Administering Avaya B189 Conference IP Phone

Release 1.0
16-604294
Issue 1
December 2013

Notice

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

Note

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

Documentation disclaimer

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

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked 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 its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED 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 AUTHORIZED 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, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

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

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

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that 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”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States

and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

VCCI-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.

Contents

Chapter 1: Introduction

Intended audience

This guide is for personnel who administer Avaya Aura® Communication Manager, DHCP, HTTP/HTTPS servers for Avaya B189 Conference IP Phones and the Local Area Network (LAN).

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
Implementing			
16-604295	Installing and maintaining Avaya B189 Conference IP Phone	Refer to procedures for installing and upgrading Avaya B189 Conference IP Phone	Installation engineers, 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 for the course.

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

Support

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

Chapter 2: Overview

Overview

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

The features of the deskphone 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. As the LEDs are visible from all angles, the deskphone visually alerts the users. Avaya B189 Conference IP Phone has ports for additional microphones.

About Avaya B189 H.323 Conference IP phones

Avaya B189 Conference IP phones use Internet Protocol (IP) technology with Ethernet line interfaces and support the H.323 protocol. These phones support DHCP, HTTP, and HTTPS to get customized settings and to download new versions of software for the phones.

The H.323 standard provides real time transmission for audio, video, and data communications over a packet network.

An Avaya B189 Conference IP phone protocol stack comprises of the following:

- H.225 for registration, admission, status (RAS), and call signaling
- H.245 for control signaling
- Real Time Transfer Protocol (RTP) and Secure Real Time Transfer Protocol (SRTP)
- Real Time Control Protocol (RTCP) and Secure Real Time Control Protocol (SRTCP)

Note:

The following terms are used interchangeably in this document as all the terms refer to the same Avaya B189 Conference IP Phone:

- Deskphone
- Conference Phone

- Phone
- IP Telephone

Chapter 3: Administration overview and requirements

Administrative requirements

This topic outlines the operating environment for the Avaya B189 Conference IP Phone as follows:

- Telephone Administration on the Avaya call server. For more information, see Communication Manager Administration on page 19.
- IP Address management for the deskphone. For more information see, Administering the DHCP and File Servers on page 39 for dynamic addressing.
- Tagging Control and VLAN administration for the phone, if applicable. For more information, see Administering Telephone Options.
- Quality of Service (QoS) administration for the phone, if appropriate. For more information, see QoS on page 30 and Administering QoS on page 21.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP).
- Interface administration for the phone, as appropriate. Administer the phone to LAN interface using the PHY1 parameter. For more information, see Network Requirements on page 27.
- Application-specific phone administration, if applicable. For more information, see Administering Applications and Options on page 79.

The table on page 12 indicates that you can administer system parameters in many ways and use many delivery mechanisms. For example:

- Maintaining the information on the call server.
- Manually entering the information with the phone dial pad.
- Administering the DHCP server.
- Editing the configuration file on the applicable HTTP or HTTPS file server.
- Modifying certain parameters with administrative permission.

Note:

You cannot administer all parameters on all delivery mechanisms.

Table 1: Alternative ways to administer the Avaya B189 Conference IP Phone

Parameter	Administrative mechanisms	Related information
Phone Administration	Avaya call server	Communication Manager Administration on page 19, Server Administration on page 39, and the applicable call server documentation.
IP Addresses	DHCP	Administering The DHCP and File Servers on page 39 and especially Administering the DHCP Server.
	Configuration file	Telephone Software and Application Files on page 49 and Administering Telephone Options.
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 66
Tagging and VLAN	DHCP	Administering The DHCP Server, and Administering Telephone Options.
	Configuration file	Administering The DHCP and File Servers on page 39 and Administering Telephone Options.
	Manual administration at the phone	About Link Layer Discovery Protocol (LLDP) on page 66.
Quality of Service	Avaya call server	Administering UDP port selection on page 20 and the applicable call server documentation.
	DHCP	Administering The DHCP and File Servers on page 39, and Administering Telephone Options.
	Configuration file	Administering The DHCP and File Servers on page 39, and Administering Telephone Options.
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 66.
Interface	DHCP	Administering The DHCP and File Servers on page 39, and Telephone Software and Application Files on page 49.
	Configuration file	Administering The DHCP and File Servers on page 39, and Telephone Software and Application Files on page 49.

Parameter	Administrative mechanisms	Related information
	LLDP	About Link Layer Discovery Protocol (LLDP) on page 66.
Application - specific parameters	Configuration file	Administering The DHCP and File Servers on page 39, and especially HTTP Generic Setup on page 46. Also, Administering Applications and Options on page 79.

For information about administering DHCP servers, see Administering the DHCP and File Servers on page 39, and more specifically, Administering the DHCP Server. For information on administering HTTP servers, see Administering the DHCP and File Servers on page 39, and more specifically, HTTP Generic Setup on page 46. For administration options, see Administering Telephone Options.

Parameter data precedence

If you administer a parameter in multiple places, the last server to provide the parameter takes precedence. The following is a list of precedence, from lowest to highest:

1. Manual administration. Call server or HTTP server or both are two exceptions for the phone parameter STATIC.
2. DHCP, except as indicated in “DHCPACK Setting of Parameter Values” in Setting up the DHCP server on page 43,
3. The 46xxsettings.txt file
4. The Avaya call server.
5. Backup files, if administered and permitted.
6. LLDP: Note: Setting the call server and file server IP addresses have the lowest precedence.

Administrative tasks

To administer Avaya B189 Conference IP Phone, complete the tasks in the order shown.

1. Administer the switch for Avaya B189 Conference IP Phone.
2. Update the 46xxsettings file with site-specific information, as applicable.
3. Update Avaya B189 Conference IP phone using Craft procedures, as applicable. For more information about Local Administrative Procedures, see *Installing and maintaining Avaya B189 Conference IP Phone*.

Administrative checklist

System and LAN administrators must use the following checklist to ensure that all phone system prerequisites and phone requirements are met prior to phone installation.

Table 2: Administrative Checklist

Task	Description	Related information
Network requirements assessment	Determine that network engineers have installed the network hardware and the network hardware can handle phone system requirements.	Network Requirements on page 27.
Call server administration	Verify that the administrator has installed the license of the call server and administered the system for Voice over IP (VoIP). Verify that the administrator has administered each phone as required.	Communication Manager Administration on page 19.
DHCP server installation	Install a DHCP application on at least one new or existing computer on the LAN.	Vendor-provided instructions.
DHCP application administration	Add IP deskphone administration to DHCP application.	Administering The DHCP Server in Server Administration on page 39.
HTTP/HTTPS server installation	Install an HTTP or HTTPS application on at least one new or existing computer on the LAN.	Vendor-provided instructions.
Application files, script file, and settings file installation on the HTTP or HTTPS server.	Download the files from the Avaya support site.	www.avaya.com/support Telephone Software and Application Files on page 49.

Task	Description	Related information
Settings file modification as you want.	Edit the settings file as required, using your own tools.	Telephone Software and Application Files on page 49.

Initialization process overview

The initialization process includes an information exchange when the phone registers. This process includes connecting to the network, DHCP processing, VPN connection, file downloads, and phone registration with the call server.

You must administer all equipment properly prior to initialization.

See*Implementing the Avaya B189 Conference IP Phone*, 16-604293 for a detailed description of initialization, power-up, and the reset process.

Note:

When you start Avaya B189 Conference IP phone without access to the HTTP server, the conference phone reuses parameters from before the reboot. The phone waits for 60 seconds and starts with the old parameters.

Related topics:

Connection to network on page 15
DHCP processing on page 15
File downloads on page 16
Registration with the call server on page 16

Connection to network

The phone is appropriately installed and powered. After a short initialization process, the phone displays the speed at which it is connected to the network and determines whether to initiate 802.1X network access procedures.

DHCP processing

If an IP address has not been manually configured in the phone, the phone initiates DHCP, as described in Administering the DHCP and File Servers on page 39. Among other data passed to the phone is the IP address of the HTTP or HTTPS server.

File downloads

Avaya B189 Conference Phones can download configuration files, language files, and certificate files from either an HTTP or HTTPS server, but they can only download software files from an HTTP server. The phone first downloads an upgrade configuration file, which tells the phone which software files it should use. The phone then downloads a settings configuration file, and based on those settings, it may then download language files and/or certificate files. Finally, the phone will download one or two new software files, depending on whether or not the software in the phone is the same as that specified in the upgrade file. For more information about this download process and settings file, see Telephone Software and Application Files on page 49.

Registration with the call server

The call server referred to in this section is Avaya Aura Communication Manager.

The phone is registered with the call server in two modes, named registration and unnamed registration.

Named registration

In this step, the phone might prompt the user for an extension and password. The phone uses that information to exchange a series of messages with the call server. For a new installation and for full service, the user can enter the phone extension and the password configured on the call server for that particular extension. The information required to restart a phone that was previously registered with an extension number is already stored on the phone.

Unnamed registration

Using this feature, you can register a phone with the call server without an extension, provided the call server also supports this feature. To invoke Unnamed Registration, either enter a null (empty) extension or password or take no action.

A phone registered with Unnamed Registration has the following characteristics:

- Only one call appearance
- No administrable features
- Outgoing calls only, subject to call server Class of Restriction or Class of Service limitations
- Conversion to normal *named* registration possible by the user entering a valid extension and password.

Other administrable options using parameters

- MCIPADD

  You can configure the phone to register to a particular call server by listing the IP addresses in the MCIPADD parameter in DHCP or the 46xxsettings.txt file. The standard

practice is to list the CLANs on the main call server, followed by any Enterprise Survivable Server (ESS) addresses, followed by any Local Spare Processor (LSP). To deviate from this practice, you can list CLANs for multiple main call servers. In general, the phone will start from the beginning of MCIPADD and attempt to register with each IP address in turn, one at a time, until the phone gets a positive response. If MCIPADD is administered, users can register to local call servers.

- UNNAMEDSTAT

  You can also administer the phone to avoid unnamed registration and remain unregistered if no extension and password are provided. .

For more information about the installation process, see *Implementing the Avaya B189 Conference IP Phone*,16-604293.

Error conditions

Assuming proper administration, most of the problems reported by phone users are likely to be LAN-based or Quality of Service. Server administration and other issues can impact user perception of IP phone performance.

For the likely operational problems after you successfully install Avaya B189 Conference IP Phone, see *Installing and maintaining Avaya B189 Conference IP Phone*, 16-604293.

For more information on the end user procedures, see *Using Avaya B189 Conference IP Phone*, 16-604295.

Chapter 4: Communication Manager Administration

Call server requirements

Before you perform administrative tasks, ensure that you have installed the proper hardware and your call server software is compatible with Avaya B189 IP Conference phones. Use the latest PBX software and IP phone firmware. Ensure that you administer the Avaya B189 conference IP Phone as a 9620 IP Deskphone on the CM station administering page.

Call server administration

For call server administration information not covered in this chapter, see the following documents on the Avaya support Web site:

- *Administering Avaya Aura Communication Manager*, 03-300509 for more instructions for administering an IP phone system on Communication Manager.

  For information on the process of adding new phones, see chapter 6,*Managing Telephones*. For related screen illustrations and field descriptions, see chapter on *Screen References*.

- *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504 for more information about switch administration for your network.

Related topics:

Administering the IP interface and addresses on page 20
Administering UDP port selection on page 20
Administering RSVP on page 20
Administering QoS on page 21
Administering IEEE 802.1Q on page 21
Administering DIFFSERV on page 21
Administering NAT on page 21

Administering the IP interface and addresses

Follow these general guidelines:

- Define the IP interfaces for each CLAN and Media processor circuit pack on the call server that uses the IP Interfaces screen. For more information, see *Administration for Network Connectivity for Avaya Communication Manager* , 555-233-504.
- On the Customer Options form, verify that the IP Stations field is set to **Y** (Yes). If it is not set to (Y), contact your Avaya sales representative.

Administering UDP port selection

You can administer the Avaya B189 Conference IP phones from the Avaya Communication Manager Network Region form to support UDP port selection. For information on specific port assignment diagrams, see *Implementing Avaya B189 Conference IP Phone*.

For information about Avaya Communication Manager implementation, see *Administration for Network Connectivity for Avaya Communication Manager, 555-233-504* on the Avaya Support Web site.

Administer the switch to use a port within the proper range for the specific LAN, and the IP deskphone(s) copy that port. If no UDP port range is administered on the switch, the IP deskphone uses an even-numbered port, randomly selected from the interval 4000 to 10000.

Administering RSVP

Avaya B189 Conference IP phones support the Resource Reservation Protocol (RSVP) for IPv4 audio connections only.

You can fully enable RSVP by provisioning CM ip-network-region.

For more information, see your Avaya server administration documentation and *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Administering QoS

The Avaya B189 Conference IP Phones support both IEEE 802.1D/Q and DiffServ. Other network-based QoS initiatives such as UDP port selection do not require support by the phones. However, they contribute to improved QoS for the entire network.

Administering IEEE 802.1Q

The Avaya B189 Conference IP phones can simultaneously support receipt of packets that are tagged, or not tagged according to the IEEE 802.1Q standard. To support IEEE 802.1Q, you can administer Avaya B189 Conference IP Phones from the network through LLDP, or by appropriate administration of the DHCP or HTTP/HTTPS servers.

You can administer the IEEE 802.IQ QoS parameters L2QAUD, and L2QSIG through the IP Network Region form. To set these parameters at the switch, see sections on *Quality of Service (QoS)* and *Voice quality administration* in *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

For information on setting these parameters manually, see *Implementing Avaya B189 Conference IP Phone*.

Administering DIFFSERV

The DiffServ values change to the values administered on the call server as soon as the phone registers. For more information on DiffServ values, see chapter on *Network Quality Administration* in *Administration for Network Connectivity for Avaya Communication Manager, 555-233-504.* Unless there is a specific need in your enterprise LAN, do not change the default values.

Administering NAT

Network Address Translation (NAT) usage can lead to problems that affect the consistency of addressing throughout your network. All Avaya B189 Conference IP phones support NAT interworking. Support for NAT does not imply support for Network Address Port Translation (NAPT). The phones do not support communication to the PBX through any NAPT device.

NAT requires specific administration on the call server. A direct Avaya IP phone-to-Avaya IP phone call with NAT requires Avaya Communication Manager Release 3.0 or later software.

For more information, see *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504 on the Avaya support Web site.

Call conferencing

This section provides information about conference call behaviors to consider when administering the call server. The deskphone application presents a user interface, based in part on the deduction of the call state. The following call states might result when the server-based features interact with the user interface:

- The system parameter Abort Conference Upon Hang-up is set to *Yes*:

  The user must dial and press the **Join** softkey for the conference to be completed. If the user hangs up during conference setup before pressing **Join**, the conference is cancelled with the held party remaining on [hard] hold. When the system parameter Abort Conference Upon Hang-up is set to *No*, the user can hang up immediately after dialing, dial a third party, and then press the **Join** softkey to have the conference proceed normally.

- The system parameter No Dial Tone Conferencing is set to *No* and the **Conference** or **Add** softkey is pressed:

  The call server automatically selects an idle call appearance for the user to dial on. This action allows the user to add the next conferee. When the system parameter No Dial Tone Conferencing is set to *Yes*, the user must manually select a call appearance after pressing the **Conference** or **Add** softkey.

Conferencing behavior changes significantly when you set the Select Line Conferencing to *Yes*. Then the No Dial Tone Conferencing is automatically set to *Yes*. Specifically the following scenarios can occur:

- If the user finishes dialing the intended conferee, pressing the initial call appearance completes the conference, as if the **Join** softkey was pressed.
- If the user has not finished dialing the intended conferee, pressing the initial call appearance cancels the conference set up. Note: The initial conference is placed on soft hold when **Conference** or **Add** button is pressed.
- If the user presses the **Conference** or **Add** softkey, then immediately presses a hard-held call appearance, the previously held call appearance is retrieved from hold and joins the existing conference.

When you set the system parameter Select Line Conferencing to *No*, the user can cancel the conference setup by pressing the call appearance on soft hold before pressing **Join**. Selecting a hard-held call appearance during conference setup establishes the held call as the intended conferee.

For either Select Line Conferencing setting, if the user is in conference setup and answers an incoming call, the incoming call is established as the intended conferee. Then the user must

press **Join** to add the answered call to the conference. If the user does not want the incoming call to be part of the conference, the user must not answer the call, or the user must answer the call and then hang up before continuing the conference setup. Pressing an in-use call appearance during conference setup makes that call appearance the intended conferee. The Toggle Swap feature works for Conference setup similar to Transfer Setup.

For more information about call transfers, see Administering call transfers.

Phone administration on Avaya Aura® Communication Manager

This section covers Avaya Aura® Communication Manager administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. You must administer Avaya Aura® Communication Manager on SAT or by Avaya Site Administration to optimize the phone user interface. The SAT provides the system-wide CM form and the particular page or screen that you need to administer for each feature. You need Communication Manager 3.1.2 or later.

Related topics:

Feature-related system parameters on page 23

Feature-related system parameters

In Avaya Communication Manager Release 4.0 and later, you can administer three system-wide parameters. When you administer these parameters on CM, the parameters are automatically downloaded to the phone during registration. You do not need to add these parameters using the settings file or set them locally for each phone. The three system parameters are: SNMP community string, SNMP Source IP addresses, and Craft Access Code (PROCPSWD).

Note:

Commenting out SNMPSTRING in the settings file will not prevent a response to an SNMP query unless the CM administration is also changed accordingly. Also, setting the SNMP flag on the IP-Options form in CM to "n" does not disable SNMP. You must enable the download flag and leave the community string value blank so that when the telephone registers, the SNMPSTRING value will remain null.

To administer these three parameters use Page 3 of the *change system-parameters ip-options form*.

Name	Description
Auto Hold	Set up CM to enable Auto Hold, so that the phone automatically places an active call on hold when the user answers or resumes a call on another call appearance. Use the System Parameters Features form, page 6.
Coverage Path	Administer a coverage path for both phone demonstration and normal operations. Use the Coverage Path form and give it a number, for example, Coverage path 1. If Voice Mail is available, administer the hunt group or VDN, depending on the type of VM system being used.
Enhanced Conference Features	Enable enhanced conference display to support the user experience for conferences. Set Block Enhanced Conference Display on the Class of Restriction (COR) form to No. Use the command **`Change COR`**, followed by a number, to view the form and make the change. This is a sample of the Class of Restriction form.

Station administration

Administer the following station features on the Station form. The Station form comprises of several pages. You must set the features covered in this section to optimize the user interface.

With Avaya Aura® Communication Manager Release 4.0 and later, you can perform central call server administration of the GROUP parameter on a station-by-station basis. This parameter is then downloaded to each applicable deskphone starting with the next deskphone boot-up. You can use the GROUP Identifier with the 46xxsettings file for administration of specific groups of deskphones. For more information, see Using the GROUP parameter to set up customized groups on page 52. You can administer the GROUP ID parameter on page 3 of the Change Station Form.

Related topics:

Administering features on page 25

Administering features

Administer the following Station Features for maximum user experience:

Name	Description
Enhanced Conference Features	Administer **Conf-dsp** (conference display) on the station form as a feature button. Users gain the benefits of enhanced conference features.
Auto select any idle appearance	Set **Auto select any idle appearance** to N (no) to optimize answering calls.

Chapter 5: Network Requirements

Network Assesment

Perform a network assessment to ensure that the network has the capacity for the expected data traffic and voice traffic, and can support jitter buffers and the following types of applications as required:

- H.323
- DHCP
- HTTP/HTTPS
- LLDP
- RADIUS

You also need QoS support to run VoIP on your configuration. For more information, see Administering UDP port selection on page 20.

Hardware requirements

- Category 5e cables that conform to the IEEE 802.3af-2003 standards, for LAN powering.
- TN2602 or TN2302 IP Media Processor circuit pack. For increased capacity, install a TN2602 circuit pack even if you have a TN2302 IP Media Processor circuit pack.
- TN799C or D Control-LAN (C-LAN) circuit pack.

To ensure that you administer the appropriate circuit packs on your server, see Communication Manager Administration on page 19.

For more information about hardware requirements in general, see *Implementing Avaya B189 Conference IP Phone*.

Server requirements

You can configure three types of servers for Avaya B189 Conference Phones:

- DHCP server: Avaya recommends that you install a DHCP server and do not use static addressing. Install the DHCP server as described in Administering the DHCP and File Servers on page 39.
- HTTP or HTTPS server:Administer the HTTP or HTTPS file server as described in HTTP Generic Setup on page 46.

While the servers listed provide different functions that relate to the Avaya B189 Conference IP Phones, the servers are not necessarily different boxes. For example, DHCP provides file management whereas HTTP provides application management, yet both functions can coexist on one hardware unit. Use any standards-based server.

For parameters related to Avaya Server information, see Communication Manager Administration on page 19, and the administration documentation for your call server. For parameters related to DHCP and file servers, see Server Administration on page 39.

Caution:

The phone obtains important information from the script files on the file server and depends on the application file for software upgrades. If the file server is unavailable when the phone resets, the phone operates based on the default administration and continues with the call server registration process. Not all features are available. To restore the features you must reset the phone when the file server is available.

Required network information

Before you administer DHCP, HTTP, and the HTTPS servers, collect the following network information. If you have more than one Gateway (router), HTTP/HTTPS server, or call server in your configuration, complete the required network information for each DHCP server before you install the phones.

Avaya B189 Conference IP phones support specifying a list of IP addresses for a gateway/ router, HTTP/HTTPS server, and Avaya call servers. Each list can contain up to 255 total ASCII characters, with IP addresses separated by commas with no intervening spaces. Depending on the specific DHCP server, the deskphone might support only 127 characters.

When you specify IP addresses for the file server or call server, use either dotted decimal format (“*xxx.xxx.xxx.xxx*”) or DNS names for IPv4 addresses. If you use DNS, the value of the DOMAIN parameter is appended to the DNS names that you specify. If DOMAIN is null, you must use DNS names that are fully qualified. For more information about DNS, see DHCP Generic Setup on page 42 and DNS addressing on page 64.

Required network information before installation for each DHCP server

- Gateway router IP addresses
- If the HTTP or the HTTPS file server IP addresses, port number, are different from the default, and the directory path if files are not located in the root directory
- Subnetwork mask
- Avaya call server IP address or addresses
- Phone IP address range
- DNS server address or addresses if applicable

As the LAN or System Administrator, you must also:

- Administer the DHCP server. See Server Administration on page 39.
- Edit the configuration file on the applicable HTTP or HTTPS file server. See Choosing the right application file and upgrade script file on page 50.

Other network considerations

Related topics:

Enabling SNMP

Avaya B189 Conference IP Phones support SNMPv2c and Structure of Management Information Version 2 (SMIv2). The phones also respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. The phones respond to queries directed either at the MIB-II or the read-only Custom MIB. Read-only means that you cannot change the values externally with network management tools.

You can restrict the IP addresses from which the phones accepts SNMP queries using the SNMPADD parameter. You can also customize your community string with the SNMPSTRING parameter.

Note:

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

Ping and traceroute

All Avaya B189 Conference IP Phones respond to a ping or traceroute message sent from the call server switch or any other network source. The call server can also instruct the phone to originate a ping or a traceroute to a specified IP address. The phone carries out that instruction and sends a message to the call server indicating the results. For more information about administering an IP telephone system on Communication Manager, see *Administrator Guide for Avaya Communication Manager*, 03-300509.

IP address and settings reuse

After you successfully register the phone with a call server, the phone saves the IP address and the parameter values in the non-volatile memory of the phone. The phone can reuse the saved parameters if the DHCP or HTTP/HTTPS server is not available for any reason after a restart. The setting for the DHCPSTD parameter indicates whether to keep the IP address if no response is received for lease renewal. If set to 1 (No) the phone strictly follows the DHCP standard with respect to giving up IP addresses when the DHCP lease expires. If set to 0 (Yes) the phone continues using the IP address until it detects reset or a conflict.

QoS

For more information about the extent to which your network can support any or all the QoS initiatives, see your LAN equipment documentation. For information about QoS implications for the Avaya B189 Conference IP Phones, see Administering QoS on page 21.

Avaya B189 Conference phones provide some detail about network audio quality. For more information, see Network Audio Quality Display on page 31.

IEEE 802.1D and 802.1Q

For more information about IEEE 802.1D and IEEE 802.1Q and Avaya B189 Conference phones, see Administering IEEE 802.1Q on page 21 and Administering a VLAN on page 62. Three bits of the 802.1Q tag are reserved for identifying packet priority to set any one of the following eight priorities to a specific packet.

- 7: Network management traffic
- 6: Voice for traffic with less than 10 ms latency and jitter
- 5: Video traffic with less than 100 ms latency and jitter
- 4: *Controlled-load* traffic for critical data applications
- 3: Traffic meriting *extra-effort* by the network for prompt delivery, for example, executive email
- 2: Reserved for future use
- 0: The default priority for traffic meriting the *best-effort* for prompt delivery of the network
- 1: Background traffic such as bulk data transfers and backups

Note:

Priority 0 is a higher priority than Priority 1.

Network audio quality

You can monitor network audio performance on the Avaya B189 Conference phones while on a call. You can view this information on the **Network Info** screen.

While on a call, you can view the network audio quality parameters in real-time. See the following table for the various parameters that you can view:

Table 3: Parameters in real-time

Parameter	Possible values
Received Audio Coding	G722
Packet Loss	No data or a percentage. The system counts late and out-of-sequence packets as lost if the packets are discarded. The system does not count the packets as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.

Parameter	Possible values
Packetization Delay	No data or an integer number of milliseconds. The number reflects the amount of delay in received audio packets, and includes any potential delay associated with the codec.
One-way Network Delay	No data or an integer number of milliseconds. The number is half the value RTCP or SRTCP computes for the round-trip delay.
Network Jitter Compensation Delay	No data or an integer number of milliseconds reporting the average delay that is introduced by the jitter buffer of the phone.

The implication for LAN administration depends on the values returned by the phone user reports and topology, loading, and QoS administration for the LAN. This information gives the administrator an idea of how network conditions affect the audio quality of the current call. Avaya assumes you have more detailed tools available for LAN troubleshooting.

IP address list and station number portability

You can specify IP address lists on the Avaya B189 Conference IP phones. On startup or on restart, the phone attempts to establish communication with these various network elements in turn. The phone starts with the first address on the respective list. If the call server denies communication with the phone or the session times out, the phone continues to the next address on the appropriate list and tries that IP address. The phone does not report failure unless all addresses on a specified list fail, improving the reliability of IP telephony.

The address list and station portability capability also make station number portability possible. Assume a situation where the company has multiple locations in London and New York, that share a corporate IP network. Users want to take the phones from the London office to New York office. When the user starts the phones in the new location, the local DHCP server usually routes the user to the local call server. The local DHCP server if configured correctly, registers the user with call server IP address in London.

For details on administration of DHCP servers for lists of alternate call servers, router/gateways, and HTTP/HTTPS servers, see Server Administration on page 39.

For more information on DNS addressing, see DNS Addressing on page 64.

TCP/UDP Port utilization

Avaya B189 Conference phones use many protocols, particularly TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and TLS (Transport Layer Security) to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP port each piece of equipment uses to support each protocol and each task within the protocol.

For more TCP/UDP port utilization information related to Communication Manager, see UDP Port Selection on page 20.

Depending on your network, you must know what ports or ranges to use in the phone operation. Knowing these ports or ranges helps you administer your networking infrastructure.

Note:

Often, the phones use ports defined by IETF or other standards bodies.

Table 4: Received packets (Destination = Avaya B189 Conference IP phone))

Destination port	Source port	Use	UDP or TCP?
22	Any	Packets received by the SSH server of the phone	TCP
The number used in the Source Port field of DNS packets sent by the phone	Any	Received DNS messages	UDP
The number used in the Source Port field of the packets sent by the HTTP client on the phone	Any	Packets received by the HTTP client on the phone	TCP
The number used in the Source Port field of the TLS/SSL packets that are sent by the HTTP client on the phone	Any	TLS/SSL packets that the HTTP client receives on the phone	TCP
68	Any	Received DHCP messages	UDP
161	Any	Received SNMP messages	UDP
1720	Any	H.323 signaling messages	TCP
The number used in the Source Port field of RAS packets that are sent by the phone	1719	H.323 RAS messages	UDP
The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd	Any	Received RTCP and SRTCP packets	UDP

Table 5: Transmitted packets (Source =B189 Conference Phone)

Destination Port	Source Port	Use	UDP or TCP?
The number used in the Source Port field of packets that are received by the SSH server of the phone.	22	Packets that are transmitted by the SSH server of the phone	TCP
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
80 unless specified otherwise	Any unused port number	Packets that the HTTP client transmits on the phone during startup	TCP
80 unless specified otherwise	Any unused port number	Packets that the HTTP client of the phone transmits after startup, for example, for backup and restore	TCP
The number used in the Source Port field of the SNMP query packet that the phone receives	161	Transmitted SNMP messages	UDP
The number used in the Source Port field of packets that are received by the HTTP server of the phone	80	Packets that the HTTP server of the phone transmits	TCP
TLSPORT	Any unused port number	TLS/SSL packets that the HTTP client of the phone transmits during startup	TCP
443 unless explicitly specified otherwise, for example in a URL	Any unused port number	TLS/SSL packets that the HTTP client of the phone transmits after startup, for example for backup or restore	TCP
514	Any unused port number	Transmitted Syslog messages	UDP
33434 - 33523, starts with 33434, increments by 1 for each message sent, 3 messages per hop, up to 30 hops	Any unused port number	Transmitted traceroute messages	UDP

Destination Port	Source Port	Use	UDP or TCP?
1719		Transmitted H.323 RAS messages	UDP
2048 – 3029		Transmitted RTP, RTCP, SRTP, and SRTCP messages	UDP
The port number received in the Transport Address field in the RCF message	1720	H.323 signaling messages	TCP
System-specific	system-specific	Transmitted signaling protocol packets	TCP
The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd	The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd	RTCP and SRTCP packets transmitted to the far end of the audio connection	UDP
RTCPMONPORT	The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd	RTCP packets transmitted to an RTCP monitor	UDP
1719	An unused port number in the range from 49300 to 49309	H.323 RAS messages	UDP
System-specific	System -specific	Transmitted signaling protocol packets	UDP
Determined by SNMP mgmt app	Any unused port number	Transmitted SNMP messages	UDP
Determined by the SSH client or the O/S of the client	Any unused port number	Transmitted SSH messages	TCP

Security

For information about toll fraud, see the respective call server documents on the Avaya support web site. The Avaya B189 Conference phones cannot guarantee resistance to all Denial of Service (DoS) attacks. However, checks and protections are in-built to resist such attacks while maintaining appropriate service to legitimate users.

All Avaya B189 Conference phones support HTTP authentication for backup and restore operations. The reprogrammable non volatile memory stores the authentication credentials and the realm. The reprogrammable nonvolatile memory is not overwritten if new phone software is downloaded. The default value of the credentials and the realm are null, set at manufacture and at any other time that user-specific data is removed from the phone or by the local administrative (Administration Menu) CLEAR procedure.

If an HTTP backup or restore operation requires authentication and the realm in the challenge matches the stored realm, the stored credentials are used to respond to the challenge without prompting the user. However, if the realms do not match, or if an authentication attempt using the stored credentials fails, the user is then prompted to input new values for backup/restore credentials.

If an HTTP authentication for a backup or restore operation is successful and if the user ID, password, or realm used is different than the values currently stored in the phone, the new values will replace the currently stored values.

You also have the following options to restrict or remove how the deskphone displays crucial network information or uses the information. For more information on these options, see Server Administration on page 39.

- Support signaling channel encryption.

  Note:

  Signaling and audio are not encrypted when unnamed registration is effective.

- Restrict the response of the Avaya B189 Conference phones to SNMP queries to only IP addresses on a list you specify.
- Specify an SNMP community string for all SNMP messages the phone sends.
- Restrict the ability of the user to use a phone *Options* application to view network data.
- Compliant with IETF RFC 1948 *Defending Against Sequence Number Attacks*, May 1996, by S. Bellovin. from Release 1.5 onwards.
- Apply the security-related parameters, SNMP community string (SNMPSTRING), SNMP Source IP addresses (SNMPADD), and (Administration Menu) Access Code (PROCPSWD) that is administered on the call server. Download the file with encrypted signaling in addition to unencrypted HTTP or encrypted HTTPS

Related topics:

Registration and Authentication on page 37
Secure Shell Support on page 37

Registration and Authentication

Avaya call servers support using the extension and password to register and authenticate Avaya B189 Conference IP phones. For more information, see the current version of your call server administration manual.

Secure Shell Support

Secure Shell (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. Release 1.0 supports only the SSHv2 version. Because of the sensitive nature of remote access, you can disable permission with the SSH_ALLOWED parameter. Even if permission is given, the deskphone has several inbuilt security features.

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

Time-to-Service

TTS changes the way IP phones register with their gatekeeper, reducing the time to come into service.

In the absence of TTS, the system uses a coupled two-step procedure to bring the IP phones into service:

1. H.323 registration
2. TCP socket establishment for call signaling

The TTS feature separates these steps. In Communication Manager Release 4.0, you can enable IP phones for service with just the registration step. TCP sockets are established later, as needed.

The TTS feature also changes the direction of socket establishment. With TTS,Communication Manager, rather than the phone, initiates socket establishment, which further improves performance. In Communication Manager Release 4, you can enable TTS by default and can also disable TTS for all IP phones in a given IP network region by changing the IP Network form. TTS applies only to IP phones whose firmware has been updated to support this feature. TTS does not apply to the following phones: third party H.323, DCP, BRI, and analog.

For more information, see the *Administrator Guide for Avaya Communications Manager*, 03-300509.

Chapter 6: Server Administration

Software prerequisites

Ensure that you own licenses to use the DHCP, HTTP, and HTTPS server software.

Note:

You can install the DHCP and the HTTP server software on the same computer.

Caution:

The firmware in the Avaya B189 Conference IP Phone reserves the IP addresses of the form 192.168.2.x for internal communications. The phone might not function properly if you configure addresses in that range.

Administering the DHCP and file Servers

Dynamic Host Configuration Protocol (DHCP) minimizes maintenance for the Avaya B189 Conference IP Phone network. With DHCP, you need not individually assign and maintain IP addresses and the other parameters on each IP phone on the network.

Depending on administration, the DHCP server provides the following information to the Avaya B189 Conference IP Phones:

- An IP address of the Avaya B189 Conference IP Phone
- An IP address of the Avaya call server
- An IP address of the HTTP or HTTPS file server
- The subnet mask
- An IP address of the router
- A DNS Server IP address

Administer the LAN so each Avaya B189 Conference phone can reach a DHCP server that contains the IP addresses and subnet mask.

The Avaya B189 Conference IP Phone cannot function without an IP address. Using the IP address reuse capability, the phone can reuse the previous IP address and parameter settings

even if the DHCP server is temporarily unavailable. A user can manually assign a different IP address to an IP deskphone. When the DHCP server finally returns, the Avaya B189 Conference IP Phone does not search for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process.

Ensure that:

- A minimum of two DHCP servers are available for reliability.
- A DHCP server is available when the IP deskphone restarts.
- A DHCP server is available at remote sites if WAN failures isolate IP deskphones from the central site DHCP servers.

The file server provides the Avaya B189 Conference IP Phone with a script file and, if appropriate, new or updated application software.

In addition, you can edit the settings file to customize phone parameters for your specific environment. For more information, see Administering Telephone Options.

Related topics:

Configuring DHCP Option 242 on page 40

Configuring DHCP Option 242

About this task

To administer DHCP option 242 for SSON, make a copy of the existing option 176 for your Avaya B189 Conference phones. Option 242 is specific to the default site and applies to DHCPv4 only. You can then perform one of the following actions:

Procedure

1. Ignore any parameters which the Avaya B189 Conference IP Phones do not support for setting through DHCP in option 242, or
2. Delete unused or unsupported Avaya B189 Conference IP Phone parameters to shorten the length of the DHCP message.

Result

You can set only the following parameters in the DHCP site-specific option for Avaya B189 Conference IP Phones, although most of them can be set in a 46xxsettings.txt file as well.

Table 6: Parameters Set by DHCP in a Site-Specific Option

Parameter	Description
DNSSRVR	Specifies the DNS server IP address or addresses.

Parameter	Description
DOMAIN	Specifies the string that is appended to DNS names in parameter values when they are resolved into IP addresses.
DOT1XSTAT	Controls 802.1X Supplicant operation.
HTTPDIR	Specifies the path name to prepend to all file names used in HTTP and HTTPS GET operations during startup. (0 to 127 ASCII characters, no spaces.) The command is *SET HTTPDIR myhttpdir*. The path relative to the root of the TLS or HTTP file server where Avaya B189 Conference IP Phones files are stored. If an Avaya file server is used to download configuration files over TLS, but a different server is used to download software files through HTTP, set the path of the Avaya server in the DHCP site-specific option, and set HTTPDIR again in the 46xxsettings.txt file with the appropriate path for the second server. HTTPDIR is the path for all HTTP operations except for BRURI.
HTTPPORT	Specifies the TCP port number to download the HTTP file.
HTTPSRVR	Specifies the IP addresses or DNS names of HTTP file servers used to download Avaya B189 Conference IP Phones software files. The files are digitally signed, so TLS is not required for security.
ICMPDU	Controls the extent to which ICMP Destination Unreachable messages are sent in response to messages sent to closed ports so as not to reveal information to potential hackers. The default is 1 which sends Destination Unreachable messages for closed ports used by traceroute.
ICMPRED	Controls whether ICMP Redirect messages are processed. The default is 0 which redirects messages that are not processed.
L2Q	specifies the 802.1Q tagging mode. The default is 0 which signifies automatic.
L2QVLAN	VLAN ID of the voice VLAN. The default is 0.
LOGLOCAL	Controls the severity level of events logged in the SNMP MIB. The default is 7.
MCIPADD	CM servers IP addresses or DNS names. If there are too many addresses or names to include all of them in the DHCP site-specific option, include at least one from each major system. Then set MCIPADD again in the 46xxsettings.txt file with the complete list of addresses. Providing a subset of the addresses through DHCP improves reliability if the file server is not available due to server or network problems.
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 which indicates that it is auto-negotiate.
PROCPSWD	Security string used to access local procedures. The default is 27238 (CRAFT).

Parameter	Description
PROCSTAT	Controls whether local Craft procedures are allowed. The default is 0 which indicates that access to all administrative options is allowed.
REREGISTER	The number of minutes the phone waits before and between re-registration attempts.
REUSETIME	The n umber of seconds to wait for successful completion of DHCP before reusing previous parameters on the default (port) VLAN. The default is 60.
SNMPADD	Allowable source IP addresses for SNMP queries. The default is “ ” (Null).
SNMPSTRING	SNMP community name string. The default is “ ” (Null).
STATIC	Controls whether to use a manually-programmed file server or CM IP address instead of those received through DHCP or a settings file. If a manually programmed file server IP address is to be used, STATIC must be set through DHCP.
TLSDIR	Specifies the path name prepended to all file names used in HTTPS GET operations during startup.
TLSPORT	Specifies the TCP port number for HTTPS file downloading.
TLSSRVR	Specifies the IP addresses or DNS names of Avaya file servers to download configuration files. Specifies that Transport Layer Security is used to authenticate the server.
TLSSRVRID	Controls whether the identity of a TLS server is checked against its certificate.
UNNAMEDSTAT	Specifies whether the deskphone will attempt unnamed registration.
VLANTEST	Controls the length of time the deskphone tries DHCP with a non-zero VLAN ID. When the interval is exceeded, the deskphone records the VLAN ID so that the VLAN ID is not used again, and DHCP continues on the default VLAN. The default is 60 seconds.

These parameters are saved in the non-volatile memory of the Avaya B189 Conference IP Phones. If the DHCP server is not available for any reason during phone restart or reboot, the phone uses these saved parameters.

DHCP Generic Setup

This document describes the generic DCHPv4 administration that works with the B189 Conference IP Phones.

Any DHCP application might work if the DHCP server is correctly configured.

Note:

Avaya does not assume responsibility for configuring your DHCP server. Contact your vendor or supplier for configuring the DHCP server correctly.

Setting up the DHCP server

About this task

DHCP server setup involves:

Procedure

1. Follow vendor instructions to install the DHCP server software.
2. Configure the DHCP server with:
   - IP addresses available for the B189 Conference IP Phones.
   - The following DHCP options for using IPv4:
     - **Option 1: Subnet mask**.
     - **Option 3: Gateway (router) IP addresses**. If using more than one address, the total list can contain up to 255 total ASCII characters. You must separate IP addresses with commas with no intervening spaces.
     - **Option 6: DNS servers address list**. If using more than one address, the total list can contain up to 127 total ASCII characters. You must separate IP addresses with commas with no intervening spaces. At least one address in Option 6 must be a valid, dotted decimal address without a zero.
     - **Option 15: DNS Domain Name**. This string contains the domain name that the system uses to resolve DNS names in system parameters into IP addresses. The system appends this domain name to the DNS name before the B189 Conference IP Phone resolves the DNS address. If you want to use a DNS name for the HTTP server, Option 15 is required. Otherwise, you can specify a DOMAIN as part of customizing HTTP. For more information, see DNS addressing on page 64.
     - **Option 51: DHCP lease time**. If the deskphone does not receive this option, the deskphone does not accept the DHCPOFFER. Avaya recommends a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the system treats the IP address lease as infinite as required by RFC 2131, Section 3.3. In this case, the deskphone does

not require renewal and rebinding procedures even if you receive Options 58 and 59.

Expired leases cause B189 Conference IP Phones to restart. Avaya recommends providing enough leases so the IP address of a B189 Conference IP Phone does not change if you briefly take the phone offline.

Note:

The DHCP standard states that when a DHCP lease expires, the device must immediately cease using the assigned IP address. However, if the network has problems and the you centralize the DHCP server, or if the DHCP server has problems, the deskphone does not receive responses to its request for a renewal of the lease. In this case the deskphone is unusable until the server can respond. Expired leases do not cause the phone to restart because you can renew expired leases. However, if the new IP address is different than the previous, the phone restarts. Ensure that after an IP address is assigned, the deskphone continues using that address after the DHCP lease expires, until the system detects a conflict with another device. With the system parameter DHCPSTD, an administrator can specify that the telephone will do one of the following: a). Comply with the DHCP standard by setting DHCPSTD to 1. b). Continue to use the IP Address after the DHCP lease expires by setting DHCPSTD to 0. This setting is the default. If you invoke the default after the DHCP lease expires, the phone continues to broadcast DHCPREQUEST messages for the current IP address. The deskphone sends an ARP Request for its own IP Address every 5 seconds until the phone receives a DHCPACK, a DHCPNAK, or an ARP Reply. After receiving a DHCPNAK, or ARP Reply, the phone displays an error message, sets the IP address to 0.0.0.0, and attempts to contact the DHCP server again. Depending on the DHCP application you choose, be aware that the application does not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client for one day or more. For example, Windows NT® DHCP reserves expired leases for about 1 day. This reservation period protects a lease for a short time. If the client and the DHCP server are in two different time zones, the clocks of the computers are not synchronized. If the client is not on the network when the lease expires, you have the time to correct the situation.

- **Option 52: Overload Option**, if required. If the B189 Conference IP Phone receives this option in a message and interprets the *sname* and *file* fields in accordance with IETF RFC 2132, Section 9.3.
- **Option 58: DHCP lease renew time**. If the B189 Conference IP phone does not receive this parameter, or if this value is greater than that for

Option 51, the phone uses the default value of T1 (renewal timer) according to IETF RFC 2131, Section 4.5.

- **Option 59: DHCP lease rebind time**. If the B189 Conference IP phone does not receive this parameter, or if this value is greater than that for Option 51, the phone uses the default value of T2 (rebinding timer) according to RFC 2131, Section 4.5
- **Option 242: Site-Specific Option Number (SSON)**. You do not have to use Option 242. If you do not use this option, you must ensure that you administer the key information, especially HTTPSRVR and MCIPADD appropriately elsewhere.

  An example of proper DHCP administration is:

  Option 242 for DHCP: **`MCIPADD`** *=xxxx.xxx.xxx.xxx*

Result

In the following table, DHCPACK Setting of Parameter Values on page 45 the B189 Conference IP phone sets the following parameter values to the DHCPACK message field and option.

Table 7: DHCPACK Setting of Parameter Values

Parameter	Set to
DOMAIN	If received, Option #15.
DHCP lease renew time	Option #58 (if received).
DHCP lease rebind time	Option #59 (if received).
DHCP lease time	Option #51 (if received).
DNSSRVR	Option #6.
HTTPSRVR	The siaddr field, if that field is not a zero.
TLSSRVR	The siaddr field, if that field is non zero.

Because the DHCP site-specific option is processed after the DHCP fields and standard options, the values set in the site-specific option supersede any values set by DHCP fields or standard options, as well as any other previously set values.

You cannot set parameters L2Q and L2QVLAN from a *site-specific option* if the parameter values were previously set by LLDP. For more information, see About Link Layer Discovery Protocol (LLDP) on page 66.

Note:

The B189 Conference IP Phones do not support Regular Expression Matching, and therefore, do not use wildcards.

In configurations where the upgrade script and the application files are in the default directory on the HTTP server, do not use the command HTTPDIR=<path>.

HTTP Generic Setup

About this task

You can store the same application software, script file, and settings file on an HTTP server as you can on a TFTP server. The B189 Conference IP phones do not support TFTP. With proper administration, the B189 Conference IP phone seeks out and uses the application software, script file, and settings file. The B189 Conference IP phone might lose some functionality, if you reset the HTTP server or the HTTP server is unavailable. For more information, see Administering the DHCP and File Servers on page 39.

Caution:

Ensure that the files defined by the HTTP server configuration are accessible from all B189 Conference IP phones that need those files. Ensure that the file names match the names in the upgrade script, including case, as UNIX systems are case-sensitive.

Note:

Use any suitable HTTP application. Commonly used HTTP applications include Apache® and Microsoft® IIS™.

Important:

You must use the Avaya Web configuration server to get HTTPS so that information is authenticated. The Avaya Web configuration server does not support backup or restore. If you intend to use HTTP for backup and restore purposes, you must use an HTTP server that is independent of the Avaya Web configuration server.

To set up an HTTP server:

Procedure

1. Install the HTTP server application.
2. Administer the system parameter HTTPSRVR to the addresses of the HTTP server.

   Include the parameter in DHCP Option 242, or the appropriate SSON Option.
3. Download the upgrade script file and application files from the Avaya website avaya.com/support to the HTTP server.

   For more information, see Telephone Software and Application Files on page 49.

Note:

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

Note:

Many LINUX servers distinguish between upper and lower case names. Ensure that you specify the settings file name accurately and also the names and values of the data within the file.

Result

If you choose to enhance the security of your HTTP environment by using Transport Layer Security (TLS), you must:

- Install the TLS server application.
- Administer the system parameter TLSSRVR to the addresses of the Avaya HTTP server.

Chapter 7: Telephone Software and Application Files

Understanding the general download process

Avaya B189 Conference IP Phones download upgrade files, settings files, language files, certificate files, and software files from a file server. Avaya B189 Conference IP Phone downloads all the file types either through HTTP or HTTPS except the software files, which can only be downloaded through HTTP. Avaya recommends HTTPS for downloading the non software file types because it ensures the integrity of the downloaded file by preventing *man in the middle* attacks. Further, after the deskphone downloads the trusted certificates, HTTPS ensures that the file server is authenticated through a digital certificate. The deskphone does not use HTTPS for software file downloads because Avaya B189 Conference IP Phones software files are already digitally signed. You need not incur additional processing overhead while downloading these relatively large files.

Note:

The files in the Software Distribution Packages discussed in this chapter are identical for file servers running HTTP and HTTPS. The generic term “file server” refers to a server running either HTTP or HTTPS.

When shipped from the factory, Avaya B189 Conference IP Phones might not contain the latest software. When Avaya B189 Conference IP Phone, the phone attempts to contact a file server, and downloads new software only if the software version available on the file server is different than the version on the phone. For subsequent software upgrades, the call server can remotely reset the phone, and the phone initiates the same process for contacting a file server.

The phone queries the file server, which, transmits a B189Hupgrade.txt file to the phone. The software files that the phone must use depend on the instructions in the upgrade file B189Hupgrade.txt.

The Avaya B189 Conference IP Phone then downloads a 46xxsettings.txt file. The settings file contains options that you have administered for any or all the phones in your network. For more information about the settings file, see About the settings file on page 51. After downloading the settings file, the phone downloads the language or the certificate files and then any new software files that the settings require.

Related topics:

Choosing the right application file and upgrade script file on page 50
Using the upgrade file on page 50
About the settings file on page 51

Choosing the right application file and upgrade script file

Software files needed to operate the Avaya B189 Conference IP Phones are packaged together in either a Zip format or RPM/Tar format distribution package. Download the package appropriate to your operating environment to your file server from the Avaya Support Web site at: http://www.avaya.com/support.

H.323 software distribution packages contain:

- One Upgrade file
- All of the Display Text Language Files
- A file named *av_prca_pem_2033.txt* that contains a copy of the Avaya Product Root Certificate Authority certificate in PEM format that may be downloaded to telephones based on the value of the TRUSTCERTS parameter
- A file named *release.xml* that is used by the Avaya Software Update Manager application

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

For detailed information about downloading files and upgrading telephone software, see *Implementing Avaya B189 Conference IP Phone.*

Using the upgrade file

The upgrade file indicates to the phone whether it needs to upgrade software. The upgrade script file also directs the phone to the settings file.

Avaya recommends that you do not alter the upgrade script file because if Avaya changes the upgrade script file in the future, any changes you have made will be lost. Avaya recommends that you use the 46xxsettings.txt file to customize your settings instead. However, you can change the settings file name, if desired, as long as you also edit the corresponding **GET** command in the upgrade script file.

About the settings file

The settings file contains the option settings you need to customize the Avaya B189 Conference IP Phones for your enterprise.

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

- Tag lines that begin with a single # (pound) character, followed by a single space character, followed by a text string with no spaces.
- **Goto** commands, of the form `GOTO tag`. **Goto** commands cause the phone to continue interpreting the settings file at the next line after a `#tag` statement. If no such statement exists, the rest of the settings file is ignored.
- Conditionals, of the form `IF $parameter_name SEQ string GOTO tag`. Conditionals cause the **Goto** command to be processed if the value of the parameter named *parameter_name*exactly matches *string*. If no such parameter named *parameter_name* exists, the entire conditional is ignored. You can use only the following parameters in a conditional statement are: GROUP, MACADDR, MODEL and MODEL4.
- **SET** commands, of the form `SET parameter_name value`. Invalid values cause the specified value to be ignored for the associated *parameter_name* so the default or previously administered value is retained. All values must be text strings, even if the value itself is numeric, a dotted decimal IP Address, etc.
- 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`. The phone attempts to download the file named by *filename*, and if the file is successfully downloaded, the downloaded file is interpreted as an additional settings file, and no additional lines are interpreted in the original file. If the file cannot be obtained, the phone continues to interpret the original file.

Download the 46xxsettings.txt template file from the Avaya Support site and edit it to add your own custom settings.

Using the GROUP parameter to set up customized groups

About this task

Different users might have the same phone model, but require different administered settings. For example, you might want to restrict call center agents from logging off, which might be an essential capability for *hot-desking* associates.

Use the GROUP parameter to set up customized groups:

Procedure

1. Identify the phones and the groups the phones belong to, and designate a number for each group.

   The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group is assigned as Group 0.

2. After you assign the GROUP assignments, edit the configuration file to enable each phone of the appropriate group to download the proper settings.

Result

The following is an example of the configuration file for the call center agent:

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

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

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

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

Chapter 8: Administering Deskphone Options

Administering options for Avaya B189 Conference Phones

You can set the parameters for DHCP, DHCP fields, and options to the required values. For more information, see Administering the DHCP and File Servers on page 39. For HTTP, set the parameters to required values in the settings file. For more information, see About the settings file on page 51.

Use the settings file to administer most parameters on the Avaya B189 Conference IP Phones. Some DHCP applications are complicated and require extensive expertise for administration.

You might choose to completely disable the capability to enter or change option settings from the dial pad. You can set the parameter PROCPSWD as part of standard DHCP/HTTP administration. Alternately, you can set PROCPSWD on the system-parameters ip-options form, in Communication Manager Release 4.0. If PROCPSWD is not null and consists of one to seven digits, a user cannot invoke any local options without first entering the PROCPSWD value on the Administration Menu Login screen.

For more information on craft options, see *Implementing Avaya B189 Conference IP Phone*.

Note:

If you configure the minimum length of the password as four digits, the password is changed to default.

Caution:

If you administer PROCPSWD as part of DHCP/HTTP administration, the value is stored and transmitted unencrypted. Therefore, PROCPSWD is not a high-security technique to inhibit a sophisticated user from getting access to local procedures unless you administer the parameter using page 3 of the system-parameters IP-options form in Communication Manager Release 4.0.

Avaya B189 Conference IP Phone : Customizable system parameters

This table lists the parameters that you can customize in the 46xxsettings file, the default values, parameter descriptions, and valid values.

Table 8: Customizable system parameters

Parameter name	Default value	Description and value range
APPNAME	“ ” (Null)	The file name of the Signed Application or Library Software Package that the phone downloads and installs during power-up or reset if the package has not already been downloaded and installed. You must set this parameter only in an upgrade file.
APPSTAT	1	Controls whether specific applications are enabled, restricted, or disabled. Values are: 1=all applications enabled, 2=Speed Dial (Contacts) changes and Call Log disabled and Redial last number only, 3=Speed Dial (Contacts) changes disabled, 0=Speed Dial (Contacts) changes, Call Log, and Redial disabled.
APPLICATIONWD	1	Controls whether the application watchdog is enabled 1 or disabled 0. The application watchdog software process, if enabled, monitors other software processes and determines whether the processes have become unresponsive. The application watchdog software process also generates a log event and either kills the process or resets the phone.
AUDASYS	3	Globally controls audible alerting. Possible system settings for audible alerting are 0 through 3 as follows: 0=Audible Alerting is Off; user cannot change this setting. 1=Audible Alerting is On; user cannot change this setting. 2=Audible Alerting is Off; user can change this setting. 3=Audible Alerting is On; user can change this setting.
AUTH	0	Script file authentication value (0=HTTP is acceptable, 1=HTTPS is required).
BAKLIGHTOFF	120	Number of minutes without display activity to wait before setting the backlight to the lowest level.

Parameter name	Default value	Description and value range
		The default is 120 minutes (2 hours). Valid values range from zero to 999 minutes (16.65 hours).
BRAUTH	0	Backup and restore authentication control. Valid values are: 1=If at least one digital certificate is downloaded based on TRUSTCERTS. The IP address of the call server with which you register the phone and the registration password of the phone are included as the credentials in an Authorization request-header in each transmitted GET and PUT method if and only if the value of BRAUTH is 1. 0=The IP address of the call server and registration password of the phone is not included as part of GET or PUT Authorization header, or no digital certificate has been downloaded.
BRURI	" " (Null)	URL used for backup and retrieval of user data. Specify the HTTP or HTTPS server and the directory path or port number to backup file. Do not specify backup file name. Value: 0-255 ASCII characters. Null is a valid value and you can enter spaces. You can specify a subdirectory, for example: `SET BRURI http://135.8.60.10/backup` This parameter puts the user backup or restore files in a subdirectory away from all other files such as bins, .txts, and others. This parameter turns on authentication for that subdirectory, without turning it on for the root directory. If this value is null or begins with a character sequence other than *http://* or *https://* the Backup or Restore option will not display to the phone user.
DHCPSTD	0	DHCP Standard lease violation flag. Indicates whether to keep the IP address if there is no response to lease renewal. If set to 1, (No) the phone strictly follows the DHCP standard with respect to giving up IP addresses when the DHCP lease expires. If set to 0,(Yes) the phone continues using the IP address until it detects reset or a conflict. For more information, see DHCP Generic Setup on page 42.
DNSSRVR	0.0.0.0	Text string containing the IP address of zero or more DNS servers, in dotted-decimal format, that is separated by commas with no intervening spaces, 0-255 ASCII characters, including commas.

Parameter name	Default value	Description and value range
DOMAIN	“ ” (Null)	Text string containing the domain name that the phone must use when it resolves the DNS names in parameter values into IP addresses. Valid values are 0-255 ASCII characters. If Null, do not leave spaces.
DOT1XEAPS	MD5	Specifies the EAP method used for 802.1X operation. Valid values are *MD5* and *TLS* .
DOT1XSTAT	0	Determines how the phone handles Supplicants. Valid values are: 0= Supplicant operation is completely disabled. 1=Supplicant operation is enabled, but responds only to received unicast EAPOL messages. 2 = Supplicant operation is enabled and responds to received unicast and multicast EAPOL messages. For more information, see About IEEE 802.1X.
ENHDIALSTAT	1	Enhanced Dialing Status. If set to 1, the Administering dialing methods feature is turned on for all associated applications. For more information, see Administering dialing methods on page 72. If set to 0, the feature is turned off.
GRATARP	0	Gratuitous ARP flag. Controls whether the phone processes gratuitous ARPS or ignores them. If you use Processor Ethernet (PE) duplication and if your phones are on the same subnet as the PE interfaces, set this parameter to 1, to allow the fastest failover to the new PE interface. Valid values are: 1 = Yes, process gratuitous ARPS 0 = No, ignore gratuitous ARPS
GUESTDURATION	2	Guest login duration in hours. One or two ASCII numeric digits. Valid values are 1, through 12.
GUESTLOGINSTAT	0	Guest login permission flag. If set to 1, the Guest Login option is listed on the Avaya Menu; if set to 0, the Guest Login option is not available.
GUESTWARNING	5	Guest login warning in minutes to indicate when to notify the user that *GUESTLOGINDURATION* will expire. One or two ASCII numeric digits. Valid values are 1 through 15.
HTTPDIR	“ ” (Null)	HTTP server directory path. The path name prepended to all file names used in HTTP *GET* operations during initialization. Value: 0-127 ASCII characters, no spaces. Null is a valid value.

Parameter name	Default value	Description and value range
		Leading or trailing slashes are not required. The command syntax is *SET HTTPDIR myhttpdir*" where *myhttpdir* is your HTTP server path. HTTPDIR is the path for all HTTP operations except for BRURI.
HTTPPORT	80	TCP port number used for HTTP file downloading. 2 to 5 ASCII numeric digits. Valid values are 80 through 65535. Note that when the file server is on Communication Manager, set this value to 81 that is the port required for HTTP downloads rather than the using the default.
HTTPSRVR	" " (Null)	IP address(es) or DNS Name(s) of HTTP file servers used to download phone files. Dotted decimal or DNS format, separated by commas,0-255 ASCII characters, including commas.
ICMPDU	0	Controls whether ICMP Destination Unreachable messages will be processed. Values are: 0=No, 1=Send limited Port Unreachable messages, 2=Send Protocol and Port Unreachable messages.
ICMPRED	0	Controls whether ICMP Redirect messages will be processed. Values are: 0=No, 1=Yes.
L2Q	0	Controls whether Layer 2 frames have IEEE 802.1Q tags (0=auto, 1=enabled, 2=disabled).
L2QVLAN	0	802.1Q VLAN Identifier (0 to 4094). Null (" ") is not a valid value and the value cannot contain spaces. VLAN identifier that IP phones use. Set this parameter only if IP phones use a VLAN that is separate from the default data VLAN. If you must configure the VLAN identifier using H.323 signaling based on Communication Manager administration forms, the VLAN should not be set here. From software Release 2.0, L2QVLAN will always be initialized from the corresponding system initialization value at power-up, but will not be initialized from the system initialization value after a reset.
LANG0STAT	1	Controls whether the user can select built-in English language text strings. Valid values are: 0 = User cannot select English language text strings 1 = User can select English language text strings. SET LANG0STAT 1

Parameter name	Default value	Description and value range
LANGxFILE	“ ” (Null)	Contains the name of the language file *x*, where *x* is 1 through 4. The file name must end in .txt. Example: SET LANG1FILE “mlf_russian.txt” LANG1FILE = LANG2FILE = LANG3FILE = LANG4FILE =
LANGSYS	“ ” (Null)	System wide language that contains the name of the default system language file, if any. Value is 0 to 32 ASCII characters. The file name must end in .txt. The default is a null string. Example: SET LANGSYS mlf_german.txt
LLDP_XMIT_SECS	30	Specifies the rate in seconds at which LLDP messages will be transmitted. Valid values are 1 to 4 ASCII numeric digits, “1” through “3600”
LOGLOCAL	0	Event Log Severity Level. Valid values are one 0-8 ASCII numeric digit. Controls the level of events logged in the endptRecentLog and endptResetLog objects in the SNMP MIB. Events with the selected level and with a higher severity level are logged. Valid values are: 0=Disabled, 1=emergencies, 2=alerts, 3=critical, 4=errors, 5=warnings, 6=notices, 7=information, 8=debug.
MCIPADD	0.0.0.0	Call Server address. Zero or more Avaya Communication Manager server IP addresses. Format is dotted-decimal or DNS name format, that is separated by commas without intervening spaces (0-255 ASCII characters, including commas). Null is a valid value.
NVHTTPSRVR	“ ” (Null)	Applies to both VPN and non-VPN settings. NVHTTPSRVR is the HTTP file server IP addresses used to initialize HTTPSRVR the next time the phone starts up. Zero to 255 ASCII characters: zero or more IP addresses in dotted decimal, colon-hex, or DNS name format, that is separated by commas without any intervening spaces. NVHTTPSRVR is provided for VPN mode so that a file server IP address can be pre configured and saved in non volatile memory. .
NVMCIPADD	“ ” (Null)	Call server IP addresses. Zero to 255 ASCII characters; zero or more IP addresses in dotted-

Parameter name	Default value	Description and value range
		decimal, colon-hex, or DNS name format, that is separated by commas without any intervening spaces.
NVTLSSRVR	“ ” (Null)	VPN and non-VPN. HTTPS file server IP addresses used to initialize TLSSRVR the next time the phone starts up. 0 to 255 ASCII characters: zero or more IP addresses in dotted decimal, colon-hex, or DNS name format, and separated by commas without any intervening spaces.
OPSTAT	111	Option status flag(s) (1 or 3 ASCII numeric digits) indicate which options are user-selectable. The default of 111 grants access to all options and related applications. Single digit valid values are: 1=user can access all options, including Logout, 2= user can access only view-oriented applications. Three-digit valid values are a concatenation of binary values, in the form *abc*, where each letter represents a 0 (disabled/off) or 1 (enabled/on), interpreted as: *a* = base settings for all user options and related applications, except as in *b* or *c*. *b* = setting for view-oriented applications (for example, the Network Information application), as applicable. *c* = setting for Logout application, if applicable. The binary 0 does not allow an end user to see or invoke options and related applications. Setting the flag to binary 1 gives full display and access to all options and related applications.
OPSTAT2	0	OPSTAT override flag. If set to 0, OPSTAT is not affected. If set to 1, OPSTAT is unaffected with the exception that any changes to customized labels in the backup file are uploaded and used as if OPSTAT permitted this action.
PHNCC	1	Telephone country code. The administered international country code for the location by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1-3 digits, from 1 to 999.
PHNDPLENGTH	5	Internal extension phone number length. Specifies the number of digits associated with internal extension numbers by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from 3 to 13.

Parameter name	Default value	Description and value range
PHNEMERGNUM	“ ” (Null)	Emergency phone/extension number. Specifies the number that the phone must dial automatically when the phone user presses the **Emerg** button. Value: 0-30 ASCII dialable characters from 0 through 9, star (*), pound (#) and no spaces. Null is a valid value.
PHNIC	011	Telephone international access code. The maximum number of digits, if any, dialed to access public network international trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-4 digits.
PHNLD	1	Telephone long distance access code. The digit, if any, dialed to access public network long distance trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 digit or “ ” (Null).
PHNLDLENGTH	10	Length of national phone number. The number of digits in the longest possible national phone number by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from “3” to “10.” Range: 1 or 2 ASCII numeric characters, from 5 to 15.
PHNOL	9	Outside line access code. The character(s) dialed, including # and *, if any, to access public network local trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-2 dialable characters, including “ ” (Null).
PHNSCRILDE	0	Window displayed when phone is in Idle state. Valid values: 0 and 1. Changed through the settings file.
PHNSCRUNREG	0	Window displayed when user is not registered. Valid values are 0 or 1.
PHY1STAT	1	Ethernet line interface setting 1=auto-negotiate, 2=10 Mbps half-duplex, 3=10 Mbps full-duplex, 4=100 Mbps half-duplex, 5=100 Mbps full-duplex, and 6=1000 Mbps full-duplex, if supported by the hardware.
PROCPSWD	27238	Text string containing the local dial pad procedure password (Null or 1-7 ASCII digits). If set, the user must enter the password immediately after accessing the Craft Access Code Entry screen, either during initialization or when Mute or the

Parameter name	Default value	Description and value range
		Contacts button for the 9610 is pressed to access a craft procedure. Intended to facilitate restricted access to local procedures even when command sequences are known. Password is viewable, not hidden.
PROCSTAT	0	Local dial pad Administrative Options status (0=all Administrative (Craft) Options are allowed, 1=only VIEW is allowed).
REREGISTER	20	Registration timer in minutes. Controls an H.323 protocol timer that you should change only under very special circumstances by someone who fully understands the system operation impact. Value is 1-120.
REUSETIME	60	The number of seconds to wait for successful completion of DHCP before reusing previous parameters on the default (port) VLAN. Valid values are 1 to 3 ASCII numeric digits, 0 and 20 through 999.
RTCPMON	“ ” (Null)	Text string containing the 4-octet IP address of the RTCP monitor currently in use, in dotted decimal or DNS Name format (0-15 ASCII characters, no spaces).
SSH_ALLOWED	1	Secure Shell (SSH) Protocol permission flag. (0=SSH is not supported, 1= SSH is supported). “Supporting SSH” means the Avaya Services organization can have remote access to the phone, using SSHv2, as described in topic Secure Shell Support.
SNMPADD	“ ” (Null)	Text string containing zero or more allowable source IP addresses for SNMP queries, in dotted decimal or DNS format, that is separated by commas, with up to 255 total ASCII characters including commas. From Communication Manager Release 4.0 onwards, you can administer the SNMP addresses on the system-parameters IP-options form also.
SNMPSTRING	“ ” (Null)	Text string containing the SNMP community name string (up to 32 ASCII characters, no spaces). From Communication Manager Release 4.0 onwards, you can administer the SNMP community string on the system-parameters IP-options form.

Parameter name	Default value	Description and value range
TIMERSTAT	0	TIMERSTAT specifies whether Timer On and Timer Off softkeys is presented to the user. 0 = Timer On and Timer Off softkeys is not presented to the user (default). 1 = Timer On and Timer Off softkeys is presented to the user.
TLSDIR	“ ” (Null)	HTTPS server directory path. The path name prepended to all file names used in HTTPS get operations during initialization. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required. The command syntax is *SET TLSDIR mytlsdir* where *mytlsdir* is your HTTPS server path. TLSDIR is the path for all HTTPS operations except for BRURI.
TLSPORT	80	TCP port number used for HTTPS file downloading. 2 to 5 ASCII numeric digits. Valid values are 80 through 65535. When the file server is on Communication Manager, set this value to 81 which is the port required for HTTPS downloads rather than the using the default value.
TLSSRVR	“ ” (Null)	IP addresses or DNS Names of HTTPS file servers used to download phone files. Dotted decimal or DNS format, separated by commas. Valid values are 0-255 ASCII characters, including commas.
TLSSRVRID	1	Controls whether the identity of a TLS server is checked against its certificate. 1 ASCII numeric digit. Valid values are: 1=Provides additional security by checking to verify that the server certificate’s DNS name matches the DNS name used to contact the server. 0=Certificate is not checked against the DNS name used to contact the server.

Note:

For more information, see Administering Applications and Options on page 79.

Administering a VLAN

This section contains information on how to administer Avaya B189 Conference IP Phones to minimize registration time and maximize performance in a Virtual LAN (VLAN) environment.

If your LAN environment does not include VLANs, set the system parameter L2Q to 2 (off) to ensure correct operation.

Related topics:

[About VLAN Tagging](#) on page 63
[The VLAN default value and priority tagging](#) on page 63
[Automatic detection of a VLAN](#) on page 64

About VLAN Tagging

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

If VLAN tagging is enabled (L2Q=0 or 1), theB189 Conference IP Phones set the VLAN ID to L2QVLAN, and VLAN priority for packets from the deskphone to L2QAUD for audio packets and L2QSIG for signaling packets. The default value (6) for these parameters is the recommended value for voice traffic in IEEE 802.1D.

The VLAN default value and priority tagging

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

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

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

You can also administer another parameter VLANTEST that defines the number of seconds the B189 Conference IP Phone waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is *60* seconds. If you use VLANTEST, the deskphone returns to the default VLAN if an invalid VLAN ID is administered or if the phone moves to a port where the L2QVLAN value is invalid.

The default value of VLANTEST is long, allowing for the scenario that a major power interruption is causing the phones to restart. Always allow time for network routers, the DHCP servers, and other equipment to be returned to service. If the deskphone restarts for any reason and the VLANTEST time limit expires, the administered VLAN ID becomes invalid. The deskphone then initiates operation with a VLAN ID of 0. Or, if the value of L2Q is 0, that is auto,

the deskphone turns off tagging until the L2QVLAN is set to a non-zero value or until the deskphone verifies that the network can support tagged frames.

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

Automatic detection of a VLAN

The phones support automatic detection of the L2QVLAN setting that is incorrect. When the value of L2QVLAN is not 0 and VLAN tagging is enabled, L2Q= 0 or 1, initially the B189 Conference IP Phone transmits DHCP messages with IEEE 802.1Q tagging and sets the VLAN ID to L2QVLAN. The phones will continue to do this for number of seconds configured by VLANTEST.

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

Note:

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

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

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

About DNS addressing

Avaya B189 Conference IP Phones support DNS addresses, dotted decimal addresses, and colon-hex addresses. The phone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the contents of DHCP Option 6. For more information, see DHCP Generic Setup on page 42. At least one address in Option 6 must be a valid, non-zero, dotted decimal address. Otherwise DNS fails. The text string for the DOMAIN system parameter, Option 15

is appended to the addresses in Option 6 before the phone attempts DNS address resolution. If Option 6 contains a list of DNS addresses, those addresses are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS by DHCP, you can specify the DNS server and or the domain name in the HTTP script file. But first SET the DNSSRVR and DOMAIN values so that you can use those names later in the script.

Note:

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

802.1X Supplicant operation

Avaya B189 Conference IP Phones that support Supplicant operation also support Extensible Authentication Protocol (EAP), and earlier, only with the MD5-Challenge authentication method. For more information about the MD5–Challenge authentication, see IETF RFC 3748.

A Supplicant identity (ID) and password of not more than 12 numeric characters are stored in reprogrammable non-volatile memory. The phone software downloads do not overwrite the ID and password. The default ID is the MAC address of the phone, converted to ASCII format without colon separators, and the default password is null. Both the ID and password are set to default values at manufacture. EAP-Response/Identity frames use the ID in the Type-Data field. EAP-Response/MD5-Challenge frames use the password to compute the digest for the Value field, leaving the Name field blank.

When you install a phone for the first time and 802.1x is in effect, the dynamic address process prompts the installer to enter the Supplicant identity and password. The IP phone does not accept null value passwords.

An IP phone can support several different 802.1X authentication scenarios, depending on the capabilities of the Ethernet data switch to which the deskphone is connected. Some switches might authenticate only a single device per switch port. This operation is known as single-supplicant or port-based operation. These switches usually send multicast 802.1X packets to authenticating devices.

The switch supports Standalone phone (Telephone Only Authenticates) - When you configure the IP phone for Supplicant Mode (DOT1XSTAT=2), the phone can support authentication from the switch.

Some switches support authentication of multiple devices connected through a single switch port. This operation is known as multi-supplicant or MAC-based operation. These switches

usually send unicast 802.1X packets to authenticating devices. These switches support the following two scenarios:

- Standalone phone (Telephone Only Authenticates) - When you configure the IP phone for Supplicant Mode (DOT1XSTAT=2), the phone can support authentication from the switch. When DOT1X is “0” or “1” the phone cannot authenticate with the switch.

About Link Layer Discovery Protocol (LLDP)

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

IEEE 802.1AB-2005 specifies the transmission and reception of LLDP. The Avaya B189 Conference IP Phones use Type-Length-Value (TLV) elements specified in IEEE 802.1AB-2005, TIA TR-41 Committee - Media Endpoint Discovery (LLDP-MED, ANSI/TIA-1057), and Proprietary elements. LLDP Data Units (LLDPDUs) are sent to the LLDP Multicast MAC address (01:80:c2:00:00:0e).

These phones:

- do not forward frames received with the 802.1AB LLDP group multicast address as the destination MAC address between the Ethernet line interface and the secondary Ethernet interface.

The Avaya B189 Conference IP phone initiates LLDP after receiving an LLDPDU message from an appropriate system. After the phone is initiated, the phone sends an LLDPDU every 30 seconds or as specified by LLDP_XMIT_SECS parameter with the following contents:

Table 9: LLDPDU transmitted by the phones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPv4 IP Address of phone.
Basic Mandatory	Port ID	MAC address of the phone.
Basic Mandatory	Time-To-Live	120 seconds.
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.
Basic Optional	System Capabilities	Bit 2 (Bridge) is set in the System Capabilities if the phone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled. Bit 5 (phone) in the System Capabilities. If Bit 5 is set in the Enabled Capabilities than the phone is registered.

Category	TLV Name (Type)	TLV Info String (Value)
Basic Optional	Management Address	Mgmt IPv4 IP Address of phone. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the phone.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports auto-negotiation status and speed of the uplink port on the phone.
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery - Class III - IP Telephone.
TIA LLDP MED	Extended Power-Via-MDI	Power Value = 0 if the phone is not currently powered through PoE, else the maximum power usage of the deskphone plus all modules and adjuncts powered by the phone in tenths of a watt.
TIA LLDP MED	Network Policy	Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value.
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Firmware Revision	BOOTNAME, Firmware Revision = RFSINUSE
TIA LLDP MED	Inventory – Software Revision	APPNAME, Software Revision = APPINUSE.
TIA LLDP MED	Inventory – Serial Number	Phone serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final D *xxx* characters removed.
Avaya Proprietary	PoE Conservation Level Support	Provides power conservation abilities and settings, Typical and Maximum Power values. OUI = 00-40-0D (hex), Subtype = 1.
Avaya Proprietary	Call Server IP Address	Call Server IP address. Subtype = 3.
Avaya Proprietary	IP Phone Addresses	Phone IP address, Phone address mask, Gateway IP address. Subtype = 4.
Avaya Proprietary	CNA Server IP Address	CNA Server IP address = in-use value from CNASRVR. Subtype = 5.

Category	TLV Name (Type)	TLV Info String (Value)
Avaya Proprietary	File Server	File Server IP address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not. Subtype = 7.
Basic Mandatory	End-of-LLDPDU	Not applicable.

On receipt of a LLDPDU message, the phones will act on the TLV elements described in the following table:

Table 10: Impact of TLVs Received by Avaya B189 Conference IP Phones on System Parameter Values

System Parameter Name	TLV Name	Impact
L2QVLAN and L2Q	IEEE 802.1 VLAN Name	The value is changed to the TLV VLAN Identifier. L2Q will be set to 1 (ON). VLAN Name TLV is only effective if the following conditions are met: • The phone is not registered with the call server. • Name begins with VOICE (letters are not case-sensitive). • The VLAN is not zero. • DHCP Client is activated. • The phone is registered but is not tagging layer 2 frames with a non-zero VLAN ID. If VLAN Name causes the phone to change VLAN and the phone already has an IP Address the phone will release the IP Address and reset. If the TLV VLAN ID matches the VLAN ID the phone is using, the VLAN ID is marked as set by LLDP. Otherwise, if already registered, the phone waits until there are no active calls, releases its IP Address, turns on tagging with the TLV VLAN ID, sets L2Q to *on* changes the default L2Q to *on* and resets. If there is no valid IP Address, the phone immediately starts tagging with the new VLAN ID without resetting.
L2Q, L2QVLAN, L2QAUD, L2QSIG, DSCPAUD, DSCPSIG	MED Network Policy TLV	L2Q - set to 2 (off) If T (the Tagged Flag) is set to 0; set to 1 (on) if T is set to 1. L2QVLAN - set to the VLAN ID in the TLV. L2QAUD and L2QSIG - set to the Layer 2 Priority value in the TLV. DSCPAUD and DSCPSIG - set to the DSCP value in the TLV.

System Parameter Name	TLV Name	Impact
		The system checks whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • the value of USE_DHCP is 0 and the value of IPADD is not *0.0.0.0*, or • the Application Type is not 1 (Voice), or • the Unknown Policy Flag (U) is set to 1.
MCIPADD	Proprietary Call Server TLV	MCIPADD will be set to this value if it has not already been set.
TLSSRVR and HTTPSRVR	Proprietary File Server TLV	TLSSRVR and HTTPSRVR will be set to this value if neither of them have already been set.
L2Q	Proprietary 802.1 Q Framing	The default L2Q is set to the value of this TLV. No change is made to the current L2 tagging, but the new default value is used on the next reboot. If TLV = 1, L2Q set to 1 (On). If TLV = 2, L2Q set to 2 (Off). If TLV = 3, L2Q set to 0 (Auto).
	Proprietary - PoE Conservation TLV	This proprietary TLV can initiate a power conservation mode that turns the phone backlight on or off in response to this TLV.
	Extended Power-Via-MDI	Power conservation mode is enabled if the received binary Power Source value is 10, and power conservation mode is disabled if the received binary Power Source value is not 10. Power conservation mode is enabled even if the phone is not powered over Ethernet because the phone sends information about the power source that it is using in a TIA LLDP MED Extended Power-Via-MDI TLV. The power management system intends to conserve local power also.

Administering settings at the phone

Implementing Avaya B189 Conference IP Phone describes how to use Administration Menu procedures at the phone for administration. The local procedures you might use as an administrator are:

- 802.1x - Enable or disable the Supplicant and the Pass-thru options.
- ADDR - Add the IP addresses for the call server, HTTP server, HTTPS server, and other network related parameters.
- CLEAR - Remove all administered values, user-specified data, option settings, etc. and return a phone to the phone's initial “out of the box” default values.
- DEBUG - Enable or disable debug mode for the button module serial port.
- GROUP - Set the group identifier on a per-phone basis.
- INT - Set or change the interface control value(s) of PHY1STAT
- RESET VALUES - Reset the phone to default values including any values administered through local procedures, and the values that were previously downloaded using DHCP or a settings file.
- RESTART PHONE- Restart the phone in response to an error condition, including the option to reset parameter values.
- SSON - To add site specific options.
- Test - To run a self test on the phone.
- VIEW - Review the Avaya B189 Conference IP Phone system parameters to verify the current parameter values and file versions.

Note:

You can use the DEBUG option only if you change the default password to the Administration Menu procedures through the PROCPSWD parameter.

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

Administering display language options

By default, Avaya B189 Conference IP Phones display information in the English language. All software downloads include language files for 13 more languages. Administrators can

specify from one to four languages for each phone to replace English. Users can then select the language in which the phone displays messages.

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

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

• US-English	• Simplified Chinese
• Japanese	• Korean
• German	• French
• Italian	• Russian
• Spanish	• Portuguese

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

- LANGxFILE - The name of a selected language file, for example, *French*. In addition to providing the language name as this value, replace the *x* in this parameter with a 1, 2, 3, or 4 to indicate which of the four languages you are specifying. For example, to indicate that German and French are the available languages, the setting is: **`LANG1FILE=mlf_german.txt`** and **`LANG2FILE=mlf_french.txt`**.
- LANG0STAT - Use this parameter to select the built-in English language when other languages are downloaded. If LANG0STAT is 0 and at least one language is downloaded, you cannot select the built-in English language. If LANG0STAT is 1 then you can select the built-in English language text strings.
- LANGSYS - The file name of the system default language file, if any.

For more information, see B189 Conference Phones - Customizable System Parameters on page 54. For more information on multiple language strings, see *Implementing Avaya B189 Conference IP Phone*.

To download a language file or to review pertinent information, go to support.avaya.com

Note:

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

Administering dialing methods

Avaya B189 Conference IP Phones have a variety of telephony-related applications that might obtain a telephone number during operation. Two dialing methods are used, depending on which version of Avaya Aura® Communication Manager that is running.

Related topics:

Understanding log digit or Smart Enbloc dialing on page 72
Using enhanced local dialing on page 72
Enhanced local dialing requirements on page 73

Understanding log digit or Smart Enbloc dialing

Avaya Aura® Communication Manager Releases 4.0 and later support the feature of a superior level of *enhanced log digit analysis*. This feature is also called smart enbloc dialing and it allows the call server to supplement the number the deskphone dials based on the call server's knowledge of the entire dialing plan. With the server supporting log digit dialing analysis, the deskphone does not attempt to enhance a number as described for enhanced local dialing, and the call server assumes responsibility for analysis and action. Smart enbloc provides a more accurate dialing method because the deskphone signals to the call server that log dialing digit analysis is requested for all calls originated by the Redial buffer(s), the local Call Log/ History applications, and all web-based dialing.

Using enhanced local dialing

For servers running a CM release earlier than 4.0, Avaya B189 Conference IP phones evaluate a stored phone number (other than those in the Contacts list) based on parameters administered in the settings file. The phone can then automatically prepend the correct digits, saving the user time and effort. This feature is Enhanced Local Dialing. If you correctly configure several important values, you can successfully implement this feature.

For more information, see B189 Conference Phones - Customizable System Parameters on page 54

The parameters relevant to the Enhanced Dialing Feature are:

- ENHDIALSTAT: Enhanced dialing status. If set to 1 which is the default value, the enhanced local dialing feature is turned on. If set to 0, enhanced local dialing is off. However, even

when the ENHDIALSTAT parameter is used, Using log digit (Smart Enbloc) dialing on page 72 takes precedence, regardless of the ENHDIALSTAT setting.

Note:

As with any parameters, the default values are used unless you explicitly administer different values. Thus, if you do not administer a given parameter or if you comment a given parameter out in the 46xxsettings file, the default value for that parameter is used.

Note:

In all cases, the digits the phones insert and dial are subject to standard Avaya server features and administration such as, Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), and so on. You can administer the system parameter ENHDIALSTAT to turn off the Enhanced Local Dialing feature.. ,

For more information on using the ENHDIALSTAT parameter, see B189 Conference Phones - Customizable System Parameters on page 54

Enhanced local dialing requirements

The enhanced local dialing feature is invoked when all the following conditions are met:

- A user invokes the Redial application, the Missed or Answered Call Log, or any Browser-based click-to-dial link to identify a telephone number to dial.
- The Phone application determines a call appearance is available for an outgoing call.
- The current value of ENHDIALSTAT is “1” (On).
- The call server has not indicated it supports smart enbloc dialing. Smart enbloc dialing is call type digit analysis available with Communication Manager Release 4.0 and later.

The Phone application takes the incoming character string, applies an algorithm, and determines the string of digits to be sent to automated call processing (ACP) for dialing. At this point the Phone application goes off-hook and sends the digits to ACP.

Note:

The Enhanced Local Dialing algorithm requires that telephone numbers be presented in a standard format.

Avaya B189 Conference IP phone supports enhanced local dialing only through a saved contact number.

Backup and restore processing

Avaya B189 Conference IP phones support the HTTP client to back up and restore the user-specific data indicated in User data saved during backup. HTTP over TLS (HTTPS) is also supported for backup or restore. For backup, the phone creates a file with all user-specific data if a backup file location is specified in system parameter BRURI. The file is sent to the server by an HTTP PUT message, with the appropriate success or failure confirmation. Only one backup or restore attempt is made for each request. Retries are the responsibility of the initiating process.

The phone stores the authentication credentials and the realm in non-volatile memory that is not overwritten if new phone software is downloaded. The default value of the credentials and the realm is set to null at manufacture and at any other time that user-specific data is removed from the deskphone.

For restore, the initiating process must supply only the backup file name. The file is requested from the server by an HTTP GET message. If successful, the file is returned to the initiating process. Otherwise a failure message is returned.

Backup and restore operations construct the URI used in the HTTP message from the value of the BRURI parameter and from the file name as follows:

- If BRURI ends with a / (a forward slash), the file name is appended.
- Otherwise, a forward slash and the file name is appended to the BRURI value.

Note:

BRURI can include a directory path and or a port number as specified in IETF RFCs 2396 and 3986.

For backup, the initiating process must supply the backup file and the file name, and the file is sent to the server through an HTTP PUT message. A success or failure indication is returned to the initiating process based on whether or not the file is successfully transferred to the server.

For restore, the initiating process must only supply the file name, and the file is requested from the server through an HTTP GET message. The file is returned to the initiating process if it is successfully obtained from the server, otherwise a failure indication is returned.

For deletion, the initiating process must only supply the file name. The server requests deletion of the file through an HTTP DELETE message. The initiating process receives a success indication, if a 2xx HTTP status code is received, otherwise a failure indication is returned.

If you use TLS, the call server registration password for the phone must be included in an Authorization request-header in each transmitted GET and PUT method. This method is intended for use by the Avaya IP Telephone File Server Application so that the phone

requesting the file transaction can be authenticated. You can downloaded the Avaya IP Telephone File Server Application from the Avaya support site.

If no digital certificates are downloaded based on the system parameter TRUSTCERTS, the phone establishes a TLS connection only to a backup and restore file server that has a Avaya-signed certificate. The Avaya certificate is included by default with the Avaya IP Telephone File Server Application, and includes the credentials. However, if at least one digital certificate has been downloaded based on TRUSTCERTS, the credentials are included only if BRAUTH is set to 1. This method is a security feature to allow control over whether the credentials are sent to servers with third-party certificates. If the server on which the Avaya IP Telephone File Server Application is installed uses a non-Avaya certificate, set BRAUTH to 1 to enable authentication of the deskphones. The default value of BRAUTH is 0.

When the call server IP address and the registration password of the phone are included as the credentials in an Authorization request-header, the call server IP address is included first in dotted-decimal format, followed by a colon, hex 3A, followed by the registration password of the phone.

Both backup and restore operations support HTTP/HTTPS authentication. The authentication credentials and realm are stored in re-programmable, non-volatile memory, which is not overwritten when new phone software is downloaded. Both the authentication credentials and realm have a default value of null, set at manufacture or at any other time user-specific data is removed from the phone. When TLS is used, the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is used for authentication. If the digital certificate of the server is signed by the Avaya Product Root Certificate Authority certificate, the call server registration password of the phone is included as the credentials in an Authorization request-header for each transmitted PUT (backup) and GET (for restore) method.

If the authority component of BRURI contains a DNS name, and if a TCP connection cannot be established to the IP address that was previously used to attempt to establish a connection with the server, the deskphone again attempts to resolve the DNS name. If a new IP address is received, the deskphone attempts to establish a connection to that address. If the deskphone receives the same IP address from the DNS server used previously, or if a TCP connection cannot be established with the new IP address, a failure indication is returned to the initiating process.

With TLS, the phone uses a TLS_RSA_WITH_AES_128_CBC_SHA cipher suite. If TLS is used but no digital certificates are downloaded based on the TRUSTCERTS value, the IP address of the call server with which the phone is registered and the registration password of the phone will be included as the credentials in an Authorization request-header in each transmitted GET and PUT method. If at least one digital certificate has been downloaded based on TRUSTCERTS, the IP address of the call server with which the phone is registered. The registration password of the phone is included in the credentials in an Authorization request-header in each transmitted GET and PUT method only if the value of BRAUTH is 1.

When the call server IP address and the registration password of the phone are included as the credentials in an Authorization request-header, the call server IP address is included first in dotted-decimal format, followed by a colon (hex 3A), followed by the registration password of the phone. The server gets the extension number of the phone from the backup or restore

file name. The server must also protect the user's credentials once they are received through the secure TLS connection.

The phone sends the registration credentials without regard to the BRAUTH setting if no certificates are downloaded. Only server certificates signed by an Avaya Root CA certificate are authenticated if no certificates are downloaded.

If an HTTP backup or restore operation requires authentication and the realm in the challenge matches the stored realm, the phone uses the stored credentials to respond to the challenge without prompting the user. However, if the stored credentials are null, or if the realms do not match, or if an authentication attempt using the stored credentials fails, the Status Line of the B189 Conference IP Phones display an HTTP Authentication or an HTTP Authentication Failure interrupt screen:`Enter backup/restore credentials`.

New values replace the stored authentication and realm values:

- When HTTP authentication for backup or restore succeeds and
- If the userid, password, or realm used differs from those values that are stored in the phone

If HTTP authentication fails, the user is prompted to enter new credentials.

Note:

Users can request a backup or restore using the Advanced Options Backup/Restore screen, as described in the user guide.

For specific error messages relating to Backup/Restore, see *Implementing Avaya B189 Conference IP Phones.*

Backup file formats

When the system parameter BRURI is non-null, user changes are automatically backed up to the file *ext*_96xxdata.txt (where *ext* is the extension number of the deskphone) on the HTTP server to a user-specified folder. The backup formats are as follows:

Table 11: Backup File Formats

Item/Data Value	Format
Generic	*name=value*
Contacts	ABKNAME*mmm*=ENTRY_NAME ABKNUMBER*mmm*=ENTRY_NUMBER_1 ABKTYPE*mmm*=ENTRYT_TYPE (where *mmm* is the one-, two-, or three-digit entry ID, with leading zeros for single and double-digit entry IDs)

About restore

When automatic or user-requested retrieval of backup data is initiated, user data and option settings are set to values contained in the backup file. The user-requested retrieval of backup data occurs only if the OPSTAT parameter setting allows the user to change those values. Therefore, any restrictions set using OPSTAT are given priority and implemented.

The backup file value is not retrieved, and the current setting remains valid:

- When a value in the backup file has changed and
- That value corresponds to an application that OPSTAT indicates should not be changed.

This method prevents a user from bypassing the administration of OPSTAT and changing options settings in the backup file.

Note:

If you administered the APPSTAT parameter to suppress changes to one or more applications, the phone backs up and restores data as usual, but ignores data for “suppressed” applications. This method prevents a user from bypassing your APPSTAT restrictions by editing the backup file. For information about APPSTAT, see Setting the Application Status flag (APPSTAT).

During backup file restoration, do not perform any user activity until the phone displays a `Retrieval successful` or `Retrieval Failed .`

Important considerations during data retrieval are as follows:

- When you create a backup file instead of editing an existing one, ensure to create the file with UTF-16 LE (little endian) characters, with Byte Order Mark (BOM) for LE of 0xFFFE.
- Backup saves data values using the generic format *name*=*value*. For specific formats, see Backup file formats on page 76.
- All identifiers, for example, *names*, are interpreted in a case-insensitive manner, except parameter values, Contact names, and numbers.
- Spaces preceding, within, or following a *name* are treated as part of the *name*.
- <CR> and <LF> (UTF-16 characters 0x000D and 0x000A, respectively) are interpreted as line termination characters.
- Blank lines are ignored.
- When an identifier is not recognized or is invalid, the entire line is ignored. Similarly, if an identifier is valid but the data itself is invalid or incomplete, the line is ignored.

- When an identifier is valid with valid and complete data, but the data is not applicable to the current state of the phone, the data is retained for possible use later, and is treated as data to be backed up at the appropriate time.
- When more than one line contains a value for an option, parameter, or Contacts entry, the last value read is retrieved, to allow new values to overwrite previous values as lines are read from the backup file. In all other cases, the line order in the backup file has no bearing on retrieval.
- The existence of invalid data does not constitute a failed retrieval. The success of the retrieval process requires the phone to get the backup file and successfully restore valid data.

Chapter 9: Administering Applications and Options

Administering guest users

About this task

A guest user is a person who logs into a Avaya B189 Conference IP Phone other than the primary phone at the home location of the user.

The guest user can log in to a phone that is across the country from the home location or one in the office near the home office. You administer permission for guest login by setting the system parameter GUESTLOGINSTAT to 1 (permitted), that displays the Guest Login option on the Main Menu.

Other related parameters you can administer are GUESTDURATION and GUESTWARNING. For more information on the parameters, see B189 Conference Phones - Customizable System Parameters on page 54.

Idle timer configuration

When the idle timer in the phone expires, you can administer the phone to turn the backlight to the lowest power level. You can put up a screen saver or set the backlight to low power mode when idle.

The related system parameters and their default values are:

System parameter	Default value
BAKLIGHTOFF	120 minutes
SCREENSAVERON	240 minutes

Glossary

802.1X
An authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access.

CA
Certificate Authority, the entity which issues digital certificates for use by other parties.

CLAN
Control LAN, a type of Gatekeeper circuit pack.

CNA
Converged Network Analyzer, an Avaya product to test and analyze network performance. Applies to IPv4 only.

This feature is not supported in Release 6.2 and later.

Digital Certificate
The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by a trusted third party known as a “Certificate Authority” (CA) such as VeriSign (www.verisign.com). The CA verifies that a public key belongs to a specific company or individual (the “Subject”), and the validation process the public key goes through to determine if the claim of the subject is correct and depends on the level of certification and the CA.

DHCP
Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.

Digital Signature
A digital signature is an encrypted digest of the file being signed. The file can be a message, a document, or a driver program. The digest is computed from the contents of the file by a one-way hash function such as MD5 or SHA-1 and then encrypted with the private part of a public or private key pair. To prove that the file was not tampered with, the recipient uses the public key to decrypt the signature back into the original digest, recomputes a new digest from the transmitted file and compares the two to see if they match. If they do, the file has not been altered in transit by an attacker.

DNS
Domain Name System, an IETF standard for ASCII strings to represent IP addresses. The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses.

EAP-TLS
Extensible Authentication Protocol, or EAP, is an authentication framework frequently used in wireless networks and Point-to-Point connections. EAP is defined in RFC 3748. EAP-Transport Layer Security (EAP-TLS), defined in RFC 5216, is an IETF open standard protocol,

	with strong security used by wireless vendors. EAP-TLS uses PKI to secure communication to a RADIUS authentication server or another type of authentication server.
H.323	A TCP/IP-based protocol for VoIP signaling.
HAC	Hearing Aid Compatibility, an Federal Communications Commission (FCC), part of the United States government Part 68 standard for handset equalization for interoperability with t-coil enabled hearing aid devices.
IKE	Internet Key Exchange Protocol, RFC 2409, which is now replaced by IKEv2 in RFC 4306.
IPsec	A security mechanism for IP that provides encryption, integrity assurance, and authentication of data. Applies only to IPv4.
LLDP	Link Layer Discovery Protocol. All deskphones with an Ethernet interface support the transmission and reception of LLDP frames on the Ethernet line interface in accordance with IEEE standard 802.1AB.
NAT	Network Address Translation, a mechanism by which IP addresses are mapped from one address space to another, and in which UDP and TCP port numbers are remapped to allow multiple devices to share the same IP address without port number conflicts.
MAC	Media Access Control, ID of an endpoint.
PSTN	Public Switched Telephone Network, the network used for traditional telephony.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks.
RSA	Rivest-Shamir-Adleman: A highly secure asymmetric cryptography method developed by RSA Security, Inc. that uses a public and private key pair. The private key is kept secret by the owner and the public key is published, usually in a digital certificate. Data is encrypted using the public key of the recipient, which can only be decrypted by the private key of the recipient. RSA is very computation intensive, thus it is often used to encrypt a symmetric session key that is then used by a less computationally-intensive algorithm to encrypt protocol data during a “session”. You can also use RSA for authentication by creating a digital signature, for which the private key of the sender is used for encryption, and the public key of the sender' is used for decryption.
RTCP	RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service.

SCEP	Simple Certificate Enrollment Protocol, used to obtain a unique digital certificate.
SIP	Session Initiation Protocol. An alternative to H.323 for VoIP signaling.
SNTP	Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP telephones.
WML	Wireless Markup Language, used by the IP phones Web Browser to communicate with WML servers.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.
VPN	Virtual Private Network, a private network constructed across a public network such as the Internet. A VPN can be made secure, even though the network uses using existing Internet connections to carry data communication. Security measures involve encrypting data before sending data across the Internet and decrypting the data at the other end. To add an additional level of security, you can encrypt the originating and receiving network address.

Index

L

N

O

P

Q

R

S

T

U

V

W