Avaya Solution Interoperability Lab

Configuring SIP Trunks among Avaya Business Communication Manager 50, Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager– Issue 1.0

Abstract

These Application Notes describe a sample configuration of a network that uses SIP trunks between Avaya Business Communication Manager 50, Avaya Aura™ Session Manager Release, Avaya Aura™ Communication Manager Access Element Release, and a second Avaya Aura™ Communication Manager operating as a Feature Server.

- 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 operates as a Feature Server for the SIP endpoints which communicates with Avaya Aura™ Session Manager over SIP trunks.
- Avaya Business Communication Manager 50 is an all-in-one platform supporting converged voice and data communications for small businesses.

□These Application Notes provide information for the setup, configuration, and
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 of a network that uses SIP trunks between Avaya Business Communication Manager 50 R5, Avaya Aura^{TM} Session Manager Release, Avaya Aura^{TM} Communication Manager Access Element Release, and a second Avaya Aura^{TM} Communication Manager operating as a Feature Server.

As shown in **Figure 1,** the Business Communication Manager 50 supports the 1230 IP and T7316E digital phones and is connected to the SM-100 (Security Module-100) network interface on Avaya Aura™ Session Manager over a SIP trunk. Avaya 9600 Series IP Telephone (H.323) and 2420 Digital Telephone are supported by the Avaya Aura™ Communication Manager Access Element. The Communication Manager Access Element is also connected over a SIP trunk to the Avaya Aura™ Session Manager. All inter-system calls are carried over these SIP trunks.

Avaya Aura™ Session Manager is managed by Avaya Aura™ System Manager. Avaya 9630 IP Telephones configured as SIP endpoints utilize the Avaya Aura™ Session Manager User Registration feature and require an Avaya Aura™ Communication Manager operating as a Feature Server. The Communication Manager Feature Server only supports IMS-SIP users that are registered to Avaya Aura™ Session Manager. The Communication Manager Feature Server is connected to Session Manager via an IMS-enabled SIP signaling group and associated SIP trunk group.

For the sample configuration, two Avaya Aura™ Session Managers running on separate Avaya S8510 Servers are deployed as a pair of active-active redundant servers to support failover testing[1]. The Avaya Aura™ Communication Manager Access Element runs on a pair of duplicated Avaya S8730 Servers with an Avaya G650 Media Gateway.

The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura™ Communication Manager.

These Application Notes will focus on the configuration of the SIP trunks and call routing needed to test calls between Business Communication Manager and stations on Avaya Aura™ Communication Manager Access Element or SIP stations registered to Avaya Aura™ Session Manager. Detailed administration of multiple Avaya Aura™ Session Managers, multiple SIP trunks on Business Communication Manager to support failover testing, configuration of the Avaya Aura™ Communication Manager Feature Server, SIP endpoints, or SIP users will not be described (see the appropriate documentation listed in **Section 9**).

[1] For more information on configuring multiple Session Managers and multiple SIP Trunks on Business Communication Manager 50 to support failover testing, see appropriate documentation in **Section 9**.

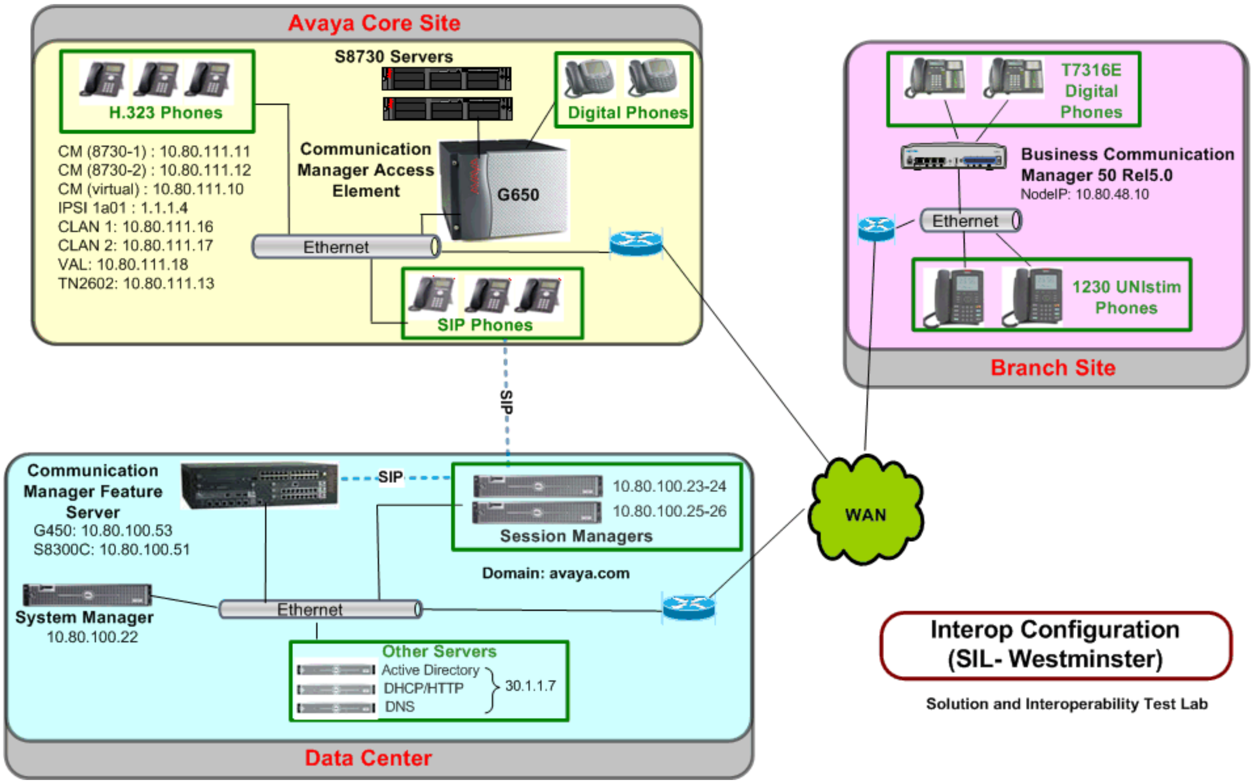


Figure 1 – Sample Configuration

1.1. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Component	Software Version
Avaya Aura™ Session Manager on Avaya S8510 server	Release 5.2.0.1.520017-11-18-2009
Avaya Aura™ System Manager	Release 5.2, Load: 5.2.0.8.27
Avaya Aura™ Communication Manager Access Element • Duplicated Avaya S8730 Servers • Avaya G650 Media Gateway	Release 5.2.1 Load: R015x.02.1.016.4
Avaya Aura™ Communication Manager Feature Server • Avaya S8300 Server	Release 5.2.1 Load: R015x.02.1.016.4
Avaya IP Telephones: • 4621SW • 9620	 FW: 2.90 FW:3.0
Avaya SIP Phones • 9630	FW: 2.5.0
Avaya Digital Telephones (2420D)	N/A
Avaya Business Communication Manager 50	Release 5 Version: 9.0.1.22.524
1230 IP Telephone	FW: 062AC6R
T7316E Digital Telephone	N/A

2. Configure Avaya Aura™ Communication Manager Feature Server

This section describes the administration of SIP trunks between the Avaya Aura™ Communication Manager Feature Server and Avaya Aura™ Session Manager using a System Access Terminal (SAT). These instructions assume the G450 Media Server is already configured on the Communication Manager Feature Server. Some administration screens have been abbreviated for clarity.

- Verify System Capabilities and Licensing
- Administer network region
- Administer IP node names
- Administer IP interface
- Administer SIP trunk group and signaling group
- Administer route pattern
- Administer numbering plan

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

2.1. Verify System Capabilities and Licensing

This section describes the procedures to configure the correct system capabilities and licensing on the Avaya Aura™ Communication Manager Feature Server. If there is insufficient capacity or a required features is not available, contact an authorized Avaya sales representative to make the appropriate changes.

2.1.1. SIP Trunk Capacity Check

Issue the **display system-parameters customer-options** command to verify that 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: 500   0
           Maximum Concurrently Registered IP Stations: 18000 4
             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: 100   0
                        Maximum Video Capable Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 50    20
```

2.1.2. AAR/ARS Routing Check

To simplify the dialing plan for users of SIP endpoints, verify that both the **ARS** and **ARS/AAR Dialing without FAC** parameters are enabled (on page 3 of system-parameters customer options).

```
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?
```

2.1.3. Enable Private Numbering

Use the “**change system-parameters customer-options**” command to verify that Private Networking is enabled as shown below:

```
display system-parameters customer-options              Page   5 of  11
                                OPTIONAL FEATURES

               Multinational Locations? y             Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n     Station as Virtual Extension? y
                    Multiple Locations? y
                                            System Management Data Transfer? n
         Personal Station Access (PSA)? y                Tenant Partitioning? n
                      PNC Duplication? n       Terminal Trans. Init. (TTI)? y
                  Port Network Support? n               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
                                                                   Wireless? y
```

2.1.4. Configure Trunk-to-Trunk Transfers

Use the “**change system-parameters features**” command to enable trunk-to-trunk transfers. This feature is needed to be able to transfer an incoming/outgoing call from/to the remote switch back out to the same or another switch For simplicity, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis.

Note that 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 a specific trunk group(s). For more information regarding how to configure a Communication Manager to minimize toll fraud, see reference 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
…
```

2.2. Add Node Name of Avaya Aura™ Session Manager

Using the **change node-names ip** command, add the node-name for one of the Avaya Aura™ Session Managers where the SIP endpoints will be registered, if not already added. For the sample configuration, SIP endpoints were registered to the first Avaya Aura™ Session Manager, labeled "ASM1" with IP address: 10.80.100.24.

```
change node-names ip                                    Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
ASM1                    10.80.100.24
Nortel-CS1000e          10.80.50.50
default                 0.0.0.0
procr                   10.80.100.51
```

2.3. Configure IP Network Region

Using the **change ip-network-region 1** command, set the **Authoritative Domain** to the correct SIP domain for the configuration. Verify the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields are set to "**yes**".

```
change ip-network-region 1                              Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: avaya.com
    Name:
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
```

2.4. Configure SIP Signaling Group and Trunk Group

2.4.1. Add Signaling Group for SIP Trunk

Use the **add signaling-group n** command, where "n" is an available signaling group number to create a SIP signaling group to connect to one of the Avaya Aura™ Session Managers. In the sample configuration, signaling group "10" and trunk group "10" were used to connect to the first Avaya Aura™ Session Manager.

The screen below shows the values used for the signaling group in the sample configuration:

- **Group Type:** "sip"
- **Transport Method:** "tcp[2]"
- **IMS Enabled?:** "y"

[2] TCP was used for the sample configuration. However, TLS would typically be used in production environments.

- **Near-end Node Name:** **"**procr" node name from **Section 2.2**
- **Far-end Node Name:** Session Manager node name from **Section 2.2**
- **Near-end Listen Port:** "5060"
- **Far-end Listen Port:** "5060"
- **Far-end Domain:** Authoritative Domain from **Section 2.3**
- **Enable Layer 3 Test:** "y"
- **Session Establishment Timer:** "3"[3]
- Default values can be used for the remaining fields

```
display signaling-group 10                                    Page   1 of   1
                                SIGNALING GROUP

Group Number: 10            Group Type: sip
                        Transport Method: tcp
  IMS Enabled? Y
     IP Video? n

    Near-end Node Name: procr                   Far-end Node Name: ASM1
 Near-end Listen Port: 5060                   Far-end Listen Port: 5060
                                            Far-end Network Region:  1
Far-end Domain: avaya.com
                                          Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate               RFC 3389 Comfort Noise? 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? y                    Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

2.4.2. Add SIP Trunk Group

Add the corresponding trunk group controlled by the signaling group using the **add trunk-group n** command, where "n" is an available trunk group number and fill in the indicated fields.

- **Group Type:** "sip"
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** "tie"
- **Signaling Group:** The number of the signaling group added in **Section 2.4.1**
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total number of trunks configured in **Section 2.1.1**).

[3] If any call originating from the SIP phone is not expected to be answered within 3 minutes, this value may need to be increased.

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

Group Number: 10                       Group Type: sip          CDR Reports: y
  Group Name: ASM1                            COR: 1        TN: 1        TAC: #10
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: 10
```

Once the add command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

On page 2, set the **Preferred Minimum Session Refresh Interval** 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, set **Numbering Format** to be *private*. Use default values for all other fields.

```
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?
```

On page 4, set **Mark Users As Phone** to “y” to send correct user information to Business Communication Manager in the SIP messages, and set the **Telephone Event Payload Type** to “101”.

```
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? n
             Telephone Event Payload Type: 101
```

2.5. Administer Numbering Plan

SIP Users registered to Session Manager should be added to either the private or public numbering table on the Communication Manager Feature Server. 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 References in **Section 9.**

To enable SIP endpoints to dial extensions defined in the Communication Manager Access Element, use the “**change private-numbering x”** command, where x is the number used to identify the private number plan. For the sample configuration, extension numbers starting with 5XX-XXXX or 6XX-XXX are used on the Communication Manager Access Element.

- **Ext Len:** Enter the extension length allowed by the dial plan
- **Ext Code:** Enter leading digit (s) from extension number
- **Trunk Grp:** Enter the SIP Trunk Group number for the SIP trunk between the Feature Server and Session Manager
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix.

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

Ext Ext                Trk         Private          Total
Len Code               Grp(s)      Prefix           Len
 7  5                  10                           7     Total Administered: 2
 7  6                  10                           7        Maximum Entries: 540
```

2.6. Configure Stations

For each SIP user defined in Session Manager, add a corresponding station on the Communication Manager Feature Server. 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. See References in **Section 9** for more information on adding SIP users in Session Manager.

The phone number defined for the station will be the number the SIP user enters to register to Session Manager. Use the "**add station x**" command where x is a valid extension number defined in the system. On page 1 of the change station form:

- **Phone Type:** Set to 9630SIP
- **Name:** Enter Display name for user
- **Security Code:** Enter number used when user logs into station. Note: this code should match the "**Shared Communication Profile Password**" field defined when adding this user in Session Manager. See References in **Section 9** for more information on adding SIP users in Session Manager.

```
add station 6663000                                         Page   1 of   6

                             STATION

Extension: 666-3000                         Lock Messages? n            BCC: 0
     Type: 9630SIP                          Security Code: 123456        TN: 1
     Port: S00006                         Coverage Path 1: 1            COR: 1
     Name: John Smith                     Coverage Path 2:              COS:
…
```

On page 6, set:

- **SIP Trunk option:** Enter SIP Trunk Group defined in **Section 2.4.2**

```
change station 6663000                                         Page   6 of   6

                             STATION
SIP FEATURE OPTIONS
         Type of 3PCC Enabled: None
                    SIP Trunk: 10
```

2.7. Configure Off-PBX-Telephone Station-Mapping

Use the "**change off-pbx-telephone station-mapping**" command for each extension associated with SIP users defined in Session Manager.

On page 1, enter the SIP Trunk Group defined in **Section 2.4.2** and use default values for other fields.

```
change off-pbx-telephone station-mapping 6663000              Page   1 of  3

                STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk      Config  Dual
 Extension                 Prefix                     Selection  Set     Mode
 666-3000         OPS          -      6663000          10         1
                               -
                               -
```

On page 2, enter the following values:

- **Mapping Mode**: "both"
- **Calls Allowed:** "all"

```
change off-pbx-telephone station-mapping 6663000              Page   2 of  3

                STATIONS WITH OFF-PBX TELEPHONE INTEGRATION


 Station       Appl    Call        Mapping    Calls      Bridged     Location
 Extension     Name    Limit       Mode       Allowed    Calls
 666-3000      OPS      3          both       all         none
                               -
```

2.8. Save Translations

Configuration of Avaya Aura™ Communication Manager Feature Server is complete. Use the **"save translations**" command to save these changes

Note: After a change on the Avaya Aura™ Communication Manager Feature Server which alters the dial plan, synchronization between Communication Manager Feature Server and Avaya Aura™ Session Manager needs to be completed and SIP phones must be re-registered. To request an on demand synchronization, log into the System Manager console and use the **Synchronize CM Data** feature under the Communication System Management menu.

3. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring the Avaya Aura™ Session Manager and includes the following items:

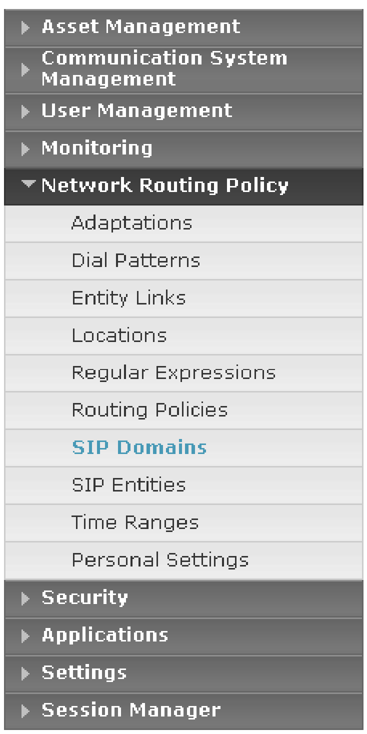
- Administer SIP domain
- Define Logical/physical Locations where SIP Entities will be located
- Specify the Listen Port on Avaya Aura™ Session Manager for UDP connections

- For each SIP entity in the sample configuration:
    - o Define SIP Entity
    - o Define Entity Links, which define the SIP trunk parameters used by Avaya Aura ™ Session Manager when routing calls to/from SIP Entities
    - o Define Routing Policies, which control call routing between the SIP Entities
    - o Define Dial Patterns

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.

Login with the appropriate credentials and accept the Copyright Notice.

Expand the **Network Routing Policy** Link on the left side of Navigation Menu. Select a specific item such as SIP Domains. When the specific item is selected, the color of the item will change to blue as shown below:



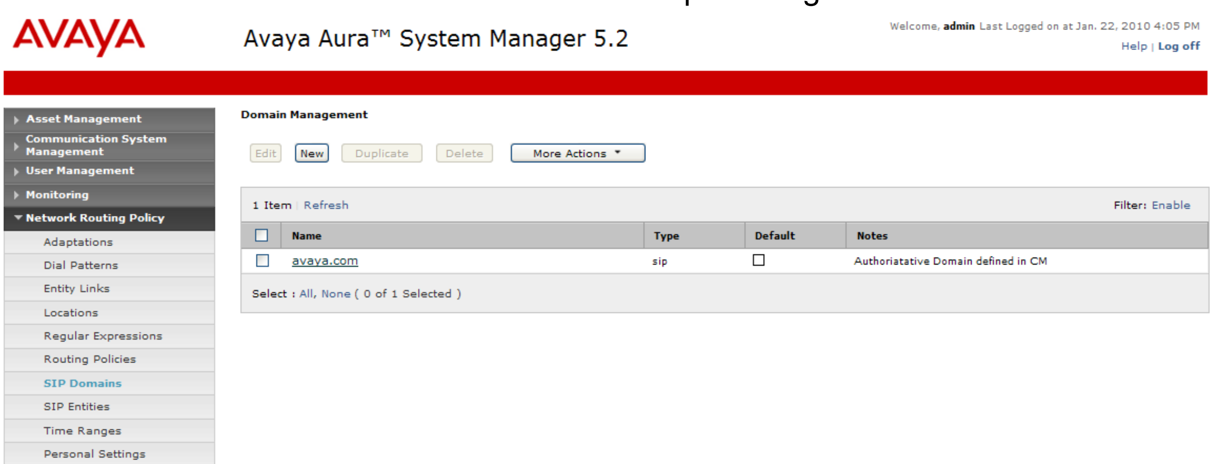
3.1. Administer SIP Domains

Expand Network Routing Policy and select **SIP Domains**.

- Click **New**
- In the *General* Section, under *Name,* enter the Authoritative Domain Name specified in **Section 2.3.**
- Under *Notes* add a brief description.

- Click **Commit** to save.

The screen below shows the information for the sample configuration.

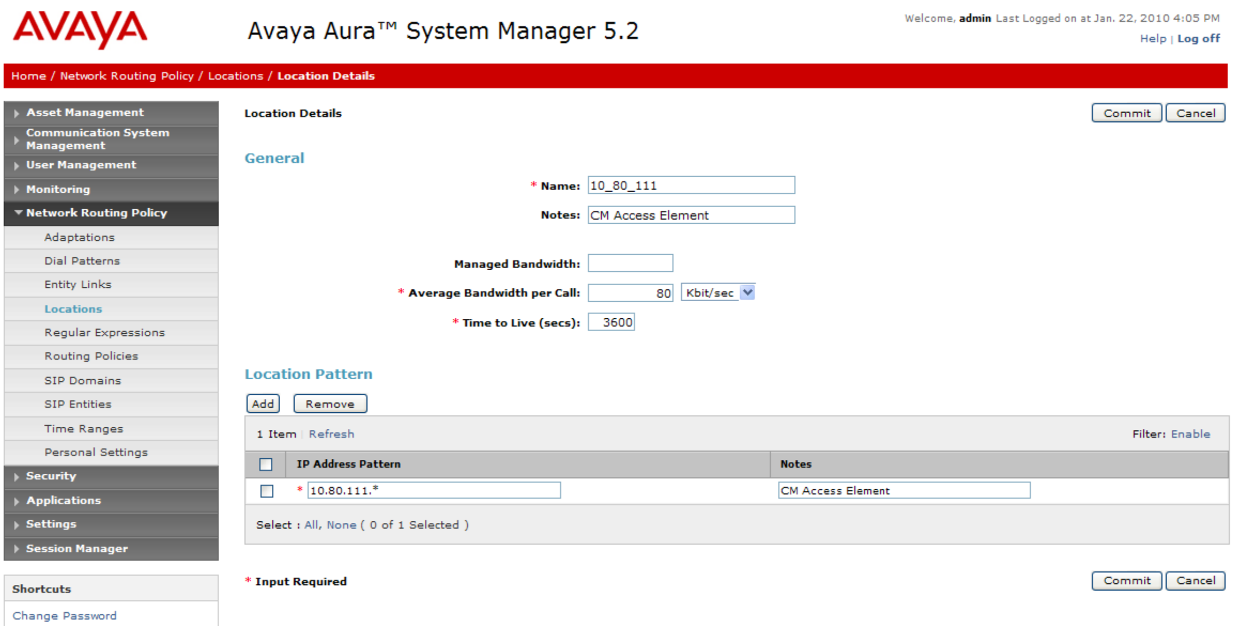


3.2. Define Locations

Expand Network Routing Policy and select **Locations.** Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

- Click **New**
- In the *General* Section, under *Name* add a descriptive name.
- In the *Location Pattern* Section, under the IP Address Pattern enter pattern used to logically identify the location
- Under *Notes* add a brief description.
- Click **Commit** to save.

The screen below shows the information for the Communication Manager Access Element in the sample configuration.



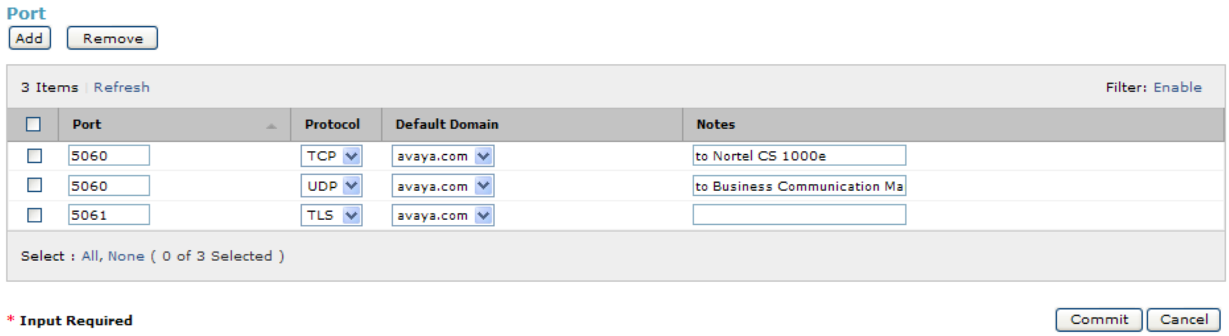
3.3. Specify Listen Port for UDP Connections

Since the Business Communication Manager only supports UDP connections, configure a listen port on the Avaya Aura™ Session Manager for UDP connections.

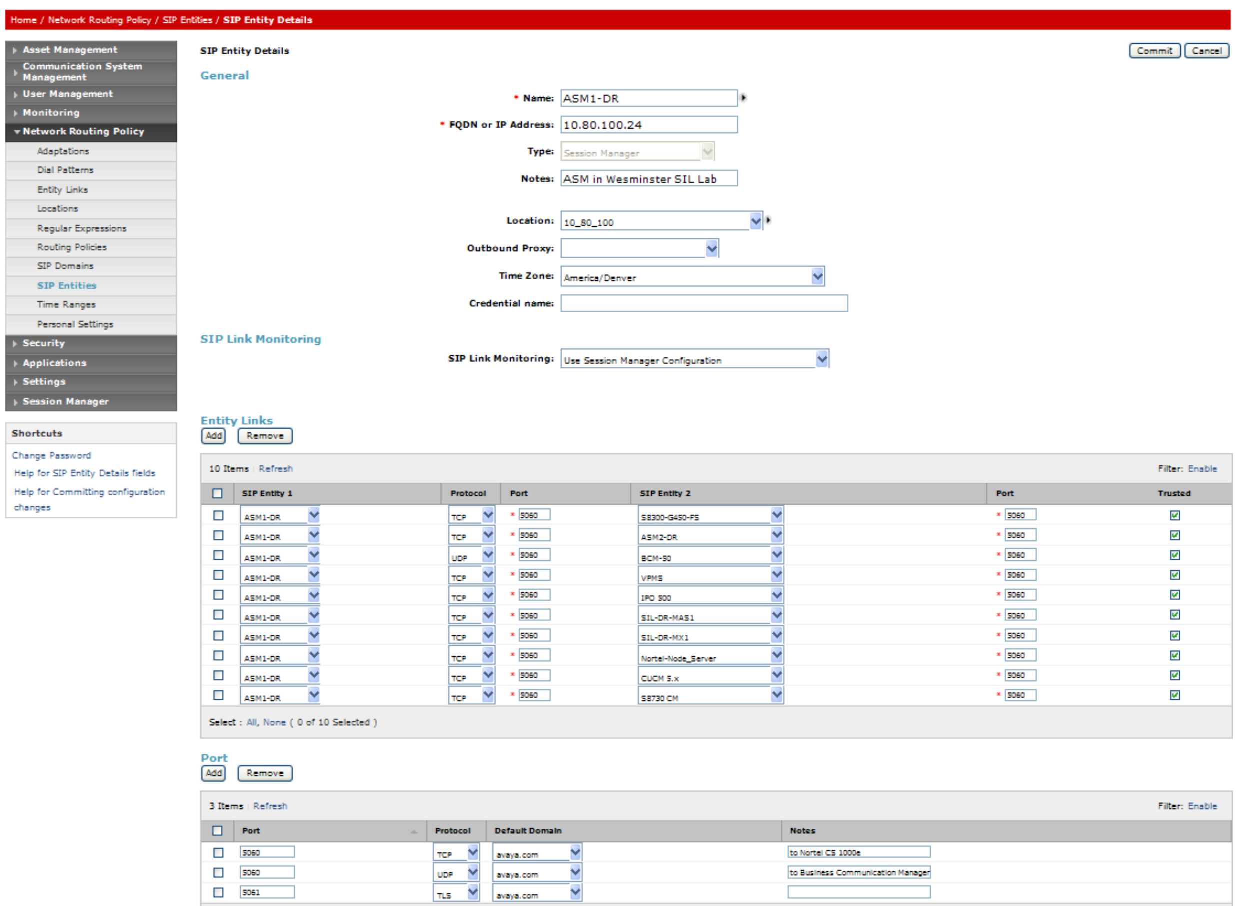
Expand Network Routing Policy and select **SIP Entities**

- Select the first Session Manager and Click **Edit**
- In the *Port* Section, Click **Add**
- Under *Port* , enter: "**5060**"
  Note: Session Manager is able to use the same port for both TCP and UDP connections.
- Under *Protocol*, select **UDP** from the drop-down menu
- Under *Default Domain*, select the domain name defined in **Section 3.1** from the drop-down menu.
  Important Note: the default domain for the listen port must be configured to use the domain name defined in **Section 3.1.**
- Under *Notes* add a brief description.

The following screen shows the addition of using port 5060 as the listen port for UDP connections:



The screen below shows the full screen defining the first Session Manager in the sample configuration:



3.4. Add Avaya Business Communication Manager 50

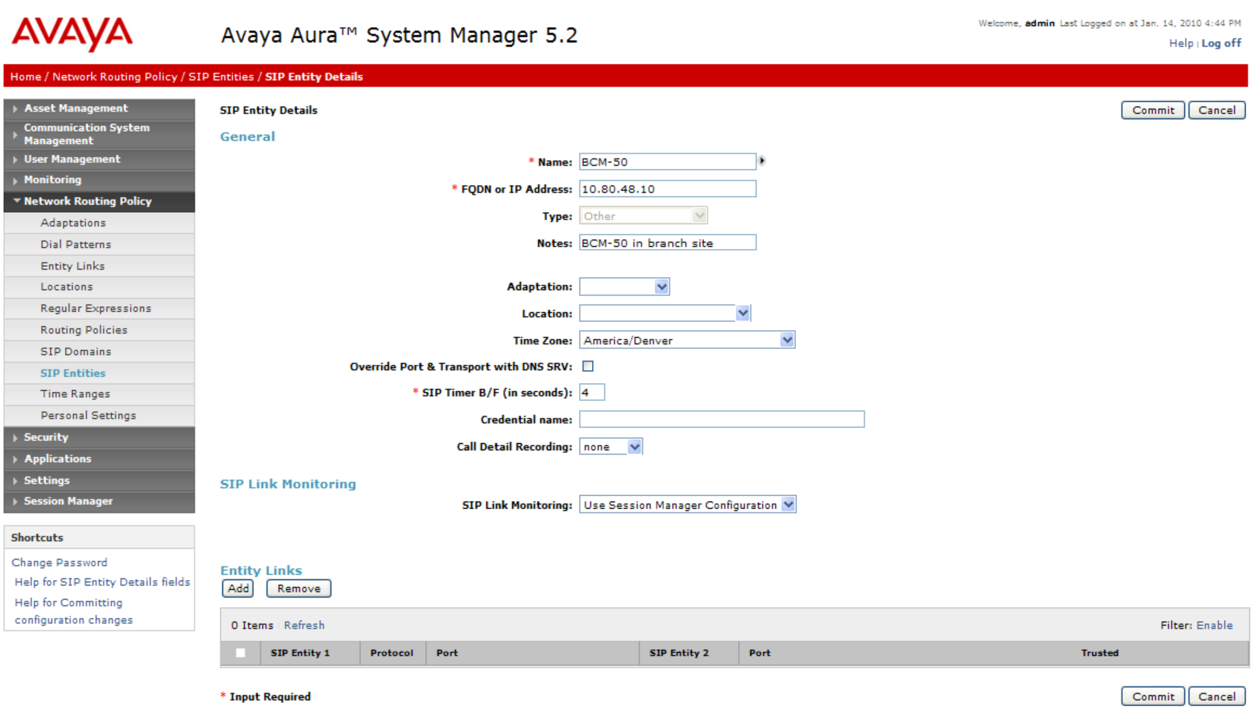
The following section captures relevant screens for configuring the Avaya Business Communication Manager 50 applicable for the sample configuration.

3.4.1. Define SIP Entity

Expand Network Routing Policy and select **SIP Entities**

- Click **New**
- In the *General* Section, under *Name* add an identifier for the Business Communication Manager.
- Under *FQDN or IP Address* enter the IP address of the Business Communication Manager 50 server.
- Under *Type* select Other.
- Under *Notes* add a brief description.
- *Location:* select the Location added in **Section 3.2** from the drop-down menu.
  Note: since location-based routing was not used in the sample configuration, selecting a value for location field is optional.
- Click **Commit** to save.

The following screen shows addition of Business Communication Manager 50. The IP address used is the IP address of the Business Communication Manager server.



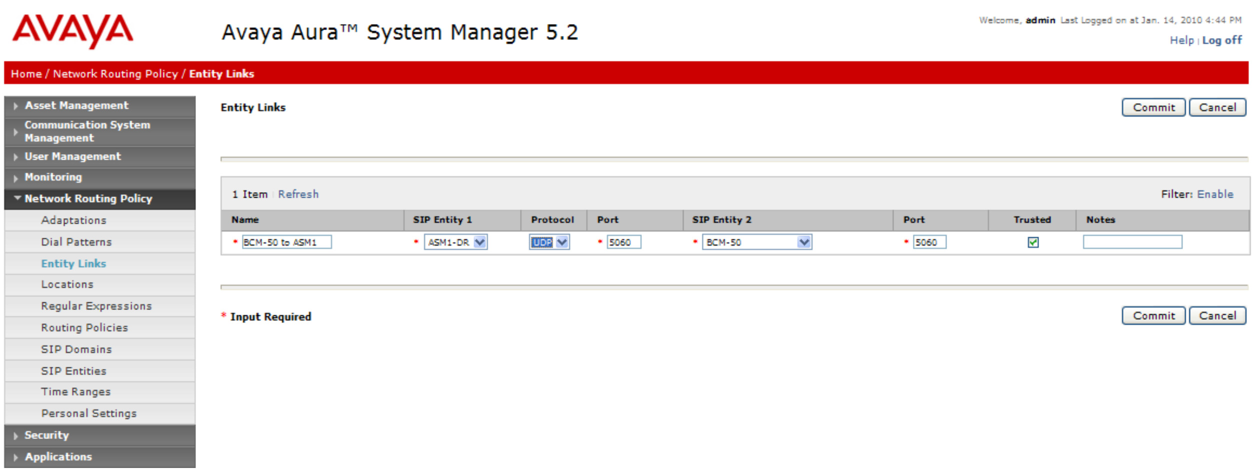
3.4.2. Define Entity Links

Expand Network Routing Policy and select **Entity Link**

- Click **New**
- Under *Name,* enter an identifier for the link to the Business Communication Manager.
- Under *SIP Entity 1,* select the first Session Manager from the drop-down menu
- Under *SIP Entity 2,* select the SIP Entity added for the Business Communication Manager in **Section 3.4.1** from the drop-down menu.

- After selecting both SIP Entities, select *UDP* as the required protocol from the *Protocol* drop-down menu. Verify port for both SIP entities is the default listen port specified in **Section 3.3.**
- Under *Notes* add a brief description.
- Click **Commit** to save.

The following screen shows the entity link defined for the Business Communication Manager.



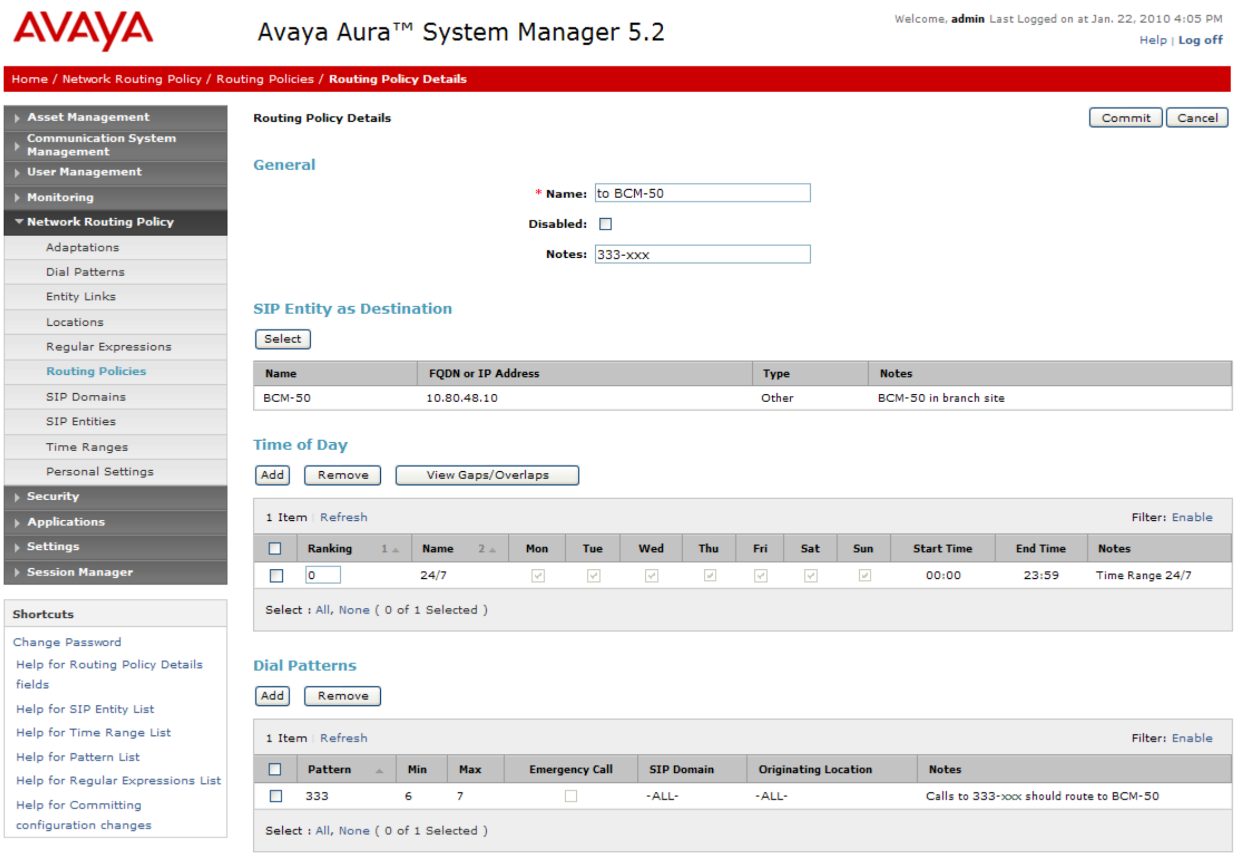
3.4.3. Define Routing Policy

Expand Network Routing Policy and select **Routing Policies**

- Click **New**
- In the 'General' section, under Name add an identifier to define the routing policy for the Business Communication Manager
- Under *Notes* add a brief description.
- In the 'SIP Entity as Destination' section, click on **Select**.
- The SIP Entity List page opens.
  Select the entry of the Business Communication Manager added in **Section 3.3.2** and click on **Select**
- The selected SIP Entity displays on the Routing Policy Details page.
- Click on **Commit** to save.

The following screen shows the routing policy defined for routing calls to the Business Communication Manager.

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.



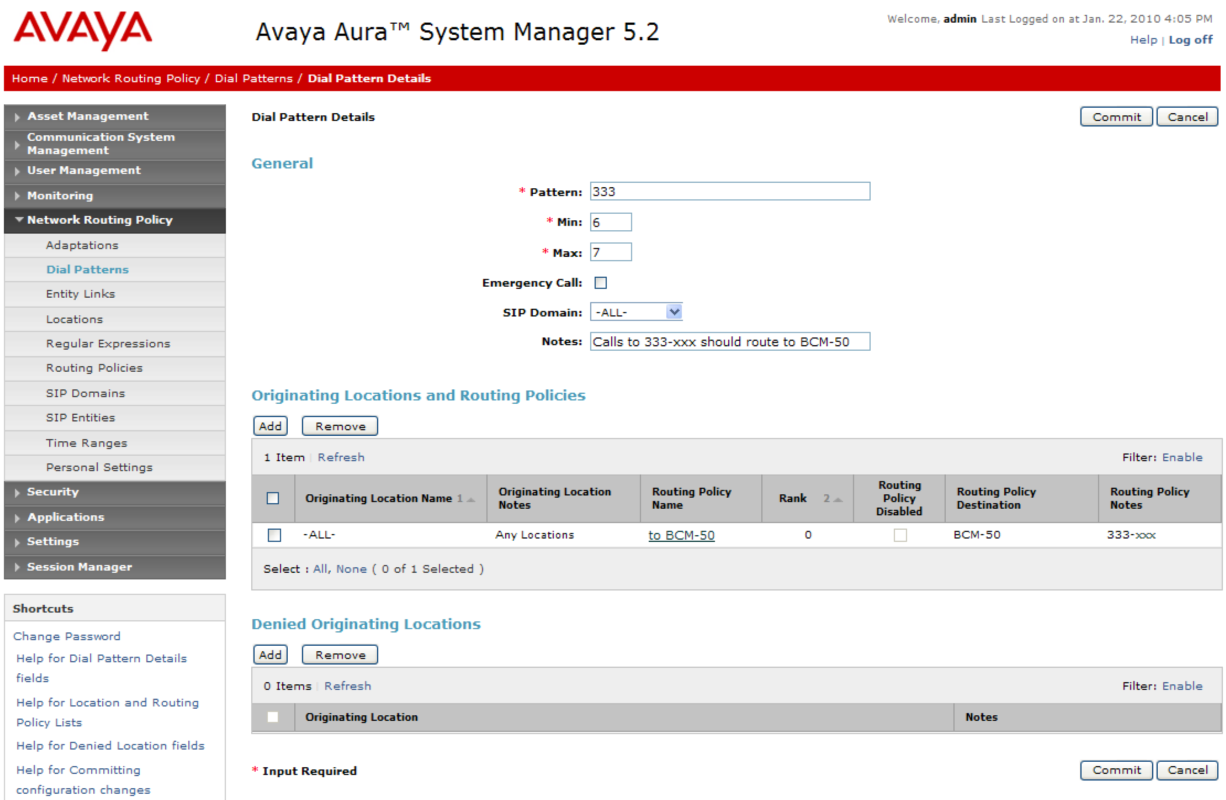
3.4.4. Define Dial Plan

Expand **Network Routing Policy and select Dial Patterns**

- Click **New**
- In the 'General' section, under *Pattern* add dial patterns for any extension numbers associated with stations on the Business Communication Manager. Under *Min* enter the minimum number digits that must to be dialed. Under *Max* enter the maximum number digits that may be dialed.
- Under SIP Domain drop-down, select the SIP Domain added in **Section 3.1** or select "All" if Session Manager should be able to accept incoming calls from all SIP domains.
- Under *Notes* add a brief description.
- In the 'Locations and Routing Policies' section click on **Add**
  - The 'Locations and Routing Policy List' page opens.
  - Under Locations, select the desired location.

- Under Routing Policies, select the one defined for Business Communication Manager in **Section 3.3.2** and click on **Select**.

The following screen shows the dial pattern defined for routing calls to the Business Communication Manager.



3.5. Add Avaya Aura^{TM} Communication Manager Access Element

The following section captures relevant screens for configuring Avaya Aura^{TM} Communication Manager Access Element applicable for the sample configuration.

In addition to the steps described in this section, other administration activities will be needed to connect the Communication Manager Access Element to both Session Managers to support failover testing.

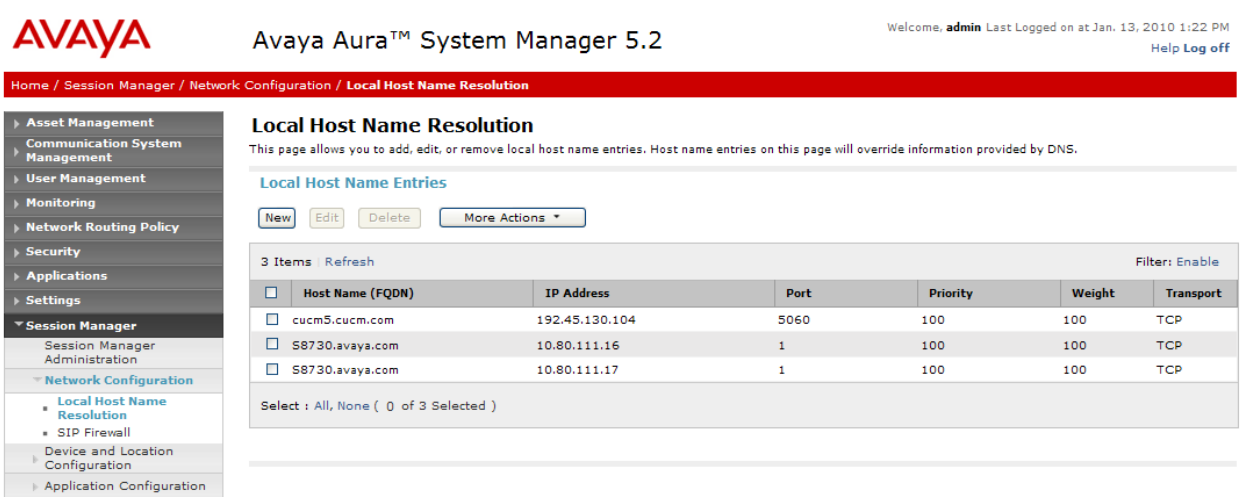
For more information on these additional administration activities, see References in **Section 9.**

3.5.1. Define Local Host Resolution Name

Since there will be multiple entities links between the Avaya Aura™ Communication Manager Access Element and Avaya Aura™ Session Manager, a FQDN should be defined for the Communication Manager Access Element to enable Session Manager to resolve multiple IP addresses for this SIP Entity.

- Expand **Network Configuration** under **Session Manager**
  - **Select Local Host Name Resolution**
    - Click **New**
    - Under *Name,* enter the FQDN name for the Communication Manager Access Element.
    - Under IP address, enter the IP address for one of the CLAN boards on the Communication Manager Access Element.
    - Repeat for the second CLAN board on the Access Element

The following screen shows addition of the Local Host Resolution Name for the Communication Manager Access Element in the sample configuration.

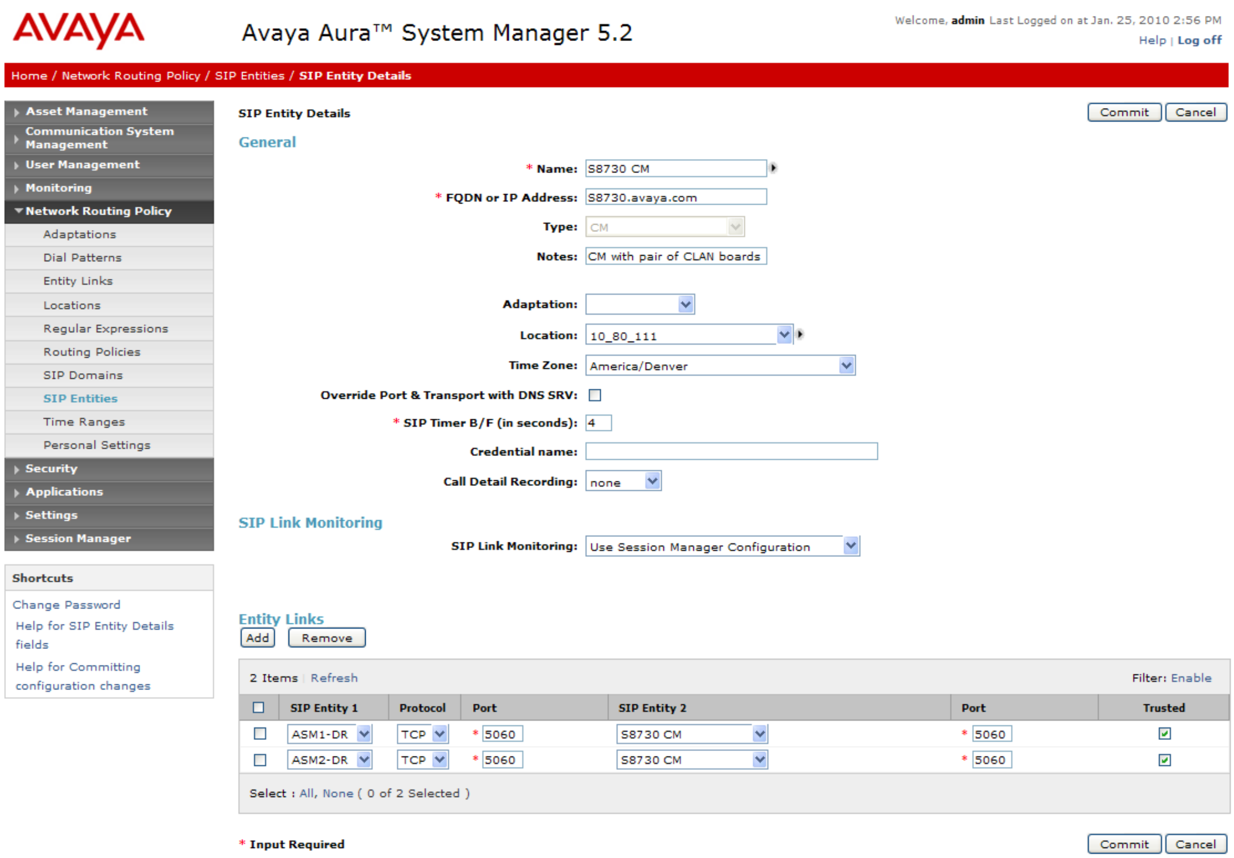


3.5.2. Define SIP Entity

- Expand Network Routing Policy and select **SIP Entities**
  - Click **New**
  - In the *General* Section, under *Name* add an identifier for the Avaya Aura™ Communication Manager Access Element.
  - Under *FQDN or IP Address,* enter the FQDN defined for the Communication Manager Access Element in **Section 3.5.1.** Under *Type* select CM. Under *Notes* add a brief description.
  - Click **Commit** to save.

Note: there are two Entity Links defined for the Communication Manager Access Element to support failover testing. For more information on the configuration of multiple Session Managers to support failover testing, see References in **Section 9.**

The following screen shows the SIP entity for the Communication Manager Access Element.

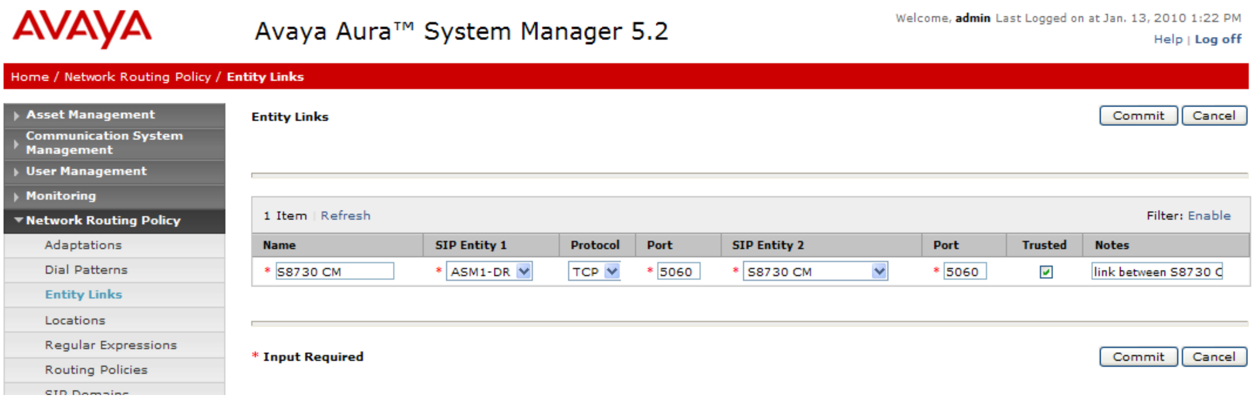


3.5.3. Define Entity Link

Expand **Network Routing Policy** and select **Entity Links**

- Click **New**
- Under *Name,* enter an identifier for the Access Element.
- Under *SIP Entity 1,* select the first Session Manager
- Under *SIP Entity 2,* select the SIP Entity added in **Section 3.5.2** for the Access Element. Select it as a *Trusted* host.
- After both SIP Entities have been selected, Modify *Protocol* field if necessary by selecting TCP from drop-down menu.
- Under *Notes* add a brief description.
- Click **Commit** to save.

The following screen shows the Entity Link defined for the Communication Manager Access Element.

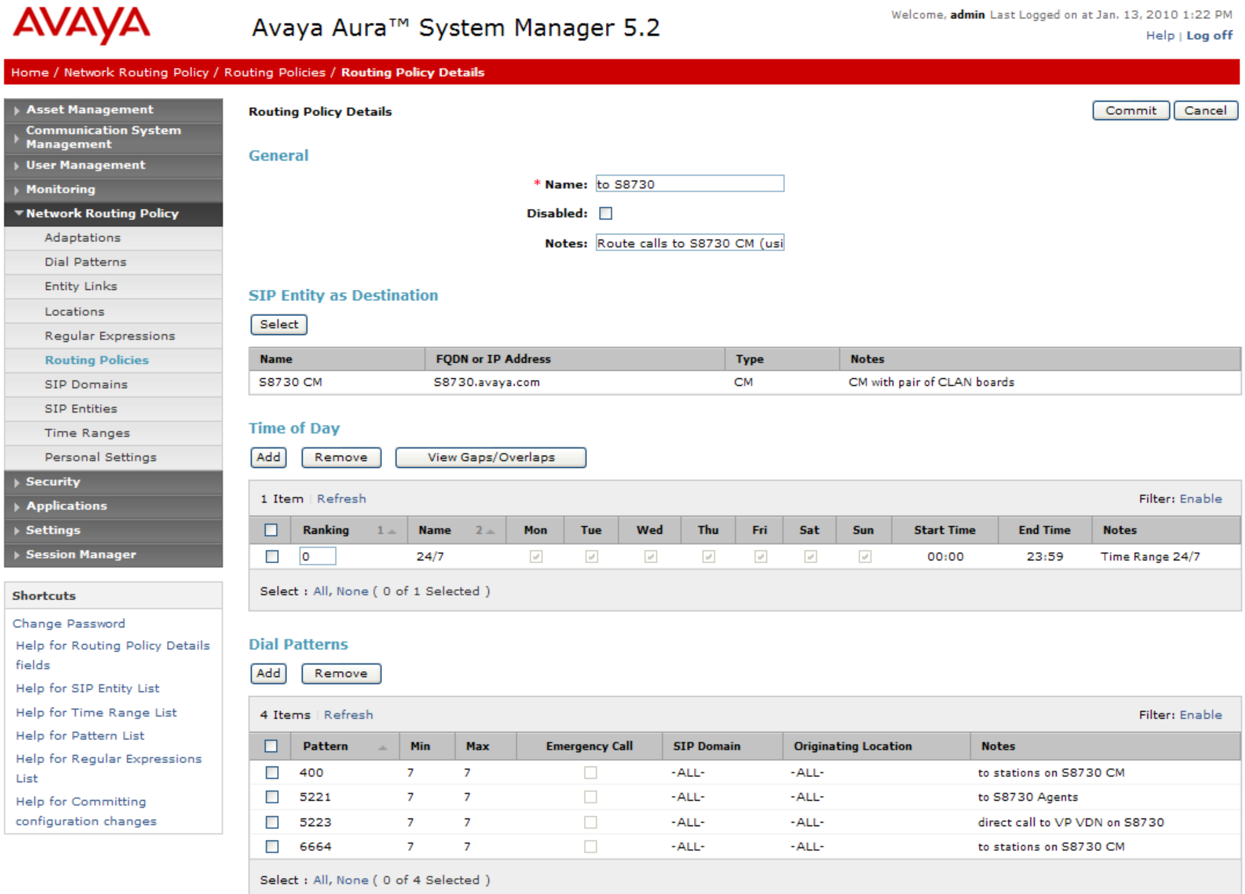


3.5.4. Define Routing Policy

Expand **Network Routing Policy** and select **Routing Polices**

- Click **New**
- In the 'General' section, under Name add an identifier for the Communication Manager Access Element.
- Under *Notes* add a brief description.
- In the 'SIP Entity as Destination' section, click on **Select**.
- The SIP Entity List page opens.
  Select the SIP Entity added in **Section 3.5.2** for the Communication Manager Access Element.
- Click on **Commit** to save.

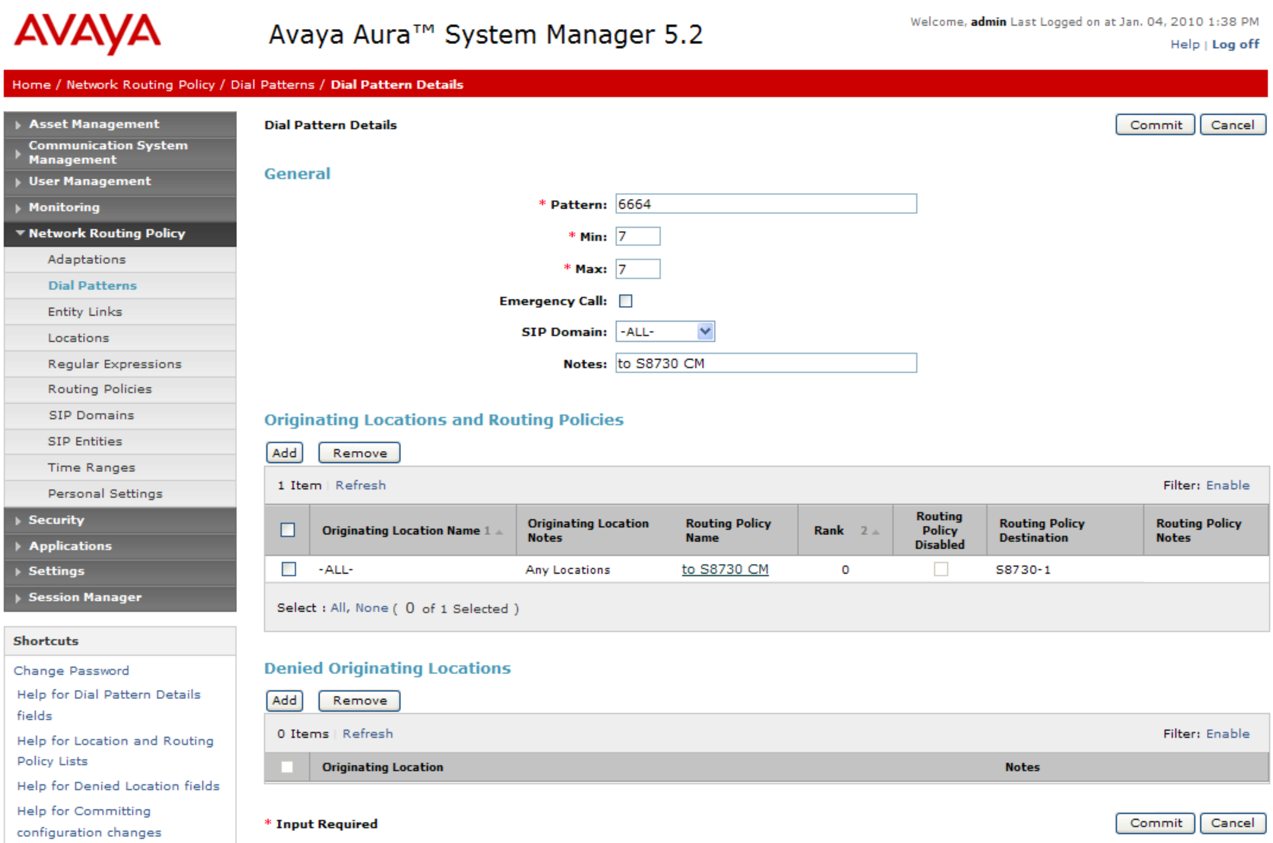
Shown below is the updated screen defining the Routing Policy for the sample configuration.



3.5.5. Define Dial Plan

- Expand **Network Routing Policy** and select **Dial Patterns**
    - o Click **New**
    - o In the 'General' section, under *Pattern* add the dial patterns associated with extensions on the Communication Manager Access Element.
    - o Under *Min* enter the minimum number digits that must to be dialed.
    - o Under *Max* enter the maximum number digits that may be dialed.
    - o Under SIP Domain, select the SIP Entity added in **Section 3.5.2.**
    - o Under *Notes* add a brief description.
        - ▪ In the 'Locations and Routing Policies' section click on **Add**
            - The 'Locations and Routing Policy List' page opens.
            - Note: since location-based routing was not used in the sample configuration, selecting a value for location field is optional.
        - ▪ Under Routing Policies, select the one defined for Communication Manager Access Element in **Section 3.5.4** and click on **Select**.

Shown below is the updated screen for the sample configuration.



3.6. Add Avaya Aura^{TM} Communication Manager Feature Server

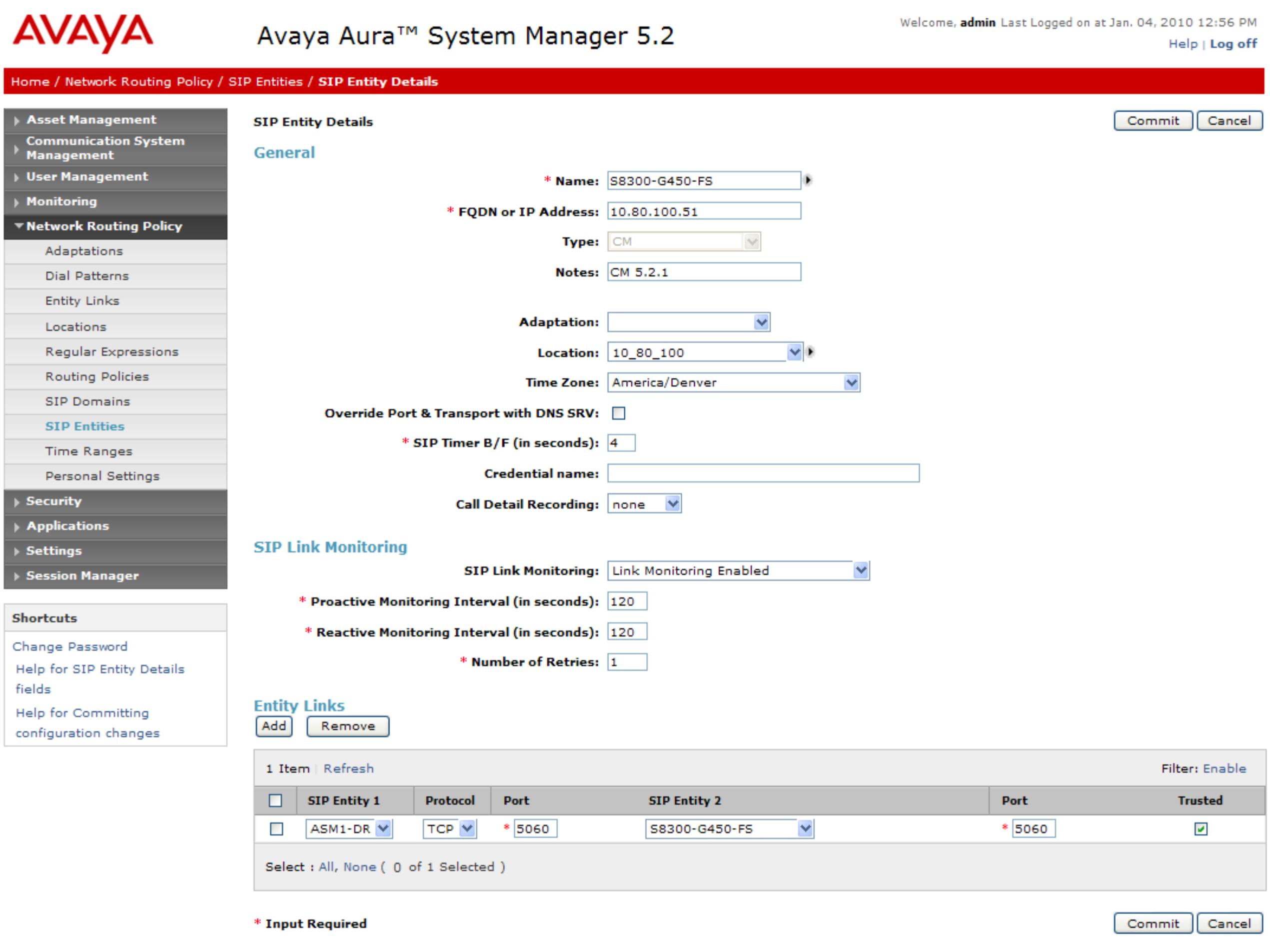
The following section captures relevant screens for configuring Avaya Aura^{TM} Communication Manager Feature Server to enable registered SIP users to make or receive calls from stations on the Business Communication Manager.

In addition to the steps described in this section, other administration activities will be needed such as defining an Application Sequence for the Feature Sequence or adding new SIP users.

For more information on these additional administration activities, see References in **Section 9.**

3.6.1. Define a SIP Entity and Entity Link

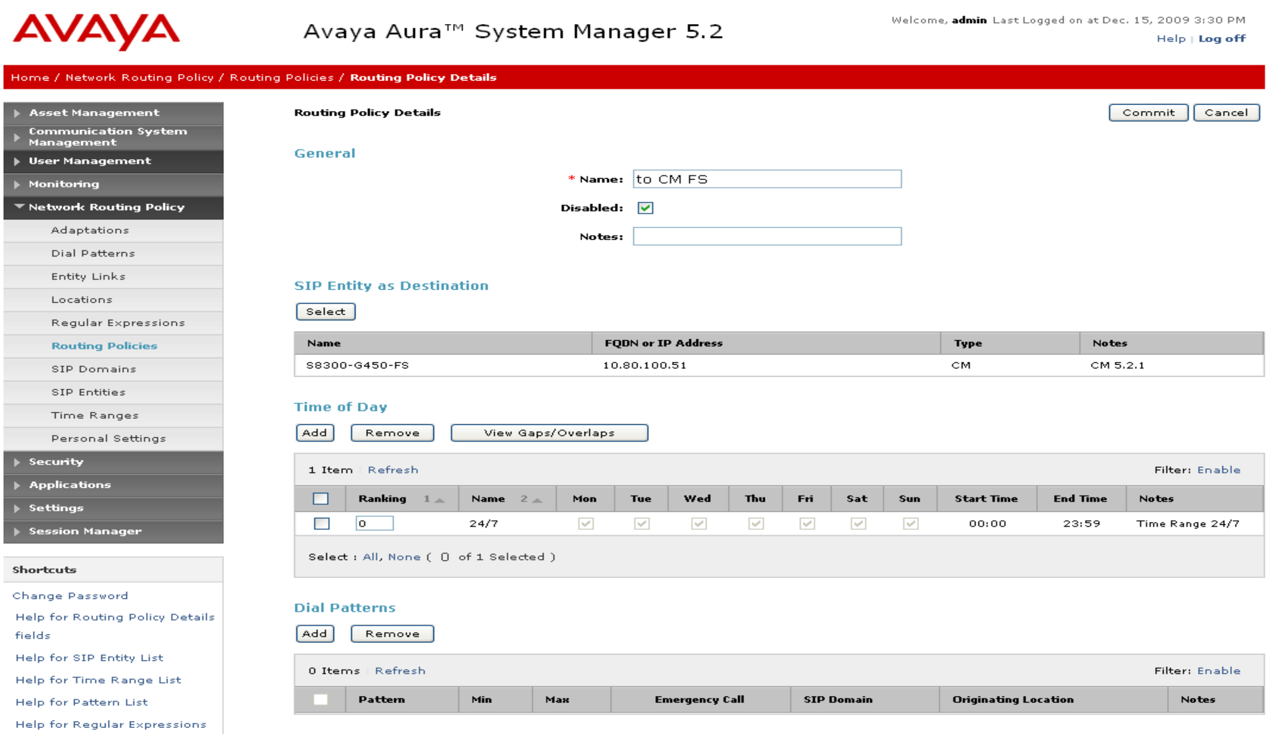
The following screen shows the addition of Communication Manager Feature Server and associated entity link for the sample configuration. The IP address used is that of the S8300C server.



3.6.2. Define Routing Policy

Since the SIP users are registered on Session Manager, the routing policy defined for the Communication Manager Feature Server does not need to include any dial patterns.

The following screen shows the Routing Policy defined for the Communication Manager Feature Server:



4. Configure Avaya Business Communication Manager 50

This section describes the relevant configuration of the Business Communication Manager 50 used to verify these Application Notes. Please consult the product documentation referenced in **Section 9** for additional information.

The Business Communication Manager is configured using the Element Manager GUI.

4.1. Administrator Applications Web Page

During the installation and initial configuration phase, the installation technician should first connect to the OAM IP port on the Business Communication Server. For more information, see the product installation documentation referenced in **Section 9.**

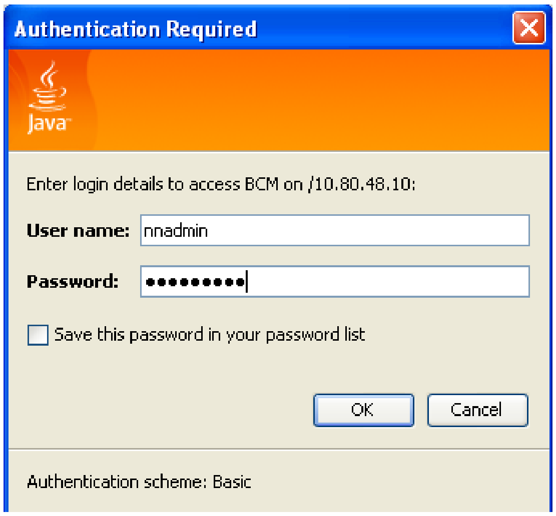
Open an Internet Explorer (IE) browser window and use the default OAM OP address of the Business Communication Manager server to open the Business Communication Manager Administrator Applications web page.

The default OAM address is: http://10.10.11.1

Note: after the system is configured with the appropriate IP settings for the customer LAN described in **Section 4.6**, the url to open the applications web page will be the IP address of the Business Communication Server.

Wait for several seconds while the application web page begins to download.

Enter the default **User name:** *nnadmin* and **Password**: *PlsChgMe!* in the Authentication dialog box as shown below:



After successful login, the following Welcome screen will be displayed:

4.2. Run Element Manager Application and Login

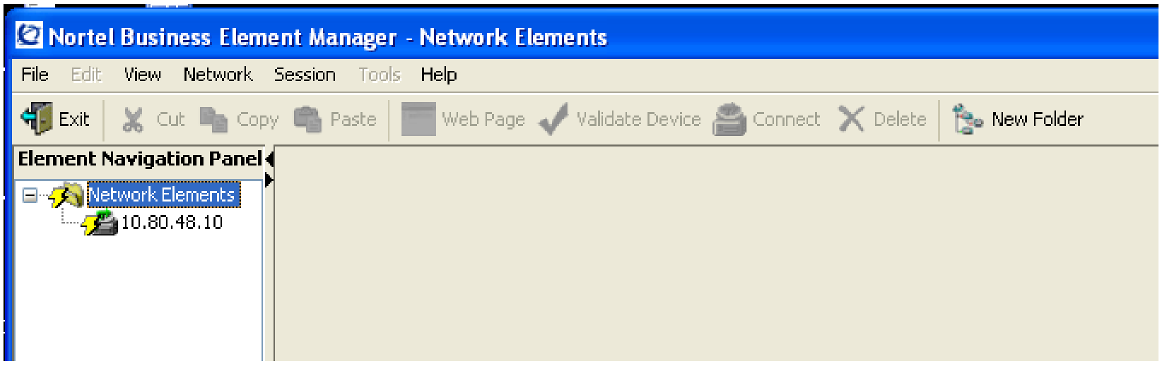
Select the Business Element Manager from the BCM applications list and select Run button to download the application to the desktop.

Wait for several seconds while the Element Manager application downloads. Enter the default user name and password to log into the Element Manager.

Select the **Confirm** button to acknowledge the copyright notice.

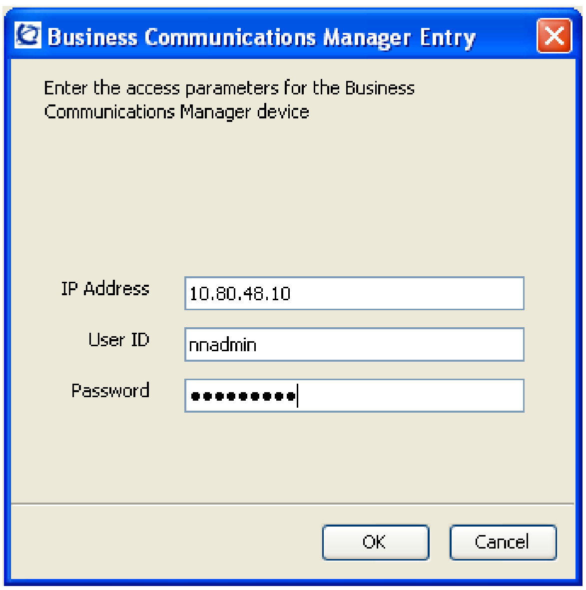
4.3. Add Business Communication Manager as an Element

After successful login, right click on the **Network Elements** folder in the **Element Navigation Panel** as shown below:

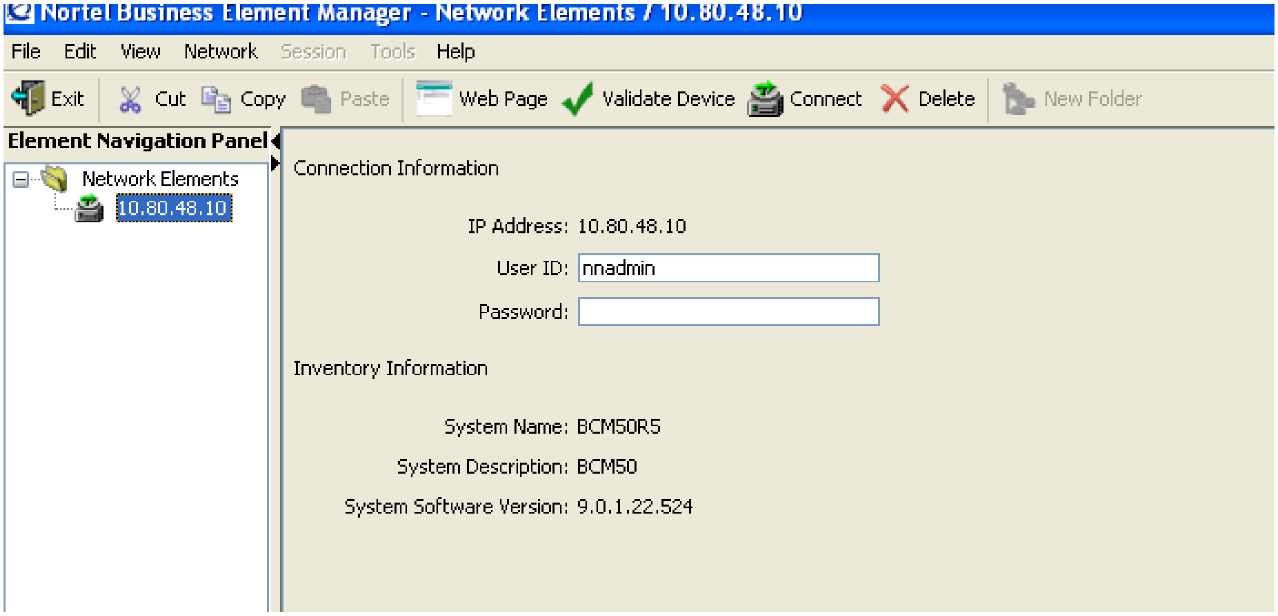


Select **New Network Element→** from the first drop-down menu and select **Business Communication Manager** from the second drop-down menu.

Enter **IP address** for the Business Communication Manager server and the default **User ID** and **Password** in the *Add Element* dialog as shown below and select OK:



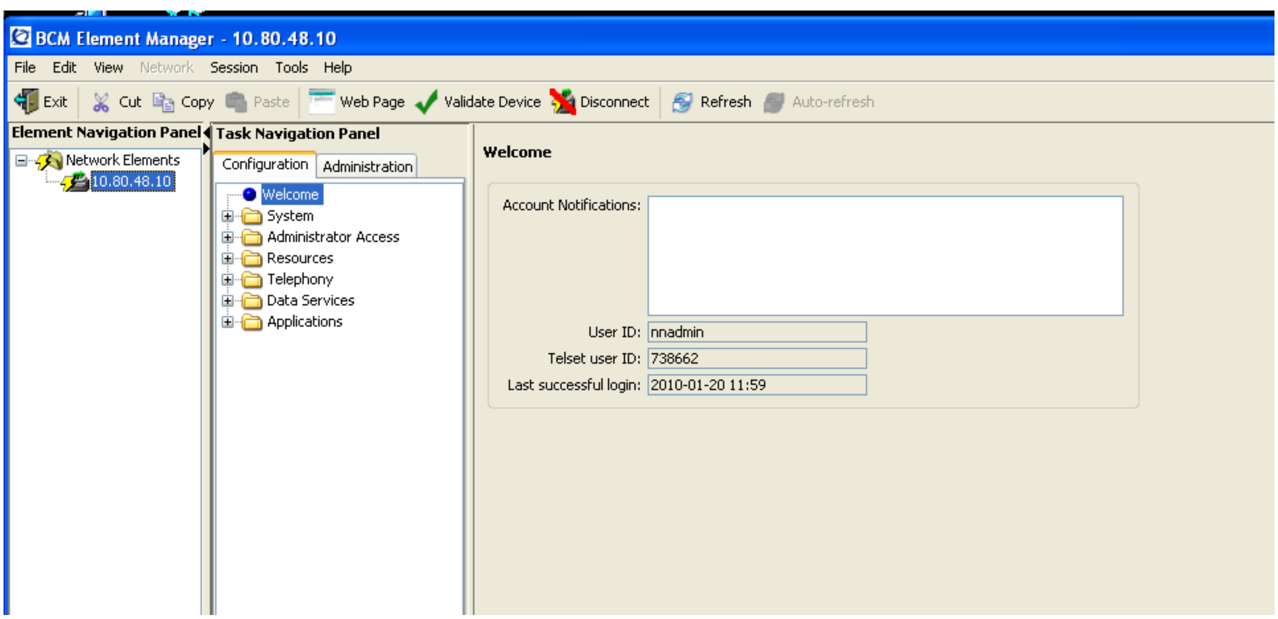
Details of the Business Communication Manager server is displayed as shown below:



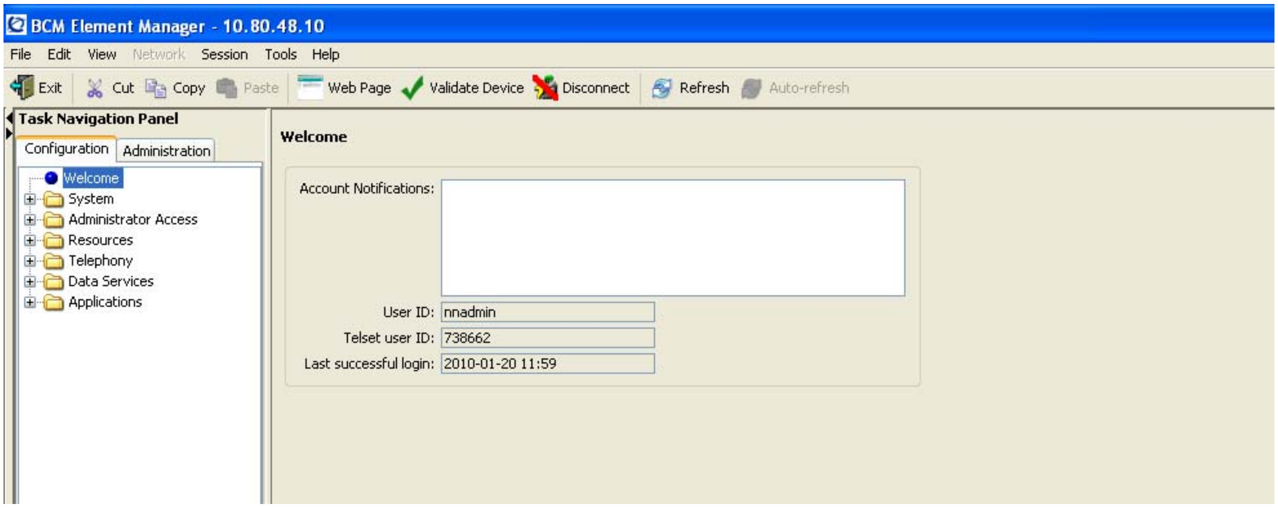
Finally, to connect to the BCM server, enter the default **Password** in the screen shown above and select the **Connect** button in the Toolbar.

4.4. Navigation

The following screen shows the initial Element Manager screen.



Note: If the Element Manager GUI is being used to configure a single Business Communication Manager server, click on the arrow in the upper right of the **Element Navigation Panel** to hide this panel as shown below:

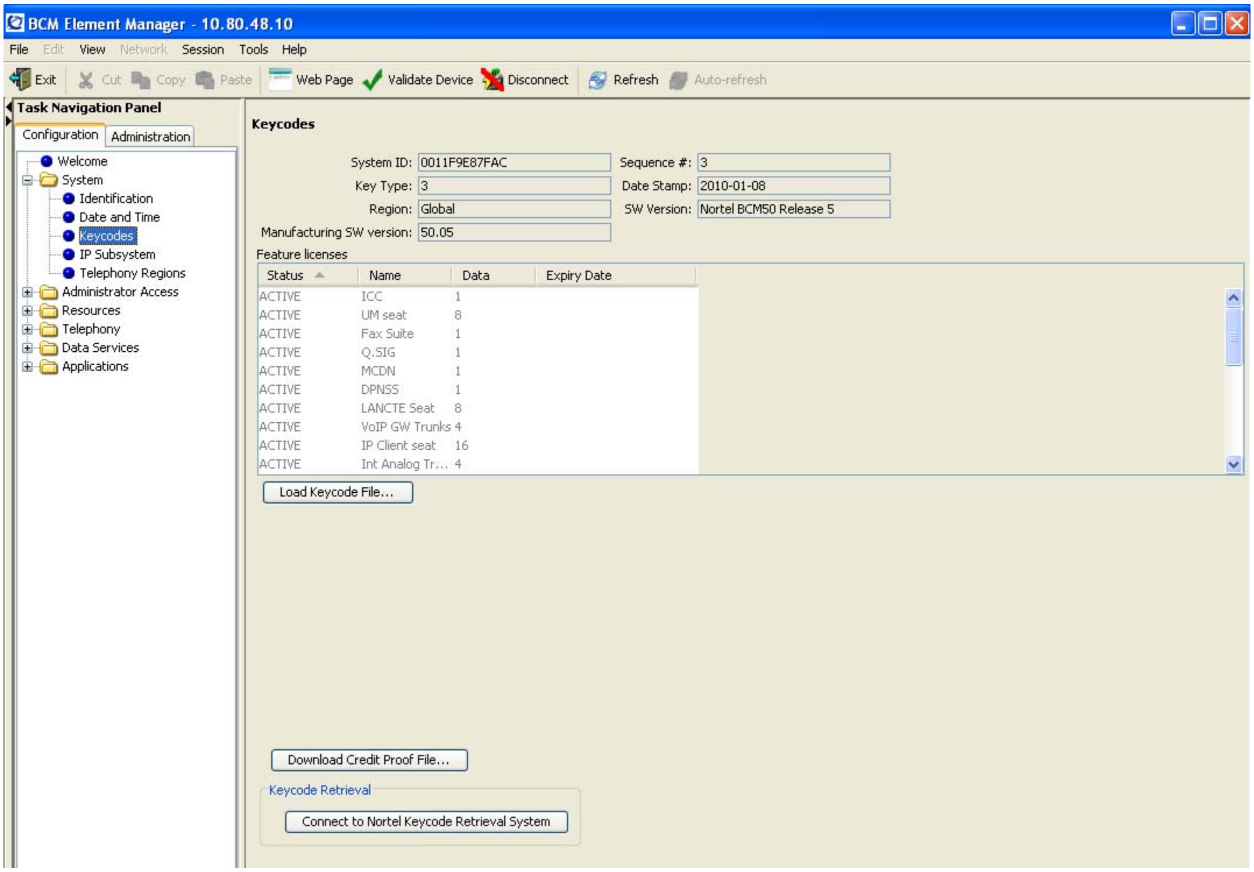


Use the **Task Navigation Panel** to navigate to specific configuration tasks.

4.5. Verify Licensing

This section describes the procedure to verify the correct system licensing has been configured on the Business Communication Manager. If there is insufficient capacity or a required features is not available, contact an authorized Avaya sales representative to make the appropriate changes.

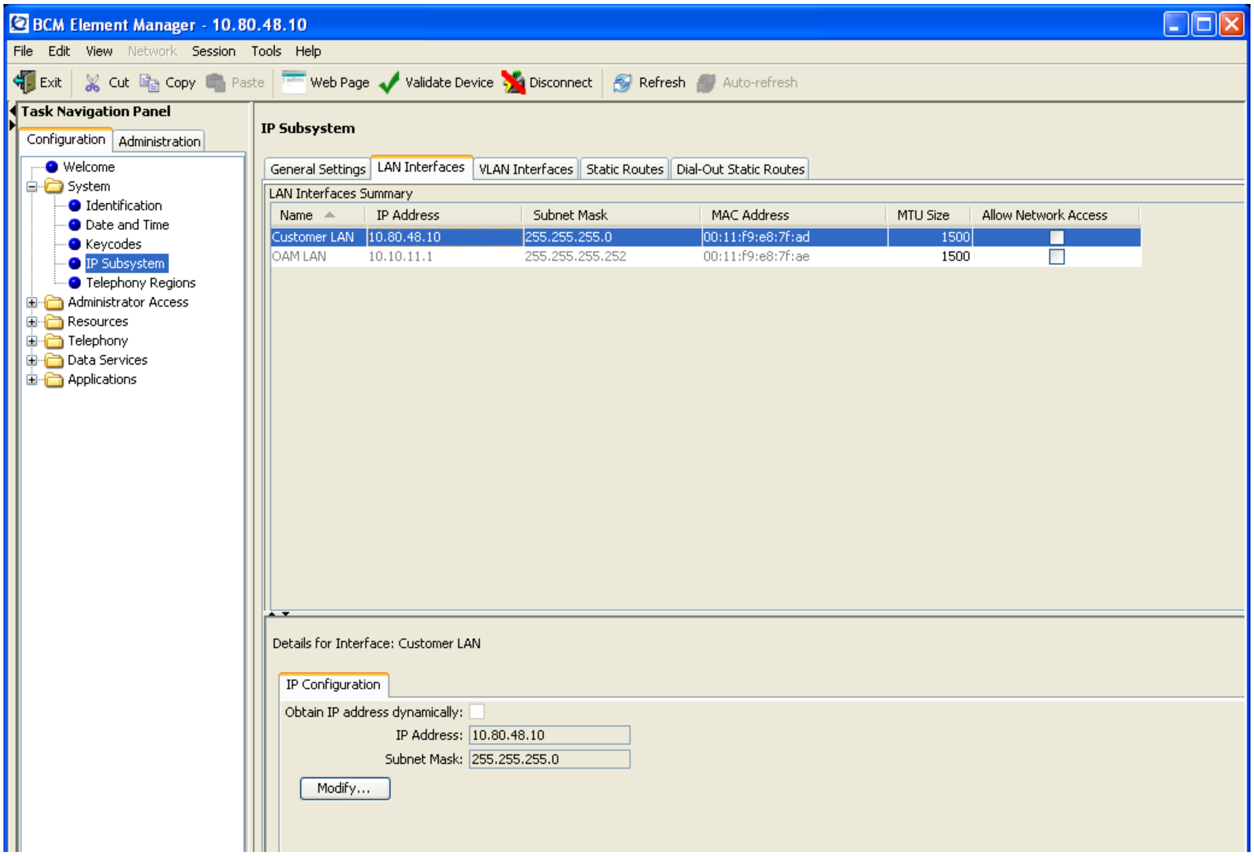
Navigate to **System → Keycodes** task in the **Task Navigation Panel**. Verify the system has sufficient licenses for IP stations and VoIP Trunks as shown below:



4.6. Configure IP Settings

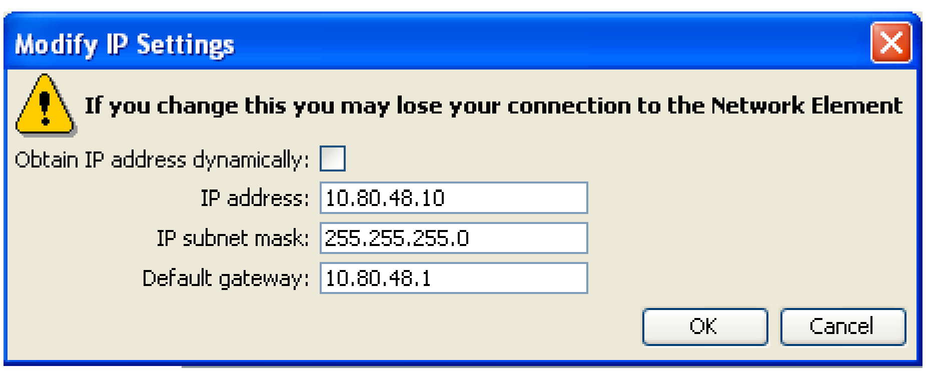
Navigate to **System → IP Subsystem** task in the **Task Navigation Panel**.

Under the *LAN Interfaces* tab, select the **Customer LAN** row in the *LAN Interface Summary* table as shown below:



Select the **Modify** button in the *IP Configuration* tab under the *Details* section of the screen to modify the IP address of the Business Communication Manager Server.

Enter the IP address for the Business Communication Manager Server and default gateway in the **Modify IP Settings** dialog as shown below:

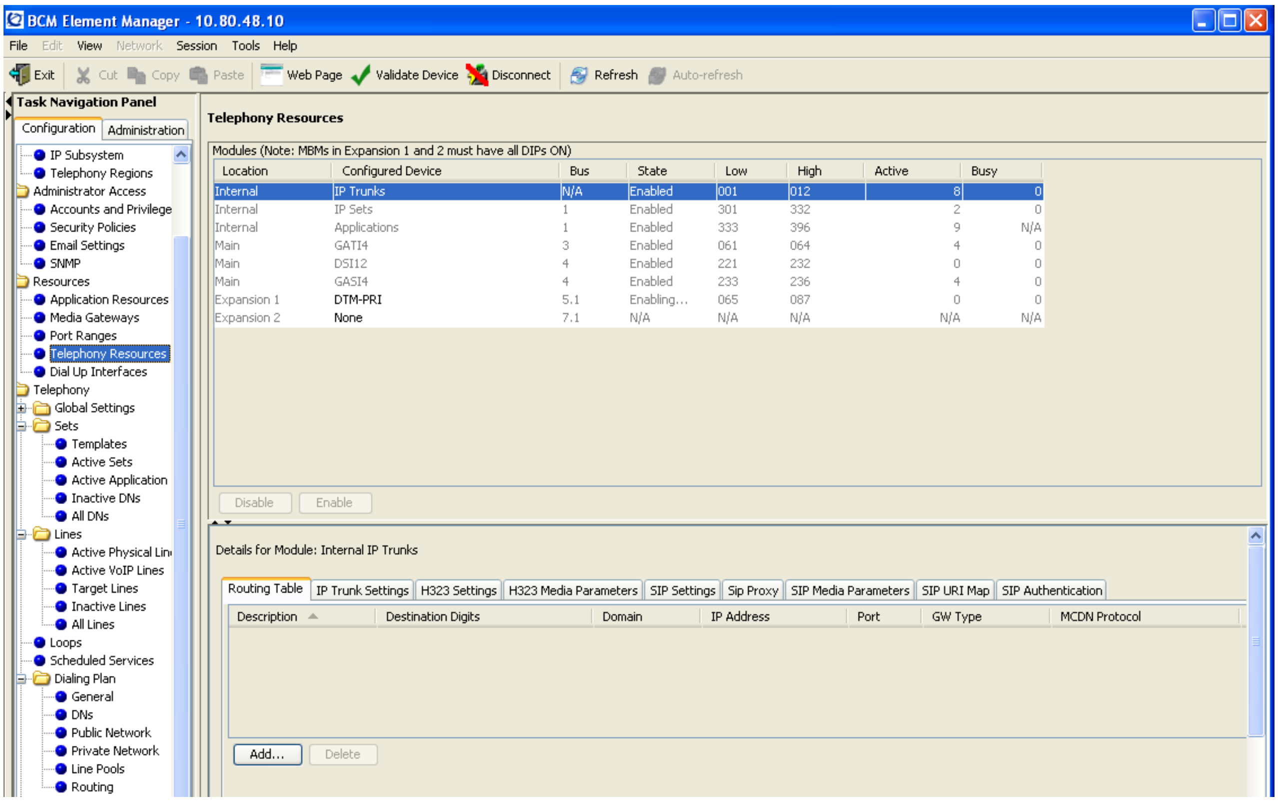


Select OK to save the changes. Note: after confirming this change, a re-login is required.

4.7. Add SIP Trunk to Avaya Aura™ Session Manager

Navigate to **Resources → Telephony Resources** task in the **Task Navigation Panel.**

Select the **IP Trunks** row in the *Telephony Resources* table. Wait for several seconds for the configuration details of IP Trunks to be displayed in the lower section of the screen as shown below:



4.7.1. Configure Routing for SIP Trunks

Under the *Routing Table* tab, select the **Add** button to add a SIP Trunk to Avaya Aura™ Session Manager[4].

Enter the following values in the **Add Remote Gateway** dialog:

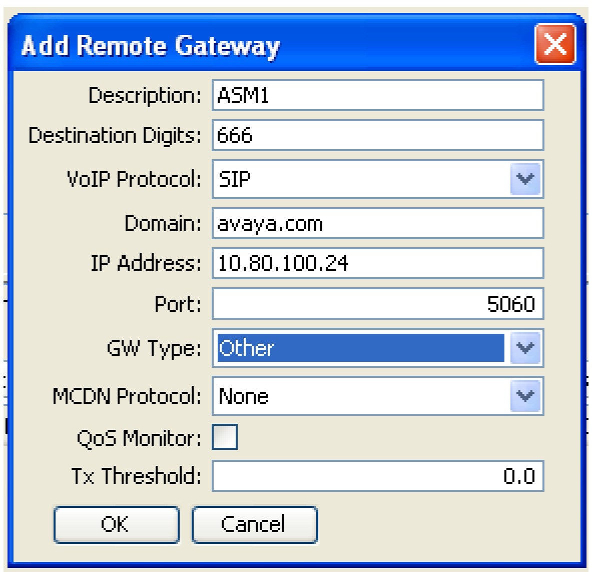
- **Description**: Enter a logical name for the trunk destination
- **Destination Digits**: Enter the set of digits or dial pattern to identify which outgoing calls should be routed to Session Manager.
- **VoIP Protocol**: select "SIP" from drop-down menu.

---

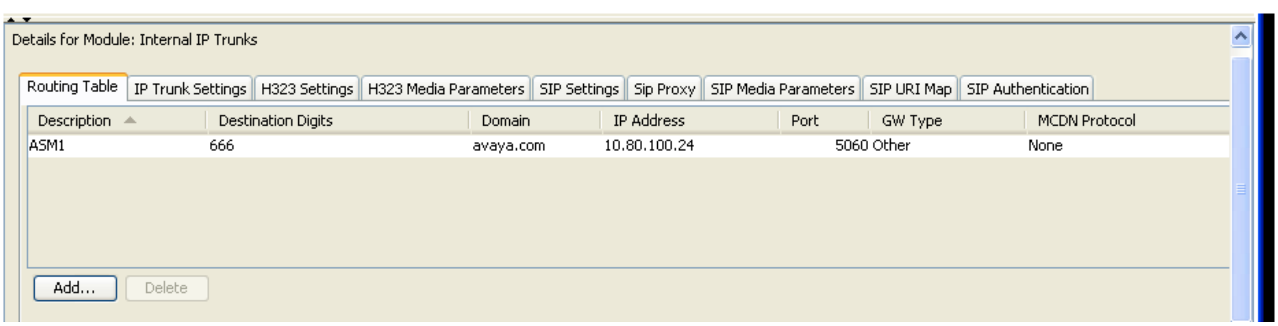
[4] Note: detailed administration of multiple Avaya Aura™ Session Managers and multiple SIP trunks on Business Communication Manager to support failover testing will not be described (see the appropriate documentation listed in **Section 9**).

- **Domain**: enter the same SIP Domain name as defined for Session Manager in **Section 3.1**.
- **IP Address**: enter the IP address associated with the SM-100 card for the first Session Manager
- **Port**: enter the UDP port number to which Business Communication Manager will send SIP messages. This value should match the value defined for UDP connections on Session Manager in **Section 3.3.**
- **GW Type**: select "Other" from the drop-down menu
- **MCDN Protocol**: select "None" from the drop-down menu
- **QoS Monitor**: Leave unchecked
- **Tx Threshold**: Leave this field at its default value of 0.0

The following dialog shows the values entered for the sample configuration.

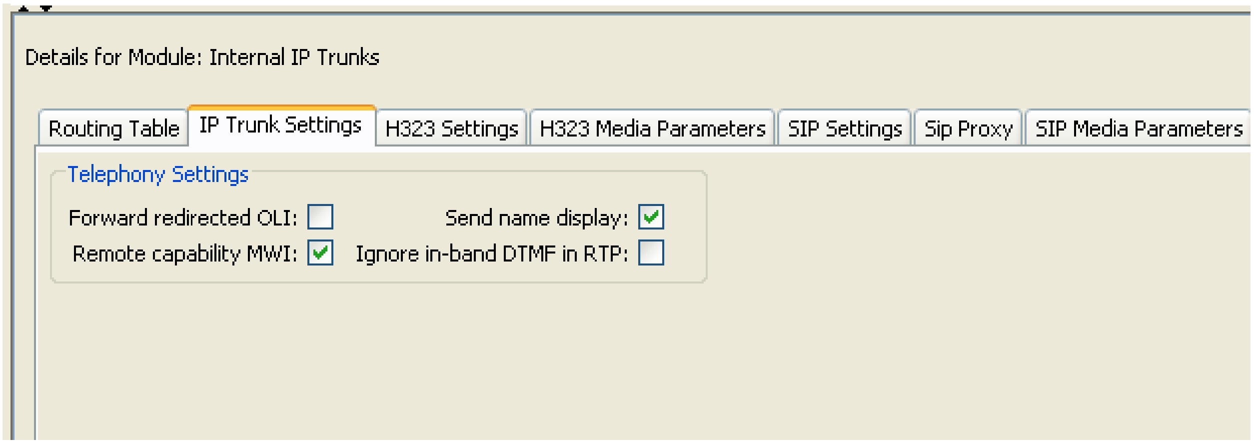


Select OK. The following screen shows the details of the *Routing Table* for the sample configuration:



4.7.2. Configure IP Trunk Settings

Under the *IP Trunk Settings* tab, verify **Send name display** is checked as shown below:

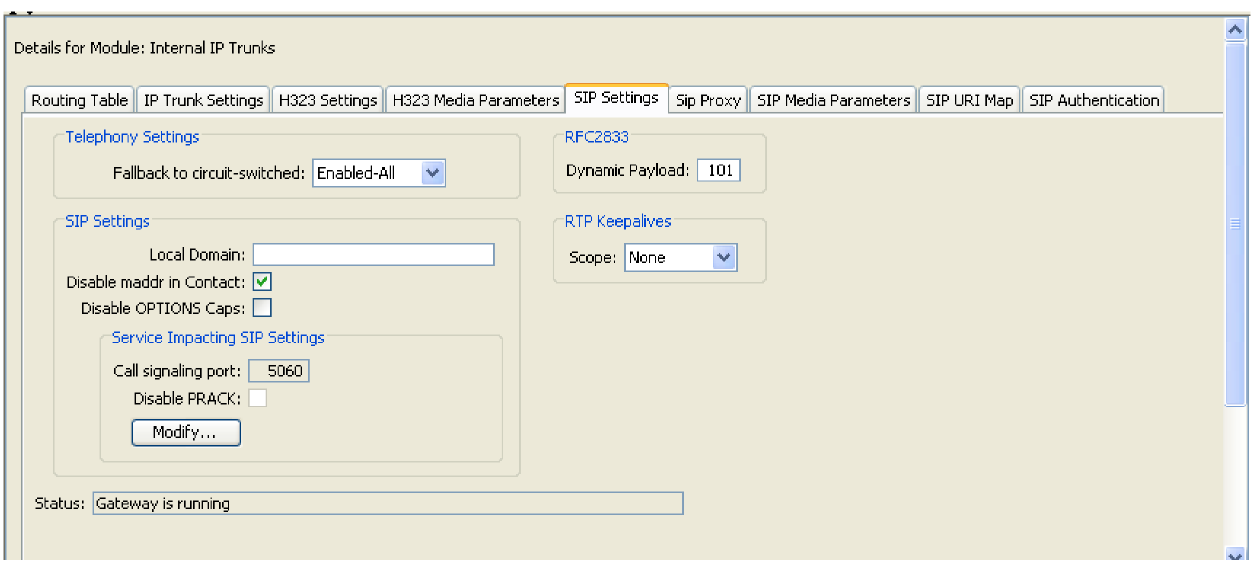


4.7.3. Configure SIP Settings

Under the *SIP Settings* tab,

- Select **Enabled-All** to re-route calls over PSTN line if SIP trunk fails.
- Enter the same payload number in **RFC2833** field as defined for the **Telephone Event Payload Type** field on Page 4 of the Add Trunk Group screen for the SIP Trunk Groups on Avaya Aura^{TM} Communication Manager (see **Sections 2.4.2** and **5.5.2**).
- Verify the **Port Number** matches the port number selected for the Business Communication Manager SIP Entity Link defined in **Section 3.4.1.**
- Leave **local domain** field blank.
- Select the **Disable maddr in Contact** field:

The following screen shows the details of the *SIP Settings* for the sample configuration:



4.7.4. Configure SIP Media Parameters

Under the *SIP Media Parameters* tab, configure the Business Communication Manager to use the same set of Codecs as defined for the Avaya Aura^{TM} Communication Manager Access Element in **Section 5.2.**

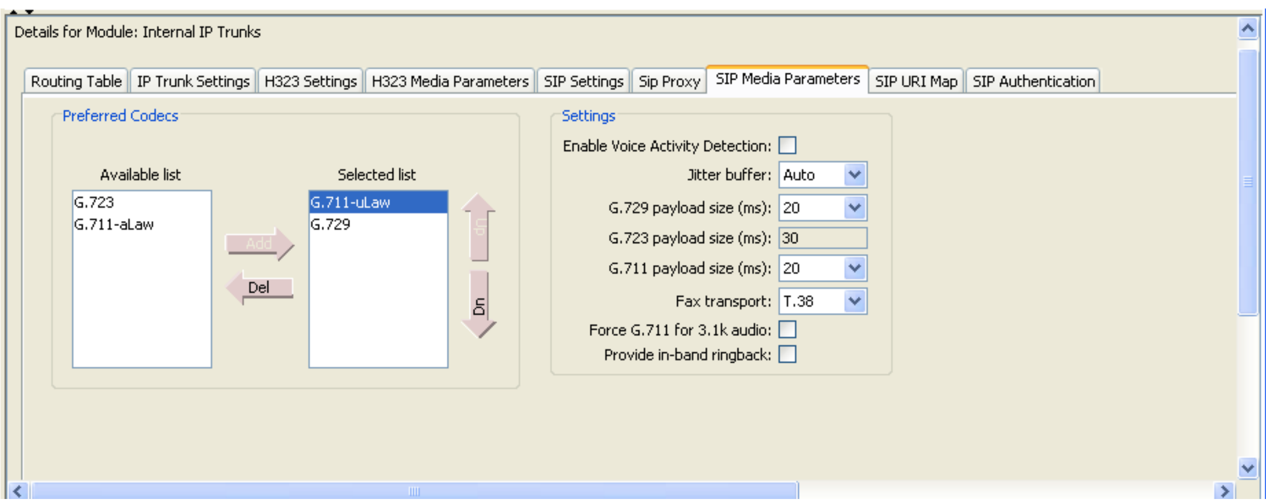
In the **Preferred Codecs** section on the left side of the page,

- select **G.711-uLaw, G.729** from the *Available List* and select the **Add** button to move these two codec choices to the *Selected List* table.
- Configure the **G.711-uLaw** codec as the first choice by moving **G.711-ulaw** to top of list.

In the codec **Settings** section on the right side of the page,

- uncheck **Enable Voice Activity Detection**.
- select 20ms as the payload size from the drop-down menu for both G.729 and G.711
- select T.38 from the drop-down menu for the **Fax transport** field.

The following screen shows the details of the *SIP Media Parameters* for the sample configuration:



4.7.5. Configure SIP Authentication

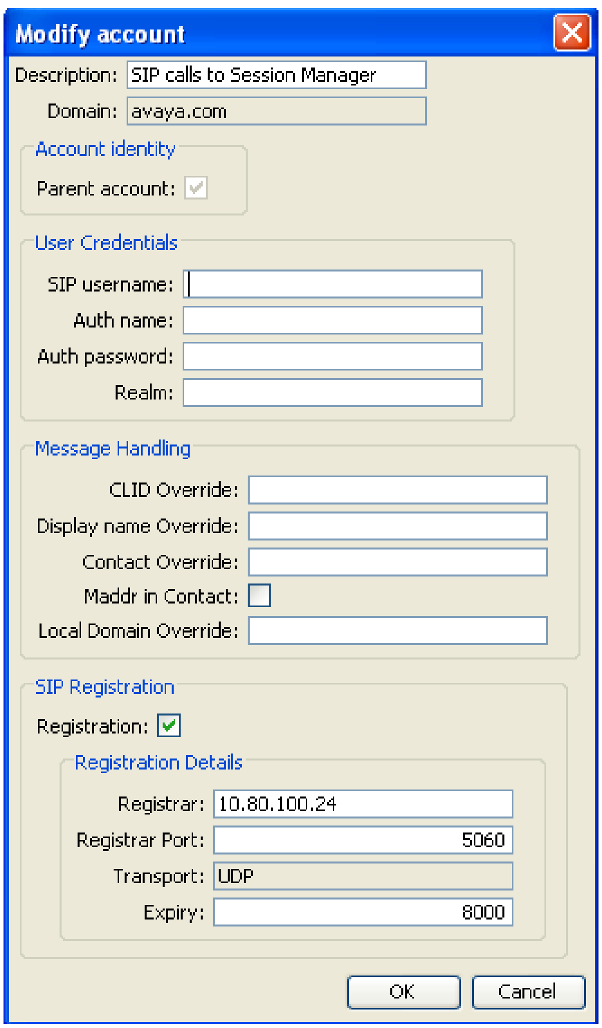
Under the *SIP Authentication* tab, configure a SIP account to enable Business Communication Manager to communicate with Avaya Aura^{TM} Session Manager.

Select **Modify** button to enter the following values in the **Modify SIP Account** dialog:

- **Description**: Enter a descriptive name for the SIP account.
- **Domain**: enter the same SIP Domain name as defined for Session Manager in **Section 3.1**.
- **Account Identity** section, select **Parent** which allows all stations to use the same account for outgoing calls to Session Manager over the SIP trunk.

- **User Credentials** section: Since authentication on a per user basis is not required in the sample configuration, fields in this section can be left blank.
- **Message Handling** section:
  - o **CLID Override**: Leave blank to send the Calling Line ID of the originating station instead of sending a generic ID for all calls from the branch office.
  - o **Display name Override**: Leave blank to send the administered name of the originating station instead of sending a generic name for all calls
  - o **Contact Override**: Leave blank
  - o **Maddr in Contact**: Leave unchecked
  - o **Local Domain Override**: Leave blank
- In the **Registration Details** section. configure the registration details as follows:
  - o **enable Registration** for this SIP Account
  - o **Registrar:** IP address Session Manager
  - o **Registration Port**: Provide the UDP port number
  - o **Expiry**: Leave the default value

The following screen shows the details of the *Modify SIP Account* dialog for the sample configuration:



4.8. Configure Sets

4.8.1. Manual Configuration of IP 1230 Phone

After installing the phone, it will be necessary to manually configure the IP address of the phone, default gateway, network mask, and IP Address of Business Communication Manager server. Alternatively, if the system will be deployed with a large number of IP stations, the IP phones can be configured to dynamically obtain their IP addresses from a DHCP server. For more information on configuring the Business Communication Manager system to use a DHCP server, see product documentation in **Section 9.**

To manually configure each phone, use the **Network Configuration** menu on the phone. Access the menu by:

- Pressing the 4 soft keys at the bottom of the display area in sequence from left to right when the IP Phone is starting and the text "Nortel" appears in the display.
- If prompted for a **password**, enter the default: 26567*738 (color*set).
- Use the Up and Down navigation keys to scroll through the **Network Configuration** parameters

When prompted, enter the appropriate values for the IP address of the phone, gateway, network mask and IP address of the Business Communication Manager server.

Select **Apply** to save the new values and re-start the phone.

Note: if one of the parameters is not included when manually configuring the phone, it will be necessary to change the parameter from *Automatic* mode to *Manual* mode. To change the mode:

- Press **Auto** on the **Network Configuration** page to switch to the **Auto Provisioning** page.
- Use the navigation keys to scroll to the specific parameter.
- Press **Man** to enable manual configuration of the specific parameter, which was previously configured automatically.
- Press **Cfg** to return to **Network Configuration** page to modify network configuration settings for the phone.
- After completing the changes, select **Apply** to save the new values and re-start the phone.

For more information on manually configuring IP Phones, see References in **Section 9.**

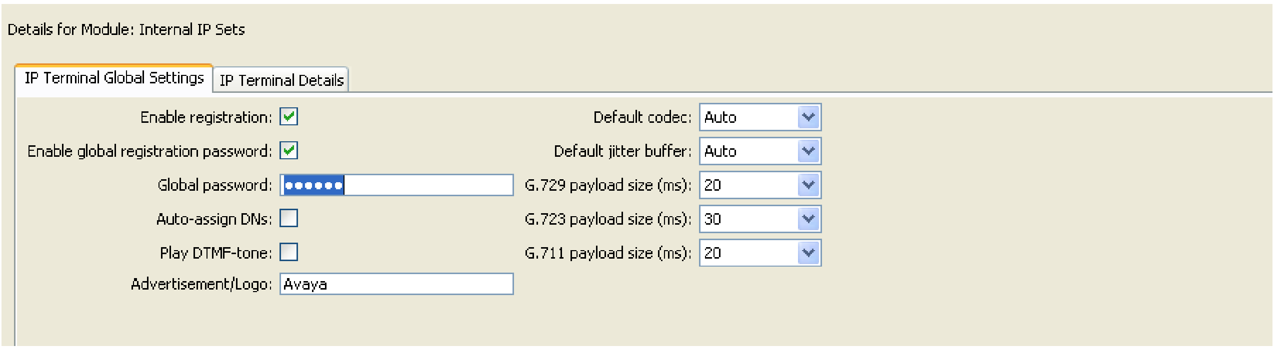
4.8.2. Configure Global IP Terminal Settings

Navigate to the **Resources → Telephony Resources** task. Select the row associated with **IP Sets** in the *Telephony Resources* table. Wait a few seconds for the configuration details of the **IP Sets** to be displayed in the lower section of the page.

Under the *IP Terminal Global Settings* tab,

- Select "Auto" from the drop-down menu for **Default codec** field
- Set the payload size (ms) for G.729 and G.711 fields to 20.
- Enter a password which will be used when IP sets register.
- Enter a name in the Logo field (optional).

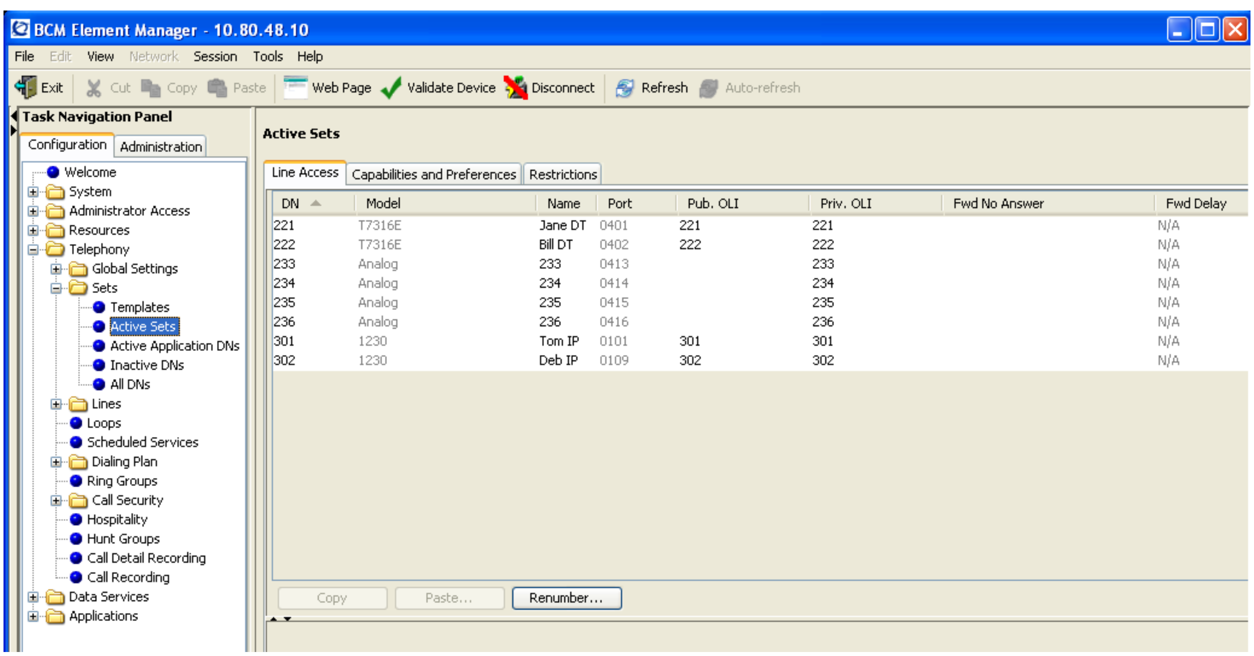
The following screen shows *IP Terminal Global Settings* for the sample configuration:



4.8.3. Configure Display Name and Published Originating Line ID

Navigate to the **Telephony → Sets → Active Sets** task. Select the row associated with an installed station to configure the **Display Name** & **Publish Originating ID** (Pub OLI) for the station.

The following screen shows the *Display Names* and *Pub. OLI* for the stations in the sample configuration:

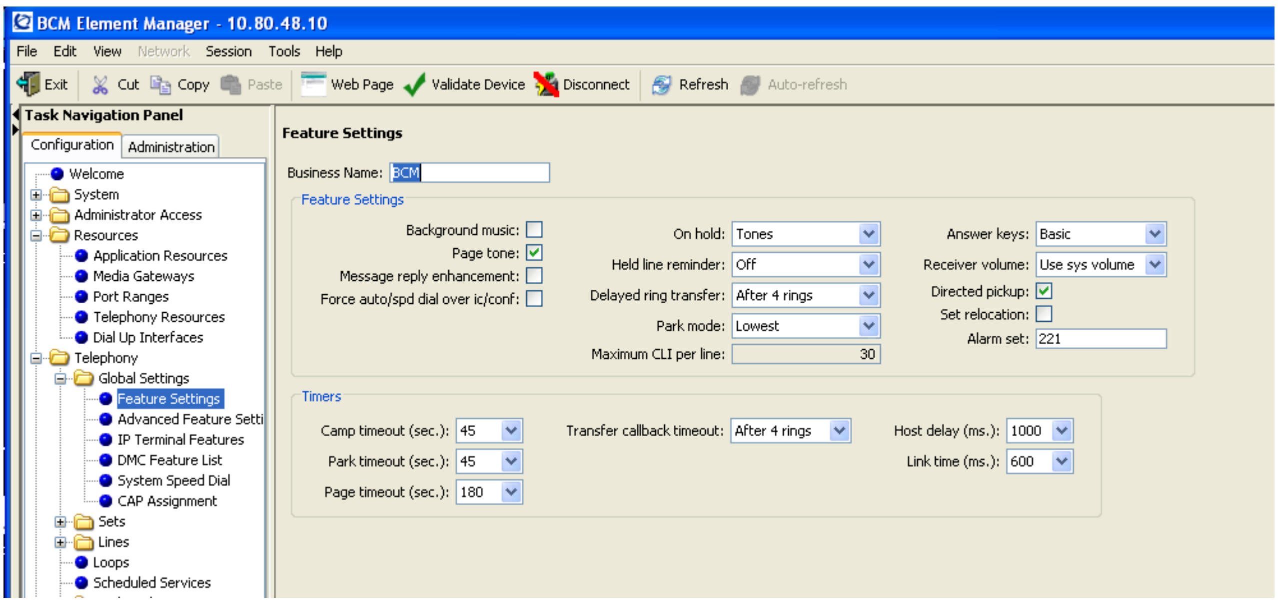


4.9. Define Business Name

Navigate to the **Telephony → Global Settings → Features Settings** task. Enter a name into the **Business Name** field on this page. This name will be sent as part of the user information in SIP messages. If the Business Name field is left blank, Business Communication Manager will not include the station name in the SIP message.

> Note: Since Business Communication Manager concatenates the station name to the end of the Business Name in the SIP message and there appears to be a fixed length for this concatenated string, using a short Business Name is recommended.

The following screen shows the *Feature Settings* for the sample configuration:



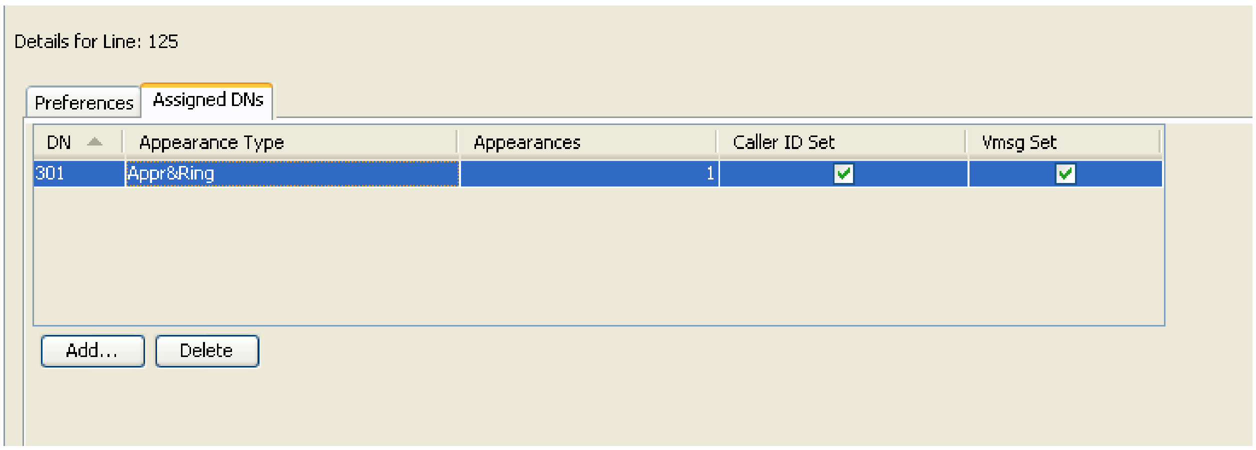
4.10. Configure Target Lines

For incoming calls from Avaya Aura™ Session Manager to ring an individual station, a target line need to be associated with an individual station.

Navigate to the **Telephony → Lines → Target Lines** task. Select an available target line from the *Target Line* table. Under the *Assigned DN* tab located in the *Details* section for the selected target line, select the **Add** button to assign a station number to the target line as shown in the **Add Line Appearance** dialog below:

Select OK to associate the station with the target line.

Select the new row in the *Assigned DN* table under the *Details* section to select **Caller ID Set** as shown below:

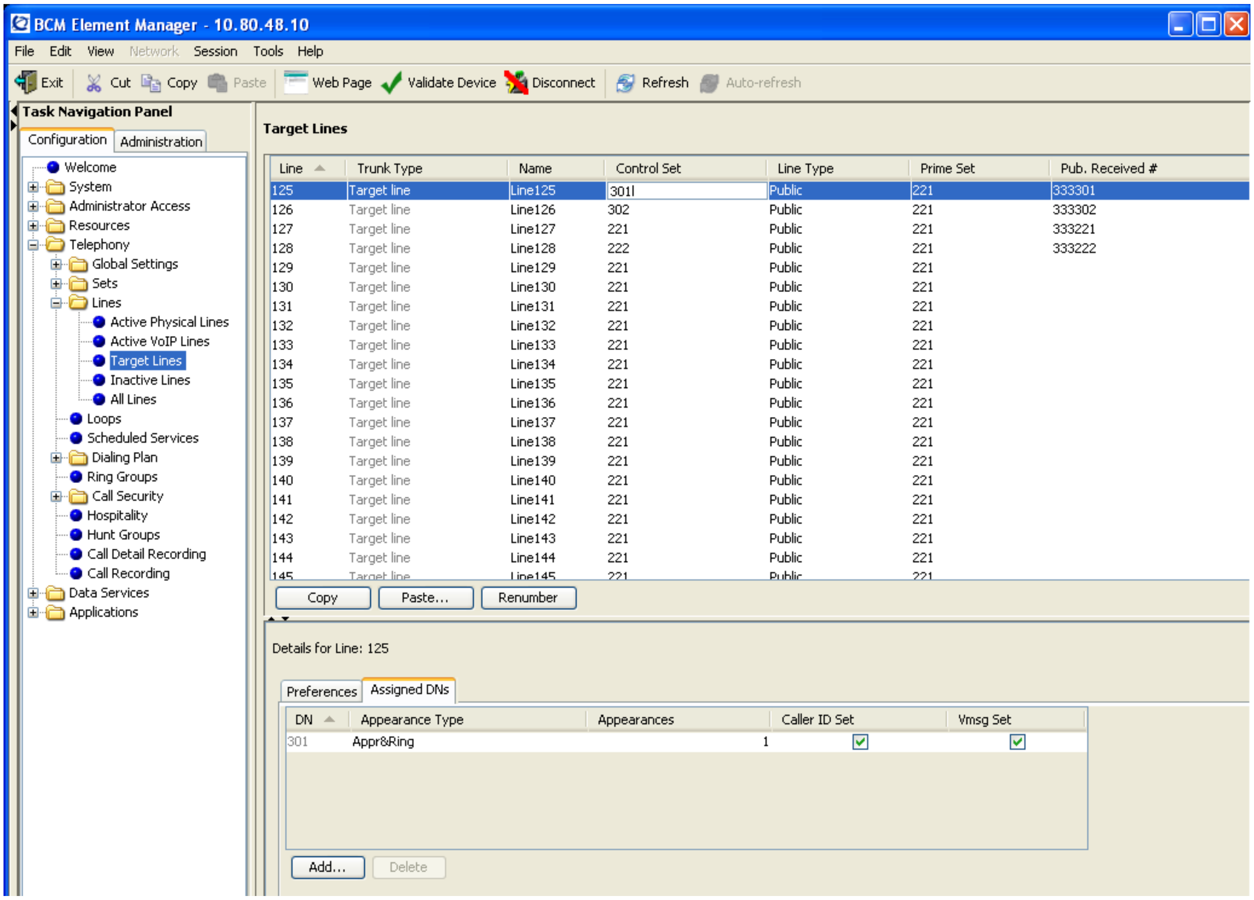


After completing the entry in the *Assigned DNs* tab in the Details section, enter the appropriate station number in *Target Lines* table on the **Control Set** field in the main page and the appropriate received digits in **Publ. Received #** field the for the selected target line.

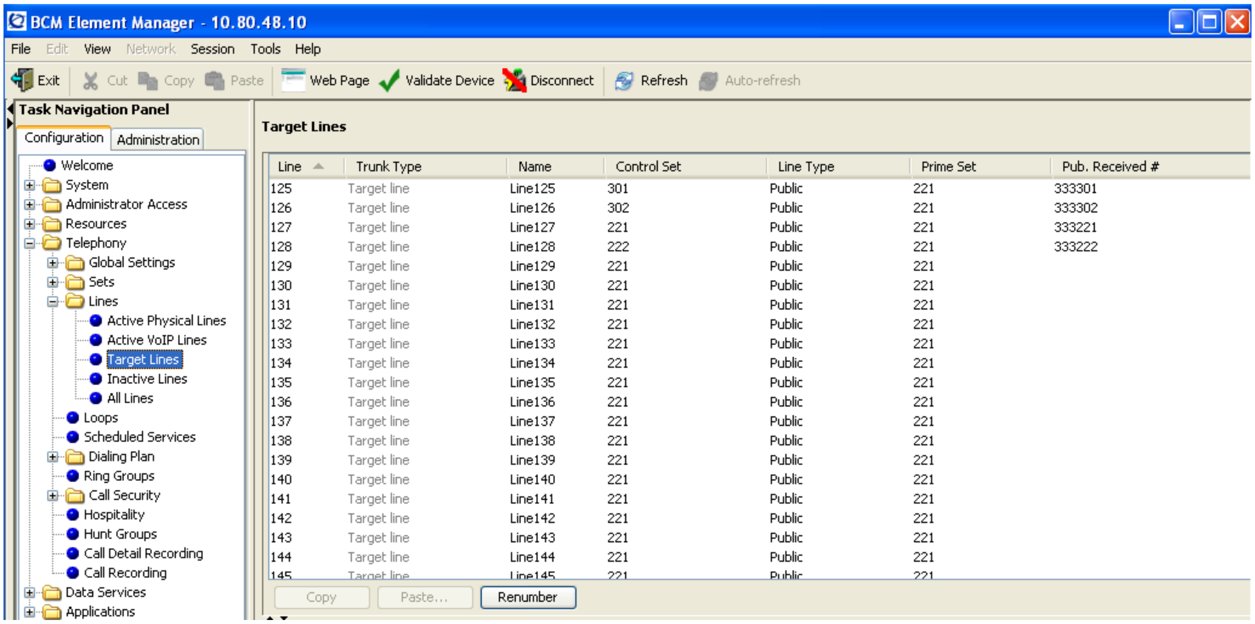
> Note: The received digits in **Publ. Received #** field should match the **Public Received DN** field configured in **Section 4.11.2.**

This change may take several seconds to complete.

The following screen shows the results of assigning station 301 to Target Line 125 in the sample configuration:



The following screen shows the complete set of *Target Lines* associated with the stations in the sample configuration:



4.11. Configure Dial Plan

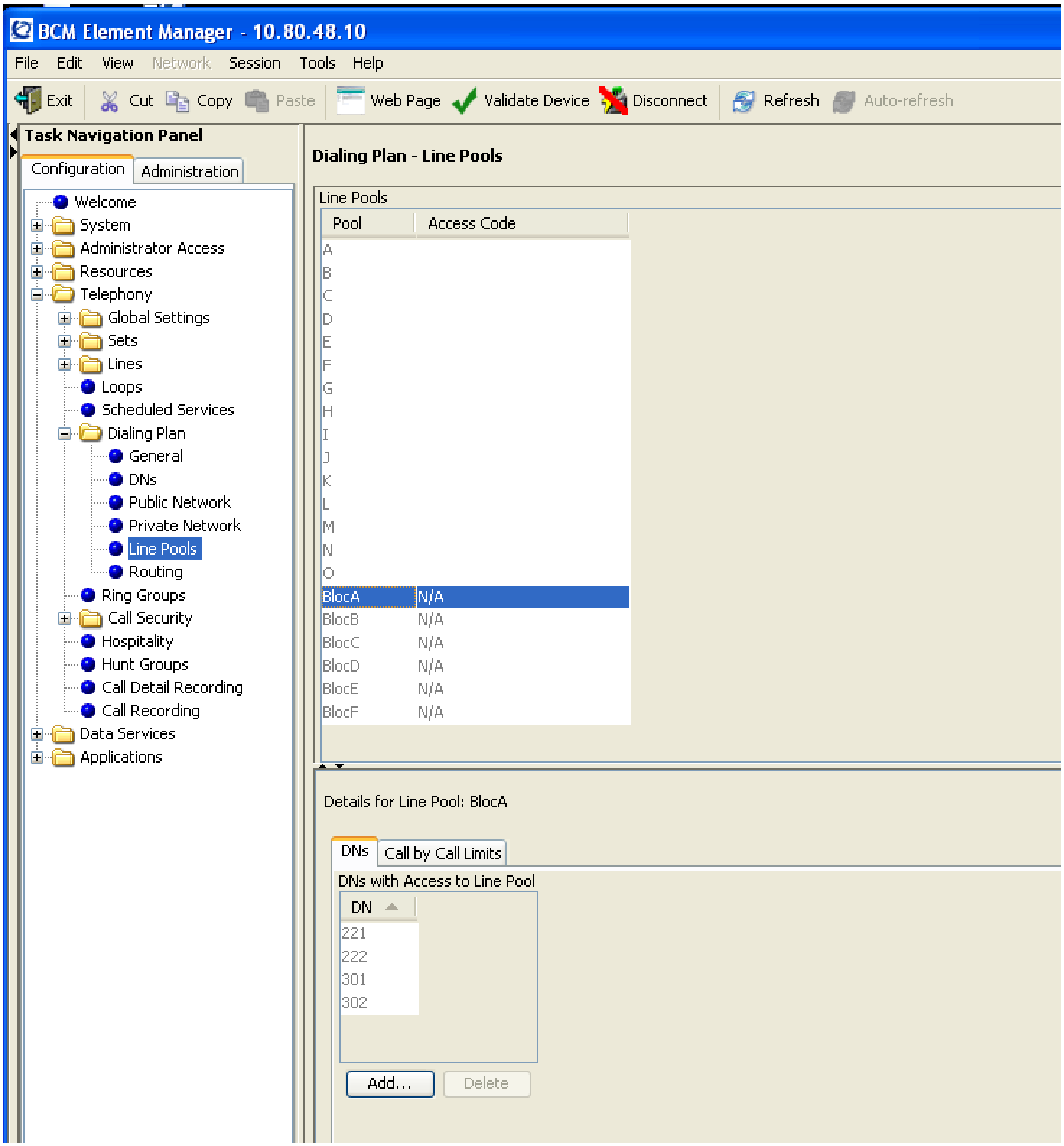
4.11.1. Configure SIP Line Pool

Navigate to the **Telephony → Dialing Plan → Line Pool** task.

Select **BlocA** from the **Line Pool** table. In the *Details* section for BlocA, select the **Add button** to allow each station to access the SIP trunk.

Note: The **BlocA** Line Pool is automatically configured as a VoIP Trunk Type in Business Communication Manager.

The screen below shows results for the sample configuration.



4.11.2. Configure Public Network

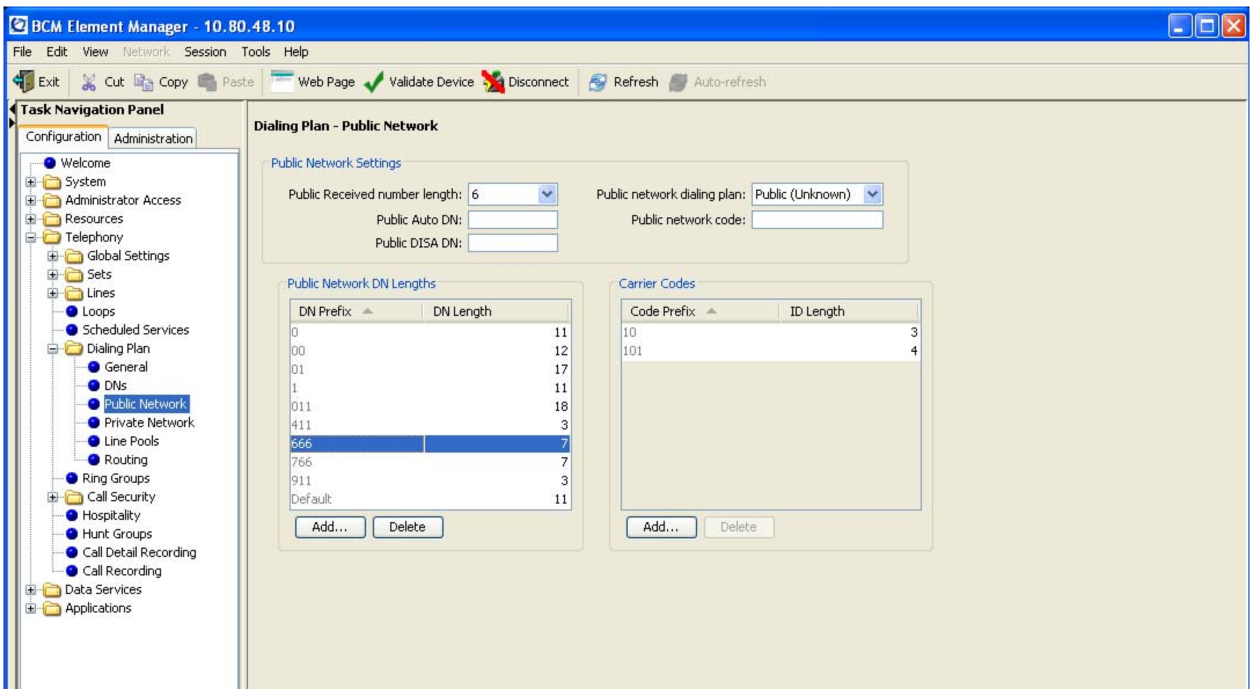
Navigate to the **Telephony → Dialing Plan → Public Network** task. In the *Public Network Settings* section, enter the number of digits for received calls. In the *Public Network DN Length* section, select the **Add** Button to define the dialed number pattern for outgoing calls to Avaya Aura™ Session Manager.

Note: the dialed number pattern shown in this section is an example and was used in the sample configuration. Other dialed number patterns may be appropriate for different customer networks.

In the sample configuration, received calls contain 6 digits and originating calls routed to Session Manager will start with the digits 666 as shown by the dialog below:

Click OK to enter the new prefix.

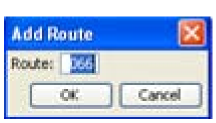
Select the new row in the *Public Network DN Lengths* table to modify the **DN Length** field as shown below.



Select Enter to save the change. Note: this change may take several seconds to finish.

4.11.3. Configure Routing

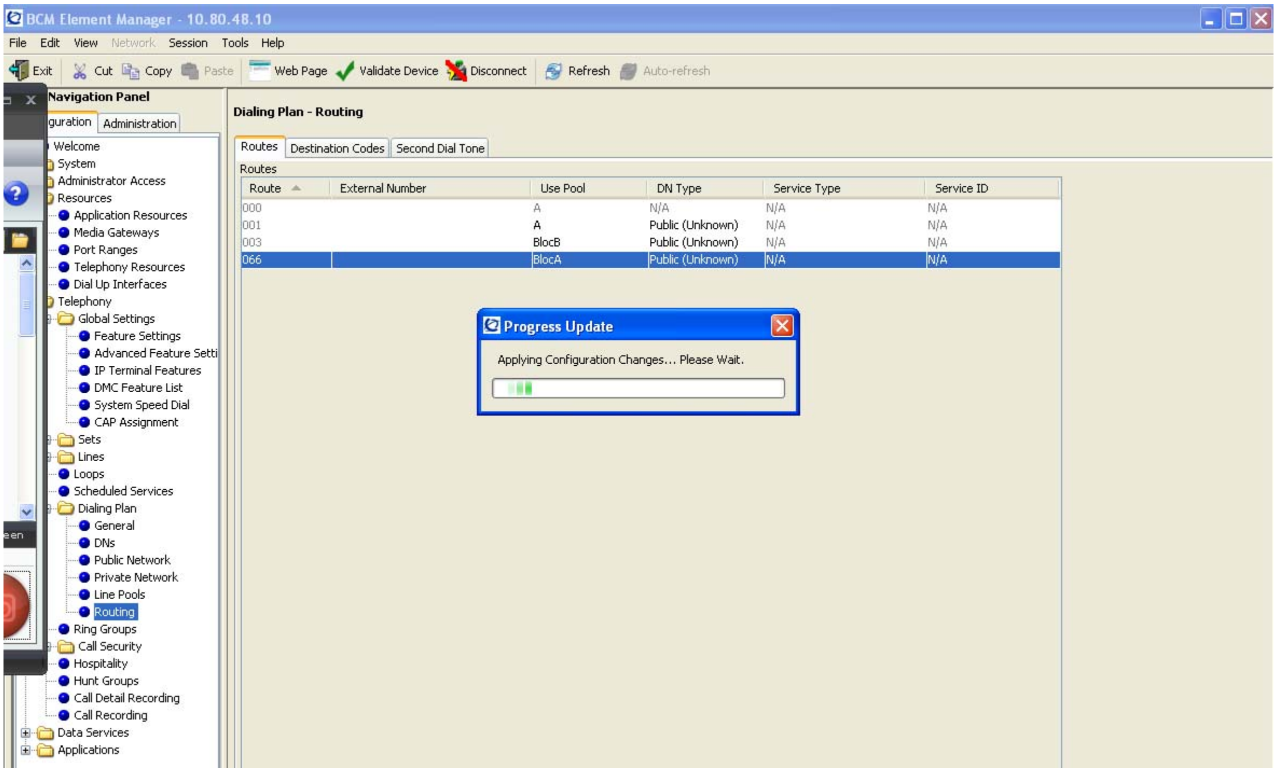
Navigate to the **Telephony → Diaing Plan → Routing** task. Under the *Routing* tab, select the **Add** button to create a route for routing calls to Avaya Aura^{TM} Session Manager. Enter an available route number in the Add Route dialog as shown below:



Select OK to add the route.

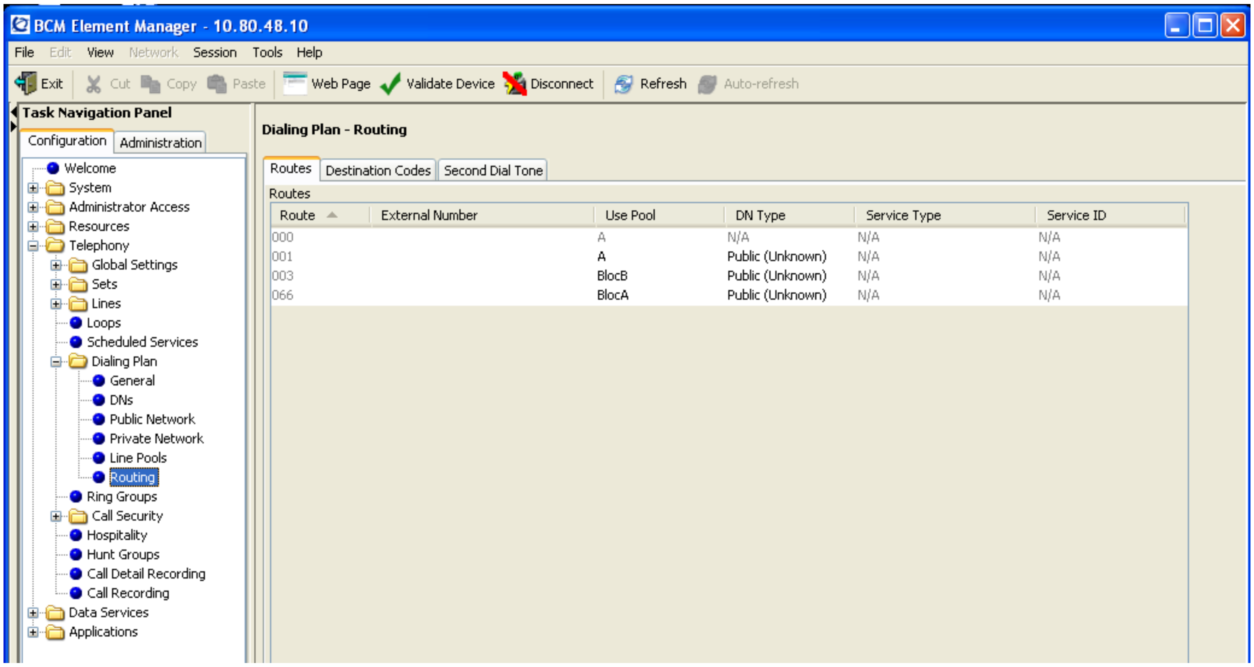
Select the row associated with the new route in the *Routes* table and select **BlocA** from the drop-down menu associated with the *Use Pool* column.

This change may take several seconds to complete as shown below:



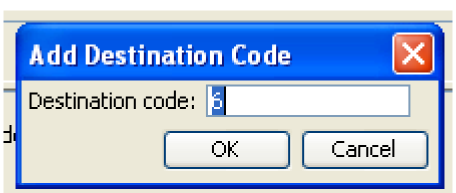
After the Line Pool change completes, select **Public** from drop-down menu associated with the *DN type* column.

The following screen shows the routes defined for the sample configuration:



4.11.4. Configure Destination Code

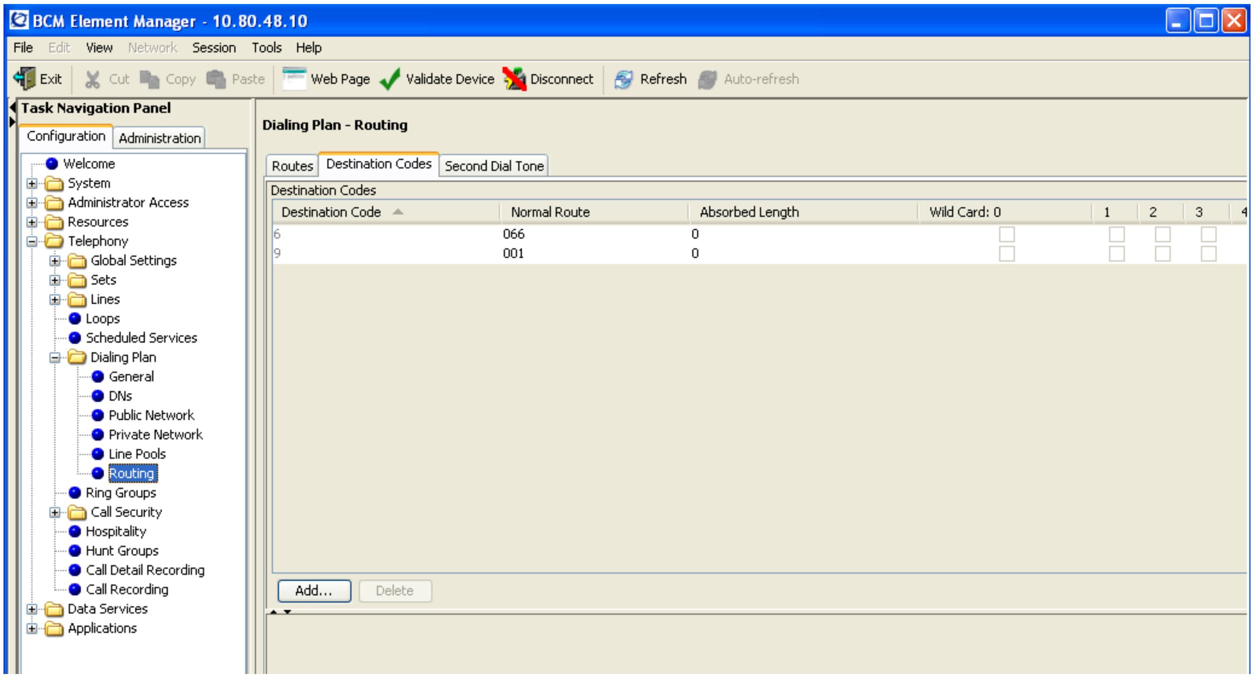
Navigate to the **Telephony → Dialing Plan → Routing** task. Under the *Destination Code* tab, select the **Add** button to create a destination code for routing calls to Avaya Aura^{TM} Session Manager. Enter the first digit of the number used for outgoing calls to Session Manager in the **Add Destination Code** dialog as shown below:



Select OK to add the destination code. Select the row associated with the new destination code in the *Destination Codes* table to configure the *Normal Route* & *Absorbed Length* fields.

- Enter the route number defined in **Section 4.11.3** in the *Normal Route* field.
- Select "**0**" from the drop-down menu associated with the *Absorbed Length* field since the number used for the destination code is the first digit in the outgoing number.

The following screen shows the details of the *Destination Codes* entry for the sample configuration:



5. Configure Avaya Aura™ Communication Manager Access Element

This section describes the administration of Communication Manager Access Element using a System Access Terminal (SAT). Some administration screens have been abbreviated for clarity. Other administrative screens are not shown in this section, as the screens are the same screens described in **Section 2.**

- Verify System Capabilities and Communication Manager Licensing
- Administer Codec Set
- Administer IP network region
- Administer IP node names
- Administer SIP trunk group and signaling group
- Administer route pattern
- Administer numbering plan

After completing these steps, the “**save translations**” command should be performed.

5.1. Verify System Capabilities and Licensing

This section describes the procedures to verify the correct system capabilities 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.

5.1.1. SIP Trunk Capacity Check

Use the "**display system-parameters customer-options"** command to verify that an adequate number of SIP trunk members are administered for the system. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

5.1.2. AAR/ARS Routing Check

Verify that **ARS** and **ARS/AAR Dialing without FAC** are enabled (on page 3 of system-parameters customer options).

5.1.3. Configure Trunk-to-Trunk Transfers

Use the "**change system-parameters features**" command to enable trunk-to-trunk transfers.

5.2. Configure Codec Type

Issue the **change ip-codec-set n** command where **n** is the number used to identify the codec set. Enter the following values:

- Enter "**G.711MU**" and **"G.729"** as supported types of Audio Codecs
- 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
```

5.3. Set IP Network Region

Using the **change ip-network-region 1** command, set the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields to "**yes**". For the **Codec Set** enter the corresponding audio codec set configured in **Section 5.2**. Set the **Authoritative Domain** to the correct SIP domain for the configuration.

```
change ip-network-region 1                                   Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: avaya.com
    Name:
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
```

5.4. Add Node Names and IP Addresses

Using the **change node-names ip** command, add the node-name and IP Addresses for the CLANs and the Session Manager, if not previously added.

```
change node-names ip                                         Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
8730-1              10.80.111.11
8730-2              10.80.111.12
ASM1                10.80.100.24
ASM2                10.80.100.26
CLAN-1              10.80.111.16
CLAN-2              10.80.111.17
```

5.5. Configure SIP Signaling Group and Trunk Group

5.5.1. Add Signaling Group for SIP Trunk

Use the **add signaling-group n** command, where “n” is an available signaling group number to create a SIP signaling group to connect to one of the Avaya Aura™ Session Managers. In the sample configuration, signaling group “10” and trunk group “10” were used to connect to the first Avaya Aura™ Session Manager.

For more information on configuring multiple SIP trunks to recover from network failures, see References in **Section 9**.

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

- **Group Type:** “sip”
- **Transport Method:** “tcp[5]”
- **IMS Enabled:** “n”
- **Near-end Node Name:** C-LAN node name from **Section 5.4**.
- **Far-end Node Name:** Session Manager node name from **Section 5.4**.
- **Near-end Listen Port:** “5060”
- **Far-end Listen Port:** “5060”

[5] TCP was used for the sample configuration. However, TLS would typically be used in production environments

- **Far-end Domain:** enter domain name for **Authoritative Domain** defined in **Section 5.3**
- **DTMF over IP:** "rtp-payload"
- **Session Establishment Timer:** "3"

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

Group Number: 10            Group Type:  sip
                        Transport Method: tcp
  IMS Enabled? n
     IP Video? n

    Near-end Node Name: CLAN-1                 Far-end Node Name: ASM1
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                       Far-end Network Region:
Far-end Domain: 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? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

5.5.2. Add SIP Trunk Group

Add the corresponding trunk group controlled the signaling group defined **Section 5.5.1** using the **add trunk-group n** command, where "n" is an available trunk group number and fill in the indicated fields.

- **Group Type:** "sip"
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** "tie"
- **Signaling Group:** The number of the signaling group added in **Section 5.5.1**
- **Number of Members:** The number of members in the SIP trunk to be allocated to calls routed to Session Manager (must be within the limits of the total number of trunks configured in **Section 5.1.1**).

Once the add 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 ASM1           COR: 1        TN: 1        TAC: #10
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: 10
```

On page 2, set the **Preferred Minimum Session Refresh Interval** 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, set **Numbering Format** to be *public*. Use default values for all other fields.

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

                     Numbering Format: public
                                              UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n

 Show ANSWERED BY on Display? y
```

On page 4, set **Mark Users As Phone** to “y” to send correct user information to Business Communication Manager in the SIP messages, and set the **Telephone Event Payload Type** to “101”.

```
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? n
              Telephone Event Payload Type: 101
```

5.6. Configure Route Pattern

Use the “**add route-pattern X**” command, when **X** is an available number to define a route pattern for routing calls over the SIP trunk group defined **in Section 5.5.1** to Session Manager**.** In the sample configuration, route pattern 10 was created as shown below:

```
add route-pattern 10                                           Page   1 of  3

                    Pattern Number: 10  Pattern Name: SIP to ASM1
                             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:                                                                  n   user
 3:                                                                  n   user
```

5.7. Administer Numbering Plan

5.7.1. Administer Uniform Dialplan

To enable stations on the Communication Manager Access Element to call SIP phones registered to Session Manager, add an entry for extension numbers associated with SIP phones to the uniform dial plan

Use the “**change uniform-dialplan x**” command, where **x** is the first digit of the extension numbers used for SIP stations.

In the sample configuration, extensions starting with “666-3XXX” are used for extensions associated with the 9630 SIP phones.

Note: the dial plan shown below is an example dial plan that was used in the sample configuration. Other dial plans may be appropriate for different customer networks.

```
change uniform-dialplan 6                                         Page   1 of  2
                              UNIFORM DIAL PLAN TABLE
                                                                 Percent Full: 0
```

```
  Matching                  Insert              Node
  Pattern       Len Del     Digits      Net Conv Num
 6663            7   0                  aar   n
 6665000         7   0                  aar   n
 777             7   0                  aar   n
 778             7   0                  aar   n
                                              n
```

5.7.2. Administer AAR analysis

This section provides the configuration of the AAR pattern used in the sample configuration for routing calls between Communication Manager Access Element and Business Communication Manager. Note that other methods of routing may be used.

Use the "**change aar analysis x**" command where **x** is the first digit of the number used to route calls to stations on Business Communication Manager.

In the sample configuration, all calls starting with "333" will be routed to Business Communication Manager:

```
change aar analysis 3                                          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
    333                   6    6     10        aar           n
    555                   7    7     10        aar           n
    6663                  7    7     10        aar           n
    6665000               7    7     10        aar           n
    8                     7    7     999       aar           n
    9                     7    7     999       aar           n
```

5.8. Save Translations

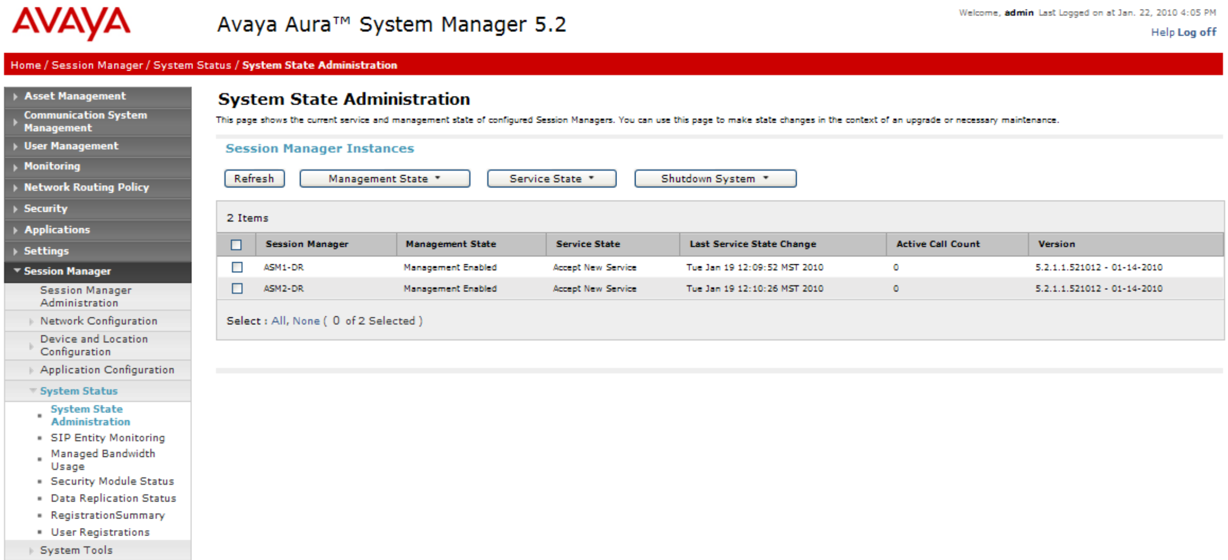
Configuration of Communication Manager Access Element is complete. Use the **"save translations**" command to save these changes

6. Verification Steps

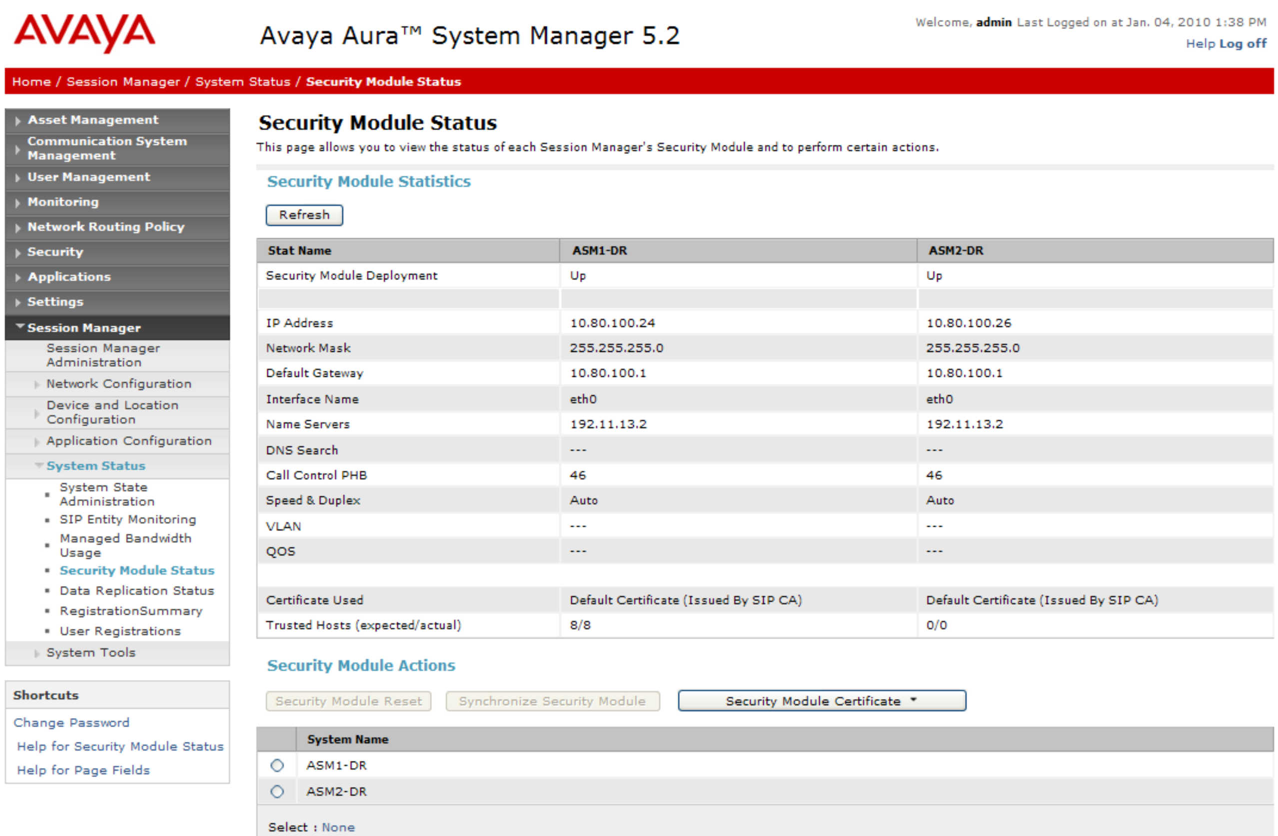
6.1. Verify Avaya Aura^{TM} Session Manager Configuration

6.1.1. Verify Avaya Aura^{TM} Session Manager is Operational

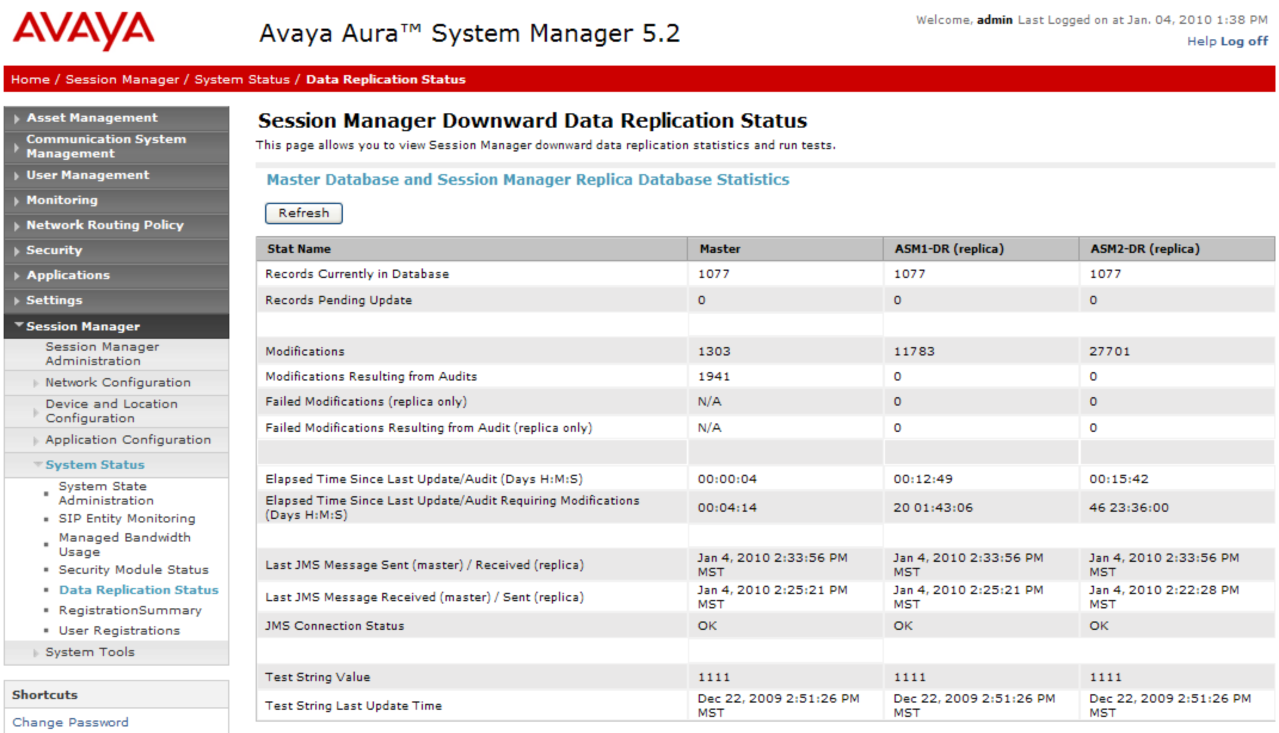
Verify the overall system status for the specific Session Manager as shown below:



Verify the status of the Security Module as shown below:

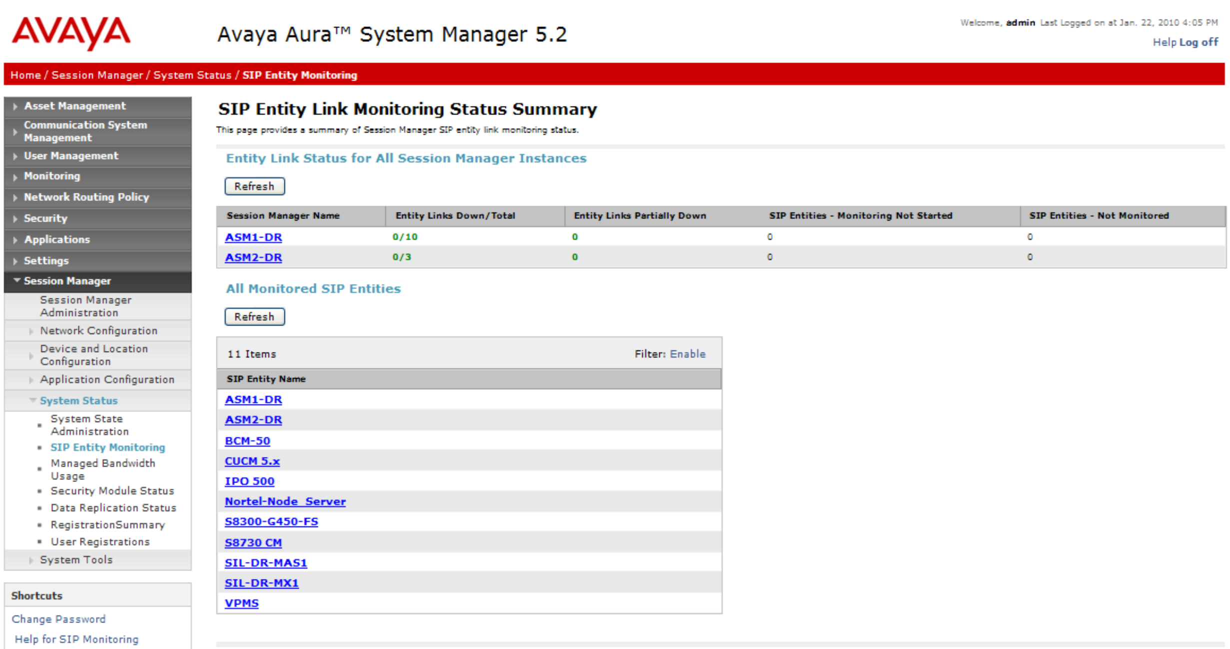


Finally, verify the data replication status is operational as shown below:

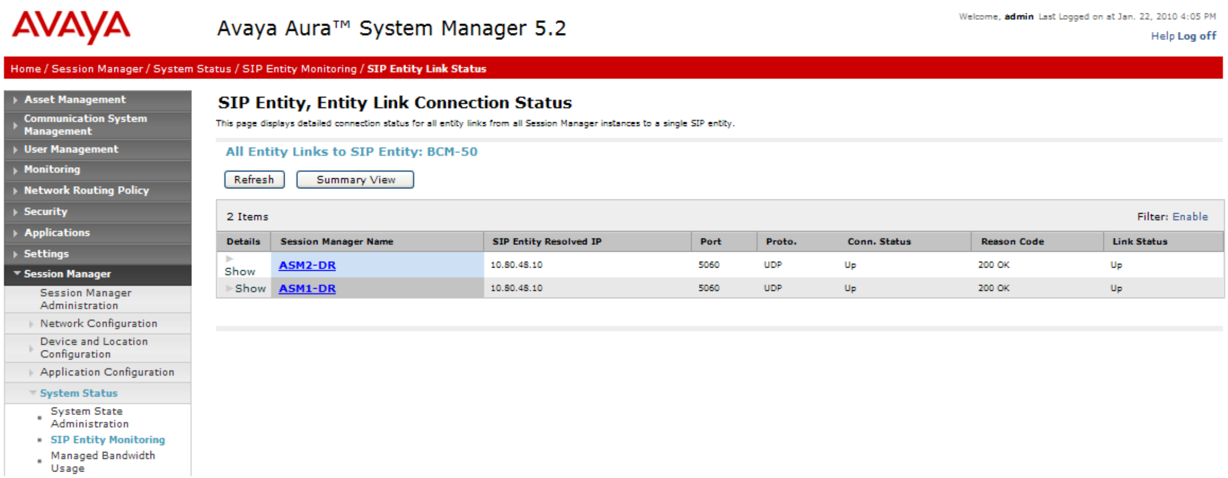


6.1.2. Verify SIP Link Status

Expand the Session Manager menu on the left and click SIP Entity Monitoring. Verify all SIP Entity Links are operational as shown below:

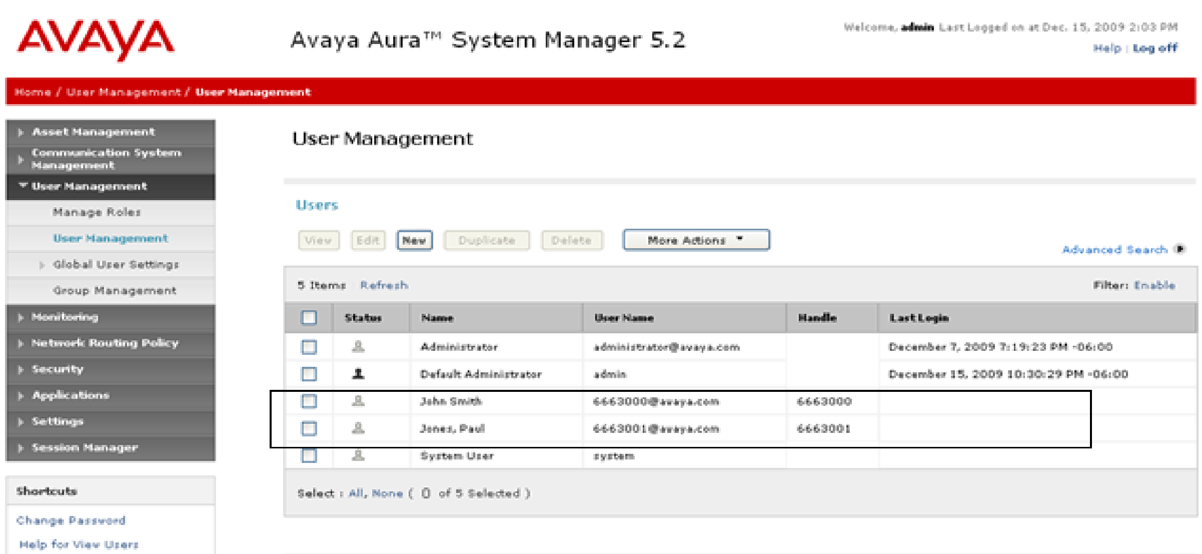


Select the corresponding SIP Entity for the Business Communication Manager and verify the link is up as shown below:

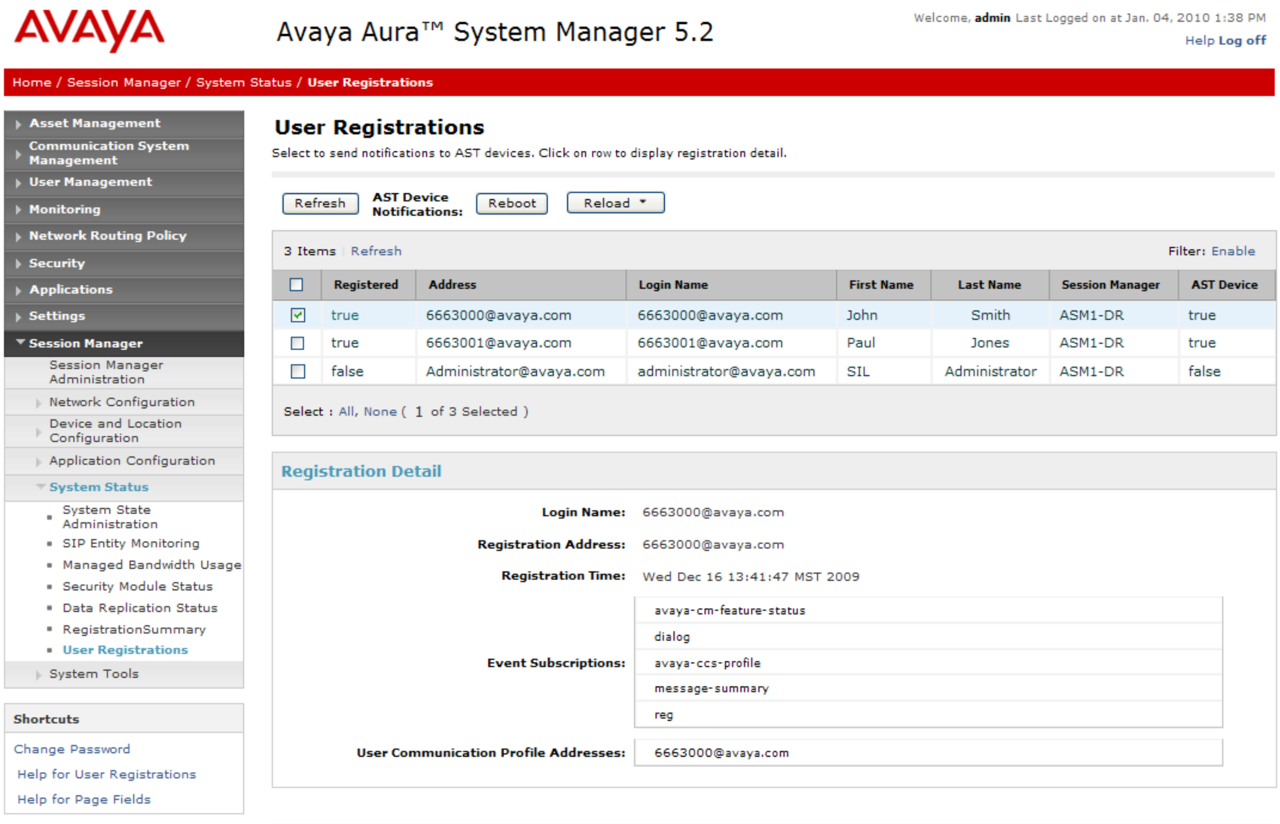


6.1.3. Verify Registrations of SIP Endpoints

Verify SIP users have been created in the Session Manager. In the sample configuration, two SIP users were created as shown in the highlighted area below:



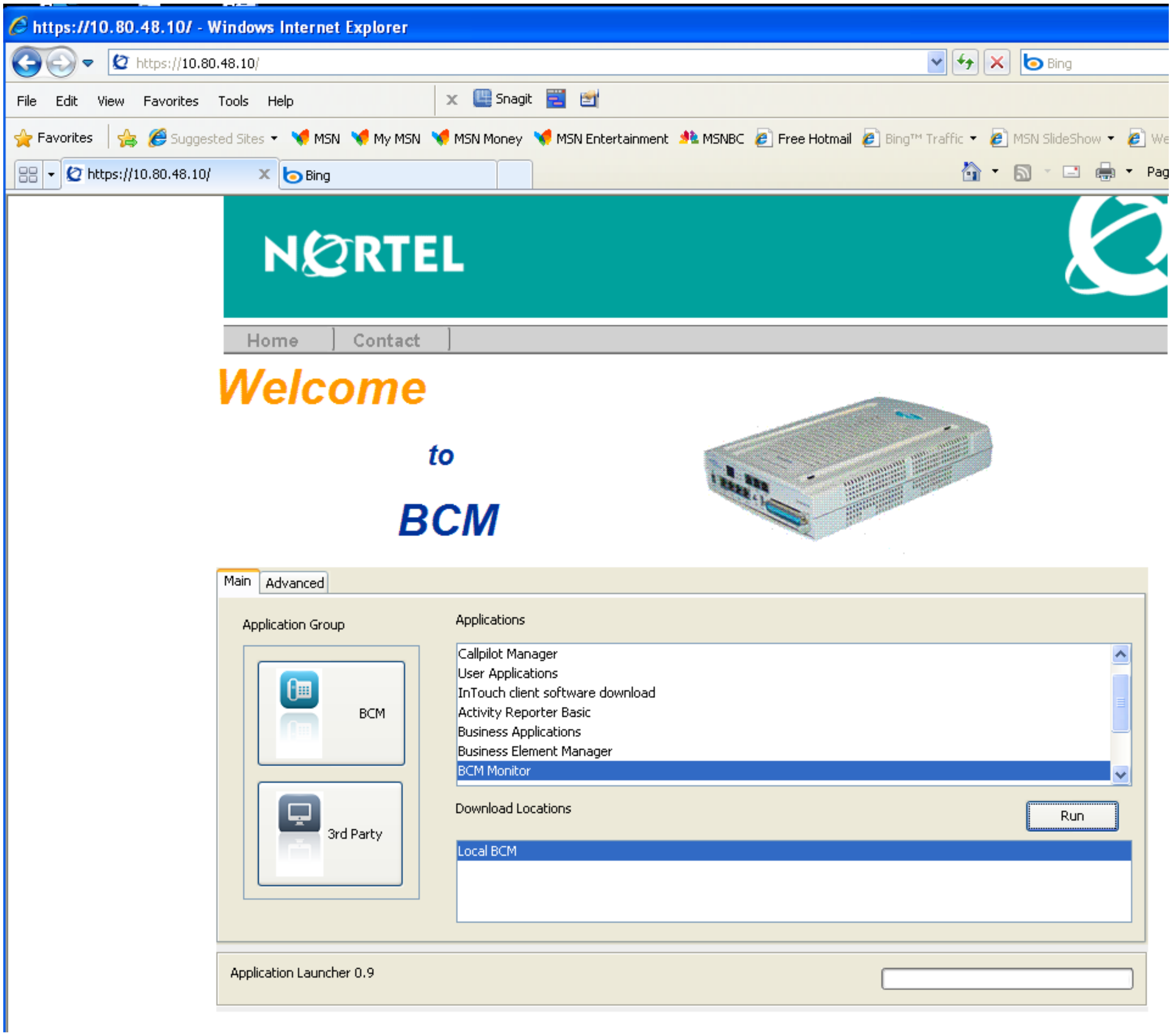
Verify the SIP endpoints have successfully registered with the Session Manager as shown below:



6.2. Verify Business Communication Manager Configuration

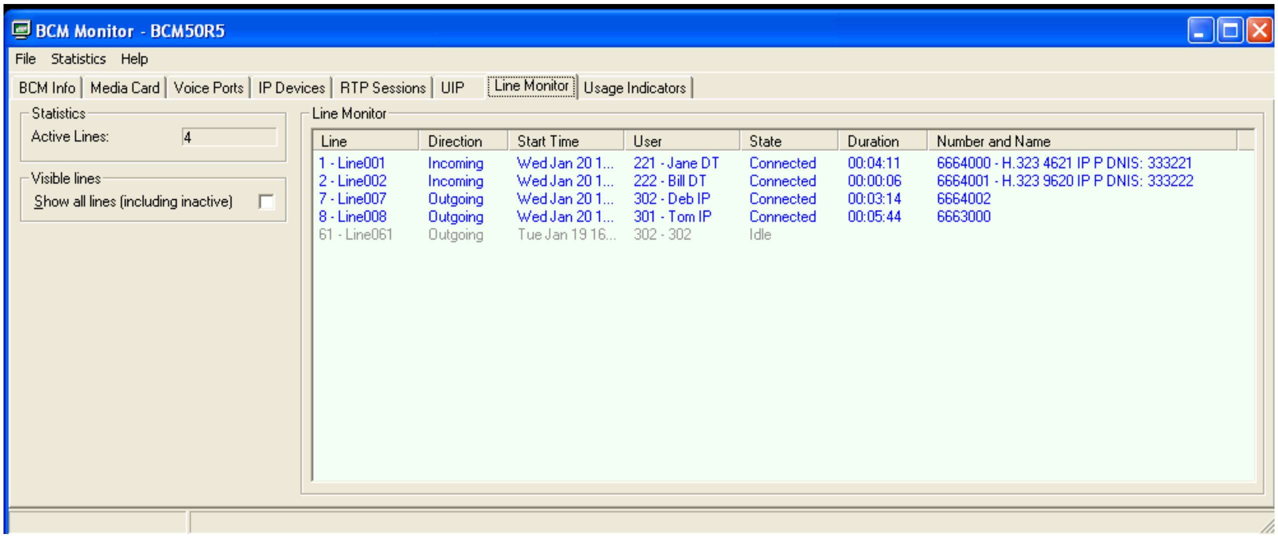
The Business Communication Monitor application monitors the status of SIP trunk calls.

Use the Business Communication Manager Application web page to open the Monitor application as shown below:

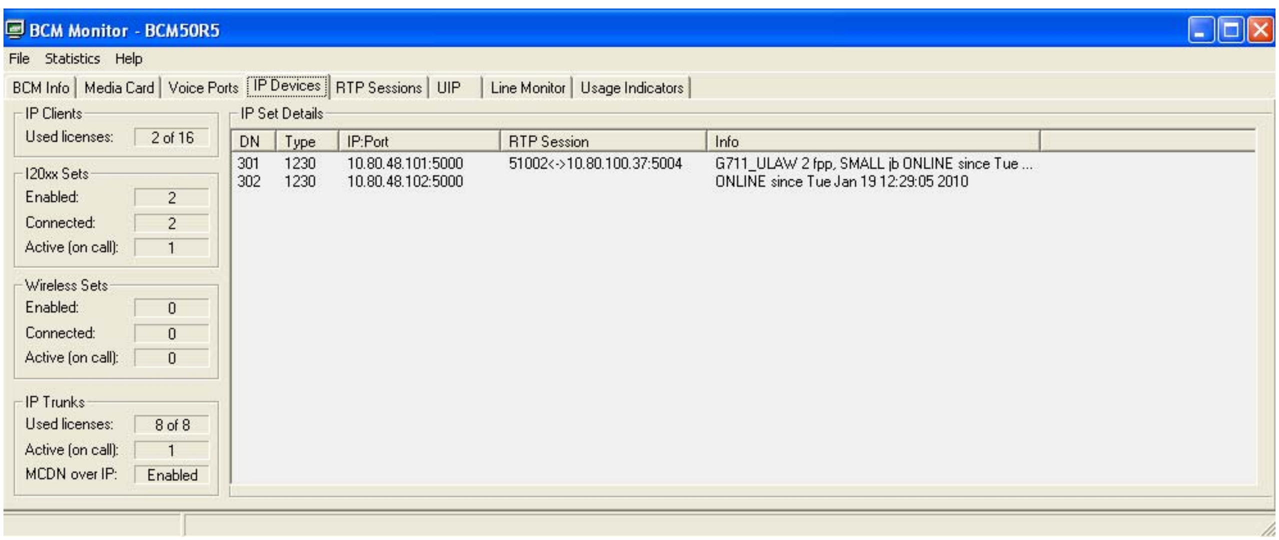


Login with the same user name and password as when logging into the Element Manager.

Navigate to the **Line Monitor** tab to see the status of SIP trunk. The following screen shows 4 calls active calls between Business Communication Manager and stations on Avaya Aura™ Communication Manager:



Use the **IP Devices** tab to monitor individual IP stations. For example, the screen below provides status of an active call from a SIP endpoint to station 301:



6.3. Verify Avaya Aura™ Communication Manager Configuration

Verify the status of the SIP trunk group by using the "**status trunk n**" command, where "**n**" is the trunk group number administered in **Section 2.4.2.**

Verify that all trunks 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 the SIP signaling groups by using the "**status signaling-group n**" command, where "**n**" is the signaling group number administered in **Section 2.4.1.**

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 defined in **Section 2.4.2** to trace trunk group activity for the SIP trunk between the Session Manager and the Communication Manager Feature Server as shown below:

```
list trace tac #10                                                  Page   1
                                LIST TRACE

time            data

11:44:50     Calling party station    6663000 cid 0x27f
11:44:50     Calling Number & Name 6663000 John Smith
11:44:50     active station    6663000 cid 0x27f
11:44:59     dial 333301 route:AAR
11:44:59     term trunk-group 10    cid 0x27f
11:44:59     dial 333301 route:AAR
11:44:59     route-pattern  10 preference 1  cid 0x27f
11:44:59     seize trunk-group 10 member 7  cid 0x27f
11:44:59     Calling Number & Name NO-CPNumber NO-CPName
11:44:59     Setup digits 333301
11:44:59     Calling Number & Name 6663000 John Smith
11:44:59     Proceed trunk-group 10 member 7  cid 0x27f
11:44:59     Alert trunk-group 10 member 7  cid 0x27f
11:44:59     G711MU ss:off ps:20
             rgn:1 [10.80.100.37]:5004
```

On the Communication Manager Feature Server, use the CM SAT command, '**list trace station xxx'**, where **xxx** is the extension number of the 9600 Series SIP telephone as shown below:

```
list trace station 6663000                                                  Page   1
                                LIST TRACE

time            data

11:46:35     active station    6663000 cid 0x282
11:46:44     dial 333301 route:AAR
11:46:44     term trunk-group 10    cid 0x282
11:46:44     dial 333301 route:AAR
11:46:44     route-pattern  10 preference 1  cid 0x282
11:46:44     seize trunk-group 10 member 8  cid 0x282
11:46:44     Calling Number & Name NO-CPNumber NO-CPName
11:46:44     Setup digits 333301
11:46:44     Calling Number & Name 6663000 John Smith
11:46:44     Proceed trunk-group 10 member 8  cid 0x282
11:46:44     Alert trunk-group 10 member 8  cid 0x282
11:46:44     G711MU ss:off ps:20
             rgn:1 [10.80.100.37]:5004
             rgn:1 [10.80.100.53]:2060
11:46:44     xoip options: fax:Relay modem:off tty:US  uid:0x50006
             rgn:1 [10.80.100.37]:5004      cid 0x27f7fe
```

6.4. Call Scenarios Verified

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

- Verify displays and talkpath for calls between different types of stations on the Communication Manager Access Element and a station on Business Communication Manager.
- Verify displays and talkpath for calls between a SIP phone registered to Session Manager and a station on Business Communication Manager.
- Supplemental Call Features:
    - Verify calls from either a station on Communication Manager Access Element or from a SIP phone registered to Session Manager to an station on Business Communication Manager can be placed on hold.
    - Verify calls from either a station on Communication Manager Access Element or from a SIP phone registered to Session Manager to an station on Business Communication Manager can be transferred to another station on the Business Communication Manager.
    - Verify calls from either a station on Communication Manager Access Element or from a SIP phone registered to Session Manager to a station on Business Communication Manager can create a conference with another station on the Business Communication Manager.
    - Verify calls from either a station on Communication Manager Access Element or from a SIP phone registered to Session Manager to a station on Business Communication Manager can be forwarded to another station on either the same switch or remote switch.
    - Repeat the hold, transfer and conference scenarios with calls originating from a station on Business Communication Manager.
- Long Duration Calls
    - Place a call from either a station on Communication Manager Access Element or from a SIP phone registered to Session Manager to a station on Business Communication Manager. Answer the call, leave the call up for at least 30 minutes, and verify displays and talkpath.
    - Place a call from either a station on Communication Manager Access Element or from a SIP phone registered to Session Manager to a station on Business Communication Manager. Answer the call, put the call on hold for at least 30 minutes, and verify displays and talkpath after returning to the call.
    - Repeat the long duration scenarios with call originating from a station on Business Communication Manager.

6.5. Known Issues

All test calls between stations on Business Communication Manager and remote stations on either the Communication Manager Access Element or SIP phones registered to Session Manager were successful.

However, the following items were observed during the test calls and were identified as known Business Communication Manager issues:

- When stations on Business Communication Manager create a 3-party conference with remote stations, the displays on the Business Communication Manager stations no longer display the name or number of the remote station. Instead, the line number of one of the SIP Trunks and the line number of the Target Line assigned to the station is displayed until the conference ends.
- When calls from stations on Business Communication Manager to remote stations are placed on hold, the displays on the Business Communication Manager stations no longer display the name or number of the remote station. Instead, the number of one of the SIP Trunk lines is displayed.
- When incoming calls from remote stations are forwarded to a second Business Communication Manager station, the name of the remote station is not displayed until the call is answered. During alerting, the line number of the Target Line assigned to the first Business Communication Manager station is displayed.

7. Acronyms

AAR	Automatic Alternative Routing (Routing on Communication Manager)
ARS	Automatic Route Selection
CLAN	Control LAN (Control Card in Communication Manager)
DCP	Digital Communications Protocol
DNIS	Dialed Number identification Service
DHCP	Dynamic Host Configuration Protocol
DTMF	Dual Tone Multi Frequency
FQDN	Fully Qualified Domain Name (hostname for Domain Naming Resolution)
GUI	Graphical User Interface
IMS	IP Multimedia Subsystem
IE	Internet Explorer
IP	Internet Protocol
IPSI	IP-services interface (Control Card in Communication Manager)
LAN	Local Area Network
OAM	Operation, Administration and Maintenance
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SAT	System Access Terminal (Communication Administration Interface)
SIL	Solution Interoperability Lab
SIP	Session Initiation Protocol
SM	Avaya Aura™ Session Manager
SMGR	System Manager (used to configure Session Manager)

SNMP	Simple Network Management Protocol
SRE	SIP Routing Element
SSH	Secure Shell
SSL	Secure Socket Layer
TAC	Trunk Access Code (Communication Manager Trunk Access)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URE	User Relation Element
URL	Uniform Resource Locator
WAN	Wide Area Network
XML	eXtensible Markup Language

8. Conclusions

These Application Notes describe how to configure a network that uses SIP trunks between Avaya Business Communication Manager 50, Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager Access Element and a second Avaya Aura™ Communication Manager operating as a Feature Server. Interoperability testing included verification of bi-directional calls among several different types of endpoints with various features including hold, transfer, and conference.

9. Additional References

This section references the product documentation relevant to these Application Notes.

Session Manager

1) Avaya Aura™ Session Manager Overview, Doc ID 03-603323, available at http://support.avaya.com.
2) Installing and Administering Avaya Aura™ Session Manager, Doc ID 03-603324, available at http://support.avaya.com.
3) Avaya Aura™ Session Manager Case Studies, dated January 2, 2010, available at http://support.avaya.com
4) Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325, available at http://support.avaya.com.

Communication Manager

5) Hardware Description and Reference for Avaya Aura™ Communication Manager (COMCODE 555-245-207) http://support.avaya.com/elmodocs2/comm_mgr/r4_0/avayadoc/03_300151_6/245207_6/245207_6.pdf
6) SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206, May 2009, available at http://support.avaya.com.
7) Administering Avaya Aura™ Communication Manager, Doc ID 03-300509, May 2009, available at http://support.avaya.com.

8) Avaya Toll Fraud Security Guide, Doc ID 555-025-600, February 2010, available at http://support.avaya.com
9) Administering Avaya Aura™ Communication Manager as a Feature Server, Doc ID 03-603479, November 2009, available at http://support.avaya.com

Business Communication Manager

10) BCM50 Administration Guide, Doc ID NN40020-600_02, available at http://support.nortel.com
11) BCM50 Networking Configuration Guide, Doc ID NN40020-603, available at http://support.nortel.com
12) BCM50 Device Configuration Guide, Doc ID NN400200-300, available at http://support.nortel.com
13) IP Phone 1200 Series Installation, Doc ID NN40050-302, available at http://support.nortel.com
14) Business Communications Manager 5.0 – Configuration – System, Doc ID NN40170-501, Rev 02.04, available at http://support.nortel.com

Avaya Application Notes

15) Configuring 9600 Series SIP Phones on Avaya Aura™ Session Manager Release 5.2, available at http://www.avaya.com
16) Configuring multiple Avaya Aura™ Session Managers to address different Network Failure Scenarios, available at http://support.avaya.com
17) Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and Nortel Communication Server 1000, November 2009, available at http://support.avaya.com

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