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.

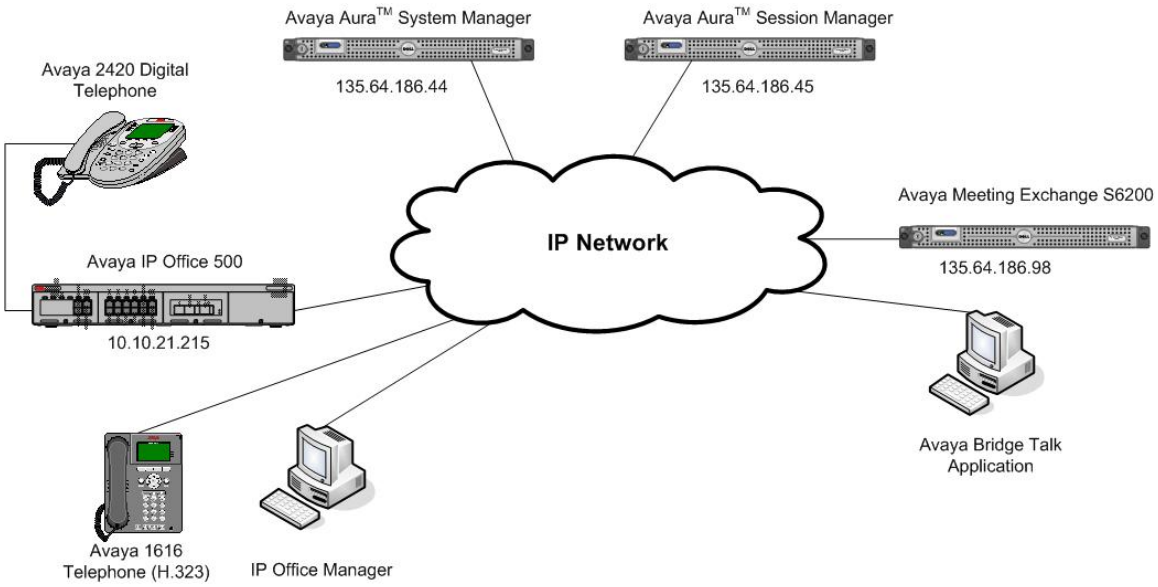


Figure 1 - Avaya Meeting Exchange Enterprise Interop Network Topology

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

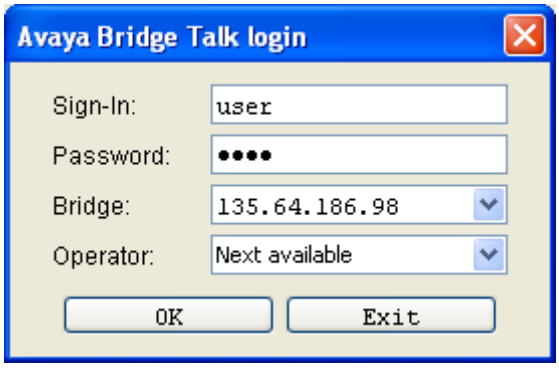
The following steps utilize the Avaya Bridge Talk application to provision a sample conference on the Meeting Exchange. This sample conference enables both Dial-In and Dial-Out access to audio conferencing for endpoints on the Public Switched Telephone Network.

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:

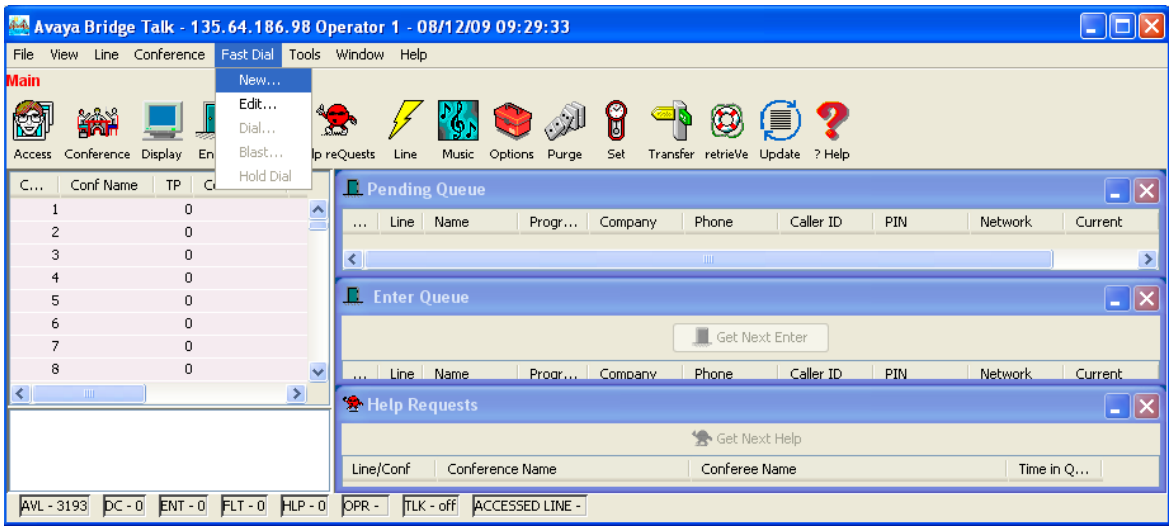
- Double-click on the desktop icon from a Personal Computer loaded with the Avaya Bridge Talk application and with network connectivity to the Meeting Exchange (Not shown).
- Enter the appropriate credentials in the **Sign-In** and **Password** fields.
- Enter the IP address of the Meeting Exchange server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



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**.

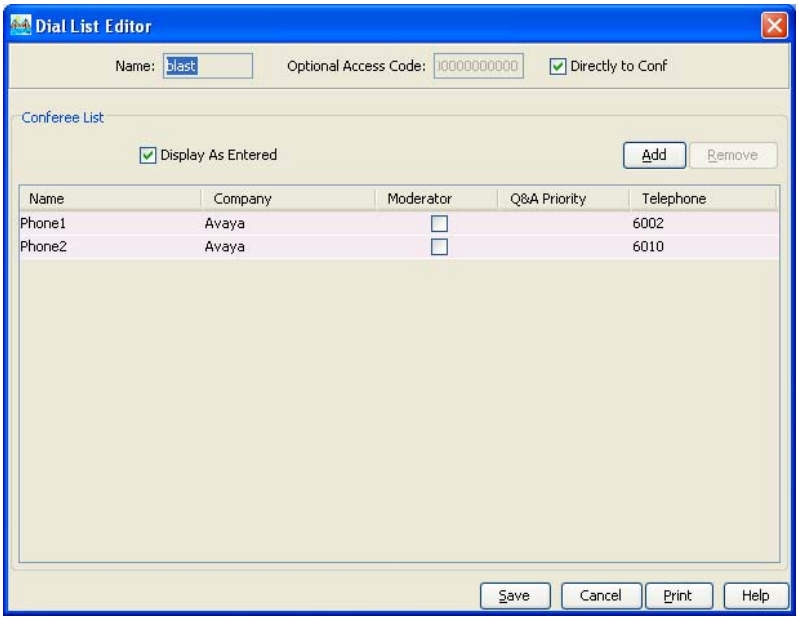


3.6.3. Creating a Dial List

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

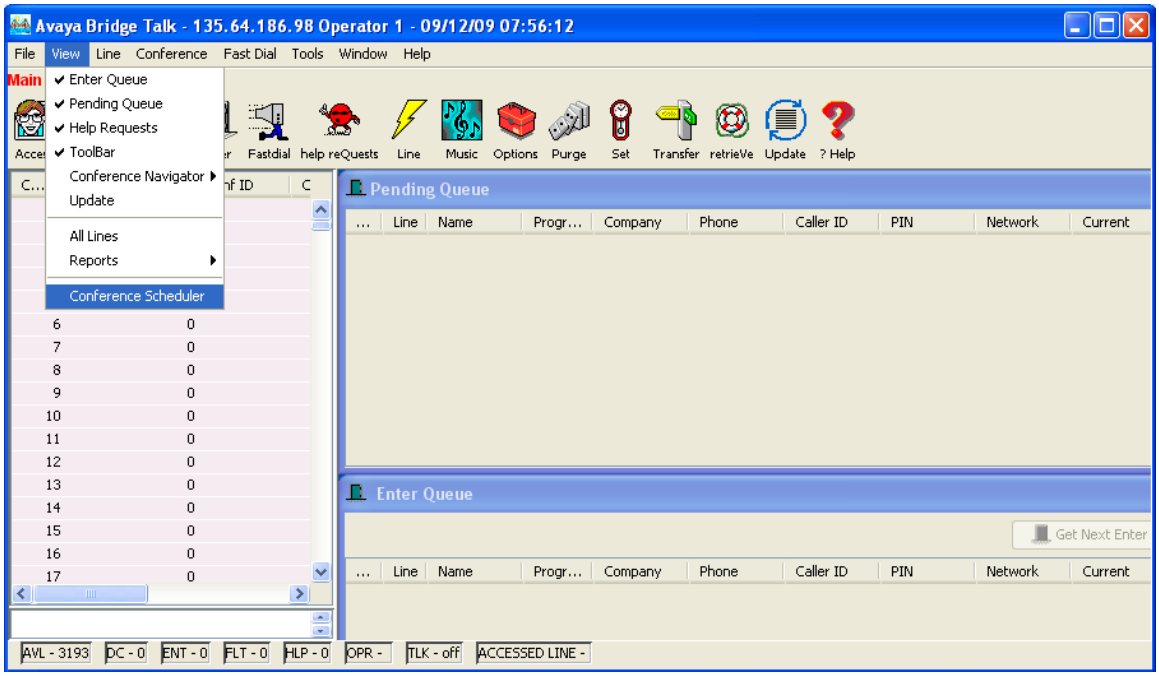
- Enter a descriptive label in the **Name** field.
- Enable conference participants on the dial list to enter the conference without a passcode by selecting the **Directly to Conf** box as displayed.
- Add entries to the dial list by clicking on the **Add** button and enter **Name**, **Company** and **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.



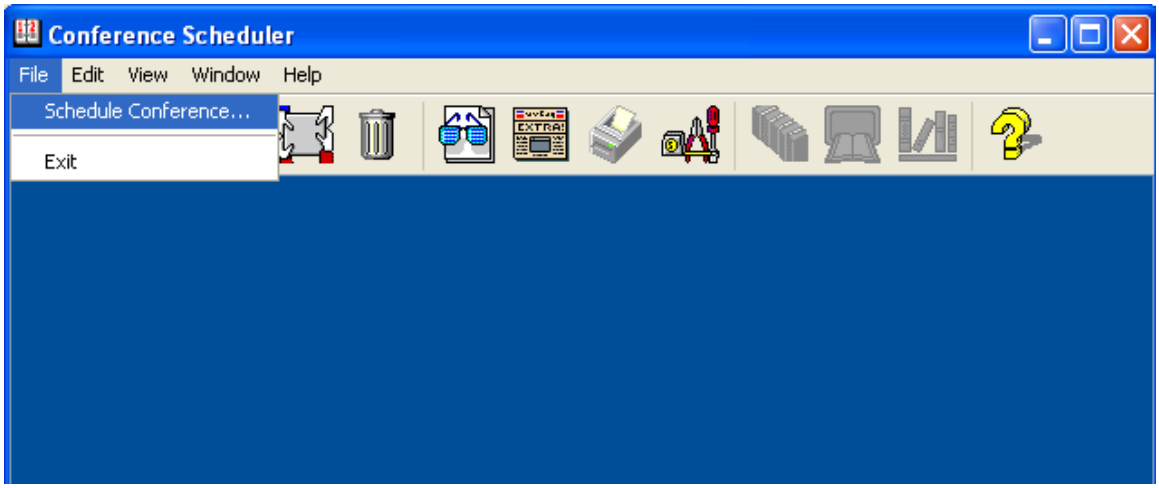
3.6.4. Conference Scheduler

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**.



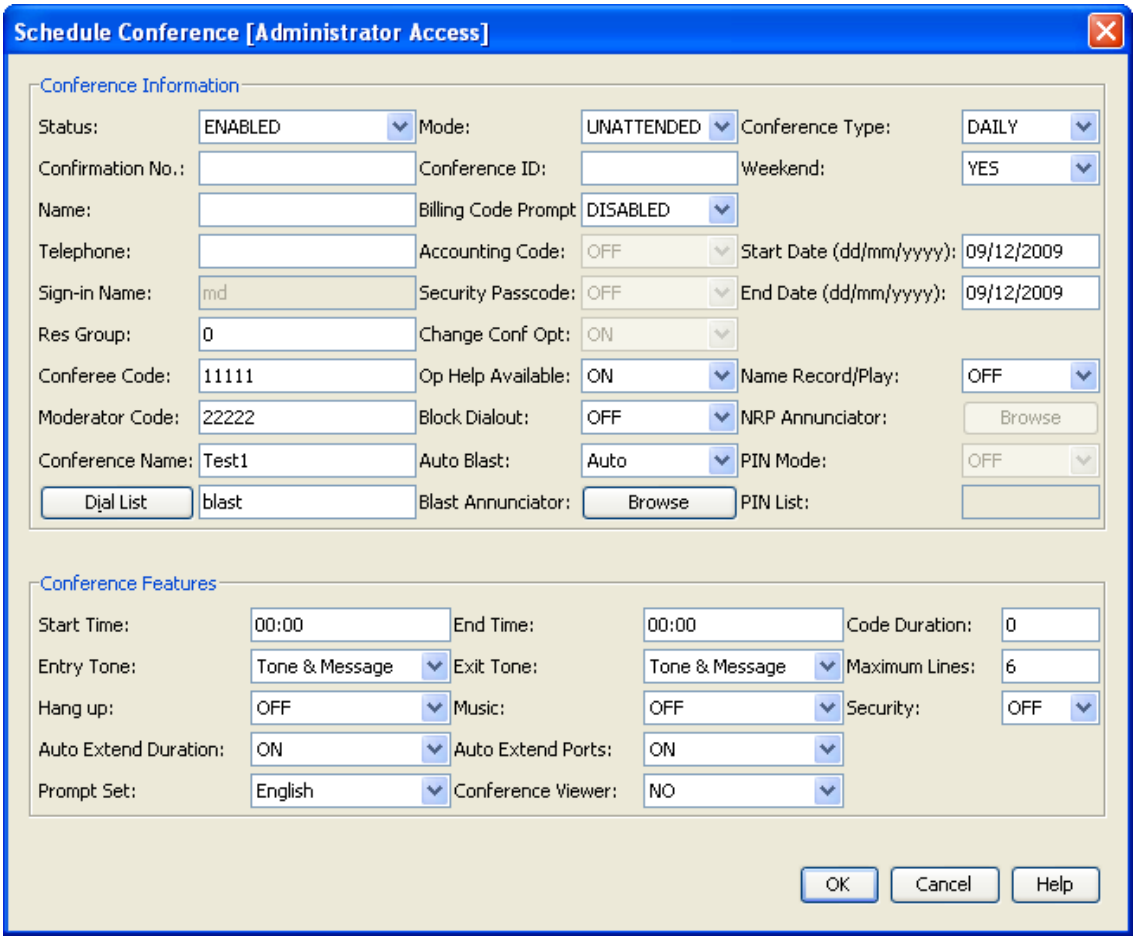
3.6.6. Provision a Conference

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.



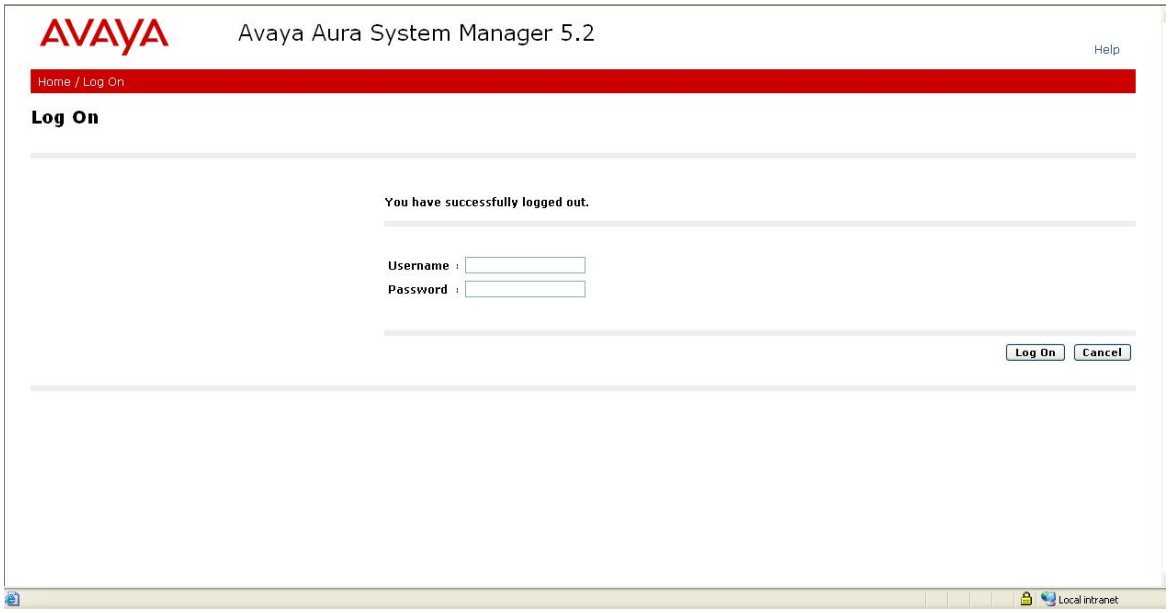
4. Configure Avaya Aura™ Session Manager

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:

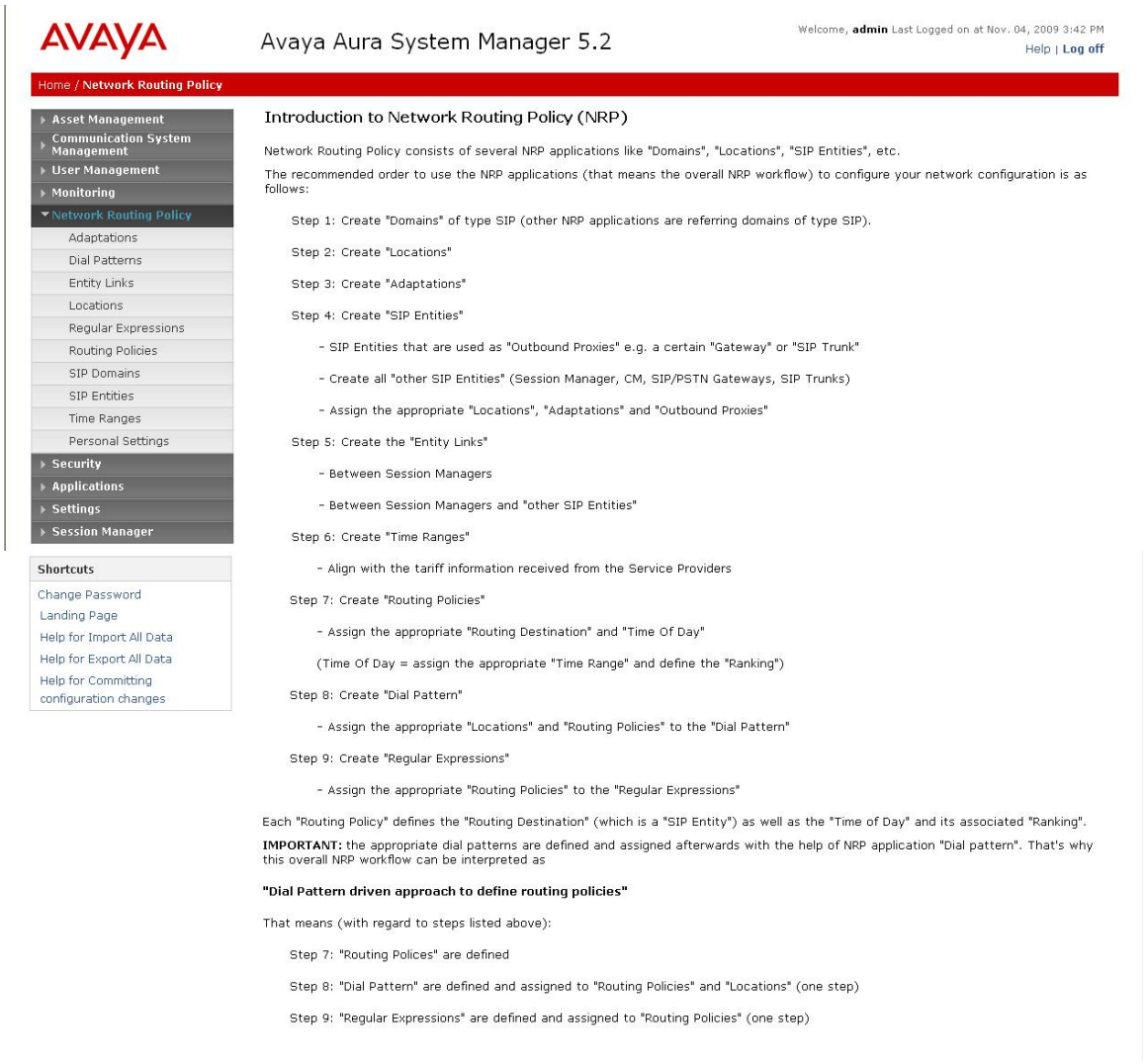
- Log in to Avaya Aura™ Session Manager
- Administer SIP domain
- Administer SIP Entities
- Administer Entity Links
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Aura™ Session Manager

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.



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

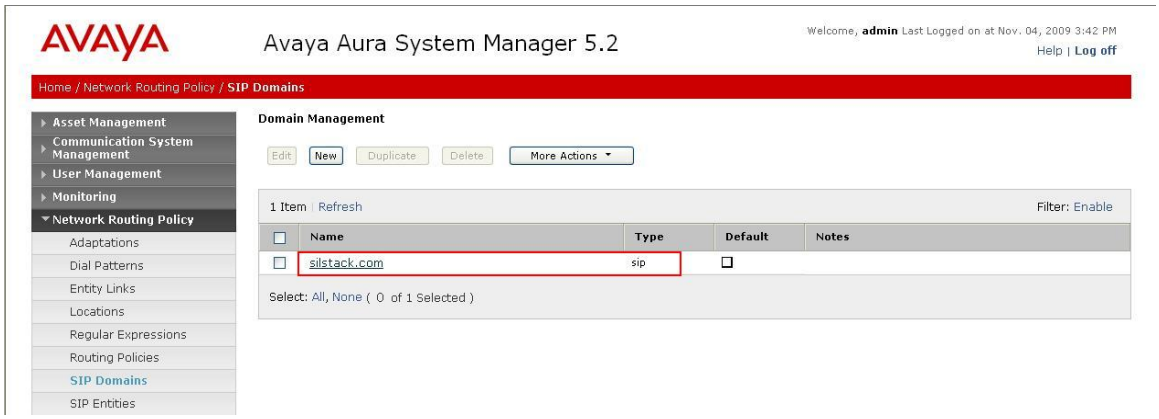


4.2. Administer SIP Domain

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.



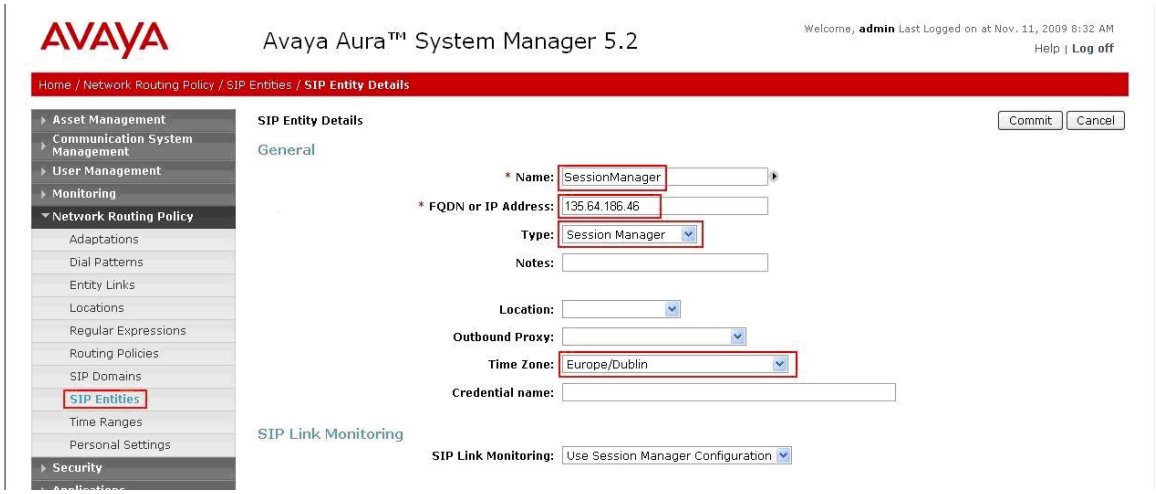
Note: Since the sample network does not deal with any foreign domains, no additional SIP Domains entry is needed.

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:**

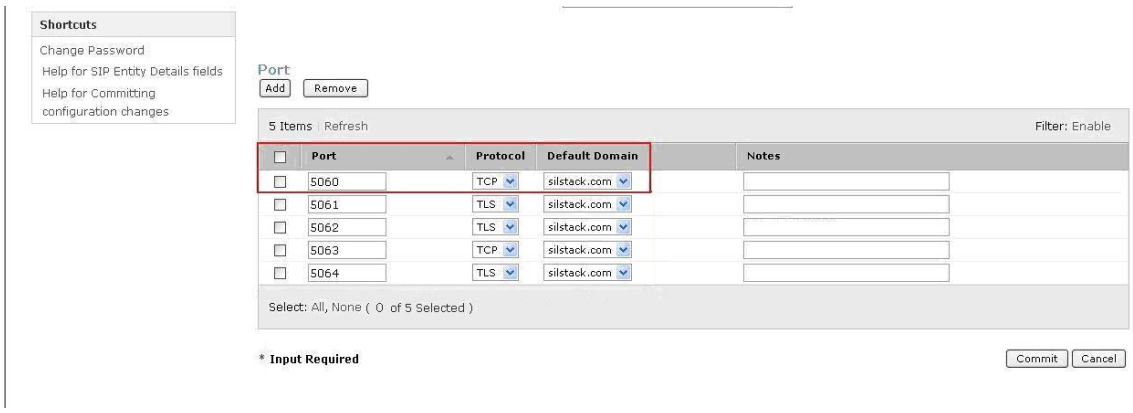
- **Name** — An informative name (e.g., **SessionManager**)
- **FQDN or IP Address** — IP address of the signaling interface on the Session Manager
- **Type** — **Session Manager** for Session Manager or **SIP Trunk** for IP Office and MX
- **Time Zone** — Time zone for this location



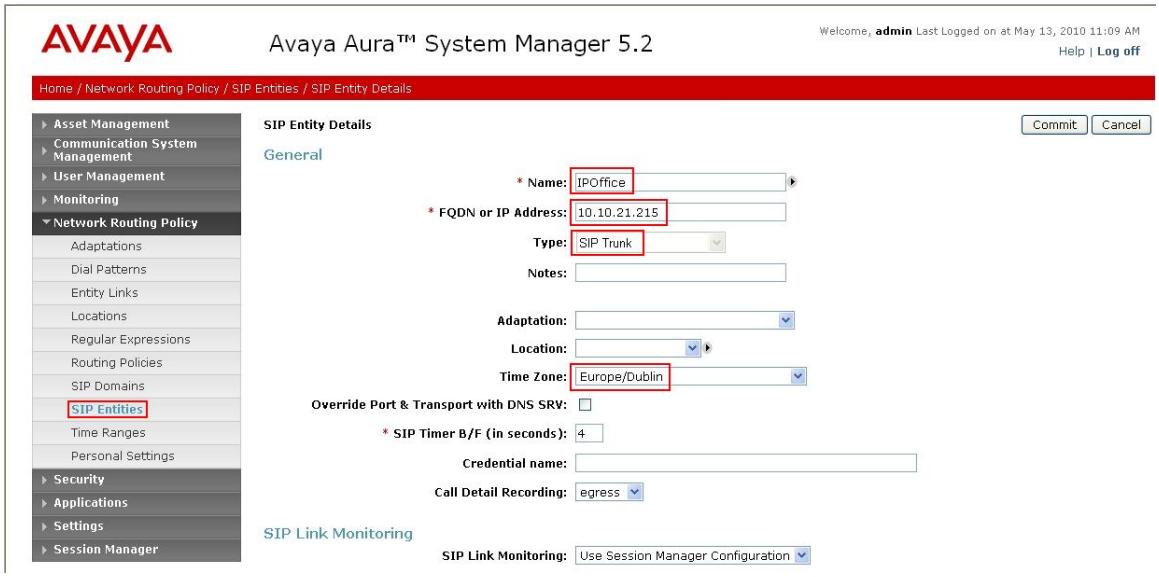
Under **Port**, click **Add,** and then edit the fields in the resulting new row.

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

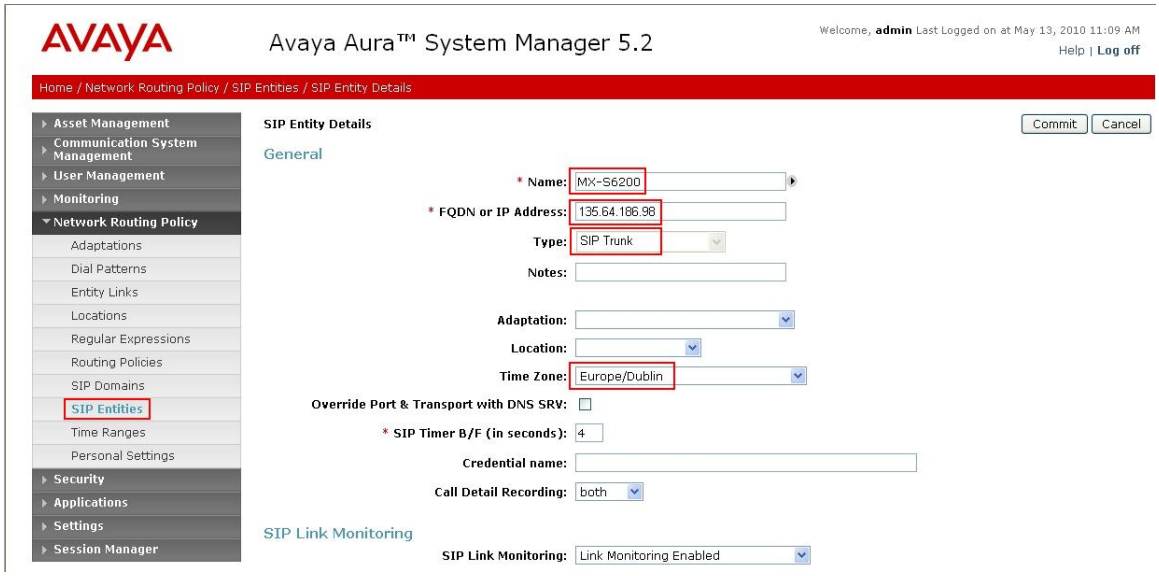
The following screen shows the Port definitions for the Session Manager SIP Entity.



The following screen shows the SIP Entity for IP Office.



The following screen shows the SIP Entity for MX.

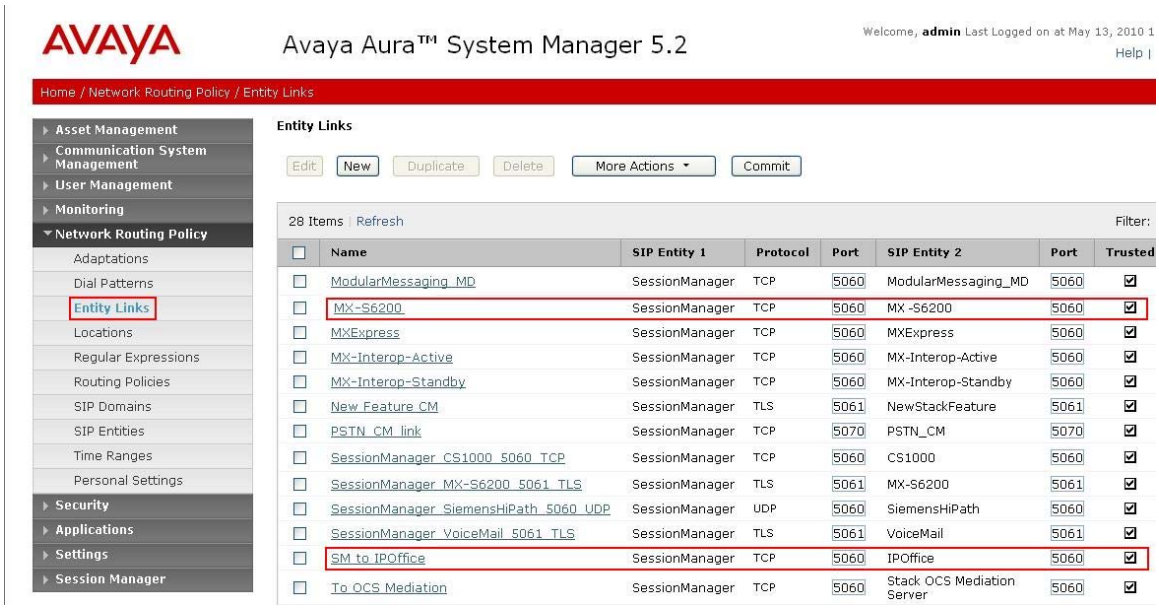


4.4. Administer Entity Links

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

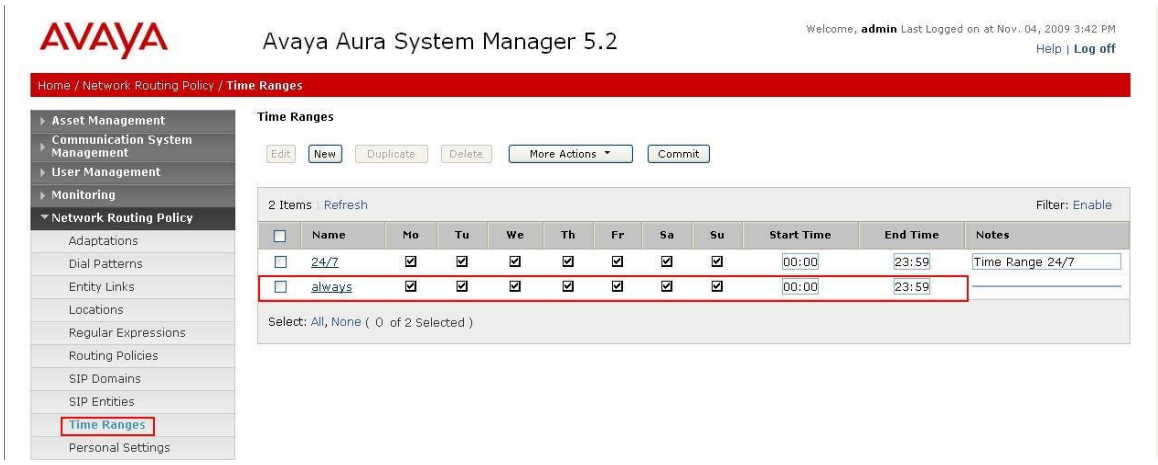
Click **Commit** to save changes. The following screen shows the Entity Links used in the sample network.



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)



4.6. Administer Routing Policies

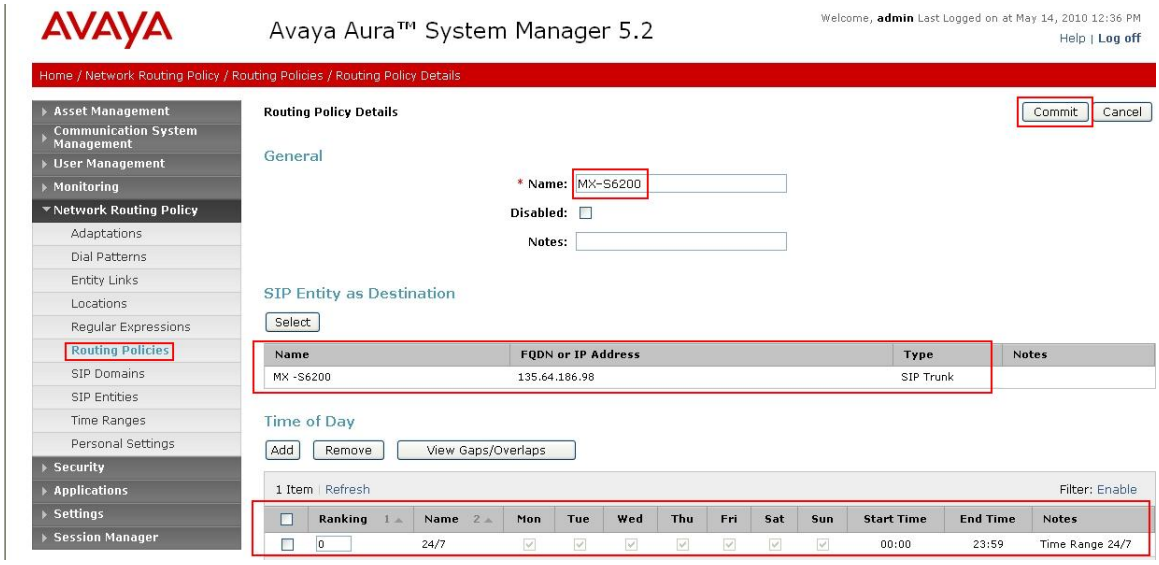
Create routing policies to direct how calls will be routed to a system. Two routing policies must be added, one for IP Office and one for MX. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).
Under **General:**

- **Name** Enter an informative **Name**

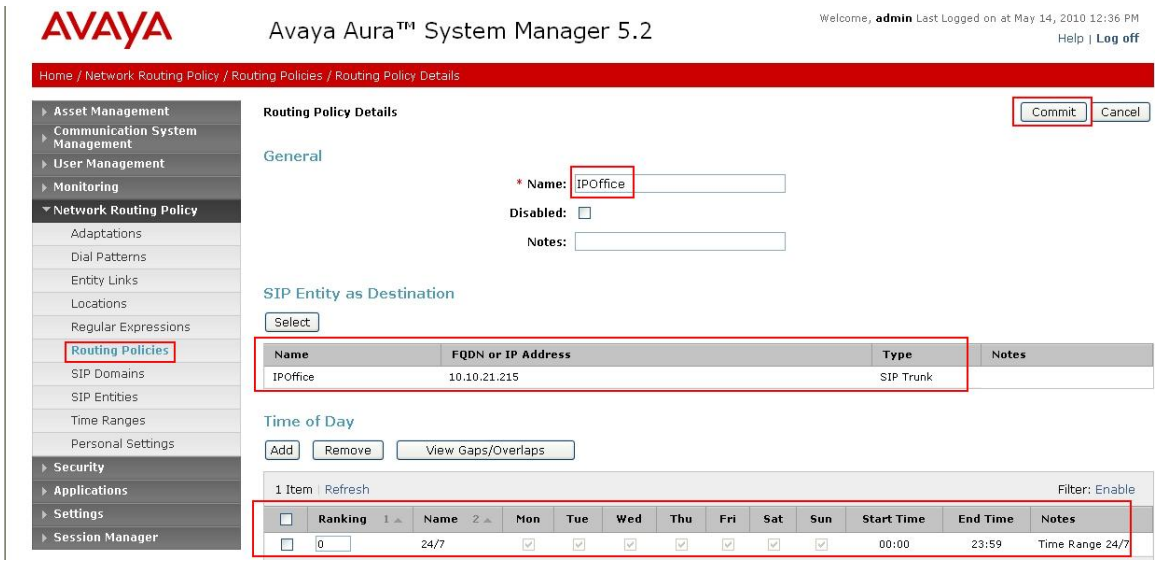
Under **SIP Entity as Destination:**
Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

Under **Time of Day:**
Click **Add**, and then select the time range configured in the previous step.

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



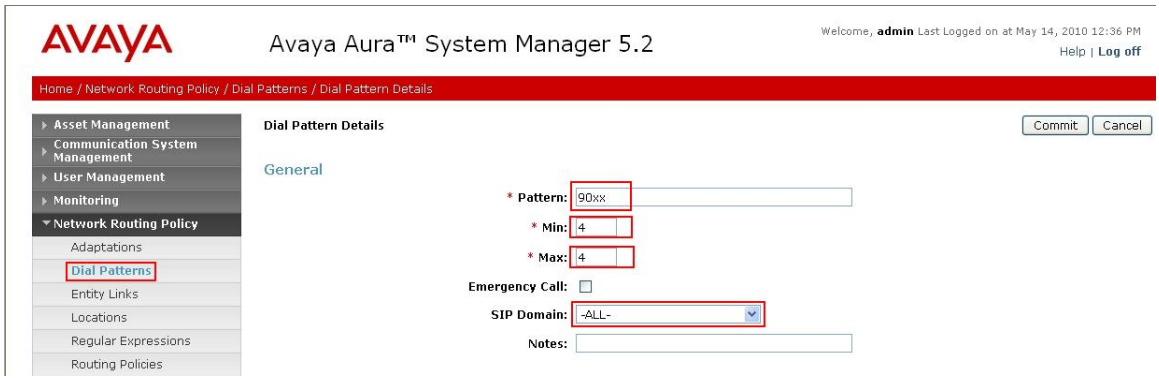
The following is screen shows the **Routing Policy Details** for IP Office



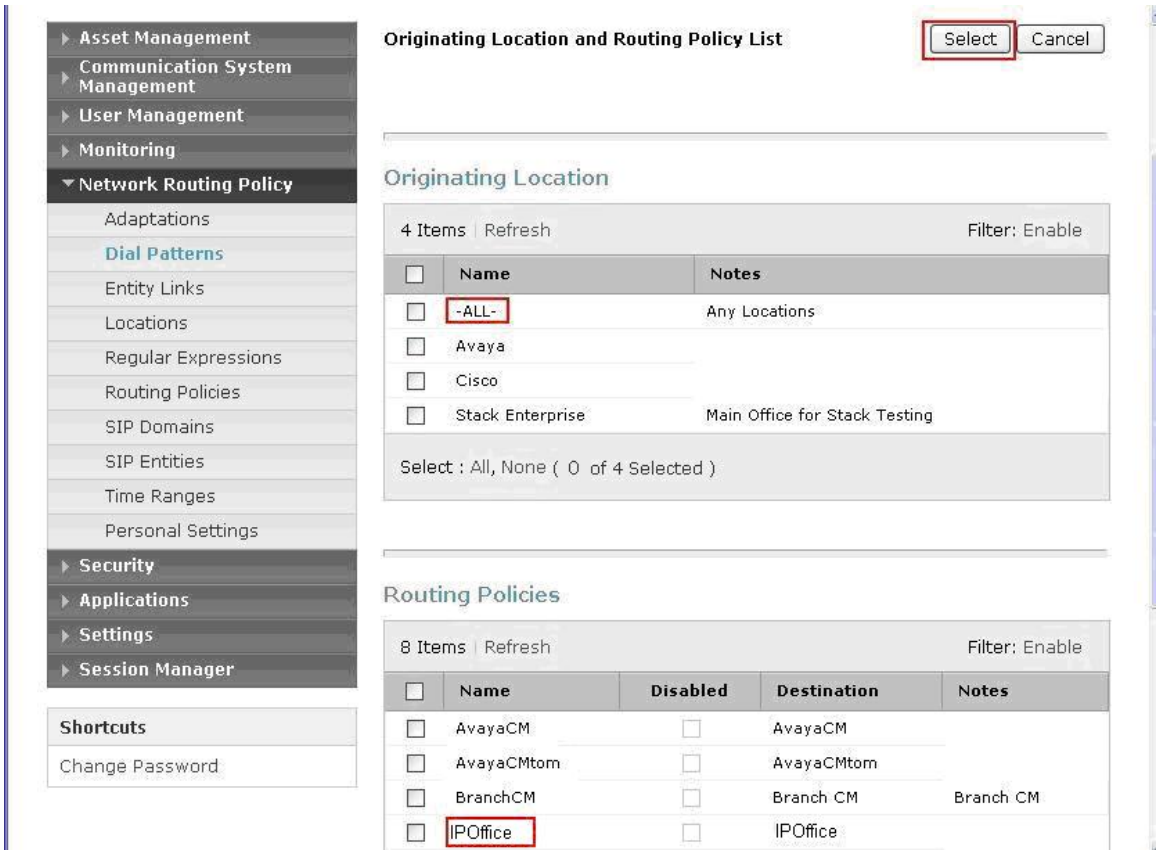
4.7. Administer Dial Patterns

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**

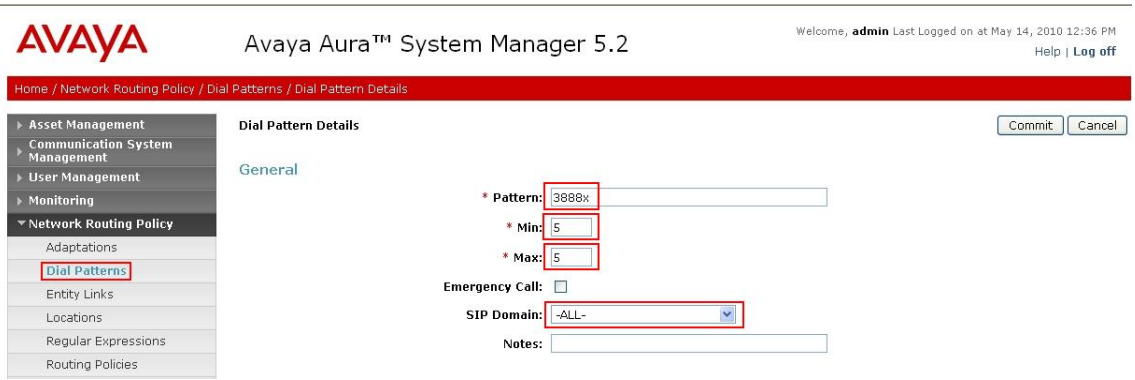


Navigate to **Originating Locations and Routing Policy List** and select **Add** (not shown). Under **Originating Location,** check the box next to **ALL** and under **Routing Policies,** check the box next to **IPOffice.** Click **Select** button to confirm the chosen options and then be returned to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

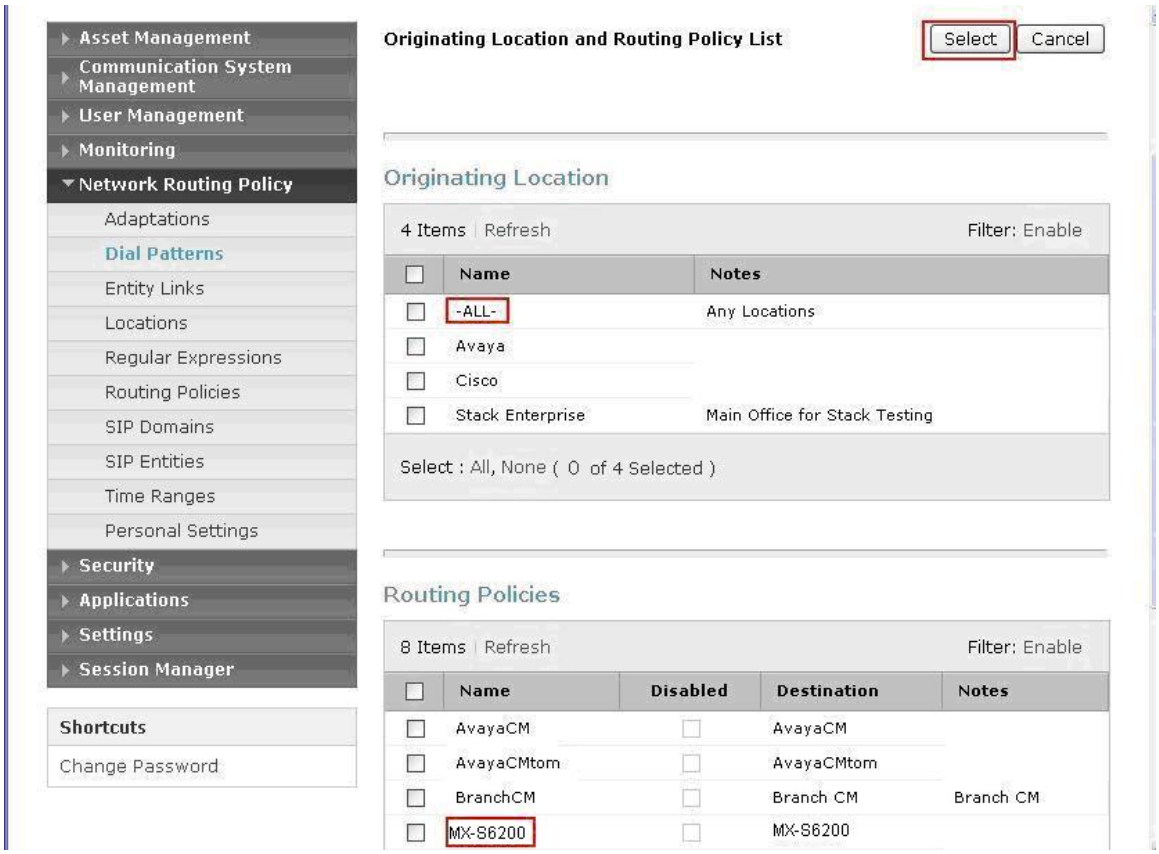


For MX Dial Pattern configuration, select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).
Under **General:**

- **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**



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.



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:

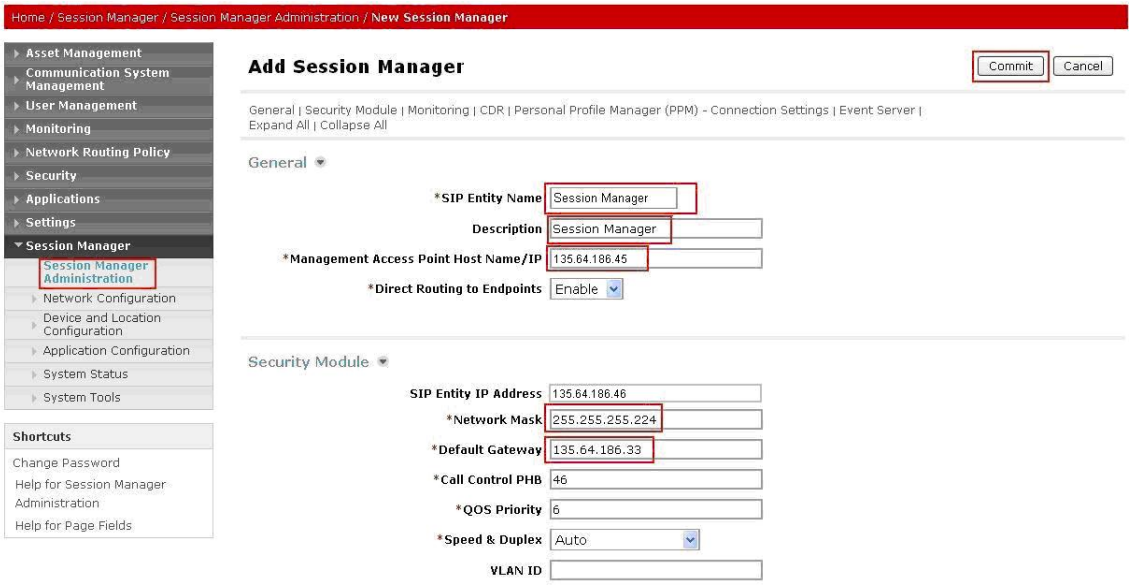
Under **General:**

- **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.



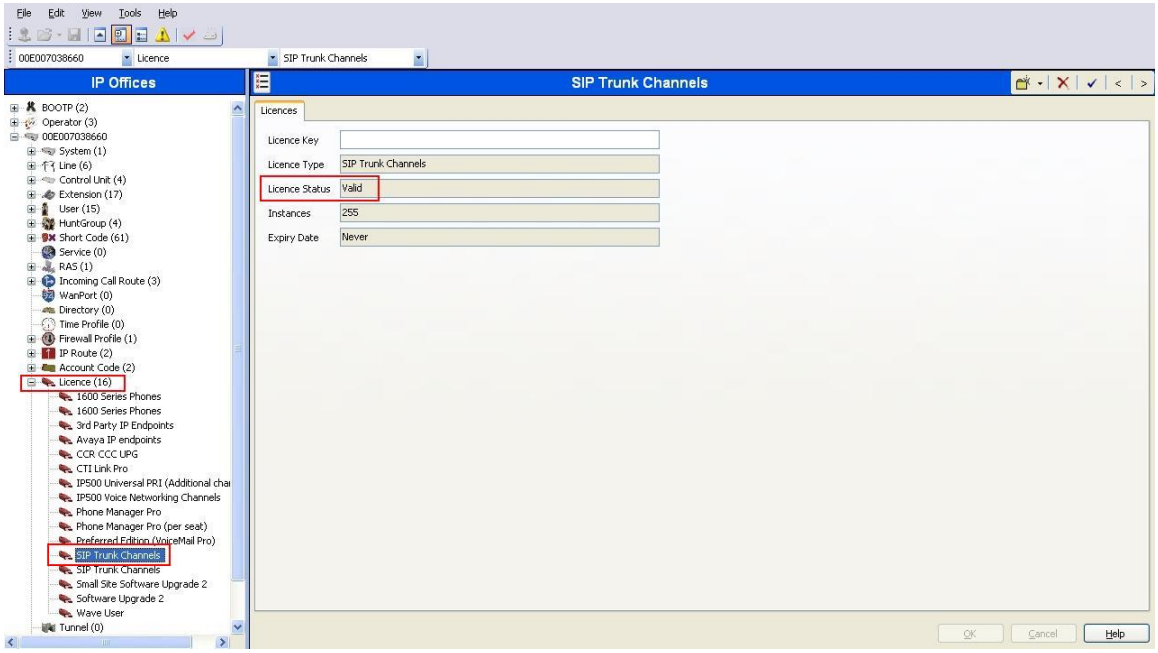
5. Configure Avaya IP Office

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

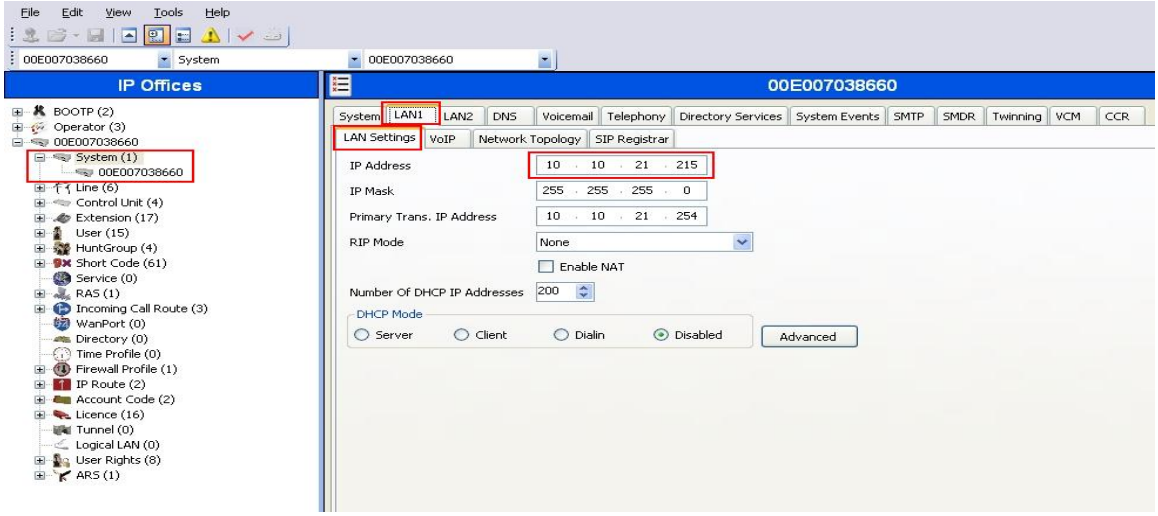
5.1. Verify IP Office License

From a PC running the Avaya IP Office Manager application, select **Start → Programs → IPOffice → 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.



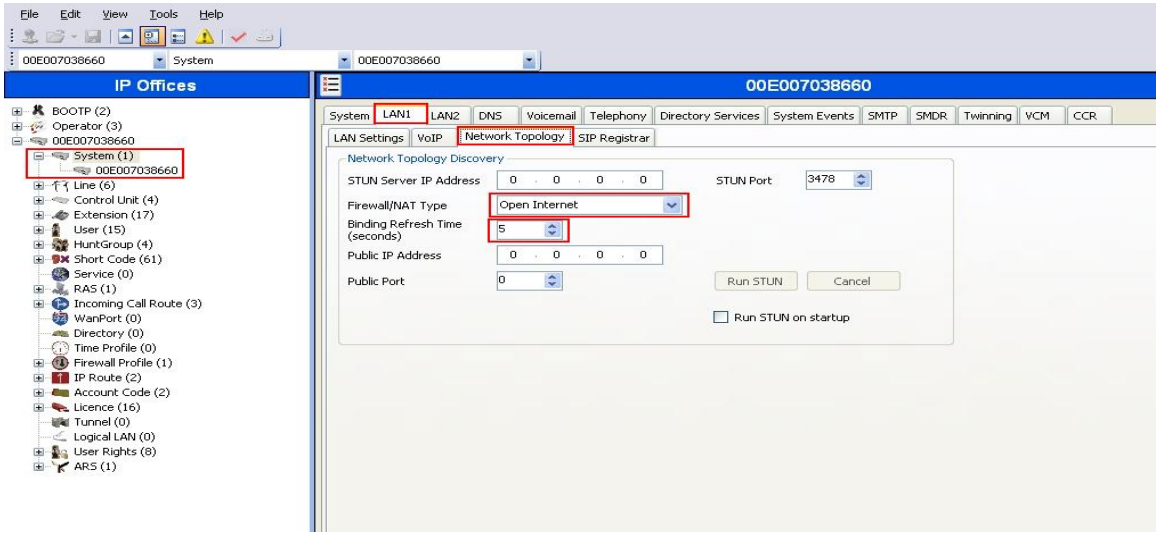
5.2. Obtain LAN IP Address

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).

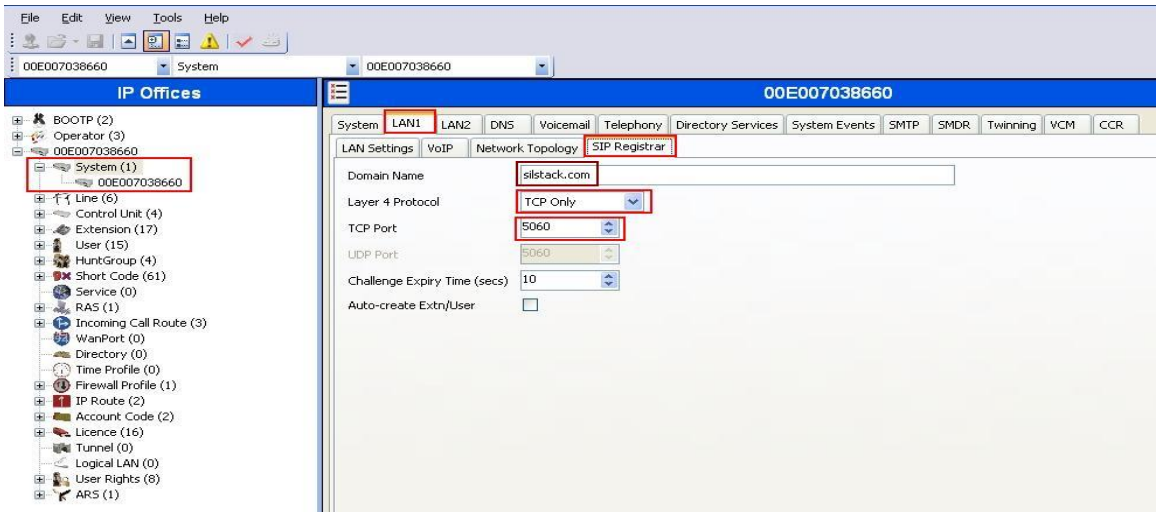


5.4. Administer SIP Registrar

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

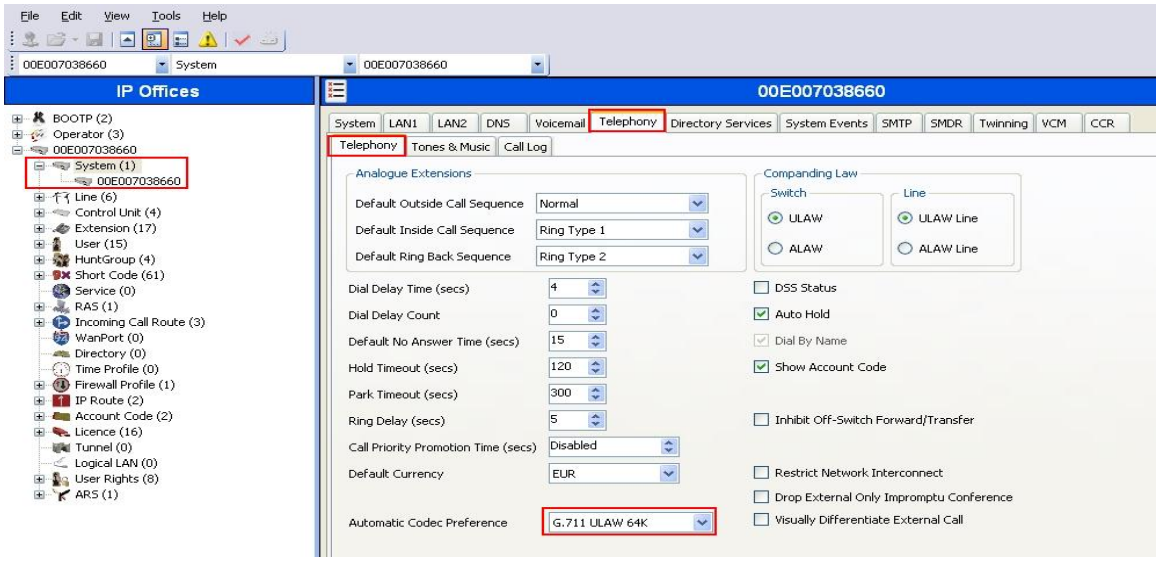
- **Domain Name** Enter a valid Domain Name.
- **Layer 4 Protocol** Select **TCP only**
- **TCP Port** Select **5060**

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).

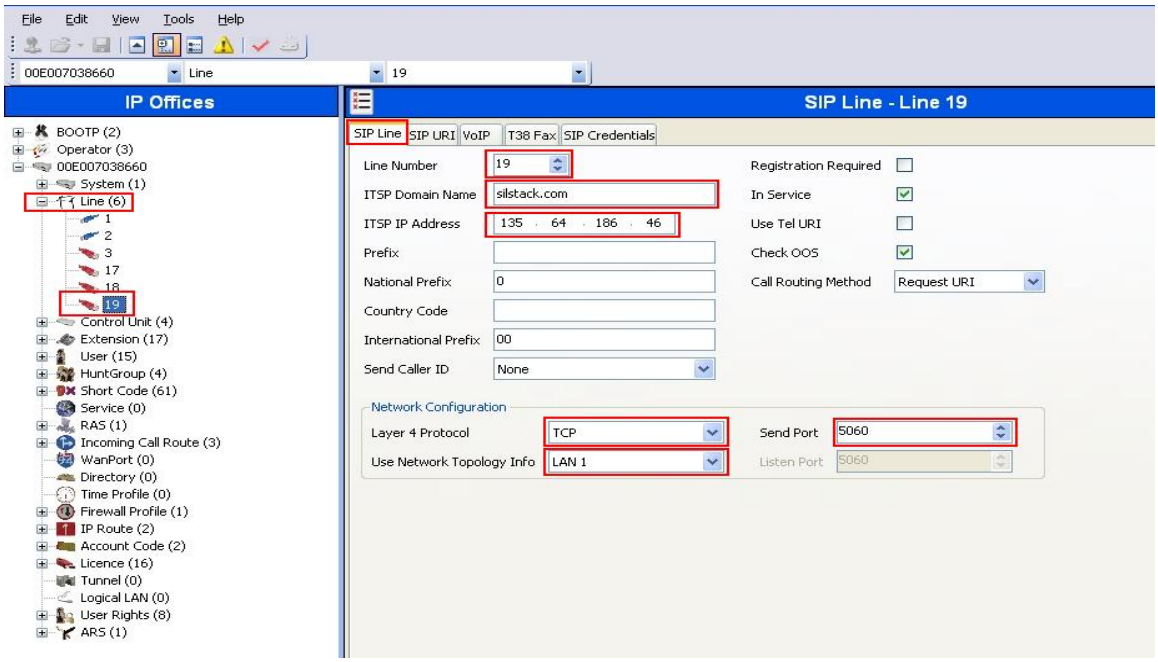


5.6. Administer SIP Trunk

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**

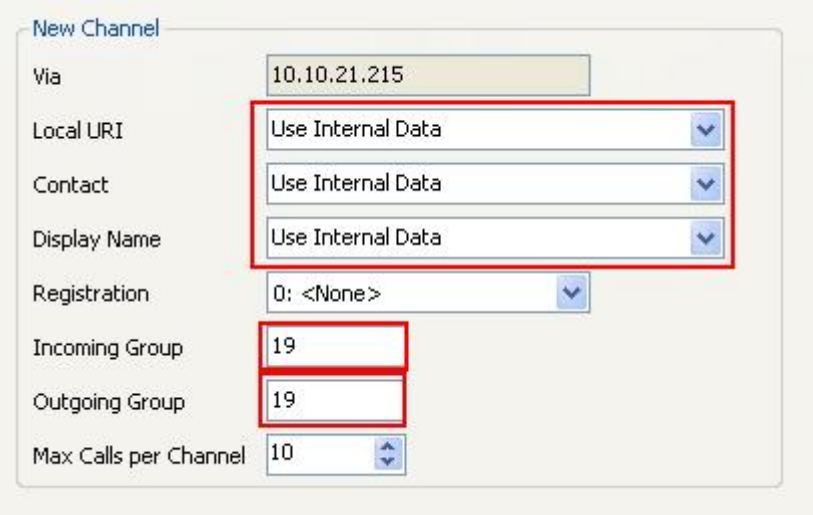
Retain default values for all other fields. Click **OK**(not shown).



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

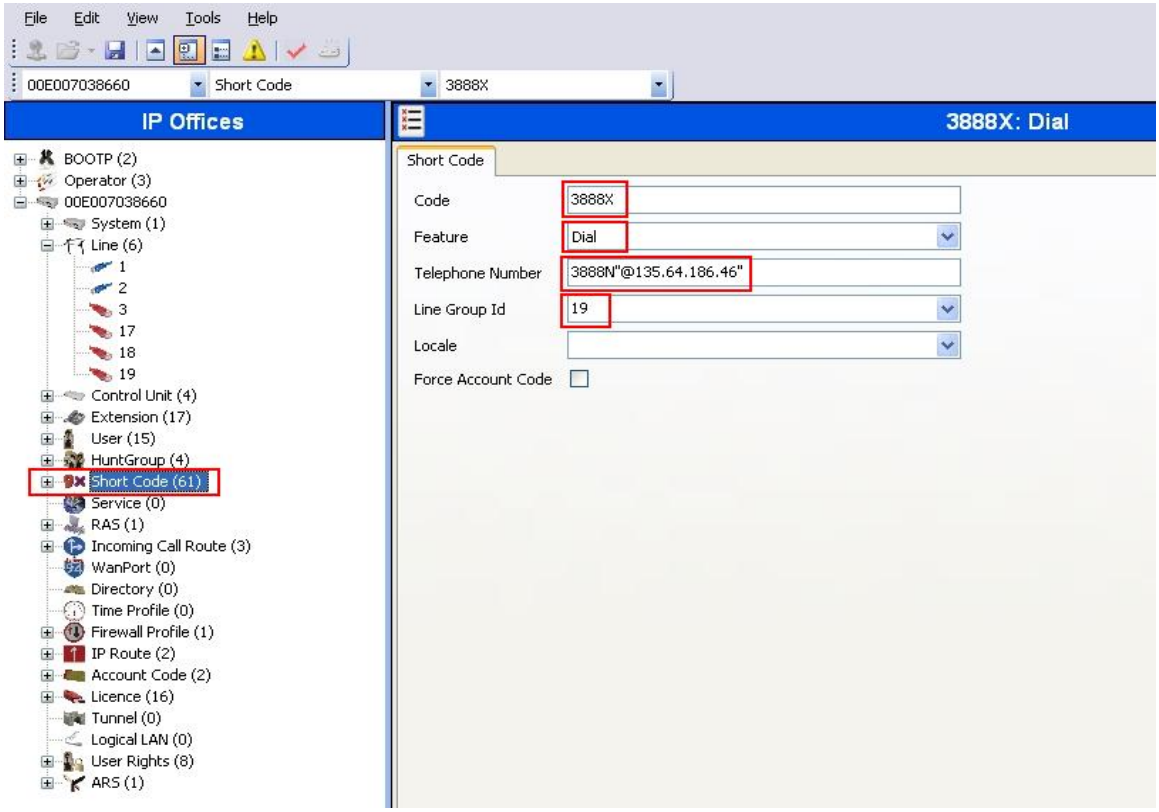
Retain default values for all other fields. Click **OK**(not shown).



5.7. Administer Short Code

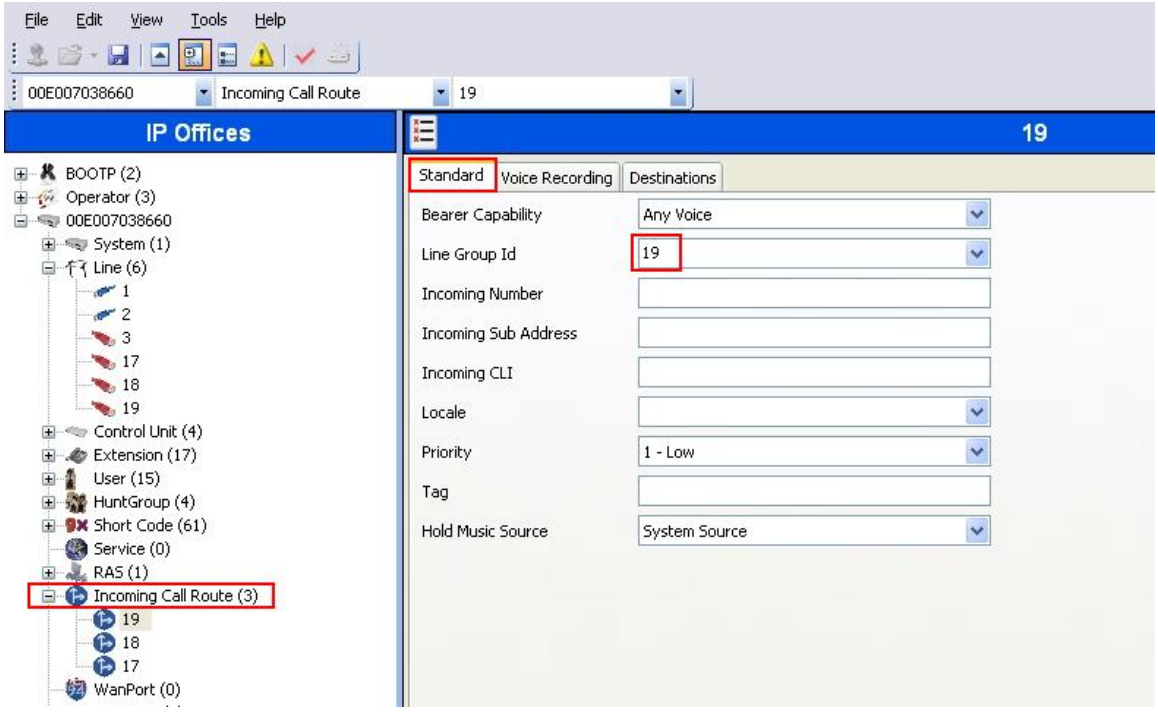
From the configuration tree in the left pane, right-click on **Short Code**, and select **New**. Enter the following details:

- **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**

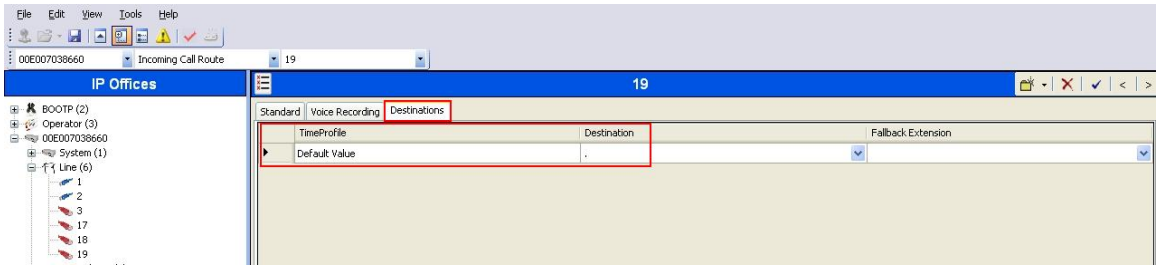


5.8. Configure Incoming Call Route

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**.

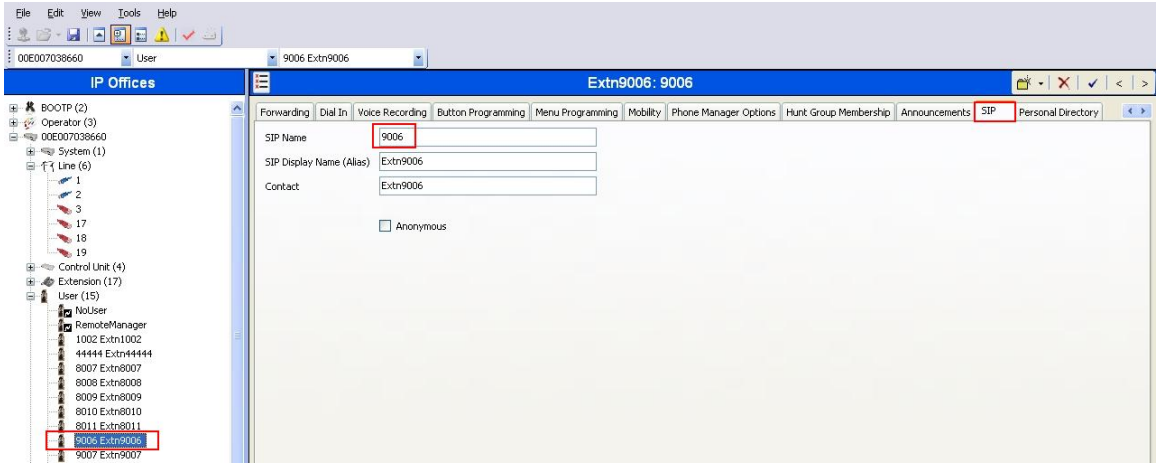


Select the **Destination** tab, enter **.** as the **Default Value**. This will enable all incoming calls to be routed to any extension.



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:

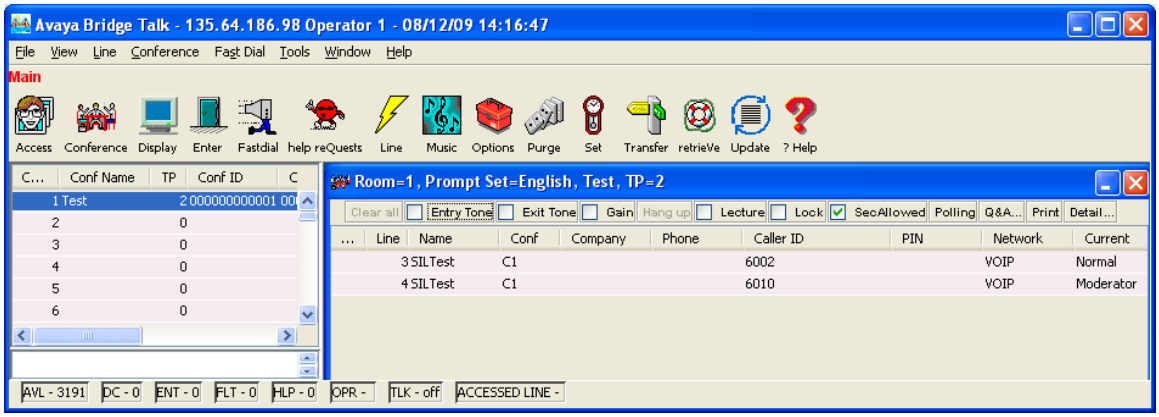
- Log in to the Meeting Exchange server console to access the CLI with the appropriate credentials.
- cd to **/usr/dcb/bin**
- At the command prompt, run the script **service mx-bridge status** and confirm all processes are running by verifying an associated 4-digit Process ID (PID) for each process.

```
[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

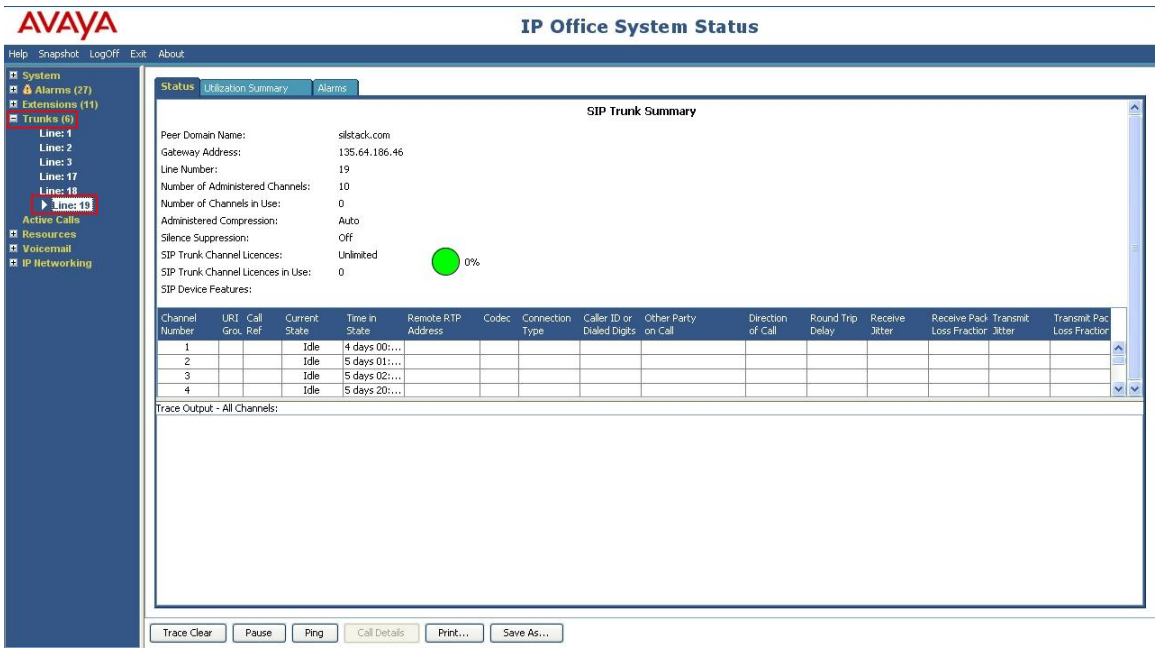
Verify end to end signalling/media connectivity between the Meeting Exchange and IP Office. This is accomplished by placing calls from the IP Office end points to the Meeting Exchange. This step utilizes the Avaya Bridge Talk application to verify calls to and from the Meeting Exchange are managed correctly, 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.



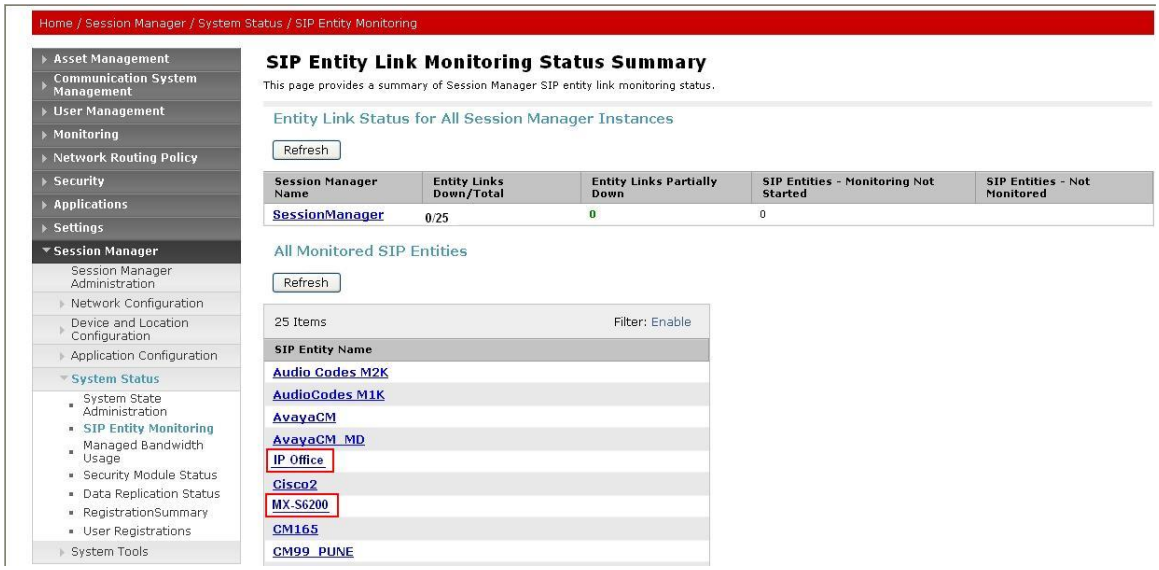
6.2. Verify Avaya IP Office

IP Office can be debugged with the System Status Application. Log into the IP Office Manager PC and select **Start → Programs → IP Office → System St**atus 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.

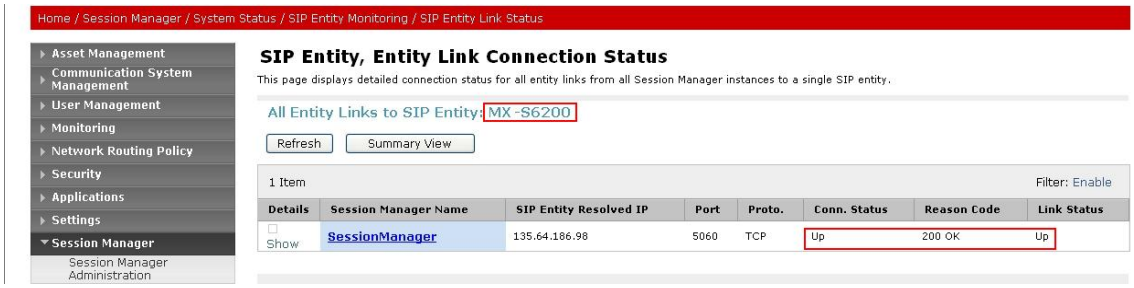


6.3. Verify Avaya Aura™ Session Manager

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.



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.



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 Aura™ Session Manager Overview, Doc # 03-603323, Issue 2

[4] Administering Avaya Aura™ Session Manager, Doc # 03-603324, Issue 2

[5] Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc # 03-603325, Issue 2

[6] Avaya IP Office Manager, Doc # 15-601011, Issue 2

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