



Avaya Solution & Interoperability Test Lab

Configuring SIP Connectivity between the Avaya Meeting Exchange Enterprise S6200 R5.2, Avaya Aura™ Session Manager R5.2 and Avaya IP Office 6.0 – Issue 1.0

Abstract

These Application Notes present the procedures for configuring SIP connectivity between the Avaya Meeting Exchange Enterprise S6200, Avaya Aura™ Session Manager and Avaya IP Office. SIP connectivity is enabled via directly connected SIP trunking from Avaya IP Office and Avaya Meeting Exchange S6200 to Avaya Aura™ Session Manager.

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

1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Meeting Exchange Enterprise S6200 and Avaya IP Office using SIP trunks. SIP trunks connect Avaya IP Office and Avaya Meeting Exchange 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 supports flexible inter-system call routing based on the dialed number, the calling number and the system location. Avaya Aura™ Session Manager can also provide protocol adaptation to allow multi-vendor systems to interoperate. Avaya Aura™ Session Manager is managed by Avaya Aura™ System Manager via the management network interface. The configuration in **Figure 1** was used to compliance test IP Office interoperability with the Distributed Meeting Exchange Enterprise S6200 system.

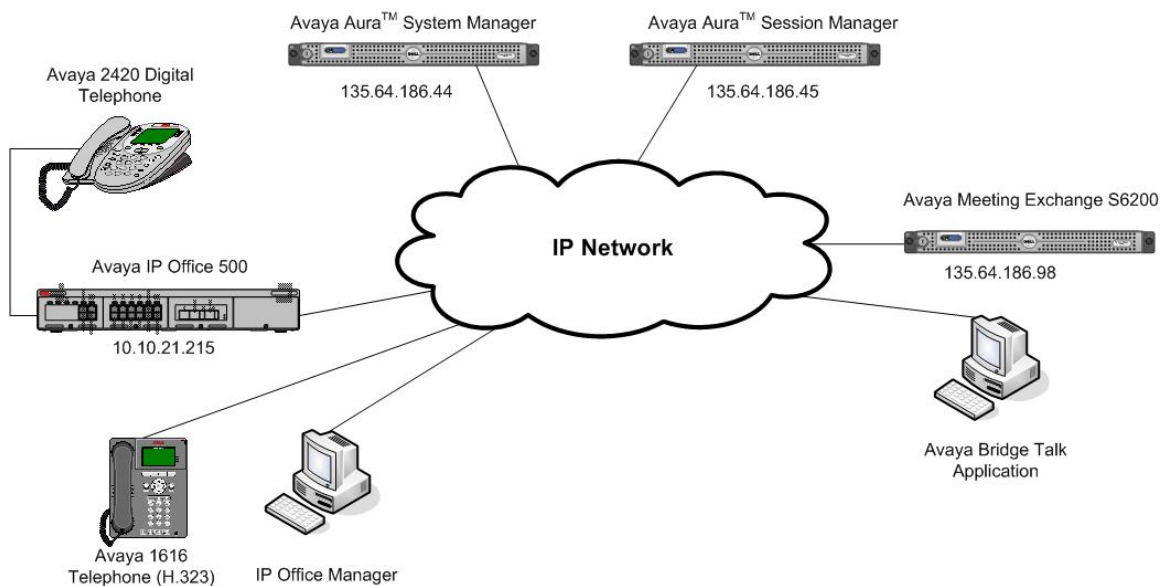


Figure 1 - Avaya Meeting Exchange Enterprise Interop Network Topology

2. Equipment and Software Validated

The following equipment and software versions were used for the sample configuration provided in these Application Notes.

Equipment	Software
Avaya S6200 server	Avaya Meeting Exchange Enterprise R5.2 (Build 5.2.1.0.4)
Windows Computer	Avaya Bridge Talk (BT) 5.2.0.0.7
IP Office	6.0.8
Avaya Digital Phone (2420)	N/A
Avaya IP Phone (1616)	1.2

Table 1: Equipment and Software Versions

3. Configure Avaya Meeting Exchange Enterprise S6200

This section describes the steps for configuring the Meeting Exchange to interoperate with IP Office via SIP trunking. It is assumed that the Meeting Exchange is installed and licensed as described in the product documentation (see reference [1]). The following steps describe the administrative procedures for configuring the Meeting Exchange:

- Configure SIP Connectivity
- Configure Dialout
- Map DNIS Entries
- Configure Audio Preferences
- Restarting the Meeting Exchange server
- Configure Bridge Talk

The following instructions require logging in to the Meeting Exchange console using an ssh connection to access the Command Line Interface (CLI) with the appropriate credentials.

3.1. Configuring SIP Connectivity

Log in to the Meeting Exchange server console using an ssh Client to access the Command Line Interface (CLI) with the appropriate credentials. Configure settings that enable SIP connectivity between the Meeting Exchange server and other devices by editing the **system.cfg** file as follows:

- Edit **/usr/ipcb/config/system.cfg**
 - Add Meeting Exchange S6200 server IP address
 - **IPAddress=(135.64.186.98)**
 - Depending on the SIP signalling protocol, TCP or UDP, add one of the following lines to populate the From Header Field in SIP INVITE messages:
 - **MyListener=<sip:6000@135.64.186.98:5060;transport=tcp>**
 - **MyListener=<sip:6000@135.64.186.98:5060;transport=udp>**
- Note:** The user field 6000, defined for this SIP URI must conform to RFC 3261. For consistency, it is selected to match the user field provisioned for the **respContact** entry (see below).
- Depending on the SIP signalling protocol, TCP or UDP , add one of the following lines to provide SIP Device Contact address to use for acknowledging SIP messages from the Meeting Exchange server:
 - **respContact=<sip:6000@135.64.186.98:5060;transport=tcp>**
 - **respContact=<sip:6000@135.64.186.98:5060;transport=udp>**
 - Add the following lines to set the Min-SE timer to **900** seconds in SIP INVITE messages from the Meeting Exchange server:
 - **sessionRefreshTimerValue= 900**
 - **minSETimerValue= 900**

3.2. Configure Dialout

To enable Dial-Out from the Meeting Exchange to IP Office, edit the **telnumToUri.tab** file as follows:

- Edit **/usr/ipcb/config/telnumToUri.tab** file with a text editor
- Add the following line to the file to route outbound calls from the Meeting Exchange to IP Office
* **sip:\$0@135.64.186.46:5060;transport=tcp**

3.3. Map DNIS Entries

The DNIS entry is the number dialled by IP Office subscribers to access a conference on Meeting Exchange. The DNIS entry needs to be mapped on Meeting Exchange to enable access to a conference. To map DNIS entries, run the **cbutil** utility on Meeting Exchange. Log in to the Meeting Exchange with a ssh connection with the appropriate credentials. Enable Dial-In access (via passcode) to conferences provisioned on the Meeting Exchange as follows:

- Add a DNIS entry for a **scan call function** corresponding to DID **38888** by entering the following command at the command prompt:
cbutil add <dnis> <rg> <msg> <ps> <ucps> <func> [-o <of> -l <ln> -c <cn> -crs <n> -cre <n> -cc <code>]
where the variables for add command is defined as follows:
 - o **<dnis>** DNIS
 - o **<rg>** Reservation Group
 - o **<msg>** Annunciator message number
 - o **<ps>** Prompt Set number (0-20)
 - o **<ucps>** Use Conference Prompt Set (y/n)
 - o **<func>** One of: DIRECT/SCAN/ENTER/HANGUP/AUTOVL/FLEX
 - o **-o <of>** Optional On-failure function – one of: ENTER/HANGUP
 - o **-l <"ln">** Optional line name to associate with caller
 - o **-c <"cn">** Optional company name to associate with caller
 - o **-crs <n>** Optional conference room start number
 - o **-cre <n>** Optional conference room end number

In this sample configuration, the DNIS entry for a **scan call function** was added corresponding to DNIS 38888 by entering the following command at the command prompt:

```
[MXSIL]# cbutil add 38888 0 247 1 N SCAN
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.
```

At the command prompt, enter **cbutil list** to verify the DNIS entries provisioned.

```
[MXSIL]# cbutil list
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.
```

DNIS	Grp	Msg	PS	CP	Function	On Failure	Line Name	Company Name	Room	Start
38888	0	247	1	N	SCAN	DEFAULT				

3.4. Configure Audio Preferences file

The **audioPreferences.cfg** file located at **/usr/ipcb/config/** specifies the order in which codecs are offered in the Session Description Protocol. Set the **telephone-event** value to **payloadType** of **120**.

```
# audioPreferences.cfg
# This table is an ordered list of MIME subtypes specifying the codecs
# supported
# by this media server. The list is specified in the order in which an SDP
# offer
# will list the various MIME subtypes on the m=audio line.
# For static payload type numbers (i.e. numbers between 0 - 96) please use the
# iana registered numbering scheme.
# See: http://www.iana.org/assignments/rtp-parameters
```

mimeSubtype	payloadType
PCMU	0
PCMA	8
G722	9
G729	18
iLBC30	97
iLBC20	98
wbPCMU	102
wbPCMA	103
telephone-event	120
iSAC	104
G726_16	105
G726_24	106
G726_32	107
G726_40	108

3.5. Restarting the Meeting Exchange Server

After the configuration changes are made, restart the services issuing the command **service mxbridge restart**

```
[mx6200-a ~]# service mx-bridge restart
/etc/init.d/mx-bridge: Restarting bridge
/etc/init.d/mx-bridge: Server type is DCB
/etc/init.d/mx-bridge: Stopping DCB conferencing server bridge via uninitdcb.sh
Stopping notificationCtrlServer service:
killproc notificationCtrlServer
[ OK ]
Sending CMD_SHUTDOWN level 3 message to the INIT_KEY queue.
Waiting for 6 processes to stop
Waiting for 2 processes to stop
Waiting for 1 processes to stop
Waiting for 1 processes to stop
destroy.
/etc/init.d/mx-bridge: mx-bridge startup
/etc/init.d/mx-bridge: Server type is DCB
.....
.....
.....
.....
Add Process Key 145 IP address 10.10.6.20
Add Process Key 146 IP address 10.10.6.20
key ID 101
key ID 102
key ID 110
===== INITDCB
=====
FirstMusic = 3199.
FirstLink = 3199.
FirstRP = 3198.
FirstOper = 3195.
numUserLCNs = 3195.
```

3.6. Bridge Talk

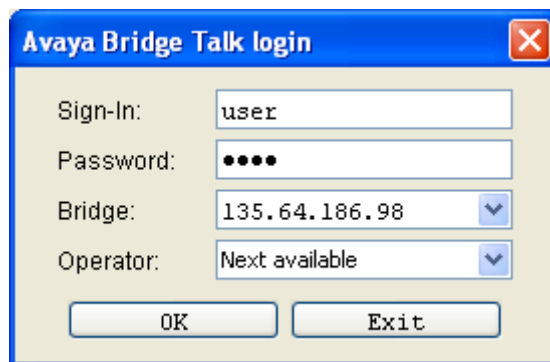
The following steps utilize the Avaya Bridge Talk application to provision a sample conference on the Meeting Exchange. This sample conference enables both Dial-In and Dial-Out access to audio conferencing for endpoints on the Public Switched Telephone Network.

Note: If any of the features displayed in the Avaya Bridge Talk screen captures are not present, contact an authorized Avaya Sales representative to make the appropriate changes.

3.6.1. Initializing Bridge Talk

Invoke the Avaya Bridge Talk application as follows:

- Double-click on the desktop icon from a Personal Computer loaded with the Avaya Bridge Talk application and with network connectivity to the Meeting Exchange (Not shown).
- Enter the appropriate credentials in the **Sign-In** and **Password** fields.
- Enter the IP address of the Meeting Exchange server (**135.64.186.98** for this sample configuration) in the **Bridge** field as shown below.

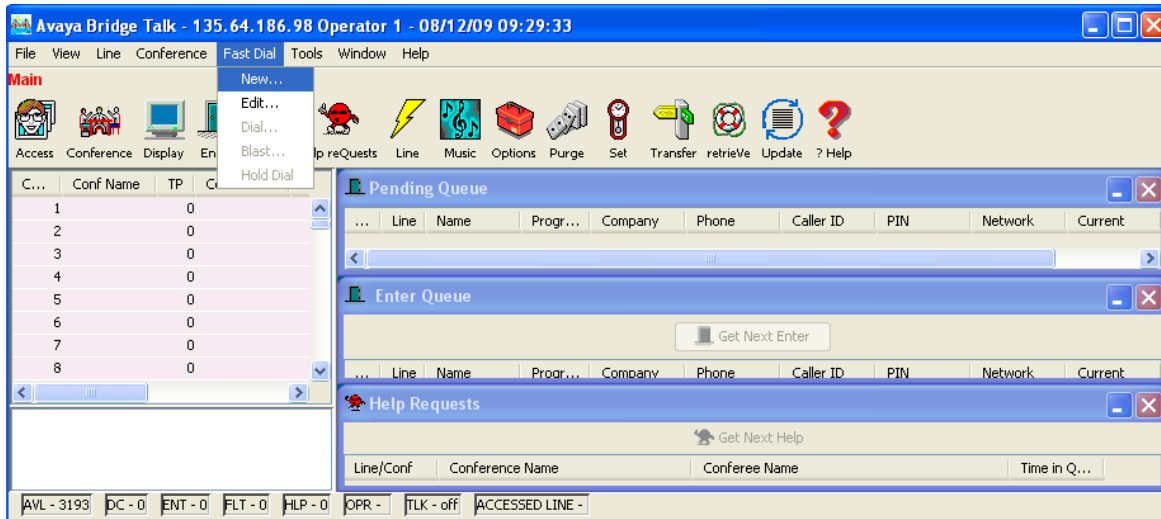


The image shows a Windows-style dialog box titled "Avaya Bridge Talk login". It contains four input fields: "Sign-In:" with the text "user", "Password:" with four dots, "Bridge:" with the IP address "135.64.186.98" and a dropdown arrow, and "Operator:" with the text "Next available" and a dropdown arrow. At the bottom are two buttons: "OK" and "Exit".

3.6.2. Creating a Dial Out list

Provision a dial list that is utilized for Dial-Out (e.g., Blast dial and Fast dial) from the Meeting Exchange.

- From the Avaya Bridge Talk Menu Bar, click **Fast Dial** → **New**.

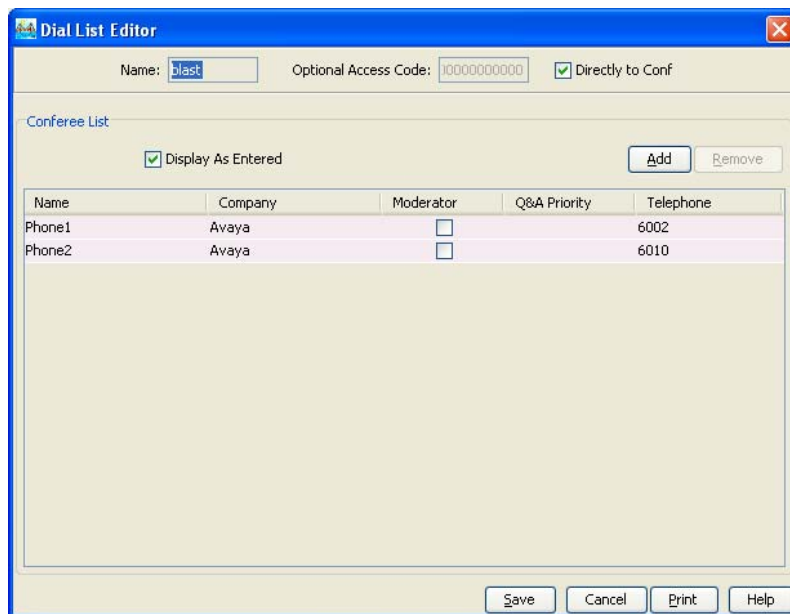


3.6.3. Creating a Dial List

From the **Dial List Editor** window that is displayed below:

- Enter a descriptive label in the **Name** field.
- Enable conference participants on the dial list to enter the conference without a passcode by selecting the **Directly to Conf** box as displayed.
- Add entries to the dial list by clicking on the **Add** button and enter **Name**, **Company** and **Telephone** number for dial out for each participant. [Optional] Moderator privileges may be granted to a conference participant by checking the **Moderator** box.

When finished, click on the **Save** button on the bottom of the screen.

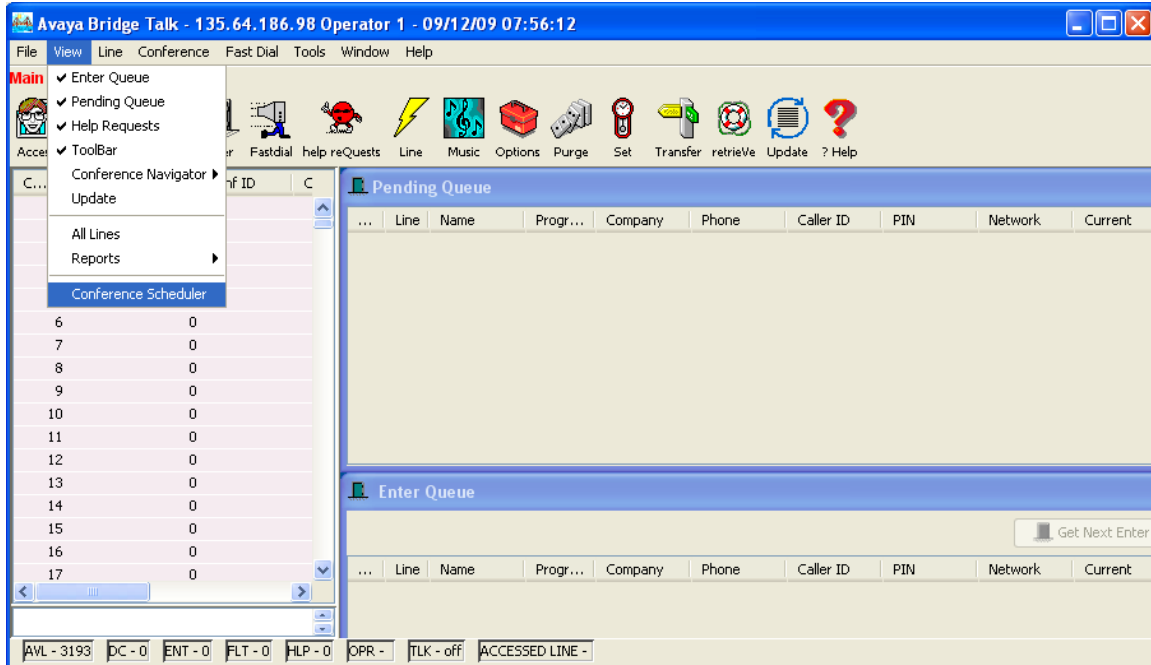


The screenshot shows the 'Dial List Editor' window. At the top, there is a 'Name' field with the value 'blast', an 'Optional Access Code' field with the value '10000000000', and a checked 'Directly to Conf' checkbox. Below this is a 'Conferee List' section with a checked 'Display As Entered' checkbox and 'Add' and 'Remove' buttons. A table lists two participants: 'Phone1' and 'Phone2', both from 'Avaya'. 'Phone1' has a 'Telephone' number of '6002' and an unchecked 'Moderator' checkbox. 'Phone2' has a 'Telephone' number of '6010' and an unchecked 'Moderator' checkbox. At the bottom of the window are 'Save', 'Cancel', 'Print', and 'Help' buttons.

Name	Company	Moderator	Q&A Priority	Telephone
Phone1	Avaya	<input type="checkbox"/>		6002
Phone2	Avaya	<input type="checkbox"/>		6010

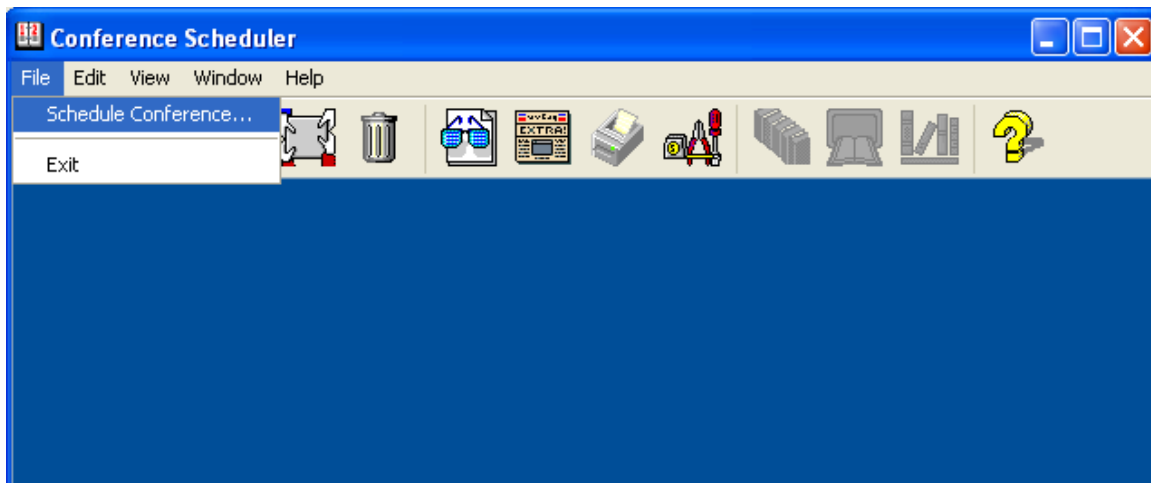
3.6.4. Conference Scheduler

From the **Avaya Bridge Talk** menu bar, click **View → Conference Scheduler** to provision a conference.



3.6.5. Scheduling a Conference

From the **Conference Scheduler** window, click **File → Schedule Conference**.



3.6.6. Provision a Conference

From the **Schedule Conference** window that is displayed, provision a conference as follows:

- Enter a unique **Conferee Code** to allow participants access to this conference.
- Enter a unique **Moderator Code** to allow participants access to this conference with moderator privileges.
- Enter a descriptive label in the **Conference Name** field.
- Administer settings to enable an **Auto Blast** dial by setting Auto/Manual as desired.

Select a dial list by clicking on the **Dial List** button, select a dial list from the **Create, Select or Edit Dial List** window that is displayed (not shown), and click on the **Select** button (to verify Dial out and Blast Dial out).

- When finished, click on the **OK** button on the bottom of the screen.

Schedule Conference [Administrator Access]

Conference Information

Status: Mode: Conference Type:
Confirmation No.: Conference ID: Weekend:
Name: Billing Code Prompt:
Telephone: Accounting Code: Start Date (dd/mm/yyyy):
Sign-in Name: Security Passcode: End Date (dd/mm/yyyy):
Res Group: Change Conf Opt:
Conferee Code: Op Help Available: Name Record/Play:
Moderator Code: Block Dialout: NRP Annunciator:
Conference Name: Auto Blast: PIN Mode:
 Blast Annunciator: PIN List:

Conference Features

Start Time: End Time: Code Duration:
Entry Tone: Exit Tone: Maximum Lines:
Hang up: Music: Security:
Auto Extend Duration: Auto Extend Ports:
Prompt Set: Conference Viewer:

4. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager. For further information on Session Manager, please consult with references [3], [4] and [5]. The procedures include the following areas:

- Log in to Avaya Aura™ Session Manager
- Administer SIP domain
- Administer SIP Entities
- Administer Entity Links
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Aura™ Session Manager

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 and accept the subsequent Copyright Legal Notice.

AVAYA Avaya Aura System Manager 5.2 Help

Home / Log On

Log On

You have successfully logged out.

Username :

Password :

Log On Cancel

Local intranet

By selecting **Network Routing Policy** from the left panel menu, a short procedure for configuring Network Routing Policy is shown on the right panel.

AVAYA

Avaya Aura System Manager 5.2

Welcome, **admin** Last Logged on at Nov. 04, 2009 3:42 PM
[Help](#) | [Log off](#)

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

Help for Export All Data

Help for Committing configuration changes

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"

(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Pattern"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Pattern"

Step 9: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".
IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of NRP application "Dial pattern". That's why this overall NRP workflow can be interpreted as

"Dial Pattern driven approach to define routing policies"

That means (with regard to steps listed above):

Step 7: "Routing Policies" are defined

Step 8: "Dial Pattern" are defined and assigned to "Routing Policies" and "Locations" (one step)

Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

TP; Reviewed:
SPOC 06/18/2010

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

14 of 40
MX52-ASM52-IPO6

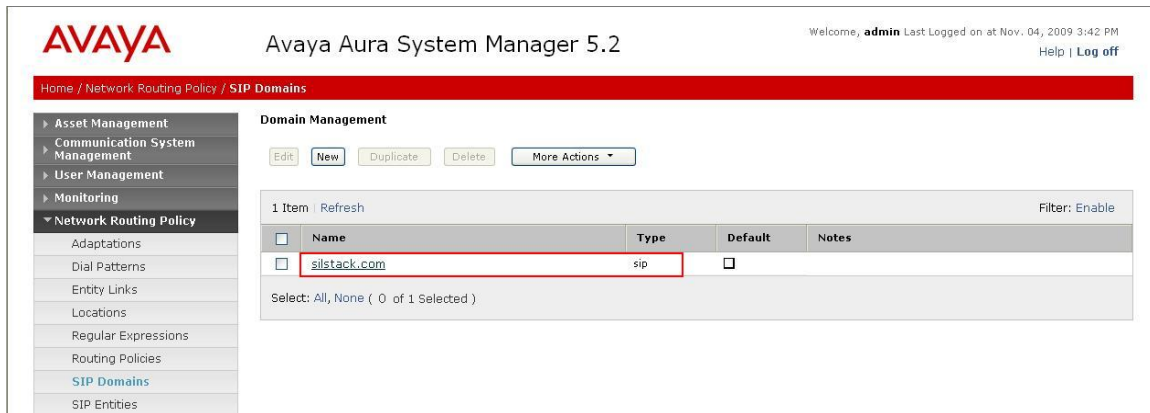
..

4.2. Administer SIP Domain

Add the SIP domain, for which the communications infrastructure will be authoritative, by selecting **SIP 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., **silstack.com**)
- **Notes** Description for the domain (optional)

Click **Commit** to save changes. Verify the domain is created as in screenshot below.



The screenshot displays the Avaya Aura System Manager 5.2 interface. The top header shows the Avaya logo and the title 'Avaya Aura System Manager 5.2'. A user login bar indicates 'Welcome, admin' and 'Last Logged on at Nov. 04, 2009 3:42 PM'. The breadcrumb trail reads 'Home / Network Routing Policy / SIP Domains'. The left sidebar contains a navigation menu with categories: Asset Management, Communication System Management, User Management, Monitoring, and Network Routing Policy. Under Network Routing Policy, several options are listed, with 'SIP Domains' highlighted in blue. The main content area is titled 'Domain Management' and includes buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below these buttons is a table with one item. The table has columns for 'Name', 'Type', 'Default', and 'Notes'. The single entry has the name 'silstack.com' (highlighted with a red box), type 'sip', and a default checkbox that is unchecked. Below the table, it says 'Select: All, None (0 of 1 Selected)'.

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

Note: Since the sample network does not deal with any foreign domains, no additional SIP Domains entry is needed.

4.3. Administer SIP Entities

A SIP Entity must be added for Session Manager 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
- **Type** **Session Manager** for Session Manager or **SIP Trunk** for IP Office and MX
- **Time Zone** Time zone for this location

The screenshot displays the Avaya Aura System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 5.2', and a user status message: 'Welcome, admin Last Logged on at Nov. 11, 2009 8:32 AM' with links for 'Help' and 'Log off'. Below this is a red breadcrumb trail: 'Home / Network Routing Policy / SIP Entities / SIP Entity Details'. On the left, a vertical menu lists various system management categories, with 'SIP Entities' highlighted under the 'Network Routing Policy' section. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows: 'Name' (text box with 'SessionManager'), 'FQDN or IP Address' (text box with '135.64.186.46'), 'Type' (dropdown menu with 'Session Manager' selected), 'Notes' (empty text box), 'Location' (dropdown menu), 'Outbound Proxy' (dropdown menu), 'Time Zone' (dropdown menu with 'Europe/Dublin' selected), 'Credential name' (empty text box), and 'SIP Link Monitoring' (dropdown menu with 'Use Session Manager Configuration' selected). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

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.

The screenshot shows a web interface for managing SIP ports. On the left, there is a 'Shortcuts' sidebar with links to 'Change Password', 'Help for SIP Entity Details fields', and 'Help for Committing configuration changes'. The main area is titled 'Port' and has 'Add' and 'Remove' buttons. Below this is a table with 5 items, showing a list of ports. The first row is highlighted with a red box. The table has columns for 'Port', 'Protocol', 'Default Domain', and 'Notes'. Below the table, there is a 'Select: All, None (0 of 5 Selected)' option and a '* Input Required' label. At the bottom right, there are 'Commit' and 'Cancel' buttons.

Port	Protocol	Default Domain	Notes
5060	TCP	silstack.com	
5061	TLS	silstack.com	
5062	TLS	silstack.com	
5063	TCP	silstack.com	
5064	TLS	silstack.com	

The following screen shows the SIP Entity for IP Office.

The screenshot shows the 'SIP Entity Details' screen for 'IPOffice'. The left sidebar contains a navigation menu with categories like 'Asset Management', 'Communication System Management', 'User Management', 'Monitoring', 'Network Routing Policy', 'Security', 'Applications', 'Settings', and 'Session Manager'. The 'SIP Entities' option is highlighted. The main area is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. Below this is a 'General' section with fields for 'Name' (IPOffice), 'FQDN or IP Address' (10.10.21.215), 'Type' (SIP Trunk), 'Notes', 'Adaptation', 'Location', and 'Time Zone' (Europe/Dublin). There is an 'Override Port & Transport with DNS SRV' checkbox. Below this is a 'SIP Link Monitoring' section with a 'SIP Link Monitoring' dropdown set to 'Use Session Manager Configuration'. At the bottom, there is a '* SIP Timer B/F (in seconds): 4' field and a 'Credential name' field. A 'Call Detail Recording' dropdown is set to 'egress'.

The following screen shows the SIP Entity for MX.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at May 13, 2010 11:09 AM
[Help](#) | [Log off](#)

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

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

4.4. 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 4.3**
- **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.

Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at May 13, 2010 1 Help |

Home / Network Routing Policy / Entity Links

Entity Links

Edit New Duplicate Delete More Actions Commit

28 Items Refresh Filter:

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	ModularMessaging_MD	SessionManager	TCP	5060	ModularMessaging_MD	5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MX-S6200	SessionManager	TCP	5060	MX-S6200	5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MXExpress	SessionManager	TCP	5060	MXExpress	5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MX-Interop-Active	SessionManager	TCP	5060	MX-Interop-Active	5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MX-Interop-Standby	SessionManager	TCP	5060	MX-Interop-Standby	5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	New Feature CM	SessionManager	TLS	5061	NewStackFeature	5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	PSTN_CM link	SessionManager	TCP	5070	PSTN_CM	5070	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SessionManager_CS1000_5060_TCP	SessionManager	TCP	5060	CS1000	5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SessionManager_MX-S6200_5061_TLS	SessionManager	TLS	5061	MX-S6200	5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SessionManager_SiemensHiPath_5060_UDP	SessionManager	UDP	5060	SiemensHiPath	5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SessionManager_VoiceMail_5061_TLS	SessionManager	TLS	5061	VoiceMail	5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM to IPOffice	SessionManager	TCP	5060	IPOffice	5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	To OCS Mediation	SessionManager	TCP	5060	Stack OCS Mediation Server	5060	<input checked="" type="checkbox"/>

4.5. Administer Time Ranges

Before adding routing policies (see next step), time ranges must be defined during which the policies will be active. In the sample network, one policy was defined that would allow routing to occur at anytime. 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)

AVAYA Avaya Aura System Manager 5.2

Welcome, **admin** Last Logged on at Nov. 04, 2009 3:42 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Time Ranges

Time Ranges

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

2 Items | [Refresh](#) Filter: Enable

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	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
<input type="checkbox"/>	always	<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 (0 of 2 Selected)

4.6. Administer Routing Policies

Create routing policies to direct how calls will be routed to a system. Two routing policies must be added, one for IP Office and one for MX. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- **Name** 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 previous step.

The following screen shows the **Routing Policy Details** for MX.

The screenshot displays the Avaya Aura System Manager 5.2 interface. The left sidebar shows the navigation menu with 'Routing Policies' highlighted. The main content area is titled 'Routing Policy Details' and contains the following sections:

- General**: Includes a text field for '* Name:' with the value 'MX-S6200', a 'Disabled:' checkbox, and a 'Notes:' text area.
- SIP Entity as Destination**: Includes a 'Select' button.
- Time of Day**: Includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons.

Below these sections is a table with 1 item. The table has columns for Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The data row shows a ranking of 0, a name of 24/7, and is checked for all days of the week, with a start time of 00:00 and an end time of 23:59.

Ranking	Name	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	Time Range 24/7

The following is screen shows the **Routing Policy Details** for IP Office

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at May 14, 2010 12:36 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
IPOffice	10.10.21.215	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

	Ranking	Name	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

4.7. Administer Dial Patterns

A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample network, 4-digit extensions beginning with **90** reside on IP Office. The 5-digit extension 38888 is for calls to the MX. To configure IP Office 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**

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at May 14, 2010 12:36 PM
[Help](#) | [Log off](#)

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

Dial Pattern Details Commit Cancel

General

* Pattern:
 * Min:
 * Max:
 Emergency Call: ☐
 SIP Domain:
 Notes:

Navigate to **Originating Locations and Routing Policy List** and select **Add** (not shown). Under **Originating Location**, check the box next to **ALL** and under **Routing Policies**, check the box next to **IPOffice**. Click **Select** button to confirm the chosen options and then be returned to the Dial Pattern screen (shown previously), select **Commit** button to save.

Originating Location and Routing Policy List Select Cancel

Originating Location

4 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	-ALL-	Any Locations
<input type="checkbox"/>	Avaya	
<input type="checkbox"/>	Cisco	
<input type="checkbox"/>	Stack Enterprise	Main Office for Stack Testing

Select : All, None (0 of 4 Selected)

Routing Policies

8 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	AvayaCM	<input type="checkbox"/>	AvayaCM	
<input type="checkbox"/>	AvayaCMtom	<input type="checkbox"/>	AvayaCMtom	
<input type="checkbox"/>	BranchCM	<input type="checkbox"/>	Branch CM	Branch CM
<input checked="" type="checkbox"/>	IPOffice	<input type="checkbox"/>	IPOffice	

For MX Dial Pattern configuration, 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**

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at May 14, 2010 12:36 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

Dial Pattern Details

Commit Cancel

General

* Pattern: 3888x

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Navigate to **Originating Locations and Routing Policies** and select **Add** (not shown). Under **Originating Location** select all locations by checking the box next to **ALL** and under **Routing Policies** select a Routing Policy by checking the box next to **MX-S6200**. Click **Select** button to confirm the chosen options. You will then be returned to the Dial Pattern screen (shown previously select **Commit** button to save).

- 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

Originating Location and Routing Policy List

Select Cancel

Originating Location

4 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	-ALL-	Any Locations
<input type="checkbox"/>	Avaya	
<input type="checkbox"/>	Cisco	
<input type="checkbox"/>	Stack Enterprise	Main Office for Stack Testing

Select : All, None (0 of 4 Selected)

Routing Policies

8 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	AvayaCM	<input type="checkbox"/>	AvayaCM	
<input type="checkbox"/>	AvayaCMtom	<input type="checkbox"/>	AvayaCMtom	
<input type="checkbox"/>	BranchCM	<input type="checkbox"/>	Branch CM	Branch CM
<input type="checkbox"/>	MX-S6200	<input type="checkbox"/>	MX-S6200	

4.8. Administer Avaya Aura™ Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the Session Manager menu on the left and select **Session Manager Administration**. Then click **Add** and 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 displays the 'Add Session Manager' configuration page. The left sidebar shows the navigation menu with 'Session Manager Administration' selected. The main content area is titled 'Add Session Manager' and includes a 'Commit' button. The form is divided into two sections: 'General' and 'Security Module'. The 'General' section contains fields for 'SIP Entity Name' (Session Manager), 'Description' (Session Manager), 'Management Access Point Host Name/IP' (135.64.186.45), and 'Direct Routing to Endpoints' (Enable). The 'Security Module' section contains fields for 'SIP Entity IP Address' (135.64.186.46), 'Network Mask' (255.255.255.224), 'Default Gateway' (135.64.186.33), 'Call Control PHB' (46), 'QOS Priority' (5), 'Speed & Duplex' (Auto), and 'VLAN ID'.

Home / Session Manager / Session Manager Administration / New Session Manager

Add Session Manager [Commit] [Cancel]

General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

General ▾

*SIP Entity Name [Session Manager]
Description [Session Manager]
*Management Access Point Host Name/IP [135.64.186.45]
*Direct Routing to Endpoints [Enable]

Security Module ▾

SIP Entity IP Address [135.64.186.46]
*Network Mask [255.255.255.224]
*Default Gateway [135.64.186.33]
*Call Control PHB [46]
*QOS Priority [5]
*Speed & Duplex [Auto]
VLAN ID []

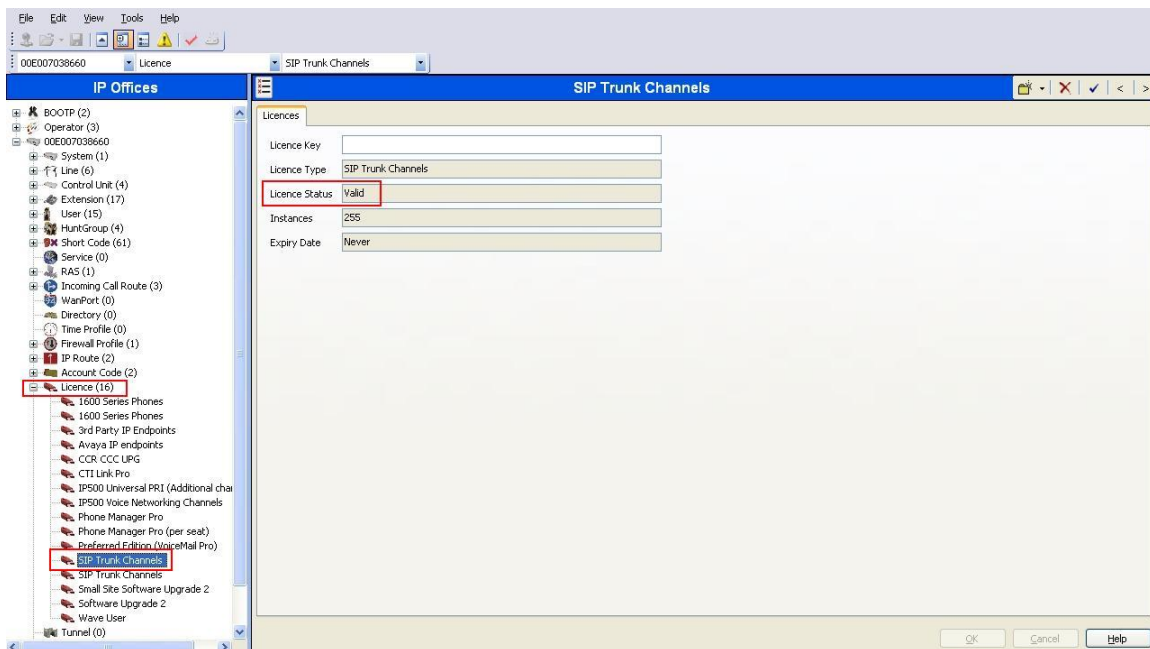
5. Configure Avaya IP Office

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

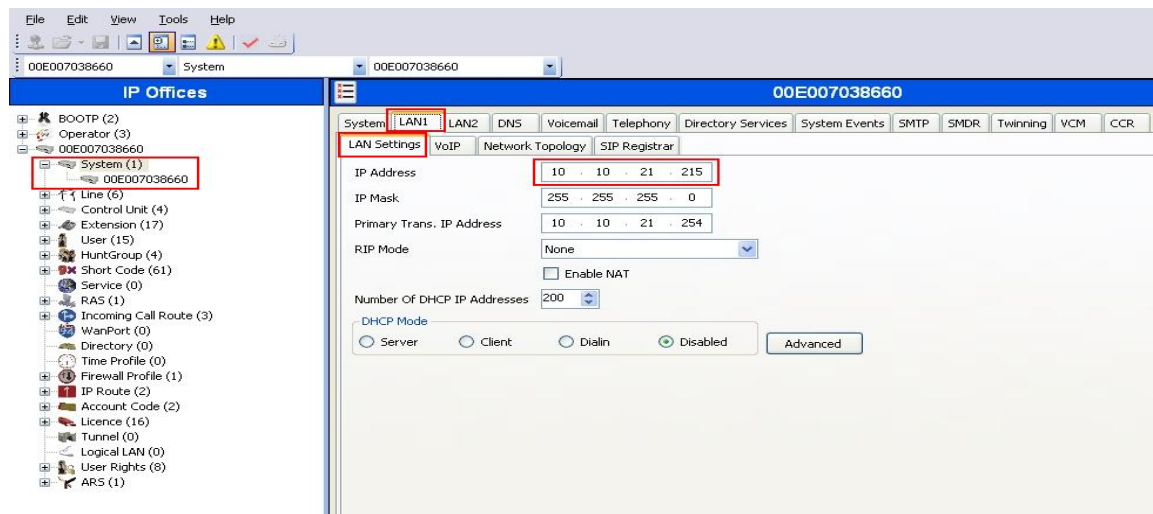
5.1. Verify IP Office License

From a PC running the Avaya IP Office Manager application, select **Start → Programs → IOffice → 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** and if not contact your Avaya representative.



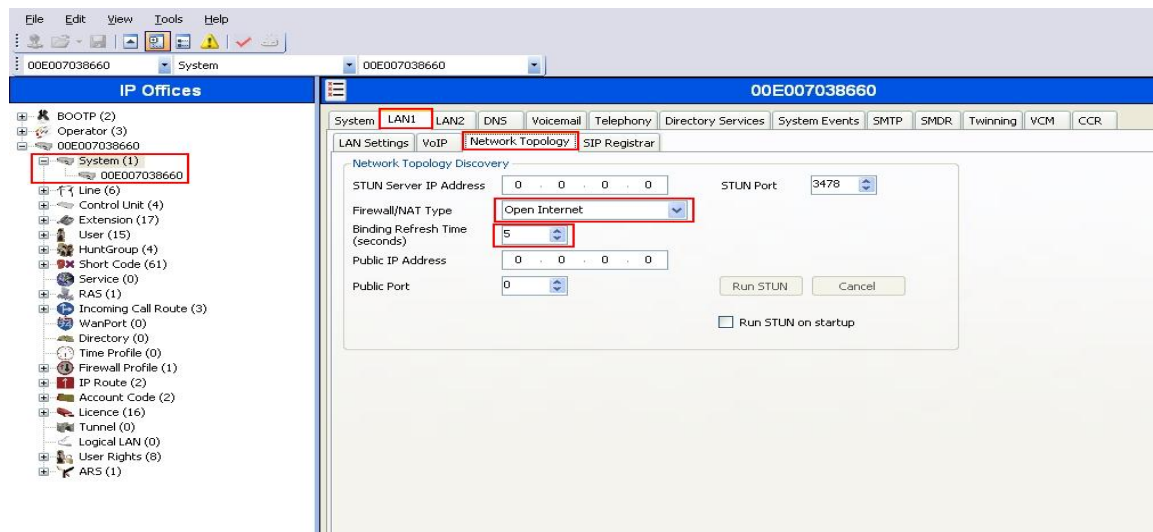
5.2. Obtain LAN IP Address

From the configuration tree in the left pane, select **System** to display the system screen in the right pane. Select the **LAN1** tab, followed by the **LAN Settings** sub-tab. The **IP address** will be the one defined for the IP Office SIP Entity in **Section 4.3** Note that IP Office can support SIP trunks on the LAN1 and/or LAN2 interfaces, and the sample configuration used the LAN1 interface.



5.3. Configure Network Topology

From the configuration tree in the left pane, select **System** to display the system screen in the right pane. Select the **LAN1** tab, followed by the **Network Topology** sub-tab. Configure **Firewall/NAT Type** to **Open Internet** and **Binding Refresh Time** to **5**. Click **OK** (not shown).

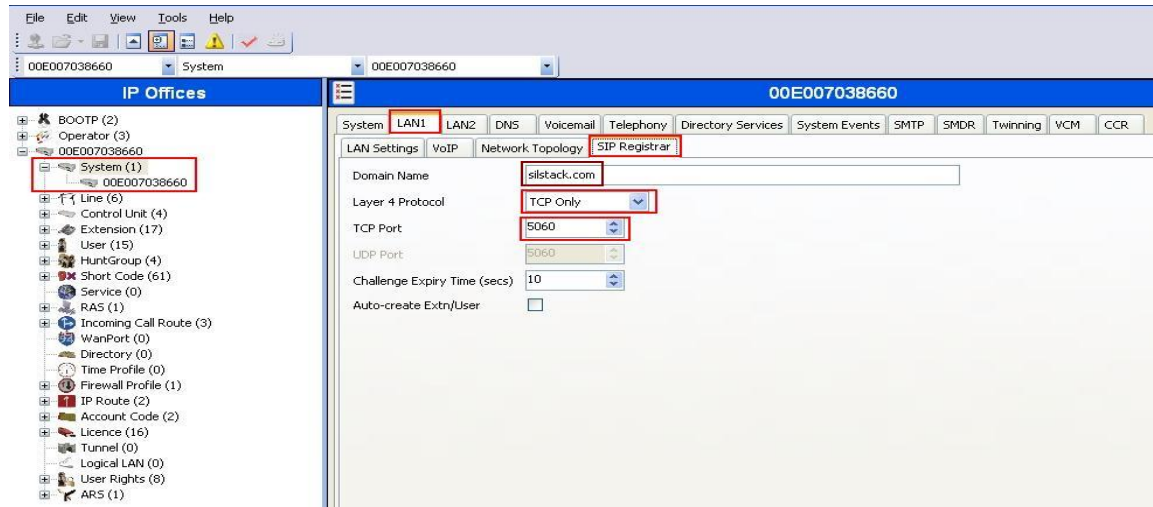


5.4. Administer SIP Registrar

Select **SIP Registrar** sub-tab in the right pane and enter following values:

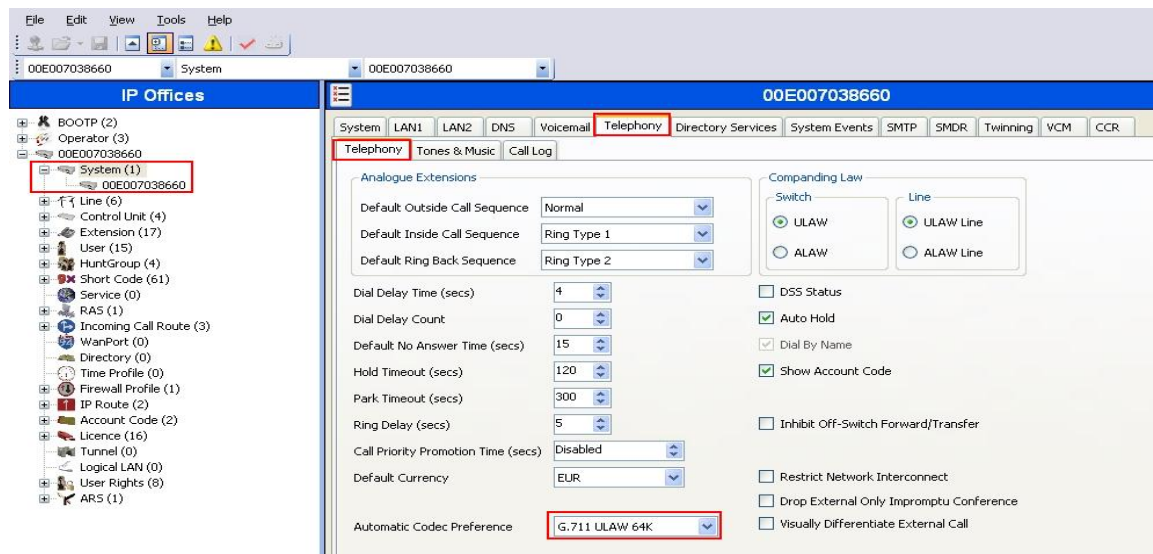
- **Domain Name** Enter a valid Domain Name.
- **Layer 4 Protocol** Select **TCP only**
- **TCP Port** Select **5060**

Click **OK**(not shown).



5.5. Administer Codec Preference

From the configuration tree in the left pane, select **System** to display the system screen in the right pane. Select the **Telephony** tab. Configure **Automatic Codec Preference** to **G.711 ULAW 64K**. Click **OK** (not shown).



5.6. 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. Select the **SIP Line** tab and enter the following values:

- **Line Number** Select a unique Line Number
- **ITSP Domain Name** Enter a Domain Name
- **ITSP IP Address** Enter the IP address for SM-100 card
- **Layer 4 Protocol** Select **TCP**
- **Send Port** Select **5060**
- **Use Network Topology Info** Select **LAN1**

Retain default values for all other fields. Click **OK**(not shown).

The screenshot displays the 'SIP Line - Line 19' configuration window. The left pane shows a configuration tree with 'Line (6)' selected. The right pane shows the 'SIP Line' tab with the following fields and values:

Field	Value
Line Number	19
ITSP Domain Name	silstack.com
ITSP IP Address	135 . 64 . 186 . 46
Prefix	
National Prefix	0
Country Code	
International Prefix	00
Send Caller ID	None
Layer 4 Protocol	TCP
Send Port	5060
Use Network Topology Info	LAN 1
Listen Port	5060

Other fields and checkboxes include: Registration Required (unchecked), In Service (checked), Use Tel URI (unchecked), Check OOS (checked), and Call Routing Method (Request URI).

Select the **SIP URI** tab and click on the **Add** button (not shown). Enter the following values:

- **Local URI** Select **Use Internal Data**
- **Contact** Select **Use Internal Data**
- **Display Name** Select **Use Internal Data**
- **Incoming Group** Enter the line number administered under the SIP Line tab above
- **Outgoing Group** Enter the line number administered under the SIP Line tab above

Retain default values for all other fields. Click **OK**(not shown).

The screenshot shows a 'New Channel' configuration window. The fields and their values are as follows:

Field	Value
Via	10.10.21.215
Local URI	Use Internal Data
Contact	Use Internal Data
Display Name	Use Internal Data
Registration	0: <None>
Incoming Group	19
Outgoing Group	19
Max Calls per Channel	10

5.7. Administer Short Code

From the configuration tree in the left pane, right-click on **Short Code**, and select **New**. Enter the following details:

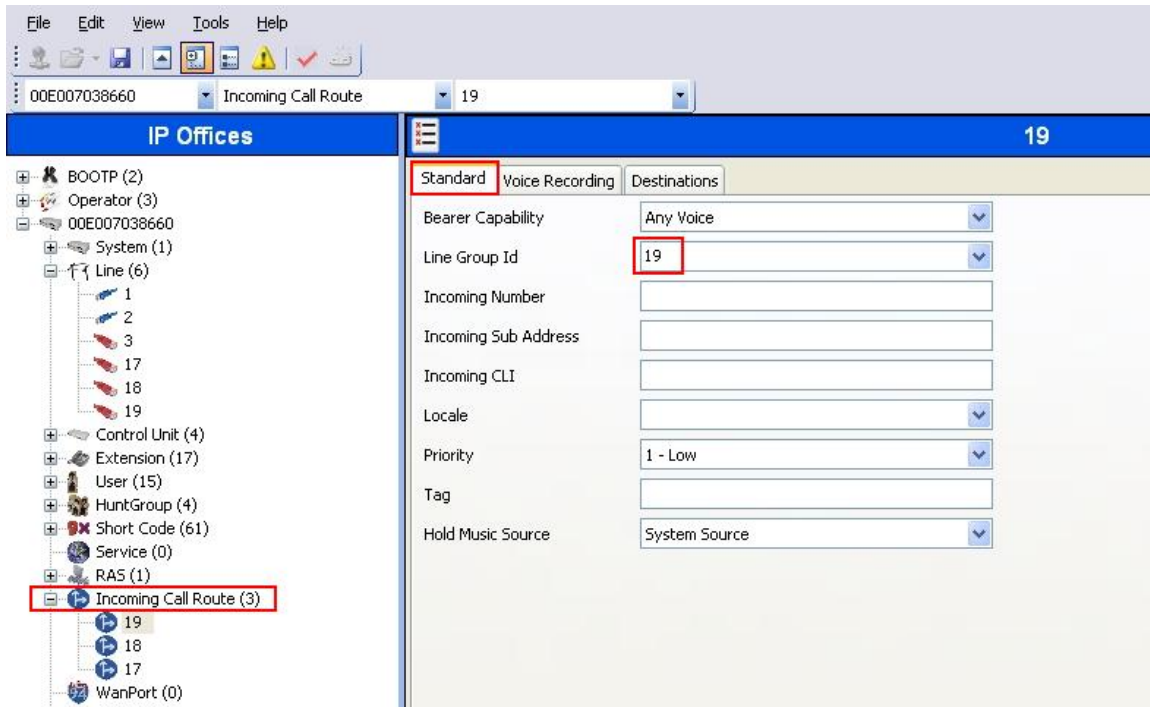
- **Code** Enter the dialing string that will be used to call into the MX
- **Feature** Select **Dial**
- **Telephone Number** Enter the phone number appended with “@<ip-address of SM-100 card>”
- **Line Group ID** Enter ID administered in **Section 5.6**

The screenshot shows the Avaya configuration interface. On the left, the 'IP Offices' tree is visible, with 'Short Code (61)' highlighted. The main pane displays the '3888X: Dial' configuration form. The form fields are as follows:

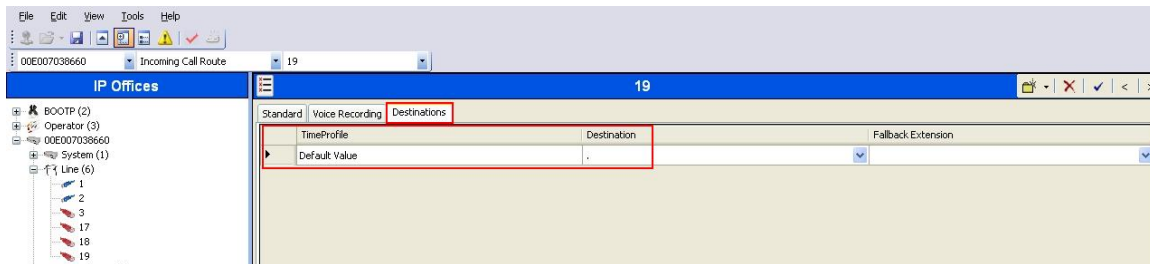
Field	Value
Code	3888X
Feature	Dial
Telephone Number	3888N@135.64.186.46
Line Group Id	19
Locale	
Force Account Code	<input type="checkbox"/>

5.8. 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, for the **Line Group Id**, use the **Line Number** value administered in **Section 5.6**.

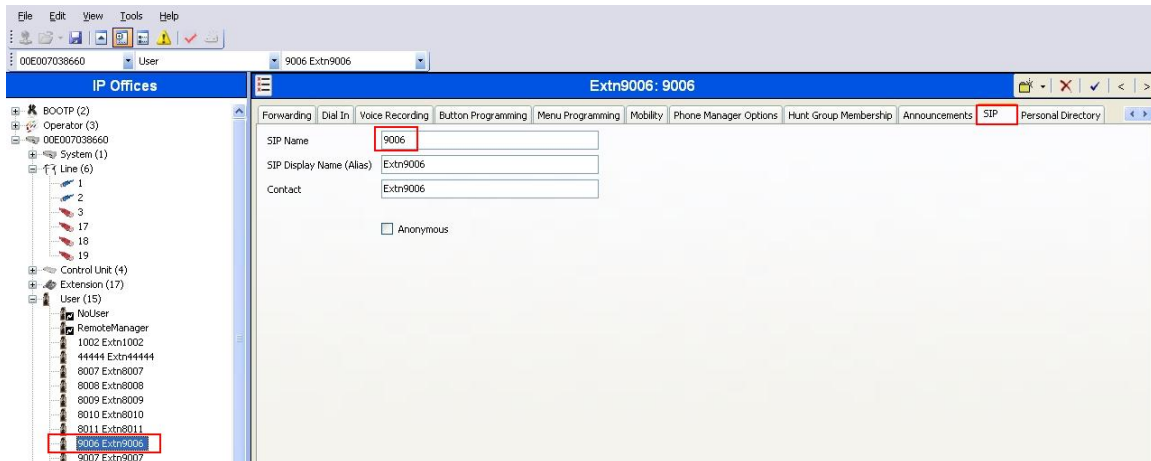


Select the **Destination** tab, enter **.** as the **Default Value**. This will enable all incoming calls to be routed to any extension.



5.9. Configure SIP User Names

From the configuration tree in the left pane, select a **User** and in the right-hand pane, 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.



5.10. Save Configuration

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

6. Verification Steps

The following steps were used to verify the administrative steps presented in these Application Notes and are applicable for similar configurations in the field. The verification steps in this section validated the following:

- The Avaya Meeting Exchange Standard S6200 Conferencing Server configuration

6.1. Verify Avaya Meeting Exchange Enterprise S6200

Verify all conferencing related processes are running on the Meeting Exchange as follows:

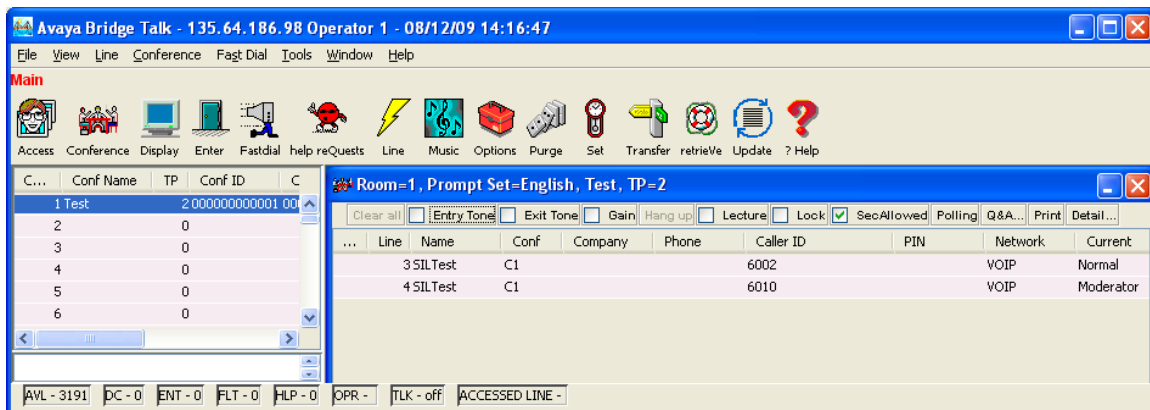
- Log in to the Meeting Exchange server console to access the CLI with the appropriate credentials.
- cd to **/usr/dcb/bin**
- At the command prompt, run the script **service mx-bridge status** and confirm all processes are running by verifying an associated 4-digit Process ID (PID) for each process.

```
[sroot@MXSIL ~]# service mx-bridge status
5042 ?      00:00:01 initdcb
5604 ?      00:00:00 log
5607 ?      00:00:00 bridgeTranslato
5608 ?      00:00:00 netservices
5626 ?      00:00:00 timer
5627 ?      00:00:00 traffic
5628 ?      00:00:00 chdbased
5629 ?      00:00:00 startd
5630 ?      00:00:00 cdr
5631 ?      00:00:00 modapid
5632 ?      00:00:00 schapid
5633 ?      00:00:01 callhand
5634 ?      00:00:00 initipcb
5644 ?      00:00:00 sipagent
5645 ?      00:00:00 msdispatcher
5646 ?      00:00:00 serverComms
5648 ?      00:00:00 softms
5649 ?      00:00:00 softms
5650 ?      00:00:00 softms
5651 ?      00:00:00 softms
5652 ?      00:00:00 softms
5653 ?      00:00:00 softms
4022 ?      00:00:00 postmaster with 9 children
```

6.1.1. Verify Call Routing

Verify end to end signalling/media connectivity between the Meeting Exchange and IP Office. This is accomplished by placing calls from the IP Office end points to the Meeting Exchange. This step utilizes the Avaya Bridge Talk application to verify calls to and from the Meeting Exchange are managed correctly, e.g., callers are added/removed from conferences. This step will also verify the conferencing applications provisioned.

- Configure a conference with Auto Blast enabled and provision a dial list. From an endpoint on the Public Switched Telephone Network, dial a number that corresponds to DNIS **38888** to enter a conference as **Moderator** (with passcode) and blast dial is invoked automatically. When answered these callers enter the conference.
- If not already logged on, log in to the Avaya Bridge Talk application with the appropriate credentials
- **Double-Click on the** highlighted **Conf #** to open a **Conference Room** window
- Verify conference participants are added/removed from conferences by observing the Conference Navigator and/or Conference Room windows.



6.2. 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, click on the **Trunks** entry and select the SIP trunk created in **Section 5.6**. Press the **Trace All** button (not shown). The messages on the line are displayed.

AVAYA

IP Office System Status

Help Snapshot LogOff Exit About

System

Alarms (27)

Extensions (11)

Trunks (6)

Line: 1

Line: 2

Line: 3

Line: 17

Line: 18

Line: 19

Active Calls

Resources

Voicemail

IP Networking

Status Utilization Summary Alarms

SIP Trunk Summary

Peer Domain Name: slistack.com

Gateway Address: 135.64.186.46

Line Number: 19

Number of Administered Channels: 10

Number of Channels in Use: 0

Administered Compression: Auto

Silence Suppression: Off

SIP Trunk Channel Licences: Unlimited

SIP Trunk Channel Licences in Use: 0

SIP Device Features:

0%

Channel Number	URI	Call Gro. 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 Pack Loss Fraction
1			Idle	4 days 00:...											
2			Idle	5 days 01:...											
3			Idle	5 days 02:...											
4			Idle	5 days 20:...											

Trace Output - All Channels:

Trace Clear

Pause

Ping

Call Details

Print...

Save As...

6.3. Verify Avaya Aura™ Session Manager

Select **Session Manager** → **System Status** → **SIP Entity Monitoring**. Verify as shown below that none of the SIP Entity Links for IP Office or MX are down, indicating that they are all reachable for routing.

The screenshot shows the 'SIP Entity Link Monitoring Status Summary' page. The left sidebar contains a navigation menu with 'Session Manager' expanded, showing 'System Status' and 'SIP Entity Monitoring'. The main content area has a title 'SIP Entity Link Monitoring Status Summary' and a subtitle 'This page provides a summary of Session Manager SIP entity link monitoring status.' Below this is a section 'Entity Link Status for All Session Manager Instances' with a 'Refresh' button. A table shows the status of SIP entities for the 'SessionManager' instance. The table has columns: 'Session Manager Name', 'Entity Links Down/Total', 'Entity Links Partially Down', 'SIP Entities - Monitoring Not Started', and 'SIP Entities - Not Monitored'. The data row shows 'SessionManager' with 0/25 down, 0 partially down, 0 not started, and 0 not monitored. Below this is a section 'All Monitored SIP Entities' with a 'Refresh' button and a list of 25 items. The list shows 'SIP Entity Name' and a 'Filter: Enable' button. The entities listed are: 'Audio Codes M2K', 'AudioCodes M1K', 'AvayaCM', 'AvayaCM_MD', 'IP Office', 'Cisco2', 'MX-S6200', 'GM165', and 'GM99_PUNE'. The 'IP Office' and 'MX-S6200' entities 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
SessionManager	0/25	0	0	0

SIP Entity Name
Audio Codes M2K
AudioCodes M1K
AvayaCM
AvayaCM_MD
IP Office
Cisco2
MX-S6200
GM165
GM99_PUNE

Click on the SIP Entity Names **IP Office** and **MX-S6200**, shown in the previous screen, and verify that the connection status is **Up**, as shown in screenshots below.

The screenshot shows the 'SIP Entity, Entity Link Connection Status' page for the 'IP Office' entity. The left sidebar contains a navigation menu with 'Session Manager' expanded, showing 'System Status' and 'SIP Entity Monitoring'. The main content area has a title 'SIP Entity, Entity Link Connection Status' and a subtitle 'This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.' Below this is a section 'All Entity Links to SIP Entity: IP Office' with 'Refresh' and 'Summary View' buttons. A table shows the connection status for the 'IP Office' entity. The table has columns: 'Details', 'Session Manager Name', 'SIP Entity Resolved IP', 'Port', 'Proto.', 'Conn. Status', 'Reason Code', and 'Link Status'. The data row shows 'SessionManager' with IP 10.10.21.215, Port 5060, Proto. TCP, Conn. Status 'Up', Reason Code '200 Ok', and Link Status 'Up'. The 'Up' status is highlighted with a red box.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SessionManager	10.10.21.215	5060	TCP	Up	200 Ok	Up

The screenshot shows the 'SIP Entity, Entity Link Connection Status' page for the 'MX-S6200' entity. The left sidebar contains a navigation menu with 'Session Manager' expanded, showing 'System Status' and 'SIP Entity Monitoring'. The main content area has a title 'SIP Entity, Entity Link Connection Status' and a subtitle 'This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.' Below this is a section 'All Entity Links to SIP Entity: MX-S6200' with 'Refresh' and 'Summary View' buttons. A table shows the connection status for the 'MX-S6200' entity. The table has columns: 'Details', 'Session Manager Name', 'SIP Entity Resolved IP', 'Port', 'Proto.', 'Conn. Status', 'Reason Code', and 'Link Status'. The data row shows 'SessionManager' with IP 135.64.186.98, Port 5060, Proto. TCP, Conn. Status 'Up', Reason Code '200 OK', and Link Status 'Up'. The 'Up' status is highlighted with a red box.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SessionManager	135.64.186.98	5060	TCP	Up	200 OK	Up

7. Verified Scenarios

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

- Place a call from the Avaya 1616 IP Telephone (H323) and the Avaya 2420 Digital Telephone to a scheduled conference on the Meeting Exchange.
- Ensure the welcome message is played from the Conferencing Bridge and there is audio between callers in the conference.
- Initiate dial out by dialling *1 on the phone's touch pad and entering the phone number. Enter the number and press 1 to make the call. When the callers answer dial *2 to return them to the main conference.
- Calls to MX with direct media shuffling (G.711 and G.729) were verified.

8. Conclusion

- As illustrated in these Application Notes, Avaya IP Office can interoperate with Avaya Meeting Exchange Enterprise S6200 using SIP trunks.

9. Additional References

All references are available at <http://support.avaya.com>

- [1] Meeting Exchange Enterprise S6200 5.2 Administration and Maintenance S6200/S6800
- [2] Avaya Meeting Exchange Enterprise Groupware Edition Version 5.2 User's Guide for Bridge Talk
- [3] Avaya AuraTM Session Manager Overview, Doc # 03-603323, Issue 2
- [4] Administering Avaya AuraTM Session Manager, Doc # 03-603324, Issue 2
- [5] Maintaining and Troubleshooting Avaya AuraTM Session Manager, Doc # 03-603325, Issue 2
- [6] Avaya IP Office Manager, Doc # 15-601011, Issue 2

©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 Applications Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Lab at interoplabnotes@list.avaya.com