Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/ 9641G IP Deskphones SIP

16-603504
Release 6.5
Issue 1
January 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Licenses

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

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

License Type (s)

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

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

Copyright

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

Third party components

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

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

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

Avaya is a registered trademark of Avaya Inc.

Downloading documents

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

Contact Avaya Support

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

FCC/Industry Canada Radiation Exposure Statement

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

Note

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

Warning

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

Contents

Chapter 1: Introduction

Purpose

This guide describes how to install and maintain 9600 Series IP Deskphones models 9601, 9608, 9608G, 9611G, 9621G, and 9641G in a Session Initiation Protocol (SIP) environment and troubleshoot problems.

To use the 9600 Series IP Deskphones models 9601, 9608, 9608G, 9611G, 9621G, and 9641G in SIP environment, you must have the following two servers in your network:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager

Note:

Any reference to HTTP in this guide applies equally to HTTPS.

Intended audience

This document is intended for personnel who install and administer SIP-based 9600 Series IP Deskphones models 9601, 9608, 9608G, 9611G, 9621G, and 9641G for a SIP environment.

CAUTION:

Avaya does not provide product support for many of the products mentioned in this document. Ensure that there is adequate technical support available for the servers involved, including, but not necessarily limited to HTTP, HTTPS and DHCP servers. If the servers are not functioning correctly, the deskphones might not be able to operate correctly.

Document changes since last issue

Issue 1	First issue of the document in January 2015, to support the 9600 Series IP Deskphones software release 6.5 for the deskphone models: 9608, 9608G, 9611G, 9621G, and 9641G.

What is new in the 6.5 release

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

Related resources

Documentation

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

Title	Description
Administering Avaya Deskphone SIP for 9601/9608/9611G/9621G/9641G	Describes how to administer SIP-based 9600 Series IP Deskphones.
Avaya Aura® Session Manager Overview	Describes features of Avaya Aura® Session Manager.
Implementing Avaya Aura® Session Manager	Describes the installation procedures and initial administration information for Avaya Aura® Session Manager.
Upgrading Avaya Aura® Session Manager	Describes how to upgrade Avaya Aura® Session Manager to a new software release.

Title	Description
Administering Avaya Aura® Session Manager	Describes how to administer Avaya Aura® Session Manager using System Manager.
Maintaining and Troubleshooting Avaya Aura® Session Manager	Describes information for troubleshooting Avaya Aura® Session Manager, resolving alarms, replacing hardware, and alarm codes and event ID descriptions.
Avaya Aura® Session Manager Case Studies	Provides functionality of Avaya Aura® Session Manager in different scenarios.
Installing and Upgrading Avaya Aura® System Manager	Describes the installation procedures and initial administration information for Avaya Aura® System Manager.
Administering Avaya Aura® System Manager	Describes how to administer Aura® System Manager.
Avaya one-X™ Deskphone SIP Installation and Maintenance Guide Release 2.6	Describes installation or troubleshooting of other 9600 Series SIP deskphones that are not covered in this guide.

The following table lists the websites for the related non-Avaya documents, such as those published by the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU).

Documents	Refer
IETF	For IETF documents that provide standards relevant to IP Telephony, visit http://www.ietf.org/rfc.html.
ITU	For ITU documents and guidelines, visit http://www.itu.int.
ISO/IEC, ANSI/IEEE	For ISO/IEC guidelines and documents on IP Telephony standards. visit http://www.iec.ch.

Support

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

Document organization

The following table lists the chapters, their description, and how they are organized in this guide.

Chapter name	Description
Chapter 1: Introduction	Provides an overview of this guide.
Chapter 2: 9600 Series IP Deskphones installation	Describes the equipment and resources required to properly install and operate SIP-based 9600 Series IP Deskphones models. Provides instructions on installing the deskphones out of the box.
Chapter 3: Local administrative options	Describes how to set local administrative options, if requested by the system or LAN administrator.
Chapter 4: Maintaining the 9601, 9608, 9608G, 9611G, 9621G, and 9641G IP deskphones	Describes maintenance actions like downloading deskphone software from the Avaya support website and customizing system values.
Chapter 5: Troubleshooting guidelines	Describes error conditions and messages that might occur during the installation of SIP-based 9600 Series IP Deskphones models.
Appendix A: Glossary	Provides a glossary of terms used in this document or which are generally applicable to SIP-based 9600 Series IP Deskphones models.

Chapter 2: 9600 Series IP Deskphones installation

Introduction

SIP-based 9600 Series IP Deskphones models support DHCP and HTTP/HTTPS over IPv4/UDP that enhances the administration and servicing of the deskphones. These deskphones use DHCP to obtain dynamic IP addresses and HTTP or HTTPS to download new software versions and customized settings.

SIP-based 9600 Series IP Deskphones models provide the ability to have one IP connection on the desktop for both a deskphone set and a PC using an Ethernet switch.

In compliance with Australian law, the following information is provided:

> This equipment shall be installed and maintained by trained service personnel. All the 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 240VAC rms to any primary/mains circuitry and 120VAC rms to any telecommunications network circuitry). To ensure that these conditions are adhered to, interconnect the equipment only with the already approved/certified equipment.

IP deskphone models

There are twelve models currently defined in the 9600 Series IP Deskphones family that run the SIP protocol. This guide covers only the following deskphone models:

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

The deskphones have an internal Ethernet switch that allows the deskphone and a PC to share the same LAN connection, if appropriate. Thus, 9600 models do not need, or work with, the 30A switched hub interface. The deskphone models 9608G, 9611G, 9621G and 9641G have a Gigabit Ethernet (GigE) interface that speeds data transmission.

This document describes the installation and post-installation maintenance issues of these IP deskphones. For details about using deskphone features, see the user documentation for each deskphone.

Software

The 9608, 9608G, 9611G, 9621G, and 9641G IP deskphones are set to use the H.323 protocol by default. To run the deskphones in a SIP environment, you must convert the deskphones to SIP settings. Further, a factory-shipped IP Deskphone may not contain the most up-to-date software for registration and SIP operation. When you connect the deskphone to your network, the deskphone connects to an HTTP server and searches for the latest software bundle available. You must download the latest SIP software bundle for deskphones to be converted to SIP, then set the SIG parameter as applicable to convert applicable deskphones to run SIP software, as described in Converting software on the 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones on page 14.

For subsequent downloads of software upgrades, Avaya Aura® Session Manager provides the capability for a remote restart of the deskphone.

Session Manager, Communication Manager, and Secondary Gateway configurations

SIP software release 6.2 is compatible with release 6.0 of Avaya Aura® Communication Manager and Avaya Aura® Session Manager. This release supports the following certified secondary gateways:

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

Preinstallation checklist

Before plugging in a 9601, 9608, 9608G, 9611G, 9621G, or 9641G deskphone, verify that all the following requirements are met. Failure to do so prevents the deskphones from working properly and can have a negative impact on the network. Print copies of this checklist for each server and deskphone.

Verify these network requirements

❑ **1.** Ensure that the LAN uses Ethernet Category 5e cabling running the IPv4 version of Internet Protocol.

❑ **2.** Ensure that the following is installed and/or set up and operative:

- Avaya Aura® Communication Manager and Avaya Aura® Session Manager, release 6.0 or greater.
- NTP Time Server.

See Session Manager, Communication Manager, and Secondary Gateway configurations for information on allowable configurations before proceeding.

❑ **3.** Ensure that the correct circuit packs are installed on the switch. For details, refer to the Avaya Communication Manager documentation at http://www.avaya.com/support.

❑ **4.** The Communication Manager call server is configured correctly, as described in *Administering Avaya Deskphone SIP for 9601/9608/9608G/9611G/9621G/9641G* and Avaya Communication Manager documentation. Both documents are available at http://www.avaya.com/support.

❑ **5.** The DHCP server and application are administered as Described in *Administering Avaya Deskphone SIP for 9601/9608/9608G/9611G/9621G/9641G*.

❑ **6.** The HTTP/HTTPS server and application are administered as described in *Administering Avaya Deskphone SIP for 9601/9608/9608G/9611G/9621G/9641G*.

❑ **7.** The SIP upgrade script and application files from the Avaya Support Web site, http://www.avaya.com/support, are loaded correctly on the HTTP/HTTPS server.

❑ **8.** If applicable, the Voice Mail server is administered as described in *Administering Avaya Deskphone SIP for 9601/9608/9608G/9611G/9621G/9641G*.

Notes:

- See *Administering Avaya Deskphone SIP for 9601/9608/9608G/9611G/9621G/9641G* for more information about:
  - Administering other network equipment
  - Administering applications like firewalls
  - Information about topics like port utilization

Requirements to verify for each IP deskphone

❑ **9.** You have an extension number and a Communication Manager security code (password) for each applicable IP deskphone.

- ❑ **10.** You have an OPTIM extension number and an Communication Manager security code (password) for each deskphone, and have configured Session Manager for each deskphone.
- ❑ **11.** A Category 5e LAN jack is available at each deskphone site and a Category 5 modular line cable is available for connecting the deskphone to the Ethernet wall jack.
- ❑ **12.** Electrical power is provided to each deskphone by a deskphone power module (SPPOE or Single Port Power over Ethernet Injector), which must be ordered separately. For PoE Input connection, use only the Listed ITE equipment with PoE output. You do not require the power module if the LAN supplies IEEE-standard power (PoE) to the deskphone.
- ❑ **13.** A Category 5e modular line cord is available for the connection between the IP deskphone and the PC, if applicable.
- ❑ **14.** Verify that the SIP-based 9600 Series IP Deskphones models 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP Deskphone package includes the following components:
  - 1 deskphone set with dual position flip- or clip-stand.
  - 1 handset capable of transmitting and receiving 7KHz audio.
  - 1 H4DU 9-foot long (when extended) 4-conductor coiled handset cord, plugged into the deskphone and the handset.
  - An "Important Notice and Warning" page which provides the URL for the Avaya support site to download all other documentation.
- ❑ **15.** 9600 Series IP Deskphones, with the exception of 9601 IP deskphone, ship from the factory with H.323 software. Existing installations might also have many IP deskphones running H.323 software. For instructions on how to convert between H.323 and SIP software, see Converting software on the 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones.

Converting software on the 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones

The 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones are set to use the H.323 protocol by default. To use these deskphones in a SIP environment, after connecting the deskphones, you must ensure that those deskphones that will run under a SIP protocol are set up properly. This section describes how to determine what your deskphone signaling protocol is and then set or convert applicable deskphones from H.323 to SIP software.

Note:

The 9601 deskphone supports only the SIP signaling, therefore you do not require H.323 to SIP conversion for the 9601 IP deskphone.

There are three methods you can use to change the signaling protocol on all or selected deskphones:

- DHCP - As of SIP software Release 6.2, you can set the SIG parameter in the Site Specific Option #242.
  Setting SIG to "2" (SIP) in Option 242 and downloading the 96x1Supgrade.txt file as part of the SIP Software Distribution Package causes all deskphones to use the SIP protocol

upon power up and initialization. Once a deskphone is registered as SIP (through the SIG setting), it will always access and download the appropriate SIP upgrade files upon reboot or reregistration.
You can also set up a group of phones, then use the SIG parameter within that GROUP to change the SIG setting for that group. For more information, see The GROUP parameter on page 62.

- Settings file - You can also set the SIG parameter in the 46xxsettings file.
- From the deskphone - Use the Setting the signaling protocol identifier (SIG) Craft procedure to change a single deskphone. A value entered via the SIG Craft procedure takes precedence over a DHCP SIG setting and over a Settings file SIG setting when the Craft procedure is used to set SIG to a value of 1 (H.323) or 2 (SIP), but not if the craft procedure is used to set SIG to 0 (Default - H.323 or SIP, depending on the software distribution package residing on the file server). For H.323, which is the factory default setting, DHCP always takes precedence over SIG Craft procedures.

There are several H.323 to SIP or SIP to H.323 conversion scenarios, and each scenario depends on whether the majority of your deskphones are H.323 or SIP:

- **H.323-centric** - an environment where the majority of IP deskphones are and will remain running the H.323 software, but some deskphones will become SIP deskphones. In an H.323-centric environment, the appropriate H.323 deskphone software files (96x1Hupgrade.txt) must reside on a HTTP server and Avaya Aura® Communication Manager must be configured with the appropriate H.323 parameters. To convert an individual deskphone from H.323 to SIP, both Avaya Aura® Session Manager and Avaya Aura® Communication Manager must be configured with the appropriate SIP parameters. For more information on conversion instructions, see Table 1: H.323 to SIP and SIP to H.323 conversion chart.
- **SIP-centric** - an environment where the majority of your deskphones are or will become SIP deskphones running SIP software. In a SIP-centric environment, the 96x1Supgrade.txt file must reside on a HTTP server and both Session Manager and Communication Manager must be configured with the appropriate SIP parameters. To convert an individual deskphone from SIP to H.323, Communication Manager must be configured with the appropriate H.323 parameters. For more information on conversion instructions, see Table 1: H.323 to SIP and SIP to H.323 conversion chart.

What makes an environment H.323-centric or SIP-centric depends on the type of upgrade script files the environment is running (H.323 or SIP, see Downloading software upgrades on page 57) and the Signaling Protocol Identifier (SIG) parameter setting. The SIG parameter has three possible values:

- Default - either H.323 or SIP, set automatically for all deskphones depending on whether your environment is H.323-centric or SIP-centric as determined by the software package you downloaded and that resides on the file server.
- H.323 - manually set to H.323 for a specific deskphone by an installer or administrator according to the procedures in this section.
- SIP - manually set to SIP for a specific deskphone by an installer or administrator according to the procedures in this section.

Note:

For information about the SIG parameter, see “Choosing the Right Application File and Upgrade Script File” in A*dministering Avaya Deskphone SIP for 9601/9608/9608G/9611G/9621G/9641G*. For information on setting or changing the SIG parameter, see Setting the signaling protocol identifier on page 48.

Note:

The chart that follows describes converting individual deskphones to or from H.323 to SIP. As of SIP software Release 6.2, all or selected groups of deskphones can be converted by setting the SIG parameter to the desired value using DHCP Option #242 or by setting SIG to "2" (SIP) in the settings file.

Table 1: H.323 to SIP and SIP to H.323 conversion chart

Environment	To convert this type of deskphone	To this type of deskphone	Then
SIP-centric	H.323 factory set	SIP	No action is required because the Signaling Protocol Identifier (SIG) defaults to SIP. Upon power-up & network connection, the deskphone automatically downloads the proper SIP files from the file server.
SIP-centric	H.323 in use	SIP	For a single deskphone, perform the **SIG** Craft procedure to change the SIG parameter value from “**1**" (H323) to “**default**” (SIP). For information, see Setting the signaling protocol identifier on page 48. Save the SIG parameter change. The deskphone will reset if necessary to get the appropriate software.
SIP-centric	SIP	H.323	Perform the **SIG** Craft procedure to change the SIG parameter value from “**default**” to “**1**" (H323). For information, see Setting the signaling protocol identifier on page 48. Save the SIG parameter change. The deskphone will reset if necessary to get the appropriate software.
H.323-centric	H.323 in use	SIP	Perform the **SIG** Craft procedure to change the SIG parameter value from “**default**” to “**2**" (SIP).” For information, see Setting the signaling protocol identifier on page 48. Save the SIG parameter change. The deskphone will reset if necessary to get the appropriate software.

Table 1: H.323 to SIP and SIP to H.323 conversion chart (continued)

Environment	To convert this type of deskphone	To this type of deskphone	Then
H.323-centric	H.323 factory set	SIP	Connect the deskphone to a power source and to the network. Press the **Program** softkey as soon as it displays in the first softkey position to access the **Craft Access Code Entry** screen. Perform the **SIG** Craft procedure and change the value from "**default**" to "**2"** (SIP). Save the SIG parameter change. The deskphone will reset if necessary to get the appropriate software.
H.323-centric	SIP	H.323	Perform the **SIG** Craft procedure to change the SIG parameter value from "**2"** (SIP) to "**default**" (H323). For information, see Setting the signaling protocol identifier on page 48. Save the SIG parameter change. The deskphone will restart if necessary to get the appropriate software.

Assembling the deskphone

CAUTION:

Be careful to use the correct jack when plugging in the deskphone. The jacks are located on the back of the deskphone housing and are flanked by icons to represent their correct use.

Powering the IP deskphone

The 9601, 9608, 9608G, 9611G, 9621G, and 9641G deskphones support IEEE 802.3af-standard LAN-based power. Before installing a 9601, 9608, 9608G, 9611G, 9621G, or 9641G deskphone, verify with the LAN administrator whether the LAN supports IEEE 802.3af, and if so, whether the deskphone should be powered locally or by means of the LAN.

When you add devices like multiple button modules, all of which must be the same model type, to applicable IP deskphones, the power class might change.

Note:

The 9601 and 9621G IP deskphones do not support button modules.

Table 2: Impact of additional devices on deskphone Power over Ethernet (PoE) class shows the effect of button module additions on the power class and indicates how to set the IEEE power switch on the back of the deskphone to accommodate different power needs.

Note:

The 9621G is a PoE Class 1 device with a 10/100 switch and does not have an IEEE power switch.

Table 2: Impact of additional devices on deskphone Power over Ethernet (PoE) class

Phone Model	Default PoE (Class "L" on IEEE switch)	One BM12 (IEEE switch setting)	Two BM12's (IEEE switch setting)	Three BM12's (IEEE switch setting)	One SBM24 (IEEE switch setting)	Two SBM24's (IEEE switch setting)	Three SBM24's (IEEE switch setting)
9608/ 9608G	Class 1	L	L	H	L	H	H
9611G	Class 1	H	H	H	H	H	H
9641G	Class 2	L	L	L	L	L	H

Important:

The last step in assembling the deskphone **must** be applying power. Apply power either by plugging the power cord into the power source (local powering) or plugging the modular line cord into the Ethernet wall jack (IEEE powering).

CAUTION:

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

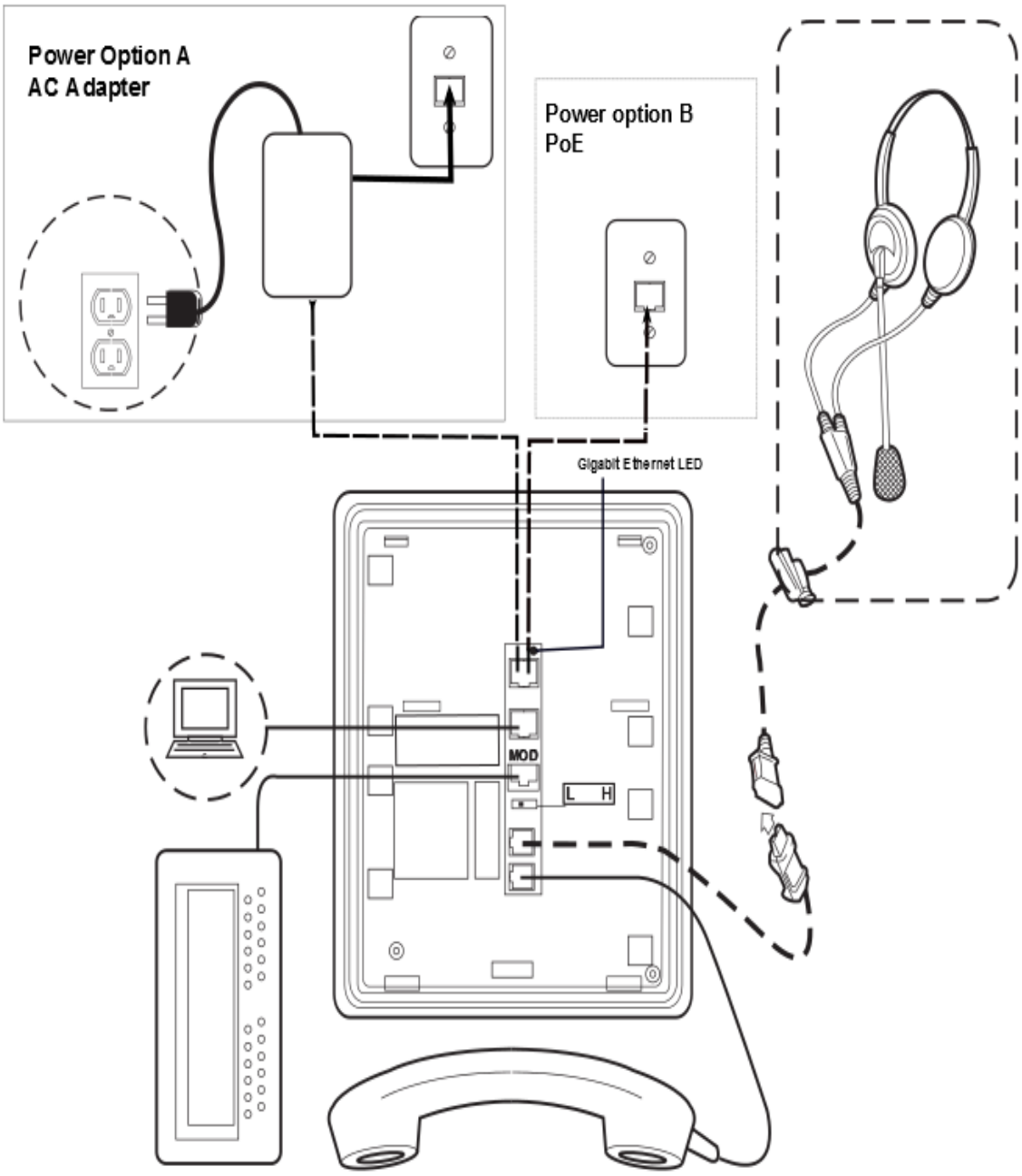
Figures 1 and 2 provide illustrations to connect cords to jacks on the deskphones covered in this guide. Use the illustrations and associated procedures as appropriate for deskphone assembly.

Deskphone model	See
9608,9608G, or 9611G	Figure 1: Connection jacks on a 9608, 9608G, or 9611G deskphone
9621G or 9641G	Figure 2: Connection jacks on a 9621G or 9641G deskphone

Note:

Deskphone models 9608G, 9611G, 9621G, and 9641G accommodate an external GigE (Gigabit Ethernet) adapter. Installation options for those devices are not shown in the illustrations that follow, but are available on the Avaya support website.

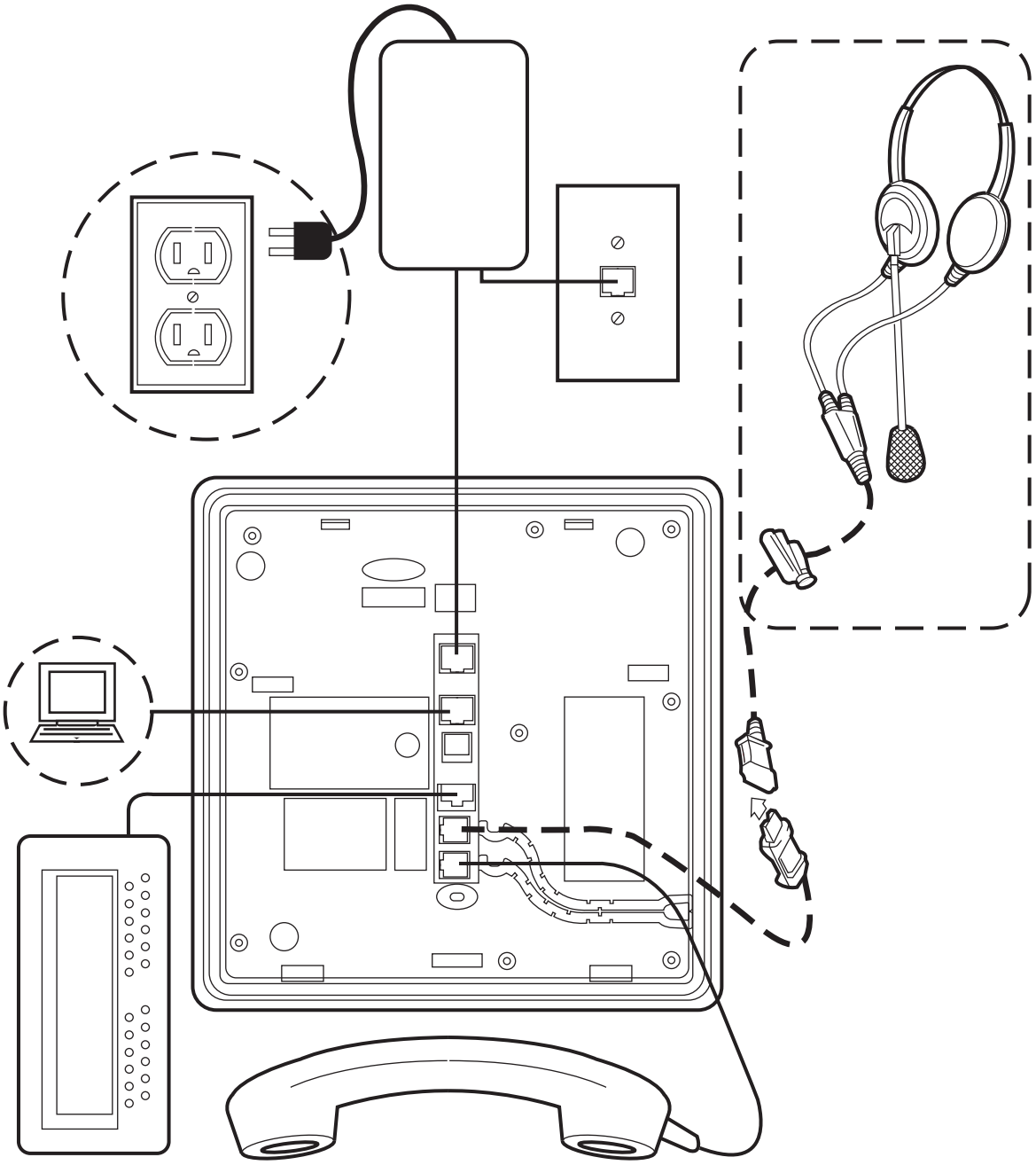
Figure 1: Connection jacks on a 9608, 9608G, or 9611G deskphone



Note:

The Gigabit Ethernet LED indicator is applicable only to the 9608G IP deskphone. This indicator lights up steady green when a link of any speed is established, blinks with any network activity, and turns off upon the loss of network connectivity.

Figure 2: Connection jacks on a 9621G or 9641G deskphone



Note:

The 9621G deskphone does not have a module port to support a button module.

1. Plug one end of the H4DU 4-conductor coiled handset cord into the deskphone and the other end into the handset.
2. Plug one end of the first Category 5e modular line cord into the Ethernet jack of the PC and the other end into the secondary Ethernet jack on SIP-based 9600 Series IP Deskphones, if appropriate.
3. To power the deskphone through IEEE-standard power (PoE), plug one end of the second Category 5e modular line cord into the Ethernet jack on the deskphone. Plug the other end of this cord into the Ethernet wall jack.
4. To power the deskphone locally, connect the cord provided with the power module (Single Port PoE Injector or SPPOE-1A) into the Ethernet jack on the phone. Note that the cord must be installed such that the end containing the ferrite EMI filter is closest to the deskphone. Plug the other end of this cord into the SPPOE-1A power injector jack labeled **DATA & POWER OUT**. Take another cord and plug it into the SPPOE-1A power injector jack labeled **DATA IN**. Plug the other end of this cord into the Ethernet wall jack. Finally, connect the SPPOE-1A to an AC power source.

Power-Up and Reset Operation (Dynamic Addressing Process)

Important:

Before starting this process, read Converting software on the 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones on page 14 to understand the requirements for converting factory-set H.323 deskphones to SIP and make any changes necessary to suit your particular environment. Also, ensure that both Avaya Aura® Communication Manager and Avaya Aura® Session Manager are properly set up for your environment.

Note:

Before starting this process you must have an OPTIM extension number for the SIP deskphone, the Communication Manager security code (password), and a login and password on the Session Manager server.

Any reference to the HTTP server applies equally to an HTTPS server.

The initial display messages, some of which are part of DHCP give a "power on" indication and dynamic feedback as the deskphone initializes. The intent of these messages is to reassure the

user that the phone is active and has not "locked up," and to provide useful information about the status of network, server or downloading operations before the availability of dial tone.

Initialization

The following process describes the software architecture as well as providing a high-level overview of how the deskphone is expected to operate during startup and software upgrades. This is by no means a comprehensive description of all of the internal tasks performed during startup.

Files are stored in five areas of reprogrammable non-volatile (flash) memory in the deskphones:

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

Two Kernel/Root File Systems are supported in case one becomes corrupted, but only one is activated when the deskphone powers up or resets. Temporary Storage is used to store a new Signed Application/Library Software Package that has been downloaded by the current application until it can be installed by a process in the active Kernel/Root File System after the next reset.

When a deskphone starts up, the boot programs check the kernel or the root file system to ensure that the files are not corrupted. If the file system is not corrupted, the programs transfer 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, it is marked as the one to be activated, the value of RFSINUSE is set to the name of the Signed Kernel/Root Software Package that was used to install that file system, and control is transferred to a process in it. If both Kernel/Root File Systems are corrupted, the deskphone will not operate and must be returned for repair.

A process in the active Kernel/Root File System first checks whether a Signed Application/Library Software Package is stored in Temporary Storage, and if it finds one, it installs the Application Software Package and/or the Library Software Package if either has a different file name than the currently installed version, replacing the existing corresponding files in the Application File System. The copy of the Signed Application/Library Software Package stored in Temporary Storage is then deleted. If a Signed Application/Library Software Package is not found in Temporary Storage, the process checks the integrity of the application files, and if they are corrupted, the process installs files from the Backup Package, replacing the corrupted application files in the Application File System. Any time an Application Software Package or a Library Software Package is installed, the value of the persistent parameter APPINUSE is set to the file name of the Signed Application/Library Software Package from which it 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. 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, starting 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 a Signed Software Package (which can contain either Kernel and Root Software Packages or Application and Library Software Packages) is downloaded, it is initially stored in volatile memory (RAM). Other downloaded files (such as Language Files and Certificate Files) are installed 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 deskphone. If it is invalid, the package is deleted. If it is valid, the signature of the Software Packages 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/Root Software Package, the Kernel Software Package and/or the Root File System Software Package is installed if either has a different file name than the currently installed version, replacing the existing corresponding files in the Kernel/Root File System that was not active during startup (a Root File System Software Package may also install new boot programs in the boot program area), that Kernel/Root File System is marked as the one to be activated after the next power-up or reset, and the value of the persistent parameter RFSINUSE is set to the file name of the Signed Kernel/Root Software Package that was installed.

Finally, if a new Signed Kernel/Root Software Package was installed, the deskphone will reset to activate the new Kernel/Root File System, which will install a new Signed Application/Library Software Package as described above if one has been stored in Temporary Storage. If a new signed Kernel/Root Software Package was not installed, the deskphone application attempts to register with a call server.

Power-Up and Reset process

When you plug the deskphone set into the Ethernet wall jack and apply power, if applicable, the following process takes place.

Note:

If the application has already been downloaded, the whole process takes approximately 1 to 2 minutes after the deskphone is plugged in. For software upgrades, including the Kernel/Root file and the application file download, the process might take 5 - 10 minutes. The duration is based on LAN loading, how many deskphones are being installed at once, and similar factors.

Do not unplug the power cord during the upgrade process.

1. The deskphone checks for the language file is use. If null, the deskphone displays English text strings.
2. The boot programs check the Kernel/Root File System that has previously been marked as the one to be activated to ensure that it has not become corrupted, and if it has not, 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, it is marked as the one to be activated, the MIB value endptRFSINUSE is set to the name of the Signed Kernel/Root Software Package that was used to install that file system, and control is transferred to it. If both Kernel/Root File Systems are corrupted, processing halts. The software checks whether a Signed Application/Library Software Package has been previously downloaded, and if one is found, the Application Software Package and/or the Library Software Package is installed if either has a different file name than the currently installed version, replacing the existing corresponding files in the Application File System. The downloaded Signed Application/Library Software Package is then deleted. If a new Signed Application/Library Software Package is not found, the integrity of the application files is checked. If they are corrupted, files from the Backup Package are installed, replacing the corrupted files in the Application File System. Any time an Application Software Package or a Library Software Package is installed, the MIB value endptAPPINUSE is set 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 loading the application files into volatile memory and as control is transferred to them, the MIB value endptAPPINUSE is displayed on the bottom text line.
3. The internal clock/calendar is set to 0:00:00 Saturday, January 1, 2000 and started.
4. The deskphone activates the Ethernet line interface, the PC Ethernet jack, and dial pad input to allow the invocation of procedures. The activation occurs as soon as possible after power-up or a reset.

   The deskphone displays the speed of the Ethernet interface in Mbps, that is, 10, 100, or 1000. The message No Ethernet displays until the software determines whether the interface is 10 Mbps, 100 Mbps, or 1000Mbps.

Note:

The Ethernet speed indicated is the LAN interface speed for both the deskphone and any attached PC, assuming the administrator has not disabled the latter interface by a PHY2STAT setting.

Important:

Pressing the **Program** softkey at any time during startup invokes the Craft Access entry procedure to allow manual settings, but only if the PROCSTAT (local dialpad procedure status) system value is “0” providing full access to local procedures or if PROCSTAT is “1” in certain instances requiring input. For information, see Chapter 3: Local administrative options. If Craft procedures are invoked, the startup process terminates. The **Program** softkey also displays in conjunction with a message describing a processing conflict, for example, when an ARP response indicates a conflict in obtaining the IP Address.

5. The deskphone sends a request to the DHCP server and invokes the DHCP process.

   The following message displays:

   ```
   DHCP: s secs
   ```

   where ***s*** is the number of seconds that have elapsed since DHCP was invoked.

6. VLAN verification and tagging occur. The following message displays:

   ```
   VLAN ID = n
   ```

   where ***n*** is the VLAN ID being used.

7. Determination of the DHCP protocol (IPv4 is done, and the applicable parameters enabled.)

   The DHCP server provides IP Addresses for the following hardware:

   The 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphone

   The HTTP/HTTPS server

   The SIP Proxy server

8. Using the list of gateway IP Addresses provided by the DHCP server, the deskphone performs a router check and verifies that the router is on the same subnet as the IP Address. The deskphone cycles through the gateway IP Addresses with ARPs or pings until it receives a response. When the router is located, received LLDP TLVs are processed. Then the HTTP process starts.

   Note:

   Any change in VLAN-related configuration parameters resulting from LLDP triggers a deskphone reset.

9. The HTTP process starts with an `HTTP GET` command, which displays on the deskphone’s Status Line.

Note:

Pressing the **Program** softkey at any time during startup invokes the Craft Access entry procedure to allow manual settings, but only if the PROCSTAT (local dialpad procedure status) system value is “0” providing full access to local procedures or if PROCSTAT is “1” in certain instances requiring input. For information, see Chapter 3: Local administrative options. If Craft procedures are invoked, the startup process terminates. The **Program** softkey also displays in conjunction with a message describing a processing conflict, for example, when an ARP response indicates a conflict in obtaining the IP Address.

10. When connected, the deskphone looks for an upgrade script file.
11. The deskphone sends and identifies an upgrade script, gets the settings file, the language file, and any firmware updates.

    Note:

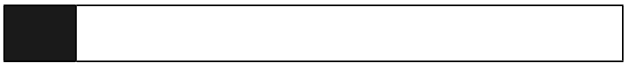
    The GET message might have to be sent several times. Each time the GET message is sent, the URI for the current HTTP request displays the SIG parameter value. The SIG parameter value determines the signaling protocol (H.323, SIP, both) and is used to determine the proper upgrade file that is downloaded. If the SIG parameter was manually set using the local administrative (Craft) SIG procedure, that value has precedence over a SIG setting in a configuration file. A change in the SIG value may require a reset so that a new or different upgrade file can be downloaded to the phone.

12. When the deskphone determines that the application file received is valid, the following message displays:

    ```
    File Obtained;please wait...
    s secs
    ```

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

13. While the application file is saved in flash memory, a progress bar shows the status:

14. The deskphone checks for LLDP messages and re-checks VLAN status and tagging. If LLDP causes a change in the values of L2Q or L2QVLAN, a reset occurs to obtain a new IP address.
15. If applicable, the deskphone attempts to download a valid device certificate using simple certificate enrollment protocol (SCEP).

Simple Certificate Enrollment Protocol (SCEP)

1. When SCEP is initiated the deskphone attempts to contact an SCEP server via HTTP, using the value of the configuration parameter MYCERTURL as the URI. The HTTP connection is established to the transport address specified by the value of the configuration parameter

HTTPPROXY if HTTPPROXY is not null and if the configuration parameter HTTPEXCEPTIONDOMAINS is null, or if HTTPEXCEPTIONDOMAINS is not null and the rightmost part of the domain portion of MYCERTURL does not match one of the values of HTTPEXCEPTIONDOMAINS. The values of the configuration parameters MYCERTKEYLEN, MYCERTCN, MYCERTDN are used in the certificate request.

2. While the deskphone is attempting to contact the SCEP server to obtain a certificate, the Title Line displays:

```
SCEP: In progress...
s secs
```

   where ***s*** is the number of seconds since SCEP was initiated.

3. If the initial attempt to contact the SCEP server is not successful the deskphone continues with start-up, and will not try to contact the SCEP server again unless it is reset or power-cycled.
4. If a connection to the SCEP server is successfully established, if the value of the configuration parameter MYCERTWAIT is 1, SCEP remains in progress until the request for a certificate is granted or rejected.
5. If the request for a certificate is granted, ***SCEP: Successful*** displays on the Title line for at least one second, and remains until it is replaced by a subsequent display.
6. The SCEP server connection terminates, and the deskphone continues with start-up. If the request for a certificate is rejected ***SCEP: Failed*** displays on the Title line for at least one second, and remains until it is replaced by a subsequent display. In this case, the SCEP server connection terminates and the deskphone continues with startup.
7. if the value of the configuration parameter MYCERTWAIT is 0 (zero), SCEP remains in progress until the request for a certificate is granted or rejected or until a response is received indicating that the request is pending for manual approval. If the request for a certificate is granted or rejected, the same text will be displayed as specified above.
8. If a response is received indicating that the request is pending for manual approval, ***SCEP: Pending*** displays on the Title line for at least one second and remains until it is replaced by a subsequent display. The connection to the SCEP server is terminated, and the deskphone continues with startup. The deskphone periodically attempts to contact MYCERTURL as specified above (but in the background without displaying any message) until the request is granted or rejected.
9. If a device certificate and private key are successfully downloaded, they are saved in non-volatile memory along with the MYCERTURL value used to obtain them.
10. When the point in time is reached at which the percentage of the interval of time specified in the device certificate's Validity object corresponding to the value of the configuration parameter MYCERTRENEW has elapsed, the deskphone periodically attempts to contact MYCERTURL as specified above (but in the background without displaying any message) to renew the certificate, until the renewal request is granted or rejected.

Registration and Login

1. Upon successful initialization and power-up, the 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones display the Login screen with the prompt to enter the user name.
2. Enter the user name or the ID assigned to the deskphone.
3. Enter the password and press **Enter**.

   The extension is visible during entry but the password displays as asterisks. The system determines whether the extension is in use.
4. The deskphone initiates SIP registration with the proxy server. The deskphone attempts to register to the SIP proxy server at the address in the SIP_CONTROLLER_LIST parameter using the user name and password provided during the login process. It also uses the SIPDOMAIN parameter. SIP_CONTROLLER_LIST provides a list of server addresses. The deskphone attempts to simultaneously register to the number of servers in the SIMULTANEOUS_REGISTRATIONS parameter. Also, the deskphone does not reboot when there is no server provisioned or the provisioned server cannot be contacted. The deskphone waits for a register response message. If no message is received before the end of the WAIT_FOR_REGISTRATION_TIMER interval, registration is retried. After every successful registration:
   - REUSE_IPADD will be set to the value of IPADD,
   - REUSE_NETMASK will be set to the value of NETMASK,
   - REUSE_ROUTERS will be set to the value of ROUTERS,
   - REUSE_ROUTER_IN_USE will be set to the value of ROUTER_IN_USE,
   - REUSE_TAGGING will be set to the value of TAGGING,
   - REUSE_L2QVLAN will be set to the value of VLAN_IN_USE, and
   - the MIB object endptVLANLIST will be set to the value of VLANLIST, and then the value of VLANLIST will be set to null.
5. The deskphone contacts PPM, logs in, and downloads the configuration file while displaying:

   Logging in

   All PPM requests include a handle element of the form:

   <handle>userhandle@domain</handle>
   where *userhandle* has the value of parameter SIP_USER_ID and domain has the value of parameter SIPDOMAIN.

   Note:

   Successful completion of this process displays the dial plan, any administered features, and any administered contacts. To test the dial plan, access an outside line and get the dial tone.

Chapter 3: Local administrative options

Introduction

During installation or after you have successfully installed a 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP Deskphone, you might be instructed to administer one of the manual procedures described in this chapter. These local administrative procedures are also referred to as Craft Procedures.

Note:

You can modify the settings file to set parameters for deskphones that download their upgrade script and application files from the same HTTP server. See Chapter 4: Maintaining the 9601, 9608, 9608G, 9611G, 9621G, and 9641G IP deskphones. Only trained installers or technicians must perform local (craft) 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 than if they are administered dynamically. Values assigned to options in static administration are not changed by upgrade scripts. These values remain stored in the deskphone until you use the local administrative procedures CLEAR or RESET.

Use these option-setting procedures only with static addressing and, as always, only if instructed by the system or LAN administrator. Do not use these option-setting procedures if you are using DHCP. DHCP is the Dynamic Addressing Process, as indicated in Power-Up and Reset Operation (Dynamic Addressing Process) on page 22.

Accessing the local or the Craft procedures

The Local or the Craft procedures can only be invoked if the value of the PROCSTAT parameter in the settings file is set to 0. Setting the PROCSTAT parameter to 0 provides full access to the local procedures.

Note:

The default password to gain access to the local procedures menu is set in PROCPSWD parameter. The factory-set default password is **27238**. You must not change the default value at the time of initial installation.

During deskphone startup:

1. During startup, invoke local procedures by pressing **Program** to display the Craft Access Command Entry screen.
2. Enter the local dialpad procedure password (0 to 7 numeric digits), as specified by the system administrator in the PROCPSWD parameter.
3. Press the **Enter** softkey.
4. For all non-touchscreen phones, use the navigation arrows to scroll to and highlight the local procedure you want, then press **Select** or **OK**. Or scroll to the procedure you want and press the corresponding line button. For touchscreen 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.

Note:

The phone restarts after exiting the craft menu.

During normal deskphone operation:

1. Invoke all local procedures by pressing **Mute**, entering the local (dialpad) procedure password (0 to 7 numeric digits), then pressing #.

   A 6-second timeout is in effect between button presses after pressing **Mute**. If you do not press a valid button within 6 seconds of pressing the previous button, the collected digits are discarded. In this case, no administrative option is invoked.
2. For non-touchscreen phones, use the navigation arrows to scroll to and highlight the local procedure you want, then press **Select** or **OK**. Or scroll to the procedure you want and press the corresponding line button. For touchscreen 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.

Entering data for administrative options

This section applies to all 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones and describes how to enter data for administrative options.

1. With the exception of a touchscreen deskphone, the first application line on any screen is automatically highlighted (selected) when the deskphone displays the screen. To select the item on that line, press the appropriate softkey at the bottom of the screen, for example, **Change**, **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 touchscreen deskphone, touching the desired line produces the same result.
2. Attempts to enter invalid data are rejected and the deskphone emits an error beep.
3. If you enter a numeric digit that causes the IP Address or subnet mask value to exceed 255, or any value to exceed its maximum field value, the deskphone plays an error beep tone. The deskphone ignores the digit entered when the error tone was played, and the cursor does not move forward.
4. If you enter a numeric digit for a value or for an IP Address or subnet mask field after entering only a zero, the new digit replaces the zero.
5. To move the cursor backwards to remove a character, press the **Bksp** softkey. When you press the backspace key, the most recently entered digit or period is erased from the display. The cursor remains in the erased character's former position.
6. The **More** softkey provides data entry options like symbols, all capital letters for text, numerals, etc.
7. Pressing **Back** or **Exit** (or touching that softkey for a touchscreen deskphone) exits the local procedures. Any changes require a deskphone restart. Otherwise, the deskphone re-displays whatever had been displayed when the Craft Local Procedures were invoked. If no 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 option was invoked.

   Note:

   If **PROCSTAT** has been administered to **1**, you will not be able to invoke any administrative options other than **V I E W**.

   The touchscreen deskphones present an onscreen keyboard that allows you to "type" the data you want to enter on the deskphone. See the applicable user guide for information about using the onscreen keyboard.

About local administrative procedures

Craft procedures allow you to customize the IP deskphone installation for your specific operating environment on a deskphone-by-deskphone basis. 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:

When running a local (Craft) procedure from the 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 (button-based) IP deskphones.

Unless otherwise prohibited using administration, a user can view but not change most of the parameters associated with Craft procedures. For more information, see the applicable users guides.

Shown As	Craft Procedure Purpose	See
802.1X	Set the 802.1X operational mode	Setting the 802.1X operational mode on page 35.
ADDR	Network Address information programming	Installing static addressing on page 37.
AGC	Enable/disable Automatic Gain Control	Enabling and disabling Automatic Gain Control on page 39.
CALIBRATION	Calibrate the touchscreen (9621G and 9641G models only)	Calibrating the touch screen on page 39.
CLEAR	Clear all values to factory defaults	Using the Clear procedure on page 40.
DEBUG	Enable/disable Debug Mode	Enabling and disabling Debug Mode on page 41.
GROUP	Set the Group Identifier	Setting the Group identifier on page 42.
HANDSET EQ	Set the handset equalization.	Setting handset audio equalization on page 44.
INT	Network Interface Control	Setting interface control on page 44.
LOG	Enable/disable Event Logging	Enabling and disabling event logging on page 45.
LOGOUT	Log off the deskphone	Logging out on page 47.

Shown As	Craft Procedure Purpose	See
RESET VALUES	Reset system initialization values to defaults	Resetting system values on page 47.
RESTART PHONE	Restart the deskphone	Restarting the deskphone on page 48.
SIG	Set the signaling protocol download flag	Setting the signaling protocol identifier on page 48.
SIP	Configure SIP call settings	Configuring SIP settings on page 49.
SNTP	Configure the time server settings	Configuring Time Server settings on page 51.
SSON	Set the Site-Specific Option Number	Setting Site-Specific Option Number on page 52.
VIEW	View current parameter values and file names	Using the View administrative option on page 53.

Setting the 802.1X operational mode

Important:

The DOT1X configuration parameter must be set to “0” or “1” for the deskphone to support 802.1X pass-thru and the DOT1XSTAT configuration parameter must be set to “1” or “2” for the deskphone to support supplicant operation. For more information, see the *Administering Avaya Deskphone SIP for 9601/9608/9608G/9611G/9621G/9641G*.

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

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select 802.1X from the Admin Procedures screen, the two settings shown represent the text strings associated with the current configuration parameter values of DOTIX (802.1X Pass-Thru Mode) and DOT1XSTAT (802.1X Supplicant Mode), defined as follows:

   For the Pass-thru mode:

   - “On” if DOT1X = 0
   - “Pass-thru mode + on & proxy logoff” if DOT1X = 1

- “Off” if DOT1X = 2

For the Supplicant:

- “Off” if DOT1XSTAT = 0
- “On” if DOT1XSTAT = 1
- “On with multicast” if DOT1XSTAT = 2

3. To change the setting, select the line you want to change and press the **Change** softkey or the Right (or Left) navigation arrow to cycle through the settings.
4. Press **Save** to store the new setting and redisplay the Craft Local Procedure screen.

Note:

The deskphone restarts if you make any change to the 802.1X data.

Preinstallation checklist for static addressing

Before performing static programming of address information, verify that all the requirements listed in Verify these network requirements on page 13 are met. You do not have to consider item 4 in this list, as it refers to the DHCP server. In addition, you must have the values for the following parameters. Failure to do so can cause data entry errors that prevent the deskphone from working. Such errors can also have a negative impact on your network. Print copies of this checklist for each subnet.

- ❑ **1.** The IP Address of the deskphone.
- ❑ **2.** The IP Address of the router.
- ❑ **3.** The IP subnet mask.
- ❑ **4.** The IP Address of the HTTP and/or /HTTPS server.
- ❑ **5.** The IP Address of the DNS Server.
- ❑ **6.** The VLAN ID (the L2QVLAN value).
- ❑ **7.** The VLANTEST value.

Installing static addressing

The usual way to assign IP Addresses to 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones is the automatic method described in Power-Up and Reset Operation (Dynamic Addressing Process) on page 22. There might be times, however, when manual assignment of IP Addresses is desired.

CAUTION:

Static addressing is necessary when a DHCP server is unavailable.

Because of the increased opportunities for text entry errors associated with static addressing, Avaya strongly recommends that a DHCP server be installed and static addressing avoided.

Use the following procedure to invoke manual address information programming.

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **ADDR** from the Admin Procedures screen, the deskphone displays the Static Addressing Local Procedure screen.The following table lists the fields that you can use to enter the required information.

Static Addressing screen		Line Description and (Configuration Parameter Value)
Use DHCP	***Yes***	Yes or No (USE_DHCP)
Phone	***nnn.nnn.nnn.nnn***	Deskphone IP Address (IPADD)
Router	***nnn.nnn.nnn.nnn***	Router in use; gateway/router IP Address(es) (ROUTER)
Mask	***nnn.nnn.nnn.nnn***	IP network mask (NETMASK)
HTTPS File Server	***nnn.nnn.nnn.nnn***	IP Address of HTTPS File Server (TLSSRVR)
HTTP File Server	***nnn.nnn.nnn.nnn***	IP Address of the HTTP File Server (HTTPSSRVR)
DNS Server	***nnn.nnn.nnn.nnn***	DNS server IP Address(es) (DNSSRVR)
802.1Q	***0=auto, 1=on, 2=off***	(L2Q)
VLAN ID	***dddd***	(L2QVLAN)
VLANTEST	***ddd***	Number of seconds to wait for a DHCP offer (VLANTEST)
Host to ping	***nnn.nnn.nnn.nnn or AVohhhhhh***	IP Address or DNS Name

where:

- ***nnn.nnn.nnn.nnn*** is the current IP Address associated with the specific address information to its left, which could be either a value previously set by a technician, or the original IP Address value if no previous change was made,

- ***dddd*** is the current value of L2QVLAN and ***ddd*** is the current value of VLANTEST, respectively.
- ***AVohhhhhh*** where ***o*** has one of the following values based on the OID (first three octets) of the deskphone's MAC address:
  - "A" if the OID is 00-04-0D,
  - "B" if the OID is 00-1B-4F,
  - "E" if the OID is 00-09-6E,
  - "L" if the OID is 00-60-1D,
  - "T" if the OID is 00-07-3B, and
  - "X" if the OID is anything else, and

  where ***hhhhhh*** are ASCII characters for the hexadecimal representation of the last three octets of the deskphone's MAC address

3. Use the navigation arrows to scroll to and highlight the address/item you want to change, then use the appropriate softkey(s) and the dialpad to change the value as described in Step 3.
4. Depending on the item you selected, choose one of the following:

If you want to	Then
Change any of the IP Address values (File, Phone, Router, Subnet Mask, &/or DNS Server)	Use the dialpad to enter the new IP Address. IP Addresses have four sets of three digits followed by a period. Pressing ***** following entry of three digits causes a period to be placed in the next position, and the cursor to advance one position to the right. For example, to enter the IP Address 111.222.333.444, press the 1 on the dialpad three times then press *****, press the **2** on the dialpad three times then press *****, press the 3 on the dialpad three times then press *****, then press the 4 on the dialpad three times. Proceed to the next step.
Change the VLAN ID value	Use the dialpad to enter the new static VLAN ID of from 0 to 4094, inclusive. Proceed to the next step.
Change the VLANTEST value	Use the dialpad to enter the new value of the **DHCPOFFER** wait period of from 0 to 999, inclusive. Proceed to the next step.
Ping a server (host) to see if it is reachable/ available	Use the dialpad to enter the IP Address or the DNS Name of the server you want to check. IP Addresses have four sets of three digits followed by a period. Pressing ***** following entry of three digits causes a period to be placed in the next position, and the cursor to advance one position to the right. Press the **Ping** softkey to initiate the check. The deskphone sends four pings and displays the results in a text block screen. If the ping fails, the message "Unable to contact host" displays.

5. Press **Save** to store the new setting and redisplay the Admin Procedures screen or **Cancel** to return to the Admin Procedures screen without saving the value entered. Or, if you sent a ping to the host server, press **OK** to return to the Static Address screen.

   Once the new values are stored, the deskphone is reset.

   If a new boot program is downloaded from the HTTP/HTTPS server after you enter static addressing information, you must reenter your static addressing information.

Enabling and disabling Automatic Gain Control

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

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **AGC** from the Admin Procedures screen, the following text displays:

Handset AGC	***On***
Headset AGC	***On***
Speaker AGC	***On***

   where, the setting shown is the text string associated with the current system value of AGCHAND, AGCHEAD, or AGCSPKR, defined as:

   - “On” if the respective AGC*XXXX* system value is “1”.
   - "Off" if the respective AGC*XXXX* system value is “0”.
3. To change the setting, select (highlight) the appropriate line and press the **Change** softkey or the **Right** or **Left** navigation arrow to toggle the selected setting from On to Off or vice versa.
4. Press **Save** to store the new setting(s), update the associated system value(s), and redisplay the Admin Procedures screen.

Calibrating the touch screen

Screen calibration properly aligns the touch screen but should only be used for a significant problem with the touch screen.

Important:

Use a pencil, a pen, or a stylus rather than 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 affect factory-set calibration data. Use the **Default** softkey to restore factory-set calibration. Calibration results are not saved as part of a backup.

To calibrate the touch screen, use the following procedure:

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select CALIBRATE SCREEN from the Admin Procedures screen, the deskphone displays three softkeys - **Start**, **Default**, and **Cancel**.
3. Take one of the following actions:

- Touch **Cancel** to return to the Admin Procedures screen without calibrating the screen.
- Touch **Default** to reset the calibration parameters to the factory-set values, as evidenced by a confirmation tone and redisplay of the Craft Local Procedure screen.
- Touch **Start** to calibrate the screen. A calibration target (+) appears at a particular point on the screen. Proceed to the next step.

4. Touch the center of the target with the stylus as soon as it appears.

   The target disappears, and a new target appears in a different part of the screen.

5. Touch the center of each target with the stylus within 10 seconds of its appearance.

   After all four targets have been touched, the deskphone plays a confirmation tone and displays a "Calibration successful" message.

6. Touch **Save** to return to the Craft Local Procedure screen. When you touch Save, the system saves the calibration data and restarts the phone to put the new calibration data into effect. Calibration results are stored in the deskphone’s non-volatile memory.
7. Touch **Cancel** at any time to return to the Craft Local Procedure screen without completing the touch screen calibration.

Using the Clear procedure

Sometimes, you might want to remove all administered values, user-specified data, and option settings. Essentially, you want to return a deskphone to its initial “clean slate” or out of the box condition. This is usually done following deskphone repair or when passing a deskphone to a

new, dedicated user when the **LOGOUT** 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, file server and call server programming, and user settings, and restores all such data to default values. This option does not affect the software load. If you have upgraded the deskphone, the deskphone retains the latest software. Once you have cleared a deskphone, you can administer it normally.

CAUTION:

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

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

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **CLEAR** from the Admin Procedures screen, the deskphone displays a confirmation screen.
3. If you do not want to clear all values, press **No** to terminate the procedure and retain the current values. Press **Yes** to clear all values to their initial default values.

   The deskphone displays the following text:

   ```
   Clearing values.
   ```

   The deskphone is cleared to its “out of the box” state, resetting the following values to their factory defaults:

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

   After clearing the values, the deskphone resets.

Enabling and disabling Debug Mode

Note:

The DEBUG option is available only if you change the default Craft password to some other value through the PROCPSWD parameter.

Use the following procedure to turn the debug mode for the button module serial port on or off.

CAUTION:

A DEBUG setting of “On” disables any button module plugged into the MOD jack on the underside of the deskphone.

1. Use the Craft password to gain access to the Admin Procedures screen.
2. When you select **DEBUG** from the Admin Procedures screen, the following text displays:

Debug Mode	On

where the setting shown is the text equivalent of the current numeric value assigned to the DEBUG_ENABLED parameter, defined as:

- “On” if DEBUG_ENABLED is 1.
- “Off” if DEBUG_ENABLED is 0.

3. Use the navigation arrows or press **Change** to toggle between the options.
4. Press **Save** to store the new setting.

   The deskphone saves the new value.

Note:

Restart the deskphone for the DEBUG settings to take effect.

Setting the Group identifier

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 The GROUP parameter on page 62.

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **GROUP** from the Admin Procedures screen, the following text displays:

```
Setting:
```

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

3. Enter a valid **Group** value (0-999).

Note:

Any changes that you make to the Group value results in the restart of the deskphone when you exit the Craft menu.

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

Administering audio equalization

The Federal Communication Commission (a branch of the US Government) in its Part 68 standard, has made Hearing Aid Compatibility (HAC) a mandatory requirement. The HAC feature is an alternative way to provide audio equalization on a handset, from the acoustic standards specified in TIA-810/920 and S004, and may be of benefit to some users of t-coil capable hearing aids.

Release 6.2 onwards, the 9600 Series IP deskphones support the ability to choose either of these standards. Because individual organizations and users differ in how they might want to implement this choice, the deskphone provides 3 ways to specify the desired audio equalization:

- **Settings File:** The administrator can set ADMIN_HSEQUAL. The default value, 1, specifies Handset equalization that is optimized for acoustic TIA 810/920 performance unless otherwise superseded by Local Procedure or User Option. The alternate value, 2, specifies HAC.
- **Local Procedure:** When users are denied access to Options for administrative reasons, but individual users need an equalization value other than the one in the settings file, the HSEQUAL Craft Procedure provides another method to administer the deskphone with the audio equalization value that you require. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**. “Default” uses the settings file value unless superseded by User Option. “Audio Opt.” is optimized for TIA-810/920 acoustic performance, and “HAC Opt.” is optimized for HAC telecoil performance.
- **User Option:** The user can select “Default” by which the deskphone uses the settings file value (unless superseded by Local Procedure), “Audio Opt.” which uses Handset equalization that is optimized for acoustic TIA 810/920 performance, or “HAC Opt.” which uses Handset equalization that is optimized for electrical FCC Part 68 HAC telecoil performance.
- Handset equalization options are effected in the following order:

  a. The deskphone uses the User Option value if selected and saved.

  b. If a Local Procedure value was selected and saved, the deskphone uses the local procedure value.

  c. If a Settings file value is specified and saved the deskphone uses that value.

  d. If none of the above options are set, the deskphone uses Handset equalization that is optimized for TIA-810/920 acoustic performance.

Setting handset audio equalization

Use the following procedure to configure the Handset Equalization settings:

1. On the user menu, navigate to **Settings > Options&Settings > Advanced Options > Handset Equalization**.
2. Using the navigational keys or by tapping the arrow icons on the screen, choose any of the following:
   - Default
   - Audio Opt
   - HAC Opt
3. Press **Save**.

Setting interface control

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

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **INT...** from the Admin Procedures screen, the following text displays with a prompt to use the Right and Left navigation arrows to select a setting:

```
Ethernet:                    Choice Selector
PC Ethernet:                 Choice Selector
```

   The values shown are the text strings associated with the current PHY1STAT on the Ethernet line and the current PHY2STAT system value on the PC Ethernet line.

   The PHY1STAT text strings are:

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

Note:

A PHY1STAT value of 6 applies only to deskphone models that support Gigabit Ethernet (GigE), otherwise this value/choice does not display.

The PHY2STAT text strings are:

- "Disabled" when PHY2STAT = 0
- "Auto" when PHY2STAT = 1
- "10Mbps half" when PHY2STAT = 2
- "10Mbps full" when PHY2STAT = 3
- "100Mbps half" when PHY2STAT = 4
- “100Mbps full” when PHY2STAT = 5
- “1000Mbps full” when PHY2STAT = 6

Note:

A PHY2STAT value of 6 applies only to deskphone models that support Gigabit Ethernet (GigE), otherwise this value/choice does not display.

3. To change the Ethernet setting, press the **Right** navigation arrow or the **Change** softkey to cycle 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), pressing the Right navigation arrow changes the value to 10 Mbps full (3). If the current value is 1000 Mbps full (6), pressing the Right navigation arrow changes the value to Auto (1).

4. To change the PC Ethernet setting, select that line and press the Right navigation arrow or **Change** to cycle through the possible settings.
5. Press **Save** to store the new setting(s) and redisplay the Admin Procedures screen.

Enabling and disabling event logging

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

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.

2. When you select **LOG** from the Admin Procedures screen, the deskphone prompts you to use the Right and Left navigation arrows to select and change a setting and displays the following text:

Log:	**Choice Selector Bar for the SYSLOG_LEVEL value defined below.**
Log Categories...	**Use only when directed to do so by Avaya Services.Set back to default when logging is no longer required.**
Remote Logging	**on/off**
Remote Log Server	**nnn.nnn.nnn.nnn**

   where the ***text string*** is the wording associated with the current system value of SYSLOG_ENABLED (1 = Enabled; 0 = Disabled) and SYSLOG_LEVEL, defined as:

   - “Emergencies” when SYSLOG_LEVEL = 0
   - “Alerts” when SYSLOG_LEVEL = 1
   - “Critical” when SYSLOG_LEVEL = 2
   - “Errors” when SYSLOG_LEVEL = 3
   - “Warning” when SYSLOG_LEVEL = 4
   - “Notices” when SYSLOG_LEVEL = 5
   - “Information” when SYSLOG_LEVEL= 6
   - “Debug” when SYSLOG_LEVEL = 7

3. To change the **Log** or **Remote Logging Enabled** setting, press the Right (or Left) navigation arrow to cycle through the valid settings. When changing the Remote Log Server value, enter the IP Address to which syslog messages should be sent.

   When changing the **Log** value, depending on the current value, the next sequential text string or value is selected and displayed as the setting. For example, if the current value is Alerts (1), pressing the Right navigation arrow changes the value to Critical (2). If the current value is Debug (7), pressing the Right navigation arrow changes the value to Emergencies (0).

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

CAUTION:

Logging has a direct impact on performance. Only turn on the required categories and turn them off as soon as logging is not required.

Logging out

Use the following procedure to log off a deskphone.

CAUTION:
Once a deskphone is logged off, you might need a password and extension to log back on.

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **LOGOUT** from the Admin Procedures screen, the deskphone displays a confirmation screen asking if you are sure you want to log out.
3. Press **No** to return to the Admin Procedures screen without logging off the deskphone. Press **Yes** to unregister the deskphone from the call server.

Resetting system values

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.

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **RESET VALUES** from the Admin Procedures screen, the deskphone displays a confirmation screen asking if you are sure you want to reset the deskphone.
3. Press **No** to return to the Admin Procedures screen without resetting the deskphone. Press **Yes** to start the deskphone reset. A reset:
   - Resets all system values and system initialization values except AUTH and AUTH_ONLY to default values.
   - Resets call server values to their defaults.
   - Resets the 802.1X identity and password to their default values.
   - Deletes any entries in the Redial buffer.
   - Does not affect user-specified data and settings like Contacts data or the deskphone login and password. To remove this type of data, see the Using the Clear procedure on page 40.

Restarting the deskphone

Use the following procedure to restart the deskphone.

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **RESTART PHONE** from the Admin Procedures screen, the deskphone displays a confirmation screen asking if you are sure you want to restart the deskphone.
3. Press **No** to return to the Admin Procedures screen without restarting the deskphone. Press **Yes** to proceed with the registration steps covered in the Power-Up and Reset Operation (Dynamic Addressing Process) on page 22.

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

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

Setting the signaling protocol identifier

Use the following procedure to set or change the Signaling Protocol Identifier when your environment has more than one protocol on a subnet. 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.

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **SIG...** from the Admin Procedures screen, the deskphone prompts you to use the Right and Left navigation arrows to select a setting and displays the following text:

Setting: *text string* **Choice Selector**

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

   - “Default” when SIG = 0
   - “H.323” when SIG = 1
   - “SIP” when SIG = 2

Note:

The SIG value “Default” can represent either SIP or H.323 depending on the upgrade file used for the deskphone.

3. To change the setting, press the **Change** softkey until you see the setting you want or use the **Right** or **Left** navigation arrow to cycle 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 SIP (2), pressing the Right arrow changes the value to 0 (default). If the current value is H.323 (1), pressing Right arrow changes the value to 2 (SIP).

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

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

Configuring SIP settings

Use this procedure to set up SIP-related settings like identifying the SIP Proxy Server.

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **SIP** from the Admin Procedures screen, the deskphone displays two choices - SIP Global Settings or SIP Proxy Server.
3. To change any of the SIP Global Settings, press **Select** or **OK** or the corresponding line button and proceed to the next step. To change the SIP Proxy Server(s), scroll down and press **Select** or **OK** or the corresponding line button and proceed instead to Step 4.

WARNING:

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

4. The deskphone displays the Global Settings screen and prompts you to use the Right and Left navigation arrows or a text entry to change a setting and displays the following settings and their active values:

Setting	Description/Example	Changes this Configuration Parameter
SIP Domain:	e.g., avaya.com	SIP_DOMAIN
Avaya Environment:	**Auto** or **No -** indicates whether only an Avaya environment (CM and Session Manager) is in effect.	DISCOVER_AVAYA_ ENVIRONMENT
Reg Policy:	**alternate** or **simultaneous**	SIPREGPROXYPOLICY
Failback Policy:	**admin** or **auto**	FAILBACK_POLICY
Avaya Config Server:	IP Address of Avaya configuration server - only if PPM is not on the same server as the SIP Proxy server.	CONFIGURATION_SERVER or CONFIGURATION_SERVER _IN_USE
Host to ping	IP Address or DNS Name of server to ping. This is not a setting but a determiner of whether a specific server is reachable. Press the **Ping** softkey to initiate the check. The deskphone sends four pings and displays the results in a text block screen. If the ping fails, the message "Unable to contact host" displays.	N/A

5. If you selected **SIP Proxy Server,** the deskphone displays the message "Select SIP proxy to configure" and displays a list of currently configured servers.
6. To add a new server, press **New** and enter the address of SIP Proxy. Then, enter values for the Transport Type and SIP Port as indicated below under changing a setting in Step 6. To change information for a configured server, select the proxy server for which you want to update the Transport Type and/or the SIP Port and press **Select** or **OK**.

7. The deskphone displays the IP Address or DNS Name of the server that you selected and its current Transport Type and SIP Port values. The deskphone prompts you to use the Right and Left navigation arrows or text entry to add/change a setting and displays the following settings and their active values:

Setting	Description/Example	Changes this Configuration Parameter
SIP Proxy Server: **Transport Type:** **SIP Port:**	**IP Address or DNS name**. For Session Manager deployments, this is the IP Address of the session manager. **TCP** or **TLS** or **UDP** If no value is entered, default of 5060 for UDP/TCP or 5061 for TLSSIPPORT is used	SIP_CONTROLLER_LIST SIPSIGNAL if Transport Type is UDP/ TCP; SIP_PORT_ SECURE if Transport Type is TLS.

8. Press **Save** to store the new setting(s) and redisplay the Admin Procedures screen.
9. **Note:** You can only change values that have been added using a Local Administrative (Craft) procedure.

Configuring Time Server settings

Use this procedure to designate a server for Simple Network Time Protocol (SNTP) and to set corresponding values.

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.

2. When you select **SNTP...** from the Admin Procedures screen, the deskphone displays the following settings and prompts you to enter the IP Address of the SNTP server:

	Description/Example	Changes this Parameter
SNTP Server:	IP address or DNS Name of the network time server.	SNTPSRVR or SNTPSRVR_IN_USE
SNTP GMT Offset:	Local time difference in hours from Greenwich Mean Time, e.g., NJ is **-5**.	GMTOFFSET
SNTP Daylight Savings Time Off/ On/Auto:	Indicates whether the deskphone should recognize Daylight Savings Time (DST)(0=no DST, 1=DST activated as per DSTOFFSET, 2=automatic based on DSTSTART and DSTSTOP values.	DAYLIGHT_SAVING_ SETTING_MODE

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

Setting Site-Specific Option Number

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.

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

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **SSON...** from the Admin Procedures screen, the following text displays:

   ```
   Setting:
   ```

   where the ***setting*** is the current system value of DHCP_SSON.
3. To change the setting, press the appropriate softkey(s) and use the dialpad to enter a valid SSON value between 128 and 255.
4. Press **Save** to store the new setting and redisplay the Admin Procedures screen.

Using the View administrative option

If you are using static addressing and encounter problems, use the following procedure to verify the current values of system parameters and file versions.

Note:

Unless otherwise prevented using administration, the user can view but not change most of the parameters associated with Craft Local Procedures. For more information about this option, see the applicable user guide(s).

If the View Network Information option is not available due to being disabled by administration, use the **ADDR** option to view IP Addresses. See Installing static addressing on page 37. The IP Addresses might have been entered incorrectly. Verify whether you were provided with correct IP Addresses.

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **VIEW** from the Admin Procedures screen, the following text displays:

Setting	Description	Associated Configuration Parameter
Model	The model of the deskphone that is set by factory procedures.	MODEL
Application File	The name of the Signed Application/Library software package.	
Kernel/RFS File	The name of the Kernel/ Root File System software package.	
Backup App File	The name of the backup copy of the Signed Application/Library software package stored in the phone.	
Group	The group identifier to download during start-up a specific configuration set for a dedicated user group.	GROUP
MAC	The MAC address of the deskphone.	MACADDR

Setting	Description	Associated Configuration Parameter
SIP Proxy Server	The SIP proxy server to which the deskphone registered successfully.	SIPPROXYSRVR_IN_USE
Router	The router used as primary gateway out of list of configured routers.	ROUTER_IN_USE
HTTPS file server	The list of IP or DNS addresses of TLS servers for HTTPS file download, settings file or language files, during startup procedure.	TLSSRVR
HTTP file server	The IP address of the HTTP server that the deskphone accessed before successfully.	HTTPSRVR_IN_USE
DNS server	The IP address of the DNS server that the deskphone accessed before successfully	DNSSRVR_IN_USE
SNTP server	The SNTP server that the deskphone used before to set or update the date and time.	SNTPSRVR_IN_USE
Protocol	Signaling protocol in effect, such as SIP	
Phone SN	Deskphone Serial Number	
PWB SN	Printed Wiring Board (circuit board) Serial Number (may not apply to all phones)	
PWB Comcode	Software-readable PWB serial number and comcode (may not apply to all phones)	PHONECC
Exchange Server	The Microsoft Exchange™ server that the deskphone uses currently.	EXCHANGE_SERVER_IN_USE

3. Use the navigation arrows to scroll through the viewable information.

4. Press **Back** at any time to return to the Admin Procedures screen.

Chapter 4: Maintaining the 9601, 9608, 9608G, 9611G, 9621G, and 9641G IP deskphones

Introduction

This chapter covers maintaining the 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones, for example, downloading a new software version from the Avaya support website. The recommended configuration is the latest call server software and the latest IP deskphone firmware.

Important:

You can convert 9600 Series IP Deskphones models, with the exception of 9601 IP deskphone, from H.323 to SIP software or from SIP to H.323 software. When converting from one protocol type to another on a given deskphone, see Converting software on the 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones on page 14. Note that, depending on the deskphone model and the software version you start from, additional steps may be required from those mentioned in this section.

Downloading software upgrades

Important:

For any new software release, ensure that you download the latest software distribution package and read any Product Support Notices (PSNs) associated with the new release. Both are available on the Avaya support website.

Review the release notes and any Read Me files associated with a distribution package.

Ensure that the settings file is not cached in your browser. To do this, clear the browser cache before downloading the settings file from the Avaya support Web site, so that you don’t get an old version.

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

SIP software distribution packages contain:

- One or more software files;

- One upgrade file (96x1Supgrade.txt);
- All of the display text language files;
- Files av_prca_pem_2033.txt and av_sipca_pem_2027.txt that contain a copy of the Avaya Product Root Certificate Authority certificate in PEM format that may be downloaded to deskphones based on the value of the TRUSTCERTS parameter. You must also include the System Manager route certificate in the TRUSTCERTS parameter for IM to work.
- File named release.xml that is used by the Avaya Software Update Manager application.

Release 6.4 software distribution packages in zip format also contain a signatures directory containing signature files and a certificate file to be used by the Avaya file server application on the Utility server. Customers using their own (non-Avaya) HTTP server can ignore or delete this directory.

Note:

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

Two configuration files are important to understand. They are:

- The upgrade file, 96x1Supgrade.txt, that tells the deskphone whether the deskphone needs to upgrade software. The deskphones attempt to read this file whenever they reset. The upgrade file is also used to point to the settings file.
- The settings file, 46xxsettings.txt, that contains the option settings that enable, disable, or otherwise customize the settings you might need to tailor the deskphones for your enterprise.

Note:

You can use one settings file for all your Avaya IP deskphones including the 9600 series IP deskphones covered in this document, and 4600 series IP deskphones, as covered in the *4600 Series IP Telephone LAN Administrator Guide* (Document 555-233-507).

Download procedure

The Avaya-provided upgrade script files and the application files included in the zip files upgrade the deskphones. You should not need to modify them. It is essential that all the files be together on the file server. When downloading a new release onto a file server with an existing release already on it, you should:

1. Stop the file server.
2. If you want to specify a port the deskphones should use to communicate with the file server, administer the desired port setting in HTTPPORT or TLSPORT, for HTTP or TLS, respectively.
3. Back up all the current file server directories as applicable.
4. Copy your ***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: BOOTNAME, GROUP, MACADDR, MODEL, and SIG.

6. Download the self-extracting executable file, or the corresponding zip file.
7. Extract all the files.
8. Copy your ***46xxsettings.txt*** file back into the download directory.
9. Check the Readme file for release-specific information.
10. Modify the ***46xxsettings.txt*** file as desired.
11. Restart the HTTP/HTTPS server.
12. Reset your Avaya IP deskphones.

You can download a default upgrade file from http://www.avaya.com/support. This file allows the deskphone to use default settings for customer-definable options. Of course, these settings can also be changed with DHCP or in some cases, from the deskphone's dialpad itself. However, you might want to open the default file and administer the options to add useful functionality to your Avaya IP deskphones. This file must reside in the same directory as the upgrade file, and must be called ***46xxsettings.txt***.

Contents of the settings file

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

- Tags, which are lines that begin with a single "#" character, followed by a single space character, followed by a text string with no spaces.
- **`Goto`** commands, of the form **GOTO *tag.*** **`Goto`** commands cause the deskphone to continue interpreting the settings file at the next line after a **# *tag*** statement. If no such statement exists, 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. The only parameters that can be used in a conditional statement are: GROUP, MACADDR, MODEL and MODEL4.
- **SET** commands, of the form **SET *parameter_name value***. Invalid values cause the specified value to be ignored for the associated ***parameter_name*** so the default or previously administered value is retained. All values must be text strings, if the value itself is numeric, you must place the numeric value inside a pair of quotation marks. For example, "192.x.y.z"
- Comments, which are statements with characters "##" in the first column.
- GET commands, of the form ***GET filename.*** The deskphone attempts to download the file named by ***filename***, and if it is successfully obtained, it will be interpreted as an additional settings file, and no additional lines will be interpreted in the original file. If the file cannot be obtained, the deskphone will continue to interpret the original file.

The Avaya-provided upgrade file includes a line that tells the deskphones to **GET *46xxsettings.txt***. This line cause the deskphone to use HTTP/HTTPS to attempt to download the file specified in the **`GET`**

command. If the file is obtained, its contents are interpreted as an additional script file. That is how your settings are changed from the default settings. If the file cannot be obtained, the deskphone continues processing the upgrade script file. If the settings file is successfully obtained but does not include any setting changes the deskphone stops using HTTP.

The settings file is under your control and is where you can identify non-default option settings, application-specific parameters, etc. You can download a template for this file from the Avaya support Web site. See Chapter 7 in the A*dministering Avaya Deskphone SIP for 9601/9608/9608G/9611G/9621G/9641G* for details about specific parameter values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

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

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

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

Downloading text language files

Language files contain the language name (as it should be presented to a user for selection), an indication of the preferred character input method, text string replacements for the built-in English text strings, where each replacement string may contain up to 120 characters. Each has a unique index that associates it with the corresponding built-in English string, an indication as to whether Chinese, Japanese or Korean glyphs should be displayed for the Unicode “Unified Han” character codes, and a Language Identification Tag for the language of the text contained in the file. A downloadable language file may also contain a translation of the language name into any or all of the languages for which a language file is included in the software distribution package. Language files must be stored in the same location as the 46xxsettings.txt file.

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 LANGUAGES** command in the 46xxsettings file before downloading a language file with the same filename.

Note:

Language files for SIP deskphones have a **.xml** filename extension whereas language files for 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones set to H.323 have a .txt filename extension.

Changing the signaling protocol

For enterprises requiring both H.323-based and SIP-based protocols, there are two ways to specify the protocol to be used by all or specific deskphones:

1. As of Release 6.2, the SIG parameter can be set in DHCP Option 242 (Site-Specific Option Number) or in the 46xxsettings.txt file. This setting will apply to all deskphones except those for which SIG has been manually configured to a value of H.323 or SIP using the SIG Craft procedure.
2. The SIG parameter can be set on a per-phone basis using the Setting the signaling protocol identifier Craft procedure.

Note:

The 9601 deskphone supports only the SIP signaling.

The GROUP parameter

You might have different communities of end users, all of which have the same model deskphone, but which require different administered settings. For example, you might want to restrict Call Center

agents from being able to log off, which might be an essential capability for “hot-desking” associates. We provide examples of the group settings for each of these situations later in this section.

The simplest way to separate groups of users is to associate each of them with a number. Use the GROUP system value for this purpose. The GROUP system value **cannot** be set in the 46xxsettings file. The GROUP system value can only be set on a deskphone-by-deskphone basis using a Craft procedure. To set up groups, first identify which deskphones are associated with which group and designate a number for each group. The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group would be assigned as Group 0.

Then, at each non-default deskphone, invoke the **GROUP** Local (Craft) Administrative procedure as specified in Chapter 3: Local administrative options and specify which GROUP number to use. Once the GROUP assignments are in place, edit the configuration file to allow each deskphone of the appropriate group to download its proper settings.

Here is an 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 GROUP1
IF $GROUP SEQ 2 goto GROUP2
{specify settings unique to Group 0}
goto END

# GROUP1
{specify settings unique to Group 1}
goto END

# GROUP2
{specify settings unique to Group 2}

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

Chapter 5: Troubleshooting guidelines

Introduction

This chapter describes problems that might occur during both installation and normal operation of the SIP deskphones and possible ways of resolving these problems.

This chapter contains the following sections:

- Descriptions of error conditions and methods for resolving them.
- Error and status messages, and methods for resolving them.

Error conditions

There are three areas where installers can troubleshoot problems before seeking assistance from the system or LAN administrator:

1. Check both the power and Ethernet wiring for the following conditions:
   - Whether all components are plugged in correctly.
   - Check LAN connectivity in both directions to all servers - DHCP, HTTP, HTTPS, Avaya Communication Manager, and/or SIP Proxy server.
   - If the deskphone is supposed to be powered from the LAN, ensure that the LAN is properly administered and is compliant with IEEE 803.3af.
2. If you are using static addressing:
   - Use the **VIEW** Craft procedure to find the names of the files being used and verify that these filenames match those on the HTTP/HTTPS server. See Using the View administrative option on page 53 for more information. Check the Avaya Web site to verify whether the correct files are being used.
   - Use the **ADDR** Craft procedure to verify IP Addresses. See Installing static addressing on page 37 for information.
3. If the 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphone is not communicating with the system (DHCP, HTTP, or Communication Manager call server), make a note of the last message displayed, as described in Table 3 and/or Table 4. Consult the system administrator.
4. If you expect the deskphone to be IEEE-powered, verify with the LAN administrator that IEEE power is indeed supported on the LAN.

DTMF tones

SIP deskphones send DTMF tones according to the SEND_DTMF_TYPE parameter setting. The default setting of this parameter sends DTMF "tones" as "telephone event" RTP packets per RFC 2833. Whether a non-SIP deskphone hears these DTMF tones depends on whether the Avaya Communication Manager media resource converts the "telephone event" RTP packets into audio RTP packets.

Power interruption

If power to a 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphone is interrupted while the deskphone is saving the application file, the HTTP/HTTPS application can stop responding. If this occurs, restart the phone.

Installation error and status messages

The 9601, 9608, 9608G, 9611G, 9621G, and 9641G IP deskphones issue messages in the currently selected language, or if the deskphone is logged off, in the language specified by the SYSTEM_LANGUAGE parameter value. If English is not the selected language, the deskphone displays messages in English only when they are associated with local procedures, for example, the **VIEW** Craft local procedure.

Most of the messages in Table 3 display only for about 30 seconds or less, and then the deskphone resets. The most common exception is `Extension in Use`, which requires manual intervention.

Table 3: Possible error and status messages during installation of 9601, 9608, 9611G, 9621G, or 9641G IP deskphones

Message	Cause/Resolution
`Address Conflict`	**CAUSE:** The deskphone has detected an IP Address conflict. **RESOLUTION:** Verify administration to identify duplicate IP Address(es).
`Bad Router`	**CAUSE:** The deskphone cannot find a router based on the information in the DHCP file. **RESOLUTION:** Use static addressing to specify a router address, or change administration on DHCP, as indicated in *Administering Avaya Deskphone SIP for 9601/9608/9608G/9611G/9621G/9641G*.

Table 3: Possible error and status messages during installation of 9601, 9608, 9611G, 9621G, or 9641G IP deskphones (continued)

Message	Cause/Resolution
`DHCP: CONFLICT`	**CAUSE:** At least one of the IP Addresses offered by the DHCP server conflicts with another address. **RESOLUTION:** Review DHCP server administration to identify duplicate IP Address(es).
`Finding router...`	**CAUSE:** The deskphone is proceeding through boot-up. **RESOLUTION:** Allow the deskphone to continue.
`No Ethernet`	**CAUSE:** When first plugged in (or during operation), the SIP IP deskphone is unable to communicate with the Ethernet. **RESOLUTION:** Verify the connection to the Ethernet jack, verify the jack is Category 5, verify power is applied on the LAN to that jack, etc.
`Restarting...`	**CAUSE:** The deskphone is in the initial stage of rebooting. **RESOLUTION:** Allow the deskphone to continue.
`SCEP: Failed`	**CAUSE:** Simple Certificate Enrollment Protocol (SCEP) has rejected a request for a certificate. **RESOLUTION:** Although the SCEP server connection is terminated, startup continues. No action required.
`Subnet conflict`	**CAUSE:** The deskphone is not on the same VLAN subnet as the router. **RESOLUTION:** Administer an IP Address on the deskphone using Installing static addressing, or administer network equipment to administer the deskphone appropriately.
`Updating: DO NOT UNPLUG THE TELEPHONE`	**CAUSE:** The deskphone is updating its software image. **RESOLUTION:** Allow the deskphone to continue.

Operational errors and status messages

Table 4 identifies some of the possible operational problems that might be encountered after successful 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphone installation. The user guide for a specific deskphone model also contains troubleshooting for users having problems with specific deskphone applications. Most of the problems reported by 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphone users are not likely to be problems with the deskphone itself. Problems are more likely LAN-based, where Quality of Service, server administration, and other issues can impact end-user perception of deskphone performance.

Table 4: Operational error conditions for 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones

Condition		Cause/Resolution
During Craft procedure access, display freezes at prompt “Press * to program”		**CAUSE:** Craft access has failed; deskphone cannot operate. **RESOLUTION:** Unplug the deskphone, then plug it in again to reset.
After Login, the progress bar shows just a few completed bars and stops moving.		**CAUSE:** Login has failed. **RESOLUTION:** Check that the LAN and File servers are operating correctly. Re-attempt login.
The deskphone continually reboots, or reboots continuously about every 15 minutes.		**CAUSE:** The deskphone cannot find the call server. **RESOLUTION:** Ensure that SIP_CONTROLLER_LIST is administered either manually or through DHCP or HTTP, as appropriate.
The message light on the deskphone turns on and off intermittently, but the deskphone never registers.		**CAUSE:** This is a hardware fault. **RESOLUTION:** The deskphone must be returned to Avaya for repair.
The deskphone stops working in the middle of a call,	**AND** no lights are lit on the deskphone and the display is not lit.	**CAUSE:** Loss of power. **RESOLUTION:** Check the connections between the deskphone, the power supply, and the power jack.
	AND power to the deskphone is fine (and the deskphone might have gone through the restarting sequence).	**CAUSE:** Loss of path to the call server or the other party’s deskphone, DHCP Lease expired, or DHCP server not available when deskphone attempts to renegotiate DHCP lease. **RESOLUTION:** As above.

1 of 6

Table 4: Operational error conditions for 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones (continued)

Condition		Cause/Resolution
The deskphone was working, but does not work now,	**AND** no lights are lit on the deskphone and the display is not lit.	**CAUSE:** Loss of power. **RESOLUTION:** Check the connections between the deskphone, the power supply, and the power jack.
	AND power to the deskphone is fine, but there is no dial tone or the call appearances or feature buttons do not work.	**CAUSE:** Loss of communication with the call server. **RESOLUTION:** Check LAN continuity from the call server to the deskphone using ARP or trace-route and from the deskphone to the call server by invoking a Feature button. Verify that administration has not changed for the LAN equipment (routers, servers, etc.) between the call server and the deskphone. Verify no one changed the deskphone settings locally using the **VIEW** and **ADDR** craft procedures, as described earlier in this guide.
	AND the deskphone was recently moved.	**CAUSE:** Loss of communication with the call server. **RESOLUTION:** As above, but pay particular attention to the possibility that the deskphone is being routed to a different DHCP server, or even a different proxy server. If so, the new server might need to be administered to support the deskphone.
	AND the network was recently changed to upgrade or replace servers, re-administer the Communication Manager call server, add or change NAT, etc.	**CAUSE:** Loss of communication with Session Manager. **RESOLUTION:** As above.

2 of 6

Table 4: Operational error conditions for 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones (continued)

Condition	Cause/Resolution
The deskphone works, but the audio quality is poor, specifically:	
the user hears echo when speaking on a handset.	**CAUSE:** Echo from digital-to-analog conversion on your Communication Manager call server trunk. **RESOLUTION:** *Option 1*: Try a different Call Quality setting under the Audio Parameters section. *Option 2*: Check whether packet loss, or jitter delay is causing this problem, by eliminating or minimizing both. *Option 3*: Verify which trunk is causing the echo, and check the trunk's Trunk Termination parameter on the call server.
the user hears echo on a headset, but not on a handset.	**CAUSE:** Improper headset adapter. **RESOLUTION:** Replace adapter with Avaya's M12LU or 3412-HIC adapters. We recommend the M12LU, since it supports Automatic Gain Control.
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 deskphone. 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 by invoking the Network Information feature under the **A** (Avaya) button on the deskphone. One or more Quality of Service (QoS) features should be implemented in the network as covered in Chapter 3: Local administrative options. **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/off settings for the AGCHAND, AGCHEAD, and AGCSPKR parameters.

3 of 6

Table 4: Operational error conditions for 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones (continued)

Condition	Cause/Resolution
The deskphone works properly except for the Speaker.	**CAUSE:** The Speaker was disabled in the settings file. **RESOLUTION:** Check the settings file and re-enable the Speaker if appropriate.
The deskphone works properly, except incoming DTMF tones are not received.	**CAUSE:** The TN2302AP board does not pass in-band DTMF tones. **RESOLUTION:** None; the board is operating as designed.
When a line is selected, a short dial tone burst sounds followed by a reorder/fast busy tone.	**CAUSE:** The extension is provisioned on Session Manager and some Communication Manager forms, but not on the off-pbx-telephone station-mapping form. Communication Manager is unable to map back to Session Manager, and rejects the line reservation. **RESOLUTION:** Map the extension on the off-pbx-telephone station-mapping form, a sample of which appears in Appendix C of the *Administering Avaya Deskphone SIP for 9601/9608/9608G/9611G/9621G/9641G*. **CAUSE:** Possible error in SIG group configuration on Communication Manager, which indicates the default region for the SIP trunk to Communication Manager. **RESOLUTION:** On the IP-network-region form, ensure that the region pointed to is configured with an **authoritative domain** that is the same as the Session Manager SIP domain. also verify that the station in question has not been redirected to a different network region on the ip-network map.
The HTTP/HTTPS script file and settings file are ignored (not being used by the deskphone).	**CAUSE:** The system value AUTH is set to 1 (HTTPS required) but no valid address is specified in TLSSRVR. **RESOLUTION:** Change AUTH to 0 (zero), or enter a valid address for TLSSRVR.

4 of 6

Table 4: Operational error conditions for 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones (continued)

Condition		Cause/Resolution
The HTTP/HTTPS script file is ignored or not used by the deskphone,	**AND** the HTTP/ HTTPS server is a LINUX or UNIX system.	**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 deskphone 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 it. Customize or change *only* the ***46xxsettings*** file, as discussed in Chapter 4: Maintaining the 9601, 9608, 9608G, 9611G, 9621G, and 9641G IP deskphones.
The MS Exchange contacts take too long to load		**CAUSE:** The correct Exchange server is not specified in the parameter EXCHANGE_SERVER_LIST in the ***46xxsettings*** file. **RESOLUTION**: Verify that the MS Exchange server being used is specified in the settings file. To view the Exchange server in use, go to: **Outlook** > **Tools>Options** > **Mail Setup** > **E-mail Accounts** > **Change**
Some settings in the settings file are being ignored while other settings are being used properly.		**CAUSE:** Improper settings file administration. **RESOLUTION:** Verify that customized settings are correctly spelled and formatted.
	AND the setting being ignored is one or more of the AGC settings.	**CAUSE:** The user changed the AGC setting(s). **RESOLUTION:** Have the user reset the AGC value(s) back to the desired setting(s).
	AND the setting being ignored is the TIMEFORMAT setting.	**CAUSE:** The time format was changed using the Avaya Menu Options & Settings. **RESOLUTION:** If the time disappears, Reboot the phone.
Deskphone power is interrupted while the deskphone is saving the application file **and** the HTTP/HTTPS application stops responding.		**CAUSE:** The HTTP/HTTPS application stops responding if power is interrupted while a deskphone is saving the application file. **RESOLUTION:** Restart the phone.

5 of 6

Table 4: Operational error conditions for 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones (continued)

Condition	Cause/Resolution
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:** Assuming the user is meant to have that application, verify the 46xxsettings script file is properly specified for your system, including case if your file server is UNIX or LINUX, and extension. Then, verify all the relevant parameters indicated in Table 7 of the A*dministering Avaya Deskphone SIP for 9601/ 9608/9608G/9611G/9621G/9641G*, are accurately specified in the 46xxsettings file.
User data disappeared when the user logged off one deskphone and logged into another deskphone.	**CAUSE:** Possible PPM problem. **RESOLUTION:** Contact the Session Manager administrator.
The deskphone displays "User logged in at another location"	**CAUSE:** The extension entered by the user during login is currently in use on another phone. **RESOLUTION:** Instruct user to log in with a different extension. Tell the user to press the 'Retry' softkey, then enter new extension and password. Or, have the user log in with the original extension, while unregistering the extension from the other phone.
Login fails	**CAUSE:** Invalid provisioning on Communication Manager or Session Manager. **RESOLUTION:** Session Manager needs to point to Communication Manager's PROCR interface for the "Media Server Admin Address." Session Manager must point to a specially-provisioned PPM Administration account on Communication Manager. The PPM Administration account on the Communication Manager side must have several specific parameters set. Specifically: login group must be "susers" additional group must be "prof18" or equivalent shell access must be "no shell access"
Multiple call appearances on incoming call	**CAUSE:** Provisioning problem. **RESOLUTION:** On the off-pbx-telephone station-mapping form, page 2, set the Bridged Calls field to "none".
A blank screensaver appears and the phone does not immediately respond to pressing the Phone button	**CAUSE:** The server IP Address in the LOGO parameter is invalid or unavailable. **RESOLUTION:** Correct/change the LOGO parameter in the settings file.

6 of 6

Network ping diagnostics

A **Ping** softkey appears when you view a network address in the Avaya Menu Network Information... option. Users can validate the routing to provisioned addresses using the **Ping** softkey.

Administrators can validate arbitrary addresses with the “Host to Ping” function using the Craft local procedure on Installing static addressing on page 37.

Ping results display in a succession of pop-up windows.

SRTP provisioning

SRTP is now supported (with TLS). To use SRTP, the network region codec set must have media encryption set up for each region that calls may traverse.

When SRTP is provisioned in Communication Manager, the default cryptosuite used is ‘aescm128-hmac80’. The 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphone also assumes that no encryption is an option provisioned in Communication Manager. If Communication Manager is provisioned with the cryptosuite aescm128-hmac80, then the following entry must be in the 46xxsettings.txt file:

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

If some other encryption set is required, the string must be set appropriately in the 46xxsettings.txt file.

Appendix A: Glossary

Term	Description
802.1P 802.1Q	802.1Q defines a layer 2 frame structure that supports VLAN identification and a QoS mechanism usually referred to as 802.1P.
802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. SIP Software Release 2.0 and up supports IEEE 802.1X using EAP-MD5 and EAP-TLS authentication methods.
Application-specific	Specific to a particular “application” running inside the deskphone. For example, configuration file downloading, 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, used, for example, to verify that the IP Address provided by the DHCP server is not in use by another device on the network.
Call Server	In an Avaya SIP environment, the “call server” is the combination of Session Manager and Communication Manager.
CLAN	Control LAN, 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. The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP Addresses. Avaya 9601, 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones can use DNS to resolve names into IP Addresses. In DHCP, TFTP, and HTTP files, DNS names can be used wherever IP Addresses were available as long as a valid DNS server is identified first.
EAP	Extensible Authentication Protocol, or EAP, a universal authentication framework frequently used in wireless networks and Point-to-Point connections defined by RFC 3748. EAP provides some common functions and a negotiation of the desired authentication methods, two of which are EAP-MD5 and EAP-TLS. When EAP is invoked by an 802.1X enabled NAS (Network Access Server) device such as an 802.11 a/b/g Wireless Access Point, modern EAP methods provide a secure authentication mechanism and negotiate a secure PMK (Pair-wise Master Key) between the client and the NAS.
H.323	A TCP/IP-based protocol for VoIP signaling.

Term	Description
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	Hypertext Transfer Protocol Secure is a widely-used communications protocol for secure communication over a computer network. It is the result of layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communication.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.
LAN	Local Area Network.
LLDP	Link Layer Discovery Protocol. All 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones with an Ethernet interface support the transmission and reception of LLDP frames on the Ethernet line interface in accordance with IEEE standard 802.1AB. SIP Software Release 2.0 and up supports LLDP.
MAC	Media Access Control, ID of an endpoint.
PPM	Personal Profile Manager, responsible for maintaining and managing end users' personal information in the system.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio and signaling quality over packet-based networks.
RTCP	Real-time Transport Control Protocol.
RTP	Real-time Transport Protocol.
SCEP	Simple Certificate Enrollment Protocol, used to obtain a digital certificate.
Session Manager	Avaya Aura® Session Manager, the SIP proxy for Avaya Aura®.
SIP	Session Initiation Protocol, an open standard defined initially by IETF RFC 3261. SIP is an alternative to H.323 for VoIP signaling.
SRTCP	Secure Real-time Transport Control Protocol.
SRTP	Secure Real-time Transport Protocol.
TCP	Transmission Control Protocol, a connection-oriented transport-layer protocol.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications.
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
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.

Term	Description
VLAN	Virtual LAN.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.

Index

Numerical

A

C

D

E

G

H

I

L

M

O

P

R

S

T

V