Avaya Solution & Interoperability Test Lab

Configuring Avaya 9600 Series IP Deskphones running Avaya one-X® SIP firmware with Avaya Aura® Session Manager Release 6.2 and Avaya Aura® Communication Manager Evolution Server Release 6.2 – Issue 1.0

Abstract

These Application Notes describe a sample configuration of Avaya 9600 Series IP Deskphones running Avaya one-X® SIP firmware with Avaya Aura® Session Manager Release 6.2 and Avaya Aura® Communication Manager Evolution Server Release 6.2.

- Avaya Aura® Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura® Communication Manager serves as an Evolution Server within the Avaya Aura® architecture and supports SIP endpoints registered to Avaya Aura® Session Manager.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested on this solution.

Table of Contents:

1. Introduction

These Application Notes describe a sample configuration for a network that uses two Avaya Aura® Session Managers to support registration of Avaya 9600 Series SIP endpoints. Two Session Managers are deployed so that one Session Manager can serve as backup for the other in case of a network or Session Manager failure.

As shown in **Figure 1,** Avaya 9600 Series IP Deskphones running Avaya one-X® SIP firmware utilize the Avaya Aura® Session Manager User Registration feature and are supported by Avaya Aura® Communication Manager. To improve the reliability of the configuration, SIP endpoints are registered to both Session Managers.

For the sample configuration, SIP endpoints are not IP Multimedia Subsystem (IMS) users and Communication Manager is configured as an Evolution Server in the Avaya Aura® architecture. When Communication Manager is configured as an Evolution Server, it applies both origination-side and termination-side features in a single step. For more information regarding configuring Communication Manager as an Evolution Server, see **Reference [8]** in **Section 9**.

Avaya Aura® Communication Manager is connected to both Session Managers via non-IMS SIP signaling groups and associated SIP trunk groups.

Avaya Aura® Communication Manager also supports non-SIP endpoints such as Avaya 9600 Series IP Deskphones (running Avaya one-X® H.323 firmware) and 2420 Digital Telephones.

Avaya Aura® Session Manager is managed by Avaya Aura® System Manager. For the sample configuration, two Avaya Aura® Session Managers running on separate Avaya S8800 Servers are deployed as a pair of active-active redundant servers. Avaya Aura® Communication Manager Evolution Server runs on a pair of duplicated Avaya S8800 servers with an Avaya G650 Media Gateway.

These Application Notes focus on the configuration of the SIP endpoints, SIP trunks and call routing. Detailed administration of other aspects of Communication Manager or Session Manager will not be described. See the appropriate documentation listed in **Section 9** for more information.

Note: IP addresses have been partially hidden in **Figure 1** for security.

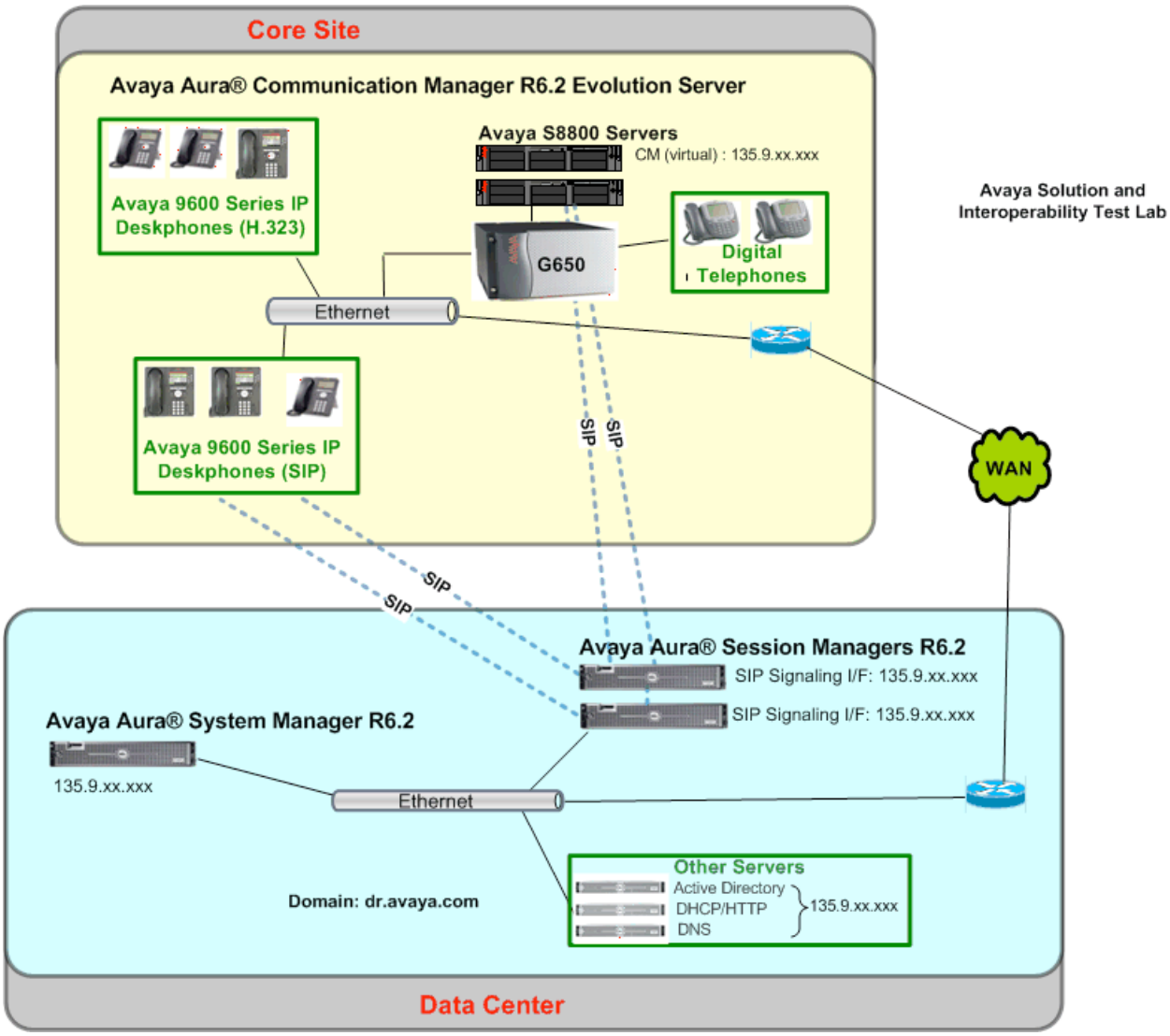


Figure 1 – Sample Configuration with redundant Avaya Aura® Session Managers

2. Equipment and Software Validated

The following components and software versions were used for the sample configuration.

Component	Software Version
Avaya Aura® Session Manager on Avaya S8800 Server	Release 6.2 Build 6.2.0.0.620118
Avaya Aura® System Manager	Release 6.2 Version: 6.2.0.0.15669-6.2.12.16
Avaya Aura® Communication Manager Evolution Server • Duplicated Avaya S8800 Servers • Avaya G650 Media Gateway	Release 6.2 Version R16x.02.0.823.0-19402
Avaya 9600 Series IP Deskphones (with Avaya one-X® SIP firmware)	Release 2.6.6
Avaya 9600 Series IP Deskphones (with Avaya one-X® H.323 firmware)	Release 3.1, SP3
Avaya 96x1 Series IP Deskphone (with Avaya one-X® SIP firmware)	Release 6.2, build 35
Avaya 96x1 Series IP Deskphone (with Avaya one-X® H.323 firmware)	Release 6.1, version: 031811 (r33)
Avaya Digital Telephones (2420D)	N/A

3. Configure Avaya Aura® Communication Manager

This section describes the steps needed to configure SIP trunks between Communication Manager Evolution Server and both Session Managers to support calls between SIP endpoints and other types of stations on Communication Manager. These instructions assume the Avaya G650 Media Server is already configured on Communication Manager Evolution Server. For information on how to administer these other aspects of Communication Manager, see **References [6]** through **[10]** in **Section 9.**

This section describes the administration of Communication Manager using a System Access Terminal (SAT). Some administration screens have been abbreviated for clarity.

The following administration steps will be described:

- Verify System Capacities and Licensing
- Configure Trunk-to-Trunk Transfers
- Configure IP Codec Set
- Configure IP Network Region
- Configure IP Node Names and IP Addresses
- Configure SIP Signaling Groups and Trunk Groups
- Configure Route Pattern
- Administer Private Numbering Plan and Uniform Dialplan
- Administer AAR Analysis
- Configure Stations
- Verify Off-PBX-Telephone Station Mapping

After completing these steps, the **save translation** command should be performed.

3.1. Verify System Capacities and Licensing

This section describes the procedures to verify the correct system capacities and licensing have been configured. If there is insufficient capacity or a required features is not available, contact an authorized Avaya sales representative to make the appropriate changes.

3.1.1. Verify Off-PBX Telephones Capacity

On **Page 1** of the **display system-parameters customer-options** command, verify an adequate number of Off-PBX Stations (OPS) Telephones are administered for the system as shown below.

```
display system-parameters customer-options                  Page   1 of  11
                                OPTIONAL FEATURES
G3 Version: V16                            Software Package: Enterprise
       Location: 2                               System ID (SID): 1
                                                                  USED
…
                     Maximum Off-PBX Telephones - EC500: 41000 0
                     Maximum Off-PBX Telephones -   OPS: 41000 32
                     Maximum Off-PBX Telephones - PBFMC: 41000 0
…
```

3.1.2. Verify SIP Trunk Capacity

On **Page 2** of the **display system-parameters customer-options** command, verify an adequate number of SIP Trunk Members are administered for the system as shown below.

```
display system-parameters customer-options                  Page   2 of  11
                                OPTIONAL FEATURES
IP PORT CAPACITIES                                            USED
                      Maximum Administered H.323 Trunks: 12000  0
           Maximum Concurrently Registered IP Stations: 18000  0
  Max Concur Registered Unauthenticated H.323 Stations: 414    0
…
                    Maximum Video Capable IP Softphones: 0      0
                        Maximum Administered SIP Trunks: 24000  90
…
```

3.1.3. Verify AAR Access Code is Configured

To enable Communication Manager to route calls to SIP endpoints, verify an Automatic Alternative Routing (AAR) access code has been defined for the system.

On **Page 1** of **change feature-access-codes** command, verify a value has been defined in the **Auto Alternate Routing (AAR) Access Code** field. In the sample configuration, "**8**" was used.

```
change feature-access-codes                                 Page   1 of  10
                            FEATURE ACCESS CODE (FAC)

…                            Attendant Access Code:
          Auto Alternate Routing (AAR) Access Code: 8
        Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                      Automatic Callback Activation: *08   Deactivation: *09

…
```

3.1.4. Verify AAR/ARS Routing is Enabled

To simplify the dialing plan for calls between SIP endpoints and other types of stations, verify the following AAR/ARS features are enabled on the system.

On **Page 3** of **system-parameters customer-options** command, verify the following features are enabled.

- **ARS?** Verify "**y**" is displayed.
- **ARS/AAR Partitioning?** Verify "**y**" is displayed.
- **ARS/AAR Dialing without FAC?** Verify "**y**" is displayed.

```
display system-parameters customer-options                    Page   3 of  11
                                OPTIONAL FEATURES

A/D Grp/Sys List Dialing Start at 01? n                          CAS Main? n
Answer Supervision by Call Classifier? n                 Change COR by FAC? n
                                   ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? n
…
```

3.1.5. Verify Private Networking is Enabled

On **Page 5** of **display system-parameters customer-options** command, verify the **Private Networking** feature is set to "**y**".

```
display system-parameters customer-options                    Page   5 of  11
                                OPTIONAL FEATURES
                  Port Network Support? y              Time of Day Routing? n
                       Posted Messages? n      TN2501 VAL Maximum Capacity? y
                                                  Uniform Dialing Plan? y
                     Private Networking? y    Usage Allocation Enhancements? y
               Processor and System MSP? y
                     Processor Ethernet? y               Wideband Switching? n
…
```

3.2. Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable trunk-to-trunk transfers. This feature is needed when an incoming call to a SIP station is transferred to another SIP station. For simplicity, the **Trunk-to-Trunk Transfer** field on **Page 1** was set to "**all**" to enable all trunk-to-trunk transfers on a system wide basis.

Note: Enabling this feature poses significant security risk by increasing the risk of toll fraud, and must be used with caution. To minimize the risk, a COS could be defined to allow trunk-to-trunk transfers for specific trunk group(s). For more information regarding how to configure Communication Manager to minimize toll fraud, see **Reference [10]** in **Section 9.**

```
change system-parameters features                                    Page   1 of  18
                            FEATURE-RELATED SYSTEM PARAMETERS

                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
…
```

3.3. Configure IP Codec Set

Use the **change ip-codec-set n** command where **n** is the number used to identify the codec set.

Enter the following values:

- **Audio Codec** — Enter "**G.711MU**" and "**G.729**" as supported types.
- **Silence Suppression** — Retain the default value "**n**".
- **Frames Per Pkt** — Enter "**2**".
- **Packet Size (ms)** — Enter "**20**".
- **Media Encryption** — Enter the value based on the system requirement. For the sample configuration, "**none**" was used.

```
change ip-codec-set 1                                        Page   1 of   2
                           IP Codec Set

    Codec Set: 1

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

     Media Encryption
 1: none
```

3.4. Configure IP Network Region

Use the **change ip-network-region n** command where **n** is an available network region.

Enter the following values and use default values for remaining fields.

- **Authoritative Domain:** Enter the correct SIP domain for the configuration. For the sample configuration, "**dr.avaya.com**" was used.
- **Name:** Enter descriptive name.
- **Codec Set:** Enter the number of the IP codec set configured in **Section 3.3.**
- **Intra-region IP-IP Direct Audio:** Enter "**yes**".
- **Inter-region IP-IP Direct Audio:** Enter "**yes**".

```
change ip-network-region 1                                  Page   1 of  19
                                IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: dr.avaya.com
    Name: SIP calls for ASM
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 16585
…
```

3.5. Add Node Names and IP Addresses

Use the **change node-names ip** command to add the node-name and IP Addresses for the "**procr**" interface on Communication Manager and the SIP signaling interface of each Session Manager, if not previously added.

In the sample configuration, the node-name of the SIP signaling interface for the first Session Manager is "**silasm7**" with an IP address of "**135.9.xx.xxx**". The node-name of SIP signaling interface for the second Session Manager is "**silasm8**" with an IP address of "**135.9.xx.xxx**".

Note: IP addresses have been partially hidden for security.

```
change node-names ip                                        Page   1 of   2
                                   IP NODE NAMES
    Name               IP Address
silasm7             135.9.xx.xxx
silasm8             135.9.xx.xxx
default             0.0.0.0
procr               135.9.xx.xxx
```

3.6. Configure SIP Signaling Groups and Trunk Groups

3.6.1. Add Signaling Groups for SIP Trunks

Use the **add signaling-group n** command, where **n** is an available signaling group number to create SIP signaling groups. In the sample configuration, trunk groups "**10**" and "**11**" and signaling groups "**10**" and "**11**" were used for connecting to both Session Managers.

On **Page 1**, enter the following values and use default values for remaining fields.

- **Group Type:** Enter "**sip**".
- **IMS Enabled?** Enter "**n**".
- **Transport Method:** Enter "**tls**".
- **Peer Detection Enabled?** Enter "**y**".
- **Peer Server:** Use default value.
  Note: default value is replaced with "**SM**" after SIP trunk to Session Manager is established.
- **Near-end Node Name:** Enter "**procr**" node name from **Section 3.5**.
- **Far-end Node Name:** Enter node name for the first Session Manager defined in **Section 3.5**.
- **Near-end Listen Port:** Verify "**5061**" is used.
- **Far-end Listen Port:** Verify "**5061**" is used.
- **Far-end Network Region**: Enter network region defined in **Section 3.4**.
- **Far-end Domain:** Enter domain name for **Authoritative Domain** field defined in **Section 3.4**.
- **DTMF over IP:** Verify "**rtp-payload**" is used.
- **Direct IP-IP Early Media?** Enter "**y**".

```
add signaling-group 10                                    Page   1 of   2
                                SIGNALING GROUP

Group Number: 10              Group Type:  sip
  IMS Enabled? n              Transport Method: tls
        Q-SIP? n                                           SIP Enabled LSP? n
     IP Video? n
  Peer Detection Enabled? y  Peer Server: others

   Near-end Node Name: procr                  Far-end Node Name: silasm7
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1
Far-end Domain: dr.avaya.com
                                            Bypass If IP Threshold Exceeded? n
       DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? n                  Direct IP-IP Early Media? y
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

Repeat this step to define a second signaling group to connect to the second Session Manager.

3.6.2. Add SIP Trunk Groups

Add the corresponding trunk groups controlled by the signaling groups defined **Section 3.6.1** using the **add trunk-group n** command where **n** is an available trunk group number.

Fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Group Type:** Enter "**sip**".
- **Group Name:** Enter a descriptive name.
- **TAC:** Enter an available trunk access code.
- **Direction:** Enter "**two-way**".
- **Outgoing Display?** Enter "**y**".
- **Service Type:** Enter "**tie**".
- **Signaling Group:** Enter the number of the signaling group added in **Section 3.6.1**.
- **Number of Members:** Enter the number of members in the SIP trunk (must be within limits configured in **Section 3.1.2**).

Note: once the **add trunk-group** command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

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

Group Number: 10                    Group Type: sip          CDR Reports: y
  Group Name: SIP Trunk to SILASM7           COR: 1        TN: 1       TAC:
#10   Direction: two-way        Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 10
                                                     Number of Members: 20
```

On **Page 2**, set the **Preferred Minimum Session Refresh Interval:** field to "**1200**".

Note: to avoid extra SIP messages, all SIP trunks connected to Session Manager should be configured with a minimum value of "**1200**".

```
add trunk-group 10                                          Page   2 of  21
                                Group Type: sip
TRUNK PARAMETERS

     Unicode Name: auto
                                          Redirect On OPTIM Failure: 5000

            SCCAN? n                                Digital Loss Group: 18
                       Preferred Minimum Session Refresh Interval(sec): 1200
```

On **Page 3**, fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Numbering Format:** Enter "**private**".
- **Show ANSWERED BY on Display?** Enter "**y**".

```
add trunk-group 10                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                       Maintenance Tests? y

                      Numbering Format: private
                                             UUI Treatment: service-provider

                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n

 Show ANSWERED BY on Display? y
```

On **Page 4**, fill in the indicated field as shown below. Default values can be used for the remaining fields.

- **Support Request History?** Enter "**y**".

```
add trunk-group 10                                          Page   4 of  21
                                     PROTOCOL VARIATIONS

                       Mark Users as Phone? y
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                  Network Call Redirection? n
                     Send Diversion Header? n
                  Support Request History? y
              Telephone Event Payload Type: 120
```

Repeat this step to define a SIP trunk group to connect to the second Session Manager.

3.7. Configure Route Pattern

This section provides the configuration of the route pattern used in the sample configuration for routing calls between SIP endpoints and other types of stations supported by Communication Manager. To support routing when the primary Session Manager is not available, the route pattern should be configured to use look-ahead routing (LAR) to select a secondary route.

Use **change route-pattern n** command where **n** is an available route pattern.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Grp No** Enter a row for each trunk group defined in **Section 3.6.2**.
- **FRL** Enter "**0**".
- **Numbering Format** Enter "**lev0-pvt**".
- **LAR** Enter "**next**" for first row. Use default value for second row.

In the sample configuration, route pattern "**10**" was created as shown below.

```
change route-pattern 10                                      Page   1 of  3
                        Pattern Number: 1   Pattern Name: SIP trunks to ASM
                          SCCAN? n     Secure SIP? n
 Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
 No          Mrk Lmt List Del  Digits                            QSIG
                          Dgts                                   Intw
1: 10   0                                                         n   user
2: 11   0                                                         n   user
3:                                                                n   user
4:                                                                n   user
5:                                                                n   user
6:                                                                n   user

  BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
 0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
1: y y y y y n  n            rest                              lev0-pvt  next
2: y y y y y n  n            rest                              lev0-pvt  none
3: y y y y y n  n            rest                                        none
4: y y y y y n  n            rest                                        none
…
```

3.8. Administer Private Numbering Plan

Extension numbers used for SIP Users registered to Session Manager must be added to either the private or public numbering table on Communication Manager. For the sample configuration, private numbering was used and all extension numbers were unique within the private network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in **Reference [7]** in **Section 9**.

Use the **change private-numbering n** command, where **n** is the length of the private number.

Fill in the indicated fields as shown below.

- **Ext Len**: Enter length of extension numbers.
  In the sample configuration, "**5**" was used.
- **Ext Code**: Enter leading digit (s) from extension number.
  In the sample configuration, "**21xxx**" and "**31xxx**" were used.
- **Trk Grp(s):** Enter trunk groups defined in **Section 3.6.2**.
  Note: if trunk group numbers are contiguous, a single row can be used. Else, add a row for each trunk group.
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix.
- **Total Length:** Enter "**5**" since a private prefix was not defined.

```
change private-numbering 5                                      Page   1 of  2
                            NUMBERING - PRIVATE FORMAT

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 5  21             10-11                       5    Total Administered: 3
 5  31             10-11                       5       Maximum Entries: 540
…
```

3.9. Administer Uniform Dial Plan

Use the **change uniform-dialplan n** command, where **n** is the first digit of the extension numbers used for SIP stations in the system.

In the sample configuration, 5-digit extension numbers starting with "**21xxx**" and "**31xxx**" were used for extensions associated with the 9600 Series SIP Deskphones.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Matching Pattern** Enter digit pattern of extensions assigned to SIP endpoints.
- **Len** Enter extension length.
- **Net** Enter "**aar**".

```
change uniform-dialplan 2                                        Page   1 of  2
                            UNIFORM DIAL PLAN TABLE
                                                               Percent Full: 0
  Matching                    Insert              Node
  Pattern        Len Del      Digits     Net Conv Num
 21               5   0                  aar  n
 31               5   0                  aar  n
```

3.10. Administer AAR Analysis

This section provides the configuration of the AAR pattern used in the sample configuration for routing calls between SIP endpoints and other stations. In the sample configuration, extension numbers starting with digits "**21xxx**" and "**31xxx**" are assigned to SIP endpoints.

Note: Other methods of routing may be used.

Use the **change aar analysis n** command where **n** is the first digit of the extension numbers assigned to SIP endpoints in the system.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Dialed String** Enter leading digit (s) of extension numbers.
- **Min** Enter minimum number of digits that must be dialed.
- **Max** Enter maximum number of digits that may be dialed.
- **Route Pattern** Enter Route Pattern defined in **Section 3.7**.
- **Call Type** Enter "**unku**".

```
change aar analysis 2                                        Page   1 of  2
                          AAR DIGIT ANALYSIS TABLE
                                 Location:  all          Percent Full:    1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    21                    5    5     10       unku          n
    31                    5    5     10       unku          n
```

3.11. Configure Stations

For each SIP user defined in Session Manager, add a corresponding station on Communication Manager Evolution Server. The extension number defined for the SIP station will be the number the SIP user enters to register to Session Manager.

Note: Instead of manually defining each station using the Communication Manager SAT interface, an alternative option is to automatically generate the SIP station when adding a new SIP user using System Manager. See **Section 4.10** for more information on adding SIP users.

Use the **add station n** command where **n** is a valid extension number defined in the system.

On **Page 1,** enter the following values and use defaults for remaining fields.

- **Type:** Enter station type corresponding to the specific device. In sample configuration "**9630SIP**" was used.
- **Port:** Leave blank. Once the command is submitted, a virtual port will be assigned (e.g. S0000).
- **Name:** Enter a display name for user.
- **Security Code:** Enter the number used to log in station. **Note:** this number should match the "**Communication Profile Password**" field defined when adding this user in System Manager. See **Section 4.10**.

```
add station 21001                                          Page   1 of  6

                              STATION

Extension: 21001                        Lock Messages? n            BCC: 0
     Type: 9630SIP                      Security Code: 123456        TN: 1
     Port:                            Coverage Path 1: 1            COR: 1
     Name: SIP Station User           Coverage Path 2:              COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19
                                                Message Lamp Ext: 21001
…
                                                          IP Video? n
```

On **Page 4,** add the desired number of **call-appr** entries in the **BUTTON ASSIGNMENTS** section. This governs how many concurrent calls can be supported. In the sample configuration, three call appearances were configured to support transfer and conferencing scenarios.

Note: Avaya 9601 IP Deskphones display only two local call appearance buttons when idle. So the number of entries shown below is not required to match the number of appearances displayed on the telephone.

```
add station 21001                                          Page   4 of  6

                              STATION
SITE DATA
…

BUTTON ASSIGNMENTS
 1: call-appr                              5:
 2: call-appr                              6:
 3: call-appr                              7:
 4:                                        8:
```

On **Page 6,** enter the following value and use defaults for remaining fields.

- **SIP Trunk:** Enter "**aar**" to use Route Pattern defined in **Section 3.7** so calls will be routed over the secondary route in case the primary Session Manager is not available.

```
add station 21001                                          Page   6 of  6

                              STATION
SIP FEATURE OPTIONS
         Type of 3PCC Enabled: None
                     SIP Trunk: aar
```

3.12. Verify Off-PBX-Telephone Station-Mapping

Use the **change off-pbx-telephone station-mapping xxx** command where **xxx** is an extension assigned to a 9600 Series SIP Deskphone to verify an Off-PBX station mapping was automatically created for the SIP station.

On **Page 1**, verify the following fields were correctly populated.

- **Application** Verify "**OPS**" is assigned.
- **Trunk Selection** Verify "**aar**" is assigned.

```
change off-pbx-telephone station-mapping 21001                Page   1 of  3

                STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk      Config  Dual
 Extension                 Prefix                    Selection  Set     Mode
 21001           OPS           -       21001           aar         1
                               -
                               -
```

On **Page 2**, verify the following fields were correctly populated.

- **Call Limit:** Verify "**3**" is assigned corresponding to the number of **call-appr** entries assigned in **Section 3.11**.
- **Mapping Mode**: Verify "**both**" is assigned.
- **Calls Allowed:** Verify "**all**" is assigned.

```
change off-pbx-telephone station-mapping 21001                Page   2 of  3

                STATIONS WITH OFF-PBX TELEPHONE INTEGRATION


 Station       Appl    Call        Mapping    Calls      Bridged     Location
 Extension     Name    Limit       Mode       Allowed    Calls
 21001         OPS      3          both       all         none
                                   -
```

3.13. Save Translations

Configuration of Communication Manager Evolution Server is complete. Use the **save translation** command to save these changes.

Note: After making a change on Communication Manager which alters the dial plan or numbering plan, synchronization between Communication Manager and System Manager must be completed and SIP telephones must be re-registered.

See **Section 4.11** for more information on how to perform an on-demand synchronization.

4. Configure Avaya Aura® Session Manager

This section describes the procedures for configuring Avaya Aura® Session Manager to support registrations of SIP endpoints.

These instructions assume other administration activities have already been completed such as defining SIP entities for each Session Manager, defining the network connection between System Manager and each Session Manager, and defining Communication Manager as a Managed Element. For more information on these additional actions, see **References [2]** and **[5]** in **Section 9.**

The following administration activities will be described:

- Define SIP Domain and Locations
- Define SIP Entity for Communication Manager Evolution Server
- Define Entity Links, which describe the SIP trunk parameters used by Session Manager when routing calls between SIP Entities
- Define Entity Link between Session Managers
- Define Routing Policies and Dial Patterns which control routing between SIP Entities
- Define Applications and Application Sequences supporting SIP Users
- Add new SIP Users
- Synchronize changes with Communication Manager.

Note: Some administration screens have been abbreviated for clarity.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL "**http://<ip-address>/SMGR**", where "**<ip-address>**" is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

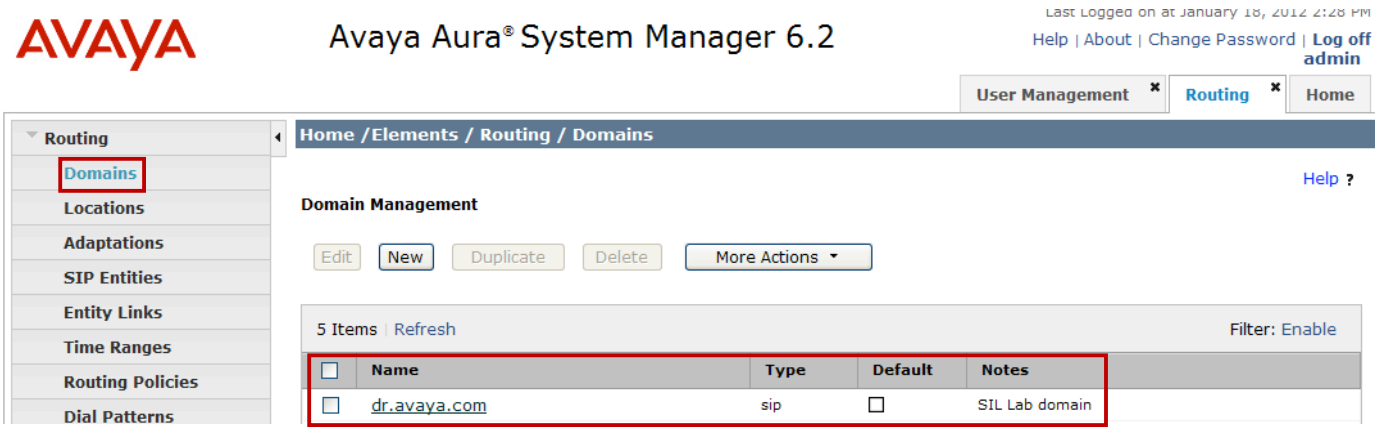
4.1. Define SIP Domains

Expand **Elements** → **Routing** and select **Domains** from the left navigation menu.

Click **New**. Enter the following values and use default values for remaining fields**.**

- **Name** Enter the Authoritative Domain Name specified in **Section 3.4**. For the sample configuration, "**dr.avaya.com**" was used.
- **Type** Select "**sip**" from drop-down menu.
- **Notes** Add a brief description. [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.



4.2. Define Locations

Locations are used to identify logical and/or physical locations where SIP Entities or SIP endpoints reside, for purposes of bandwidth management or location-based routing.

Expand **Elements** → **Routing** and select **Locations** from the left navigation menu.

Click **New** (not shown)**.** In the **General** section, enter the following values and use default values for remaining fields.

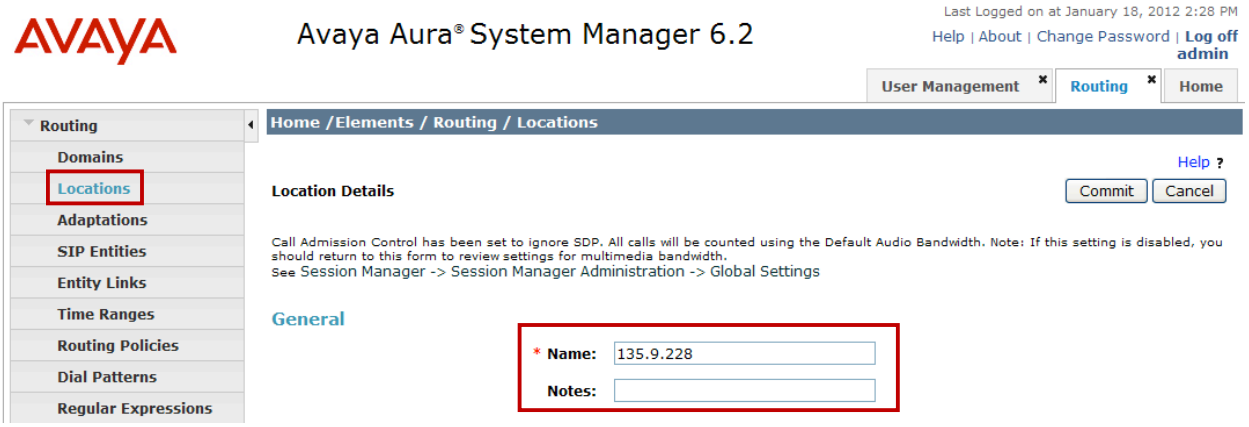
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional].

Scroll down to the **Location Pattern** section and lick **Add** and enter the following values.

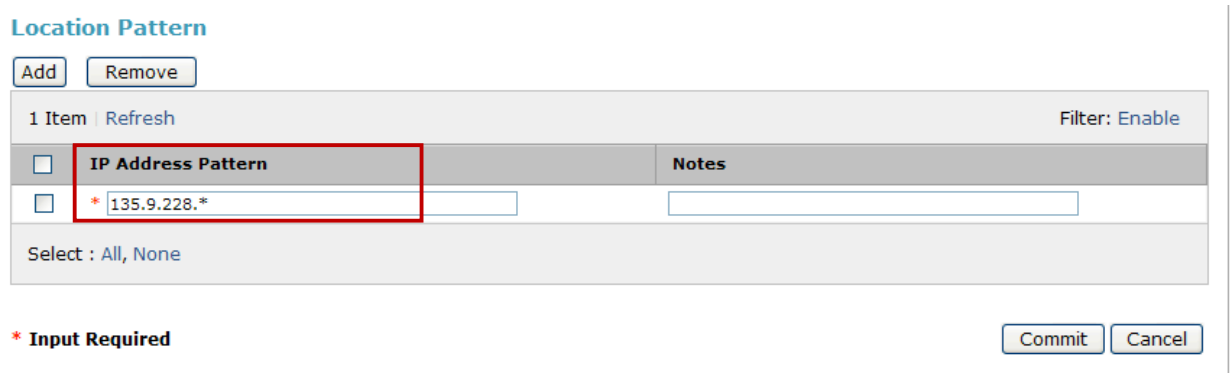
- **IP Address Pattern** Enter the logical pattern used to identify the location. For the sample configuration, "**135.9.228.***" was used.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows a Location used for SIP endpoints in the sample configuration.



Note: screen has been abbreviated for clarity.



Repeat the steps to define a second location for Communication Manager.

4.3. Define SIP Entities

A SIP Entity must be added for Communication Manager Evolution Server. To add a SIP Entity, expand **Elements → Routing** and select **SIP Entities** from the left navigation menu.

Click **New** (not shown)**.** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Name:** Enter an identifier for new SIP Entity. In the sample configuration, "**cm7**" was used.
- **FQDN or IP Address:** Enter IP address of "**procr**" interface defined in **Section 3.5**
- **Type:** Select "**CM**" for Communication Manager.
- **Location:** Select Location defined for Communication Manager in **Section 4.2**.
- **Notes:** Enter a brief description. [Optional].

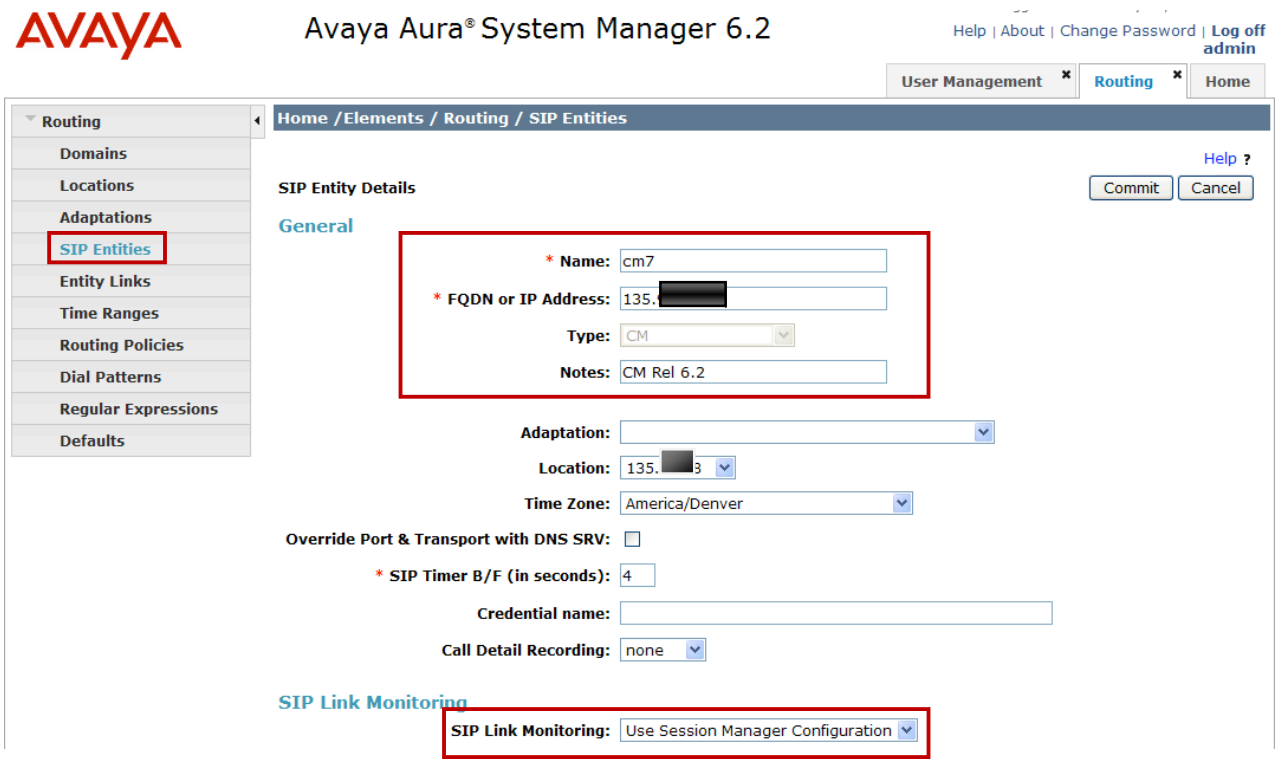
In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select "**Use Session Manager Configuration**".

Click **Commit** to save SIP Entity definition.

The following screen shows the SIP Entity defined for Communication Manager.

Note: IP addresses of the "**procr**" interface and **Location** fields have been partially hidden for security.



4.4. Define Entity Links

A SIP trunk between Session Manager and Communication Manager is described by an Entity Link. In the sample configuration, SIP Entity Links were added between Communication Manager Evolution Server and each Session Manager.

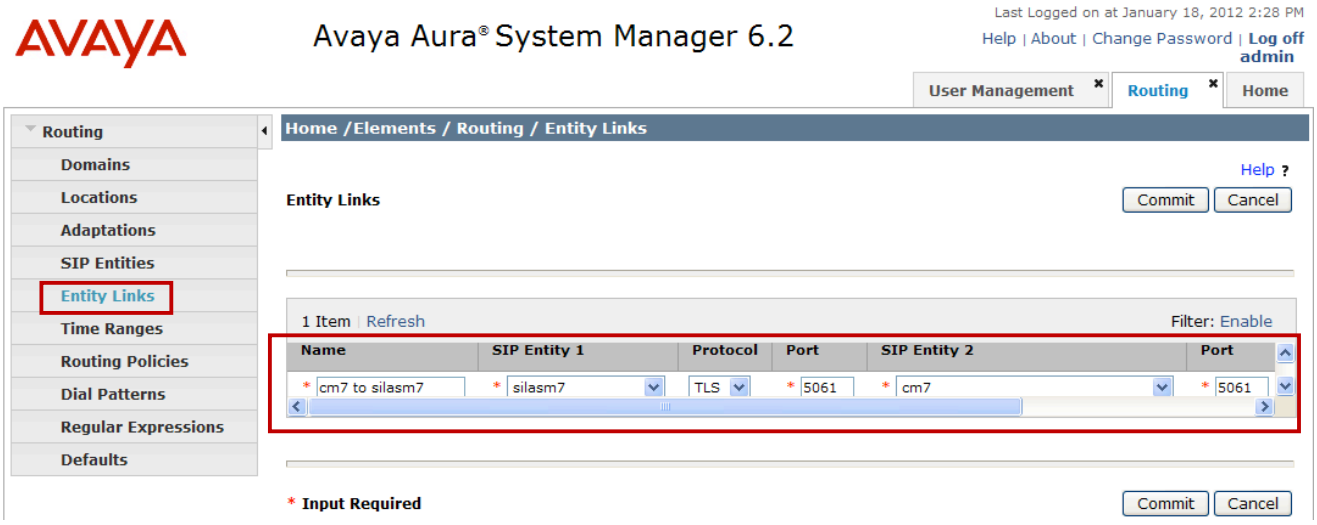
To add an Entity Link, expand **Elements → Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

- **Name** Enter an identifier for the link to Communication Manager.
- **SIP Entity 1** Select one of Session Managers previously defined.
- **SIP Entity 2** Select the SIP Entity added for Communication Manager defined in **Section 4.3** from drop-down menu.
- **Protocol** After selecting both SIP Entities, verify "**TLS**" is selected as the required Protocol.
- **Port** Verify **Port** for both SIP entities is "**5061**".
- **Trusted** Enter ☑.

Click **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined between Communication Manager Evolution Server and one of the Session Managers.



Repeat this step to define Entity Link between Communication Manager and the second Session Manager.

4.5. Define Entity Link between Avaya Aura® Session Managers

To provide redundancy and enable sessions to be alternatively routed through the second Session Manager in the case of a network failure, define an Entity Link between Session Managers.

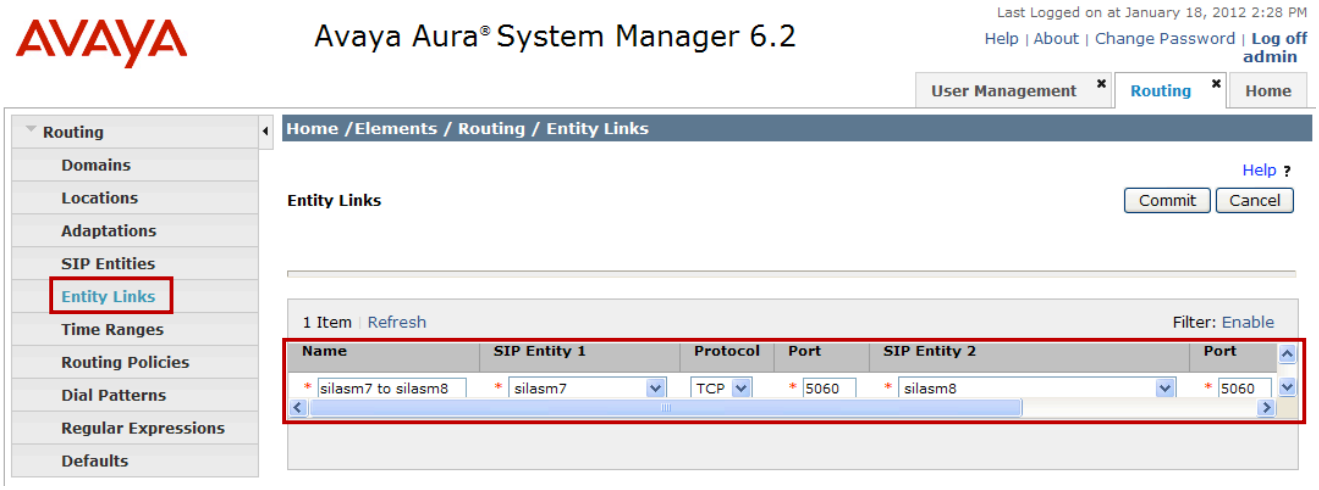
Expand **Elements** → **Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

- **Name** Enter an identifier for the link to each telephony system.
- **SIP Entity 1** Select one of Session Managers previously defined.
- **SIP Entity 2** Select second Session Manager.
- **Protocol** After selecting both SIP Entities, select "**TCP**" as the required Protocol.
- **Port** Verify **Port** for both SIP entities is "**5060**".
- **Trusted** Enter ☑.
- **Notes** Enter a brief description. [Optional].

Click **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined between Session Managers in the sample configuration.



4.6. Define Routing Policy

Routing policies describe the conditions under which calls will be routed to non-SIP stations on Communication Manager Evolution Server.

Note: Since the SIP users are registered to Session Manager, a routing policy does not need to be defined for calls to SIP endpoints supported by Communication Manager Evolution Server.

To add a routing policy, expand **Elements → Routing** and select **Routing Policies.**

Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier for Communication Manager Evolution Server.
- **Disabled:** Leave unchecked.
- **Retries:** Retain default value of "**0**".
- **Notes:** Enter a brief description. [Optional].

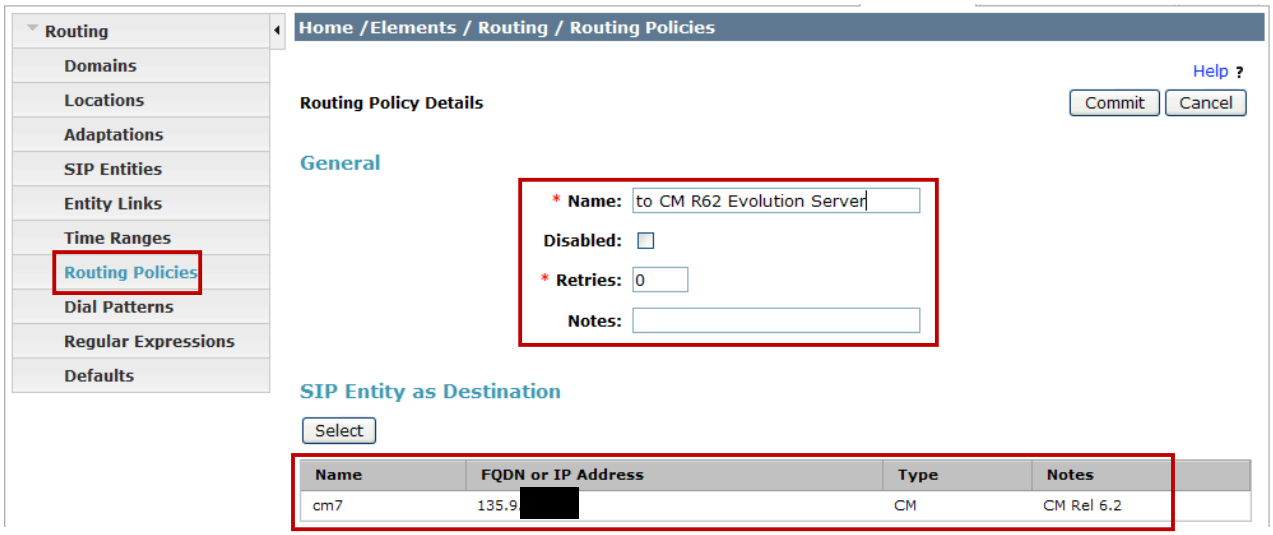
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown).

- Select the SIP Entity defined for Communication Manager Evolution Server in **Section 4.3** and click **Select.**
- The selected SIP Entity displays on the **Routing Policy Details** page.

Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

Note: the routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

The following screen shows the Routing Policy for Communication Manager Evolution Server.



4.7. Define Dial Pattern

This section describes the steps to define a dial pattern to route calls to non-SIP stations on Communication Manager. In the sample configuration, 5-digit extensions beginning with "**32xxx**" are assigned to IP (H.323) and digital stations managed by Communication Manager.

Note: Since the SIP users are registered to Session Manager, a dial pattern does not need to be defined for SIP stations supported by Communication Manager Evolution Server.

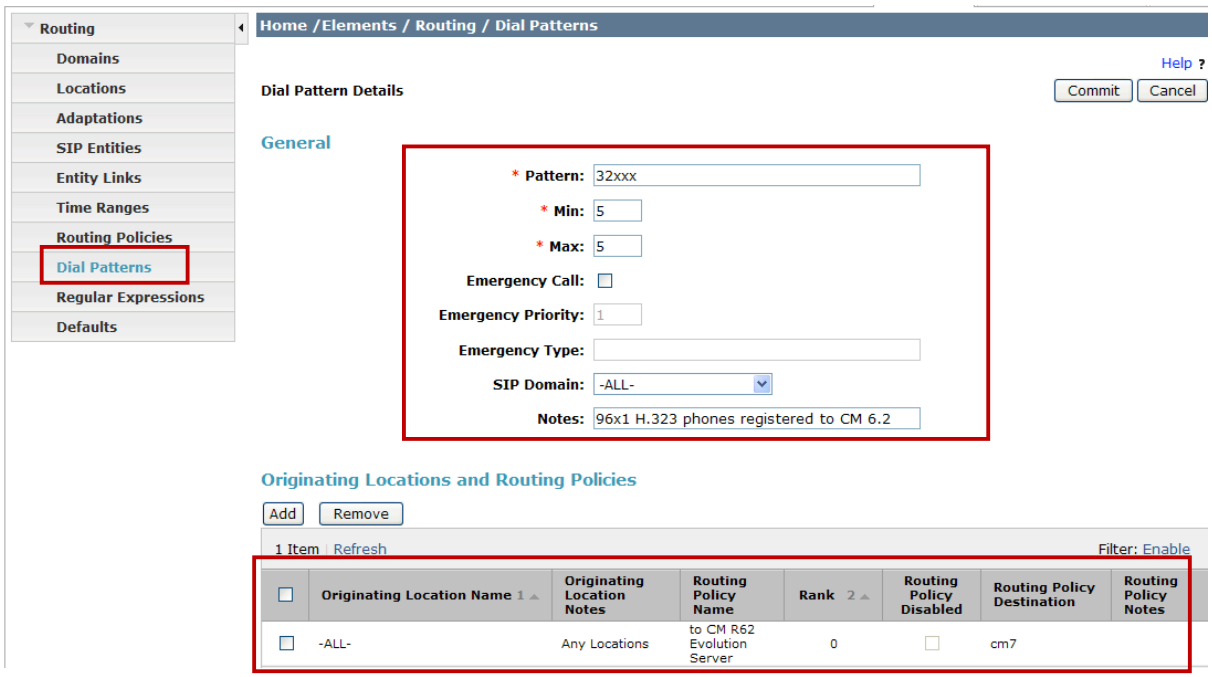
To define a dial pattern, expand **Elements → Routing** and select **Dial Patterns.** Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for extension numbers of non-SIP stations.
- **Min:** Enter the minimum number digits that must be dialed.
- **Max:** Enter the maximum number digits that may be dialed.
- **SIP Domain:** Select the SIP Domain from drop-down menu or select "**ALL**" if Session Manager should accept incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional].

In the **Originating Locations and Routing Policies** section, click **Add.**
The **Originating Locations and Routing Policy List** page opens (not shown).

- In **Originating Locations** table, select "**ALL**" .
- In **Routing Policies** table, select the appropriate Routing Policy defined for Communication Manager Evolution Server in **Section 4.6.**
- Click **Select** to save these changes and return to **Dial Patterns Details** page.

Click **Commit** to save the new definition. The following screen shows the Dial Pattern defined for routing calls to Communication Manager Evolution Server.



4.8. Define Application

To support non-IMS SIP users registered to Session Manager, an Application must be defined for Communication Manager Evolution Server.

To define a new Application, navigate to **Elements → Session Manager → Application Configuration → Applications** from the left navigational menu.

Click **New** (not shown). In the **Application** section on the **Application Editor** page, enter the following values.

- **Name** — Enter name for the application. In the sample configuration, "**CM7**" was used.
- **SIP Entity** — Select SIP Entity for Communication Manager Evolution Server defined in **Section 4.3**.
- **CM System for SIP Entity:** — Select name of Managed Element previously defined for Communication Manager Evolution Server. In the sample configuration, "**cm7**" was used.
- **Description:** — Enter description [Optional].

Leave fields in the **Application Attributes (optional)** section blank.

Click **Commit** to save the new definition.

The screen below shows the Application defined for Communication Manager Evolution Server.

4.9. Define Application Sequence

The second step in defining an Application to support non-IMS SIP Users registered to Session Manager is to define an Application Sequence.

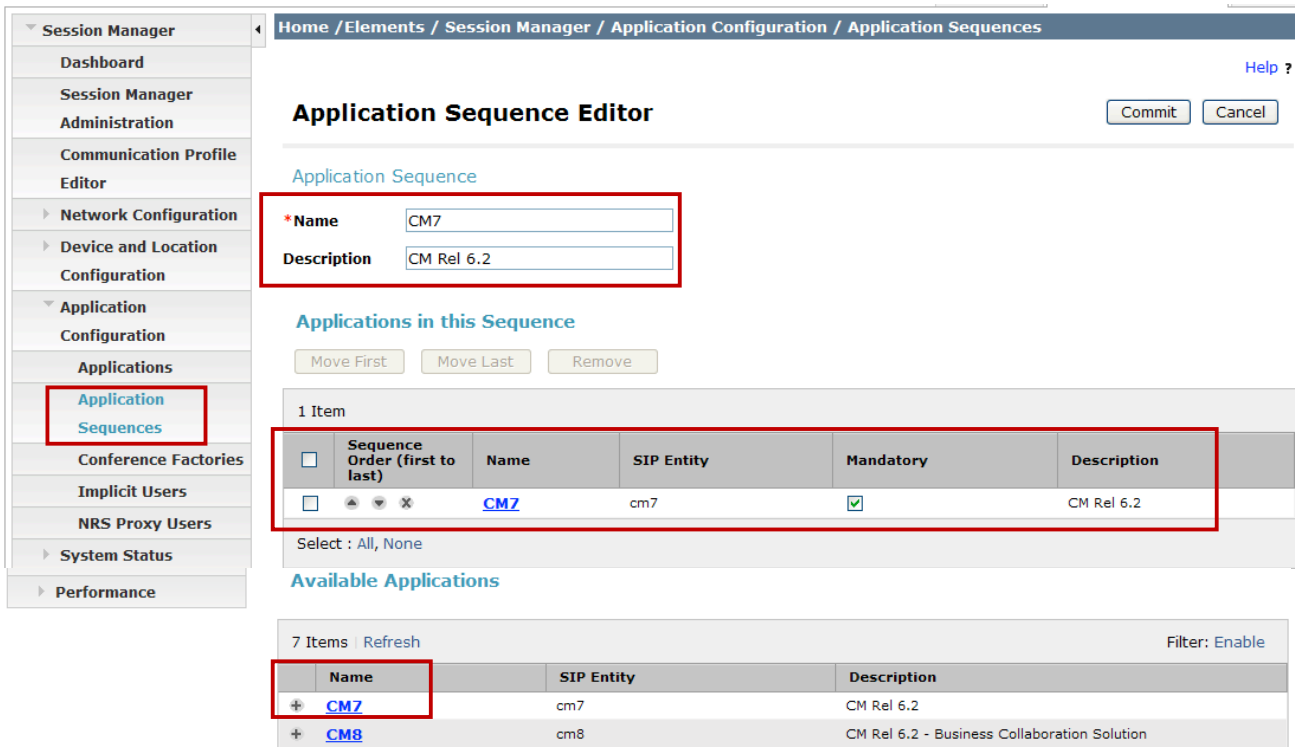
Navigate to **Elements → Session Manager → Application Configuration → Application Sequences** from the left navigation menu.

Click **New** (not shown). In the **Application Sequence** section, enter the following values.

- **Name** Enter name for the application.
- **Description** Enter description [Optional].

In the **Available Applications** table, click + icon associated with the Application for Communication Manager Evolution Server defined in **Section 4.8** to select this application.

Verify a new entry is added to the **Applications in this Sequence** table as shown below.



Note: The Application Sequence defined for Communication Manager Evolution Server must contain a single Application.

Click **Commit** to save the new Application Sequence.

4.10. Add SIP Users

Add new SIP users for each 9600 Series SIP station defined in **Section 3.11.** Alternatively, use the option in **Step 5** below to automatically generate the station after adding a new SIP user.

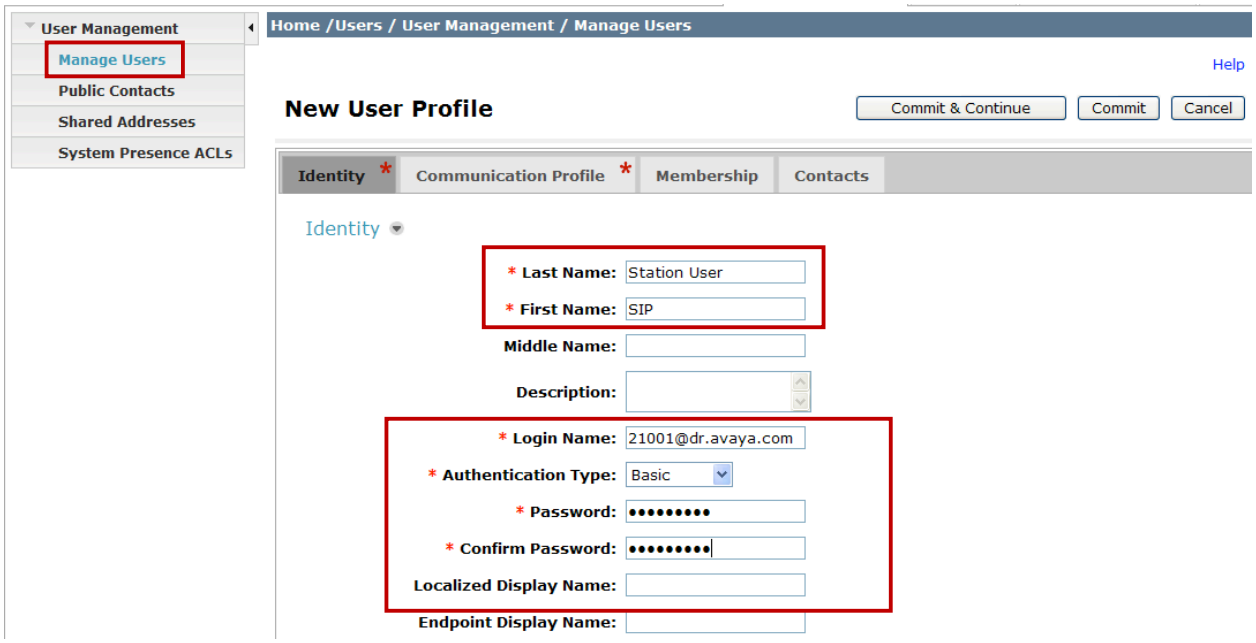
To add new SIP users, expand **Users → User Management** and select **Manage Users** from left navigation menu.

Note: to support failover, each SIP user was defined with multiple SIP Registrations.

Step 1: Click **New** (not shown). Enter values for the following required attributes for a new SIP user in the **Identity** section and use default values for remaining fields.

- **Last Name:** Enter last name of user.
- **First Name:** Enter first name of user.
- **Login Name:** Enter "**extension number@<domain>**" where "**<domain>**" matches the domain defined in **Section 4.1**.
- **Authentication Type:** Verify "**Basic**" is selected.
- **Password:** Enter password used to log into System Manager.
- **Confirm Password:** Repeat value entered above.
- **Localized Display Name:** Enter display name for user [Optional].

The screen below shows results from **Step 1** for a new SIP user.

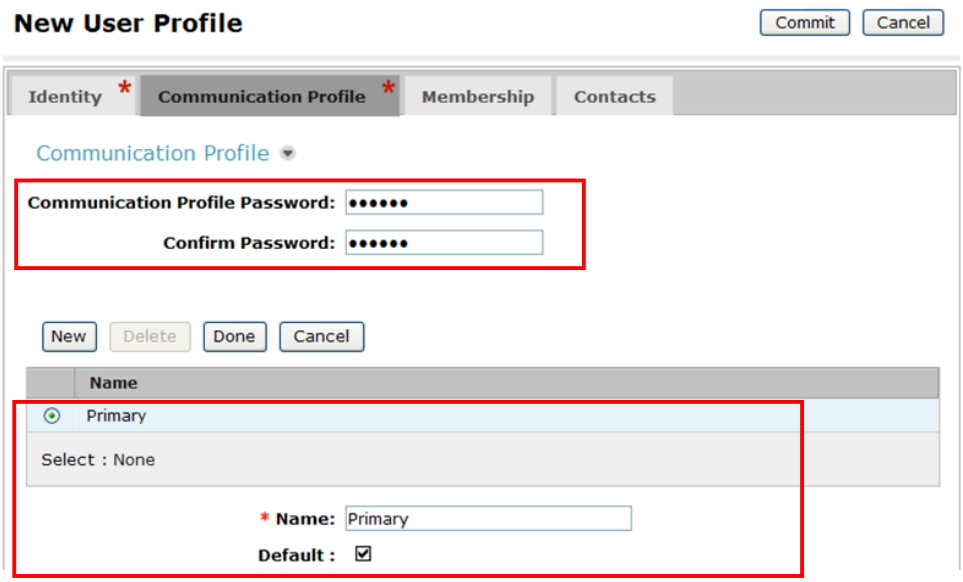


Click **Commit & Continue** to save changes from **Step 1**.

Step 2: Select **Communication Profile** tab and enter the value the endpoint will use to register to Session Manager in the **Communication Profile Password** and **Confirm Password** fields.

Note: Communication Profile Password should match the **Security Code** field defined in **Section 3.11.**

Verify there is a default entry identified as the **Primary** profile as shown below:



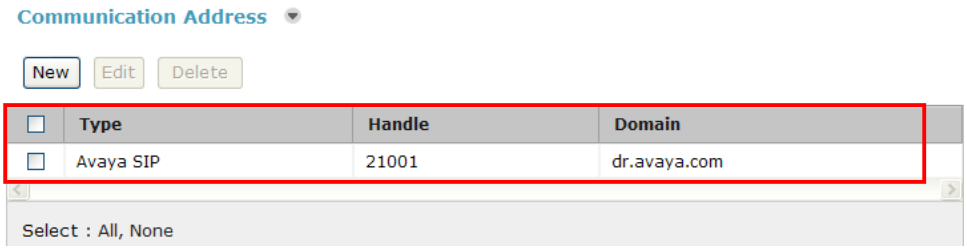
If an entry does not exist, select **New** and enter values for the following required attributes:

- **Name:** Enter "**Primary**".
- **Default:** Verify ☑ has been entered.

Step 3: Expand **Communication Address** sub-section and select **New** to define a **Communication Address** for the new user. Enter values for the following required attributes:

- **Type:** Select "**Avaya SIP**" from drop-down menu.
- **Fully Qualified Address:** Enter same extension number as used for **Login Name** in **Step 1**. **Note:** value is shown in **Handle** field after address is added.
- **Domain:** Verify value matches Domain name defined in **Section 4.1**.

Click **Add** (not shown) to save the Communication Address. The screen below shows results from **Step 3:**

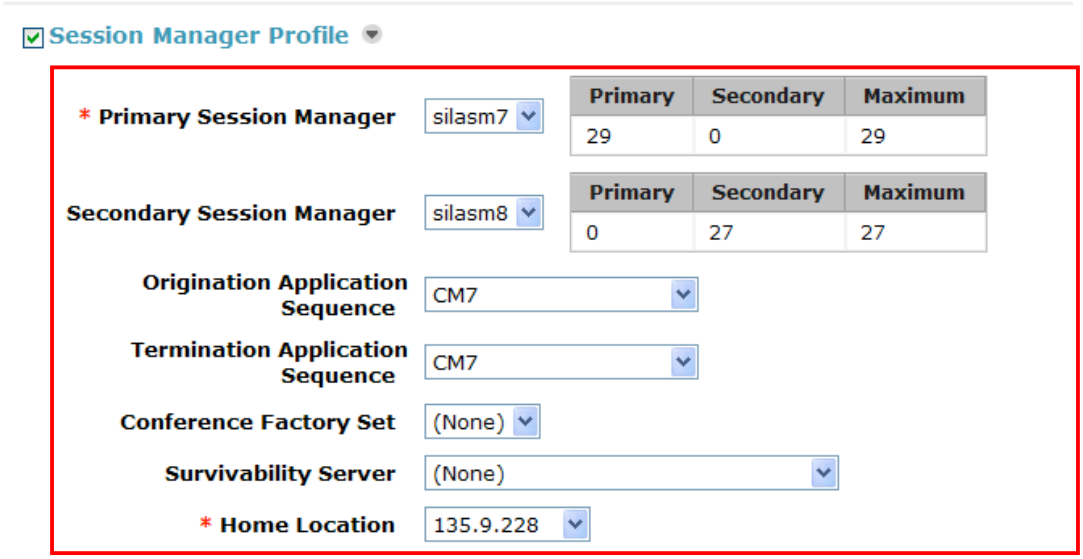


Step 4: Scroll down to the **Session Manager Profile** section and enter ☑ to expand section.

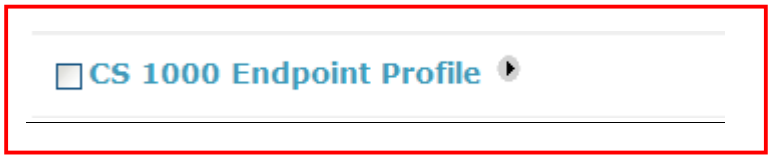
Enter the following values.

- **Primary Session Manager** — Select one of the Session Managers.
- **Secondary Session Manager** — Select the second Session Manager as the backup SIP Registrar.
- **Origination Application Sequence** — Select **Application Sequence** defined in **Section 4.9** for Communication Manager.
- **Termination Application Sequence** — Select **Application Sequence** defined in **Section 4.9** for Communication Manager.
- **Conference Factory Set** — Retain the default value of "**(None)**".
- **Survivability Server** — Select "**(None)**" from drop-down menu.
- **Home Location** — Select **Location** defined in **Section 4.2**.

The screen below shows results from **Step 4**.



Note: After selecting the values for the **Session Manager Profile** section, verify the **CS 1000 Endpoint Profile** section is not selected as shown below.

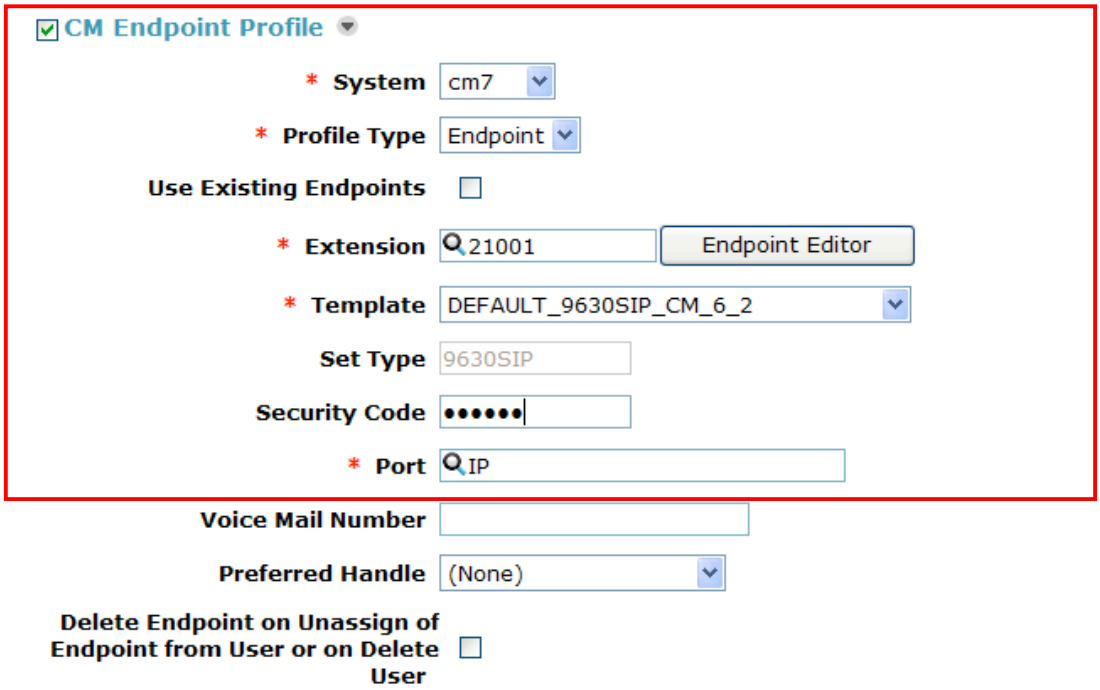


Step 5: Scroll down to the **CM Endpoint Profile** section and enter ☑ to expand section.

Enter the following values and use defaults for remaining fields.

- **System** — Select Managed Element defined for Communication Manager Evolution Server.
- **Profile Type** — Select "**Endpoint**".
- **Use Existing Endpoints** — Leave unchecked to automatically create new endpoint when a new user is created.
  Else, enter ☑ if endpoint is already defined.
- **Extension** — Enter same extension number used for **Login Name** in **Step 1**.
- **Template** — Select template for type of SIP phone.
- **Security Code** — Enter numeric value used to register the SIP endpoint.
  Note: this field should match the value entered for the **Communication Profile Password** field in **Step 2**.
- **Port** — Select "**IP**" from drop down menu.
- **Voice Mail Number** — Enter **Pilot Number** for Avaya Modular Messaging or Avaya Aura® Messaging if installed. Else, leave field blank.
- **Delete Station on Unassign of Endpoint** — Enter ☑ to automatically delete station when **Endpoint Profile** is un-assigned from user [Optional].

The screen below shows the results from **Step 5** when adding a new SIP user in the sample configuration.

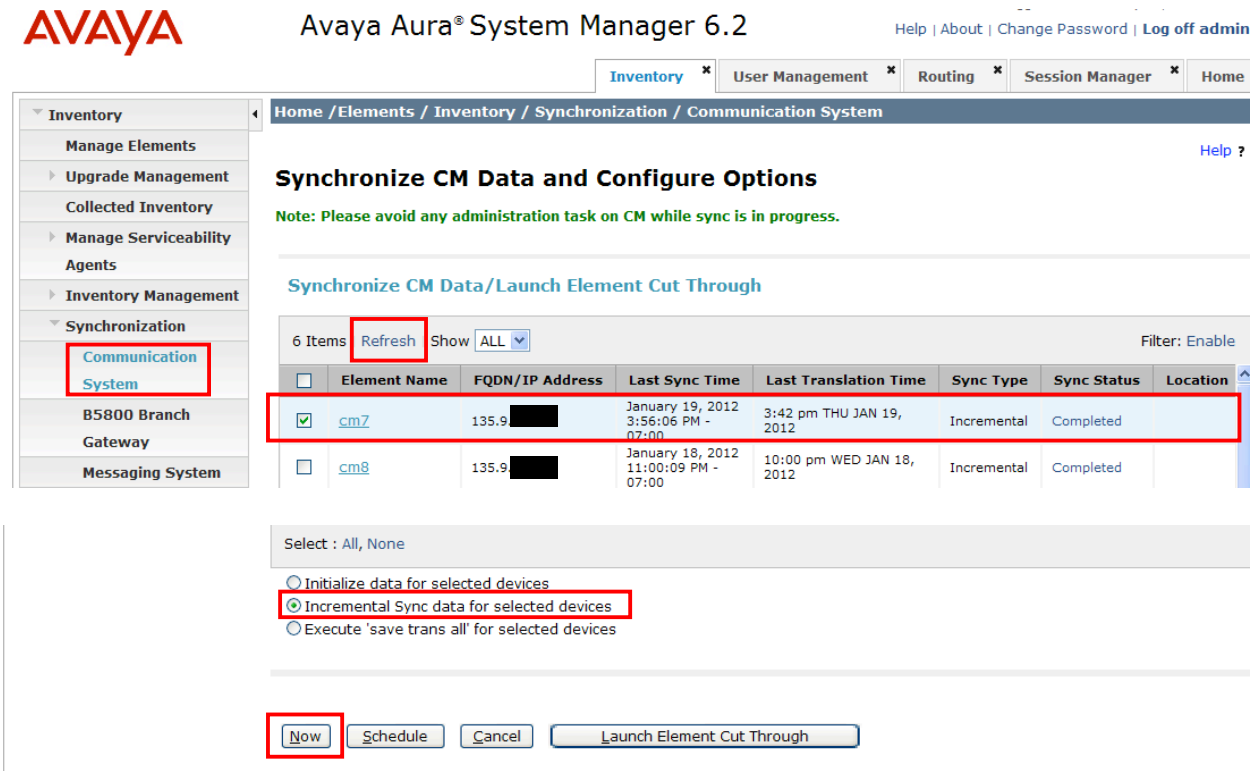


Click **Commit** (not shown) to save definition of the new user.

4.11. Synchronize Changes with Avaya Aura® Communication Manager

After completing these changes in System Manager, perform an on demand synchronization. Navigate to **Elements → Inventory → Synchronization → Communication System.**

On the **Synchronize CM Data and Configure Options** page, expand the **Synchronize CM Data/Launch Element Cut Through** table and select the row associated with Communication Manager Evolution Server as shown below.



Click ⊙ to select **Incremental Sync data for selected devices** option. Click **Now** to start the synchronization.

Use the **Refresh** button in the table header to verify status of the synchronization.

Verify synchronization successfully completes by verifying the status in the **Sync Status** column shows "**Completed**".

Note: Depending on the number of administration changes made, synchronization might take several minutes to complete.

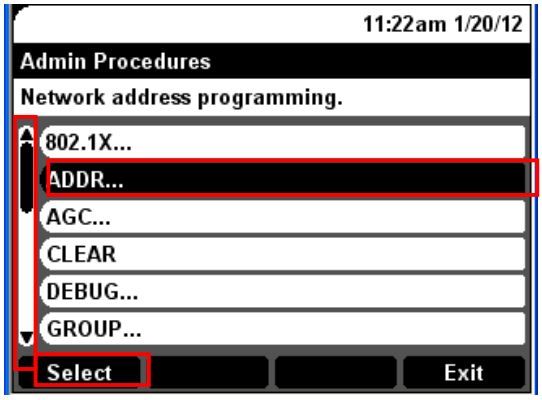
5. Manual Configuration of Avaya 9600 Series IP Deskphones

This section defines the steps to manually configure Avaya 9600 Series IP Deskphones running Avaya one-X® SIP firmware to register to both Session Managers.

5.1. Configuring IP Addresses

Enter the appropriate password on the keypad to acesss the Avaya 9600 Series IP Deskphone **Administration Procedure**. The screen shown below will be displayed on the Deskphone.

Note: These screens are from an Avaya 9630 IP Deskphone although all Avaya 9600 Series SIP Deskphones use the same basic settings and procedures.



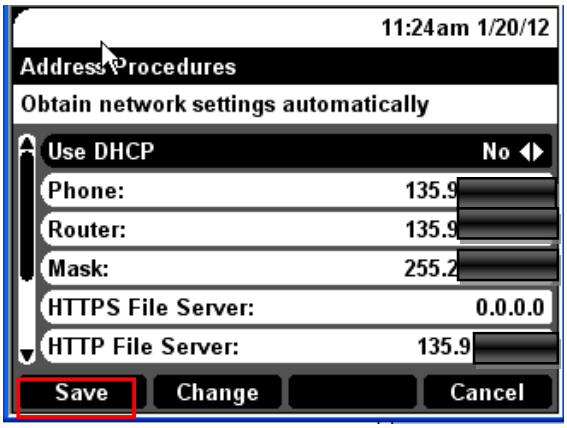
Using down arrow, scroll down one row to highlight **ADDR.…** field and press **Select**.

Using the **up** and **down** arrows, select the appropriate fields from the **Address Procedures** menu to specify settings for the specific network configuration and press **Change** to edit each field.

To manually configure the telephone, select "**No**" for **Use DHCP** field and enter appropriate IP addresses for **Phone, Router**, and **Mask.** Enter appropriate value for either the **HTTPS File Server** or **HTTP File Server** fields.

The screen below shows the configuration of these fields in the sample configuration.

Note: IP addresses have been partially hidden for security.



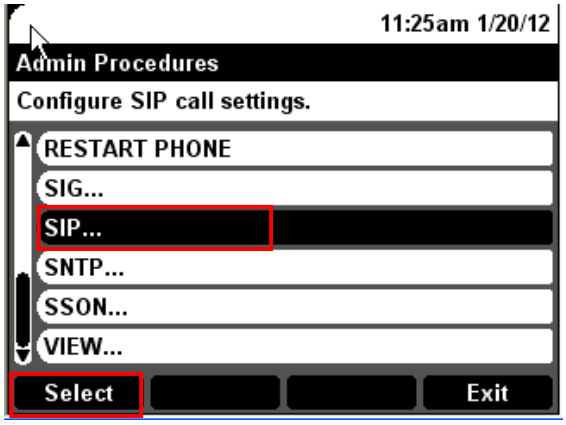
Continue scrolling down to see the fields for **DNS Server**, **802.1Q**, **VLAN ID**, and **VLAN Test**. Enter appropriate values for each field for the specific network configuration.

Once all fields in this section have been entered, press **Save** to save the new values and return to the main **Admin Procedures** menu.

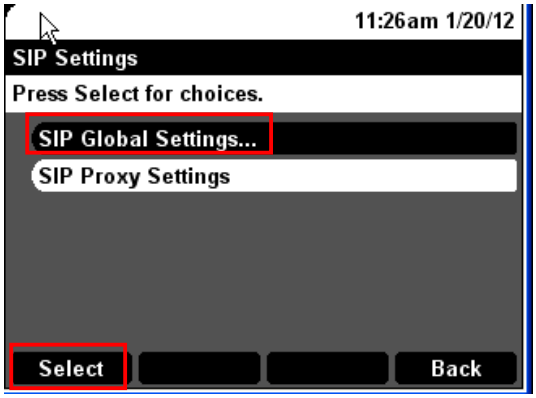
5.2. Configure SIP Global and Proxy Settings

The section describes the administration steps to configure the SIP Domain, the SIP Proxy Server IP address and other SIP settings.

Step 1: From the main **Admin Procedures** menu, scroll down and highlight **SIP…** field. Press **Select** to edit SIP settings.



Step 2: Highlight **SIP Global Settings…** on the **SIP Settings** menu and press **Select.**

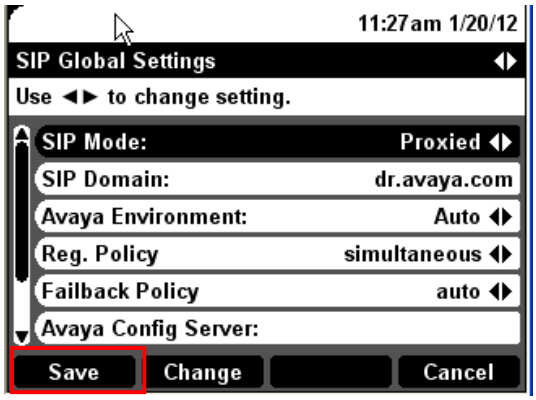


Step 3: Press **Change** to edit **SIP Global Settings**.

Enter the following values and use defaults for remaining fields:

- **SIP Mode:** Select "**Proxied**".
- **SIP Domain:** Enter the appropriate domain name. For the sample configuration, "**dr.avaya.com**" was used.
- **Avaya Environment:** Select "**Auto**".
- **Reg. Policy** Select "**simultaneous**" to support registration to both Session Managers.
- **Failback Policy** Select "**auto**".
- **User ID field** Select "**no**" (not shown).

The screens below show the results from **Step 3** for the sample configuration.



Press **Save** to save updated settings and return to **SIP Settings** menu.

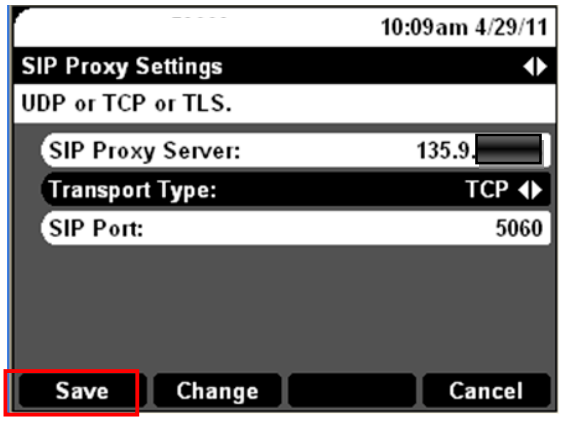
Step 4: On the **SIP Settings** menu, highlight **SIP Proxy Settings** (not shown) and press **Select.**

Select **NEW** (not shown).

Enter the following information for the primary Session Manager.

- **SIP Proxy Server:** Enter IP Address of SIP signaling interface for Session Manager.
- **Transport Type:** Select "**TCP**".
- **SIP Port:** Enter "**5060**".

The screen below shows the results from **Step 4** for the sample configuration.



Step 5: Press **Save.** Repeat the above step to enter the information for the second Session Manager.

Step 6: Press **Save** to save the information for the second Session Manager. Press **Back** two times to return to the main **Admin Procedures** menu.

Step 7: Press **Exit** to complete the configuration. The phone will reboot.

6. Verification Steps

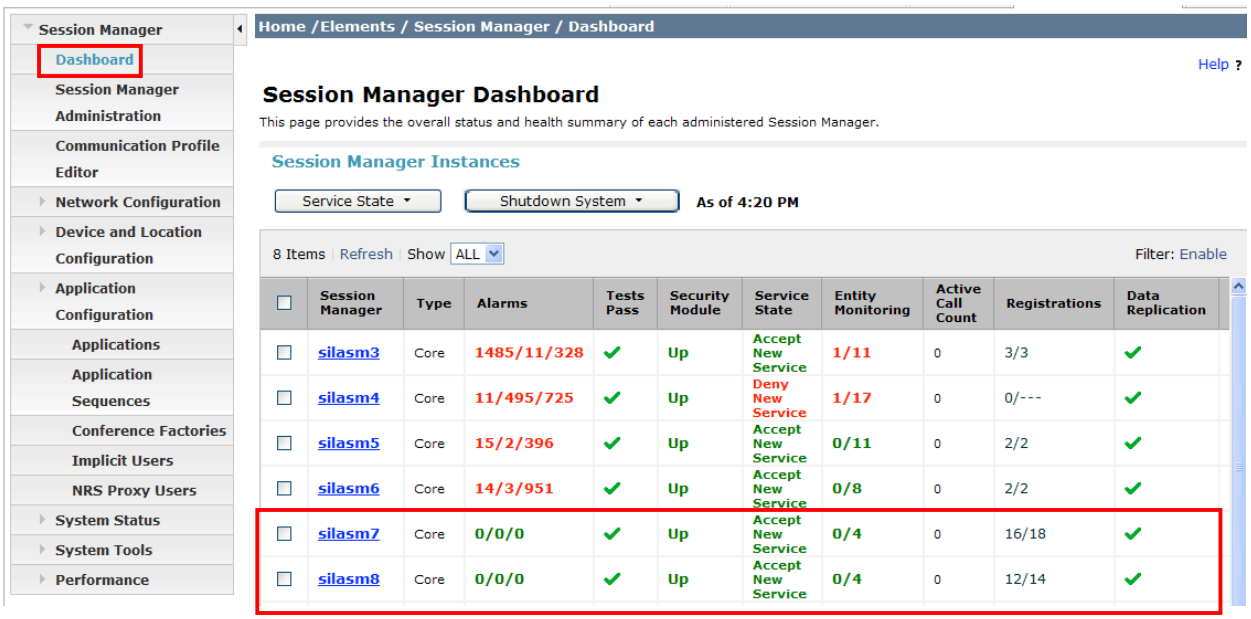
6.1. Verify Avaya Aura® Session Manager Configuration

Step 1: Verify Avaya Aura® Session Manager is Operational

Expand **Elements → Session Manager** and select **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
- **Data Replication** ✔



Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication
silasm3	Core	1485/11/328	✔	Up	Accept New Service	1/11	0	3/3	✔
silasm4	Core	11/495/725	✔	Up	Deny New Service	1/17	0	0/---	✔
silasm5	Core	15/2/396	✔	Up	Accept New Service	0/11	0	2/2	✔
silasm6	Core	14/3/951	✔	Up	Accept New Service	0/8	0	2/2	✔
silasm7	Core	0/0/0	✔	Up	Accept New Service	0/4	0	16/18	✔
silasm8	Core	0/0/0	✔	Up	Accept New Service	0/4	0	12/14	✔

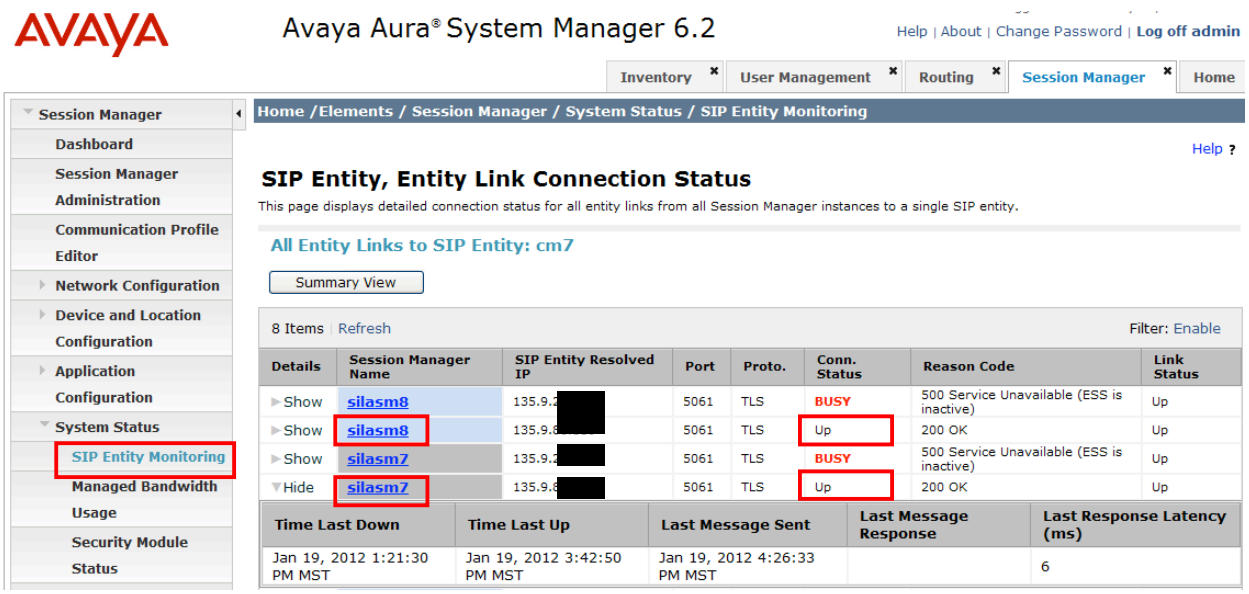
Step 2: Verify SIP Entity Link Status

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** to view more detailed status information for the specific SIP Entity Links used for calls between SIP endpoints and non-SIP stations on Communication Manager Evolution Server.

Select the SIP Entity for Communication Manager Evolution Server from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

In the **All Entity Links to SIP Entity: cm7** table, verify the **Conn. Status** for both links is "**Up**" as shown below:

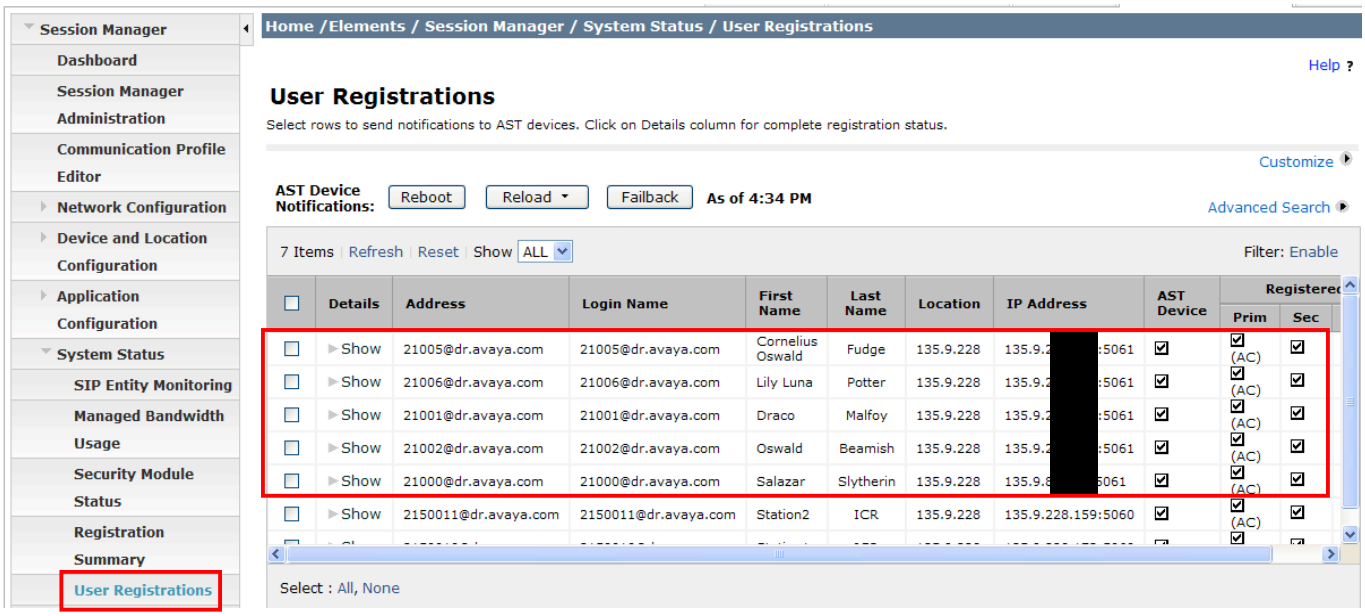
Click **Show** to view more information associated with the selected Entity Link.



Step 3: Verify Registrations of SIP Endpoints

Navigate to **Elements → Session Manager →System Status → User Registrations** to verify the SIP endpoints have successfully registered with both Session Managers.

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



6.2. Verify Avaya Aura® Communication Manager Operational Status

Verify the status of one of SIP trunk groups on Communication Manager Evolution Server by using the **status trunk n** command, where **n** is one of the trunk group numbers administered in **Section 3.6.2.**

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

```
status trunk 10
                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy
0010/001 T00006   in-service/idle    no
0010/002 T00007   in-service/idle    no
0010/003 T00008   in-service/idle    no
0010/004 T00009   in-service/idle    no
0010/005 T00014   in-service/idle    no
0010/006 T00015   in-service/idle    no
0010/007 T00043   in-service/idle    no
0010/008 T00044   in-service/idle    no
0010/009 T00045   in-service/idle    no
0010/010 T00046   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 administered in **Section 3.6.1.**

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

```
status signaling-group 10
                          STATUS SIGNALING GROUP

        Group ID: 10                              Active NCA-TSC Count: 0
      Group Type: sip                              Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

Use the SAT command, **list trace tac #**, where **tac #** is the trunk access code for one of the trunk groups defined in **Section 3.6.2** 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 endpoint using extension "**21001**" to a second SIP endpoint on extension "**31001**".

Note: Trace has been edited to partially hide IP addresses for security purposes.

```
list trace tac #010                                          Page   1
                                LIST TRACE
time            data
13:11:10 TRACE STARTED 01/20/2012 CM Release String cold-02.0.823.0-19402
13:11:15 SIP<INVITE sip:21001@dr.avaya.com;avaya-cm-fnu=off-hook SIP
13:11:15 SIP</2.0
13:11:15     Call-ID: 12_9306d51b4856bf4fac6ed8_I@135.9.xxx.xxx
13:11:15 SIP>SIP/2.0 183 Session Progress
13:11:15     Call-ID: 12_9306d51b4856bf4fac6ed8_I@135.9.xxx.xxx
13:11:17 SIP>SIP/2.0 484 Address Incomplete
13:11:17     Call-ID: 12_9306d51b4856bf4fac6ed8_I@135.9.xxx.xxx
13:11:17 SIP<INVITE sip:31001@dr.avaya.com SIP/2.0
13:11:17     Call-ID: 12_9306d51b4856bf4fac6ed8_I@135.9.xxx.xxx
13:11:17 SIP>SIP/2.0 100 Trying
13:11:17     Call-ID: 12_9306d51b4856bf4fac6ed8_I@135.9.xxx.xxx
13:11:17     dial 31001
13:11:17     term station      31001 cid 0x5
13:11:17 SIP>INVITE sip:31001@dr.avaya.com SIP/2.0
13:11:17     Call-ID: 80b2783a1f48e11c004f23e83400
13:11:17 SIP<ACK sip:21001@dr.avaya.com;avaya-cm-fnu=off-hook;routei
13:11:17 SIP<nfo=0-0-1068-0imsorig;nrindex=0 SIP/2.0
13:11:17     Call-ID: 12_9306d51b4856bf4fac6ed8_I@135.9.xxx.xxx
13:11:17 SIP<SIP/2.0 100 Trying
13:11:17     Call-ID: 80b2783a1f48e11c004f23e83400
13:11:17 SIP>INVITE sip:31001@dr.avaya.com SIP/2.0
13:11:17     Call-ID: 80b2783a1f48e11c004f23e83400
13:11:17 SIP>SIP/2.0 100 Trying
13:11:17     Call-ID: 80b2783a1f48e11c004f23e83400
13:11:18 SIP>SIP/2.0 180 Ringing
13:11:18     Call-ID: 80b2783a1f48e11c004f23e83400
13:11:18 SIP<SIP/2.0 180 Ringing
13:11:18     Call-ID: 80b2783a1f48e11c004f23e83400
13:11:18 SIP>SIP/2.0 180 Ringing
13:11:19 SIP>SIP/2.0 200 OK
13:11:19     Call-ID: 80b2783a1f48e11c004f23e83400
13:11:19 SIP<SIP/2.0 200 OK
13:11:19     Call-ID: 80b2783a1f48e11c004f23e83400
13:11:19     G729 ss:off ps:20
             rgn:1 [135.9.xxx.xxx]:5004
             rgn:1 [135.9.xxx.xxx]:5004
13:11:19 SIP>SIP/2.0 200 OK
13:11:19     Call-ID: 12_9306d51b4856bf4fac6ed8_I@135.9.xxx.xxx
13:11:19     active station      31001 cid 0x5
13:11:19     G729 ss:off ps:20
             rgn:1 [135.9.xxx.xxx]:5004
             rgn:1 [135.9.xxx.xxx]:5004
13:11:19 SIP<ACK sip:31001@135.9.xxx.xxx:5061;transport=tls;epv=%3csi
```

On Communication Manager, use the SAT command, **list trace station xxx**, where **xxx** is a valid extension number for a SIP telephone. For example, the trace below illustrates call between the same SIP endpoints as the previous trace.

Note: Trace has been edited to partially hide IP addresses for security purposes.

```
list trace station 21001                                          Page   1
                                LIST TRACE
time            data
13:15:18 TRACE STARTED 01/20/2012 CM Release String cold-02.0.823.0-19402
13:15:23 SIP<INVITE sip:21001@dr.avaya.com;avaya-cm-fnu=off-hook SIP
13:15:23 SIP</2.0
13:15:23     Call-ID: 1a_9367c91b486d074facd0b8_I@135.9.xxx.xxx
13:15:23 SIP>SIP/2.0 183 Session Progress
13:15:23     Call-ID: 1a_9367c91b486d074facd0b8_I@135.9.xxx.xxx
13:15:23     active station      21001 cid 0x7
13:15:23 SIP>SIP/2.0 484 Address Incomplete
13:15:23     Call-ID: 1a_9367c91b486d074facd0b8_I@135.9.xxx.xxx
13:15:23 SIP<INVITE sip:31001@dr.avaya.com SIP/2.0
13:15:23     Call-ID: 1a_9367c91b486d074facd0b8_I@135.9.xxx.xxx
13:15:23 SIP>SIP/2.0 100 Trying
13:15:23     Call-ID: 1a_9367c91b486d074facd0b8_I@135.9.xxx.xxx
13:15:23     dial 31001
13:15:23     term station      31001 cid 0x7
13:15:23 SIP>INVITE sip:31001@dr.avaya.com SIP/2.0
13:15:23     Call-ID: 8024e8cb1f48e11df04f23e83400
13:15:23 SIP<ACK sip:21001@dr.avaya.com;avaya-cm-fnu=off-hook;routei
13:15:23 SIP<nfo=0-0-1068-0imsorig;nrindex=0 SIP/2.0
13:15:23     Call-ID: 1a_9367c91b486d074facd0b8_I@135.9.xxx.xxx
13:15:23 SIP<SIP/2.0 100 Trying
13:15:23     Call-ID: 8024e8cb1f48e11df04f23e83400
13:15:23 SIP>INVITE sip:31001@dr.avaya.com SIP/2.0
13:15:23     Call-ID: 8024e8cb1f48e11df04f23e83400
13:15:23 SIP>SIP/2.0 100 Trying
13:15:23     Call-ID: 8024e8cb1f48e11df04f23e83400
13:15:24 SIP>SIP/2.0 180 Ringing
13:15:24     Call-ID: 8024e8cb1f48e11df04f23e83400
13:15:24 SIP<SIP/2.0 180 Ringing
13:15:24     Call-ID: 8024e8cb1f48e11df04f23e83400
13:15:24 SIP>SIP/2.0 180 Ringing
13:15:24     Call-ID: 1a_9367c91b486d074facd0b8_I@135.9.xxx.xxx
13:15:25 SIP>SIP/2.0 200 OK
13:15:25     Call-ID: 8024e8cb1f48e11df04f23e83400
13:15:25 SIP<SIP/2.0 200 OK
13:15:25     Call-ID: 8024e8cb1f48e11df04f23e83400
13:15:25     G729 ss:off ps:20
             rgn:1 [135.9.xxx.xxx]:5004
             rgn:1 [135.9.xxx.xxx]:5004
13:15:25 SIP>SIP/2.0 200 OK
13:15:25     Call-ID: 1a_9367c91b486d074facd0b8_I@135.9.xxx.xxx
13:15:25     active station      31001 cid 0x7
13:15:25     G729 ss:off ps:20
             rgn:1 [135.9.xxx.xxx]:5004
             rgn:1 [135.9.xxx.xxx]:5004
13:15:25 SIP<ACK sip:31001@135.9.xxx.xxx:5061;transport=tls;epv=%3csi
```

6.3. Call Scenarios Verified

Verification scenarios for the configuration described in these Application Notes included the following call scenarios:

Basic Calls:

- Place a call from a SIP endpoint to other SIP stations or to other non-SIP stations. Answer the call and verify talk path.
- Place a call from a SIP endpoint to other SIP stations or to other non-SIP stations. Answer the call and place the call on Hold. Return to the held call and verify talk path.
- Verify calls can be transferred from a SIP endpoint to other SIP stations or to other non-SIP stations.
- Verify calls can be forwarded from a SIP endpoint to other SIP stations or to other non-SIP stations.
- Verify that a SIP endpoint can create a conference with other SIP endpoints and non-SIP stations.
- Repeat the above scenarios with calls originating from non-SIP stations on Communication Manager Evolution Server to SIP endpoints.

Failure Scenarios:

- Change Management State of the primary Session Manager to "**Deny New Service**".
    - Verify a SIP endpoint can still make calls to other SIP stations or to non-SIP stations. Answer the calls and verify talk path.
    - Verify a SIP endpoint can still make calls to other SIP stations or to non-SIP stations. Answer the call and place the call on Hold. Return to the held call and verify talk path.
- During an active call, disable network connectivity to primary Session Manager.
    - Verify talk path on the active call after the failover. Disconnect the call and verify the call is properly cleared.
    - Verify talk path on the active call after the failover. Place the call on Hold. Return to the held call and verify talk path.
    - During failover, verify a SIP endpoint can still make calls to another station (including both SIP and non-SIP stations). Answer the call and verify talk path.
    - During failover, verify a SIP endpoint can still make calls to another station (including both SIP and non-SIP stations). Answer the call and place the call on Hold. Return to the held call and verify talk path.
- Disable the SIP trunk between Communication Manager and the primary Session Manager.
    - Verify a SIP endpoint can still make calls to other SIP stations or to non-SIP stations. Answer the calls and verify talk path.
    - Verify a SIP endpoint can still make calls to other SIP stations or to non-SIP stations. Answer the call and place the call on Hold. Return to the held call and verify talk path
- Repeat the above scenarios with calls originating from non-SIP stations on Communication Manager Evolution Server to a SIP endpoint.

7. Acronyms

AAR	Automatic Alternate Routing (Routing on Communication Manager)
ARS	Automatic Route Selection (Routing on Communication Manager)
FQDN	Fully Qualified Domain Name (hostname for Domain Naming Resolution)
IMS	IP Multimedia Subsystem
IP	Internet Protocol
LAR	Look-ahead Routing
RTP	Real Time Protocol
SAT	System Access Terminal (Communication Administration Interface)
SIP	Session Initiation Protocol
SMGR	Avaya Aura® System Manager (used to configure Session Manager)
TAC	Trunk Access Code (Communication Manager Trunk Access)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator

8. Conclusion

These Application Notes describe how to configure a network with Avaya Aura® Session Manager Release 6.2 and Avaya Aura® Communication Manager Release 6.2. Avaya Aura® Communication Manager serves as a Evolution Server within the Avaya Aura® architecture and supports Avaya 9600 Series SIP endpoints registered to Avaya Aura® Session Manager. Avaya 9600 Series IP Deskphones (running Avaya one-X® H.323 firmware) and 2420 Digital Telephones are also supported Avaya Aura® Communication Manager.

The network in the sample configuration uses two Avaya Aura® Session Managers deployed as a pair of active-active redundant servers. 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.

Interoperability testing included making bi-directional calls between SIP endpoints and several other types of stations on Communication Manager Evolution Server. In addition, various features including hold, transfer and conference were tested on these calls. Finally, testing was performed to verify calls between SIP endpoints and other types of stations on Avaya Aura® Communication Manager Evolution Server were successful even when there were network connectivity issues or when one of the Session Managers was not available.

9. Additional References

Avaya Product documentation relevant to these Application Notes is available at http://support.avaya.com.

Avaya Aura® Session Manager

1) Avaya Aura® Session Manager Overview, Doc ID 100068105.
2) Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473.
3) Avaya Aura® Session Manager Case Studies, Doc ID 03-603478.
4) Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325.
5) Administering Avaya Aura® Session Manager, Doc ID 03-603324.

Avaya Aura® Communication Manager

6) SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206.
7) Administering Avaya Aura® Communication Manager, Doc ID 03-300509.
8) Administering Avaya Aura® Communication Manager Server Options, Doc ID 03-603479.
9) Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide, Doc ID 210-100-500.
10) Avaya Toll Fraud Security Guide, Doc ID 555-025-600.

Avaya IP Deskphones (SIP)

11) Avaya one-X® Deskphone SIP Administrator Guide. December 6, 2010.
12) Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.6. June 7, 2010.
13) Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 6.1 for 9601 IP Deskphone, December 6, 2010.
14) Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 6.0 for 9608, 9611G, 9621G and 9641G IP Deskphones, November 22, 2010.
15) Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 2.6, June 7, 2010.

Avaya Application Notes

16) Configuring 9600 Series IP Deskphones running Avaya one-X® SIP firmware with Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Communication Manager Evolution Server Release 6.0.1.
17) Configuring multiple Avaya Aura® Session Managers to address different Network Failure Scenarios.
18) Configuring Avaya 10x0 Series SIP Video Endpoints with Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Communication Manager Evolution Server Release 6.0.1

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com