Implementing and Administering the Avaya A175 Desktop Video Device with the Avaya Flare™ Experience
Release 1.0

16-603739
Issue 2
March 2012

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this 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.

For the most current versions of documentation, go to the Avaya support Web site http://www.avaya.com/support and search for "one-X Deskphone SIP".

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for 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 of the time and we have no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

License

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

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

License Types:

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

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" below for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and product(s) 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 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. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

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

T9 Text Input and other products are covered by one or more of the following patents: U.S. Pat. Nos. 5,187,480,5,818,437, 5,945,928, 5,953,541, 6,011,554, 6,286,064, 6,307,548, 6,307,549, and 6,636,162,6,646,573, 6,970,599; Australia Pat. Nos. 727539, 746674, 747901; Austria Pat. Nos. AT225534, AT221222; Brazil P.I. No. 9609807-4; Canada Pat. Nos. 1,331,057, 2,227,904,2,278,549, 2,302,595; Japan Pat. Nos. 3532780, 3492981; United Kingdom Pat. No. 2238414B; Hong Kong Standard Pat. No. HK1010924; Republic of Singapore Pat. Nos. 51383, 66959, 71979; European Pat. Nos. 1 010 057 (98903671.0), 1 018 069 (98950708.2); Republic of Korea Pat. Nos. KR201211B1, KR226206B1, 402252; People's Republic of China Pat. No. ZL96196739.0; Mexico Pat. Nos. 208141, 216023, 218409; Russian Federation Pat. Nos. 2206118, 2214620, 2221268; additional patent applications are pending.

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 telecommunication services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call the 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 Web site: http://www.avaya.com/support. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

FCC/Industry Canada Radiation Exposure Statement

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

Warning

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

Contents

Chapter 1: Introduction

About This Guide

This guide describes how to install, administer, and maintain the Avaya A175 Desktop Video Device with the Avaya Flare™ Experience. The Avaya A175 supports the Session Initiation Protocol (SIP). Both of the following must be installed to use the Avaya A175:

- Avaya Communication Manager Release 6.0 and greater, and
- Avaya Aura™ Session Manager (SM) Release 6.0 and greater.

Note:

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

This document does not cover installation or administration for Avaya Aura™ Session Manager. Find full documentation for Avaya Aura™ Session Manager on the Avaya support Web site, www.avaya.com/support, specifically *Installing and Upgrading Avaya Aura™ Session Manager* (Document Number 03-603473) and *Administering Avaya Aura™ Session Manager* (Document Number 03-603324).

For details about using the features provided by the Avaya A175, see the user documentation for the Avaya A175. All Avaya A175 documentation is also available on the Avaya support Web site http://www.avaya.com/support.

Intended Audience

This document is intended for personnel who install and administer the Avaya A175.

⚠ **CAUTION:**

Avaya does not provide product support for many of the products mentioned in this document. Take care to ensure that there is adequate technical support available for the servers involved, including, but not necessarily limited to, HTTP, HTTPS, and DHCP servers. If the servers are not functioning correctly, the Avaya A175 might not be able to operate correctly.

Document Organization

The guide contains the following sections:

Chapter 1: Introduction	Provides an overview of this guide.
Chapter 2: Avaya A175 Desktop Video Device Installation	Describes the equipment and resources required to properly install and operate the Avaya A175. Provides instructions on installing the Avaya A175 out of the box.
Chapter 3: Administration Overview and Requirements	Provides an overview of the administrative process and describes general hardware, software, and operational requirements.
Chapter 4: Network Requirements	Describes administrative requirements for your Local Area Network.
Chapter 5: Communication Manager Administration	Describes how to administer Avaya Communication Manager to operate with Avaya A175.
Chapter 6: Session Manager (SM) Administration	Covers Session Manager configuration for Avaya A175.
Chapter 7: Server Administration	Describes DHCP and HTTP/HTTPS administration for the Avaya A175.
Chapter 8: Local Administrative Options	Describes how to set local administrative options, if requested by the system or LAN administrator.
Chapter 9: Avaya A175 Desktop Video Device Software and Files	Describes Avaya A175 software, covers software downloads, and provides information about the configuration file.
Chapter 10: Administering Avaya A175 Desktop Video Device Options	Describes customizeable application-specific parameters, to provide administrative control of Avaya A175 functions and options.
Chapter 11: System Failover and Survivability	Provides detailed information about survivability, including configuration, parameter setup, and characteristics of each failover state.
Appendix A: Restart Scenarios	Explains the different scenarios possible for the sequence of the restart process.
Appendix B: Glossary of Terms	Provides a glossary of terms used in this document or which can be applicable to the Avaya A175.
Appendix A: Restart Scenarios	Explains the different scenarios possible for the sequence of the restart process.
Appendix B: Glossary of Terms	Provides a glossary of terms used in this document or which are generally applicable to the Avaya A175.

Online Documentation

See the Avaya support site at http://www.avaya.com/support for Avaya A175 technical and end user documentation.

Web sites that list related, non-Avaya documents, such as those published by the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU) are provided in the sections that follow.

IETF Documents

IETF documents provide standards relevant to IP Telephony and are available for free from the IETF Web site: http://www.ietf.org/rfc.html.

ITU Documents

Access the ITU Web site for more information about ITU guidelines and documents, available for a fee from the ITU Web site: http://www.itu.int.

ISO/IEC, ANSI/IEEE Documents

Access the ISO/IEC standards Web site for more information about IP Telephony standards, guidelines, and published documents: http://www.iec.ch.

.

Customer Support

For Avaya A175 support, call the Avaya support number provided to you by your Avaya representative or Avaya reseller.

Information about Avaya products can be obtained at the following URL:

http://www.avaya.com/support

Chapter 2: Avaya A175 Desktop Video Device Installation

Introduction

The Avaya A175 Desktop Video Device uses Internet Protocol (IP) technology with Ethernet interfaces.

The Avaya A175 supports DHCP and HTTP/HTTPS over IPv4/UDP which enhance the administration and servicing of the device. This device uses DHCP to obtain dynamic IP Addresses and HTTP or HTTPS to download new software versions and customized settings.

The Avaya A175 provides the ability to have one IP connection on the desktop for both the Avaya A175 and a PC using an Ethernet switch.

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

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

Base and Handset

The Avaya A175 has an optional base and handset with cradle.

The base has an internal Ethernet switch that allows the Avaya A175 and a PC to share the same LAN connection, if appropriate. Thus, the base station for the Avaya A175 does not need, or work with, the 30A switched hub interface.

Software

A factory-shipped Avaya A175 will not contain the most up-to-date software for registration. When the Avaya A175 is first connected to your network, a software download from an HTTP server might be initiated. The software download gives the Avaya A175 upgraded functionality.

Pre-Installation Checklist

Before plugging in the Avaya A175, verify that all the following requirements are met. Failure to do so prevents the Avaya A175 from working properly and can have a negative impact on the network. Print copies of this checklist for each server and Avaya A175.

Verify These Network Requirements

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

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

- Avaya Communication Manager (CM) Release 6.0 or greater.
- Avaya Aura™ Session Manager, Release 6.0 or greater.
- NTP Time Server.

See Pre-Installation Checklist for information on allowable configurations before proceeding.

⚠ **Important:**

The above must be configured properly to support SIP. The CM Outboard Proxy SIP (OPS) Station Form must be completed to enable SIP prior to plugging in the Avaya A175. For information, see *SIP Support in Avaya Communication Manager Running on Avaya S8XXX Servers* (Document Number 555-245-206).

□ **3.** The following circuit packs are installed on the switch:

- TN2602 IP Media Processor circuit pack. Sites with a TN2302 IP Media Processor circuit pack are strongly encouraged to install a TN2602 circuit pack to benefit from increased capacity.
- TN799B, C, or D Control-LAN (C-LAN) circuit pack.

⚠ **Important:**

Avaya A175 firmware requires TN799C V3 or greater C-LAN circuit pack(s). For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya support Web site http://www.avaya.com/support.

Later versions of the Communication Manager S87XX or 85XX can use Processor Ethernet in place of the C-LAN. The media processor resources are embedded on the gateway. See the gateway documentation for media processor capacity.

□ **4.** The Communication Manager (CM) call server is configured correctly, as described in this guide and Avaya Communication Manager documentation. Both documents are available at http://www.avaya.com/support.

□ **5.** The DHCP server and application are administered as described in this guide.

□ **6.** The HTTP server and application are administered as described in this guide.

□ **7.** The Avaya A175 upgrade script and application files from the Avaya Support Web site,
http://www.avaya.com/support, are loaded correctly on the HTTP/HTTPS server.

Verify These Network Requirements (continued)

❑ **8.** If applicable, the Voice Mail server is administered as described in this guide.

Notes:

- Any or all of the server applications mentioned in items 5-8 can be co-resident on the same hardware, subject to the specific restrictions of each individual application.
- See this guide for more information about:
  - administering other network equipment,
  - administering applications like firewalls, and
  - information about topics like port utilization.

Requirements to Verify for Each Avaya A175 Desktop Video Device

❑ **9.** You have an extension number and an Avaya Communication Manager security code (password) for each applicable Avaya A175.

❑ **10.** You have an OPTIM extension number and an Avaya Communication Manager security code (password) for each Avaya A175, and have configured Session Manager for each Avaya A175.

❑ **11.** A Category 5e LAN jack is available at each Avaya A175 site, if applicable.

❑ **13.** 1 Category 5e modular line cord is available for the connection between the Avaya A175 and the PC, if applicable.

❑ **14.** Verify that the Avaya A175 package includes the following components:

- 1 Avaya A175
- 1 Battery
- 1 AC power module and cord
- *Setting up the Avaya A175 Desktop Video Device.*

The optional Avaya A175 Base and Handset package includes the following components:

- 1 base which supports the Avaya A175.
- 1 handset cradle.
- 1 handset capable of transmitting and receiving 7KHz audio.
- 1 H4DU 9-foot long (when extended) 4-conductor coiled handset cord that plugs into the handset cradle and the handset.
- 1 modular cord that plugs into the base station and the handset cradle.
- *Setting up the Avaya A175 Desktop Video Device Base and Handset.*

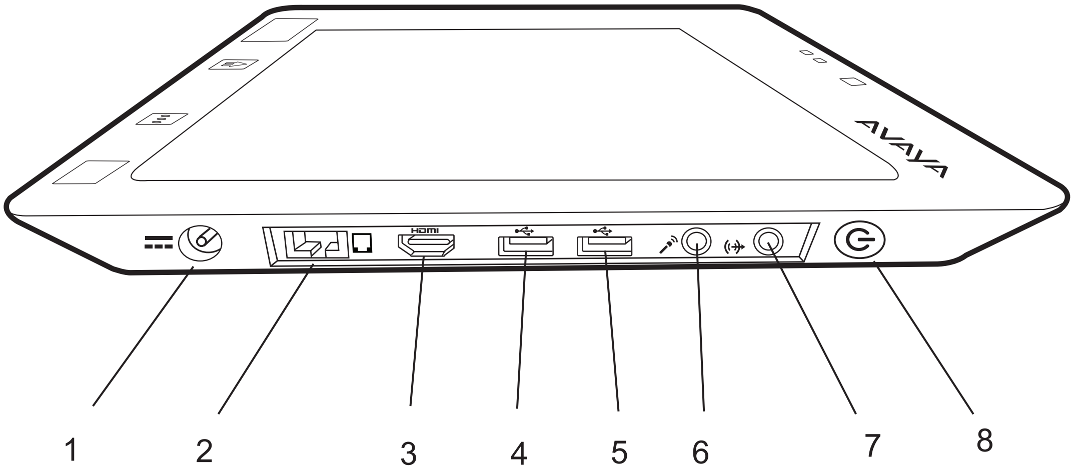
Note:

The Avaya A175 base supports wideband headsets with an HIS cord. Without the base, the Avaya A175 supports a PC-type headset with 3.5 mm plugs.

Assembling the Avaya A175

Figure 1 shows the ports on the Avaya A175.

Figure 1: Side view of the Avaya A175



Number	Name	Description
1	Power port	Enables you to connect the power supply to the Avaya A175.
2	Ethernet port	Enables you to connect the Avaya A175 to your LAN.
3	HDMI port	Not supported in Release 1.0.
4	USB port	Enables you to connect a USB device (for example, a keyboard or a mouse).
5	USB port	Enables you to connect a USB device (for example, a keyboard or a mouse).
6	Microphone port	Enables you to connect an external microphone.
7	Speaker port	Enables you to connect external speakers.
8	Power button	Turns the Avaya A175 on and off.

Note:

The Avaya A175 supports a PC-type headset with 3.5 mm plugs.

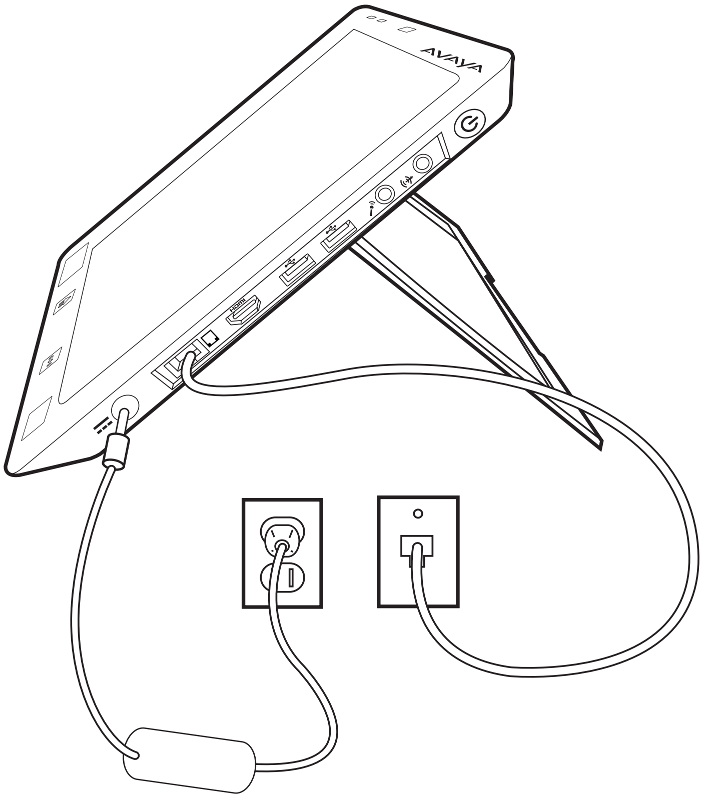
CAUTION:

Be careful to use the correct ports when plugging in the Avaya A175. The ports are located on the Avaya A175 and are flanked by icons to represent their correct use.

Installing the Avaya A175

Figure 2 shows the basic connections for the Avaya A175.

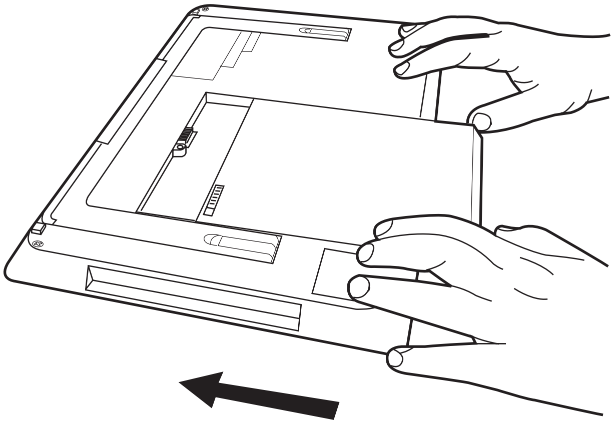
Figure 2: Basic connections for the Avaya A175



To assemble the Avaya A175:

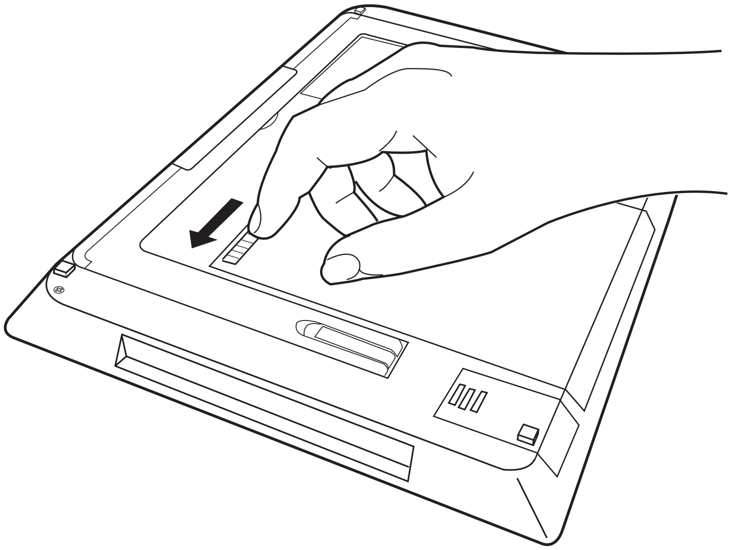
1. Insert the battery into the slot on the back of the Avaya 175 (Figure 3).

Figure 3: Insert battery



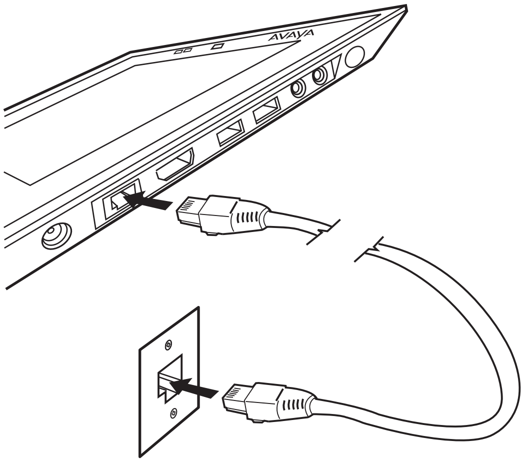
2. Slide the latch to secure the battery (Figure 4).

Figure 4: Slide battery latch



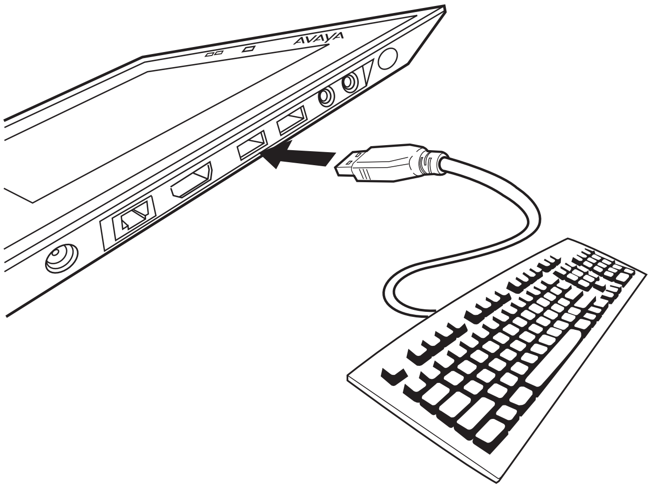
3. Plug one end of a Category 5e modular line cord into the Ethernet jack on the Avaya A175 (Figure 5).

Figure 5: Connect to the Ethernet



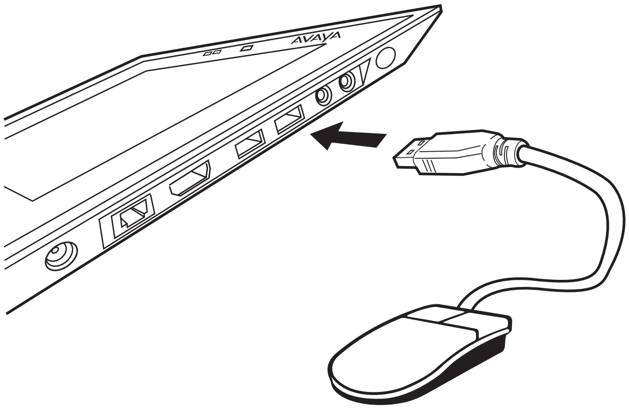
4. Plug the other end of the Category 5e modular line cord into the Ethernet wall jack (Figure 5).
5. Optional: Plug a USB keyboard into the USB port on the Avaya A175 (Figure 6).

Figure 6: Connect optional USB keyboard



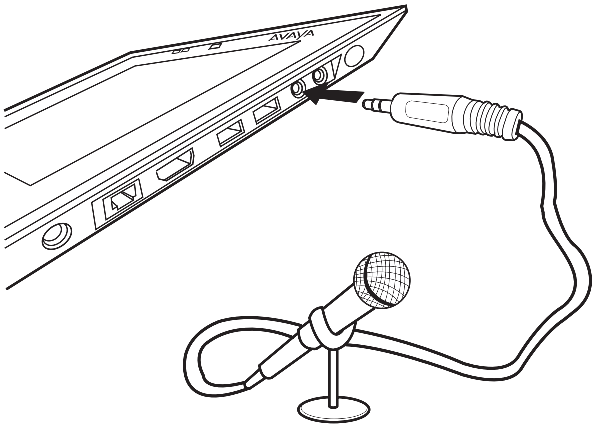
6. Optional: Plug a USB mouse into the USB port on the Avaya A175 (Figure 7).

Figure 7: Connect optional USB mouse



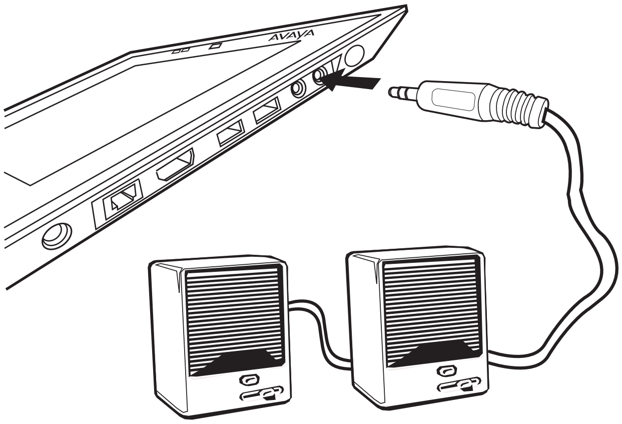
7. Optional: Plug an external microphone into the microphone jack on the Avaya A175 (Figure 8).

Figure 8: Connect optional microphone



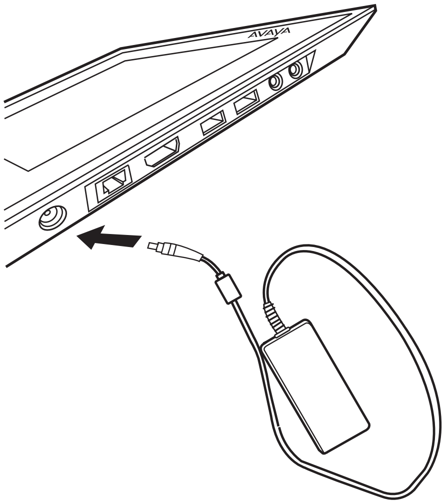
8. Optional: Plug external speakers into the speaker jack on the Avaya A175 (Figure 9).

Figure 9: Connect optional external speakers



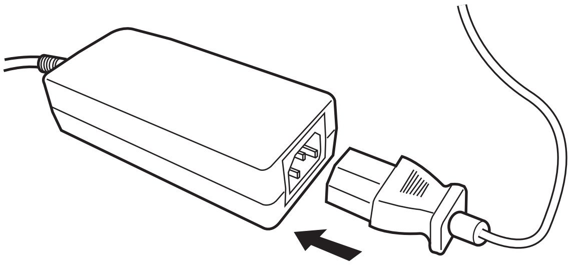
9. Plug the power supply into the power jack on the Avaya A175 (Figure 10).

Figure 10: Connect power supply



10. Plug the power cord into the power supply (Figure 11).

Figure 11: Connect power cord

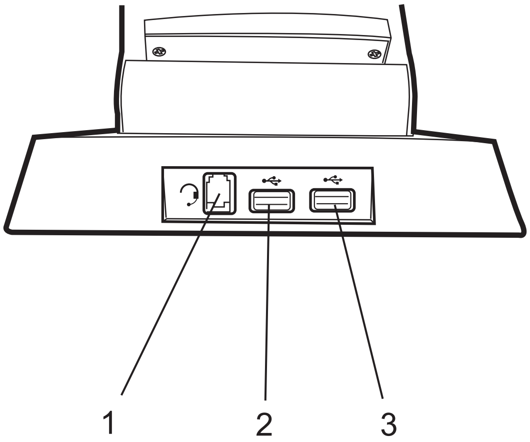


11. Plug the other end of the power cord into an AC power source.

Installing the Avaya A175 with the Base and Handset

Figure 12 shows the ports on the front of the optional base for the Avaya A175.

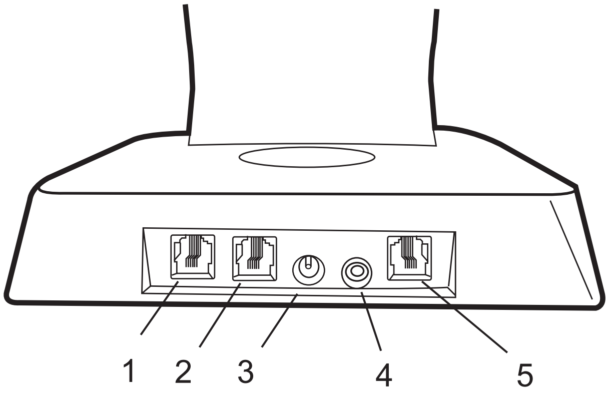
Figure 12: Front view of the base



Number	Name	Description
1	Headset port	Enables you to connect a wideband headset with an HIS cord to the Avaya A175.
2	USB port	Enables you to connect a USB device (for example, a keyboard or a mouse).
3	USB port	Enables you to connect a USB device (for example, a keyboard or a mouse).

Figure 13 shows the ports on the back of the optional base for the Avaya A175.

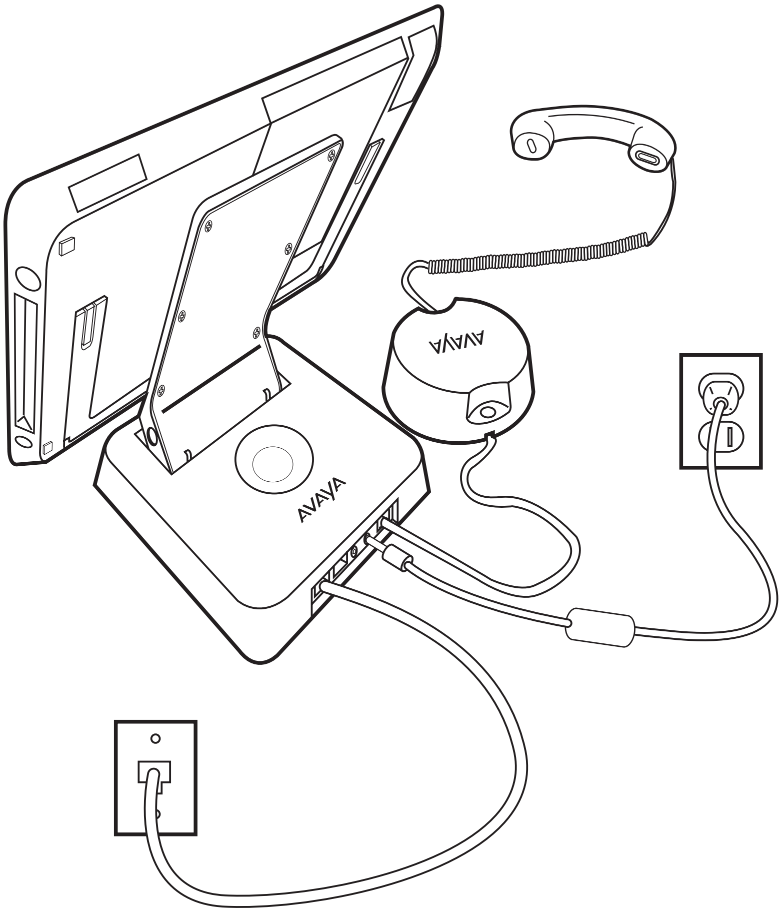
Figure 13: Front view of the base



Number	Name	Description
1	Ethernet port	Enables you to connect the Avaya A175 to your LAN.
2	Auxiliary Ethernet port	Enables an auxiliary device (such as a PC) to share the Ethernet connection to your LAN.
3	Power port	Enables you to connect the power supply to the Avaya A175.
4	Speaker port	Enables you to connect external speakers.
5	Handset cradle port	Enables you to connect the optional handset cradle. (The handset connects to the cradle.)

Figure 14 shows the connections for the Avaya A175 with the base and handset.

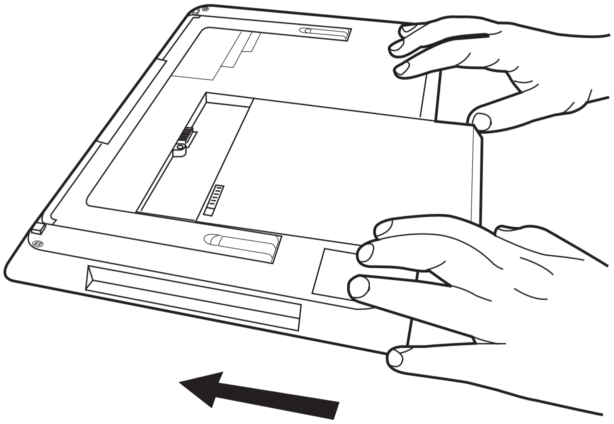
Figure 14: Connections for the Avaya A175 with the Base and Handset



To install the A175 with the base and handset:

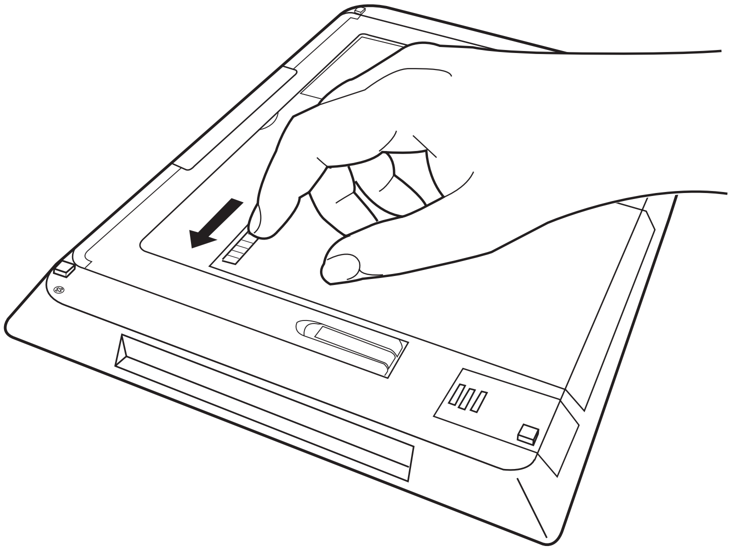
1. Insert the battery into the slot on the back of the Avaya 175 (Figure 15).

Figure 15: Insert battery



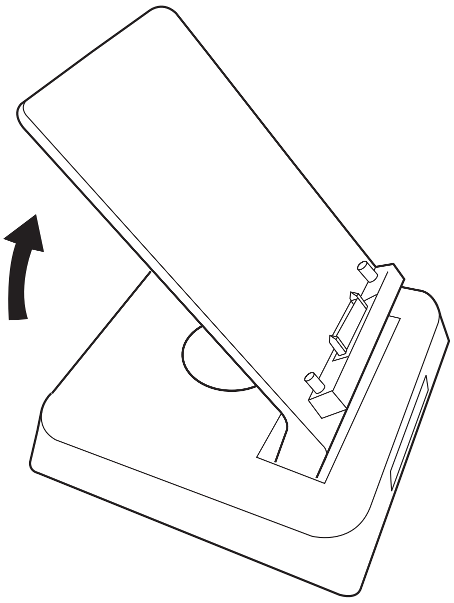
2. Slide the latch to secure the battery (Figure 16).

Figure 16: Slide battery latch



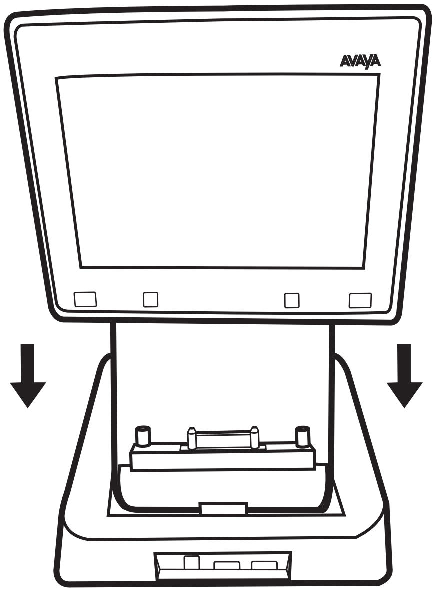
3. Raise the base stand (Figure 17).

Figure 17: Raise base stand



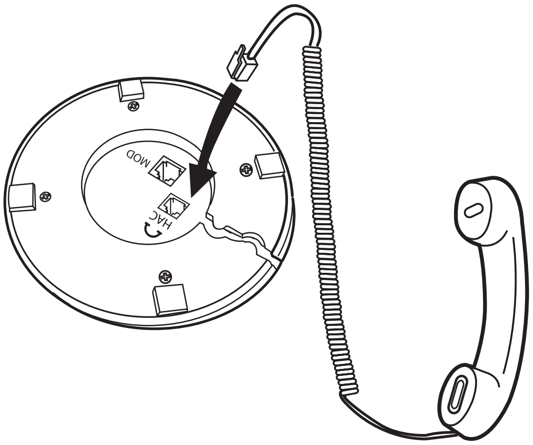
4. Insert the Avaya A175 onto the base (Figure 18).

Figure 18: Insert A175 onto base



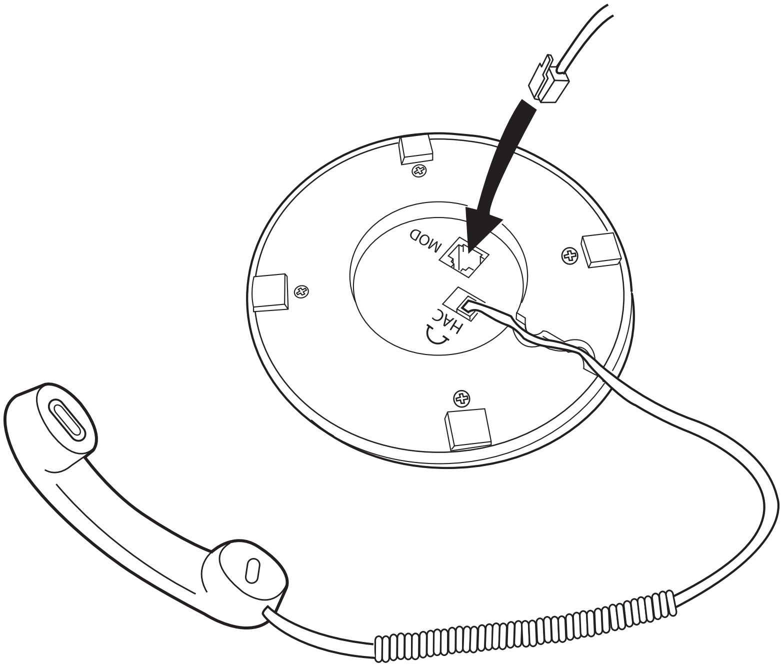
5. Plug the handset cord into the HAC jack on the bottom of the handset cradle (Figure 19).

Figure 19: Plug handset cord into handset cradle



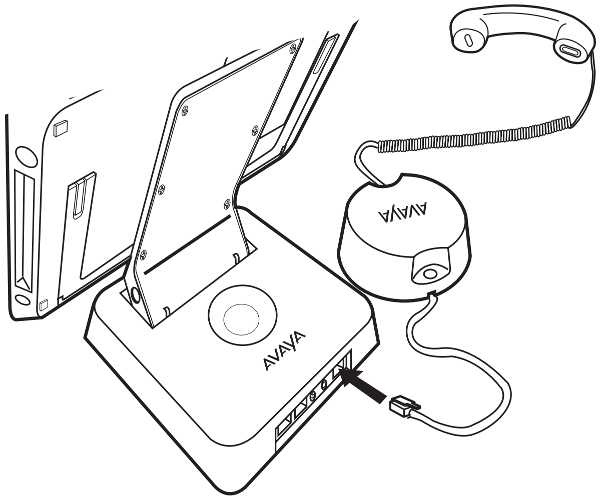
6. Plug one end of the modular cord into the MOD jack on the bottom of the handset cradle (Figure 20).

Figure 20: Plug modular cord into handset cradle



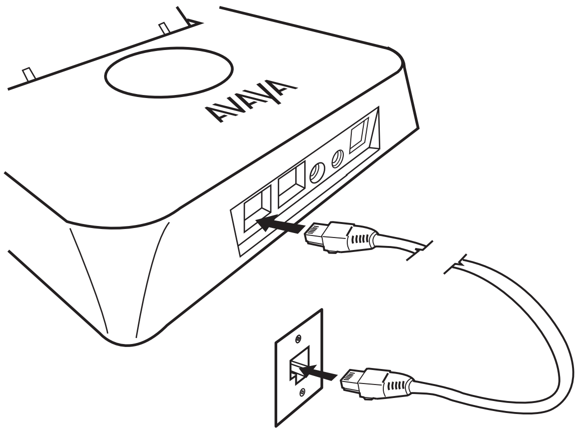
7. Plug the other end of the modular cord into the modular jack on the back of the base (Figure 21).

Figure 21: Connect handset cradle to base



8. Plug one end of a Category 5e modular line cord into the Ethernet jack on the back of the base (Figure 22).

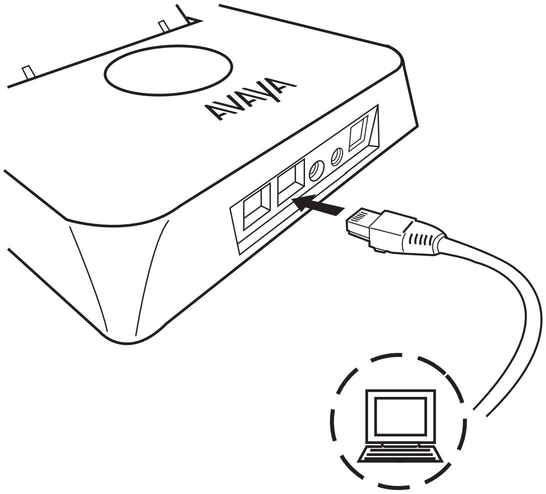
Figure 22: Connect to Ethernet



9. Plug the other end of the Category 5e modular line cord into the Ethernet wall jack (Figure 22).

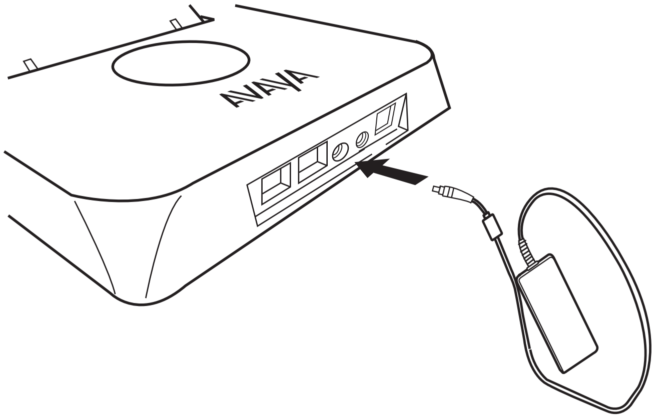
10. Optional: If you want to share your Ethernet connection with your PC, plug a Category 5e modular line cord from the PC in to the auxiliary PC jack on the back of the base (Figure 23).

Figure 23: Connect optional PC



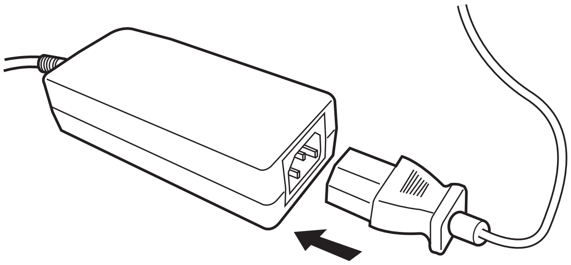
11. Plug the power supply into the power jack on the back of the base (Figure 24).

Figure 24: Connect power supply



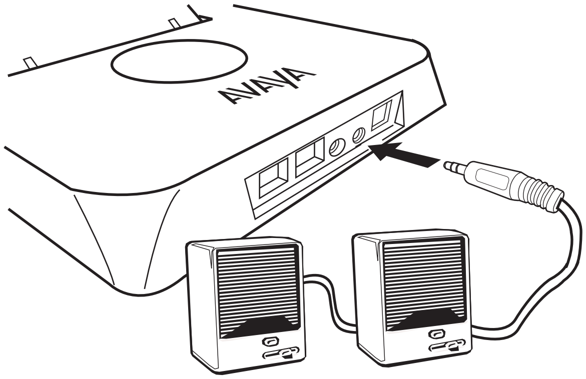
12. Plug the power cord into the power supply (Figure 25).

Figure 25: Connect power cord



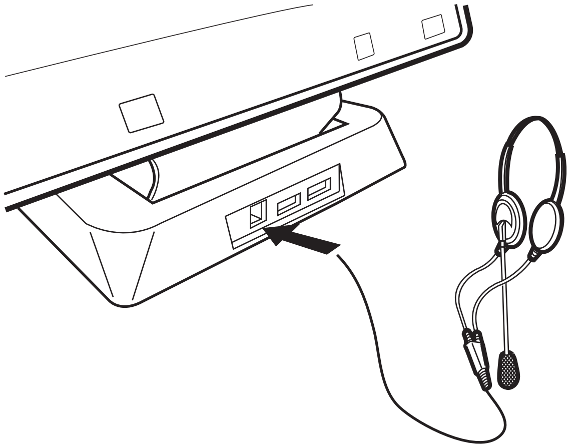
13. Optional: Plug external speakers into the speaker jack on the back of the base (Figure 26).

Figure 26: Connect optional external speakers



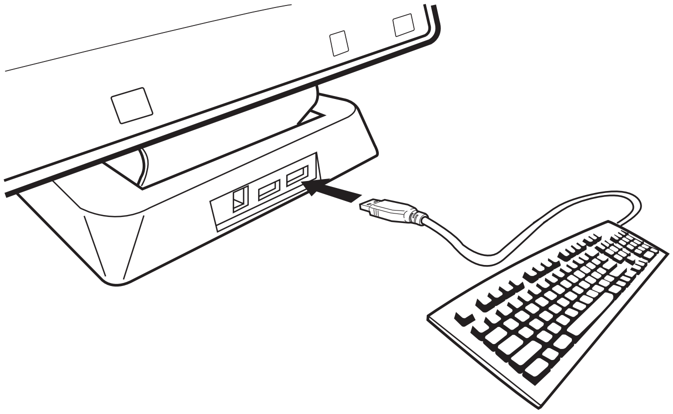
14. Optional: Plug a headset into the headset jack on the front of the base (Figure 27).

Figure 27: Connect headset



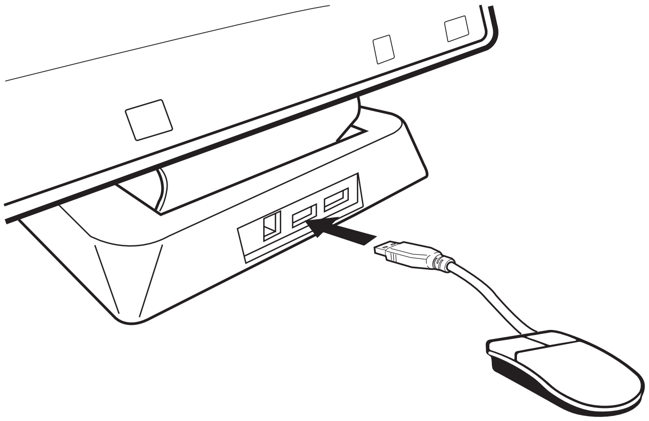
15. Optional: Plug a USB keyboard into the USB port on the front of the base (Figure 28).

Figure 28: Connect optional USB keyboard



16. Optional: Plug a USB mouse into the USB port on the front of the base (Figure 29).

Figure 29: Connect optional USB mouse



17. Plug the other end of the power cord into an AC power source.

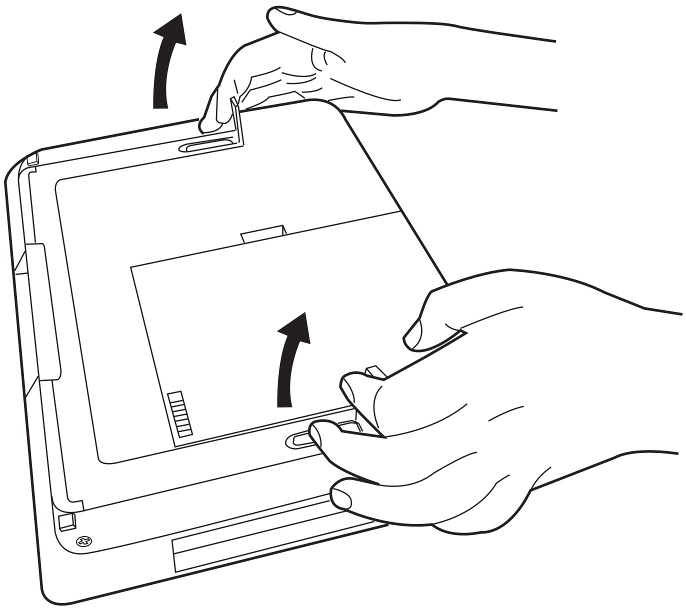
Using the Built-in Stands on the Avaya A175

The Avaya A175 provides two built-in stands on the back of the device. The small stand displays the Avaya A175 at a shallow angle on your desk. The large stand displays the Avaya A175 at sharp angle.

To set up the small built-in stand:

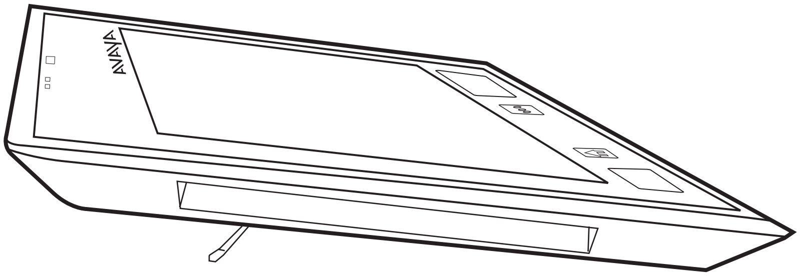
1. Place the Avaya A175 on a flat surface with its screen facing down.
2. Lift up the two small stand supports (Figure 30).

Figure 30: Lift small stand supports



3. Turn the Avaya A175 over, and place it on a flat surface (Figure 31).

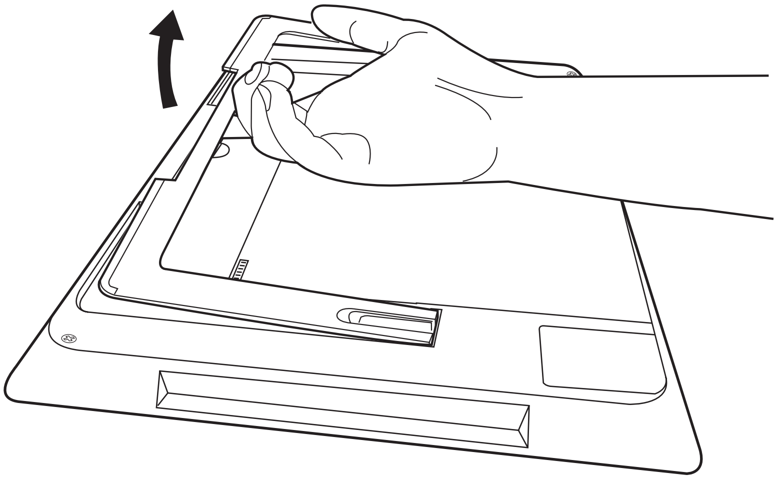
Figure 31: Avaya A175 with small stand



To set up the large built-in stand:

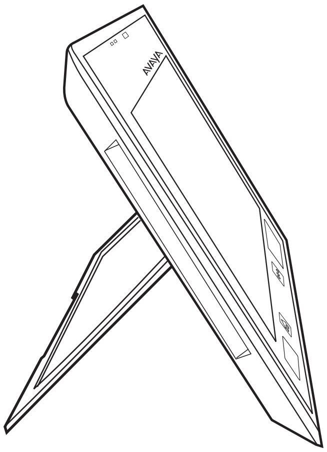
1. Place the Avaya A175 on a flat surface with its screen facing down.
2. Lift up the large stand support (Figure 32).

Figure 32: Lift large stand support



3. Turn the Avaya A175 over, and place it on a flat surface (Figure 33).

Figure 33: Avaya A175 with large stand

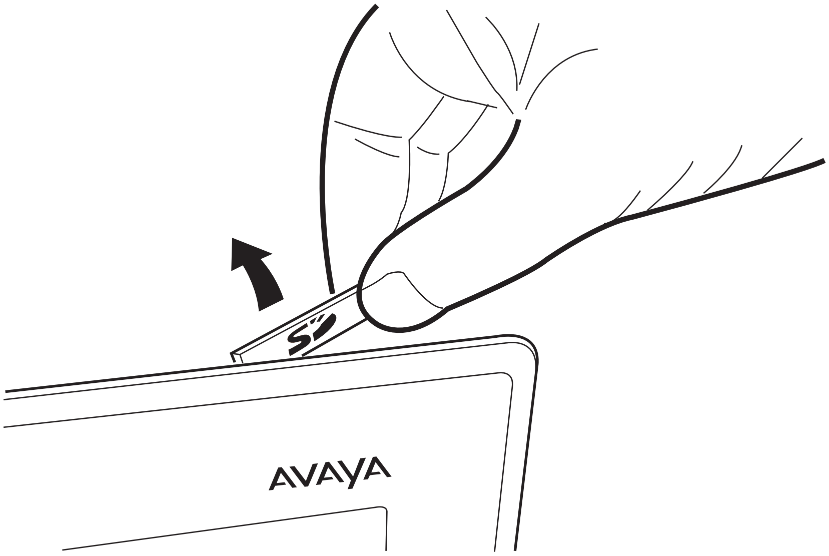


Installing an SD Card in the Avaya A175

To install an SD card:

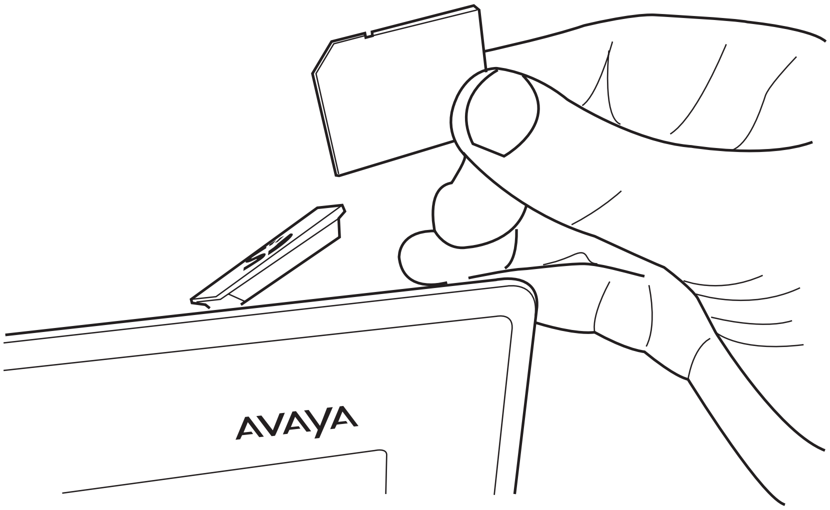
1. Lift up the rubber cover of the SD port along the top of the Avaya A175 (Figure 34).

Figure 34: Lift cover of SD port



2. Insert the SD card into the port, and push it down into place (Figure 35).

Figure 35: Insert SD card



3. Place the rubber cover over the port.

Dynamic Addressing Process/Device Startup

⚠ **Important:**

Before starting this process, ensure that both Avaya Communication Manager (CM) and Session Manager (SM) are properly set up for your environment.

Note:

Before starting this process you must have an OPTIM extension number for the Avaya A175, the Avaya Communication Manager security code (password), and a login and password on the SM server.

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

The following description of the process of installing the Avaya A175 assumes that the process is executed successfully. For errors that might be encountered during the process and the messages displayed, see Chapter 12: Troubleshooting Guidelines.

When you plug the Avaya A175 into the Ethernet wall jack and turn on the device, if applicable, the following process takes place.

Note:

Do not turn off the Avaya A175 during the download process.

1. The Avaya A175 activates the Ethernet line interface or WiFi interface to allow the invocation of procedures. The activation occurs as soon as possible after power-up or a reset.
2. During hardware initialization, configuration parameters are set to default values. The system initialization values for contrast and brightness are checked for non-null values, and set accordingly. The Avaya name is displayed.
3. The Avaya A175 sends a request to the DHCP server and invokes the DHCP process.
4. The DHCP server provides IP Addresses for the following hardware:
   - The Avaya A175
   - The HTTP/HTTPS server
   - The SIP Proxy server
5. Using the list of IP Addresses provided by the DHCP server, the Avaya A175 performs a router check and verifies that the router is on the same subnet as the IP Address. The Avaya A175 cycles through the gateway IP Addresses with ARPs or pings until it receives a response.
6. The HTTP process starts with an `HTTP GET` command.
7. When connected, the Avaya A175 looks for the upgrade script file (Axxxupgrade.txt).

8. The HTTP server sends and identifies an upgrade script, gets the settings file (Axxxsettings.txt), and any firmware updates. (Firmware updates are installed in the background.)

   ⚠ **Important:**

   Do not turn off the Avaya A175 during the download process

   The GET message might have to be sent several times. Each time the GET message is sent, the URI for the current HTTP request displays.

Registration and Login

1. Upon successful initialization and power-up, the Avaya A175 displays the following message in the Top bar of the screen:

   Not logged in
2. Touch the Availability area on the Top bar.
3. In the Extension box, enter extension assigned to this device.
4. In the Password box, enter the password, and touch the **Log in** button.

   The extension is visible during entry but the password displays as asterisks. The system determines whether the extension is in use.
5. The Avaya A175 initiates SIP registration with the proxy server. The Avaya A175 attempts to register to the SIP proxy server at the address in the SIP_CONTROLLER_LIST parameter using the extension and password provided during the login process. It also uses the SIPDOMAIN parameter. The Avaya A175 uses a SIP URI. SIP_CONTROLLER_LIST provides a list of server addresses. The Avaya A175 attempts to register to only the first server in the list. Also, the Avaya A175 does not reboot when there is no server provisioned or the provisioned server cannot be contacted. If the server address is a hostname or a fully-qualified domain name (FQDN), the Avaya A175 will do a DNS Any lookup of the server address before proceeding with the SIP registration. The Avaya A175 waits for a register response message. If no message is received before the end of the REGISTERWAIT interval, registration is retried.
6. The Avaya A175 contacts PPM, logs in, and downloads the configuration file.
7. When the Avaya A175 successfully logs into the server, the message “Login” appears in the Top bar.

Chapter 3: Administration Overview and Requirements

Overview

The Avaya A175 Desktop Video Device supports the SIP signaling protocol.

SIP was developed by the IETF. SIP provides for real time audio, video, and data communications transmission over a packet network. SIP uses various messages, or methods, to provide:

- Registration (REGISTER),
- Call signaling (INVITE, BYE)
- Control signaling (SUBSCRIBE, NOTIFY)

The Avaya A175 supports uses built-in Avaya SIP Certificates for trust management. Trust management involves downloading certificates for additional trusted Certificate Authorities (CA) and the policy management of those CAs. Identity management is handled by Simple Certificate Enrollment Protocol (SCEP) with device certificates and private keys.

Note:

SRTP is not supported in Release 1.0.

Post-installation, software upgrades automatically download to the Avaya A175 using the proper signaling protocol.

The conditions under which the Avaya A175 need to operate are summarized as follows:

- Station Administration on the Communication Manager (CM) call server, as covered in Chapter 5: Communication Manager Administration.
- Administration on Avaya Aura™ Session Manager (SM), as covered in *Administering Avaya Aura™ Session Manager* (Document Number 03-603324).
- IP Address management for the Avaya A175, as covered in Chapter 2: Avaya A175 Desktop Video Device Installation for dynamic addressing. For static addressing, see Static Addressing Installation on page 91.
- VLAN administration for the Avaya A175, if appropriate, as covered in Chapter 10: Administering Avaya A175 Desktop Video Device Options.
- Quality of Service (QoS) administration for the Avaya A175, if appropriate.
- Protocol administration, for example, Simple Network Management Control (SNMP).
- Interface administration for the device, as appropriate. Administer the Avaya A175 to LAN interface using the PHY1 parameter described in Chapter 4: Network Requirements.

Table 1 indicates that you can administer system configuration parameters in a variety of ways and use the following administrative mechanisms:

- Administering the information on the call server.
- Manually entering the information using the Settings menu in the Avaya A175 user interface.
- Administering the DHCP server.
- Editing the configuration file on the applicable HTTP or HTTPS file server.
- User modification of certain parameters, when given administrative permission to do so.

Note:

Not all parameters can be administered on all administrative mechanisms. See the applicable chapters in this guide for specific information.

Table 1: Administration Alternatives and Options for Avaya A175

Parameter(s)	Administrative Mechanisms	For More Information See:
Station Administration	Avaya Communication Manager and SM	Chapter 5: Communication Manager Administration, Chapter 7: Server Administration, and Appendix B: Glossary of Terms. For Session Manager administration, see *Administering Avaya Aura™ Session Manager* (Document Number 03-603324), available on the Avaya support site.
IP Addresses	DHCP (strongly recommended)	DHCP and File Servers on page 75, and especially DHCP Server Administration on page 76.
	Settings file	Chapter 9: Avaya A175 Desktop Video Device Software and Files and Chapter 10: Administering Avaya A175 Desktop Video Device Options.
	Manual administration at the Avaya A175	Static Addressing Installation on page 91.
VLAN	DHCP	DHCP Server Administration on page 76, and Chapter 10: Administering Avaya A175 Desktop Video Device Options.
	Settings file	DHCP and File Servers on page 75 and Chapter 10: Administering Avaya A175 Desktop Video Device Options.
	Manual administration at the Avaya A175	Static Addressing Installation on page 91.
Network Time Server (NTS)	DHCP Settings file	DHCP Server Administration on page 76 and Network Time Protocol (NTP) Server on page 52.

Table 1: Administration Alternatives and Options for Avaya A175 (continued)

Parameter(s)	Administrative Mechanisms	For More Information See:
Quality of Service	Settings file	Chapter 10: Administering Avaya A175 Desktop Video Device Options.
Interface	DHCP	DHCP and File Servers on page 75, and Chapter 9: Avaya A175 Desktop Video Device Software and Files.
	Settings file (strongly recommended)	DHCP and File Servers on page 75, and Chapter 9: Avaya A175 Desktop Video Device Software and Files.
	Manual administration at the Avaya A175	"Secondary Ethernet Interface Enable/Disable."
Application - specific parameters	DHCP	DHCP and File Servers on page 75, and especially DHCP Server Administration on page 76. Also, Chapter 10: Administering Avaya A175 Desktop Video Device Options.
	Settings file (strongly recommended)	DHCP and File Servers on page 75, and especially HTTP Generic Setup on page 88. Also, Chapter 10: Administering Avaya A175 Desktop Video Device Options.

General information about administering DHCP servers is covered in DHCP and File Servers on page 75, and more specifically, DHCP Server Administration on page 76. General information about administering HTTP servers is covered in DHCP and File Servers on page 75, and more specifically, HTTP Generic Setup. Once you are familiar with that material, you can administer Avaya A175 options as described in Chapter 10: Administering Avaya A175 Desktop Video Device Options.

Parameter Data Precedence

As shown in Table 1: Administration Alternatives and Options for Avaya A175, you can administer a given parameter in a number of ways. The precedence, from lowest to highest, is:

1. DHCP
2. Settings file (Axxxsettings.txt)

   ⚠ **Important:**
   Set flivver parameters in the settings file and not in SM.

3. Personal Profile Manager (PPM) through SM

4. Manual administration, unless the system parameter USE_DHCP is set to 1 (Get IP Address automatically by DHCP), or backup file data obtained through PPM.

For example, if the SIP outbound proxy server address is defined to have the precedence information so that the value retrieved from DHCP server has a lower precedence than the value retrieved from the settings file, and the value retrieved from the settings file is higher than the value retrieved from PPM, then the following determination occurs:

- If the most recent value the Avaya A175 has is from DHCP and new server address information is retrieved from the settings file, the Avaya A175 will use the new value from the settings file.
- If later on, the Avaya A175 receives a new server address value from PPM, it will not use this value because PPM's precedence as a data source for the server address is lower than the current value (which came from the settings file).
- If the server to which a specific Avaya A175 points is changed manually using the Craft (local administrative) procedure, that value now takes precedence over the previous value.

The Administrative Process

The following list depicts administration for a typical Avaya A175 network. Your own configuration might differ depending on the servers and system you have in place.

1. Avaya Communication Manager (6.0 or greater) administered for Avaya A175 devices. Administer Avaya A175 on CM as 96*40*SIP.
2. SM 6.0 administered.
3. LAN and applicable servers (file servers, Network Time server) administered to accept the Avaya A175.
4. Avaya A175 software downloaded from the Avaya support site.
5. Axxxsettings file updated with site-specific and SIP-specific information, as applicable.
6. Avaya A175 devices installed.
7. Individual Avaya A175 devices updated using Craft procedures, as applicable. For more information, see Chapter 8: Local Administrative Options on page 89
8. Survivability administration to set up the local SIP gateway and administer additional controllers in the settings file as applicable.

Administrative Checklist

Use the following checklist as a guide to system and LAN administrator responsibilities. This high-level list helps ensure that all system prerequisites and requirements are met prior to Avaya A175 installation and startup.

Note:

One person might function as both the system administrator and the LAN administrator in some environments.

Table 2: Administrative Checklist

Task	Description	For More Information See:
Network Requirements Assessment	Determine that network hardware is in place and can handle Avaya A175 system requirements.	Chapter 4: Network Requirements.
Administer Avaya Communication Manager	Verify that the call server has a valid license file and is administered for Voice over IP (VoIP).	Chapter 5: Communication Manager Administration.
	Verify the individual Avaya A175 devices are administered as desired on the CM station form(s).	Chapter 5: Communication Manager Administration.
Administer the Proxy Server	Administer for Avaya Aura Session Manager (SM).	*Administering Avaya Aura™ Session Manager* (Document Number 03-603324), available on the Avaya support Web site, http://www.avaya.com/support.
DHCP server installation	Install a DHCP application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
Administer DHCP application	Add Avaya A175 administration to the DHCP application.	DHCP Server Administration.
Administer Network Time Server	Set value(s) for Simple Network Time Protocol (SNTP)	Option 42 under HTTP Generic Setup.
HTTP/HTTPS server installation	Install an HTTP/HTTPS application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
A175 software tar file, Axxxupgrade.txt file, and Axxxsettings.txt file installation on HTTP/ HTTPS server	Download the files from the Avaya support site.	http://www.avaya.com/support Chapter 9: Avaya A175 Desktop Video Device Software and Files.

1 of 2

Table 2: Administrative Checklist (continued)

Task	Description	For More Information See:
Modify settings file as needed	Edit the settings file as necessary for your environment, using your own tools.	Chapter 9: Avaya A175 Desktop Video Device Software and Files.
Administer devices locally as applicable	As a Group:	The GROUP System Value on page 112.
	Individually:	The applicable Craft Local Procedures.
Installation of Avaya A175 devices in the network		Avaya A175 Desktop Video Device Installation on page 15.

2 of 2

Avaya A175 Initialization Process

These steps offer a high-level description of the information exchanged when the Avaya A175 initializes and registers. This description assumes that all equipment is properly administered ahead of time. This description can help you understand how the Avaya A175 devices relate to the routers and servers in your network.

Step 1: Avaya A175 to Network

The Avaya A175 is appropriately installed and powered. After a short initialization process, the Avaya A175 identifies the LAN speed and sends a message out into the network, identifying itself and requesting further information. A router on the network receives and relays this message to the appropriate DHCP server.

Note:

The Avaya A175 can connect to the LAN via an Ethernet interface or a WiFi interface. You can specify the type of connection from the Avaya A175 user interface.

Step 2: Avaya A175 to DHCP Server

The DHCP server provides information to the Avaya A175, as described in DHCP and File Servers on page 75. Among other data passed to the device is the IP Address of the HTTP or HTTPS server.

Step 4: Avaya A175 and File Server

The Avaya A175 can download upgrade files, software, certificates, and settings files from either an HTTP or HTTPS server. The Avaya A175 queries the file server, which transmits an upgrade file to the Avaya A175. At a minimum, this Axxxupgrade.txt file tells the Avaya A175 which software tar file the Avaya A175 must use.

The Avaya A175 uses the Axxxupgrade.txt file to determine if it has the proper software tar file. If the Avaya A175 determines it does not have the proper software file, the Avaya A175 requests a download from the file server. The file server then downloads the file and conducts some checks to ensure that the file was downloaded properly. When the download is complete, the Avaya A175 will prompt the user to restart the device.

If the Avaya A175 determines it already has the proper file, the Avaya A175 proceeds as described in the next paragraph.

The Avaya A175 checks and loads the software file, and then uses the Axxxupgrade.txt file to look for the Axxxsettings.txt file, if appropriate. The optional settings file can contain settings you have administered for any or all of the Avaya A175 devices in your network. For more information about this download process and settings file, see Chapter 9: Avaya A175 Desktop Video Device Software and Files.

Note:

Unlike the SIP telephones, the Avaya A175 polls the file server at regular intervals to determine if it has the proper software. The Avaya A175 will download the software in the background without affecting the user. When the download is complete, the Avaya A175 will prompt the user to restart the device.

Step 5: Avaya A175 and SIP Proxy Server

In this step, the Avaya A175 might prompt the user for an extension and password. The Avaya A175 uses that information to exchange a series of messages with SM, which in turn communicates with Avaya Communication Manager (CM). For a new installation and for full service, the user can enter the extension and the SM password. For a restart of an existing installation, this information is already stored on the Avaya A175. The Avaya A175 and SM and CM exchange more messaging. The expected result is that the Avaya A175 is appropriately registered.

For more information about the installation process, see the Installation chapter.

Error Conditions

Assuming proper administration, most of the problems reported by Avaya A175 users are likely to be LAN-based. Quality of Service, server administration, and other issues can impact user perception of Avaya A175 performance.

Troubleshooting Guidelinescovers possible operational problems that might be encountered after successful installation. The user guide also contains guidance for users having problems with specific Avaya A175 applications.

Chapter 4: Network Requirements

Network Assessment

Perform a network assessment to ensure that the network will have the capacity for the expected data, voice, and video traffic, and that it can support for all applications:

- SIP,
- DHCP, and
- HTTP/HTTPS.

Also, QoS support is required to run VoIP on your configuration. For more information, see Appendix B: Glossary of Terms and the QoS parameters L2QAUD, L2QSIG, DSCPAUD, DSCPSIG, L2QVID, and DSCPSIG in Table 14: Avaya A175 Customizeable System Parameters. (L2QVID and DSCPSIG supports 3 bit priority and DSCP of the video packets.)

Server Requirements

The following server types can be configured for the Avaya A175:

- DHCP server
- HTTP or HTTPS server
- SIP Proxy (controller) or Registration server
- Network Time Protocol server for SNTP
- SM SIP Proxy Server (controller) to be used as a gateway for survivability
- Microsoft Exchange server
- LDAP server
- Avaya Aura™ Presence server

Note:

Avaya A175 devices need Avaya Aura Session Manager (SM) to work properly. The SIP Proxy and Registration servers reside on the SM server. Avaya Communication Manager (CM) is considered a “feature server” behind SM that provides Outboard Proxy SIP (OPS) features.

While the servers listed provide different functions that relate to the Avaya A175 devices, they are not necessarily different boxes. For example, DHCP provides network information whereas

HTTP provides configuration and application file management, yet both functions can co-exist on one hardware unit. Any standards-based server is recommended.

For parameters related to Avaya Communication Manager information, see Chapter 5: Communication Manager Administration. For parameters related to DHCP and file servers, see Chapter 7: Server Administration.

⚠ **Important:**
The Avaya A175 devices obtain important information from the Axxxupgrade.txt file on the server(s) and depend on the file for software upgrades.

DHCP Server

Avaya recommends that a DHCP server and application be installed and that static addressing be avoided. Install the DHCP server and application as described in DHCP and File Servers on page 75.

HTTP/HTTPS Server

Administer the HTTP or HTTPS file server and application as described in HTTP Generic Setup on page 88.

Network Time Protocol (NTP) Server

Avaya A175 devices require NTP server support to set the time and date, used in system log time stamps and other time/date functions. The NTP server is typically needed by one or more servers within the enterprise. Administration of the NTP server is beyond the scope of this document.

Presence Server

The Avaya A175 supports the Avaya Aura Presence server when the following conditions exist:

- PRESENCE_SERVER contains the IP address of the Presence server.
- ENABLE_PRESENCE is set to 1.

The following standards and guidelines dictate how presence is handled:

- Using the following SIP/SIMPLE RFCs:
  - RFC 3863 *Presence Information Data Format*,

  - RFC 4479 *A Data Model for Presence*, and
  - RFC 4480 *RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)*.

- Using general Avaya enhancements for rich telephony presence, as follows:

```
<xsd:choice>
    <xsd:element name="unknown" />
    <xsd:element name="onhook" />
    <xsd:element name="do-not-disturb" />
    <xsd:element name="on-a-call" type="avp:Participants" />
    <xsd:element name="on-a-conference" type="avp:Participants" />
    <xsd:any namespace="##other" maxOccurs="unbounded"
        processContents="lax" />
</xsd:choice>
```

- Using the subscription to the SIP resource list event package, as follows:
  - RFC 4662 - A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists.
  - The identifier for the resource list for a user xxx@yyy.com is list-xxx@yyy.com.
  - The Avaya A175 supports non-hierarchical resource lists corresponding to UPM Contact Lists. When subscribing to list, the Avaya A175 will specify the SIP URI sip: + list- + user@domain.com, in other words the regular SIP URI with list- inserted before the username.
  - If the Avaya A175 has subscribed to the Presence.winfo and Resource.list events, it accepts the following presence information and passes it to the user interface for further processing: unknown, onhook, on-a-call, do-not-disturb, on-a-conference and Away.
- WINFO SUBSCRIBE is used to allow or block a presence subscription in response to a pending watcher. When the Avaya A175 receives a NOTIFY for watcher info with the watcher status of “pending” it PUBLISHes a (custom) presauth.winfo event package with the event “approved” for all the watchers.
- If the PRESENCE_SERVER parameter is set and contains an IP address, the Avaya A175 will replace the domain on the Request-URI header of any outbound presence-related messages with this IP address. The To header will remain intact in the form user@domain.tld.
- Support for configuration of a port number for the presence server. Using a port number allows the presence server to run multiple SIP servers on a single host to enable it to achieve its target scale of 20k users (and approximately 60k communication addresses, 10 presence changes and 10 messages per user per hour).

See Presence Notification for information on how the Avaya A175 handles presence messages.

Required Network Information

Before you administer DHCP and HTTP/HTTPS, as applicable, complete the information in Table 3. If you have more than one router, HTTP/TLS server and subnetwork mask in your configuration, complete Table 3 for each DHCP server.

The Avaya A175 devices support specifying a list of IP Addresses for a gateway/router and the HTTP/HTTPS server. 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 application, only 127 characters might be supported.

When specifying IP Addresses for the file server, use either dotted decimal format ("xxx.xxx.xxx.xxx") or DNS names. If you use DNS, the system value DOMAIN is appended to the IP Addresses you specify. If DOMAIN is null, the DNS names must be fully qualified, in accordance with IETF RFCs 1034 and 1035. For more information about DNS, see HTTP Generic Setup on page 88 and Local Administrative (Craft) Options Using the Avaya A175 User Interface on page 148.

Table 3: Required Network Information Before Installation - Per DHCP Server

1. Gateway (router) IP Address(es)	
2. HTTP server IP Address(es)	
3. Subnetwork mask	
4. HTTP server file path (HTTPDIR)	
5. Avaya A175 IP Address range *From*: *To*:	
6. DNS server address(es)	If applicable.
7. HTTPS server address(es)	If applicable.

The default file server file path is the "root" directory used for all transfers by the server. All files are uploaded to or downloaded from this default directory. In configurations where the upgrade (Axxxupgrade.txt) and software files are in the default directory, do not use item 4 in Table 3.

As the LAN or System Administrator, you are also responsible for:

- Administering the DHCP server as described in Chapter 7: Server Administration.
- Editing the configuration file on the applicable HTTP or HTTPS file server, as covered in Avaya A175 Desktop Video Device Software and Files.

Other Network Considerations

SNMP

The Avaya A175 devices support SNMPv1, SNMPv2, and SNMPv3.The Avaya A175 devices provide read-only access to the following MIBs:

- SNMP V2 MIB
- SNMP Community MIB
- SNMP Framework MIB
- SNMP Target MIB
- SNMP Notification MIB
- SNMP USM MIB
- SNMP VACM MIB
- Avaya A175 Custom MIB

Note:

The Avaya A175 does not support SNMP notifications (traps/INFORMs).

The SNMP service is configured through the Axxxsettings.txt file. For more information, see Chapter 7: Server Administration and Table 14: Avaya A175 Customizeable System Parameters.

Note:

SNMP is disabled by default. Administrators must initiate SNMP by setting the SNMPADD and SNMPSTRING system values appropriately.

For more information about SNMP and MIBs, see the IETF Web site listed in Appendix B: Glossary of Terms. The Avaya A175 Custom MIB is available for download in *.txt format on the Avaya support Web site at http://www.avaya.com/support.

Registration and Authentication

An Avaya A175 requires an outboard proxy SIP (OPS) extension on Avaya Communication Manager and a login and password on the SM Server to register and authenticate it. Registration is described in the Initialization process, in Avaya A175 Desktop Video Device Installation on page 15. For further information, see *Maintaining and Troubleshooting Avaya Aura™ Session Manager* (03-603325), available on the Avaya support Web site, http://www.avaya.com/support and your call server administration manual.

Reliability and Performance

All Avaya A175 devices respond to a ping or traceroute message sent from Avaya Communication Manager or any other network source and originate a ping.

If applicable, the Avaya A175 devices test whether the network Ethernet switch port supports IEEE 802.1D/q tagged frames by ARPing the router with a tagged frame. For more information, see Local Administrative (Craft) Options Using the Avaya A175 User Interface on page 148. If your LAN environment includes Virtual LANs (VLANs), your router must respond to ARPs for VLAN tagging to work properly.

QoS

For more information about the extent to which your network can support any or all of the QoS initiatives, see your LAN equipment documentation. Avaya A175 devices provide some detail about network audio quality. For more information see, Network Audio Quality Display on the Avaya A175 on page 57.

IEEE 802.1D and 802.1Q

For more information about IEEE 802.1D and IEEE 802.1Q and the Avaya A175 devices, see Local Administrative (Craft) Options Using the Avaya A175 User Interface on page 148. Three bits of the 802.1Q tag are reserved for identifying packet priority to allow any one of eight priorities to be assigned to a specific packet.

- **7:** Network management traffic
- **6:** Voice traffic with less than 10ms latency
- **5:** Voice traffic with less than 100ms latency
- **4:** “Controlled-load” traffic for critical data applications
- **3:** Traffic meriting “extra-effort” by the network for prompt delivery, for example, executive e-mail
- **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 Display on the Avaya A175

The Avaya A175 gives the user an opportunity to monitor network audio performance while on a call using the Avaya menu Network Information option. For more information, see the Avaya A175 user guide.

While on a call, the Avaya A175 displays network audio quality parameters in real-time, as shown in Table 4:

Table 4: Parameters in Real-Time

Parameter	Possible Values
Received Audio Coding	***G.711***, ***G.722***, ***G.726A***, or ***G.729***.
Packet Loss	No data or a percentage. Late and out-of-sequence packets are counted as lost if they are discarded. Packets are not counted as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.
Packetization Delay	No data or an integer number of milliseconds. The number reflects the amount of audio data in each RTP packet.
One-way Network Delay	No data or an integer number of milliseconds. The number is one-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 introduced by the jitter buffer of the device.

The implication for LAN administration depends on the values the user reports and the specific nature of your LAN, like topology, loading, and QoS administration. This information gives the user 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.

SIP Station Number Portability

The Avaya A175 provides station number portability. On startup or a reboot, the Avaya A175 attempts to establish communication with its home Personal Profile Manager (PPM) server based on the User Name and Password.

Assume a situation where the company has multiple locations in London and New York, all sharing a corporate IP network. Users want to take their Avaya A175 and its functionality from their offices in London to their New York office. When users start up their Avaya A175 devices in the new location and enter their credentials, the local PPM server usually routes them to the local call server. With proper administration of the local PPM server, the Avaya A175 knows to try its home PPM server, the one in London. The user can then be automatically registered with the London PPM server.

TCP/UDP Port Utilization

The Avaya A175 uses a variety of 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 ports each piece of equipment uses to support each protocol and each task within the protocol.

Depending on your network, you might need to know what ports or ranges are used in the operation of the Avaya A175 devices. Knowing these ports or ranges helps you administer your networking infrastructure.

Note:

In many cases, the ports used are the ones called for by IETF or other standards bodies.
Some of the explanations in Table 5 and Table 6 refer to configuration parameters or options settings. For more information about parameters and settings, see Administering Options for the Avaya A175.

Table 5: Received Packets (Destination = Avaya A175)

Destination Port	Source Port	Use	UDP or TCP?
The number used in the Source Port field of the DNS query sent by the Avaya A175	Any	Received DNS messages	UDP
The number used in the Source Port field of the packets sent by the Avaya A175 device's HTTP client	Any	Packets received by the Avaya A175 device's HTTP client	TCP
The number used in the Source Port field of the TLS/SSL packets sent by the Avaya A175 device's HTTP client	Any	TLS/SSL packets received by the Avaya A175 device's HTTP client	TCP
68	Any	Received DHCP messages	UDP
The number used in the Source Port field of the SNTP query sent by the Avaya A175	Any	Received SNTP messages	UDP
161	Any	Received SNMP messages	UDP
50000	Any	Received CNA test request messages	UDP
The number used in the Source Port field of registration messages sent by the Avaya A175 device's CNA Agent	Any	Received CNA registration messages	TCP

1 of 2

Table 5: Received Packets (Destination = Avaya A175) (continued)

Destination Port	Source Port	Use	UDP or TCP?
PORTAUD or the port number reserved for CNA RTP tests	Any	Received RTP packets	UDP
PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd) or the port number reserved for CNA RTP tests plus or minus one, as for PORTAUD, above	Any	Received RTCP and SRTCP packets	UDP
If signaling is initiated by the Avaya A175 = the number used in the Source Port field of the signaling packets sent by the Avaya A175 If signaling is initiated by the server = System-Specific	Any	Received signaling protocol packets	UDP/TCP
			2 of 2

Table 6: Transmitted Packets (Source = Avaya A175)

Destination Port	Source Port	Use	UDP or TCP?
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
80 unless explicitly specified otherwise (i.e. in a URL)	Any unused port number	Packets transmitted by the Avaya A175 device’s HTTP client	TCP
123	Any unused port number	Transmitted SNTP messages	UDP
The number used in the Source Port field of the SNMP query packet received by the Avaya A175	161	Transmitted SNMP messages	UDP
443 unless explicitly specified otherwise (i.e. in a URL)	Any unused port number	TLS/SSL packets transmitted by the Avaya A175 device’s HTTP client	TCP
514	Any unused port number	Transmitted Syslog messages	UDP
			1 of 3

Table 6: Transmitted Packets (Source = Avaya A175) (continued)

Destination Port	Source Port	Use	UDP or TCP?
CNAPORT	Any otherwise unused port number	Transmitted CNA registration messages	TCP
The port number specified in the test request message	50000	Transmitted CNA test results messages	UDP
System-specific	Any unused port number	Transmitted signaling protocol packets	TCP
FEPORT or the port number specified in a CNA RTP test request	PORTAUD, which must be in the range specified by the RTP_PORT_LOW and RTP_PORT_RANGE parameters or the port number reserved for CNA RTP tests	Transmitted RTP packets	UDP
FEPORT + 1 (if FEPORT is even) or FEPORT -1 (if FEPORT is odd) or the port number specified in a CNA RTP test request plus or minus one, as with FEPORT above	PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd) or the port number reserved for CNA RTP tests plus or minus one, as for PORTAUD, above	RTCP and SRTCP packets transmitted to the far-end of the audio connection	UDP

2 of 3

Table 6: Transmitted Packets (Source = Avaya A175) (continued)

Destination Port	Source Port	Use	UDP or TCP?
RTCPMONPORT	PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd)	RTCP packets transmitted to an RTCP monitor	UDP
System-specific	Any unused port number	Transmitted signaling protocol packets	UDP
			3 of 3

IP Address Reuse

IP Address reuse allows the Avaya A175 to reuse IP addresses during the DHCP process. IP Address reuse prevents infinite looping when separate VLAN servers are used for voice and data VLANs, and response is received from the DHCP server on the data VLAN, but not on the voice VLAN.

Unless otherwise indicated, the values described here during IP address reuse are internally provisioned or set by the process itself and not by manual administration.

Router(s) in Use:

if no responses are received from the router(s) indicated in the configuration parameter ROUTER (set using DHCP Option 3 or by a local administrative procedure), and if REUSE = 1, then ROUTER_IN_USE will be set to REUSE_ROUTER_IN_USE. With the exception of the ROUTER configuration parameter, the other router-related parameters are internally set system values.

VLAN Check:

During the VLAN check, if a reset is to be done and VLAN_IN_USE is not zero, VLAN_IN_USE will be added to VLANLIST if it is not already on VLANLIST.

The VLAN detection process described in VLAN Detection on page 127 is followed If tagging is off or if tagging is on and L2QVLAN is > 0, and if REUSETIME > 0, and if REUSE_IPADD is not “0.0.0.0”. If VLANTEST expires, the value of VLAN_IN_USE is added to VLANLIST if it is not already on VLANLIST.

If a DHCPOFFER is not received within REUSETIME seconds, or if a DHCPOFFER is received that contains a value of L2QVLAN that is on VLANLIST, REUSE will be set to 1, IPADD will be set to the value of REUSE_IPADD, NETMASK will be set to the value of REUSE_NETMASK, ROUTER will be set to the value of REUSE_ROUTERS, and if the value of REUSE_TAGGING is 1, 802.1Q tagging will be turned on with a VLAN ID equal to the value of L2QVLAN_INIT, DHCP will then enter the “extended” REBINDING state, and operation will proceed as normal.

After a successful registration, the following system values are set:

REUSE_IPADD will be set to the value of IPADD,

REUSE_NETMASK will be set to the value of NETMASK,

REUSE_ROUTERS will be set to the value of ROUTER,

REUSE_ROUTER_IN_USE will be set to the value of ROUTER_IN_USE,

REUSE_TAGGING will be set to the value of TAGGING,

L2QVLAN_INIT will be set to the value of VLAN_IN_USE,

the MIB object endptVLANLIST will be set to the value of VLANLIST and then the value of VLANLIST will be set to null.

Security

For information about toll fraud, see the respective call server documents on the Avaya support Web site. The Avaya A175 devices cannot guarantee resistance to all Denial of Service attacks. However, there are checks and protections to resist such attacks while maintaining appropriate service to legitimate users.

Avaya A175 devices support Transport Layer Security (TLS) for signaling. This standard allows the Avaya A175 to establish a secure connection to a HTTPS server, in which the upgrade and settings file can reside. This setup adds security over another alternative.

Note:

SRTP is not supported in Release 1.0.

Communications between the Avaya A175 and the Personal Profile Manager (PPM) can also be secured by setting the CONFIG_SERVER_SECURE_MODE parameter.

You also have a variety of optional capabilities to restrict or remove how crucial network information is displayed or used. These capabilities are covered in more detail in Chapter 7: Server Administration and include:

- Depending on the SIGSIGNAL parameter, supporting signaling channel encryption while registering, and when registered, with appropriately administered Avaya Communication Manager.
- Restricting the response of the Avaya A175 devices to SNMP queries to only IP Addresses on a list you specify.
- Specifying an SNMP community string for all SNMP messages the Avaya A175 sends.
- Restricting Avaya A175 user interface access to Craft Local Procedures to experienced installers and technicians and requiring password entry to access Craft procedures.
- Restricting the end user’s ability to use the Avaya A175 to view network data.

Chapter 5: Communication Manager Administration

Call Server Requirements

Avaya Communication Manager (CM) extends advanced telephony features to the Avaya A175 via Outboard Proxy SIP (OPS) support. This feature set offers enhanced calling features in advance of SIP protocol definitions and Avaya A175 implementations.

Before you perform administration tasks, ensure that the proper hardware is in place, and your call server software is compatible with the Avaya A175 devices. Avaya recommends the latest CM software and the latest Avaya A175 firmware.

Supported SIP Environments

The Avaya A175 requires CM 6.0 with Session Manager 6.0.

To deploy the Avaya A175 in survivability mode, you will need CM 6.0, Session Manager 6.0, and a secondary third-party SIP proxy/gateway, specifically the Audiocodes gateway MP114, MP118 Firmware Version 5.40.

For specific administration instructions about the Avaya A175, see Administering Stations on page 70.

Communication Manager Administrative Requirements for SM

For information about CM administrative requirements with Avaya Aura Session Manager, see the Avaya Aura™ Session Manager document library and the Avaya Aura System Manager document library on the Avaya support site.

Initial Direct Media

Configure Initial Direct Media to enable Pt2Pt video calls.

Auto Hold

Avaya A175 devices always provide auto hold, regardless of whether or not the Auto Hold parameter is administered on the Avaya Communication Manager IP Network System Parameters form.

Call Transfer Considerations

The Avaya A175 device's transfer operation is controlled locally by the Avaya A175 and is not affected by the settings Abort Transfer?, Transfer Upon Hang-up and Toggle Swap, on page 7 of the system-parameters features screen.

Conferencing Call Considerations

The Avaya A175 device's conference operation is controlled locally by the Avaya A175 and is not affected by the settings Abort Conference Upon Hang-up, No Dial Tone Conferencing, Select Line Conferencing and Toggle Swap, on page 7 of the system-parameters features screen.

Avaya A175 Administration

Table 7 summarizes the calling features available on the Avaya A175 devices. Some features are supported locally at the Avaya A175, while others are only available with Avaya Session Manager and Communication Manager with OPS.

The features shown in Table 7 can be used from the Avaya A175. Communication Manager automatically handles many other standard calling features such as call coverage, trunk selection using Automatic Alternate Routing (AAR), or Automatic Route Selection (ARS), Class Of Service/Class Of Restriction (COS/COR), and voice messaging. Details on feature operation and administration can be found in the *Feature Description and Implementation for Avaya Communication Manager* (Document Number 555-245-205) and any of the CM administration documents available on the Avaya support site. The Avaya SIP solution configures all Avaya A175 devices in Communication Manager as OPS.

Note:

Features activated in CM can only be deactivated via CM; features activated during failover can only be deactivated during the failover period.

Table 7: Avaya A175 Feature Support

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with CM/SM
3-Way Conferencing	Yes	
6-way Conference Bridge		Yes
Automatic Call Back/ Cancel		Yes
Call Forward All Calls (on/off)		Yes
Call Forward Busy/ Don't Answer (on/off)	Yes	Yes
Call Forward Unconditional (on/off)	Yes	
Call Hold	Yes (Consultation Hold)	Yes
Call Management - incoming, outgoing call screening		Yes
EC500 Enable		Yes
EC500 Disable		Yes
Extend Call for EC500		Yes
Message Waiting Indication	User can access their voice mailbox using the Message button if the parameter PSTN_VM_NUM is administered	
Send All Calls Enable/ Disable		Yes

1 of 2

Table 7: Avaya A175 Feature Support (continued)

Feature	Survivable Operation with Third-Party Proxy	Normal Operation with CM/SM
Transfer - attended	Yes	Yes
Transfer - unattended	Yes	Yes
Transfer to Voice Mail		Yes
		2 of 2

CM/SIP Configuration Requirements

This section refers to Communication Manager (CM) administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. The system-wide CM form and the particular page that needs to be administered for each feature are provided. These features, which already exist, are not required but are recommended because they optimize the Avaya A175 interface. For endpoint configuration requirements for Avaya Aura™ Session Manager, see *Administering Avaya Aura Communication Manager as a Feature Server* (Document Number 03-603479) and related Avaya Aura Session Manager documents, all available on the Avaya support site.

Table 8: CM/SIP Configuration Requirements

Task/Form	Command	Field(s)	Value(s)
IP Network Region		RTCP Report Period (secs)	Avaya A175 devices have a fixed reporting period. Note that this parameter is only displayed if "Use Default Server Parameters?" is set to "n".
IP Network Region		Authoritative Domain	Make sure that the Authoritative Domain is set to the same value as SIP Domain for Solution.
Off-PBX Telephones Station Mapping	change off-pbx-station mapping xxxx		Bridged call items on this form MUST be “none” or “orig.” The default is “none.”
Feature - Related System Parameters (page 1)	change system-parameters features	Music/Tone on Hold	This CM setting controls the music on hold capability for all endpoints, including Avaya A175 devices.
			1 of 4

Table 8: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Define the dial plan formats on the Dialplan Analysis Table form	change dialplan analysis	Call Type	Includes all extensions and OPS Feature Name Extensions (FNEs). To define the FNEs for the OPS features listed in Table , a FAC must also be specified for the corresponding feature. In a sample configuration, extensions are five digits in length and begin with 3 or 4, FNEs are five digits beginning with 7, and the access codes have various formats as indicated with the Call Type of "fac."
Define the access codes corresponding to the OPS FNEs on the Feature Access Code form	change feature-access-codes	Various fields on pages 1-5 of the form	
After defining the FACs, define the FNEs not provisioned by CM feature buttons using the command	change off-pbx-telephone feature-name-extensions		Used to support both OPS and Extension to Cellular.
Set the appropriate service permissions to support OPS features on the Class of Service form	change cos	Varied	y (Yes) or n (No)
			2 of 4

Table 8: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Add a station for each Avaya A175 to be supported using the Station form (page 1)	add station ***xxxxxx*** (where ***xxxxxx*** represents the extension number)	Extension	Assign the same extension as the CM call server extension administered in SM.
		(Station) Type	Use 9640SIP.
		Port	System-populated.
		Coverage Path	For voice messaging or other hunt group, if available.
		COS and COR	Same values as administered in the previous COS & COR section(s).
		Name	The person associated with the Avaya A175. This name should match what is entered for name in the Avaya SES proxy configuration.
		Message Lamp Ext	Enter the extension of the station you want to track with the message waiting lamp. (Usually the same extension initially entered on the Station form.)
Continue adding station information for the Avaya A175 using the Station form (page 2)	add station ***xxxxxx*** (where ***xxxxxx*** represents the extension number)	Bridged Call Alerting	Set to "y" if the extension for this Avaya A175 will have a "bridged" appearance defined on another non-SIP telephone. Note that no other attributes of the bridged appearance feature apply to Avaya A175 devices (e.g. off-hook indication, bridge-on, etc.).
		AUDIX Name	Enter the name of the voice messaging system administered for this system.
		Coverage After Forwarding	This field, with a default of "s" for system, governs whether an unanswered forwarded call is given CM coverage treatment.
		Per Station CPN Send Calling Number?	If CM is configured to always send Caller ID, you can individually block certain stations by setting this field to "n". This field also needs to be set to "n" if you want to use the "Calling Number nblock" FNE.

3 of 4

Table 8: CM/SIP Configuration Requirements (continued)

Task/Form	Command	Field(s)	Value(s)
Continue adding station button assignments for the Avaya A175 using the Station form (page 4)		BUTTON ASSIGNMENTS 1. call-appr 2. call-appr etc.	Fill in the number of call appearances ("call-appr" buttons) to be supported for this Avaya A175. Use the following guidelines to determine the correct number: To support certain transfer and conference scenarios, the minimum number of "call-appr" buttons should be 3.
Stations With Off-PBX Telephone Integration form (page 1)	change off-pbx-telephone station-mapping ***xxxxxx*** where ***xxxxxx*** represents the extension number of the station being configured	Station Extension Application Dial Prefix Phone Number Trunk Selection Configuration Set	Use to map the Communication Manager extension to the same SM call server extension. The Application is "OPS." Enter the other appropriate field values, for example, the Trunk Selection value indicates the SIP trunk group. The Configuration Set value can reference a set that has the default settings in Communication Manager.
Stations With Off-PBX Telephone Integration form (page 2)	change off-pbx-telephone station-mapping ***xxxxxx*** where ***xxxxxx*** represents the extension number of the station being configured	Call Limit	Change the call limit to match the number of "call-appr" entries in the Add Station form PLUS one. This setting should always be set to a minimum of three.

4 of 4

Administering Stations

This section refers to Communication Manager (CM) administration on the Avaya Aura™ System Manager. Administer the following items on the Station form. Avaya recommends setting the features covered in this section because they optimize the user interface.

Administering Features

The following buttons can be administered for an Avaya A175, unless otherwise noted:

Administrable Station Features

Feature	Administration Notes
3-Way Conferencing	
6-Way Conference Bridge	
Bridged Call Appearances	
Busy Indicator	
Call Appearances	
Call Forward (all)	
Call Forward Deactivation	
Call Forward Unconditional	
Call Forwarding (busy/ don’t answer)	
Call Hold	
Call management (incoming, outgoing call screening)	
Consultation Hold	
EC500 Enable/Disable	
EC500 Extend Call	
Message Waiting Indication	
Send All Calls	
Transfer (Attended)	
Transfer (Unattended - one button transfer)	

For additional information about administering Avaya Communication Manager for Avaya A175 devices, see the following Avaya documents, available on the Avaya Support Web site:

- *Administrator Guide for Avaya Communication Manager* (Document 03-300509).
- *Feature Description and Implementation for Avaya Communication Manager* (Document 555-245-205).

- *Administering Avaya Aura™ Communication Manager as a Feature Server* (Document Number 03-603479) and related Avaya Aura Session Manager documents.

Chapter 6: Session Manager (SM) Administration

Introduction

This chapter provides references to SM documents on administration and configuration.

Avaya Aura™ Session Manager Administration

For an administrative overview of Session Manager and details for administrative requirements and procedures, see the following documents available on the Avaya support Web site www.avaya.com/support:

- *Avaya Aura™ Session Manager Overview* (Document Number 03-603323)
- *Installing and Upgrading Avaya Aura™ Session Manager* (Document Number 03-603473)
- *Administering Avaya Aura™ Session Manager* (Document Number 03-603324)
- *Maintaining and Troubleshooting Avaya Aura™ Session Manager* (Document Number 03-603325)
- *Network Case Study for Avaya Aura™ Session Manager* (Document Number 03-603478)

Log into System Manager and perform the following steps:

1. Make sure the extension for each Avaya A175 user is administered as follows:
   - Set type is set to **9640SI**P.
   - Port is set to **IP**.
   - IP Softphone is enabled.
   - IP Video is enabled.
   - There are five call appearances.
   - EC500 is administered as a feature.
2. After all of the A175 users are administered, log into Avaya Communication Manager and use the change off-pbx-telephone station-mapping command to add each A175 user extension to OPS. Make sure each extension is routed to the correct trunk for Session Manager.

Chapter 7: Server Administration

Software Checklist

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

Note:
You can install the DHCP and HTTP server software on the same machine.

DHCP and File Servers

Dynamic Host Configuration Protocol (DHCP) minimizes maintenance for an Avaya A175 network by removing the need to individually assign and maintain IP Addresses and other parameters for each Avaya A175 on the network.

The DHCP server provides the following information to the Avaya A175 devices:

- IP Address of the Avaya A175 device(s)
- IP Address of the HTTP or HTTPS server
- IP Address of the NTP (Network Time Protocol) server (using Option 42)
- The subnet mask
- IP Address of the router
- DNS Server IP Address

Administer the LAN so each Avaya A175 can access a DHCP server that contains the IP Addresses and subnet mask.

⚠ **Important:**
An Avaya A175 cannot function without an IP Address. The failure of a DHCP server at boot time leaves all the affected Avaya A175 devices unusable. A user can manually assign an IP Address to an Avaya A175. When the DHCP server finally returns, the Avaya A175 never looks for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process.

Avaya recommends that:

- A minimum of two DHCP servers be available for reliability.
- A DHCP server be available when the Avaya A175 reboots.

- A DHCP server be available at remote sites if WAN failures isolate Avaya A175 devices from the central site DHCP server(s).

A (HTTP or HTTPS) file server, which may run on the same physical computer as Communication Manager, provides the Avaya A175 with a Axxxupgrade.txt file and, if appropriate, new or updated A175 software. You can edit the settings file (Axxxsettings.txt) to customize Avaya A175 parameters for your specific environment. For more information, see Chapter 10: Administering Avaya A175 Desktop Video Device Options.

DHCP Server Administration

This section concentrates on the simplest case of a single LAN segment. Information provided here can be used for more complex LAN configurations.

⚠ **Important:**

Before you start, understand your current network configuration. An improper installation will cause network failures or reduce the reliability and performance of your network.

Configuring DHCP for Avaya A175

Avaya A175 devices allow you to specify the value of some configuration parameters using DHCP option 242. If you have Avaya A175 devices that use option 176, you can make a copy of an existing option 176. Then, using that copy to administer DHCP option 242, you can either:

- leave any parameters the Avaya A175 devices do not support in Option 242 to be ignored, or
- delete unused or unsupported Avaya A175 parameters to shorten the DHCP message length.

The following parameters for Avaya A175 devices can be set in DHCP Option 242. Most of the same parameters can be set in a Axxxsettings.txt file as well, as described in Table 14: Avaya A175 Customizeable System Parameters.

Table 9: Parameters Set by DHCP

Parameter	Description
HTTPDIR	Specifies the path to prepend to all configurations and data files the Avaya A175 might request when starting up, i.e., the path, relative to the root of the HTTP file server, to the directory in which the device configuration and date files are stored. The path may contain no more than 127 characters and may contain no spaces. If an Avaya file server is used to download configuration files over HTTPS, but a different server is used to download software files via HTTP, set the path of the Avaya server in the DHCP site-specific option, and set HTTPDIR again in the Axxxsettings.txt file with the appropriate path for the second server. HTTPDIR is the path for all HTTP operations. The command is "SET HTTPDIR=<path>". In configurations where the upgrade (Axxxupgrade.txt) and binary files are in the default directory on the HTTP server, do not use the HTTPDIR=<path>.
HTTPPORT	Destination port for HTTP requests (default is 80).
HTTPSRVR	IP Address(es) or DNS name(s) of HTTP file server(s) used for file download (settings file and software) during startup. 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 (sends Destination Unreachable messages for closed ports used by traceroute).
ICMPRED	Controls whether ICMP Redirect messages are processed. The default is 0 (redirect messages are not processed).
L2Q	802.1Q tagging mode. The default is 0 (automatic).
L2QVLAN	VLAN ID of the voice VLAN. The default is 0.
LOGSRVR	Syslog server IP or DNS address.
MTU_SIZE	Maximum transmission unit size. Used to accommodate older Ethernet switches that cannot support the longer maximum frame length of tagged frames (since 802.1Q adds 4 octets to the frame).
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 (auto-negotiate).
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 (auto-negotiate).
PROCPSWD	Security string used to access local procedures. The default is 27238.
PROCSTAT	Controls whether local procedures are enabled. The default is 0 (enabled).
SIP_CONTROLLER_LIST	SIP proxy/registrar server IP or DNS address(es). (0 to 255 characters; zero or one IP Address in dotted decimal or DNS name format, separated by commas without any intervening spaces.) The default is null.
SNTPSRVR	List of SNTP server IP or DNS address(es) used to retrieve date and time via SNTP
TLSDIR	Used as path name that is prepended to all file names used in HTTPS GET operations during initialization (0-127 character string).

Table 9: Parameters Set by DHCP (continued)

Parameter	Description
TLSPORT	Destination TCP port used for requests to https server (0-65535). The default is 443.
TLSSRVR	IP Address(es) or DNS name(s) of Avaya file server(s) used to download configuration files. **Note:** Transport Layer Security is used to authenticate the server.
VLANTEST	Number of seconds to wait for a DHCPOFFER on a non-zero VLAN. The default is 60 seconds.

DHCP Generic Setup

This section is limited to describing a generic administration that works with the Avaya A175. Three DHCP software alternatives are common to Windows operating systems:

- Windows NT® 4.0 DHCP Server
- Windows 2000® DHCP Server
- Windows 2003® DHCP Server

Any other DHCP application might work. It is the responsibility of the customer to install and configure the DHCP server correctly.

DHCP server setup involves:

1. Installing the DHCP server software according to vendor instructions.
2. Configuring the DHCP server with:
   - IP Addresses available for the Avaya A175 devices.
   - The following DHCP options:
     - **Option 1 - Subnet mask**.
       As described in Table 3, item 3.
     - **Option 3 - Gateway (router) IP Address(es)**.
       As described in Table 3, item 1. 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.
     - **Option 6 - DNS server(s) address list**.
       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. At least one address in Option 6 must be a valid, non zero, dotted decimal address.
     - **Option 12 - Host Name**.
       Value is **AV*ohhhhhh***, where: o has one of the following values based on the OID (first three octets) of the device’s MAC address: “A” if the OID is 00-04-0D, “B” if the OID is 00-1B-4F), “E” if the OID is 00-09-6E, “L” if the OID is 00-60-1D, “T” if the OID is

00-07-3B, and “X” if the OID is anything else, and where hhhhhh are ASCII characters for the hexadecimal representation of the last three octets of the device’s MAC address.

- **Option 15 - DNS Domain Name**.
  This string contains the domain name to be used when DNS names in system parameters are resolved into IP Addresses. This domain name is appended to the DNS name before the Avaya A175 attempts to resolve the DNS address. Option 15 is necessary if you want to use a DNS name for the HTTP server. Otherwise, you can specify a DOMAIN as part of customizing HTTP as indicated in Local Administrative (Craft) Options Using the Avaya A175 User Interface on page 148.
- **Option 42 - SNTP Server**.
  This option specifies a list of IP Addresses indicating NTP servers available to the Avaya A175. List servers in the order of preference.The minimum length is 4, and the length must be a multiple of 4.
- **Option 51 - DHCP lease time**.
  If this option is not received, the DHCPOFFER is not be accepted. Avaya recommends a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the IP Address lease is assumed to be infinite as per RFC 2131, Section 3.3, so that renewal and rebinding procedures are not necessary even if Options 58 and 59 are received. Expired leases cause Avaya A175 devices to reboot. Avaya recommends providing enough leases so an IP Address for an Avaya A175 does not change if it is briefly taken offline.

Note:

Regarding Option 51: The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP Address. If the network has problems and the only DHCP server is centralized, the server is not accessible to the given Avaya A175. In this case the Avaya A175 is not usable until the server can be reached. Avaya recommends that once assigned an IP Address, the Avaya A175 continues using that address after the DHCP lease expires, until a conflict with another device is detected. As Table 14: Avaya A175 Customizeable System Parameters indicates, the system parameter DHCPSTD allows an administrator to specify that the Avaya A175 will either: a). Comply with the DHCP standard by setting DHCPSTD to “1”, or b). Continue to use its IP Address after the DHCP lease expires by setting DHCPSTD to “0.” The latter case is the default. If the default is invoked, after the DHCP lease expires the Avaya A175 sends an ARP Request for its own IP Address every five seconds. The request continues either forever, or until the Avaya A175 receives an ARP Reply. After receiving an ARP Reply, the Avaya A175 displays an error message, sets its IP Address to 0.0.0.0, and attempts to contact the DHCP server again. Log events are generated for either case.

- **Option 52 - Overload Option, if desired**.
  If this option is received in a message, the Avaya A175 interprets the **sname** and **file** fields in accordance with IETF RFC 2132,
  Section 9.3, listed in Appendix B: Glossary of Terms.

Note:

Option 53 - DHCP message type.
Value is 1 (DHCPDISCOVER) or 3 (DHCPREQUEST). If a DHCPACK is received in response to a DHCPREQUEST sent to renew the Avaya A175 device's IP address lease, a log event record is generated with a Log Category of "DHCP". If a DHCPNAK is received in response to a DHCPREQUEST sent to renew the Avaya A175 device's IP address lease, the Avaya A175 will immediately cease use of the IP address, a log event record will be generated, IPADD will be set to "0.0.0.0", and the Avaya A175 will enter the DHCP INIT state.

- **Option 55 - Parameter Request List**.
  Acceptable values are:
  1 (subnet mask),
  3 (router IP Address[es])
  6 (domain name server IP Address[es])
  7 (log server)
  15 (domain name)
  26 (Interface MTU)
  42 (NTP servers)
  SSON (site-specific option number)

- **Option 57 - Maximum DHCP message size**.
  Value is 1000.

- **Option 58 - DHCP lease renew time**.
  If not received or if this value is greater than that for Option 51, the default value of T1 (renewal timer) is used as per IETF RFC 2131, Section 4.5, listed in Glossary of Terms.

- **Option 59 - DHCP lease rebind time**.
  If not received or if this value is greater than that for Option 51, the default value of T2 (rebinding timer) is used as per RFC 2131, Section 4.5

The Avaya A175 devices do not support Regular Expression Matching, and therefore, do not use wildcards. For more information, see Administering Avaya A175 Desktop Video Device Options on page 115.

Avaya recommends that you administer DHCP servers to deliver only the options specified in this section and Table 9. Administering additional, unexpected options might have unexpected results, including causing the Avaya A175 to ignore the DHCP server.

Examples of good DNS administration include:

- Option 6: “***aaa.aaa.aaa.aaa***”
- Option 15: “***dnsexample.yourco.com,zzz.zzz.zzz.zzz***”
- Option 42: "***aaa.aaa.aaa.aaa***"

Depending on the DHCP application you choose, be aware that the application most likely does not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client a day or more. For example, Windows NT®

DHCP reserves expired leases for about one 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 in sync, or the client is not on the network when the lease expires, there is time to correct the situation.

The following example shows the implication of having a reservation period: Assume two IP Addresses, therefore two possible DHCP leases. Assume three Avaya A175 devices, two of which are using the two available IP Addresses. When the lease for the first two Avaya A175 devices expires, the third Avaya A175 cannot get a lease until the reservation period expires. Even if the other two Avaya A175 devices are removed from the network, the third Avaya A175 remains without a lease until the reservation period expires.

In Table 10, the Avaya A175 sets the system values to the DHCPACK message field values shown.

Table 10: DHCPACK Setting of System Values

System Value	Set to
DHCP lease time	Option #51 (if received).
DHCP lease renew time	Option #58 (if received).
DHCP lease rebind time	Option #59 (if received).
DOMAIN	Option #15 (if received).
DNSSRVR	Option #6 (if received, which might be a list of IP Addresses).
HTTPSRVR	The **siaddr** field, if that field is non-zero.
IPADD	The **yiaddr** field.
LOGSRVR	Option #7 (if received).
MTU_SIZE	Option #26.
NETMASK	Option #1 (if received).
ROUTER	Option #3 (if received, which might be a list of IP Addresses).
SNTPSRVR	Option #42.

Windows NT 4.0 DHCP Server

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start-->Settings-->Control Panel**.
2. Double-click the **Network** icon.
3. Verify that **Microsoft DHCP Server** is listed as one of the Network Services on the **Services** tab.
4. If it is listed, continue with the next section. If it is not listed, install the DHCP server.

Creating a DHCP Scope for the Avaya A175

Use the following procedure to create a DHCP scope for the Avaya A175.

1. Select **Start-->Programs-->Admin Tools-->DHCP Manager**.
2. Expand **Local Machine** in the DHCP Servers window by double clicking it until the **+** sign changes to a **-** sign.
3. Select **Scope-->Create**.
4. Using information recorded in Table 3: Required Network Information Before Installation - Per DHCP Server:

   Define the **Telephone IP Address Range**.

   Set the **Subnet Mask**.

   To ***exclude*** any IP Addresses you do not want assigned to Avaya A175 devices within the **Start** and **End** addresses range:

   a. In the **Exclusion Range Start Address** field, enter the ***first IP Address*** in the range that you want to exclude.

   b. In the **Exclusion Range End Address** field, enter the ***last IP Address*** in the range that you want to exclude.

   c. Click the **Add** button.

   d. Repeat steps a. through c. for each IP Address range to be excluded.

   Note:

   > Avaya recommends that you provision the Avaya A175 devices with sequential IP Addresses. Also do not mix Avaya A175 devices and PCs in the same scope.

5. Under **Lease Duration**, select the **Limited To** option and set the ***lease duration*** to the maximum.

6. Enter a ***sensible name*** for the **Name** field, such as “A175 Devices."
7. Click **OK**.

   A dialog box prompts you: `Activate the new scope now?`
8. Click **No**.

Note:

Activate the scope only after setting all options.

Editing Custom Options

Use the following procedure to edit custom options.

1. Highlight the newly created scope.
2. Select **DHCP Options-->Defaults** in the menu.
3. Click the **New** button.
4. In the **Add Option Type** dialog box, enter an appropriate custom option name, for example, “A175OPTION.”
5. Change the **Data Type Byte** value to **String**.
6. Enter **242** in the **Identifier** field.
7. Click the **OK** button.

   The **DHCP Options** menu displays.
8. Select the **Option Name** for 242 and set the *value string*.
9. Click the **OK** button.
10. For the **Option Name** field, select **003 Router** from the drop-down list.
11. Click **Edit Array**.
12. Enter the ***Gateway IP Address*** recorded in Table 3: Required Network Information Before Installation - Per DHCP Server for the **New IP Address** field.
13. Select **Add** and then **OK**.

Adding the DHCP Option

Use the following procedure to add the DHCP option.

1. Highlight the scope you just created.
2. Select **Scope** under **DHCP Options**.
3. Select the **242** option that you created from the **Unused Options** list.
4. Click the **Add** button.
5. Select option **003** from the **Unused Options** list.

6. Click the **Add** button.
7. Click the **OK** button.
8. Select the **Global parameter** under **DHCP Options**.
9. Select the **242** option that you created from the **Unused Options** list.
10. Click the **Add** button.
11. Click the **OK** button.

Activating the Leases

Use the following procedure to activate the leases.

- Click **Activate** under the **Scope** menu.

  The light-bulb icon for the scope lights.

Verifying Your Configuration

This section describes how to verify that the **A175OPTIONs** are correctly configured for the Windows NT® 4.0 DHCP server.

Verify the Default Option, 242 96XXOPTION

1. Select **Start-->Programs-->Admin Tools-->DHCP Manager**.
2. Expand **Local Machine** in the DHCP servers window by double clicking until the **+** sign changes to a **-** sign.
3. In the DHCP servers frame, click the *scope* for the Avaya A175.
4. Select **Defaults** from the **DHCP_Options** menu.
5. In the **Option Name** pull-down list, select **242 A175OPTION**.
6. Verify that the **Value String** box contains the correct string from DHCP Server Administration.

   If not, update the string and click the **OK** button twice.

Verify the Scope Option, 242 A175OPTION

1. Select **Scope** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 A175OPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct string from DHCP Generic Setup on page 78.

   If not, update the string and click the **OK** button.

Verify the Global Option, 242 A175OPTION

1. Select **Global** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 A175OPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct value from DHCP Generic Setup on page 78. If not, update the string and click the **OK** button.

Windows 2000 DHCP Server

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start-->Program-->Administrative Tools-->Computer Management**.
2. Under **Services and Applications** in the Computer Management tree, find **DHCP**.
3. If DHCP is not installed, install the DHCP server. Otherwise, proceed directly to Creating and Configuring a DHCP Scope for instructions on server configuration.

Creating and Configuring a DHCP Scope

Use the following procedure to create and configure a DHCP scope.

1. Select **Start-->Programs-->Administrative Tools-->DHCP**.
2. In the console tree, click the *DHCP server* to which you want to add the DHCP scope for the Avaya A175 devices. This is usually the name of your DHCP server machine.
3. Select **Action-->New Scope** from the menu.

   Windows displays the **New Scope Wizard** to guide you through rest of the setup.
4. Click the **Next** button.

   The **Scope Name** dialog box displays.
5. In the **Name** field, enter a name for the scope such as “A175 Devices," then enter a brief comment in the **Description** field.
6. When you finish Steps 1 - 5, click the **Next** button.

   The **IP Address Range** dialog box displays.
7. Define the range of IP Addresses used by the Avaya A175 devices listed in Table 3: Required Network Information Before Installation - Per DHCP Server. The **Start IP Address** is the first IP Address available to the Avaya A175 devices. The **End IP Address** is the last IP Address available to the Avaya A175 devices.

   Note:

   Avaya recommends not mixing Avaya A175 devices and PCs in the same scope.
8. Define the **subnet mask** in one of two ways:

   - The number of bits of an IP Address to use for the network/subnet IDs.

- The subnet mask IP Address.

  Enter only one of these values. When you finish, click the **Next** button.

  The **Add Exclusions** dialog box displays.

9. Exclude any IP Addresses in the range specified in the previous step that you do not want assigned to an Avaya A175.

   a. In the **Start Address** field under **Exclusion Range**, enter the ***first IP Address*** in the range you want to exclude.

   b. In the **End Address** field under **Exclusion Range**, enter the ***last IP Address*** in the range you want to exclude.

   c. Click the **Add** button.

   d. Repeat steps a. through c. for each IP Address range that you want to exclude.

   Note:

   > You can add additional exclusion ranges later by right clicking the **Address Pool** under the newly created scope and selecting the **New Exclusion Range** option.

   Click the **Next** button after you enter all the exclusions.

   The **Lease Duration** dialog box displays.

10. For all Avaya A175 devices that obtain their IP Addresses from the server, enter **30 days** in the **Lease Duration** field. This is the duration after which the IP Address for the device expires and which the device needs to renew.

11. Click the **Next** button.

    The **Configure DHCP Options** dialog box displays.

12. Click the **No, I will activate this scope later** button.

    The **Router** (Default Gateway) dialog box displays.

13. For each router or default gateway, enter the ***IP Address*** and click the **Add** button.

    When you are done, click the **Next** button.

    The **Completing the New Scope Wizard** dialog box displays.

14. Click the **Finish** button.

    The new scope appears under your server in the DHCP tree. The scope is not yet active and does not assign IP Addresses.

15. Highlight the newly created scope and select **Action-->Properties** from the menu.

16. Under **Lease duration for DHCP clients**, select **Unlimited** and then click the **OK** button.

    ⚠ **CAUTION:**

    > IP Address leases are kept active for varying periods of time. To avoid having calls terminated suddenly, make the lease duration unlimited.

Adding DHCP Options

Use the following procedure to add DHCP options to the scope you created in the previous procedure.

1. On the DHCP window, right-click the **Scope Options** folder under the scope you created in the last procedure.

   A drop-down menu displays.

2. In the left pane of the DHCP window, right click the **DHCP Server name**, then click **Set Predefined Options...**.
3. Under **Predefined Options and Values**, click **Add**.
4. In the **Option Type Name** field, enter ***any appropriate name***, for example, “Avaya A175 Devices.”
5. Change the **Data Type** to **String**.
6. In the **Code** field, enter **242**, then click the **OK** button twice.

   The **Predefined Options and Values** dialog box closes, leaving the DHCP dialog box enabled.

7. Expand the newly created scope to reveal its **Scope Options**.
8. Click **Scope Options** and select **Action-->Configure Options** from the menu.
9. In the **General** tab page, under the **Available Options**, check the **Option 242** checkbox.
10. In the **Data Entry** box, enter the ***DHCP IP telephone option string*** as described in DHCP Generic Setup on page 78.

    Note:

    You can enter the text string directly on the right side of the **Data Entry** box under the ASCII label.

11. From the list in **Available Options**, check option **003 Router**.
12. Enter the ***gateway (router) IP Address*** from the IP Address field of Table 3: Required Network Information Before Installation - Per DHCP Server.
13. Click the **Add** button.
14. Click the **OK** button.

Activating the New Scope

Use the following procedure to activate the new scope.

1. In the DHCP console tree, click the **IP Telephone Scope** you just created.
2. From the **Action** menu, select **Activate**.

   The small red down arrow over the scope icon disappears, indicating that the scope was activated.

HTTP Generic Setup

You can store the A175 software file, Axxxupgrade.txt file, and Axxxsettings.txt file on an HTTP server. With proper administration, the Avaya A175 seeks out and uses that material. Some functionality might be lost by a reset if the HTTP server is unavailable. For more information, see DHCP and File Servers on page 75.

Note:

The Avaya A175 devices do not support TFTP; you must use HTTP or HTTPS instead.

Important:

The files defined by HTTP server configuration must be accessible from all Avaya A175 devices that might request those files. Ensure that the file names match the names in the upgrade script, including case, since UNIX systems are case-sensitive.

Note:

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

Important:

To set up an HTTP server:

- Install the HTTP server application.
- Administer the system parameter HTTPSRVR to the address of the HTTP server. Include this parameter in DHCP Option 242 or the appropriate SSON Option.

- Download the Axxxupgrade.txt file and software files from the Avaya Web site http://www.avaya.com/support to the HTTP server. For more information, see Chapter 9: Avaya A175 Desktop Video Device Software and Files.

Note:

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

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

- Install the TLS server application.
- Administer the system parameter TLSSRVR to the address(es) of the Avaya HTTP server.

Chapter 8: Local Administrative Options

Introduction

During installation or after you have successfully installed an Avaya A175, you might be instructed to administer one of the manual procedures described in this chapter. These local administrative procedures are also referred to as Craft Procedures.

Note:

> You can modify the settings file to set parameters for Avaya A175 devices that download their upgrade script and application files from the same HTTP server.

CAUTION:

> Only trained installers or technicians should perform local (craft) procedures. Perform these procedures **only** if instructed to do so by the system or LAN administrator.
>
> Static administration of these options causes upgrades to work differently than if they are administered dynamically. Values assigned to options in static administration are not changed by upgrade scripts. These values remain stored in the Avaya A175 until the Avaya A175 is reset, as indicated in Performing a Factory Data Reset on page 92.
>
> Use these option-setting procedures **only** with static addressing and, as always, only if instructed by the system or LAN administrator. Do **not** use these option-setting procedures if you are using DHCP. DHCP is the Dynamic Addressing Process, as indicated in Dynamic Addressing Process/Device Startup on page 41.

About Local Administrative Procedures

Local administrative (Craft) procedures allow you to customize the Avaya A175 installation for your specific operating environment on a device-by-device basis. You can perform the following local administrative procedures:

- Change the network address information programming. See Static Addressing Installation on page 91.
- Enable/disable Automatic Gain Control. See Disabling/Enabling Automatic Gain Control on page 92.
- Clear all values to factory defaults. See Performing a Factory Data Reset on page 92.

- Set the Group Identifier. See Changing the Group Identifier on page 94.
- Set Network Interface Control. See Disabling/Enabling Event Logging on page 96.
- Reset system initialization values to defaults. See Performing a Factory Data Reset on page 92.
- Restart the device. See Restarting the Avaya A175 on page 99.
- Configure SIP call settings. See Configuring SIP Settings on page 100.
- Configure the time server settings. See Configuring the SNTP Settings on page 102.
- Set the Site-Specific Option Number. See Viewing System Parameters and File Versions on page 103.

Pre-Installation Checklist for Static Addressing

Before performing static programming of address information, verify that all the requirements listed in the Pre-Installation Checklist are met. You do not have to consider item 4 on page 12, as it refers to the DHCP server. In addition, you must have the values for the following parameters. Failure to do so can cause data entry errors that prevent the device from working. Such errors can also have a negative impact on your network. Print copies of this checklist for each subnet.

□ **1.** The IP Address of the device.

□ **2.** The IP Address of the router.

□ **3.** The IP subnet mask.

□ **4.** The IP Address of the HTTP and/or /HTTPS server.

□ **5.** The IP Address of the DNS server.

□ **6.** The VLAN ID (the L2QVLAN value).

□ **7.** The VLANTEST value.

Static Addressing Installation

The usual way to assign IP Addresses to Avaya A175 devices is the automatic method described in Dynamic Addressing Process/Device Startup on page 41. There might be times, however, when manual assignment of IP Addresses is desired.

> ⚠ **CAUTION:**
>
> Static addressing is necessary when a DHCP server is unavailable.
>
> Because of the increased opportunities for text entry errors associated with static addressing, Avaya strongly recommends that a DHCP server be installed and static addressing avoided.

Use the following procedure to manually set the HTTP/HTTPS file server address.

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings panel, touch **Network & Wireless**.
4. From the Network & wireless panel, touch **Ethernet settings**.
5. From the Ethernet settings panel, touch Ethernet settings.

   The Configure Ethernet Device panel appears.
6. Configure the settings in this panel.
7. When finished, touch the **Save** button.

Changing the Proxy Settings

Use the following procedure to manually set the proxy settings to access the internet.

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings panel, touch **Network & Wireless**.
4. From the Network & wireless panel, touch **Proxy settings**.

   The Proxy settings panel appears.
5. Configure the settings in this panel.
6. When finished, touch the **Save** button.

Changing the Network Connection

Use the following procedure to manually specify how the Avaya A175 connects to your LAN.

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings panel, touch **Network & Wireless**.
4. From the Network & wireless panel, touch **Network Connections**.

   The Network Connections panel appears.
5. Touch the appropriate setting.
6. When finished, touch the **Save** button.

Disabling/Enabling Automatic Gain Control

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

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

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings panel, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.
6. From the Administrator panel, touch **AGC**.
7. Touch the appropriate AGC setting to toggle it on/off.

Performing a Factory Data Reset

Sometimes, you might want to remove *all* administered values, user-specified data, and option settings. Essentially, you want to return an Avaya A175 to its initial “clean slate” or out of the box condition. This is usually done following Avaya A175 repair or when passing an Avaya A175 to a new, dedicated user.

The **Clear** option erases all administered data — static programming, file server and call server programming, and user settings, and restores all such data to default values. The Avaya A175 will be cleared to its “out of the box” state, resetting the following values to their factory defaults:

- All system values and system initialization values.
- User options, parameter settings, identifiers and password.
- Any user data like Contacts and History are deleted.

This option does not affect the software load itself. If you have upgraded the Avaya A175, the device retains the latest software. Once you have cleared an Avaya A175, you can administer it normally.

⚠ **CAUTION:**

> This procedure erases all administered data (for example, contacts, without any possibility of recovering the data.

Use the following procedure to clear the Avaya A175 of its administrative, user-assigned, and options values.

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings panel, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.
6. From the Administrator Options panel, touch **Clear**.

   A dialog box appears, prompting you to confirm your action.
7. Touch the **Yes** button to clear all values to their initial default values.

   After clearing the values, the Avaya A175 resets.

Disabling/Enabling Debug Mode

Use the following procedure to turn the debug mode on or off.

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings panel, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.
6. From the Administrator pane, touch **DEBUG**.

7. Touch the appropriate DEBUG setting to toggle it on/off.

Changing the Site-Specific Option Number Setting

⚠ **CAUTION:**

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

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

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings panel, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.

   The DHCP Site Specific Option Number displays the current system value.
6. From the Administrator Options panel, touch **DHCP Site Specific Option Number**.
7. Enter a valid SSON value between 128 and 255, and then touch the **OK** button.

Changing the Group Identifier

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

Note:

Perform this procedure only if the LAN Administrator instructs you to do so. For more information about groups, see The GROUP System Value on page 112.

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings pane, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.

   GROUP displays the current system value.
6. From the Administrator pane, touch **GROUP**.

7. In the GROUP panel, enter a valid **Group** value (0-999).
8. Touch the **Save** button.

Changing the Ethernet Interface Settings

Use the following procedure to set or change the Ethernet interface status and the PC Ethernet interface status.

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings pane, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.
6. From the Administrator pane, touch **Interfaces**.

   The following settings are displayed:

   - Ethernet
   - PC Ethernet

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

   The PHY1STAT text strings are:

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

   The PHY2STAT text strings are:

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

- "1000Mbps full" when PHY2STAT = 6

7. To change the Ethernet setting, touch **Ethernet**, and then touch the appropriate setting.
8. To change the PC Ethernet setting, touch **PC Ethernet**, and then touch the appropriate setting.

Disabling/Enabling Event Logging

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

1. Touch the **Applications** menu fan to display the Applications fan.
2. On the Applications fan, touch **Settings**.
3. From the Settings pane, touch **Administrator Options**.
4. In the Password box, enter ***27238***.
5. Touch the **Ok** button.
6. From the Administrator pane, touch **Log**.
7. To set the log categories:
   a. Touch **Log Categories**.
   b. Touch the appropriate log categories.
   c. When finished, touch the **Back** button.
8. To set the remote logging options:
   a. Touch **Remote Logging**.
   b. Touch **Remote Logging** to toggle it on/off. SYSLOG_ENABLED is defined as:
      - 1 = Enabled
      - 0 = Disabled]

   c. If Remote Logging is enabled (on), touch **Log Level**, and then touch the appropriate log level.

      SYSLOG_LEVEL is defined as:
      - "Emergencies" when SYSLOG_LEVEL = 0
      - "Alerts" when SYSLOG_LEVEL = 1
      - "Critical" when SYSLOG_LEVEL = 2
      - "Errors" when SYSLOG_LEVEL = 3
      - "Warning" when SYSLOG_LEVEL = 4
      - "Notice" when SYSLOG_LEVEL = 5

- "Information" when SYSLOG_LEVEL= 6
- "Debug" when SYSLOG_LEVEL = 7

d. To set the Remote Log Server address, touch **Log Server Address**, enter the IP Address to which syslog messages should be sent, and then touch the **OK** button.

e. Touch the **Back** button.

9. To set the local logging options:

a. Touch **Local Logging**.

b. Touch **Local Logging** to toggle it on/off. SYSLOG_ENABLED is defined as:

- 1 = Enabled
- 0 = Disabled]

c. If Local Logging is enabled (on), touch **Log Level**, and then touch the appropriate log level.

SYSLOG_LEVEL is defined as:

- "Emergencies" when SYSLOG_LEVEL = 0
- "Alerts" when SYSLOG_LEVEL = 1
- "Critical" when SYSLOG_LEVEL = 2
- "Errors" when SYSLOG_LEVEL = 3
- "Warning" when SYSLOG_LEVEL = 4
- "Notice" when SYSLOG_LEVEL = 5
- "Information" when SYSLOG_LEVEL= 6
- "Debug" when SYSLOG_LEVEL = 7

d. Touch the **Back** button.

Changing the Site-Specific Option Number Setting

⚠ **CAUTION:**

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

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

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.

3. From the Settings panel, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.

   The DHCP Site Specific Option Number displays the current system value.
6. From the Administrator Options panel, touch **DHCP Site Specific Option Number**.
7. Enter a valid SSON value between 128 and 255, and then touch the **OK** button.

Changing the Presence Settings

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

To reset the Avaya A175:

1. Touch the **Applications** menu fan to display the Applications fan.
2. On the Applications fan, touch **Settings**.
3. From the Settings pane, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.
6. From the Administrator Options panel, touch **PRESENCE**.

   The Presence Options panel appears.
7. Perform one of the following steps:
   - If you want to change the address of the presence server, touch **Presence Server Address**, enter the IP address of the presence server in the Presence Server Address panel, and touch the **Save** button.
   - If you want to change the presence XMPP port, touch **Presence XMPP Port**, enter the port number in the Presence XMPP Port panel, and touch the **Save** button
   - If you want to change the presence query timeout setting, touch **Presence Query Timeout**, enter the timeout value in the Presence Query Timeout panel, and touch the **Save** button

Resetting the System Values

Use the following procedure to reset the Avaya A175 initialization values to the default settings.

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings panel, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.
6. From the Administrator Options panel, touch **Clear**.

   A dialog box appears, prompting you to confirm your action.
7. Touch the **Yes** button to clear all values to their initial default values.

   After clearing the values, the Avaya A175 resets.

Restarting the Avaya A175

Use the following procedure to restart the Avaya A175.

Note:
> A restart does not affect user-specified data and settings like Contacts data or the username and password.

To restart the Avaya A175:

1. Touch the **Applications** menu fan to display the Applications fan.
2. On the Applications fan, touch **Settings**.
3. From the Settings pane, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.
6. From the Administrator pane, touch **REBOOT**.

   A dialog box appears, prompting you to confirm your action.
7. Touch the **Ok** button to restart the Avaya A175.

.

Resetting the Password for the Avaya A175

Use the following procedure to reset the "unlock" password for the Avaya A175.

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings panel, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.
6. From the Administrator Options panel, touch **Clear**.

   A dialog box appears, prompting you to confirm your action.
7. Touch the **Yes** button to clear all values to their initial default values.

   After clearing the values, the Avaya A175 resets.

Configuring SIP Settings

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

To configure SIP-related setting on the Avaya A175:

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings pane, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.
6. From the Administrator Options panel, touch **SIP Settings**.

7. To change the SIP global settings, touch **SIP Global Settings**.

   From the SIP Global Settings pane, you can modify the following settings:

Setting	Description/Example	Changes this Configuration Parameter
`SIP Mode:`	**Proxied**.	SIP_MODE
`SIP Domain:`	e.g., avaya.com	SIP_DOMAIN
`Avaya Environment:`	**Auto** or **No -** indicates whether only an Avaya environment (CM & SM) is in effect.	DISCOVER_AVAYA_ ENVIRONMENT
`Reg Policy:`	**alternate** or **simultaneous**	SIPREGPROXYPOLICY
`Failback Policy:`	**admin** or **auto**	FAILBACK_POLICY
`Avaya Config Server:`	IP Address of Avaya configuration server - only if PPM is not on the same server as the SIP Proxy server.	CONFIGURATION_SERVER or CONFIGURATION_SERVER _IN_USE
`User ID Field:`	Activates (**yes**) /deactivates (**no**) User ID field on Login screen.	ENABLE_SIP_USER_ID

8. Make your changes.
9. When finished, touch the **Back** button.
10. To add a new SIP proxy or modify your existing SIP proxy settings:
    a. Touch **SIP Proxy Settings** from the SIP Settings panel.

       The SIP Proxy Settings pane displays a list of currently configured servers.

    b. To add a new SIP proxy:
       1. Touch **Add new SIP Proxy**.

          The Add SIP Proxy panel appears.
       2. In the SIP Proxy Server box, enter the IP address of the Session Manager. (This changes the SIP_CONTROLLER_LIST configuration parameter.)
       3. Select the transport type. Choices are TLS, TCP, and UDP. (This changes the SIPSIGNAL configuration parameter.)
       4. In the SIP Proxy Port box, enter the SIP proxy port. If no value is entered, the default of 5060 for UDP/TCP or 5061 for TLS is used.

5. Touch the **Save** button.

c. To change an existing SIP proxy:

1. From the Proxy List area, touch the SIP proxy you want to modify.
2. In the Edit SIP Proxy dialog box, make your changes.
3. When finished, touch the **Save** button.

Configuring the SNTP Settings

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

To configure time server settings on the Avaya A175:

1. Touch the **Applications** menu fan to display the Applications fan.
2. On the Applications fan, touch **Settings**.
3. From the Settings pane, touch **Administrator Options**.
4. In the Password box, enter the administration password.
5. Touch the **Ok** button.
6. From the Administrator Options panel, touch **SNTP**.

   From the SNTP Options panel, you can modify the following settings:

	Description/Example	Changes this Parameter
SNTP Server Address:	IP address or DNS Name of the network time server.	SNTPSRVR or SNTPSRVR_IN_USE
SNTP Daylight Savings Time:	Indicates whether the Avaya A175 should recognize Daylight Savings Time (DST). Choices are Off (0=no DST), On (1=DST activated as per DSTOFFSET), and Auto (2=automatic based on DSTSTART and DSTSTOP values).	DAYLIGHT_SAVING_SETTING_MODE

7. From the SNTP Options panel, touch the SNTP option you want to change.
8. Make your changes.
9. When finished, touch the **Save** button.

Viewing System Parameters and File Versions

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

1. Touch the **Applications** menu title to display the Applications menu fan.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings panel, touch **About phone**.

   About phone panel displays the following information:

   - hardware
   - MAC address
   - network
   - status
   - battery use
   - firmware
   - legal

Chapter 9: Avaya A175 Desktop Video Device Software and Files

General Download Process

The Avaya A175 devices download upgrade files, settings files, certificate files, and software files from a file server. All of the file types can be downloaded either via HTTP or HTTPS except the software files, which can only be downloaded via HTTP. Avaya recommends HTTPS for downloading the file types because it ensures the integrity of the downloaded file by preventing "man in the middle" attacks. Further, once the trusted certificates are downloaded into the device, HTTPS ensures that the file server itself will be authenticated via a digital certificate. HTTPS is not used for software file downloads because Avaya A175 software files are already digitally signed, so there is no need to incur additional processing overhead while downloading these relatively large files. The HTTPS protocol applies only if the server supports Transport Layer Security (TLS) encryption.

Note:

> The Axxxupgrade.txt file and settings file 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 A175 devices might not contain the latest software. When the Avaya A175 is first plugged in, it will attempt to contact a file server, and will download new software if the software version available on the file server is different than the version on the Avaya A175. For subsequent software upgrades, the call server provides the capability to remotely reset the Avaya A175, which then initiates the same process for contacting a file server.

The Avaya A175 queries the file server, which transmits an Axxxupgrade.txt file to the Avaya A175. The Axxxupgrade.txt file tells the Avaya A175 which software file the Avaya A175 must use. The software file is easily updated for future enhancements. To ensure that is it using the latest software, the Avaya A175 requests a download of the proper software file from the file server. The file server downloads the file and conducts some checks to ensure that the file was downloaded properly. If the Avaya A175 determines it already has the proper file, the Avaya A175 proceeds to the next step.

Note:

> Unlike the SIP telephones, the Avaya A175 polls the file server at regular intervals to determine that it has the latest software. If a newer version is available, the A175 downloads it in the background without affecting the user.

After checking and loading the software file, the Avaya A175, if appropriate, uses the Axxxupgrade.txt file to look for the Axxxsettings.txt file. The settings file contains options you have administered for any or all of the Avaya A175 devices in your network. For more information about the settings file, see Contents of the Settings File on page 109.

Software

For software upgrades, Session Manager (SM) provides the capability for a remote reboot of the Avaya A175 devices. As a result of a message from SM, the Avaya A175 automatically starts reboot procedures. If new software is available on the file server, the Avaya A175 downloads it as part of the reboot process.

Avaya A175 Upgrade and Software Files

Choosing the Software File and Upgrade File

Every software release contains the files needed to operate the Avaya A175 devices. Each SIP software bundle contains:

- An upgrade file, **Axxxupgrade.txt**, which allows you to upgrade to the new software release. The Axxxupgrade.txt file tells the Avaya A175 whether a software upgrade is needed. All Avaya A175 devices attempt to read this file whenever they are turned on or reset. (The Avaya A175 devices also poll the file server at regular intervals to determine whether a newer version of the software is available.) The upgrade file also causes the Avaya A175 to download the Axxxsettings.txt file.
- The latest software for all current Avaya A175 devices.
- Avaya Certificate Authority (CA) certificate files that can be downloaded to the Avaya A175 devices when the TRUSTCERTS parameter is used to specify the Certificate Authorities that are to be trusted by the Avaya A175 devices.
- Other useful information such as a ReadMe file.

Each software bundle comes in one or more formats. Download the appropriate software bundle to your file server from the Avaya support Web site at: http://www.avaya.com/support. Note that all files must reside in the same directory on your file server.

Upgrade File (Axxxupgrade.txt)

The **Axxxupgrade.txt** file tells the Avaya A175 whether the device needs to upgrade its software. The Avaya A175 devices attempt to read this file on the file server whenever they are turned on or reset. This file allows the Avaya A175 to use default settings for customer-definable options. The Axxxupgrade.txt file also points to the Settings File (Axxxsettings.txt), where you can set provide values to override the default values for any settings you want to customize for your specific environment.

Note:

The Avaya A175 polls the file server at regular intervals to determine whether it has the latest software. If a newer version is available, the Avaya A175 downloads it in the background without affecting the user.

The Axxxupgrade.txt file is part of the software bundle you download from http://www.avaya.com/support.

Specific instructions are provided in the Readme file that accompanies the software bundle. The HTTP download directory holds the Avaya A175 backup and application software files the Avaya A175 will download.

Settings File (Axxxsettings.txt)

The settings file contains the parameters that you can use to customize the Avaya A175 devices for your enterprise.

Note:

Avaya recommends that the settings file have the name **Axxxsettings.txt**. The Avaya A175 devices can use Avaya-provided default values and operate without this file if you have no settings you want to customize. Note that you can also change these settings with DHCP (for information see Configuring DHCP for Avaya A175) or, in some cases, from the Avaya A175 user interface using local administrative (Craft) procedures.

Note:

Use one settings file for all your Avaya A175 devices.

The settings file can include five types of statements, one per line. Any invalid statement is ignored. The statement types are:

- SET statements of the form **SET *parameter_name value***. If the desired value contains a blank or a comma, the entire value must by placed within double quotes.
- GET statements of the form **GET *filename***, which cause the device to get the named file from the same file server and directory from which it got the current file. If the file is not available, the device continues to execute the current file.
- GOTO statements, of the form **GOTO *tag***. GOTO statements cause the device to continue interpreting the configuration file after a line that begins with a “**# tag**” statement. If no such line exists in the upgrade or settings file after the GOTO, the device ignores anything in the file after the GOTO.
- Tags are lines that begin with a **#** tag; tag is an unquoted string and cannot contain a space or comma.

- IF statements, of the form **IF $*name SEQ string*** **GOTO *tag***, where name is one of the system parameters shown in table #A#. Conditionals cause the GOTO command to be processed if the (string equivalent) value of name is equal to string. Note that the string comparison ignores case, so “Abc” matches “ABC” or “abc”. If no such name exists, the entire conditional is ignored. As for SET statements, the string must be included in double quotes if it includes spaces or commas. Any string may be double quotes, so 1 and “1” are equivalent as are “abc” and abc.

Any line which does not match one of the previous statement types is ignored and, therefore, can be treated as a comment. By convention, in the upgrade and settings files distributed by Avaya, any line intended to be ignored by the device or read as a comment starts with “**##**”.

Table 11: Settings File System Parameters That Can Be Tested in an IF Statement

Parameter	Description
BOOTNAME	The name of the boot code file in the device.
MACADDR	MAC address of the device (hh:hh:hh:hh:hh:hh; automatically supplied by a device).
MODEL	Device Model identifier (8 ASCII characters; automatically supplied by a phone).
MODEL4	The first four digits of the model identifier (automatically supplied by a device).
PWBCC	Avaya identification number for the printed circuit board (automatically supplied by a device).
GROUP	Group identifier (must be manually set on a device).

The ***Axxxupgrade.txt*** files distributed by Avaya start with a ***GOTO GETSET*** command based on the value of the SIG parameter to download whatever software is available (indicated by a SIG value of 0). This is the default SIG value.

The ***Axxxupgrade.txt*** files distributed by Avaya end with the statement ***GET Axxxsettings.txt.*** If you need to redefine the values of any parameters for your installation, do so in the ***Axxxsettings.txt*** file and not in the ***Axxxupgrade.txt*** file. The reason for using the Axxxsettings.txt file is because each new Avaya release you download will include a new version of ***Axxxupgrade.txt***, which will overwrite any changes you have made to your previous copy of that file.

Avaya recommends that you do **not** alter the Axxxupgrade.txt file. If Avaya changes the Axxxupgrade.txt file in the future, any changes you have made will be lost. Avaya recommends that you use the ***Axxxsettings*** 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 Axxxupgrade.txt file.

For more information on customizing your settings file, see Contents of the Settings File.

Contents of the Settings File

The final step in processing the Axxxupgrade.txt file is to GET the Axxxsettings.txt file. The default Axxxsettings.txt file contains explanatory material and default values on lines that start with ##. A parameter value can be changed and implemented by changing its value and removing the two ##'s at the beginning of the line.

The following are example settings only. Your settings will vary from the settings shown. This sample assumes specification of a DNS Server, identifying SIP-specific settings, and setting the time/date.

```
##
##
## Define the Domain Name Server to be "dns.example.yourco.com"
## Note that quotes are only needed for parameters that contain
  spaces.
##
SET DNSSRVER dnsexample.yourco.com
##
##
## SIP Proxy/Registrar servers list
##  SIP_CONTROLLER_LIST provides ability to configure SIP Proxy/
  Registrar list.
##  The format is host[:port];[transport:xxx]. A comma seperated
  list in this
##  format can be provided. Host can be DNS name or IP address. Port
  is optional.
##  If port is not specified then default value of 5060 for TCP and
  UDP and 5061 for
##  TLS will be used. Transport type is optional. It can be tcp or
  udp or tls.
##  Default value of tls will be used if it is not provided.
SET SIP_CONTROLLER_LIST proxy1,proxy2:5070;transport=udp
##
##
## Presence Enabled
##   Determines whether presence functionality is
##   enabled on the phone.
##     0 for No
##     1 for Yes
SET ENABLE_PRESENCE 1
##
##
```

```
##  SIPDOMAIN sets the domain name to be used during
##  registration.  The default is null ("") but valid values
##  are 0 to 255 ASCII characters with no spaces.
SET SIPDOMAIN   example.com
##
##
##  SNTPSRVR sets the IP address or Fully-Qualified
##  Domain Name (FQDN) of the SNTP server(s) to be used.
##  The default is null ("") but valid values are zero or
##  more IP addresses in dotted-decimal or DNS format,
##  separated by commas without intervening spaces, to a
##  maximum of 255 ASCII characters.
##  You may also want to use the ntp pool of servers.
##  See http://www.pool.ntp.org/use.html
##
SET SNTPSRVR  192.168.0.5
##
##
##  GMTOFFSET sets the time zone the phone should use. The
##  default is -5:00; see the 9600 Series SIP Telephone LAN
##  Admin Guide for format and setting alternatives.
SET GMTOFFSET "-6:00"
##
##
##  DSTOFFSET sets the daylight savings time adjustment
##  value. The default is 1 but valid values are 0, 1, or 2.
## SET DSTOFFSET "1"
##
##
##  DSTSTART sets the beginning day for daylight savings
##  time. See the 9600 Series
##  SIP Telephone LAN Admin Guide for format and setting
##   alternatives.
## SET DSTSTART  "2SunMar2L"
##
##   NOTE:
##   The default DSTSTART and DSTSTOP parameters reflect the
##   new 2007 Daylight Savings Time values for North America
##
##   DSTSTOP sets the ending day for daylight savings time.
## SET DSTSTOP   "1SunNov2L"
##
------------------------------
```

See Administering Options for the Avaya A175 for details about specific values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

VLAN separation controls whether or not traffic received on the secondary Ethernet interface is forwarded on the voice VLAN and whether network traffic received on the data VLAN is forwarded to the device. Add commands to the Axxxsettings.txt file to enable VLAN separation. The following three lines will enable VLAN separation when the data VLAN ID is "yyy" and the data traffic priority is "z":

- Enable VLAN separation by setting the parameter to 1: `SET VLANSEP "1"`
- Define the data VLAN ID (for any computer connected to the second ethernet port on the device) to be 'yyy': `SET PHY2VLAN "yyy"`
- Define the priority of the data traffic to be 'z': `SET PHY2PRIO "z"`

Note:

When the configuration parameter VLANSEP is set to "1" you should configure the network switch so that 802.1Q tags are not removed from frames forwarded to the device.

The GROUP System Value

You might have different communities of users, all of which have the same device model, but which require different administered settings. For example, you might want to group users by time zones or work activities.

Use the GROUP system value for this purpose:

1. identify which Avaya A175 devices are associated with which group, and designate a number for each group. The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group is assigned as Group 0.
2. At each non-default Avaya A175, instruct the installer or user to invoke the GROUP Craft Local procedure and specify which GROUP number to use. The GROUP System value can only be set on a device-by-device basis.
3. Once the GROUP assignments are in place, edit the configuration file to allow each Avaya A175 of the appropriate group to download its proper settings.

Here is an example of a settings file with Avaya A175 devices in three different groups - group "0" (the default), group "1", and group "2":

```
## First check if this device is in group 1. If it is, jump to the
  tag GROUP1

##

IF $GROUP SEQ 1 goto GROUP1

##

## Now check if this device is in group 2. If it is, jump to the tag
  GROUP2
  IF $GROUP SEQ 2 goto GROUP2

##

## The device is not in either GROUP 1 or 2 so it is in GROUP 0
  {specify settings unique to Group 0}
  goto END

# GROUP1

## GROUP 1-only settings go here
  {specify settings unique to Group 1}
  goto END

# GROUP2

## GROUP 2-only settings go here
  {specify settings unique to Group 2}
  # END

## The settings here apply to all three groups
  {specify settings common to all Groups}
```

Chapter 10: Administering Avaya A175 Desktop Video Device Options

Administering Options for the Avaya A175

This chapter explains how to change parameters to customize them for your operating environment. In all cases, you are setting a system parameter in the Avaya A175 to a desired value.

DNS Addressing

The Avaya A175 devices support DNS addresses and dotted decimal addresses. The Avaya A175 attempts to resolve a non-ASCII-encoded dotted decimal IP Address by checking the contents of DHCP Option 6. See DHCP Generic Setup on page 78 for information. 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, Table 14) is appended to the address(es) in Option 6 before the Avaya A175 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 Domain name in the HTTP script file. But first **SET** the **DNSSRVR** and **DOMAIN** values so you can use those names later in the script.

Note:

Administer Options 6 and 15 appropriately with DNS servers and Domain names respectively.

Emergency Number Administration

Set the PHNEMERGNUM configuration parameter in the settings file to assign an emergency telephone number. This telephone number will be automatically dialed whenever the **Emergency** button is selected on the Login screen, or the Unlock Code screen, or when the user chooses the **Yes** button on an Emergency pop-up panel.

Note:

> If SM is not operable, Emergency Number calling is not operable. When using UDP, the Emergency button may not work.
>
> When in failover, the Emergency Number must be provisioned on the SIP gateway or the user will not be able to dial it.

When the device is registered with an Avaya server and is in a logged out state, a call to the Emergency number shows a SIP URI username of "anonymous" in the From and Contact headers of the INVITE message. For example:

From: sip:anonymous@avaya.com;tag=-961235f46856f74-5_F135.8.62.174, and Contact: <sip:anonymous@135.8.62.174;transport=tcp>)

The device will always accept an incoming INVITE with a SIP URI username of "anonymous" in the To header with the IP address of the device. For example:

To: <sip:anonymous@135.8.62.174;transport=tcp>

This allows for incoming public service access point (PSAP) calls in both the registered inactive state and the registered state.

Enhanced Local Dialing

The Avaya A175 devices have a variety of telephony-related applications that might obtain a telephone number during operation. For example, the History saves a number of an incoming caller, but does not consider that the user has to then prepend the saved number with a digit to dial an outside line, and possibly a digit to dial long distance.

Avaya A175 devices can evaluate a raw telephone number, based on administered parameters. The Avaya A175 can automatically prepend the correct digits, saving the user time and effort. This is the Enhanced Local Dialing feature. The key to the success of this feature is accurate administration of several important values, summarized below.

The system values relevant to the Enhanced Dialing Feature are:

- **ENHDIALSTAT** - Enhanced dialing status. If set to “1” the enhanced local dialing feature is partially enabled, meaning dialing rules do not apply to dialing from the Contacts list. If set to "2" the enhanced local dialing feature is fully enabled and does apply to dialing from the Contacts list. If set to “0” enhanced local dialing is off.
- **PHNCC** - the international country code of the Communication Manager (CM) call server. For example, “1” for the United States, “44” for the United Kingdom, and so on.
- **PHNDPLENGTH** - the length of the dial plan on the CM call server.
- **PHNIC** - the digits the CM call server dials to access public network international trunks. For example, “011” for the United States.
- **PHNLD** - the digit dialed to access public network long distance trunks on the CM call server.
- **PHNLDLENGTH** - the maximum length, in digits, of the national telephone number for the country in which the CM call server is located.
- **PHNOL** - the character(s) dialed to access public network local trunks on the CM call server.

Note:

In all cases, the values you administer are the values relevant to the location of the CM call server at which the Avaya A175 devices are registered. If an Avaya A175 is in Japan, but its CM call server is in the United States, set the **PHNCC** value to “1" for the United States.

In all cases, the digits the Avaya A175 insert and dial are subject to standard CM call server features and administration. This includes Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), and so on.

As indicated in Table 14, you can administer the system parameter **ENHDIALSTAT** to turn off the Enhanced Local Dialing feature.

Setting the Dial Plan on Avaya A175 Devices

Note:

> This section only applies to operations with a secondary controller where CM/SM/PPM are not available.
> In a failover situation, the dial plan is played locally even if a proxy connection is not available; the user may hear a dial tone but cannot make a call.

During manual dialing, a dial plan allows a call to be initiated without using a **Call** button and without waiting for the expiration of a timeout interval. The dial plan consists of one or more format strings. When the dialed digits match a format string in the DIALPLAN configuration parameter, the call is initiated. (In an Avaya/SM environment, PPM retrieves the equivalent dial plan information in another format, thus the dial plan information from CM).

Valid characters in a format string, and their meanings, are as follows:

digits 0 through 9, inclusive = Specific dialpad digits
* = the dialpad character *
= the dialpad character # (but only if it is the first character in the dialed string – see below)
x = any dialpad digit (i.e., 0-9)
Z or **z** = present dial tone to the user (for example, for Feature Access Code (FAC) entry)
[ ] = any one character within the brackets is a valid match for a dial plan string
- = any one digit between the bounds within the brackets, inclusive, is a match
+ = the character following the + can repeat 0 or more additional times, for a valid match

An individual valid dial plan is any combination of the above characters. If there are multiple valid dial plans, separate each one from the next using an OR symbol ("|"). If the dial plan text string begins or ends with an OR symbol, that symbol is ignored. Users cannot modify the dial plan.

Dial plan example:

“[2-4]xxx|[68]xxx|*xx|9Z1xxxxxxxxxx|9z011x+”

where:

[2-4]xxx: Four-digit dial extensions, with valid extensions starting with 2, 3, or 4;
[68]xxx: Four-digit dial extensions, with valid extensions starting with 6 or 8;
***xx**: Two-digit Feature Access Codes, preceded by a *;
9Z1xxxxxxxxxx: Network Access Code (“9 for an outside line”), followed by dial tone, followed by any string of 10 digits– typical instance of Automatic Route Selection (ARS) for standard US long distance number;
9z011x+: Network Access Code (“9 for an outside line”), followed by dial tone, followed by at least one digit – typical instance of Automatic Route Selection (ARS) for US access to international numbers of unknown, and variable, length.

Additional parameters that affect dialing are as follows:

COUNTRY - Country of operation for specific dial tone generation.

PSTN_VM_NUM (PSTN access number for Voice Mail system) - This parameter specifies the telephone number to be dialed automatically when the Avaya A175 user presses the Messaging button under a non-AST controller. The device places a PSTN call out from the local office and back in to the location that houses the voice mail server. Additional codes necessary to reach a specific user's voice-mail box may also be included.

Example 1. `SET PSTN_VM_NUM 96135550123`

ENABLE_REMOVE_PSTN_ACCESS_PREFIX - When the Avaya A175 is operating with a non-AST controller and the value of the parameter is 0, the PSTN access prefix, defined by the parameter PHNOL, is retained in the outgoing number. If the value is 1, then the PSTN access prefix is stripped from the outgoing number.

PHNLAC - A string representing the device’s local area code. When set, this parameter indicates the endpoint's local area code, which along with the parameter LOCAL_DIAL_AREA_CODE, allows users to dial local numbers with more flexibility.

Example: `SET PHNLAC 617`

LOCAL_DIAL_AREA_CODE - A flag indicating whether the user must dial the area code for calls within same area code regions. When the parameter is 0, the user does not need to dial the area code; when this parameter is 1, the user needs to dial the area code. When this parameter is enabled (1), the area code parameter (PHNLAC) should also be configured (i.e., not the empty string).

Example: `SET LOCAL_DIAL_AREA_CODE 1`

Example 1 - Setting the parameter configuration:

```
SET ENHDIALSTAT 2

SET PHNOL 27

SET PHNCC 1

SET PHNDPLENGTH 7

SET PHNLDLENGTH 11

SET PHNLD 0

SET PHNIC 001
```

Example 2 - In the Contacts list, save Contact X with the telephone number 41018989:

PHNLAC Parameter Value	LOCAL_DIAL_AREA_CODE Parameter Value	Step to Execute	Result
020	1	Call X from Contacts list	Device sends an invite message with 2702041018989.
020	0	Call X from Contacts list	Device sends an invite message with 2741018989 and does not insert the local area code.
Null	1	Call X from Contacts list	Device sends an invite message with 2741018989 and does not insert the local area code.

See Table 14 for a definition of the DIALPLAN parameter.

Voice Mail Integration

Using the Axxxsettings.txt file, you can enable Avaya A175 users to access their voice messages by touching the Voice Mail icon in the Top bar of the Avaya A175 user interface. To administer the Avaya A175 to access the voice mail system, set the following parameter:

MSGNUM - Specify the extension that must be dialed to access the voice mail system.

Presence Notification

Presence notification occurs only if the ENABLE_PRESENCE parameter (set using the Axxxsettings.txt file) is set to 1 (Enabled/On).

The Avaya A175 PUBLISHes its status based on the conditions shown in Table 12.

Table 12: Presence notification in a Session Manager environment

Phone Status	PUBLISHED Presence
On hook	Onhook
Send All Calls active	do-not-disturb

Table 12: Presence notification in a Session Manager environment (continued)

Off hook	on-a-call
On a conference call The Avaya A175 determines it is on a conference call by the presence of the "isfocus" feature parameter in the Contact header.	on-a-conference

Presence User Interface

Presence provides information about other SIP users to the Avaya A175 user.

The Presence status is displayed on the Contacts cards and the History cards in the Avaya A175. To track the presence of a contact, the Avaya A175 user must add that contact to the Buddies group.

During failover, no presence tracking occurs.

The Avaya A175 supports rich presence with the Avaya Aura ™ Presence Server (PS) for the following states:

- On hook and available
- Off hook
- Not Registered
- Send All Calls
- On a conference call
- Away

There are two different aspects of presence in a Session Manager (SM) environment:

- Sent Presence - The Avaya A175 sends the following presence states:
  - On hook and Available: Sent when Avaya A175 is registered and no other states apply.
  - Off hook/On the Phone: Sent when the Avaya A175 is active on a call.
  - Not Registered: The state is not sent when the Avaya A175 is unregistered. But the state is rendered at a tracking device.
  - Busy: Sent when "Send All Calls" is activated. This is the same as Do Not Disturb and the same icon is used for both.
  - On a Conference call
- Received Presence - The Avaya A175 receives and renders the following presence states:
  - All those stated above for sent presence.

- Away: Sent when the Avaya A175 is "locked."

Presence Administration

Avaya A175 presence is "off" by default. To turn presence on, you must administer the following settings in the Axxxsettings.txt file:

ENABLE_PRESENCE - The default of "0" indicates presence tracking is not enabled. A setting of "1" enables presence of individuals whose have been added to the Buddies group in the Avaya A175 Contacts.

f you want to enable automatic update of the phone presence status when the user goes on/off hook, administer the following setting in the Axxxsettings.txt file:

ENABLE_AUTOMATIC_ON_THE_PHONE_PRESENCE - This parameter controls whether "on the phone" presence status is sent out automatically when user whose presence is tracked is on a call (or goes off-hook). Calls on bridged line appearances (that local user has not bridged to) do not affect the trigger of the "on the phone" presence update. The default of "0" indicates this option is disabled; when the person whose presence is being tracked goes off-hook, his or her presence is not reported. A setting of "1" enables automatic on the phone presence. When the user goes off-hook, no special presence is reported

Integrating Microsoft™ Exchange

Users can configure the Avaya A175 to access and manage their Microsoft Exchange account. Once configured, the Avaya A175 automatically downloads the following items from Microsoft Exchange:

- contacts (which are placed in the Exchange group in the Contacts menu fan)
- calendar events (which are placed in your calendar on the Avaya A175)
- email messages

The Avaya A175 will automatically synchronize with the user’s Microsoft Exchange account (that is, contacts, calendar, and email) at regular intervals to ensure that the user has the most up-to-date information. The procedure for configuring access to Microsoft Exchange is described in the Avaya A175 user guide.

From an administrative perspective, there are no configuration parameters in the settings file that you must administer before your end users can integrate Microsoft Exchange with their Avaya A175 devices.

Administering Instant Messaging

The Avaya A175 enables users to send and receive instant messages to other SIP users on the company’s enterprise network. To enable Instant Messaging, you must configure the following settings in the Axxxsettings.txt file:

INSTANT_MSG_ENABLED - The default of "0" indicates Instant Messaging is disabled. A setting of "1" enables Instant Messaging.

INSTANT_MSG_IDENTITY_QUERY_TIMEOUT - This parameter sets the time in seconds (1-10) for the Query Subscription Timeout. This is the number of seconds to wait for a NOTIFY response for a Presence SUBSCRIBE query. The default is 5 seconds.

Integrating Avaya Meeting Exchange

To enable Avaya A175 users to set up and manage conferences using Avaya Meeting Exchange, you must configure the following setting in the Axxxsettings.txt file:

CONFERENCE_SERVER_ADDRESS - Specify the conferencing server IP address. The default is null (""). Valid values are zero or an IP address in dotted decimal format.

LDAP Directory Integration

The Avaya A175 enables users search and use information from an LDAP directory. To enable LDAP directory searches from the Avaya A175, you must configure the following settings in the Axxxsettings.txt file:

DIRSRVR - Enter the IP address of the LDAP directory server. The default is null (""). Valid values are zero or more IP addresses in dotted-decimal or DNS format separated by commas without intervening spaces. Maximum is 255 ASCII characters.

DIRLDAPPORT - Enter the TCP port number of the LDAP directory server. The default port number is 389.

DIRTOPDN - This is the directory topmost distinguished name. You must set this value to a non-null value to enable the LDAP application. You should set DIRTOPDN to the LDAP root entry. The default is null ("").

DIRSRCHTIME - This parameter sets the directory search time (in seconds). Valid values are 1-60. The default is 5 seconds.

DIRFULLNAME - This parameter sets the default LDAP search value. The Avaya A175 only supports searches on names. The default is **cn**, which stands for "complete name" in LDAP.

Note:

Changing the default DIRFULLNAME value is not recommended unless your LDAP directory uses a different term for this data field.

DIRTELNUM - This parameter specifies the directory telephone number field. The default is **telephonenumber**.

Note:

Changing the default DIRTELNUM value is not recommended unless your LDAP directory uses a different term for this data field.

DIRMOBILE - This parameter specifies the directory mobile number field. The default is **mobile**.

Note:

Changing the default DIRMOBILE value is not recommended unless your LDAP directory uses a different term for this data field.

DIRMAIL - This parameter specifies the directory mail field. The default is **mail**.

Note:

Changing the default DIRMAIL value is not recommended unless your LDAP directory uses a different term for this data field.

DIRCOMPANYNAME - This parameter specifies the directory company name field. The default is **companyname**.

Note:

Changing the default DIRCOMPANYNAME value is not recommended unless your LDAP directory uses a different term for this data field.

DIRLOCATION - This parameter specifies the directory location field. The default is **l**.

Note:

Changing the default DIRLOCATION value is not recommended unless your LDAP directory uses a different term for this data field.

DIRBNTUSERDOMAINID - This parameter specifies the directory network user domain ID field. The default is **ntuserdomainid**.

Note:

Changing the default DIRBNTUSERDOMAINID value is not recommended unless your LDAP directory uses a different term for this data field.

DIRFIRSTNAME - This parameter specifies the directory first name field. The default is **givenname**.

Note:

Changing the default DIRFIRSTNAME value is not recommended unless your LDAP directory uses a different term for this data field.

DIRLASTNAME - This parameter specifies the directory last name field. The default is **sn**.

Note:

Changing the default DIRLASTNAME value is not recommended unless your LDAP directory uses a different term for this data field.

Administering the Unlock Password

The Avaya A175 provides a "lock out" mechanism that "locks" the Avaya A175 after a specified interval of inactivity. When the Avaya A175 becomes locked, the user must enter the unlock password. When the Avaya A175 is locked, the only actions a user can perform are:

- answer a call
- make a call to the emergency number

To enable the lock out mechanism on the Avaya A175, you must configure the following settings in the Axxxsettings.txt file:

PASSWORD_POLICY_ENABLE_PASSWORD - Enter **1** to enable the lock out mechanism. The default is 0. (The lock out mechanism is disabled.)

PASSWORD_POLICY_PASSWORD_LENGTH - Specify the length of the unlock password. The Avaya A175 chooses the more secure setting between the value you specify here and ActiveSync. The default is 6.

PASSWORD_POLICY_ALPHANUMERIC_PASSWORD - Specify whether the unlock password shall include alphanumeric characters. Values are:

- 0: Do not enforce password complexity (that is, anything is allowed).
- 1: Digits-only is enforced.
- 2: Alphanumeric is enforced. (This is the default.)
- 3: Both alphanumeric and special characters are enforced.

The Avaya A175 chooses the more secure setting between the value you specify here and ActiveSync.

PASSWORD_POLICY_PASSWORD_FAILED_ATTEMPTS_ENABLE - Specify whether to track the number of failed attempts to enter the unlock password. Values are:

- 0: Disables tracking of failed password attempts. (This is the default.)
- 1: Enables tracking of failed password attempts.

PASSWORD_POLICY_PASSWORD_FAILED_ATTEMPTS - Specify the number of failed attempts at which the Avaya A175 is locked and prevents any more unlock attempts. The default is 8. This setting is used only if PASSWORD_POLICY_PASSWORD_FAILED_ATTEMPTS_ENABLE is set to 1 (enabled).

PASSWORD_POLICY_INACTIVITY_LOCK_TIMEOUT - Specify the time interval (in minutes) of inactivity at which the Avaya A175 will become locked. Valid values are 1 to 1440 minutes. The default is 60 minutes.

Language Selection

Upon startup, Avaya A175 devices are factory-set to display information in the English language. Using the Welcome Wizard, users can select the language they want to use. The following languages are supported:

- French
- Latin American Spanish
- German
- Brazilian Portuguese
- Italian
- Russian
- Simplified Chinese
- Japanese
- Korean
- English

To run the Welcome Wizard, perform the following steps:

1. Touch the Applications menu title to display the Applications menu fan.
2. From the Applications menu fan, touch **Welcome Wizard**.
3. From the Language panel, touch the button for the language you want to use, and then touch the **Next** button.
4. Keep touching the **Next** button to proceed through each panel in the Welcome Wizard.
5. When you get to the Finish panel, touch the **Finish** button.

Setting the Date and Time on Avaya A175 Devices

Avaya A175 devices need a source of date and time information. This typically comes from a network time server running the Simple Network Time Protocol (SNTP). The Avaya A175 devices use several administrative parameters for this functionality. The parameter SNTPSRVR defines the server's IP Address(es). GMTOFFSET defines the offset from Greenwich Mean

Time (GMT). DSTSTART and DSTSTOP define the start and end of Daylight Savings Time, respectively. DSTOFFSET defines the Daylight Savings Time offset from Standard Time. Finally, DATETIMEFORMAT defines the format of the date and time display. See Table 14 for definitions and valid values for SIP Date and Time parameters.

VLAN Considerations

This section contains information on how to administer Avaya A175 devices 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.

VLAN Tagging

IEEE 802.1Q tagging (VLAN) is a useful method of managing VoIP traffic in your LAN. Avaya recommends that you establish a *voice* VLAN, set L2QVLAN to that VLAN, and provide voice traffic with priority over other traffic. You can set VLAN tagging manually, by DHCP, or in the Axxxsettings.txt file.

If VLAN tagging is enabled (L2Q= 0 or 1), the Avaya A175 devices set the VLAN ID to L2QVLAN, and the VLAN priority for packets from the device to L2QAUD for audio packets and L2QSIG for signalling packets. The default value (6) for these parameters is the recommended value for voice traffic in IEEE 802.1D.

Regardless of the tagging setting, an Avaya A175 will always transmit packets at absolute priority over packets from secondary Ethernet. The priority settings are useful only if the downstream equipment is administered to give the *voice* VLAN priority.

> ⚠ **Important:**
> VLAN tags are always removed from frames that egress (go out of) the secondary Ethernet interface.

VLAN Detection

The Avaya A175 devices support automatic detection of the condition where the L2QVLAN setting is incorrect. When VLAN tagging is enabled (L2Q= 0 or 1) initially the Avaya A175 transmits DHCP messages with IEEE 802.1Q tagging and the VLAN set to L2QVLAN. The Avaya A175 devices will continue to do this for VLANTEST seconds.

- If the VLANTEST timer expires and L2Q=1, the Avaya A175 sets L2QVLAN=0 and transmits DHCP messages with the default VLAN (0).

- If the VLANTEST timer expires and L2Q=0, the Avaya A175 sets L2QVLAN=0 and transmits DHCP messages without tagging.
- If VLANTEST is 0, the timer will never expire.

Note:

Regardless of the setting of L2Q, VLANTEST, or L2QVLAN, you must have DHCP administered so that the Avaya A175 will get a response to a DHCPDISCOVER when it makes that request on the default (0) VLAN.

After VLANTEST expires, if an Avaya A175 receives a non-zero L2QVLAN value, the Avaya A175 will release the IP Address and send DHCPDISCOVER on that VLAN. Any other release will require a manual reset before the Avaya A175 will attempt to use a VLAN on which VLANTEST has expired. See the Reset procedure in Chapter 3.

The Avaya A175 ignores any VLAN ID administered on the Communication Manager call server.

VLAN Default Value and Priority Tagging

The system value **L2QVLAN** is initially set to “0” and identifies the 802.1Q VLAN Identifier. This default value indicates “priority tagging” as defined in IEEE 802.IQ Section 9.3.2.3. Priority tagging specifies that your network closet Ethernet switch automatically insert the switch port default VLAN without changing the user priority of the frame (cf. IEEE 802.1D and 802.1Q).

The VLAN ID = 0 (zero) is used to associate priority-tagged frames to the port/native VLAN of the ingress port of the switch. But some switches do not understand 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:

- Ensure that the switch configuration lets frames tagged by the Avaya A175 through without overwriting or removing them.
- Set the system value **L2QVLAN** to the ***VLAN ID*** appropriate for your voice LAN.

Another system value you can administer is **VLANTEST**. VLANTEST defines the number of seconds the Avaya A175 waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is “60” seconds. Using VLANTEST ensures that the Avaya A175 returns to the default VLAN if an invalid VLAN ID is administered or if the Avaya A175 moves to a port where the L2QVLAN value is invalid. The default value is long, allowing for the scenario that a major power interruption is causing the Avaya A175 devices to restart. Always allow time for network routers, the DHCP servers, etc. to be returned to service. If the Avaya A175 restarts for any reason and the VLANTEST time limit expires, the Avaya A175 assumes the administered VLAN ID is invalid. The Avaya A175 then initiates registration with the default VLAN ID.

Setting **VLANTEST** to “**0**” has the special meaning of telling the phone to use a non-zero VLAN indefinitely to attempt DHCP. In other words, the Avaya A175 does not return to the default VLAN.

Note:

> If the Avaya A175 returns to the default VLAN but must be put back on the L2QVLAN VLAN ID, you must Reset the Avaya A175. See the Reset procedure.

⚠ **Important:**

> If a VLAN ID is provisioned using DHCP, then L2QVLAN and VLANTEST must be provisioned in all DHCP servers that the Avaya A175 can potentially use.

VLAN Separation

VLAN separation is available to control access to the voice VLAN from the secondary Ethernet interface, and to control whether broadcast traffic from the data VLAN is forwarded to the Avaya A175. The following system parameters control VLAN separation:

- **VLANSEP** - enables (1) or disables (0) VLAN separation.
- **PHY2VLAN** - specifies the VLAN ID to be used for frames forwarded to the network from the secondary Ethernet interface.
- **PHY2PRIO -** the layer 2 priority value to be used for tagged frames forwarded to the network from the secondary Ethernet interface.

Table 13 provides several VLAN separation guidelines.

Table 13: VLAN Separation Rules

If		Then
VLANSEP is “1” (On/Enabled)	**AND** the device is tagging frames with a VLAN ID not equal to PHY2VLAN, **AND** the PHY2VLAN value is not zero.	**Tagged Frames received on the secondary Ethernet interface:** All tagged frames received on the secondary Ethernet interface are changed before forwarding to make the VLAN ID equal to the PHY2VLAN value and the priority value equal to the PHY2PRIO value. Untagged frames received on the secondary Ethernet interface are not changed before forwarding to the network. Tagged frames with a VLAN ID of zero (priority-tagged frames) will be changed before they are forwarded such that the VLAN ID of the forwarded frame is equal to the PHY2LAN value and the priority value is equal to the PHY2PRIO value. **Tagged Frames received on the line interface:** Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2VLAN. Tagged frames received on the Ethernet line interface will only be forwarded to the Avaya A175 if the VLAN ID equals the VLAN ID used by the Avaya A175. Untagged frames are not changed will continue to be forwarded or not forwarded as determined by the Ethernet switch forwarding logic. Tagged frames with a VLAN ID of zero (priority-tagged frames) will be forwarded to the secondary Ethernet interface or to the Avaya A175 as determined by the forwarding logic of the Ethernet switch, but the tag will still be removed from frames that egress from the secondary Ethernet interface.
VLANSEP is “1” (On/Enabled)	**AND** the Avaya A175 is not tagging frames, **OR** if the Avaya A175 is tagging frames with a VLAN ID equal to PHY2VLAN, **OR** if the PHY2VLAN value is zero.	Frames forwarded to the network from the secondary Ethernet interface will not be changed before forwarding. Tagging is not added or removed and the VLAN ID and priority does not change for frames received on the secondary interface. Tags are still removed for frames that egress from the secondary interface. The Ethernet switch forwarding logic determines whether frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the Avaya A175 without regard to specific VLAN IDs or the existence of tags.

1 of 2

Table 13: VLAN Separation Rules (continued)

If		Then
VLANSEP is “0”,	**OR** the Avaya A175 is not tagging frames, **OR** the Avaya A175 is tagging frames with a VLAN ID equal to PHY2VLAN.	Frames forwarded to the network from the secondary Ethernet interface will not be changed before forwarding. Tagging is not added or removed and the VLAN ID and priority does not change for frames received on the secondary interface. Tags are still removed for frames that egress from the secondary interface. The Ethernet switch forwarding logic determines whether frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the Avaya A175 without regard to specific VLAN IDs or the existence of tags.
		2 of 2

Avaya A175 Customizable Parameters

Table 14 lists:

- the parameter names,
- their default values,
- the valid ranges for those values, and
- a description of each parameter.

Table 14 is a comprehensive list of all the parameters you can configure. However, you do not have to set every parameter. In most cases, you will include only those parameters in the settings file that are specific to your own environment and let the devices use the default values for the remaining ones.

Note:

> At a minimum, be sure to set these important SIP-related parameters: SIP_CONTROLLER_LIST, SIPDOMAIN, SNTPSRVR, ENABLE_PRESENCE, GMTOFFSET, DSTOFFSET, DSTSTART, and DSTSTOP.

For DHCP, the DHCP Option sets certain parameters to the desired values as discussed in DHCP and File Servers on page 75. For HTTP, the parameters in Table 14 are set to desired values in the script (Axxxsettings) file. For more information on working with the settings file, see Contents of the Settings File on page 109.

Avaya recommends that you administer options on the Avaya A175 devices using script files. This is because some DHCP applications have limits on the amount of user-specified information. The administration required can exceed those limits for the more full-featured devices.

Some parameters can be changed using the local administrative (Craft) procedures. For example, you might choose to completely disable the capability for users to enter or change option settings from the Avaya A175 using local administrative (Craft) procedures. You can set the system value, PROCPSWD, as part of standard DHCP/HTTP administration. If PROCPSWD is non-null and consists of 1 to 7 digits, a user cannot access the Administrator Options and perform local administrative procedures from the Avaya A175.

⚠ **Important:**

PROCPSWD is likely stored on the server “in the clear” and is sent to the Avaya A175 in the clear. Therefore, do not consider PROCPSWD as a high-security technique to inhibit a sophisticated user from obtaining access to local procedures.

Administering PROCPSWD limits access to all local procedures.

Note:

There are several ways to change configuration parameters, for example, using DHCP options, the Axxxsettings file, or using local administrative (manual) procedures, and a specific procedure exists to determine which value the Avaya A175 should use. Parameter Data Precedence on page 45 describes the order in which parameter values are determined.

Table 14: Avaya A175 Customizeable System Parameters

Parameter Name	Default Value	Description and Value Range
ASTCONFIRMATION	32	Sets the time that the device waits to validate an active subscription when it SUBSCRIBES to the "avaya-cm-feature-status" package. Valid values are 16 - 3600 (seconds).
AUTH	0	Authentication flag for settings file download. Values are: 0=secure setting file download is not required 1=secure setting file download is required
CONFERENCE_SERVER_ ADDRESS	" " (Null)	Text string containing the conferencing server IP address. Valid values are 0 or IP address in dotted decimal format.
CONFIG_SERVER_ SECURE_MODE	1	Indicates whether or not secure communication via HTTPS is required to access the configuration server. 0 = Use HTTP. 1 = Use HTTPS. 2 = Use HTTPS if SIP transport mode is TLS; otherwise, use HTTP.
CONTROLLER_SEARCH_ INTERVAL	4	Time in seconds that the device waits to complete the maintenance check for monitored controllers. Valid values are 4 - 3600 (seconds).

1 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DAYLIGHT_SAVING_ SETTING_MODE	2	Controls daylight saving setting. Values are: 0=daylight saving time is deactivated (no offset to local time) 1=daylight saving time is activated (offset to local time as configured in "DSTOFFSET") 2=the device switches automatically to daylight saving time and back according to the contents of "DSTSTART" and "DSTSTOP".
DIRBNTUSERDOMAINID	ntuserdomainid	Specifies the directory network user domain ID field. The default is **ntuserdomainid**.
DIRCOMPANYNAME	companyname	Specifies the directory company name field.
DIRFIRSTNAME	givenname	Specifies the directory first name field. The default is **givenname**.
DIRFULLNAME	cn	Sets the default LDAP search value. The Avaya A175 only supports searches on names.
DIRLASTNAME	sn	Specifies the directory last name field.
DIRLDAPPORT	389	The TCP port number of the LDAP directory server.
DIRLOCATION	l	Specifies the directory location field.
DIRMAIL	mail	Specifies the directory mail field.
DIRMOBILE	mobile	Specifies the directory mobile number field.
DIRSRCHTIME	5	Sets the directory search time (in seconds). Valid values are 1-60.
DIRSRVR	" " (Null)	IP address of the LDAP directory server. Valid values are zero or more IP addresses in dotted-decimal or DNS format separated by commas without intervening spaces. Maximum is 255 ASCII characters.
DIRTELNUM	telephonenumber	Specifies the directory telephone number field.
DIRLTOPDN	" " (Null)	The directory topmost distinguished name. You must set this value to a non-null value to enable the LDAP application. You should set DIRTOPDN to the LDAP root entry.
DISPLAY_NAME_ NUMBER	0	Indicates whether the calling party's number will be displayed next to the caller name on an incoming call. If this parameter is not set, only the caller name is shown. Valid values are: 1 = Show caller's name and number. 0 = Show caller's name only.
DNSSRVR	0.0.0.0	Text string containing the IP Address of zero or more DNS servers, in dotted-decimal format, separated by commas with no intervening spaces (0-255 ASCII characters, including commas).

2 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DOMAIN	" " (Null)	Text string containing the domain name to be used when DNS names in system values are resolved into IP Addresses. Valid values are 0-255 ASCII characters.
DSCPAUD	46	Differentiated Services Code Point for audio. Values range from 0 to 63.
DSCPSIG	34	Differentiated Services Code Point for signaling. Values range from 0 to 63.
DSCPVID	26	Sets the DiffServ value for video streams from the device. Valid values are 0 - 63.
DSTOFFSET	1	Used for daylight saving time calculation in hours. Values range from 0 to 2.
DSTSTART	2Sun Mar2L	Used to identify start date for automatic change to Daylight Saving Time. Default string length with a format of either *odddmmmht* or *Dmmmht*, where: *o* = one character representing an ordinal adjective of "1" (first), "2" (second), "3" (third), "4" (fourth) or "L" (last) *ddd* = 3 characters containing the English abbreviation for the day of the week *mmm* = 3 characters containing the English abbreviation for the month *h* = one numeric digit representing the time to make the adjustment, exactly on the hour at hAM (0h00 in military format), where valid values of h are "0" through "9" *t* = one character representing the time zone relative to the adjustment where "L" is local time and U is universal time *D* = one or two ASCII digits representing the date of the month from "1" or "01" to "31", or the character "L", which means the last day of the month)

3 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DSTSTOP	1SunNov2L	Used to identify stop date for automatic change to Daylight Saving Time. Default string length with a format of either *odddmmmht* or *Dmmmht*, where: *o* = one character representing an ordinal adjective of "1" (first), "2" (second), "3" (third), "4" (fourth) or "L" (last) *ddd* = 3 characters containing the English abbreviation for the day of the week *mmm* = 3 characters containing the English abbreviation for the month *h* = one numeric digit representing the time to make the adjustment, exactly on the hour at hAM (0h00 in military format), where valid values of h are "0" through "9" *t* = one character representing the time zone relative to the adjustment where "L" is local time and U is universal time *D* = one or two ASCII digits representing the date of the month from "1" or "01" to "31", or the character "L", which means the last day of the month)
DTMF_PAYLOAD_TYPE	120	RTP dynamic payload used for RFC 2833 signaling. Range is 96 to 127.
ENABLE_AUTOMATIC_ON_THE_PHONE_PRESENCE	1	Enable/disable automatic on the phone presence status update when the user goes on/off hook. Values are: 0 = disabled 1 = enabled
ENABLE_EARLY_MEDIA	1	Flag that indicates if SIP early is enabled. If enabled and 18x progress message includes early SDP, Spark uses that information to open a VoIP channel to the far-end before the call is answered. Values are 0=disabled; 1=enabled.
ENABLE_G711A	1	Enable or disable G711A codec capability of the device. If the parameter is set to 1, the device includes G711A capability in an outbound INVITE request, and accepts G711A when received in an incoming INVITE request. Values are 0=disabled; 1=enabled.
ENABLE_G711U	1	Enable or disable G711U codec capability of the device. If the parameter is set to 1, the device includes G711U capability in an outbound INVITE request, and accepts G711U when received in an incoming INVITE request. Values are 0=disabled; 1=enabled.

4 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
ENABLE_G722	0	Enable or disable G722 capability of the device. If the parameter is set to 1, the device includes G722 capability in an outbound INVITE request, and accepts G722 when received in an incoming INVITE request. If set to 0, processing of G722 as a capability is disabled. Values are 0=disabled, off; 1=enabled, on.
ENABLE_G726	1	Enable or disable G726 capability of the device. If the parameter is set to 1, the device includes G726 capability in an outbound INVITE request, and accepts G726 when received in an incoming INVITE request. Values are 0=disabled, off; 1=enabled, on.
ENABLE_G729	1	Enable or disable G729A codec capability of the device. Values are: 0=G.729 disabled. If set to 0, processing of G729A as a capability is disabled. 1 = The device advertises a preference for "G.729(A) enabled, without Annex B support" in an outbound INVITE request, and accepts either G729A or G729A with annex B support [G.729AB] when received in a 200OK response or an incoming INVITE request. If set to 1, Incoming INVITE request: the device accepts either G729(A) or G729AB. 2 = The device advertises a preference for "G.729(A) enabled, with Annex B support [G.729AB]"in an outbound INVITE request, and accepts either G729A or G729AB when received in a 200OK response or an incoming INVITE request. If the parameter is set to 2, Incoming INVITE request: the device accepts either G729A or G729AB.
ENABLE_PRESENCE	0	Enable or disable complete Presence functionality. If disabled, Presence icons do not show in Contacts or Call History Lists, Presence is not displayed to the user, incoming Presence updates are ignored, and menu items of User Interface to set Presence options are not displayed (if available). Values are 0=disabled, off; 1=enabled, on.

5 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
ENHDIALSTAT	1	Enhanced Dialing Status. Valid range is 0 to 2. If set to “0” the feature is turned off. If set to “1” it is partially enabled (dialing rules do not apply for dialing from Contacts). If set to “2”, the Setting the Date and Time on Avaya A175 Devices feature is fully enabled (dialing rules also apply for dialing from Contacts). Note that If CTDC_SUPPORT is enabled, Enhanced Local Dialing is automatically disabled, independent of the actual setting of ENHDIALSTAT. If CTDC_SUPPORT is disabled, Enhanced Local Dialing is processed as defined by ENHDIALSTAT.
FAILBACK_POLICY	"auto"	The policy in effect for recovery from Failover. Valid values are: "admin" = If set to admin, the device waits for administrative intervention before attempting to failback to a higher priority controller. "auto" = If set to auto, the device periodically checks the availability of the primary controller and fails back to it if it is available. Note: If set via the settings file this value is given a precedence of 4. If set via PPM in the ListOfMaintenanceData element of the getAllEndpointConfigurationResponse this value is given a precedence of 5.
FAILED_SESSION_ REMOVAL_TIMER	30	Timer to automatically remove a failed call session. Range in seconds is 5 to 999.
FAST_RESPONSE_ TIMEOUT	4	The value of the Fast Response Timer for Failover. Valid values are: 0 - 32 (seconds). Note: If set via the settings file this value is given a precedence of 4. If set via PPM in the ListOfMaintenanceData element of the getAllEndpointConfigurationResponse this value is given a precedence of 5.
FAST_RESPONSE_TIMEOUT	4	Provides ability to configure the fast response timer. Valid values are 0 - 32 (seconds). When it is set to 0, the timer is disabled. When it is set to any value from 1 - 32, the timer will be started for the set value. The timer terminates INVITE transactions if no SIP response is received within a specified number of seconds after sending the request.
G726_PAYLOAD_TYPE	110	RTP dynamic payload used for G.726. Range is 96 to 127.

6 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
GMTOFFSET	0:00	Offset used to calculate time from GMT reference time. Default string length positive or negative number of hours and minutes less than 13 hours. Consists of 1 to 6 characters, optionally beginning with "+" or "-", followed by one or two number digits whose combined value is from "0" to "12" optionally followed by a ":" and two numeric digits whose combined value is from "00" to "59".
HTTPDIR	" " (Null)	HTTP server directory path. The path name prepended to all file names used in HTTP and HTTPS get operations during initialization/HTTP downloads. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required. The command syntax is "GET HTTPDIR *myhttpdir*" where "myhttpdir" is your HTTP server path. HTTPDIR is the path for all HTTP operations.
HTTPEXCEPTION DOMAINS	" " (Null)	Domains to be excluded for SCEP. String representing zero or one domains in a URL of 0 to 255 characters in dotted decimal or DNS name format with multiple domains delimited by commas.
HTTPPORT	80	Destination TCP port used for requests to the HTTP server during initialization. Range is 0 - 65535.
HTTPPROXY	" " (Null)	Zero or one IP or DNS address of the HTTP server for SCEP. 0 to 255 characters in dotted decimal or DNS name format followed by a colon and port number. The colon and port number are optional. If this parameter is not null, this (proxy) transport address is used to set up the HTTP connection as the transport protocol for SCEP.
HTTPSRVR	0.0.0.0	List of IP Address(es) or DNS Name(s) of HTTP file server(s) used to download device files. HTTP server addresses can be in dotted decimal or DNS format, and must be separated by commas (0-255 ASCII characters, including commas).
INGRESS_DTMF_VOL_ LEVEL	-12	RFC 2833 Digit event "volume" level. The power level of the tone, expressed in dBm0 after dropping the sign. (from RFC 2833 section 3.5 "Payload Format." Values are: -20 to -7.
INSTANT_MSG_ENABLED	0	Enable/disable Instant Messaging function. Values are: 0 = disabled 1 = enabled

7 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
INSTANT_MSG_IDENTITY_ QUERY_TIMEOUT	5	Sets the time (in seconds) for the Query Subscription Timeout. This is the number of seconds to wait for a NOTIFY response for a Presence SUBSCRIBE query. Valid values are 1 - 10 (seconds).
INTER_DIGIT_TIMEOUT	5	This is the timeout that takes place when user stops inputting digits. The timeout is treated as digit collection completion, and when it occurs, the application sends out an invite. Range in seconds of 1 to 10.
L2Q	0	Requests 802.1Q tagging mode (auto/on/off). Values are: 0 = auto 1 = on 2 = off
L2QAUD	6	Layer 2 audio priority value. Range from 0 to 7.
L2QSIG	6	Layer 2 signaling priority value. Range from 0 to 7.
L2QVID	5	Layer 2 priority value for video packets from the device. Range from 0 to 7.
L2QVLAN	n/a	802.1Q VLAN Identifier (0 to 4094). Null (" ") is not a valid value and the value cannot contain spaces. This parameter is preserved in RAM which survives reset and stored to flash (as L2QVLAN_INIT) only upon successful registration. This value is initialized from L2QVLAN_INIT after power-up. This value will not be initialized from L2QVLAN_INIT after reset, but can be modified using the ADDR craft procedure.
LOCAL_LOG_LEVEL	3	Numerical code of severity level. Store entries to the local event log, if event occurs with a severity level whose numerical code is equal to or less than the LOCAL_LOG_LEVEL value. Values are: 0 (emergencies), 1 (alerts), 2 (critical), 3 (errors), 4 (warning), 5 (notice), 6 (informational), 7 (debug).
LOG_CATEGORY		Comma-separated list of keywords in standard string format representing logging categories (software modules or functions to be included in lower level logging). Logging implementation blocks all traces at level "Warning" or lower, unless the category corresponding to a given trace is enabled. If the LOCAL_LOG_LEVEL is set to "Warning" or lower, this parameter would enable low-level traces from the adaptors or manager as indicated. Applies to all logging mechanisms (syslog and local log). Example: "ALSIP, SESSION" enables debug level traces from the ALSIP adaptor and Session manager.

8 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
LOGSRVR	" " (Null)	Syslog server IP or DNS address. 0 to 255 characters: zero or one IP Addresses in dotted decimal or DNS name format.
MSGNUM	" " (Null)	Voice mail system telephone/extension number. Used for non-failover situations. Specifies the number to be dialed automatically when the device user presses the **Message** button. Note: Set via the following mechanisms in precedence order (highest to lowest); PPM, settings file and DHCP.
MTU_SIZE	1500	Maximum Transmission Unit size. Range is 1496 or 1500 only octets.
NO_DIGITS_TIMEOUT	20	Number of seconds of delay after going "off-hook" or getting secondary dial tone before device automatically plays a warning tone and does not accept dial input any longer. Range in seconds is 1 to 60.
OUTBOUND_ SUBSCRIPTION_ REQUEST_DURATION	86400	Number of seconds used in initial SUBSCRIBE messages. This is the suggested duration value of the device, which might be lowered by the server, depending on the server configuration. Range is 60-31536000. Note that the default value is equal to one day and the maximum value represents one year.
PASSWORD_POLICY_ALPHA NUMERIC_PASSWORD	2	Specify whether the unlock password shall include alphanumeric characters. Values are: 0 = Do not enforce password complexity (that is, anything is allowed). 1 = Digits-only is enforced. 2 = Alphanumeric is enforced. 3 = Both alphanumeric and special characters are enforced. The Avaya A175 chooses the more secure setting between the value you specify here and ActiveSync.
PASSWORD_POLICY_ENABL E_PASSWORD	0	Enables/disables the lock out mechanism. Values are: 0 = off 1 = on
PASSWORD_POLICY_INACTI VITY_LOCK_TIMEOUT	60	Controls the inactivity lockout timer. Valid values are 1 - 1440 minutes.
PASSWORD_POLICY_PASSW ORD_FAILED_ATTEMPTS	8	Controls the number of failed attempts before the device is locked out.

9 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PASSWORD_POLICY_PASSWORD_FAILED_ATTEMPTS_ENABLE	0	Specify whether to track the number of failed attempts to enter the unlock password. Values are: 0 = Disables tracking of failed password attempts. 1 = Enables tracking of failed password attempts.
PASSWORD_POLICY_PASSWORD_LENGTH	6	Specifles the length of the unlock password. The Avaya A175 chooses the more secure setting between the value you specify here and ActiveSync.
PHNEMERGNUM	" " (Null)	If set, the number dialed when the Emergency button is touched, or when a pop-up screen for making an emergency call is confirmed.
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 device 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.”
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. Range: 1 digit (0 to 9) or " " (Null). Needed for "Enhanced Local Dialing Algorithm".
PHNLDLENGTH	10	Length of national telephone number. The number of digits in the longest possible national telephone number. Range: 5 to 15. Needed to for "Enhanced Local Dialing Algorithm".
PHNOL	9	Outside line access code. The character(s) dialed, including # and *, if any, to access public network local trunks. Range: 0-2 dialable numeric digits, including " " (Null).

10 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PHY1STAT	1	Ethernet line interface setting (1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex, and 6=1Gbps full-duplex if supported by the hardware). Speed and duplex issues are summarized and the best practice is provided in the *Avaya Application Solutions: IP Telephony Deployment Guide*, Document Number 555-245-600 Issue 6, January 2008 on page 290. This document is available from the Avaya support website.
PHY2PRIO	0	Layer 2 priority value for frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is "1" (enabled). Values are from 0-7 and correspond to the drop-down menu selection.
PHY2STAT	1	Secondary Ethernet interface setting (0=Secondary Ethernet interface off/disabled, 1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex), and 6=1Gbps full-duplex (if supported by the hardware). Speed and duplex issues are summarized and the best practice is provided in the *Avaya Application Solutions: IP Telephony Deployment Guide*, Document Number 555-245-600 Issue 6, January 2008 on page 290. This document is available from the Avaya support website.
PHY2VLAN	0	VLAN identifier used by frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is “1” (enabled). Value is 1-4 ASCII numeric digits from “0” to “4094.” Null is not a valid value, nor can the value contain spaces.
PRESENCE_SERVER	" " (Null)	The address and optional port of a single Presence Server. Used to access a server for presence indications. In some environments the address of the SIP proxy/registrar may be different than the presence server; in this case the presence server is set via this parameter. If both addresses are the same, it is not necessary to set PRESENCE_SERVER (shall remain null). Valid values are 0 to 255 characters: one IP address in dotted decimal or DNS name format, with an optional port (separated from the address by a colon).
PRESENCE_XMPP_PORT	5222	Sets the TCP port used for the Presence server. Valid values are 0 - 65535.

11 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PROCPSWD	27238	Text string containing the local (dialpad) procedure password (Null or 1-7 ASCII digits). If set, password must be entered immediately after accessing the Craft Access Code Entry screen, either during initialization or when Mute (or Contacts 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	Controls access to Craft local (dialpad) administrative procedures. Values are: 0 = Full access to craft local procedures 1 = restricted access to craft local procedures
RDS_INITIAL_RETRY_ ATTEMPTS	15	Indicates how many times the PPM adaptor should try to download from PPM before giving up on connecting to the PPM server. Values are: 1-30.
RDS_INITIAL_RETRY_ TIME	2	Remote Data Source initial retry time in seconds; indicates the initial delay for a retry to connect to the PPM server. Valid range is 2-60 (seconds).
RDS_MAX_RETRY_TIME	600	Remote data source maximum retry time; indicates the maximum delay interval (in seconds) before giving up on PPM server connection. Values are: 2-3600 (seconds).
RECOVERYREGISTER WAIT	60	Reactive monitoring interval in seconds for Failover. Valid values are: 10 - 36000 Note: If set via the settings file this value is given a precedence of 4. If set via PPM in the ListOfMaintenanceData element of the getAllEndpointConfigurationResponse this value is given a precedence of 5.
REGISTERWAIT	900	Number of seconds for next re-registration to SIP server. The default value is 900 seconds UDP arrangements can be handled by setting the value of the parameter to a lower value in the settings file. Range in seconds: 30 to 86400.
RTCPCONT	1	Enables/disables the RTCP in parallel to RTP audio streams. Values are 0=RTCP disabled, 1=RTCP enabled.
RTP_PORT_LOW	5004	Specifies lower limit of a port range to be used by RTP/RTCP or SRTP/SRTCP connections, for example, to adapt to firewall traversal policies. Values: 1024-65503.

12 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
RTP_PORT_RANGE	40	Specifies the width of the port range to be used by RTP/RTCP or SRTP/SRTCP connections, for example, to adapt to firewall traversal policies. The upper limit is calculated by the value of RTP_PORT_LOW plus the value of RTP_PORT_RANGE, taking into consideration the overall limit of 65535. Values: 32-64511.
SEND_DTMF_ TYPE	2	Defines whether DTMF tones are send in-band (regular audio) or out-band (negotiation and transmission of DTMF according to RFC 2833, with fallback to send in-band DTMF tones, if far end does not support RFC2833). Values are 1=in-band DTMF; 2=RFC2833 procedure.
SIG_PORT_LOW	1024	Lower limit of port range for signaling to support by the phone. Values range from 1024 to 65503.
SIG_PORT_RANGE	64511	Port range for signaling to support by the device. Values range from 32 to 64511.
SIMULTANEOUS_ REGISTRATION	3	The number of Session Managers in the configuration with which the device will simultaneously register. Valid range is 1 through 3.

13 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SIP_CONTROLLER_LIST	" " (Null)	List of SIP proxy/registrar server IP or DNS address(es). Server(s) used to address SIP registrations and signaling, if operating in proxy mode (in case of several entries first address always first, etc.). When operating in an Avaya Environment SIP_CONTROLLER_LIST is also used to access Personal Profile Manager (PPM). This parameter is considered the list of "Configured Controllers" for Failover logic. When this parameter has multiple IP Addresses, the ordering of the list defines the priority of the controllers for selection during Failover; the first element of the list is the highest priority, the last element is the lowest priority. For information on Failover, see Chapter 10: Administering Avaya A175 Desktop Video Device Options. Format: host[:port][;transport=xxx] where *host* is an IP address in dotted decimal format or DNS name, *port* is the optional port number (if not specified, the default port value of 5060 for UDP and TCP or 5061 for TLS is used), *transport* is the optional transport type (where *xxx* is tls, tcp, or udp) and if not specified, the default value of TLS is used. The first element of this parameter (if applicable) has the highest precedence within the parameter. This parameter can have 0 to 255 characters indicating zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.
SIPDOMAIN	" " (Null)	SIP domain name for registration. 0 to 255 characters: string representing domain name.
SIPREGPROXYPOLICY	"alternate"	SIP registration proxy policy. A policy to control how the device treats the list of controllers/servers in the SIP_CONTROLLER_LIST parameter. Valid values are: "alternate" = This is the preferred registration method with SIP proxy controllers. If there is no Active Controller, then all Configured Controllers are Monitored Controllers. If there is an Active Controller, the Monitored Controllers are all controllers whose priority is higher than the current Active Controller. "simultaneous" = All controllers in the configured controller list are Monitored Controllers.

14 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SNMP_ENABLE	0	Enable/disable device SNMP agent. Values are: 0 = disable (default) 1 = enable SNMPv1 and v2 only 2 = enable SNMPv3 only
SNMPSTRING	" " (Null)	Text string containing the SNMP community name string (up to 32 ASCII characters, no spaces).
SNMP_V3_AUTH_PASSWORD	" " (Null)	Represents the R/O SNMPv3 authentication password. This value must be set to enable viewing of the device’s MIB using SNMPv3.
SNMP_V3_ENCRYPT_ PASSWORD	" " (Null)	Represents the R/O SNMPv3 encryption password. This value must be set to enable viewing of the device’s MIB using SNMPv3.
SNMP_V3_USERNAME	" " (Null)	Represents the R/O SNMPv3 username. This value must be set to enable viewing of the device’s MIB using SNMPv3.
SNTPSRVR	" " (Null)	Used to retrieve date and time via SNTP (in case of several entries first address always first, etc.). Zero to 255 characters: zero or more IP Addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.
SUBSCRIBE_SECURITY	2	Controls the use of SIP and SIPS subscriptions. Valid values are 0 - 2: If=0, the device uses SIP for both the Request URI and the Contact Header regardless of whether SRTP is enabled. If=1, the device uses SIPS for both the Request URI and the Contact Header if SRTP is enabled (TLS is on and MEDIAENCRYPTION has at least one valid crypto suite). If=2 and the PPM does not show a FS-DeviceData FeatureName with a FeatureVersion of 2 in the response to the getHomeCapabilities request, the device uses SIP for both the Request URI and the Contact Header. If=2 and the PPM does show a FS-DeviceData FeatureName with a FeatureVersion of 2 or greater in the response to the getHomeCapabilities request, the device uses SIPS for both the Request URI and the Contact Header if SRTP is enabled (TLS is on and MEDIAENCRYPTION has at least one valid crypto suite).
TCP_KEEP_ALIVE_ INTERVAL	10	Time interval (number of seconds) after which TCP keep-alive packets are re-transmitted. The interval is started by the system TCP/IP stack (when TCP keep-alive is enabled with specified time intervals). Values are 5-60 seconds.

15 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
TCP_KEEP_ALIVE_ STATUS	1	Indicates whether TCP/IP keep-alive should be enabled at the system. Values are 0=TCP keep alive disabled, 1=TCP keep alive enabled.
TCP_KEEP_ALIVE_TIME	60	This time interval is the time the Avaya A175 will wait before sending out a TCP keep-alive message (TCP ACK message) to the far-end. The time is controlled by the system's TCP/IP stack. The timer is restarted after application level data (for example, a SIP message) is sent over the socket. When the system is idle, this keep-alive time expires and results in sending a TCP ACK (keep-alive) packet. Valid values are 10-3600 (seconds).
TLSSRVRID	1	Flag to indicate if TLS server identification is required. Valid values are: 0 = no certificate match necessary; TLS/SSL connection will be established anyway. 1 = certificate match required; TLS/SSL connection will only be established if the server's identity matches the server's certificate.
TRUSTCERTS	" " (Null)	File names of certificates to be used for authentication. List of file names separated by commas (0 to 1024 characters).
USE_QUAD_ZEROS_ FOR_HOLD	0	Flag that indicates whether a= directional attributes or 0.0.0.0 IP Address is used in the SDP to signal hold operation. 0=use “a= directional attributes”, 1=use quad zeros.
VIDEO_ENABLE_H263	1	Determines whether the H.263 codec is available on the device. 0 = No. 1 = Yes.
VIDEO_ENABLE_H264	1	Determines whether the H.264 codec is available on the device. 0 = No. 1 = Yes.
VLANSEP	1	Enables or disables VLAN separation. Controls whether frames received from the line interface are forwarded to the phone or to the secondary Ethernet interface based on VLANID. Also affects whether frames received on the secondary Ethernet interface are changed before forwarding to the line interface. Values are: 1=On/Enabled, 0= Off/Disabled. This parameter is used with several related parameters. For more information, see VLAN Separation on page 129.

16 of 17

Table 14: Avaya A175 Customizeable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
VLANTEST	60	Number of seconds to wait for a DHCPOFFER when using a non-zero VLAN ID (1-3 ASCII digits, from “0” to “999”).
WAIT_FOR_ REGISTRATION_TIMER	32	Time in seconds the SIP application will wait for a register response message. If no message is received, registration is retried. Range is 4-3600 (seconds).
WAIT_FOR_ UNREGISTRATION_ TIMER	32	Time the SIP application waits before declaring un-registration to be complete. Under normal circumstances un-registration includes termination of all active SIP dialogs, and SIP registration. Range is 4-3600 (seconds).

17 of 17

Local Administrative (Craft) Options Using the Avaya A175 User Interface

Chapter 3 details how to use local (Craft) procedures at the user interface for administration. The local procedures you might use most often as an administrator are:

- **Ethernet Settings** - Static address programming.
- **Debug** - Enable or disable debug mode for the device.
- **Group** - Set the group identifier on a per-device basis.
- **Interface** - Locally enable or disable the secondary Ethernet hub.
- **Reset** - Remove all administered values, user-specified data, option settings, etc. and return an Avaya A175 to its initial “out of the box” default values
- **Reboot** - Restart the Avaya A175 in response to an error condition, including the option to reset system values.
- **SIP Global Settings** - Configure SIP call settings.
- **View settings**- Review the system parameters for the device to verify current values and file versions.

Chapter 11: System Failover and Survivability

This chapter provides general administrative and detailed information about failover, transition, and failback.

SIP Software Releases and Survivability

Avaya A175 software provides support for simultaneous calls from multiple servers to accommodate situations that can occur due to network or server failures. This release also ensures that contact data is preserved and actionable during failover transition. Additionally, Avaya A175 software adds support for the following secondary gateways:

- Juniper ISR
- Avaya Secure Routers

Avaya A175 devices fail over to a secondary controller for alternate registration (Session Manager (SM) failover to a non-AST controller). Simultaneous registration occurs between SMs/BSM (Branch Session Manager) as opposed to alternate registration from SM to a non-AST controller.

Avaya A175 software supports Contact caching and caching limits in a Session Manager environment. Multiple operations on a cached contact are not allowed. Avaya 175 software also supports preserved media connections/calls.

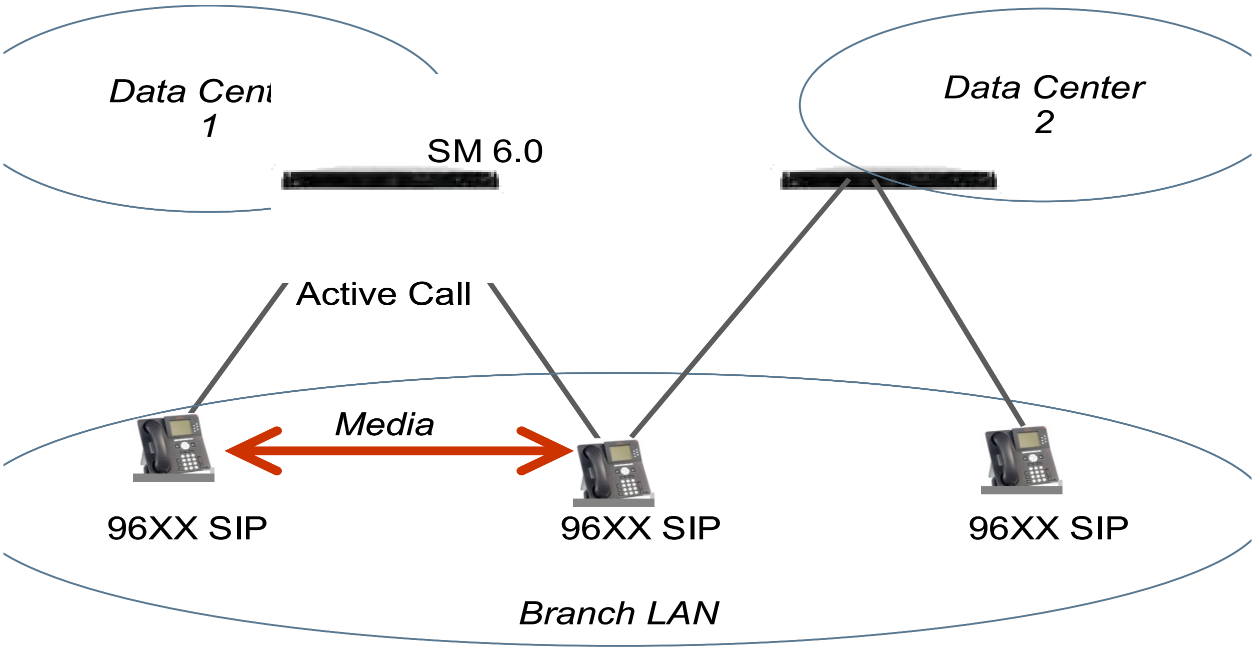
With SM and non-AST controllers, the PPMs are in sync and the data is sent to the PPM; data is cached only in case of failure.

SIP Survivability Configuration Examples

Several survivability configurations are available, depending on your controller and system management environment, as shown in the illustrations that follow.

Avaya A175 Configuration Example:

Avaya A175 offers simultaneous registration with multiple controllers, and improved feature availability during and after failover to a secondary controller.



Hardware/Software Requirements

- Supported local (secondary) gateway with Proxy or B2BUA capabilities.

Provisioning Survivability for Avaya A715

The following steps provide a brief overview of the provisioning process:

1. Set the applicable failover configuration parameters (described in Survivability Configuration) in the Axxxsettings file.
2. Provision the gateway per the Application Notes, available on the Avaya support Web site.
3. Load the Avaya A175 firmware and associated files on the file server.
4. Reboot all registered Avaya A175 devices.

Survivability Configuration

Avaya recommends using the settings file instead of SM to set these parameters. Avoid mixed sources for configuration of SIP servers.

By administering survivability configuration parameters using the Axxxsettings file (or using the default values if applicable), the Avaya A175 devices can quickly switch to an active controlling server and experience minimal disruption. The failover/failback parameters, described in detail in Table 14: Avaya A175 Customizeable System Parameters, are:

- CONTROLLER_SEARCH_ INTERVAL - The time the Avaya A175 waits to complete the maintenance check for Monitored Controllers.
- FAILBACK_POLICY - Failback Policy.
- FAST_RESPONSE_ TIMEOUT - Fast Response Timer.
- RECOVERYREGISTER WAIT - Reactive Monitoring Interval in seconds.
- REGISTERWAIT - Proactive Monitoring Interval in seconds.
- SIP_CONTROLLER_LIST - Configured Controller list. A comma-separated list of SIP URIs, a hostname, or numeric IP address. If null, DHCP/DNS will provide the defaults.
- SIPREGPROXYPOLICY - Registration Policy.

Note:

The survivability parameters can be provisioned in the Axxxsettings.txt file, but Personal Profile Manager values will take precedence over values in the Axxxsettings.txt file.

Setting a Controller via the User Interface

Survivability parameters can be provisioned via the Avaya A175 user interface. When setting survivability parameters, consider these points:

- The SIP proxy settings screen shows the SIP proxy server addresses (or DNS names) from the list of configured controllers in descending priority from top to bottom. Note that duplicate entries are removed from the list of configured controllers.
- If the administrator clears the controllers in the setting file, the only way to clear the values that are displayed on the SIP proxy screen that are downloaded from PPM is to clear the values on the Avaya A175.
- If no controller has been set, a controller can be set via the Administrator options (local administrative (Craft) procedures). The user can log in successfully with a controller at this point.

Controller Determination and Survivability Activity

The Avaya A175 performs controller determination and verification after a successful user login. The Avaya A175 then periodically performs failover checks. The steps are:

1. Determine Controllers to Monitor

The list of controllers to monitor is built from the Configured Controller(s) list using the SIPREGPOLICY parameter setting as a guide. The list of SIP Proxies/Registrars can be obtained from the network DHCP servers, retrieved from the Axxxsettings file, retrieved from a PPM (Personal Profile Manager), or configured via the Avaya A175 user interface. Similarly, the administrative/automatic failback parameters and the monitoring intervals might be obtained via the Axxxsettings file, the PPM, or the Avaya A175 device’s user interface.

The priority order in which the list is obtained is as follows:

1. Avaya A175 user interface (set using local administrative (Craft) procedure)
2. PPM
3. Settings file
4. DHCP (Option 242)

Each of these sources might provide a list of controllers (servers). The contents of each one of these lists is assumed to be in priority order.

2. Determine which Monitored Controllers are Available

Using the Monitored Controllers list, the Avaya A175 performs DNS queries to resolve hostnames and the signaling protocol (TLS, TCP, UDP in that order when no DNS NAPTR or SIP URI parameter is located). To determine which of the Monitored Controllers is actually available to provide service, the device performs a maintenance activity for each Monitored Controller. The Avaya A175 starts the controller search timer and sends a SIP REGISTER (adding bindings) message to each controller, which may necessitate establishing a TLS or TCP connection to the controller.

The controller is considered available once a 200 OK response is received in response to the REGISTER request. Once a controller has been marked as available, the Avaya A175unregisters from the controller. If all the Monitored Controllers are available before the end of the CONTROLLER_SEARCH_INTERVAL the device continues with selecting the Active Controller. If at least one Monitored Controller is available at the end of the CONTROLLER_SEARCH_INTERVAL, the device continues determining which controllers are available.

If a failure response to the REGISTER request is received, the controller is considered unavailable and depending on the failure code, either retries the query, provides the requested credentials, abandons the query, or stops monitoring this specific controller entirely.

If no response to the REGISTER request is received within the timeout period, the device retries the monitoring attempt using the RECOVERYREGISTERWAIT parameter value as a guideline.

3. Select the Active Controller

If the value of the SIPREGPROXYPOLICY parameter is "alternate" and a user is logged in, the device must attempt and maintain a single active SIP registration with the highest priority Available Controller. The device attempts to register using the username and password provided during the login process. It also uses the SIPDOMAIN parameter. The Avaya A175 uses a SIP URI unless SRTP is enabled where a SIPS URI is used. When registration is successful, the device sets the SIPPROXYSRVR_IN_USE parameter to the IP address of this (Active) Controller. The device also performs the other registration tasks.

If the value of the SIPREGPROXYPOLICY parameter is "simultaneous" and a user is logged-in, the device attempts and maintains active SIP registrations with all Available Controller(s).

If the value of the FAILBACK_POLICY parameter is "automatic", the device’s active controller will always be the highest priority available controller. If the value of the FAILBACK_POLICY parameter is "admin", then a controller lower down the priority list may be active.

The device initiates a search for a new Active Controller whenever one of the following triggers is encountered:

- Fast Response Timer Expiry,
- TCP keep-alive failure (or other socket error),
- If the FAILBACK_POLICY parameter is set to "admin" and the device receives an administrative failback trigger,
- An incoming INVITE is received from a non-Active controller,
- A re-registration with the Active Controller times out, or

Whenever one of these triggers is encountered and a user is logged in, the Avaya A175 initiates parallel REGISTER transactions with every controller in its configured list, including the currently active controller.

4. AST Feature Determination

After the Active controller has been selected, the Avaya A175 determines if that controller supports the AST (Advanced SIP Telephony) feature set or not. The device sends a SUBSCRIBE request to the active controller for the "Feature Status Event Package" (avaya-cm-feature-status). If the request succeeds, the device proceeds with PPM Synchronization. If the request is either rejected, is proxied back to the device, or does not receive a response, the Avaya A175 assumes that AST features are not available.

If AST is not supported, the Avaya A175 operates in a mode where AST features are not available.

Failover/Failback Behavior

System Performance

The survivability characteristics of the system as a whole are dependant on the configuration and behaviors of all the SIP network elements such as phones and proxy servers as well as the traditional network elements like routers and DNS servers. The endpoint detects a failure within approximately 90 seconds of the time the failure occurs when TCP or TLS connections are used. Once a failure has been detected, the endpoint completes its selection of an ‘Active’ controller within approximately 5 seconds.

With simultaneous registration, available in a multiple SM environment, both failover/failback transition time and behavior is minimized.

Avaya A175 Behavior During Failover

During failover, Avaya A175 Devices will:

- Locate multiple controller addresses in priority order,
- Detect the availability of each controller,
- Transition automatically to lower priority controllers whenever a high priority controller fails or becomes unreachable (automatic failover),
- Transition from lower priority controllers to a high priority controller (failback) either automatically or as a result of explicit administrator activity,
- Preserve active calls to the greatest extent possible in the event of a transition, and
- Preserve as many call and system features as possible when operating under failure conditions.
- Be in a pushable state during transition, when the primary controller is lost and device is not connected to a secondary controller. Once the device is registered on secondary controller and regardless if the device is active on a call, the device is in a pushable state, just as if were connected to primary server. The device is always in a pushable for state for all normal or barge-in Top Line. Display, Audio Receive/Transmit, or phonexml pushes for all transition conditions.

In general, the device does not attempt to preserve SIP transactions in progress when a controller failure is detected, and some mid-call features like conferencing can fail. However, in some scenarios the same transaction may succeed if re-attempted once the transition to a new controller has been completed.

The Avaya A175 always registers to a configured controller with the credentials (username/password) of the user who is currently logged-in, even if the device transitions from one controller to another.

As described in the Avaya A175 user guide, certain features may not be available and functionality may be limited or work differently during any stage of failover, "limbo," transition, or failback. Calls can still be placed and received, and other Avaya A175 functions remain active. The following apply when an Avaya A175 is in failover mode:

- If the user is active on a call, a failover icon displays when failing over to a non-AST controller and messages like "Link recovery." "Limited phone service." and "Calls may be lost." inform the user of a failover situation. The message "Limited phone service" also displays during failover transition from one Session Manager server to another when the subscriptions have not yet been moved successfully to the secondary SM.
- When failing over to a third party secondary controller, an Acquiring Services message appears during failover and failback transitions to an active controller and a Call Preservation message may appear on the Avaya A175. Most other options and applications except for local administrative (Craft) options are unavailable until an active controller is found. However, the user can access the Contacts, Call Forward feature, or History.
- If a call is active when failover occurs, that call will remain active. The user cannot initiate new calls while the device transitions to the alternate server.
- Call appearance information does not display while dialing, but does appear when Call button is pressed.
- Call connection may take longer than usual.
- Upon failover, any active conference calls, call transfers, and held calls will be dropped.
- Emergency calls may or may not work, depending on the stage of failover and the functionality available on the alternate server.
- Bridged call appearances are not available.
- During the transition stage, incoming calls may not be received and may go to voice mail.
- Call forwarding may not be available unless the extension to which calls are being forwarded is on the same server as the forwarding extension.
- The Voice Mail icon on the Top bar is cleared (that is, the number of voice mail messages is not displayed), but voice mail may still be available, if the voice mail server to which calls are being sent is not in failover.
- Contacts can be accessed and changed during and after failover to the alternate server.
- Access may be limited to local contacts only. Users may be unable to access a corporate LDAP directory.
- If the Avaya A175 is logged out during failover, the local cache is cleared and the Avaya A175 may become inoperable until it can be reset on the original controller after failback.
- Avaya A175 will accept calls from any of the proxies it is registered with when the device is simultaneously registered to multiple controllers. There is no visual indication to the user differentiating calls from different feature servers. In the case of Multiple Feature Servers, one feature server can know about one call on the device and another feature server or controller can know about another call on another call appearance. The second Feature

Server does not have any information about the first call displayed on the Avaya A175 and there will be limitation in the features that can be applied to the first call. When there are multiple controllers, one controller may know about one call on the Avaya A175 and another controller can know about another call offered to the Avaya A175. If both controllers are connected to the same feature server e.g., CM, CM "knows" about both calls and the user can resume a held call, conference call, or call transfer normally. If both controllers are not connected to the same feature server, the second Feature Server would not have any information about the first call displayed on the Avaya A175. In this scenario, features that can be applied to the first call would be limited because all the call data is stored in CM; SM does not store any information related to any call.

- Preserved Media Connections - In an active-active scenario where the primary SM fails, any active shuffled or direct media call will be preserved if a new call is received while a preserved call is active. The Avaya A175 allows the user to manually put the active (media preserved) call on hold or allows the user to switch to the new call and automatically put the preserved call on hold using auto-hold. A media preserved call displays the failover icon in place of a call-associated icon that is left justified on an application line preceding the displayed name or phone number. When active on a media preserved call, Conference and Transfer are not available. The device can receive incoming calls at this point but is not available to make outgoing calls or to invoke AST features. The device supports media preservation sufficient for alternate registration; if a device experiences a mid-dialog failure (for example, a timed out or failed SIP request, or a socket-level failure), the device behaves as if the dialog had been terminated (but does not send a BYE) and preserves the media session until the near-end user hangs up.

Failover/Failback Administrative Monitoring and Logging

It is ultimately up to the Avaya A175 to determine which of its configured controllers is the Active Controller. This information is available in the SNMP MIB, which the network administrator can view; the Active Controller is the SIPPROXYSRVR_IN_USE value. The Avaya A175 sends an SNMP notification whenever a transition occurs. In addition, whenever the appropriate level of logging is enabled, the device logs its transitions from one server to another.

User Interface/Failover Experience

The user interface experiences described below expand upon the information provided in Failover/Failback Behavior.

User Interface in Failover/Failback

- Failover (F/O) transition - Connection to SM failed, the Avaya A175 detects F/O and blocks new invites while the device is in transition.
- Stable in F/O where the non-primary proxy is the active controller.
- Fail Back (F/B) transition to normal - The Avaya A175 detects that the primary server is up, regardless if the secondary is up. New invites are blocked while the device is in transition. The Avaya A175 is in a stable Normal mode with SM as the active controller. Any cached changes (for example, to Contacts) are updated to the PPM once the Avaya A175 is registered back to the primary controller.

User Experience for Transitions

For failover to a secondary controller for alternate registration (SES F/O to SM to a non-AST controller), transition is comprised of the following conditions:

- Limbo - The Avaya A175 has lost its connection to its primary controller, but has not yet detected this condition regardless of whether a user is on a call or not.
- Acquiring Services - The Avaya A175 has detected a lost connection to the primary controller and displays an Acquiring Services message if the device is idle.
- Call Preservation - During an active call, the Avaya A175 has detected a lost connection to the primary controller and displays a Call Preservation message.

Transition from one SM to another SM/BSM (Branch System Manager) is comprised of the following conditions:

- Limbo - The Avaya A175 has lost its connection to its primary controller, but has not yet detected this condition, regardless of whether a user is on a call or not.
- Moving Subscriptions Interval (MSI) - The Avaya A175 has detected a lost connection to the primary controller and since it has already registered with a non-primary controller, this is the interval between limbo and successful subscription to the non-primary controller. The subscription can be moved regardless of whether a user is on a call or not. The Call Preservation message or the Acquiring Services message are not displayed during MSI.
- Call Preservation - During an active call, the Avaya A175 has detected a lost connection to the primary controller and exhibits media preservation behavior.
- The failover icon displays on the Top bar when failing over to a non-AST controller or in the very short interval after limbo and before a successful subscription from one SM to another (or BSM) in the same community.

User Experience During Stable Failover

- A Failover “warning” icon displays on the Top bar. The Failover icon is shown whenever the primary call server is not active. The Failover icon provides a continuous reminder indicating the Avaya A175 has detected that the primary server is unavailable and that features will be limited until the primary server returns.
- Multiple Call Appearances are consistent with Normal Operation.
- If a call originates using the secondary server, Hold, Conference and Transfer will be supported.
- AST features (FNUs and Bridged call appearances) are unavailable when failing over to a non-AST controller.
- Unsupported features are not displayed.
- The dial plan does not remain as it was in normal operation. The dial plan in failover is set with the DIALPLAN parameter which should contain all needed strings while failed over. Calls between sets in the branch are supported, using their usual extensions.
- Outgoing Calls that would normally route to the SM/CM will instead be routed to the local gateway.
- Emergency calls (to the provisioned emergency numbers as defined in the dial plan) will be permitted whether those devices are in failover or normal mode. The Emergency button is available when a new controller is found.
- The Voice Mail icon on the Top bar will be cleared, but voice mail is still available.
- One-button voice mail access will be available if the central voice mail system continues to operate and will make a PSTN call to the voice mail system. Depends on correct provisioning.
- Local Avaya A175 features will be available: audio selection (speaker / headset / handset), mute.
- Local Avaya A175 applications will be available: History, Volume Control, local contacts, email, Facebook, and web browser but cannot be changed.
- Basic local features if provisioned (call forwarding) will be available: call hold, consultative hold, Attended Transfer, Unattended Transfer, call forward all, three party conferencing of calls originated in Failover Operation (including drop last party).
- Presence is not supported.
- Craft changes may be made and are saved locally on the Avaya A175.
- If the Avaya A175 is logged out during failover, the local cache is cleared.

User Experience During Fail Back

Fail Back (F/B) transition occurs when the Avaya A175 detects that the primary server is up, regardless if secondary controller is up.

- Failback will not happen during an active call. If no calls are in progress, failback occurs and the user interface returns to its normal appearance.
- While switching from one server to another (including while waiting for an active call to end) reject any new inbound calls (including emergency callbacks) or outbound call requests.
- AST features return.

User Interface Feature Failover Operation

Feature	Normal Operation with CM	Failover Operation with a Generic SIP Gateway
Make call	Yes	Yes
Receive call	Yes	Yes
Call Hold	Yes	Yes
Consultative Hold	Yes	Yes
Ad hoc conferencing	Yes, up to 6 parties	Yes, up to 3 parties
Last party drop	Yes	No
Forward all my calls/SAC	Yes	Yes
Attended call transfer	Yes	Yes
Unattended call transfer	Yes	Yes
EC500 on/off	Yes	No
Bridge line and call appearances	Yes	No
Extend-call	Yes	No
Hold recall	Yes	No
Transfer recall	Yes	No

Feature	Normal Operation with CM	Failover Operation with a Generic SIP Gateway
Busy indicator	Yes	One-button dial - Yes Busy indicator - No
Voice mail indicator	Yes	No

Appendix A: Restart Scenarios

Scenarios for the Restart Process

When the Avaya 175 starts, it checks the upgrade file (Axxxupgrade.txt) on the server to determine if the software image currently installed on the Avaya A175 matches the software image specified in the upgrade file on the server. If the software image on the Avaya A175 does not match, it downloads the software image in the background. Once the download is complete, the Avaya A175 will prompt the user to restart the device.

The Avaya A175 polls the server once every hour to determine if a new software image is available. When a new software image is available, the Avaya A175 downloads the software image in the background. Once the download is complete, the Avaya A175 will prompt the user to restart the device.

Note:

The file names used in this appendix are examples only. Your particular file names are likely to be different.

Restart the Avaya A175

Use the following procedure to restart the Avaya A175.

Note:

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

To restart the Avaya A175:

1. Touch the **Applications** menu title to display the Applications fan title.
2. On the Applications menu fan, touch **Settings**.
3. From the Settings pane, touch **Administrator Options**.
4. In the Password box, enter administration password.
5. Touch the **Ok** button.
6. From the Administrator pane, touch **Reboot**.

   A dialog box appears, prompting you to confirm your action.
7. Touch the **Ok** button to restart the Avaya A175.

Appendix B: Glossary of Terms

Terms Used in This Guide

802.1D **802.1Q**	802.1Q defines a layer 2 frame structure that supports VLAN identification and a QoS mechanism usually referred to as 802.1D.
802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access.
Application - specific	Specific to a particular “application” running inside the deskphone. For example, configuration file downloading, HTTP push, and the Web browser are all internal applications that use the HTTP protocol. Similarly, the RTCP and CNA clients are internal applications that can invoke traceroute. This term does not include Web-page-based “applications” rendered in the Web browser.
ARP	Address Resolution Protocol, used, for example, to verify that the IP Address provided by the DHCP server is not in use by another Avaya A175 Device.
Call Server	In an Avaya SIP environment, the “call server” is the combination of SIP Enablement Services (SES) and Avaya Communication Manager.
CLAN	Control LAN, type of Gatekeeper circuit pack.
CNA	Converged Network Analyzer.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
DNS	Domain Name System, an IETF standard for ASCII strings to represent IP addresses. The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP Addresses. Avaya A175 Devices can use DNS to resolve names into IP Addresses. In DHCP, TFTP, and HTTP files, DNS names can be used wherever IP Addresses were available as long as a valid DNS server is identified first.
EAP	Extensible Authentication Protocol, or EAP, a universal authentication framework frequently used in wireless networks and Point-to-Point connections defined by RFC 3748. EAP provides some common functions and a negotiation of the desired authentication methods, two of which are EAP-MD5 and EAP-TLS. When EAP is invoked by an 802.1X enabled NAS (Network Access Server) device such as an 802.11 a/b/g Wireless Access Point, modern EAP methods provide a secure authentication mechanism and negotiate a secure PMK (Pair-wise Master Key) between the client and the NAS.

Gatekeeper	H.323 application that performs essential control, administrative, and managerial functions in the media server. Sometimes called CLAN in Avaya documents.
H.323	A TCP/IP-based protocol for VoIP signaling.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	A secure version of HTTP.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.
LAN	Local Area Network.
MAC	Media Access Control, ID of an endpoint.
PPM	Personal Profile Manager, part of the SIP Enablement Services (SES) platform. PPM is responsible for maintaining and managing end users' personal information in the system.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks.
RTCP	Real-time Transport Control Protocol.
RTP	Real-time Transport Protocol.
SCEP	Simple Certificate Enrollment Protocol, used to obtain a digital certificate.
SES	SIP Enablement Services.
Session Manager (SM)	Avaya Aura™ Session Manager, the SIP proxy for Avaya Aura™, an alternative to SES as of SIP software Release 2.5.
SIP	Session Initiation Protocol, an open standard defined initially by IETF RFC 3261. SIP is an alternative to H.323 for VoIP signaling.
SRTCP	Secure Real-time Transport Control Protocol.
SRTP	Secure Real-time Transport Protocol.
System - specific	Specific to a particular type of call server, for example, Avaya Communication Manager (CM). "System-specific signaling" refers to messages specific to the signaling protocol used by the system, for example, H.323 and/or CCMS messages used by CM and IP Office. "System-specific procedures" refers to deskphone software procedures that are specific to the call server with which the software is intended to be used.
TCP	Transmission Control Protocol, a connection-oriented transport-layer protocol.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications.

UDP	User Datagram Protocol, a connectionless transport-layer protocol.
Unnamed Registration	Registration with Avaya Communication Manager by an Avaya A175 Device with no extension. Allows limited outgoing calling.
URI & URL	Uniform Resource Identifier and Uniform Resource Locator. Names for the strings used to reference resources on the Internet (for example, HTTP://....). URI is the newer term.
VLAN	Virtual LAN.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.

Index