Avaya Solution & Interoperability Test Lab

Configuring Alcatel OmniPCX Enterprise with Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Manager 6.1 – Issue 1.0

Abstract

These Application Notes present a sample configuration for a network consisting of an Avaya Aura® Communication Manager and Alcatel OmniPCX Enterprise. These two systems are connected via a common Avaya Aura® Session Manager.

Testing was conducted via the Internal Interoperability Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The purpose of this interoperability application note is to validate Alcatel OmniPCX Enterprise (OXE) with Avaya Aura® Communication Manager (CM) which are both connected to an Avaya Aura® Session Manager via a separate SIP Trunk. Voicemail integration between Alcatel OmniPCX Enterprise and Avaya Aura® Messaging was not included in the scope of this Application Notes. The sample network is shown in **Figure 1**, where the Alcatel OmniPCX Enterprise supports the Alcatel ipTouch 4028 / 4038 / 4068 IP Telephones. SIP trunks are used to connect Avaya Aura® Communication Manager and Alcatel OmniPCX Enterprise to Avaya Aura® Session Manager. All inter-system calls are carried over these SIP trunks. Avaya Aura® Session Manager can support flexible inter-system call routing based on dialed number, calling number and system location, and can also provide protocol adaptation to allow for multi-vendor systems to interoperate. Avaya Aura® Session Manager is managed by a separate Avaya Aura® System Manager, which can manage multiple Avaya Aura® Session Managers.

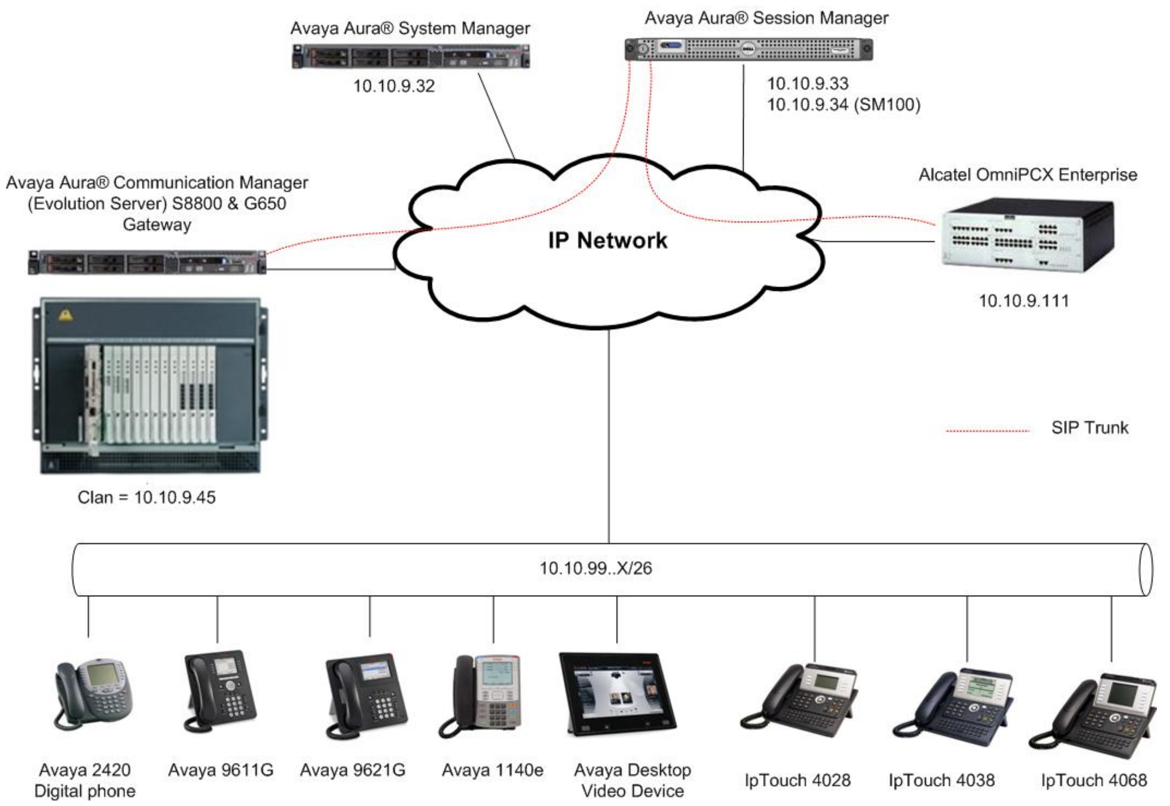


Figure 1: Connection of Alcatel OmniPCX Enterprise and Avaya Aura® Communication Manager via Avaya Aura® Session Manager using SIP Trunks

Alcatel phones are registered to Alcatel OmniPCX Enterprise. Alcatel OmniPCX Enterprise registered stations use extensions 3600x. One SIP trunk is provisioned to the Avaya Aura® Session Manager to manage calls to/from Alcatel OmniPCX Enterprise. One SIP trunk is provisioned to the Avaya Aura® Session Manager to manage calls to/from Avaya Aura® Communication Manager.

2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration:

Hardware Component	Software Version
Avaya S8800 Media Servers with G650 Media Gateway	Avaya Aura® Communication Manager 6.0.1 (R016x.00.1.510.1)
Avaya S8510 Server	Avaya Aura® Session Manager 6.1 SP0
Avaya S8800 Server	Avaya Aura® System Manager 6.1 SP0
Avaya A175 Desktop Video Device	1.0.1
Avaya 1140 IP Telephone (SIP)	04.00.04.00
Avaya 96x1 IP Telephone (SIP)	6.1 SP2
Avaya 96x1 IP Telephone (H.323)	6.0 SP2
Avaya 2420 Digital Telephone	-
Alcatel OmniPCX Enterprise	9.1 (I1.605-16-c)
Alcatel ipTouch NOE Telephone	4.20.71

3. Configure Avaya Aura® Communication Manager

This section shows the configuration in Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). These Application Notes assumed that the basic configuration has already been administered. For further information on Communication Manager, please consult with reference **Error! Reference source not found.**. The procedures include the following areas:

- Verify Avaya Aura® Communication Manager License
- Administer System Parameters Features
- Administer IP Node Names
- Administer IP Network Region and Codec Set
- Administer SIP Signaling Group and Trunk Group
- Administer Route Pattern
- Administer Private Numbering
- Administer Locations
- Administer Dial Plan and AAR analysis
- Save Changes

3.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameter customer options** command to compare 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.

Note: The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                      Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 30    0
           Maximum Concurrently Registered IP Stations: 18000 9
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                        Maximum Video Capable Stations: 10    1
                    Maximum Video Capable IP Softphones: 10    4
                       Maximum Administered SIP Trunks: 100   55
```

3.2. Administer System Parameters Features

Use the **change system-parameters features** command to allow for trunk-to-trunk transfers. This feature is needed to allow for transferring an incoming/outgoing call from/to a remote switch back out to the same or different 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: This feature poses significant security risk and must be used with caution. As an alternative, the trunk-to-trunk feature can be implemented using Class Of Restriction or Class Of Service levels.

```
change system-parameters features                               Page   1 of  18
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
                             Music/Tone on Hold: none
              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n
```

3.3. Administer IP Node Names

Use the **change node-names ip** command to add entries for Communication Manager and Session Manager that will be used for connectivity. In the sample network, **clan** and **10.10.9.45** are entered as **Name** and **IP Address** for the CLAN card in Communication Manager running on the Avaya S8800 Server. In addition, **sm100** and **10.10.9.34** are entered for Session Manager.

```
change node-names ip                                             Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
sm100               10.10.9.34
clan                10.10.9.45
default             0.0.0.0
gateway             10.10.9.1
medpro              10.10.9.46
procr               10.10.9.42
procr6              ::
```

3.4. Administer IP Network Region and Codec Set

Use the **change ip-network-region n** command, where **n** is the network region number to configure the network region being used. In the sample network, ip-network-region 1 is used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise and a descriptive **Name** for this ip-network-region. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec Set** to **1** to use ip-codec-set 1.

```
change ip-network-region 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: mmsil.local
    Name: To ASM61
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: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Use the **change ip-codec-set n** command, where **n** is the existing codec set number to configure the desired audio codec.

```
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
```

3.5. Administer SIP Signaling Group and Trunk Group

3.5.1. SIP Signaling Group

In the test configuration, Communication Manager acts as an Evolution Server. An IMS enabled SIP trunk is not required. Use signal group 150 along with trunk group 150 to reach the Session Manager. Use the **add signaling-group n** command, where **n** is the signaling-group number being added to the system. Use the values defined in **Section 3.3** and **3.4** for **Near-end Node Name**, **Far-End Node-Name** and **Far-End Network Region**. The **Far-end Domain** is left blank so that the signaling group accepts any authoritative domain. Set **IMS Enabled** to **n** and **Peer Detection Enabled** to **y**.

```
add signaling-group 150                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 150            Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                             SIP Enabled LSP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: clan                  Far-end Node Name: sm100
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1

Far-end Domain:
                                             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                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

3.5.2. SIP Trunk Group

Use the **add trunk-group n** command, where **n** is the new trunk group number being added to the system. The following screens show the settings used for trunk group 150. Enter the following:

- **Group Type** sip
- **TAC** a numeric value i.e. **150**
- **Service Type** **tie**
- **Signaling Group** the signaling group defined in **Section 3.5.1**, i.e. **150**
- **Number of Members** set to a numeric value, i.e. **10**

```
add trunk-group 150                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 150                  Group Type: sip          CDR Reports: y
  Group Name: Trunk 150                   COR: 1        TN: 1        TAC: 150
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 150
                                                     Number of Members: 10
```

Navigate to **Page 3** and enter **private** for **Numbering Format**.

```
add trunk-group 150                                           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

                                Modify Tandem Calling Number: no
 Show ANSWERED BY on Display? y
```

Navigate to P**age 4** and enter **97** for **Telephone Event Payload Type** and **From** for **Identity for Calling Party Display.**

```
add trunk-group 150                                           Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? y
                Network Call Redirection? n
                   Send Diversion Header? n
                 Support Request History? y
            Telephone Event Payload Type: 97


       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: From
                             Enable Q-SIP? n
```

3.6. Administer Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use the **change route-pattern n** command, where **n** is the route pattern number specified in **Section 3.9**. Configure this route pattern to route calls to trunk group number **150** configured in **Section 3.5.2.** Assign the lowest **FRL** (facility restriction level) to allow all callers to use this route pattern. Assign **0** to **No. Del Dgts**.

```
change route-pattern 150                                        Page   1 of   3
                    Pattern Number: 150 Pattern Name: 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: 150  0                   0                                          n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    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            unre                                        none
 2: y y y y y n  n            rest                                        none
 3: y y y y y n  n            rest                                        none
 4: y y y y y n  n            rest                                        none
```

3.7. Administer Private Numbering

Use the **change private-numbering** command to define the calling party number to be sent out through the SIP trunk. In the sample network configuration below, all calls originating from a 5-digit extension beginning with **40** and **41** will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

```
change private-numbering 0                                     Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext           Trk        Private          Total
Len Code          Grp(s)     Prefix           Len
 5  40                                         5     Total Administered: 4
 5  41                                         5        Maximum Entries: 540
```

3.8. Administer Locations

Use the change locations command to define the proxy route to use for outgoing calls. In the sample network the proxy route will be the trunk group defined in **Section 3.5.2**.

```
change locations                                                Page   1 of   1
                                   LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y

 Loc  Name          Timezone Rule  NPA                                Proxy Sel
 No                  Offset                                             Rte Pat
 1:  Main           + 00:00   0                                         150
```

3.9. Administer Dial Plan and AAR analysis

Configure the dial plan for dialing 5-digit extensions beginning with **36** to stations registered with Alcatel OXE. Use the **change dialplan analysis** command to define **Dialed String 36** as an **aar Call Type**.

```
change dialplan analysis                                         Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1           3   dac
   36          5   aar
   39990       5   ext
   39995       5   aar
   40          5   ext
   41          5   ext
   6           3   fac
   7           5   ext
   *           2   fac
   #           2   fac
```

Use the **change aar analysis 0** command to configure an **aar** entry for **Dialed String 36** to use **Route Pattern 150.** Add an entry for the SIP phone extensions which begin with **41**. Use **unku** for **call type**.

```
change aar analysis 0                                            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
    36                    5    5     150      unku         n
    3999                  5    5     150      unku         n
    41                    5    5     150      unku         n
```

3.10. Save Changes

Use the **save translation** command to save all changes.

```
save translation

                               SAVE TRANSLATION

           Command Completion Status                         Error Code

           Success                                           0
```

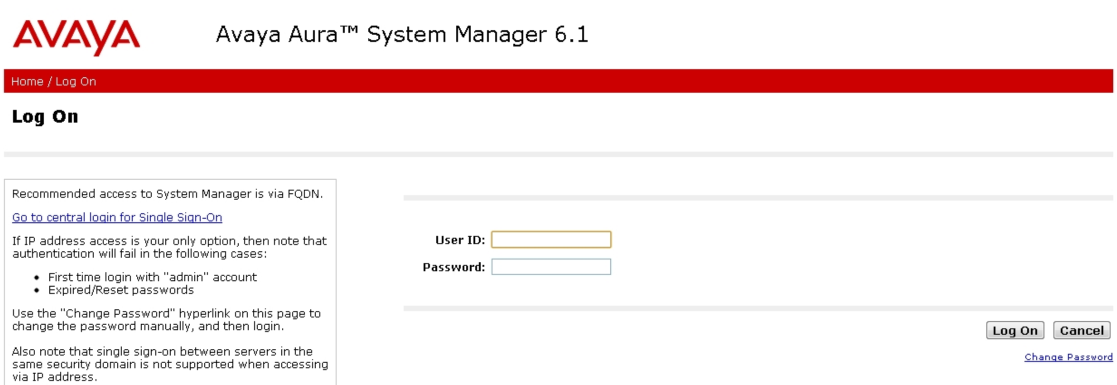
4. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. For further information on Session Manager, please consult with references **[1]**, **[2]**, and **[3]**. The procedures include the following areas:

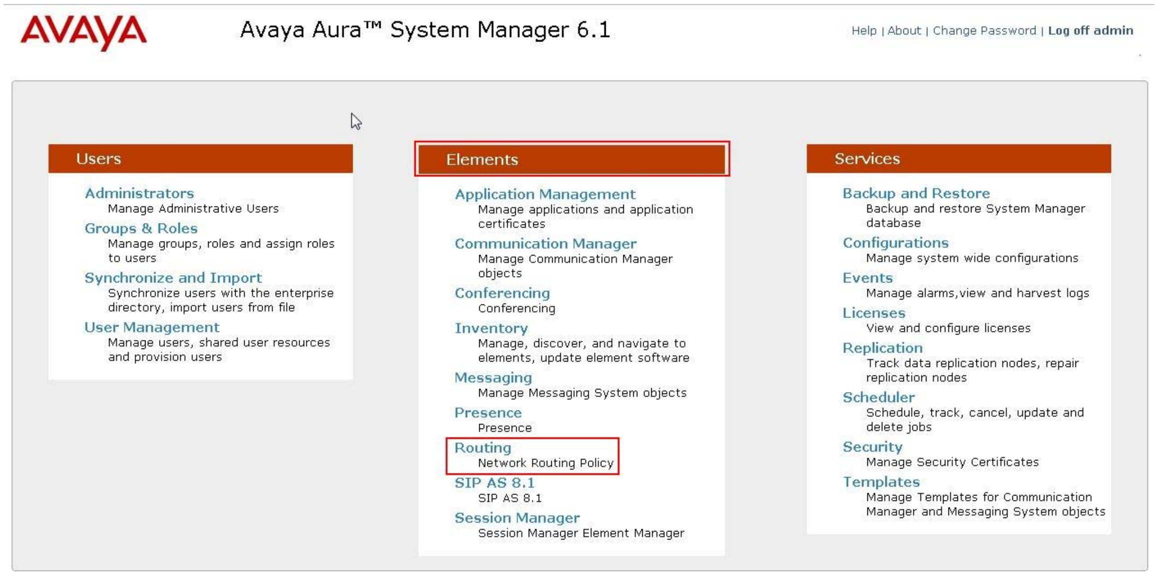
- Log in to Avaya Aura® Session Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Aura® Session Manager
- Add Avaya Aura® Communication Manager as an Evolution Server
- Administer SIP users

4.1. Log in to Avaya Aura® Session Manager

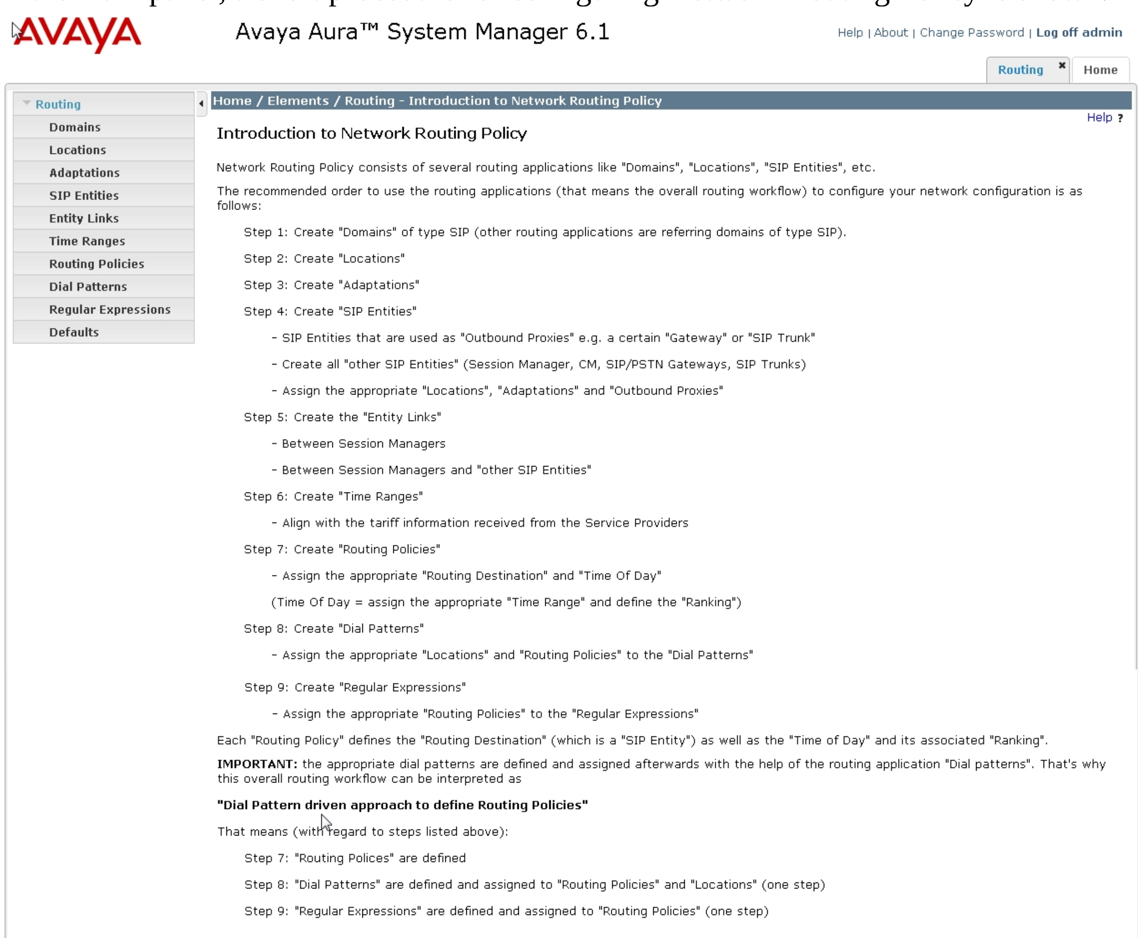
Access the System Manager using a Web Browser and entering ***http://<ip-address>/SMGR***, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials.



In the next screen under **Elements** column select **Routing**.



In the main panel, a short procedure for configuring Network Routing Policy is shown.

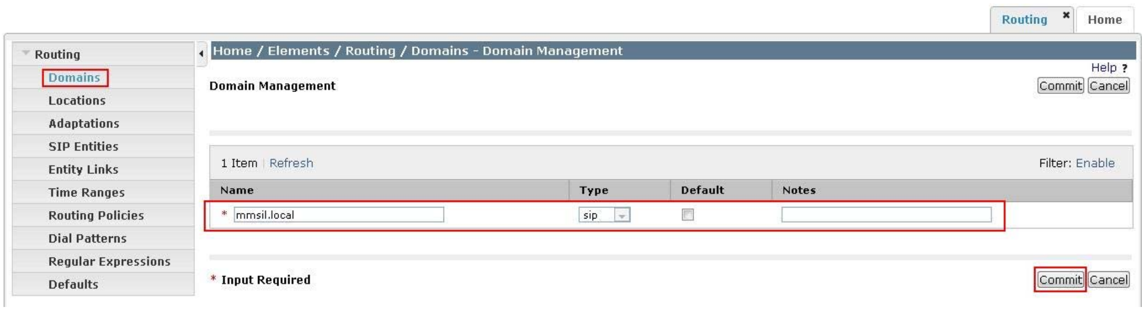


4.2. Administer SIP Domain

Add the SIP domain, for which the communications infrastructure will be authoritative, by selecting **Domains** on the left panel menu and clicking the **New** button (not shown) to create a new SIP domain entry. Complete the following options:

- **Name** The authoritative domain name (e.g., **mmsil.local**)
- **Type** **SIP**
- **Notes** Description for the domain (optional)

Click **Commit** to save changes.



4.3. Administer Locations

Session Manager uses the origination location to determine which dial patterns to look at when routing the call if there are dial patterns administered for specific locations. Locations are also used to limit the number of calls coming out of or going to a physical location. This is useful for those locations where the network bandwidth is limited. To add a Location, select **Locations** on the left panel menu and then click the **New** button (not shown). Enter the following for each **Location**:

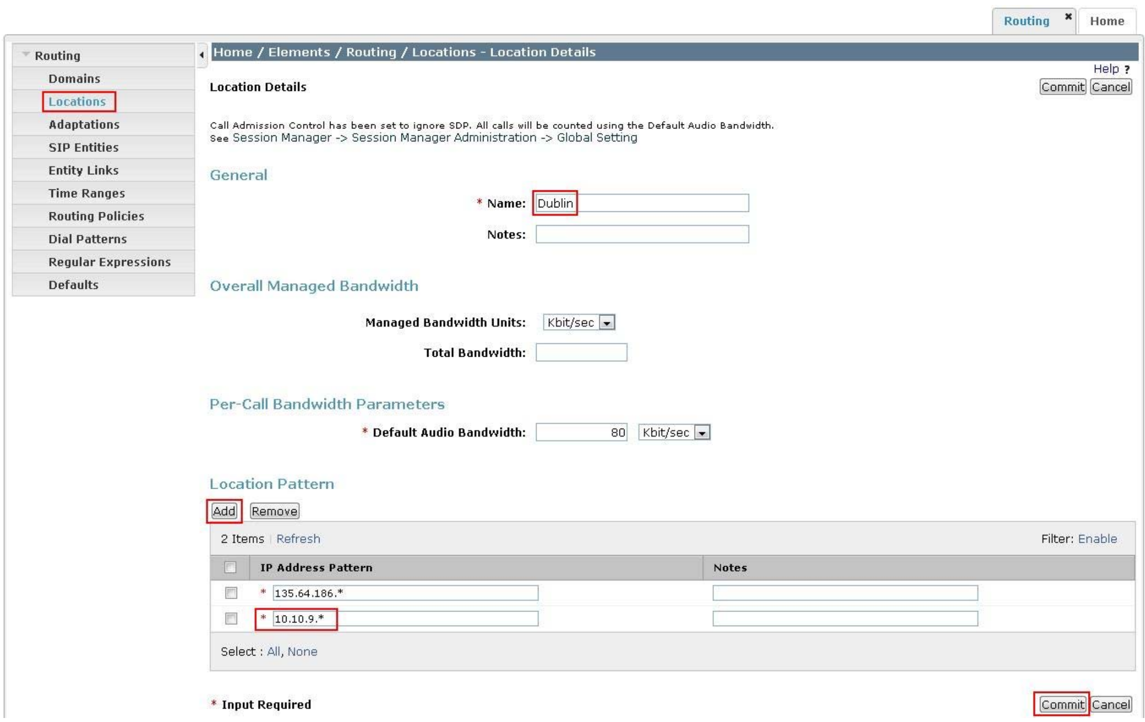
Under **General:**

- **Name** An informative name (e.g. Dublin)

Under **Location Pattern:**

- **IP Address Pattern** An IP address pattern for this location

Select **Add** to add more locations. Click **Commit** to save changes.

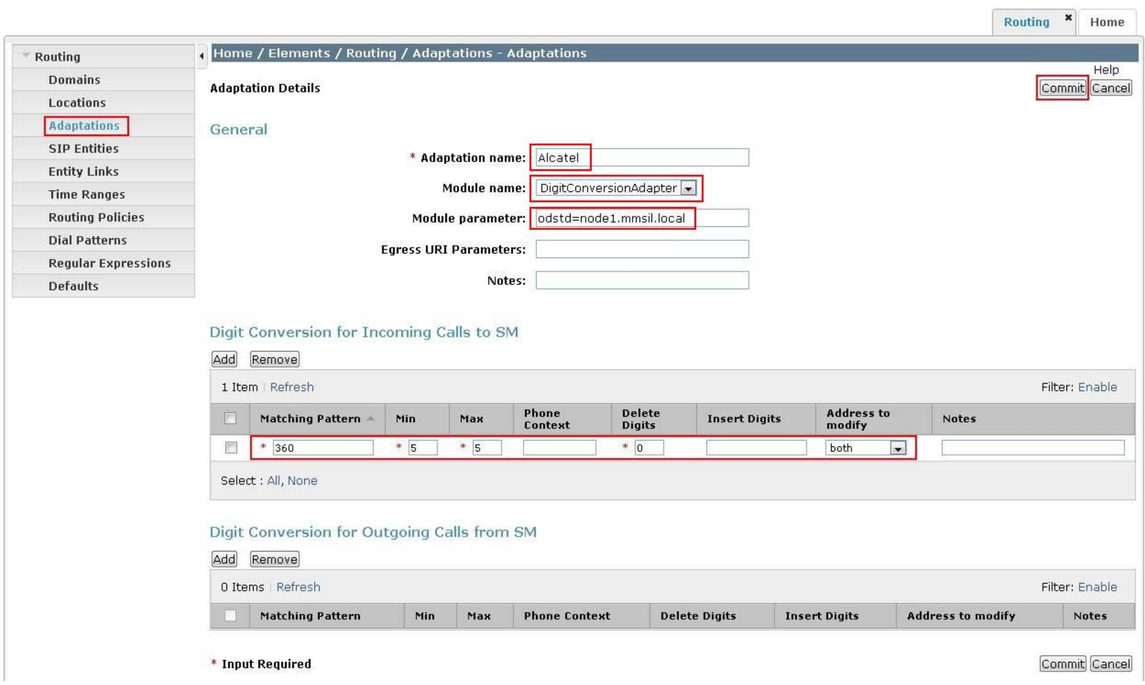


4.4. Administer Adaptations

Create an adaptation entry for a call to Alcatel OXE. For the Alcatel OXE adaptation, enter the following information:

- **Name** — An informative name for the adaptation
- **Adaptation Module** — Enter a DigitConversionAdapter to ensure the request URI domain on outgoing calls to Alcatel OXE is node1.mmsil.local (the Alcatel FQDN). See **Section 5.2**
- **Digit Conversion for incoming Calls to SM** — Matching Pattern **360** with a minimum and maximum of 5 digits long, which is the dial pattern for a station registered with Alcatel OXE. Delete Digits has value **0** to indicate no digits are to be deleted.

Click **Commit** to save changes.



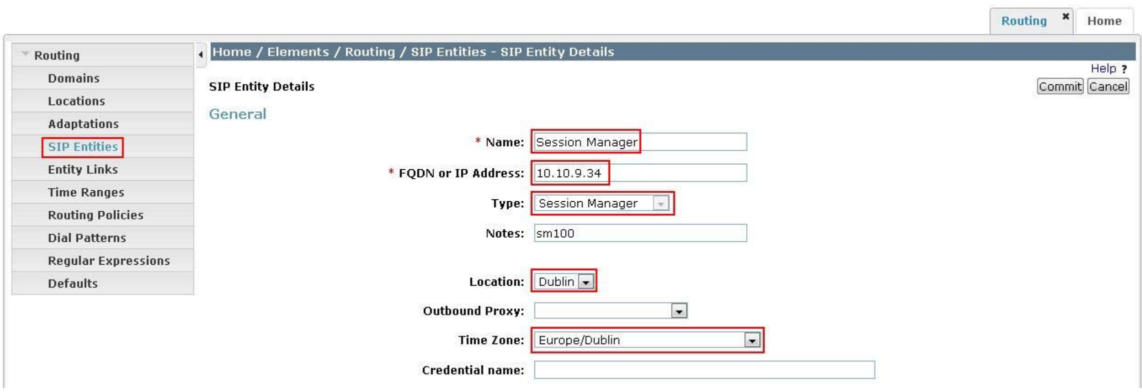
4.5. Administer SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by a SIP Trunk. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). Enter the following for each SIP Entity:

Under **General:**

- **Name** — An informative name (e.g., **SessionManager**)
- **FQDN or IP Address** — IP address of the signaling interface on the Session Manager, CM or OXE.
- **Type** — **Session Manager** for Session Manager, **CM** for CM and **SIP Trunk** for OXE.
- **Location** — **Dublin**
- **Time Zone** — Time zone for this location

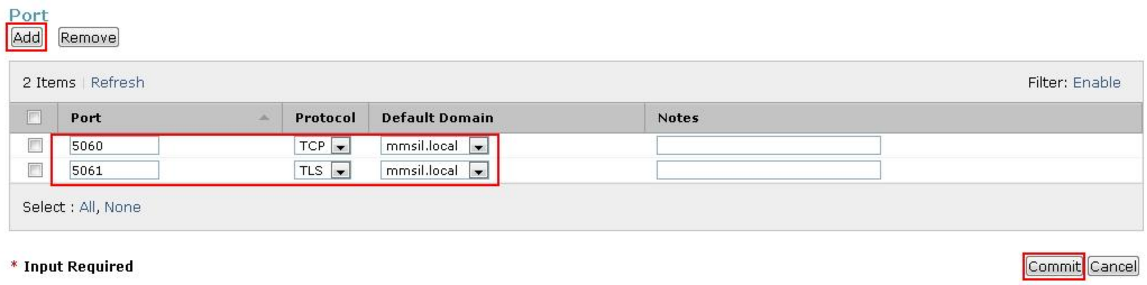
The following screen shows the SIP Entity for Session Manager.



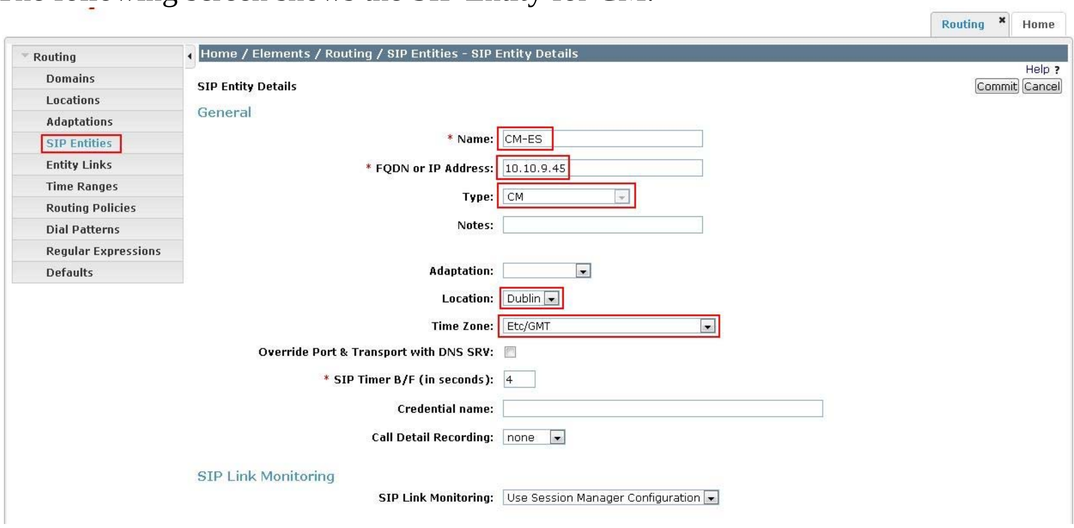
Under **Port**, click **Add,** and then edit the fields in the resulting new row.

- **Port** Port number on which the system listens for SIP requests
- **Protocol** Transport protocol to be used to send SIP requests

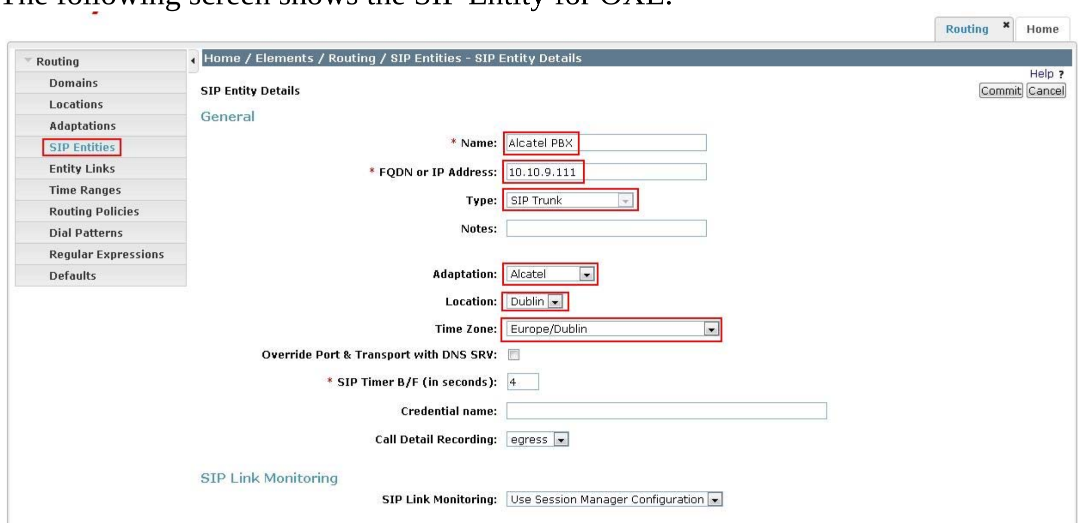
The following screen shows the Port definitions for the Session Manager SIP Entity. Click **Commit** to save changes.



The following screen shows the SIP Entity for CM.



The following screen shows the SIP Entity for OXE.

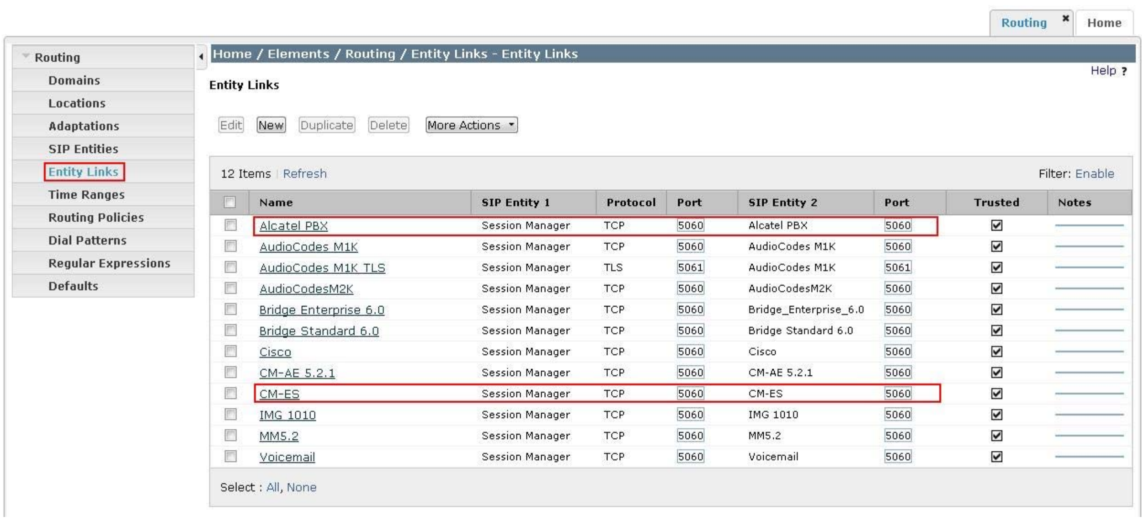


4.6. Administer Entity Links

A SIP trunk between a Session Manager and a telephony system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- **Name** An informative name
- **SIP Entity 1** Select **SessionManager**
- **Port** Port number to which the other system sends its SIP requests
- **SIP Entity 2** The other SIP Entity for this link, created in **Section 4.5**
- **Port** Port number to which the other system expects to receive SIP requests
- **Trusted** Whether to trust the other system
- **Protocol** Transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in the sample network.



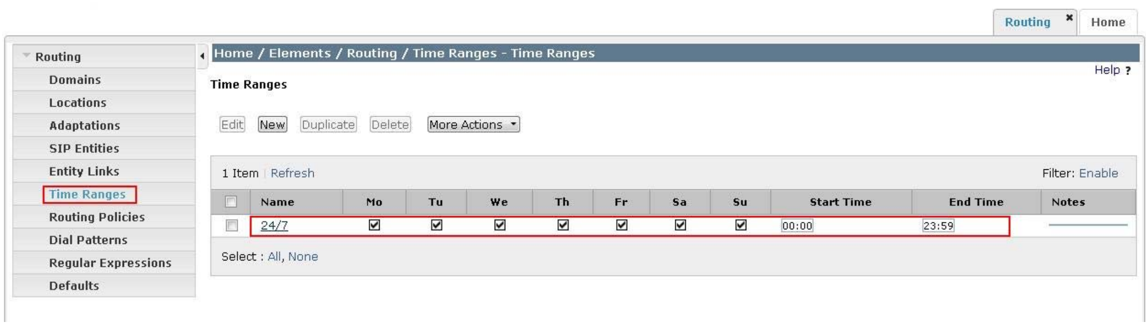
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
Alcatel PBX	Session Manager	TCP	5060	Alcatel PBX	5060	☑	
AudioCodes M1K	Session Manager	TCP	5060	AudioCodes M1K	5060	☑	
AudioCodes M1K TLS	Session Manager	TLS	5061	AudioCodes M1K	5061	☑	
AudioCodesM2K	Session Manager	TCP	5060	AudioCodesM2K	5060	☑	
Bridge Enterprise 6.0	Session Manager	TCP	5060	Bridge_Enterprise_6.0	5060	☑	
Bridge Standard 6.0	Session Manager	TCP	5060	Bridge Standard 6.0	5060	☑	
Cisco	Session Manager	TCP	5060	Cisco	5060	☑	
CM-AE 5.2.1	Session Manager	TCP	5060	CM-AE 5.2.1	5060	☑	
CM-ES	Session Manager	TCP	5060	CM-ES	5060	☑	
IMG 1010	Session Manager	TCP	5060	IMG 1010	5060	☑	
MM5.2	Session Manager	TCP	5060	MM5.2	5060	☑	
Voicemail	Session Manager	TCP	5060	Voicemail	5060	☑	

4.7. Administer Time Ranges

Before adding routing policies (see next step), time ranges must be defined during which the policies will be active. To add this time range, select **Time Ranges** from the left panel menu and then click **New** on the right. Fill in the following fields.

- **Name** An informative name (e.g. always)
- **Mo** through **Su** Check the box under each day of the week for inclusion
- **Start Time** Enter start time (e.g. **00:00** for start of day)
- **End Time** Enter end time (e.g. **23:59** for end of day)

In Session Manager, a default policy (**24/7**) is available that would allow routing to occur at anytime. This time range was used in the sample network.



4.8. Administer Routing Policies

Create routing policies to direct how calls will be routed to a system. Two routing policies must be added, one for Communication Manager (H.323 and Digital phones) and one for Alcatel OXE. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

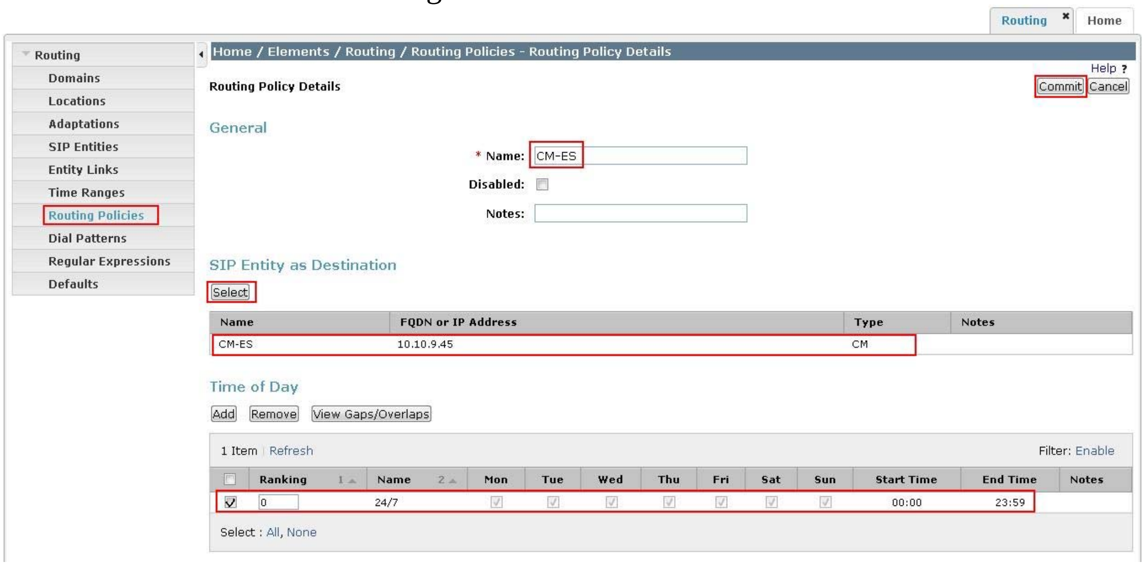
Under **General:**

- Enter an informative **Name**
- Under **SIP Entity as Destination:**
- Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

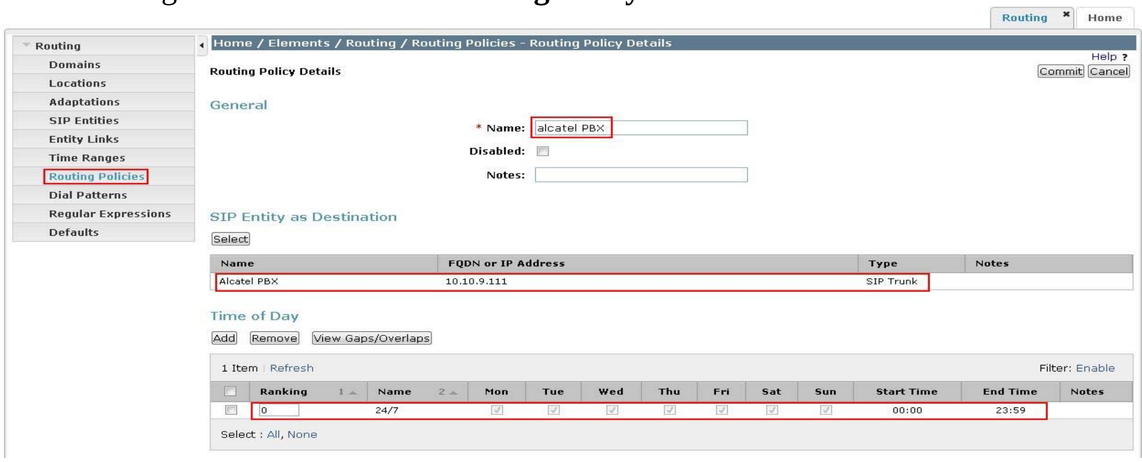
Under **Time of Day:**

- Click **Add**, and then select the time range configured in the **Section 4.7.**

Click **Commit** to save changes. The following screen shows the **Routing Policy Details** for calls to Communication Manager.



The following is screen shows the **Routing Policy Details** for Alcatel OXE.

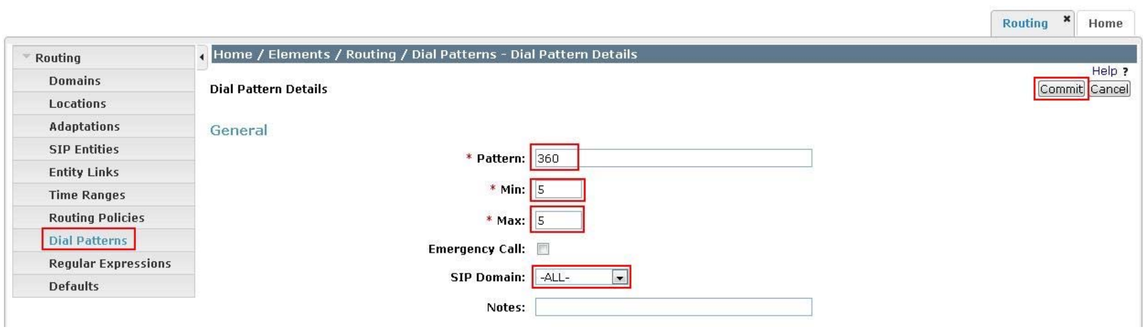


4.9. Administer Dial Patterns

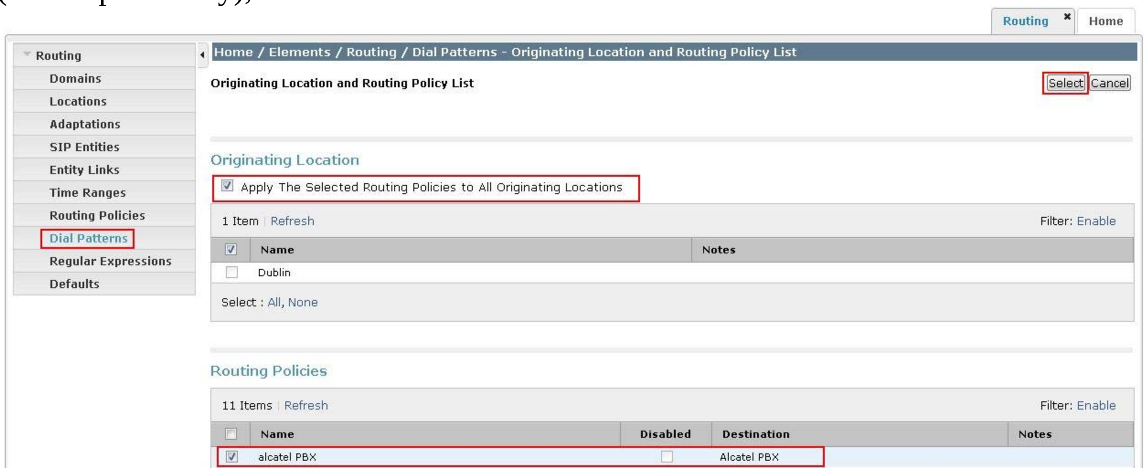
A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample network, 5-digit extensions beginning with **360** reside on Alcatel OXE and 5-digit extensions beginning with **40** (H.323 and Digital phones) reside on CM. To configure the Alcatel OXE Dial Pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General:**

- **Pattern** Dialed number or prefix
- **Min** Minimum length of dialed number
- **Max** Maximum length of dialed number
- **Notes** Comment on purpose of dial pattern
- **SIP Domain** Select **ALL**



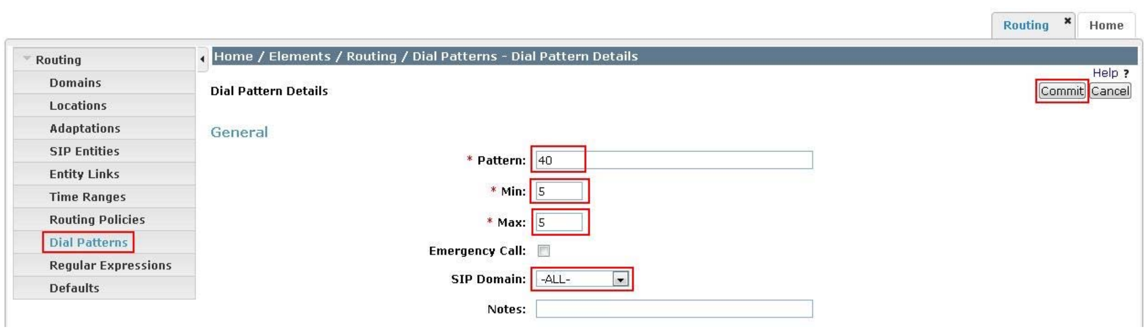
Navigate to **Originating Locations and Routing Policy List** and select **Add** (not shown). Under **Originating Location** select **Apply The Selected Routing Policies to All Originating Locations** and under **Routing Policies** select **Alcatel PBX.** Click **Select** button to confirm the chosen options and then be returned to the Dial Pattern screen (shown previously), select **Commit** button to save.



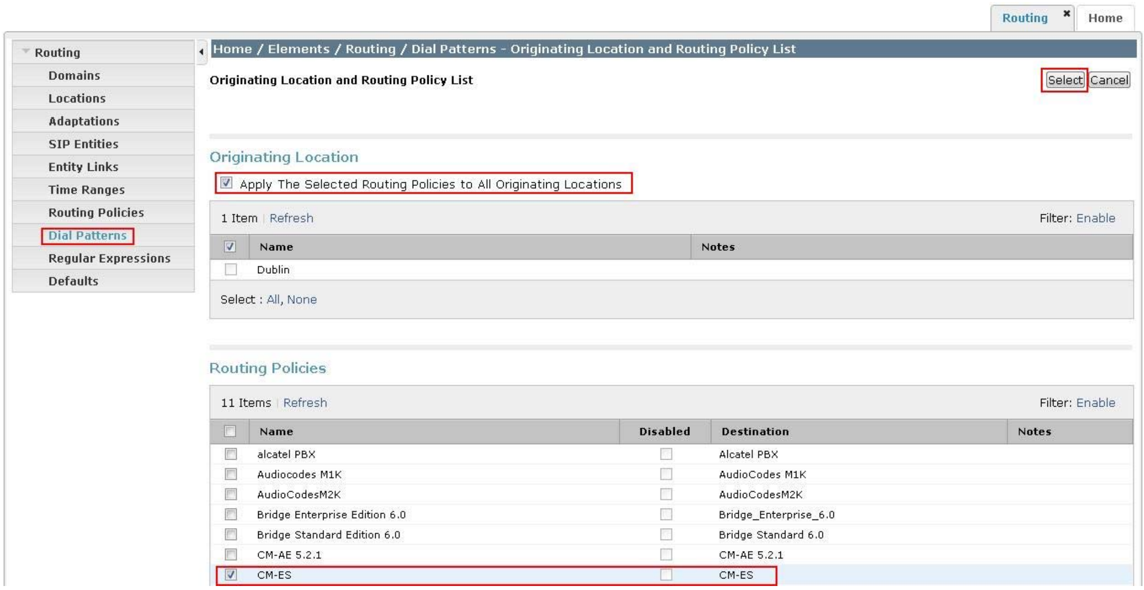
A dial pattern must be defined that will direct calls to CM (H.323 and Digital phones). To configure the CM Dial Pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General:**

- **Pattern** Dialed number or prefix
- **Min** Minimum length of dialed number
- **Max** Maximum length of dialed number
- **Notes** Comment on purpose of dial pattern
- **SIP Domain** Select **ALL**

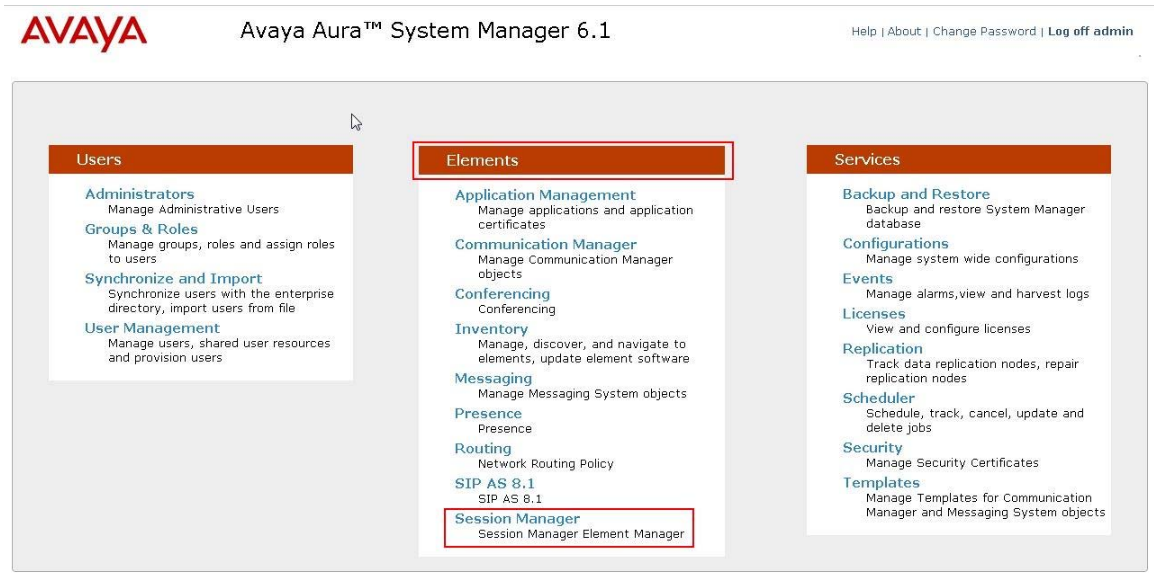


Navigate to **Originating Locations and Routing Policy List** and select **Add** (not shown). Under **Originating Location** select all locations by checking the box next to **Apply The Selected Routing Policies to All Originating Locations** and under **Routing Policies** select the Routing Policy created for CM in **Section 4.8**. Click **Select** button to confirm the chosen options and then be returned to the Dial Pattern screen (shown above), select **Commit** button to save.



4.10. Administer Avaya Aura® Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. On the SMGR management screen under the **Elements** column select **Session Manager**.



In the left panel on the next screen, select **Session Manager Administration** and in the right panel under **Session Manager Instances** select **New** (not shown). Fill in the fields as described below and shown in the following screen:

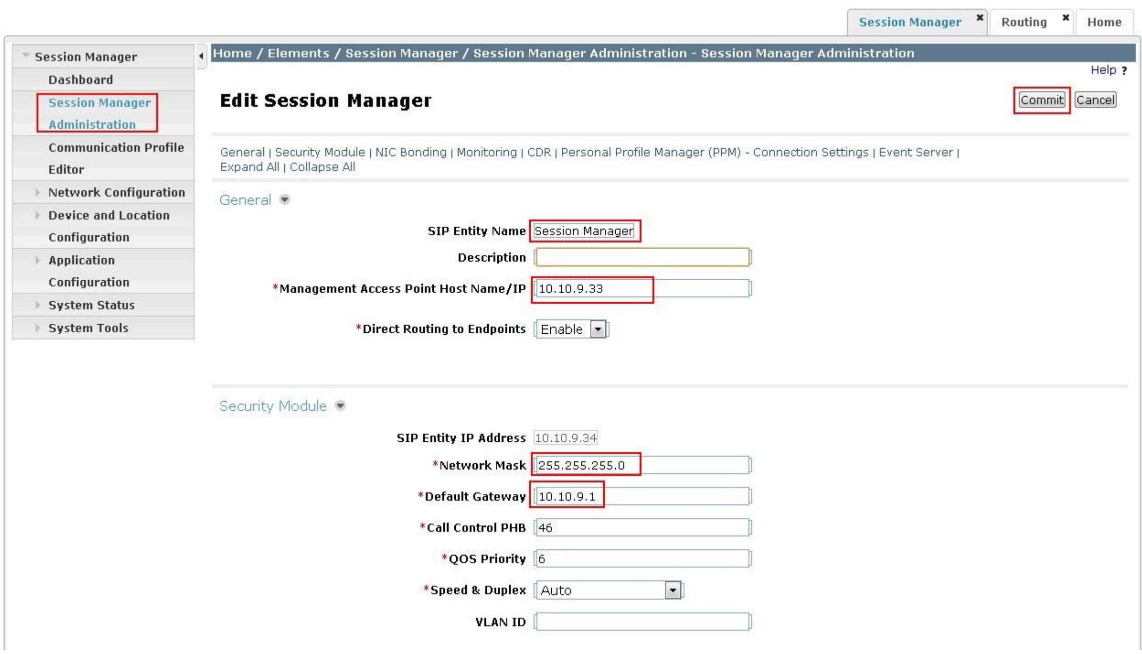
Under **General:**

- **SIP Entity Name** Select the name of the SIP Entity added for Session Manager
- **Description** Descriptive comment (optional)
- **Management Access Point Host Name/IP** Enter the IP address of the Session Manager management interface

Under **Security Module:**

- **Network Mask** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.

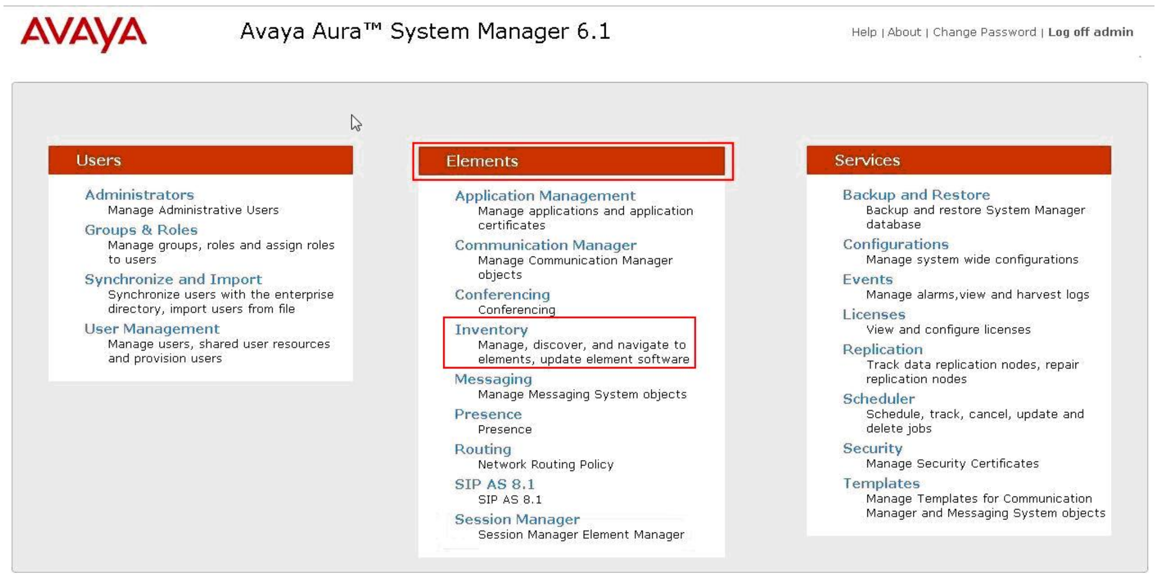


4.11. Add Avaya Aura® Communication Manager as an Evolution Server

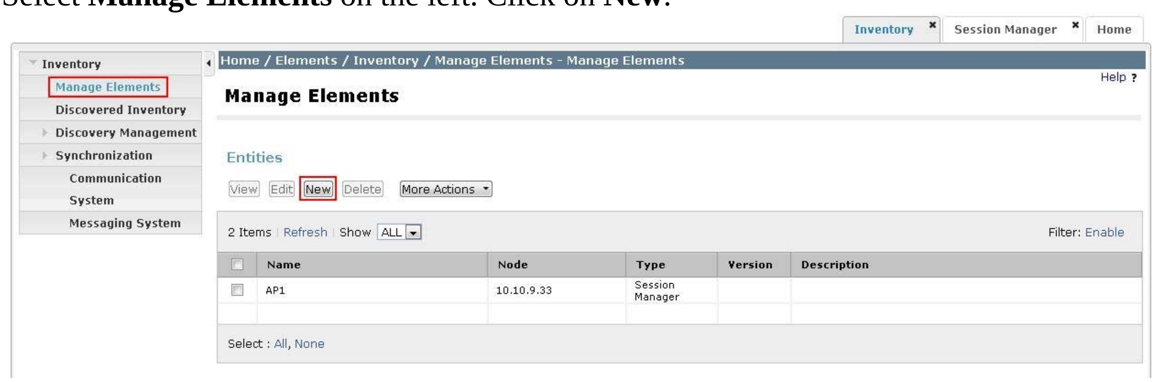
In order for Communication Manager to provide configuration and Evolution Server support to SIP phones when they register to Session Manager, Communication Manager must be added as an application.

4.11.1. Create a CM Instance

On the SMGR management screen under the **Elements** column select **Inventory**.



Select **Manage Elements** on the left. Click on **New**.

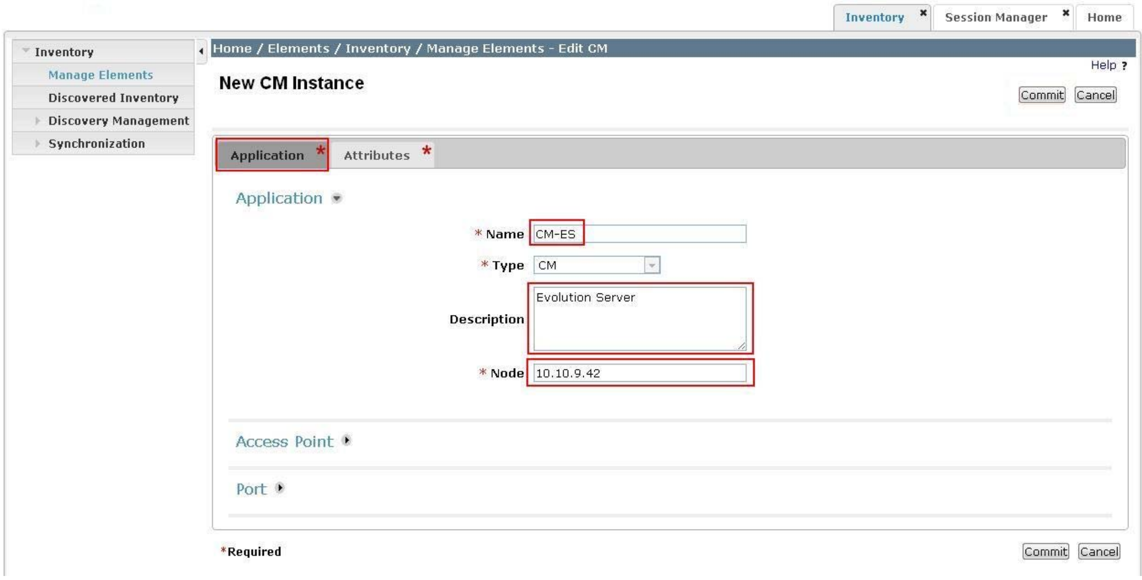


On the next screen (not shown), for **Type** select **CM**.

Click on the **Applications** tab and enter the following fields. Use defaults for the remaining fields:

- **Name** A descriptive name
- **Description** A description of the CM instance

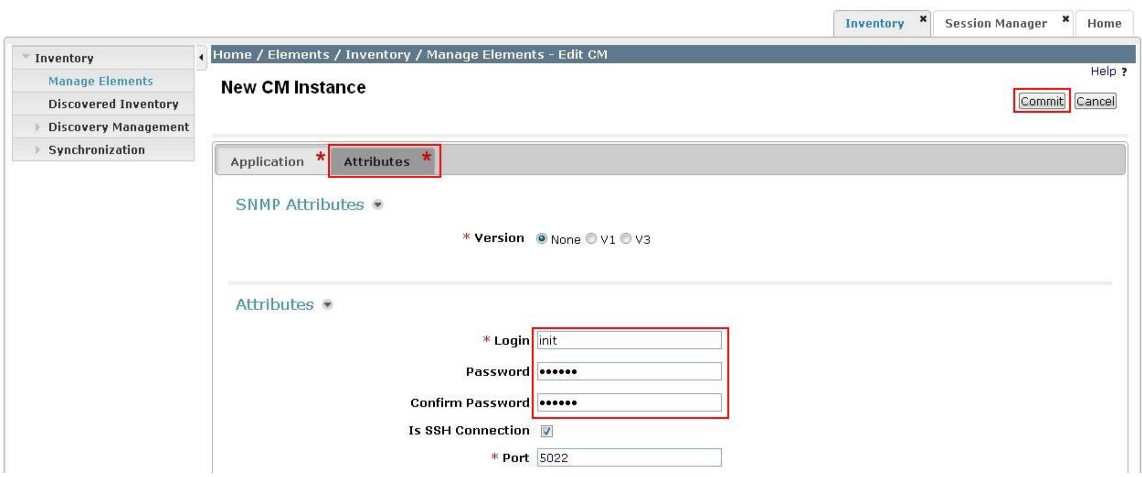
- **Node** Enter the IP address for CM SAT access



Click on the **Attributes** tab and enter the following:

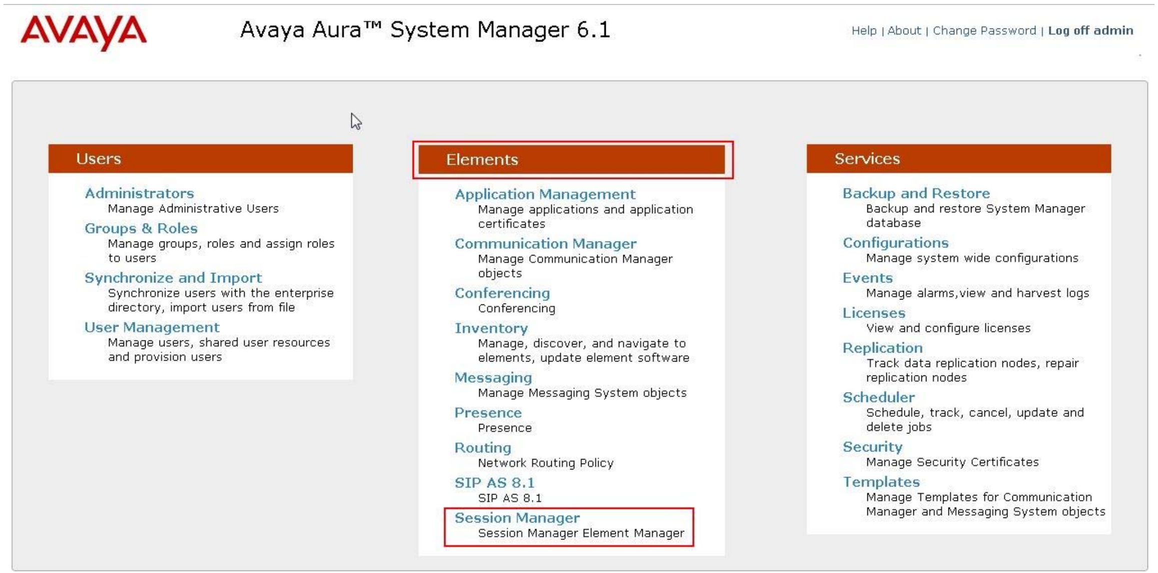
- **Login** Login used for SAT access
- **Password** Password used for SAT access
- **Confirm Password** Password used for SAT access

Click on **Commit** to save.



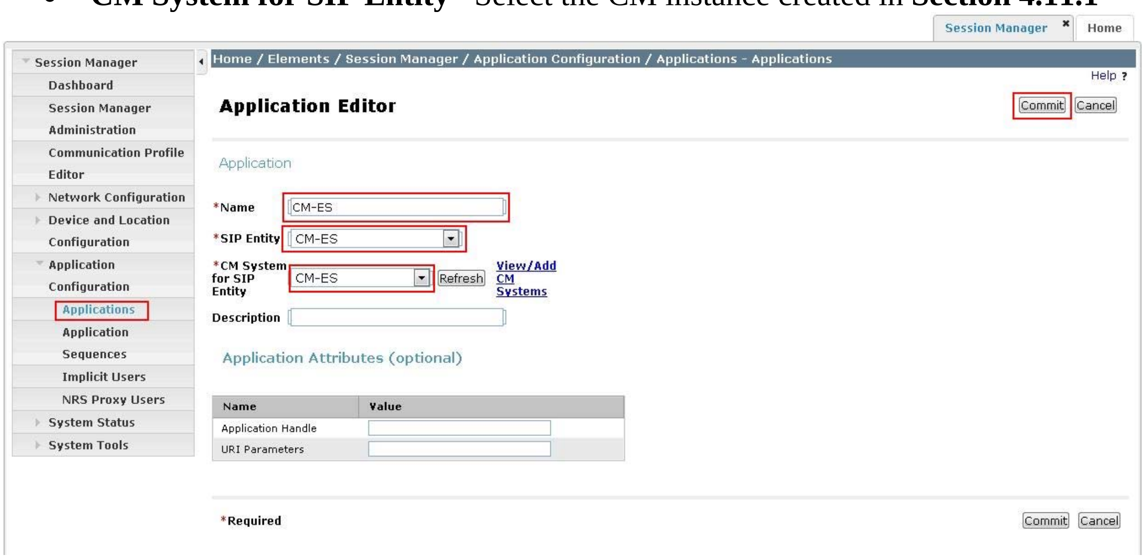
4.11.2. Create an Evolution Server Application

On the SMGR management screen under the **Elements** column select **Session Manager**.



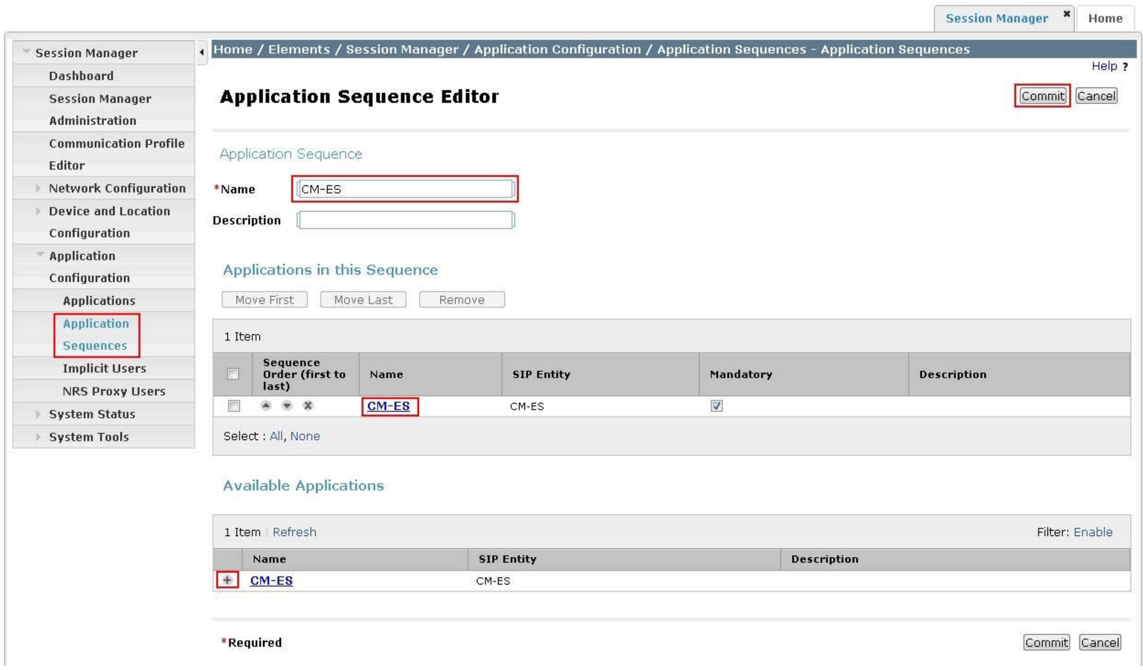
Select **Application Configuration → Applications** on the left menu. Click on **New** (not shown). Enter following fields and use defaults for the remaining fields. Click on **Commit** to save.

- **Name** A descriptive name
- **SIP Entity** Select the CM SIP Entity defined in **Section 4.5**
- **CM System for SIP Entity** Select the CM instance created in **Section 4.11.1**



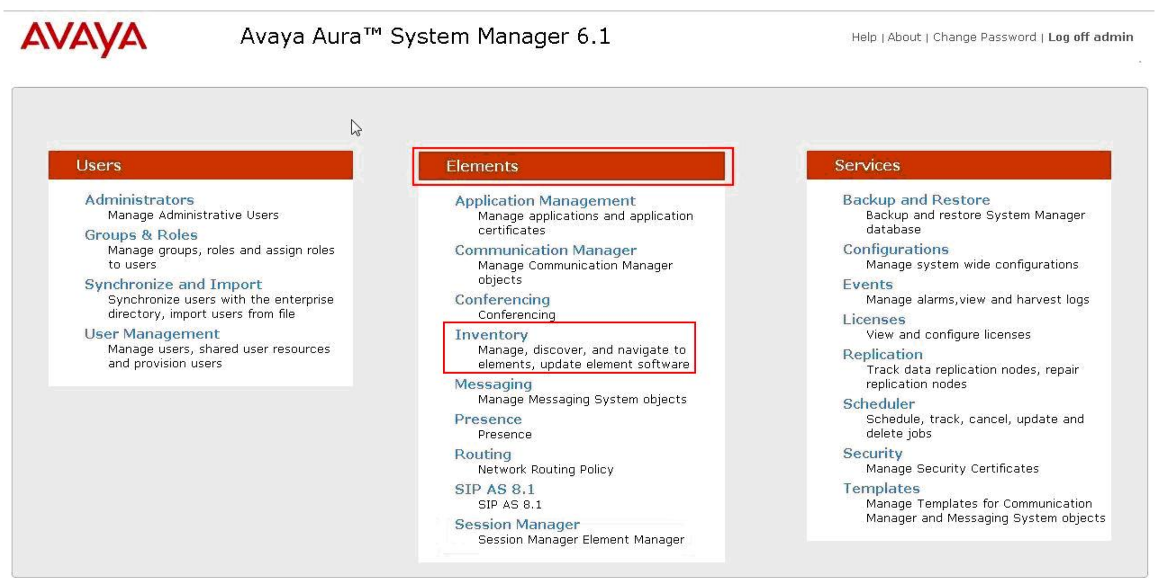
4.11.3. Create an Evolution Server Application Sequence

Select **Application Configuration → Application Sequences** on the left menu. Click on **New** (not shown). Enter a descriptive **Name**. Click on the + sign next to the appropriate **Available Applications** and they will move up to the **Applications in this Sequence** section. Click on **Commit** to save.

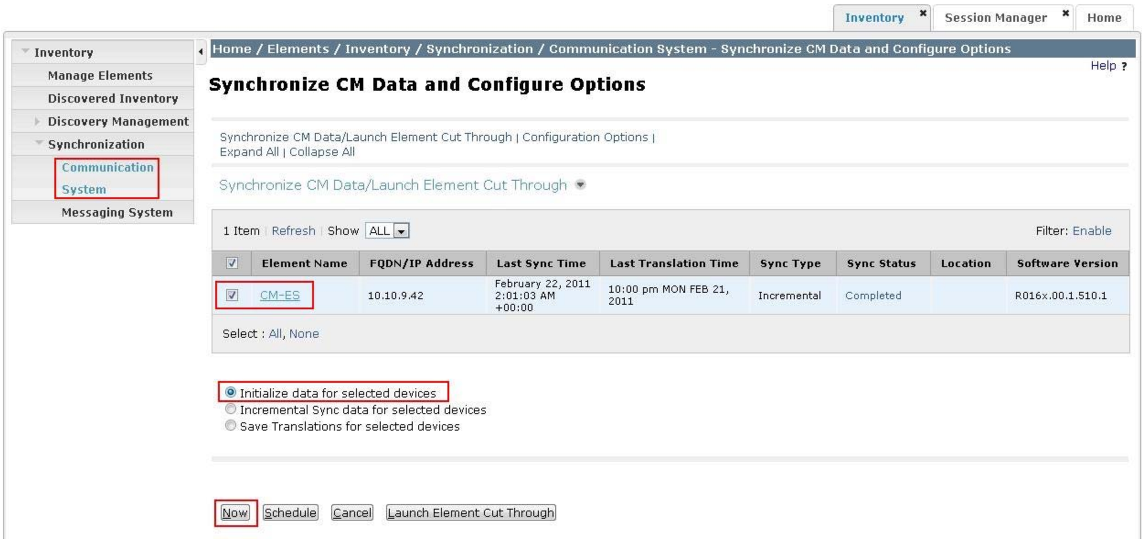


4.11.4. Synchronize Avaya Aura® Communication Manager Data

On the SMGR management screen under the **Elements** column select **Inventory**.

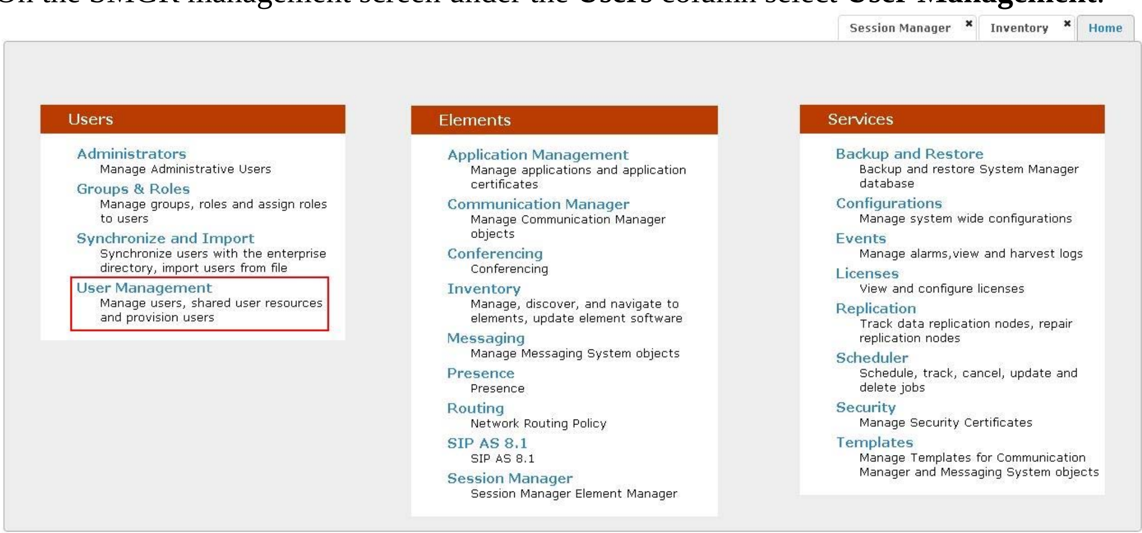


Select **Synchronization → Communication System** on the left. Select the appropriate **Element Name**. Select **Initialize data for selected devices**. Then click on **Now**. This may take some time.

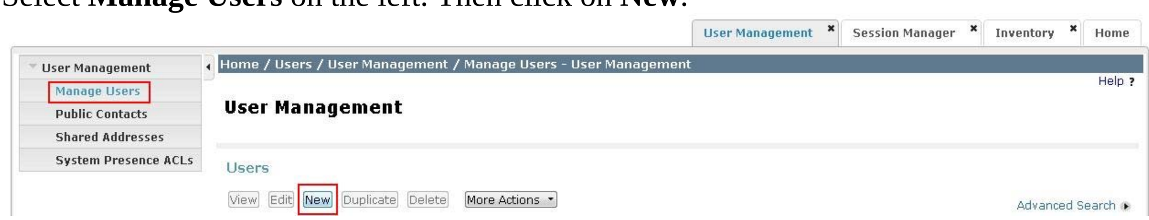


4.12. Administer SIP Users

SIP users must be added via Session Manager and the details will be updated on the CM. On the SMGR management screen under the **Users** column select **User Management**.

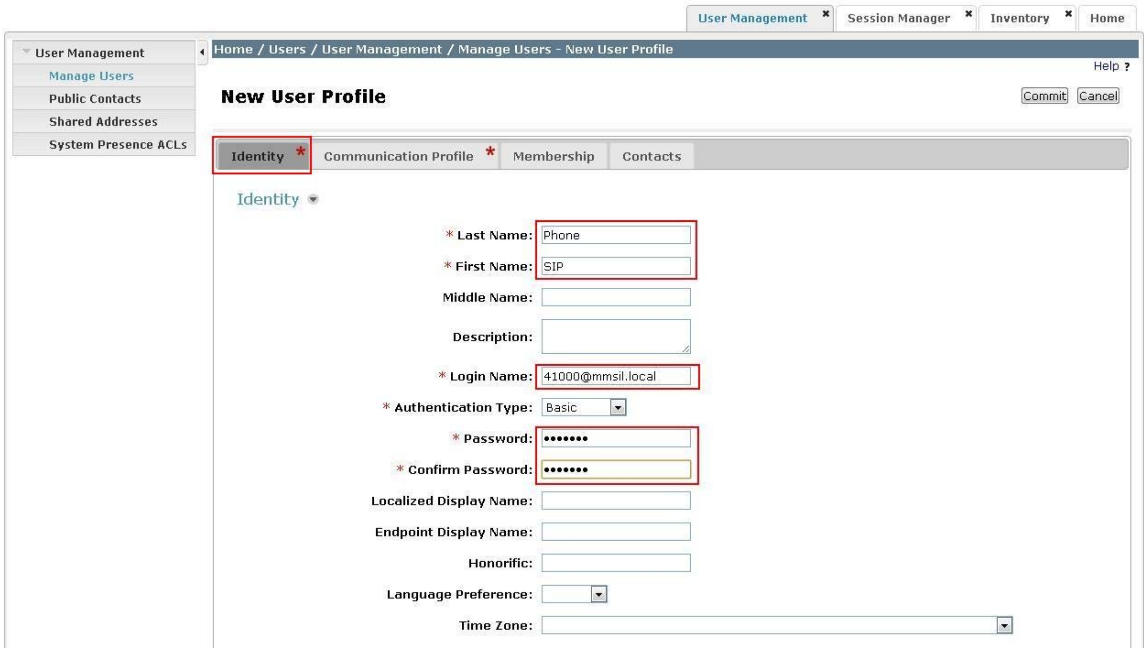


Select **Manage Users** on the left. Then click on **New**.



Click on the **Identity** tab and enter the following and use defaults for other fields:

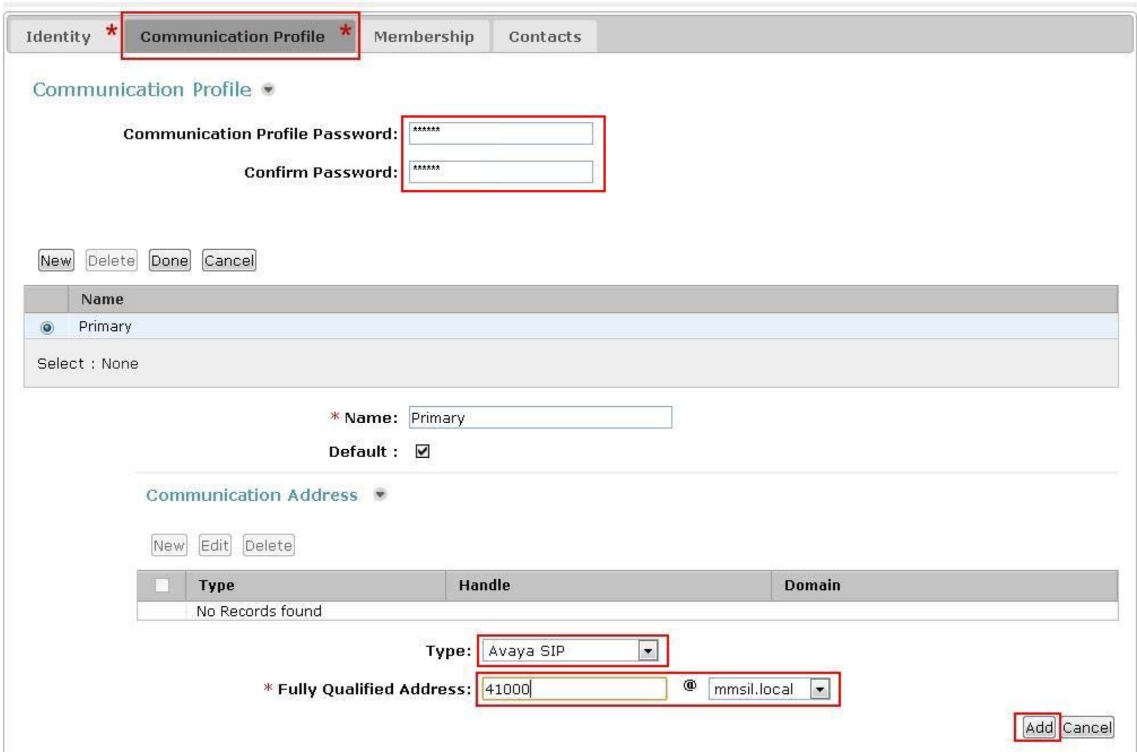
- **Last Name** A desired last name
- **First Name** A desired first name
- **Login Name** The desired phone extension number@domain.com where domain was defined in **Section 4.2**
- **Password** Password for user to log into System Manager (SMGR)



Click on the **Communication Profile** tab. Enter the following and defaults for the remaining fields:

- **Shared Communication Profile Password** Password to be entered by the user when logging into the phone
- **Type** Select **Avaya SIP**
- **Fully Qualified Address** Enter the extension number and select the domain

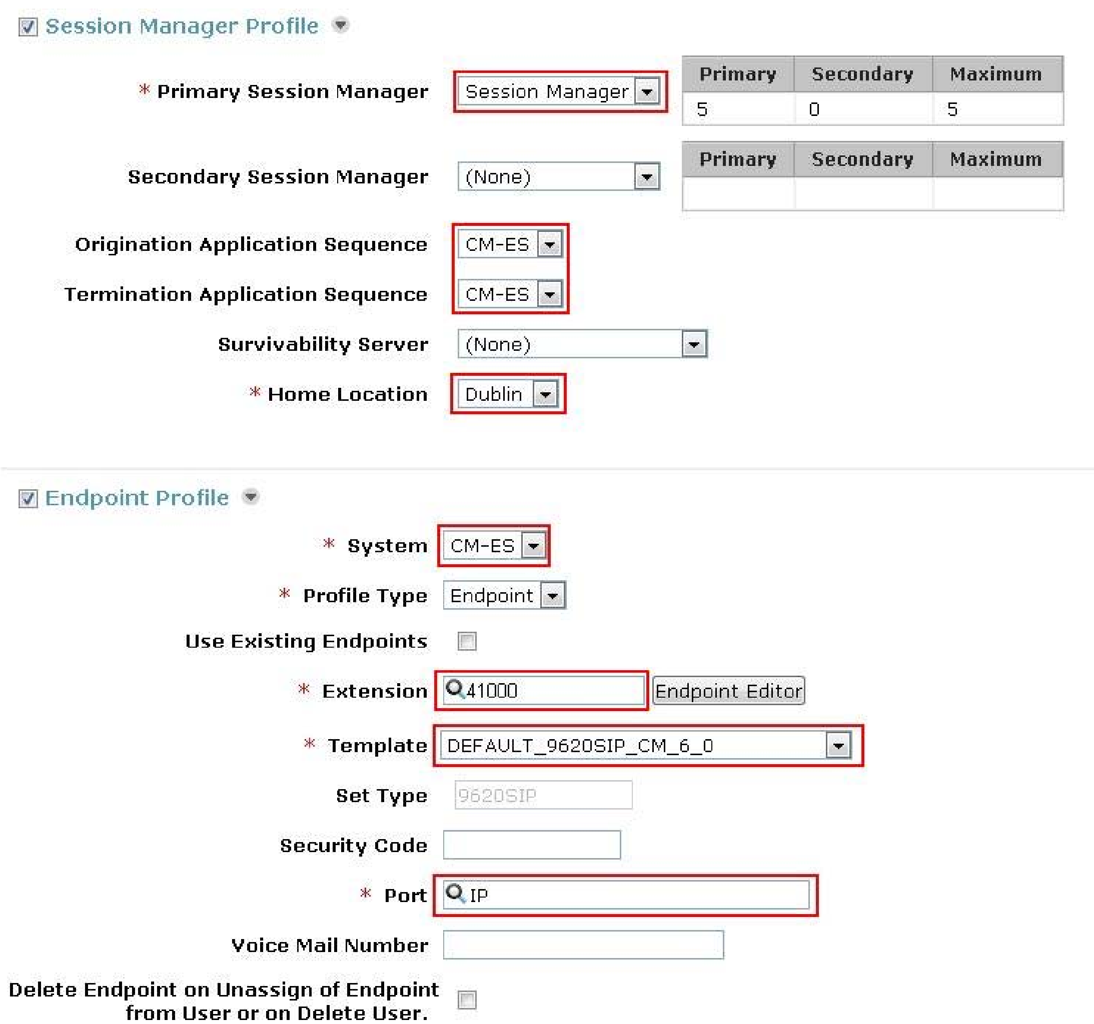
Click on **Add**.


Identity
Communication Profile
Membership
Contacts
Communication Profile
Communication Profile Password:
Confirm Password:
New
Delete
Done
Cancel
Name
Primary
Select : None
* Name:
Primary
Default :
Communication Address
New
Edit
Delete
Type
Handle
Domain
No Records found
Type:
Avaya SIP
* Fully Qualified Address:
41000
@
mmsil.local
Add
Cancel

Navigate to the **Session Manager Profile** and **Endpoint Profile** sections. Select the appropriate Session Manager server for **Primary Session Manager**. For **Origination Application Sequence** and **Termination Application Sequence** select the application sequence created in **Section 4.11.3**. Choose the **Home Location** created in **Section 4.3**. Click on **Endpoint Profile** to expand that section. Enter the following fields and use defaults for the remaining fields:

- **System** Select the CM Entity
- **Extension** Enter a desired extension number
- **Template** Select a telephone type template
- **Port** Select **IP**

Click on **Commit** to save (not shown).



5. Configure Alcatel OmniPCX Enterprise

This section shows the configuration in Alcatel OmniPCX Enterprise. All configurations in this section are administered using the Command Line Interface. These Application Notes assumed that the basic configuration has already been administered. For further information on Alcatel OmniPCX Enterprise, please consult with reference **Error! Reference source not found.**. The procedures include the following areas:

- Verify Alcatel OXE Licences
- Access the Alcatel OXE Manager
- Administer IP Domain
- Administer SIP Trunk Group
- Administer SIP Gateway
- Administer SIP Proxy
- Administer SIP External Gateway
- Administer Network Routing Table
- Administer Prefix Plan
- Administer Codec on SIP Trunk Group

Note: All configuration is completed using the OXE manager menu. To enter the menu, type **mgr** at the CLI prompt.

5.1. Verify Alcatel OXE Licenses

From the CLI prompt, use the **spadmin** command and from the menu shown, select option 2 **Display active file**. This will show the license files installed on the system.

```
    Display current counters .......................... 1
    Display active file ............................... 2
    Check active file coherency ....................... 3
    Install a new file ................................ 4
    Read the system CPUID ............................. 5
    CPU-Ids management ................................ 6
    Display active and new file ....................... 7
    Display OPS limits ................................ 8
    Display ACK code .................................. 9
    Exit .............................................. 0
```

5.2. Access the Alcatel OXE Manager

Establish a Telnet connection to the CS board of the OXE. At the CLI prompt type **mgr** and a menu is then presented.

```
+-Select an object-----------------+
|                                  |
| -> Shelf                         |
|    Media Gateway                 |
|    PWT/DECT System               |
|    System                        |
|    Translator                    |
|    Classes of Service            |
|    Attendant                     |
|    Users                         |
|    Users by profile              |
|    Set Profile                   |
|    Groups                        |
|    Speed Dialing                 |
|    Phone Book                    |
|    Entities                      |
|    Trunk Groups                  |
|    External Services             |
|    Inter-Node Links              |
|    X25                           |
|    DATA                          |
|    Applications                  |
|    Specific Telephone Services   |
|    ATM                           |
|    Events Routing Discriminator  |
|    Security and Access Control   |
|    IP                            |
|    SIP                           |
|    DHCP Configuration            |
|    Alcatel-Lucent 8&9 Series     |
|    SIP Extension                 |
|    Encryption                    |
|    Passive Com. Server           |
|    SNMP Configuration            |
|                                  |
+----------------------------------+
```

5.3. Administer IP Domain

To create an IP domain select **IP → IP domain.** Complete the following option:

- **IP Domain Name** **node1.mmsil.local**, this is the domain name the OXE expects in the from header for incoming SIP Invites

Click **ctrl+v** to complete.

```
+-Create: IP domain-----------------------------------------------------------------------+
¦                                                                                          ¦
¦             Node Number (reserved) : 1                                                   ¦
¦                Instance (reserved) : 1                                                   ¦
¦                   IP Domain Number : 0                                                   ¦
¦                                                                                          ¦
¦                     IP Domain Name : node1.mmsil.local                                   ¦
¦                            Country + Default                                             ¦
¦      Intra-domain Coding Algorithm + Default                                             ¦
¦      Extra-domain Coding Algorithm + Default                                             ¦
¦ FAX/MODEM Intra domain call transp + NO                                                  ¦
¦ FAX/MODEM Extra domain call transp + NO                                                  ¦
¦      G722 allowed in Intra-domain  + NO                                                  ¦
¦       G722 allowed in Extra-domain + NO                                                  ¦
¦             Tandem Primary Domain : -1                                                   ¦
¦        Domain Max Voice Connection : -1                                                  ¦
¦              IP Quality of service : 0                                                   ¦
¦                     Contact Number : ------------------------------                      ¦
¦                  Backup IP address : -----------------------------------------------     ¦
¦                     Trunk Group ID : 10                                                  ¦
¦    IP recording quality of service : 0                                                   ¦
¦                     Time Zone Name + System Default                                      ¦
¦                 Calling Identifier : ------------------------------                      ¦
¦     Supplement. Calling Identifier : ------------------------------                      ¦
¦             SIP Survivability Mode + NO                                                  ¦
¦                                                                                          ¦
+------------------------------------------------------------------------------------------+
```

5.4. Administer SIP Trunk Group

To add a SIP Trunk Group select **Trunk Groups → Create.** Complete the following options:

- **Trunk Group ID** A desired ID number
- **Trunk Group Type** **T2**
- **Trunk Group Name** A desired name

Click **ctrl+v** to continue.

```
+-Create: Trunk Groups-------------------------------------------------------------+
|                                                                                  |
|              Node Number (reserved) : 1                                          |
|                      Trunk Group ID : 10                                         |
|                                                                                  |
|                    Trunk Group Type + T2                                         |
|                    Trunk Group Name : To sm100                                   |
|              UTF-8 Trunk Group Name : -------------------------------------------|
|              Number Compatible With : -1                                         |
|                      Remote Network : 255                                        |
|                  Shared Trunk Group + False                                      |
|                    Special Services + Nothing                                    |
|                                                                                  |
+----------------------------------------------------------------------------------+
```

On the next screen complete the following options:

- **Q931 Signal Variant** **ABC-F**
- **T2 Specification** **SIP**

Click **ctrl+v** to complete configuration.

```
+-Create: Trunk Groups---------------------------------------------------------+
|                                                                              |
|                         Node number : 1                                      |
|                Transcom Trunk Group + False                                  |
|            Auto.reserv.by Attendant + False                                  |
|            Overflow trunk group No. : -1                                     |
|                     Tone on seizure + False                                  |
|                 Private Trunk Group + False                                  |
|                 Q931 Signal variant + ABC-F                                  |
|                  SS7 Signal variant + No variant                             |
|            Number Of Digits To Send : 0                                      |
|              Channel selection type + Quantified                             |
|  Auto.DTMF dialing on outgoing call + NO                                      |
|                    T2 Specification + SIP                                    |
|   Homogenous network for direct RTP + NO                                      |
|                 Public Network COS  : 0                                      |
|                     DID transcoding + False                                  |
|            Can support UUS in SETUP + True                                   |
|                                                                              |
|                               Implicit Priority                              |
|                                                                              |
|                     Activation mode : 0                                      |
|                      Priority Level : 0                                      |
|                                                                              |
|                           Preempter + NO                                     |
|      Incoming calls Restriction COS : 10                                     |
|      Outgoing calls Restriction COS : 10                                     |
|              Callee number mpt1343  + NO                                     |
|                     Overlap dialing + YES                                    |
|              Call diversion in ISDN + NO                                     |
|                                                                              |
+------------------------------------------------------------------------------+
```

5.5. Administer SIP Gateway

To configure a SIP Gateway select **SIP → SIP Gateway.** Complete the following options:

- **SIP Trunk Group** SIP trunk group number defined in **Section 5.4**
- **DNS Local Domain Name** Enter domain name for the OXE

Click **ctrl+v** to complete.

```
+-Review/Modify: SIP Gateway---------------------------------------------------------+
|
|            Node Number (reserved) : 1
|               Instance (reserved) : 1
|               Instance (reserved) : 1
|
|                    SIP Subnetwork : 9
|                   SIP Trunk Group : 10
|                        IP Address : 10.10.9.111
|               Machine name - Host : node1
|             SIP Proxy Port Number : 5060
|        SIP Subscribe Min Duration : 1800
|        SIP Subscribe Max Duration : 86400
|                     Session Timer : 1800
|                 Min Session Timer : 1800
|              Session Timer Method + RE_INVITE
|             DNS local domain name : mmsil.local
|                          DNS type + DNS A
|               SIP DNS1 IP Address : -----------------------------------------------
|               SIP DNS2 IP Address : -----------------------------------------------
|                        SDP in 18x + False
|                       Cac SIP-SIP + False
|   INFO method for remote extension + True
|      Dynamic Payload type for DTMF : 97
+------------------------------------------------------------------------------------+
```

5.6. Administer SIP Proxy

To configure a SIP Proxy select **SIP → SIP Proxy.** Complete the following options:

- **Minimal authentication method SIP None**

Click **ctrl+v** to complete.

```
+-Review/Modify: SIP Proxy-----------------------------------------------------------+
|
|            Node Number (reserved) : 1
|               Instance (reserved) : 1
|               Instance (reserved) : 1
|              SIP initial time-out : 500
|                      SIP timer T2 : 4000
|                Dns Timer overflow : 5000
|                  Recursive search + False
|      Minimal authentication method + SIP None
|
|              Authentication realm : --------------------------------------------------
|  Only authenticated incoming calls + False
|                  Framework Period : 3
|     Framework Nb Message By Period : 25
|        Framework Quarantine Period : 1800
|            TCP when  long messages + True
|
+------------------------------------------------------------------------------------+
```

5.7. Administer SIP External Gateway

Configure a SIP connection to the Session Manager by creating a SIP External Gateway. Select **SIP → SIP Ext Gateway → Create.** Complete the following options:

- **SIP External Gateway ID** A desired ID number
- **Gateway Name** A desired name
- **SIP Remote domain** Enter sm100 ip address from **Section 3.3**
- **SIP Port Number** **5060**
- **SIP Transport Type** **TCP**
- **Trunk Group Number** The trunk group number defined in **Section 5.4**
- **SDP in 18x** This must be set to **False** for Avaya Digital to Alcatel ipTouch calls to work
- **Minimal authentication method** **SIP None**

Click **ctrl+v** to complete.

```
+-Create: SIP Ext Gateway--------------------------------------------------------------+
|
|             Node Number (reserved) : 1
|                Instance (reserved) : 1
|            SIP External Gateway ID : 0
|
|                       Gateway Name : Session Manager
|                  SIP Remote domain : 10.10.9.34
|                     PCS IP Address : -----------------------------------------------
|                    SIP Port Number : 5060
|                 SIP Transport Type + TCP
|                 RFC3262 Forced use + True
|                   Belonging Domain : --------------------------------------------------
|                    Registration ID : --------------------------------------------------
|        Registration ID P_Asserted + False
|                 Registration timer : 0
|                 SIP Outbound Proxy : --------------------------------------------------
|                  Supervision timer : 0
|                 Trunk group number : 10
|                        Pool Number : -1
|                     Outgoing realm : --------------------------------------------------
|                  Outgoing username : --------------------------------------------------
|
|                  Outgoing Password : ----------
|                            Confirm : ----------
|
|                  Incoming username : --------------------------------------------------
|                  Incoming Password : ----------
|                            Confirm : ----------
|
|  RFC 3325 supported by the distant + True
|                           DNS type + DNS A
|                SIP DNS1 IP Address : -----------------------------------------------
|                SIP DNS2 IP Address : -----------------------------------------------
|                         SDP in 18x + False
|     Minimal authentication method + SIP None
|   INFO method for remote extension + False
|        Send only trunk group algo + False
|                             To EMS + False
|                Routing Application + False
|      Dynamic Payload type for DTMF : 97
+--------------------------------------------------------------------------------------+
```

5.8. Administer Network Routing Table

In the sample configuration, network number 15 was used. To administer the routing table for network number 15, select **Translator → Network Routing Table** and then select **15**. Complete the following options:

- **Associated Ext SIP gateway** Use the SIP External Gateway ID defined in **Section 5.7**

Click **ctrl+v** to complete.

```
+-Review/Modify: Network Routing Table------------------------------+
|                                                                   |
|             Node Number (reserved) : 1                            |
|                Instance (reserved) : 1                            |
|                     Network Number : 15                           |
|                                                                   |
|     Rank of First Digit to be Sent : 1                            |
|     Incoming identification prefix : --------                     |
|                      Protocol Type + ABC_F                        |
|       Numbering Plan Descriptor ID : 11                           |
|                     ARS Route list : 0                            |
|                    Schedule number : -1                           |
|                     ATM Address ID : -1                           |
|                Network call prefix : --------                     |
|                     City/Town Name : --------------------         |
|                Send City/Town Name + False                        |
|         Associated Ext SIP gateway : 0                            |
|           Enable UTF8 name sending + True                         |
|                                                                   |
+-------------------------------------------------------------------+
```

5.9. Administer Prefix Plan

In the sample configuration, Avaya SIP phones are 5 digits in length and begin with 41. To administer the prefix plan for dialing Avaya SIP phones from OXE, select **Translator → Prefix Plan → Create.** Complete the following options:

- **Number** **41**
- **Prefix Meaning** **Routing No**

Click **ctrl+v** to continue.

```
+-Create: Prefix Plan---------------------------------------------------+
|                                                                       |
|             Node Number (reserved) : 1                                |
|                Instance (reserved) : 1                                |
|                             Number : 41                               |
|                                                                       |
|                     Prefix Meaning + Routing No.                      |
|                                                                       |
+-----------------------------------------------------------------------+
```

On the next screen complete the following options:

- **Network Number** Use network number administered in **Section 5.8**
- **Node Number/ABC-F Trunk Group**
  Use the trunk group number administered in **Section 5.4**
- **Number of Digits** **5**

Click **ctrl+v** to complete.

```
+-Create: Prefix Plan-------------------------------+
|                                                   |
|                    Network Number : 15            |
|      Node Number/ABC-F Trunk Group : 10           |
|                  Number of Digits : 5             |
|      Number With Subaddress (ISDN) + NO           |
|               Default X25 ID.pref. + NO           |
|                                                   |
+---------------------------------------------------+
```

5.10. Administer Codec on SIP Trunk Group

To create a codec on the SIP Trunk Group select **Trunk Groups → Trunk Group.** The parameter **IP Compression Type** has two possible values, G711 and Default. If the parameter **Default** is chosen then this value is determined by the parameter **Compression Type** administered in **System → Other System Param. → Compression Parameters.** Compression type is either G.729 or G.723.

```
+-Review/Modify: Compression Parameters-------------------------------------+
|                                                                           |
|             Node Number (reserved) : 1                                    |
|                Instance (reserved) : 1                                    |
|                Instance (reserved) : 1                                    |
|                      System Option + Compression Type                     |
|                                                                           |
|                   Compression Type + G 729                                |
|                                                                           |
+---------------------------------------------------------------------------+
```

For the above values to hold true, all other options for compression in the Alcatel OXE must be set to non-compressed options. Ensure the following parameters are set accordingly:

Navigate to **IP → IP Domain**

- Intra-Domain Coding Algorithm = default
- Extra-Domain Coding Algorithm = default

Navigate to **IP → TSC/IP**

- Default Voice Coding Algorithm = without compression

Navigate to **IP → INT/IP**

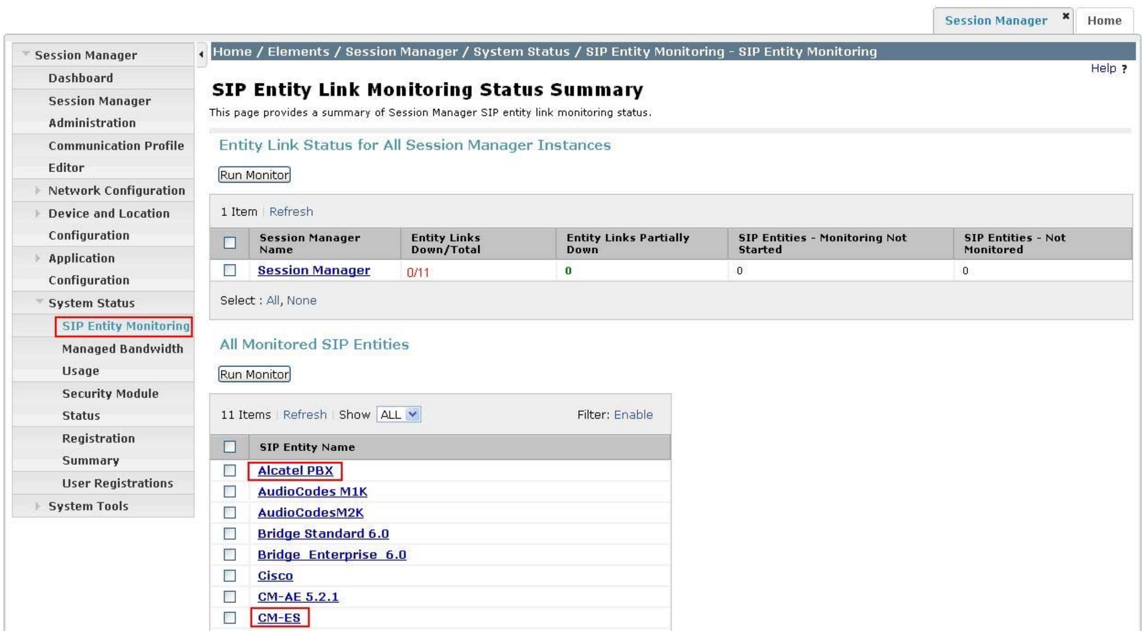
- Default Voice Coding Algorithm = without compression

6. Verification

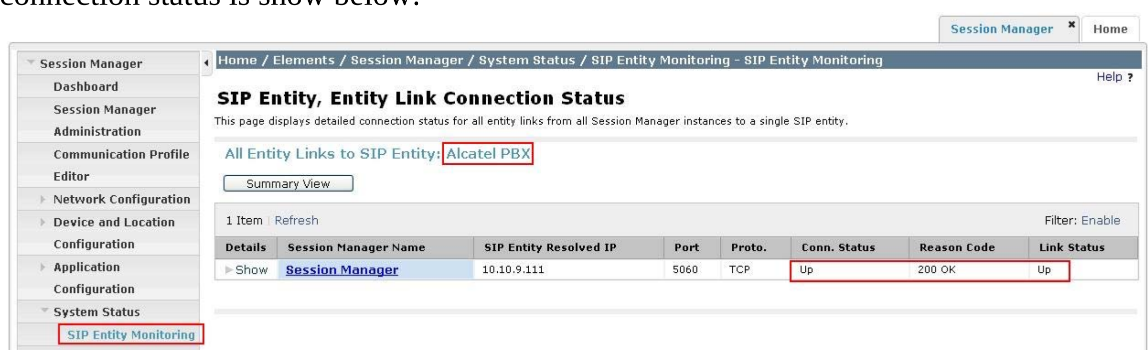
This section provides the verification tests that can be performed on Session Manager, Communication Manager and Alcatel OmniPCX Enterprise to verify their proper configuration.

6.1. Verify Avaya Aura® Session Manager

On the SMGR management screen under the **Elements** column select **Session Manager**. On the left menu, select **System Status → SIP Entity Monitoring**. Verify as shown below that none of the SIP entities for Alcatel or CM links are down, indicating that they are all reachable for routing.



Click on the SIP Entity Names **Alcatel PBX** and **CM-ES**, shown in the previous screen, and verify that the connection status is **Up**, as shown in the following screenshots. Alcatel connection status is show below:



Communication Manager connection status is show below:

6.2. Verify Avaya Aura® Communication Manager

Verify the status of the SIP trunk group by using the **status trunk n** command, where **n** is the trunk group number being investigated. Verify that all trunks are in the **in-service/idle** state as shown below.

```
status trunk 150

                             TRUNK GROUP STATUS

Member    Port     Service State      Mtce Connected Ports
                                      Busy

0150/001 T00001   in-service/idle    no
0150/002 T00002   in-service/idle    no
0150/003 T00003   in-service/idle    no
0150/004 T00004   in-service/idle    no
0150/005 T00005   in-service/idle    no
0150/006 T00006   in-service/idle    no
0150/007 T00007   in-service/idle    no
0150/008 T00008   in-service/idle    no
0150/009 T00009   in-service/idle    no
0150/010 T00010   in-service/idle    no
```

Verify the status of the SIP signaling-group by using the **status signaling-group n** command, where **n** is the signaling group number being investigated. Verify that the signaling group is in the **in-service** state as shown below.

```
status signaling-group 150
                         STATUS SIGNALING GROUP

        Group ID: 150
      Group Type: sip

     Group State: in-service
```

6.3. Verify Alcatel OmniPCX Enterprise

Verify the status of the SIP trunk group by using the **trkstat n** command, where **n** is the trunk group number being investigated. Verify that all trunks are in the **Free** state as shown below.

```
trkstat 10

+==============================================================================+
|   S I P   T R U N K   S T A T E     Trunk group number : 10                  |
|                                     Trunk group name   : To ASM60            |
|                                     Number of Trunks   : 62                  |
+------------------------------------------------------------------------------+
|   Index :     1    2    3    4    5    6    7    8    9   10   11   12   13  |
|   State :     F    F    F    F    F    F    F    F    F    F    F    F    F  |
+------------------------------------------------------------------------------+
|   Index :    14   15   16   17   18   19   20   21   22   23   24   25   26  |
|   State :     F    F    F    F    F    F    F    F    F    F    F    F    F  |
+------------------------------------------------------------------------------+
|   Index :    27   28   29   30   31   32   33   34   35   36   37   38   39  |
|   State :     F    F    F    F    F    F    F    F    F    F    F    F    F  |
+------------------------------------------------------------------------------+
|   Index :    40   41   42   43   44   45   46   47   48   49   50   51   52  |
|   State :     F    F    F    F    F    F    F    F    F    F    F    F    F  |
+------------------------------------------------------------------------------+
|   Index :    53   54   55   56   57   58   59   60   61   62                 |
|   State :     F    F    F    F    F    F    F    F    F    F                 |
+------------------------------------------------------------------------------+
|  F:  Free    |    B: Busy    |   Ct: busy Comp trunk   |  Cl: busy Comp link   |
|  WB: Busy Without B Channel|   Cr: busy Comp trunk for RLIO inter-ACT link   |
|  WBD: Data Transparency without chan.| WBM: Modem transparency without chan. |
|  D: Data Transparency      |   M: Modem transparency                         |
+------------------------------------------------------------------------------+
```

6.4. Verified Scenarios

The following scenarios have been verified for the configuration described in these Application Notes.

- Basic calls between various telephones on Communication Manager and Alcatel OXE can be made in both directions using G.711MU/A-law and G.729A.
- Proper display of the calling and called party name and number information was verified for all telephones with the basic call scenario.
- Supplementary calling features were verified. The feature scenarios involved additional endpoints on the respective systems, such as performing an unattended transfer of the SIP trunk call to a local endpoint on the same site, and then repeating the scenario to transfer the SIP trunk call to a remote endpoint on the other site. The supplementary calling features verified are shown below.
    - Unattended transfer
    - Attended transfer
    - Hold/Unhold
    - Consultative hold
    - Call forwarding
    - Conference
    - Calling number block
    - DTMF tone sending

7. Conclusion

As illustrated in these Application Notes, Alcatel OmniPCX Enterprise can interoperate via Avaya Aura® Session Manager with Avaya Aura® Communication Manager using SIP trunks. The following is a list of interoperability items observed:

- In the case where an Avaya Digital phone dials an Alcatel phone, there is no audio path. To resolve this issue, set "SDP in 18x" to false in the SIP Ext Gateway configuration in the Alcatel OmniPCX Enterprise.
- In the case where an Avaya phone dials an Alcatel phone and then the Alcatel phone performs an unattended transfer to another Avaya phone, an issue was seen whereby the Alcatel OmniPCX Enterprise tears down the completed call after 20 seconds. To prevent this from happening, disable shuffling on the Avaya Aura® Communication Manager.
- In the case where an Avaya phone dials an Alcatel phone and then the Alcatel phone performs an unattended transfer to another Alcatel phone, an issue was seen whereby the completed call was torn down after 5 seconds and the SIP trunk on the Alcatel OmniPCX Enterprise side was blocked. To prevent this happening, do not assign a DNS ip address in the SIP External Gateway configuration in the Alcatel OmniPCX Enterprise.
- For conference calls and attended/unattended transfers, phone displays were not updated correctly for both username and number. This is an Alcatel OmniPCX Enterprise issue as SIP 180 & 200 messages sent by Alcatel OmniPCX Enterprise do not contain a user part in the contact header.

8. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com

[1] *Avaya Aura® Session Manager Overview*, Doc # 03603323, Issue 1 Release 6.1
[2] *Administering Avaya Aura® Session Manager*, Doc # 03603324, Issue 1 Release 6.1
[3] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc # 03603325, Issue 1 Release 6.1
[4] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, Issue 6.0

Product documentation for Alcatel products may be found at
http://enterprise.alcatel-lucent.com/?dept=ResourceLibrary&page=Landing

[5] http://enterprise.alcatel-lucent.com/?product=OmniPCXEnterprise&page=overview

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