Installing and Maintaining Avaya B189 IP Conference Phone

Release 6.8.5
Issue 1
November 2020

© 2013-2020, Avaya Inc.
All Rights Reserved.

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Shrinkwrap License (SR). End User 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”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Regulatory Statements

Japan Statements

Class B Statement

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

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。　　ＶＣＣＩ－Ｂ

Denan Power Cord Statement

Danger:

Please be careful of the following while installing the equipment:

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

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

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

México Statement

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

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

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

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

Power over Ethernet (PoE) Statement

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

Taiwan Low Power Radio Waves Radiated Devices Statement

802.11b/802.11g/BT:

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

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

低功率電波輻射性電機管理辦法

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

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

EU Countries

This device when installed complies with the essential requirements and other relevant provisions of the EMC Directive 2014/30/EU, Safety LV Directive 2014/35/EU, and Radio Equipment Directive 2014/53/EU. A copy of the Declaration may be obtained from https://support.avaya.com or Avaya Inc., 2605 Meridian Parkway Suite 200. Durham, NC 27713 USA.

General Safety Warning

- Use only the Avaya approved Limited Power Source power supplies specified for this product.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction 7
Purpose 7
Chapter 2: Overview 8
Overview 8
Connection layout 8
Chapter 3: Installing the deskphone 11
Avaya B189 Conference IP Phone 11
Recommendations to improve audio quality 11
Updating phone software for installation 13
Pre-installation checklist 13
Plugging in Avaya B189 Conference IP Phone 15
Plugging in and resetting the phones using the Dynamic Addressing Process 15
Understanding the plug in and reset process 16
Understanding Unnamed registration 19
PA system 20
Connectors and controls of a PA interface box 20
Connecting a PA interface box to a conference phone 21
Chapter 4: Maintaining Avaya IP phone 22
Software distribution packages 22
Upgrading software packages 23
Contents of the settings file 24
Downloading text language files 25
Applying settings to logical groups 25
Chapter 5: Using local Administration menu procedures 26
Administration menu procedures 26
Entering the Administration Menu 26
Entering and validating IPv4 addresses 27
Local administrative menu 27
Setting the operational mode to 802.1X 28
Using the preinstallation checklist 29
Changing IP address information 29
Enabling and disabling the debug mode 31
Clearing the phone settings 31
Managing the PA system 32
Enabling the auxiliary port for the PA system 32
Turning on the internal speaker and microphones 33
Changing the group identifier 33
Changing Ethernet interface control 34
Logging off from the phone 34

Resetting system values 35
Restarting the phone 35
Changing SSON settings 36
Performing a self-test 36
Chapter 6: Troubleshooting 38
Resolving error conditions 38
Failure to hear DTMF tones 39
Correcting a power interruption 39
Using the VIEW procedure for troubleshooting 39
Installation error and status messages 41
Operational errors and status messages 45
LLDP Troubleshooting 49
Proposed Solution 50
LLDP setup and troubleshooting steps 50
Proposed solution for DHCP configured deskphones 50
Proposed solution for script-configured deskphones 51
Proposed solution for LLDP-configured deskphones 51
Secure Shell Support 51
Chapter 7: Related resources 53
Documentation 53
Training 53
Support 53

Chapter 1: Introduction

Purpose

This guide is for personnel who install theAvaya B189 Conference IP Phone, Local Area Network (LAN), and the related server system.

Chapter 2: Overview

Overview

Avaya B189 IP Conference Phone is a multiline H.323 conference phone that you can use to make calls and hold conferences with HD quality voice.

The features of the conference phone include a 5-inch touch screen, mute, and volume control buttons, one On-hook/Off-hook button, and a Phone button. You can navigate the menu only through the touch screen. Bi-color LEDs provide visual indication of an incoming call, call in progress, call on hold, and a muted microphone.

Avaya B189 IP Conference Phone supports Public Address (PA) system and two-way communication with external microphones and speakers. As the LEDs are visible from all angles, the conference phone visually alerts the users. You can attach additional microphones to the conference phone to cover a wide area. The conference phone supports both Auto dialing and Edit dialing.

Connection layout

The following table lists the connections that are available on the conference phone.

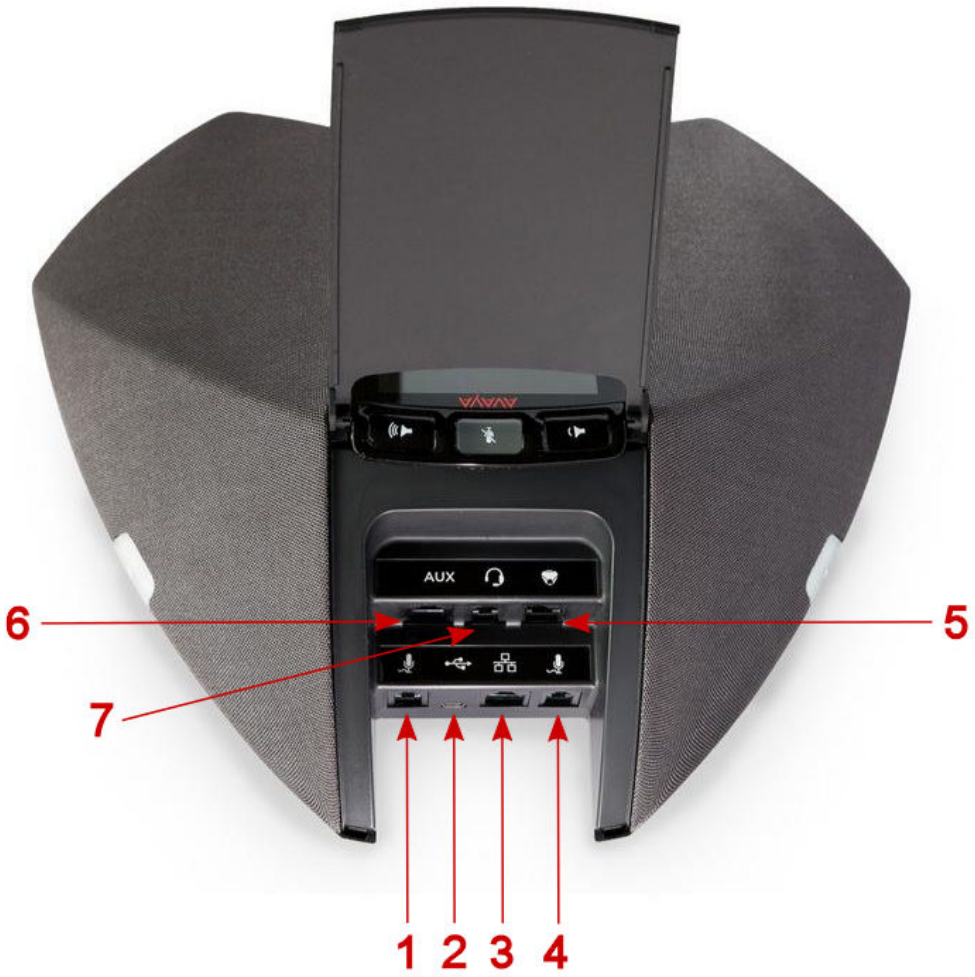


Figure 1: Connection layout on Avaya B189 IP Conference Phone

Callout number	Description
1	Left side expansion microphone port
2	USB Connection Note: This connection is reserved for future use.
3	RJ 45 Network connection socket
4	Right side expansion microphone port
5	Daisy chain connection socket Note: This connection is reserved for future use.
6	Auxiliary connection port. This port is used to connect to a PA system using PA System Interface Box.
7	Headset connection port This connection is reserved for future use.

Figure 2: Connection layout on Avaya B189 IP Conference Phone

Callout number	Description
1	SD card slot. The SD card slot is not supported.

Chapter 3: Installing the deskphone

Avaya B189 Conference IP Phone

The Avaya B189 Conference IP Phone product line uses Internet Protocol (IP) technology with Ethernet interfaces.

Avaya B189 Conference IP Phone supports DHCP and HTTP/HTTPS over IPv4 including Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP). Both the protocols enhance deskphone administration and servicing.

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

Recommendations to improve audio quality

If your laptop is open, position the screen at a 45–degree angle away from the conference phone or the expansion microphones. Else, the audio will get distorted. Consider the following recommendations before and during a conference :

- Turn off noisy fans.
- Turn down the volume of mobile devices.
- Do not drum your fingers or tap a pen on the table.
- Turn your laptop screen in a direction that does not obstruct the microphone.
- Do not place papers or folders on top of the extra microphones on the table.
- Do not rest your chin on your hand while talking.
- Close the door or the windows to keep out external sounds.
- Prevent miscellaneous noise by muting the microphone when you are not talking.

Additional audio recommendations

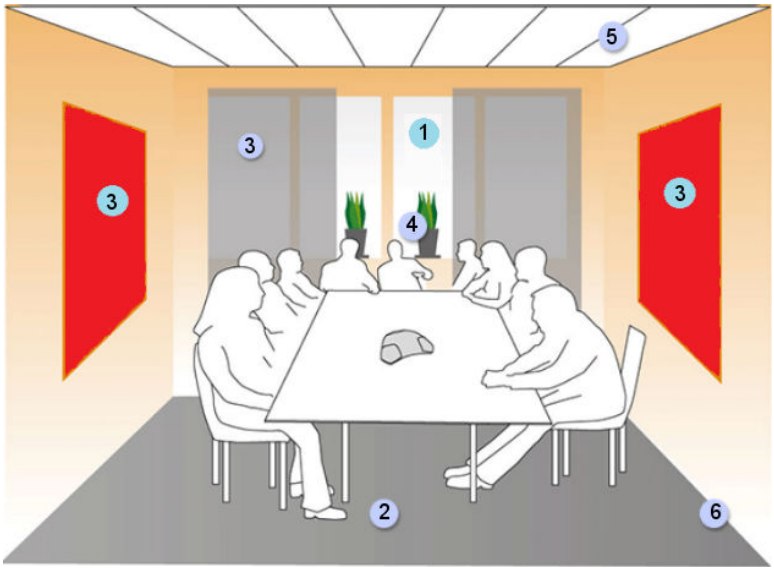


Figure 3: Setting up the conference room

Decorate and furnish the room to reduce reverberation because a cold room causes sound to bounce around the room. If you are still dissatisfied with the audio quality, consider the following options:

1. Choose a room where there is no noise from traffic or an air conditioner.
2. Select a room that has wall-to-wall carpeting, which reduces the reverberations.
3. Use long curtains or wall hangings if the room has large windows or a high ceiling.
4. Use potted plants or artificial plants as decorative aids to reduce reverberation.
5. Install sound damping panels if the ceiling is too high.
6. Seek advice from an interior designer to redecorate the conference room.

Headsets and expansion microphones

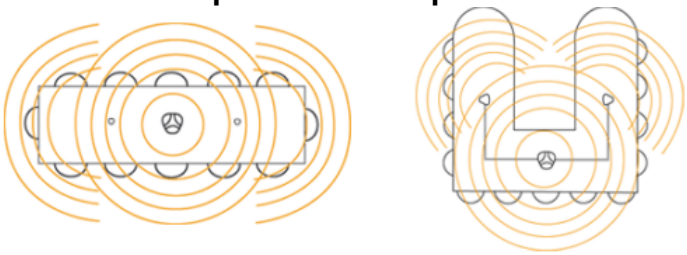


Figure 4: Placement of the expansion microphones

During a presentation, the speaker stands away from the participants. The speaker must use a wireless headset to transmit the voice clearly to the conference phone. To double the voice-pickup range, place expansion microphones on either side of the phone.

PA system connection

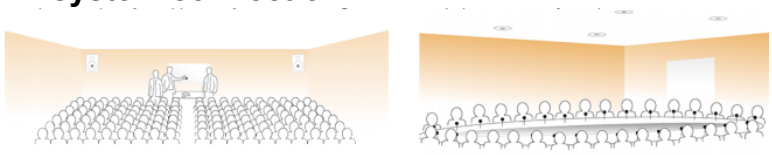


Figure 5: PA interface box in larger rooms

To encourage active participation in larger conference rooms, provide microphones for all participants. Use a PA interface box to connect the external speakers and the microphones of the participants in the room.

Updating phone software for installation

About this task

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

For subsequent downloads of software upgrades, the Avaya call server provides the capability for a remote restart of the IP phone. When you restart the phone, the phone automatically restarts and performs a download if new software is available. For more information, see About software distribution packages on page 22 and Downloading software packages on page 23.

Pre-installation checklist

Print copies of this checklist for each server and deskphone.

Requirements for your network:	
❑	The LAN uses Ethernet Category 5e cable to run the IPv4 version of Internet Protocol.
❑	Your call server must haveAvaya Aura®Communication Manager Release 6.2 or later version installed.

Table continues…

Requirements for your network:	
❑	Verify that you have installed the following circuit packs on the switch: • TN2602 or TN2302IP Media Processor circuit pack. Avaya recommends that sites with a TN2302 IP Media Processor circuit pack must install a TN2602 circuit pack to benefit from increased capacity. • TN799C or D Control-LAN (C-LAN) circuit pack. **Important:** Release 6.0 or later requires TN799C V3 or greater C-LAN circuit pack(s). For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya Support website.
❑	Verify that you have configured the Avaya call server correctly. For more information, see *Administering Avaya B189 IP Conference Phone, 16–604294*, and Communication Manager documentation on the Avaya Support website.
❑	Verify that you have administered the DHCP server and application correctly. For more information, see *Administering Avaya B189 IP Conference Phone, 16–604294*, and Communication Manager documentation on the Avaya Support website.
❑	Verify that you have administered the HTTP/HTTPS server and application correctly. For more information, see *Administering Avaya B189 IP Conference Phone, 16–604294*, and Communication Manager documentation on the Avaya Support website.
❑	Verify that you have loaded the upgrade script and application files from the Avaya Support website correctly on the HTTP/HTTPS server.
❑	If applicable, administer the DNS server. For more information, see *Administering Avaya B189 IP Conference Phone, 16–604294*, and Communication Manager documentation on the Avaya Support website.

Note:

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

Requirements for each deskphone:	
❑	Verify that you have an extension number and an Communication Manager security code (password) for each applicable IP deskphone. If your call server and the phone settings file support unnamed registration, you do not need an extension or password. However, without an extension or password, the phone has limited functionality. For information about unnamed registration, see About unnamed registration on page 19.
❑	Verify that a Category 5e LAN jack is available at each phone site and a Category 5 modular line cable that connects the deskphone to the LAN jack. Cat 5 cables with an RJ45 plug have a plug size restriction of 36 mm.
❑	Verify that each deskphone receives power through a POE switch or SPPoE adapter. For PoE Input connection, use only with UL listed I.T.E. equipment with PoE output. PoE must support Class 3.

Plugging in Avaya B189 Conference IP Phone

Caution:

Use the correct jack when you plug in the phone. You can find the jacks at the rear of the phone housing. Flip the cover to see the connecting jacks. Icons on the side of the jacks represent the correct use of each

Procedure

1. Plug one end of the CAT5 cable into the corresponding jack in the phone.
2. Connect the other end of the CAT5 cable to the wall connector as show in the following figure.

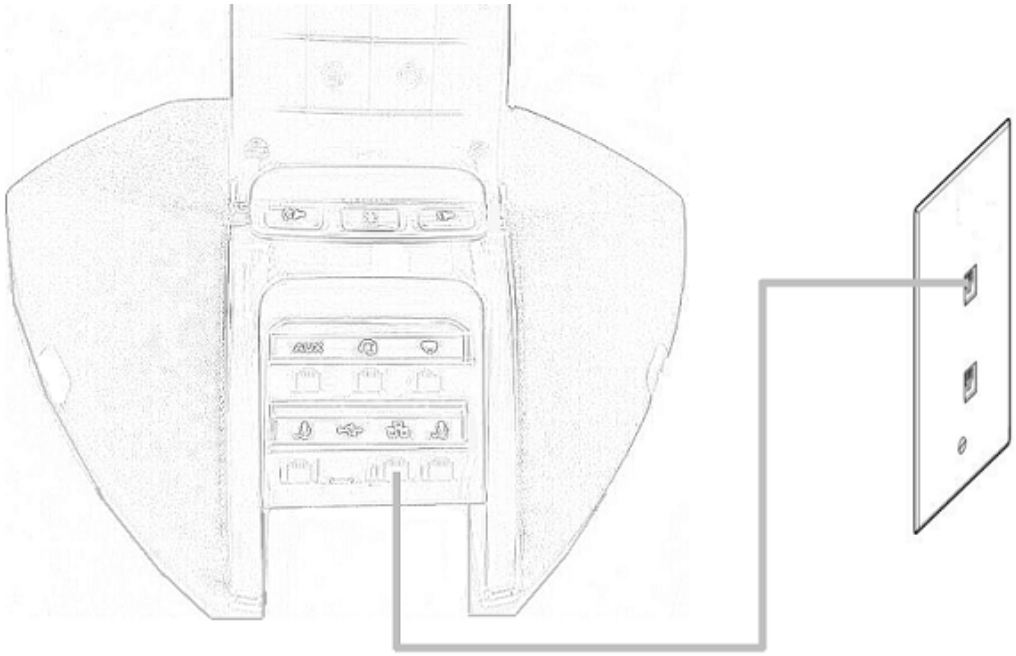


Figure 6: Connecting Avaya B189 Conference IP Phone to a wall LAN connector

The phone powers on.

Plugging in and resetting the phones using the Dynamic Addressing Process

Note:

Before you start this process, you must have an extension number for the IP phone and the Communication Manager security code (password) for that extension, unless you intend to

use the deskphone with unnamed registration. Any reference to an HTTP server applies equally to an HTTPS server. You can plug in and reset the phone successfully using the following description.

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

Understanding the plug in and reset process

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

Note:

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

1. The system checks the system initialization value for the language file in use (NVLANGFILE) for a non-null value, in which case the text strings in that language file are used for text display. Otherwise, the display shows English text strings.
2. The boot programs check the Kernel or the Root File System that has previously been marked as the one to be activated to ensure that it has not become corrupted. If the Kernel or the Root File System is not corrupted, the system transfers control to a process in that file system. If that file system is corrupted, the boot program checks the other Kernel/Root File System. If that file system is not corrupted, the file system is marked as the one to be activated. The system then sets the value of RFSINUSE to the name of the Signed Kernel or Root Software Package that was used to install that file system, and the control is transferred to the Signed Kernel or Root Software Package. If both Kernel and Root File Systems are corrupted, the system halts the processing. The software checks whether a Signed Application or Library Software Package has been previously downloaded. If the system finds the Application Software Package or the Library Software Package the Application Software Package or the Library Software Package is installed. If either the Application Software Package or the Library Software Package has a different file name than the currently installed version, the system replaces the existing corresponding files in the Application File System. The system then deletes the downloaded Signed Application or Library Software Package. If a new Signed Application or Library Software Package is not found, the integrity of the application files is checked. If the files are corrupted, the system installs the files from the Backup Package, replacing the corrupted files in the Application File System. Each time an Application Software Package or a Library Software Package is installed, the system sets the value of the persistent parameter APPINUSE to

the file name of the Application Software Package that was installed. If the application files are not corrupted, or after the Backup Package has been installed, control is transferred to the application installed in the Application File System. While the system loads the application files into volatile memory and transfers control is transferred to the application files, the bottom text line shows the value of the APPINUSE parameter.

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

   The phone displays the speed of the Ethernet interface in Mbps, that is, 10, 100, or 1000. The phone then displays the message `Program` below the speed until the software determines whether the interface is 10 Mbps, 100 Mbps, or 1000 Mbps.
5. The IP phone sends a request to the DHCP server and invokes the DHCP process.

   The phone displays one of the following messages:

   - `DHCP: s secs`

   where *s* is the number of seconds that have elapsed after the DHCP process was started. The phone displays the first message if 802.1Q tagging is off and access to local programming procedures is not disabled or restricted. The phone displays the second message if 802.1Q tagging is on and access to local programming procedures is disabled or restricted. If the first and second message alternate every 2 seconds, 802.1Q tagging is on. When the phone displays both messages alternately, access to local programming procedures is not disabled or restricted.

   Finally, the phone displays the third message if 802.1Q tagging is off and access to local programming procedures is disabled or restricted.
6. The system determines the DHCP protocol and the applicable parameters that are enabled.

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

   - The phone
   - The HTTP/HTTPS server
   - The TN799C or D Control-LAN (C-LAN) circuit pack on the media server
7. Using the list of gateway IP addresses provided by the DHCP server, the phone performs a router check. The phone cycles through the gateway IP addresses with ARPs or pings until it receives a response. When the router is located, the router processes the received LLDP TLVs. Then the HTTP process starts.
8. While the IP phone connects to the HTTP server, the phone displays one of the following messages:

   `HTTP: n ipadd`

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

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

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

    For HTTP, *n* is the number of HTTP requests made by the phone and *uri* is the URI for the current HTTP request.
11. While the upgrade script file is being downloaded, all IP phones display the following message: `HTTP: n sc etag`

    where *n* is the number of the IP address obtained from the HTTP server, *sc* is the status code of the HTTP response, and *etag* is the value of the ETag header.
12. When the phone establishes the validity of the application file received, the phone displays the following message: `File Obtained; please wait..... s secs`

    where *s* is the number of seconds that elapse while non-volatile memory is erased.
13. While the application file is saved in flash memory, all IP phones display the following message: `Saving to flash 1% 1 secs`

    where the percentage of the file and the number of elapsed seconds increase as the application file is stored in flash memory.
14. The phone contacts the Avaya Communication Manager and displays a login screen that displays the following:

    `Extension`, `Password` text boxes, and a **Login** button.

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

1. Enter a new extension and the password.

   Note:

   Unnamed registration is registering a phone with the call server without entry of an extension or password. You must set the UNNAMEDSTAT parameter to enable unnamed registration. The phones that are registered unnamed have limited functionality.

   All IP phones display the following:

   ```
   Extension

   Password


   Log In
   ```
2. Enter the extension number and password and press **Log In**.

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

Note:

The phone stops at the discovery mode in the following conditions:

- The login credentials are incorrect.
- The phone is logged in but one of the gatekeepers is not reachable because of an upgrade or a network outage. In the discovery mode, press **Reset**. The phone deletes the credentials from the memory, reboots, and displays the Login page.

  In the registration mode, the phone restarts, but it does not delete the login credentials.

When this process is complete, you can hear a dial tone when you press the Phone On-hook/Off-hook button. The dial tone indicates that the IP phone is installed successfully.

Understanding Unnamed registration

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

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

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

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

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

Unless otherwise disabled, the deskphone automatically attempts to register unnamed if no action is taken on the deskphone extension entry screen within 60 seconds. To disable and prevent

Unnamed registration, enter an ID or password. The system ignores Unnamed registration after any dialpad entry.

PA system

You can connect the Avaya B189 Conference IP Phone to a built-in Public Address (PA) system that is installed in places such as boardrooms, lecture halls, and auditoriums. You can connect a PA interface box to an existing PA system.

Note:

The PA interface box is not included with the Avaya B189 Conference IP Phone.

The Avaya B189 Conference IP Phone provides settings to match various types of equipments.

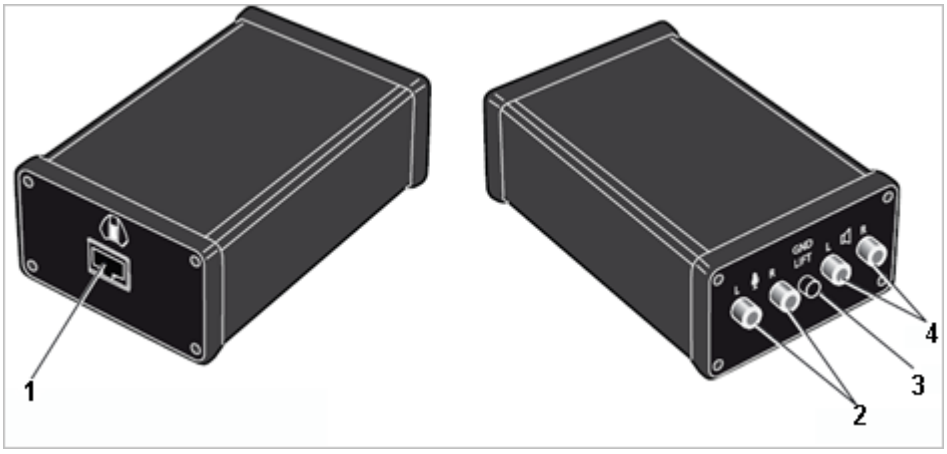
Components included

The following components are included with the conference phone:

- A 2.5 metres connection cable

Specification	Output	Input
Connector	2xRCA	2xRCA
Impedance	100Ω	2kΩ
Output level	-8dBV RMS	+3dBV RMS

Connectors and controls of a PA interface box



Number	Name
1	AUX connector to connect to a conference phone.
2	RCA connectors to connect an external microphone mixer.
3	Ground lift pushbutton to avoid ground-loop hum problems caused by multiple ground paths.
4	RCA connectors to connect an external amplifier.

Connecting a PA interface box to a conference phone

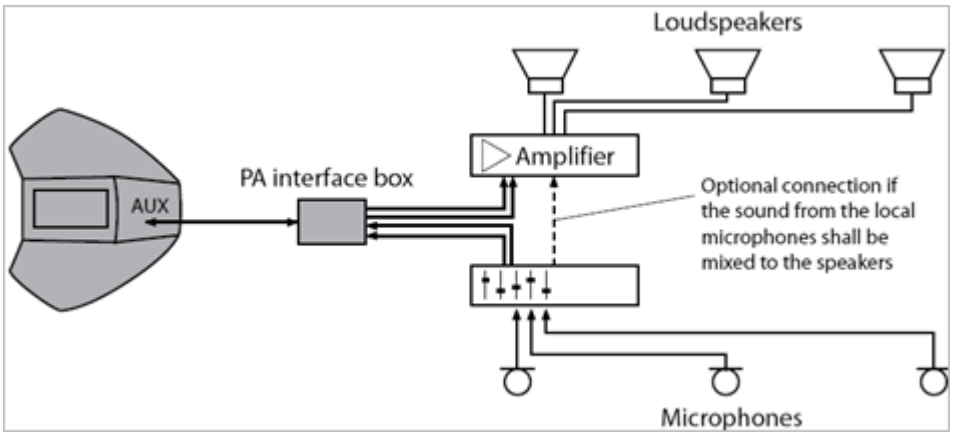
About this task

Use the following procedure to connect the PA interface box to the conference phone

Procedure

1. Connect the PA interface box to the AUX port on the conference phone with the cable provided with the phone.
2. Connect the external amplifier to the RCA connectors marked with a speaker.
3. Connect the microphone mixer to the RCA connectors marked with a microphone.

Example



Chapter 4: Maintaining Avaya IP phone

Related links

Software distribution packages on page 22
Upgrading software packages on page 23
Contents of the settings file on page 24
Downloading text language files on page 25
Applying settings to logical groups on page 25

Software distribution packages

The software distribution packages contain the following:

- Software files.
- Upgrade file, `B189Hupgrade.txt`
- All the display text language files. For example, `mlf_SB189_v78_korean.txt`
- A file named `av_prca_pem_2033.txt` that contains a copy of the Avaya Product Root Certificate Authority certificate in PEM format. You can downloaded this file to the phones based on the value of the TRUSTCERTS parameter.
- Updated MIB file.
- A file named `release.xml` that is used by the Avaya Software Update Manager application.

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

Two configuration files are:

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

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

Related links

Maintaining Avaya IP phone on page 22

Upgrading software packages

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

1. Stop the file server.
2. Administer the required port setting in HTTPPORT or TLSPORT for HTTP or TLS, respectively if you want to specify a port the phones must use to communicate with the file server.

   Note:

   B189 Conference IP Phones v6.6.2 and later do not support HTTPS with MV_IPTEL or IIS 6. It is recommended to upgrade to the current version of an HTTPS server that supports TLS 1.2.

   Note:

3. Back up all the current file server directories as applicable.
4. Copy the `46xxsettings.txt` file to a backup location.
5. Remove all the files in the download directory. This ensures that you do not have an inappropriate binary or configuration file on the server. The only system values that can be used in the Conditional statement are: GROUP, MACADDR, MODEL, MODEL4, and SIG_IN_USE.

   Download the self-extracting executable file or the corresponding zip file.
6. Extract all the files.
7. Copy the `46xxsettings.txt` file back into the download directory.
8. Modify the `46xxsettings.txt` file as required.
9. Reset your phones.

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

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

Related links

Maintaining Avaya IP phone on page 22

Contents of the settings file

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

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

  Note:

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

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

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

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

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

For details about specific parameter values, see Chapter 7 in the *Administering Avaya B189 IP Conference Phone*. Specify settings that are different from default values, although you can also specify default values.

Related links

Maintaining Avaya IP phone on page 22

Downloading text language files

About this task

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

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

Related links

Maintaining Avaya IP phone on page 22

Applying settings to logical groups

You might have different communities of end users with the same phone model but requiring different administered settings. This section provides examples of the group settings for each of these situations.

You can separate groups of users is to associate each of them with a number. Use the GROUP parameter for this purpose. You cannot set GROUP system value in the `46xxsettings.txt` file. The GROUP parameter can only be set on a phone-by-phone basis. To set the GROUP parameter, first identify which phones are associated with which group, and designate a number for each group. The number can be any integer from 0 to 999, with 0 as the default. The largest group is assigned as Group 0.

Then, at each phone that does not have default parameters, instruct the installer or end-user to invoke the local **Administration Menu** procedure. After the GROUP assignments are in place, edit the configuration file to allow each phone of the appropriate group to download its proper settings.

Related links

Maintaining Avaya IP phone on page 22

Chapter 5: Using local Administration menu procedures

Administration menu procedures

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

Local administrative options have one form that provides access to all the capabilities and functions described in this chapter.

When you set PROCSTAT to 0, you have full access to local Craft procedures and you can invoke local craft procedures through the **Craft Procedures** option under Main menu on the deskphone.

Caution:

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

- You download a new boot file.
- You reset the IP phone.

Entering the Administration Menu

Procedure

1. On the phone, tap **Settings**.

   The phone displays the **Settings** screen and the options that are available.

2. Tap **Administration Menu**.

   The deskphone displays the **Administration Login** screen.

3. In the **Password** text box, enter the password.

4. Tap **Log In**.

   The phone displays the **Administration Procedures** screen and the options that are available.

Entering and validating IPv4 addresses

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

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

- If you enter a valid value a period displays. The space after the field displays a period.
- The cursor moves to the next space.

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

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

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

Local administrative menu

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

For touch screen-based deskphones, simply touching a line or a softkey produces to select a line

Craft Procedure value (in English)	Craft Procedure Purpose	See
8021X	Set 802.1X operational mode	Setting The 802.1X Operational Mode on page 28
ADDR	Address information programming	Use the pre-installation checklist and Changing IP address information on page 29.

Table continues…

Craft Procedure value (in English)	Craft Procedure Purpose	See
CLEAR	Clear all values to factory defaults	Clearing the deskphone settings on page 31
ADJUNCT SETUP	Manage the PA system	Managing the PA system on page 32
DEBUG	Enable/disable Debug Mode	Enabling and disabling the debug mode
GROUP	Set the Group Identifier	Changing The group identifier on page 33
INT	Interface Control	Changing Ethernet interface control on page 34
LOGOUT	Log off the deskphone	Loging off the deskphone on page 34
RESET VALUES	Reset system initialization values to defaults	Resetting system values on page 35
RESTART PHONE	Restart the deskphone	Restarting the deskphone on page 35
SSON	Set the Site-Specific Option Number	Changing SSON settings on page 36
TEST	Initiate a self-test	Performing a self-test on page 36
VIEW	View current parameter values and file names	Using The VIEW craft procedure for troubleshooting on page 39.

Setting the operational mode to 802.1X

About this task

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

Procedure

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

   802.1X Supplicant

   The options that are displayed depend on the following parameters as set in the `46xxsettings.txt` file:

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

2. Tap the line you want to change.

   A green tick mark is set next to the option that you have selected.

3. To change the setting, tap the option again.

4. Tap **Save** to store the new setting and redisplay the **Administrative Menu** screen.

Using the preinstallation checklist

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

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

Changing IP address information

About this task

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

Caution:

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

Use the following procedure to invoke manual address information programming.

Procedure

1. Tap and select ADDR from the Administration Menu screen. The next screen displays the following fields with the prompt `Select address to change.`

Static addressing field	Field value	Description
IP Address	nnn.nnn.nnn.nnn	phone IP address (IPADD)
Call Server	nnn.nnn.nnn.nnn	Call Server in use; media server IP address
Router IP address	nnn.nnn.nnn.nnn	Router in use; gateway/router IP address
Subnet Mask	nnn.nnn.nnn.nnn	IP network mask (NETMASK)

Table continues…

Static addressing field	Field value	Description
HTTP Server	nnn.nnn.nnn.nnn	IP address of HTTP File Server in use
HTTPS Server	nnn.nnn.nnn.nnn	IP address of HTTPS (TLS) File Server in use
802.1Q	L2Q text string As defined by the selected L2Q text string	L2Q setting text description
VLAN ID	dddd	NVL2QVLAN
Static VLAN Test	ddd	VLANTEST

where:

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

2. Scroll to and tap the line for the address you want to change.
3. Select one of the following as appropriate to the item you selected:

Task	Steps
To change any of the IP address values such as Phone, Call Server, Router, Mask, and File Server	Use the key pad on the screen to enter the new IP address. IP addresses have three sets of three digits followed by a period. Tapping star (*) following entry of three digits causes a period to be placed in the next position, and the cursor to advance one position to the right. For example, to enter the IP address 111.222.333.444 in IPv4 format, tap the number 1 on the key pad three times, then tap *****, tap the number 2 on the key pad three times, then tap *****, tap the number 3 on the key pad three times then tap *****, then tap the number 4 on the key pad three times. Proceed to the next step.
To change the 802.1Q value	Tap 802.1Q. On the 802.1Q screen, scroll and tap the indicated options of **Auto**, **On**, or **Off**. The indicated options are the text strings corresponding to the L2Q values defined as *Auto* if L2Q=0, *On* if L2Q=1, and *Off* if L2Q= 2 .
To change the VLAN ID value	Use the key pad on the screen to enter the new static VLAN ID of from 0 to 4094, inclusive. Proceed to the next step.
To change the VLANTEST value	Use the key pad on the screen to enter the new value of the DHCPOFFER wait period of from 0 to 999.

4. Tap **Save** to store the new setting and redisplay the Administration Menu screen or **Cancel** to return to the Administration Menu screen without saving the value entered.

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

Enabling and disabling the debug mode

Before you begin

If the default password is used, the setting associated with the serial port cannot be changed.

About this task

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

Procedure

1. Access the Administration Procedures.
2. On the Administration Procedures screen, tap **Debug**.

   The Debug procedures screen displays the following options:

Setting	Status
Log Mode	Off
Serial Port	Off
Log to file	Off
Phone Report	**Note:** The **Phone Report** is always available. If the URI is not present, the report is stored on the phone
SSH	Off

3. Tap an option to turn it off or on. To generate a phone report, tap **Phone Report** and then tap **Create** on the **Phone Report** screen that the phone displays.

   The report is generated and saved in the nnn_report.gz debug file in the backup folder specified by BRURI.
4. If you have made any changes to the settings, tap **Save** to save the settings.

Clearing the phone settings

About this task

Sometimes, you might want to remove *all* administered values, user-specified data, and option settings and return a phone to its factory settings. You might have to remove all administered values when you give a phone to a new, dedicated user and when the **LOGOFF** option is not

sufficient. For example, a new user is assigned the same extension, but requires different permissions than the previous user.

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

- The software load. If you upgrade the phone, the phone retains the latest software. After you clear a phone of the settings, you can administer the phone normally.

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.

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

Procedure

1. Select **CLEAR** from the Administration Menu menu.

   The phone prompts for confirmation.

2. Press one of the following:

   - **Clear**: To clear all values to use initial default values.
   - **Cancel**: If you do not want to clear all values and to terminate the procedure and retain the current values.

   The phone displays the following text:

   ```
   Clearing values...
   ```

   The phone is reset to the default factory settings.

   - All system values and system initialization values.
   - 802.1X identity and password.
   - User options, parameter settings, identifiers, and password.

   After clearing the values, the phone resets.

Managing the PA system

Enabling the auxiliary port for the PA system

About this task

Use the following procedure to enable the auxiliary port for the PA system.

Procedure

1. Go to the Administrative Menu screen.
2. Tap **ADJUNCT SETUP**.
3. Tap **Enable Port**.
4. Tap **PA System**.
5. Tap **Save**.

Turning on the internal speaker and microphones

Procedure

1. Go to the Administrative Menu screen.
2. Tap **ADJUNCT SETUP**.
3. Tap **PA Mode Setup**.
4. Turn on the internal speaker and microphones by tapping the corresponding line.

Changing the group identifier

About this task

When updating the local Craft procedure or Admin menu procedures press the appropriate softkey on IP phone.

Note:

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

Procedure

1. Select **Group** from the Administration Procedures screen.

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

   The deskphone displays the Administration Procedures screen.

Changing Ethernet interface control

About this task

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

Procedure

1. When you select INT from the Administration Procedures screen, the phone displays the following options:

   The options that are displayed are the text strings associated with the current PHY1STAT on the Ethernet line.

   - **Auto** when PHY1STAT = 1
   - **10 Mbps half** when PHY1STAT = 2
   - **10 Mbps full** when PHY1STAT = 3
   - **100 Mbps half** when PHY1STAT = 4
   - **100 Mbps full** when PHY1STAT = 5
   - **1000 Mbps full** when PHY1STAT = 6
2. To change the setting, scroll up or down as required and tap the new setting.
3. Tap **Save** to store the new settings and redisplay the Administration Procedures screen.

Logging off from the phone

About this task

Use the following procedure to log off from a phone.

Caution:

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

Procedure

1. When you select **LOGOUT** from the Administration Menu procedures screen, the phone displays the following text:

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

   Press **Cancel** to return to the Administration Menu procedures screen without logging off the phone.

Resetting system values

About this task

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

Caution:

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

Procedure

1. Select RESET VALUES from the Administration Procedures screen. The phone displays the following text:
2. Press one of the following:
   - **Reset**: To start the phone reset.
   - **Cancel**: To return to the previous screen.

   The phone resets from the beginning of registration, which might take a few minutes. The phone resets:
   - All system values and system initialization values except AUTH and AUTH_ONLY to default values.
   - The 802.1X ID and Password to their default values.
   - Call server values to their defaults.
   - Any entries in the Redial buffer.
   - Does not affect user-specified data and settings like Contacts data or the phone login and password.

Restarting the phone

About this task

Use the following procedure to restart the phone.

Procedure

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

   ```
   Press Restart to confirm.
   ```
2. Tap **Cancel** to return to the Administration Procedures screen without restarting the phone.

   Press **Restart** to proceed with the registration steps.

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

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

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.

Use the following procedure to set the Site-Specific Option Number (SSON). SSON default value is 242.

Procedure

1. Select SSON from the Administration Procedures screen.

   The phone displays the current SSON value with a numeric keypad on the screen.

2. To change the setting, use the Key pad on the screen to enter a valid SSON value between 128 and 255.
3. Tap **Save** to store the new setting and redisplay the Administration Procedures screen.

Performing a self-test

About this task

Note:

Avaya B189 Conference IP Phone stores two software code images in reprogrammable non-volatile memory. The primary image, called the “big app” must be running to perform a self-test. The backup image, called the “little app” does not support the self-test.

Use the following procedure to perform self-testing:

Procedure

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

   ```
   Press Test to confirm.
   ```

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

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

The test performs the following actions:

The screen glows red, green and blue color consecutively and plays the standard ring tone with each color change.

The MUTE LED glows blue or red or is off.

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

3. Press or tap **Back** to return to the Administration Menu screen.

Chapter 6: Troubleshooting

Related links

Resolving error conditions on page 38
Failure to hear DTMF tones on page 39
Correcting a power interruption on page 39
Using the VIEW procedure for troubleshooting on page 39
Installation error and status messages on page 41
Operational errors and status messages on page 45
LLDP Troubleshooting on page 49
LLDP setup and troubleshooting steps on page 50
Secure Shell Support on page 51

Resolving error conditions

About this task

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

Procedure

1. Check both the power and Ethernet wiring for the following conditions:
   - Check whether all components are plugged in correctly.
   - Check LAN connectivity in both directions to all servers - DHCP, HTTP, and HTTPS.
   - If the deskphone is powered from the LAN, ensure that the LAN is properly administered and is compliant with IEEE 802.3af.
2. If you use static addressing:
   - Use the VIEW option to find the names of the files being used and verify that these filenames match those on the HTTP/HTTPS server. Check the Avaya Support site at www.support.avaya.com to verify whether the correct files are being used.
   - Use the ADDR option to verify IP addresses.
3. If the deskphone is not communicating with the system, DHCP, HTTP, or Avaya Media Server, make a note of the last message displayed.

Consult the system administrator. Sometimes, you can correct problems relating to Communication Manager and HTTP communications by setting the HTTPPORT value to 81 which is the port required for HTTP downloads rather than the using the default.

Related links

Troubleshooting on page 38

Failure to hear DTMF tones

As H.323 telephones do not send DTMF tones to non-H.323 telephones, the user need not perform troubleshooting for failure to hear DTMF tones from a B189 phone. The TN2302AP board does not pass in-band DTMF tones.

Related links

Troubleshooting on page 38

Correcting a power interruption

If power to a B189 Conference phone is interrupted while the phone is saving the application file, the HTTP/HTTPS application can stop responding. If this occurs, restart the phone.

Related links

Troubleshooting on page 38

Using the VIEW procedure for troubleshooting

About this task

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

Note:

You can use the ADDR option to view IP addresses if needed. The IP addresses might have been entered incorrectly. Verify whether you were provided with correct IP addresses.

Procedure

1. Select **VIEW** from the Administration Menu Screen.

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

2. Tap the category that you want to see.

   The information for that category is displayed.

Table 1: IP Parameter Values

Name	System Value	Format
IP address (Phone)	*nnn.nnn.nnn.nnn*	Phone IP address, IPADD value.
Call Server	*nnn.nnn.nnn.nnn*	IP address of the call server currently in use, otherwise *0.0.0.0.*
Router IP address	*nnn.nnn.nnn.nnn*	Up to 15 ASCII characters, the IP address of the router in use.
Subnet Mask	*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 or *On* if 802.1Q tagging is 1. If 802.1Q tagging is off (2), this line is not displayed.
Static 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.
802.1X Supplicant		

Table 2: Quality of Service Parameters

Parameter	System value	Format
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.

Table 3: Miscellaneous Parameters

Parameter	System value	Format
Model	*B189Dccc*	Up to 8 ASCII characters, MODEL serial number.
Phone SN	*ccccccccccccccccc*	Telephone Serial Number, up to 18 ASCII characters.
MAC	*hh:hh:hh:hh:hh:hh*	Each octet of the MAC address displays as a pair of hexadecimal numbers.
Group	*nnn*	Up to three ASCII numeric characters: GROUP value.
Protocol	*cccccccc*	Up to eight ASCII characters, currently only *H.323*
Application File	*filename.ext*	Four to 32 ASCII characters as primary application.
Ethernet Port	*cccccccc* Ethernet	Two to eight ASCII characters, either *1000 Mbps*, *100 Mbps*, *10 Mbps*, or *No*.
Kernel/RFS file	*bootcodename*	One to 32 ASCII characters (backup image name).
Backup App File	*filename.ext*	Four to 32 ASCII characters (backup application).

3. Scroll across the screen to the entry you want to view.
4. Press **Back** at any time to return to the Administration Procedures screen.

Related links

Troubleshooting on page 38

Installation error and status messages

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

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

Table 4: Possible error and status messages during installation of a phone

Message	Cause/Resolution
`802.1X Failure`	CAUSE: Incorrect credentials provided for authentication or credentials not provided at all. RESOLUTION: Follow the display prompts and reenter the 802.1X ID and password.
`IPv4 address Conflict`	CAUSE: The phone has detected an IP address conflict. RESOLUTION: Verify administration settings to identify duplicate IP addresses.
`Authentication Error`	CAUSE: The call server does not recognize the extension entered. RESOLUTION: Confirm the extension is correct and is correctly administered on the switch. Then try registration again, and enter the extension accurately.
`Bad FileSv address`	CAUSE: The HTTP/HTTPS server IP address in the IP phone's memory is all zeroes. RESOLUTION: Depending on the specific requirements of your network, this may not be an error. If appropriate, either administer the DHCP server with the proper address of the HTTP/HTTPS server, or administer the phone locally using the ADDR option.
`Bad Router?`	CAUSE: The phone cannot find a router based on the information in the DHCP file for GIPADD. RESOLUTION: Use static addressing to specify a router address, or change administration on DHCP.
`Call Error`	CAUSE: The user was on a call when the connection to the gatekeeper went down due to a network outage or a gatekeeper problem. The phone attempted to automatically register with the same or another gatekeeper, but the responding gatekeeper had no record of the call. RESOLUTION: Wait for the call to end, and if the phone does not automatically register, restart the phone.
`Connecting...`	CAUSE: The phone is attempting to establish a TCP connection with the call server. A resource needed to establish the connection might not be available or the 10 second buffer on switch-related actions might have expired. RESOLUTION: Allow the phone to continue attempts to connect to TCP.
`Contacting call server...`	CAUSE: The phone has rebooted successfully and is attempting to register with the call server. RESOLUTION: Allow the phone to continue.
`DHCP: CONFLICT`	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).

Table continues…

Message	Cause/Resolution
`Discover` *aaa.bbb.ccc.ddd*	CAUSE: The phone is attempting to find Communication Manager. RESOLUTION: Long display of this message implies failure of the Communication Manager server or a network problem that an administrator must fix. The administrator must ensure that there is network connectivity to Communication Manager, user extension is defined, and the Communication Manager server is up.
`Discovering...`	CAUSE: The phone is attempting to find a Communication Manager. RESOLUTION: Long display of this message implies failure of the Communication Manager server or a network problem that an administrator must fix. The administrator must ensure that there is network connectivity to Communication Manager, user extension is defined, and the Communication Manager server is up. The user can also press the **RESET** button for the phone to reboot, but this will erase the stored credentials.
`EEPROM error, repair required`	CAUSE: Application file was not downloaded or saved correctly. RESOLUTION: The phone automatically resets and attempts to re-initialize.
`Emergency Option`	CAUSE: Incompatible emergency option. RESOLUTION: This must not happen. Contact Avaya support.
`Extension in Use` `Extension in use: <NNNN> Press continue to take over this extension Login|Continue`	CAUSE: The call server detects an extension conflict with an existing set or Softphone. RESOLUTION: By pressing **Continue**, you can force the current phone to register and thereby disconnect the other user. When **Login** is selected instead, the phone re-prompts for entry of a different extension and password.
`Finding router...`	CAUSE: This phone is proceeding through boot-up. RESOLUTION: Allow the phone to continue.
`Gatekeeper Error`	CAUSE: The gatekeeper rejects the registration attempt for an unspecified reason. RESOLUTION: Review gatekeeper and call server administrations, including IP network parameters.
`Gateway Error`	CAUSE: DEFINITY Release 8.4 does not have an H.323 station extension for this phone. RESOLUTION: On the station administration screen, ensure the DCP set being aliased for this IP phone has an H.323 station extension administered, in accordance with switch administration instructions.
`Incompatible`	CAUSE: This release of the call server does not support the current version of the IP phone. RESOLUTION: Upgrade to the current version of Communication Manager (3.0 or greater) software.

Table continues…

Message	Cause/Resolution
`Invalid file`	CAUSE: The phone does not have sufficient room to store the downloaded file. RESOLUTION: Verify that the proper filename is administered in the script file, and the correct application file is located in the appropriate location on the HTTP or HTTPS server.
`IP address Error`	CAUSE: The gatekeeper reports an invalid IP address. RESOLUTION: This must not happen. Contact Avaya support.
`License Error`	CAUSE: The call server does not support IP telephony. RESOLUTION: Contact Avaya to upgrade your license.
`Limit Error`	CAUSE: The call server has reached its limit of IP stations. RESOLUTION: Un-register phones that are not in use, or contact Avaya to upgrade your license.
`NAPT Error`	CAUSE: A device between the phone and the call server is invoking Network address Port Translation (NAPT), which the phone do not support. RESOLUTION: Contact the System Administrator to remove or re-administer the device.
`No Ethernet`	CAUSE: When first plugged in, the IP phone is unable to communicate with the Ethernet. RESOLUTION: Verify the connection to the Ethernet jack, verify if the jack is Category 5, verify if power is applied on the LAN to that jack.
`Packet Error`	CAUSE: Protocol timeout error. RESOLUTION: Reenter the correct extension and password. If the condition persists, contact the system administrator.
`Password Error`	CAUSE: The call server does not recognize the password entered and displays the *Login Error* screen. RESOLUTION: Confirm whether the password is correct, then try registering again, and enter the password accurately.
`Request Error`	CAUSE: The gatekeeper does not accept the registration request sent by the phone as the request is not formatted properly. RESOLUTION: The phone will automatically attempt to register with the next gatekeeper on its list. If the problem persists, reboot the phone.
`Restarting...`	CAUSE: The phone is in the initial stage of rebooting. RESOLUTION: Allow the phone boot process to continue.
`Subnet conflict`	CAUSE: The phone is not on the same VLAN subnet as the router. RESOLUTION: Press star (*) to administer an IP address on the phone. For information on configuring an IP address, see administer network equipment to administer the phone appropriately.

Table continues…

Message	Cause/Resolution
`System busy`	CAUSE: Most likely, the number of IP endpoints on the call server is already at maximum capacity. Network resource may not be unavailable. RESOLUTION: The phone attempted to access a network resource such as DHCP server, HTTP server, or the call server and was not successful. Check the resource being called upon for its availability. If the resource appears operational and is properly linked to the network, verify that the addressing is accurate and that a communication path exists in both directions between the phone and the resource.
`System Error`	CAUSE: The call server has an unspecified problem. RESOLUTION: Consult your Avaya Media Server administration and troubleshooting documentation.
`Undefined Error`	CAUSE: The call server has rejected registration for an unspecified reason. RESOLUTION: Consult your Avaya Media Server administration and troubleshooting documentation.
`Updating: DO NOT UNPLUG THE phone`	CAUSE: The phone is updating its software image. RESOLUTION: The phone update process must be continued.
`Waiting for LLDP`	CAUSE: No File Server or Call Server has been administered, so the phone is expecting to get the missing data through LLDP. RESOLUTION: Administer the missing data by one of the following methods: Statically, dynamically in DHCP, in the 46xxsettings file for Call Server addresses, or by LLDP.
`Wrong Set Type`	CAUSE: The call server does not recognize the set type. RESOLUTION: Ensure the call server is properly administered to register a compatible phone for the IP address and extension.

Related links

Troubleshooting on page 38

Operational errors and status messages

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

Table 5: Operational error conditions

Condition		Cause/Resolution
The phone continually reboots, or reboots continuously about every 15 minutes.		CAUSE: The phone cannot find the HTTP/HTTPS server and/or call server. RESOLUTION: Ensure that MCIPADD is administered either manually or through DHCP or HTTP, as appropriate. Alternately, this might be a firmware fault because the MAC address in memory is corrupted; in this case, you must return the phone to Avaya for repair.
The phone stops working in the middle of a call,	AND no lights are lit on the phone and the display is not lit.	CAUSE: Loss of power. RESOLUTION: Check the connections between the phone, the power supply, and the power jack. For example, verify whether static addressing was not used or that any changes to static addresses were entered correctly. Follow POE guidelines to troubleshoot POE related problems.
	AND power to the phone is normal and the phone might have gone through the restarting sequence.	Loss of path to the Avaya call server, expiry of DHCP lease, or unavailable DHCP server when telephone attempts to renegotiate DHCP lease. RESOLUTION: As above.
The phone was working, but does not work now,	AND no lights are lit on the phone and the display is not lit.	CAUSE: Loss of power. RESOLUTION: Check the connections between the phone, the power supply, and the power jack. Follow POE guidelines to troubleshoot POE related problems.
	AND power to the phone is normal, but there is no dial tone. The display might show “System Busy.”	CAUSE: Loss of communication with the call server. RESOLUTION: Check LAN continuity from the call server to the phone using ARP or trace-route and from the phone to the call server. Verify that LAN administration has not changed for the Gatekeeper, TN 2302AP boards, or the LAN equipment (routers, servers, etc.) between the switch and the phone. Verify that telephone settings are not changed locally using VIEW and ADDR information, as described earlier in this guide. Verify that the telephone volume is set high. Finally, conduct a self-test.
	AND the phone was recently moved.	CAUSE: Loss of communication with the call server. RESOLUTION: As above, but verify whether the phone is being routed to a different DHCP server, or even a different call server switch. If so, the new server or switch might need to be administered to support the phone.

Table continues…

Condition		Cause/Resolution
	AND the network was recently changed to upgrade or replace servers, re-administer the Avaya Media Server, add or change NAT, etc.	CAUSE: Loss of communication with the call server. RESOLUTION: As above.
The phone works properly, but you cannot hear incoming DTMF tones.		CAUSE: The TN2302AP board does not pass in-band DTMF tones. RESOLUTION: None; the board is operating as designed.
The phone works properly, but you cannot hear incoming DTMF tones.		CAUSE: Call server suppresses sidetone DTMF. RESOLUTION: After completing call server administration, enable On-Hook Dialing on the Change-System-Parameters screen. If the user has enabled Hands-Free Answer (HFA), answers a call using the Speaker, switches to the handset, and presses dialpad buttons, the phone does not transmit DTMF tones. Disable HFA to hear DTMF tones.
Hands-Free Answer (HFA) is administered but the phone did not automatically answer a call.		CAUSE: HFA only works if the phone is idle. The phone ignores a second call if a call, including the ringing tone is in progress. RESOLUTION: None.
The phone does not use and ignores the HTTP or HTTPS script file and settings file.		CAUSE: The system value AUTH is set to 1 which indicates that HTTPS is required but no valid address is specified in TLSSRVR. RESOLUTION: Change AUTH to 0 (zero), or enter a valid address for TLSSRVR.
The HTTP or HTTPS script file is ignored or not used by the phone,	AND the HTTP or HTTPS server is a LINUX or UNIX system.	CAUSE: The phone expects lines of the script file to terminate with a **<Carriage Return> <Line Feed>**. Some UNIX applications only terminate lines with **<Line Feed>**. Editing the script file with a UNIX-based editor can strip a**<Carriage Return>** from the file. Doing so causes the entire file to be treated as a comment, and thus be ignored. RESOLUTION: Edit the script file with a Windows® —based editor, or another editor that does not strip out the **<Carriage Return>**. CAUSE: UNIX and LINUX systems use case-sensitive addressing and file labels. RESOLUTION: Verify the file names and path in the script file are accurately specified.

Table continues…

Condition		Cause/Resolution
	AND phone administration recently changed.	CAUSE: The B189Hupgrade.txt file was edited incorrectly, renamed, etc. RESOLUTION: Download a clean copy of the `B189Hupgrade.txt` file from the Avaya support web site at http://www.avaya.com/support, and do not edit or rename the file. Customize or change *only* the `46xxsettings.txt` file as required.
The system ignores some settings in the settings file while other settings are being used properly.		CAUSE: Improper administration of settings file. RESOLUTION: Verify that customized settings are correctly spelled and formatted. See *Administering Avaya B189 Conference IP Deskphone*, 16–604294.
Telephone power is interrupted while the phone is saving the application file and the HTTP/HTTPS application stops responding.		CAUSE: The HTTP or HTTPS server stops responding if power is interrupted while a phone is saving the application file. RESOLUTION: Restart the phone.
The user indicates an application or option is not available.		CAUSE: The `46xxsettings.txt` file script is not pointed to accurately, or is not properly administered to allow the application. RESOLUTION: Verify that the `46xxsettings.txt` file script is properly specified for your system, verify that the file server is UNIX or LINUX, and verify the extension. Then verify that all the relevant parameters indicated in Chapter 7 of the *Administering Avaya B189 Conference IP Deskphone*, 16–604294, are accurately specified in the `46xxsettings.txt` file.

Table continues…

Condition		Cause/Resolution
User data disappeared when the user logged out of one phone and logged in to another phone.		CAUSE: The second phone is unable to gain access to the backup file. RESOLUTION: Verify that the first phone creates a backup file. Verify whether appropriate administration was done in accordance with Chapter 7 of the *Administering Avaya B189 Conference IP Deskphone*, 16–604294. Then verify that the second phone is administered to retrieve data from the same location as the first phone. Then verify that all the relevant parameters indicated in Chapter 7 of the *Administering Avaya B189 Conference IP Deskphone*, 16–604294, are accurately specified in the `46xxsettings.txt` file. Finally, verify that the HTTP and HTTPS server on which the backup file is located is operational and accessible from the second phone.

Related links

Troubleshooting on page 38

LLDP Troubleshooting

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

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

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

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

Related links

Troubleshooting on page 38

Proposed Solution

Procedure

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

LLDP setup and troubleshooting steps

For manually programmed deskphones, use the Administration Menu ADDR procedure to set the call server to a valid IP address.

Note:

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

Related links

Troubleshooting on page 38

Proposed solution for DHCP configured deskphones

Procedure

1. Using the Administration menu *ADDR* procedure, set *Phone* to **0.0.0.0**.
2. Verify or set *SSON* to **242** which is the default value.
3. Administer the DHCP server option 242 to include **MCIPADD=***xxx.xxx.xxx.xxx* where *xxx.xxx.xxx.xxx* is the call server IP address.
4. Verify that the DHCP server and the deskphone are on the same VLAN.

5. Verify the *DHCP server* port 67 and or the *DHCP client* port 68 are not blocked on the switch.
6. Verify the configuration of the DHCP Relay Agent on the switch or on a separate PC, for example, MS Windows Server 2000/2003 whether the deskphones and DHCP Server are placed on different networks or subnets. DHCP broadcast messages do not, by default, cross the router interface.

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 B189Hupgrade.txt file contains the line **`GET 46xxsettings.txt`** as the last command line of the upgrade file.
3. Verify that the deskphone can reach the HTTP server and whether the HTTP server is activated.
4. Verify that the B189Hupgrade.txt and 46xxsettings.txt files are placed in the proper directory of the HTTP server to access these files.

Proposed solution for LLDP-configured deskphones

About this task

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

Note:

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

Note:

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

Secure Shell Support

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

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

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

The deskphones support 2048-bit asymmetric key length for SSH server.

You can configure the idle or inactivity time that will disable SSH with the *SSH_IDLE_TIMEOUT* parameter.

Related links

Troubleshooting on page 38

Chapter 7: Related resources

Documentation

Document number	Title	Use this document to:	Audience
Using			
16-604295	Using Avaya B189 Conference IP Phone	Refer to procedures for using Avaya B189 Conference IP Phone.	End users
Administering			
16-604294	Administering Avaya B189 Conference IP Phone	Refer to administrative tasks that you can perform for Avaya B189 Conference IP Phone.	End users and administrators

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and click **Go** to search the course.

Course Code	Course Title
ACIS-6002 ACIS	Avaya Aura® Communication Manager and CM Messaging - Embedded (R6.x)
APSS-1300 APSS	Avaya Networking Solutions

Support

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

Index

Numerics

802.1X operational mode, setting 28

A

Administration menu 26
audio
    expansion microphone 11
    room settings 11
Avaya support website 53

C

clear settings
    phone administration
        clear settings 31
conference
    audio quality 11
connect a PA interface box to a conference phone 21
connectors and controls of a PA interface box 20
craft procedure 39

D

debug mode
    enabling and disabling 31
Downloading Text Language Files 25
DTMF Tones 39
dynamic addressing process 15

E

enable the auxiliary port for the PA system 32
Error Conditions 38
error messages 41

G

group identifier 33
GROUP Parameter 25

I

intended audience 7
Interface Control 34
IP Deskphone
    Requirements 13

L

Language Files for text entry, Downloading 25
layout
    connections 8
LLDP troubleshooting 49
Local administrative procedures 27
logoff procedure 34

O

operation errors 45
overview 11

P

PA interface box 20
    connectors and controls 20
    connect to a PA system 21
PA system 20
phone
    entering the administration menu 26
    overview 8
    restarting 35
plugging in 15
power interruption 39
power-up and reset process 16
Pre-Installation Checklist 13
Pre-Installation Checklist for Static Addressing 29
purpose 7

R

related courses 53
related documentation 53
Requirements, for each IP Deskphone 13
resetting the phone 15
reset values
    phone administration
        reset values 35

S

Secure Shell Support 51
self-test 36
settings
    audio quality 11
settings file, contents 24
Site-Specific Option Number Setting 36
Software 13
software distribution packages 22
software upgrades 22

SSON Procedure 36
Static Addressing
    Pre-Installation Checklist 29
status messages 41, 45
support 53

T

troubleshooting 39
    DTMF tones 39
    power interruption 39
Troubleshooting
    Error Conditions 38
troubleshooting LLDP 49
turn on the internal microphone and speakers 33

U

unnamed registration 19