



## **Avaya Solution & Interoperability Test Lab**

---

# **Configuring SIP Trunks between Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager 5.2.1, and Avaya IP Office Release 5.0 – Issue 1.0**

## **Abstract**

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Aura™ Communication Manager 5.2.1 and Avaya IP Office using SIP trunks. Session Initiated Protocol (SIP) is a standard based communication protocol capable of supporting voice, video, instant messaging and other multi-media communication. These Application Notes will outline a solution for using SIP as a trunk protocol between Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager 5.2.1 and Avaya IP Office.

## **Table of Content**

1	Introduction.....	4
2	Equipment and Software Validated .....	5
3	Configure Avaya IP Office .....	6
3.1	Verify IP Office License .....	6
3.2	Obtain LAN IP Address.....	7
3.3	Configure Network Topology.....	7
3.4	Administer SIP Registrar .....	8
3.5	Administer Codec Preference .....	8
3.6	Administer SIP Trunk .....	9
3.7	Administer Short Code .....	10
3.8	Configure Incoming Call Route.....	11
3.9	Configure SIP User Names .....	11
3.10	Save Configuration .....	12
4	Configure Avaya Aura™ Session Manager.....	12
4.1	Specify SIP Domain.....	13
4.2	Add Locations.....	13
4.3	Add SIP Entities.....	15
4.4	Add Entity Links.....	18
4.5	Add Time Ranges .....	19
4.6	Add Routing Policies .....	21
4.7	Add Dial Patterns.....	22
5	Configure Avaya Aura™ Communication Manager Access Element .....	25
5.1	Verify Communication Manager License.....	25
5.2	Configure System Parameters Features .....	26
5.3	Configure IP Node Names .....	26
5.4	Configure IP Interface for C-LAN.....	27
5.5	Configure IP Codec Sets and Network Regions .....	27
5.6	Configure SIP Signaling Group and Trunk Group .....	28
5.6.1	SIP Signaling Group .....	28
5.6.2	SIP Trunk Group.....	29
5.7	Configure Route Pattern .....	30
5.8	Configure Private Numbering.....	31
5.9	Administer Dial Plan and AAR Analysis .....	31
5.10	Save Translations .....	32
6	Configure Avaya Aura™ Communication Manager Feature Server.....	33
6.1	Verify Communication Manager License.....	33
6.2	Configure System Parameters Features .....	33
6.3	Configure IP Node Names .....	34
6.4	Configure SIP Signaling Group and Trunk Group .....	34
6.4.1	SIP Signaling Group .....	34
6.4.2	SIP Trunk Group.....	35
6.5	Configure Route Pattern .....	36
6.6	Configure Private Numbering.....	36
6.7	Administer Dial Plan and AAR Analysis .....	37

6.8	Save Translations .....	37
7	Verification Steps.....	38
7.1	Verify Avaya Aura™ Communication Manager.....	38
7.2	Verify Avaya Aura™ Session Manager .....	42
7.3	Verify Avaya IP Office.....	43
7.4	Verification Scenarios.....	44
8	Conclusion .....	45
9	Additional References.....	45

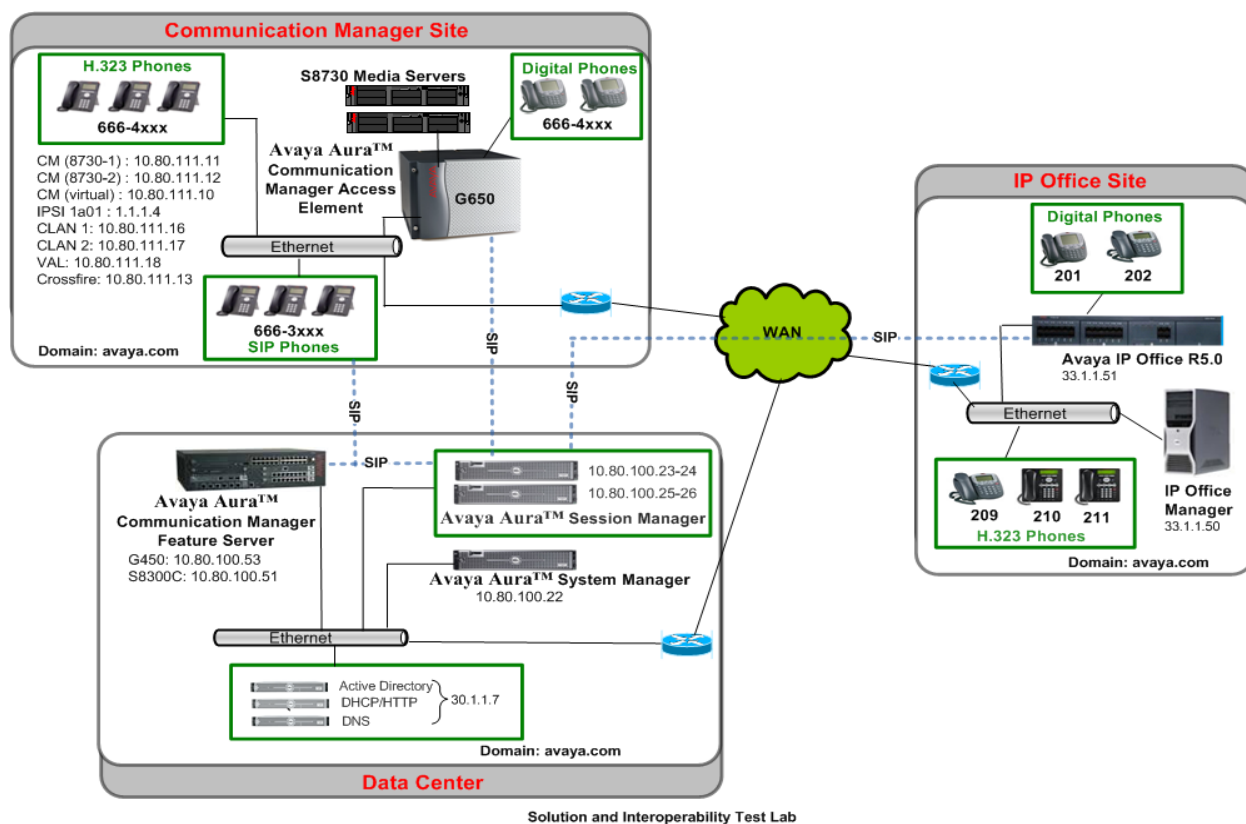
# 1 Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Aura™ Communication Manager 5.2.1 and Avaya IP Office using SIP trunks. Session Initiated Protocol (SIP) is a standard based communication protocol capable of supporting voice, video, instant messaging and other multi-media communication. These Application Notes will outline a solution for using SIP as a trunk protocol between Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager 5.2.1 and Avaya IP Office.

As shown in **Figure 1**, the Avaya 96xx IP Telephone (H.323) and 2420 Digital Telephone are supported by Communication Manager which serves as an Access Element within the Avaya Aura™ Session Manager architecture. The Avaya 5610 and 1608 IP Telephones (H.323) and 54xx Digital Telephones are supported by Avaya IP Office 500. SIP trunks are used to connect these two systems to Avaya Aura™ Session Manager, using its SM-100 (Security Module) network interface. 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 multi-vendor systems to interoperate. It is managed by a separate Avaya Aura™ System Manager, which can manage multiple Avaya Aura™ Session Managers by communicating with their management network interfaces. Avaya 9620 IP Telephones configured as SIP users utilizes the Avaya Aura™ Session Manager User Registration feature and require Communication Manager Feature Server. Communication Manager as a feature server only supports IMS-SIP users that are registered to Avaya Aura™ Session Manager. The Communication Manager Feature Server is connected to Session Manager via an IMS-enabled SIP signaling group and associated SIP trunk group.

For the sample configuration, Avaya Aura™ Session Manager runs on an Avaya S8510 Server, and Avaya Aura™ Communication Manager 5.2.1 runs on an Avaya S8730 Server with Avaya G650 Media Gateway. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura™ Communication Manager 5.2.1 and Avaya IP Office on the 500 platform.

These Application Notes will focus on the configuration of the SIP trunks and call routing. Detailed administration of Session Manager, Communication Manager Feature Server, Communication Manager Access Element and the endpoint telephones will not be described (see the appropriate documentation listed in **Section 9**).



**Figure 1 – Sample Configuration**

## 2 Equipment and Software Validated

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

Hardware Component	Software Version
Avaya S8510 Server	Avaya Aura™ Session Manager Release 5.2 (Build 520011)
	Avaya Aura™ System Manager, Release 5.2 (5.2.7.0)
Avaya S8730 Servers with G650 Media Gateway	Avaya Aura™ Communication Manager Release 5.2 (R015x.02.1.016.4)
Avaya S8300C Server with G450 Media Gateway	Avaya Aura™ Communication Manager Release 5.2 (R015x.02.1.016.4)
Avaya 9630 IP Telephone (H.323)	2.0
Avaya 9630 IP Telephone (SIP)	2.5.5.17
Avaya 2420 Digital Telephone	NA
Avaya IP Office Server	Release 5.0 (8)
Avaya 5410 & Avaya 5420 Digital Telephones	NA
Avaya 1608 IP Telephone (H.323)	ha1608ual_2110.bin
Avaya 5610 IP Telephone (H.323)	2.9

### 3 Configure Avaya IP Office

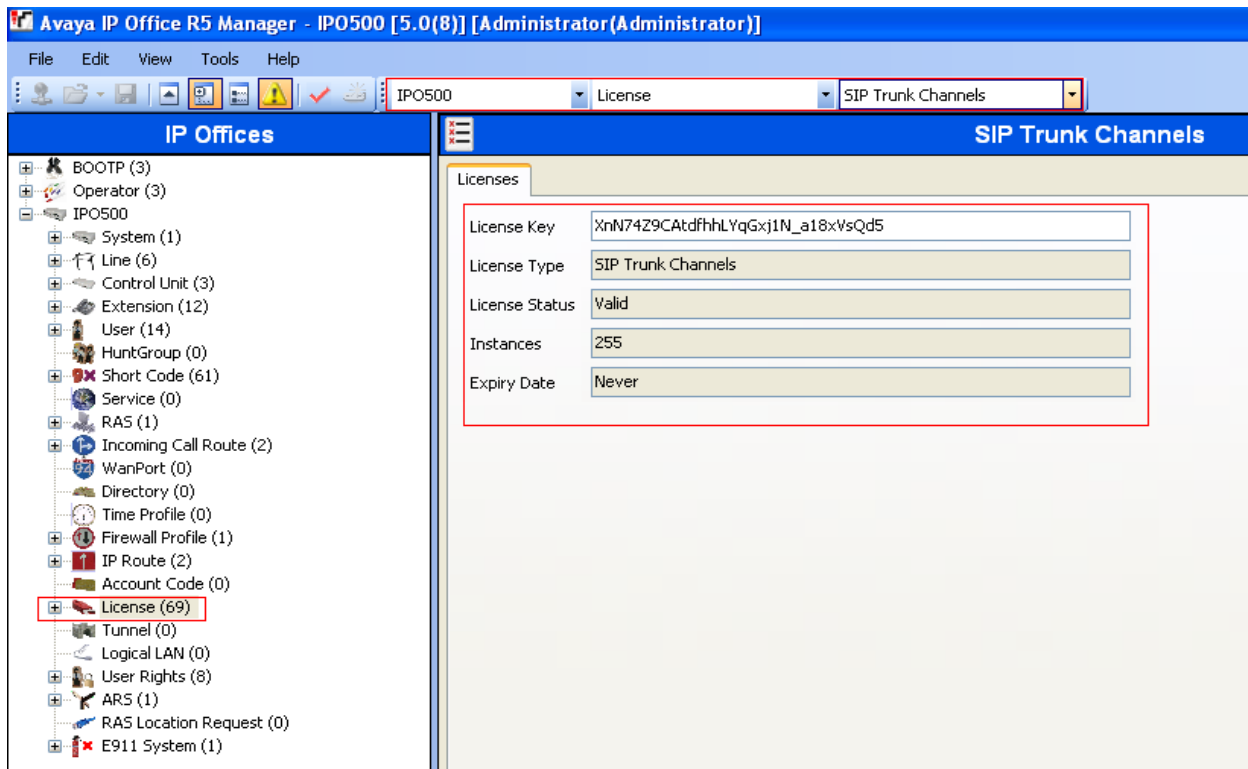
This section provides the procedures for configuring Avaya IP Office. The procedures include the following areas:

- Verify IP Office license
- Obtain LAN IP address
- Configure Network Topology
- Administer SIP Registrar
- Administer Codec Preference
- Administer SIP Trunk
- Administer Short Code
- Configure Incoming Call Route
- Configure Users SIP Names

#### 3.1 Verify IP Office License

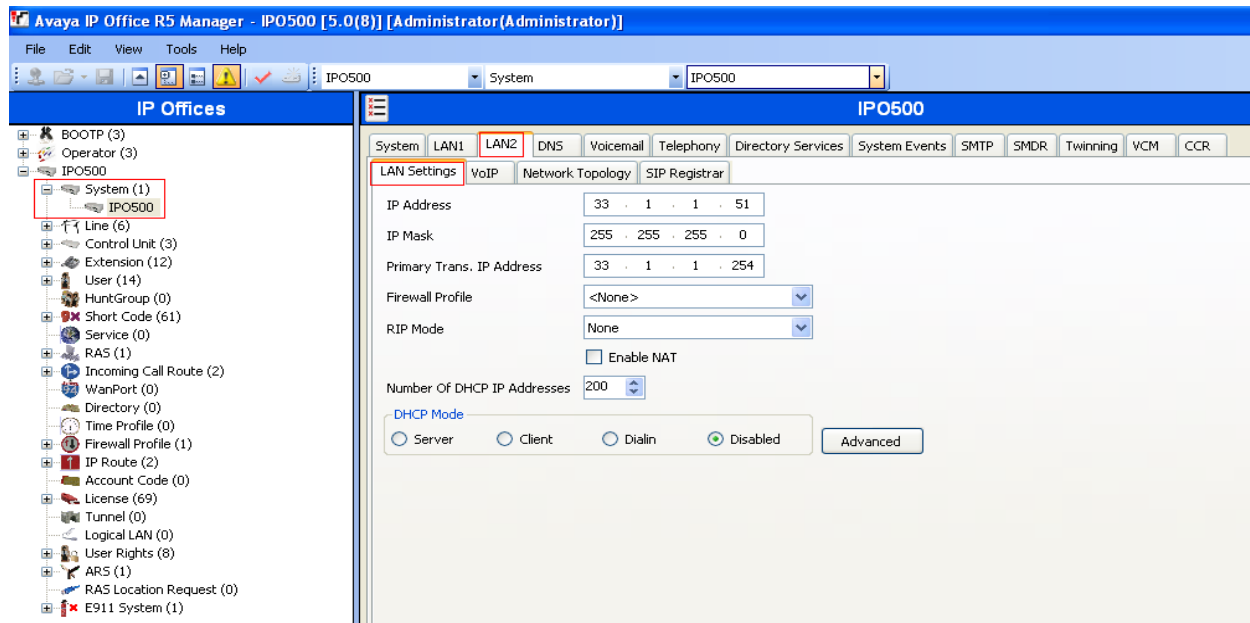
From a PC running the Avaya IP Office Manager application, select **Start > Programs > IP Office > Manager** to launch the Manager application. Select the proper IP Office system, and log in with the appropriate credentials.

The **Avaya IP Office Manager** screen is displayed. From the configuration tree in the left pane, select **License > SIP Trunk Channels** to display the **SIP Trunk Channels** screen in the right pane. Verify that the **License Status** is “Valid”.



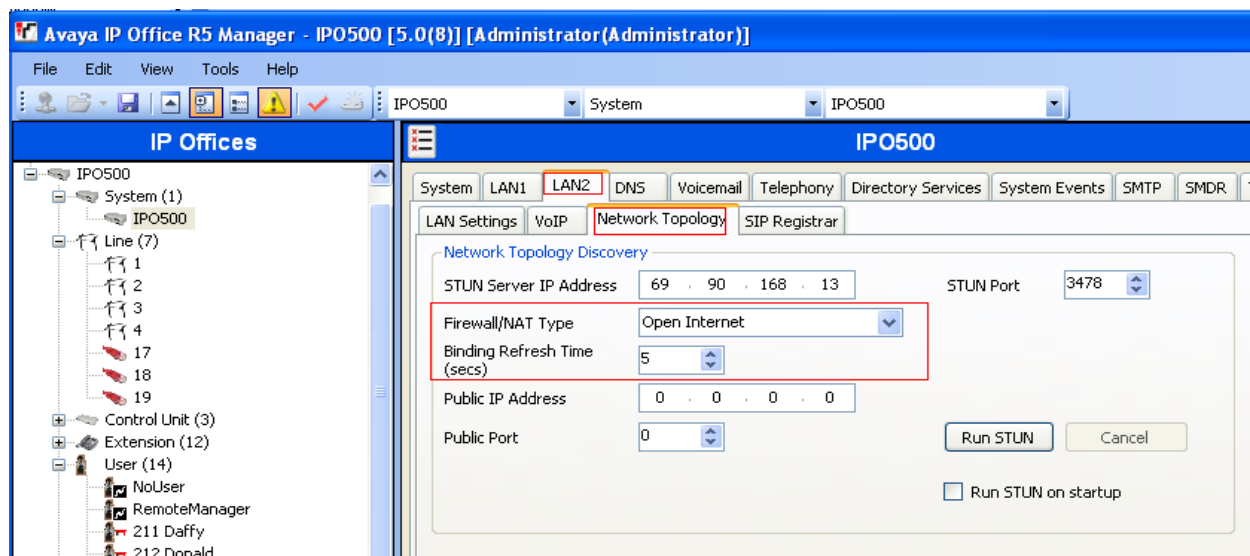
## 3.2 Obtain LAN IP Address

From the configuration tree in the left pane, select **System** to display the **IPO500** screen in the right pane. Select the **LAN2** tab, followed by the **LAN Settings** sub-tab in the right pane. Make a note of the **IP Address**, which will be used later to configure SIP trunks. Note that IP Office can support SIP trunks on the LAN1 and/or LAN2 interfaces, and the sample configuration used the LAN2 interface.



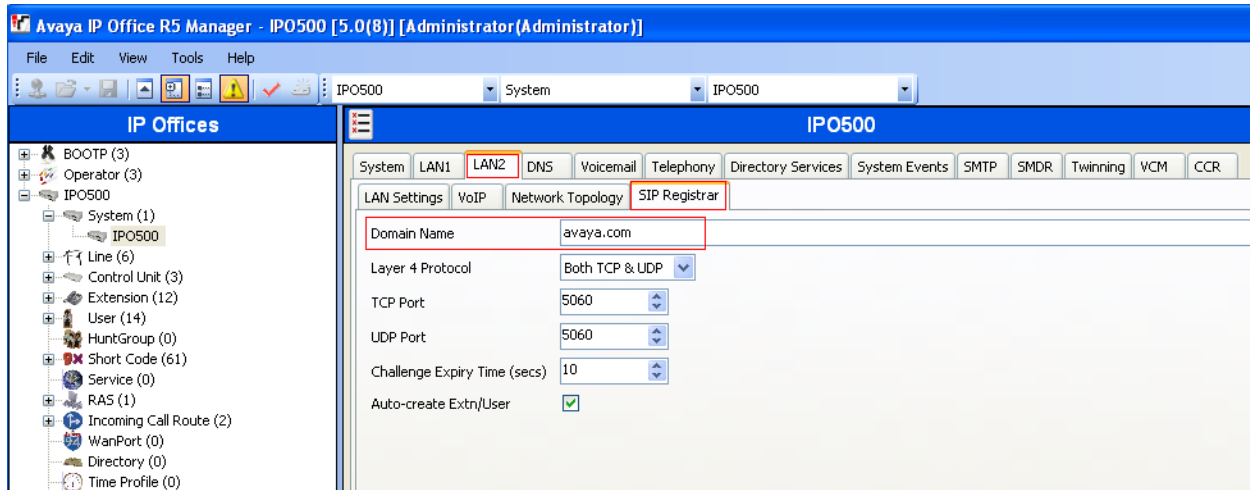
## 3.3 Configure Network Topology

From the configuration tree in the left pane, select **System** to display the **IPO500** screen in the right pane. Select the **LAN2** tab, followed by the **Network Topology** sub-tab in the right pane. Configure **Firewall/NAT Type** to “Open Internet”. Configure **Binding Refresh Time** to “5”. Click **OK**.



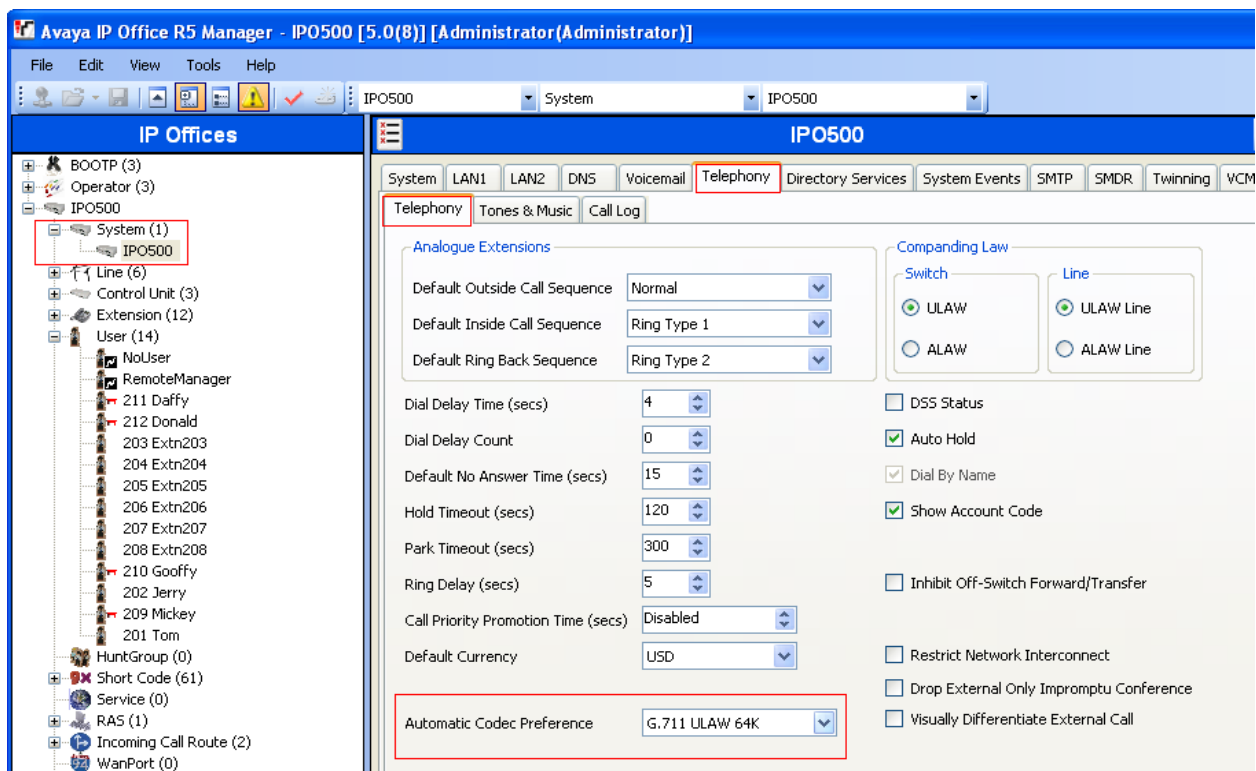
### 3.4 Administer SIP Registrar

Select **SIP Registrar** sub-tab in the right pane. Enter a valid **Domain Name**. Make a note of the **Layer 4 Protocol** and **TCP Port** and **UDP Port** numbers. These will be used later to configure SIP trunks. Click **OK**.



### 3.5 Administer Codec Preference

From the configuration tree in the left pane, select **System** to display the **IPO500** screen in the right pane. Select the **Telephony** tab. Configure **Automatic Codec Preference** to “G.711 ULAW 64K”. Click **OK**.





### 3.6 Administer SIP Trunk

From the configuration tree in the left pane, right-click on **Line** and select **New > SIP Line** to add a new SIP Trunk. Enter the “IP address for Session Manager” in **ITSP IP Address** field. Make a note of the **Line Number**. Select **Layer 4 Protocol** as “TCP” and **Send Port** “5060”. Select “LAN2” in the **Use Network Topology Info**. Retain default values for all other fields. Click **OK**.

Avaya IP Office R5 Manager - IPO500 [5.0(8)] [Administrator/Administrator]]

File Edit View Tools Help

IPO500 Line 17

**IP Offices**

- BOOTP (3)
- Operator (3)
- IPO500
  - System (1)
  - IPO500
    - Line (6)
      - 1
      - 2
      - 3
      - 4
      - 17
      - 18
    - Control Unit (3)
    - Extension (12)
    - User (14)
    - HuntGroup (0)
    - Short Code (61)
    - Service (0)
    - RAS (1)
    - Incoming Call Route (2)
    - WanPort (0)
    - Directory (0)
    - Time Profile (0)
    - Firewall Profile (1)
    - IP Route (2)
    - Account Code (0)

**SIP Line - Line 17**

SIP Line SIP URI VoIP T38 Fax

Line Number 17

ITSP Domain Name

ITSP IP Address 10 . 80 . 100 . 24

Primary Authentication Name

Primary Authentication Password

Primary Registration Expiry (mins) 60

Secondary Authentication Name

Secondary Authentication Password

Secondary Registration Expiry (mins) 60

Send Caller ID None

Registration Required ☐

In Service ☒

Use Tel URI ☐

**Network Configuration**

Layer 4 Protocol TCP Send Port 5060

Use Network Topology Info LAN 2 Listen Port 5060

Select the **SIP URI** tab, and click on **Add...** radio button. In the **Incoming Group** and **Outgoing Group** enter the “Line Number” from the above step. Retain default values for all other fields. Click **OK**.

New Channel

Via 33.1.1.51

Local URI Use Authentication Name

Contact Use Authentication Name

Display Name Use Authentication Name

Registration Primary

Incoming Group 17

Outgoing Group 17

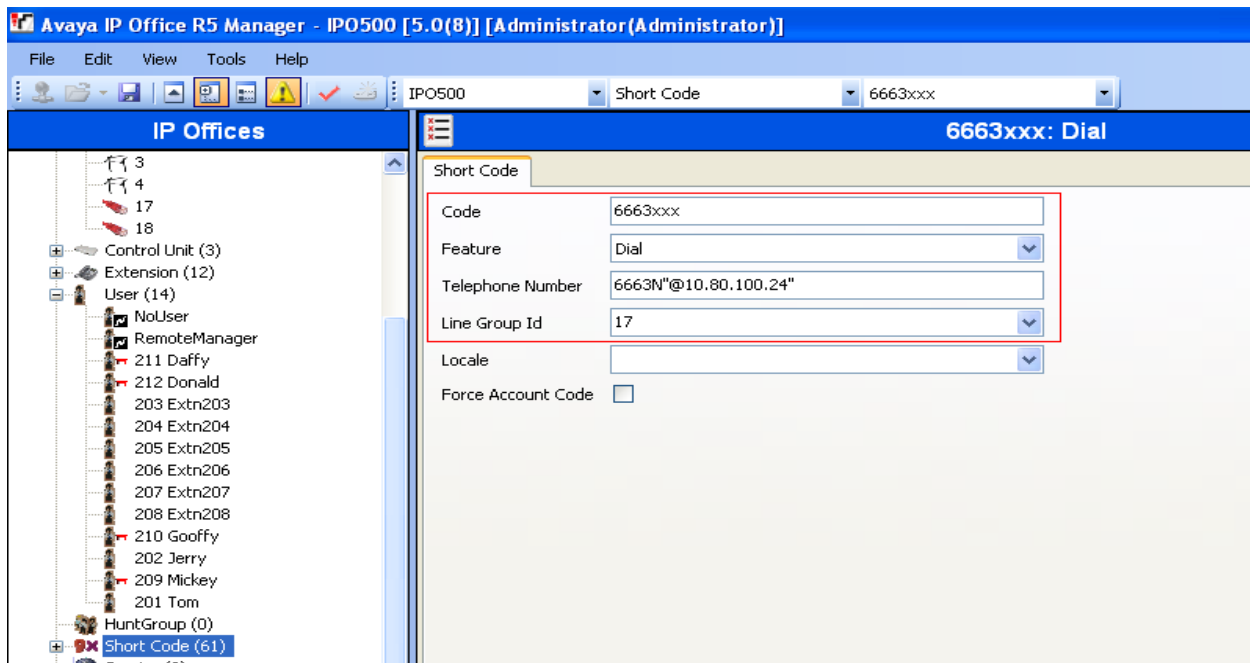
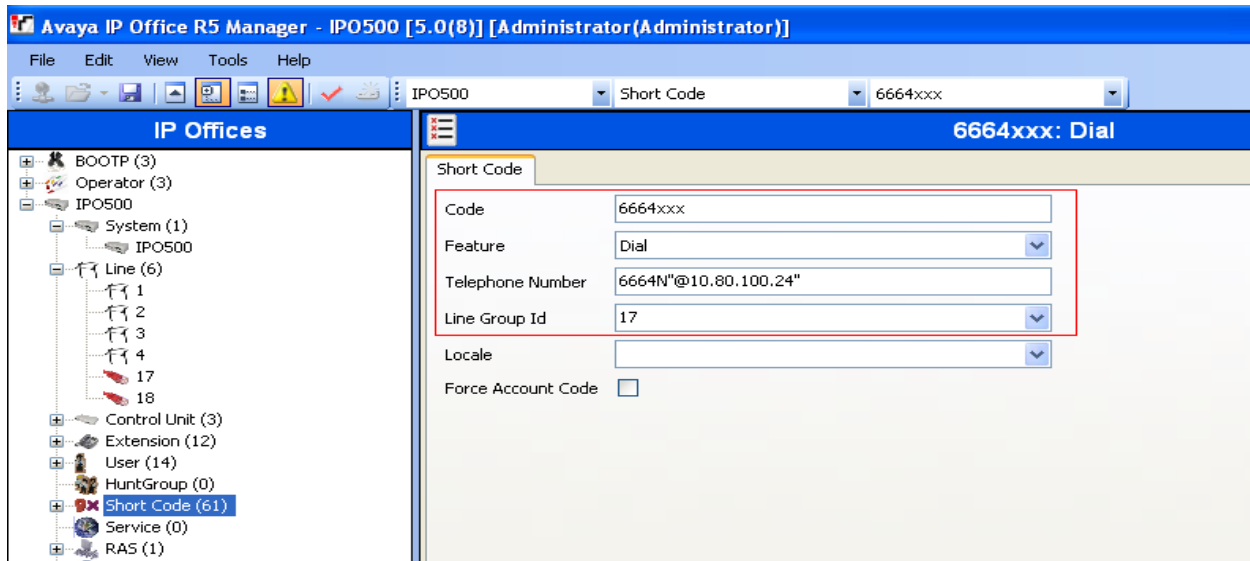
Max Calls per Channel 10

OK

Cancel

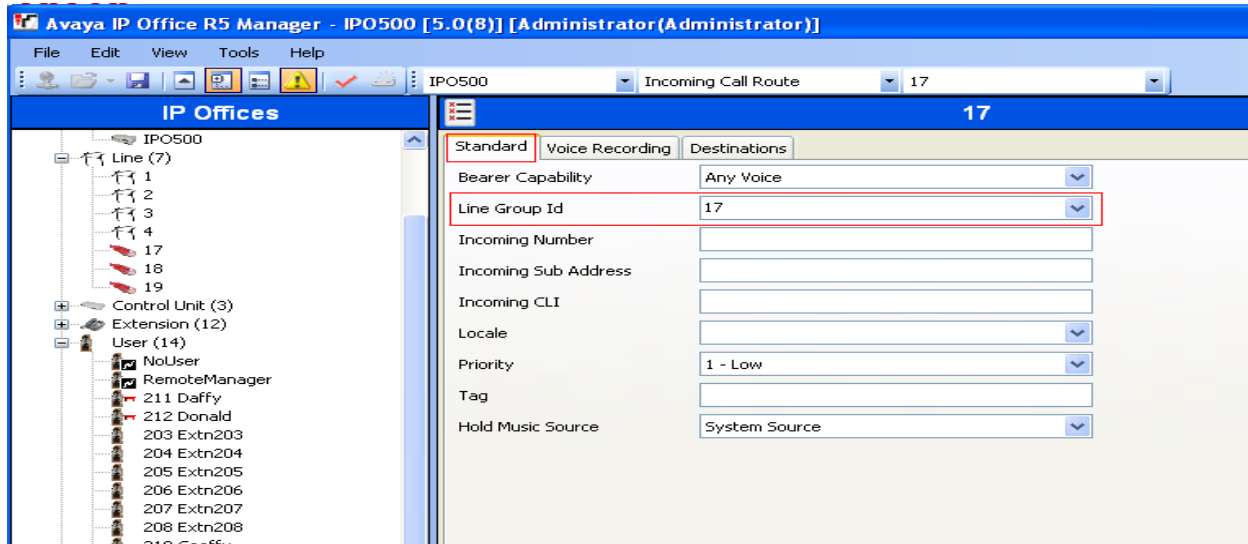
### 3.7 Administer Short Code

From the configuration tree in the left pane, right-click on **Short Code**, and select **New**. Enter the dialing string that will be used to call the users on Communication Manager in the **Code** field. Select “Dial” from the drop down menu for **Feature** and enter the phone number appended with “@<ip-address of Session Manager>” in the **Telephone Number**. Select SIP trunk administered in **Section 3.6** in the **Line Group Id**. Shown below are two short code which were added for the sample configuration.

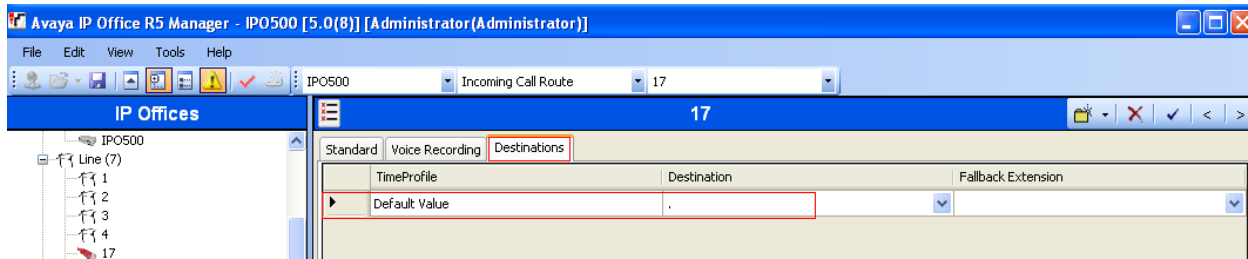


### 3.8 Configure Incoming Call Route

From the configuration tree in the left pane, right-click on **Incoming Call Route**, and select **New**. Under the **Standard** tab, enter the SIP trunk administered in **Section 3.6** in the **Line Group Id**.

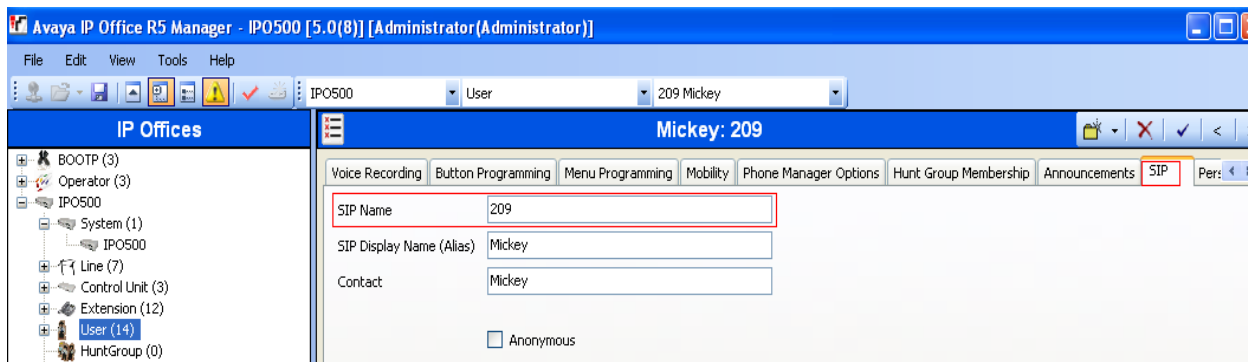


Under the **Destination** tab, enter “.” as the Default Value. This will enable all incoming calls to be routed to any extension.



### 3.9 Configure SIP User Names

From the configuration tree in the left pane, right-click on **User** and select **SIP** tab. Modify the **SIP Name** to be the same as the user’s extension number. The other fields can be left as default. Repeat this for all users.



### 3.10 Save Configuration

Select **File > Save Configuration** to save and send the configuration to the IP Office server.

## 4 Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Avaya Aura™ Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities corresponding to the SIP telephony systems and Avaya Aura™ Session Manager
- Entity Links, which define the SIP trunk parameters used by Avaya Aura™ Session Manager when routing calls to/from SIP Entities
- Time Ranges during which routing policies are active
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Session Manager Server to be managed by Avaya Aura™ System Manager.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura™ System Manager, using the URL “http://<ip-address>/IMSM”, where “<ip-address>” is the IP address of Avaya Aura™ System Manager. Log in with the appropriate credentials and accept the Copyright Notice. The menu shown below is displayed. Expand the **Network Routing Policy** Link on the left side as shown. The sub-menus displayed in the left column below will be used to configure all but the last of the above items (**Sections 4.1 through 4.7**).

**AVAYA**

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 10, 2009 3:37  
[Help](#) | [Log](#)

Home / Network Routing Policy

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

▶ Security

▶ Applications

▶ Settings

▶ Session Manager

Shortcuts

[Change Password](#)

[Landing Page](#)

[Help for Import All Data](#)

Introduction to Network Routing Policy (NRP)

Network Routing Policy consists of several NRP applications like "Domains", "Locations", "SIP Entities", etc.  
The recommended order to use the NRP applications (that means the overall NRP workflow) to configure your network configuration is as follows:  
  
Step 1: Create "Domains" of type SIP (other NRP applications are referring domains of type SIP).  
  
Step 2: Create "Locations"  
  
Step 3: Create "Adaptations"  
  
Step 4: Create "SIP Entities"  

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

  
Step 5: Create the "Entity Links"  

- Between Session Managers
- Between Session Managers and "other SIP Entities"

  
Step 6: Create "Time Ranges"  

- Align with the tariff information received from the Service Providers

  
Step 7: Create "Routing Policies"  

- Assign the appropriate "Routing Destination" and "Time Of Day"

## 4.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **SIP Domains** on the left and clicking the **New** button on the right. The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., “avaya.com”)
- **Notes:** Descriptive text (optional).

Click **Commit**.

The screenshot shows the Avaya Aura™ System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name, and a user greeting. A red breadcrumb trail indicates the path: Home / Network Routing Policy / SIP Domains. On the left, a sidebar menu lists various management categories, with 'SIP Domains' highlighted under 'Network Routing Policy'. The main content area, titled 'Domain Management', contains action buttons (Edit, New, Duplicate, Delete, More Actions) and a table with one item: 'avaya.com' of type 'sip'. Below the table is a selection summary: 'Select : All, None ( 0 of 1 Selected )'.

Name	Type	Default	Notes
avaya.com	sip	<input type="checkbox"/>	

## 4.2 Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management. For the sample configuration, Locations are added for the Communication Manager Feature Server, Communication Manager Access Element and IP Office.

To add a location, select **Locations** on the left and click on the **New** button on the right. The following screen will then be shown. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under *Location Pattern*:

- **IP Address Pattern:** A pattern used to logically identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows the information for IP Office. Click **Commit** to save.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Dec. 2:51 PM [Help](#)

Home / Network Routing Policy / Locations / Location Details

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

**Locations**

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

▶ Security

▶ Applications

▶ Settings

▶ Session Manager

Location Details Commit

General

\* Name: IPO 500

Notes:

Managed Bandwidth:

\* Average Bandwidth per Call: 80 Kbit/sec

\* Time to Live (secs): 3600

Location Pattern

Add Remove

1 Item | Refresh Filter:

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 33.1.1.*	

Select : All, None ( 0 of 1 Selected )

\* Input Required

Commit

The following screen shows the updated Locations after all the three locations are added.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Dec. 3:44 PM

Home / Network Routing Policy / Locations

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

**Locations**

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

Location

Edit New Duplicate Delete More Actions Commit

5 Items | Refresh

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	10_80_100	CM Feature Server
<input type="checkbox"/>	10_80_111	CM Access Element
<input type="checkbox"/>	Cisco subnet 192_45_130	CUCM
<input type="checkbox"/>	IPO_500	
<input type="checkbox"/>	Nortel-CS1000e	

Select : All, None ( 0 of 5 Selected )

### 4.3 Add SIP Entities

A SIP Entity must be added for Avaya Aura™ Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration a SIP Entity is added for the ASM, the C-LAN board in the Avaya G650 Media Gateway, and Avaya IP Office. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the ASM or the signaling interface on the telephony system.
- **Type:** “Session Manager” for Avaya Aura™ Session Manager,  
“CM” for Communication Manager Access Element,  
“CM” for Communication Manager Feature Server, and  
“SIP Trunk” for Avaya IP Office.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

Under *SIP Link Monitoring*:

- **SIP Link Monitoring:** Select “Use Session Manager Configuration” for Communication Manager Access Element, Session Manager and Avaya IP Office.  
  
Select “Link Monitoring Enabled” for Communication Manager Feature Server,

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The following screen shows addition of Avaya Aura™ Session Manager. The IP address used is that of the SM-100 Security Module.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Dec. 10, 2009 [Help](#)

Home / Network Routing Policy / SIP Entities / SIP Entity Details

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

**SIP Entities**

Time Ranges

Personal Settings

▶ Security

SIP Entity Details

Commit

General

\* Name: ASM1-DR

\* FQDN or IP Address: 10.80.100.24

Type: Session Manager

Notes: ASM in Westminster SIL Lab

Location: 10\_80\_100

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring: Use Session Manager Configuration

SIP Link Monitoring

The following screen shows addition of Avaya IP Office.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Dec. 10, 2009 [Help](#)

Home / Network Routing Policy / SIP Entities / SIP Entity Details

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

**SIP Entities**

Time Ranges

Personal Settings

▶ Security

▶ Applications

▶ Settings

▶ Session Manager

SIP Entity Details

Commit

General

\* Name: IPO 500

\* FQDN or IP Address: 33.1.1.51

Type: SIP Trunk

Notes: IPO in WM

Adaptation:

Location: IPO 500

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

SIP Link Monitoring: Use Session Manager Configuration

SIP Link Monitoring



The following screen shows addition of Communication Manager Access Element. The IP address used is that of the C-LAN board in the Avaya G650 Media gateway.

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 10, 2009 [Help](#)

Home / Network Routing Policy / SIP Entities / SIP Entity Details

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

Security

Applications

Settings

Session Manager

SIP Entity Details

Commit

General

\* Name:

S8730-1

\* FQDN or IP Address:

10.80.111.16

Type:

CM

Notes:

S8730 Pair CLAN-1

Adaptation:

Location:

10\_80\_111

Time Zone:

America/Denver

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

The following screen shows addition of Communication Manager Feature Server. The IP address used is that of the S8300C server.

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 10, 2009 [Help](#)

Home / Network Routing Policy / SIP Entities / SIP Entity Details

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

Security

Applications

Settings

Session Manager

SIP Entity Details

Commit

General

\* Name:

S8300-G450-FS

\* FQDN or IP Address:

10.80.100.51

Type:

CM

Notes:

CM 5.2.1

Adaptation:

Location:

10\_80\_100

Time Zone:

America/Denver

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:

Link Monitoring Enabled

\* Proactive Monitoring Interval (in seconds):

120

\* Reactive Monitoring Interval (in seconds):

120

\* Number of Retries:

1

PV; Reviewed:  
SPOC 01/31/2010

Solution & Interoperability Test Lab Application Notes  
©2010 Avaya Inc. All Rights Reserved.

17 of 46  
ASM-CM-IPO


## 4.4 Add Entity Links

A SIP trunk between Avaya Aura™ Session Manager and a telephony system is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Avaya Aura™ Session Manager.
- **Port:** Port number to which the other system sends SIP requests  
In the sample configuration, TCP Protocol was used.
- **SIP Entity 2:** Select the name of the other system.
- **Port:** Port number on which the other system receives SIP requests
- **Trusted:** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity specified in **Section 4.3** will be denied.

Click **Commit** to save each Entity Link definition. The following screens illustrate adding the three Entity Links for:

1. Avaya IP Office
2. Communication Manager Access Element
3. Communication Manager Feature Server

 Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 10, 2009 4:49 PM  
[Help](#) | [Log off](#)

Home / Network Routing Policy / Entity Links

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

Entity Links

Commit

Cancel

1 Item [Refresh](#) Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ASM1-DR_IPO 500_	* ASM1-DR	TCP	* 5060	* IPO 500	* 5060	<input checked="" type="checkbox"/>	

\* Input Required 

Commit

Cancel

## Entity Links

[Commit](#) [Can](#)

1 Item | [Refresh](#) Filter: Enab

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ASM1 to S8730	* ASM1-DR	TCP	* 5060	* S8730-1	* 5060	<input checked="" type="checkbox"/>	

\* Input Required

[Commit](#) [Can](#)

## Entity Links

[Commit](#) [Cancel](#)

1 Item | [Refresh](#) Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ASM-to-S8300	* ASM1-DR	TCP	* 5060	* S8300-G450-FS	* 5060	<input checked="" type="checkbox"/>	

\* Input Required

[Commit](#) [Cancel](#)

## 4.5 Add Time Ranges

Before adding routing policies (see next section), time ranges must be defined during which the policies will be active. In the sample configuration, one policy was defined that would allow routing to occur at anytime. To add this time range, select **Time Ranges**, and click on the left and click on the **New** button on the right. Fill in the following:

- **Name:** A descriptive name (e.g., “Anytime”).
- **Mo through Su** Check the box under each of these headings
- **Start Time** Enter 00:00.
- **End Time** Enter 23:59

Click **Commit** to save this time range.



- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▼ Network Routing Policy
  - Adaptations
  - Dial Patterns
  - Entity Links
  - Locations
  - Regular Expressions
  - Routing Policies
  - SIP Domains
  - SIP Entities
  - Time Ranges**
  - Personal Settings

Time Ranges

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions ▾](#) [Commit](#)

1 Item   <a href="#">Refresh</a>										Filter: <a href="#">Enable</a>	
<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	<a href="#">24/7</a>	<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"/>	<input type="text" value="00:00"/>	<input type="text" value="23:59"/>	<input type="text" value="Time Range 24/7"/>
Select : All, None ( 0 of 1 Selected )											

## 4.6 Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 4.3**. Two routing policies must be added – one for IP Office, one for Communication Manager Access Element. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **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 select the time range configured in the previous section.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition.

The following screens show the Routing Policy for IP Office.

 Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 14, 2009 3:51 PM

[Help](#) | [Log off](#)

Home / Network Routing Policy / Routing Policies / Routing Policy Details

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

Security

Applications

Settings

Session Manager

Shortcuts

[Change Password](#)

Routing Policy Details

Commit

Cancel

General

\* Name:

to IPO 500

Disabled:

☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
IPO 500	33.1.1.51	SIP Trunk	IPO in WM

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	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	Time Range 24/7

Select : All, None ( 0 of 1 Selected )

The following screens show the Routing Policy for Communication Manager Access Element.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Dec. 14, 2009 3:51 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Routing Policies / **Routing Policy Details**

**Routing Policy Details** [Commit](#) [Cancel](#)

**General**

\* **Name:**

**Disabled:** ☐

**Notes:**

**SIP Entity as Destination**

[Select](#)

Name	FQDN or IP Address	Type	Notes
S8730-1	10.80.111.16	CM	S8730 Pair CLAN-1

**Time of Day**

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

1 Item | [Refresh](#) Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	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	Time Range 24/7

Select : All, None ( 0 of 1 Selected )

**Shortcuts**

[Change Password](#)

[Help for Routing Policy Details](#)

No Routing Policy is required for Communication Manager Feature Server, as these phones are registered directly to Session Manager.

## 4.7 Add Dial Patterns

Define dial patterns to direct calls to the appropriate SIP Entity. 7-digit extensions beginning with “6664” reside on Communication Manager Access Element, and 3-digit extensions beginning with “2” reside on Avaya IP Office. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right. Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Avaya Aura™ Communication Manager Access Element:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain specified in **Section 4.1**
- **Notes** Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

In the sample configuration, all calls originating from endpoints connected to Avaya IP Office dial “666-xxxx” where “4xxx” is the 4-digit extension on Communication Manager Access Element.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 14, 2009 3:51 PM

[Help](#) | [Log off](#)

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

- Asset Management
- Communication System Management
- User Management
- Monitoring
- Network Routing Policy
  - Adaptations
  - Dial Patterns**
  - Entity Links
  - Locations
  - Regular Expressions
  - Routing Policies
  - SIP Domains
  - SIP Entities
  - Time Ranges
  - Personal Settings
- Security
- Applications
- Settings
- Session Manager

Shortcuts

Dial Pattern Details

Commit Cancel

General

\* Pattern: 6664

\* Min: 7

\* Max: 7

Emergency Call: ☐

SIP Domain: -ALL-

Notes: to S8730 CM

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to S8730 CM	0	<input type="checkbox"/>	S8730-1	

Select : All, None ( 0 of 1 Selected )

In the sample configuration, all calls originating from endpoints connected to Communication Manager Access Element or Feature server dial “2xx” where “2xx” is the 3-digit extension on Avaya IP Office.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 14, 2009 3:51 PM

[Help](#) | [Log off](#)

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

- Asset Management
- Communication System Management
- User Management
- Monitoring
- Network Routing Policy
  - Adaptations
  - Dial Patterns**
  - Entity Links
  - Locations
  - Regular Expressions
  - Routing Policies
  - SIP Domains
  - SIP Entities
  - Time Ranges
  - Personal Settings
- Security
- Applications
- Settings
- Session Manager

Shortcuts

Dial Pattern Details

Commit Cancel

General

\* Pattern: 2

\* Min: 3

\* Max: 3

Emergency Call: ☐

SIP Domain: -ALL-

Notes: To IPO

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to IPO 500	0	<input type="checkbox"/>	IPO 500	

Select : All, None ( 0 of 1 Selected )





## 5 Configure Avaya Aura™ Communication Manager Access Element

This section describes configuring Avaya Aura™ Communication Manager Access Element in the following areas. Some administration screens have been abbreviated for clarity.

- Verify Communication Manager license
- Administer system parameters features
- Administer IP node names
- Administer IP interface
- Administer IP codec set and network region
- Administer SIP trunk group and signaling group
- Administer SIP trunk group members and route patterns
- Administer private numbering
- Administer dial plan and AAR analysis

### 5.1 Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

The license file installed on the system controls the maximum 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:		500	0	
Maximum Concurrently Registered IP Stations:		18000	4	
Maximum Administered Remote Office Trunks:		0	0	
Maximum Concurrently Registered Remote Office Stations:		0	0	
Maximum Concurrently Registered IP eCons:		0	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		0	0	
Maximum Video Capable IP Softphones:		0	0	
Maximum Administered SIP Trunks:		50	20	

## 5.2 Configure System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers. Submit the change.

This feature is needed to be able to transfer an incoming/outgoing call from/to the remote switch back out to the same or another switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented using Class Of Restriction or Class Of Service levels. Refer to the appropriate documentation in **Section 9** for more details.

```
change system-parameters features                               Page 1 of 18
                        FEATURE-RELATED SYSTEM PARAMETERS
                        Self Station Display Enabled? n
                        Trunk-to-Trunk Transfer: all
                        Automatic Callback with Called Party Queuing? n
Automatic Callback - No Answer Timeout Interval (rings): 3
                        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
```

## 5.3 Configure IP Node Names

Use the “change node-names ip” command to add entries for the C-LAN that will be used for connectivity, and Avaya Aura™ Session Manager and Avaya IP Office. The actual node names and IP addresses may vary. Submit these changes.

```
change node-names ip                                           Page 1 of 2
                        IP NODE NAMES
Name                   IP Address
8730-1                 10.80.111.11
8730-2                 10.80.111.12
ASM1                 10.80.100.24
CLAN-1              10.80.111.16
CLAN-2                 10.80.111.17
IPO                 33.1.1.51
VAL                   10.80.111.18
XFire                 10.80.111.13
default               0.0.0.0
gateway1              10.80.111.1
procr                 0.0.0.0
```

## 5.4 Configure IP Interface for C-LAN

Add the C-LAN to the system configuration using the “add ip-interface 1a03” command. The actual slot number may vary. In this case, “1a03” is used as the slot number. Enter the C-LAN node name assigned from **Section 5.3** into the **Node Name** field.

Enter proper values for the **Subnet Mask** and **Gateway Node Name** fields. In this case, “24” and “Gateway001” are used to correspond to the network configuration in these Application Notes. Set the **Enable Interface** and **Allow H.323 Endpoints** fields to “y”. Default values may be used in the remaining fields. Submit these changes.

<b>add ip-interface 1a03</b>		Page 1 of 3
IP INTERFACES		
<b>Type: C-LAN</b>		
Slot: 01A03		Target socket load and Warning level: 400
Code/Suffix: TN799 D		Receive Buffer TCP Window Size: 8320
<b>Enable Interface? y</b>		<b>Allow H.323 Endpoints? y</b>
VLAN: n		Allow H.248 Gateways? y
Network Region: 1		Gatekeeper Priority: 5
IPV4 PARAMETERS		
<b>Node Name: CLAN-1</b>		
<b>Subnet Mask: /24</b>		
<b>Gateway Node Name: gateway1</b>		

## 5.5 Configure IP Codec Sets and Network Regions

Configure the IP codec set to use for calls to the Avaya IP Office. Use the “change ip-codec-set n” command, where “n” is an existing codec set number to be used for interoperability. Enter the desired audio codec type in the **Audio Codec** field. Retain the default values for the remaining fields and submit these changes.

<b>change ip-codec-set 1</b>		Page 1 of 2	
IP Codec Set			
Codec Set: 1			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: G.711MU	n	2	20
2: G.729	n	2	20
3:			
Media Encryption			
1: none			

In the test configuration, network region “1” was used for calls to the Avaya IP Office via Avaya Aura™ Session Manager. Use the “change ip-network-region 1” command to configure this network region. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise network (See **Section 3.4**). This value is used to populate the SIP domain in the From header of SIP INVITE messages for outbound calls. It is also must match the SIP domain in the request URI of incoming INVITEs from other systems. For the **Codec Set** field, enter the corresponding audio codec set configured above in this section. Enable the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio**. These settings will enable direct media between Avaya IP telephones and the far end. Retain the default values for the remaining fields, and submit these changes.

<b>change ip-network-region 1</b>		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: avaya.com	
Name:		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 16585		
DIFFSERV/TOS PARAMETERS	RTCP Reporting Enabled? y	
Call Control PHB Value: 46	RTCP MONITOR SERVER PARAMETERS	
Audio PHB Value: 46	Use Default Server Parameters? y	
Video PHB Value: 26	change	

## 5.6 Configure SIP Signaling Group and Trunk Group

### 5.6.1 SIP Signaling Group

In the test configuration, trunk group “10” and signaling group “10” were used to reach Avaya Aura™ Session Manager. Use the “add signaling-group n” command, where “n” is an available signaling group number. Enter the following values for the specified fields, and retain the default values for all remaining fields. Submit these changes.

- **Group Type:** “sip”
- **Transport Method:** “tcp”
- **Near-end Node Name:** C-LAN node name from **Section 5.3**.
- **Far-end Node Name:** Avaya Aura™ Session Manager node name from **Section 5.3**.
- **Near-end Listen Port:** “5060”
- **Far-end Listen Port:** “5060”
- **Far-end Network Region:** Avaya network region number “1” from **Section 5.5**.
- **DTMF over IP:** “rtp-payload”

**Note:** Leave the Far End Domain as blank.

add signaling-group 10		Page 1 of 1
SIGNALING GROUP		
Group Number: 10	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
IP Video? n		
Near-end Node Name: CLAN-1	Far-end Node Name: ASM1	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 10	

## 5.6.2 SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total trunks configured in **Section 5.1**).

add trunk-group 10		Page 1 of 21
TRUNK GROUP		
Group Number: 10	Group Type: sip	CDR Reports: y
Group Name: SIP trunk to ASM1	COR: 1	TN: 1 TAC: #10
Direction: two-way	Outgoing Display? y	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: tie	Auth Code? n	
Signaling Group: 10		
Number of Members: 10		

Navigate to **Page 3**, and enter “private” for the **Numbering Format** field as shown below. Use default values for all other fields.

add trunk-group 10		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
UII Treatment: service-provider		

Navigate to **Page 4**, and enter “101” for the **Telephone Event Payload Type** field as shown below. Use default values for all other fields. Submit these changes.

add trunk-group 10		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? y		
Prepend '+' to Calling Number? n		
Send Transferring Party Information? n		
Network Call Redirection? n		
Send Diversion Header? n		
Support Request History? y		
Telephone Event Payload Type: 101		

## 5.7 Configure 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 an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name:** A descriptive name.
- **Grp No:** The trunk group number from **Section 5.6.2**.
- **FRL:** Enter a level that allows access to this trunk, with 0 being least restrictive.
- **No. Del Dgts:** Enter “3”. For the sample configuration, the user dials “233-2xx”, however “233” will be deleted and only “2xx” will be sent to Session Manager via the SIP trunk.

change route-pattern 15		Page 1 of 3
Pattern Number: 15 Pattern Name:		
SCCAN? n Secure SIP? n		
Grp FRL NPA Pfx Hop Toll No. Inserted		DCS/ IXC
No Mrk Lmt List Del Digits		QSIG
		Intw
1: 10 0	3	n user
2:		n user
3:		n user
4:		n user
5:		n user
6:		n user
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR		
0 1 2 M 4 W Request		Dgts Format
		Subaddress
1: y y y y y n n	rest	none

## 5.8 Configure Private Numbering

Use the “change private-numbering 3” command, to define the calling party number to be sent to Avaya IP Office. Add an entry for the trunk group defined in **Section 5.6.2** to reach Avaya IP Office endpoints. In the sample configuration, all calls originating from endpoints connected to Communication Manager Access Element dial “233-2xx” where “2xx” is the 3-digit extension on Avaya IP Office. The call will be routed over the SIP trunk defined in **Section 5.6.2**. Submit these changes.

change private-numbering 3					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
6	233	10	233	6	Total Administered: 5
7	666	10	303	10	Maximum Entries: 540
7	6664	2		7	
7	6665	10		7	
7	6664003	10		7	

## 5.9 Administer Dial Plan and AAR Analysis

This section provides sample Automatic Alternate Routing (AAR) used for routing calls with dialed digits 233-2xx to Avaya IP Office. Note that other methods of routing may be used. Use the “change dialplan analysis” command, and add an entry to specify use of AAR for routing of digits 233-2xx. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case “2”.
- **Total Length:** Length of the full dialed number, in this case “6”
- **Call Type:** “aar”

change dialplan analysis									Page 1 of 12
DIAL PLAN ANALYSIS TABLE									
Location: all									Percent Full: 1
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	attd							
1	2	dac							
2	6	aar							
400	7	ext							
500	5	ext							
522	7	ext							
666	7	ext							
71	5	aar							
777	7	ext							
8	1	fac							
9	1	fac							
*	3	fac							
#	3	dac							

Use the “change aar analysis 233” command, and add an entry to specify how to route the calls to Avaya IP Office endpoints. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case “233”.
- **Total Min:** Minimum number of digits.
- **Total Max:** Maximum number of digits.
- **Route Pattern:** The route pattern number from **Section 5.7**.
- **Call Type:** “aar”

change aar analysis 233							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all							Percent Full: 1	
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
	<b>233</b>	<b>6</b>	<b>6</b>	<b>15</b>	<b>aar</b>		<b>n</b>	
	3	7	7	999	aar		n	
	4	7	7	999	aar		n	
	5	7	7	999	aar		n	
	522	7	7	20	aar		n	
	6	7	7	10	aar		n	
	6663	7	7	20	aar		n	
	6665000	7	7	20	aar		n	
	7	7	7	2	lev0		n	
	8	7	7	999	aar		n	
	9	7	7	999	aar		n	

## 5.10 Save Translations

Configuration of Communication Manager Access Element is complete. Use the “save Translations command to save these changes.



## 6 Configure Avaya Aura™ Communication Manager Feature Server

This section covers the administrative steps to route calls between SIP endpoints registered to Session Manager and Avaya IP Office via the SIP trunk. Avaya 9620 IP Telephones configured as SIP users utilizes the Avaya Aura™ Session Manager User Registration feature and require Communication Manager Feature Server. Communication Manager as a feature server only supports IMS-SIP users that are registered to Avaya Aura™ Session Manager. The Communication Manager Feature Server is connected to Session Manager via an IMS-enabled SIP signaling group and associated SIP trunk group. Actual administration for SIP endpoints is not covered in this document.

This section describes configuring Avaya Aura™ Communication Manager Feature Server in the following areas. Some administrative screens are not shown in this section, as they might be similar to **Section 5**.

- Verify Communication Manager license
- Administer system parameters features
- Administer IP node names
- Administer IP interface
- Administer IP codec set and network region
- Administer SIP trunk group and signaling group
- Administer SIP trunk group members and route patterns
- Administer private numbering
- Administer dial plan and AAR analysis

### 6.1 Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections. The license file installed on the system controls the maximum permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

### 6.2 Configure System Parameters Features

Use the “change system-parameters features” command to allow for **trunk-to-trunk transfers** as shown in **Section 5.2**.

## 6.3 Configure IP Node Names

Use the “change node-names ip” command to add entries for Avaya Aura™ Session Manager and Avaya IP Office. The actual node names and IP addresses may vary. Submit these changes.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
ASM1	10.80.100.24	
default	0.0.0.0	
procr	10.80.100.51	
IPO	33.1.1.51	

## 6.4 Configure SIP Signaling Group and Trunk Group

### 6.4.1 SIP Signaling Group

In the test configuration, trunk group “10” and signaling group “10” were used to reach Avaya Aura™ Session Manager. Use the “add signaling-group n” command, where “n” is an available signaling group number. Enter the following values for the specified fields, and retain the default values for all remaining fields. Submit these changes.

- **Group Type:** “sip”
- **Transport Method:** “tcp”
- **IMS Enabled:** “y”
- **Near-end Node Name:** procr
- **Far-end Node Name:** Avaya Aura™ Session Manager node name from **Section 6.3**.
- **Near-end Listen Port:** “5060”
- **Far-end Listen Port:** “5060”
- **DTMF over IP:** “rtp-payload”
- **Enable Layer 3 Tests:** “y”

**Note:** Leave the Far End Domain as blank.

add signaling-group 10		Page 1 of 1
SIGNALING GROUP		
Group Number: 10	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? y		
IP Video? n		
Near-end Node Name: procr	Far-end Node Name: ASM1	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? Y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 10	

## 6.4.2 SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Manager

add trunk-group 10		Page 1 of 21	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: SIP trunk to ASML	COR: 1	TN: 1	TAC: #10
Direction: two-way	Outgoing Display? y		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Signaling Group: 10	
		Number of Members: 10	

Navigate to **Page 3**, and enter “private” for the **Numbering Format** field as shown below. Use default values for all other fields. Submit these changes.

add trunk-group 10		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	

## 6.5 Configure 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 an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name:** A descriptive name.
- **Grp No:** The trunk group number from **Section 6.4.2**.
- **FRL:** Enter a level that allows access to this trunk, with 0 being least restrictive.
- **No. Del Dgts:** Enter “3”. For the sample configuration, the user dials “233-2xx”, however “233” will be deleted and only “2xx” will be sent to Avaya IP Office via the SIP trunk.

change route-pattern 15													Page		1 of		3						
Pattern Number: 15													Pattern Name:										
SCCAN? n													Secure SIP? n										
Grp		FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/		IXC								
No				Mrk	Lmt	List	Del	Digits					QSIG										
							Dgts					Intw											
1:		10		0									3		n		user						
2:																	n		user				
3:																	n		user				
4:																	n		user				
5:																	n		user				
6:																	n		user				
		BCC		VALUE		TSC		CA-TSC		ITC		BCIE		Service/Feature		PARM		No. Numbering		LAR			
		0		1		2		M		4		W				Request		Dgts		Format			
																	Subaddress						
1:		y		y		y		y		y		n		n		rest					none		

## 6.6 Configure Private Numbering

Use the “change private-numbering 3” command, to define the calling party number to be sent to Avaya IP Office. Add an entry for the trunk group defined in **Section 6.4.2** to reach Avaya IP Office endpoints. In the sample configuration, all calls originating from endpoints connected to Communication Manager Access Element dial “233-2xx” where “2xx” is the 3-digit extension on Avaya IP Office. The call will be routed over the SIP trunk defined in **Section 6.4.2**. Submit these changes.

change private-numbering 3						Page 1 of 2		
NUMBERING - PRIVATE FORMAT								
Ext	Ext		Trk	Private	Total			
Len	Code		Grp(s)	Prefix	Len			
7	5		10		7	Total Administered: 3		
7	6		10		7	Maximum Entries: 540		
6	233		10	233	6			

## 6.7 Administer Dial Plan and AAR Analysis

This section provides sample Automatic Alternate Routing (AAR) used for routing calls with dialed digits 233-2xx to Avaya IP Office. Note that other methods of routing may be used. Use the “change dialplan analysis” command, and add an entry to specify use of AAR for routing of digits 233-2xx. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case “2”.
- **Total Length:** Length of the full dialed number, in this case “6”
- **Call Type:** “aar”

change dialplan analysis							Page 1 of 12		
DIAL PLAN ANALYSIS TABLE									
Location: all							Percent Full: 1		
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call	
String	Length	Type	String	Length	Type	String	Length	Type	
0	1	attd							
1	2	dac							
2	6	aar							
#	3	dac							

Use the “change aar analysis 233” command, and add an entry to specify how to route the calls to Avaya IP Office endpoints. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case “233”.
- **Total Min:** Minimum number of digits.
- **Total Max:** Maximum number of digits.
- **Route Pattern:** The route pattern number from **Section 6.5**.
- **Call Type:** “aar”

change aar analysis 233							Page 1 of 2		
AAR DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 2		
	Dialed String	Total		Route	Call	Node	ANI		
		Min	Max	Pattern	Type	Num	Reqd		
233		6	6	15	aar		n		
522		7	7	10	aar		n		
666		7	7	10	aar		n		
7		7	7	10	aar		n		

## 6.8 Save Translations

Configuration of Communication Manager Feature Server is complete. Use the “save Translations command to save these changes.

**Note:** After a change on Communication Manager Feature Server which alters the dial plan, synchronization between Communication Manager Feature Server and Session Manager needs to be completed and SIP phones must be rebooted. To force synchronization, execute “stop -s sm-mgmt” followed by “start -s sm-mgmt” on Session Manager command line interface.

## 7 Verification Steps

This section provides the tests that can be performed on Avaya IP Office, Communication Manager and Session Manager to verify proper configuration of these systems.

### 7.1 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 administered in **Section 5.6** and **Section 6.4**. Verify that all trunks are in the “in-service/idle” state as shown below. Perform this on both Communication Manager Access Element and Feature Server.

```
status trunk 10

                                TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                                Busy

0010/001 T00024    in-service/idle    no
0010/002 T00025    in-service/idle    no
0010/003 T00026    in-service/idle    no
0010/004 T00027    in-service/idle    no
0010/005 T00028    in-service/idle    no
0010/006 T00029    in-service/idle    no
0010/007 T00030    in-service/idle    no
0010/008 T00031    in-service/idle    no
0010/009 T00032    in-service/idle    no
0010/010 T00033    in-service/idle    no
```

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.6** and **Section 6.4**. Verify the signaling group is “in-service” as indicated in the **Group State** field shown below. Perform this on both Communication Manager Access Element and Feature Server.

```
status signaling-group 10

                                STATUS SIGNALING GROUP

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

Make a call between the Avaya 9600 Series IP Telephone and the Avaya IP Office 500 IP Telephone. Verify the status of connected SIP trunks on Communication Manager Access Element SAT terminal by using the “status trunk x/y”, where “x” is the number of the SIP trunk group from **Section 5.6.2** to reach Avaya Aura™ Session Manager, and “y” is the member number of a connected trunk. Verify on Page 1 that the **Service State** is “in-service/active”. On Page 2, verify that the IP addresses of the C-LAN and Avaya Aura™ Session Manager are shown in the **Signaling** section. The Audio Connection will be “ip-direct”. The Near-end IP address will be the IP address of the 9620 IP Telephone and the Far end IP address will be the IP address of the Avaya IP Office.

status trunk 10/7		Page 1 of 3
TRUNK STATUS		
Trunk Group/Member: 0010/007	Service State: in-service/active	
Port: T00030	Maintenance Busy? no	
Signaling Group ID: 10		
IGAR Connection? no		
Connected Ports: S00009		

<b>status trunk 10/7</b>		Page 2 of 3
CALL CONTROL SIGNALING		
Near-end Signaling Loc: 01A0317		
<b>Signaling</b>	<b>IP Address</b>	<b>Port</b>
<b>Near-end:</b>	<b>10.80.111.16</b>	<b>: 5060</b>
<b>Far-end:</b>	<b>10.80.100.24</b>	<b>: 5060</b>
H.245 Near:		
H.245 Far:		
H.245 Signaling Loc:	H.245 Tunneled in Q.931? no	
<b>Audio Connection Type: ip-direct</b>	<b>Authentication Type: None</b>	
Near-end Audio Loc:	Codec Type: G.711MU	
<b>Audio</b>	<b>IP Address</b>	<b>Port</b>
<b>Near-end:</b>	<b>10.80.50.38</b>	<b>: 10106</b>
<b>Far-end:</b>	<b>33.1.1.51</b>	<b>: 49156</b>
Video Near:		
Video Far:		
Video Port:		
Video Near-end Codec:	Video Far-end Codec:	

Make a call between the Avaya 9600 Series IP Telephone registered to Session Manager and the Avaya IP Office 500 IP Telephone. Verify the status of connected SIP trunks on Communication Manager Feature Server SAT terminal by using the “status trunk x”, where “x” is the number of the SIP trunk group from **Section 6.4.2**.

**Note:** Two ports on the trunk will be used for this call.

<b>status trunk 10</b>				
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0010/001	T00006	<b>in-service/active</b>	<b>no</b>	<b>T00008</b>
0010/002	T00007	in-service/idle	no	
0010/003	T00008	<b>in-service/active</b>	<b>no</b>	<b>T00006</b>
0010/004	T00009	in-service/idle	no	
0010/005	T00014	in-service/idle	no	
0010/006	T00015	in-service/idle	no	
0010/007	T00043	in-service/idle	no	
0010/008	T00044	in-service/idle	no	
0010/009	T00045	in-service/idle	no	
0010/010	T00046	in-service/idle	no	

Issue “status trunk x/y”, where “x” is the number of the SIP trunk group to reach Avaya Aura™ Session Manager, and “y” is the member number of a connected trunk. Verify on Page 1 that the **Service State** is “in-service/active”. On Page 2, verify that the IP addresses of the S8300C Media Server and Avaya Aura™ Session Manager are shown in the **Signaling** section. The Audio Connection will be “ip-direct”. The IP address will be the IP address of the 9620 IP Telephone and the IP address of Avaya IP Office in the **Audio** section. In the screen below, 10.80.50.41 is the IP address of the 9620 IP Telephone registered to Session Manager.

status trunk 10/1		Page 1 of 3	
TRUNK STATUS			
Trunk Group/Member: 0010/001		Service State: in-service/active	
Port: T00006		Maintenance Busy? no	
Signaling Group ID: 10			
IGAR Connection? no			
Connected Ports: T00008			
status trunk 10/01		Page 2 of 3	
CALL CONTROL SIGNALING			
Near-end Signaling Loc: 01A0017			
Signaling	IP Address	Port	
Near-end:	10.80.100.51	: 5060	
Far-end:	10.80.100.24	: 5060	
H.245 Near:			
H.245 Far:			
H.245 Signaling Loc:		H.245 Tunneled in Q.931? no	
Audio Connection Type: ip-direct		Authentication Type: None	
Near-end Audio Loc:		Codec Type: G.711MU	
Audio	IP Address	Port	
Near-end:	33.1.1.51	: 49156	
Far-end:	10.80.50.41	: 5004	



Issue “status trunk x/y”, where “x” is the number of the SIP trunk group to reach Avaya Aura™ Session Manager, and “y” is the member number of a connected trunk. Verify on Page 1 that the **Service State** is “in-service/active”. On Page 2, verify that the IP addresses of the S8300C Media Server and Avaya Aura™ Session Manager are shown in the **Signaling** section. The IP address will be the IP address of the 9620 IP Telephone and the IP address of Avaya IP Office in the **Audio** section. In the screen below, 10.80.50.41 is the IP address of the 9620 IP Telephone registered to Session Manager.

<b>status trunk 10/3</b>		<b>Page 1 of 3</b>
TRUNK STATUS		
Trunk Group/Member: 0010/003		Service State: in-service/active
Port: T00008		Maintenance Busy? no
Signaling Group ID: 10		
IGAR Connection? no		
<b>Connected Ports: T00006</b>		
<b>status trunk 10/3</b>		<b>Page 2 of 3</b>
CALL CONTROL SIGNALING		
Near-end Signaling Loc: 01A0017		
Signaling	IP Address	Port
<b>Near-end:</b>	<b>10.80.100.51</b>	<b>: 5060</b>
<b>Far-end:</b>	<b>10.80.100.24</b>	<b>: 5060</b>
H.245 Near:		
H.245 Far:		
H.245 Signaling Loc:		H.245 Tunneled in Q.931? no
<b>Audio Connection Type: ip-direct</b>		Authentication Type: None
Near-end Audio Loc:		Codec Type: G.711MU
Audio	IP Address	Port
<b>Near-end:</b>	<b>10.80.50.41</b>	<b>: 5004</b>
<b>Far-end:</b>	<b>33.1.1.51</b>	<b>: 49156</b>

## 7.2 Verify Avaya Aura™ Session Manager

Expand the Session Manager menu on the left and click SIP Entity Monitoring.



Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 14, 2010 10:55 PM

[Help](#) [Log](#)

Home / Session Manager / System Status / SIP Entity Monitoring

- Asset Management
- Communication System Management
- User Management
- Monitoring
- Network Routing Policy
- Security
- Applications
- Settings
- Session Manager
  - Session Manager Administration
  - Network Configuration
  - Device and Location Configuration
  - Application Configuration
  - System Status
    - System State Administration
    - SIP Entity Monitoring
    - Managed Bandwidth Usage
    - Security Module Status
    - Data Replication Status
    - RegistrationSummary
    - User Registrations
  - System Tools

### SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

#### Entity Link Status for All Session Manager Instances

[Refresh](#)

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
<a href="#">ASM1-DR</a>	1/7	0	0	0

#### All Monitored SIP Entities

[Refresh](#)

7 Items Filter: [Enable](#)

##### SIP Entity Name

[IPO 500](#)

[Nortel-Node Server](#)

[S8300-G450-FS](#)

[S8730-1](#)

[S8730-2](#)

[SIL-DR-MAS1](#)

[VPMS](#)

Select the corresponding SIP Entity and verify that the links are up as shown below for Avaya IP Office.

▶ Asset Management
▶ Communication System Management
▶ User Management
▶ Monitoring
▶ Network Routing Policy
▶ Security
▶ Applications
▶ Settings
▼ Session Manager
Session Manager Administration
▶ Network Configuration
▶ Device and Location Configuration
▶ Application Configuration
▼ System Status
System State Administration
▶ <b>SIP Entity Monitoring</b>
Managed Bandwidth Usage
Security Module Status
Data Replication Status
RegistrationSummary
User Registrations
▶ System Tools

## SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: IPO 500



1 Item		Filter: <a href="#">Enable</a>					
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
<input type="checkbox"/> Show	<a href="#">ASM1-DR</a>	33.1.1.51	5060	TCP	Up	200 Ok	Up

## 7.3 Verify Avaya IP Office

IP Office can be debugged with the System Status Application. Log into the IP Office Manager PC and select Start > Programs > IP Office > System Status to launch the application. Log into the application using the appropriate credentials.

In the left panel, double-click on the Trunks entry and select SIP trunk created in **Section 3.6**. Press the **Trace All** button. The messages on the line are displayed.



## IP Office System Status

Help Snapshot LogOff Exit About

System  
 Alarms (2)  
 Extensions (11)  
 Trunks (6)  
   Lines: 1 - 4  
   ▶ Line: 17  
   Line: 18  
 Active Calls  
 Resources  
 Voicemail  
 IP Networking

Status Utilization Summary Alarms

## SIP Trunk Summary

Peer Domain Name: sip://10.80.100.24  
 Gateway Address: 10.80.100.24  
 Line Number: 17  
 Number of Administered Channels: 10  
 Number of Channels in Use: 1  
 Administered Compression: Auto  
 Silence Suppression: Off  
 SIP Trunk Channel Licences: Unlimited  
 SIP Trunk Channel Licences in Use: 1  
 SIP Device Features:

0%

Channel Number	URI Grou. Ref	Call Ref	Current State	Time in State	Remote RTP Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Pack. Loss Fraction	Transmit Jitter	Transmit Loss Fraction
1	1	48	Connected	00:05:42	10.80.50.38	G711 ...	RTP Relay		Extn 209, Mickey	Outgoing					
2			Idle	2 days 03:...											
3			Idle	2 days 03:...											

## Trace Output - All Channels:

12/11/09 11:07:04 AM-651ms Line = 17, Channel = 1, SIP Message = Invite, Call Ref = 48, Direction = From Switch, From = Mickey@33.1.1.51, To = 6664003@10.80.100.24  
 12/11/09 11:07:04 AM-666ms Line = 17, Channel = 1, SIP Message = Response, Call Ref = 48, Direction = To Switch, From = Mickey@33.1.1.51, To = 6664003@10.80.100.24, Response = 100 Trying  
 12/11/09 11:07:04 AM-668ms Call Ref = 48, Originator State = Dialing, Type = User, Destination State = Dialing, Type = Trunk  
 12/11/09 11:07:04 AM-771ms Line = 17, Channel = 1, SIP Message = Response, Call Ref = 48, Direction = To Switch, From = Mickey@33.1.1.51, To = 6664003@10.80.100.24, Response = 180 Ringing  
 12/11/09 11:07:04 AM-773ms Call Ref = 48, Alerting, Line = 17, Channel = 1  
 12/11/09 11:07:04 AM-774ms Call Ref = 48, Originator State = Ringback, Type = User, Destination State = Outgoing Alerting, Type = Trunk  
 12/11/09 11:07:04 AM-903ms Line = 17, Channel = 1, SIP Message = Response, Call Ref = 48, Direction = To Switch, From = Mickey@33.1.1.51, To = 6664003@10.80.100.24, Response = 200 Ok  
 12/11/09 11:07:07 AM-906ms Line = 17, Channel = 1, SIP Message = Ack, Call Ref = 48, Direction = From Switch, From = Mickey@33.1.1.51, To = 6664003@10.80.100.24  
 12/11/09 11:07:07 AM-911ms Call Ref = 48, Originator State = Connected, Type = User, Destination State = Connected, Type = Trunk  
 12/11/09 11:07:07 AM-911ms Call Ref = 48, Answered, Line = 17, Channel = 1  
 12/11/09 11:07:07 AM-966ms Line = 17, Channel = 1, SIP Message = Invite, Call Ref = 48, Direction = To Switch, From = 6664003@10.80.100.24, To = Mickey@33.1.1.51  
 12/11/09 11:07:07 AM-969ms Line = 17, Channel = 1, SIP Message = Response, Call Ref = 48, Direction = From Switch, From = 6664003@10.80.100.24, To = Mickey@33.1.1.51, Response = 100 Trying  
 12/11/09 11:07:07 AM-972ms Line = 17, Channel = 1, SIP Message = Response, Call Ref = 48, Direction = From Switch, From = 6664003@10.80.100.24, To = Mickey@33.1.1.51, Response = 200 Ok  
 12/11/09 11:07:08 AM-105ms Line = 17, Channel = 1, SIP Message = Ack, Call Ref = 48, Direction = To Switch, From = 6664003@10.80.100.24, To = Mickey@33.1.1.51

## 7.4 Verification Scenarios

Verification scenarios for the configuration described in these Application Notes included the following. Proper display of the calling and called party name and number information was verified for all calls.

- Place a call from an extension on the Avaya IP Office to an extension on Communication Manager Access Element. Answer the call and verify talkpath.
- Repeat previous case in the opposite direction.
- Place a call from an extension on the Avaya IP Office to an extension on Communication Manager Feature Server. Answer the call and verify talkpath.
- Repeat previous case in the opposite direction.
- Verify that calls can be transferred from an extension on Avaya IP Office to an extension on Communication Manager.
- Verify that calls can be transferred from an extension on Communication Manager to an extension on Avaya IP Office.
- Verify that extensions on Avaya IP Office can conference in extensions on Communication Manager.
- Verify that extensions on Communication Manager can conference in extensions on Avaya IP Office.

## 8 Conclusion

These Application Notes describe how to configure a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Aura™ Communication Manager 5.2.1 and Avaya IP Office using SIP trunks. Interoperability testing included verification of successful bi-directional calls among several types of endpoints with various features including transfer, and conference.

## 9 Additional References

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

### Session Manager:

- [1] Avaya Aura™ Session Manager Overview, Doc ID 03-603323, available at <http://support.avaya.com>.
- [2] Installing and Administering Avaya Aura™ Session Manager, Doc ID 03-603324, available at <http://support.avaya.com>.
- [3] Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>.

### Communication Manager:

- [4] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc ID 555-245-206, May 2009, available at <http://support.avaya.com>.
- [5] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, May 2009, available at <http://support.avaya.com>.
- [6] *Administering Avaya Aura™ Communication Manager as a Feature Server*, Doc ID 03-603479, November 2009, available at <http://support.avaya.com>

### IP Office:

- [7] Avaya IP Office Manager, Doc ID 15-601011, available at <http://support.avaya.com>.

### Avaya Application Notes:

- [8] *Configuring 96xx SIP Phones on Avaya Aura™ Session Manager Release 5.2*, available at <http://www.avaya.com>.

---

**©2010 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](mailto:interoplabnotes@list.avaya.com)