wideband codec icon and Local Network Quality icon

Chapter 3: Installing the Deskphone

Avaya IP Deskphones

The Avaya 9600 Series IP Deskphones product line uses Internet Protocol (IP) technology with Ethernet interfaces.

The 9600 Series IP deskphones support DHCP and HTTP/HTTPS over IPv4/IPv6 including Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP). Both the protocols enhance deskphone administration and servicing respectively.

These deskphones use DHCP to obtain dynamic IP addresses. The deskphones use HTTP to download firmware files and HTTP/HTTPS to download configuration files.

With all 9600 Series IP deskphones, you need only one Ethernet connection from the enterprise switch to connect both deskphone and personal computer. You can connect your personal computer and deskphone using an Ethernet cable.

The following information pertains to Australian law:

This equipment must be installed and maintained by trained service personnel. All input/output ports are classified as Safety Extra Low Voltage (SELV, in the meaning of IEC 60950). To maintain safety compliance when connecting the equipment electrically to other equipment, the interconnecting circuits shall be selected to provide continued conformance of clause 2.3 for SELV circuits (generally, double/reinforced insulation to 240 Vac rms to any primary/mains circuitry and 120 Vac rms to any telecommunications network circuitry). To ensure that these conditions are adhered to, interconnect the equipment only with the already approved/certified equipment.

Updating phone software for installation

About this task

A phone that is shipped from the factory might not contain the most up-to-date software for registration and operation. When you first plug in the phone, a software download from an HTTP server might be initiated. The software download provides the phone upgraded functionality.

For subsequent downloads of software upgrades, the Avaya call server provides the capability for a remote restart of the IP phone. When you restart the phone, the phone automatically restarts and performs a download if new software is available. For more information, see About software distribution packages on page 59 and Downloading software packages on page 60.

Pre-installation checklist

Print copies of this checklist for each server and deskphone.

Requirements for your network:	
❑	The LAN uses Ethernet Category 5e cable to run the IPv4 or IPv6 version of Internet Protocol.
❑	Your call server must haveAvaya Aura®Communication Manager Release 6.2 or later version installed. Avaya only supports 9608, 9608G, 9611G, 9621G, 9641G and 9641GS deskphones running on Communication Manager 6.2 or later.
❑	Verify that you have installed the following circuit packs on the switch: • TN2602 or TN2302IP Media Processor circuit pack. Avaya recommends that sites with a TN2302 IP Media Processor circuit pack must install a TN2602 circuit pack to benefit from increased capacity. • TN799C or D Control-LAN (C-LAN) circuit pack. **Important:** Release 6.0 or later requires TN799C V3 or greater C-LAN circuit pack(s). For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya Support website.
❑	Verify that you have configured the Avaya call server correctly. For more information, see *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323* and Communication Manager documentation on the Avaya Support website.
❑	Verify that you have administered the DHCP server and application correctly. For more information, see *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323* and Communication Manager documentation on the Avaya Support website.
❑	Verify that you have administered the HTTP/HTTPS server and application correctly. For more information, see *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323* and Communication Manager documentation on the Avaya Support website.
❑	Verify that you have loaded the upgrade script and application files from the Avaya Support website correctly on the HTTP/HTTPS server.
❑	If applicable, administer the DNS server. For more information, see *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323* and Communication Manager documentation on the Avaya Support website.
❑	If applicable, administer the WML server. For more information, see *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323* and Communication Manager documentation on the Avaya Support website.

Note:

All server applications, such as DHCP and DNS, can co-reside on the same hardware subject to the specific restrictions of each individual application.

Requirements for each deskphone:	
❑	Verify that you have an extension number and an Communication Manager security code (password) for each applicable IP deskphone. If your call server and the phone settings file support unnamed registration, you do not need an extension or password. However, without an extension or password, the phone has limited functionality. For information about unnamed registration, see About unnamed registration on page 30.
❑	Verify that a Category 5e LAN jack is available at each phone site and a Category 5 modular line cable that connects the deskphone to the LAN jack. Cat 5 cables with an RJ45 plug have a plug size restriction of 36 mm.
❑	Verify that each deskphone receives power through a Telephone Power Module, which you must order separately. For PoE Input connection, use only with UL listed I.T.E. equipment with PoE output. If LAN supplies IEEE-standard power, or Power over Ethernet, to the deskphone, the phone does not require a power module.
❑	One Category 5e modular line cord to connect the IP deskphone and the computer, if applicable.
❑ ❑	Verify that the deskphone set package includes the following components: • One phone set with dual position flip-stand or clip-stand • One wideband handset capable of transmitting and receiving 7 KHz audio. • One H4DU 9-foot long 4-conductor coiled handset cord, plugged into the phone and the handset. • A “Important Notice and Warning” page which provides the URL for the Avaya Support website to download all other documentation. • To use 9641G in a call center environment: a 9600 Dual Headset Adapter Kit (PK25) (Comcode: 700500729) and 9641G Call Center Faceplate Kit (PK25) (Comcode: 700500728) that contains 25 Dual Headset Adapter (DHA) units and 25 9641G removable CC-faceplate units respectively. If applicable, verify that the you have staged the phone administered the phone with applicable VPN settings. For information on the VPN settings, see *VPN Setup Guide for 9600 Series IP Telephones, 16-602968*.

Note:

For sites using wired headsets, the 9600 Series IP deskphones support only the Jabra GN1216 Headset cord and the Plantronics HIS headset cord. For more information, contact your Avaya representative.

Plugging in the deskphone

About this task

Caution:

Use the correct jack when you plug in the deskphone. You can find the jacks at the rear of the deskphone housing. Icons on the side of the jacks represent the correct use of each jack.

You can only provide power to the

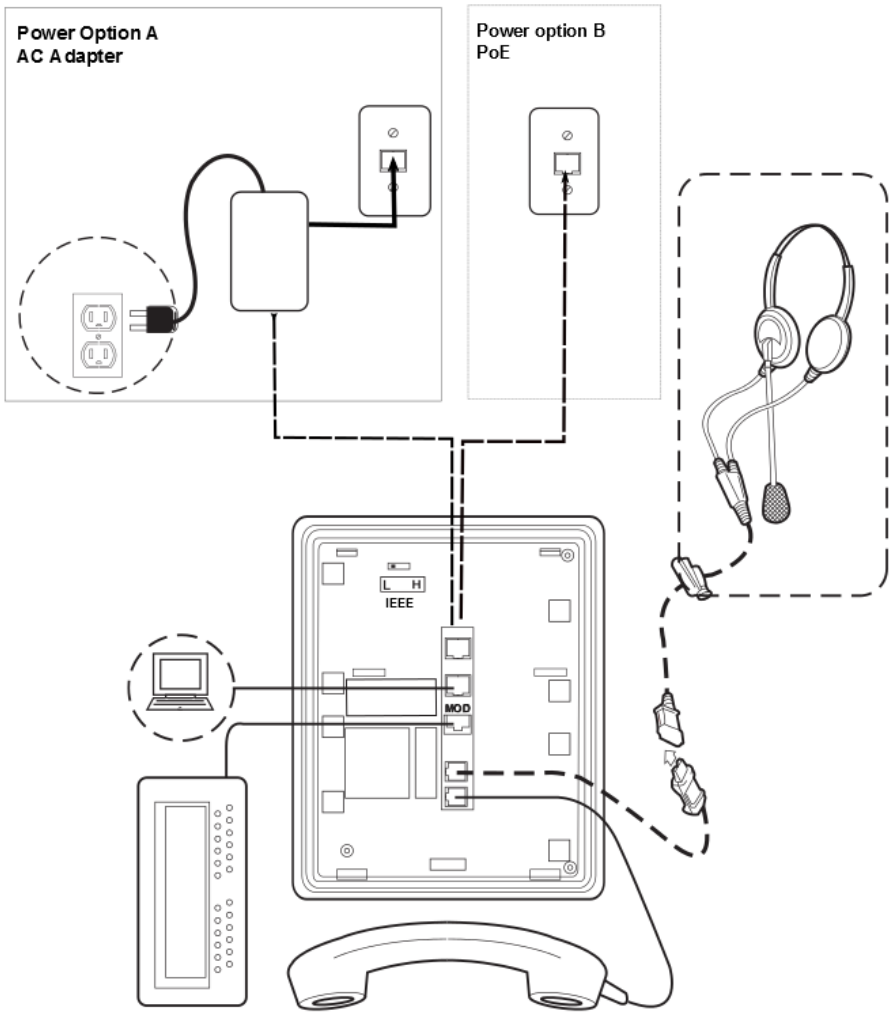
Note:

Note:

In 9611G, 9641G, and 9641GS, the USB interface supports USB login, use of digital pictures from a USB device as a screensaver, and import or export of contact lists by a Flash drive. The 9608 does not support USB devices, and the 9621G model does not have a USB jack. Since the power consumption of the drive varies from product to product, you cannot state how a USB will impact PoE power class. When the drive attempts to register with the deskphone, the deskphone determines if its current power class setting is adequate to support the drive. If power is adequate, the deskphone lets the drive register. If the power is not adequate, the deskphone will alert the user to change the power class by changing the IEEE power switch setting from L to H. In extreme situations, the total power consumption with the addition of a USB device may be greater than what the Class 3 power source can provide. In that case, the deskphone detects this and instructs the user to use an auxiliary power supply or to temporarily disconnect one or more of the modules while the USB device is in use. The system parameter USBPOWER determines for which power class or classes to enable power to the USB interface. For more information, see *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*.

Caution:

Failure to connect the proper cables with the proper jacks might result in an outage in part of your network.



Completing the power connection

Procedure

1. Plug one end of the H4DU 4-conductor coiled handset cord into the phone and the other end into the handset.

2. Plug one end of the first Category 5 modular line cord into the Ethernet jack of the PC and the other end into the secondary Ethernet jack on the phone, if appropriate.
3. For an IEEE-powered deskphone, plug one end of the second Category 5 modular line cord into the Ethernet jack on the phone. Plug the other end of this cord into the Ethernet wall jack.
4. For a locally powered deskphone, connect the Category 5 modular line cord provided with the IP Phone Single Port PoE Injector SPPOE-xx, where *xx* represents the model number into the Ethernet jack on the phone. Plug the femite end of this cord into the deskphone. Plug the other end of this cord into the SPPOE-xx power injector jack labeled **DATA & POWER OUT**. Plug another Category 5 cord into the SPPOE-xx power injector jack labeled **DATA IN**. Plug the other end of this cord into the Ethernet wall jack. Finally, connect the SPPOE-xx to an AC power source.

Installing a Dual Headset Adapter (DHA)

About this task

You can install a Dual Headset Adapter (DHA) on call center deskphones. The supervisor can monitor calls in progress by attaching a DHA directly to a deskphone or to an attached button module. The 9621G does not support a DHA.

Order the 9600 Dual Headset Adapter Kit (PK25) (Comcode 700500729), which includes dual headset adapters and required cables for 25 deskphones.

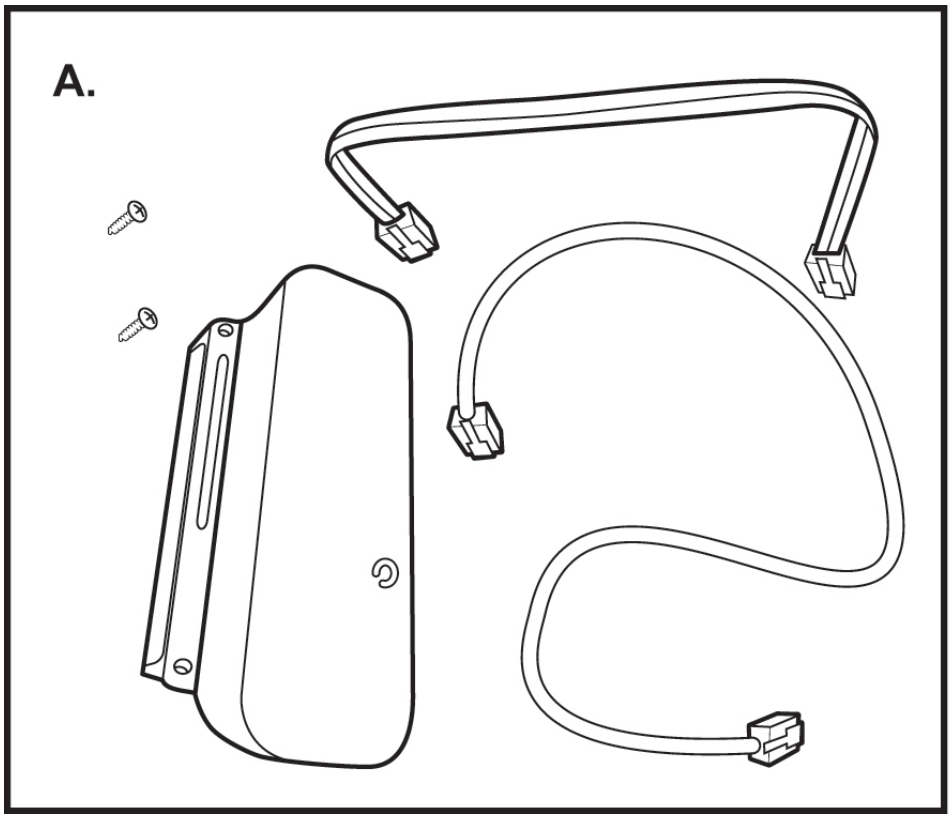


Figure A shows the DHA Package Contents.

To install a DHA directly to the deskphone and alternatively to an attached button module, see the following figure.

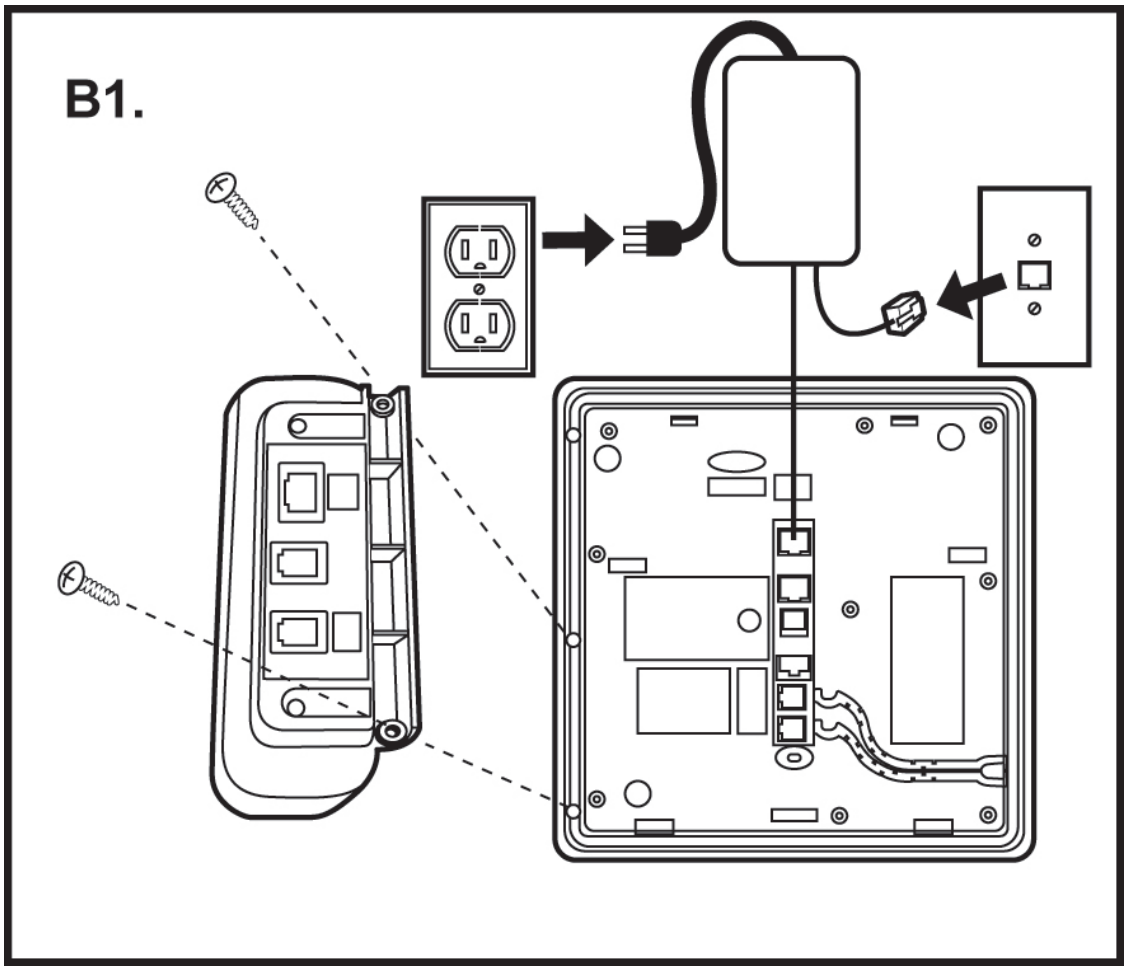


Figure B1 :Attaching the DHA to a deskphone.

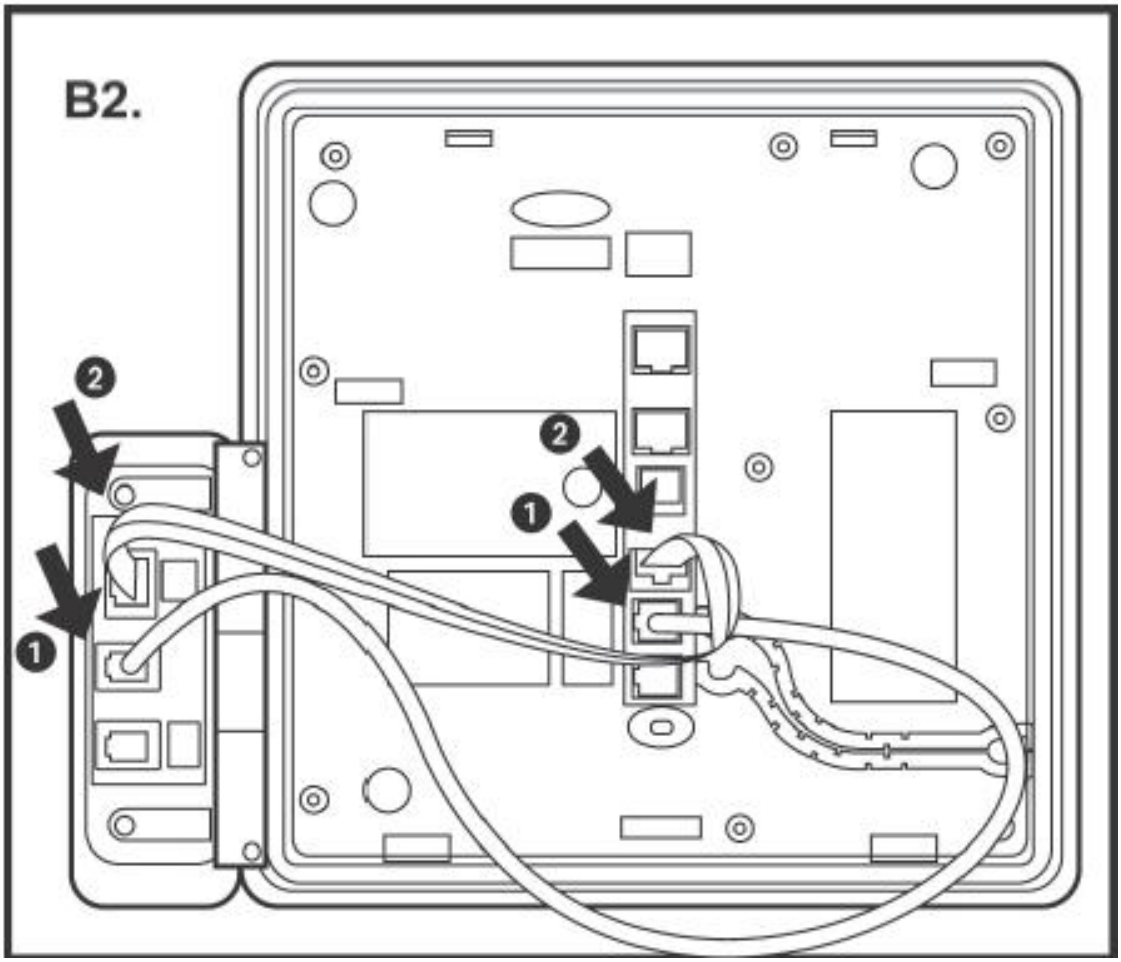


Figure B2 : Attaching the DHA to the phone power and audio cables.

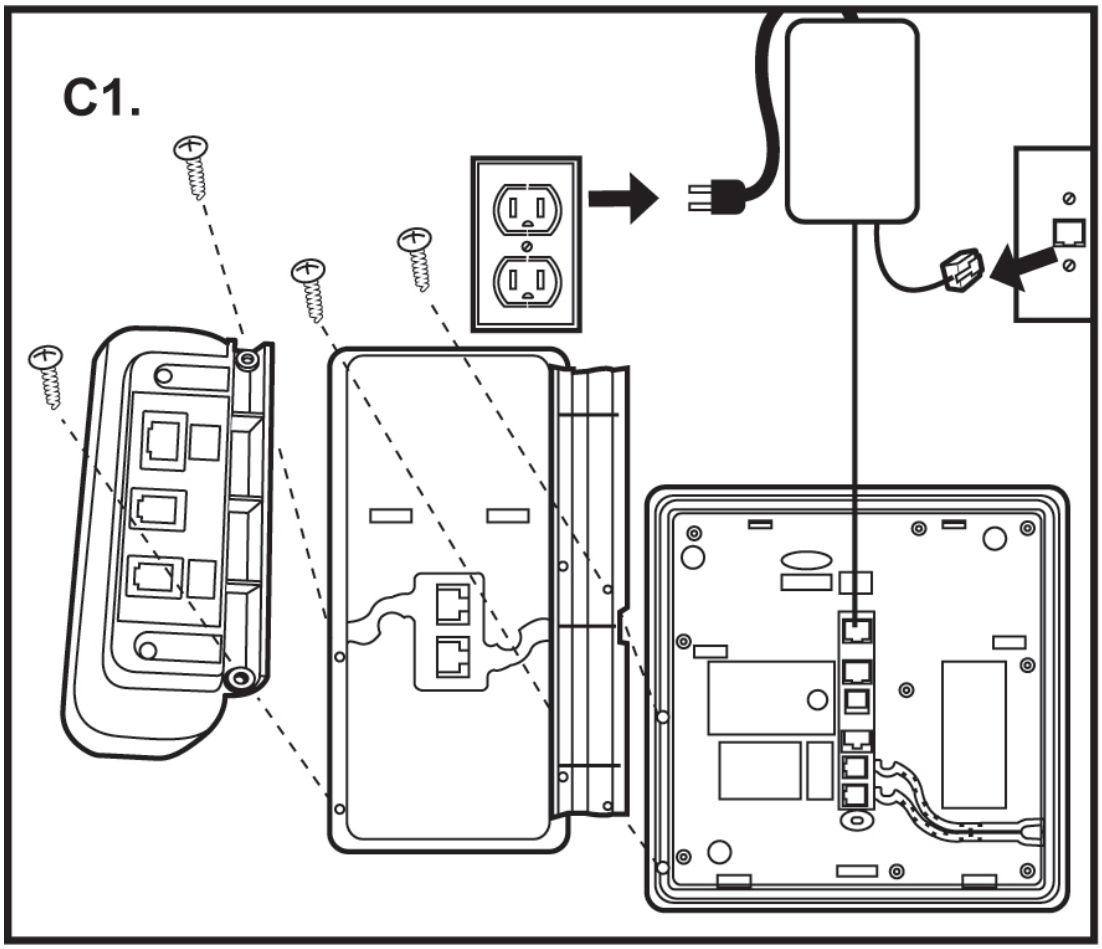


Figure C1: Attaching the DHA to an (optional) button module.

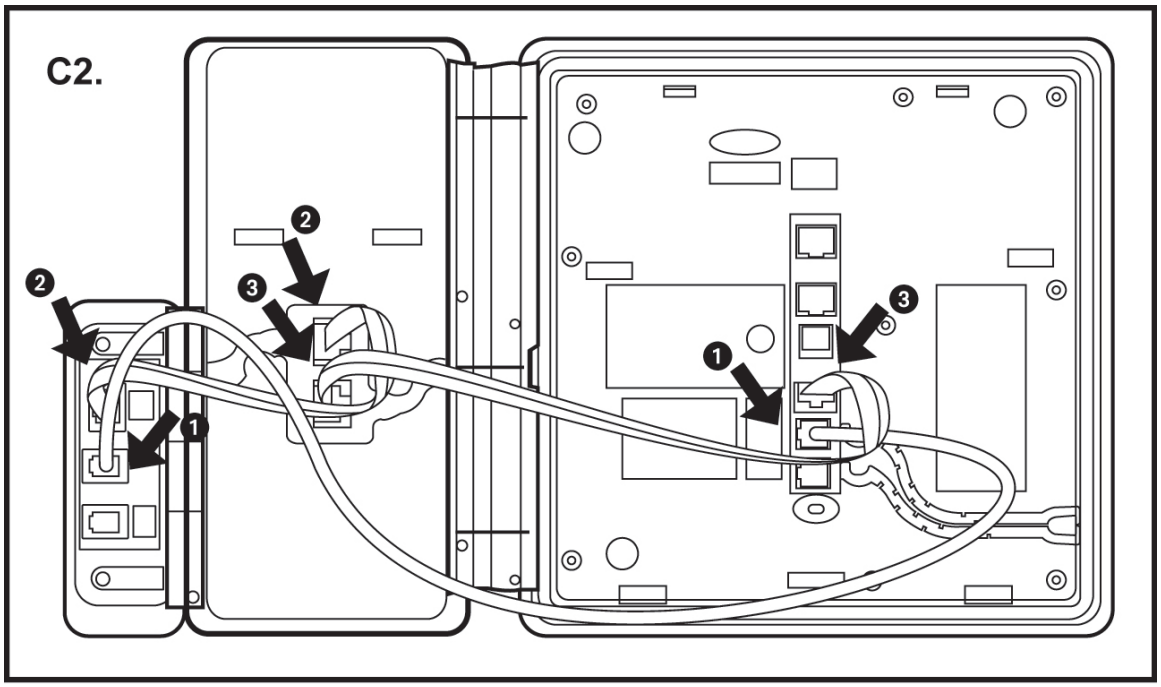


Figure C2: Attaching cable connection of the DHA to an optional button module and the deskphone.

9641G Call Center faceplate installation

About this task

The 9641G IP deskphones used in a call center come with special faceplate kits: 9641G Call Center Faceplate Kit (PK25) (Comcode 700500728). The removeable faceplate has the following features:

- Covers the handset pockets
- Maintains the switch hook “down” position
- Covers the **Forward** and **Headset** buttons
- Relabels the **Speaker** button as the **Release** button to facilitate ending calls

Note:

To allow **Release** button operation for 9641G deskphones, administer the **Release** button with the AGTSPKRSTAT parameter set to 2 and the CALLCTRSTAT parameter set to 1.

To install the 9641G Call Center faceplate:

Procedure

1. If already connected, remove the HAC cord from the underside of the phone.
2. With the phone facing up and resting flat on a hard surface, pry up a corner of the standard faceplate. Use your fingers, a flat screwdriver, or other non-sharp device. Continue prying around the edge of the standard faceplate until the faceplate is released from the phone.

3. Align the tabs on the 9641G Call Center faceplate with the slots on the outer edges of the deskphone and push down to lock the tabs into the slots.
4. Ensure that the display bezel surrounding the screen is in proper position.
5. Plug the HAC cord back into the underside of the phone.

Plugging in and resetting the deskphone using the Dynamic Addressing Process

Note:

Before you start this process you must have an extension number for the IP deskphone and the Communication Manager security code (password) for that extension, unless you intend to use the deskphone with unnamed registration. For more information, see About unnamed registration on page 30. Any reference to the HTTP server applies equally to an HTTPS server. You can run the plug in and reset process successfully using the following description. If you see error messages, see Chapter 5: Troubleshooting on page 67.

As the deskphone initializes, you see messages, some of which are part of DHCP process, with a power on indication and dynamic feedback. These messages indicate that the phone is active and not locked. You also receive useful information, about the status of the network, the server, or the downloading operations, before the dial tone.

Phone initialization

This section description describes the software architecture on which the requirements are based and provides an overview of how you can expect the phone to operate during startup and software upgrades. This description is not a comprehensive description of all internal tasks performed during startup.

The system stores the files in five areas of reprogrammable nonvolatile or flash memory in the phones:

- A boot program area
- Two Kernel/Root File Systems
- One Application File System
- One Temporary Storage area

The phone supports two Kernel or Root File Systems for backup if one file system is corrupted but activates only one file system when the phone starts or resets. Temporary Storage stores a new Signed Application or Library Software Package that the current application downloads. You can then install the package in the active Kernel or Root File System after the next reset.

When a phone starts, the boot programs check the Kernel or Root File System that was marked as the one to be activated. If this file system is not corrupted, the boot program transfers control to a process in that file system. If that file system is corrupted, the boot program checks the other Kernel/Root File System.

If that file system is not corrupted, the system:

- Marks that file system as the file system to be activated
- Sets the value of RFSINUSE to the name of the Signed Kernel or Root Software Package that was used to install that file system
- Transfers control to a process in the file system

If both Kernel/Root File Systems are corrupted, the phone becomes nonfunctional and you must return the phone for repairs.

A process in the active Kernel/Root File System first checks whether a Signed Application or a Library Software Package is stored in Temporary Storage. If yes, the process installs the Application Software Package or the Library Software Package. The system installs both if either software package has a different file name than the currently installed version and replaces the existing corresponding files in the Application File System. The process then deletes the copy of the Signed Application or Library Software Package stored in Temporary Storage. If the process does not find a Signed Application or Library Software Package in Temporary Storage, the process checks the integrity of the application files. If the files are corrupted, the process installs files from the Backup Package and replaces the corrupted application files in the Application File System. Each time an Application Software Package or a Library Software Package is installed, the system sets the value of the persistent parameter APPINUSE to the file name of the Signed Application or Library Software Package from which the package was installed. If the application files are not corrupted, or after the Backup Package has been installed, the system transfers control to the application installed in the Application File System. Note that the processes in the Kernel/Root File System do not connect to the network or download files.

The application then connects to the network, obtains any necessary IP address information, and download files. The file download begins with the upgrade and settings configuration files, and including Signed Software Packages and other separately downloaded files such as Language Files and Certificate Files. When the phone downloads a Signed Software Package which can contain either Kernel and Root Software Packages or Application and Library Software Packages, it is initially stored in volatile memory (RAM). The system installs the other downloaded files such as Language Files and Certificate Files directly in the Application File System.

When either type of Signed Software Package is downloaded, the Signing Authority Certificate is extracted from the package and is validated using a copy of the Avaya Product Root Certificate Authority Certificate that is contained in the existing application software files. If the Signing Authority Certificate is invalid, the package is deleted. If the Signing Authority Certificate is valid, the Hardware Version File in the package is validated using the corresponding Signature File in the package and the Signing Authority Certificate. If the signature is invalid, the package is deleted. If the signature is valid, the Hardware Version File is used to validate whether the package is valid for the model and hardware version of the phone. If the package is invalid, the package is deleted. If the package is valid, the signature of the software package is validated using the corresponding Signature Files in the package and the Signing Authority Certificate. If either signature is invalid, the package is deleted.

If the signatures are valid and the signed software package is a Signed Application/Library Software Package, the package is stored in Temporary Storage. If the Backup Flag is set in the Hardware Version File, a copy of the Signed Application / Library Software Package is also stored as the Backup Package, replacing the previous Backup Package.

If the signatures are valid and the Signed Software Package is a Signed Kernel or a Root Software Package, the system installs the Kernel Software Package or the Root File System Software Package or both, if either has a different file name than the currently installed version. The system replaces the existing corresponding files in the Kernel/Root File System that was not active during startup. A Root File System Software Package might also install new boot programs in the boot program area. The system then marks the Kernel or the Root File System as the one to be activated after the next power-up or reset. The system then sets the value of the persistent parameter RFSINUSE to the file name of the Signed Kernel/Root Software Package that was installed.

If a new Signed Kernel or Root Software Package was installed, the phone activates the new Kernel or Root File System that will install the new Signed Application or Library Software Package stored in Temporary Storage. If a new Signed Kernel or Root Software Package was not installed, the phone application registers with a call server.

Understanding the plug in and reset process

Plug the phone into the Ethernet wall jack. The phone receives power from the port and performs the following processes:

Note:

Do not unplug the phone during the download process. Wait for the download process to complete. If the application was downloaded earlier, the whole process takes approximately 1 to 2 minutes after the phone is plugged in. For software upgrades, including the boot file and application file download, the process might take 5 to 10 minutes. The duration depends on factors such as LAN loading and the number of phones being installed.

During hardware initialization, the system initialization values NVCONTRAST and NVBRIGHTNESS are checked for non-null values, and set accordingly. phones with bit-mapped display screens show the Avaya IP phone name and logo.

1. The system checks the system initialization value for the language file in use (NVLANGFILE) for a non-null value, in which case the text strings in that language file are used for text display. Otherwise, the display shows English text strings.
2. The boot programs check the Kernel or the Root File System that has previously been marked as the one to be activated to ensure that it has not become corrupted. If the Kernel or the Root File System is not corrupted, the system transfers control to a process in that file system. If that file system is corrupted, the boot program checks the other Kernel/Root File System. If that file system is not corrupted, the file system is marked as the one to be activated. The system then sets the value of RFSINUSE to the name of the Signed Kernel or Root Software Package that was used to install that file system, and the control is transferred to the Signed Kernel or Root Software Package. If both Kernel and Root File

Systems are corrupted, the system halts the processing. The software checks whether a Signed Application or Library Software Package has been previously downloaded. If the system finds the Application Software Package or the Library Software Package the Application Software Package or the Library Software Package is installed. If either the Application Software Package or the Library Software Package has a different file name than the currently installed version, the system replaces the existing corresponding files in the Application File System. The system then deletes the downloaded Signed Application or Library Software Package. If a new Signed Application or Library Software Package is not found, the integrity of the application files is checked. If the files are corrupted, the system installs the files from the Backup Package, replacing the corrupted files in the Application File System. Each time an Application Software Package or a Library Software Package is installed, the system sets the value of the persistent parameter APPINUSE to the file name of the Application Software Package that was installed. If the application files are not corrupted, or after the Backup Package has been installed, control is transferred to the application installed in the Application File System. While the system loads the application files into volatile memory and transfers control is transferred to the application files, the bottom text line shows the value of the APPINUSE parameter.

3. The system starts and sets the internal clock/calendar is set to 0:00:00 Saturday, January 1, 2000.
4. The phone activates the Ethernet line interface , the PC Ethernet jack, and dial pad input to allow the start of procedures. The activation occurs soon after power-up or a reset.

   The phone displays the speed of the Ethernet interface in Mbps, that is, 10, 100, or 1000. The phone then displays the message `No Ethernet * to program` until the software determines whether the interface is 10 Mbps, 100 Mbps, or 1000 Mbps.

   Note:

   The Ethernet speed is the LAN interface speed for both the phone and any attached computer, if the administrator has not disabled the latter interface by a PHY2STAT setting.

   Important:

   When you press the star (*) after the system displays a `* to program` message. The initialization process can support an interrupt that invokes the Craft Access entry procedure to allow manual settings, only if the local dialpad procedure status (PROCSTAT) system value is 0. The zero PROCSTAT value provides full access to local procedures. If PROCSTAT is *1* the Craft Access entry procedure can be invoked only when a `* to program` message displays, but only the VIEW procedure is available. For information, see Chapter 5: Using Local Administrative (Craft) Options. on page 33
5. The IP phone sends a request to the DHCP server and invokes the DHCP process.

   The phone displays one of the following messages:

   - DHCP: *s* secs * to program
   - `DHCP: s secs VLAN ID = n`

where *s* is the number of seconds that have elapsed after the DHCP process was started. The phone displays the first message if 802.1Q tagging is off and access to local programming procedures is not disabled or restricted. For more information, see Chapter 3: Using Local Administrative (Craft) Options . on page 33 The phone displays the second message if 802.1Q tagging is on and access to local programming procedures is disabled or restricted. If the first and second message alternate every 2 seconds, 802.1Q tagging is on. When the phone displays both messages alternately, access to local programming procedures is not disabled or restricted. Finally, the phone displays the third message if 802.1Q tagging is off and access to local programming procedures is disabled or restricted.

6. The system determines the DHCP protocol , IPv4 or IPv6 protocol, and the applicable parameters that are enabled.

   Important:

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

   Note:

   The IPV6STAT parameter overrides both the DHCPSTAT parameter setting and manual programming. If DHCPSTAT is set to enable DHVPv6, DHCPSTAT is disabled if IPV6STAT is 0 and disabled. Manual programming overrides DHCPSTAT, therefore even if DHCPSTAT is set to enable DHCPv4 or DHCPv6, the DoDHCPV4 or DoDHCPV6 will be set to 0 and disabled if an IP address of the corresponding type has been manually programmed.

   The DHCP server provides the IP addresses for the following hardware:

   - The phone
   - The HTTP/HTTPS server
   - The TN799C or D Control-LAN (C-LAN) circuit pack on the media server

7. Using the list of gateway IP addresses provided by the DHCP server, the phone performs a router check. The phone cycles through the gateway IP addresses with ARPs or pings until it receives a response. When the router is located, the router processes the received LLDP TLVs. Then the HTTP process starts.
8. While the IP phone connects to the HTTP server, the phone displays one of the following messages:

   `HTTP: n ipadd`

   or `HTTP: n ipadd * to program`

   or `HTTP: n ipaddProgram`

   where *n* is the number of the IP address obtained from the HTTP server and *ipadd* is the IP address.

Important:

Pressing star (*) at this time invokes the Craft Access entry procedure to allow manual settings. For information, see Chapter 3: Using Local Administrative (Craft) Options. on page 33

9. When connected, the phone looks for an upgrade script file.
10. The HTTP server sends and identifies an upgrade script.

    The phone might send the GET message several times. Each time the GET message is sent, all IP phones display the following message: `HTTP: n uri`

    For HTTP, *n* is the number of HTTP requests made by the phone and *uri* is the URI for the current HTTP request.

    Note:

    The SIG parameter value determines the signaling protocol whether H.323 or SIP, and is used to determine the proper upgrade file that is downloaded. If you set the SIG parameter manually using the local administrative Craft SIG procedure, that value takes precedence over a SIG setting in a configuration file. A change in the SIG value might require a reset to the phone so that a new or different upgrade file can be downloaded to the phone.

11. While the upgrade script file is being downloaded, all IP phones display the following message: `HTTP: n sc etag`

    where *n* is the number of the IP address obtained from the HTTP server, *sc* is the status code of the HTTP response, and *etag* is the value of the ETag header.

12. When the phone establishes the validity of the application file received, the phone displays the following message: `File Obtained; please wait..... s secs`

    where *s* is the number of seconds that elapse while non-volatile memory is erased.

13. While the application file is saved in flash memory, all IP phones display the following message: `Saving to flash 1% 1 secs`

    where the percentage of the file and the number of elapsed seconds increase as the application file is stored in flash memory.

14. The phone contacts the Avaya Communication Manager and displays a login screen that displays the following:

    `Login`, `Enter Extension`, or `Enter Extension and press Enter or OK`.

Steps to be performed by user after phone displays login and extension prompts:

1. Enter a new extension and press **OK**. To register the phone without the extension or password (unnamed), press only **OK** or make no entry and wait 60 seconds.

   Note:

   Unnamed registration is registering a phone with the call server without entry of an extension or password. You must set the UNNAMEDSTAT parameter to enable

unnamed registration. phones that are registered unnamed have limited functionality. For more information, see About unnamed registration on page 30.

All IP phones display the following:

```
Login

Enter Password

Enter Password and press Enter or OK
```

2. Enter the extension number and password and press **OK**. To register the phone without the extension or password (unnamed), press **OK** or make no entry and wait 60 seconds.

   To register the phone without the extension or password (unnamed), press **Log In** or make no entry and wait 60 seconds.

   You can see the extension as you enter the extension, but the password is displayed as stars (*). The system determines whether the extension is in use.

   When this process is complete, you can hear a dial tone when you press the **Speaker** button or lift the handset. The dial tone indicates that the IP phone was installed successfully.

   Note:

   Volume levels of the speaker, the headset, the ringer, and the handset are initialized to the default levels upon power-up and after a deskphone reset.

Understanding unnamed registration

In an IP phone, when you register with a call server, and receive limited service, without requiring an extension and password entry, this functionality is called as Unnamed registration. Unnamed registration is useful in the following environments:

- “Hot-desking” environments where a time gap exists between one user logging out and another user logging in on the same deskphone.
- Road warrior mode of use where a traveller can run the telephony features and functionality by taking over the office deskphone extension.

In both examples, the user unregisters the deskphone by logging off or by taking the office deskphone extension over to another deskphone. Without unnamed registration, the deskphone in the first example will wait for an extension and password entry and the deskphone in the second example will continue attempting to register at regular intervals. The disadvantage of a unregistered deskphone is that no one can use the deskphone, for example, to report a building emergency like a fire.

In Unnamed registration, the deskphone registers without an extension and password. Because there is no extension, telephony functionality is limited, specifically:

- The user has only one call appearance, and hence, cannot transfer or conference calls.

- The user has no administered feature buttons, and cannot invoke on-hook dialing.
- The user cannot reach extension-based information, such as the Contacts data of a given user or Option settings.
- The user is limited to the calling capability administered for PSA (Personal Station Access) on the call server, for example, access to an emergency number.
- The deskphone cannot receive any outside calls.

Unless otherwise disabled, the deskphone automatically attempts to register unnamed if no action is taken on the deskphone Extension entry screen within 60 seconds. To disable and prevent unnamed registration, enter an ID or password. The system ignores unnamed registration after any dialpad entry.

Administrators can disable unnamed registration by appropriately administering the system parameter UNNAMEDSTAT. For more information, see *Administering Avaya IP Deskphone H.323 9608, 9608G, 9611G, 9621G, and 9641G*. Unnamed registration appears to the end user like Communication Manager TTI Mode and is similar from an administration perspective. For more information about TTI, see your Communication Manager documentation.

Post-installation checklist

To ensure that the deskphone is properly installed, verify that the following requirements are complete.

Requirement	Reference	Status
Has the deskphone acquired an IP address?	See Deskphone initialization on page 24.	
Are able to make a call from the deskphone?	See *Using Avaya 9608/9608G/9611G IP Deskphones SIP*, *Using Avaya 9621G/9641G/ 9641GS IP Deskphones SIP*.	
Are you able to perform backup-restore?	See Deskphone initialization on page 24.	
Are you able to change deskphone settings?	See Accessing Craft procedures during normal operation on page 36.	
Are you able to upgrade your phone?	See BROKEN LINK: Downloading and saving the software	

Table continues…

Requirement	Reference	Status
For security considerations, have you configured the deskphone setup with TLS signaling? Have you installed the appropriate private network authentication certificates?	See *Administering Avaya 9601/9608/9608G/ 9611G/9621G/9641G/ 9641GS IP Deskphones SIP*	

Chapter 4: Using local Administrative Menu procedures

Related Links

About local Craft procedures

During or after you successfully install an IP phone, a system message might instruct you to administer one of the manual procedures described in this chapter. These local administrative procedures are also referred to as Craft procedures.

Local Administrative Options has two forms: One provides access to all the capabilities and functions described in this chapter.

The other provides access only to an administrable level of VPN capabilities and functions.

Using the VPN-specific option, the administrator can grant VPN users access to the VPN procedure itself, while preventing these users from gaining access to any other Local Administrative Procedure. The administrator may grant the VPN user permission to change VPN settings or only to view the settings. For more information about access to VPN-only Local Administrative Options, see the *VPN Setup Guide for 9600 Series IP Telephones, 16-602968*.

Caution:

Only trained installers or technicians should perform local administrative procedures. Perform these procedures only if instructed to do so by the system or LAN administrator. Static administration of these options causes upgrades to work differently with static administration of these options than by dynamic administration. Values assigned to options in static administration do not change with upgrade scripts. These values remain stored in the phone until one of the following happens:

- You download a new boot file
- You reset the IP phone. See Resetting system values on page 54.

Related Links

Using local Administrative Menu procedures on page 33

Accessing local Craft procedures

Note:

In addition to the procedures listed here, the administrator may allow access to only the VPN procedure, by setting the VPNCODE parameter in the settings file. For more information on access to VPN-only Local Administrative Options, see *VPN Setup Guide for 9600 Series IP Telephones, 16-602968*.

When you set PROCSTAT to 0, you have full access to local Craft procedures and you can invoke local craft procedures during initialization or whenever the deskphone displays this message:

```
* to program
```

You can also initiate the Craft procedure at any other time the initialization process can support a processing interrupt. If you set PROCSTAT to 1, the system allows access only to the VIEW craft

procedure for debugging purposes. You can invoke local Craft procedures only when the "`* to program`" message displays during initialization.

Note:

The system supports the `* to program` message is supported even if the value of PROCSTAT is 1, when the messages `Address conflict`, `Subnet conflict`, `Bad router?` and `Bad FileSv address` display. You can gain execute the Craft procedures in response to these messages as the situations requires corrective input.

Note:

The factory-set default Craft Access Code (PROCPSWD) is **27238**.

Related Links

Using local Administrative Menu procedures on page 33

Running Craft procedures

Procedure

1. Press ***** to display the Craft Access Code Entry screen during deskphone startup and start local procedures:

   ```
   Enter code:__
   # = OK
   ```

2. Enter the local dialpad procedure password that can be composed of any numeric digits fro zero to seven, as specified by the system administrator in the system value PROCPSWD.

   For security purposes, the deskphone displays a star (*) for each numeric dialpad press. If you are using a touch screen deskphone, and need to go back one space during password entry, use the **Contacts** button. You can use the left arrow button or the designated softkey for non-touch screen phones.

3. Press **#** when the password entry is complete.

   The entry is compared to the PROCPSWD value. If they match, the deskphone displays the Craft Local Procedure screen, and the message Select procedure and press Start.

4. For all non-touch screen phones, use the navigation arrows to scroll to and highlight the local procedure you want, then press **Start** or **OK**.

   You can also scroll to the procedure you want and press the corresponding line button. For touch screen phones, scroll to the local procedure you want if it not already displayed then touch the line on which the local procedure you want appears.

Related Links

Using local Administrative Menu procedures on page 33

Accessing Craft procedures during normal operation

Procedure

1. To run the local procedures, press the **Mute** button, enter the password using the designated digits from zero to seven, then press the pound (#) key.

   If you are using a touch screen phone and need to move one space back during password entry, use the Contacts button. In case of non-touch screen phones, use the left arrow button or the designated softkey.

   A six second time-out is in effect between button presses after you press the **Mute** button. If you do not press a valid button within 6 seconds of pressing the previous button, the phone discards the collected digits. In this case, no administrative option is run.

   *The system compares the entry to the PROCPSWD value. If the entries match, the deskphone displays the Craft Local Procedure screen, and prompts **Select** procedure and press **Start**.*

2. For non-touch screen phones, use the navigation arrows to scroll to and highlight the local procedure you want, then press **Start** or **OK**.

   You can also scroll to the procedure you want, then press the corresponding line button. For touch screen phones, scroll to the local procedure you want if it not already displayed then touch the line on which the phone displays the local procedure that you want to select.

   Note:

   As of Release 6.3, you can also enter the craft menu when the deskphone is in off-hook idle state and the user has logged out.

Related Links

Using local Administrative Menu procedures on page 33

Entering data for administrative options

About this task

This section applies to all 9600 Series IP deskphones and describes how to enter data for administrative options.

Procedure

1. With the exception of a touch screen deskphone, the first application line on any screen is automatically highlighted selected when the phone displays the screen.

   To select an item, press the appropriate softkey at the bottom of the screen, for example, **Change** or **Save**, or **OK** . To select a different line, use the down or up navigation arrows to change the line focus. When the desired line is highlighted, then press a softkey or **OK** to select that line. For a touch screen deskphone, touching the desired line produces the same result.

Note:

The deskphone emits an error beep if you attempt to enter invalid data.

2. If you enter a numeric digit that exceeds the maximum field value of the IP Address or subnet mask value, that is exceeds 255, the phone emits an error beep tone. The system ignores the digit, and the cursor does not move forward.
3. If you enter a zero followed by a numeric digit for a value, an IP Address, or a subnet mask field, the new digit replaces the zero.

   If you press star (*) and enter an IPv4 address, the system inserts a decimal point into the input buffer and moves the cursor to the next character location. If the star (*) button is pressed and the user is entering an IPv6 address, the system inserts a colon into the input buffer and the cursor is moved to the next character location.

   For more information on IPv4 and IPv6 format, see Entering and validating IPv4 and IPv6 addresses on page 38
4. To go back one space on non-touch screen phones, press the leftmost softkey. In case of a touch screen deskphone, use the **Bksp** softkey instead.

   When you press the applicable button or key to backspace, the most recently entered digit or period is erased from the display. The cursor remains in the erased character's former position.
5. Press **Exit** or tap the softkey for a touch screen deskphone to exit the local procedures.

   Important:

   If any changes were made using the 802.1X procedure or the ADDR procedure, if the value of SIG was changed to SIP or if the Crafts Entry screen was invoked during startup, the deskphone immediately resets when you press or touch **Exit**. If no 802.1X, SIG, or ADDR changes were made, or if the local procedures were invoked post-startup, the deskphone redisplays the screen or other display that was effective when the craft options was invoked.

   Note:

   If PROCSTAT has been administered to 1, you will not be able to invoke any administrative options other than VIEW.

   Note:

   Some touch screen deskphones present an onscreen keyboard with which you can *type* the data that you want to enter on the display. See the applicable user guide for information about using the onscreen keyboard.

Related Links

Using local Administrative Menu procedures on page 33

Entering and validating IPv4 and IPv6 addresses

The dial pad uses numeric-only entry when an IPv4 address or the subnet mask is entered. On a touch screen use a single tap. Use an asterisk to place a period within the address being entered.

When you press star (*) on the dial pad with the cursor in one of the three fields towards the left of the display, the following happens:

- The field where you are trying to enter a value displays a zero if no value is entered.
- If you enter a valid value a period displays. The space after the field displays a period.
- The cursor moves to the next space.

When you press star (*) with the cursor in one of the three fields to the right side of the display, the system beeps to inidicate an error and the cursor remains in the field to the right. Pressing the “*” button while the cursor is in the last (right most) field results in an error beep and the cursor being left where it is. If you enter all three dots that separate the fields and if the value of each field is valid, the IPv4 address or subnet mask is complete.

The value of a given field might be invalid when you:

- Enter a digit that makes the value of the first field of an IPv4 address exceed 223.
- Enter a digit that makes the value of the last three fields of an IPv4 address exceed 255.
- Enter a digit that makes the value of any field of a subnet mask exceed 255.

Enter an IPv6 address using only numbers on the dial pad. Use single tap for touch screen telephones, except for *2* and *3* which are alphanumeric multitap fields. When you press *2* the deskphone initially enters a 2, followed by A, B, C, and back to 2. When you press *3* the deskphone initially enters a *3*, followed by D, E, and back to *3*. While the cursor is in any of the leftmost seven fields, when you press the star (*) button makes the value for the field being entered to be terminated (a zero is displayed if nothing else is), a colon to be displayed in the space after the field, and the cursor to move to the next space. Pressing “*” while the cursor is in the last (right most) field results in an error beep and the cursor being left where it is. An IPv6 address is considered to be complete only if all the following conditions are met:

- All seven colons that separate the fields are entered OR the text input field contains at most one pair of consecutive colons
- If one pair of consecutive colons is present, the final field is not “1” or “01”.
- If one pair of consecutive colons is present, the address format is not “::FFFF:hhhh;hhhh”.
- The value of each field is valid. The following actions cause the value of a given field to be considered invalid:
  - Entering a digit that would cause the value of the first field of an IPv6 address to exceed FD.
  - Entering a third consecutive colon.
  - Entering a second pair of consecutive colons.

In a given text entry field, if the either an IPv4 or an IPv6 address can be specified, the initial field can be ambiguous with respect to whether the entry is an IPv4 or IPV6 address, for example, *123* might be an IPv4 *123 decimal* or an IPv6 *0123 hex*. In such cases, text entry follows the IPv6 rules

that hexadecimal characters are allowed and the "*" key inserts a colon character. If the entry is a hex character (A-F) or a fourth character is entered in the field, the telephone accepts the input is IPv6 format. Otherwise, the telephone makes the initial validity check when you enter a field boundary, a colon or decimal point. This initial typographic character determines whether the overall address must be in IPv4 format with a decimal point or in IPv6 format with a colon. Once this character is entered, the telephone examines the contents of the first field to ensure consistency with the field boundary. That is the absence of hex characters, and at most three characters of value 255 or less, in the first field if the field boundary is a decimal point. If the first field contains any content inappropriate for the entered field boundary, an error beep is generated. You cannot enter more content until the contradiction in the text string is deleted, meaning either the field boundary is deleted or the cursor is moved back and the field contents edited). After you enter content that identifies the format of the IP address appropriate to IPv4 or IPv6, the rest of the address entry conforms to that format.

Related Links

Using local Administrative Menu procedures on page 33

Local administrative Craft procedures menu

Using the administrative procedures, you can customize the IP deskphone installation for your specific operating environment. This section provides a description of each local administrative option covered in this guide, with references to the pages on which the option appears.

Note:

For touch screen-based deskphones, simply touching a line or a softkey produces the same result as selecting a line or a softkey on non-touchscreen or button-based IP deskphones. Depending upon the privileges assigned to the user by administrator, an end user can view but cannot change most of the parameters associated with Craft procedures. For more information, see the applicable user guides.

Administrative Procedure value (in English)	Purpose	See
8021X	Set 802.1X operational mode	Setting the Operational Mode to 802.1X on page 41.
ADDR	Address information programming	Using the pre-installation checklist on page 42.
AGC	Enable/disable Automatic Gain Control	Disabling/enabling automatic gain control on page 45.
CALIBRATE SCREEN	Calibrate the touch screen	Calibrating the Touch Screen on page 44.
CLEAR	Clear all values to factory defaults	Clearing the deskphone settings on page 46.

Table continues…

Administrative Procedure value (in English)	Purpose	See
CONT	Adjust the contrast of any Button Modules and any non-color deskphones	Adjusting contrast on button modules and non-color deskphones on page 48.
DEBUG	Enable/disable Debug Mode	Disabling/enabling debug mode on page 48.
GROUP	Set the Group Identifier	Changing the group identifier on page 50.
HSEQUAL	Handset audio equalization	Setting handset audio equalization on page 50
INT	Interface Control	Changing Ethernet interface control on page 51.
LOG	Enable/disable Event Logging	Disabling/enabling event logging on page 52.
LOGOUT	Log off the deskphone	Loging off The deskphone on page 53.
MLS	View Multi-Language text Strings	Viewing multi-language strings on page 54.
RESET VALUES	Reset system initialization values to defaults	Resetting system values on page 54.
RESTART PHONE	Restart the deskphone	Restarting The deskphone on page 55.
SIG	Set the signaling protocol download flag	Changing the signaling protocol on page 56.
SSON	Set the Site-Specific Option Number	Changing SSON settings on page 57.
TEST	Initiate a self-test	Performing a self-test on page 57.
VIEW	View current parameter values and file names	Using The VIEW craft procedure for troubleshooting on page 68.
VPN	Administer and view Virtual Private Network (VPN) settings	*VPN Setup Guide for 9600 Series IP Telephones, 16-602968.*

Note:

1. A 9608 and 9608G deskphone always lists the CONT procedure. Other color deskphones list the CONT only if the deskphone has at least one button module attached.
2. If the deskphone software has VPN and media encryption disabled, VPN will not appear on the Craft procedures menu list. To determine if this applies to the deskphone, go to the About Avaya IP Deskphone screen through the Avaya (A) Menu or Home screen as applicable to the phone, and select the Settings list. The *About Avaya IP Deskphone* screen with a *U* appended to the software release indicates the phone has VPN and media encryption disabled.

Related Links

Using local Administrative Menu procedures on page 33

Setting the operational mode to 802.1X

About this task

Use the following procedure to set or change the operational mode.

Note:

When updating local Craft procedures from a touch screen deskphone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP deskphone.

Procedure

1. When you select 802.1X from the **Craft Procedures** screen, the deskphone displays the following:

   ```
   Supplicant:
   Pass-thru:
   ```

   where the Supplicant line is the text string associated with the current system value of DOTIXSTAT. The DOTIXSTAT parameter configures the 802.1X Supplicant Mode operation control, defined as:

   The options that are displayed depend on the following parameters as set in the settings file:

   - *Disabled* if DOT1XSTAT = 0
   - *Unicast-only* if DOT1XSTAT = 1
   - Unicast/multicast if DOT1XSTAT = 2

     and the Pass-thru line is a text string associated with the current system value of DOT1X where:

   - *Enabled mode* if DOT1X = 0
   - *Enabled w/Logoff* if DOT1X = 1
   - *Disabled* if DOT1X = 2

2. Select the line you want to change.

   Depending on which line you selected to change, the phone displays the following text:

   ```
   Current setting:
   New Setting:
   ```

3. To change the setting, press the Right or Left navigation arrow to navigate through the applicable settings .

   Depending on the current value, the deskphone selects the next sequential text string displays it as the New setting. For example when you change the Pass-thru mode, if the current value is Pass-thru mode, pressing the Choice Selector causes the deskphone to display P-t w/Logoff. If the current setting is disabled, pressing the Choice Selector changes the new setting to Pass-thru mode.

4. Press **Save** to store the new setting and redisplay the **Craft Procedures** screen.

Related Links

Using local Administrative Menu procedures on page 33

Using the preinstallation checklist

Before performing static programming of address information, verify that the call system meets all the requirements listed in the *Requirements to verify for your network* section of the Creating the pre-installation checklist on page 14. You can skip item 4., as it refers to the DHCP server. In addition, you must have the values for the following parameters. To prevent data entry errors that have a negative impact on your network, obtain and print copies of the following parameters for each subnet:

- The IP Address of the call server.
- The IP Address of the gateway or the router.
- The IP netmask.
- The IP Address of the HTTP server.

Related Links

Using local Administrative Menu procedures on page 33

Changing IP address information

About this task

Use this procedure to assign a static IP address to the deskphone.

Caution:

Static addressing is necessary when a DHCP server is unavailable. But static addressing has room for text entry errors. So Avaya recommends that you install a DHCP server and do not use static addressing.

Important:

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

Note:

When updating Local Craft procedures from a touch screen phone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP phone.

Use the following procedure to invoke manual address information programming.

Procedure

1. Select ADDR from the Craft Procedures screen. The next screen displays the following fields with the prompt `Select address to change.`

Static addressing field	Field value	Description
Phone (IPv4)	nnn.nnn.nnn.nnn	phone IP address (IPADD)
Phone (IPv6)	hhhh:hhhh::hhhh:hhhh:hhhh	phone IP address (NVIPADDV6)
Call Server	nnn.nnn.nnn.nnn hhhh:hhhh::hhhh:hhhh:hhhh	Call Server in use; media server IP address
Router (IPv4)	nnn.nnn.nnn.nnn	Router in use; gateway/router IP address
Mask (IPv4)	nnn.nnn.nnn.nnn	IP network mask (NETMASK)
HTTP Server	nnn.nnn.nnn.nnn hhhh:hhhh::hhhh:hhhh:hhhh	IP address of HTTP File Server in use
HTTPS Server	nnn.nnn.nnn.nnn hhhh:hhhh::hhhh:hhhh:hhhh	IP address of HTTPS (TLS) File Server in use
802.1Q	L2Q text string	L2Q setting text description
VLAN ID	dddd	NVL2QVLAN
VLAN Test	ddd	VLANTEST

   where:

   - *nnn.nnn.nnn.nnn* is the current IP address in IPv4 format associated with the specific address information on the left side, which could be either a value previously set by a technician, or the original value of NVIPADD if no previous change was made.
   - *hhhh:hhhh:hhhh:hhhh:hhhh* is the current IP address in IPv6 format associated with the specific address information on the left side, which could be either a value previously set by a technician, or the original value of NVIPADD if no previous change was made.
   - *L2Q text string* is the text string associated with the current system value of L2Q where *Auto* = an L2Q value of *0*, *On* = an L2Q value of *1*, and Off = an L2Q value of *2*.
   - *dddd* is the current value of NVL2QVLAN and *ddd* is the current value of VLANTEST, respectively.

2. Use the navigation arrows to scroll to and highlight the address you want to change, then press **Change** to display the change screen for that specific address value.
3. Select one of the following as appropriate to the item you selected:

Task	Steps
To change any of the IP address values such as	Use the dial pad to enter the new IP address. IP addresses have three sets of three digits followed by a period. Pressing star (*) following entry of three digits causes a period to be placed in the next

Table continues…

Phone, Call Server, Router, Mask, and File Server	position, and the cursor to advance one position to the right. If you press the star (*) and enter an IPv6 address, a colon is inserted into the input buffer and the cursor is moved to the next character location. The exceptions are entry of a Router or Mask address, which follows the IPv4 method of inserting a period rather than a colon. For information on entry and validation of addresses in either format, see Entering and validating IPv4 and IPv6 addresses on page 38. For example, to enter the IP address 111.222.333.444 in IPv4 format, press the number 1 on the dial pad three times then press *, press the number 2 on the dial pad three times then press *, press the 3 on the dial pad three times then press *, then press the 4 on the dial pad three times. To enter an IP address in IPv6 format, use the dial pad in numeric-only mode entry. Tap the desired dial pad key once for touch screen phones, except for *2* and *3* which are alphanumeric. Use multi-tap for touch screen phones. For example, pressing button *2* initially enters a *2*, followed by *A*, *B*, *C*, and back to *2*. Pressing button *3* initially enters a *3*, followed by *D*, *E*, *F*, and back to *3*. Proceed to the next step.
To change the 802.1Q value	Use the Right navigation arrow to navigate through the text strings corresponding to the L2Q values defined as *Auto* if L2Q=0, *On* if L2Q=1, and *Off* if L2Q= 2 until the text string of the value you want to change to displays. Proceed to the next step.
To change the VLAN ID value	Use the dial pad to enter the new static VLAN ID of from 0 to 4094, inclusive. Proceed to the next step.
To change the VLANTEST value	Use the dial pad to enter the new value of the DHCPOFFER wait period of from 0 to 999. Proceed to the next step.

4. Press **Save** to store the new setting and redisplay the Craft Procedures screen or **Cancel** to return to theCraft Procedures screen without saving the value entered.

   Once the new values are stored, the phone resets automatically.

Related Links

Using local Administrative Menu procedures on page 33

Calibrating the touch screen

About this task

Use screen calibration for proper alignment of the touch screen of 9621G and 9641G deskphones. You cannot use screen calibration on 9641GS deskphones.

Important:

Use a stylus instead of your finger to touch the calibration points precisely.

Note:

The CLEAR Craft procedure clears any calibration data set using the CALIBRATE SCREEN Craft procedure, but does not change factory settings of calibration data. Use the **Default** softkey to restore factory-set calibration. You cannot save calibration results as part of a backup operation.

Procedure

1. When you select CALIBRATE SCREEN from the Craft Local Procedure Screen, the telephone displays three softkeys - **Start**, **Default**, and **Cancel**.
2. Perform one of the following actions:
   - Touch **Cancel** to return to the Craft Local Procedure screen without calibrating the screen.
   - Touch **Default** to reset the calibration parameters to the factory-set values. The system plays a confirmation tone and displays the Craft Local Procedure screen.
   - Touch **Start** to calibrate the screen. The screen displays a calibration target with a plus sign (+) at a particular point. Proceed to the next step.
3. Touch the center of the target with the stylus as soon as the target appears.

   The target disappears, and a new target appears in a different part of the screen.
4. Touch the center of each target with the stylus within 10 seconds of its appearance.

   After you touch all four targets, the system plays a confirmation tone sounds displays a *Calibration successful* message.
5. Touch **Save** to return to the Craft Local Procedure screen. The system stores the calibration results in the nonvolatile memory of the telephone.
6. Touch **Cancel** at any time to return to the Craft Local Procedure screen without completing the touch screen calibration.

Related Links

Using local Administrative Menu procedures on page 33

Disabling or enabling automatic gain control

About this task

Use the following procedure to turn automatic gain control for the handset, headset, or the Speaker to on or off.

Note:

When updating local Craft procedures from a touch screen deskphone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP deskphone.

Note:

The user can potentially override the AGC local procedure settings. For more information, see *Avaya 9600 IP Deskphone H.323 9608, 9608G, and 9611 User Guide* and the *Avaya 9600 Series IP Deskphone H.323 9621 and 9641 User Guide*. If the values are changed, the backup file stores the AGC values set by the user and does not save any setting established using this local procedure.

Procedure

1. When you select AGC from the Craft Local Procedure Screen, the phone displays the options in the following table. Select the appropriate line and press **Change** to toggle it to On or Off as required.

Options available under AGC	
Handset Automatic Gain control	On
Headset Auto Gain Control	On
Speaker Auto Gain Control	On

   where the *setting* is the text string associated with the current system value of NVAGCHAND, NVAGCHEAD, or NVAGCSPKR, defined as:

   - *On* if the respective NVAGC*XXXX* system value is *1*.
   - *Off* if the respective NVAGC*XXXX* system value is *0*.

2. Press **Save** to store the new setting, update the associated system value, and redisplay the Craft Local Procedure screen.

Related Links

Using local Administrative Menu procedures on page 33

Clearing the deskphone settings

About this task

Sometimes, you might want to remove *all* administered values, user-specified data, and option settings and return a phone to its factory settings. You might have to remove all administered values when you give a phone to a new, dedicated user and when the **LOGOFF** option is not sufficient. For example, a new user is assigned the same extension, but requires different permissions than the previous user.

The **CLEAR** option erases all administered data—static programming, HTTP and HTTPS server programming, and user settings including Contact button labels and locally programmed Feature button labels, and restores all such data to default values. Using the **CLEAR** option does not affect:

- The software load. If you upgrade the phone, the phone retains the latest software. After you clear a phone of the settings, you can administer the phone normally.
- The user configuration stored in backup/restore file server.

Caution:

This procedure erases all administered data without any possibility of recovering the data. Neither the boot code nor the application code is affected by this procedure.

Note:

When updating Craft procedures from a touch screen phone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP phone.

Use the following procedure to clear the phone of the administrative, user-assigned, and options values.

Procedure

1. Select **CLEAR** from the **Admin Procedures** menu. The phone displays the `Press Clear again to confirm.` message.
2. Tap Press **Clear** to clear all values to use initial default values.

   Tap Press **Cancel**. If you do not want to clear all values and to terminate the procedure and retain the current values.

   The phone displays the following text:

   ```
   Clearing values...
   ```

   The phone is reset to the default factory settings.

   - All system values and system initialization values.
   - 802.1X identity and password.
   - User options, parameter settings, identifiers, and password.
   - Any user data like Contact Lists or Call Logs are deleted.

   After clearing the values, the phone resets.

Related Links

Using local Administrative Menu procedures on page 33

Adjusting contrast on button modules and non-color deskphones

About this task

Note:

When updating local or Craft procedures from a touch screen deskphone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP deskphone.

bar

Use the following procedure to adjust the contrast of any button module when attached to any 9600 Series IP deskphone or any non-color IP deskphone. The 9611G, 9621G, 9641G and 9641GS each have a color display, and contrast adjustment is not applicable. Fifteen contrast levels are available.

Procedure

1. When you select CONT from the Craft Local Procedure Screen, the deskphone prompts you to use the Right and Left navigation arrows to change the contrast for button module shown as Module: 1 or the contrast for the deskphone shown as Phone: contrast.
2. To change the setting, press the Right or Left navigation arrow to navigate through the settings.

   By default, the contrast button is set to the middle of the contrast setting.

   As you press the navigation arrow, the next higher or lower contrast level is selected and displayed as the setting.
3. If more than one button module is attached, scroll down to that line, for example, to Module: 2 and repeat Step 2 to change the contrast.
4. Press **Save** to store the new contrast settings and redisplay the Craft Local Procedure screen.

Related Links

Using local Administrative Menu procedures on page 33

Debug mode

About this task

You can use the debug mode to send all your debug data in a file, nnn_report.gz where you replace nnn by the deskphone extension as specified by the user during registration.

Note:

The DEBUG option is available for use only if you change the default password to the craft menu through the PROCPSWD parameter. If you do not change the default password, the option is available only in a read-only mode.

The new value of the PROCPSWD parameter must be 4 to 7 numeric digits, "0000" through "9999999". However if value of PROCPSWD is less than 4 digits after you install Release 6.2.4 or later, the value will be changed back to the default value of 27238.

Procedure

1. Scroll and select DEBUG from the Craft Local Procedure Screen. Press **Start**. The deskphone displays, the following text:

Setting	Options available
Serial Port	Adjunct/CLI
Log to file	On/Off
Phone Report	Press **Change** when you select the Phone Report option results in a **Create** option displayed on the phone screen. Press **Create** to send the report to the backup folder specified by BRURI. **Note:** The **Phone Report** option is available only if backup and restore is enabled.
Port Mirroring	On/Off
Profile	H.323 signaling over TLS
Service	Service mode control/Service mode record
SSH Status	**Enabled/Disabled** **Note:** The SSH Status option displays an **Active** status if an SSH connection is already established.

2. Scroll to the option that you want to change and press **Change** or touch **OK** to toggle the selected setting from the available options. The deskphone displays the softkeys **Save**, **Change**, and **Cancel**.
3. If you have made any changes to the Debug Mode option, then you must press or touch the **Save** option. This action resets the phone and saves the changes to the debug screen.

Note:

When SSH is manually enabled, the SSH port will only be opened for one SSH connection. When that connection is terminated, the port will be closed, and it must be reopened (SSH must be re-enabled) from the Craft Debug procedure if another connection is to be established.

Related Links

Using local Administrative Menu procedures on page 33

Changing the group identifier

About this task

Note:

When updating Craft procedures from a touch screen deskphone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP deskphone.

Use the following procedure to set or change the group identifier.

Note:

Perform this procedure only if the LAN Administrator instructs you to do so. For more information about groups, see Applying settings to logical groups on page 66.

Procedure

1. When you select GROUP from the Craft Procedures screen, the following text displays:

```
Current Setting:
New Setting:
```

   where the *setting* is the current system value of NVGROUP.

2. In the **Group** text box, enter a valid **Group** value from 0 to 999.
3. Press **Save** to store the new setting. The deskphone displays the Craft Procedures screen.

Related Links

Using local Administrative Menu procedures on page 33

Setting handset audio equalization

About this task

Note:

Use the following procedure to set or change the handset audio equalization value.

Procedure

1. When you select HSEQUAL from the Craft Procedures screen, the following displays:
   - Current Setting:
   - New Setting:

   Where the Current Setting is the current value of HSEQUALIZATION, an internal parameter that combines the audio equalization specifications of the settings file, user option, and Local Procedure.

The values are *Default* TIA-810/920 and S004 is used, *Audio Opt* TIA-810/920 and S004 is used, or *HAC Opt* HAC is used. The only difference between *Default* and *Audio Opt* is that in the second case, either the settings file, the user option, or the Local Procedure has explicitly selected TIA-810/920 and S004.

2. Press **Save** to store the new setting and redisplay the Craft Procedures screen.

Related Links

Using local Administrative Menu procedures on page 33

Changing Ethernet interface control

About this task

Note:

When updating Craft Procedures from a touch screen phone, tapping the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP phone.

Use the following procedure to set or change the interface control value.

Procedure

1. When you select INT from the Craft Procedures screen, the phone displays the following options with a prompt to use the Right and Left navigation arrows to select a setting:

Ethernet	Choice Selector
PC Ethernet	Choice Selector

The options that are displayed are the text strings associated with the current PHY1STAT on the Ethernet line and the current PHY2STAT system value on the PC Ethernet line.

- **Auto** when PHY1STAT = 1
- **10 Mbps half** when PHY1STAT = 2
- **10 Mbps full** when PHY1STAT = 3
- **100 Mbps half** when PHY1STAT = 4
- **100 Mbps full** when PHY1STAT = 5
- **1000 Mbps full** when PHY1STAT = 6

The PHY2STAT text strings are:

- **Disabled** when PHY2STAT = 0
- **Auto** when PHY2STAT = 1
- **10 Mbps half** when PHY1STAT = 2
- **10 Mbps full** when PHY1STAT = 3

- **100 Mbps half** when PHY1STAT = 4
- **100 Mbps full** when PHY1STAT = 5
- **1000 Mbps full** when PHY1STAT = 6

2. To change the Ethernet setting, press the Right navigation arrow to navigate through the possible settings.

   Depending on the current value, the next sequential text string is selected and displayed as the setting. For example, if the current value is 10 Mbps half (2) and if you press the Right navigation arrow, the value changes to 10 Mbps full (3). If the current value is 1000 Mbps full (6) and if you press the navigation arrow, the value changes to Auto (1).

3. To change the PC Ethernet setting, select that line and press the Right navigation arrow to navigate through the possible settings.
4. Press **Save** to store the new settings and redisplay theCraft Procedures screen.

Related Links

Using local Administrative Menu procedures on page 33

Disabling and enabling event logging

About this task

Note:

When updating local Craft procedures from a touch screen deskphone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP deskphone.

Use the following procedure to enable or disable logging of system events.

Procedure

1. When you select *LOG* from the Craft Local Procedure Screen, the deskphone prompts you to use the Right and Left navigation arrows to select a setting and displays the following text:

Log: *text string*	Choice Selector

   where the *text string* is the wording associated with the current system value of NVLOGSTAT, defined as:

   - **Disabled** when NVLOGSTAT = 0
   - **Emergencies** when NVLOGSTAT = 1
   - **Alerts** when NVLOGSTAT = 2
   - **Critical** when NVLOGSTAT = 3
   - **Errors** when NVLOGSTAT = 4
   - **Warnings** when NVLOGSTAT = 5

- **Notices** when NVLOGSTAT = 6
- **Information** when NVLOGSTAT = 7
- **Debug** when NVLOGSTAT = 8

2. To change the setting, press the Right or Left navigation arrow to navigate through the settings.

   Depending on the current value, the next sequential text string is selected and displayed as the setting. For example, if the current value is Alerts (2), pressing the Right navigation arrow changes the value to Critical (3). If the current value is Debug (8), pressing the Right navigation arrow changes the value to Disabled (0).

3. Press **Save** to store the new setting and redisplay the Craft Local Procedure screen.

Related Links

Using local Administrative Menu procedures on page 33

Logging off from the phone

About this task

Use the following procedure to log off from a phone.

Note:

If a user registered has logged in through a USB device, the following procedure is not applicable. The only way to log off a phone registered with a USB device is by removing the device.

Note:

When updating lLocal Craft Procedures from a touch screen phone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP phone.

Caution:

Once you are logged off from a phone, you might need a password and extension to log back in.

Procedure

1. When you select **LOGOUT** from the Local Craft Procedures screen, the phone displays the following text:

   ```
   Press Log Out again to confirm.
   ```

2. Press or tap **Log Out** to log off from the phone.

   Press or tap **Cancel** to return to the Local Craft Procedures screen without logging off the phone.

Related Links

Using local Administrative Menu procedures on page 33

Viewing multilanguage strings

About this task

Note:

When updating local Craft procedures from a touch screen deskphone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP deskphone.

Use this procedure to view the language strings available on the deskphone. A language string is any set of words or phrases on the IP deskphone user interface in the currently active language.

Procedure

1. Select MLS from the Craft Procedures screen. The deskphone displays the following text:

   ```
   Tag # N

   Text string for tag # N        text string
   ```

   where *N* is the label associated with a specific language in the downloaded language file and *text string* is the wording associated with that Tag number.

2. Use the Up and Down navigation arrows to scroll through the list of text strings.

   Use the Right and Left navigation arrows to scroll right or left one character at a time to view the entire text string, if it exceeds the available display line space.

3. Press **Back** to return to the Craft Procedures screen.

Related Links

Using local Administrative Menu procedures on page 33

Resetting system values

About this task

Note:

When updating Craft procedures from a touch screen deskphone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP deskphone.

Use the following procedure to reset all system initialization values to the application software default values.

Caution:

This procedure erases all static information, without any possibility of recovering the data.

Procedure

1. Select RESET VALUES from the Craft Procedures screen. The deskphone displays the following text:

   ```
   Press Reset to confirm.
   ```

2. Press **Cancel** to return to the Craft Procedures screen without resetting the deskphone.

   Press **Reset** to start the deskphone reset.

   The deskphone resets from the beginning of registration, which might take a few minutes. The deskphone resets:

   - All system values and system initialization values except AUTH and NVAUTH to default values.
   - The 802.1X ID and Password to their default values.
   - Call server values to their defaults.
   - Any entries in the Redial buffer.
   - Do not affect user-specified data and settings like Contacts data or the deskphone login and password. To remove this type of data, see Clearing the deskphone settings on page 46.

Related Links

Using local Administrative Menu procedures on page 33

Restarting the phone

About this task

Note:

When updating local Craft Administration Menu procedures from a touch screen phone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP phone.

Use the following procedure to restart the phone.

Procedure

1. Select **RESTART PHONE** from the Craft Procedures screen. The phone displays the following text:

   ```
   Press Restart to confirm.
   ```

2. Press**Cancel** to return to the Craft Procedures screen without restarting the phone.

Press **Restart** to proceed with the registration steps. For more information, see Powering-up and resetting the phone (Dynamic Addressing Process) on page 24.

A restart does not affect user-specified data and settings like Contacts data or the phone login and password.

The completion of the restart procedure depends on the status of the boot and application files.

Related Links

Using local Administrative Menu procedures on page 33

Setting or changing the signaling protocol

About this task

Note:

When updating local Craft procedures from a touch screen deskphone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP deskphone.

Use the following procedure to set or change the Signaling Protocol Identifier. A valid SIG Protocol Identifier is either 0 (default), 1 (H.323), or 2 (SIP).

Note:

Perform this procedure only if the LAN Administrator instructs you to do so.

Procedure

1. Select SIG from the Craft Local Procedures screen. The deskphone prompts you to use the Right and Left navigation arrows to select a setting and displays the following text:

   ```
   Sig: text string                Choice Selector
   ```

   where the *text string* is the wording associated with the current system value of NVSIG, defined as:

   - **Default** when NVSIG = 0
   - **H.323** when NVSIG = 1
   - **SIP** when NVSIG = 2

2. Press the Right or Left navigation arrow to navigate through the settings to change the setting.

   Depending on the current value, the next sequential text string is selected and displayed as the setting. For example, if the current value is SIP (2), pressing the Right arrow changes the value to 0 (default). If the current value is H.323 (1), pressing the Right arrow changes the value to 2 (SIP).

3. Press **Save** to store the new setting and redisplay the Craft Procedures screen.

The remainder of this procedure depends on the status of the boot and application files.

Related Links

Using local Administrative Menu procedures on page 33

Changing SSON settings

About this task

Caution:

Do not perform this procedure if you are using static addressing. Perform this procedure only if you are using DHCP and the LAN administrator instructs you to do this.

Note:

When updating Craft Procedures from a touch screen phone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP phone.

Use the following procedure to set the Site-Specific Option Number (SSON).

Procedure

1. Select SSON from the Craft Procedures screen.

   The phone displays the following text:

   ```
   Current setting:
   New Setting:
   ```

   where the *setting* is the current system value of NVSSON.

2. To change the setting, use the dial pad to enter a valid SSON value between 128 and 255.
3. Press**Save** to store the new setting and redisplay the Craft Procedures screen.

Related Links

Using local Administrative Menu procedures on page 33

Performing a self-test

About this task

Note:

9600 series IP deskphone stores two software code images in reprogrammable non-volatile memory. The primary image, called the “big app” must be running to perform a self-test. The backup image, called the “little app” does not support the self-test.

Note:

When updating localCraft Procedures from a touch screen deskphone, touching the line you want to change or the applicable softkey produces the same result as selecting a line and pressing the applicable softkey on a non-touch screen IP deskphone.

Use the following procedure to perform self-testing:

Procedure

1. Tap or select **TEST** from the Craft Procedures screen. The phone displays the following text:

   ```
   Press Test to confirm.
   ```

2. Tap or press **Test** to start phone testing.

   Tap or press **Cancel** to return to the Craft Procedures screen without testing the phone.

   The test performs the following actions:

   - Removes labels on all softkeys .
   - Illuminates groups of LEDs at a time on the phone and any attached button modules sequentially for about a half second. Illumination starts with the upper half of the phone and continues through the lower half of any attached button module in a repeating cycle.
   - Shows pixels on the display with highest intensity.

   After approximately 5 seconds, the top phone screen displays either *Self-test passed* or *Self-test failed*.

3. Press or tap **Back** to return to the Craft Procedures screen.

Related Links

Using local Administrative Menu procedures on page 33

Chapter 5: Maintaining 9600 Series IP Deskphones

Related Links

[About software distribution packages](#) on page 59
[Downloading software packages](#) on page 60
[Contents of the settings file](#) on page 61
[Downloading text language files](#) on page 65
[Changing the signaling protocol](#) on page 65
[Applying settings to logical groups](#) on page 66

About software distribution packages

Software distribution packages contain the files that are required for 9600 Series IP Deskphones. These files are packaged together either in a Zip format or an RPM/Tar format. Download the appropriate package from the Avaya support site.

The software distribution packages contain the following:

- Software files.
- One upgrade file such as 96x1Hupgrade.txt.
- All the display text language files. For example, mlf_SB189_v78_korean.txt
- A file named *av_prca_pem_2033.txt* that contains a copy of the Avaya Product Root Certificate Authority certificate in PEM format. You can downloaded this file to the phones based on the value of the TRUSTCERTS parameter.
- Updated MIB file.
- A file named *release.xml* that is used by the Avaya Software Update Manager application.

Software distribution packages in Zip format also contain a signatures directory containing signature files and a certificate file that the Avaya file server application will use on the Utility server. Customers using their own HTTP server can ignore or delete this directory.

Note:

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

Note:

Settings files are not included in the software distribution packages because the files overwrite the existing file and settings.

Two configuration files are:

- The upgrade file, that notifies the phone to upgrade software. The phone attempts to read this file after a reset. The upgrade file also contains directions to the settings file.
- The settings file contains the option settings that enable, disable, or otherwise customize the settings you might need to tailor the Avaya IP phones for your enterprise.

  Note:

  You can use one settings file for all your Avaya IP deskphones..

Related Links

Maintaining 9600 Series IP Deskphones on page 59

Downloading software packages

You can use the upgrade file and the application files included in the Software Distribution Package that Avaya provides to upgrade the phones. Do not modify the upgrade files. You must save all the essential files on your file server. When you download a new release onto a file server that has an existing release:

1. Stop the file server.
2. Administer the required port setting in HTTPPORT or TLSPORT for HTTP or TLS, respectively if you want to specify a port the phones must use to communicate with the file server.
3. Back up all the current file server directories as applicable.
4. Copy the 46xxsettings.txt file to a backup location.
5. Remove all the files in the download directory. This ensures that you do not have an inappropriate binary or configuration file on the server. The only system values that can be used in the Conditional statement are: GROUP, MACADDR, MODEL, MODEL4, VPNACTIVE, and SIG_IN_USE.

   Download the self-extracting executable file or the corresponding zip file.
6. Extract all the files.
7. Copy the 46xxsettings.txt file back into the download directory.

8. Check the Readme file for release-specific information.
9. Modify the 46xxsettings.txt file as required.
10. Restart the HTTP and the HTTPS server.
11. Reset your phones.

You can download the default upgrade file from http://www.avaya.com/support. With this file, the phone uses default settings for customer-definable options.

These settings can also be changed with DHCP or in some cases, from the dial pad of the phone.

You might want to open the default file and administer the options to add useful functionality to your Avaya IP phones. Ensure that the file resides in the same directory as the upgrade file and named as the file as 46xxsettings.scr or 46xxsetting.txt. The Avaya IP phones can operate without this file.

Note:

Most Windows systems interpret the file extension `*.scr` as a screen saver. The 4600 IP phones originally used *.scr to indicate a script file. The settings file must have the extension `*.txt`.

Related Links

Maintaining 9600 Series IP Deskphones on page 59

Contents of the settings file

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

- Tags that are lines that begin with a single pound (#) character followed by a single space character and a text string with no spaces.
- **Goto** commands, of the form `GOTO tag`. **Goto** commands cause the phone to continue interpreting the settings file at the next line after a `#tag` statement. If such a statement does not exist, the rest of the settings file is ignored.
- Conditionals, of the form `IF $parameter_name SEQ string GOTO tag`. Conditionals cause the **Goto** command to be processed if the value of the parameter named *parameter_name* exactly matches *string*. If no such parameter named *parameter_name* exists, the entire conditional is ignored. You can use the following parameters in a conditional statement: GROUP, MACADDR, MODEL, MODEL4, VPNACTIVE and SIG_IN_USE.
- **SET** commands, of the form `SET parameter_name value`. The system ignores any invalid values for the associated *parameter_name* so the default or previously administered value is retained. All values must be text strings, even if the value itself is numeric or a dotted decimal IP Address.
- Comments, which are statements with a pound (#) character in the first column.

Note:

Enclose all data in quotation marks for proper interpretation.

- GET commands, of the form `GET filename`. If the phone downloads the file named as filename, the phone interprets the file as an additional settings file and does not interpret additional lines in the original file. If the phone cannot obtain the file, the telephone continues to interpret the original file.

The Avaya-provided upgrade file includes lines that direct the phone to `GET 46xxsettings.txt` and `46xxsettings.scr`.

These lines cause the phone to use HTTP/HTTPS to attempt to download the file specified in the **GET** command. If the phone obtains the file, its contents are interpreted as an additional script file. If the file cannot be obtained, the phone continues processing the upgrade script file.

The phone processes the upgrade script file so that if there is no 46xxsettings.scr file, the phone looks for a 46xxsettings.txt file. If the phone obtains the settings file successfully but does not include any setting changes the phone stops using HTTP. This process happens when you initially download the script file template from the Avaya Support website, before you make any changes. When the settings file contains no setting changes, the phone does not go back to the upgrade script file.

You can customize the settings file and identify non-default option settings, application-specific parameters, and other settings. You can download a template for this file from the Avaya Support website.

For details about specific parameter values, see Chapter 7 in the *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*. Specify settings that are different from default values, although you can also specify default values.

Related Links

Maintaining 9600 Series IP Deskphones on page 59
46xxsettings parameters retained during reboot on page 62

46xxsettings parameters retained during reboot

During a reboot, if the deskphone is unable to access the `46xxsettings` file, it does not retain the values of all the parameters. For the list of retained parameters, see the following table.

Parameter	Retained
AGCHAND	Y
AGCHEAD	Y
AGCSPKR	Y
AGTCALLINFOSTAT	Y
AGTFWDBTNSTAT	Y

Table continues…

Parameter	Retained
AGTGREETINGSTAT	Y
AGTLOGINFAC	Y
AGTLOGOUTFAC	N
AGTSPKRSTAT	Y
AGTTIMESTAT	N
AGTTRANSLPRI	Y
AGTTRANSLPK	Y
AGTTRANSLCLBK	N
AGTTRANSLTO	Y
AGTTRANSLICOM	Y
AGTVUSTATID	Y
AGTACTIVESK	N
APPNAME	N
APPSTAT	Y
AUDIOENV	Y
AUDIOSTHD	Y
AUDIOSTHS	Y
AUTH	Y
BAKLIGHTOFF	Y
BRAUTH	Y
BRURI	Y
CALCSTAT	Y
CALLCTRSTAT	Y
CLDELCALLBK	Y
DHCPSTD	Y
FBONCASCREEN	Y
GUESTDURATION	N
GUESTLOGINSTAT	N
GUESTWARNING	N
HEADSYS	Y
HOMEIDLETIME	N
LOGBACKUP	Y
LOGMISSEDONCE	Y
LOGSRVR	N
LOGLOCAL	Y

Table continues…

Parameter	Retained
LOGUNSEEN	Y
LANGSYS	N
LANGxFILE	Y
LANG0STAT	N
MSGNUM	N
OPSTAT	Y
OPSTAT2	Y
OPSTATCC	Y
PROCSTAT	Y
PROCPSWD	Y
PHY1STAT	Y
PHY2STAT	Y
PHNCC	Y
PHNDPLENGTH	Y
PHNIC	Y
PHNLDLENGTH	N
PHNLD	Y
PHNOL	Y
PHNSCRALL	N
QKLOGINSTAT	Y
RFSNAME	N
REREGISTER	N
SNMPADD	Y
SNMPSTRING	Y
SIG	Y
SCREENSAVERON	Y
SCREENSAVER	Y
TIMERSTAT	N
TPSLIST	N
USBPOWER	Y
USBLOGINSTAT	Y
UNNAMEDSTAT	Y
VLANTEST	Y
VPNPROC	Y
WORLDCLOCKAPP	N

Table continues…

Parameter	Retained
WEATHERAPP	N
WMLHOME	N
WMLPORT	N
WMLPROXY	N

Related Links

Contents of the settings file on page 61

Downloading text language files

About this task

You must save the language files used for text entry and display purposes in the same location as the 46xxsettings file or in the HTTP Server directory. The HTTP Server directory is defined using the `SET HTTPDIR HTTP` server directory path command.

You can download a new language file version only if the filename differs from the language file previously downloaded. Alternately, you can remove the old language file using an empty `SET LANGxFILE` command in the 46xxsettings file before downloading a language file with the same filename.

Related Links

Maintaining 9600 Series IP Deskphones on page 59

Changing the signaling protocol

About this task

For enterprises requiring both H.323 and SIP-based protocols, you can specify the protocol for all or specific deskphones in the following two ways:

Procedure

1. As of Release 6.0, you can set the SIG parameter in DHCP Option 242 (Site-Specific Option Number) or in the 46xxsettings.txt file.

   This setting will apply to all telephones except those for which SIG has been manually configured to a value of H.323 or SIP using the SIG Craft procedure.

2. You can set the SIG parameter on a per-phone basis using the SIG Craft procedure. For more information, see Changing the signaling protocol on page 45 on page 56.

Related Links

Maintaining 9600 Series IP Deskphones on page 59

Applying settings to logical groups

You might have different communities of end users with the same phone model but requiring different administered settings. For example, you might want to restrict Call Center agents from logging out, an essential capability for *hot-desking* associates. This section provides examples of the group settings for each of these situations.

You can separate groups of users is to associate each of them with a number. Use the GROUP parameter for this purpose. You cannot set GROUP system value in the 46xxsettings file. The GROUP parameter can only be set on a phone-by-phone basis. To set the GROUP parameter, first identify which phones 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. The largest group is assigned as Group 0.

Then, at each phone that does not have default parameters, instruct the installer or end-user to invoke the GROUP Local Administrative Craft procedure. For more information, see About local Craft procedures on page 34 and specify which GROUP number to use. After the GROUP assignments are in place, edit the configuration file to allow each phone of the appropriate group to download its proper settings.

Here is an illustration of a possible settings file for the example of a Call Center with hot-desking associates at the same location:

`IF $GROUP SEQ 1 goto CALLCENTER IF $GROUP SEQ 2 goto HOTDESK` {specify settings unique to Group 0} **`goto END`**

`# CALLCENTER` {specify settings unique to Group 1} **`goto END`**

`# HOTDESK` {specify settings unique to Group 2}

`# END` {specify settings common to all Groups}

Related Links

Maintaining 9600 Series IP Deskphones on page 59

Chapter 6: Troubleshooting

Related Links

Resolving error conditions

About this task

Installers can troubleshoot problems before seeking assistance from the system or LAN administrator in four areas:

Procedure

1. Check both the power and Ethernet wiring for the following conditions:
   - Check whether all components are plugged in correctly.
   - Check LAN connectivity in both directions to all servers - DHCP, HTTP, HTTPS, DEFINITY®/MultiVantage™.
   - If the deskphone is powered from the LAN, ensure that the LAN is properly administered and is compliant with IEEE 802.3af.
2. If you use static addressing:
   - Use the VIEW option to find the names of the files being used and verify that these filenames match those on the HTTP/HTTPS server. For more information, see Using the VIEW craft procedure for troubleshooting on page 68. Check the Avaya Support site at www.support.avaya.com to verify whether the correct files are being used.
   - Use the ADDR option to verify IP addresses. For more information, see Changing IP address information on page 42.

3. If the deskphone is not communicating with the system, DHCP, HTTP, or Avaya Media Server, make a note of the last message displayed. For more information, see Installation error and status messages on page 72 and Operational errors and status messages on page 76.

   Consult the system administrator. Sometimes, you can correct problems relating to Communication Manager and HTTP communications by setting the HTTPPORT value to 81.

4. If you want the deskphone to be IEEE-powered, verify with the LAN administrator that IEEE power is indeed supported on the LAN.

Related Links

Troubleshooting on page 67

Failure to hear DTMF tones

As H.323 telephones do not send DTMF tones to non-H.323 telephones, the user need not perform troubleshooting for failure to hear DTMF tones from a 9600 Series IP phone. The TN2302AP board does not pass in-band DTMF tones.

Related Links

Troubleshooting on page 67

Correcting a power interruption

If power to a 9600 Series IP deskphone is interrupted while the phone is saving the application file, the HTTP/HTTPS application can stop responding. If this occurs, restart the phone.

Related Links

Troubleshooting on page 67

Using the VIEW procedure for troubleshooting

About this task

Use the following procedure to verify the current values of system parameters and file versions.

Note:

If administered through OPSTAT, end users can gain access to the Network Information option from the *Phone Settings* option of Avaya Menu to view but not change most of the parameters associated with Craft Local Procedures.. For more information about this option, see the applicable user guides.

Important:

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

Note:

You can use the ADDR option to view IP addresses if needed. For more information on using the *ADDR* option, see Changing IP address information on page 42. The IP addresses might have been entered incorrectly. Verify whether you were provided with correct IP addresses.

Procedure

1. Select **VIEW** from the Craft Local Procedure Screen.

   The phone displays the following options: **IP Parameters**, **Quality of Service**, and **Miscellaneous**.

2. Tap the category that you want to see.

   The information for that category is displayed.

   Note:

   Use the Right navigation arrow to scroll through the viewable information. For more information on system parameters, seeTable 1 Parameter Values on page 69.

Table 1: Parameter Values

Name	System Value	Format
Phone (IPv4)	*nnn.nnn.nnn.nnn*	Phone IP address, IPADD value.
Phone (IPv6)	*hhhh:hhhh::hhhh:hhhh:hhhh*	Phone IP address, NVIPADDV6 value.
Phone (IPv6LL)	*hhhh:hhhh::hhhh:hhhh:hhhh*	Phone IP address, IPADDV6LL value.
Call Server	*nnn.nnn.nnn.nnn*	IP address of the call server currently in use, otherwise *0.0.0.0.*
Supplicant	*ccccccccccccccc*	Text equivalent of DOT1XSTAT. If 0, Disabled; if 1, Unicast-only; if 2, Unicast/multicast.
Pass-thru	*ccccccccccccccc*	Text equivalent of DOT1X. If 0, Enabled; if 1, Enabled w/Logoff; if 2, Disabled.
Router (IPv4)	*nnn.nnn.nnn.nnn*	Up to 15 ASCII characters, the IP address of the router in use.
Mask (IPv4)	*nnn.nnn.nnn.nnn*	Up to 15 ASCII characters, NETMASK value.
HTTP server	*nnn.nnn.nnn.nnn*	IP address of last HTTP server used successfully during initialization or *0.0.0.0.* if no file server was used successfully.

Table continues…

Name	System Value	Format
HTTPS server	*nnn.nnn.nnn.nnn*	IP address of last HTTPS server used successfully during initialization or *0.0.0.0.* if no file server was used successfully.
802.1Q	*cccc*	Text string corresponding to the L2Q value.
VLAN ID	*cccc*	Up to 4 ASCII characters. Value is L2QVLAN text *Auto* if 802.1Q tagging is 0 or *On* if 802.1Q tagging is 1. If 802.1Q tagging is off (2), this line is not displayed.
VLAN Test	*ccc*	Up to 3 ASCII characters. Value is VLANTEST value if 802.1Q tagging is 0 or 1. If 802.1Q tagging is off (2), this line is not displayed.
Scroll **Right** to see the following additional parameters/values:		
L2 Audio	*n*	L2QAUD,layer 2 audio priority value.
L2 Signaling	*n*	L2QSIG,layer 2 signaling priority value.
L3 Audio	*nn*	DSCPAUD, Differentiated Services Code Point for audio.
L3 Signaling	*nn*	DSCPSIG, Differentiated Services Code Point for signaling.
Scroll **Right** to see the following additional parameters/values:		
Ethernet		Text string corresponding to PHY1STAT value, for example,*auto 100 Mbps HDX*, *1000 Mbps FDX*.
PC Ethernet		Test string corresponding to PHY2STAT value, for example, *disabled*, *100 Mbps HDX*, *1000 Mbps FDX*.
Scroll **Right** to see the following additional parameters/values:		
Model	*96ccDccc*	Up to 8 ASCII characters, MODEL serial number.
Phone SN	*cccccccccccccccc*	Phone Serial Number, up to 18 ASCII characters.
PWB SN	*cccccccccccccccc*	Printed Circuit board Serial Number, up to 18 ASCII characters. Applies only to 96xx IP phones that have a software-readable PWB serial number and Comcode.

Table continues…

Name	System Value	Format
		Note: This parameter is not supported in Release 6.3 and later.
PWB comcode	*nnnnnnnnn*	Nine ASCII numeric characters. Applies only to 96xx IP phones that have a software-readable PWB serial number and Comcode. **Note:** This parameter is not supported in Release 6.3 and later.
MAC address	*hh:hh:hh:hh:hh:hh*	Each octet of the MAC address displays as a pair of hexadecimal numbers.
Group	*nnn*	Up to three ASCII numeric characters: GROUP value.
Protocol:	*cccccccc*	Up to eight ASCII characters, currently only *H.323*
Application File	*filename.ext*	Four to 32 ASCII characters as primary application.
Ethernet	*cccccccc* Ethernet	Two to eight ASCII characters, either *1000 Mbps*, *100 Mbps*, *10 Mbps*, or *No*.
Kernel/RFS file	*bootcodename*	One to 32 ASCII characters (backup image name).
Backup App File	*filename.ext*	Four to 32 ASCII characters (backup application).
Button Module 1	*ccccccccccccc*	14 ASCII characters. Version identifier of the software in the first attached Button Module, if applicable.
Button Module 2	*ccccccccccccc*	14 ASCII characters. Version identifier of the software in the second attached button module, if applicable.
Button Module 3	*ccccccccccccc*	14 ASCII characters. Version identifier of the software in the third attached button module, if applicable.
Proxy Server	WMLPROXY	Proxy server used for WML functions.

Table continues…

Name	System Value	Format
Voice Language File	NVVOXFILE	Language file (NVVOXFILE) designated for voice-initiated dialing. Not applicable for software Release 6.0.

3. Use the Right navigation arrow to scroll through the information shown in the table.
4. Press **Back** at any time to return to the Craft Procedures screen.

Related Links

Troubleshooting on page 67

Installation error and status messages

9600 Series IP phones display messages in the currently selected language or in the language specified by the LANGSYS parameter value, if the phone is logged off. If English is not the selected language, the phone displays messages in English only when the message are associated with local procedures, for example, MUTE VIEW.

The phone displays most of the messages for only about 30 seconds, and then the phone is reset. The most common exception is `Extension in Use`, display more than 30 seconds and which remains until you perform any further action on the phone.

Note:

For VPN-related error and status messages, see the *VPN Setup Guide for 9600 Series IP Telephones, 16-602968*.

Table 2: Possible error and status messages during installation of 9600 Series IP phones

Message	Cause/Resolution
`802.1X Failure`	CAUSE: Incorrect credentials provided for authentication or credentials not provided at all. RESOLUTION: Follow the display prompts and reenter the 802.1X ID and password.
`IPv4 or IPv6 address Conflict`	CAUSE: The phone has detected an IP address conflict. RESOLUTION: Verify administration settings to identify duplicate IP addresses.
`Authentication Error`	CAUSE: The call server does not recognize the extension entered. RESOLUTION: Confirm the extension is correct and is correctly administered on the switch. Then try registration again, and enter the extension accurately.
`Bad FileSv address`	CAUSE: The HTTP/HTTPS server IP address in the IP phone's memory is all zeroes.

Table continues…

Message	Cause/Resolution
	RESOLUTION: Depending on the specific requirements of your network, this may not be an error. If appropriate, either administer the DHCP server with the proper address of the HTTP/HTTPS server, or administer the phone locally using the ADDR option. For details on the ADDR option, see Using Local Administrative (Craft) Options on page 33.
`Bad Router?`	CAUSE: The phone cannot find a router based on the information in the DHCP file for GIPADD. RESOLUTION: Use static addressing to specify a router address, or change administration on DHCP.
`Call Error`	CAUSE: The user was on a call when the connection to the gatekeeper went down due to a network outage or a gatekeeper problem. The phone attempted to automatically register with the same or another gatekeeper, but the responding gatekeeper had no record of the call. RESOLUTION: Wait for the call to end, and if the phone does not automatically register, restart the phone.
`Connecting...`	CAUSE: The phone is attempting to establish a TCP connection with the call server. A resource needed to establish the connection might not be available or the 10 second buffer on switch-related actions might have expired. RESOLUTION: Allow the phone to continue attempts to connect to TCP.
`Contacting call server...`	CAUSE: The phone has rebooted successfully and is attempting to register with the call server. RESOLUTION: Allow the phone to continue.
`DHCP: CONFLICT * to program`	CAUSE: At least one of the IP address offered by the DHCP server conflicts with another address. RESOLUTION: Review DHCP server administration to identify duplicate IP address(es).
`DHCPv6 Failure: (with message)`	CAUSE: The phone receives a reply message with a Status Code option that contains a status-code of 1 which means *UnspecFail* or a reply in response to a *Renew* or *Rebind* message with a Status Code option containing a status-code value other than 0 that indicates *Success* or 5 which indicates *UseMulticast*. RESOLUTION: In the first case, DHCPv6 will be restarted. If this message is the result of a status-code value other than 1 or 5, IPADDV6 will be set to null; if dual-stack operation is enabled the phone will also cease use of its IPv4 address and IPADD will be set to null, and DHCP operation will proceed.
`Discover` *aaa.bbb.ccc.ddd*	CAUSE: The phone is attempting to find Communication Manager. RESOLUTION: Long display of this message implies failure of the Communication Manager server or a network problem that an administrator must fix. The administrator must ensure that there is network connectivity to Communication Manager, user extension is defined, and the Communication Manager server is up.
`Discovering...`	CAUSE: The phone is attempting to find a Communication Manager.

Table continues…

Message	Cause/Resolution
	RESOLUTION: Long display of this message implies failure of the Communication Manager server or a network problem that an administrator must fix. The administrator must ensure that there is network connectivity to Communication Manager, user extension is defined, and the Communication Manager server is up.
`EEPROM error, repair required`	CAUSE: Application file was not downloaded or saved correctly. RESOLUTION: The phone automatically resets and attempts to re-initialize.
`Emergency Option`	CAUSE: Incompatible emergency option. RESOLUTION: This must not happen. Contact Avaya support.
`Extension in Use` `Extension in use: <NNNN> Press continue to take over this extension Login| Continue`	CAUSE: The call server detects an extension conflict with an existing set or Softphone. RESOLUTION: By pressing **Continue**, you can force the current phone to register and thereby disconnect the other user. When **Login** is selected instead, the phone re-prompts for entry of a different extension and password.
`Finding router...`	CAUSE: This phone is proceeding through boot-up. RESOLUTION: Allow the phone to continue.
`Gatekeeper Error`	CAUSE: The gatekeeper rejects the registration attempt for an unspecified reason. RESOLUTION: Review gatekeeper and call server administrations, including IP network parameters.
`Gateway Error`	CAUSE: DEFINITY Release 8.4 does not have an H.323 station extension for this phone. RESOLUTION: On the station administration screen, ensure the DCP set being aliased for this IP phone has an H.323 station extension administered, in accordance with switch administration instructions. Since the 9600 Series IP phones are not supported on DEFINITY Release 8.4, you must upgrade to a release that supports these phones.
`Incompatible`	CAUSE: This release of the call server does not support the current version of the IP phone. RESOLUTION: Upgrade to the current version of Communication Manager (3.0 or greater) software.
`Invalid file`	CAUSE: The phone does not have sufficient room to store the downloaded file. RESOLUTION: Verify that the proper filename is administered in the script file, and the correct application file is located in the appropriate location on the HTTP or HTTPS server.
`IP address Error`	CAUSE: The gatekeeper reports an invalid IP address. RESOLUTION: This must not happen. Contact Avaya support.
`License Error`	CAUSE: The call server does not support IP telephony. RESOLUTION: Contact Avaya to upgrade your license.

Table continues…

Message	Cause/Resolution
`Limit Error`	CAUSE: The call server has reached its limit of IP stations. RESOLUTION: Un-register phones that are not in use, or contact Avaya to upgrade your license.
`NAPT Error`	CAUSE: A device between the phone and the call server is invoking Network address Port Translation (NAPT), which the 9600 Series IP phones do not support. RESOLUTION: Contact the System Administrator to remove or re-administer the device.
`No Ethernet`	CAUSE: When first plugged in, the IP phone is unable to communicate with the Ethernet. RESOLUTION: Verify the connection to the Ethernet jack, verify if the jack is Category 5, verify if power is applied on the LAN to that jack.
`Packet Error`	CAUSE: Protocol timeout error. RESOLUTION: Reenter the correct extension and password. If the condition persists, contact the system administrator.
`Password Error`	CAUSE: The call server does not recognize the password entered and displays the *Login Error* screen. RESOLUTION: Confirm whether the password is correct, then try registering again, and enter the password accurately.
`Request Error`	CAUSE: The gatekeeper does not accept the registration request sent by the phone as the request is not formatted properly. RESOLUTION: The phone will automatically attempt to register with the next gatekeeper on its list. If the problem persists, reboot the phone.
`Restarting...`	CAUSE: The phone is in the initial stage of rebooting. RESOLUTION: Allow the phone boot process to continue.
`Subnet conflict * to program`	CAUSE: The phone is not on the same VLAN subnet as the router. RESOLUTION: Press star (*) to administer an IP address on the phone. For information on configuring an IP address, see Changing IP address information on page 42, or administer network equipment to administer the phone appropriately.
`System busy`	CAUSE: Most likely, the number of IP endpoints on the call server is already at maximum capacity. Network resource may not be unavailable. RESOLUTION: The phone attempted to access a network resource such as DHCP server, HTTP server, or the call server and was not successful. Check the resource being called upon for its availability. If the resource appears operational and is properly linked to the network, verify that the addressing is accurate and that a communication path exists in both directions between the phone and the resource.
`System Error`	CAUSE: The call server has an unspecified problem. RESOLUTION: Consult your Avaya Media Server administration and troubleshooting documentation.

Table continues…

Message	Cause/Resolution
`Undefined Error`	CAUSE: The call server has rejected registration for an unspecified reason. RESOLUTION: Consult your Avaya Media Server administration and troubleshooting documentation.
`Updating: DO NOT UNPLUG THE phone`	CAUSE: The phone is updating its software image. RESOLUTION: The phone update process must be continued.
`Waiting for LLDP`	CAUSE: No File Server or Call Server has been administered, so the phone is expecting to get the missing data through LLDP. RESOLUTION: Administer the missing data by one of the following methods: Statically, dynamically in DHCP, in the 46xxsettings file for Call Server addresses, or by LLDP. For more information, see LLDP Troubleshooting on page 81.
`Wrong Set Type`	CAUSE: The call server does not recognize the set type. RESOLUTION: Ensure the call server is properly administered to register a compatible phone for the IP address and extension.

Related Links

Troubleshooting on page 67

Operational errors and status messages

The following table identifies some of the possible operational problems that might be encountered after successful 9600 Series IP phone installation. The user guide for a specific phone model also contains troubleshooting for users having problems with specific IP phone applications. Most of the problems reported by phone users are LAN-based, where Quality of Service, server administration, and other issues can impact end-user perception of IP phone performance.

Table 3: Operational error conditions for 9600 Series IP Phones

Condition	Cause/Resolution
The phone continually reboots, or reboots continuously about every 15 minutes.	CAUSE: The phone cannot find the HTTP/HTTPS server and/or call server. RESOLUTION: Ensure that MCIPADD is administered either manually or through DHCP or HTTP, as appropriate. Alternately, this might be a firmware fault because the MAC address in memory is corrupted; in this case, you must return the phone to Avaya for repair.
The message light on the phone turns on and off intermittently, but the phone never registers.	CAUSE: This is a hardware fault. RESOLUTION: You must return the phone to Avaya for repair.

Table continues…

Condition		Cause/Resolution
The phone stops working in the middle of a call,	AND no lights are lit on the phone and the display is not lit.	CAUSE: Loss of power. RESOLUTION: Check the connections between the phone, the power supply, and the power jack. For example, verify whether static addressing was not used or that any changes to static addresses were entered correctly. Follow POE guidelines to troubleshoot POE related problems.
	AND power to the phone is normal and the phone might have gone through the restarting sequence.	Loss of path to the Avaya call server, expiry of DHCP lease, or unavailable DHCP server when telephone attempts to renegotiate DHCP lease. RESOLUTION: As above.
The phone was working, but does not work now,	AND no lights are lit on the phone and the display is not lit.	CAUSE: Loss of power. RESOLUTION: Check the connections between the phone, the power supply, and the power jack. Follow POE guidelines to troubleshoot POE related problems.
	AND power to the phone is normal, but there is no dial tone. The display might show “System Busy.”	CAUSE: Loss of communication with the call server. RESOLUTION: Check LAN continuity from the call server to the phone using ARP or trace-route and from the phone to the call server by invoking a Feature button. Verify that LAN administration has not changed for the Gatekeeper, TN 2302AP boards, or the LAN equipment (routers, servers, etc.) between the switch and the phone. Verify that telephone settings are not changed locally using VIEW and ADDR information, as described earlier in this guide. Verify that the telephone volume is set high. Finally, conduct a self-test.
	AND the phone was recently moved.	CAUSE: Loss of communication with the call server. RESOLUTION: As above, but verify whether the phone is being routed to a different DHCP server, or even a different call server switch. If so, the new server or switch might need to be administered to support the phone.
	AND the network was recently changed to upgrade or replace servers, re-administer the Avaya Media Server, add or change NAT, etc.	CAUSE: Loss of communication with the call server. RESOLUTION: As above.
The phone works, but the audio quality is poor, specifically:		

Table continues…

Condition		Cause/Resolution
	the user hears echo when speaking on a handset.	CAUSE: Echo from digital-to-analog conversion on your Avaya Media Server trunk. RESOLUTION: Identify the trunk that is causing the echo, and swap the Trunk Termination parameter for that trunk on the call server.
	the user hears an echo on a headset, but not on a handset.	CAUSE: Improper headset cord. RESOLUTION: Ensure that an headset cord approved by Avaya is being used.
	the user is on Speaker and hears no echo, but the far-end hears echo.	CAUSE: Room acoustics. RESOLUTION: Ensure that there are six inches or so of blank space to the right of the phone. If that is insufficient, use the handset.
	the user experiences sudden silences such as gaps in speech, or static, clipped or garbled speech, etc.	CAUSE: Jitter, delay, dropped packets, etc. RESOLUTION: You can have the user provide diagnostic data to Avaya support by invoking the Network Information feature under the **A** (Avaya Menu) or **Home** button on the phone. One or more Quality of Service (QoS) features should be implemented in the network. For information on QoS, seeUsing Local Administrative (Craft) Options on page 33. CAUSE: Improper non-Category 5 wiring. RESOLUTION: Replace non-Category 5 wiring with Category 5 wiring.
	the user hears fluctuations in the volume level which are worse when the Speaker is on, or at the beginning of a call, or when a call goes from no one talking abruptly to a loud voice.	CAUSE: The user has changed the Automatic Gain Control (AGC) or environmental acoustics are not consistent with the current audio settings. RESOLUTION: Try different *On* or *Off* settings for the AGCHAND, AGCHEAD, and AGCSPKR parameters.
The phone works properly except for the Speaker.		CAUSE: The Speaker was turned off at the call server. RESOLUTION: Administer the call server to allow that station's Speaker to operate. If that does not work, do a self-test on the phone, as explained in Performing a self-test on page 57.
The phone works properly, but you cannot hear incoming DTMF tones.		CAUSE: The TN2302AP board does not pass in-band DTMF tones. RESOLUTION: None; the board is operating as designed.

Table continues…

Condition		Cause/Resolution
The phone works properly, but you cannot hear incoming DTMF tones.		CAUSE: Call server suppresses sidetone DTMF. RESOLUTION: After completing call server administration, enable On-Hook Dialing on the Change-System-Parameters screen. If the user has enabled Hands-Free Answer (HFA), answers a call using the Speaker, switches to the handset, and presses dialpad buttons, the phone does not transmit DTMF tones. Disable HFA to hear DTMF tones.
Hands-Free Answer (HFA) is administered but the phone did not automatically answer a call.		CAUSE: HFA only works if the phone is idle. The phone ignores a second call if a call, including the ringing tone is in progress. RESOLUTION: None.
The phone does not use and ignores the HTTP or HTTPS script file and settings file.		CAUSE: The system value AUTH is set to 1 which indicates that HTTPS is required but no valid address is specified in TLSSRVR. RESOLUTION: Change AUTH to 0 (zero), or enter a valid address for TLSSRVR.
The HTTP or HTTPS script file is ignored or not used by the phone,	AND the HTTP or HTTPS server is a LINUX or UNIX system.	CAUSE: The phone expects lines of the script file to terminate with a **<Carriage Return> <Line Feed>**. Some UNIX applications only terminate lines with **<Line Feed>**. Editing the script file with a UNIX-based editor can strip a**<Carriage Return>** from the file. Doing so causes the entire file to be treated as a comment, and thus be ignored. RESOLUTION: Edit the script file with a Windows® — based editor, or another editor that does not strip out the **<Carriage Return>**. CAUSE: UNIX and LINUX systems use case-sensitive addressing and file labels. RESOLUTION: Verify the file names and path in the script file are accurately specified.
	AND phone administration recently changed.	CAUSE: The 96xxupgrade.txt file was edited incorrectly, renamed, etc. RESOLUTION: Download a clean copy of the 96xxupgrade.txt file from the Avaya support web site at http://www.avaya.com/support, and do not edit or rename the file. Customize or change *only* the 46xxsettings file as required. For more information, seeMaintaining 9600 Series IP phones on page 59.
The system ignores some settings in the settings file while other settings are being used properly.		CAUSE: Improper administration of settings file. RESOLUTION: Verify that customized settings are correctly spelled and formatted.

Table continues…

Condition		Cause/Resolution
The system ignores some settings in the settings file while other settings are being used properly,	AND the setting being ignored is one or more of the AGC settings.	CAUSE: The user changed the AGC settings, which were placed in the backup or restore file of the user. RESOLUTION: The user can reset the AGC values back to the required settings, or the backup file can be edited to delete the custom AGC settings.
Telephone power is interrupted while the phone is saving the application file and the HTTP/HTTPS application stops responding.		CAUSE: The HTTP or HTTPS server stops responding if power is interrupted while a phone is saving the application file. RESOLUTION: Restart the phone
The user indicates an application or option is not available.		CAUSE: The 46xxsettings script file is not pointed to accurately, or is not properly administered to allow the application. RESOLUTION: Verify that the 46xxsettings script file is properly specified for your system, verify that the file server is UNIX or LINUX, and verify the extension. Then verify that all the relevant parameters indicated in Chapter 7 of the *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*, are accurately specified in the 46xxsettings file.
User data disappeared when the user logged out of one phone and logged in to another phone.		CAUSE: The second phone is unable to gain access to the backup file. RESOLUTION: Verify that the first phone creates a backup file. Verify whether appropriate administration was done in accordance with Chapter 7 of the *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*. Then verify that the second phone is administered to retrieve data from the same location as the first phone. Then verify that all the relevant parameters indicated in Chapter 7 of the *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*, are accurately specified in the 46xxsettings file. Finally, verify that the HTTP and HTTPS server on which the backup file is located is operational and accessible from the second phone.
The user reports that button module buttons are not labeled properly.		CAUSE: Improper administration on the call server. RESOLUTION: Verify correct administration.
The user reports that personalized labels cannot be placed on	AND the user has tried using the Program AD button feature.	CAUSE: Improper administration on the call server. RESOLUTION: Verify correct administration.

Table continues…

Condition		Cause/Resolution
the button module's buttons,		
	AND the user has tried using the Personalize Labels option on the phone.	CAUSE: The user pressed the button module button to indicate which button to relabel. RESOLUTION: The user should use the list displayed on the phone, scroll to highlight the desired button label, and press either **OK** or the corresponding line button.
The user reports inability to gain access to Contacts or backed-up Call Log entries, or user options.	AND the user is registered via a USB login.	CAUSE: The phone is working as designed. RESOLUTION: Remove the USB device and log in locally.
The user reports that pressing *My Pictures* causes the default Avaya or administered custom screensaver to appear.	AND the user is registered via a USB login.	CAUSE: One or more files in the USB pictures directory are not in proper .jpg format or are too large for the given phone to display. RESOLUTION: Check the file format and verify that height/width limits as specified in the User Guide are followed.
Touchscreen phones only. User gets *Could Not Access Internet Service* message from the World Clock or Weather application.		CAUSE: WMLPROXY and or WMLPORT have not been properly administered. RESOLUTION: Administer the missing data in the 46xxsettings file. For more information on the settings file, see the *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*.

Related Links

Troubleshooting on page 67

LLDP Troubleshooting

If the *Waiting for LLDP* message appears for more than a few seconds, the message generally indicates a problem with getting a value for the call server IP address. This error can occur due to incorrect settings in script files or in the way the network is configured.

On booting, the phone must obtain a valid IP address for the call cerver. The phone can obtain the value, known as MCIPADD, from several sources:

- A static or manually programmed address on the phone.
- The 46xxsettings.txt file MCIPADD setting.
- A DHCP offer using option 242 that includes the MCIPADD setting.
- Link Layer Discovery Protocol or *LLDP*.

If the phone cannot find MCIPADD through any of these means, it will fail to register with the Call Server and will display the *Waiting for LLDP* message several times before rebooting. For example, if the MCIPADD value was specified in the 46xxsetting file and the network file server fails, the phone will not be able to read the MCIPADD value or any of the 46xxsettings file parameters. Therefore, do not use this method of providing MCIPADD.

Related Links

Troubleshooting on page 67

Proposed Solution

Procedure

1. A more robust way to provide this value is to use DHCP. You can administer the DHCP server to provide MCIPADD using DHCP Option 242. You can also administer the TLSSRVR, HTTPSRVR and L2QVLAN parameters using this option. phones using non-static addressing automatically use the DHCP request method. Option 242 is the default DHCP offer and may get MCIPADD and other addresses using this way.
2. The phone displays the *Waiting for LLDP* message when both the HTTP and HTTPS Server IP address are not administered. To administer the HTTP and/or HTTPS server, use the Craft ADDR procedure and enter the correct HTTP and or HTTPS File Server IP address in the File Server field.
3. An alternative protocol known as LLDP can also supply call server, and file server with HTTP and HTTPS IP addresses. This IETF standard protocol requires the network to be equipped and configured to support LLDP. You can provide HTTP and the HTTPS Server and call server IP addresses with LLDP in the network using proprietary Transport Layer Values (TLVs) to pass information to the phones.

LLDP setup and troubleshooting steps

Note:

If system value *STATIC* is set to 0 which is the default setting, the DHCP or the 46xxsettings file might overwrite the static addresses.

Note:

See *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323* for details on how to set “STATIC” to use manually programmed IP addresses.

Related Links

Troubleshooting on page 67

Proposed solution for DHCP configured deskphones

Procedure

1. Using the Craft *ADDR* procedure, set *Phone* to **0.0.0.0**.
2. Verify or set *SSON* to **242** which is the default value.
3. Administer the DHCP server option 242 to include **MCIPADD**=*xxx.xxx.xxx.xxx* where *xxx.xxx.xxx.xxx* is the call server IP address.
4. Verify that the DHCP server and the deskphone are on the same VLAN.
5. Verify the *DHCP server* port 67 and or the *DHCP client* port 68 are not blocked on the switch.
6. Verify the configuration of the DHCP Relay Agent on the switch or on a separate PC, for example, MS Windows Server 2000/2003 whether the deskphones and DHCP Server are placed on different networks or subnets. DHCP broadcast messages do not, by default, cross the router interface.

   Note:

   Do not embed spaces in DHCP Option 242 strings. For more information, see *DHCP Server Administration* in *Administering 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*.

Proposed solution for script-configured deskphones

Procedure

1. Edit the 46xxsettings.txt file to contain a valid Call Server IP address with the line **SET MCIPADD** *xxx.xxx.xxx.xxx* where *xxx.xxx.xxx.xxx* is the Call Server IP address.
2. Verify that the 96xxupgrade.txt file contains the line **GET 46xxsettings.txt** as the last command line of the upgrade file.
3. Verify that the deskphone can reach the HTTP server and whether the HTTP server is activated.
4. Verify that the 96xxupgrade.txt and 46xxsettings.txt files are placed in the proper directory of the HTTP server to access these files.

Proposed solution for LLDP-configured deskphones

About this task

For LLDP-configured deskphones, activate the switch the deskphone is connected to for LLDP. This is currently only possible with Extreme switches. Activating the switch for LLDP enables the switch

to send appropriate IP addresses using Avaya/Extreme Proprietary HTTP and/or HTTPS Server and/or Call Server TLVs.

Note:

The deskphone obtains the HTTP and or HTTPS Server and Call Server IP addresses from LLDP only if the addresses were not configured through other means such as DHCP Server, Script File, or statically.

Note:

Set the switch LLDP repeat timer to less than 30 seconds.

SLA Monitor agent

SLA Mon™ technology is a patented Avaya technology embedded in Avaya products to facilitate advanced diagnostics. The deskphones support SLA Mon™ agent which works with a Avaya Diagnostic Server (ADS). SLA Mon™ server controls the the SLA Mon™ agents to execute advanced diagnostic functions, such as:

- Endpoint Diagnostics
  - The ability to remotely control IP phones, to assist end users with IP Phone configuration and troubleshooting.
  - The ability to remotely generate single and bulk test calls between IP phones.
  - The ability to remotely execute limited packet captures on IP phones to troubleshoot and diagnose IP phone network traffic.
- Network Monitoring
  - The ability to monitor multiple network segments for performance in terms of packet loss, jitter, and delay.
  - The ability to monitor hop-by-hop QoS markings for voice and video traffic.

Note:

The root trusted certificate used for the SLA Mon™ server certificate must be added to the trusted certificate list administered using TRUSTCERTS.

For example: SET TRUSTCERTS *slamonRootCA.crt, rootCertRNAAD.cer*

Related Links

Troubleshooting on page 67

Secure Shell Support

The phone supports the Secure Shell (SSH) v2 protocol. The SSH protocol is a tool that the Avaya services organization can use to remotely connect to IP deskphones to monitor, diagnose, or debug

deskphone performance. Because of the sensitive nature of remote access, you can disable permission with the SSH_ALLOWED parameter.

The deskphone displays a security warning message at start of the session. You can specify your own file using SSH_BANNER_FILE, or the deskphone will use the following default file:

```
This system is restricted solely to authorized users for legitimate
business purposes only. The actual or attempted unauthorized access,
use, or modification of this system is strictly prohibited. Unauthorized
users are subject to company disciplinary procedures and or criminal and
civil penalties under state, federal, or other  applicable domestic and
foreign laws. The use of this system may be monitored and recorded for
administrative and security reasons. Anyone accessing this system
expressly consents to such monitoring and recording, and is advised that
if it reveals possible evidence of criminal activity, the evidence of
such activity may be provided to law  enforcement officials. All users
must comply with all corporate instructions regarding the protection of
information assets.
```

If you require a custom warning message, you can set SSH_BANNER_FILE to an absolute URL, or the name of the file on the standard file server such as HTTPSRVR.

The Avaya technician can match the SSH fingerprint displayed under debug with the fingerprint present in the SSH client. This information is used to verify whether the administrator is logged on to the correct SSH server. The SSH fingerprint is not displayed when the FIPS mode is enabled. The deskphones support 2048-bit asymmetric key length for SSH server.

You can also administer the *SSH_IDLE_TIMEOUT*parameter to configure the duration of inactivity that will disable SSH.

Related Links

Troubleshooting on page 67

Chapter 7: Glossary

Glossary Terms	Description
802.1D	802.1Q defines a layer-2 frame structure that supports VLAN identification
802.1Q	QoS mechanism is usually referred to as 802.1D.
802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. Applicable 9600 Series IP deskphones support IEEE 802.1X for pass-through and for Supplicant operation with the EAP-MD5 authentication method.
Application - specific	Specific to a particular “application” running inside the deskphone. For example, configuration file downloading, backup and restore of user data, HTTP push, and the Web browser are all internal applications that use the HTTP protocol. Similarly, the RTCP and CNA clients are internal applications that can invoke traceroute. This term does not include Web page-based “applications” rendered in the Web browser.
ARP	Address Resolution Protocol that you can use to verify that the IP address that the DHCP server provides is not in use by another IP deskphone.
CLAN	Control LAN, a type of Gatekeeper circuit pack.
CNA	Converged Network Analyzer.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
DNS	Domain Name System, an IETF standard for ASCII strings to represent IP Addresses. DNS is a distributed Internet directory service that translates domain names and IP Addresses. For example, 9600 Series IP Deskphones use DNS to resolve names into IP Addresses. DHCP, TFTP, and HTTP files use DNS names wherever IP addresses are available and a valid DNS server exists.
Gatekeeper	H.323 application that performs essential control, administrative, and managerial functions in the media server. Sometimes called CLAN in Avaya documents.
H.323	A TCP/IP-based protocol for VoIP signaling.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	A secure version of HTTP.
IEEE	Institute of Electrical and Electronics Engineers, an organization that, among other things, produces standards applicable to Local Area Network equipment.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.

Table continues…

LAN	Local Area Network.
MAC	Media Access Control, the ID of an endpoint.
QoS	Quality of Service, mechanisms that improve audio quality over packet-based networks.
RTCP	Real-time Transport Control Protocol.
RTP	Real-time Transport Protocol.
SRTCP	Secure Real-time Transport Control Protocol.
SRTP	Secure Real-time Transport Protocol.
System - specific	Specific to a particular type of call server, for example, Communication Manager. “System-specific signaling” refers to messages specific to the signaling protocol used by the system, for example, H.323 or CCMS messages or both messages used by Communication Manager and IP Office. “System-specific procedures” refers to deskphone software procedures that are specific to the call server with which the software is intended to be used.
TCP	Transmission Control Protocol, a connection-oriented transport-layer protocol.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL) that is compatible with SSL 3.0. Using TLS, you can ensure privacy and data integrity between two communicating applications.
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
Unnamed Registration	A type of registration with Communication Manager in which the IP deskphone does not need an extension. This type of IP deskphone has limited outgoing calling facility.
URI & URL	Uniform Resource Identifier and Uniform Resource Locator. Names for the strings used to reference resources on the Internet (for example, HTTP://....). URI is the newer term.
USB	Universal Serial Bus. An industry standard used by PCs and various devices for communication.
VLAN	Virtual LAN.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.

Index

Numerics

A

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U