Implementing End-to-End SIP
Vol 1: Endpoint Deployment

December 2013
Issue 2

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

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

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

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

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

Open Source Attribution
The Product utilizes open source and third-party software. For copyright notifications and license text of third-party open source components, please see the file named Avaya/Gateway/LegalNotices.txt in the directory in which you have installed the software.

Trademarks
Avaya, Avaya Aura, and one-X are either registered trademarks or trademarks of Avaya Inc.
All non-Avaya trademarks are the property of their respective owners.

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

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

Contents

Introduction

Purpose

This document demonstrates the quickest and easiest way to deploy SIP endpoints during Avaya Aura® installation and have SIP endpoints and basic call features work as designed. It also covers verifying that critical initial administration was done correctly and provides information on setting up the endpoints.

This document does not cover all the installation and configuration of the Avaya Aura® solution, but rather focuses on administering users.

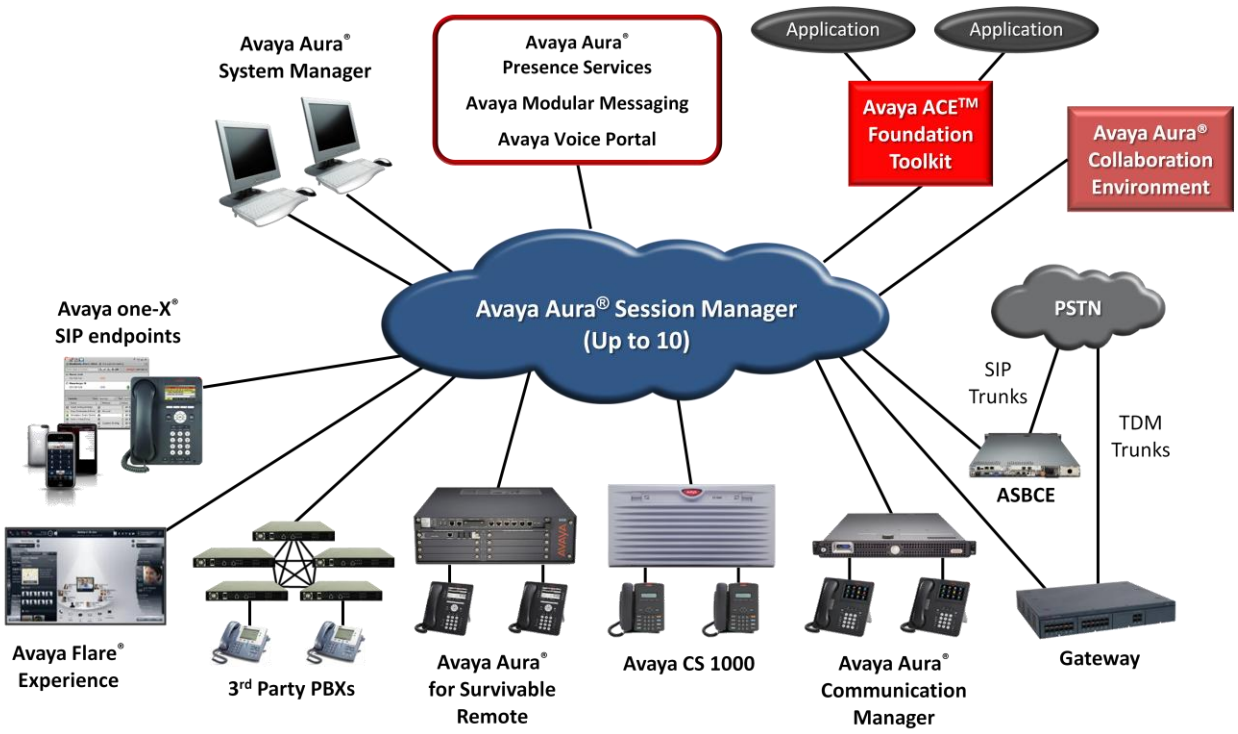
Intended audience

This document is intended for implementation engineers responsible for end-to-end SIP deployment, including customers, partners and Avaya associates.

Avaya Aura® SIP overview

The Avaya Aura® SIP solution is a rich, highly interoperable set of SIP components that take enterprise communications architecture to the next level. At the core of the solution is the Avaya Aura® Session Manager providing SIP interoperability, centralized numbering plan, SIP normalization, SIP routing, and many other SIP services to create a secure and easy to manage enterprise backbone network. At the access layer of the solution are the SIP endpoints working seamlessly with the Avaya Aura® core to provide world class enterprise services.

Below is a typical SIP configuration used to define the configuration steps for successfully deploying a SIP solution.



Required components

For a properly operational SIP endpoint, an enterprise needs the following components:

- **System Manager** (SMGR), Release 6.3.5 - At least one SMGR must be installed with the latest service pack, configured, and connected to the network. SMGR provides the central administration interface used to configure the Session Manager and Communication Manager components. The SMGR's WebLM License Server is frequently configured to provide license services to the other solution components.

- **Session Manager** (SM), Release 6.3.5 - One or more Session Managers are installed with the latest service pack, configured, and connected to the network. Session Manager serves as the SIP registrar and outbound proxy for the endpoints, and it routes

SIP messages during call setup, modification, and teardown. Session Manager also contains the Personal Profile Manager (PPM), which provides for backup and restore of endpoint-resident data like contacts, endpoint parameters, etc.

- **Communication Manager** (CM), Release 6.3.3 – At least one Communication Manager is installed with the latest service pack, configured, and connected to the network. Communication Manager handles call origination and termination for endpoints, implements a rich set of telephony features, and participates in call routing in concert with Session Manager.

- **DHCP Server** - A DHCP server is installed, configured, and connected to the network, and the DHCP scope(s) are administered as needed. The customer may provide the DHCP server, or may activate the DHCP server resident in an Avaya Aura® Utility Services server, if one is available in the system. Endpoints get their IP address from the DHCP server during the initial connection to the network. The endpoints also use the fileserver FQDN/IP address specified in a DHCP option string to communicate with the fileserver for software updates and to retrieve the settings file that automatically configures the endpoint parameters.

- **HTTP Server** – An HTTP server (fileserver) is installed, configured, and connected to the network. The telephone upgrade script, settings file, and latest release of software are properly configured and loaded onto the HTTP server. The endpoints contact the HTTP server to download their settings file and to check for (and download) new software updates.

- **SIP Endpoints** - All of the SIP telephones are physically installed and are running the latest SIP software. In this document, SIP endpoints include the following:

    - Avaya one-X® Communicator ("softphone")
    - Avaya SIP one-X™ Deskphones ("hardphone")
    - Avaya B179 SIP Conference Phone
    - The Avaya Flare® Experience for Windows and iPad®
    - The Avaya A175 Desktop Video Device with the Flare® Experience ("ADVD")

  There are currently 2 different generations of Avaya SIP hardphones, each running different versions of SIP software. These endpoints are collectively called out in this document as 96xx or 96x1, and the specific models map as follows:

  [**96xx**] 9620, 9620C, 9620L, 9630, 9630G, 9640, 9640G, 9650, and 9650C

  [**96x1**] 9601, 9608, 9611G, 9621G and 9641G

  The 96xx hardphones use 2.6.x SIP software releases, and the 96x1 hardphones use 6.3.x SIP software releases. Both generations of SIP hardphones can also be configured as H.323 hardphones, by loading H.323 software instead of SIP software. This document focuses on SIP deployments, but some customers will deploy both H.323 and SIP versions in the same environment, and we'll consider the special requirements of such environments.

High-level end-to-end SIP deployment process

The SIP endpoint deployment sequence consists of four high-level activities:

1. Collect the configuration data required to install the endpoints on the system.

2. Perform user administration in System Manager, the DHCP server, and the fileserver. As a first step in this administration, confirm that the System Manager, Session Manager, and Communication Manager core administration required to support your SIP endpoints has already been properly performed, and address any misconfiguration.

3. Unpack, assemble, and connect each endpoint to the LAN. Perform manual **endpoint administration** (*See Task #9: Change Endpoint's Signaling Type from H.323 to SIP*). Confirm that each endpoint successfully registers to the system, that you can login on the endpoint, and that all the expected feature controls and displays subsequently appear on the endpoint.

4. Using System Manager, administer two users for testing purposes. Log those users into two networked SIP endpoints, and verify that they can call each other and that buttons, indicators, and displays on the endpoints function correctly.

Related resources

Avaya documentation

Component	Reference
System Platform Release 6.3	Installing and Configuring Avaya Aura® System Platform Release 6.3 Administering Avaya Aura® System Platform Release 6.3
System Manager Release 6.3	Implementing Avaya Aura® System Manager Release 6.3 Administering Avaya Aura® System Manager Release 6.3
Session Manager Release 6.3	Deploying Avaya Aura® Session Manager Release 6.3 Installing Service Packs for Avaya Aura ® Session Manager Release 6.3 Administering Avaya Aura® Session Manager Release 6.3
Communication Manager Release 6.3	Implementing Avaya Aura® Communication Manager Release 6.3 Administering Avaya Aura® Communication Manager Release 6.3
Presence Services Release 6.2	Implementing Avaya Aura® Presence Services Release 6.2 Administering Avaya Aura® Presence Services Release 6.2
Utility Services Release 6.3	Accessing and Managing Avaya Aura® Utility Services Release 6.3
96x1 SIP Endpoint Release 6.3	Administering Avaya 9601/9608/9611G/9621G/9641G IP Deskphones SIP, Release 6.3 Installing and Maintaining Avaya Deskphone SIP for 9601/9608/9611G/9621G/9641G IP Deskphones, Release 6.3
96XX SIP Endpoint Release 2.6.10	Administering Avaya one-X® Deskphone SIP for 9620/9620C/9620L/9630/9630G/9640/9640G/9650/9650C IP deskphones Release 2.6.10 Avaya one-X(R) Deskphone SIP Installation and Maintenance Guide Release 2.6

Component	Reference
A175 Device with Flare (ADVD)	Implementing and Administering Avaya A175 Desktop Video Device with the Avaya Flare® Experience Release 1.1
Avaya one-X® Communicator	Implementing Avaya one-X® Communicator Administering Avaya one-X® Communicator Avaya one-X® Communicator Centralized Admin Tool
Avaya Flare® Experience	Administering Avaya Flare® Experience for Windows Release 1.1 Implementing Avaya Flare® Experience for Windows Release 1.1 Administering Avaya Flare® Experience for iPad Devices Release 1.1 Implementing Avaya Flare® Experience for iPad Devices Release 1.1
Avaya B179 SIP Conference Phone	Avaya B179 SIP Conference Phone Installation and Administration Guide

General references

- SIP Communication for Dummies - ISBN: 978-0-470-38114-4
- SIP Demystified by Gonzalo Camarillo (ISBN 0-07-137340-3)
- **SIP: Understanding the Session Initiation Protocol 3rd Edition (Artech House Telecommunications)** by Alan Johnston (ISBN-10: 160783995, ISBN-13: 978-1607839958

Useful links

- Avaya Support Site
- Avaya Product Licensing and Delivery System (PLDS)
- The SIP School
- Avaya Mentor Youtube Videos (700+ How-to Videos prepared by Avaya Services Engineers)

Training

Avaya Learning offers the following training courses. Go to http://www.avaya-learning.com.

Course#	Suggested Pre-Requisite Courses
ATC01270WEN	Quick SIP
ATC01290WEN	SIP Essentials
ATI01672VEN	Avaya Aura CM Fundamentals
ATU01730WEN	Avaya Aura CM Architecture, Protocols and Features

Course#	Communication Manager 6.x Courseware
ATC01842OEN	CM and System Manager
5U00041I	Avaya Aura Communication Manager Administration
ATI02348IEN	Avaya Aura™ Communication Manager Implementation
ATI02348VEN	Avaya Aura™ Communication Manager Implementation
ATC00421VEN	Administering and Maintaining Avaya Aura System Platform (6.0)

Course#	Session Manager 6.x Courseware
5U00105W	Avaya Aura® Session Manager Overview
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00104W	Avaya Aura® Session Manager 6.2 Delta: Overview

Course#	System Manager 6.x Courseware
5U00106W	Avaya Aura® System Manager Overview
5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00103W	Avaya Aura® System Manager 6.2 Delta: Overview

Course#	Presence Services
ATI02210VEN	Presence Server Implementation
ATI01445WEN	System Platform Installation for CM R6.0
ATI01732WEN	Licensing for Avaya Aura Communication Manager
4U00115I	Avaya Aura CM Implementation Upgrade (R5.X to R6.X)
4U00115V	Avaya Aura CM Implementation Upgrade (R5.X to R6.X)

Document updates

Avaya frequently updates documents. Make sure you have the latest version of this document and all Avaya documentation by accessing the Avaya portal.

Send us your comments

Avaya appreciates any comments or suggestions that you might have about this product documentation. Please send your comments to charlesrogers@avaya.com.

Checklist for configuring SIP endpoints

Use this checklist to guide you through the configuration tasks for SIP endpoint deployment.

Task #	Task Description	Notes	√
Task 1 **Page** **17**	Collect configuration data for the following components: • SIP endpoints • System Manager • DHCP server • HTTP server		
Task 2 **Page** **21**	Confirm administration of the following components for endpoint support: • System Manager • Session Manager • Communication Manager		
Task 3 **Page** **24**	Download the latest endpoint software zipfiles from support.avaya.com, ftp.avaya.com, or plds.avaya.com, and copy them onto the HTTP(S) fileserver.		
Task 4 **Page** **36**	Administer the HTTP(S) fileserver		
Task 5 **Page** **42**	Administer DHCP server scope		
Task 6 **Page** **44**	Administer User in System Manager		
Task 7 **Page** **51**	Unpack and assemble the endpoint		
Task 8 **Page** **53**	Connect the endpoint to the Network		
Task 9 **Page** **55**	Change endpoint's signaling type from H.323 to SIP (if appropriate)	The 9601SIP Phone, ADVD, and Avaya B179 SIP Conference Phone are SIP-only. 96XX and 96X1 phones ship from the factory configured as H.323, and require signaling type change to SIP.	
Task 10 **Page** **57**	Confirm endpoint software upgrade		

Task #	Task Description	Notes	√
Task 11 Page 59	Login and confirm feature subscription		
Task 12 Page 59	Test call and feature operation		

Task #1: Collect Configuration Data

Collect and populate values in the tables included below. Separate tables appear for:

- Data for System Manager
- Data for the Telephone Set
- Data for DHCP (Option 242 Parameters)
- Data for HTTP(S) Fileserver

You may acquire these values from the solution design engineer, the implementation engineer, the customer, or you may create them yourself. Implementation teams often build a detailed workbook or workbooks for the solution, and such documents should contain all the information you need.

NOTE: If you are responsible for creating this information from scratch, you ***must*** understand the effects of dial-plans and numbering-plans on proper selection of Communication Manager phone extensions and SIP user handles. Please read **"Implementing End-to-End SIP, Vol 2: Designing SIP Telephone Signaling, Number and Dial Plan Options"**.

Data for System Manager

Each entry in the table corresponds to a field on the screens that SMGR provides for user administration. The shaded rows in the table provide navigational information to help you locate those screens and fields in the SMGR web interface. You can use the Help feature on any SMGR screen to retrieve detailed field descriptions: click the *Help* link at the top right-hand corner of the form.

Field Label	Value	Note:
Home > Users > User Management > Manage Users > Identity (tab)		
Last Name		
First Name		
Login Name		SIP-handle@SIP-domain
Password		For self-admin access to SMGR
Localized Display Name		
Endpoint Display Name		
Language Preference		
Time Zone		
Home > Users > User Management > Manage Users > Communication Profile (tab)		
Communication Profile (Section)		
Communication Profile Password		For phone login
Communication Address (Section)		
Handle Type		SIP
Handle Fully Qualified Address		handle@SIPdomain
Handle Type		E.164
Handle Fully Qualified Address		handle@SIPdomain

Session Manager Profile (Section)		
Primary Session Manager		Must be an SM
Secondary Session Manager		Must be an SM
Origination Application Sequence		Must include CM (See Note)
Termination Application Sequence		Must include CM (See Note)
Survivability Server		Must be SM or BSM
Home Location		
Endpoint Profile (Section)		
System		
Profile Type		
Use Existing Endpoints		
Extension		
Endpoint Template		
Voice Mail Number		
Delete Endpoint on Unassign/Delete		

Messaging Profile (Section)		
System		
Use Existing Subscriber on System		
Mailbox Number		
Template		
Password		
Delete Subscriber on Unassign/Delete		

Note: CM must appear in the application sequences for call origination and call termination sequences. For CM-ES (Evolution Server) deployments, CM is the only application in each sequence. For CM-FS (Feature Server) deployments, CM must appear in the application sequences, but other applications may appear in those sequences as well. For a discussion of the differences between CM Evolution Server and CM Feature Server, see "***Chapter 2: Overview***" in Administering Avaya Aura(R) Communication Manager Server Options, Release 6.3.

Data for the telephone set

Populate values in the following table:

Name	Description	Form/Location	Value
Username	Telephone Username	Login Screen	
Password	Telephone Password	Login Screen	

Notes:

1. Username is set to the telephone's extension. Username and Password are ***numeric***.

Data for DHCP (Option 242 Parameters)

Populate values in the following table:

Name	Description	Value	Purpose
HTTPSRVR	Non-secure Fileserver IP Address/FQDN -		To contact fileserver to download files
TLSSRVR	Secure Fileserver IP Address/FQDN		To contact fileserver to download files
VLANTEST	Number of seconds to wait for DHCPOFFER on a non-zero VLAN		DHCP Offer timeout value. Default is 60.
L2Q	802.1Q tagging mode		For Voice/Data VLAN deployments. Values are 0 for off, 1 for on.
L2QVLAN	VLAN ID of Voice VLAN		For Voice/Data VLAN deployments.
SNTPSRVR	SNTP Server IP Address/FQDN List		Time Servers (Optional – this can also be set in the 46xxsettings.txt file)

Notes:

1. Example of a minimal DHCP Option 242 String:
   TLSSRVR=135.64.150.167,HTTPSRVR=135.64.150.167

Data for HTTP(S) Fileserver

Populate values for the 46xxsettings.txt file entries in the following table. The first three entries in this table are the *minimum* set of values needed to get SIP endpoints working. The other nine entries shown in the table are used for typical deployments as well, and many other parameters in addition to these are available to support the entire endpoint feature set. *Appendix G: Proper Selection of 46xxsettings.txt Values* provides guidance for creating your 46xxsettings.txt file.

Name	Description	Value
SIPDOMAIN	SIP Domain Name	
SIP_CONTROLLER_LIST (See Note 2 below)	Session Manager IP Addresses/FQDNs	
SIMULTANEOUS_REGISTRATIONS	Enable registration to more than one SM at a time.	
SIG (See Note 1 below)	Signaling Type (H.323 or SIP)	2
GMTOFFSET	Time Zone Offset from GMT	
DSTOFFSET	Daylight Savings Time Offset	
DSTSTART	Daylight Savings Time Start	
DSTSTOP	Daylight Savings Time Stop	
ENABLE_PRESENCE	Enable Presence	
PHNEMERGNUM	Emergency dial string	
PSTN_VM_NUM	PSTN Voicemail Dial String for failover VM access	Optional
MSGNUM	Internal Voicemail Dial String	Optional

Notes:

1. SIP_CONTROLLER_LIST is a comma-separated list of SIP Proxy FQDN/IP Addresses. example: 192.168.10.25:5061;transport=tls;192.168.2.2:5061;transport=tls
2. The value of SIG is always 2 for SIP endpoints, but with 96x1 endpoints, you must configure the 46xxsettings.txt file to correctly handle mixed environments of both H.323 and SIP endpoints. For some environments, the **best practice** is to leave the SET SIG directive commented out in 46xxsettings.txt. See *Appendix C: Administration guidance and detailed descriptions* and *Appendix G: Proper Selection of 46xxsettings.txt Values* for detailed guidance.

Task #2: Confirm System Component Administration

A detailed exploration of the complete configuration and administration of the all the Aura system components is beyond the scope of this document. However, the step-by-step tasks presented in the following sections depend on specific pre-configuration of SMGR, SM, and CM. You must verify that the necessary pre-configuration is in place, before you can deploy and test the endpoints. By logging into System Manager and visiting all the configuration locations listed below, you confirm that the necessary pre-configuration has been done, and you gain a better understanding of the system topology and interaction of the components.

See *Appendix A: Verifying administration* for additional guidance.

System Manager

System Manager (SMGR) provides the central administration interface. You use it to perform all the administration tasks associated with Session Manager and Communication Manager.

SMGR Access and permissions

1. **Login Access** – Confirm that you can login to the SMGR browser interface. You must enter either an IP address or FQDN (preferred) in your browser address field, and your username and password must authenticate in SMGR. If you plan to login as *admin* and are the first person to login to SMGR using the *admin* account, you must change the default *admin* password (admin123) before you can actually login. The SMGR login page provides a link specifically for that purpose. **Best Practice**: be sure to record the new SMGR password as part of the official solution documentation!
2. **Navigation** – Confirm that you understand the navigational scheme provided by the SMGR user interface. In the following discussion, navigational cues are provided in italics, e.g., [*Home -> Elements -> Routing -> Domains]* tells you which sequence of tabs or links to click in your browser, in order to arrive at the desired page or section.
3. **Permissions** – *[Home -> Users -> Administrators]* Confirm that your login account possesses the System Administrator and Network Administrator **roles,** so that you can modify SM, CM, and User configuration. The default ***admin*** user account has both of these roles.

Routing Configuration

1. **SIP Domain** - *[Home -> Elements -> Routing -> Domains]* Confirm that the SIP Domain that you will configure in your SIP endpoints is defined here.
2. **Locations** - *[Home -> Elements -> Routing -> Locations]* Confirm that the physical location(s) associated with your SIP endpoints are defined here.
3. **Adaptations** - *[Home -> Elements -> Routing -> Adaptations]* Confirm whether or not any special SIP message manipulation is configured to route SIP messages into (ingress) or out of (egress) SM. Examples include deletion or insertion of digits when incoming or outgoing dial strings match a particular pattern.
4. **SIP Entities** - *[Home -> Elements -> Routing -> SIP Entities]* Confirm that your Session Manager(s), Communication Manager(s), and Presence Services Server(s) all have SIP entities defined here.
5. **Entity Links** - *[Home -> Elements -> Routing -> Entity Links]* Confirm that the links that interconnect your Session Manager(s), Communication Manager(s), and Presence

Services Server(s) exist, and that link parameters such as transport protocol (UDP, TCP, TLS) and port number are specified for those links.

6. **Routing Policies** - *[Home -> Elements -> Routing -> Routing Policies]* Confirm that the routing policies defined for your CM(s) are based on the desired dial patterns, SIP Domain, and Locations that your phones will use.
7. **Dial Patterns** - *[Home -> Elements -> Routing -> Dial Patterns]* Confirm that the dial patterns that you expect SM to encounter are correctly specified.

Inventory Management

1. **SM, CM, Presence Element Management** - *[Home -> Elements -> Inventory -> Manage Elements]* This page contains entries for all of the SIP entities that SMGR manages. To manage a SIP entity, SMGR needs contact information like management IP address and port, and it needs login credentials so it can login to that entity and act on behalf of the administrator. When you use SMGR to administer the buttons and features on a 96x1 phone (for example), SMGR uses the access information to login to CM and run the "change station" command to configure the phone in CM. Confirm that your Session Manager(s), Communication Manager(s), and Presence Services Server(s) have entries on this page.
2. **CM Synchronization Management** - *[Home -> Elements -> Inventory -> Synchronization -> Communication System]* Because SM and CM work together to handle calls from/to your SIP endpoints, they must use the same configuration data for those endpoints. Changes made in CM must be synchronized to SM. This typically happens automatically, but sometimes it is necessary for you to force recent CM changes to be synchronized into SM, and this page offers a control to do that immediately. You can also use the page to determine whether or not recent changes made in CM have been automatically synchronized into SM yet. Confirm that your CM(s) are regularly synchronized, and whether the last synchronization attempt succeeded.

Session Manager

1. **Dashboard** - *[Home -> Elements -> Session Manager -> Dashboard]* This page tells you whether your Session Managers are healthy and ready to accept SIP service requests. If an SM is in the state, "Deny New Service", your endpoints will not be able to register to that SM, and will instead attempt registration with other SMs that may be accepting new service requests. The dashboard also tells you about SM alarms, the up/down status of all that Session Manager's entity links, the number of users registered to it, number of active calls, and whether Data Replication is current (see next item). Confirm that your SM is healthy, in the "Accept New Service" state, and that its monitored links are up.
2. **Replication** - *[Home -> Services -> Replication]* Session Managers use an internal database initialized and updated by SMGR. SMGR keeps the master copy of the database, and continuously replicates that copy to all the Session Managers and Presence Services servers that it manages. The Replication page shows you whether the SM database is up-to-date with the master copy in SMGR (green) or not (yellow, red, or no entry). If replication status for a Session Manager is not "Synchronized", endpoints may not be able to register with that SM, and if they are already registered, they may not receive updates when you modify their configuration in SMGR. Confirm that your SM(s) and Presence Services Server(s) all show green status.
3. **User Registration Status** - *[Home -> Elements -> Session Manager -> System Status -> User Registrations]* This page provides considerable information for each registered endpoint, and shows which administered endpoints are not registered. As you add each

new SIP endpoint to the system, you use this information to confirm that the endpoint registered to its primary, secondary, and survivable SM, which SM is its active SM, and whether it requested and received all its feature subscriptions from that SM. Other endpoint information presented includes the endpoint's IP address, location, login name, MAC address, device model, and software version. Since you may not yet have configured any SIP stations on this system, there may be no entries visible. However, if any SIP endpoints have already been configured and SIP User Registrations are displayed now, confirm that they are properly registered to primary and secondary SMs. Click "Show" in the "Details" column to examine their Event Subscription status. A properly registered and subscribed Advanced SIP Telephony (AST) endpoint displays five Event Subscriptions:

a. avaya-cm-feature-status
b. reg
c. avaya-ccs-profile
d. message-summary
e. dialog

96xx, 96x1, ADVD, Avaya one-X® Communicator, Avaya Flare® Experience for Windows, and Avaya Flare® Experience for iPad® Devices are all AST endpoints. The B179 Conference Phone is not.

Communication Manager

1. Entity Link Status - *[Home -> Elements -> Session Manager -> System Status -> SIP Entity Monitoring]* The lower half of this page provides a listing of all Monitored SIP Entities for this particular SM. Find your CM's SIP Entity Name in the list and click on the name (not the checkbox). The page that loads shows whether or not the SM-to-CM link is up and what IP address, port and protocol are in use for that link. If the link is down, then the CM may be using a different SM for processing calls. If the CM has no healthy SM entity links, then it cannot participate in call processing. Confirm that the Link Status for your CM is "Up".
2. Definition of Application Sequences for CM - *[Home -> Elements -> Session Manager -> Application Configuration -> Application Sequences]* CM handles call origination and termination processing for its configured endpoints. When you use SMGR to administer a SIP endpoint, you designate specific origination and termination *application sequences* for the endpoint. The application sequences specify a CM to do that origination or termination work. If the application sequence is not defined, then when you try to administer an SM profile for a new endpoint, the required CM will not appear in the drop-down menu for origination and termination processing, and your administration will be blocked. Confirm that your CM appears in the list of configured application sequences.
3. Element Cut-through to CM – *[Home -> Elements -> Inventory -> Synchronization -> Communication System]* Click the checkbox for your CM, and then click the "Launch Element Cut Through" button at the bottom of the page.
    a. Enter "change system-parameters features" in the "Command:" box, and click the "Send" button next to it. Click the "Prev Page" button at the top of the display to go to Page 19. Confirm that "SIP Endpoint Managed Transfer" is set to "y". If it is not, change it to "y". Click the "Enter" button.
    b. Enter "change system-parameters ip-options in the "Command:" box, and click the "Send" button next to it. Confirm that "Override ip-codec-set for SIP direct-

media connections" is set to "y". If it is not, change it to "y". Click the "Enter" button.

c. Enter "list signaling-group" in the "Command:" box, and click the "Send" button next to it. In the list of signaling groups, identify the one associated with Session Manager SIP trunk. Note the "Grp No." of that signaling group. Click the "Cancel" button. Enter "change signaling-group <Grp No.>" in the "Command:" box and click the "Send" button (<Grp No.> is the number of the signaling group to examine). Confirm that both "Direct IP-IP Audio Connections?" and "Direct IP-IP Early Media?" checkboxes are set to "y". One enables the other, so if the first is set to "n", the second doesn't appear on the form. If they are not "y", change them both to "y" and click "Enter", then "Done". Otherwise, just click "Done".

Task #3: Download the Latest Endpoint Software

Always confirm that the SIP endpoints will run the latest versions of production software available from the Avaya Support Website, http://support.avaya.com. This section provides detailed instructions to help you understand and accomplish that task, and because the support site continues to evolve over time, ***you should read this section at least once***, even if you've previously downloaded endpoint software from the support site.

The Avaya 96xx and 96x1 telephones ship with H.323 software, and replacing that default software with the latest SIP software is a requirement. The ADVD and 9601 are SIP-only models, so they always ship with SIP software. However, the shipped software typically will not be the latest production SIP software available, so they require software upgrade as well.

As of the date of this document, the latest SIP endpoint software versions are displayed in the following table:

Endpoint	Version	Released
96xx SIP Telephone	2.6.10 (2.6 Service Pack 10)	May 30, 2013
96x1 SIP Telephone	6.3.0	Nov 4, 2013
Avaya Desktop Video Device with the Avaya Flare® Experience (ADVD)	1.1.3	May 16, 2013
Avaya Flare® Experience for iPad®	1.1.4	Dec 6, 2013
Avaya Flare® Experience for Windows	1.1.4	Sept 26, 2013
Avaya one-X® Communicator	6.1.9 (6.1 Service Pack 9)	Sept 16, 2013
Avaya B179 Conference Phone	2.3.8 (media encryption disabled)	Nov 8, 2013
Avaya B179 Conference Phone	2.3.9 (media encryption enabled)	Nov 8, 2013

A link to the Release Notes file or README file for each software download is available on the same web page under the "RELATED DOCUMENTS" category. The Release Notes list the models of phones that the software supports and describe new capabilities, issues fixed, and outstanding issues with that specific release. The notes also provide information useful for installation or upgrade of the software and point out any dependencies. ***The Release Notes document is required reading.*** You also must review any active ***Product Correction Notices (PCN) or Product Support Notices (PSN),*** to check for late-breaking developments that have occurred since the Release Notes were published. *Appendix E - Signing up for PCN/PSN notifications* provides detailed instructions for accessing PCNs and PSNs and for subscribing to

update notifications, so that you will receive automatic update announcements whenever new or updated PCNs and PSNs are published.

Downloading 96xx and 96x1 software

The following procedure provides browser navigational guidance to view and download the latest published software, Release Notes, and PCNs/PSNs for the 96xx and 96x1 telephone sets:

1. Browse to http://support.avaya.com.

2. Click on “Products” (top center of the screen). The “Products” page appears.

3. Enter “one-X® Deskphone” in the “Enter Product Name” box. As you type the characters, matching strings appear in a drop-down menu for that box. Select the first matching entry by clicking on it. The “Choose Release” drop-down menu box then opens, just to the right of the “Enter Product Name” box.

4. Select the desired release in the “Choose Release” drop-down menu:
   a. SIP 6.3.x for 96x1 SIP Phones
   b. SIP 2.6.x for 96XX SIP Phones

   The “Avaya one-X® Deskphone” page appears.

5. Note the PCN, PSN, and Release Notes links that appear under the “NOTICES & RELEASE NOTES” topic at the top right of the page. Now is a good time to retrieve the documentation listed there. For each of these documents, right-click the link, and select “Save link as …”. In the dialogue box that Windows opens, browse to a suitable place on your PC, and click “Save” to download the file. Be sure to read these documents before deploying the new software for the endpoint.

6. Scroll down the page to the “LATEST DOWNLOADS” section. Examine the displayed download links, and locate the link for the 46xxsettings.txt file. Right-click the link, and select “Save link as …”. In the dialogue box that Windows opens, browse to a suitable place on your PC, and click “Save” to download the file.

7. Now locate the link in the same section for the most recent software release. There may be multiple software links, so be sure to identify the link for the most recent release, e.g., “Avaya one-X® Deskphone SIP 6.3.0 Software for the 9601/9608/9611G/9621G/9641G IP Deskphones” is more recent than a similar title showing release 6.2.1. Click on the link for the desired software download. The “Downloads & Documents” page for that software appears.

8. Please note the “DATE RELEASED:” Information, and then read the “SUMMARY:” text in the upper part of the page. If there are references to README files or other important technical information in the SUMMARY text, please do **NOT** ignore them! Notice that this page provides a section at the top right for “RELATED DOCUMENTS”, and a link to the Release Notes typically appears here. If you did not already download the Release Notes in the previous step, now is a good time to do it.

9. Scroll down to the bottom of the page, and click on the download link for the software zipfile. If your browser automatically downloads selected files to your PC's "Downloads" directory, that download will now occur. Otherwise, you will have to interact with a dialogue box to tell Windows where to store the file on your PC. Download the file.

The software downloads are zip archives containing all the relevant files for the release except for the 46xxsettings.txt file, which you download separately. The key files of interest in the zip archives for the 96xx and 96x1 endpoints are described in the following tables. The tables do not cover all the files contained in each zip archive: archives also include language files, certificate files, and a release.xml file that describes the contents of the zip archive.

96xx - Avaya one-X® Deskphone SIP Downloads Release 2.6 Service Pack 10
[**96xx-IPT-SIP-R2_6_10-132005.zip**]

File	Description
96xxupgrade.txt	The 96xx upgrade script. The 96xx SIP telephones process this file to determine whether they are running the latest **SIP** software. A directive within this file causes the endpoint to download and process the 46xxsettings.txt file [GET 46xxsettings.txt]
hb96xxua3_00.bin	The 96xx R2.6 SIP boot application
SIP96xx_2_6_10_1.bin	The 96xx R2.6 SP10 SIP telephone application

96x1 - Avaya one-X® Deskphone SIP Release 6.3.0
[**96x1-IPT-SIP-R6_3_0-092313.zip**]

File	Description
96x1Supgrade.txt	The 96x1 upgrade script. The 96x1 SIP telephones process this file to determine whether they are running the latest **SIP** software. A directive within this file causes the endpoint to download and process the 46xxsettings.txt file [GET 46xxsettings.txt]
S96x1_SALBR6_3_0r73_V4r83.orig.tar	The 96x1 SIP telephone application tarfile for the 9601, 9608, 9611G, 9621G and 9641G deskphones
S96x1_SALBR6_3_0r73_V4r83.tar	The 96x1 SIP telephone application ***upgrade*** tarfile for the 9601, 9608, 9611G, 9621G and 9641G deskphones
S96x1_UKR_V18r2741_V18r2741.tar	The 96x1 6.2 SIP platform system (i.e., kernel and root file system) tarfile for the 9601, 9608, 9611G, 9621G and 9641G telephones

Downloading ADVD Software

The following procedure provides browser navigational guidance to view and download the latest published software, Release Notes, and PCNs/PSNs for the Avaya Desktop Video Device with the Avaya Flare® Experience, also called “ADVD” or “A175”:

1. Browse to http://support.avaya.com.

2. Click on “Products” (top center of the screen). The “Products” page appears.

3. Enter “Desktop Video Device” in the “Enter Product Name” box. As you type the characters, matching strings appear in a drop-down menu for that box. Select the first matching entry by clicking on it. The “Choose Release” drop-down menu box then opens, just to the right of the “Enter Product Name” box.

4. Select the most recent release in the “Choose Release” drop-down menu, e.g., “1.1.x”. The “Desktop Video Device” page appears.

5. Note the PCN, PSN, and Release Notes links that appear under the “NOTICES & RELEASE NOTES” topic at the top right of the page. Now is a good time to retrieve the documentation listed there. For each of these documents, right-click the link, and select “Save link as …”. In the dialogue box that Windows opens, browse to a suitable place on your PC, and click “Save” to download the file. Be sure to read these documents before deploying the new software for the endpoint. You may find release notes for more than one software release. If that is the case, just download the most recent document.

6. Scroll down the page to the “LATEST DOWNLOADS” section. Examine the displayed download links, and locate the link for the most recent software release. There may be multiple software links, so be sure to identify the link for the most recent release, e.g., “Software Release 1.1.3 for the Avaya A175 Desktop Video Device with the Avaya Flare® Experience” is more recent than a similar title showing release 1.1.2. Click on the link for the desired software download. The “Downloads & Documents” page for that software appears.

7. Please note the “DATE RELEASED:” Information, and then read the “SUMMARY:” text in the upper part of the page. If there are references to README files or other important technical information in the SUMMARY text, please do **NOT** ignore them! Notice that this page provides a section at the top right for “RELATED DOCUMENTS”, and a link to the Release Notes typically appears here. If you did not already download the Release Notes in the previous step, now is a good time to do it.

8. Scroll down the page until you locate the link for the Axxxsettings.txt file. Right-click the link, and select “Save link as …”. In the dialogue box that Windows opens, browse to a suitable place on your PC, and click “Save” to download the file.

9. Now click on the link for the software zipfile, e.g., “**A175-IPT-SIP-R1_1_3-021913.zip, 1.1.x**”. This action opens a Single Sign-On (SSO) dialogue for access to https://plds.avaya.com. You are required to authenticate, and if authentication succeeds, a new webpage opens to the PLDS download page for the desired software zipfile. Click the Download link on that page, choose the Download Manager (“Click to

download your file now") or a browser download ("click here") and download the software zipfile to your computer.

The software download is a zip archive containing all the relevant files for the release, including the Axxxsettings.txt file. The key files of interest in the zip archive for the ADVD are described in the following table. The table does not cover all the files contained in the zip archive: the archive also includes a certificate file, a release.xml file that describes all the contained files, and signature files for all of the files contained in the zip archive.

Avaya A175 Desktop Video Device with the Avaya Flare® Experience, Release 1.1.3 [A175-IPT-SIP-R1_1_3-021913.zip, PLDS Download Pub Id ADV00000015]

File	Description
Axxxupgrade.txt	The ADVD upgrade script. The ADVDs process this file to determine whether they are running the latest **SIP** software. A directive within this file causes the endpoint to download and process the Axxxsettings.txt file [GET Axxxsettings.txt]
SIP_A175_1_1_3-021002.tar	The ADVD software tarfile

Downloading Avaya Flare® Experience for Windows

The current navigation instructions to view and download the latest posted software for Avaya Flare® Experience for Windows are as follows:

1. Browse to http://support.avaya.com

2. Click "PRODUCTS" (at the top of the screen). The system displays the "Enter Product Name" box.

3. Enter "Avaya Flare Experience" in the product name box. Select the first matching entry in the drop-down menu that appears. The "Choose Release" drop-down menu box then opens. Select "All" in the "Choose Release" drop down menu.

4. Note the document links for Release Notes, PCNs, and PSNs that appear under the "NOTICES & RELEASE NOTES" topic at the top right of the page. Now is a good time to retrieve relevant documentation listed there. For each of these documents, right-click the link, and select "Save link as …". In the dialogue box that Windows opens, browse to a suitable place on your PC, and click "Save" to download the file. Be sure to read these documents before deploying the new software for the endpoint. You may find release notes for more than one software release. If that is the case, just download the most recent document. If the "View All>" link appears at the bottom of the list, click it to see the entire list of available documents.

5. Look for the software download in the "LATEST DOWNLOADS" section on the lower left of the page. If more than one Avaya Flare® Experience for Windows release is available, click on the link for latest available version, e.g., "**Avaya Flare® Experience for Windows Release 1.1 Service Pack 4**". A summary page then appears for that download.

6. Please note the "DATE RELEASED:" Information, and then read the "SUMMARY:" text. If there are references to README files or other important technical information in the SUMMARY text, please do **NOT** ignore them!

7. Under the "RELATED DOCUMENTS" category at the top right side of the screen, you should see another link to the release notes. If you didn't already retrieve them on the previous page, click on the release notes link here, e.g., "**Avaya Flare® Experience for Windows Release 1.1 SP4 Release Notes**". The browser will typically load the file for viewing. Click "File -> Save Page as" (or the equivalent for your browser), and save the release notes file to your computer.

8. At the bottom of the page, click on the link for the software zipfile, e.g., "**flarewin-1.1.4.23-dist.zip, 1.1.x".** This action opens a webpage for https://plds.avaya.com. You are required to authenticate, and if authentication succeeds, the webpage opens the PLDS download page for the desired software zipfile. Click the Download link on that page and download the software zipfile to your computer.

The key files of interest in the zip archive for the Avaya Flare® Experience for Windows are as follows:

Avaya Flare® Experience for Windows, Release 1.1, Service Pack 4 Sept 26, 2013 [flarewin-1.1.4.23-dist.zip, PLDS Download Pub Id FE000000009]

File	Description
Flare-Windows-1.1.4.23.msi	The installer package for Avaya Flare® Experience for Windows, containing all the files, settings and configuration information necessary to install the application
dotNetFx40_Full_x86_x64.exe	The Microsoft .NET Framework 4.0 standalone installer, used to install the .NET Framework 4.0 software on computers that do not yet have it installed.

Downloading Avaya Flare® Experience for iPad®

Before downloading the software to your iPad®, download and review the Release Notes for the Avaya Flare® Experience for iPad® as follows:

1. Browse to http://support.avaya.com

2. Click “PRODUCTS” (at the top of the screen). The system displays the “Enter Product Name” box, under the “Products” page title.

3. Enter “Avaya Flare Experience” in the product name box. Select the first matching entry in the drop-down menu that appears. The “Choose Release” drop-down menu box then opens. Select “All” in the “Choose Release” drop-down menu.

4. Under the “NOTICES & RELEASE NOTES” category at the right side of the page, notice the links for Release Notes, PCNs, and PSNs. You may also notice that the document links provided apply to either Avaya Flare® Experience for iPad® or Avaya Flare® Experience for Windows. Click on the “View All>” link at the bottom of the list to see all the documentation for Avaya Flare® Experience.

5. Under the “FILTERS” listing at the left side of the page, uncheck all the boxes except the ones for “Release Notes & Software Update Notes” “Product Support Notices”, and “Product Correction Notices”.

6. Click on the link for the most recent release notes specific to the iPad® product, e.g., “**Avaya Flare® Experience for iPad® Devices Release 1.1 SP4 Release Notes**”. The browser will typically load the file for viewing. Click “File -> Save Page as” (or the equivalent for your browser), and save the release notes file to your computer.

The software for Avaya Flare® Experience for iPad® is distributed on the Apple iTunes® App Store rather than in PLDS or ftp.avaya.com. To download and install the latest posted software for Avaya Flare® Experience for iPad®, proceed as follows:

1. On your iPad® 2 (or later hardware version) access the App Store by touching the “App Store” icon.

2. Double-touch the search button (button with a magnifying-glass icon at the top right of the screen) to open the screen keyboard. If the button label displays the character string for a previous search, click the “X” at the right side of the button to clear the button label back to its default, “Search Store”.

3. Enter “Avaya Flare” using the screen keyboard. Touch the “Avaya Flare® Experience” entry in the drop-down menu that appears. The screen displays the available Apps for Avaya Flare® Experience. One of these may show a red Avaya Flare® icon that has a white corner label with the characters “CFE” on it. That version is the “Customer Feedback Edition”, and you should select it only if you are participating in a trial of the beta software.

4. Select the non-CFE version by touching it anywhere except on the “INSTALL” button. The App preview display expands to show “Details”, “Ratings and Reviews”, and “Related” information screens. On the “Details” screen, click the “More” control at the lower right of the display, and scroll down to the “Information” block near the bottom of the text. Confirm that the Version (1.1.4) and Release Date (Dec 6, 2013) are correct for your intended deployment.

5. Touch the “INSTALL” button to download the App and install it. The button label changes from “INSTALL” to “INSTALLING”, and a progress bar appears within the product icon on the display.

6. When the download and install are complete, the “INSTALLING” button label changes to “OPEN”, and you can now launch the App by touching the “OPEN” button.

Since you use the App Store to upgrade software directly on the iPad®, you typically don’t need a browser URL to access the software. However, if you do need such a URL, the direct iTunes® App Store link for the software package for the Avaya Flare® Experience 1.1.4 for iPad®, Dec 6, 2013 is:

https://itunes.apple.com/us/app/avaya-flare-experience/id509528816?mt=8

Downloading Avaya one-X® Communicator Client software

The Avaya one-X® Communicator download is client software that you install on a PC. It is self-contained and requires no access to a fileserver for upgrade or settings file as do some of the other SIP endpoints. To view and download the latest posted client software and Release Notes for Avaya one-X® Communicator:

1. Go to: http://support.avaya.com

2. Click Products (at the top of the screen). The system displays the "Enter Product Name" box.

3. Enter "one-x communicator" in the Product Name box, and click on the matching entry that appears in the drop-down menu as you type. The "Choose Release" box appears.

4. Select the latest version in the "Choose Release" drop-down menu, e.g., "6.1.x"

5. At the lower left side of the screen, under "LATEST DOWNLOADS", click on the link for the latest software version, e.g., "Avaya one-X® Communicator R6.1 with Service Pack 9". The download page for that software appears.

6. Under the "RELATED DOCUMENTS" section at the top right of the page, click on the Release Notes link, e.g., "**Avaya one-X® Communicator Release 6.1 SP9 Release Notes**". The browser will typically load the file for viewing. Click "File -> Save Page as" (or the equivalent for your browser), and save the release notes file to your computer. Click the browser back arrow to return to the download page, or click on the appropriate tab, if the browser opened a new page for the Release Notes display. NOTE: The Release Notes .pdf document is also packaged in the software download zipfile.

7. Note the "Date Released" and version information in the SUMMARY description at the top of the page, and check for any additional information in README files or other notices.

8. At the bottom of the page, click on the link for the software zipfile, e.g.,"**onexc_6.1.9.04.zip, 6.1.x**". This action opens a webpage for https://plds.avaya.com. You are required to authenticate, and if authentication succeeds, the webpage opens the PLDS download page for the desired software zipfile. Click the Download link on that page and download the software zipfile to your computer.

The key files of interest in the zip archive for the Avaya one-X® Communicator Release 6.1 SP8 are as follows:

Avaya one-X® Communicator, Release 6.1, Service Pack 9 Sept 16, 2013
[onexc_6.1.9.04.zip, PLDS Download Pub Id OXC00000048]

File	Description
onexc_setup_6.1.9.04_132.msi	The MSWindows installer package for Avaya one-X® Communicator for Windows, containing files, settings and configuration information necessary to install the application
dotNetFx40_Full_x86_x64.exe	The Microsoft .NET Framework 4.0 standalone installer, used to install the .NET Framework 4.0 software on computers that do not yet have it installed.
LICENSE.rtf	License Terms & Conditions Copy
oneX_Communicator_Client_6_1_SP9_Release_Notes.pdf	Release Notes for this package
onexcuiadmin.exe	1XC GUI for Administrators
Setup.exe	MSWindows 1XC Installer
Setup_Citrix.exe	Citrix Environment 1XC Installer
vcredist_x86.exe	MS Visual C++ Redistributable package
vstor40_x64.exe	MS Visual Studio Tools for Office Runtime, 64-bit version
vstor40_x86.exe	MS Visual Studio Tools for Office Runtime, 32-bit version

Once you have downloaded and unpacked the software, you can install and configure that software on the target PC using the procedures provided in the implementation guide, "**Implementing Avaya one-X® Communicator**".

Downloading Avaya B179 SIP Conference Phone software

The current navigation path to view and download the latest posted client software for Avaya B179 SIP Conference Phone is:

1. Browse to: http://support.avaya.com
2. Click Products (top center of the screen). The system displays the "Enter Product Name" box.
3. Enter "B179" in the Product Name box, and click on the "B179 Conference Phone" drop-down listing entry that appears while you are typing.
4. The "Choose Release" drop-down menu box appears. Select "B179 SIP 2.3.x" from the list. The "B100 Series Conference Phones" page loads.

5. Under the “LATEST DOWNLOADS” section at the lower left of the page, click on the link for the latest B179 SIP Conference Phone Software, e.g., “**Avaya B179 Conference Phone Firmware – Release 2.3.2 Service Pack 2**”

6. Please note the “DATE RELEASED:” Information, and then read the “SUMMARY:” text in the upper part of the page. If there are references to README files or other important technical information in the SUMMARY text, be sure to read them.

7. Notice that this page provides a section at the top right for “RELATED DOCUMENTS”, and a link to the Release Notes typically appears here, e.g., “**Release Notes for Avaya B179 Conference Phone Release 2.3.8 and 2.3.9**”. Click on this link, and your browser will typically load the file for viewing. Click “File -> Save Page as” (or the equivalent for your browser), and save the release notes file to your computer. Click on the browser back-arrow to return to the software download page.

8. **NOTE**: Read the “Configuration notes” at the end of the release notes document before attempting to upgrade your B179 SIP Conference Phone with the new software release! Prior software version 2.2.5 cannot be safely upgraded to later software versions, and if your B179 phones currently have version 2.2.5, you must first perform a reset to factory default software before attempting the upgrade. The instructions for this procedure are provided in the “**Avaya B179 SIP Conference Phone Installation and Administration Guide**”, which you can download using the link provided at the end of this section. The instructions appear on or near page 39.

9. Select the proper software version and file type for your deployment, and click the link for that version and type, e.g., “**AVAYA_B179_v2.3.8.kt, B179 SIP 2.3.x**”. Save the file to your PC. NOTE: Two different file types are available for download:

    a. Files with .kt extension – These are the software files for the B179 SIP Conference Phone. The format is a proprietary Konftel format, hence the “.kt” extension. You use this file type for upgrades if you are manually upgrading the phones.

    b. Files with .zip extension – These are zip archives containing the .kt software files as well as .xml version/release files, a certificate file, and signature files for all the files contained in the archive. You use this file type for upgrades if you are upgrading a group of phones using a device management server.

Once you have downloaded the software upgrade file(s), you can install that software on the B179 SIP Conference Phones via the phone menus (browser), via a device management server, or via SD card. A detailed procedure for each of these methods is provided in “**Avaya B179 SIP Conference Phone Installation and Administration Guide**”.

Task #4: Administer the Fileserver

Install software files on the fileserver

In the previous section, you downloaded the latest 96xx, 96x1, or ADVD software zipfiles from the http://support.avaya.com website. Now you extract the files contained within that zipfile and place them in the distribution directory of the customer's HTTP(S) fileserver. When the 96xx, 96x1, and ADVD endpoints boot, they request those files from the fileserver as part of their boot sequence. The software zipfile contains the following files:

1. For 96xx phones, the software upgrade script file, **96xxupgrade.txt**. The phone executes this script to load and activate the appropriate upgrade software file. The last line in the script directs the phone to retrieve the 46xxsettings.txt file from the fileserver and execute it.
2. For 96x1 SIP phones, the SIP software upgrade script file, **96x1Supgrade.txt**. The phone executes this script to load and activate the appropriate upgrade software file. The last line in the script directs the phone to retrieve the 46xxsettings.txt file from the fileserver and execute it.
3. Phone software image upgrade files, e.g., **S96x1_SALBR6_3_0r73_V4r83.tar**.
4. Language files, e.g., **Mlf_Russian.xml**.
5. Security certificate files, e.g., **av_csca_pem_2032.txt**.

The phones always request the **upgrade script file** first during a reboot. That allows them to upgrade their software to the latest load before attempting a complete boot sequence. The phone retrieves the software specified in the upgrade script, activates it, and reboots automatically. During the reboot, the phone again requests the upgrade script file, but this time the software is already up-to-date, so it next requests the 46xxsettings.txt file from the fileserver and executes it in order to set its internal feature-enabling parameters. Finally, the phone requests the language and certificate files, and then displays the "Username:" and "Password:" prompts, indicating that it is ready for user login.

Install or update the 46xxsettings.txt file on the fileserver

The software zipfile does not contain the **46xxsettings.txt** file, the script file which the phones execute to configure their features. You must download the latest version of that file from support.avaya.com, and modify it appropriately before placing it on the customer's fileserver. The ADVD endpoint uses the file, Axxxsettings.txt, instead of the 46xxsettings.txt file. For simplicity, we'll use "46xxsettings.txt" to refer to either file, since they serve the same purpose, but systems that have ADVDs in addition to SIP hardphones must have both the 46xxsettings.txt and Axxxsettings.txt files on the fileserver.

If the customer's fileserver already has a 46xxsettings.txt file, as is the case for previously-installed H.323 endpoints, then you must:

1. Backup the existing 46xxsettings.txt file.
2. Merge the customer-specific directives in the existing 46xxsettings.txt file into the latest 46xxsettings.txt file that you downloaded from the Avaya support website in the previous section. You can use your favorite text-file editor to perform this merge.

3. Configure any additional directives needed specifically for the SIP phones. Please refer to the additional guidance provided in *Appendix C: Administration guidance and detailed descriptions* and *Appendix G: Proper Selection of 46xxsettings.txt Values*
4. Carefully review the conditional logic in the file, confirming that the changes for the SIP phones do not affect H.323 phones that should remain H.323 phones. This is an especially **critical** task when you introduce 96xx/96x1 SIP endpoints into an environment that already has 96xx/96x1 endpoints permanently deployed as H.323 endpoints. A simple oversight or error in this process can disable the customer's normally-functioning H.323 phones without warning at the next phone reboot.
5. Place the resulting merged and updated 46xxsettings.txt file in the HTTP fileserver's distribution directory.

If this will be the first 46xxsettings.txt file in the customer environment, you use much the same procedure, but there is no previous 46xxsettings.txt file that would require a merge, so you can skip step 2.

Configure 96xx and 96x1 Sets to be SIP Endpoints

The 9601 and ADVD are SIP-only endpoints, so when rebooting, they always request the 96x1Supgrade.txt and Axxxupgrade.txt script files, respectively.

96xx and 96x1 sets can be deployed as either H.323 or SIP phones. Both types use their internal SIG parameter to determine whether they should run SIP software or H.323 software, but the mechanics of changing from H.323 to SIP or upgrading to the latest software differ for the 96x1 versus the 96xx phones.

Both 96xx and 96x1 phones ship from the factory with SIG set to "0" (default) and with H.323 software installed. Converting them to SIP requires changing their internal SIG parameter.

SIG Parameter Considerations for 96xx Phones

SIG takes on one of three values with specific implications for 96xx phones:

0 - Default (96xx phone upgrades to SIP software)
1 - H.323 (96xx phone upgrades to H.323 software)
2 - SIP (96xx phone upgrades to SIP software)

96xx H.323 and SIP phones share a common upgrade script, **96xxupgrade.txt**, so 96xx phones always request that file. The script contains conditional statements that test the value of SIG, and tell the phone which software to download from the fileserver based on the above SIG values.

The value of SIG can only be changed manually on a 96xx phone. You use the local craft procedures access, MUTE 27238#, to select SIG in the menu, set it to SIP (2), Save, and Exit. The phone automatically reboots as a SIP phone, requests the 96xxupgrade.txt script file again, and this time, the conditional logic in the file steers the phone to a SIP software upgrade.

The common upgrade script file is an important consideration specific to the 96xx sets. You must carefully assess the needs of the entire population of endpoints that share the common upgrade script file in the deployment environment:

- Are all 96xx sets that share the fileserver intended to be converted to SIP, or will only a subset be SIP and the remainder remain H.323?

- In the target environment, what are the existing phones' SIG variables already set to? By default, the 96xxupgrade.txt file that is included in the 96xx SIP software zipfile assumes all sets are to be converted to SIP except those with SIG=1/H.323. Therefore, sets with SIG=0/Default and SIG=2/SIP will be converted to SIP sets. The 96xx software download page on support.avaya.com offers a downloadable file titled, "Alternate_96xxupgrade.txt, SIP 2.6.x", which can be manually edited and renamed "96xxupgrade.txt", if there will be a greater subset of H.323 to SIP sets deployed (and therefore only SIG=2/SIP converts to SIP). Always verify the SIG variable value and the particulars of the 96xxupgrade.txt conditional logic to make sure that it meets your specific environment's needs.

SIG Parameter Considerations for 96x1 Phones

In contrast to the 96xx phones, rebooting 96x1 phones request a protocol-specific upgrade script filename based on the SIG parameter's value:

SIG	Protocol	Upgrade Script Filename
0	Default	Based on software already on the set: 96x1**H**upgrade.txt for H.323 phones, 96x1**S**upgrade.txt for SIP phones
1	H.323	96x1**H**upgrade.txt
2	SIP	96x1**S**upgrade.txt

SIG can be set manually on 96x1 phones via the Local Craft Procedures menu. However, unlike the 96xx phones, the 96x1 phones can also have SIG changed *automatically* via the "**SET SIG 2**" directive in the 46xxsettings.txt file or in the DHCP Option #242 string.

NOTE: The ability to *automatically* change the phone's SIG variable on a reboot can have a dark side: incautious deployment can unexpectedly cause all rebooting 96x1 phones to convert from SIP to H.323 software or vice-versa.

IMPORTANT NOTE: Because factory-new 96x1 phones are configured as H.323, they always attempt to download the H.323-specific **96x1Hupgrade.txt** file from the fileserver on their first boot. If that file is not present on the fileserver, the phones' boot sequence fails, and they block. The 96x1 SIP software zipfile that you downloaded in Task #3 above does not include a file named, "96x1Hupgrade.txt". If the fileserver distribution directory does not already contain a file named, "96x1Hupgrade.txt", then you can choose one of the following options to continue:

- If manual intervention is acceptable, then you can access the local craft procedures menu on the blocked phone by entering MUTE 27238#. Set the value of SIG to SIP,

Save, and then Exit. The phone will reboot and request the 96x1Supgrade.txt file on the next fileserver access. That will succeed, and the phone can come into service normally as a SIP phone.

- Where manual intervention is not acceptable, you can modify the DHCP Option 242 string to include "SET SIG 2" before attaching the new phones to the LAN. During their boot sequence, they change the SIG variable at the same time that they get their IP Address, so they subsequently request the 96x1Supgrade.txt file and self-convert to SIP without attempting an H.323 software upgrade.

  NOTE: Because this tactic converts to SIP all 96x1 phones served by this particular DHCP server, you would only use it in an environment that has no H.323 96x1 phones.

- Another automatic technique that does not require a DHCP Option 242 change: you can install on the fileserver the current 96x1 H.323 software release *in addition to the already-installed 96x1 SIP software*. Set the value of SIG to 2 (i.e., SIP) in the 46xxsettings.txt file. In this scenario, a new 96x1 phone first upgrades its H.323 software to the latest version on the fileserver and reboots. Following the reboot, the phone reads in the 46xxsettings.txt file and changes its SIG value to 2 (SIP), which causes the phone to reboot automatically. On this reboot, the phone requests a SIP software upgrade, reboots again, and comes into service normally as a SIP phone. This method is automatic, but a new 96x1 phone requires at least 3 reboots before it comes up as a SIP phone with the latest software.

  NOTE: if the system is a mixed environment with both H.323 and SIP endpoints, you must use conditional logic statements in the 46xxsettings.txt file to steer the H.323 phones that must remain H.323 phones around the "SET SIG 2" directive that you configured for the SIP phones to use. Otherwise, all the H.323 phones will convert to SIP the next time they reboot.

Configure the 46xxsettings.txt file for SIP Endpoint Features

When the endpoints get to the end of the upgrade script file, they encounter the "GET 46xxsettings.txt" directive:

```
# GETSET
GET 46xxsettings.txt
# END
```

The GET directive makes them request the 46xxsettings.txt file from the fileserver and execute it. The 46xxsettings.txt file is a script file that specifies the customer's registration, subscription, and feature configuration for 96xx, 96x1, and ADVD endpoints.

The default 46xxsettings.txt file is a large file (6,606 lines). The 46xxsettings.txt file that you download from support.avaya.com has all but 133 lines commented out, i.e., a "##" at the beginning of a line comments it out. The remaining 133 lines are labels and conditional logic used to steer particular phone models to their respective file sections. Therefore, the default 46xxsettings.txt file doesn't enable any features. To enable a feature, you uncomment its directive, i.e., you remove the "##" at the beginning of its line and set its parameters to appropriate values. For example:

change
SET DOMAIN mycompany.com
to
SET DOMAIN avaya.com

NOTE: The recommended **best practice** for production environments is to remove all comment lines that are not relevant to the settings you actually enable. This shrinks the file to a more manageable size, reducing the risk that you'll introduce an error in a cluttered, lengthy file. You can keep an unmodified copy of the default 46xxsettings.txt file on your PC, should you need to enable additional directives or reference the original comments.

For the purposes of this section, your immediate goal is basic SIP phone installation, and the key directives that you enable within this file allow the 96xx and 96x1 endpoints to initially register with their Avaya Aura Session Manager(s). You must uncomment these directives and set appropriate values. These directives can be found by searching the 46xxsettings.txt file with your text editor. The directives that you activate are SIPDOMAIN, SIP_CONTROLLER_LIST, and SIMULTANEOUS_REGISTRATIONS. The relevant entries have been extracted from the latest 46xxsettings.txt file and are shown below, with the directives in **bold** font:

```
#############  CALL SERVER SETTINGS (ALL SIP)  #############
##
## SIPDOMAIN specifies the domain name to be used during SIP
registration.
##  The value can contain 0 to 255 characters; the default value is
null ("").
##  This parameter is supported by:
##       1603  SIP  R1.0 and later software releases
##       16CC  SIP  R1.0 and later software releases
##       364x  SIP  R1.0 and later software releases (up to 60
characters only)
##       46xx  SIP  R2.2 and later software releases
##       96x0  SIP  R1.0 and later software releases
##       96x1  SIP  R6.0 and later software releases
SET SIPDOMAIN    "example.com"

############  CALL SERVER SETTINGS (LATEST SIP)  ############
##
## SIP_CONTROLLER_LIST specifies a list of SIP controller designators,
##  separated by commas without any intervening spaces,
##  where each controller designator has the following format:
##  host[:port][;transport=xxx]
##  host is an IP address in dotted-decimal or DNS name format.
##  [:port] is an optional port number.
##  [;transport=xxx] is an optional transport type where xxx can be
tls, tcp, or udp.
##  If a port number is not specified a default value of 5060 for TCP
and UDP or 5061 for TLS is used.
##  If a transport type is not specified, a default value of tls is
used.
##  The value can contain 0 to 255 characters; the default value is
null ("").
##  This parameter is supported by:
##       1603  SIP  R1.0 and later software releases
```

```
##       96x0  SIP  R2.4.1 and later software releases
##       96x1  SIP  R6.0 and later software releases
SET SIP_CONTROLLER_LIST
proxy1:5061;transport=tls,proxy2:5061;transport=tls

## SIMULTANEOUS_REGISTRATIONS specifies the number of Session Managers
##  with which the telephone will simultaneously register.
##  Valid values are 1, 2 or 3; the default value is 3.
##  This parameter is supported by:
##       96x0  SIP  R2.6 and later software releases
##       96x1  SIP  R6.0 and later software releases
SET SIMULTANEOUS_REGISTRATIONS 3
```

SIPDOMAIN must match the SIP Domain provisioned on Avaya Aura Session Manager (using SMGR) and the Avaya Aura Communication Manager Server.

SIP_CONTROLLER_LIST indicates in order of priority, the Primary, Secondary, and Tertiary (SIP Survivable Server) Session Managers, to which the 96xx and 96x1SIP phones attempt to simultaneously register.

NOTE: the port number and transport elements of the SIP_CONTROLLER_LIST string may be optional for your installation. If you omit them in the string, the phones default them to port **5061** and **tls**.

That is, this SIP_CONTROLLER_LIST:

```
SET SIP_CONTROLLER_LIST proxy1:5061;transport=tls,proxy2:5061;transport=tls
```

Is functionally identical to this SIP_CONTROLLER_LIST:

```
SET SIP_CONTROLLER_LIST proxy1,proxy2
```

SIMULTANEOUS_REGISTRATIONS indicates the maximum number of Avaya Aura Session Managers to which phones will simultaneously register. For example, if you have two SMs, you set this value to two. The default value is 3, to allow for a survivable remote, i.e., Branch Session Manager, or "BSM", in addition to the primary and secondary SMs.

NOTE: SIMULTANEOUS_REGISTRATIONS applies **only** to Avaya Aura® Session Managers and Avaya Aura® Branch Session Managers. If you have two SMs and a 3rd-party survivable SIP server, you have three SIP Controllers, but you would only set SIMULTANEOUS_REGISTRATIONS to 2. If your solution deploys three SMs and no BSMs and uses only TLS for the transport protocol, you can specify 3 simultaneous registrations. Before configuring such an arrangement, please read the relevant detailed discussion in *Appendix C: Administration guidance and detailed descriptions.*

The "Data for HTTP(S) Fileserver" table in the *Task #1: Collect Configuration Data* section provides some additional directives that you may find desirable for your initial installation.

Once these parameter values are modified and uncommented, save the file (as text) on the fileserver, and save a backup copy as well.

As you build out your system, you'll need to enable additional features on the 96xx, 96x1, and ADVD endpoints, e.g., Instant Messaging, Presence, etc. For additional background and guidance, please see *Appendix G: Proper Selection of 46xxsettings.txt Values.*

Task #5: Administer the DHCP Server

The Avaya 96xx, 96x1, and ADVD SIP sets can process, via DHCP Option #242, a subset of configuration parameters that are provided in the 46xxsettings.txt or Axxxsettings.txt files. The document, Administering Avaya 9601/9608/9611G/9621G/9641G IP Deskphones SIP, Release 6.3, lists the specific parameters that can be set via DHCP Option #242. The document, *Implementing and Administering Avaya A175 Desktop Video Device with the Avaya Flare® Experience Release 1.1*, provides the same information for the ADVD. In these guides, the table is named: "**Parameters Set by DHCP"**. The DHCP settable parameters for the 96xx, 96x1, and ADVD models are shown in the following table, and defined in the respective administration guides:

Parameter	96xx	96x1	ADVD
DNSSRVR	X	X	
DOMAIN	X	X	
DOT1X	X	X	
DOT1XSTAT	X	X	
DSTOFFSET	X	X	X
DSTSTART	X	X	X
DSTSTOP	X	X	X
GMTOFFSET	X	X	X
HTTPDIR	X	X	X
HTTPPORT	X	X	X
HTTPSRVR	X	X	X
ICMPDU	X	X	X
ICMPRED	X	X	X
L2Q	X	X	X
L2QVLAN	X	X	X
LOCAL_LOG_LEVEL	X	X	
LOGSRVR	X	X	X
MSGNUM	X	X	X
MTU_SIZE	X	X	X
PHY1STAT	X	X	X
PHY2STAT	X	X	X
PROCPSWD	X	X	X
PROCSTAT	X	X	X
SIG	X	X	
SIP_CONTROLLER_LIST	X	X	X
SNTPSRVR	X	X	X
TLSDIR	X	X	X
TLSPORT	X	X	X
TLSSRVR	X	X	X
VLANTEST	X	X	X

A typical DHCP Option #242 string will vary depending on the customer's unique deployment environment, and on whether LLDP-MED is used instead of DHCP to provision certain parameters. Also, when customers segregate their LAN traffic into voice and data populations by implementing VLANs, the phones will encounter two DHCP scopes: one for data and one for voice. Each scope provides its own Option #242 string, as the following example illustrates.

Voice/Data VLAN Example:

- The SIP telephone initially connects to the default "Data VLAN", using the IP address it acquires during its first DHCP discovery sequence not using 802.1Q tagged frames.
- The DHCP server provides DHCP Option #242 for the Data VLAN scope, which specifies the VLAN ID for the "Voice VLAN" and enables 802.1Q tagging by setting L2Q=1. For example, if the Voice VLAN is VLAN ID 100, then the initial DHCP Option #242 string looks like this:

  L2Q=1,L2QVLAN=100.

- Once the SIP telephone obtains the "Voice VLAN ID" via DHCP Option #242, it releases its IP address on the "Data VLAN" and repeats the DHCP discovery process, this time with 802.1Q tagging enabled. It uses the L2QVLAN value (100 in this case) for the "Voice VLAN", and initiates a new DHCP request on the "Voice VLAN". The "Voice VLAN" Option #242 string might look like this:

  HTTPSRVR=192.168.13.6,TLSSRVR=192.168.13.6,SNTPSRVR=192.168.13.8

  Where HTTPSRVR is the non-secure fileserver address, TLSSRVR is the secure fileserver address, and SNTPSRVR is the secure time server address.

It is important that at least the fileserver address is provided in DHCP Option #242 for the SIP sets. They must access the fileserver in order to:

1. Initiate the download of the correct upgrade script:
   - 96xx: 96xxupgrade.txt
   - 96x1: 96x1Supgrade.txt
   - ADVD: Axxxupgrade.txt

2. Download/upgrade their software based on their signaling type (SIP or H.323) and the software versions available on the fileserver.

3. Download and process the 46xxsettings.txt or Axxxsettings.txt file, to set the remaining configuration parameters.

Because the 46xxsettings.txt file can specify <u>all</u> the other available configuration parameters, the recommended **best practice** is to specify **<u>only</u>** the fileserver address(s) in the DHCP Option #242 string, and have the phones use the 46xxsettings.txt file for everything else. Example exception: you may choose to specify GMTOFFSET, DSTOFFSET, DSTSTART, and DSTSTOP in the Option #242 string, if your endpoints reside in different time zones, and you don't want to implement location-specific 46xxsettings.txt files.

Please note that you can also implement location-specific (or user-job-function-specific) phone behaviors by using the GROUP feature in the 46xxsettings.txt file and in the phones. You manually assign each phone to a GROUP using the phone's Local Craft Procedures menu, and then add conditional logic to the 46xxsettings.txt file to steer a GROUP's phones to the correct directives for their location or functional sub-group. To see how this scheme works, examine the default 46xxsettings.txt file, and search for lines containing the string "GROUP". The default file provides five example GROUPs that you can use as a template.

Task #6: Administer User in System Manager

Task Overview

You now use the Avaya Aura® System Manager (SMGR) web interface to administer the user for the endpoint. The administered data includes:

- **User Identity**: user name, login name, display name, language preference, time zone
- **Communication Profile**: telephone password, user handle(s), which Avaya Aura® Session Managers (SM) to use for registration, which Avaya Aura® Communication Manager(s) (CM) to use for call origination and termination, location, extension, set type and features (including all CM-specific station administration), voicemail number/mailbox/password
- **Roles**: for example, End-User, Auditor, Administrator, etc.
- **Contacts**: private contacts, presence buddies.

When you submit the completed user administration, SMGR then provides the new user information to the SM(s) and Presence Server via database replication and to CM by logging into the CM and executing the "add station" command. Now the SM(s) have all the information necessary for the endpoint to successfully register when it is connected to the LAN. When the user subsequently logs in on the endpoint, the phone downloads its feature subscriptions and data from SM (button definitions, enabled features, contact lists, etc.), and the user can then originate and receive calls using the endpoint.

Note: The System Manager administration forms have drop-down menus that allow you to select which SM, which CM, etc. the endpoint will use for registration and calls. If the prerequisite system administration has not been performed for those selections, then the SMGR drop-down menus will be empty, or will not offer the selection you need, and you will not be able to complete user administration. When you executed *Task #2: Confirm System Component Administration*, you confirmed that the prerequisite system administration has been properly completed. You must have performed that confirmation before you attempt to administer the first user!

Accessing the System Manager administration interface

1. Open a browser (Firefox, Internet Explorer, Chrome, etc.) and enter the SMGR secure HTTP URL:

   https://example-smgr-fqdn or https://192.168.13.3/

2. Login using an account configured with the Network Administrator and System Administrator roles. The default “admin” account has such privileges, but if you are not authorized to use it, you can use any SMGR account that has those roles assigned to it.

3. Go to **Users > User Management > Manage Users**

4. Click **New**. The system displays the “New User Profile” page. Note that there are four tabs: Identity, Communication Profile, Membership, and Contacts.

5. Begin with the Identity tab, and fill in the fields using the values that you previously provided in the SMGR table in the configuration data section Data for System Manager.

Configuring User Profile – Identity

1. If you are not already on the Identity tab of the New User Profile page, navigate to **Users > User Management > Manage Users**, and click **New**.

2. Fill in the user’s **Last Name.**

3. Fill in the user’s **First Name.**

4. Fill in the **Login Name**. The format of the entry is user-handle@domain. This login is typically extension@SIP-Domain, where “extension” is the CM extension used to login the phone. However, the handle can also be an alphanumeric string.

   Example: user1@avaya.com

5. Confirm that “Basic” is selected in the **Authentication Type** drop-down menu.

6. Enter the user’s desired password for self-administration access to SMGR in the **Password** field.

7. Re-enter the user’s desired self-administration password in the **Confirm Password** field.

8. Fill in the **Localized Display Name**. This is typically the user’s full name.

9. Fill in the **Endpoint Display Name**. This is also typically the user’s full name, but it may differ from the Localized Display Name for locations where the endpoint cannot handle the Localized Display Name, i.e., because the endpoint display does not support a particular location-specific character set.

10. Select the desired language in the **Language Preference** drop-down menu.

11. Select the desired time zone in the **Time Zone** drop-down menu.

Configuring User Profile - Communication Profile

1. Select the Communication Profile tab.

2. Fill in the **Communication Profile Password** field. This is the password the user enters to login on the SIP phone.

3. Fill in the **Confirm Password** field.

4. Leave the **Name** field set to the default, “Primary”.

Configuring User Communication Address

1. If the Communication Address section is not fully expanded, click the right-arrow-circle icon to the right of “Communication Address” to open the section.

2. Click **New**.

3. Select the type of communication address in the **Type** drop-down menu. The type specifies the category of communications infrastructure for which the communication address will be used. Examples include E.164, Avaya SIP, Googletalk, IBM Sametime, Jabber, Lotus Notes, etc. You must configure at least an **Avaya SIP** communication address, and most installations also require an **E.164** type communication address.

4. Enter the user’s handle in the **Fully Qualified Address** field, and then select the appropriate domain in the @ drop-down menu. The user’s handle may be any of several character strings, including a username, an extension (short, long, canonical, E.164), etc. You must specify a handle/dial string that will provide a correct source or destination address for the type of infrastructure that will process it.

   Note: Please see **“Implementing End-to-End SIP, Vol 2: Designing SIP Telephone Signaling, Number and Dial Plan Options",** for detailed guidance in selecting the correct SIP handle and CM dial string. Once you’ve selected the correct format for the first user, you can continue to use it for other users in the same community, **but it is critically important that the selected handle and dial string are compatible with the SM-CM topology deployed.** If the entire Volume 2 seems intimidating, focus on the four example configuration scenarios discussed there, and determine which one most closely matches your topology. Then choose your handles and dial strings based on the guidance for that scenario.

5. If the user requires more than one Communication Address, click the “New” button to add the next one. Repeat as many times as necessary, to complete the list of addresses.

Configuring User Session Manager Profile

1. If the Session Manager Profile section is not fully expanded, click the right-arrow-circle icon to the right of “Session Manager Profile” to open the section.

2. Select the primary Session Manager from the **Primary Session Manager** drop-down menu.

3. Select the secondary Session Manager from the **Secondary Session Manager** drop-down menu.

4. Select the entry for the correct CM in the **Origination Application Sequence** drop-down menu.

5. Select the entry for the correct CM in the **Termination Application Sequence** drop-down menu. (**Note**: for CMs configured as Evolution Servers, the same CM provides both origination and termination processing, so the same drop-down menu selection is used for both this field and the one above it. This document addresses only systems using CM-Evolution Servers at this time.)

6. If your system has a Branch Session Manager (BSM) for survivability scenarios involving your SIP phones, then select that BSM in the drop-down instead of the default. Otherwise, leave the **Survivability Server** drop-down menu selection at the default, "(None)". Survivability servers that are not SMs or BSMs (e.g., Avaya Secure Router SR2330, IP Office) cannot be specified in this field.

7. Select the correct location from the **Home Location** drop-down menu.

Configuring User Endpoint Profile

1. If the Endpoint Profile section is not fully expanded, click the right-arrow-circle icon to the right of "Endpoint Profile" to open the section.

2. Select the correct CM system for the endpoint from the **System** drop-down menu.

3. Leave the **Profile Type** drop-down menu selection at "Endpoint".

4. Choose the appropriate action:

    a. If the extension for this user has not been previously configured in this CM, skip the **Use Existing Endpoints** check-box, leaving it unchecked.

    b. If the extension is already configured in CM, but is not currently associated with a user, and you intend to assign your user that extension, click the **Use Existing Endpoints** check-box.

5. Enter the extension in the **Extension** field. Use the canonical form, i.e., on a CM with a 7-digit dial plan, enter the 7-digit dial string for the extension.

6. From the **Template** drop-down menu, select the template definition most suitable for the specific endpoint you're deploying. Example: for a 9641G SIP telephone, choose DEFAULT_9641SIP_CM_6_3 in the drop-down menu listing. Note that the **Set Type** field automatically populates when you complete your selection. Default templates used for the various available SIP endpoints other than 96xx and 96x1 are:

    a. ADVD – ADVD
    b. Avaya one-X® Communicator – DEFAULT_9641SIP_CM_6_3
    c. Avaya Flare® Experience for Windows – DEFAULT_9641SIP_CM_6_3
    d. Avaya Flare® Experience for iPad® Devices – DEFAULT_9641SIP_CM_6_3

e. Avaya B179 SIP Conference Phone – DEFAULT_9641SIP_CM_6_3

Note: If the endpoint is for a mobile user, select the highest-number station type that a user will log into. For example, if a user logs into 9620 and 9630 stations, administer that user's station with type 9630. The highest-number station type is used because a user can log into that station as well as lower-number station types and have similarly-labeled buttons. For example, a user with station type 9630 can log into a 9630, 9620, 9610, and 9601 station. Although that user can log into a station type 9640, some of the buttons may be undefined, mislabeled, or confusing. Also, some buttons administered on a 9630 station are not accessible when logged into a 9620 station.

7. Skip the **Security Code** field. It is not relevant for SIP endpoints.

8. Enter "IP" in the **Port** field.

9. Enter the voice mail system telephone number in the **Voice Mail Number** field, if voicemail integration is part of your deployment.

10. If you want the system to automatically delete this user's station in CM whenever that user is unassigned or deleted in System Manager, check the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check-box.

11. For the SIP endpoints other than 96xx and 96x1, you must modify some of the default station parameter/feature/button settings provided by the station template that you selected in the **Template** field. Click the "Endpoint Editor" button. System Manager will display all the CM parameter/feature/button settings that appear on the "add station" CM forms, and you can make the required changes. The following changes are necessary for the various non-96xx/96x1 SIP endpoints:

    a. ADVD – 5 call appearances, enable IP SoftPhone, enable IP Video SoftPhone, enable Bridged Call Alerting (for bridged call appearances).
    b. Avaya one-X® Communicator – 3 call appearances, enable IP Video SoftPhone, enable Bridged Call Alerting (for bridged call appearances)
    c. Avaya Flare® Experience for Windows – 8 call appearances, enable IP SoftPhone, enable IP Video SoftPhone, enable Bridged Call Alerting (for bridged call appearances).
    d. Avaya Flare® Experience for iPad® Devices – 8 call appearances, enable IP SoftPhone, enable IP Video SoftPhone, enable Bridged Call Alerting (for bridged call appearances).
    e. Avaya B179 SIP Conference Phone – 4 call appearances

Configuring User Messaging Profile (optional)

1. If the Messaging Profile section is not fully expanded, click the right-arrow-circle icon to the right of "Messaging Profile" to open the section.

2. Select the desired messaging system from the **System** drop-down menu.

3. If the user is already configured as a subscriber on the messaging system, click the **Use Existing Subscriber on System** check-box. Otherwise, leave it unchecked.

4. If you checked the **Use Existing Subscriber…** check-box in the previous step, enter the user's mailbox number in the **Mailbox Number** field.

5. Select the correct template for the user from the **Template** drop-down menu. Example: DEFAULT_CMM_6_2

6. Enter the numeral, 1, in the **Password** field. That value causes the user to be prompted to change voicemail password on next login to messaging.

7. If you want the system to automatically delete this user's mailbox whenever the user is deleted or this messaging profile is removed in SMGR, check the **Delete Subscriber on Unassign of Subscriber from User or Delete User** check-box.

Configuring User Profile – Membership (optional)

1. Click on the **Membership** tab at the top of the form.

2. Click **Assign Roles**.

3. Check the check-box for any role that is appropriate for this user. All users have the End-User check-box checked by default.

4. Click **Select** at the bottom of the form to return to the New User Profile form.

Configuring User Profile – Contacts (optional, but required for Presence)

Note: 96xx require a minimum of 2.6.6 software for presence. 96x1 phones require SIP software later than 6.0.3/6.1.3 to support presence.

1. Click on the **Contacts** tab at the top of the form.

2. Click **Add**.

3. Check the check-box for any contact that should be included on this user's contact list.

4. Click the Select button. The list of contacts for this user is now populated.

5. To make any particular contact a "Presence Buddy" (that is., to subscribe to the contact's presence updates), click the check-box on that contact's line, and then click the Edit button.

6. Enter the contact's first and last name in the **Label** field.

7. Check the **Presence Buddy** check-box.

8. Click **Add**.

9. Confirm that the contact now shows “Yes” in the “Presence Buddy” column of the contact list.

10. Click **Commit** to save the entire user profile.

Saving CM translations

Note: You must perform this procedure! If you do not save CM translations, and the CM restarts before the next periodic translation save (10:00 PM daily by default), the CM administration that was performed for your user is lost. Your only option if that happens is to delete the user and start over.

1. Navigate to **Elements >Inventory >Synchronization >Communication System**

2. Click the check-box for your CM system.

3. Select the radio button next to **Save Translations for the selected devices**.

4. Click **Now** at the bottom of the form.

5. When the form has refreshed, confirm that “Completed” appears under **Sync Status** for your CM System.

At this point, you have:

- Downloaded and extracted the latest SIP software files, language files, and certificate files and transferred them into the distribution directory of the fileserver. The phones can download these files during their boot sequence.

- Configured the DHCP scope(s). The phones will be able to get IP addresses on the correct VLAN and acquire their fileserver address.

- Reviewed and confirmed the conditional logic in the 96xxupgrade.txt file. If you have a mixed H.323/SIP 96xx phone population, the rollout of new SIP phones will not cause existing H.323 phones to convert to SIP, when you intend them to remain H.323.

- Merged the customer’s existing 46xxsettings.txt file with the latest published 46xxsettings.txt file, enabled the directives necessary for proper endpoint registration, and placed the resulting file in the distribution directory of the fileserver. The phones can retrieve and execute this file, and can then register with their Session Manager(s).

- Configured in the 46xxsettings.txt file the appropriate SIG values and conditional logic to convert new H.323 96x1 phones to SIP, if automatic conversion is your intent.

- Edited the 46xxsettings.txt file to configure additional feature parameter settings, so that phone features like IM, presence, etc., will function properly.

- Administered users in SMGR so that users may login on the phones and CM, SM, and Presence Services will interwork with the phones as they register, subscribe to features, and make calls.

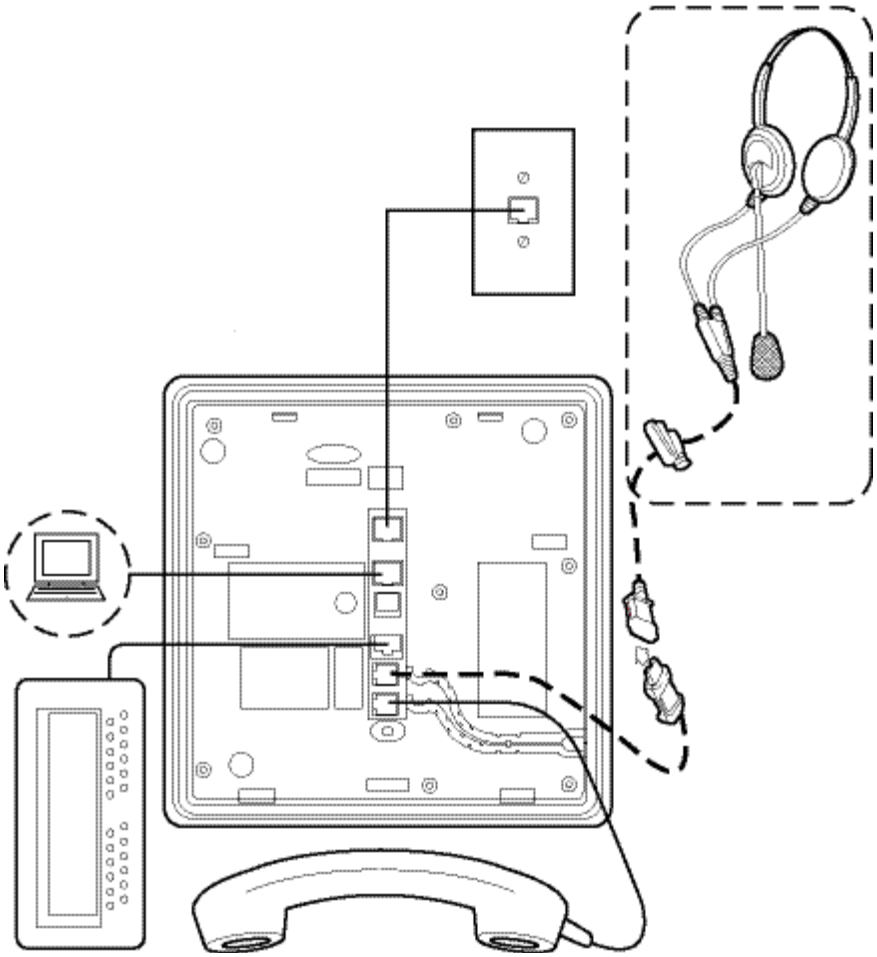
Now you are ready to unpack, assemble, network, and initially configure the SIP endpoints.

Task #7: Unpack and Assemble the Endpoint

Follow the assembly instructions in the installation guide for the particular model of phone:

For 96xx phones, *Avaya one-X(R) Deskphone SIP Installation and Maintenance Guide Release 2.6*
For 96x1 phones, *Installing and Maintaining Avaya Deskphone SIP for 9601/9608/9611G/9621G/9641G IP Deskphones, Release 6.3*
For ADVD, *Avaya A175 Desktop Video Device Installation and Safety Instructions*.
For B179 SIP Conference Phones, *Avaya B179 SIP Conference Phone Installation and Administration Guide*

Typical connectivity for the 96x1 phones is shown in the following diagram from the Installation and Maintenance Guide:



Confirm with the customer the method used to power the phone:

- IP Phone Single Port PoE Injector, SPPOE-1A, sometimes called a “power brick”. NOTE: the earlier 1151C and 1151D external power supplies may NOT be used with the 96x1 series of phones.
- Power over Ethernet – IEEE 802.3af, with power being provided by the customer’s Ethernet switches. The 96xx and 96x1 phones are all either Class I or Class II PoE devices. The Avaya B179 SIP Conference Phone is a Class III PoE device, and it may alternatively be powered by its own AC Power Adapter.

If you plan to equip the phone with button module(s), be aware that:

- 12-button and 24-button modules cannot be mixed on a single phone.
- Adding button modules to a phone increases its power consumption. This may become an issue if the customer’s data infrastructure has limited Power-over-Ethernet capacity per port. The “*Assembling the Deskphone*” of the *Installing and*

Maintaining Avaya Deskphone SIP for 9601/9608/9611G/9621G/9641G IP Deskphones, Release 6.3 includes a table that specifies the additional power consumption for various combinations of phone and button modules.

Task #8: Connect the Endpoint to the Network

96xx and 96x1 Endpoints First LAN Connection

Connect the set to the customer LAN with an Ethernet cable attached to the LAN port on the set. Be careful to use only the jack with the Network symbol for this connection. That symbol resembles the silhouette of an RJ45 jack.

Concerns include:

- Phones are not shipped with Ethernet cables. You must provide the cable at installation time.
- Cabling must be appropriate for the expected line speed. Use Cat-5E or better manufactured cables (endpoints attached at the factory) as a **best practice**.
- Those endpoints with model names that end in "G", i.e., 9611G, 9621G, and 9641G, have integrated **G**igabit Ethernet-capable switches, and will autonegotiate line speed to that level if the customer's Ethernet switch also supports it.
  IMPORTANT: Confirm that the customer's interconnecting cabling is compatible with Gigabit Ethernet operation. Customer installations that use 110-blocks or many types of "Ethernet Patch Panels" for cable interconnection are NOT compatible with Gigabit Ethernet operation, although they are acceptable for 100BaseT operation when installed properly. If the cabling is not suitable for Gigabit Ethernet, it will be necessary to lock the switch ports and phones to 100BaseT, or else configure the customer's Ethernet switches to restrict speed autonegotiation above 100BaseT.
- Some customer desktops may have only a single network jack available, and you must interconnect the phone with another networked device. In such cases, confirm that such a connection does not block forwarding of tagged packets to all downstream connected devices. Stated differently, ensure that each connected endpoint can access the correct VLAN, "voice" or "data", for normal operation.

When you connect the phone to the network, it will power up and begin its normal boot sequence. Details of the boot sequence are provided in *Appendix G: Proper Selection of 46xxsettings.txt Values*. As explained previously, you may need to interrupt the boot sequence of a 96xx or 96x1 phone in order to change its SIG variable to SIP. Otherwise, you expect the phone to perform its normal startup operations, upgrade its software, retrieve its configuration settings, and then offer you a login screen.

ADVD First LAN Connection

The ADVD first LAN connection looks very much like that of the 96x1 SIP phone:

1. The ADVD acquires its VLAN, IP address, and fileserver addresses from the DHCP server, using the Option 242 string parameters just like the 96x1 phone.
2. The ADVD requests the Axxxupgrade.txt script file from the fileserver and executes it. The ADVD determines whether the software available on the fileserver is newer than its current software, and self-upgrades in the background if it is.
3. The ADVD requests the Axxxsettings.txt script file from the fileserver and executes it, setting the remainder of its internal parameters in accordance with the directives in that script file.
4. The ADVD displays the user login control, indicating that it is networked and ready for the user to login with extension and password.

Avaya one-X® Communicator First LAN Connection

You launch Avaya one-X® Communicator on a PC which is already connected to the LAN, so application start-up uses the already-connected network to register with a SIP Controller for the first time. You must configure minimal networking and registration parameters for the registration to succeed. You perform that configuration in one of three ways:

1. Via the Setup Wizard, a GUI which activates automatically when you first launch one-X® Communicator. It walks you through the initial setup process, and when you've provided the required values, including the SIP vs. H.323 selection, SIP Controller IP address, SIP Domain, etc., it then registers with the SIP controller.

2. Manually, using the Telephony Configuration form in the user interface "Settings" interface. You can launch this interface at any time, even after the application has been in use for some time, to set or modify parameters. If you modify an existing H.323 one-X® Communicator installation to convert it to SIP, you must restart the application, so the change can take effect.

3. Via *Auto Configure Settings*, using the Avaya one-X® Communicator Centralized Administration Tool, which is driven by:

    a. Directives in the 46xxsettings.txt file on the customer's fileserver.
    b. XML configuration files that you create, in order to modify the default directives retrieved from the 46xxsettings.txt file.

    This tool is used in large-scale deployments. You can save the settings in XML files and use these files to configure Avaya one-X® Communicator settings on more than one user PC.

Detailed instructions for the Setup Wizard and manual setup are provided in ***Implementing Avaya one-X® Communicator*****.**

Detailed instructions for building the XML configuration files for the Auto Configure Settings option are provided in ***Avaya one-X® Communicator Centralized Administration Tool Guide*****.**

Avaya Flare® Experience for Windows First LAN Connection

When you initially launch Avaya Flare® Experience for Windows, it displays the "Settings" dialogue box, and you fill in the parameters required for connection, i.e., SIP Controller FQDN or IP Address, Port, Transport Type, SIP Domain, dialing rules for your location, LDAP server address, if you have one, etc. When you have supplied the parameters, the application registers, and you can login and make calls.

Avaya Flare® Experience for iPad® Devices First LAN Connection

When you initially launch Avaya Flare® Experience for iPad® Devices, you Accept the End User License Agreement and then tap the "Settings" button. You then fill in the Service parameters required for connection, i.e., SIP Controller FQDN or IP Address, Port, Transport Type, and SIP Domain. There are also sections for dialing rules for your location, LDAP server address, if you have one, conference and presence server information, etc. When you have supplied the parameters, you tap "Done" to close the Settings dialogue, the application registers, and you can login and make calls.

Avaya B179 SIP Conference Phone First LAN Connection

Detailed instructions for the first connection of the Avaya B179 SIP Conference Phone are provided in the "*Avaya B179 SIP Conference Phone Installation and Administration Guide*" beginning on page 2. You configure the phone's network parameters using the built-in keypad and display, and once the phone is networked, you can access its administration interface via web browser:

1. You access the keypad/display settings administration by pressing the gear symbol key at top center of the keypad, then navigate using the display menus to the Settings section. The Network Parameters are accessed using the "Advanced" settings menu option, and you must supply the administrator's PIN code to modify them. The default PIN code is "1234".
2. Browser login for administration is "Admin" with PIN code 1234. The browser displays the administration GUI, on which the various administration categories appear as tabs, e.g., SIP, Network, Media, LDAP, Web Interface, Time & Region, etc.

Task #9: Change Endpoint's Signaling Type from H.323 to SIP

Some Avaya endpoint types can operate as either H.323 or SIP, while others are SIP-only:

SIP-Only Endpoints: No Change Required

9601 SIP phones, the ADVD, the Avaya B179 SIP Conference Phone, and the Flare Experience for Windows and iPad can only function as SIP endpoints. Skip to *Task #10: Confirm Software Update*.

Avaya one-X® Communicator: Settings Change

The Avaya one-X® Communicator client is configured as H.323 or SIP when you select the desired protocol value in the **Settings** GUI during installation and configuration of the client software. This is always a *manual* operation, i.e., no automatic mechanism changes the client behavior from one protocol to the other at any time. Set the desired protocol during first client startup, and skip to *Task #10: Confirm Software Update*.

96xx Phones: Changing the SIG Parameter

96xx phones rely on the internal SIG parameter to control whether they operate as H.323 or SIP phones, and you can only change the phone's SIG parameter *manually*. When you first connect new 96xx phones to the LAN, the display shows progress bars that advance as the phone loads its internal software and begins to execute it:

1. When the phone displays **"* to program**", hit the "*****" button.
2. The phone displays "**Enter code:**". Enter 27238# on the keypad. The phone displays the local craft procedures menu.
3. Scroll down to "**SIG**", press "**Start**" to select it.
4. Change the value to "**SIP**".
5. Press "**Save**".
6. Press "**Exit**", and the phone reboots with SIG set to SIP.

96x1 Phones: Changing the SIG Parameter

96x1 telephones use the SIG variable much like 96xx phones do, but with 96x1 phones, you can change the phone's SIG variable *manually*, or you can cause it to change *automatically* in the phone by including "SET SIG 2" in the DHCP Option 242 string or the 46xxsettings.txt file, either of which effects a reboot of the phone with SIG changed to the new value.

If you elect to use the manual method, interrupt the initial boot sequence by pressing the "Program" button when it first appears on the phone display during boot, enter the code, 27238#, and set SIG to SIP as with the 96xx phone above.

If you have configured the DHCP Option 242 string or 46xxsettings.txt file to automatically change SIG to SIP, observe the phone display while it repeatedly reboots, to confirm that it requests the 96x1Supgrade.txt file from the fileserver and then upgrades to the SIP software. When the phone finally displays "Username:" and "Password:", hit the MUTE button followed by 27238#, scroll down to SIG, and confirm that SIG is now set to SIP. Use "Back" and then "Exit" to return to the login screen without rebooting the phone.

NOTE: if "**SET SIG 2**" is activated in the 46xxsettings.txt file, you must also provide conditional logic in that same file to steer those H.323 96x1 phones that must remain H.323 phones around it, else all your customer's H.323 96x1 phones will self-convert to SIP the next time they reboot.

Complicating factors to consider prior to deployment:

The customer may require different features or software releases for various groups of phones. For example, introduction of a new software release may be trialed on only a subset of phones initially, not the entire population. You may need to implement the GROUP feature on the phones, in the 96xxupgrade.txt file, in the 96x1Supgrade.txt file, and in the 46xxsettings.txt file, to manage these select groups of phones. The default 46xxsettings.txt file that you download from support.avaya.com comes with five GROUP directives that you can utilize as a template for this purpose, and to understand how group settings work. You must program the phone's GROUP parameter manually, using the local craft procedures menu. To limit specific software upgrades to only phones in a GROUP, you must manually edit the 96xxupgrade.txt or 96x1Supgrade.txt files and build the conditional GROUP statements yourself.

NOTE: Custom modifications that you make to the 96xxupgrade.txt or 96x1Supgrade.txt files disappear when new software releases are unpacked on the fileserver, and newer versions of those files overwrite the existing versions. Be sure to manage such changes manually during deployment of new software files, if you have modified your upgrade script file(s).
The customer may operate a mixed protocol environment, deploying both H.323 phones and SIP phones of the same hardware model. The customer may also wish to modify the mix over time, i.e., gradually migrate all the H.323 phones to SIP in phases.
The customer typically deploys more than one model of phone, e.g., 9611G, 9621G, etc., or multiple families of phones, e.g., 46xx, 96xx, 96x1, etc. Be sure that conditional statements you add to the 46xxsettings.txt file affect all the intended phone models.
Poorly-implemented changes in the 46xxsettings.txt file on the fileserver can cause 96x1 phones to spontaneously convert protocols at their next reboot, provoking a complete service outage for the affected phones.
When you automatically convert 96x1 phones from H.323 to SIP via the "SET SIG 2" directive in the 46xxsettings.txt file, you typically increase the time required for new phone first-boot 20-30 minutes per phone. More time is required because the phone initially upgrades to the latest H.323 software and reboots before it reads the 46xxsettings.txt file to get the new SIG value. Then it must again reboot, download SIP software, and reboot again to complete the conversion process.

Task #10: Confirm Software Update

Confirm that the software running in the various endpoints is at the current desired release level.

96xx and 96x1 SIP Software Confirmation

1. When the phone has completed its boot sequence, it displays "**Username**:" and "**Password**:".
2. Hit the MUTE button followed by 27238#
3. Scroll down to "**VIEW**…"
4. Hit "**Select**"
5. Scroll down to "**Application file:**" and confirm that the software release matches that of the software upgrade file contained in the software zipfile that you downloaded in Task #1.
6. Use "**Back**" and then "**Exit**" to return to the login screen without rebooting the phone.

Avaya one-X® Communicator Software Release Confirmation

1. Launch one-X® Communicator on a PC.
2. When the “Avaya one-X® Communicator Login” applet appears, click on the gear symbol in the upper right corner of the applet to see the “Settings” menu.
3. Click on “About Avaya one-X® Communicator”. The product version dialog opens.
4. Confirm that the Product Version displayed is the expected software version.
5. Click “OK” to close the product version dialog.

Avaya Desktop Video Device with the Flare® Experience Software Release Confirmation

1. Power-up the ADVD.
2. When the display shows the left-side and right-side “fans” for selecting features, touch the “Apps” control under the left-side “Applications” fan. The “Apps” control expands into an “Apps” fan.
3. Scroll down the list of Apps and touch the “Settings” control. The “Settings” application opens in the center of the display.
4. Touch the “About phone” control.
5. Scroll down to “Software Version”, and confirm that the displayed version is the expected software version.
6. Touch the “X” in the upper right corner of the “Settings” window to close the window.

Avaya Flare® Experience for Windows Software Release Confirmation

1. Launch the Avaya Flare® Experience for Windows on a PC.
2. When the application opens, click on the gear symbol along the top border of the window to open the “Settings” applet.
3. In the navigational listing at the left side, click on “About”.
4. Confirm that the software release version displayed is the expected version.
5. Click “Cancel” to close the Settings applet.

Avaya Flare® Experience for iPad® Software Revision Confirmation

1. Launch the Avaya Flare® Experience for iPad® Devices on an iPad®.
2. When the application opens, touch the gear symbol along the top border of the window to open the “Settings” applet.
3. Scroll down to the end of the list of categories, and touch “Support Information”
4. Confirm that the software release version displayed is the expected version.
5. Click “Done” to close the Settings applet.

Avaya B179 SIP Conference Phone Software Release Confirmation:

Confirm the appropriate software release on the Avaya B179 SIP Conference Phone using the keypad/display or the Web Browser Administration GUI:

1. Keypad/Display – Settings key (Gear Symbol) -> Status -> Device
2. Admin GUI – Check the current software version on the Settings -> Provisioning tab.

Task #11: Login and confirm feature subscription

When a SIP endpoint registers with Session Manager, it provides its user's identity. Prior to first login, it does not have that information, so it asks for it via the "Username:" and "Password:" prompts on the login screen. You enter your username and password, and Session Manager authenticates that information against the values that you provided when you administered the endpoint in SMGR. Username is typically the extension of the endpoint, and the password is the "Communication Profile Password" from the "Communication Profile" tab in SMGR User Management. If authentication succeeds, SM registers the endpoint. If the endpoint is Advanced SIP Telephony (AST) capable, the SM's Personal Profile Manager (PPM) then downloads feature information to the endpoint.

Use SMGR to check registration status: *[Home -> Elements -> Session Manager -> System Status -> User Registrations]* Locate your endpoint in the list of users, and confirm that it is registered to its primary, secondary, and survivable SMs, which SM is its active SM, and whether its AST checkbox is checked or not. Click "Show" in the "Details" column to examine Event Subscription status. A properly registered and subscribed Advanced SIP Telephony (AST) endpoint displays five Event Subscriptions:

a. avaya-cm-feature-status
b. reg
c. avaya-ccs-profile
d. message-summary
e. dialog

96xx, 96x1, ADVD, Avaya one-X® Communicator, Avaya Flare® Experience for Windows, and Avaya Flare® Experience for iPad® Devices are all AST endpoints. The B179 Conference Phone is not.

Task #12: Testing call and feature operation

Point-to-point call

1. Initial Conditions: two SIP telephones are installed and registered to the primary Session Manager, and each telephone has a user logged in on it.

2. Confirm successful registration for each telephone:

    a. Login to SMGR via the same account that was used to administer both telephones.

    b. Navigate to **Elements > Session Manager > System Status > User Registrations**

c. Locate the line for each of the two telephones, and confirm that

   - The “Prim” and “Sec” checkboxes in the “Registered” column are both checked, that is, the telephone is registered to both primary and secondary Session Managers.

   - The “AST Device” checkbox is checked, i.e., the telephone registration is complete and PPM download has succeeded.

d. Click the “Show” entry in the first column for the first telephone, and confirm the information for that telephone, including:

   - Registration Address
   - All Addresses
   - Primary SM
   - Secondary SM
   - Event Subscriptions (PPM download information) include the following:
     - avaya-cm-feature-status
     - reg
     - avaya-ccs-profile
     - message-summary
     - dialog
   - Device Type
   - Device Model
   - Device Version

e. Click the “Hide” entry to cause the first-column label to revert to “Show” and to close the Registration Detail box. Repeat these two steps for the other telephone.

3. Make a point-to-point call:

   a. Take one telephone off hook and dial the extension of the other telephone.

   b. Confirm that the second telephone rings and that the first telephone hears ringback.

   c. Answer the second telephone and confirm that talk-path exists in each direction by speaking into one telephone and by listening at the other. Confirm that the audio is clear and understandable. Ensure that the call stays up and passes two-way audio for one minute, to confirm that the endpoint-to-endpoint setup dialogue is completely established.

   d. On the originating telephone, place the call on hold, and confirm that both telephones show the call on hold.

   e. On the originating telephone, resume the call, and confirm that the call is still up and that both telephones have talk path.

f. Hang up the originating telephone, and confirm that both telephones show the call terminated.

g. Repeat the call, this time using the second telephone to call the first telephone.

Lamp/Button/Display confirmation

1. Initial Conditions: two SIP telephones are installed and registered to the primary Session Manager, and each telephone has a user logged in on it. (Same process as for the previous point-to-point call test).

2. On each telephone, press the “PHONE” button, and observe that the display shows the extension of that telephone, the correct date and time, multiple idle call appearances, and soft buttons appropriate for the telephone model, e.g., Redial, Send All, Emerg., Lock.

3. Call one telephone from the other, and answer on the second telephone.

4. Confirm that the called telephone displays the calling party’s name on the call appearance, and that the elapsed call time counter on that same line is counting up.

5. Confirm that the calling telephone displays the dialed number on the call appearance, and that the elapsed call time counter on that same line is counting up.

6. Hang up the call using either telephone, and confirm that both telephones show the call terminated.

7. Check the history logs on both telephones, and confirm that the just completed call was logged.

Network Parameter confirmation

1. Initial Conditions: two SIP telephones are installed and registered to the primary Session Manager, and each telephone has a user logged in on it. (Same as for the previous tests).

2. On each telephone, access the Network Information screen. For example, on a 9641G SIP telephone:

    a. Press the “HOME” button

    b. Touch the “Settings” icon on the screen

    c. Touch the “Network Information” item on the displayed list

    d. Touch the “IP Parameters” item on the displayed list

3. Confirm that the displayed network parameters are correct for the telephone’s LAN environment.

4. Call one telephone from the other, and answer on the second telephone.

5. On either telephone, access the Audio Parameters screen. For example, on a 9641G SIP telephone:

    a. Press the “HOME” button

    b. Touch the “Settings” icon on the screen

    c. Touch the “Network Information” item on the displayed list

    d. Touch the “Audio Parameters” item on the displayed list

6. Wait one minute to allow initial measurement to complete.

7. Confirm that measured values for packet loss, delay, and jitter, are being displayed, and that the values are within Avaya Best Practice specifications for IP telephony, i.e.:

    a. Delay: 80ms to 180ms for business communication quality

    b. Jitter: 20ms or less

    c. Packet Loss: 3% or less for business communications quality

8. Hang up the call.

Appendix A: Verifying administration

General

Verify:

- All domains for which this collection of Session Managers is authoritative are administered (**Home > Elements > Routing > Domains** screen)
- All desired locations are administered (**Home > Elements > Routing > Locations** screen), with the correct bandwidth parameters (for Call Admission Control) and location patterns (for location determination based on IP address).
- All SIP entities are administered for other trunk gateways, SIP service provider trunks, and messaging systems.
- Adaptation is administered as needed for these SIP entities.
- Each of these SIP entities has an associated routing policy (**Home > Elements > Routing > Routing Policies** screen).
- All necessary dial patterns are administered (**Home > Elements > Routing >Dial Patterns** screen) with a routing policy for every relevant originating location or a routing policy for originating location **All**.

Session Manager

For each Session Manager, verify:

- A SIP entity has been administered (**Home > Elements > Routing > SIP Entities**) with the address of the Security Module (typically on interface eth2 of the Session Manager server) and correct domain for the listen port(s).
- A Session Manager instance has been administered (**Home >Elements > Session Manager > Session Manager Administration**) with the correct SIP entity and the address of the management interface (typically on interface eth0 of the Session Manager server) for every Session Manager in the enterprise.
- For each Session Manager SIP Entity, both the TCP and the TLS ports are open to accept connections to SIP endpoints. Although the enterprise *could* work with only one of these ports open, it is a **best practice** to open both so that devices that only support one of the protocols are supported and endpoints can be administered to change from TCP-TLS and vice versa easily. The ports are *opened* by entering the port number and protocol into the SIP Entity screen for each Session Manager.

- The Session Manager's service state has been set (**Home > Elements > Session Manager > Dashboard**) to **Accept New Service**.

- At least one entity link (transport TLS is recommended) has been administered (**Home > Elements > Routing > Entity Links**) between this Session Manager and every other Session Manager to which it can route calls.

Communication Manager

For each Communication Manager, verify:

- A SIP entity for application sequencing has been administered (**Home > Elements > Routing > SIP Entities**) with the address of the Communication Manager's procr interface or C-LAN. This SIP entity does not have adaptation administered.

- At least one signaling group has been administered (**Home > Elements > Communication Manager > Network >Signaling Groups**) connecting Communication Manager to each Session Manager that uses the Communication Manager for application sequencing.

- If needed, a SIP entity and at least one signaling group has been administered for use of the Communication Manager as a Trunk Gateway. If needed, an adaptation with module name **DigitConversionAdapter** has been administered (**Home > Elements > Routing > Adaptations**) and added to the SIP entity.

- Each signaling group's **Group Type** field has been set to "SIP". If Communication Manager is acting as a Feature Server, the **IMS Enabled** field has been set to "y"; if Communication Manager is acting as an Evolution Server or a Trunk Gateway, the **IMS Enabled** field has been set to "n". The **Peer Detection Enabled** field has been set to "y".

- At least one entity link has been administered (**Home > Elements > Routing > Entity Links**) between the Communication Manager and every Session Manager that routes calls to that Communication Manager. The port and transport (TLS is recommended) associated with the Communication Manager on the **Entity Link** screen matches the near-end port and transport administered on the **Signaling Group** screen. Similarly, the port associated with the Session Manager on the **Entity Link** screen matches the far-end port administered on the **Signaling Group** screen. Additionally, the far-end domain on the **Signaling Group** screen is the same as the authoritative domain for the corresponding IP network region and the domain administered on the Session Manager's listen port.

- **Direct IP-IP Audio Connections** and **Initial IP-IP Direct Media** fields have been enabled on the **Signaling Group** screen to minimize usage of Communication Manager's VoIP resources. When direct media is used with Modular Messaging, there is a short delay, but Modular Messaging is able to correct any clipping of the first announcements.

- For each signaling group, a corresponding SIP trunk group has been administered (**Home > Elements > Communication Manager > Network >Trunk Group**) with

enough members to handle the expected call load.

- One or more separate trunks between SM and CM are configured for use by SIP telephone calls. This trunk is set to use private numbering (set to private – page 3 of **Home > Elements > Communication Manager > Groups > Trunk Group**).

- The extension range of SIP telephones is configured in the CM private numbering table ("change private-numbering").

- Communication Manager has been administered (**Home > Elements > Session Manager > Application Configuration > Applications**) as a sequenced application.

- The Communication Manager sequenced application has been added (**Home > Elements > Session Manager > Application Configuration > Application Sequences**) as the first application in an application sequence. Communication Manager must be added in the inventory and synchronized before it is added as an application. Also Communication Manager is first added as an Application, not a Sequenced Application.

- The feature access code for Auto Alternate Routing (AAR) has been set (**Home > Elements > Communication Manager > System > Feature Access Codes**).

- The **UDP Extension Search Order** field has been set to local-extensions-first (**Home > Elements > Communication Manager > System > Dialplan Parameters**).

Appendix B: Administration best practices

Administration best practices

The following list provides guidance on how to ensure a better installation experience.

- Read the relevant documentation beforehand to make sure you understand what needs to be configured and that you have a clear understanding of all the fields and their options. Refer to the screen-level help when in doubt.

- Make sure that the software release installed supports the configuration and features the customer expects. You may need to upgrade to provide the expected features. Read the Solution and Offer Definitions carefully

- Use a worksheet to capture all the administration details, including hostnames, IP addresses, user names and passwords, customer-preferred settings. Pay particular attention to information that goes into multiple fields.

- Always use System Manager to administer Communication Manager features when applicable. This ensures that the Communication Manager translation files are in sync with System Manager database.

- When installing or upgrading System Manager, use the fully qualified domain name (FQDN) as the hostname where the FQDN is requested.

- Session Manager and System Manager must be able to resolve both hostname to IP and IP to hostname. Confirm that /etc/hosts contains the relevant entries on both systems.

- **Align CM route pattern trunk choices with each SIP endpoint's primary/secondary SM configuration**. In order to minimize the additional traffic that results when polling SUBSCRIBEs get to CM from what CM considers to be the wrong trunk (i.e., from a non-primary SM), the configuration in both SMGR and CM must be aligned. The SMGR assignment of the primary and secondary SM controllers for each endpoint must match the CM Route Pattern administration for that endpoint's extension.

  Here an example of how that alignment should be for two extensions (5000 and 6000). Assuming the following CM configuration:
  - Route Pattern 1 with first choice trunk 1 going to SM1, and second trunk 2 to SM2.
  - Route Pattern 2 with first choice trunk 3 going to SM3, and second trunk 4 to SM4.

  For example to assign extension 5000 to have primary SM1 and secondary SM2, then configure:
  - On SMGR: assign SIP extension 5000 to primary SM1 and secondary SM2.
  - On CM: Assign extension 5000 to Route Pattern 1.

For example to assign extension 6000 to have primary SM3 and secondary SM4, then configure:

- On SMGR: assign SIP extension 6000 to primary SM3 and secondary SM4.
- On CM: Assign extension 6000 to Route Pattern 2.

- See **"Implementing End-to-End SIP, Vol 2: Designing SIP Telephone Signaling, Number and Dial Plan Options"** for best practices information regarding use of: OPTIM tables, public and private numbering tables, and incoming call handling tables (ICHT).

- To better understand CAC requirements and configuration, read "***Avaya Aura® Call Admission Control (CAC) and Bandwidth Management Best Practices***", COMPAS ID: 151364, before implementing SIP endpoints.

Endpoint best practices

The following list provides guidance on how to ensure a better installation experience.

- Refer to the detailed information on setup and configuration of **DHCP** and **HTTP** servers used to deploy endpoint software. That information is provided in the following locations:
  1. *Task #4: Administer the Fileserver* in this document.
  2. *Task #5: Administer the DHCP Server* in this document.
  3. *Task #9: Change Endpoint's Signaling Type from H.323 to SIP* in this document.
  4. *Task #10: Confirm Software Update* in this document.
  5. *Appendix C: Administration guidance and detailed descriptions* in this document.
  6. *Appendix G: Proper Selection of 46xxsettings.txt Values* in this document.
  7. Endpoint Implementation and Administration Guides on support.avaya.com
  8. Endpoint Installation and Maintenance Guides on support.avaya.com
  9. Read Me or Release Notes files corresponding to each endpoint software release on support.avaya.com

- Before upgrading the endpoint software, review the latest Administration Guide or Readme/Release-Notes file to learn about new capabilities. Also, add new settings, as appropriate, to your existing 46xxupgrade.txt file before installing the software.

- For mixed SIP/H.323 customer environments, see *Appendix C: Administration guidance and detailed descriptions* for **best practices**.

- The 46xxsettings.txt file provides some configuration options that can only be enabled in the 46xxsettings.txt file, and not in Communication Manager or Session Manager, e.g., codec set, media encryption, country tones, etc. Ensure that you understand whether the features that you activate require configuration in the 46xxsettings.txt file.

- When you change an Advanced SIP Telephony (AST) endpoint's administration in SMGR:
  1. SMGR logs into CM on your behalf and executes station commands to effect those changes.
  2. SMGR updates its own database with the new station parameters.
  3. SMGR replicates the now-updated database to all the SMs.

4. The Personal Profile Manager (PPM) in the endpoint's *active* SM downloads the changes to the endpoint.

This chain of updates can occur with very little perceptible delay, i.e., the changes you make in SMGR appear in the endpoint almost immediately. However, it can also take a while for the changes to propagate to the endpoint. You can force the endpoint changes to occur in real time by directing the affected endpoint to *reload* its configuration parameters from SM: [Elements > Session Manager > System Status > User Registrations -> Reload] Alternatively, you can manually log the endpoint out and back in to force it to re-download its parameters.

- The administrator can use one or more of four options to configure the Session Managers that a 96xx or 96x1 endpoint will use as a SIP Controller:

    1. In the DHCP Option 242 string, with the SET SIP_CONTROLLER_LIST directive.
    2. in the 46xxsettings file, with the SET SIP_CONTROLLER_LIST directive.
    3. In SMGR user administration, under Session Manager Profile [Home > Users > User Management > Manage Users > Communication Profile (tab) -> Session Manager Profile (section)], by specifying the Primary SM, Secondary SM, and Survivability Server. The phone gets this list via PPM download after it has registered and subscribed to a particular SM.
    4. In the phone itself, using the manual local craft procedures menu (press MUTE, enter 27238#, scroll to and select SIP -> SIP Proxy Server).

    Because the phone can be subject to all of these configuration methods, the phone's internal SIP_CONTROLLER_LIST can change when the phone reboots. The phone implements a priority algorithm to create and rearrange its SIP_CONTROLLER_LIST based on the source of the changes. The priority assignment, from highest to lowest, is:

    1. Manual on-the-phone-changes performed with local craft procedures
    2. PPM downloads
    3. 46xxsettings.txt directives
    4. DHCP Option 242 directives
    5. LLDP Directives

    The ordering of the entries in the controller list depends on the priority of the source of each specific entry. That is, If address C came from the PPM, address A came from the 46xxsettings.txt file, and address B came from the DHCP option 242 string, the resulting list would be C, A, B.

    No duplicates are allowed in the list. If two sources supply the same address, the phone keeps the higher-priority source's entry. It also remembers the source for that entry, in case another, higher-priority source later supplies the same address, and the address may then move to a higher position in the list.

    An address can be *removed* from the list in four ways:

    1. You *clear* the phone. This action removes all the addresses in the list.
    2. A source provides a different set of addresses than it previously provided. For example, if the 46xxsettings.txt file originally provided addresses A, B, and C, and when the phone reboots, it now supplies only addresses B and C, the phone

removes address A from the list if no other sources have also provided address A. If another source also provides address A, then A stays in the list, but it moves down the list because it is provided by a lower-priority source.

3. The phone attempts to register using an address, and the SM with that address is not the designated primary or secondary SM for the phone. In that case, the SM returns a 301 Moved message, and the phone removes that SM's address from the list. The 301 Moved message will typically include the primary, secondary, and survivable remote SM information that is configured for the phone in SMGR. In that case, the phone replaces its internal SIP Controller List with the new list provided in the 301 Moved message.
4. You use the manual Delete capability on the phone to remove an entry. **NOTE**: this only works for entries that were generated manually in the first place. It will not work on a PPM-sourced entry, for example.

Additional rules are applied at each source, and recommended **best practice** may dictate a particular usage:

1. The DHCP Option 242 string is limited to 255 characters, so lengthy controller lists that specify port and transport type for each FQDN/IP Address can quickly fill up the string. Also, recommended best practice dictates that the SIP controller list be specified in the 46xxsettings.txt file and that the Option 242 string contain no SIP Controller list.
2. The 46xxsettings.txt file directive, ENABLE_PPM_SOURCED_SIPPROXYSRVR, when set to zero, causes the phone to ignore the PPM's controller list. It defaults to 1 in the phones, so the PPM list is <u>not</u> ignored unless you set this directive to zero in the 46xxsettings.txt file. If you wish to keep the higher-priority PPM from overriding the SIP controller list provided by your 46xxsettings.txt file, this directive allows you to do that.
3. If TCP is required for signaling instead of TLS, the 46xxsettings.txt file's ENABLE_PPM_SOURCED_SIPPROXYSRVR must be set to zero in the 46xxsettings file. Otherwise the TCP setting will be overwritten to TLS when the server settings are downloaded from PPM.
4. The PPM's SIP controller list is created according to your *Primary SM*, *Secondary SM*, and *Survivability Server* entries in SMGR's Session Manager Profile configuration for the endpoint. Because those entries must specify SM or BSM SIP servers only, you can't use the PPM to configure 3rd Party or other non-SM SIP controllers for the phones: you must do that in the 46xxsettings.txt file, but since it has lower priority than the PPM, you may find it necessary to use the ENABLE_PPM_SOURCED_SIPPROXYSRVR directive to cause the endpoint to ignore the PPM's list (see previous item above), and force a particular list using the 46xxsettings.txt file.
5. Manual configuration entered on the phone via local craft procedures is the highest priority, and it overrides all other sources.

- Verify that the configuration parameter SIMULTANEOUS_REGISTRATIONS is set to the number of **Session Managers** or **Branch Session Managers** to which the endpoint *simultaneously* registers. The count must not include any other type of servers, e.g., 3rd party SIP proxies, Avaya Secure Router SR2330 SIP Survivability Module, etc. *Alternate Registration* is used for any other type of server.

- Values added with the CRAFT menu are not removed until manually deleted in the same way or the telephone values are either reset or cleared. Neither the settings file nor PPM downloads are able to override these values.

- PPM performs dial plan optimization to reduce the number of entries sent to the telephone. So if you have multiple ARS/AAR entries that start with the same digits, PPM will send the widest range.
  For example:

```
    Dialed              Total          Route     Call
    String            Min     Max    Pattern   Type
01                     11      11       1        pubu
01483308000            11      11       3        pubu
```

  With this configuration, only 01 is sent to the telephone.
  Also note that if Min and Max entries were different, then PPM would send 01+, which would cause an interdigit timeout and dial delay. Therefore, try to avoid flexible-length entries when building the ARS/AAR tables.

- Ensure SIP station IP addresses are configured in Communication Manager's **IP-Network-Map** screen to enable correct location-based dialing and Call Admission Control calculations.

- If turning on Initial IP-IP Direct Media (early media), ensure call progress tones are as expected for that location. If not, verify that the country parameter is set correctly in the 46xxsettings file.

Appendix C: Administration guidance and detailed descriptions

Administering endpoint TLS/TCP

When administering Session Manager, you configure two ports for each Session Manager: TCP and TLS. Both ports are open, which allows endpoint administration to determine which protocol to use via the 46xxsettings.txt file.

For TLS ports

Note: Regarding TCP vs. TLS, CM typically likes the SIP telephones to use the same transport and port that is used for the **SM-to-CM Entity Link,** i.e., that the CM configures as a Signaling group.

If all SIP endpoints are required to use TLS, then, as a best practice, the 46xxsettings.txt file should have the following line administered:

SET SIP_CONTROLLER_LIST www.xxx.yyy.zz1:***5061;transport=tls***,
www.xxx.yyy.zz2:**5061;transport=tls**

where:

www.xxx.yyy.zz1 is the IP address of the primary Session Manager, and
www.xxx.yyy.zz2 is the IP address of the secondary Session Manager

You can omit the port number for a Session Manager in SIP_CONTROLLER_LIST. Then the phone defaults to port 5061 for TLS or port 5060 for TCP.
You can omit the transport type in SIP_CONTROLLER_LIST. Then the phone defaults to TLS for that Session Manager.

Note: If a survivable remote is administered, you can also add a third element to the SIP Controller List, specifying the IP address, port, and protocol for the survivable remote. This addition is not required, however. If the survivable remote is administered for the endpoint in System Manager as part of the user's Communication Profile, then the endpoint gets that information via PPM download when it registers with the primary or secondary Session Manager, so no addition to the 46xxsettings.txt file is required for the survivable remote. However, if you initially connect the phone to the system at a time when only the survivable remote is available, i.e., both primary and secondary SM are not reachable, then the phone could still perform its initial registration with the survivable remote. This should be a fairly rare scenario, however: if both primary and secondary SMs are currently unreachable, you probably have more pressing business at hand than adding a new phone to the system.

Note: If the installation has more than one community of telephones that has this ordered pair of Session Manager addresses, you must provide a unique 46xxsettings.txt file for each community.

Finally, you must administer the number of SIP proxies (i.e., Session Managers, Survivable Remotes) that exist—either 1 or 2, when there is no survivable remote, or 3 when a survivable

remote is in use for this community.

SET SIMULTANEOUS_REGISTRATIONS 2

Note: You can also specify three SM IP addresses, should your solution actually have three SMs and no BSM. The phone will simultaneously attempt to register with all three SMs, but only two of the three will actually accept a registration from that phone. That's because, in SMGR user communication profile configuration, you can specify only two SMs for a phone, a *primary SM* and a *secondary SM*. When the phone attempts to register with the third SM, which is neither the primary nor the secondary SM specified in SMGR, that SM checks its database and finds that it is not the primary or secondary for that phone. Then it returns a ***301 Moved*** SIP response that contains a replacement SIP_CONTROLLER_LIST intended to point the phone at its proper primary SM, secondary SM, and survivable SM (BSM).

For TCP ports

If all endpoints are required to use TCP, then the 46xxsettings.txt file must have the following line administered:

*SET SIP_CONTROLLER_LIST www.xxx.yyy.zz1:**5060;transport=tcp**,*
www.xxx.yyy.zz2:**5060;transport=tcp**

where:

www.xxx.yyy.zz1 is the IP address of the primary Session Manager, and
www.xxx.yyy.zz2 is the IP address of the secondary Session Manager

Also, make sure the following line is set:

SET ENABLE_PPM_SOURCED_SIPPROXYSRVR 0

This setting instructs the SIP telephones to ignore the SIP Controller List that they get from PPM during registration with Session Manager, and use only the Session Manager addresses, ports, and transport protocols specified in the 46xxsettings.txt file's SIP_CONTROLLER_LIST.

Note: If a survivable remote is administered, you can add a third element to the SIP_CONTROLLER_LIST setting, specifying the IP address, port, and protocol for the survivable remote.

Note: If the installation has more than one community of telephones that has this ordered pair of Session Manager addresses, you must provide a unique 46xxsettings.txt file for each community.

Finally, you must administer the number of SIP proxies (i.e., Session Managers, Survivable Remotes) that exist—either 1 or 2, when there is no survivable remote, or 3 when a survivable remote is in use for this community.

SET SIMULTANEOUS_REGISTRATIONS 2

Changing the protocol

Once the enterprise is fully initialized and all telephones are up and running, if a change to the transport protocol for one of the telephones is desired, it must be done manually, by changing the protocol on the telephone itself. Use the following procedure to manually change the protocol:

1. Confirm that the SIP endpoint is not in use.
2. Press the MUTE 27238# sequence to access the local craft procedures menu.
3. Select SIP > SIP Proxy Server to display the list of all defined SIP Proxy Servers.
4. Select each defined SIP Proxy Server in turn.
5. Change the Transport Type to TCP, if changing from TLS to TCP.
6. Select the **Save** softkey.
7. Once all SIP Proxy Servers are changed to TCP, exit the CRAFT menu.
   The telephone re-registers using TCP; there is no need to reboot the telephone.

Upgrading software on the telephone

Use the following procedure to upgrade the software on the telephone from one version of SIP software to another version.

1. Download the new software distribution package from the Avaya support web site (https://support.avaya.com) into the distribution directory of your HTTP server. This is not usually the same as the root directory of the server on which HTTP is running. For example, if you are using Apache for the HTTP server, the distribution directory is defined by the DocumentRoot parameter in httpd.conf.
2. Extract the files using *WinZip* or a similar utility program. For example, for Windows use *WinZip*, and for Linux use *unzip*.
3. Check support.avaya.com to see if a new 46xxsettings.txt (for 96xx, 96x1, Avaya one-X® Communicator) or Axxxsettings.txt (for ADVDs) is available. If a new version exists, download it and merge the settings from the existing 46xxsettings.txt file into it. Enable settings as needed for any new parameters that control new capabilities supported by the software. See the Readme file, Release Notes, or Administration Guide for details of new capabilities. Backup the current 46xxsettings.txt file, and then replace it with the new merged file.

   Note: It is not necessary to change any settings in the 46xxsettings.txt file to download the new software; that is taken care of automatically by the 96xxupgrade.txt or 96x1Supgrade.txt files included in the package. However, if the existing 96xxupgrade.txt or 96x1Supgrade.txt files have been customized, and if the changes must be carried forward, then you must merge that customization into the new upgrade.txt files in the package:

   1. Backup the existing 96xxupgrade.txt and 96x1Supgrade.txt files.

2. Rename the existing upgrade.txt files, so they will not be overwritten when you unpack the new software package.
3. Unpack the software package.
4. Edit the new upgrade.txt files, and merge the custom modifications from the existing files into the new upgrade.txt files.
5. Remove the old (now renamed) upgrade.txt files.

4. You can reset telephones via System Manager's **Home > Elements >Session Manager > System Status >User Registrations** page**.**

5. Process the telephones in batches, so that the number of telephones upgrading simultaneously does not overwhelm the capabilities of your server or the bandwidth available in your network.

   Note: Because batch size varies based on each system's network bandwidth, fileserver capacity, and other factors, there is currently no generic guidance for selection of batch size.

6. Start with small batches and increase batch size carefully, while closely monitoring system performance.

7. To reset a group of phones instead of all the phones at once, select specific users using **Filter** and by checking the checkboxes for the users to be upgraded. Click the **Reboot** button in the "AST Device Notifications" section at the top of the form.

8. Verify via System Manager's **Home > Elements > Session Manager > System Status >Registration Summary** and **Home > Elements > Session Manager > System Status >User Registrations** that users are re-registered correctly.

The telephones download the new software automatically and automatically restart once more to install it. **Do not unplug the telephones or disrupt power while the upgrade is in progress**.

Migrating existing H.323 endpoints to SIP software

Use the following procedures to migrate existing endpoints from H.323 to SIP software. As part of the H.323 to SIP telephone migration, the user is logged out and is *not* logged back in. Therefore, additional steps are needed to validate the migration.

Note: This procedure assumes that the migration of users is performed in batches, and that those batches of users are done relatively at the same time. If that is not the case, and significant time elapses between batches, consider the following items:

- After each migration batch is completed, change the **SET SIG** to default (0) (or via DHCP option 242) so that 96x1 users are not unintentionally migrated to SIP.

- Use the GROUPS feature in the 46xxsettings.txt file to manage the migration.

Pre-administer the users-to-be-migrated in System Manager

1. Each H.323 user-to-be-migrated requires additional administration (referred to here as "pre-administration") in order for that user's endpoint to function as a SIP endpoint once the migration is complete. Complete that administration on System Manager, using the same process as for new SIP installations documented previously.

2. For 96x1 phones**, do not** change the **SET SIG** in 46xxsettings.txt (or via DHCP option 242) until you are ready to start the migration.

3. Pre-administer on System Manager all targeted users for the SIP migration. However, be sure to leave their assigned template and station type as their currently assigned H.323 template and station type.

   Note: As part of this pre-administration, confirm that on each H.323 phone, feature button (CallFwd, EC500, SendCalls) locations *start on button 9 or higher*. If any feature buttons are defined on lower-numbered buttons, then after the migration to SIP, you will have buttons that do not function properly.

4. Make a test call to validate that the System Manager and Communication Manager changes were completed correctly. This call confirms that the pre-administration of the targeted users in System Manager, Session Manager, and Communication Manager has not affected the users' capability to make calls while their endpoints are still using H.323 software.

5. Download the new SIP software distribution package from the Avaya support web site (https://support.avaya.com) into the distribution directory of your HTTP server. This is not usually the same as the root directory of the server on which HTTP is running. For example, if you are using Apache, the distribution directory is defined by the DocumentRoot parameter in httpd.conf.

6. Extract the files using the appropriate utility program. For example, for Windows use WinZip, and for Linux use unzip.

7. Check support.avaya.com to see if a new 46xxsettings.txt (for 96xx, 96x1, Avaya one-X® Communicator) or Axxxsettings.txt (for ADVDs) is available. If a new version exists, download it and merge the settings from the existing 46xxsettings.txt file into it. Enable settings as needed for any new parameters that control new capabilities supported by the software. See the Readme file, Release Notes, or Administration Guide for details of new capabilities. Backup the current 46xxsettings.txt file, and then replace it with the new merged file.

8. **Note**: Do not change the **SET SIG** type until you are ready to migrate the 96x1 users.

Migrating the endpoints from H.323 to SIP

Repeat the following steps for each batch of users being migrated:

1. From Communication Manager use the command `list registered-ip-stations` to determine the list of users currently registered. If you do this using Avaya Site Administration, you can download the list into an Excel spreadsheet for later review.

2. Either change **SET SIG** in 46xxsettings.txt file to 2 or set via DHCP Option 242. **Note**: Any telephones that uses DHCP server or HTTP server pulls the new SIP software.

3. Reset the 96x1 telephones in batches, so that the number of telephones upgrading simultaneously does not overwhelm the capabilities of your server or the bandwidth available in your network.

    a. The telephones download the new software automatically and self-restart once more to install.

    b. Do not unplug the telephones or disrupt power while the upgrade is in progress.

    c. Reset the telephones using the Communication Manager command `reset ip-stations`.

    d. Using either SNMP or parsing of the HTTP access and error logs, verify that the endpoints have the correct software.

    e. Run the Communication Manager command `list registered-ip-stations`; users that were reset should no longer be listed.

    f. For migrated users use System Manager's **Home >Elements > Communication Manager > Endpoints > Manage Endpoints > More Actions > Global Endpoint Change** to change the **Set Type** to SIP; that is, 9630 to 9630SIP.

Using SIP and H.323 endpoints in a mixed environment

Customers who are already using Avaya H.323 telephones and who elect to deploy Avaya SIP telephones will typically support both H.323 and SIP telephones in a mixed environment for some time. The following table illustrates how to convert to/from SIP and H.323.

Environment	To convert this type of desk phone	To convert this type of desk phone	Then
H.323 – centric	H.323 in use	SIP	Perform the SIG Craft procedure to change the SIG parameter value from default to 2 (SIP). Save the SIG parameter change. The desk telephone will reset.
H.323 – centric	H.323 factory set	SIP	Connect the desk phone to a power source and to the network. Press the Program soft-key as soon it displays in the first soft-key position to access the Craft Access Code Entry screen. Perform the SIG Craft procedure and change the value from 'default' to '2' (SIP). Save the SIG parameter change. The desk phone will reset.
H.323 – centric	SIP	H.323	Perform the SIG Craft procedure to change the SIG parameter value from '2' (SIP) to 'default 1' (H.323). Save the SIG parameter change. The desk phone will reset.

Note: The following procedure applies only to the 96xx telephones. It is not needed for the 96x1 telephones.

These instructions modify the existing 96xxupgrade.txt script file to cause any 96xx phones with SIG=SIP to skip all the directives in the current 96xxupgrade.txt file (because they apply to H.323 phones only), and instead, immediately load the 96xxupgrade.txt file that is packaged with the new SIP software. You rename the new 96xxupgrade.txt file to 96xxupgrade_SIP.txt, so that it can reside in the same directory as the current 96xxupgrade.txt. H.323 phones will continue to use the existing 96xxupgrade.txt file, and the new SIP 96xx phones will load the new 96xxupgrade_SIP.txt file and upgrade to the new SIP software.

1. Unpack the 96xx SIP software zipfile on the HTTP server, but use a temporary directory other than the distribution directory, so that the new 96xxupgrade.txt file will not overwrite the current one during unpacking.

2. Copy the new SIP software files into the same HTTP server distribution directory that already holds the H.323 software files, but do not copy the new 96xxupgrade.txt file there.

3. In the temporary directory where you unpacked the software zipfile, rename the new 96xxupgrade.txt file to 96xxupgrade_SIP.txt and copy this file to the distribution directory on the HTTP server.

4. Edit the current 96xxupgrade.txt file, and add the highlighted lines as shown. H.323 phones will continue to do what they normally would, but SIP phones skip the H.323 configuration and immediately load 96xxupgrade_SIP.txt, the new SIP software upgrade script file.

```
IF $SIG SEQ 2 GOTO SIP
IF $MODEL4 SEQ 9610 goto BACKUPAPP96XX
IF $MODEL4 SEQ 9620 goto BACKUPAPP96XX
IF $MODEL4 SEQ 9630 goto BACKUPAPP96XX
IF $MODEL4 SEQ 9640 goto BACKUPAPP96XX
IF $MODEL4 SEQ 9650 goto BACKUPAPP96XX
IF $MODEL4 SEQ 9670 goto BACKUPAPP9670
goto END

# BACKUPAPP96XX
IF $VPNACTIVE SEQ 1 GOTO PHONEAPP96XX
IF $BOOTNAME SEQ hb96xxua3_1_02_S.bin goto PHONEAPP96XX
SET APPNAME hb96xxua3_1_02_S.bin
goto GETSET

# BACKUPAPP9670
IF $VPNACTIVE SEQ 1 GOTO PHONEAPP9670
IF $BOOTNAME SEQ hb9670ua3_1_02_S.bin goto PHONEAPP9670
SET APPNAME hb9670ua3_1_02_S.bin
goto GETSET

############################################################
##            Check phone application version             ##
############################################################
# PHONEAPP96XX
SET APPNAME ha96xxua3_1_02_S.bin
goto GETSET

# PHONEAPP9670
SET APPNAME ha9670ua3_1_02_S.bin
goto GETSET


############################################################
##           Get additional configuration files           ##
############################################################

# GETSET
GET 46xxsettings.txt
goto END

# SIP
GET 96xxupgrade_SIP.txt
goto END
```

```
# END
```

Appendix D: Troubleshooting

Before calling Avaya support

Before calling Avaya support for assistance, make sure to have as much of the information below as possible:

- Telephone model, software version
- Software versions of
  - Communication Manager
  - System Manager
  - Session Manager
  - Presence Services
- Logs found in following locations:
  - Telephone
  - Session Manager
  - Communication Manager
  - Fileserver
  - Presence Server
  - DHCP server
  - LDAP server
- Turn on logging (in addition to what is normally logged, for example, debug logging)
  - **NOTE**: The phone's Debug menu option is not available, if the local procedures password for the phone is set to the default, i.e., "27238" or "craft". In order to enable Debug features on a phone, you must change the value of the PROCPSWD directive in the 46xxsettings.txt file to something other than the default password. Then you must reboot the phone, so it picks up that change. Don't forget to record the new value in solution documentation, if you elect to allow the new value to persist rather than change it back to the default.
- How the telephone is administered in System Manager and on the telephone itself
- settings file
- DHCP option 242 string
- Any traces taken (for example, traceSM, list trace station, MST traces, PPM trace)
- Telephone parameters visible through the local craft procedures menu on the telephone, that is, mute-craft#
- Telephone MIB retrievals

Troubleshooting tips

If you experience problems, try these troubleshooting tips.

Error seen	Likely problem	Solution

Cannot log into the telephone	SIP telephone did not register to Session Manager	• Verify that the user id and password for the telephone match what was administered. • Verify that the SIP domain parameter in the settings file contains the same SIP domain as the Session Manager that it is registered to. • Verify that the telephone is able to reach the Session Manager, and verify that it is using the Security Module IP address.

Function buttons are not showing	User id and password may not be administered correctly	• Verify that the userid and password for the telephone match what was administered • Verify that the SIP domain name is correct on the IP Network Region screen, in System Manager under Domains, and in the 46xxsettings file. • Verify that System Manager is synchronized with Session Manager via Home / Services / Replication. • Verify that the telephone is automatically configured by System Manager in Communication Manager. • Verify that there are enough OPS licenses on Communication Manager. • Verify that the telephone is recognized as an AST telephone. If not, then the telephone did not get any features from Communication Manager, which would have happened during the PPM registration process with Communication Manager. The reason why the PPM process did not complete successfully may be because • Adaptation is manipulating SIP domain, and during PPM process the telephone is not authorized to communicate with Communication Manager because of incorrect domain parameters. Verify the domain settings. • The password is not correctly administrated in the Communication profile password and or in Endpoint profile security code. • If the public or private table is not set up correctly in CM for the SIP Stations, PPM issues can occur (no body in polling NOTIFY messages).
Icon does not display on Avaya one-X® Desktop	Protocol not set to TLS	Verify that the protocol is set to TLS on the SIP Entity screen.

Cannot complete a call successfully	Mismatch between Session Manager and Communication Manager administration	• Verify that the Authoritative Domain field on the Network Regions screen matches the what was configured in the … • Verify that the authoritative domain is configured via Home / / Elements / Routing and matches the domain configured in the 46xxsettings file. Or when manually configured on the telephone, the domain is configured on the telephone itself. • For calls coming in on a SIP trunk from a foreign SIP domain, verify that a SIP trunk was configured whose signaling-group contains a Far-end Domain Name value that matches this foreign domain or a blank value**.**
When testing features, you hear a busy or intercept tone	The station button may be misassigned.	Check Communication Manager for the correct FNE, proper permissions under COS/COR, and the proper station button assignment to support the feature.
The MWI does not light when a message is left.	May be a SIP domain mismatch	Ensure that the SIP trunk signaling group Far-end Domain Name field on which the NOTIFY message to Session Manager is sent contains the SIP domain of the correct Session Manager.
Voice quality is poor		Refer to the administration and maintenance books for the particular 96xx telephone.
Cannot make outside calls via SIP carrier through SBC. Carrier or SBC is rejecting the call with error 404. Trace is showing sip:anonymous@anonymous.invalid	Public or Private unknown table is not configured.	Configure the extension range with DDI prefix in the Public unknown table.

Appendix E - Signing up for PCN/PSN notifications

A Product Change Notice (PCN) should accompany a software update (for example, Service Pack or Patch that should be applied universally). A Product Support Notices (PSN) typically issued when there is no patch/Service Pack/Release fix, and the Business Unit or Services must alert Avaya Direct, Business Partners, and Customers to be aware of an issue or change. In addition, a PSN can document a workaround if one is available, steps to take to recover logs, software, etc.

Both notices alert you to important issues which directly impact Avaya products. You can view PCNs and PSNs by visiting the Avaya Support website, http://support.avaya.com, and navigate as follows:

1. Select “PRODUCTS” at the top center of the screen.
2. Click A-Z List, and select your specific product of interest. For example, select, "Avaya one-X® Deskphone" to bring up the Avaya one-X® Deskphone page.
3. Click on “Choose Release”, and select a release from the drop-down menu, e.g., “SIP 6.2.x”.
4. On the upper right side of the page, you see a "NOTICES & RELEASE NOTES" section. Click the "View All>" link at the end of the list of documents.
5. At the left side of the “Downloads & Documents” page under “FILTERS”, click the checkboxes for “Product Support Notices” and “Product Correction Notices”, and uncheck all the other boxes.
6. The list of links for available PCNs and PSNs appears in the center of the page. Clicking on a link loads the .pdf file for viewing in your browser. You can read it there, or you can save it to your PC for later reading.

Manually viewing PCN's and PSN's is useful, but you should also sign-up for new-document notifications, so that you are informed regarding new developments in timely fashion. This proactive notification system is performed by the Avaya E-Notification process, which also provides notifications for new/updated product documentation, patches, and service packs.

To sign up for Avaya E-Notifications:

1. Go to the Avaya Support website: http://support.avaya.com

2. Enter your Username and Password, and click the “LOG IN” button to Sign in to the site. If you are not yet registered, click the “REGISTERN NOW” link to do so.

3. Once you are signed in, click “Set E-Notifications” under “ALERTS & REPORTS” at the bottom right side of the page. The “E-NOTIFICATIONS” page displays.

4. You can select from 5 General Notification categories on the left side of the form, or you can click “Add More Products” on the right side of the form and select various types of notifications for specific products and specific releases. Be sure to click the “Update” button for General Notifications, or the “Submit” button for product-specific notifications.

Appendix F: Signaling and Dial Plans

This appendix has been moved to a separate document, ***"Implementing End-to-End SIP, Vol 2: Designing SIP Telephone Signaling, Number and Dial Plan Options".***

Appendix G: Proper Selection of 46xxsettings.txt Values

What is the 46xxsettings.txt Role During the Phone Boot Sequence?

Each time that a 96XX or 96X1 SIP phone boots, it performs the following sequence of activities:

1. Initialize internal hardware and software and enable the network interface.
2. Contact a DHCP server to acquire a LAN address and Option information from the DHCP server's scope configuration. The Option information specifies the IP address of the file server that the phone will contact next.
3. Contact the fileserver and retrieve the 96xxupgrade.txt file (for 96xx phones) or the 96x1Supgrade.txt file (for 96x1 SIP phones) and the 46xxsettings.txt file.
4. Execute the 96xxupgrade.txt or 96x1Supgrade.txt file to determine whether a software upgrade is required. If it is, retrieve the software upgrade file from the fileserver and self-upgrade. This process typically results in several reboots, as there are multiple software files (e.g., boot image, application image, intermediate upgrade image) and reboots may be necessary for all of them.
5. If the software was already up to date, or if the phone just finished its self-upgrade, proceed with the boot sequence. Execute the **46xxsettings.txt** script file, setting the appropriate variables in the phone's configuration data. The directives and values used include the settings necessary for the phone to contact and register with its SIP controllers.
6. Next, the phone displays the login screen, and the user can enter account credentials to log into the phone. (If the phone has cached user credentials from a previous session, it may log in on behalf of the user automatically.)
7. The phone now registers with a SIP controller, subscribes to features, and downloads additional configuration (e.g., contacts, dial plan information, etc.) from the Personal Profile Manager. Once these downloads are complete, the phone is ready to make calls.

Where do Phone Configuration Parameters Come From?

The configuration parameters that control the phone originate from one of the following locations:

1. **DHCP** - Option information that is specified in the DHCP server's scope for the phone's LAN subnet. Such information can include many parameters, but as a **best practice**, Avaya recommends limiting the Option 242 string contents to the fileserver IP address(es), and then specifying any other needed parameters in the 46xxsettings.txt file.
2. **LLDP** – If a customer system implements a Link Layer Discovery Protocol (LLDP) service or server on the LAN, then the phone may receive Link Layer Discovery Protocol Data Units (LLDPDUs) that can set phone parameters (e.g., VLAN ID) and perform other basic network administration. This document does not focus in depth on LLDP, concentrating instead on DHCP for initial setting of phone network parameters. For a detailed discussion of LLDP, please refer to the section titled, "***About Link Layer***

Discovery Protocol (LLDP)", in Administering Avaya 9601/9608/9611G/9621G/9641G IP Deskphones SIP, Release 6.3.

3. **Settings File** - Directives and values specified in the 46xxsettings.txt file that the phone retrieves from the fileserver.
4. **PPM** - Configuration values downloaded from the Personal Profile Manager (PPM) in Session Manager. These values are created by administrative operations in System Manager, and include station features, dial plan information, contacts, etc. The PPM acquires them during System Manager to Session Manager database replication.
5. **Manual Entry** - Configuration that is manually entered on the phone by the installer or user, using the local craft procedures menu (aka, "craft" interface).
6. **Cached Values** - Values from previous sessions that are stored in non-volatile memory on the phone.

Which Configuration Source Takes Priority?

For some directives or values, the same variables can be set by more than one of these sources, i.e., the phone might initially get its SIP proxy IP address from DHCP, and then have that value overridden by 46xxsettings.txt directives. The replacement value might subsequently be replaced again through a PPM download, and the user might decide to manually override all those mechanisms and enter the SIP proxy address manually on the phone.

If you set two different values for the same parameter through PPM and the 46xxsettings.txt file, the PPM settings override the settings in the 46xxsettings.txt file. Similarly, SIP call settings entered manually into the phone through the local craft procedures menu take precedence over other sources for this data, e.g., 46xxsettings.txt, or PPM. The only way to override these static settings is to go into the local craft procedures menu and remove the settings or perform a "Clear" of the deskphone from the local craft procedures menu. You can find a detailed discussion of the order of precedence of the different configuration sources in the "***Administrative Alternatives and Options***" section of Administering Avaya 9601/9608/9611G/9621G/9641G IP Deskphones SIP, Release 6.3.

46xxsettings.txt Default File

Default 46xxsettings.txt and Axxxsettings.txt (settings file specific to the ADVD) files are available for download from support.avaya.com:

Endpoint	URL
Avaya one-X® Deskphone SIP 96X1 Release 6.3	46xxsettings.txt
Avaya one-X® Deskphone SIP 96XX Release 2.6.10	46xxsettings.txt
Avaya Desktop Video Device A175 (ADVD) Release 1.1.x	Axxxsettings.txt

The default files have all lines commented out with "##" at the beginning of each line. To make a directive take effect or assign a particular value, you edit the file, remove the "##" at the beginning of that line, modify the line as needed, and then write the file back out. Each directive in the file is accompanied by a block of comment text that explains its function and possible values in detail.

The large amount of comment text interspersed with control statements makes the file a bit difficult to read, especially during initial setup and testing. You can simplify things by populating all the desired lines in the file with your values, and then removing all the comment text.

The 46xxsettings.txt file contains conditional statements and go-to statements in addition to GET and SET statements. You use conditional statements to custom tailor the file for each type of station that you deploy. For example, you can group statements that you only want to apply to 9641G stations into a section of the file that is only reached for 9641G stations.

Similarly, you can use the GROUP parameter in conditional statements to custom-tailor phone behaviors for specific communities of stations in your user population. You define a GROUP in the 46xxsettings.txt file and edit in the settings appropriate to that GROUP. Then you set that GROUP value on the station manually, in order to add it to that specific community of phones. The GROUP capability is valuable any time you want to apply special treatment to only a subset of all the stations.

Minimum Settings to Get SIP Phones Working

The minimum 46xxsettings.txt file entries required to get SIP calls working are shown in the following table:

Name	Description	Example Value
SIG (See Note 1)	Signaling Type (H.323 or SIP)	2
SIPDOMAIN	SIP Domain Name	sip.company.com
SIP_CONTROLLER_LIST	SIP Proxy Server (SM) IP Addresses	192.168.10.15:5060;transport=tcp
SIMULTANEOUS_REGISTRATIONS	Register with multiple SMs, i.e., primary SM, secondary SM, survivable remote SM.	2

Note 1: You only set the SIG parameter in 46xxsettings.txt, when you intend for booting 96x1 H.323 phones to automatically convert to SIP without human intervention.

Recommended additional entries include:

Name	Description	Example Value
ENABLE_PRESENCE	Enable Presence	1
SNTPSRVR	Secure Network Time Protocol Server IP address	192.168.50.44
GMTOFFSET	Time Zone Offset from GMT	“-7:00”
DSTOFFSET	Daylight Savings Time Offset	“1”
DSTSTART	Daylight Savings Time	“2SunMar2L”

	Start	
DSTSTOP	Daylight Savings Time Stop	"1SunNov2L"
PHNEMERGNUM	Emergency Phone Number	9911

Other directives are necessary if you wish to enable Instant Messaging, integrate with a voice messaging system, use the phone's WML browser to search for contacts in an enterprise directory, etc. The list of all such directives is provided in the Administrator Guide for the phone. For the 96x1 phones, you'll find that information in chapter 7, "Administering Deskphone Options", of the document, *Administering Avaya 9601/9608/9611G/9621G/9641G IP Deskphones SIP, Release 6.3*.

Appendix H: Session Manager's Personal Profile Manager (PPM)

What is the Personal Profile Manager?

The PPM is a software module within Session Manager. It evolved from the similar PPM in Avaya's first SIP proxy server, *SIP Enablement Services* (SES). It implements a Java-based Web Service using industry standard frameworks, and it runs as a Java HTTP Servlet in Session Manager's JBOSS (a JSR 289 Servlet Container).

The PPM:

- Implements a Web Service that endpoints use to retrieve and manage SIP-related user data.
- Enables Avaya SIP Telephony (AST) features on endpoints that can support them.
- Uses an open standards interface (published WSDL) to allow interoperability with third party endpoints like the Toshiba SIP Phone.
- Supports Mobility by allowing users to maintain features and settings across enterprise locations.

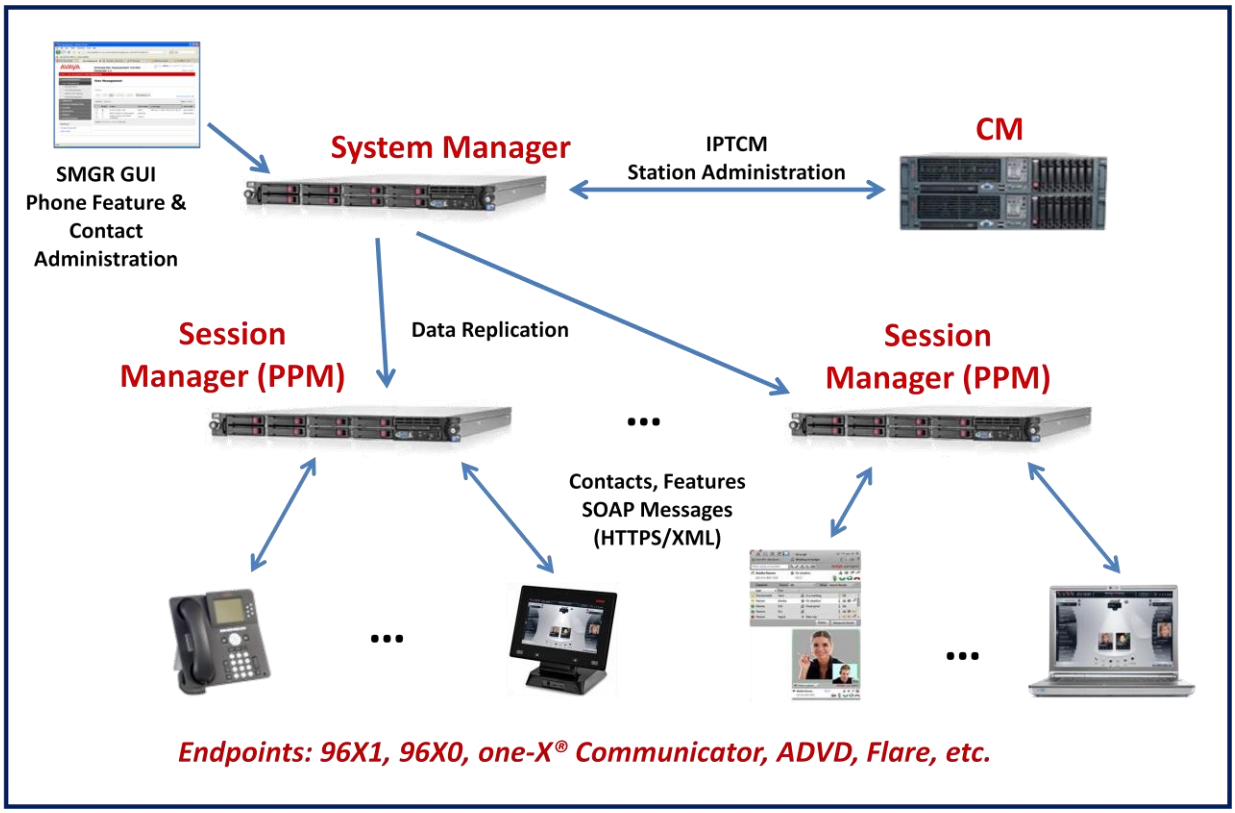
What is the purpose of the PPM?

- Provide Secure, Unified Interface to SIP Clients
  - Direct and easy to use interface vs. internal schemas
  - Define interfaces to be easily consumed by endpoints
    - E.g. pre-sorted data sets
- Account for Differences in Endpoint Versions, Models, Vendors

  - Avaya one-X® Desktop Edition (aka SIP Softphone), Toshiba SIP Phone, one-X® Communicator SW are not always aligned
- Provide Re-Usable Service Interface for Universal Integration
  - E.g., DevConnect PPM SDK
- Run on Multiple Platforms, from Embedded to Enterprise

Personal Profile Manager Architecture

The following diagram illustrates how the Personal Profile Manager communicates with the other components in the solution:

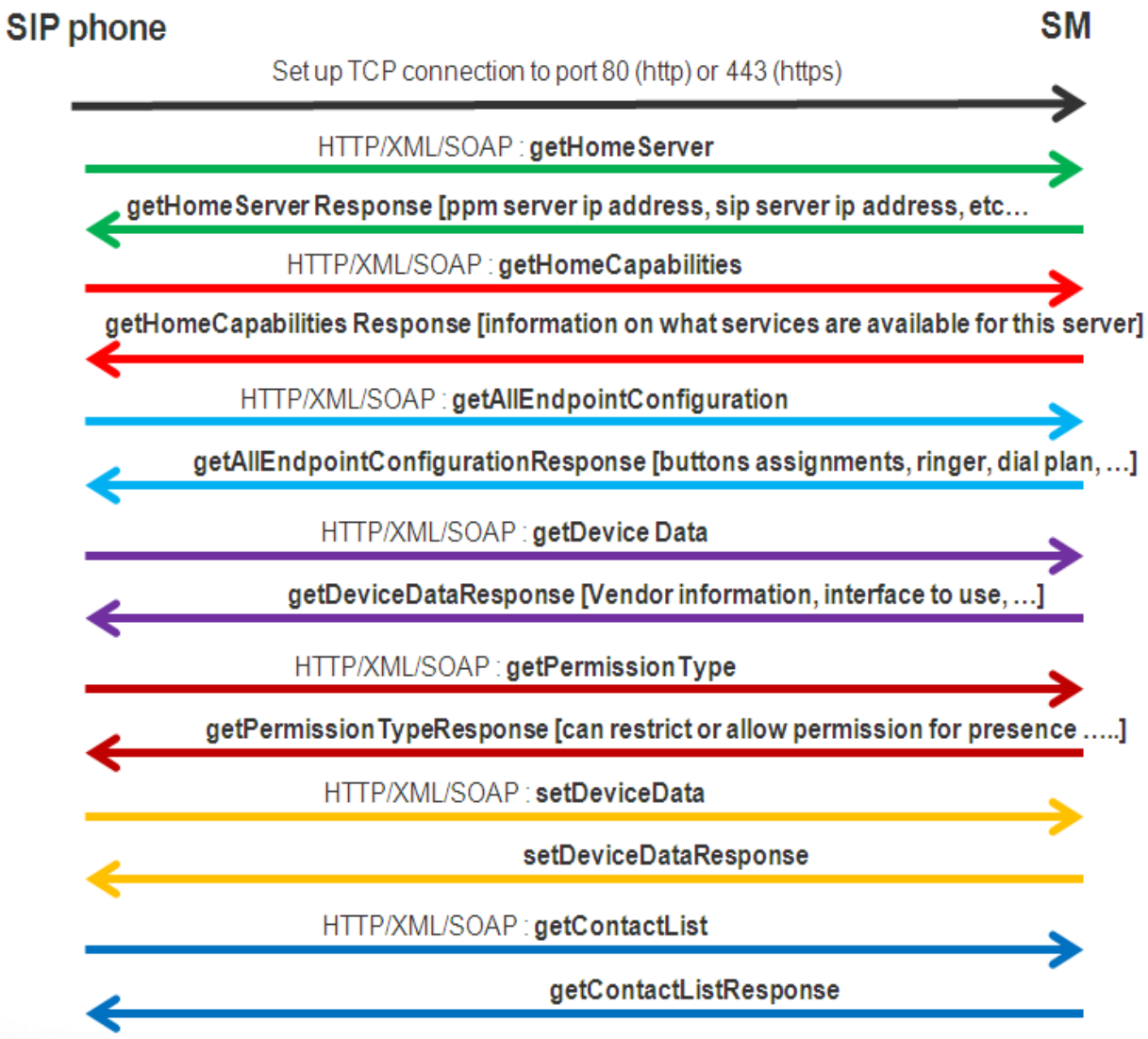


1. **Station Administration** - The System Manager (SMGR) Web Console interface appears at the upper left of the diagram. The system administrator uses this interface to create stations and configure station features and contact lists.
2. **IPTCM (IP Telephony Centralized Management)** - **System Manager** interworks with **Communication Manager** (CM) during the station administration process, so that all desired station features are provisioned and captured in the SMGR database as well as in CM's translation files.
3. **Database Replication** - The SMGR then replicates its database to all Session Managers (SMs) via the Data Replication Service (DRS), so that the SMs have exact copies of the SMGR data.
4. **Initial PPM Download to Endpoints** - When they reboot, AST-capable SIP endpoints (96x1, 96x0, one-X® Communicator, ADVD, Flare® Experience for Windows or iPad®, etc.) register with SM, subscribe to PPM feature packages, and then request PPM data

downloads to configure their features, buttons, and contact lists. The PPM gets the requested information from the database that was replicated to the SM from SMGR. The endpoint requests and PPM responses are carried in Simple Object Access Protocol (SOAP) XML message bodies contained in HTTPS messages.

5. **Subsequent PPM-Endpoint Updates/Syncs** - Once the endpoints are fully in service, SOAP updates continue to flow between the PPM and the endpoints as contact lists and features are changed by the user and by the system administrator.

Personal Profile Manager (PPM) flow



Appendix I: Acronyms and Terms

1-9

1XC – Avaya one-X® Communicator

A

AAR – Automatic Alternate Routing
ADVD – Avaya Desktop Video Device
ARS – Automatic Route Selection
AST – Avaya Advanced SIP Telephony

B

C

CAC – Call Admission Control
C-LAN – The TN799DP “Control-LAN” CM Ethernet Interface circuit pack.
CM – Avaya Aura® Communication Manager
COR – Class of Restriction
COS – Class of Service
CRAFT – The term commonly used for the local craft procedures manual programming telephone interface. The installer accesses local craft procedures by entering (mute-button)craft# or (mute-button)27238# to activate the interface.

D

DDI – Direct Dial-In
DHCP – Dynamic Host Configuration Protocol

DID – Direct Inward Dialing
DRS – Data Replication Service
DST – Daylight Saving Time

E

F

FAC – Feature Access Code
FRL – Facility Restriction Level
FNE – Feature Named Extension
FNU – Feature Named Uniform Resource Identifier (URI)
FQDN – Fully Qualified Domain Name

G

GUI – Graphical User Interface

H

H.323 – (Not an acronym) An ITU-T IP Telephony Signaling Protocol Specification. The term is commonly used as an adjective to refer to VoIP telephones that use H.323 instead of SIP for registration and signaling.

HTML – Hypertext Markup Language
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol Secure

I

ICHT – Incoming Call Handling Table
IM – Instant Messaging
IMS – Internet Multimedia Subsystem

IP – Internet Protocol
IPTCM – IP Telephony Centralized Management

J

JBOSS – Java Bean Open Source Software
JSR – Java Specification Request

K

L

LAN – Local Area Network
LLDP – Link Layer Discovery Protocol

M

MIB – Management Information Base
MST – Message Sequence Tracer
MWI – Message Waiting Indicator

N

NIC – Network Interface Card
NTP – Network Time Protocol

O

OPS – Off-PBX Station
OPTIM – Off-PBX Telephony Integration & Mobility

P

PBX – Private Branch Exchange
PCN – Product Correction Notice
PLDS – Avaya Product Licensing and Delivery System
POE – Power over Ethernet (IEEE 802.3af)
PPM – Personal Profile Manager
PROCR – The CM “Processor Ethernet” interface implemented on the CM Server’s LAN NIC.
PSN – Product Support Notice
PSTN – Public Switch Telephone Network

Q

R

S

SBC – Session Border Controller
SES – SIP Enablement Services
SIP – Session Initiation Protocol
SM – Avaya Aura® Session Manager
SMGR – Avaya Aura® System Manager
SMTP – Simple Mail Transfer Protocol
SNMP – Simple Network Management Protocol
SNTP – Secure Network Time Protocol
SOAP – Simple Object Access Protocol
SP – Avaya Aura® System Platform
SPPOE – Single Port Power over Ethernet injector
SRVR – Server
SSH – Secure Shell (RFC 4253)

T

TCP – Transmission Control Protocol

TLS – Transmission Layer Security

U

UDP – Uniform Dial Plan
URI – Uniform Resource Identifier

V

VLAN – Virtual Local Area Network

W

WML – Wireless Markup Language
WSDL – Web Services Description Language

X

XML – Extensible Markup Language

Y

Z