



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.

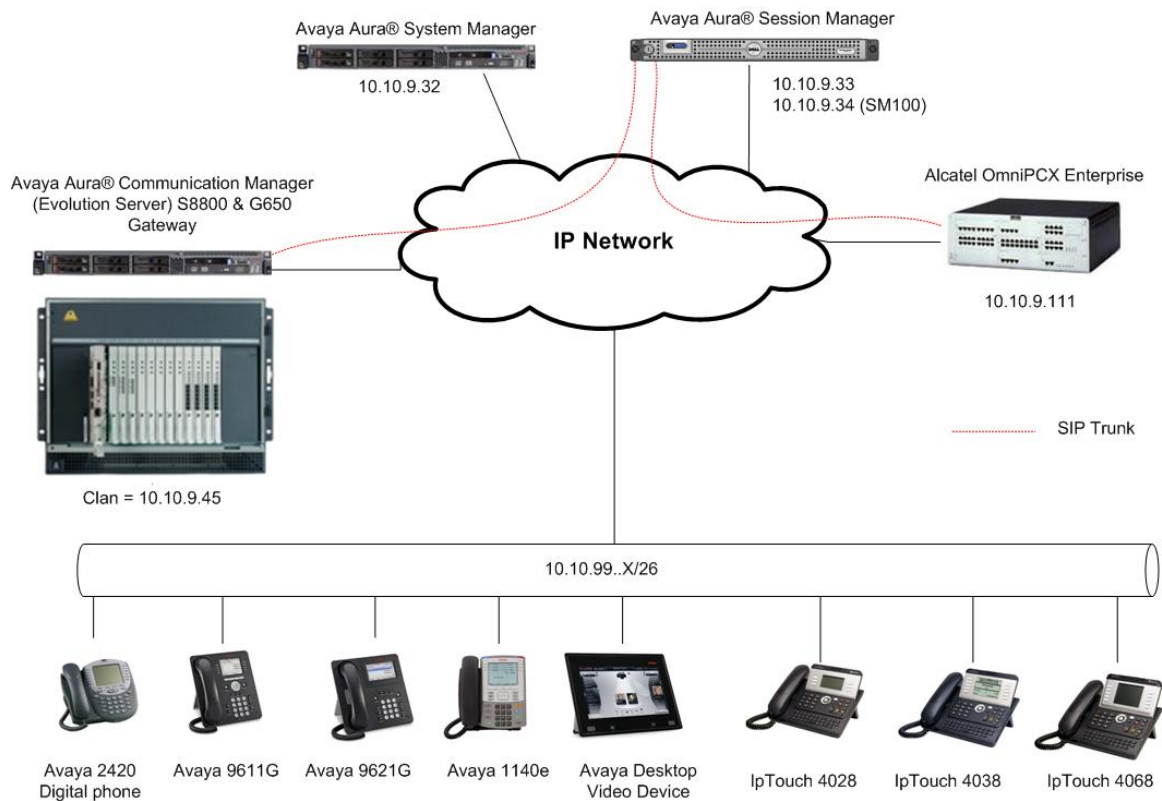


Figure 1: Connection of Alcatel OmniPCX Enterprise and Avaya Aura[®] Communication Manager via Avaya Aura[®] Session Manager using SIP Trunks

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 Attdd-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
Codec Set: 1      Intra-region IP-IP Direct Audio: yes
                  Inter-region IP-IP Direct Audio: yes
                  IP Audio Hairpinning? n
UDP Port Min: 2048
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
H.323 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
                                                                AUDIO RESOURCE RESERVATION PARAMETERS
                                                                RSVP Enabled? n
```

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
                               UI Treatment: service-provider
                               Replace Restricted Numbers? n
                               Replace Unavailable Numbers? n
                               Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y
```

Navigate to **Page 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												
															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											
1:	y	y	y	y	y	n	n																				
2:	y	y	y	y	y	n	n																				
3:	y	y	y	y	y	n	n																				
4:	y	y	y	y	y	n	n																				

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 String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call 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 String	Total		Route	Call	Node	ANI
		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.

AVAYA Avaya Aura™ System Manager 6.1

Home / Log On

Log On

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

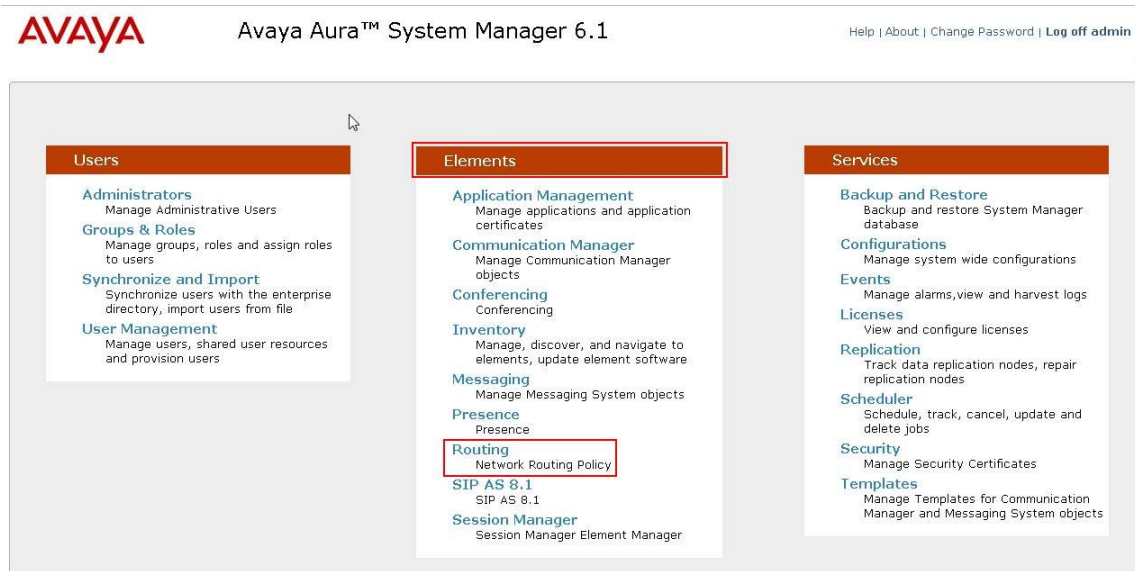
Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

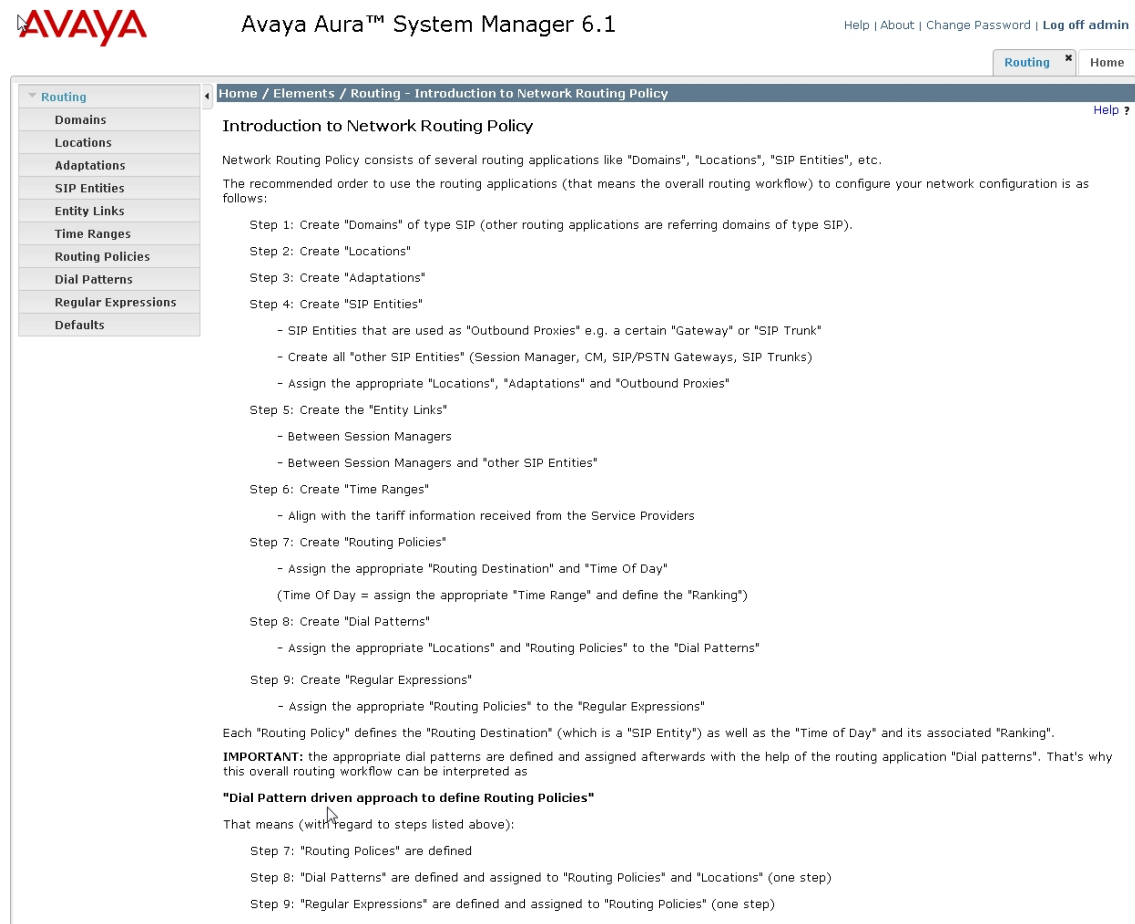
Password:

[Change Password](#)

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.

The screenshot shows a web-based interface for managing SIP domains. On the left is a sidebar menu with 'Routing' expanded and 'Domains' selected. The main area has a breadcrumb trail 'Home / Elements / Routing / Domains - Domain Management' and a title 'Domain Management'. Below the title is a table with one item, 'mmsil.local'. The table has columns for Name, Type, Default, and Notes. The 'Name' column contains 'mmsil.local', 'Type' is 'sip', 'Default' is unchecked, and 'Notes' is empty. A red box highlights the 'Name' and 'Type' fields. At the bottom right, there are 'Commit' and 'Cancel' buttons. A message '* Input Required' is displayed at the bottom left.

Name	Type	Default	Notes
* mmsil.local	sip	<input type="checkbox"/>	

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.

Routing x Home

Home / Elements / Routing / Locations - Location Details

Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting

General

* Name: Dublin

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

2 Items Refresh Filter: Enable

IP Address Pattern	Notes
* 135.64.186.*	
* 10.10.9.*	

Select : All, None

* Input Required

Commit Cancel

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.

The screenshot shows the 'Adaptations - Adaptations' configuration page. The left sidebar lists various routing elements, with 'Adaptations' selected. The main area is divided into sections for 'Adaptation Details' and 'Digit Conversion'.

Adaptation Details:

- General:**
 - Adaptation name:** Alcatel
 - Module name:** DigitConversionAdapter
 - Module parameter:** lodstd=node1.mmsil.local
 - Egress URI Parameters:**
 - Notes:**

Digit Conversion for Incoming Calls to SM:

1 Item | Refresh | Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 360	* 5	* 5		* 0		both	

Select : All, None

Digit Conversion for Outgoing Calls from SM:

0 Items | Refresh | Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
--	------------------	-----	-----	---------------	---------------	---------------	-------------------	-------

* Input Required

Buttons: Commit, Cancel

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.

The screenshot shows a web application interface for configuring SIP Entities. On the left is a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted with a red box), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. The form contains the following fields: 'Name' (text input with value 'Session Manager'), 'FQDN or IP Address' (text input with value '10.10.9.34'), 'Type' (dropdown menu with value 'Session Manager'), 'Notes' (text input with value 'sm100'), 'Location' (dropdown menu with value 'Dublin'), 'Outbound Proxy' (text input), 'Time Zone' (dropdown menu with value 'Europe/Dublin'), and 'Credential name' (text input). At the top right of the form are 'Commit' and 'Cancel' buttons. The breadcrumb path at the top reads 'Home / Elements / Routing / SIP Entities - SIP Entity Details'.

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.

Port
Add Remove

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	mmsil.local	
<input type="checkbox"/>	5061	TLS	mmsil.local	

Select : All, None

*** Input Required** **Commit** Cancel

The following screen shows the SIP Entity for CM.

Routing * Home

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: CM-ES

* FQDN or IP Address: 10.10.9.45

Type: CM

Notes:

Adaptation:

Location: Dublin

Time Zone: Etc/GMT

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Commit Cancel

The following screen shows the SIP Entity for OXE.

Routing * Home

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: Alcatel PBX

* FQDN or IP Address: 10.10.9.111

Type: SIP Trunk

Notes:

Adaptation: Alcatel

Location: Dublin

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Commit Cancel

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
<input type="checkbox"/>	Alcatel PBX	Session Manager	TCP	5060	Alcatel PBX	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	AudioCodes M1K	Session Manager	TCP	5060	AudioCodes M1K	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	AudioCodes M1K TLS	Session Manager	TLS	5061	AudioCodes M1K	5061	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	AudioCodesM2K	Session Manager	TCP	5060	AudioCodesM2K	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Bridge_Enterprise_6.0	Session Manager	TCP	5060	Bridge_Enterprise_6.0	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Bridge_Standard_6.0	Session Manager	TCP	5060	Bridge_Standard_6.0	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Cisco	Session Manager	TCP	5060	Cisco	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	CM-AE 5.2.1	Session Manager	TCP	5060	CM-AE 5.2.1	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	CM-ES	Session Manager	TCP	5060	CM-ES	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	IMG_1010	Session Manager	TCP	5060	IMG 1010	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	MMS_2	Session Manager	TCP	5060	MMS.2	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Voicemail	Session Manager	TCP	5060	Voicemail	5060	<input checked="" type="checkbox"/>	

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.

The screenshot shows the 'Time Ranges' configuration page in Session Manager. The left sidebar has a menu with 'Time Ranges' highlighted. The main content area shows a table with one item named '24/7'. The table has columns for Name, Mo, Tu, We, Th, Fr, Sa, Su, Start Time, End Time, and Notes. The '24/7' item has checkboxes for all days of the week (Mo through Su) checked, and Start Time '00:00' and End Time '23:59'. Below the table, there is a 'Select : All, None' option.

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

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 screenshot shows the 'Routing Policy Details' configuration page for a policy named 'CM-ES'. The left sidebar contains a menu with 'Routing Policies' highlighted. The main area is divided into three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. In the 'General' section, the 'Name' field is set to 'CM-ES'. In the 'SIP Entity as Destination' section, the 'Select' button is highlighted, and a table below shows the selected entity 'CM-ES' with FQDN '10.10.9.45' and Type 'CM'. In the 'Time of Day' section, the 'Add' button is highlighted, and a table shows a single time range '24/7' for all days of the week from 00:00 to 23:59.

Name	FQDN or IP Address	Type	Notes
CM-ES	10.10.9.45	CM	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	

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

Routing Policy Details

General

* Name: alcatel PBX

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Alcatel PBX	10.10.9.111	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

Ranking	1	Name	2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0		24/7		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select: All, None

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**

Dial Pattern Details

General

* Pattern: 360

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

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.

Routing * Home

Home / Elements / Routing / Dial Patterns - Originating Location and Routing Policy List

Originating Location and Routing Policy List Select Cancel

Originating Location

☒ Apply The Selected Routing Policies to All Originating Locations

1 Item Refresh Filter: Enable

<input checked="" type="checkbox"/>	Name	Notes
<input type="checkbox"/>	Dublin	

Select : All, None

Routing Policies

11 Items Refresh Filter: Enable

<input checked="" type="checkbox"/>	Name	Disabled	Destination	Notes
<input checked="" type="checkbox"/>	alcatel PBX	<input type="checkbox"/>	Alcatel PBX	

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**

Routing * Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details Help ?

General

* Pattern: :40

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Commit Cancel

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.

Routing Home

Home / Elements / Routing / Dial Patterns - Originating Location and Routing Policy List

Originating Location and Routing Policy List Select Cancel

Originating Location

☒ Apply The Selected Routing Policies to All Originating Locations

1 Item Refresh Filter: Enable

<input checked="" type="checkbox"/>	Name	Notes
<input type="checkbox"/>	Dublin	

Select : All, None

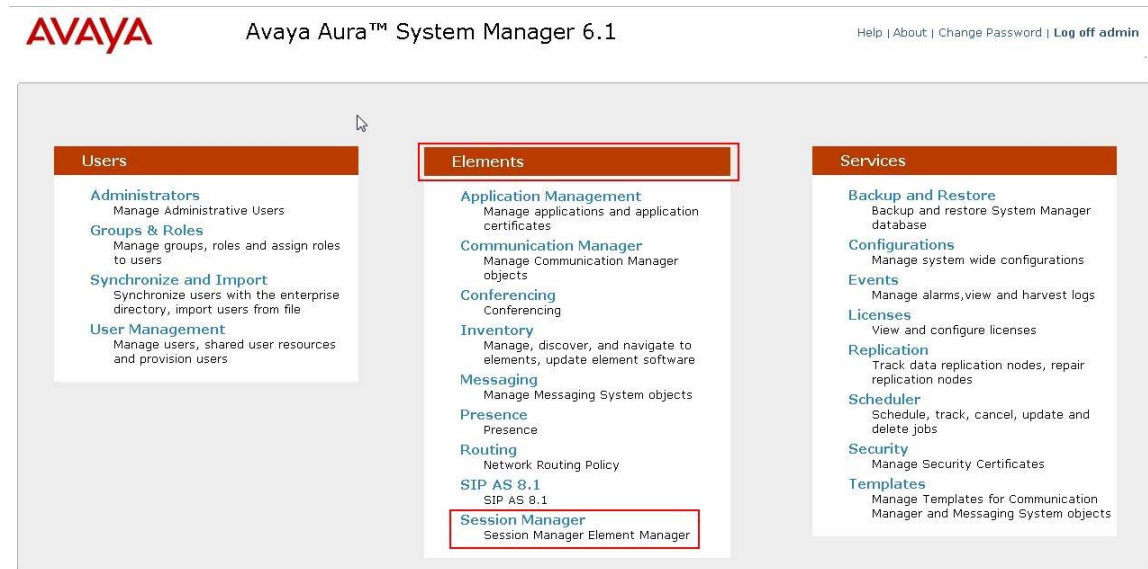
Routing Policies

11 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	alcatel PBX	<input type="checkbox"/>	Alcatel PBX	
<input type="checkbox"/>	Audiocodes M1K	<input type="checkbox"/>	AudioCodes M1K	
<input type="checkbox"/>	AudioCodesM2K	<input type="checkbox"/>	AudioCodesM2K	
<input type="checkbox"/>	Bridge Enterprise Edition 6.0	<input type="checkbox"/>	Bridge_Enterprise_6.0	
<input type="checkbox"/>	Bridge Standard Edition 6.0	<input type="checkbox"/>	Bridge Standard 6.0	
<input type="checkbox"/>	CM-AE 5.2.1	<input type="checkbox"/>	CM-AE 5.2.1	
<input checked="" type="checkbox"/>	CM-ES	<input type="checkbox"/>	CM-ES	

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.

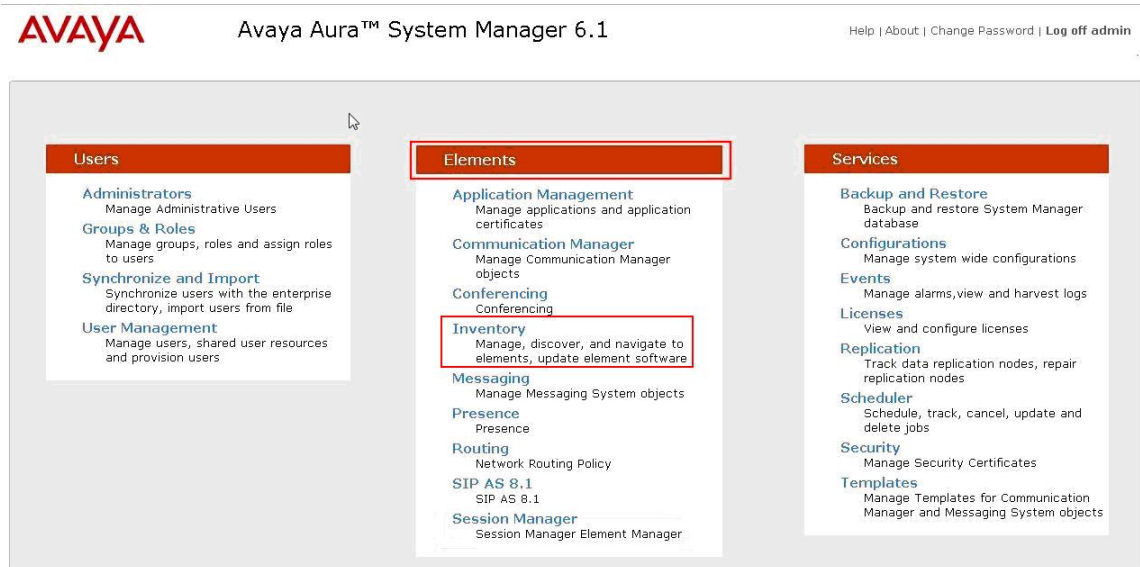
The screenshot shows the 'Edit Session Manager' configuration page. The left sidebar contains a navigation menu with 'Session Manager Administration' selected. The main content area is titled 'Edit Session Manager' and has a 'Commit' button. The configuration is organized into two sections: 'General' and 'Security Module'. The 'General' section includes fields for 'SIP Entity Name' (set to 'Session Manager'), 'Description', '*Management Access Point Host Name/IP' (set to '10.10.9.33'), and '*Direct Routing to Endpoints' (set to 'Enable'). The 'Security Module' section includes fields for 'SIP Entity IP Address' (set to '10.10.9.34'), '*Network Mask' (set to '255.255.255.0'), '*Default Gateway' (set to '10.10.9.1'), '*Call Control PHB' (set to '46'), '*QOS Priority' (set to '6'), '*Speed & Duplex' (set to 'Auto'), and 'VLAN ID'.

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

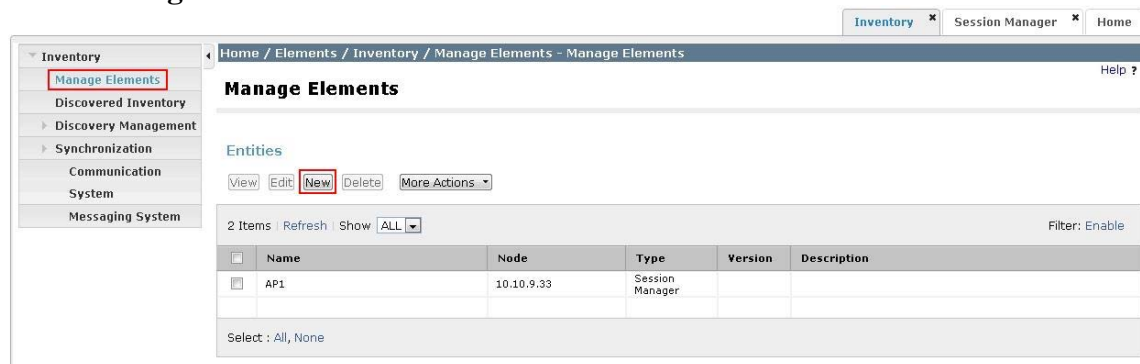
In order for Communication Manager to provide configuration and Evolution Server support to SIP phones when they register to Session Manager, Communication Manager must be added as an application.

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

The screenshot shows the 'New CM Instance' form in the 'Application' tab. The form has two tabs: 'Application' and 'Attributes'. The 'Application' tab is active. The form contains the following fields:

- Name:** CM-ES
- Type:** CM
- Description:** Evolution Server
- Node:** 10.10.9.42
- Access Point:** (empty)
- Port:** (empty)

At the bottom of the form, there is a legend indicating that an asterisk (*) denotes a required field. The 'Commit' and 'Cancel' buttons are located at the bottom right of the form.

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.

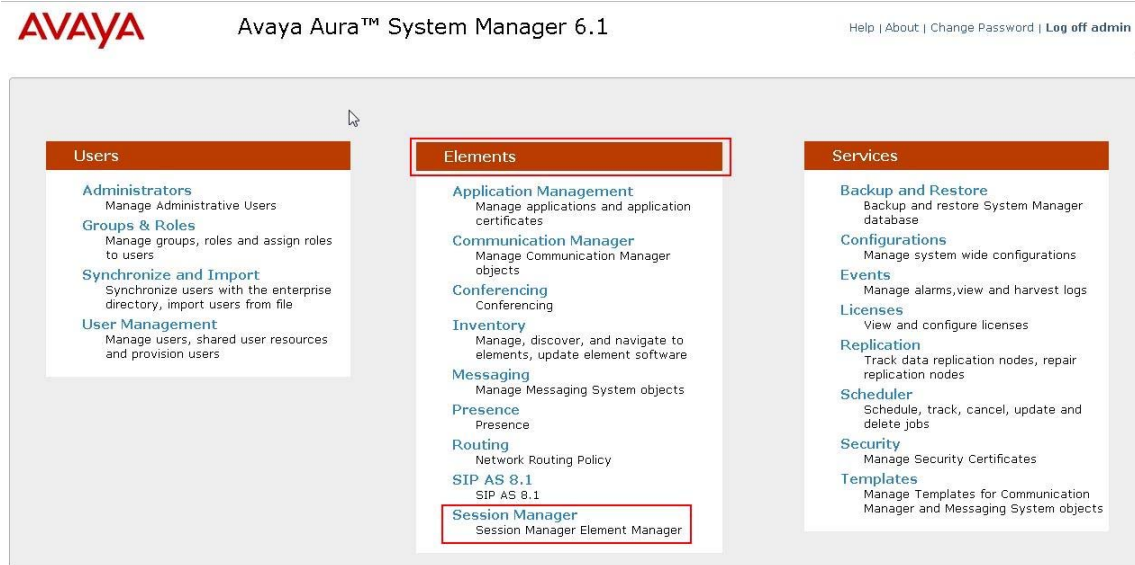
The screenshot shows the 'New CM Instance' form in the 'Attributes' tab. The form has two tabs: 'Application' and 'Attributes'. The 'Attributes' tab is active. The form contains the following fields:

- SNMP Attributes:**
 - Version:** None (selected), V1, V3
- Attributes:**
 - Login:** init
 - Password:** (masked with dots)
 - Confirm Password:** (masked with dots)
 - Is SSH Connection:** ☒
 - Port:** 5022

At the bottom of the form, there is a legend indicating that an asterisk (*) denotes a required field. The 'Commit' and 'Cancel' buttons are located at the bottom right of the form.

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**

Session Manager x Home

Home / Elements / Session Manager / Application Configuration / Applications - Applications

Help ?

Application Editor [Commit] [Cancel]

Application

*Name [CM-ES]

*SIP Entity [CM-ES]

*CM System for SIP Entity [CM-ES] Refresh View/Add CM Systems

Description []

Application Attributes (optional)

Name	Value
Application Handle	[]
URI Parameters	[]

*Required [Commit] [Cancel]

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.

The screenshot shows the 'Application Sequence Editor' window. On the left is a navigation tree with 'Application Sequences' highlighted. The main area has a breadcrumb trail: 'Home / Elements / Session Manager / Application Configuration / Application Sequences - Application Sequences'. Below this is a 'Commit' button. The 'Application Sequence' section contains a 'Name' field with 'CM-ES' and an empty 'Description' field. The 'Applications in this Sequence' section shows a table with one item: 'CM-ES' with a 'Mandatory' checkbox checked. Below this is a 'Select: All, None' option. The 'Available Applications' section shows a table with one item: 'CM-ES'. At the bottom, there is a '* Required' label and 'Commit' and 'Cancel' buttons.

Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
1	CM-ES	CM-ES	<input checked="" type="checkbox"/>	

Name	SIP Entity	Description
CM-ES	CM-ES	

4.11.4. Synchronize Avaya Aura® Communication Manager Data

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

The screenshot shows the 'Avaya Aura™ System Manager 6.1' main menu. It has three main columns: 'Users', 'Elements', and 'Services'. The 'Elements' column is highlighted with a red box. Within the 'Elements' column, the 'Inventory' option is highlighted with a red box. The 'Inventory' description is 'Manage, discover, and navigate to elements, update element software'. Other options in the 'Elements' column include 'Application Management', 'Communication Manager', 'Conferencing', 'Messaging', 'Presence', 'Routing', 'SIP AS 8.1', and 'Session Manager'. The 'Users' column includes 'Administrators', 'Groups & Roles', 'Synchronize and Import', and 'User Management'. The 'Services' column includes 'Backup and Restore', 'Configurations', 'Events', 'Licenses', 'Replication', 'Scheduler', 'Security', and 'Templates'.

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.

Synchronize CM Data and Configure Options

Synchronize CM Data/Launch Element Cut Through | Configuration Options |
Expand All | Collapse All

Synchronize CM Data/Launch Element Cut Through ▾

1 Item Refresh Show ALL Filter: Enable

<input checked="" type="checkbox"/>	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version
<input checked="" type="checkbox"/>	CM-ES	10.10.9.42	February 22, 2011 2:01:03 AM +00:00	10:00 pm MON FEB 21, 2011	Incremental	Completed		R016x.00.1.510.1

Select : All, None

☒ Initialize data for selected devices
☐ Incremental Sync data for selected devices
☐ Save Translations for selected devices

Now Schedule Cancel Launch Element Cut Through

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**.

Users

- Administrators**
Manage Administrative Users
- Groups & Roles**
Manage groups, roles and assign roles to users
- Synchronize and Import**
Synchronize users with the enterprise directory, import users from file
- User Management**
Manage users, shared user resources and provision users

Elements

- Application Management**
Manage applications and application certificates
- Communication Manager**
Manage Communication Manager objects
- Conferencing**
Conferencing
- Inventory**
Manage, discover, and navigate to elements, update element software
- Messaging**
Manage Messaging System objects
- Presence**
Presence
- Routing**
Network Routing Policy
- SIP AS 8.1**
SIP AS 8.1
- Session Manager**
Session Manager Element Manager

Services

- Backup and Restore**
Backup and restore System Manager database
- Configurations**
Manage system wide configurations
- Events**
Manage alarms, view and harvest logs
- Licenses**
View and configure licenses
- Replication**
Track data replication nodes, repair replication nodes
- Scheduler**
Schedule, track, cancel, update and delete jobs
- Security**
Manage Security Certificates
- Templates**
Manage Templates for Communication Manager and Messaging System objects

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

User Management

Users

View Edit **New** Duplicate Delete More Actions

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)

The screenshot shows the 'New User Profile' form in the Avaya System Manager interface. The 'Identity' tab is selected and highlighted with a red box. The form contains the following fields:

- Last Name:** Phone
- First Name:** SIP
- Middle Name:**
- Description:**
- Login Name:** 41000@mmsil.local
- Authentication Type:** Basic
- Password:**
- Confirm Password:**
- Localized Display Name:**
- Endpoint Display Name:**
- Honorific:**
- Language Preference:**
- Time Zone:**

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).

☒ **Session Manager Profile** ▼

* **Primary Session Manager** Session Manager ▼

Primary	Secondary	Maximum
5	0	5

Secondary Session Manager (None) ▼

Primary	Secondary	Maximum

Origination Application Sequence CM-ES ▼

Termination Application Sequence CM-ES ▼

Survivability Server (None) ▼

* **Home Location** Dublin ▼

☒ **Endpoint Profile** ▼

* **System** CM-ES ▼

* **Profile Type** Endpoint ▼

Use Existing Endpoints ☐

* **Extension** 41000 Endpoint Editor

* **Template** DEFAULT_9620SIP_CM_6_0 ▼

Set Type 9620SIP

Security Code

* **Port** IP

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User or on Delete User. ☐

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.

The screenshot shows the 'SIP Entity Link Monitoring Status Summary' page. The left sidebar has 'SIP Entity Monitoring' selected under 'System Status'. The main content area shows a summary table with one item, 'Session Manager', where all link counts are 0. Below this is a list of 'All Monitored SIP Entities' including Alcatel PBX, AudioCodes M1K, AudioCodes M2K, Bridge Standard 6.0, Bridge Enterprise 6.0, Cisco, CM-AE 5.2.1, and CM-ES. The names 'Alcatel PBX' and 'CM-ES' are highlighted with red boxes.

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
Session Manager	0/11	0	0	0

SIP Entity Name
Alcatel PBX
AudioCodes M1K
AudioCodes M2K
Bridge Standard 6.0
Bridge Enterprise 6.0
Cisco
CM-AE 5.2.1
CM-ES

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:

The screenshot shows the 'SIP Entity, Entity Link Connection Status' page for 'Alcatel PBX'. The left sidebar has 'SIP Entity Monitoring' selected. The main content area shows a table with connection details for the 'Session Manager' instance. The 'Conn. Status' is 'Up' and the 'Link Status' is 'Up', both highlighted with red boxes.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	Session Manager	10.10.9.111	5060	TCP	Up	200 OK	Up

Communication Manager connection status is show below:

The screenshot shows the Avaya Aura Communication Manager web interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, and System Status. The 'SIP Entity Monitoring' option is highlighted. The main content area is titled 'SIP Entity, Entity Link Connection Status' and displays a table of connection status for all entity links. The table has columns for Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The 'Session Manager' entry is highlighted, showing a resolved IP of 10.10.9.45, port 5060, TCP protocol, and a connection status of 'Up'.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	Session Manager	10.10.9.45	5060	TCP	Up	200 OK	Up

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>

©2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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