Avaya one-X® Deskphone H.323 9608, 9611G, 9621G, and 9641G Installation and Maintenance Guide

Release 6.2
16-603603
Issue 3
February 2012

© 2012 Avaya Inc.

All Rights Reserved.

Notice

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

Note

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by 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 Web sites 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 its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

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

License types

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

Shrinkwrap License (SR). Customer 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”). (see “Third-party Components” for more information).

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

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

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 Web site: http://support.avaya.com. Suspected security

vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

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 designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

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

FCC/Industry Canada Radiation Exposure Statement

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

Warning

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

Power over Ethernet (PoE) warning

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

Contents

Chapter 1: About This Guide 7
- Deskphone models this guide covers 7
- Change History 7
- What's New in This Release 8

Chapter 2: Installing the Deskphone 11
- About Avaya one-X® Deskphones 11
- Updating deskphone software for installation 11
- Creating the pre-installation checklist 12
- Powering the deskphone 14
- Completing the power connection 18
- Installing a Dual Headset Adapter (DHA) 19
- 9641G Call Center faceplate installation 24
- About powering-up and resetting the deskphone (Dynamic Addressing Process) 25
- About deskphone initialization 25
- How the power-up and reset process works 27
- About unnamed registration 31

Chapter 3: Using Local Administrative (Craft) Options 33
- About local (Craft) procedures 33
- Accessing local (Craft) procedures 34
- Accessing Craft procedures during startup 34
- Accessing Craft procedures during normal operation 35
- Entering data for administrative options 36
- About entering and validating IPv4 and IPv6 addresses 37
- Local administrative (Craft) procedures menu 38
- Setting the 802.1X Operational Mode 40
- Using the pre-installation checklist 42
- Changing IP address information 42
- Calibrating the Touch Screen 45
- Disabling/enabling automatic gain control 46
- Clearing the deskphone settings 47
- Adjusting contrast on button modules and non-color deskphones 48
- Disabling/enabling debug mode and sending the debug report to server 49
- Changing the group identifier 50
- Setting handset audio equalization 50
- Changing Ethernet interface control 51
- Disabling/enabling event logging 52
- Logging off the deskphone 53
- Viewing multi-language strings 54
- Resetting system values 55
- Restarting the deskphone 56
- Setting or changing the signaling protocol 57
- Changing SSON settings 58
- Performing a self-test 58

Chapter 4: Maintaining 9600 Series IP Deskphones 61

About software distribution packages 61
Downloading software packages 62
Contents of the settings file 63
Downloading text language files 64
Changing the signaling protocol 65
Applying settings to logical groups 65
Chapter 5: Troubleshooting 67
Resolving error conditions 67
Failure to hear DTMF tones 68
Correcting a power interruption 68
Using the VIEW craft procedure for troubleshooting 68
Installation error and status messages 72
Operational errors and status messages 76
LLDP Troubleshooting 82
Proposed Solution 82
LLDP setup and troubleshooting steps 83
Proposed solution for DHCP—configured deskphones 83
Proposed solution for script-configured deskphones 84
Proposed solution for LLDP-configured deskphones 84
Secure Shell Support 85
Chapter 6: Terms Used in This Guide 87
Index 89

Chapter 1: About This Guide

Deskphone models this guide covers

There are fifteen telephone set models currently defined in the Avaya one-X® 9600 Series IP Deskphone family, as shown below. Only the 9608, 9611G, 9621G, and 9641G models are covered in this guide; the remaining models are described in the *Avaya one-X® Deskphone H.323 Administrator Guide (Document Number 16-300694)*:

• 9608	• 9620C	• 9630G	• 9650
• 9610	• 9620L	• 9640	• 9650C
• 9611G	• 9621G	• 9640G	• 9670G
• 9620	• 9630	• 9641G	

The deskphones have an Ethernet switch that allows the telephone and a PC to share the same LAN connection, if appropriate. Thus, these models do not need, or work with, the 30A switched hub interface. The 9611G, 9621G, and 9641G models have a gigabit Ethernet (GigE) interface, which speeds data transmission. The 9641 also has an integrated Bluetooth™ interface; setup of a Bluetooth device is described in the *Avaya one-X® Deskphone H.323 for 9621/9641 IP Telephone User Guide* (Document Number 16-602638).

This document describes the installation of four of the above deskphones (9608, 9611G, 9621G, and 9641G) and post-installation maintenance issues for those phones. For details about using deskphone features, see the user documentation for each deskphone. For information about desk or wall mounting, see the instructions boxed with the telephone. Wall or desk mount instructions are also available on the Avaya support Web site http://www.avaya.com/support.

Change History

Issue 1	This was the first release of this document, issued in August, 2010 to support 9600 Series IP deskphone Software Release 6.0 and the addition of four new

	deskphone models: 9608, 9611G, 9621G, and 9641G. Release 6.0 was numbered to be compatible with Release 6.0 of Avaya Aura®™ Communication Manager. 9600 Series IP deskphone software Release 6.0 is only supported on the 9608, 9611G, 9621G, and 9641G deskphones.
Issue 2	This was the second release of this document, issued in April, 2011 to support enhancements to the 9608, 9611G, 9621G, and 9641G deskphones.
Issue 3	This is the current release of this document, issued in February, 2012 to support enhancements to the 9608, 9611G, 9621G, and 9641G deskphones. What's New in This Release on page 8 describes Release 6.2 in more detail. Note that for 9600 Series IP deskphones other than the 9608, 9611G, 9621G, and 9641G, Software Release 3.1, issued in November, 2009 still applies.

What's New in This Release

New material in this issue to support Release 6.2 software includes the following features and functionality that apply only to the 9608, 9611G, 9621G, and 9641G IP deskphones:

- The Debug procedure has been expanded to allow technicians to send immediate debug reports to specified servers.
- A version of software that disables VPN and media encryption can be downloaded from the Support website; it is identified on the About Avaya one-X screen with a "U" appended to the software release.
- Secure Shell (SSH) protocol is supported. This protocol is intended to help Avaya Services monitor telephone performance.
- EAP-TLS (Extensible Authentication Protocol with TLS authentication) is supported, in part as enabled or disabled with the DOT1XEAPS parameter.
- For call center agents logging in from other than the phone, (e.g from a PC), the AGTIDVUSTAT parameter can be used to specify a VuStats format number to enable the telephone to determine the call center agent's Agent ID, which is essential if Agent Greetings are to be used.
- A software application watchdog automatically monitors other software processes to determine whether they have become unresponsive, at which point it generates a log event and either kills the process or resets the telephone. This application watchdog can be disabled or re-enabled with the APPLICATIONWD parameter.
- Bluetooth functionality can be disabled from the settings file, with the BLUETOOTHSTAT parameter.
- A recording tone can be played when the user is on a call, with the RECORDINGTONE parameter. This would be relevant to sites where a recording device is connected to the telephone and legal requirements mandate warning both parties of the call to that fact.

- Users have a new Option under Call Settings called ‘Audible Headset Alerting’ that, when enabled, allows alerting through an attached headset in addition to the telephone’s speaker.
- Support for control of handset audio equalization has been made available through the settings file administration, end user option, and Local Procedure. Equalization is available to optimize the audio for telecoil or T-coil Hearing Aid operation, or for Acoustic Performance.
- Sidetone values for Headset and Handset administration have been made consistent between intervals.
- Support for Converged Network Analyzer (CNA) has been withdrawn; any applicable administration will be ignored as of Release 6.2.
- Call Center agents have their Greetings stored on the telephone between logins, in addition to storage on a file server.
- The default value of HEADSYS has been changed. The new default is tied to the current value of CALLCTRSTAT. If CALLCTRSTAT has value “1”, HEADSYS has default value “1”. Otherwise, CALLCTRSTAT has value “0”, and the default value of HEADSYS is likewise 0. In either case, though, you have the normal ability to override defaults by explicitly setting HEADSYS in the settings file.

Chapter 2: Installing the Deskphone

About Avaya one-X® Deskphones

The 9600 Series IP deskphone product line uses Internet Protocol (IP) technology with Ethernet interfaces. The 9608, 9611G, 9621G, and 9641G deskphones introduced in Release 6.0 supplement the existing Avaya IP Solutions platform.

The 9600 Series IP deskphones introduced in Release 6.0 support DHCP and HTTP/HTTPS over IPv4/UDP and IPv6/UDP (including Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP); both protocols enhance deskphone administration and servicing. These deskphones use DHCP to obtain dynamic IP Addresses and HTTP or HTTPS to download new software versions or customized settings for the deskphones.

All 9600 Series IP deskphones 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 240 Vac rms to any primary/mains circuitry and 120 Vac rms to any telecommunications network circuitry). To ensure that these conditions are adhered to, interconnect the equipment only with the already approved/certified equipment.

Updating deskphone software for installation

About this task

As shipped from the factory, a deskphone may not contain the most up-to-date software for registration and operation. When the deskphone is first plugged in, a software download from an HTTP server might be initiated. The software download gives the deskphone upgraded functionality.

For subsequent downloads of software upgrades, the media server provides the capability for a remote restart of the IP telephone. As a consequence of restarting, the deskphone automatically starts reboot procedures which result in a download if new software is available. See About software distribution packages on page 61 and Downloading software packages on page 62 for information.

Creating the pre-installation checklist

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

Requirements to verify for your network:		
❑	1.	The LAN uses Ethernet Category 5e cabling running the IPv4 or IPv6 version of Internet Protocol.
❑	2.	Your call server is updated with Communication Manager (Communication Manager) Release 6.0 or later. Avaya supports 9608, 9611G, 9621G, and 9641G deskphones running Software Release 6.0 and later only on Communication Manager 6.0 or later.
❑	3.	The following circuit packs are installed on the switch: • TN2602 or TN2302IP Media Processor circuit pack. Sites with a TN2302 IP Media Processor circuit pack are strongly encouraged to install a TN2602 circuit pack to benefit from increased capacity. • TN799C, or D Control-LAN (C-LAN) circuit pack. **Important:** Release 6.0 or greater requires TN799C V3 or greater C-LAN circuit pack(s). For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya support Web site http://www.avaya.com/support.
❑	4.	The Avaya call server is configured correctly, as described in the *Avaya one-X® Deskphone H.323 Administrator Guide* and Communication Manager documentation. Both documents are available at: http://www.avaya.com/support.
❑	5.	The DHCP server and application are administered as described in the *Avaya one-X® Deskphone H.323 Administrator Guide*.
❑	6.	The HTTP/HTTPS server and application are administered as described in the *Avaya one-X® Deskphone H.323 Administrator Guide*.
❑	7.	The upgrade script and application files from the Avaya Support Web site, http://www.avaya.com/support, are loaded correctly on the HTTP/HTTPS server.

Requirements to verify for your network:		
❑	8.	If applicable, the DNS server is administered as described in the *Avaya one-X® Deskphone H.323 Administrator Guide*.
❑	9.	If applicable, the WML server is administered as described in the *Avaya one-X® Deskphone H.323 Administrator Guide*.

Note:

Any or all of the server applications mentioned in items 5.-9. can be co-resident on the same hardware, subject to the specific restrictions of each individual application. See the *Avaya one-X® Deskphone H.323 Administrator Guide* for more information about administering other network equipment, administering applications like firewalls, and information about topics like port utilization.

Requirements to verify for each deskphone:		
❑	10.	You have an extension number and an Communication Manager security code (password) for each applicable IP telephone. If your call server supports unnamed registration, and the telephone settings file allows unnamed registration, you do not need to provide an extension or password for the telephone. However, if you do not provide an extension or password, the telephone will have very limited telephone functionality. (For information, see About unnamed registration on page 31.)
❑	11.	A Category 5e LAN jack is available at each telephone site and a Category 5 modular line cable is available for connecting the deskphone to the Ethernet wall jack. Cat 5 cables with an RJ45 plug have a plug size restriction of 36mm.
❑	12.	Electrical power may be provided to each telephone by a Telephone Power Module (which must be ordered separately). For PoE Input connection, use only with UL listed I.T.E. equipment with PoE output. If the LAN will supply IEEE-standard power (Power over Ethernet) to the telephone, no power module is required.

❑	13.	1 Category 5e modular line cord is available for the connection between the IP deskphone and the PC, if applicable.
❑ ❑	14. 15.	Verify that the deskphone set package includes the following components: • 1 telephone set with dual position flip- or clip-stand. • 1 wideband handset capable of transmitting and receiving 7KHz audio. • 1 H4DU 9-foot long (when extended) 4-conductor coiled handset cord, plugged into the telephone and the handset. • An “Important Notice and Warning” page which provides the URL for the Avaya support site to download all other documentation. • If the 9641G will be used in a Call Center environment, the 9600 Dual Headset Adapter Kit (PK25) (Comcode: 700500729) and 9641G Call Center Faceplate Kit (PK25) (Comcode: 700500728) may be ordered, which contains 25 Dual

		Headset Adapter (DHA) units and 25 9641G removable CC-faceplate units respectively. If applicable, verify that the phone has been staged and administered with applicable VPN settings as specified in the *VPN Setup Guide for 9600 Series IP Telephones (Document 16-602968).*

Note:

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

Powering the deskphone

About this task

Caution:

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

The 9608, 9611G, 9621G, and 9641G deskphones can be locally powered only with the new Telephone Power Module (DC power jack), the IP Phone Single Port PoE Injector (SPPOE-xx), which is available separately (Comcode 700500725). In addition, all deskphones support IEEE 802.3af-standard LAN-based power. Before installing a 9608, 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) or a USB device to applicable IP deskphones, the power class may change. The table on page 15 shows the effect of such 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. For USB devices, the telephone displays instructions for any additional power needs upon registering the device.

Note:

The 9621G is a PoE Class 2 device with a 10/100/1000 switch and does not have an IEEE power switch.

Note:

If the IEEE switch on the backside of the deskphone is set to H, the telephone will register as a Class 3 device, even if the actual power usage is applicable to Class 1 or 2.

Table 1: Impact of Additional Devices on Telephone Power over Ethernet Power 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	Class 1	L	L	H	L	H	H
9611G	Class 1	H	H	H	H	H	H
9621G	Class 2	Not Applicable; the 9621G does not support Button Modules or USB devices.					
9641G	Class 2	L	L	L	L	L	H

Note:

The phone monitors its power consumption to stay within the guidelines of the IEEE 802.3af specification. Connecting a Dual Headset Adapter could lead to a change in power classification and may require a change to the switch setting as well.

Note:

For the 9611G and 9641G, the USB interface supports USB Login, using digital pictures from a USB device as a screensaver, and importing/exporting contact lists via a Flash drive. The only exceptions are the 9608, which does not support USB devices, and the 9621G model, which does not have a USB jack. Since the power consumption of the drive will vary from product to product, it is not possible to state what its impact on PoE power class will be. When the drive attempts to register with the telephone, the telephone will determine if its current power class setting is adequate to support the drive. If power is adequate, the telephone will let the drive register. If it is not adequate, the telephone will alert the user to change the power class by changing the IEEE power switch setting from “L” to “H.” In extreme situations, the total power consumption with the addition of a USB device may be greater than what the Class 3 power source can provide. In that case, the telephone detects this and instructs the user to use an Auxiliary power supply or to temporarily disconnect one or more of the modules while the USB device is in use. The system parameter USBPOWER determines for which power class(es) to enable power to the USB interface; see Chapter 7 in the *Avaya one-X® Deskphone H.323 Administrator Guide*.

Important:

The last step in assembling the 9600 Series IP deskphone must be applying power with any modules and/or adapters (and excluding USB devices, headsets, etc.). 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). See Completing the power connection on page 18 for details.

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 telephone assembly.

Telephone Model:	See:
9608 or 9611G	Connection jacks on a 9608 or 9611G deskphone on page 17
9621G or 9641G	Connection jacks on a 9621G or 9641G deskphone on page 18

Note:

Some deskphone models, for example the 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 Web site.

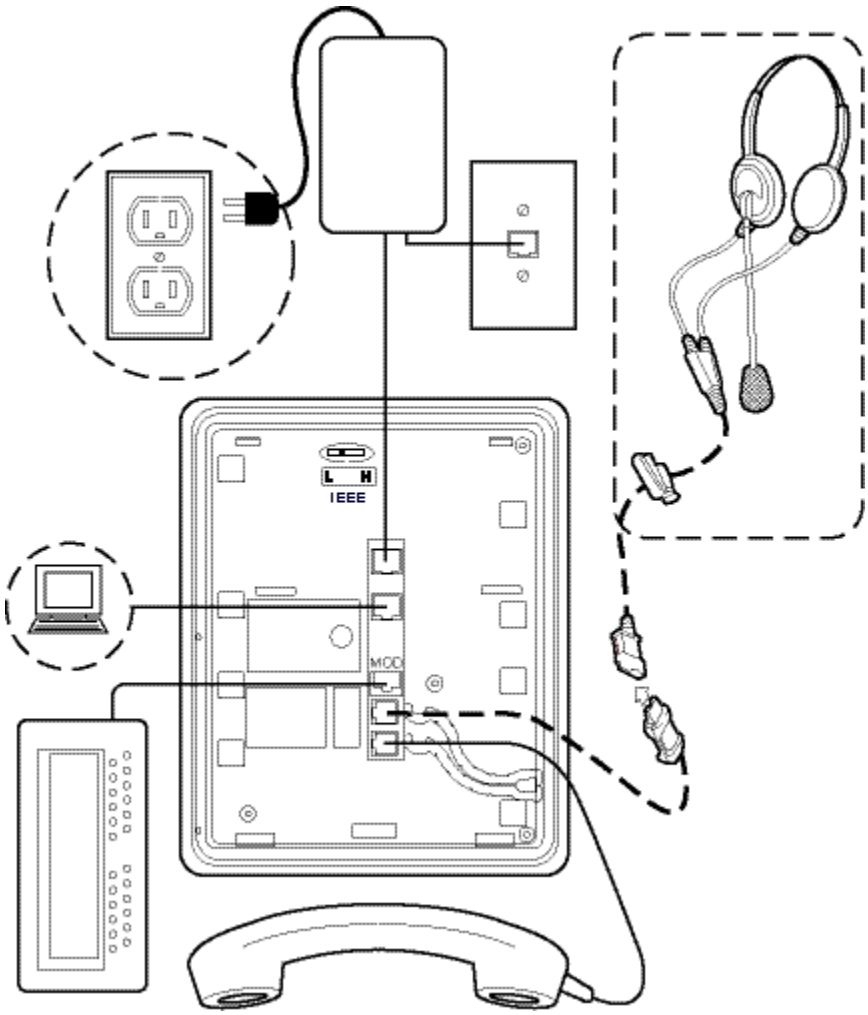


Figure 1: Connection jacks on a 9608 or 9611G deskphone

Note that some models of the 9608 deskphone may have the IEEE switch below the button module switch denoted by MOD.

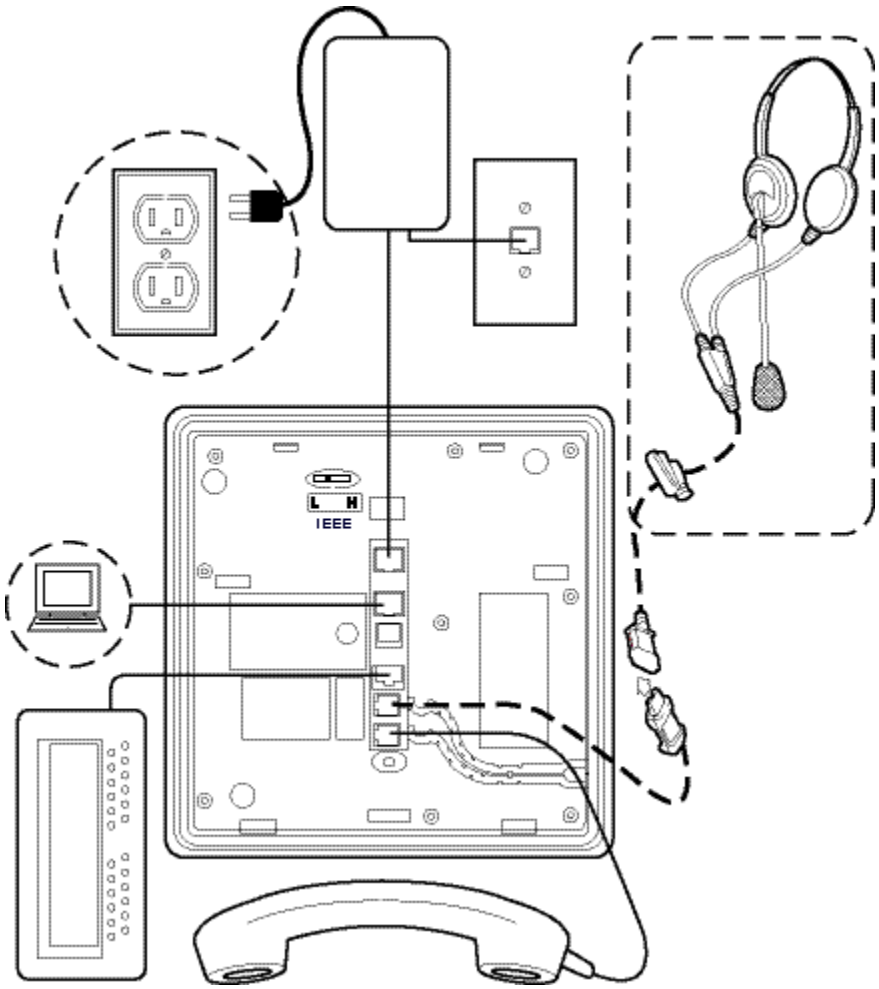


Figure 2: Connection jacks on a 9621G or 9641G deskphone

Note that the 9621G does not support a button module, USB device, or a Dual Headset Adapter. It does not have a IEEE power switch.

Completing the power connection

Procedure

1. Plug one end of the H4DU 4-conductor coiled handset cord into the phone and the other end into the handset.
2. Plug one end of the first Category 5 modular line cord into the Ethernet jack of the PC and the other end into the secondary Ethernet jack on the phone, if appropriate.

3. If the deskphone is to be IEEE-powered, plug one end of the second Category 5 modular line cord into the Ethernet jack on the phone.

   Plug the other end of this cord into the Ethernet wall jack. You are now finished. Do not proceed to Step 4.

4. If the deskphone is to be powered locally, connect the Category 5 modular line cord provided with the IP Phone Single Port PoE Injector (SPPOE-xx, where *xx* represents the model number) into the Ethernet jack on the phone. Plug the femite end of this cord into the deskphone. Plug the other end of this cord into the SPPOE-xx power injector jack labeled **DATA & POWER OUT**. Plug another Category 5 cord into the SPPOE-xx power injector jack labeled **DATA IN**. Plug the other end of this cord into the Ethernet wall jack. Finally, connect the SPPOE-xx to an AC power source.

Installing a Dual Headset Adapter (DHA)

About this task

As of software Release 6.1, a Dual Headset Adapter (DHA) is available for installation on call center deskphones. The DHA allows a supervisor to monitor calls in progress and can be attached either directly to a 9641G, 9611G, or 9608 deskphone or to an attached button module. The 9621G does not support a DHA.

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

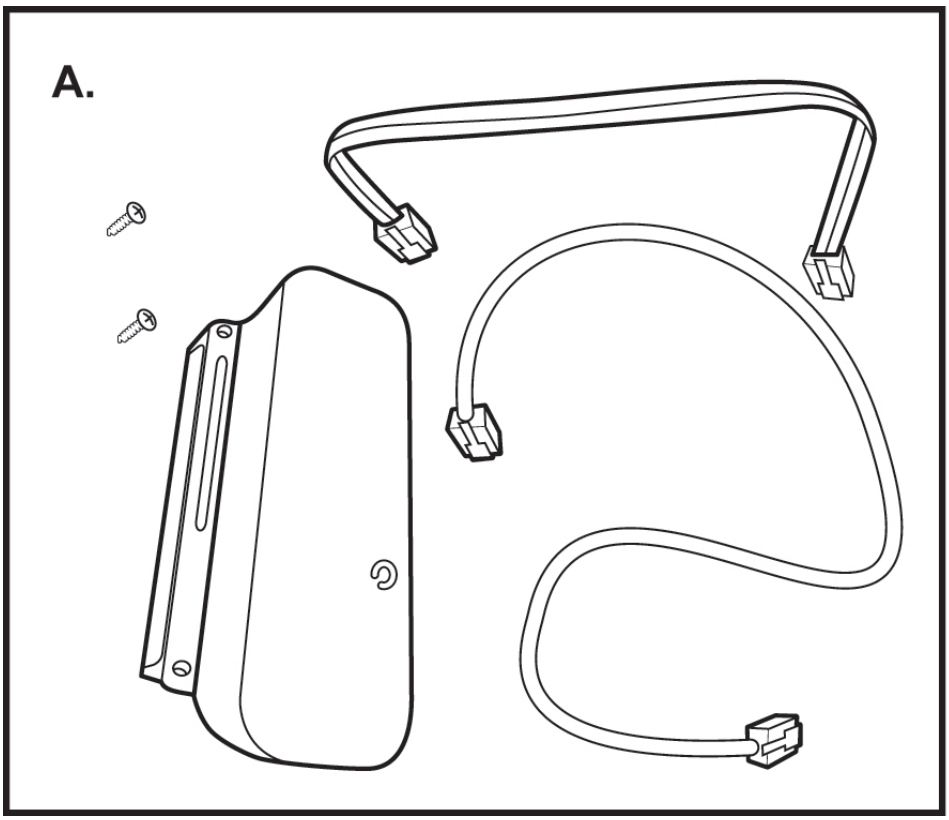


Illustration A shows the DHA Package Contents.

The following illustrations show how to install a DHA directly to the deskphone and (alternately) to an attached button module.

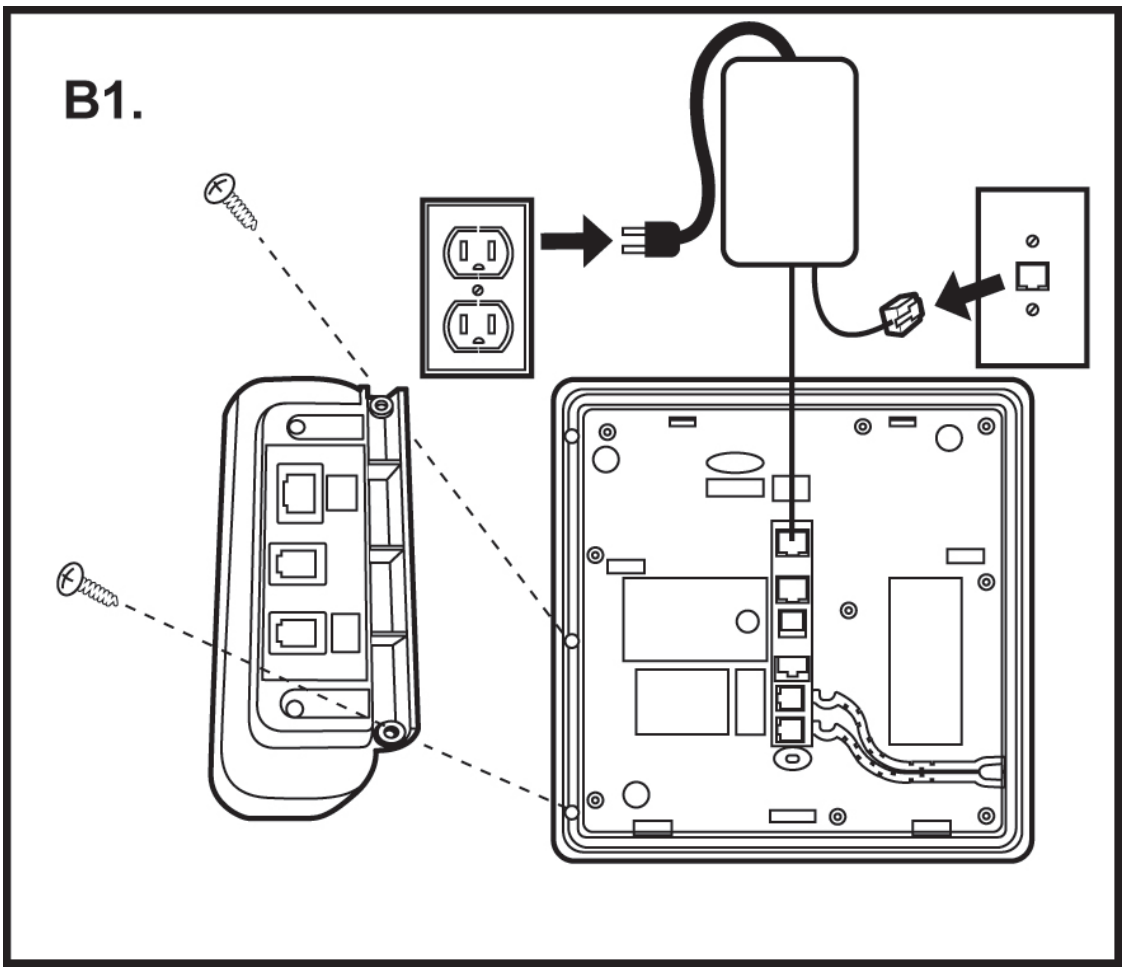


Illustration B1 shows how to attach the DHA to a deskphone.

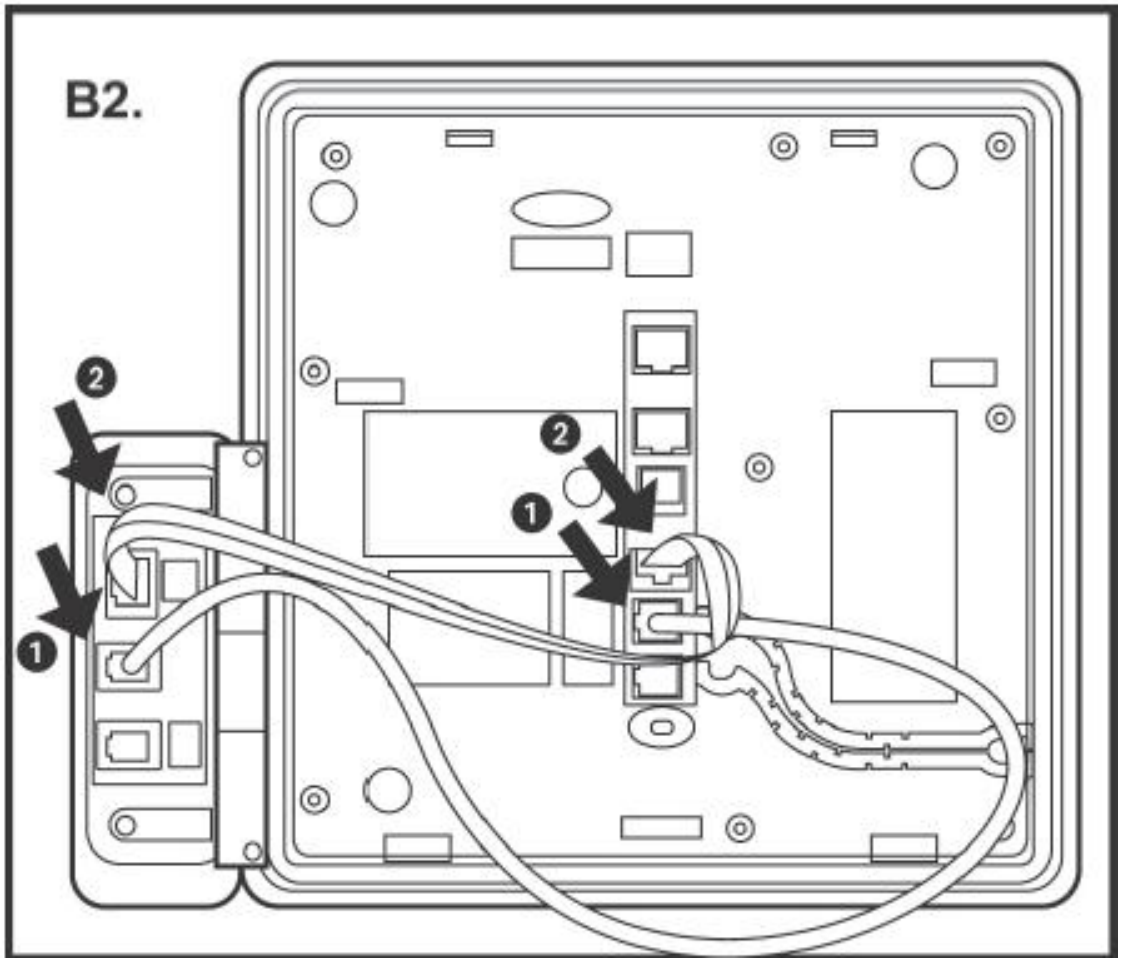


Illustration B2 shows how to connect the DHA power and audio cables.

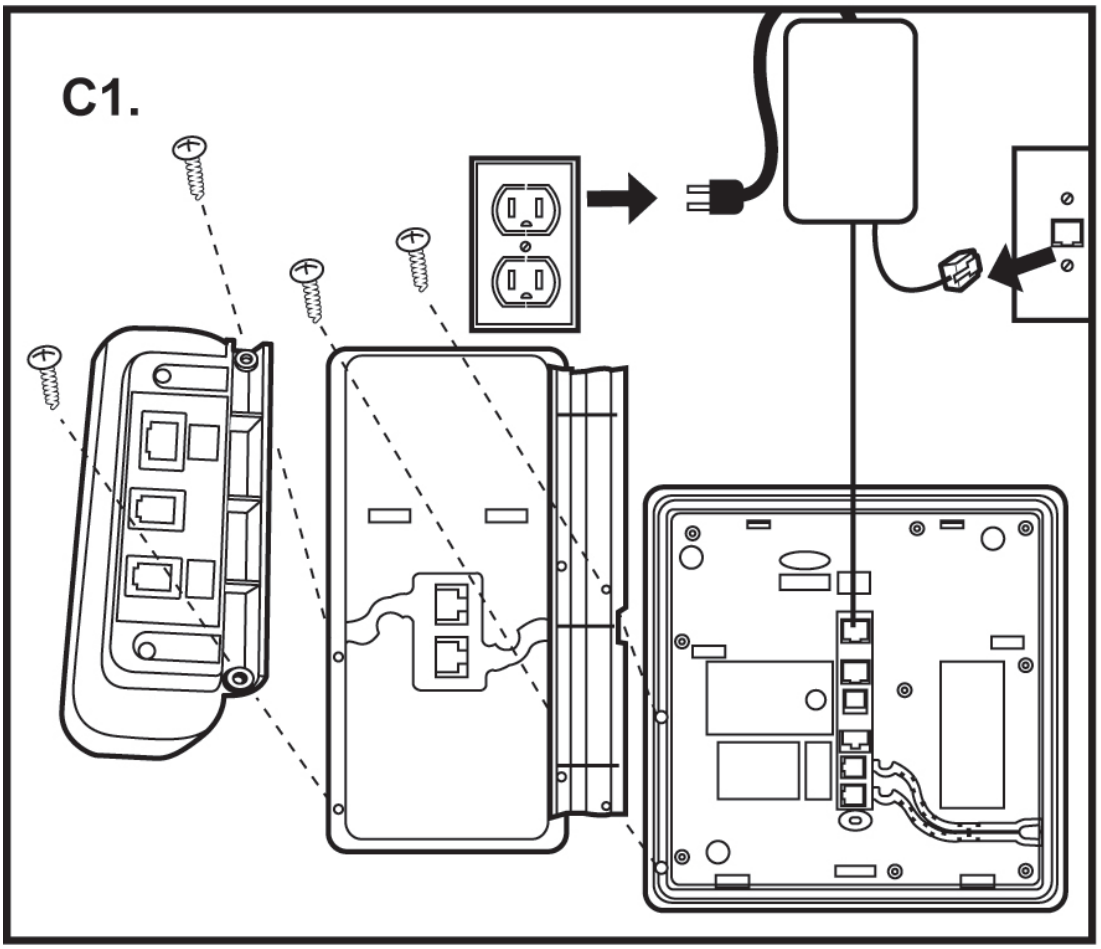


Illustration C1 shows how to connect the DHA to an (optional) button module.

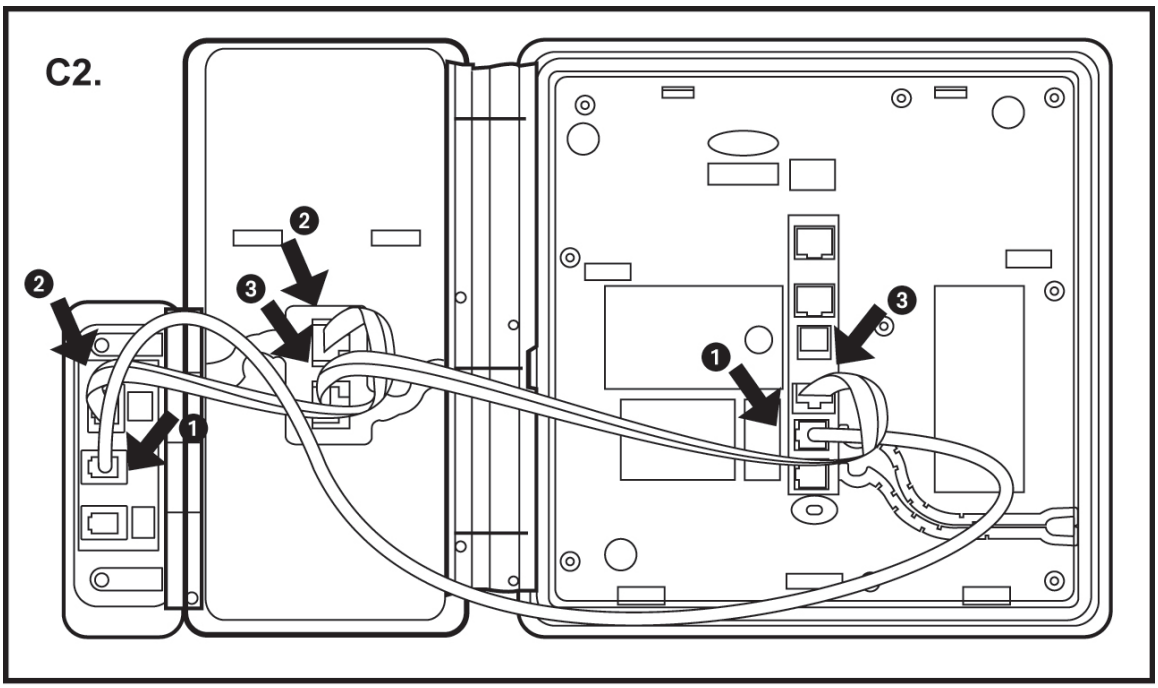


Illustration C2 shows the cable connection of the DHA to an optional button module and the deskphone.

9641G Call Center faceplate installation

About this task

Special faceplate kits are available for 9641G IP Deskphones (9641G Call Center Faceplate Kit (PK25) (Comcode 700500728) used in a call center. The removeable faceplate has the following features:

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

Note:

The **Release** button must be administered as such, the AGTSPKRSTAT parameter set to "2" and the CALLCTRSTAT parameter set to "1" to allow Release button operation for 9641G deskphones.

To install the 9641G Call Center faceplate:

Procedure

1. If already connected, remove the HAC cord from the underside of the phone.
2. With the phone face-up and resting flat on a hard surface, pry up a corner of the standard faceplate. (Use your fingers, a flat screwdriver, or other non-sharp device.) Continue prying around the edge of the standard faceplate until it is released from the phone.
3. Align the tabs on the 9641G Call Center faceplate with the slots on the deskphone's outer edges and push down to lock the tabs into the slots.
4. Be sure that the display bezel surrounding the screen is in its proper position.
5. Plug the HAC cord back into the underside of the phone.

About powering-up and resetting the deskphone (Dynamic Addressing Process)

Note:

Before starting this process you must have an extension number for the IP telephone and the Communication Manager security code (password) for that extension, unless the deskphone will use unnamed registration. For more information, see About unnamed registration on page 31. Any reference to the HTTP server applies equally to an HTTPS server. The following description of the process of IP deskphone power-up or reset assumes that the process is executed successfully. For errors that might be encountered during the process and the messages displayed, see Chapter 5: Troubleshooting on page 67.

The initial display messages, some of which are part of DHCP give a "power on" indication and dynamic feedback as the telephone 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.

About deskphone initialization

The following description describes the software architecture upon which the requirements are based, as well as providing a high-level overview of how the telephone 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, and
- one Temporary Storage area.

Two Kernel/Root File Systems are supported in case one becomes corrupted, but only one is activated when the telephone 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 telephone starts up, 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, it 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 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 telephone 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 telephone. 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 telephone 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 telephone application attempts to register with a call server.

How the power-up and reset process works

When you plug the IP 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 phone is plugged in. For software upgrades, including the boot file and application file download, the process might take 5 to 10 minutes. The duration is based on LAN loading, how many telephones are being installed at once, and similar factors. Do not unplug the power cord during the download process.

During hardware initialization, the system initialization values NVCONTRAST and NVBRIGHTNESS are checked for non-null values, and set accordingly. The Avaya one-X® name and logo display on sets with bit-mapped displays.

1. The system initialization value for the language file in use (NVLANGFILE) is checked for a non-null value, in which case the text strings in that language file are used for text display. Otherwise, English text strings are displayed.
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 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 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 value of the persistent parameter APPINUSE 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 value of the APPINUSE parameter 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 telephone 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 telephone displays the speed of the Ethernet interface in Mbps, that is, 10, 100, or 1000. The message `No Ethernet * to program` 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 telephone and any attached PC, assuming the administrator has not disabled the latter interface by a PHY2STAT setting.

   Important:

   Pressing * (asterisk) whenever a "`* to program`" message displays or whenever the initialization process can support an interrupt invokes the Craft Access entry procedure to allow manual settings, but only if the PROCSTAT (local dialpad procedure status) system value is "0." The zero PROCSTAT value provides full access to local procedures. If PROCSTAT is "1" the Craft Access entry procedure

can be invoked only when a "`* to program`" message displays but only the VIEW procedure is available. For information, see Chapter 3: Using Local Administrative (Craft) Options. on page 33

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

   One of the following messages displays:

   `DHCP: s secs * to program`

   or `DHCP: s secs VLAN ID = n`

   or `DHCP: s secs`

   where *s* is the number of seconds that have elapsed since DHCP was invoked. The first messageappears if 802.1Q tagging is off and access to local programming procedures is not disabled or restricted. (See Chapter 3: Using Local Administrative (Craft) Options on page 33 for specifics.) The middle message appears if 802.1Q tagging is on and access to local programming procedures is disabled or restricted. If the first and middle messages alternate every two seconds, 802.1Q tagging is on. When both messages alternate, access to local programming procedures is not disabled or restricted. Finally, the third message appears if 802.1Q tagging is off and access to local programming procedures is disabled or restricted.

6. Determination of the DHCP protocol (IPv4 or IPv6) is done, and the applicable parameters enabled.

   Important:

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

   Note:

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

   The DHCP server provides IP Addresses for the following hardware:

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

7. Using the list of gateway IP Addresses provided by the DHCP server, the telephone performs a router check. The telephone 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.

8. While the IP telephone connects to the HTTP server, the telephone displays one of the following messages :

   `HTTP: n ipadd`

   or `HTTP: n ipadd * to program`

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

   Important:

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

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

    The GET message might have to be sent several times. Each time the GET message is sent, all IP telephones display the following message: `HTTP: n uri`

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

    Note:

    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.

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

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

12. When the telephone determines that the application file received is valid, the following message displays: `File Obtained; please wait..... s secs`

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

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

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

14. The telephone contacts the Avaya Media Server and attempts to log in.

All IP telephones display a version of the following prompts for an extension: `Login`, `Enter Extension`, or `Enter Extension and press Enter or OK`.

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

    Note:

    Unnamed registration is the capability to register a telephone with the call server without entry of an extension or password. The UNNAMEDSTAT parameter must be set to enable unnamed registration. Telephones registered unnamed have limited functionality. For more information, see About unnamed registration on page 31.

    All IP telephones display a version of the following prompts for a password:

    ```
    Login

    Enter Password

    Enter Password and press Enter or OK
    ```

16. Enter the password and press **OK**. To register the telephone without the extension or password (unnamed), press **OK** or make no entry and wait 60 seconds.
17. The extension is visible as you enter it but the password displays as asterisks. The system determines whether the extension is in use.
18. Successful completion of this process produces a dial tone when the **Speaker** button is pressed or the handset is lifted.

    The IP telephone was installed successfully.

About unnamed registration

Unnamed registration is a capability an IP telephone can have to register with a call server, and receive limited service, without requiring an extension and password entry. Typical environments where this functionality is useful include:

- “Hot-desking” environments where there is a period of time between one user logging out and another user logging in on the same telephone.
- Using the Avaya Softphone application in “road warrior” mode, which allows a traveller to invoke the telephony features and functionality by taking over the office telephone extension. This takeover unregisters the office telephone.

In both examples, the user unregisters the telephone by logging off or by taking the office telephone extension over to another telephone. Without unnamed registration, the telephone in the first example will just wait for an extension and password entry and the telephone in the

second example will continue attempting to register at regular intervals. The downside of a telephone being unregistered is that no one can use the telephone, for example, to report a building emergency like a fire.

Unnamed registration allows the telephone to register without an extension and password. Because there is no extension, telephony functionality is limited, specifically:

- The user has only one call appearance, and hence, cannot transfer or conference calls.
- The user has no administered feature buttons, and cannot invoke on-hook dialing.
- Extension-based information, like a given user's Contacts data or Option settings are not available.
- The user is limited to the calling capability administered for PSA (Personal Station Access) on the call server, for example, access to an emergency number.
- The telephone cannot receive any outside calls.

Unless otherwise disabled, the telephone automatically attempts to register unnamed if no action is taken on the telephone Extension entry screen within 60 seconds. Initiating any ID or password entry disables and prevents unnamed registration from occurring. Unnamed registration is ignored after any dialpad entry.

Administrators can disable unnamed registration by appropriately administering the system parameter UNNAMEDSTAT, as indicated in Chapter 7 of the *Avaya one-X® Deskphone H.323 Administrator Guide*. Unnamed registration appears to the end user like Communication Manager TTI Mode, and is similar from an administration perspective. For more information about TTI, see your Communication Manager documentation.

Chapter 3: Using Local Administrative (Craft) Options

About local (Craft) procedures

During installation or after you have successfully installed an 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.

There are two forms of Local Administrative Options. One allows access to all the capabilities and functionality described in this chapter while the other allows access only to an administrable level of VPN capabilities and functionality. The VPN-specific option allows the administrator to grant VPN users access to the VPN procedure itself, while preventing these users from accessing any other Local Administrative Procedure. The administrator may grant the VPN user permission to change VPN settings or only to view them. For more information on access to VPN-only Local Administrative Options, see the *VPN Setup Guide for 9600 Series IP Telephones (Document 16-602968)*.

Note:

You can modify the settings file to set parameters for any IP deskphones that download their upgrade script and application files from the same HTTP server. See Chapter 4: Maintaining 9600 Series IP Deskphones on page 61 and “9600 Series IP Telephone Scripts and Application Files” in Chapter 4 of the *Avaya one-X® Deskphone H.323 Administrator Guide*.

Caution:

Only trained installers or technicians should 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 telephone until either:

- a new boot file is downloaded, or
- the IP telephone is reset, as indicated in Resetting system values on page 55.

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 Powering-up and resetting the deskphone (Dynamic Addressing Process) on page 25.

Accessing local (Craft) procedures

Note:

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

When PROCSTAT is “0” (full access to local Craft procedures) you can invoke local craft procedures during initialization whenever this message displays:

```
* to program
```

or at any other time the initialization process can support a processing interrupt. If PROCSTAT is set to “1” (access allowed only to the VIEW craft procedure for debugging purposes), you can invoke local Craft procedures only when the “`* to program`” message displays during initialization.

Note:

The “`* to program`” message is supported even if the value of PROCSTAT is “1” when the messages “`Address conflict`,” “`Subnet conflict`,” “`Bad router?`” and “`Bad FileSv address`” display. Allowing Craft procedure access in response to these messages prevents situations in which input is required but not allowed.

Note:

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

Accessing Craft procedures during startup

Procedure

1. During deskphone startup, invoke local procedures by pressing ***** to display the Craft Access Code Entry screen:

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

2. Enter the local dialpad procedure password (0 to 7 numeric digits), as specified by the system administrator in the system value PROCPSWD.

   For security purposes, the telephone displays an asterisk for each numeric dialpad press. If you are using a touchscreen deskphone, and need to backspace during

password entry, use the Contacts button; for non-touchscreen phones, use the left arrow button or the designated softkey.

3. Press # when the password entry is complete.

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

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

Accessing Craft procedures during normal operation

Procedure

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

   If you are using a touchscreen phone and need to backspace during password entry, use the Contacts button; for non-touchscreen phones, use the left arrow button or the designated softkey.

   A six second time-out is in effect between button presses after pressing the **Mute** button. 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.

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

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

About this task

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

Procedure

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

   To select the item on that line, press the appropriate softkey at the bottom of the screen, for example, **Change** or **Save**, or the **OK** button. 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 telephone 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, an error beep tone sounds, the digit is ignored, 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.

   If the asterisk dialpad button is pressed and the user is entering an IPv4 address, a decimal point is inserted into the input buffer and the cursor is moved to the next character location. If the asterisk dialpad button is pressed and the user is entering an IPv6 address, a colon is inserted into the input buffer and the cursor is moved to the next character location. See Entering and validating IPv4 and IPv6 addresses on page 37 for additional information on entering data in IPv4 and IPv6 format.

5. To backspace on non-touchscreen phones, press the leftmost softkey; for a touchscreen deskphone, use the **Bksp** softkey instead.

   When you press the applicable button or key to backspace, the most recently entered digit or period is erased from the display. The cursor remains in the erased character's former position.

6. Pressing **Exit** (or touching that softkey for a touchscreen deskphone) exits the local procedures.

   Important:

   If any changes were made using the 802.1X procedure or the ADDR procedure, if the value of SIG was changed to 2 (SIP) or if the Crafts Entry screen was invoked during startup, the telephone immediately resets upon pressing/touching **Exit**. If no 802.1X, SIG, or ADDR changes were made, or if the local procedures

were invoked post-startup, the telephone redisplays the screen (or other display) that was effective when the craft options was invoked.

Note:

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

Note:

Some touchscreen deskphones present an onscreen keyboard that allows you to “type” the data you want to enter on the display. See the applicable user guide for information about using the onscreen keyboard.

About entering and validating IPv4 and IPv6 addresses

The dialpad uses numeric-only entry (single-tap for touchscreen telephones)when an IPv4 address or the subnet mask is entered, except for entry of an asterisk to place a period within the address being entered. While the cursor is in any of the leftmost three fields, pressing the “*” button on the dial pad causes the value for the field being entered to be terminated (a zero is displayed if nothing else is), a period to be displayed in the space after the field, and the cursor to move to the next space. Pressing the “*” button while the cursor is in the last (right most) field results in an error beep and the cursor being left where it is. An IPv4 address or subnet mask is considered to be complete only if all three 'dots' that separate the fields are entered and if the value of each field is valid. The following actions cause the value of a given field to be considered invalid:

- Entering a digit that would cause the value of the first field of an IPv4 address to exceed 223.
- Entering a digit that would cause the value of the last three fields of an IPv4 address to exceed 255.
- Entering a digit that would cause the value of any field of a subnet mask to exceed 255.

When entering an IPv6 address the dialpad uses numeric-only entry (single-tap for touchscreen telephones, except for “2” and “3” which are alphanumeric multi-tap). Pressing dialpad button “2” initially enters a “2”, followed by “A”, “B”, “C”, and back to “2”. Pressing dialpad button “3” initially enters a “3”, followed by “D”, “E”, “F”, and back to “3”. While the cursor is in any of the leftmost seven fields, pressing the “*” (asterisk) dialpad button causes the value for the field being entered to be terminated (a zero is displayed if nothing else is), a colon to be displayed in the space after the field, and the cursor to move to the next space. Pressing “*” while the cursor is in the last (right most) field results in an error beep and the cursor being left

where it is. An IPv6 address is considered to be complete only if all the following conditions are met:

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

In a given text entry field, if the either an IPv4 or an IPv6 address can be specified, the initial field can be ambiguous with respect to whether the entry is an IPv4 or IPV6 address (for example, “123” might be an IPv4 “123 decimal” or an IPv6 “0123 hex”). In such cases, text entry follows the IPv6 rules that hexadecimal characters are allowed and the “*” key inserts a colon character. If the entry is a hex character (A-F) or a fourth character is entered in the field, the telephone assumes the input is IPv6 format. Otherwise, the telephone makes the initial validity check when a field boundary (colon or decimal point) is entered. This initial typographic character determines whether the overall address should be in IPv4 format (a decimal point is entered) or in IPv6 format (a colon is entered). Once this character is entered, the telephone examines the contents of the first field to ensure it is consistent with the field boundary (no hex characters, and at most three characters of value 255 or less, in the first field if the field boundary is a decimal point). If the first field contains any content inappropriate for the entered field boundary, an error beep is generated and more content cannot be entered until the contradiction in the text string is deleted, meaning either the field boundary is deleted or the cursor is moved back and the field contents edited). Once content is entered that unambiguously identifies the format of the IP address (a decimal point for IPv4, or a colon for IPv6), the rest of the address entry is set according to that format, as specified in the bullet lists above.

Local administrative (Craft) procedures menu

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

Note:

For touch screen-based deskphones, simply “touching” a line or a softkey produces the same result as selecting a line or a softkey on non-touchscreen (button-based) IP

Deskphones. Unless otherwise prohibited using administration, an end user can view but not change most of the parameters associated with Craft procedures. For more information, see the applicable user guide(s).

Shown As (this value always displays in English)	Craft Procedure Purpose	See
8021X	Set 802.1X operational mode	Setting The 802.1X Operational Mode on page 40.
ADDR	Address information programming	Using The pre-installation checklist on page 42 and Changing IP address information on page 42.
AGC	Enable/disable Automatic Gain Control	Disabling/enabling automatic gain control on page 46.
CALIBRATE SCREEN	Calibrate the touch screen	Calibrating The Touch Screen on page 45.
CLEAR	Clear all values to factory defaults	Clearing the deskphone settings on page 47.
CONT	Adjust the contrast of any Button Modules and any non-color deskphones	Adjusting contrast on button modules and non-color deskphones on page 48.
DEBUG	Enable/disable Debug Mode	Disabling/enabling debug mode on page 49.
GROUP	Set the Group Identifier	Changing The group identifier on page 50.
HSEQUAL	Handset audio equalization	Setting handset audio equalization on page 50
INT	Interface Control	Changing Ethernet interface control on page 51.
LOG	Enable/disable Event Logging	Disabling/enabling event logging on page 52.
LOGOUT	Log off the telephone	Loging off The deskphone on page 53.
MLS	View Multi-Language text Strings	Viewing multi-language strings on page 54.
RESET VALUES	Reset system initialization values to defaults	Resetting system values on page 55.
RESTART PHONE	Restart the telephone	Restarting The deskphone on page 56.

Shown As (this value always displays in English)	Craft Procedure Purpose	See
SIG	Set the signaling protocol download flag	Changing The signaling protocol on page 57.
SSON	Set the Site-Specific Option Number	Changing SSON settings on page 58.
TEST	Initiate a self-test	Performing a self-test on page 58.
VIEW	View current parameter values and file names	Using The VIEW craft procedure for troubleshooting on page 68.
VPN	Administer and/or view Virtual Private Network (VPN) settings	*VPN Setup Guide for 9600 Series IP Telephones(Document 16-602968).*

Note:

1. If this is a 9608, the CONT procedure is always listed. Otherwise, the telephone is a color phone and CONT is listed if and only if the telephone has at least one button module attached.
2. If the telephone software has VPN and media encryption disabled, VPN will not appear on this list. To determine if this applies to the telephone, go to the About Avaya one-X screen via the Avaya (A) Menu or Home screen as applicable to the phone, and select the Settings list. An About Avaya one-X screen with a “U” appended to the software release indicates the phone has VPN and media encryption disabled.

Setting the 802.1X Operational Mode

About this task

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

Note:

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

Procedure

1. When you select 802.1X from the Craft Local Procedure Screen, the following text displays:

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

   where the Supplicant line is the text string associated with the current system value of DOTIXSTAT (802.1X Supplicant Mode operation control), defined as:

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

     and the Pass-thru line is a text string associated with the current system value of DOT1X (802.1X Supplicant Mode)

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

2. Select (highlight) the line you want to change, then press **Change**.
3. Depending on which line you selected to change, the following text displays:

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

   where, if you selected the Supplicant line, the *setting* is the text string associated with the current system value of DOTIXSTAT, or if you selected the Pass-thru line, the *setting* is the text string associated with the current system value of DOTIX.

4. To change the setting, press the Right (or Left) navigation arrow to cycle through the applicable settings.

   Depending on the current value, the next sequential text string is selected and displayed as the New setting. For example when changing the Pass-thru mode, if the current value is Pass-thru mode, pressing the Choice Selector displays P-t w/ Logoff. If the current setting is disabled, pressing the Choice Selector changes the new setting to Pass-thru mode.

5. Press/touch **Save** to store the new setting and redisplay the Craft Local Procedure screen.

Using the pre-installation checklist

Before performing static programming of address information, verify that all the requirements listed in the" Requirements to verify for your network" section of the Creating the pre-installation checklist on page 12 are met. You do not have to consider item 4., 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 telephone from working. Such errors can also have a negative impact on your network. Print copies of this checklist for each subnet.

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

Changing IP address information

About this task

The usual way to assign IP Addresses to IP telephones is the automatic method described in Powering-up and resetting the deskphone (Dynamic Addressing Process) on page 25. 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.

Important:

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

Note:

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

Use the following procedure to invoke manual address information programming.

Procedure

1. When you select ADDR from the Craft Local Procedure Screen, the Static Addressing Local Procedure screen displays as follows with the prompt `Select address to change.`

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

where:

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

- *dddd* is the current value of NVL2QVLAN and *ddd* is the current value of NVVLANTEST, respectively.

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

If you want to	Then
Change any of the IP Address values (Phone, Call Server, Router, Mask, &/or File Server)	Use the dialpad to enter the new IP Address. IP Addresses have three sets of three digits followed by a period. Pressing ***** (asterisk) 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. If the asterisk dialpad button is pressed and the user is entering an IPv6 address, a colon is inserted into the input buffer and the cursor is moved to the next character location; the exceptions are entry of a Router or Mask address, which follows the IPv4 method of inserting a period rather than a colon. In addition to the examples that follow, entry and validation of addresses in either format is described in Entering and validating IPv4 and IPv6 addresses on page 37. For example, to enter the IP Address 111.222.333.444 in IPv4 format, press the number 1 on the dialpad three times then press *****, press the number 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. To enter an IP Address in IPv6 format the dialpad uses numeric-only entry (single-tap the desired dialpad key for touchscreen telephones), except for “2” and “3” which are alphanumeric (multi-tap for touchscreen telephones). For example, pressing button “2” initially enters a “2”, followed by “A”, “B”, “C”, and back to “2”. Pressing button “3” initially enters a “3”, followed by “D”, “E”, “F”, and back to “3”. Proceed to the next step.
Change the 802.1Q value	Use the Right navigation arrow to cycle through the text strings corresponding to the L2Q values defined as “Auto” if L2Q=0, “On” if L2Q=1, and “Off” if L2Q= 2 until the text string of the value you want to change to displays. Proceed to the next step.
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.

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

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

Calibrating the Touch Screen

About this task

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

Important:

Use 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:

Procedure

1. When you select CALIBRATE SCREEN from the Craft Local Procedure Screen, the telephone displays three softkeys - **Start**, **Default**, and **Cancel**.
2. Take one of the following actions:
   - Touch **Cancel** to return to the Craft Local Procedure screen without calibrating the screen.
   - Touch **Default** to reset the calibration parameters to the factory-set values, 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.
3. 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.
4. Touch the center of each target with the stylus within 10 seconds of its appearance.
   After all four targets have been touched, a confirmation tone sounds and a “Calibration successful” message displays.

5. Touch **Save** to return to the Craft Local Procedure screen. Calibration results are stored in the telephone's non-volatile memory.
6. Touch **Cancel** at any time to return to the Craft Local Procedure screen without completing the touch screen calibration.

Disabling/enabling automatic gain control

About this task

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

Note:

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

Note:

The user can potentially override the AGC local procedure settings, as described in the telephone user guide. If overridden, the backup file stores the AGC value(s) set by the user and ignores any setting established using this local procedure.

Procedure

1. When you select AGC from the Craft Local Procedure Screen, the following text displays:

Handset Automatic Gain control	On
Headset Auto Gain Control	On
Speaker Auto Gain Control	On

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

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

2. To change the setting, select (highlight) the appropriate line.

   Press **Change** to toggle the selected setting from On to Off or vice versa.

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

Clearing the deskphone settings

About this task

Sometimes, you might want to remove *all* administered values, user-specified data, and option settings. Essentially, you want to return a telephone to its initial “clean slate” or out of the box condition. This is usually done when passing a telephone to a new, dedicated user when the **LOGOFF** option is not sufficient. For example, a new user is assigned the same extension, but requires different permissions than the previous user.

The **CLEAR** option erases all administered data—static programming, HTTP and HTTPS server programming, and user settings including Contact button labels and locally programmed Feature button labels, and restores all such data to default values. The **CLEAR** option does not affect the software load itself. If you have upgraded the telephone, the telephone retains the latest software. Once you have cleared a telephone, you can administer it normally.

Caution:

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

Note:

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

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

Procedure

1. When you select CLEAR from the Craft Local Procedure Screen, the telephone displays the prompt `Press Clear again to confirm.`
2. If you do not want to clear all values, press **Cancel** to terminate the procedure and retain the current values.

   Press **Clear** to clear all values to their initial default values.

   The telephone displays the following text:

   ```
   Clearing values...
   ```

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

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

After clearing the values, the telephone resets.

Adjusting contrast on button modules and non-color deskphones

About this task

Note:

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

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

Procedure

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

   The factory default setting is the middle setting.

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

Disabling/enabling debug mode and sending the debug report to server

About this task

You can use the debug mode to send all your debug data in a file called nnn_report.gz where nnn is replaced by the telephone extension as specified by the user during registration.

Procedure

1. Select DEBUG from the Craft Local Procedure Screen, the following text displays:

Debug Mode	On
Send report to server ...	

   where the setting is the text string associated with the current system value of NVDEBUG, defined as:

   - “On” if the NVDEBUG system value is “1”
   - “Off” if the NVDEBUG system value is “0”

   Note:

   The second option Send report to server… is displayed only if the value of BRURI begins with a character sequence of “http://” or “https://”.

   The option will not be displayed if the value of BRURi is set to 'Null'.

2. The Status Line initially displays *Press Change to change the setting*. Press **Change** or touch **On** to toggle the selected setting from On to Off or vice versa. The softkeys **Save**, **Change**, and **Cancel** are displayed.
3. Select the second option using the navigation keys or the touch screen only after the first option is set to On. The Status line displays the options **Send** and **Cancel**.
4. Press or touch **Send** to send the debug data file to the specified location. If the file is saved successfully, the Top Line displays *Backup successful* for about five seconds. If the debug report file cannot be saved for any reason (e.g. the server is not available or refuses the request), the Top Line displays *Backup failed*.
5. If you have made any changes to the Debug Mode option, then you must press or touch the **Save** option. This action resets the phone and saves the changes to the debug screen.

   Pressing either **Save** or **Cancel** displays the Craft Local Procedure menu screen.

Changing the group identifier

About this task

Note:

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

Use the following procedure to set or change the Group Identifier.

Note:

Perform this procedure only if the LAN Administrator instructs you to do so. For more information about groups, see Applying settings to logical groups on page 65.

Procedure

1. When you select GROUP from the Craft Local Procedure Screen, the following text displays:

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

   where the *setting* is the current system value of NVGROUP.
2. Enter a valid **Group** value (0-999).
3. Press **Save** to store the new setting and redisplay the Craft Local Procedure screen.

Setting handset audio equalization

About this task

Note:

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

Procedure

1. When you select HSEQUAL from the Craft Local Procedure Screen, the following displays:

- Current Setting:
- New Setting:

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

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

2. Press **Save** to store the new setting and redisplay the Craft Local Procedure Screen.

Changing Ethernet interface control

About this task

Note:

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

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

Procedure

1. When you select INT from the Craft Local Procedure 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
- **1000Mbps full** when PHY1STAT = 6

The PHY2STAT text strings are:

- **Disabled** when PHY2STAT = 0
- **Auto** when PHY2STAT = 1
- **10Mbps half** when PHY1STAT = 2
- **10Mbps full** when PHY1STAT = 3
- **100Mbps half** when PHY1STAT = 4
- **100Mbps full** when PHY1STAT = 5
- **1000Mbps full** when PHY1STAT = 6

2. To change the Ethernet setting, press the Right navigation arrow 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 10Mbps half (2), pressing the Right navigation arrow changes the value to 10Mbps full (3). If the current value is 1000Mbps full (6), pressing the navigation arrow changes the value to Auto (1).
3. To change the PC Ethernet setting, select that line and press the Right navigation arrow to cycle through the possible settings.
4. Press **Save** to store the new setting(s) and redisplay the Craft Local Procedure screen.

Disabling/enabling event logging

About this task

Note:

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

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

Procedure

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

Log: *text string*	Choice Selector

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

   - **Disabled** when NVLOGSTAT = 0
   - **Emergencies** when NVLOGSTAT = 1
   - **Alerts** when NVLOGSTAT = 2
   - **Critical** when NVLOGSTAT = 3
   - **Errors** when NVLOGSTAT = 4
   - **Warnings** when NVLOGSTAT = 5
   - **Notices** when NVLOGSTAT = 6
   - **Information** when NVLOGSTAT = 7
   - **Debug** when NVLOGSTAT = 8

2. To change the setting, press the Right (or Left) navigation arrow to 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 Alerts (2), pressing the Right navigation arrow changes the value to Critical (3). If the current value is Debug (8), pressing the Right navigation arrow changes the value to Disabled (0).

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

Logging off the deskphone

About this task

Use the following procedure to log off a telephone.

Note:

If a user registered (logged in) via a USB device, this procedure is not applicable. The only way to log off a telephone registered with a USB device is by removing the device.

Note:

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

Caution:

Once a telephone is logged off, a password and extension might be needed to log back on.

Procedure

1. When you select LOGOUT from the Craft Local Procedure Screen, the telephone displays the following text:

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

2. Press **Cancel** to return to the Craft Local Procedure screen without logging off the telephone.

   Press **Log Out** to unregister the telephone from the call server.

Viewing multi-language strings

About this task

Note:

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

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

Procedure

1. When you select MLS from the Craft Local Procedure Screen, the following text displays:

   ```
   Tag # N

   Text string for tag # N        text string
   ```

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

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

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

3. Press **Back** to return to the Craft Local Procedure screen.

Resetting system values

About this task

Note:

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

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

Caution:

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

Procedure

1. When you select RESET VALUES from the Craft Local Procedure Screen, the telephone displays the following text:

   ```
   Press Reset to confirm.
   ```

2. Press **Cancel** to return to the Craft Local Procedure screen without resetting the telephone.

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

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

   - Resets all system values and system initialization values except AUTH and NVAUTH to default values.
   - Resets the 802.1X ID and Password to their default values.
   - Resets call server values to their defaults.
   - Deletes any entries in the Redial buffer.

- Does not affect user-specified data and settings like Contacts data or the telephone login and password. To remove this type of data, see Clearing the deskphone settings on page 47.

Restarting the deskphone

About this task

Note:

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

Use the following procedure to restart the telephone.

Procedure

1. When you select RESTART PHONE from the Craft Local Procedure Screen, the telephone displays the following text:

   ```
   Press Restart to confirm.
   ```

2. Press **Cancel** to return to the Craft Local Procedure screen without restarting the telephone.

   Press **Restart** to proceed with the registration steps covered in the Powering-up and resetting the deskphone (Dynamic Addressing Process) on page 25.

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

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

Setting or changing the signaling protocol

About this task

Note:

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

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

Note:

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

Procedure

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

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

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

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

2. To change the setting, press 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 the Right arrow changes the value to 2 (SIP).

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

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

Changing SSON settings

About this task

Caution:

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

Note:

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

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

Procedure

1. When you select SSON from the Craft Local Procedure Screen, the following text displays:

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

   where the *setting* is the current system value of NVSSON.
2. To change the setting, use the dialpad to enter a valid SSON value between 128 and 255.
3. Press **Save** to store the new setting and redisplay the Craft Local Procedure screen.

Performing a self-test

About this task

Note:

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

Note:

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

For self-testing, use the following procedure:

Procedure

1. When you select TEST from the Craft Local Procedure Screen, the telephone displays the following text:

   ```
   Press Test to confirm.
   ```

2. Press **Cancel** to return to the Craft Local Procedure screen without testing the telephone.

   Press **Test** to start telephone testing.

   The test performs the following actions:

   - All softkeys are unlabeled.
   - Groups of no more than 13 LEDs at a time on the telephone and any attached button modules illuminate sequentially for about a half second. Illumination starts with the upper half of the telephone and continues through the lower half of any attached button module in a repeating cycle.
   - Pixels on the display are shown at their highest intensity.

     After approximately 5 seconds, the top Application line displays either “Self-test passed” or “Self-test failed.”

3. Press **Back** to return to the Craft Local Procedure screen.

Chapter 4: Maintaining 9600 Series IP Deskphones

About software distribution packages

Important:

For any new software release, be sure to 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 Web site at http:// www.avaya.com/support.

As of H.323 software Release 6.0 and later, Software Distribution Packages containing the files needed to operate the 9600 Series IP deskphones are packaged together in either a Zip format or an RPM/Tar format distribution package. You download the package appropriate to your operating environment to your file server from the Avaya support Web site at: http:// www.avaya.com/support based on the protocol you are using (H.323 or SIP) for all or the majority of your deskphones.

H.323 software distribution packages contain the following:

- One or more software files
- One upgrade file (96x1Hupgrade.txt)
- All of the display text language files
- A file named “av_prca_pem_2033.txt” that contains a copy of the Avaya Product Root Certificate Authority certificate in PEM format that may be downloaded to telephones based on the value of the TRUSTCERTS parameter
- file named “release.xml” that is used by the Avaya Software Update Manager application

Release 6.0 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:

The H.323 software Release 6.0 upgrade script file is not the same upgrade script file used for the 9600 Series IP deskphones running software Release 3.1.

Note:

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

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, which tells the deskphone whether the telephone 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 contains the option settings that enable, disable, or otherwise customize the settings you might need to tailor the Avaya IP Deskphones for your enterprise.

Note:

You can use one settings file for all your Avaya IP telephones including the 9600 Series IP deskphones covered in this document and in the *Avaya one-X® Deskphone H.323 Administrator Guide*, and 4600 Series IP telephones, as covered in the *4600 Series IP Telephone LAN Administrator Guide* (Document 555-233-507).

Downloading software packages

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

1. Stop the file server.
2. If you want to specify a port the telephones 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 Telephones.

You can download a default upgrade file from http://www.avaya.com/support. This file allows the telephone to use default settings for customer-definable options. Of course, these settings can also be changed with DHCP or in some cases, from the telephone's dialpad itself. However, you might want to open the default file and administer the options to add useful functionality to your Avaya IP Telephones. This file must reside in the same directory as the upgrade file, and must be called 46xxsettings.scr or 46xxsetting.txt. The Avaya IP Telephones can operate without this file.

Note:

Most Windows systems interpret the file extension `*.scr` as a screen saver. The 4600 IP Telephones originally used *.scr to indicate a script file. We highly recommend that the settings file have the extension `*.txt`.

Contents of the settings file

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

- Tags, which are lines that begin with a single "#" character, followed by a single space character, followed by a text string with no spaces.
- **`Goto`** commands, of the form `GOTO` *`tag`*. **`Goto`** commands cause the telephone 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. In pre-6.0 software releases, BOOTNAME and SIG could also be used. In software release 3.1 and later, VPNACTIVE can also be used. In software release 6.0 and later, SIG_IN_USE can also be used.
- **SET** commands, of the form `SET` *`parameter_name value`*. Invalid values cause the specified value to be ignored for the associated *parameter_name* so the default or

previously administered value is retained. All values must be text strings, even if the value itself is numeric, a dotted decimal IP Address, etc.

- Comments, which are statements with a "#" character in the first column.

Note:

Enclose all data in quotation marks for proper interpretation.

- GET commands, of the form `GET filename` . The telephone will attempt to download the file named by *filename*, and if it is successfully obtained, it will be interpreted as an additional settings file, and no additional lines will be interpreted in the original file. If the file cannot be obtained, the telephone will continue to interpret the original file.

The Avaya-provided upgrade file includes lines that tell the telephone to `GET 46xxsettings.txt` and `46xxsettings.scr`. These lines cause the telephone 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 telephone continues processing the upgrade script file. The upgrade script file is processed so that if there is no 46xxsettings.scr file, the telephone looks for a 46xxsettings.txt file. If the settings file is successfully obtained but does not include any setting changes the telephone stops using HTTP. This happens when you initially download the script file template from the Avaya support Web site, before you make any changes. When the settings file contains no setting changes, the telephone does not go back to the upgrade script file.

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 *Avaya one-X® Deskphone H.323 Administrator Guide* for details about specific parameter values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

Downloading text language files

About this task

Language files that will be used for text entry and display purposes must be stored in the same location as the 46xxsettings file or under the HTTP Server directory, defined using the `SET HTTPDIR HTTP server directory path` command.

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

Changing the signaling protocol

About this task

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

Procedure

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

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

2. You can set the SIG parameter on a per-phone basis using the SIG Craft procedure as described in Changing the signaling protocol on page 45 on page 57.

Applying settings to logical groups

You might have different communities of end users, all of which have the same model telephone, but which require different administered settings. For example, you might want to restrict Call Center agents from being able to Logoff, 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 parameter for this purpose. The GROUP system value cannot be set in the 46xxsettings file. The GROUP parameter can only be set on a telephone-by-telephone basis. To do so, first identify which telephones 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 telephone, instruct the installer or end-user to invoke the GROUP Local Administrative (Craft) procedure as specified in Chapter 3: Using Local Administrative (Craft) Options on page 33 and specify which GROUP number to use. Once the GROUP assignments are in place, edit the configuration file to allow each telephone of the appropriate group to download its proper settings.

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

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

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

 # HOTDESK {specify settings unique to Group 2}

 # END {specify settings common to all Groups}

Chapter 5: Troubleshooting

Resolving error conditions

About this task

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

Procedure

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, DEFINITY®/MultiVantage™.
   - If the telephone is supposed to be powered from the LAN, ensure that the LAN is properly administered and is compliant with IEEE 802.3af.
2. If you are using static addressing:
   - Use the VIEW option to find the names of the files being used and verify that these filenames match those on the HTTP/HTTPS server. See Using the VIEW craft procedure for troubleshooting on page 68 for more information. Check the Avaya Web site to verify whether the correct files are being used.
   - Use the ADDR option to verify IP Addresses. See Changing IP address information on page 42 for information.
3. If the deskphone is not communicating with the system (DHCP, HTTP, or Avaya Media Server), make a note of the last message displayed, as described in Installation error and status messages on page 72 and/or Operational errors and status messages on page 76.

   Consult the system administrator. Sometimes problems with Communication Manager - HTTP communications can be corrected by setting the HTTPPORT value to 81.
4. If you expect the telephone to be IEEE-powered, verify with the LAN administrator that IEEE power is indeed supported on the LAN.

Failure to hear DTMF tones

H.323 telephones do not send DTMF tones to non-H.323 telephones. The failure to hear DTMF tones sent by a far-end 9600 Series IP deskphone does not require any action on the user's part. The TN2302AP board does not pass in-band DTMF tones.

Correcting a power interruption

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

Using the VIEW craft procedure for troubleshooting

About this task

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

Note:

If so administered through OPSTAT, end users can access the Network Information option from the Avaya Menu's Phone Settings option to 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).

Important:

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

Note:

You can use the ADDR option to view IP addresses if needed. See Changing IP address information on page 42 in Chapter 3. The IP addresses might have been entered incorrectly. *Verify whether you were provided with correct* IP Addresses.

Procedure

1. When you select VIEW from the Craft Local Procedure Screen, the following system parameters display, as shown in Table 1 Parameter Values on page 69.

Note:

Use the Right navigation arrow to scroll through the viewable information where indicated in Table 1 Parameter Values on page 69.

Table 2: Parameter Values

Name	System Value	Format
Phone (IPv4)	*nnn.nnn.nnn.nnn*	Deskphone IP Address; IPADD value.
Phone (IPv6)	*hhhh:hhhh::hhhh:hhhh:hhhh*	Deskphone IP Address; NVIPADDV6 value.
Phone (IPv6LL)	*hhhh:hhhh::hhhh:hhhh:hhhh*	Deskphone IP Address; IPADDV6LL value.
Call Server	*nnn.nnn.nnn.nnn*	IP Address of the call server currently in use, otherwise “0.0.0.0.”
Supplicant	*ccccccccccccccc*	Text equivalent of DOT1XSTAT: if 0, Disabled; if 1, Unicast-only; if 2, Unicast/ multicast.
Pass-thru	*ccccccccccccccc*	Text equivalent of DOT1X; if 0, Enabled; if 1, Enabled w/ Logoff; if 2, Disabled.
Router (IPv4)	*nnn.nnn.nnn.nnn*	Up to 15 ASCII characters: the IP Address of the router in use.
Mask (IPv4)	*nnn.nnn.nnn.nnn*	Up to 15 ASCII characters: NETMASK value.
HTTP server	*nnn.nnn.nnn.nnn*	IP Address of last HTTP server used successfully during initialization or “0.0.0.0” if no file server was used successfully.
HTTPS server	*nnn.nnn.nnn.nnn*	IP Address of last HTTPS server used successfully during initialization or “0.0.0.0” if no file server was used successfully.
802.1Q	*cccc*	Text string corresponding to the L2Q value.
VLAN ID	*cccc*	Up to 4 ASCII characters. Value is L2QVLAN text “Auto” if 802.1Q tagging is 0

Name	System Value	Format
		or “On” if 802.1Q tagging is 1. If 802.1Q tagging is off (2), this line is not displayed.
VLAN Test	*ccc*	Up to 3 ASCII characters. Value is VLANTEST value if 802.1Q tagging is 0 or 1. If 802.1Q tagging is off (2), this line is not displayed.
Scroll **Right** to see the following additional parameters/values:		
L2 Audio	*n*	L2QAUD; layer 2 audio priority value.
L2 Signaling	*n*	L2QSIG; layer 2 signaling priority value.
L3 Audio	*nn*	DSCPAUD; Differentiated Services Code Point for audio.
L3 Signaling	*nn*	DSCPSIG; Differentiated Services Code Point for signaling.
Scroll **Right** to see the following additional parameters/values:		
Ethernet		Text string corresponding to PHY1STAT value, for example, “auto,” “100Mbps HDX,” 1000Mbps FDX.”
PC Ethernet		Test string corresponding to PHY2STAT value, for example, “disabled,” “100Mbps HDX,” 1000Mbps FDX.”.
Scroll **Right** to see the following additional parameters/values:		
Model	*96ccDccc*	Up to 8 ASCII characters: MODEL serial number.
Phone SN	*ccccccccccccccccc*	Telephone Serial Number, up to 18 ASCII characters.
PWB SN	*ccccccccccccccccc*	Printed Wiring Board (circuit board) Serial Number, up to 18 ASCII characters. Applies only to 96xx IP Deskphones that have a software-readable PWB serial number and comcode.

Name	System Value	Format
PWB comcode	*nnnnnnnnn*	9 ASCII numeric characters. Applies only to 96xx IP Deskphones that have a software-readable PWB serial number and comcode.
MAC address	*hh:hh:hh:hh:hh:hh*	Each octet of the MAC address displays as a pair of hexadecimal numbers.
Group	*nnn*	Up to 3 ASCII numeric characters: GROUP value.
Protocol:	*cccccccc*	Up to 8 ASCII characters, currently only “H.323.”
Application File	*filename.ext*	4 to 32 ASCII characters (primary application).
Ethernet	*cccccccc* Ethernet	2 to 8 ASCII characters, either “1000Mbps”, “100Mbps”, “10Mbps”, or “No.”
Kernel/RFS file	*bootcodename*	1 to 32 ASCII characters (backup image name).
Backup App File	*filename.ext*	4 to 32 ASCII characters (backup application).
Button Module 1	*ccccccccccccc*	14 ASCII characters. Version identifier of the software in the first attached Button Module, if applicable.
Button Module 2	*ccccccccccccc*	14 ASCII characters. Version identifier of the software in the second attached Button Module, if applicable.
Button Module 3	*ccccccccccccc*	14 ASCII characters. Version identifier of the software in the third attached Button Module, if applicable.
Proxy Server	WMLPROXY	Proxy server used for WML functions.
Voice Language File	NVVOXFILE	Language file (NVVOXFILE) designated for voice-initiated dialing. Not applicable for software Release 6.0.

2. Use the Right navigation arrow to scroll through the viewable information shown in the table.

3. Press **Back** at any time to return to the Craft Local Procedure screen.

Installation error and status messages

The 9600 Series IP deskphones issue messages in the currently selected language, or if the telephone is logged off, in the language specified by the LANGSYS parameter value. If English is not the selected language, the telephone displays messages in English only when they are associated with local procedures, for example, MUTE V I E W.

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

Note:

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

Table 3: Possible error and status messages during installation of 9600 Series IP deskphones

Message	Cause/Resolution
`802.1X Failure`	CAUSE: Incorrect credentials provided for authentication or not provided at all. RESOLUTION: Follow the display prompts and reenter the 802.1X ID and password.
`IPv4 or IPv6 Address Conflict`	CAUSE: The telephone has detected an IP Address conflict. RESOLUTION: Verify administration to identify duplicate IP Address(es).
`Authentication Error`	CAUSE: The call server does not recognize the extension entered. RESOLUTION: Confirm the extension is correct and is correctly administered on the switch. Then try registration again, taking particular care to enter the extension accurately.
`Bad FileSv Address`	CAUSE: The HTTP/HTTPS server IP Address in the IP telephone's memory is all zeroes. RESOLUTION: Depending on the specific requirements of your network, this may not be an error. If appropriate, either administer the DHCP server with the proper address of the HTTP/HTTPS server, or administer the telephone locally using the ADDR option. The ADDR option is explained in Using Local Administrative (Craft) Options on page 33.
`Bad Router?`	CAUSE: The telephone cannot find a router based on the information in the DHCP file for GIPADD.

Message	Cause/Resolution
	RESOLUTION: Use static addressing to specify a router address, or change administration on DHCP, as indicated in the *Avaya one-X™ Deskphone H.323 Administrator Guide*.
`Call Error`	CAUSE: The user was on a call when the connection to the gatekeeper went down, perhaps due to a network outage or a gatekeeper problem. The telephone attempted to automatically register with the same, or another, gatekeeper, but the responding gatekeeper had no record of the call. RESOLUTION: Wait for the call to end, and if the telephone does not automatically register, restart the telephone.
`Connecting...`	CAUSE: The telephone is attempting to establish a TCP connection with the call server. A resource needed to establish the connection might not be available or the 10 second buffer on switch-related actions might have expired. RESOLUTION: Allow the telephone to continue TCP connect attempts.
`Contacting call server...`	CAUSE: The telephone has rebooted successfully and is moving on to attempt to register with the call server. RESOLUTION: Allow the telephone to continue.
`DHCP: CONFLICT * to program`	CAUSE: At least one of the IP Address offered by the DHCP server conflicts with another address. RESOLUTION: Review DHCP server administration to identify duplicate IP Address(es).
`DHCPv6 Failure: (with message)`	CAUSE: A Reply message was received with a Status Code option that contains a status-code of 1 (UnspecFail) or a Reply message was received in response to a Renew or Rebind message with a Status Code option containing a status-code value other than 0 (Success) or 5 (UseMulticast). RESOLUTION: In the first case, DHCPv6 will be restarted. If this message is the result of a status-code value other than 1 or 5, IPADDV6 will be set to null; if dual-stack operation is enabled the phone will also cease use of its IPv4 address and IPADD will be set to null, and DHCP operation will proceed.
`Discover` *aaa.bbb.ccc.ddd*	CAUSE: The telephone is attempting to find a DHCP server, and the user is allowed to view IP Addresses. RESOLUTION: If this message appears for more than a few seconds, verify with the LAN Administrator that a DHCP server is appropriately administered on the network. If there is not supposed to be a DHCP server, you must “break into” the Discovering process and use static addressing. See Changing IP address information on page 42. To break into the Discovering process, press the **#** button, and when you see the “`100Mbs`” or “`10Mbs`” message, quickly press the ***** (asterisk) button.
`Discovering...`	CAUSE: The 96xx deskphone is attempting to find a DHCP server and the user is *not* allowed to view IP Addresses.

Message	Cause/Resolution
	RESOLUTION: If this message appears for more than a few seconds, verify with the LAN Administrator that a DHCP server is appropriately administered on the network. If there is not supposed to be a DHCP server, you must “break into” the Discovering process and use static addressing. See Changing IP address information on page 42. To break into the Discovering process, press the # button, and when you see the “`1000Mbps`”, “`100Mbps`” or “`10Mbps`” message, quickly press the ***** (asterisk) button.
`EEPROM error, repair required`	CAUSE: Downloaded application file was not downloaded or saved correctly. RESOLUTION: The telephone automatically resets and attempts to re-initialize.
`Emergency Option`	CAUSE: Incompatible emergency option. RESOLUTION: This should never happen. Contact Avaya.

`Extension in Use`
`Extension in use: <NNNN>`
`Press continue to take over this extension`
`Login|Continue`
	CAUSE: The call server detects an extension conflict with an existing set or Softphone.
	RESOLUTION: You can force the current telephone to register and thereby disconnect the other user by pressing **Continue**. When **Login** is selected instead, the deskphone re-prompts for entry of (a different) extension and password.

`Finding router...`	CAUSE: The telephone is proceeding through boot-up. RESOLUTION: Allow the telephone to continue.
`Gatekeeper Error`	CAUSE: The gatekeeper rejects the registration attempt for an unspecified reason. RESOLUTION: Review gatekeeper/call server administrations, including IP network parameters.
`Gateway Error`	CAUSE: DEFINITY Release 8.4 does not have an H.323 station extension for this telephone. RESOLUTION: On the station administration screen, ensure the DCP set being aliased for this IP deskphone has an H.323 station extension administered, in accordance with switch administration instructions. Since the 9600 Series IP Deskphones are not supported on DEFINITY Release 8.4, you must upgrade to a release that does support these telephones.
`Incompatible`	CAUSE: This release of the call server does not support the current version of the IP telephone. RESOLUTION: Upgrade to the current version of Communication Manager (3.0 or greater) software.
`Invalid file`	CAUSE: The telephone does not have sufficient room to store the downloaded file.

Message	Cause/Resolution
	RESOLUTION: Verify the proper filename is administered in the script file, and that the proper application file is located in the appropriate location on the HTTP/HTTPS server.
IP Address Error	CAUSE: The gatekeeper reports an invalid IP Address. RESOLUTION: This should never happen. Contact Avaya.
License Error	CAUSE: The call server does not support IP telephony. RESOLUTION: Contact Avaya to upgrade your license.
Limit Error	CAUSE: The call server has reached its limit of IP stations. RESOLUTION: Un-register telephones not in use, or contact Avaya to upgrade your license.
NAPT Error	CAUSE: A device between the telephone and the call server is invoking Network Address Port Translation, which the 9600 Series IP deskphones do not support. RESOLUTION: Contact the System Administrator to remove or re-administer the device.
No Ethernet	CAUSE: When first plugged in, the IP telephone 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.
Packet Error	CAUSE: Protocol timeout error. RESOLUTION: Reenter the correct extension and password. If the condition persists, contact the System Administrator.
Password Error	CAUSE: The call server does not recognize the password entered and displays the Login Error screen. RESOLUTION: Confirm the password is correct, then try registration again, taking particular care to enter the password accurately.
Request Error	CAUSE: The gatekeeper believes the telephone's registration request is improperly formatted. RESOLUTION: The telephone will automatically attempt to register with the next gatekeeper on its list. If the problem persists, reboot the telephone.
Restarting...	CAUSE: The telephone is in the initial stage of rebooting. RESOLUTION: Allow the telephone to continue.
Subnet conflict * to program	CAUSE: The telephone is not on the same VLAN subnet as the router. RESOLUTION: Press ***** (asterisk) to administer an IP Address on the telephone using Changing IP address information on page 42, or administer network equipment to administer the telephone appropriately.
System busy	CAUSE: Most likely, the number of IP endpoints on the call server is already at maximum, Less likely, network resource is unavailable.

Message	Cause/Resolution
	RESOLUTION: The telephone was attempting to access a network resource (DHCP server, HTTP server, or the call server) and was not successful. Check the resource being called upon for its availability. If the resource appears operational and properly linked to the network, verify that addressing is accurate and that a communication path exists in both directions between the telephone and the resource.
`System Error`	CAUSE: The call server has an unspecified problem. RESOLUTION: Consult your Avaya Media Server administration and troubleshooting documentation.
`Undefined Error`	CAUSE: The call server has rejected registration for an unspecified reason. RESOLUTION: Consult your Avaya Media Server administration and troubleshooting documentation.
`Updating: DO NOT UNPLUG THE TELEPHONE`	CAUSE: The telephone is updating its software image. RESOLUTION: Allow the telephone to continue.
`Waiting for LLDP`	CAUSE: No File Server and/or Call Server has been administered, so the telephone is expecting to get the missing data via LLDP. RESOLUTION: Administer the missing data by one of the following methods: statically, dynamically in DHCP, in the 46xxsettings file (for Call Server addresses), or by LLDP. For more information, see LLDP Troubleshooting on page 82.
`Wrong Set Type`	CAUSE: The call server does not recognize the set type. RESOLUTION: Ensure the call server is properly administered to expect the appropriate telephone for the IP Address and extension.

Operational errors and status messages

The table below identifies some of the possible operational problems that might be encountered after successful 9600 Series IP deskphone installation. The user guide for a specific telephone model also contains troubleshooting for users having problems with specific IP telephone applications. Most of the problems reported by deskphone users are not likely to be problems with the telephone itself. Problems are more likely LAN-based, where Quality of Service, server administration, and other issues can impact end-user perception of IP telephone performance.

Table 4: Operational error conditions for 9600 Series IP deskphones

Condition		Cause/Resolution
The telephone continually reboots, or reboots continuously about every 15 minutes.		CAUSE: The deskphone cannot find the HTTP/HTTPS server and/or call server. RESOLUTION: Ensure that MCIPADD is administered either manually or through DHCP or HTTP, as appropriate. Alternately, this might be a firmware fault because the MAC address in memory is corrupted; in this case, return the telephone to Avaya for repair.
The message light on the telephone turns on and off intermittently, but the telephone never registers.		CAUSE: This is a hardware fault. RESOLUTION: The telephone must be returned to Avaya for repair.
The telephone stops working in the middle of a call,	AND no lights are lit on the telephone and the display is not lit.	CAUSE: Loss of power. RESOLUTION: Check the connections between the telephone, the power supply, and the power jack. For example, verify that either static addressing was not used or that any changes to static addresses were entered correctly.
	AND power to the telephone is fine (and the telephone might have gone through the restarting sequence).	CAUSE: Loss of path to the Avaya call server, DHCP Lease expired, or DHCP server not available when telephone attempts to renegotiate DHCP lease. RESOLUTION: As above.
The telephone was working, but does not work now,	AND no lights are lit on the telephone and the display is not lit.	CAUSE: Loss of power. RESOLUTION: Check the connections between the telephone, the power supply, and the power jack.
	AND power to the telephone is fine, but there is no dial tone. The display might show “System Busy.”	CAUSE: Loss of communication with the call server. RESOLUTION: Check LAN continuity from the call server to the telephone using ARP or trace-route and from the telephone to the call server by invoking a Feature button. Verify that LAN administration has not changed for the Gatekeeper, TN 2302AP boards, or the LAN equipment (routers, servers, etc.) between the switch and the telephone. Verify no one changed the telephone settings locally using the VIEW and ADDR Craft codes, as described earlier in this guide. Verify the telephone volume is set high enough. Finally, conduct a self-test.

Condition		Cause/Resolution
	AND the telephone was recently moved.	CAUSE: Loss of communication with the call server. RESOLUTION: As above, but pay particular attention to the possibility that the telephone is being routed to a different DHCP server, or even a different call server switch. If so, the new server or switch might need to be administered to support the telephone.
	AND the network was recently changed to upgrade or replace servers, re-administer the Avaya Media Server, add or change NAT, etc.	CAUSE: Loss of communication with the call server. RESOLUTION: As above.
The telephone 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 Avaya Media Server trunk. RESOLUTION: Verify which trunk is causing the echo, and swap 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 cord. RESOLUTION: Ensure that an Avaya-approved headset cord is being used.
	the user is on Speaker and hears no echo, but the far-end hears echo.	CAUSE: Room acoustics. RESOLUTION: Ensure that there are six inches or so of blank space to the right of the telephone. 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 Menu) or **Home** button on the telephone. One or more Quality of Service (QoS) features should be implemented in the network as covered in Chapter 3:Using Local Administrative (Craft) Options on page 33. CAUSE: Improper non-Category 5 wiring. RESOLUTION: Replace non-Category 5 wiring with Category 5 wiring.
	the user hears fluctuations in the	CAUSE: The user has changed the Automatic Gain Control (AGC) or environmental

Condition		Cause/Resolution
	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.	acoustics are not consistent with the current audio settings. RESOLUTION: Try different on/off settings for the AGCHAND, AGCHEAD, and AGCSPKR parameters.
The telephone works properly except for the Speaker.		CAUSE: The Speaker was turned off at the call server. RESOLUTION: Administer the call server to allow that station's Speaker to operate. If that does not work, do a self-test on the telephone, as explained in the Performing a self-test on page 47 on page 58.
The telephone 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.
The telephone works properly, except sidetone DTMF is not heard.		CAUSE: Call server suppresses sidetone DTMF. RESOLUTION: On call server administration, on the Change-System-Parameters screen, enable On-Hook Dialing. If the user has Hands-Free Answer (HFA), answers a call using the Speaker and switches to the handset, pressing dialpad buttons does not send DTMF tones. This is a known bug, and the only current resolution is to disable HFA.
Hands-Free Answer (HFA) is administered but the telephone did not automatically answer a call.		CAUSE: HFA only works if the telephone is idle. A second call is ignored if it comes in while a call is in progress, including ringing before the first call is answered. RESOLUTION: None.
The HTTP/HTTPS script file and settings file are ignored (not being used by the telephone).		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.
The HTTP/HTTPS script file is ignored or not used by the telephone,	AND the HTTP/ HTTPS server is a LINUX or UNIX system.	CAUSE: The telephone expects lines of the script file to terminate with a **<Carriage Return> <Line Feed>**. Some UNIX applications only terminate lines with **<Line Feed>**. Editing the script file with a UNIX-based editor can strip a**<Carriage**

Condition		Cause/Resolution
		Return> from the file. Doing so causes the entire file to be treated as a comment, and thus be ignored. RESOLUTION: Edit the script file with a Windows® —based editor, or another editor that does not strip out the **<Carriage Return>**. CAUSE: UNIX and LINUX systems use case-sensitive addressing and file labels. RESOLUTION: Verify the file names and path in the script file are accurately specified.
	AND telephone 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 9600 Series IP Deskphones on page 61.
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.
Some settings in the settings file are being ignored while other settings are being used properly,	AND the setting being ignored is one or more of the AGC settings.	CAUSE: The user changed the AGC setting(s), which were placed in the backup/restore file of the user. RESOLUTION: The user can reset the AGC value(s) back to the desired setting(s), or the backup file can be edited to delete the custom AGC settings.
Telephone power is interrupted while the telephone is saving the application file and the HTTP/HTTPS application stops responding.		CAUSE: The HTTP/HTTPS server stops responding if power is interrupted while a telephone is saving the application file. RESOLUTION: Restart the HTTP/HTTPS server, as applicable.
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 Chapter 7 of the *Avaya one-X™ Deskphone H.323*

Condition		Cause/Resolution
		Administrator Guide, are accurately specified in the 46xxsettings file.
User data disappeared when the user logged off one telephone and logged into another telephone.		CAUSE: The second telephone is unable to access the backup file. RESOLUTION: Verify that the first telephone created a backup file by checking that the appropriate administration was done in accordance with Chapter 7 of the *Avaya one-X® Deskphone H.323 Administrator Guide*. Then verify that the second telephone is administered to retrieve data from the same location as the first telephone. Again, check that the appropriate administration was done in accordance with Chapter 7 of the *Avaya one-X® Deskphone H.323 Administrator Guide* Finally, verify that the HTTP/HTTPS server on which the backup file is located is operational and accessible from the second telephone.
The user reports button module buttons are not labeled when they should be.		CAUSE: Improper administration on the call server. RESOLUTION: Verify correct administration.
The user reports personalized labels cannot be placed on the button module's buttons,	AND the user has tried using the Program AD button feature.	CAUSE: Improper administration on the call server. RESOLUTION: Verify correct administration.
	AND the user has tried using the Personalize Labels option on the telephone.	CAUSE: The user has been pressing the button module button to indicate which button to relabel. RESOLUTION: The user should use the list displayed on the telephone, scroll to highlight the desired button label, and press either **OK** or the corresponding line button.
The user reports inability to access Contacts or backed-up Call Log entries, or user options.	AND the user is registered via a USB login.	CAUSE: The telephone is working as designed. RESOLUTION: Remove the USB device and log in locally.
The user reports that pressing "My Pictures" causes the default (Avaya) or administered (custom)	AND the user is registered via a USB login.	CAUSE: One or more files in the USB pictures directory are not in proper .jpg format or are too large for the given telephone to display. RESOLUTION: Check the file format and verify that height/width limits as specified in the User Guide are followed.

Condition		Cause/Resolution
screensaver to appear,		
Touchscreen deskphones only. User gets “Could Not Access Internet Service” message from the World Clock or Weather application.		CAUSE: Most likely, WMLPROXY and/or WMLPORT have not been properly administered. RESOLUTION: Administer the missing data in the 46xxsettings file, as indicated in the *Avaya one-X® Deskphone H.323 Administrator Guide*.

LLDP Troubleshooting

If the “Waiting for LLDP” message appears for more than a few seconds, it generally indicates a problem with getting a value for the Call Server IP address. This can occur due to incorrect settings in script files or in the way the network has been configured.

When the telephone boots, it expects to find a valid IP address for the Call Server. This value, known as MCIPADD, can come from several sources:

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

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

Proposed Solution

Procedure

1. A more robust way to provide this value is to use DHCP. The DHCP server can be administered to provide MCIPADD using DHCP Option 242. (Note that TLSSRVR, HTTPSRVR and L2QVLAN can also be administered using this option). Telephones using non-static addressing automatically do a DHCP request (Option 242 is the 96xx default DHCP offer) and may get MCIPADD (and other addresses) this way.

2. Another reason for receiving the “Waiting for LLDP” message is that both the HTTP and HTTPS Server IP address are not administered. To administer the HTTP and/or HTTPS server, use the Craft ADDR procedure and enter the correct HTTP and/or HTTPS File Server IP address in the File Server field.
3. An alternative protocol known as LLDP can also supply call server and file server (HTTP and/or HTTPS) IP addresses. This IETF standard protocol requires the network to be equipped and configured to support LLDP. With LLDP in the network, HTTP and/or HTTPS Server and Call Server IP addresses can be provided using proprietary TLVs (Transport Layer Values) to pass information to the telephones. See the *Avaya one-X® Deskphone H.323 Administrator Guide* for detailed information about LLDP processing.

LLDP setup and troubleshooting steps

For manually (statically) programmed telephones use the Craft ADDR procedure to set the Call Server to a valid IP address. Changing IP address information on page 42 covers the ADDR procedure in detail.

Note:

If system value “STATIC” is set to “0” (the default), static addresses may be overwritten by DHCP or the 46xxsettings file.

Note:

See the *Avaya one-X® Deskphone H.323 Administrator Guide* for details on how to set “STATIC” to use manually programmed IP addresses.

Proposed solution for DHCP—configured deskphones

Procedure

1. Using the local (Craft) ADDR procedure, set “Phone” to **0.0.0.0**.
2. Verify or set SSON to **242** (this is the default).
3. Administer the DHCP server option 242 to contain **MCIPADD=***xxx.xxx.xxx.xxx*where *xxx.xxx.xxx.xxx* is the Call Server IP Address.
4. Verify that the DHCP server and the telephone are on the same VLAN.
5. Verify the “DHCP server” port (67) or/and “DHCP client” port (68) are NOT blocked on the switch.
6. Verify the configuration of the DHCP Relay Agent (on the switch or on a separate PC, for example, MS Windows Server 2000/2003) if the telephones and DHCP

Server are placed on different networks (subnets). DHCP broadcast messages do not, by default, cross the router interface. See http://technet2.microsoft.com/WindowsServer/en/library/929704d8-0e1c-4b8d-b424-16c312ad1edf1033.mspx
for more details about configuration of a DHCP Relay Agent on Windows Server 2003.

Note:

Do not embed spaces in DHCP Option 242 strings. For more information, see "DHCP Server Administration" in Chapter 5 of the *Avaya one-X® Deskphone H.323 Administrator Guide*.

Proposed solution for script-configured deskphones

Procedure

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

   For more information, see "HTTP Generic Setup" in Chapter 5 of the *Avaya one-X® Deskphone H.323 Administrator Guide*.

Proposed solution for LLDP-configured deskphones

About this task

For LLDP-configured deskphones, activate the switch the telephone is connected to for LLDP. This is currently only possible with Extreme switches. Activating the switch for LLDP enables the switch to send appropriate IP addresses using Avaya/Extreme Proprietary HTTP and/or HTTPS Server and/or Call Server TLVs.

Note:

The telephone gets HTTP and/or HTTPS Server and Call Server IP Addresses from LLDP only if they were not configured via other means (DHCP Server, Script File, statically).

Note:

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

Note:

For more information, see “ About Link Layer Discovery Protocol (LLDP)” in Chapter 7 of the *Avaya one-X® Deskphone H.323 Administrator Guide*.

Secure Shell Support

Secure Shell (SSH) protocol is a tool that the Avaya Services organization can use to remotely connect to IP telephones to monitor, diagnose, or debug telephone performance. Only the SSHv2 version is supported. Because of the sensitive nature of remote access, you can disable permission with the SSH_ALLOWED parameter. Even if permission is given, the telephone takes several security precautions. First, a security warning message is displayed. You can specify your own file using SSH_BANNER_FILE, or the following default file will be used:

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

If you want to use a custom warning message, SSH_BANNER_FILE can be set to an absolute URL, or alternatively the name of the file on the standard file server (e.g. HTTPSRVR).

In addition to the warning message, you can administer the amount of inactivity time that will disable SSH (with SSH_IDLE_TIMEOUT), the number of failed login attempts that will disable SSH (with SSH_LOCKOUT_ATTEMPTS), the number of seconds the telephone delays between failed login attempts (with SSH_LOGIN_DELAY), or the user name permitted for SSH logins SSH_USERNAME.

Chapter 6: Terms Used in This Guide

802.1D 802.1Q	802.1Q defines a layer 2 frame structure that supports VLAN identification and a QoS mechanism usually referred to as 802.1D.
802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. Applicable 9600 Series IP deskphones support IEEE 802.1X for pass-through and for Supplicant operation with the EAP-MD5 authentication method.
Application - specific	Specific to a particular “application” running inside the telephone. For example, configuration file downloading, backup and restore of user data, HTTP push, and the Web browser are all internal applications that use the HTTP protocol. Similarly, the RTCP and CNA clients are internal applications that can invoke traceroute. This term does not include Web-page-based “applications” rendered in the Web browser.
ARP	Address Resolution Protocol, used, for example, to verify that the IP Address provided by the DHCP server is not in use by another IP telephone.
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. 9600 Series 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.
Gatekeeper	H.323 application that performs essential control, administrative, and managerial functions in the media server. Sometimes called CLAN in Avaya documents.
H.323	A TCP/IP-based protocol for VoIP signaling.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	A secure version of HTTP.
IEEE	Institute of Electrical and Electronics Engineers, an organization that, among other things, produces standards applicable to Local Area Network equipment.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.

LAN	Local Area Network.
MAC	Media Access Control, ID of an endpoint.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks.
RTCP	Real-time Transport Control Protocol.
RTP	Real-time Transport Protocol.
SRTCP	Secure Real-time Transport Control Protocol.
SRTP	Secure Real-time Transport Protocol.
System - specific	Specific to a particular type of call server, for example, Communication Manager. “System-specific signaling” refers to messages specific to the signaling protocol used by the system, for example, H.323 and/or CCMS messages used by Communication Manager and IP Office. “System-specific procedures” refers to telephone software procedures that are specific to the call server with which the software is intended to be used.
TCP	Transmission Control Protocol, a connection-oriented transport-layer protocol.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). 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.
Unnamed Registration	Registration with Communication Manager by an IP telephone with no extension. Allows limited outgoing calling.
URI & URL	Uniform Resource Identifier and Uniform Resource Locator. Names for the strings used to reference resources on the Internet (for example, HTTP://....). URI is the newer term.
USB	Universal Serial Bus. An industry standard used by PCs and various devices for communication.
VLAN	Virtual LAN.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.

Index

Numerics

802.1X Operational Mode, Setting the 40
9600 Series IP deskphone 56
Restart 56
9600 Series IP Deskphone 14
Powering the 14

A

Administrative Options 36
Entering Data for 36
AGC 46
Automatic Gain Control, Disable/Enable 46

C

Calibrating the Touch Screen 45
Call Center faceplate installation (9641G) 24
Change History 7
Changing the Signaling Protocol 65
Clear Procedure 47
Connection Jacks for 9621G/9641G Models 14
Connection Jacks on 9608 or 9611G Models 14
Contrast, Adjusting for Button Modules or Non-Color IP Telephones 48
Craft Procedures, Accessing 34

D

Disable Event Logging 52
Disable/Enable Automatic Gain Control (AGC) 46
Document Organization 7
Download File Content 61
Downloading Software Upgrades 61
Downloading Text Language Files 64
DTMF Tones 68
Dual Headset Adapter, installing 19
Dynamic Addressing Process 25

E

Enable Automatic Gain Control (AGC) 46
Enable Event Logging 52
Entering Data for Administrative Options 36
Error and Status Messages During Installation of 9600 Series IP Deskphones 72
Error and Status Messages, Installation 72
Error Conditions 67
Event Logging 52

F

Faceplate installation, for 9641G use in call center 24

G

Group Identifier 50
GROUP Parameter 65

H

Handset audio equalization 50
Setting 50

I

Initialization 25
Installing a Dual Headset Adapter 19
Interface Control 51
IP Deskphone 12
Requirements 12
IP Deskphone Models 7

L

Language Files for text entry, Downloading 64
legal notices 2
LLDP Troubleshooting 82
Local (Craft) Procedures, Accessing 34
Local Administrative Procedures, About 38
LOG Procedure 52
Logoff Procedure 53

M

Models 7

O

Online Documentation 8
Operational Errors and Status Messages 76

P

Parameter Values 68
Power Interruption 68
Power-Up and Reset Operation 25
Power-Up and Reset Process 27
Powering the IP Deskphone 14
Pre-Installation Checklist 12
Pre-Installation Checklist for Static Addressing 42

R

Requirements, for each IP Deskphone 12
Reset Operation 25
Reset System Values 55

S

Secure Shell Support 85
Self-Test 58
Settings File, Contents 63
SIG Procedure 57
Signaling Protocol Identifier 57
Signaling Protocol, Changing 65
Site-Specific Option Number Setting 58
Software 11
Software Upgrades, Downloading 61
SSON Procedure 58
Static Addressing 42
    Pre-Installation Checklist 42
System Parameter Values, troubleshooting 68
System Values, Reset 55

T

TEST Procedure 58
Touch Screen, Calibrating 45
Troubleshooting 67, 68, 72, 76
    DTMF Tones 68
    Error Conditions 67
    Installation Error and Status Messages 72
    Operational Errors and Status Messages 76
    Parameter Values 68
    Power Interruption 68
    VIEW Administrative Option 68
Troubleshooting LLDP 82

U

Unnamed Registration 31

V

VIEW Administrative Option 68

W

What's New 8