Avaya one-X for Apple SIP Clients

Administrator guide

March 2012

Notice

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

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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(s) 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 this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site:

http://www.avaya.com/support . Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.:

Licenses

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

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

License type(s)

Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including 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. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

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

Preventing toll fraud

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

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, one-X Portal, Communication Manager, Application Enablement Services, Modular Messaging, and Conferencing are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

http://www.avaya.com/support

Avaya support

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

http://www.avaya.com/support

Table of Contents

Overview

Avaya one-X for Apple SIP Clients Administrator guide includes the procedure to administer Avaya one-X® Communicator for Mac OS X and Avaya one-X® Mobile SIP for iOS.

Avaya one-X® Communicator for Mac OS X is a communication tool using which you can manage your telephony tasks. Avaya one-X® Communicator for Mac OS X provides you with simple, intuitive access to all of your contacts and the features of the desk telephone in a simple soft phone on your Apple computer.

Avaya one-X® Mobile SIP for iOS helps you to manage your telephonic communication tasks by providing you with simple, intuitive access to all of your contacts, and the features of the desk phone in a simple soft phone. Avaya one-X Mobile SIP for iOS adds the capability of Voice over Wi-Fi on a corporate wireless-enabled, Avaya Aura SIP environment.

Basic features

The Avaya one-X Communicator for Mac OS X and the Avaya one-X Mobile SIP for iOS have the following common basic features:

- Full set of call-control features, including transfer and ad-hoc conferencing
- User preference settings to configure dial plans and emergency number
- Dial from call logs
- PSTN access through Avaya Aura® Communication Manager (Communication Manager)

Following are basic features of Avaya one-X Communicator for Mac OS X:

- Select and control microphone and speaker
- Click-to-dial capability
- User preference settings to control connections to the Avaya Aura environment and to the corporate directory
- Docking and undocking of the dial pad
- Click to access voice mail
- Redial the last number
- Speed dial
- Desktop access to your contact list and enterprise directory

Avaya OneX Communicator for Mac OS X 1.0.0 supports two usage modes:

- My Computer: Place and receive calls using the computer resources.

- Other Phone: Place, receive, and control calls using the GUI to an external phone.

Avaya OneX Communicator for MacOS X 1.0.1 only supports the My Computer usage mode.

For more information, see *Usage modes* in *Avaya one-X Communicator for Mac OS X User Guide* on the Avaya Support Web site support.avaya.com.

Following are basic features of Avaya one-X Mobile SIP for iOS:

- Voice over Wi-Fi connectivity
- Call persistence
- Voice mail message - waiting indicator
- Favorites list and use the Favorites list to speed-dial your top contacts
- Configure access to your corporate directory, and to your Microsoft Exchange contacts information
- Bridged Line Appearances
- ASM-ASM failover

Recommendations

Ensure that you upgrade Communication Manager, Media Servers, and SIP Enablement Services or Avaya Aura® Session Manager (Session Manager) with the latest Service Pack or patches for maximum client stability.

Visit the Avaya support Web site at support.avaya.com to access software and firmware downloads.

Prerequisites

Server-side requirements for Avaya one-X® Communicator for Mac OS X and Avaya one-X Mobile SIP for iOS

You must have one of the following two combination of servers for the Avaya one-X® Communicator for Mac OS X and Avaya one-X Mobile SIP for iOS:

- Avaya Aura® Communication Manager 5.2 and Avaya Aura® SIP Enablement Services 5.2
- Avaya Aura® Communication Manager 6.X and Avaya Aura® Session Manager 6.X

Client-side requirements for Avaya one-X® Communicator for Mac OS X

Your device must meet the following minimum requirements to use the Avaya one-X® Communicator for Mac OS X:

Hardware:

- Processor: Intel 1.6 GHz or higher
- Memory: 1 GB of RAM
- Hard disc space: 1 GB

Note:
Avaya one-X® Communicator for Mac OS X supports 64-bit operation.

Software:

- Avaya one-X® Communicator for Mac OS X 1.0.1: MacOS X Lion (10.7.x).
- Avaya one-X® Communicator for Mac OS X 1.0.0: MacOS X Leopard (10.5.x) or MacOS X Snow Leopard (10.6.x).

Client-side requirements for Avaya one-X Mobile SIP for iOS

The following minimum requirements must be met to use the Avaya one-X Mobile SIP for iOS:

Hardware:

- iPod touch 4th generation
- iPhone 3GS or iPhone 4 or 4S
- iPad 1 or iPad 2

Software:

- iOS 4.3 or later

Obtaining the software

Obtaining the Avaya one-X® Communicator for Mac OS X application

To obtain the Avaya one-X® Communicator for Mac OS X licensed software, send a request to apslicense@avaya.com with the following information:

- Customer name
- Avaya partner name (if applicable)
- SAP order number
- Product name, that is, Avaya one-X Communicator for Mac OS X
- Number of licenses ordered

Once the request is received and processed, instructions for downloading the software will be e-mailed to the e-mail address that the request was originated from. You should receive a response within 48 hours; response time can vary depending on the demand.

Obtaining the Avaya one-X Mobile SIP for iOS application

You can obtain the Avaya one-X Mobile SIP for iOS application from the iTunes App Store. You can find the Avaya one-X Mobile SIP for iOS application by searching for the keyword **Avaya one-X Mobile SIP**.

To obtain the Avaya one-X Mobile SIP for iOS license, your Avaya representative must request a license file from apslicense@avaya.com. The license request e-mail must include the following:

- Customer name
- Avaya partner name (if applicable)
- SAP order number
- Product name, that is, Avaya one-X Mobile SIP for iOS
- Number of licenses ordered

For instructions on configuring the license server, see Configuring the license file for Avaya one-X Mobile SIP for iOS on page 31.

If you are already using the existing iOS client, ensure the following for the license file:

- IT administrators must set up the license file on the Web server before you start updating your clients to 1.0.2.
- IT administrators should proactively publish your updated user settings information in your user community, describing the new *Configuration* URL address entry.

Configuring Communication Manager 5.2

This section provides procedures for configuring IP codec sets and associating Session Initiation Protocol (SIP) telephone numbers with off-PBX telephone stations in Communication Manager 5.2.

IP codecs set identify the codecs to use in Voice over IP (VoIP) calls. An off-PBX telephone is a telephone which Communication Manager does not control; for example, a cellular phone, a desk phone, or a SIP client. However, you can apply the Communication Manager features and calling privileges to an off-PBX telephone by associating a local, on-PBX extension with the off-PBX telephone. These on-PBX telephones, which are associated with off-PBX telephones are known as outboard proxy SIP (OPS) stations.

You must perform the configuration steps on the Communication Manager system access terminal (SAT).

Note:
Configuration information in the following sections only lists those fields for which you must enter a value. All the other fields use default values.

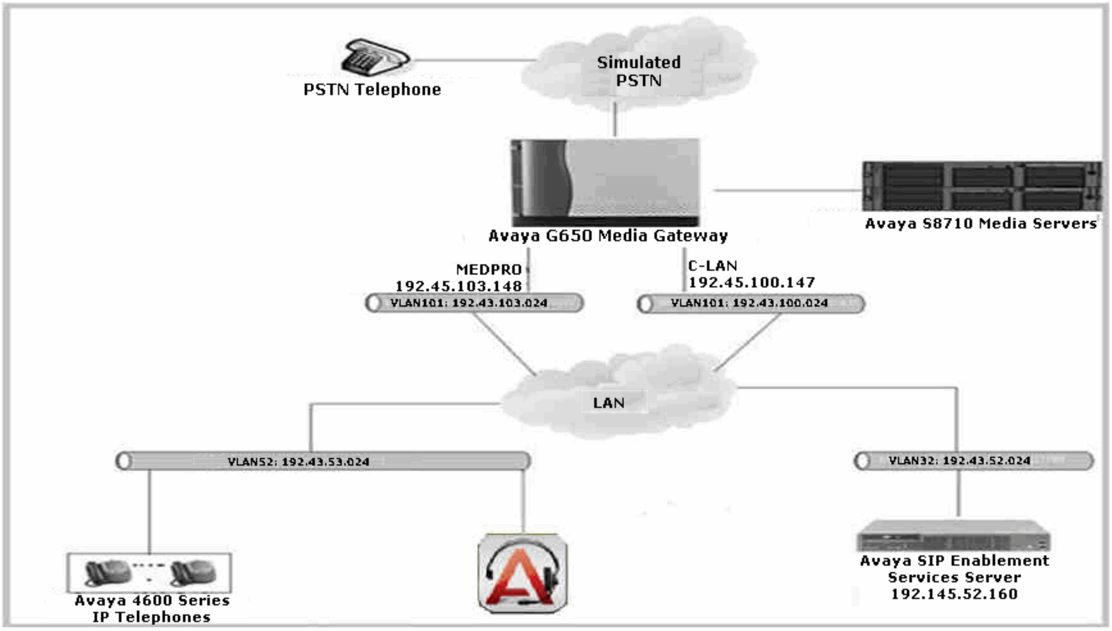


Figure 1: Sample network setup for Communication Manager 5.2

The sample network setup for Communication Manager 5.2 consists of a pair of Avaya S8710 Media Servers, an Avaya G650 Media Gateway, an Avaya SIP Enablement Services (SES) server, and the Avaya one-X® Communicator for Mac OS X and Avaya one-X® Mobile SIP for iOS. Communication Manager is installed on the S8710 Media Servers. The solution described is also extensible to other Avaya Media Servers and Media Gateways. For completeness, Avaya H.323 IP telephones have been provided. The analog PSTN telephone is included to demonstrate calls routed by Communication Manager between the Avaya one-X mobile SIP for iOS and PSTN.

Call from SIP user

1. The Avaya SIP client originates a call to a user on the PSTN. The system delivers the call request to SES. If the originator were an H.323, digital, or an analog end point, then the system directly sends the call request to PSTN through the media gateway from Avaya S8710 Media Server running Communication Manager.

2. SES routes the call over the SIP trunk to the Avaya 8710 Server running Communication Manager for origination services. Therefore, Communication Manager can apply the appropriate call restrictions to the end point, handle call routing, and track the status of the SIP client, which is an off-PBX station.

   Station is added first as an off-PBX station in Communication Manager. An off-PBX telephone is a phone that Communication Manager does not control, such as a cellular phone, a home telephone, or a SIP telephone. However, Communication Manager features and calling privileges can be applied to an off-PBX telephone by associating a local, on-PBX extension with the off-PBX telephone. This approach is taken for SIP telephones that register with the Avaya SES server and Session Manager and intend to use Communication Manager for call origination and termination services. Similarly, on the Avaya SIP servers, the number of the SIP telephone is administratively associated with the extension of the on-PBX station.

3. After applying the origination services, Communication Manager routes the call to PSTN.

Call from PSTN user

1. A user on the PSTN dials a DID number assigned to the Avaya SIP client at the enterprise site.
2. Based on the DID, the system routes the call to Avaya 8710 server running Communication Manager over PSTN trunk.
3. Since the call is destined for an Avaya SIP client, Communication Manager routes the call to SES over SIP trunk.
4. SES terminates the call to the Avaya SIP client.
5. If the destination of the call is an H.323, digital, or analog end point, then Communication Manager terminates the call directly to the end point.

Opening SAT

You can access the SAT interface by any of the following processes:

- Putty
- Provision

For example, perform the following steps to access SAT through Putty:

1. Double click on the Putty.exe file to open the **Putty Configuration** window.

   Note:
   Contact Avaya professional service personnel to get a copy of the Putty software.

2. On the **Host Name (or IP Address)** field, enter the IP address of your Communication Manager server.

3. Click **Open**.
4. On the command prompt, enter your user id and press **Enter**.
5. Enter your password and press **Enter**.
6. On the **Enter your terminal type** field, enter the type of your terminal, for example **sunt**.
7. Enter `n` and press **Enter**.
8. Enter `autosat` and press **Enter**.
9. Enter your password and press **Enter**.
10. Enter a **Terminal Type**, for example, `sunt`.
    The SAT interface opens.

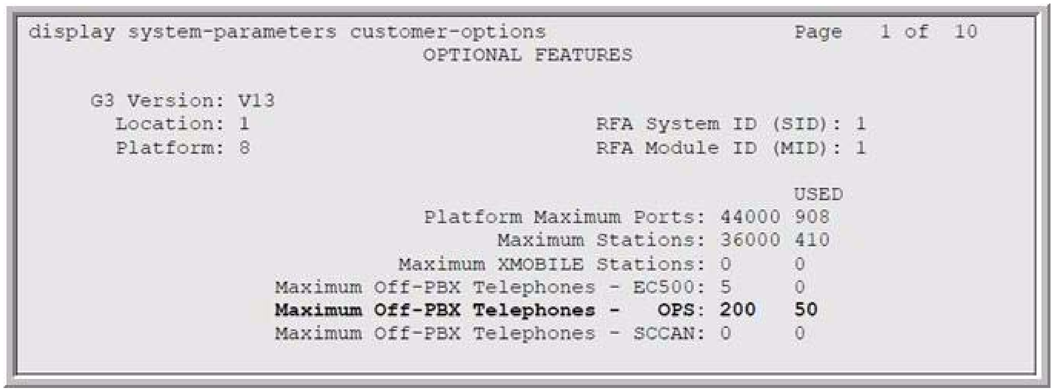
Verifying the capacity

To perform capacity verification:

1. On the SAT interface, enter the following command:

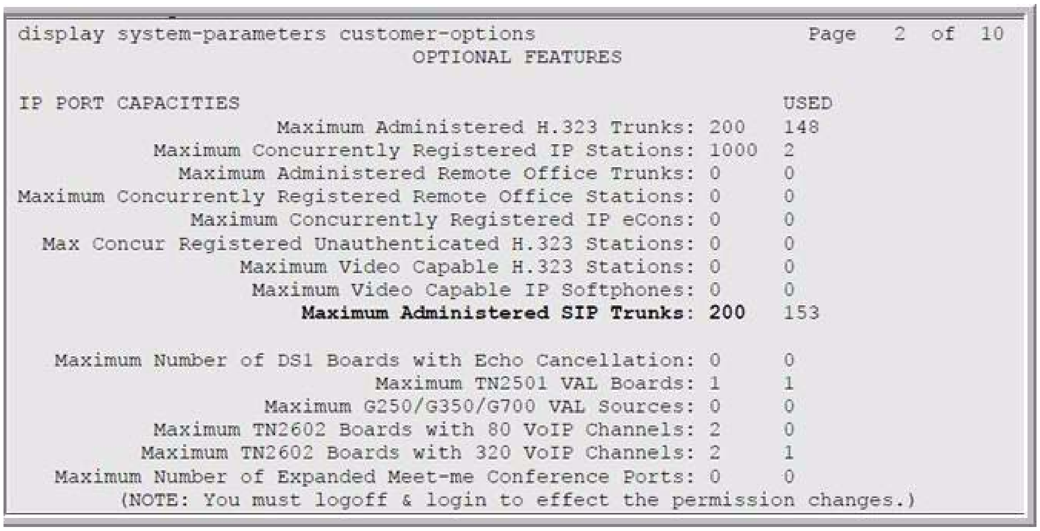
   `display system-parameters customer-options`

2. On the **OPTIONAL FEATURES** page, verify that there are sufficient **Maximum Off-PBX Telephones – OPS** licenses.



```
display system-parameters customer-options                    Page   1 of  10
                                OPTIONAL FEATURES

     G3 Version: V13
       Location: 1                            RFA System ID (SID): 1
       Platform: 8                            RFA Module ID (MID): 1

                                                                USED
                              Platform Maximum Ports: 44000 908
                                    Maximum Stations: 36000 410
                            Maximum XMOBILE Stations: 0     0
                  Maximum Off-PBX Telephones - EC500: 5     0
                  Maximum Off-PBX Telephones -   OPS: 200   50
                  Maximum Off-PBX Telephones - SCCAN: 0     0
```

3. On the next page of the **OPTIONAL FEATURES** page, verify that the number of SIP trunks supported by the system is sufficient for the number of trunks to use.

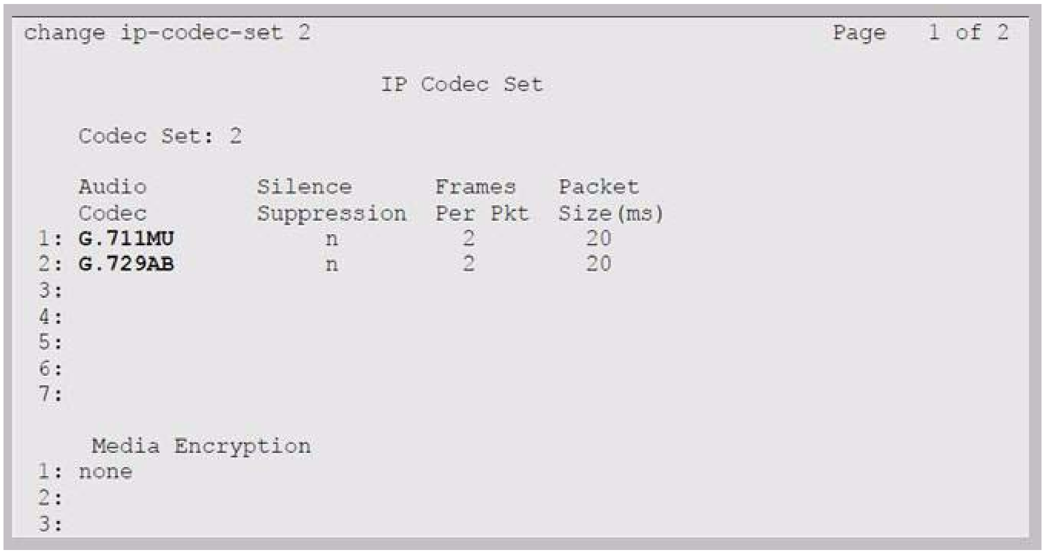


```
display system-parameters customer-options                      Page   2  of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 200    148
           Maximum Concurrently Registered IP Stations: 1000   2
             Maximum Administered Remote Office Trunks: 0      0
Maximum Concurrently Registered Remote Office Stations: 0      0
              Maximum Concurrently Registered IP eCons: 0      0
  Max Concur Registered Unauthenticated H.323 Stations: 0      0
                  Maximum Video Capable H.323 Stations: 0      0
                   Maximum Video Capable IP Softphones: 0      0
                       Maximum Administered SIP Trunks: 200    153

   Maximum Number of DS1 Boards with Echo Cancellation: 0      0
                             Maximum TN2501 VAL Boards: 1      1
                     Maximum G250/G350/G700 VAL Sources: 0      0
           Maximum TN2602 Boards with 80 VoIP Channels: 2      0
          Maximum TN2602 Boards with 320 VoIP Channels: 2      1
   Maximum Number of Expanded Meet-me Conference Ports: 0      0
        (NOTE: You must logoff & login to effect the permission changes.)
```

Configuring IP codec set

1. On the SAT interface, enter the following command:
   `change ip-codec-set n`
   Where ***n*** is the number of the IP codec set. Enter a value between one and seven for the IP codec set number.

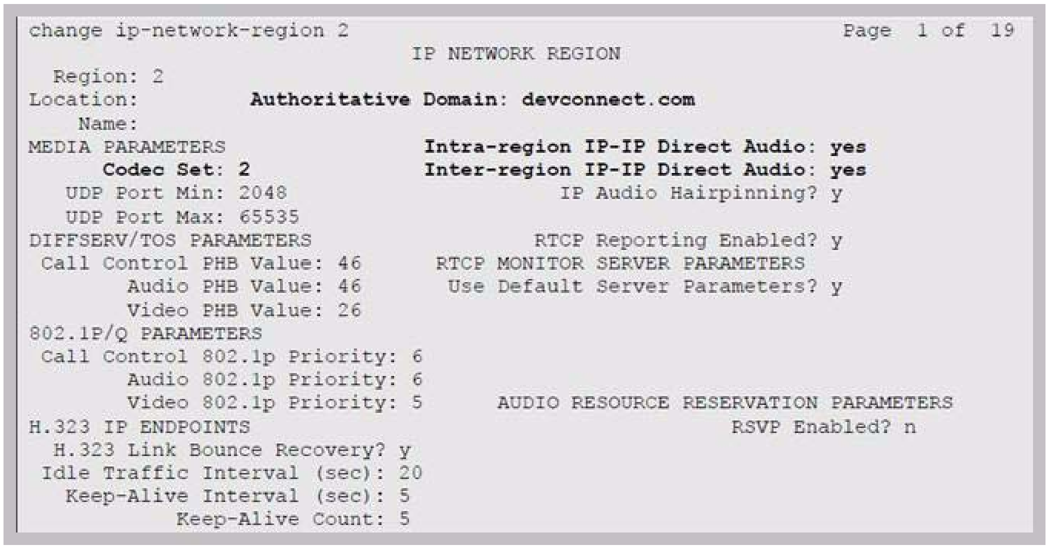
   Note:
   For the compliance testing, **G.711MU** and **G.729AB** were used and **Media Encryption** was set to **none** as SIP telephony does not support encryption.



```
change ip-codec-set 2                                          Page   1 of  2

                              IP Codec Set

    Codec Set: 2

    Audio         Silence       Frames   Packet
    Codec         Suppression   Per Pkt  Size(ms)
 1: G.711MU           n           2        20
 2: G.729AB           n           2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption
 1: none
 2:
 3:
```

2. Enter the following command:
   `change ip-network-region n`
   Where ***n*** is the network region value. Enter a value between one and 250 for the network region value.

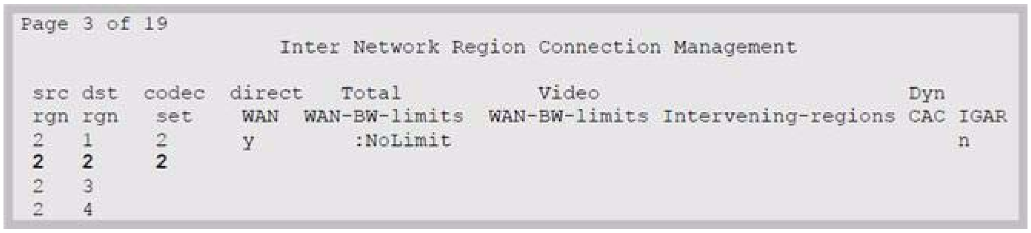
3. Specify the following fields:
   - **Authoritative Domain**: This must match the SIP domain
   - **Intra-region IP-IP Direct Audio**
   - **Codec Set**
   - **Inter-region IP-IP Direct Audio**



```
change ip-network-region 2                                      Page  1 of  19
                               IP NETWORK REGION
  Region: 2
Location:         Authoritative Domain: devconnect.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                    RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Configuring IP network region

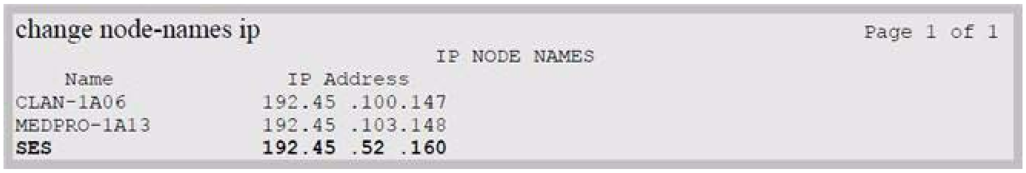
On the next page of the **IP NETWORK REGION Connection Management** page, enter **y** to enable inter-region connectivity between regions as shown in the following image:



```
Page 3 of 19
                     Inter Network Region Connection Management

 src dst  codec  direct   Total           Video                         Dyn
 rgn rgn   set    WAN  WAN-BW-limits  WAN-BW-limits Intervening-regions CAC IGAR
 2   1     2      y        :NoLimit                                          n
 2   2     2
 2   3
 2   4
```

Configuring IP node names

1. On the SAT interface, enter the following command:
   `change node-names ip`
2. Add a node name for SES server along with the IP address as shown in the following image:



```
change node-names ip                                                    Page  1 of  1
                                         IP NODE NAMES
    Name                 IP Address
CLAN-1A06              192.45 .100.147
MEDPRO-1A13            192.45 .103.148
SES                    192.45 .52  .160
```

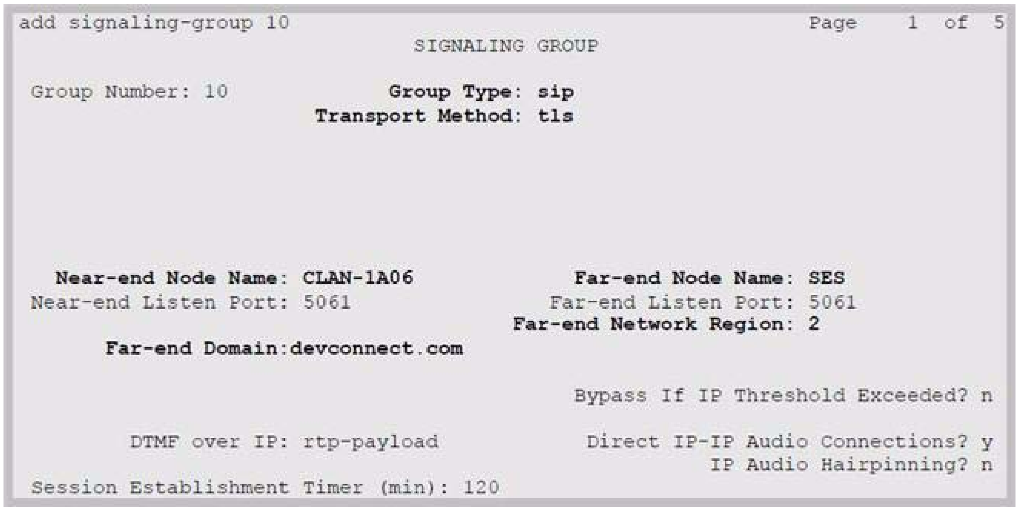
Configuring SIP signaling

1. On the SAT interface, enter the following command:

   `add signaling-group`

2. Specify the following fields:

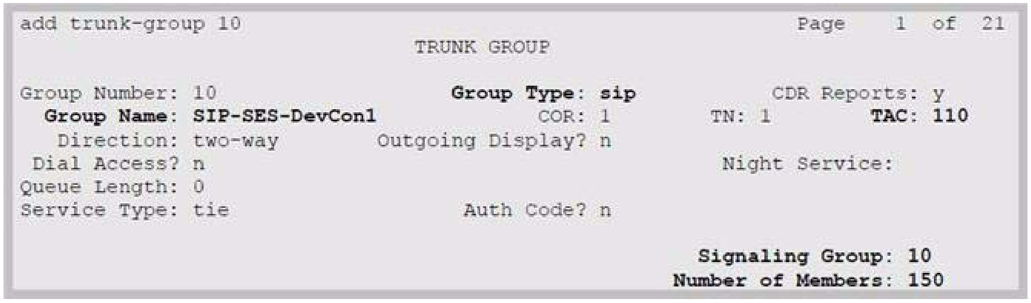
   - **Group Type**: Set to sip
   - **Transport Method**: Set to tls
   - **Near-end Node Name**: Set to CLAN name
   - **Far-end Node Name**: Set to Avaya SIP Enablement Services server name
   - **Far-end Network Region**: Set to the configured region
   - **Far-end Domain**: This must match the SIP domain



```
add signaling-group 10                                          Page    1  of  5
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
                        Transport Method: tls







  Near-end Node Name: CLAN-1A06             Far-end Node Name: SES
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 2
      Far-end Domain:devconnect.com

                                            Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
                                                      IP Audio Hairpinning? n
 Session Establishment Timer (min): 120
```

Configuring SIP trunking

1. On the SAT interface, enter the following command:
   `add trunk-group`
2. Specify the following fields:
   - **Group Type**: Set to sip.
   - **TAC**: Trunk access code, set to any number with one to four digits. You can use the characters asterisk (*) and pound sign (#) as the first digit.
   - **Signaling Group**: Set to the same value as the group number you have configured to ise for SIP trunk.
   - **Number of Members**: Set to any value between zero and 250.
   - **Group Name**: Enter a descriptive name for the group name.



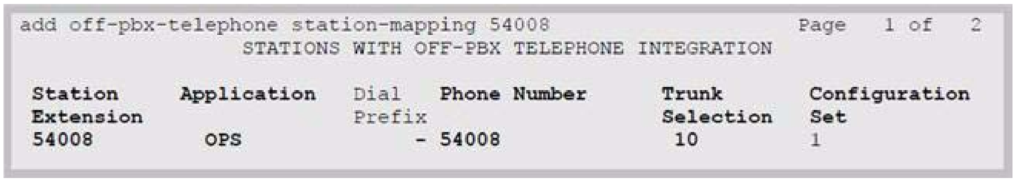
```
add trunk-group 10                                               Page   1  of  21
                                TRUNK GROUP

Group Number: 10                 Group Type: sip          CDR Reports: y
  Group Name: SIP-SES-DevCon1            COR: 1        TN: 1        TAC: 110
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                        Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                      Signaling Group: 10
                                                    Number of Members: 150
```

Configuring SIP stations

To configure an OPS station:

1. On the SAT interface, enter the following command:
   `add station` ***`extension number`***
   Where ***`extension number`*** is the local extension number of the user.
2. On the page 1 of the **STATION** form, specify the following:
   - **Type**: Set to 96XX SIP
   - **Port**: Set to X for administration without hardware (AWOH) as SIP stations are not directly connected to Communication Manager.
   - **Name:** Enter a descriptive name.
   - **IP Soft phone**: Set to y.
3. Go to next page of STATION form 2.

4. If the connectivity between Communication Manager and Modular Messaging is SIP, then you need to have the following settings while configuring the STATION:
   - **LWC Reception**: spe
   - **MWI Served User Type**: sip-adjunct
5. On the **BUTTON ASSIGNMENT** field, add the number of call appearances entries.
   The number of call appearances must match the value of the **Call Limit** field on the page 2 of the **STATION WITH OFF-PBX TELEPHONE INTEGRATION** page.
6. Enter the following command:
   `add off-pbx-telephone station-mapping`
7. Specify the following fields:
   - **Station Extension**: Specify the extension of the OPS station that you have configured.
   - **Application**: Set to OPS.
   - **Phone Number**: Enter the number of the station that Avaya one-X® Communicator for Mac OS X will use for registration and call termination.
     It is not necessary that the phone number has to be the same as the **Station Extension**.
   - **Trunk Selection**: Set to the trunk group number, which you have built between the SIP Enablement Services server and the Communication Manager server.



```
add off-pbx-telephone station-mapping 54008                    Page   1 of   2
                     STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station      Application    Dial    Phone Number      Trunk       Configuration
 Extension                   Prefix                    Selection   Set
 54008          OPS              -  54008               10         1
```

8. Go to page 2 of the **STATION WITH OFF-PBX TELEPHONE INTEGRATION** page and verify that the value of the **Call Limit** field matches the number of call appearances you have configured on step 4.

Configuring Avaya Aura SIP Enablement Services server

Avaya one-X® Communicator for Mac OS X registers with Avaya Aura® SIP Enablement Services server using SIP user accounts.

This section provides the steps for creating SIP user accounts in Avaya SIP Enablement Services server and associating the ISP users with the Communication Manager OPS station extension.

1. Open the Web browser of your computer.
2. On the address bar, enter: *xx.xx.xx.xx/admin*
   Where xx.xx.xx.xx is the IP address of your SIP Enablement Services server.

3. Log in with your administrator credentials.
4. Click the **Launch Administration Web Interface** link.
5. On the Administration Web interface, click the plus sign (**+**) to expand the options under **Server Configuration**.
6. Click **System Properties** and verify that the **SIP Domain** matches the **Far-end Domain** you have configured for the signaling group on Communication Manager.
7. Click **+** to expand the options under **Communication Manager Server**.
8. Click **Add**.
9. On the **Add Communication Manager Server** window, specify the following parameters:
    - **Communication Manager Server Interface Name**: Enter a descriptive name of the Communication Manager server.
    - **SIP Trunk Link Type**: Enter the **Transport Method** field value as **tls**.
    - **SIP Trunk IP Address**: Enter the CLAN IP address which you have specified while adding IP-Node names.
    - Click **Add** > **Continue**.
10. On the left pane of the SIP Enablement Services administration Web interface, expand **Users** and click **Add**.
11. On the **Add User** window, specify the following fields:
    - **Primary Handle**: Enter the telephone number for Avaya one-X® Communicator for Mac OS X. The number must match the Phone Number and Station Number used while adding the communicator.
    - **Password** and **Confirm Password**: Specify the password that the Avaya one-X® Communicator must use to register with the SIP Enablement Services server.
    - **Host**: Select the IP address or the Fully Qualified Domain Name (FQDN) of the SIP Enablement Services server.
12. **First Name** and **Last Name**: Enter the first name and the last name of the user.
13. Select the **Add Communication Manager Extension** check box.
14. Click **Add** > **Continue**.
15. On the **Add Communication Manager Server Extension** window, specify the following fields:
    - **Extension**: Specify the extension of the Communication Manager OPS station you have configured.
    - **Communication Manager Server**: Specify the Communication Manager where you have configured the OPS station.
16. Click **Add** > **Continue**.
17. On the bottom of the right panel, click **Continue**.

Note:

Repeat steps 10 through 17 to add additional SIP users for Avaya one-X® Communicator for Mac OS X.

Configuring Communication Manager 6

This section provides procedures to configure SIP trunks between Communication Manager and Session Manager.

If there is insufficient capacity, or a feature is not available, contact an authorized Avaya sales representative to make the appropriate changes.

Before you begin, ensure that Media Server is already configured on Communication Manager.

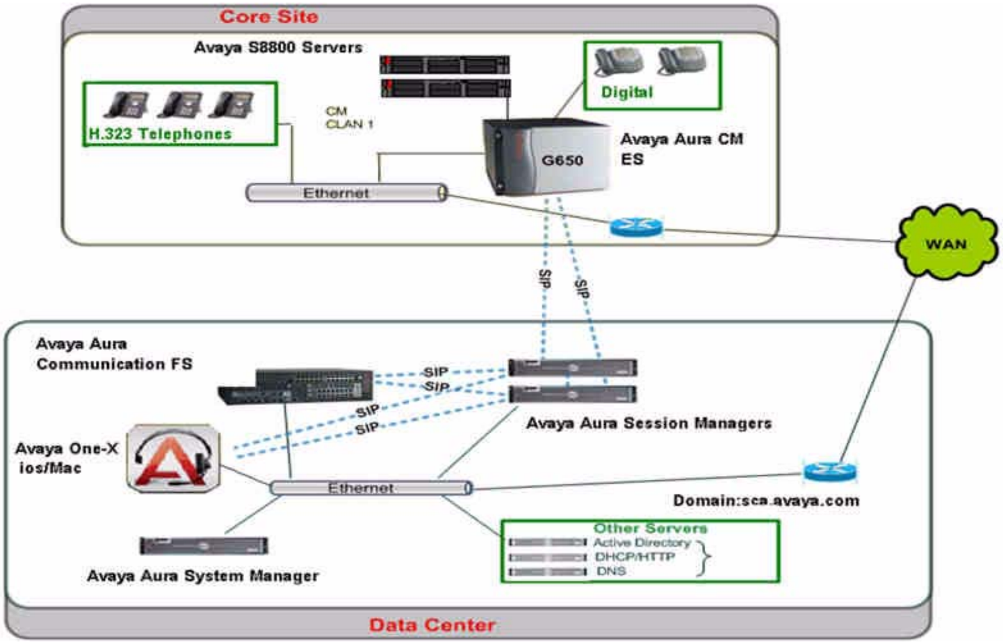


Figure 2: Sample network setup for Communication Manager 6

The sample network setup for Communication Manager 6 uses two Session Managers to support registration of Avaya one-X® Mobile SIP for iOS. Two Session Managers are deployed so that one Session Manager can serve as backup for the other in case of network or a Session Manager failure.

Note:

Avaya one-X® Communicator for Mac OS X does not support ASM failover.

Avaya one-X® Mobile SIP for iOS configured as SIP end points utilizes the Session Manager User Registration feature and is supported by the Communication Manager Feature Server. To improve reliability of the configuration, the SIP clients are registered to Session Manager. The sample configuration includes the Communication Manager Feature Server supporting IP Multimedia Subsystem (IMS) - SIP users registered to Session Manager. Communication Manager Feature Server is connected to both Session Managers via IMS-enabled SIP signaling groups and associated SIP trunk groups.

Avaya 9600-series IP telephones (H.323) and digital telephones are supported by a second Communication Manager that serves as an Evolution Server within the Session Manager architecture. The Communication Manager Evolution Server is connected over SIP trunks to both Session Managers. All intra-system calls are carried over these SIP trunks. Session Manager is managed by Avaya Aura® System Manager (System Manager). For the sample configuration, two Session Managers running on separate Avaya S8800 Servers are deployed as a pair of active-active redundant servers. Communication Manager Feature Server runs on the Avaya S8300D server with Avaya 450 Media Gateway.

Verifying capacity, routing, and networking

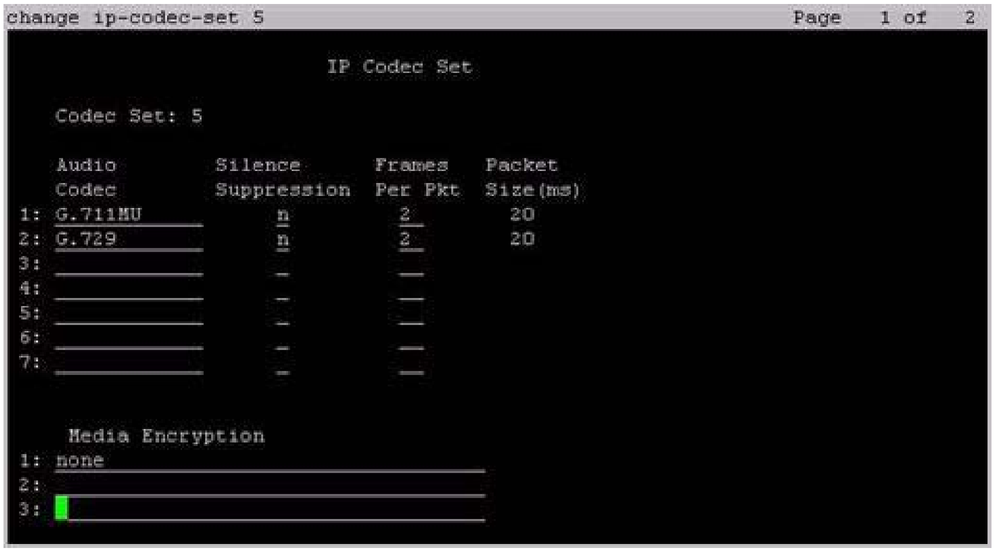
1. On the SAT interface, enter the following command:
   `display system-parameters customer-options`
   To know how to open the SAT interface, see Opening SAT on page 11.
2. On page 1 of the **OPTIONAL FEATURES** window, verify that the number specified for the **Maximum off-PBX Telephones - (OPS)** field is sufficient.
3. On page 2, verify that the number specified for the **Maximum Administered SIP Trunks** field is sufficient.
4. On page 3, enter **y** for the following fields:
   - **ARS?**
   - **ARS/AAR Partitioning?**
   - **ARS/AAR Dialing without FAC?**
5. Verify that the value of the **Private Networking** field is set to `y`.

Configuring Trunk-To-Trunk Transfers

1. On the SAT interface, enter the following command:
   `change system-parameters feature`
2. Set the value of the **Trunk-To-Trunk Transfer** field to **all**.

Configuring IP codec set

1. On the SAT interface, enter the following command:
   `change ip-codec-set n`
   Where *n* is the number used to identify the codec set.
2. On the **IP Codec Set** window, verify that the following fields has the values as specified:
   - **Audio Codec**: **G.711MU** and **G.729** as supported types
   - **Silence Suppression: n**
   - **Frames Per Pkt: 2**
   - **Packet Size (ms): 20**



```
change ip-codec-set 5                                          Page   1 of   2

                             IP Codec Set

    Codec Set: 5

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU            n          2       20
 2: G.729              n          2       20
 3:
 4:
 5:
 6:
 7:


     Media Encryption
 1: none
 2:
 3:
```

Configuring IP network region

1. On the SAT interface, enter the following command:
   `change ip-network-region n`
   Where *n* is an available network region.
2. Specify values for the following fields:
   - **Authoritative Domain**: Enter the current SIP domain for the configuration.
   - **Name**: Enter a descriptive name for the network region.
   - **Codec Set**: Enter the number of the configured IP codec set.
   - **Intra-region IP-IP Direct Audio**: Enter **yes**.

- **Inter-region IP-IP Direct Audio**: Enter **yes**.

Adding node names

On the SAT interface, enter the following command and specify the node names and IP addresses for Communication Manager and the virtual SM-100 Security Module of each Session Manager:

```
change node-names ip
```

Configuring SIP signaling groups and trunk groups

1. On the SAT interface, enter the following command:
   `add signaling group n`
   Where *n* is the signaling group number.
2. Specify the following fields:
   - **Group Type**: Enter **sip**.
   - **IMS Enabled**: Enter **y**.
   - **Transport Method**: Enter **tls**.
   - **Peer Detection Enabled?**: Enter **y**.
   - **Peer Server**: Use the default value.
   - **Near-end Node Name**: Enter the node name you had defined for Communication Manager.
   - **Far-end Node Name**: Enter the node name you had defined for Session Manager.
   - **Near-end Listen Port**: Enter **5061**.
   - **Far-end Listen Port**: Enter **5061**.
   - **Far-end Network Region**: Enter network region that you had entered while configuring IP network region.
   - **Far-end Domain**: Enter the same domain name, which you had entered for the **Authoritative Domain** field while configuring IP network region.
   - **DTMF over IP**: Enter **rtp-payload**.

Note:
If there is more than one Session Manager, repeat the above procedure for each Session Manager.

Adding SIP trunks

1. On the SAT interface, enter the following command:
   `add trunk-group n`
   Where *n* is the trunk group number.
2. On the page 1 of the **TRUNK GROUP** window, specify the following fields:
   - **Group Type**: Enter **sip**.
   - **Group Name**: Enter a name for the group.
   - **TAC**: Enter an trunk access code.
   - **Direction**: Enter **two-way**.
   - **Outgoing Display?**: Enter **y**.
   - **Service Type**: Enter **tie**.
   - **Signaling Group**: Enter the number of the signaling group.
   - **Number of Members**: Enter the number of members in the SIP trunk.
3. On page 3, specify the following fields:
   - **Numbering Format**: Enter **private**.
   - **Show ANSWERED BY on Display**: Enter **y**.
4. On page 5, specify the following fields:
   - **Support Request History**: Enter **y**.
   - **Telephone Event Payload Type**: Enter **120**.

Configuring route pattern

1. On the SAT interface, enter the following command:
   `change route-pattern n`
   Where *n* is an available route pattern.
2. Specify the following fields:
   - **Grp No**: Enter a row for each trunk group you have created.
   - **FLR**: Enter **0**.
   - **Numbering Format**: Enter **lev0-pvt**.
   - **LAR**: Enter **next** for first row. Use the default value for the second row.

Administering numbering plan

1. On the SAT interface, enter the following command:
   `change private-numbering n`
   Where ***n*** is the length of the private number.
2. Specify the following fields:
   - **Ext Len**: Enter the length of the extension numbers.
   - **Ext Code**: Enter the leading digit from the extension numbers.
   - **Trk Grp(s)**: Enter name of the trunk group.
   - **Private Prefix**: Leave this field blank, unless you define an enterprise canonical numbering scheme in Session Manager.
   - **Total Length**: Enter **7**.

Administering AAR digit analysis

1. On the SAT interface, enter the following command:
   `change aar analysis n`
   Where ***n*** is the first digit of the extension number you have defined.
2. Specify the following fields:
   - **Dialed String**: Enter leading digit of extension numbers.
   - **Min**: Enter the minimum number of digits that must be dialled.
   - **Max**: Enter the maximum numbers of digits that must be dialled.
   - **Route Pattern**: Enter the Route Pattern.
   - **Call Type**: Enter **unkn**.

Configuring stations

1. On the SAT interface, enter the following command:
   `add station n`
   Where ***n*** is an extension number.
2. On page 1, specify values for the following fields and use the default values for the remaining fields:
   - **Type**: Enter **96XX SIP** corresponding to the specific device.

- **Port**: Leave this field blank.
  The system assigns a virtual port.
- **Name**: Enter a display name for the user.
- **Security Code**: Enter the number with which user logs into station.

Note:

Ensure that the number that you enter in the **Security Code** field matches the Shared Communication Profile Password field you had defined while adding the user in the System Manager.

3. If the connectivity between Communication Manager and Modular Messaging is SIP, then you need to have the following settings while configuring the STATION form 2:
   - **LWC Reception**: spe
   - **MWI Served User Type**: sip-adjunct

Verifying off-PBX -Telephone station mapping

1. On the SAT interface, enter the following command:
   `change off-pbx-telephone station-mapping xxx`
   Where ***xxx*** is an extension assigned to a 96XX SIP series telephone you have added.
2. Specify the following fields:
   - **Application**: Enter **OPS**.
   - **Trunk Selection**: Enter **aar**.
   - **Mapping Mode**: Enter **both**.
   - **Calls Allowed**: Enter **all**.

Saving translations

To save the changes that you have made while configuring Communication Manager, enter the following command on the SAT interface:

```
save translation
```

Configuring Session Manager

This section provides procedures to add new SIP users in Session Manager.

Before adding SIP stations on Session Manager, you must perform the following tasks:

- Defining SIP domain and locations.
- Defining SIP entities for each Session Manager and each Communication Manager.
- Defining entity links, which describe the SIP trunk parameters used by Session Manager when routing calls between SIP entities.
- Defining entity link between Session Managers.
- Defining routing policies and dial patterns, which control routing between SIP entities.
- Defining managed elements.
- Defining application and application sequences supporting SIP users.

Note:
For more information, read the respective guides of Session Manager and Communication Manager on Avaya support Web site at support.avaya.com

Adding SIP users

1. Open the Web browser of your computer.
2. On the address bar, enter: *xx.xx.xx.xx/admin*
   Where *xx.xx.xx.xx* is the IP address of your Session Manager.
3. Log in with your administrative credentials.
4. On the left navigation menu, expand **Users** and select **Manage Users**.
5. Under **Manage Users**, click **New**.
6. In the **General** area, specify the following mandatory fields:
   - **Last Name**: Enter the last name of the user.
   - **First Name**: Enter the first name of the user.
7. In the **Identity** area, specify the following fields:
   - **Login Name**: Enter extension number@domain.
   - **Authentication Type**: Select **Basic**.
   - **SMGR Login Password**: Enter password to log into System Manager.
   - **Confirm Password**: Re-enter the password.
   - **Shared Communication Profile Password**: Enter a numeric value to use to login to SIP client.

Note:
The value must match the Security Code field defined on station form while adding station in Communication Manager or the Feature Server.

- **Confirm Password**: Re-enter the numeric password.
- **Localized Display Name**: Enter display name for user.

8. In the **Communication Profile** area, click **New**.
9. On the **Name** field, enter **Primary**.
10. Select the **Default** check box.
11. In the **Communication Address** area, click **New**.
12. Specify the following fields:
    - **Type**: Select **Avaya SIP** from the list.
    - **Fully Qualified Address**: Enter the same extension number as the **Login Name**.
    - **Domain**: Same as Session Manager to support SIP endpoints.
13. Click **Add**.
14. In the **Session Manager Profile** area, specify the following fields:
    - **Primary Session Manager**: Select one of the Session Managers.
    - **Secondary Session Manager**: For users with single SIP registration, select **None**. For users with multiple SIP registrations, select the second Session Manager as backup SIP registrar.
    - **Original Application Sequence**: Select the same application sequence as defined in Session Manager to support SIP IMS users for Communication Manager Feature Server.
    - **Termination Application Sequence**: Select the same application sequence as defined in Session Manager to support SIP IMS users for Communication Manager Feature Server.
    - **Survivability Server**: Select **None**.
    - **Home Location**: Select the same location as defined to identify the logical or physical location of the SIP entity.
15. In the **Endpoint Profile** area, specify the following fields:
    - **System**: Select the Management Element defined for Communication Manager Feature Server.
    - **Use Existing Endpoints**: Select if you have already defined an endpoint while adding station in Communication Manager as OPS.
    - **Extension**: Use the same extension number as you have used in **Login Name**.
    - **Template**: Select a template for type of SIP clients.
    - **Security Code**: Enter the same numeric value as you have used in the step 7.
    - **Port**: Select **IP**.

- **Delete Station on Un-assign of Endpoint**: Select to automatically delete the station when the Endpoint Profile is unassigned from user.

16. To save the changes, click **Commit**.

Synchronizing with Communication Manager

After making the changes in the System Manager, perform an on demand synchronization.

1. On the Session Manager configuration Web page, click **Elements** > **Inventory** > **Synchronization** > **Communication System**.
2. On the **Synchronize CM Data and Configure Options** page, expand the **Synchronize CM Data/Launch Element Cut Through** table.
3. Select the **Communication Manager Feature Server** row.
4. Select the **Incremental Sync data for selected devices** check box.
5. To start the synchronization, click **Now**.
   You can verify the status of the synchronization by using the refresh button on the table header.

Configuring Avaya one-X® Communicator as a SIP endpoint on Communication Manager and Session Manager

Use the Avaya Aura® System Manager administration interface to add a user. For the procedure, see *Installing and Configuring Avaya Aura® Session Manager* and *Installing and Configuring Avaya Aura® System Platform* guides on the Avaya Support Web site, support.avaya.com.

Communication Manager supports Avaya 96XX SIP series telephones.

Note:
Do not configure any of the Avaya 96XX SIP series as a SIP client.

To assign AUDIX One-Step Recording:

1. Change the system-parameters features.
2. Click **Next** until you see the **AUDIX One-Step Recording** menu.

To translate the telephony feature buttons:

1. Change the display buttons and view buttons.

2. Click **Next** until you see the **AUDIX Recording** tab.
3. In the **Translation** field, enter a translation name for **AUDIX Recording** into the user-defined language.
4. Press **Enter**.

To assign a feature button to a telephone:

1. Enter the extension number in the **Extension** field and press **Enter**.
2. Click **Next** until you se the **Button Assignment** field.
3. Right-click on an unassigned button.
4. Click **AUDIX Recording**.
5. In the **Ext** field, enter the AUDIX hunt group extension of the user.
6. Press **Enter** to save your settings.

Configuring the EC500 feature

To configure the EC500 (extend to cellular) feature:

1. Log on to Communication Manager.
2. Run command:
   ```
   change off-pbx-telephone station-mapping <station number>
   ```
   You will see a list of OPS features.
3. Add a new row with the following information:
   Application = EC500
   Phone number = user mobile number
4. Specify the other values same as of the OPS row.
5. Click **Save**.

Configuring the license file for Avaya one-X Mobile SIP for iOS

Using the Avaya one-X Mobile SIP for iOS application is governed through use of a license file. For instructions on obtaining the license file for Avaya one-X Mobile SIP for iOS, see Obtaining the Avaya one-X Mobile SIP for iOS application on page 8.

To enable the operation of the Avaya one-X Mobile SIP for iOS client within an enterprise on the Web server, set the license configuration file provided by Avaya. The license data is a static file returned as a text document, that is, a *.plist* file, by the Webserver. The license configuration file must be accessible by a URL so that:

- Avaya one-X Mobile SIP for iOS clients can gain access to the URL. When you try to connect to the iOS client through Virtual Private Network (VPN), ensure that you can reach the Web server outside the enterprise. To reach the Web server outside the enterprise, you might require external access using a proxy infrastructure or a VPN tunnel before launching the iOS client.
- The URL does not require additional client authentication.
- Although, the Avaya one-X Mobile SIP for iOS client caches the URL to deal with a situation where the Web server might be temporarily unavailable, the Web server must be of the *Enterprise* class with a minimal downtime.
- All the Avaya one-X Mobile SIP for iOS clients attempt to access the URL before they register or re-register with the Session Manager or SES. This occurs when the client starts; or when connectivity to the SM/SES is lost, and then returns. The load on the Webserver in normal operation is determined by the total number of the Avaya one-X Mobile SIP for iOS clients being started within a given time period, as well as by the amount of *roaming,* where a client is mobile, loses, and subsequently re-gains network connectivity. This could be as little as once per day per active client, or as frequently as several times an hour, if the client is frequently moving in and out of the network coverage.

Verifying steps for configuring Session Manager and Communication Manager

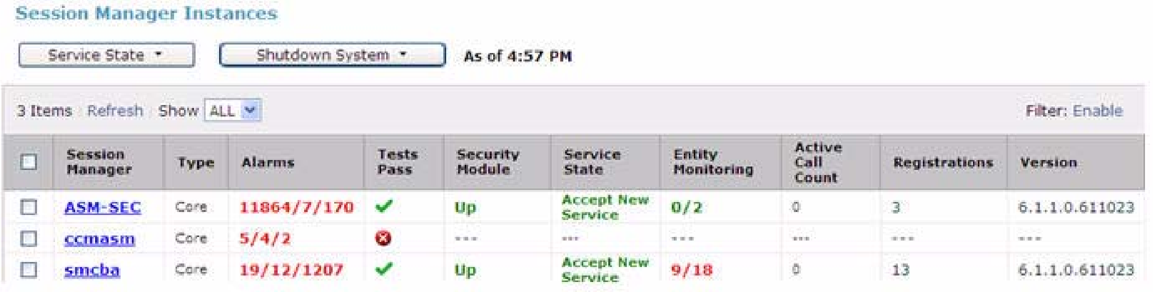
Verifying the Session Manager configuration

Verifying whether Session Manager is operational

Navigate to **Elements** > **Session Manager** > **Dashboard** to verify the overall system status for both Session Managers.

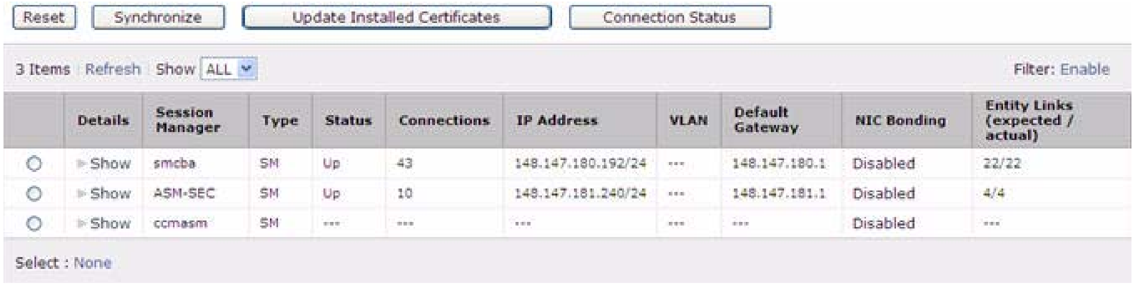
Specifically, verify the status of the following fields as shown below:

- **Tests Pass** - ✓
- **Security Module** - Up
- **Service State** - Accept New Service



□	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
□	ASM-SEC	Core	11864/7/170	✓	Up	Accept New Service	0/2	0	3	6.1.1.0.611023
□	ccmasm	Core	5/4/2	☒	---	---	---	---	---	---
□	smcba	Core	19/12/1207	✓	Up	Accept New Service	9/18	0	13	6.1.1.0.611023

Navigate to **Elements** > **Session Manager** > **System Status** > **Security Module Status** to view more detailed status information on the status of Security Module for the specific Session Manager. Verify that the **Status** column displays **Up** as shown below:



	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)
○	▸ Show	smcba	SM	Up	43	148.147.180.192/24	---	148.147.180.1	Disabled	22/22
○	▸ Show	ASM-SEC	SM	Up	10	148.147.181.240/24	---	148.147.181.1	Disabled	4/4
○	▸ Show	ccmasm	SM	---	---	---	---	---	Disabled	---

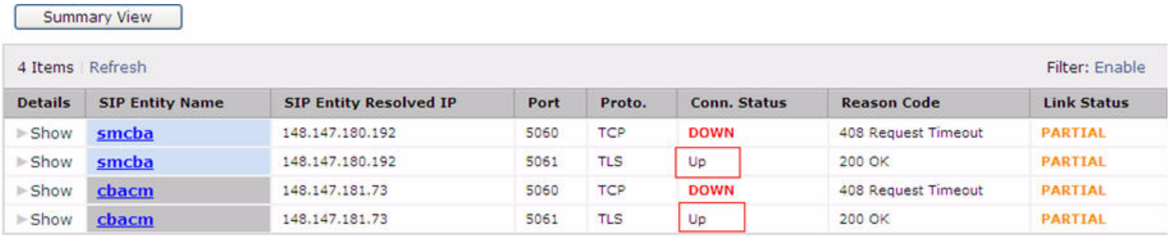
Repeat this step to verify the status of the second Session Manager.

Verifying SIP Entity Link status

Navigate to **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring** to view more detailed status information for one of the SIP Entity Links.

Select the SIP Entity for Communication Manager Evolution Server from the **All Monitored SIP Entities** table to open the **SIP Entity**, **Entity Link Connection Status** page.

In the **All Entity Links to SIP Entity: S8800-CM 6.0 ES** table, verify that the **Conn. Status** for both links is **Up**. Click **Show** in the **Details** column to view additional status information for the selected link as shown below:



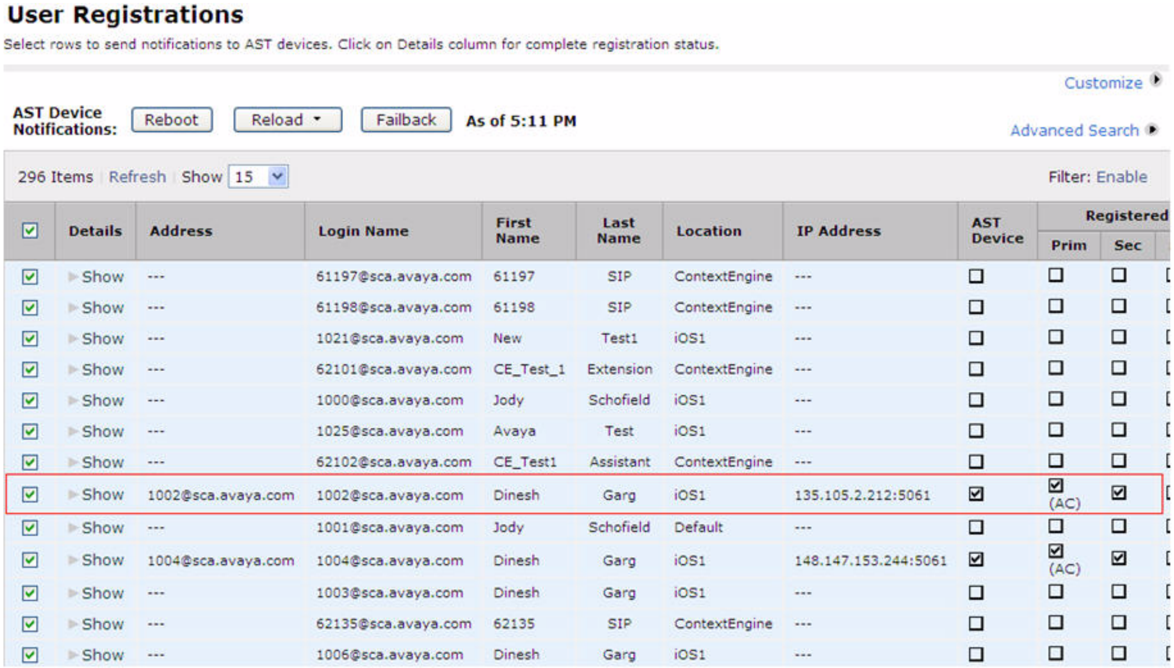
Details	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▸Show	smcba	148.147.180.192	5060	TCP	DOWN	408 Request Timeout	PARTIAL
▸Show	smcba	148.147.180.192	5061	TLS	Up	200 OK	PARTIAL
▸Show	cbacm	148.147.181.73	5060	TCP	DOWN	408 Request Timeout	PARTIAL
▸Show	cbacm	148.147.181.73	5061	TLS	Up	200 OK	PARTIAL

Repeat the steps to verify the Entity Link status for other SIP Entities.

Verifying registrations of the SIP endpoints

Navigate to **Elements** > **Session Manager** > **System Status** > **User Registrations** to verify the SIP endpoints have successfully registered with at least one Session Manager.

For example, the screen below highlights three SIP users who have successfully registered with both Session Managers.



User Registrations

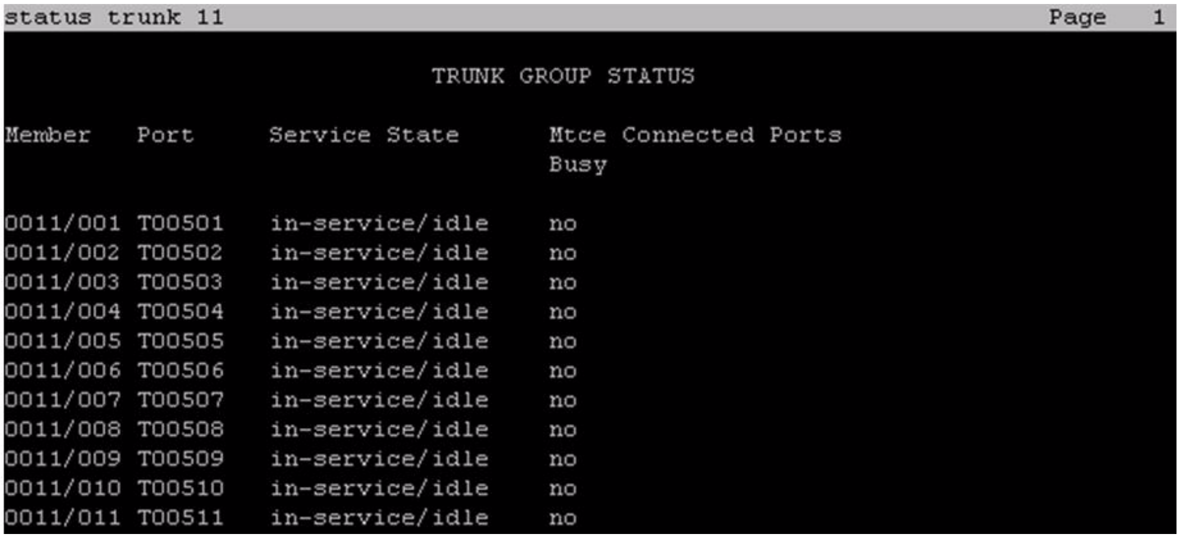
Select rows to send notifications to AST devices. Click on Details column for complete registration status.

☑	Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	Registered	
									Prim	Sec
☑	▸ Show	---	61197@sca.avaya.com	61197	SIP	ContextEngine	---	□	□	□
☑	▸ Show	---	61198@sca.avaya.com	61198	SIP	ContextEngine	---	□	□	□
☑	▸ Show	---	1021@sca.avaya.com	New	Test1	iOS1	---	□	□	□
☑	▸ Show	---	62101@sca.avaya.com	CE_Test_1	Extension	ContextEngine	---	□	□	□
☑	▸ Show	---	1000@sca.avaya.com	Jody	Schofield	iOS1	---	□	□	□
☑	▸ Show	---	1025@sca.avaya.com	Avaya	Test	iOS1	---	□	□	□
☑	▸ Show	---	62102@sca.avaya.com	CE_Test1	Assistant	ContextEngine	---	□	□	□
☑	▸ Show	1002@sca.avaya.com	1002@sca.avaya.com	Dinesh	Garg	iOS1	135.105.2.212:5061	☑	☑ (AC)	☑
☑	▸ Show	---	1001@sca.avaya.com	Jody	Schofield	Default	---	□	□	□
☑	▸ Show	1004@sca.avaya.com	1004@sca.avaya.com	Dinesh	Garg	iOS1	148.147.153.244:5061	☑	☑ (AC)	☑
☑	▸ Show	---	1003@sca.avaya.com	Dinesh	Garg	iOS1	---	□	□	□
☑	▸ Show	---	62135@sca.avaya.com	62135	SIP	ContextEngine	---	□	□	□
☑	▸ Show	---	1006@sca.avaya.com	Dinesh	Garg	iOS1	---	□	□	□

Verifying Communication Manager

Verify the status of one of SIP trunk groups on the Communication Manager Evolution Server by using the **`status trunk n`** command, where **n** is one of the trunk group numbers.

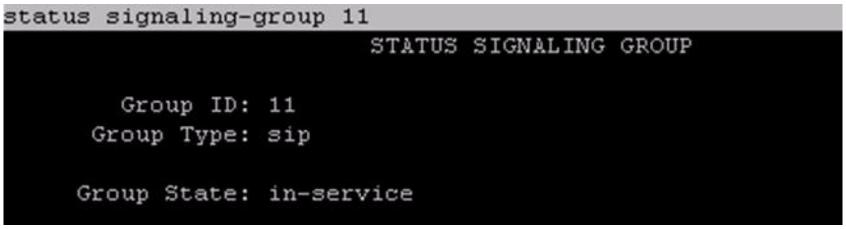
Verify that all trunks in the trunk group are in the **in-service/idle** state as shown below:



```
status trunk 11                                                  Page   1

                                TRUNK GROUP STATUS

Member    Port      Service State        Mtce Connected Ports
                                         Busy

0011/001  T00501    in-service/idle      no
0011/002  T00502    in-service/idle      no
0011/003  T00503    in-service/idle      no
0011/004  T00504    in-service/idle      no
0011/005  T00505    in-service/idle      no
0011/006  T00506    in-service/idle      no
0011/007  T00507    in-service/idle      no
0011/008  T00508    in-service/idle      no
0011/009  T00509    in-service/idle      no
0011/010  T00510    in-service/idle      no
0011/011  T00511    in-service/idle      no
```

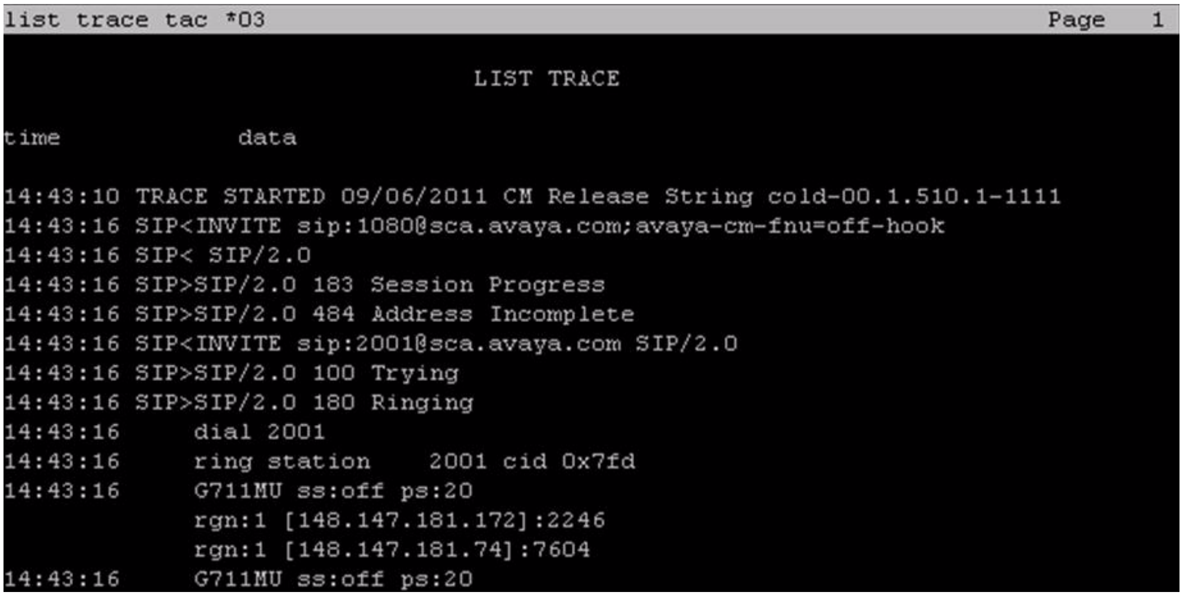
Verify the status of one of the SIP signaling groups by using the **`status signaling-group`** command, where **n** is one of the signaling group numbers.

Verify the signaling group is **in-service** as indicated in the **Group State** field shown below:



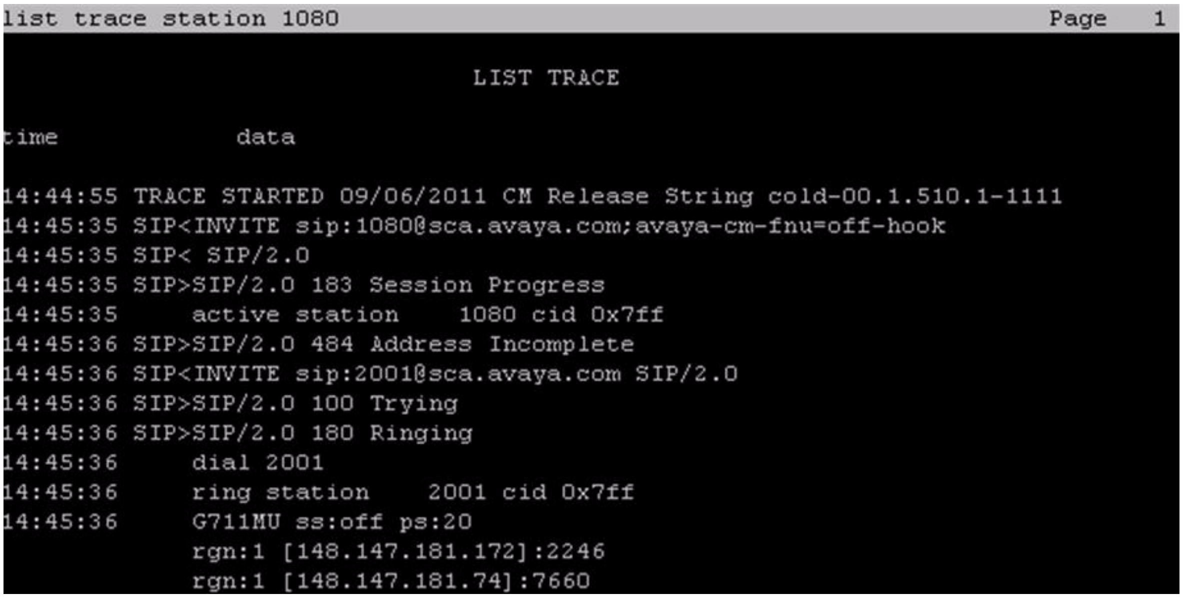
```
status signaling-group 11
                         STATUS SIGNALING GROUP

        Group ID: 11
      Group Type: sip

     Group State: in-service
```

Use the **`list trace tac #`** SAT command, where **tac #** is the trunk access code for one of the trunk groups to trace trunk group activity for the SIP trunk between Session Manager and Communication Manager. For example, the trace below illustrates a call from a SIP telephone to an IP station.



```
list trace tac *03                                                    Page   1

                                LIST TRACE

time            data

14:43:10 TRACE STARTED 09/06/2011 CM Release String cold-00.1.510.1-1111
14:43:16 SIP<INVITE sip:1080@sca.avaya.com;avaya-cm-fnu=off-hook
14:43:16 SIP< SIP/2.0
14:43:16 SIP>SIP/2.0 183 Session Progress
14:43:16 SIP>SIP/2.0 484 Address Incomplete
14:43:16 SIP<INVITE sip:2001@sca.avaya.com SIP/2.0
14:43:16 SIP>SIP/2.0 100 Trying
14:43:16 SIP>SIP/2.0 180 Ringing
14:43:16     dial 2001
14:43:16     ring station    2001 cid 0x7fd
14:43:16     G711MU ss:off ps:20
             rgn:1 [148.147.181.172]:2246
             rgn:1 [148.147.181.74]:7604
14:43:16     G711MU ss:off ps:20
```

On Communication Manager, use the **`list trace station xxx`** SAT command, where **xxx** is a valid extension number for a SIP telephone. For example, the trace below illustrates a call from a SIP telephone to an IP station.



```
list trace station 1080                                             Page   1

                                LIST TRACE

time            data

14:44:55 TRACE STARTED 09/06/2011 CM Release String cold-00.1.510.1-1111
14:45:35 SIP<INVITE sip:1080@sca.avaya.com;avaya-cm-fnu=off-hook
14:45:35 SIP< SIP/2.0
14:45:35 SIP>SIP/2.0 183 Session Progress
14:45:35     active station    1080 cid 0x7ff
14:45:36 SIP>SIP/2.0 484 Address Incomplete
14:45:36 SIP<INVITE sip:2001@sca.avaya.com SIP/2.0
14:45:36 SIP>SIP/2.0 100 Trying
14:45:36 SIP>SIP/2.0 180 Ringing
14:45:36     dial 2001
14:45:36     ring station    2001 cid 0x7ff
14:45:36     G711MU ss:off ps:20
             rgn:1 [148.147.181.172]:2246
             rgn:1 [148.147.181.74]:7660
```

Verifying call scenarios

Verification scenarios for the configuration described in these application notes includes the following call scenarios:

Basic calls:

- Place a call from Avaya one-X Mobile SIP for iOS registered to Session Manager to a station on the Communication Manager Evolution Server. Answer the call and verify the talk path.
- Place a call from Avaya one-X Mobile SIP for iOS registered to Session Manager to a station on the Communication Manager Evolution Server. Answer the call and place the call on *Hold*. Return to the held call and verify the talk path.
- Verify that the calls can be transferred from Avaya one-X Mobile SIP for iOS registered to Session Manager to an extension on the Communication Manager Evolution Server.
- Verify that the calls can be forwarded from Avaya one-X Mobile SIP for iOS registered to Session Manager to an extension on the Communication Manager Evolution Server.
- Verify that the SIP phone registered to Session Manager can create a conference with other Avaya one-X Mobile SIP for iOS and stations on the Communication Manager Evolution Server.

- Repeat the above scenarios with calls originating from stations on the Communication Manager Evolution Server to Avaya one-X Mobile SIP for iOS registered to Session Manager.

Failure scenarios:

- Change the management state of the primary Session Manager to **Deny New Service**.
- Verify that Avaya one-X Mobile SIP for iOS with multiple registrations can still make calls to stations on the Communication Manager Evolution Server. Answer the calls and verify the talk path.
- Verify that Avaya one-X Mobile SIP for iOS with multiple registrations can still make calls to stations on the Communication Manager Evolution Server. Answer the call and place the call on *Hold*. Return to the held call and verify the talk path.
- Verify that Avaya one-X Mobile SIP for iOS with multiple registrations can still transfer calls to stations on the Communication Manager Evolution Server.
- Verify that Avaya one-X Mobile SIP for iOS with multiple registrations can still forward calls to stations on the Communication Manager Evolution Server.
- Verify that Avaya one-X Mobile SIP for iOS with multiple registrations can still create a conference with other stations on the Communication Manager Evolution Server.
- Repeat the above scenarios with calls originating from stations on the Communication Manager Evolution Server to Avaya one-X Mobile SIP for iOS with multiple registrations.
- Change the management state of the primary Session Manager back to **Accept New Service**. Repeat the above scenarios when the SIP trunk between the Communication Manager Feature Server and primary Session Manager is unavailable.

Feature buttons

The Avaya one-X® Communicator for Mac OS X and the Avaya one-X Mobile SIP for iOS have the following common feature buttons:

Button	Description
Automatic Call Back	This feature enables you to request the Avaya Communications Manager system to call you back if you call an extension which is busy.
Call Forwarding All Calls	This feature enables you to forward all calls to specified extension.
Call Forwarding Busy/Don't Answer	This feature enables you to forward calls to any extension when your extension is busy or if you do not answer.
Call Park and Call Unpark	This feature enables you to place the current call in call park state and you can retrieve the call from any other extension within the system. The **Call Unpark** button is available on Communication Manager 5.x, but not available on Communication Manager 6.x. To activate this feature, the Communication Manager 6.x users must dial a FAC.
Call Pickup	To allow the user to answer a call received on a call pickup group. All members of a group can answer a call that rings at any telephone in the group. If more than one telephone rings, the system selects the call that rings the longest.
Extend call	To extend the current call to an associated other number which is usually a cell phone. The associated mobile number rings and is in conference with the active call. Ensure that you take care while using Extend Call when the *other number* is the cell phone number of the same client that is in use for one-X Mobile SIP for iOS. The iOS device brings the cell phone application to the foreground and gives audio priority to the cellular device. The SIP client loses control of microphone and speaker.
EC 500 (extension to cellular)	Using this feature, you can turn on and off the extending of the office calls to the your mobile phone. When the office phone receives a call, the configured mobile telephone also rings at the same time.

Button	Description
One-Step Recording	This feature enables you to activate and deactivate the recording of active calls to AUDIX.
Whisper page	To talk privately to a party in an existing call. The specific party receives your call without disrupting the existing conversation; other parties to that call cannot hear the Whisper Page tone or your conversation. The Whisper page feature is present in dial pad and calls screen. You can tap the whisper page, give the extension and then Communication Manager establishes the call. No dialing rules are applied.

Note:

> The changes that you make on the Communication Manager will be effective after the synchronization of the Session Manager with the Communication Manager.

The feature buttons specific to Avaya one-X® Communicator for Mac OS X are as follows:

Button	Description
Calling Party Number Blocking	This feature enables you to block the sending of the calling party number for a call.
Calling Party Number Unblocking	This feature enables you to deactivate the Calling Party Number Blocking feature.
Call Pickup Extended	This feature allows you to pickup calls from another Call Pickup Group, but within the same *extended* group. The **Call Pickup Extended** button is available on Communication Manager 5.x, but not available on Communication Manager 6.x. To activate this feature, the Communication Manager 6.x users must dial a FAC.
Malicious Call Trace (MCT)	This feature enables you to send a message to the MCT extensions that you want to trace a malicious call. MCT activation also starts recording the call if your system has an MCT voice recorder.

Button	Description
Send All Calls	This feature enables you to direct all your incoming calls to another number.
Transfer to Voicemail	This feature enables you to transfer the calls to AUDIX mail, where the caller can leave a message.

Port usage

Avaya one-X Communicator for MAC OS X and Avaya one-X Mobile SIP for iOS in release 1.0 provide primarily telephony and directory support and do not support the unified communications functions, such as visual voice mail and presence, that Avaya one-X Communicator for Windows supports. Hence, they use a subset of the ports used by Avaya one-X Communicator for Windows.

Note:

For details refer to ***Avaya one-X Communicator R6 Port Utilization Matrix*** guide.

The Avaya one-X Communicator for Mac OS X and Avaya one-X Mobile SIP for iOS use the following ports for communication:

Port number	Protocol	Purpose
80	Http	To retrieve user profile information from the personal profile manager (PPM) on the SIP Enablement Services or Session Manager.
443	Https	To retrieve the profile information of the user from the Personal Profile Manager (PPM) on the SIP Enablement Services or Session Manager. Used to communicate to the Session Manager to obtain features and configuration settings as part of Avaya Advanced SIP Telephony (AST).
1024~64511	TCP	To send messages to SIP Enablement Services or Session Manager.
5060	UDP	To send messages to SIP Enablement Services or Session Manager.
5000~5040	RTP	To transmit audio.

Port number	Protocol	Purpose
389		To communicate with the Lightweight Directory Access Protocol (LDAP) server. **Note:** Customers whose directory services are provided using Active Directory may need to use the *Global Catalog* port, see port number 3268 on page 43, instead to produce proper LDAP responses.
5060 (TCP) or 5061 (TLS)	SIP	SIP clients typically uses TCP on port numbers 5060 and/or TLS on 5061 to connect to SIP servers and other SIP end points. Port 5060 is commonly used for non-encrypted signaling traffic, whereas port 5061 is typically used for traffic encrypted with Transport Layer Security (TLS). **Note:** Avaya one-X Mobile SIP for iOS does not support SIP signalling over UDP. Avaya one-X Mobile SIP for iOS supports SIP signaling over TCP and TLS: ● Only TCP is supported for the Communication Manager 5.2 and SIP Enablement Services 5.2. ● TLS is not supported with the SIP Enablement Services 5.2. ● TCP and TLS are supported for Avaya Aura 6.0 and 6.1.

Port number	Protocol	Purpose
5004-5045	UDP	The other ports used are for the media path (audio - used for RTP/RTCP media streams).
3268		The use of LDAP to access a corporate directory is optional. Typically port 3268 is used, but an IT department may choose to use a different port for their LDAP server. Avaya one-X Communicator for MAC OS has preferences settings for directory access, where the port number can be specified. Avaya one-X Mobile SIP for iOS uses the built-in contacts system and setting on the device. Both LDAP directory lookup and contacts synchronized from external address books such as Microsoft Exchange and Google are supported.

Note:

Ports for H.323, one-X Portal API, Presence and IM, User Preferences, settings discovery, and video (used by one-X C Windows) are not used by Avaya one-X Communicator for MAC or the iOS client.

Locating the log files

Locating log files for Avaya one-X® Communicator for Mac OS X

The Avaya one-X® Communicator for Mac OS X stores the log files in the following location:

`Users/<User Name>/Library/Preferences/Avaya/SIP Communicator/Logs`

Locating log files for Avaya one-X Mobile SIP for iOS

Log files and other troubleshooting data are not accessible to the end users of iOS applications.

Avaya Support has a set of procedures to collect troubleshooting data from the Avaya one-X Mobile SIP for iOS application.

If you need to collect logs or other troubleshooting information, visit the Avaya support Web site, support.avaya.com.

Troubleshooting information

Troubleshooting for Avaya one-X® Communicator for Mac OS X

The following table provides a basic troubleshooting checklist for Avaya one-X® Communicator for Mac OS X:

Issues	**Check**
Unable to login?	The call server IP extension number and password
Unable to access voice mail?	Voice mail password
Poor voice quality?	QoS value Echo cancellation Gain control Noise cancellation
Unable to dial?	Dialing rules
Unable to access the corporate directory?	Corporate directory configuration
Unable to dial external numbers?	Check that dialing rules are properly configured. By default, Communicator prefixes a *1* to the dialed number as the long-distance code.

Troubleshooting for Avaya one-X Mobile SIP for iOS

The following table provides a basic troubleshooting checklist for Avaya one-X Mobile SIP for iOS:

Issues	**Check**
Unable to login?	Add the domain name
Unable to access the corporate directory?	Accounts configuration

Issues	Check
It takes too long to launch applications in the iOS device and to go from one window to another	● Restart your iOS device regularly. To restart the iOS device: – Hold the power button and the home button for about ten seconds. – Turn off your iOS device. – Hold the power button for about two seconds to restart your iOS device. **Note:** Do this every week for maintenance. ● Ensure that you empty safari cache by performing the following steps: – Go to Safari, then to **Settings**. – Click **Clear Cache**.
Please check the configuration URL. Cannot connect to call server.	Provide a valid URL. An invalid configuration URL can be due to the following reasons: 1. The license server IP specified is incorrect. 2. http or https is not specified as a communication protocol. 3. The configuration file in the URL does not contain **plist** as the extension.
Error in the service configuration. Cannot connect to call server.	Please contact your Web server administrator, so that the original license file is placed on the server.
Service Configuration has expired. Cannot connect to call server.	Your license for the Avaya one-X SIP client has expired. You must renew your license.
Configuration not enabled at server. Cannot connect to call server.	Please check the license file name provided in the configuration URL. The license file that you are currently trying to verify is not meant for Avaya One-X SIP client.

Appendix A: Wi-Fi best practices for Avaya one-X Mobile SIP for iOS

When you are using an iOS device as a VoIP client on a Wi-Fi network there are a number of factors that need to be considered to ensure optimum performance, security, and reliability. You must also be aware of the limitations that are based on the iOS device Wi-Fi implementation by Apple. The following section will discuss the parameters of the Wi-Fi network and supporting infrastructure that can be setup to optimize performance and security as well as any limitations with the iOS device when used as a VoIP client.

- When using a home Wi-Fi router obtain and load the latest firmware for the device in accordance with the instructions of the manufacturer.
- When using an enterprise class Wi-Fi security switch, ensure that the latest software release is used.
- Remove the Wi-Fi settings from your network for any devices that connect to your Wi-Fi router. When you remove the Wi-Fi settings, you prevent the devices from attempting to connect to your network with the old configuration. Once you apply the new settings, you can reconnect the devices to your network.
- iOS devices (iOS 4.x) currently do not support Wi-Fi Multimedia (WMM) based on IEEE 802.11e Quality of Service (QoS) extensions. Therefore, create a unique profile also known as the Wi-Fi network name or the Service Set Identifier (SSID) to be dedicated for the iOS devices on the network. Do not allow other types of devices, such as, PCs to share this SSID. Do not configure QoS as it will not be used. The SSID must have a unique name that is not used by any existing Wi-Fi network in the reception area of the device.
- For applications where a Wi-Fi security switch/router is used, consider establishing a VLAN for use by traffic carried on your new SSID. Configure the new VLAN with dedicated bandwidth control to Session Manager.
- For applications where a Wi-Fi security switch/router is used, configure the switch/router so that all the inbound traffic going to the new SSID is given higher traffic priority. This feature may not exist on some Wi-Fi switch/routers.
- Disable hidden networks. Hidden networks do not broadcast their SSID, and devices find it difficult to detect the hidden network resulting in increased connection time and reduced reliability of auto-connection.
- Disable MAC address authentication or filtering if you are not planning to restrict the devices that are allowed on this SSID. When enabled, you can configure a list of MAC addresses for the Wi-Fi router using the MAC address authentication or filtering feature and restrict access to only devices with addresses that are in the list. Devices with MAC addresses not in the list fail to associate with the Wi-Fi network.

- Set security to WPA2 personal, often referred to as AES. AES is currently the strongest form of security that Wi-Fi products offer, and ensure you have AES security for all purposes. While you enable WPA2, select a strong password based on the guidelines provided by your enterprise. If you have older Wi-Fi devices on your network that do not support WPA2 personal, then you can opt for the WPA/WPA2 mode, often referred to as the WPA mixed mode. In the WPA mixed mode, the new devices use the stronger WPA2 AES encryption, while the older devices connect to the old WPA TKIP-level encryption. If your Wi-Fi router does not support WPA/WPA2 mode, then you can choose the WPA Personal (TKIP) mode.
- Connecting from client to Session Manager or SES through a Network Address Translation (NAT), causes connection problems with the SIP signaling. The client will connect, but it will not operate correctly. Avoid connecting to Session Manager or SES through a NAT. The exception to this case is if Virtual Private Network (VPN) is used. A VPN connection will traverse though a NAT correctly, and client will operate correctly.
- When a mobile device moves around, it may associate with Access Points (APs) that are part of a different subnet or part of a different SSID. In this case the iOS device will behave differently depending on whether you are in a call or not. The following table describes what happens and the corresponding action you should take. As many of these combinations of subnets and SSIDs requires manual intervention, it is recommended that a single SSID for iOS devices is used throughout the enterprise and where possible a single subnet for a geographic location is used. In a typical scenario where you will be using the iOS device off the home network through a VPN and then come in to your enterprise work location, you may have to manually select the correct SSID as the iOS device does not always go to the last SSID that was used at a location.

Table 1: Impact of changing SSID and subnet conditions.

Condition	SSID	Subnet	Call Maintenance	Will client register automatically	Does client have to be manually registered	Do you have to restart the client	Do you have to manually select the SSID	Do you have to renew the DHCP
1	Same	Same	Yes	--	--	No	No	No
2	Diff	Same	No	Yes	--	No	Yes**	No
3	Same	Diff	No	No	N/A	Yes	No	Yes
4	Diff	Diff	No	Yes	--	No	Yes**	No
5#	Same Separate WLAN	Same Separate WLAN	No	Yes	--	No	No	No

Note:
For condition 5, the APs are not part of the same Security Switched network.

- Design the Wi-Fi AP distribution based on best practices for designing VoIP Wi-Fi networks rather than for straight data. Areas of weak signal cause voice quality issues and may cause calls to drop. A signal strength and bandwidth that still supports degraded data transmission can cause VoIP calls to drop or be of poor quality.
- Design the density and placement of the Wi-Fi AP to consider the iPhone Wi-Fi density. Plan for six to eight active calls per AP. Adjust AP density accordingly in the denser areas, employing load-balancing between APs where appropriate. The iPhone Wi-Fi capability is not as good as a laptop or of a dedicated Wi-Fi phone. A Wi-Fi network that works for dedicated Wi-Fi handsets does not imply that the Wi-Fi network is acceptable for VoIP iPhones or other smart phones.
- Disable 40 MHz settings for the 2.4 GHz band that is the GN band on your APs to prevent interference as per the recommendation of Apple. Note that this may not be possible on a home Wi-Fi router.
- Disable the 802.11b band to increase VoIP capacity per AP.
- Disable the lower speeds, such as, 1, 2, and 5.5 Mb/s. Change the 6Mb/s to mandatory, the beacon rate to 6Mb/s, and set multicast to automatic. Set all other rates to supported. Note that this may not be possible on a home Wi-Fi router.
- When moving from one AP zone to the another while on an active call, the iOS device will tend to stay associated with the original AP for long. This results in signal strength decreasing to a point where voice quality will be severely degraded. This effect is due to the inherit design of the iOS Wi-Fi implementation (up to iOS 4.3.3) and is not due to the design of the VoIP client. This is also independent of the density of APs. Hence, it is not recommended to use iOS device in an active call while moving between APs.

Appendix B: Security recommendations for administrators

- Use role assignments and assign security groups to appropriately restrict access to operations.
- Instruct users not to share their login ID and password. For accountability, each user must have a unique login ID.
- Periodically review and update the list of administered users, roles, and permissions of the administered users.
- Review administration logs on a regular basis to ensure that the system is operating properly.
- Review audit logs on a regular basis to ensure that the system is operating properly.
- Review security logs and alarms on a regular basis to monitor possible security events.

Index