Avaya Solution & Interoperability Test Lab

Application Notes for Empirix Hammer IP with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Endpoint Emulation with Secure SIP (SIPS) / Transport Layer Security (TLS) – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Empirix Hammer IP test system with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using Secure SIP (SIPS) with SIP endpoint emulation. Hammer IP validates IP-based systems by testing the actual network under anticipated traffic conditions to provide a complete understanding of expected performance. Hammer IP can be used to assess and monitor network performance, reliability and quality of VoIP services in an Avaya IP telephony network. In this configuration, Hammer IP emulates SIP endpoints that register with Avaya Aura® Session Manager and originates and terminates calls through Avaya SIP telephony network. In addition, this solution supports SIPS to secure the SIP signaling using TLS (Transport Layer Security) and Secure Real-time Transport Protocol (SRTP) to protect the RTP data. While the call is active, Hammer IP can send DTMF tones and voice media, and provide voice quality metrics. Call progress can also be monitored, and at the completion of the test, test reports can be generated. The Hammer IP provides a collection of applications used to configure the system; create, schedule, and monitor tests; and create reports.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1 Introduction

These Application Notes describe the configuration steps required to integrate the Empirix Hammer IP test system with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using Secure SIP (SIPS) with SIP endpoint emulation. Hammer IP validates IP-based systems by testing the actual network under anticipated traffic conditions to provide a complete understanding of expected performance. Hammer IP can be used to assess and monitor network performance, reliability and quality of VoIP services in an Avaya IP telephony network. In this configuration, Hammer IP emulates SIP endpoints that register with Avaya Aura® Session Manager and originates and terminates calls through Avaya SIP telephony network. In addition, this solution supports SIPS to secure the SIP signaling using TLS (Transport Layer Security) and Secure Real-time Transport Protocol (SRTP) to protect the RTP data. While the call is active, Hammer IP can send DTMF tones and voice media, and provide voice quality metrics. Call progress can also be monitored, and at the completion of the test, test reports can be generated. The Hammer IP provides a collection of applications used to configure the system; create, schedule, and monitor tests; and create reports.

The following set of Hammer IP applications were used during the compliance testing:

- **Hammer Configurator** used to configure and manage the system.
- **Hammer TestBuilder** used to create and run test scripts.
- **Hammer System Monitor** used to monitor SIP registration status and call progress.
- **Hammer Call Summary Monitor** used to monitor call completion and to create reports.

The following Application Notes are related to this solution.

- *Application Notes for Empirix Hammer IP with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunk Emulation with Secure SIP (SIPS) / Transport Layer Security (TLS)* **[4]**

2 General Test Approach and Test Results

Interoperability compliance testing covered feature and serviceability testing. The feature testing was conducted by originating and terminating calls using SIP endpoint channels on Hammer IP and establishing the calls through the Avaya SIP telephony network using SIPS/TLS and SRTP. The compliance test also covered monitoring various reports on the Hammer IP during and after the test runs, and checking the status of various SIP resources on Communication Manager. The serviceability testing focused on verifying the ability of the Hammer IP to recover from adverse conditions, such as disconnecting the Ethernet cable and rebooting the server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1 Interoperability Compliance Testing

The interoperability compliance testing focused on verifying that the Hammer IP can register with Avaya Aura® Session Manager as SIP endpoints, establish calls, send voice media, and provide voice quality metrics using SIPS/TLS and SRTP. The following features and functionality were covered:

- SIP endpoint registration with Avaya Aura® Session Manager using SIPS/TLS.
- Originating and terminating calls through Avaya SIP telephony network using SIPS/TLS and SRTP.
- Support of G.711mu-law and G.729 codecs.
- Support of direct IP-to-IP media (also known as "Shuffling" which allows IP endpoints to send audio RTP packets directly to each other without using media resources on the Avaya Media Gateway). Calls with Shuffling and IP Audio Hairpinning disabled were also verified.
- Generating voice quality metrics with Shuffling disabled.
- DTMF support.
- Originating calls from SIP endpoints and terminating calls on SIP endpoints and SIP trunks.

Note: Performance and load testing was not the focus of the compliance test.

2.2 Test Results

All test cases passed. Empirix Hammer IP was successful in originating calls using SIP endpoint emulation and terminating calls on channels emulating SIP endpoints and SIP trunks using SIPS/TLS and SRTP. Note that this solution does not currently support Direct IP-IP Media (i.e., Shuffling) with SIP trunks that use SIPS/TLS.

Important Note: The purpose of this compliance test was to verify interoperability between Empirix Hammer IP and Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP endpoint emulation using SIPS/TLS and SRTP. That is, the goal was to verify that Hammer IP can register SIP endpoints with Session Manager and establish calls. This was successfully verified. If a Hammer test encounters failed calls, there are various items to consider, including:

- The **Guard Time** and **Stagger** parameters may be set too aggressively (e.g., Hammer IP may be initiating too many calls too quickly) and the configuration under test may not be able to handle the load generated by Hammer IP. These parameters should be considered carefully for each test. It may be necessary to slow down the test to a rate that can be reasonably handled by the test configuration.

- Resources may be getting exhausted in the Avaya media gateway. These resources may include media processing resources, touch-tone receivers (TTRs), network trunks, and TDM bus resources.

Generally speaking, call failures encountered in Hammer IP are usually a result of one of the issues mentioned above.

2.3 Support

Technical support on the Empirix Hammer IP can be obtained via phone, website, or email.

- **Phone:** (978) 313-7002
- **Web:** http://www.empirix.com/support/maintenance.aspx
- **Email:** supportcontract@empirix.com

3 Reference Configuration

The network diagram shown in **Figure 1** illustrates the test configuration. In this configuration, Session Manager receives calls from Hammer IP, which emulates SIP endpoints. The call is routed through the Avaya SIP telephony network. The call is eventually routed back to the Hammer IP where it is terminated. SIP signaling is protected using SIPS/TLS and RTP data is protected using SRTP. While the call is established, the Hammer IP sends voice media (i.e., RTP traffic) using an audio recording. This allows voice quality metrics to be provided at the end of each call. The Hammer IP applications running on the Hammer IP server were used to configure the system, create and monitor the tests, and view the test reports.

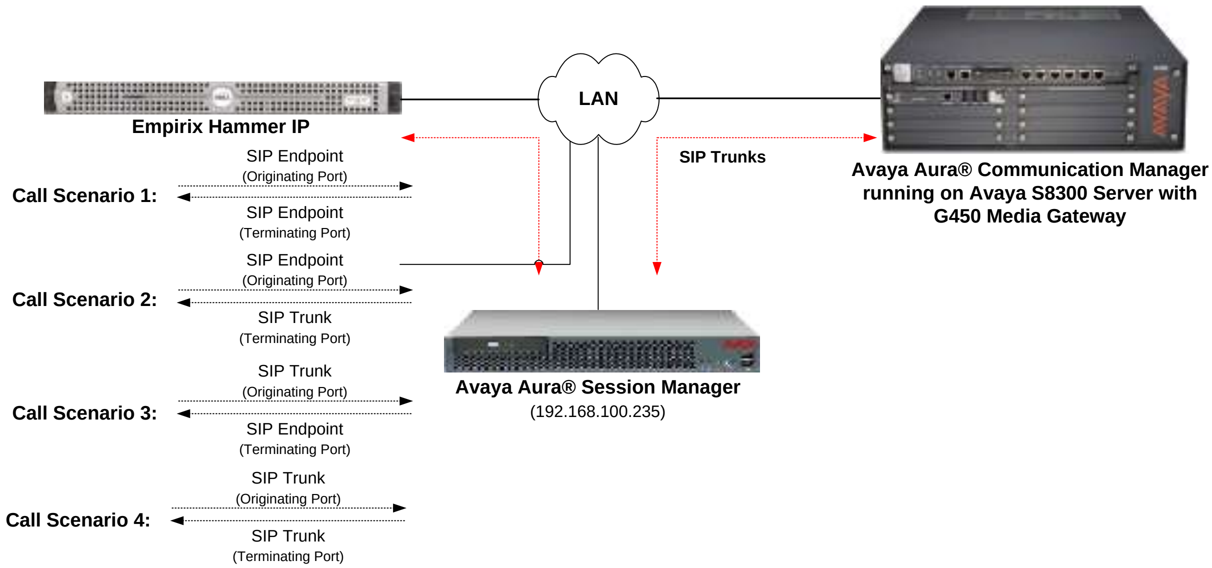


Figure 1: Empirix Hammer IP with Avaya SIP Telephony Network

4 Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager running on S8300 Server	6.3 SP 12 (R016x.03.0.124.0 with Patch 22505)
Avaya G450 Media Gateway	FW 36.12.0
Avaya Aura® System Manager	6.3.15 (Build No. 6.3.0.8.5682-6.3.8.5506 Software Update Revision No: 6.3.15.12.3972)
Avaya Aura® Session Manager running on an S8800 Server	6.3.15 (6.3.15.0.631503)
Empirix Hammer IP running on Microsoft Windows Server 2008 R2 with Dual 2.40 GHz Intel Xeon CPU and 12.0 GB of RAM	6.2.0.79

5 Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Administer IP Node Names
- Administer IP Codec Set
- Administer IP Network Region
- Administer SIP Trunk Group to Session Manager
- Administer SIP Stations
- Administer AAR Call Routing

Communication Manager is configured through the System Access Terminal (SAT).

5.1 Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for the S8300 Server in the G450 Media Gateway (*procr*) and Session Manager (*lz-asm*). The host names will be used in other configuration screens of Communication Manager.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
devcon13            10.32.24.20
lz-asm              192.168.100.235
procr               192.168.100.10
procr6              ::

( 5  of 5    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.2 Administer IP Codec Set

In the **IP Codec Set** form, specify the audio codec(s) required by the test that will be run on the Hammer IP. The form is accessed via the **change ip-codec-set 1** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, G.711MU, G.729AB, and G.729A codecs were used. In the IP codec set form, specify the appropriate codec being used by the Hammer test. If SRTP is required for the test, set **Media Encryption** to *1-srtp-aescm128-hmac80* as shown below. This is the media encryption supported by Hammer IP. Below is the IP codec set configured for G.711 mu-law and SRTP.

```
change ip-codec-set 1                                           Page   1 of   2

                          IP Codec Set
    Codec Set: 1

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU            n         2        20
 2:
 3:
 4:
 5:
 6:
 7:

     Media Encryption
 1: none
 2: 1-srtp-aescm128—hmac80
 3:
```

5.3 Administer IP Network Region

In the **IP Network Region** form, specify the codec set to be used for Hammer calls and specify whether **IP-IP Direct Audio** (Shuffling) is required for the test. Shuffling allows audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway. Note that if Shuffling is enabled, audio traffic does not egress the Hammer IP since the calls would be shuffled. The **Authoritative Domain** for this configuration is *devcon.com*.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: devcon.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                   RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.4 Administer SIP Trunk to Session Manager

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*. See **Section 7** for instructions on managing TLS certificates.
- The **Enforce SIPS URI for SRTP** field may be enabled if SIPS should be enforced when SRTP is being used.
- Specify the S8300 and the Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form.
- Ensure that the TCP port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *devcon.com*.
- The **Direct IP-IP Audio Connections** field was disabled on this form.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

```
add signaling-group 60                                        Page   1 of   3
                                SIGNALING GROUP

 Group Number: 60             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                  Far-end Node Name: lz-asm
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: devcon.com
                                           Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload          Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                   IP Audio Hairpinning? n
         Enable Layer 3 Test? y
                                                Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to Hammer IP. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```
add trunk-group 60                                                   Page   1 of  21
                                TRUNK GROUP

Group Number: 60                   Group Type: sip            CDR Reports: y
  Group Name: To lz-asm                   COR: 1        TN: 1        TAC: 1060
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 60
                                                   Number of Members: 40
```

5.5 Administer SIP Stations

Configure a SIP station for each SIP channel on the Hammer IP. Set the **Type** field to either *9620SIP* or *9630SIP*. Set the **Port** field to *IP* and configure a descriptive **Name**. For the compliance test, 20 SIP stations were used with extensions ranging from 46101 to 46120. The first group of 10 channels (extensions 46101 to 46110) were used to originate calls. The calls were then terminated on the remaining 10 channels (extensions 46111 to 46120). Repeat this procedure for each channel required by the Hammer test. The SIP station was configured automatically by System Manager as described in **Section 6.7**.

```
display station 46101                                                    Page   1 of   6
                                     STATION

Extension: 46101                         Lock Messages? n               BCC: 0
     Type: 9620SIP                       Security Code:                  TN: 1
     Port: S00000                      Coverage Path 1:                 COR: 1
     Name: Hammer, SIP                 Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19
                                                 Message Lamp Ext: 46101

        Display Language: english

          Survivable COR: internal
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                                         IP Video? n
```

Configure the **Stations with Off-PBX Telephone Integration** form so that calls destined for a SIP endpoint on the Hammer IP are routed to Session Manager, which will then route the call to the Hammer IP. On this form, specify the extension of the SIP endpoint and set the **Application** field to *OPS*. The **Phone Number** field is set to the digits to be sent over the SIP trunk. In this case, the SIP telephone extensions configured on Session Manager also match the extensions of the corresponding stations on Communication Manager. However, this is not a requirement. Finally, the **Trunk Selection** field is set to *aar*. This field specifies Auto Alternate Routing (AAR) routing. In this case, the **Trunk Selection** field would be set to *aar* to trigger AAR routing. Configuration of the **AAR Analysis** and **Route Pattern** forms would also be required. Refer to **[1]** for information on routing calls using AAR or ARS. Repeat this step for each SIP endpoint required on the Hammer IP (e.g., extensions 46101 to 46120).

```
change off-pbx-telephone station-mapping 46101                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 46101            OPS          -      46101            aar        1
```

5.6 Administer AAR Call Routing

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and enter add an entry that routes digits beginning with "46" to route pattern 60 as shown below.

```
change aar analysis 4                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    46                    5    5     60       aar          n
    5                     7    7     254      aar          n
    6                     5    5     2        aar          n
    7                     5    5     3        aar          n
```

Configure a preference in **Route Pattern** 60 to route calls over SIP trunk group 60 as shown below.

```
change route-pattern 60                                         Page   1 of   3
                    Pattern Number: 60  Pattern Name: To lz-asm
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 60   0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user
```

6 Configure Avaya Aura® Session Manager

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

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities corresponding to Session Manager and Communication Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Application Sequence
- Define Communication Manager as Administrable Entity (i.e., Managed Element)
- Add SIP Users
- Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

6.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **Domains** on the left and clicking the **New** button on the right (not shown). The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., *devcon.com*).
- **Type:** Set to *SIP*.
- **Notes:** Descriptive text (optional).

Click **Commit**.

Since the sample configuration does not deal with any other domains, no additional domains need to be added.

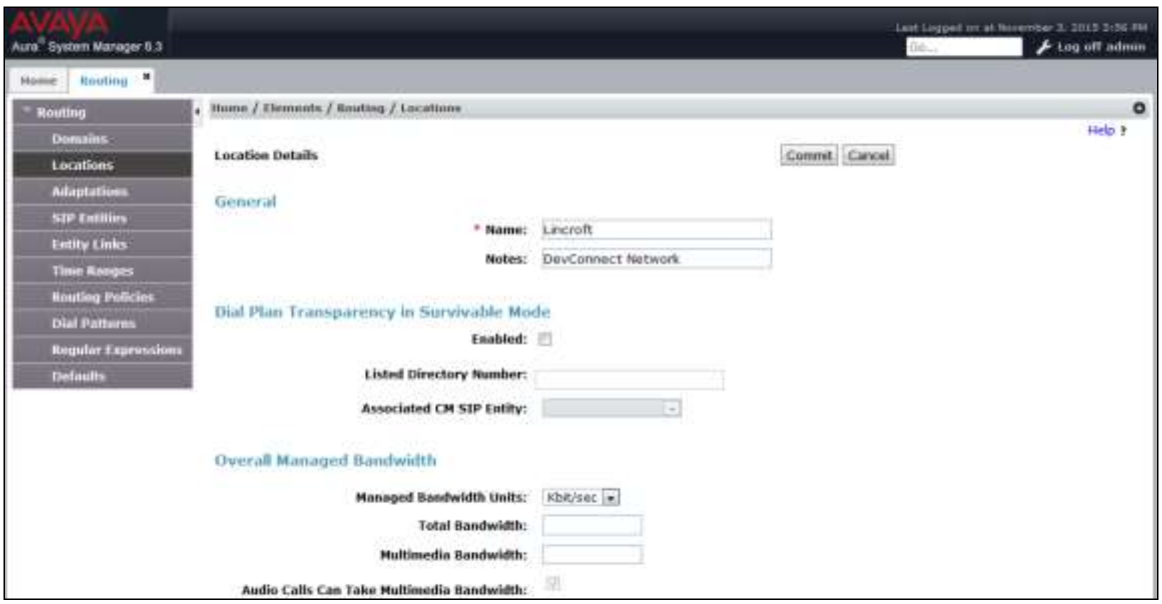
6.2 Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

Under *General*:

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

The screen below shows addition of the *Lincroft* location, which includes Avaya Aura® Communication Manager and Avaya Aura® Session Manager.



Under *Location Pattern*:

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

Click **Commit** to save the **Location** definition.

6.3 Add SIP Entities

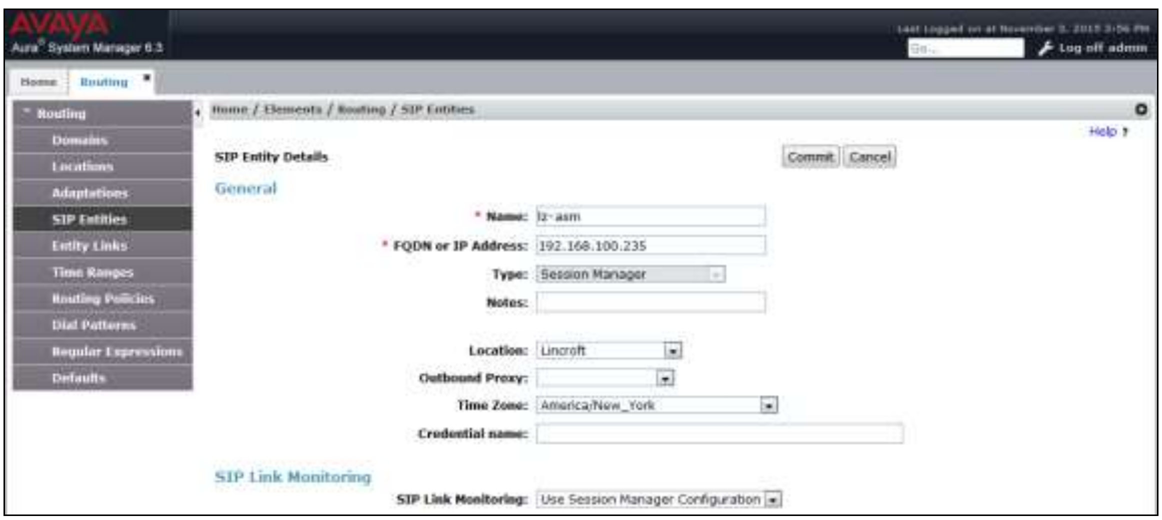
In the sample configuration, a SIP Entity is added for Session Manager and the S8300 Server in the G450 Media Gateway.

6.3.1 Avaya Aura® Session Manager

A SIP Entity must be added for Session Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Session Manager.
- **Type:** Select *Session Manager*.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.



Under *Port*, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain** The domain used for the enterprise (e.g., *devcon.com*).

Defaults can be used for the remaining fields. Click **Commit** (not shown) to save the SIP Entity definition.

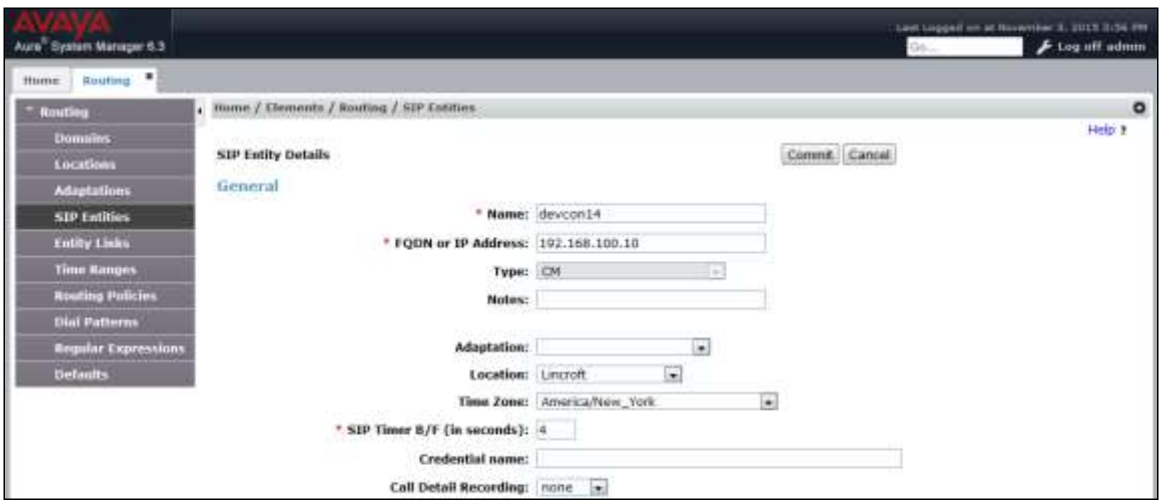
6.3.2 Avaya Aura® Communication Manager

A SIP Entity must be added for the Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., S8300 Server) on the telephony system.
- **Type:** Select *CM*.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

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



6.4 Add Entity Link

The SIP trunk from Session Manager to Communication Manager is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name (e.g., *lz-asm to devcon14*).
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the appropriate protocol.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of Communication Manager.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Select *Trusted*. *Note: If Trusted is not selected, calls from the associated SIP Entity specified in **Section 6.3.2** will be denied.*

Click **Commit** to save the Entity Link definition.

Note: See **Section 7** for instructions on managing TLS certificates.

6.5 Define Communication Manager as Managed Element

Before adding SIP users, Communication Manager must be added to System Manager as a managed element. This action allows System Manager to access Communication Manager over its administration interface. Using this administration interface, System Manager will notify Communication Manager when new SIP users are added.

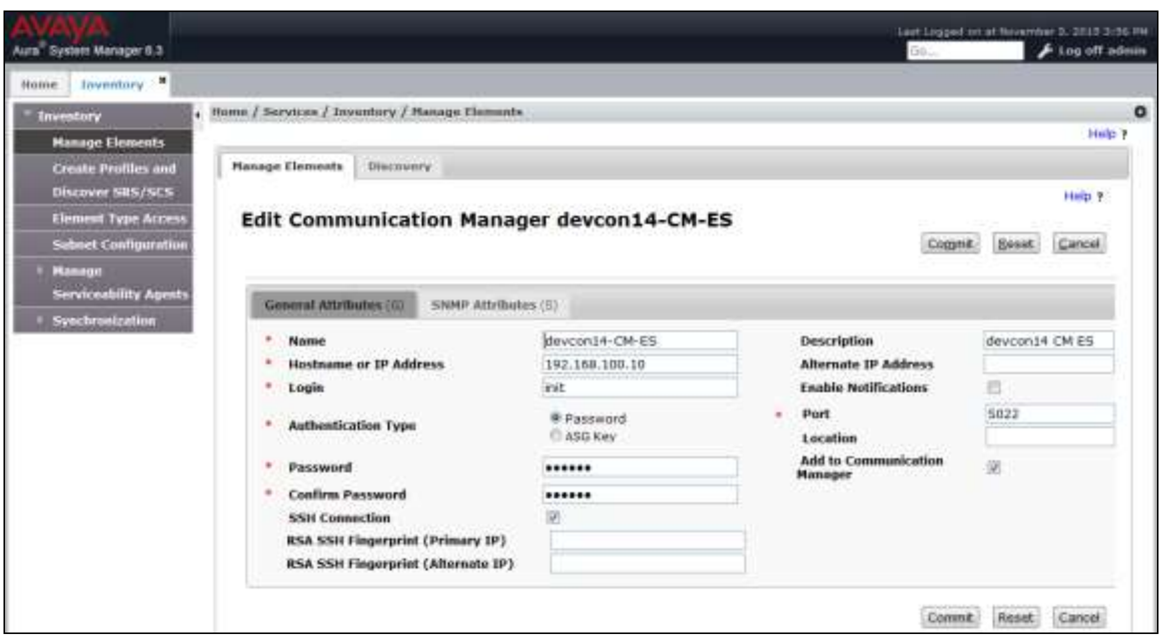
To define Communication Manager as a managed element, select **Services→Inventory→Manage Elements** on the left and click on the **New** button (not shown) on the right. In the **Application Type** field that is displayed, select *CM*.

In the **New CM Instance** screen, first select Communication Manager as the Type (not shown), and then fill in the following fields as follows:

Under *General Attributes*:

▪ **Name:**	Enter an identifier for Communication Manager.
▪ **Hostname or IP Address:**	Enter the IP address of the administration interface for Communication Manager.
▪ **Login / Password:**	Enter the login and password used for administration access.
▪ **Authentication Type:**	Select Password.
▪ **SSH Connection:**	Select checkbox.
▪ **Port:**	Enter the port number for SSH administration access (5022).

Defaults can be used for the remaining fields. Click **Commit** to save the settings.

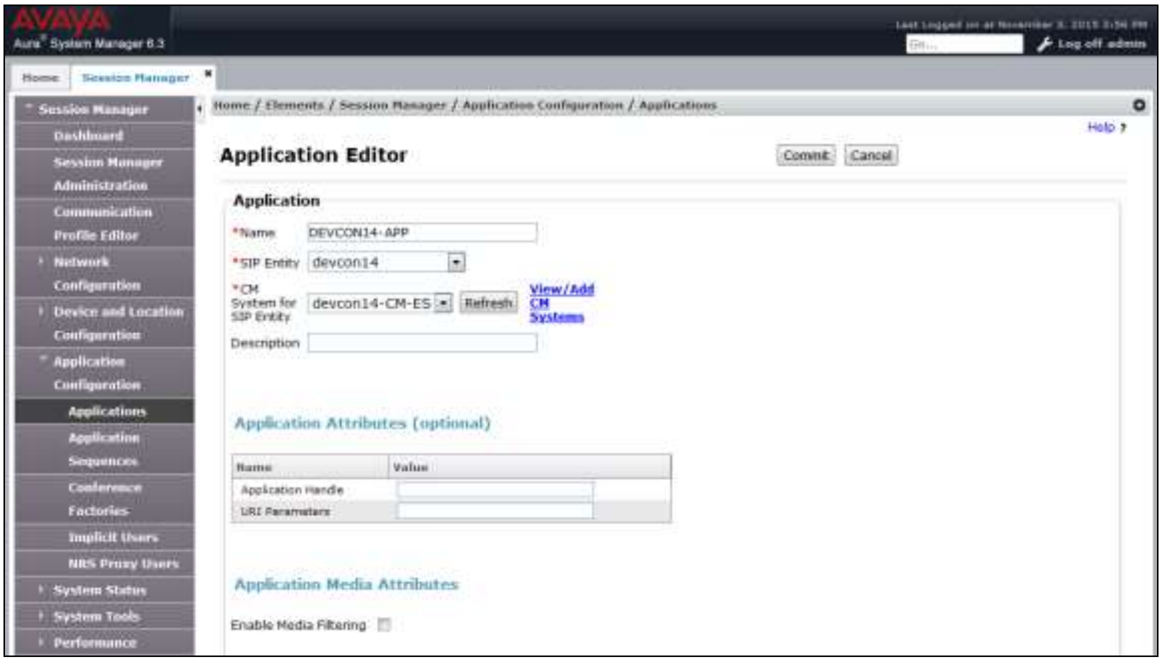


6.6 Add Application Sequence

To define an application for Communication Manager, navigate to **Elements → Session Manager → Application Configuration → Applications** on the left and select **New** button (not shown) on the right. Fill in the following fields:

- **Name:** Enter name for application.
- **SIP Entity:** Select the Communication Manager SIP entity.
- **CM System for SIP Entity** Select the Communication Manager managed element.

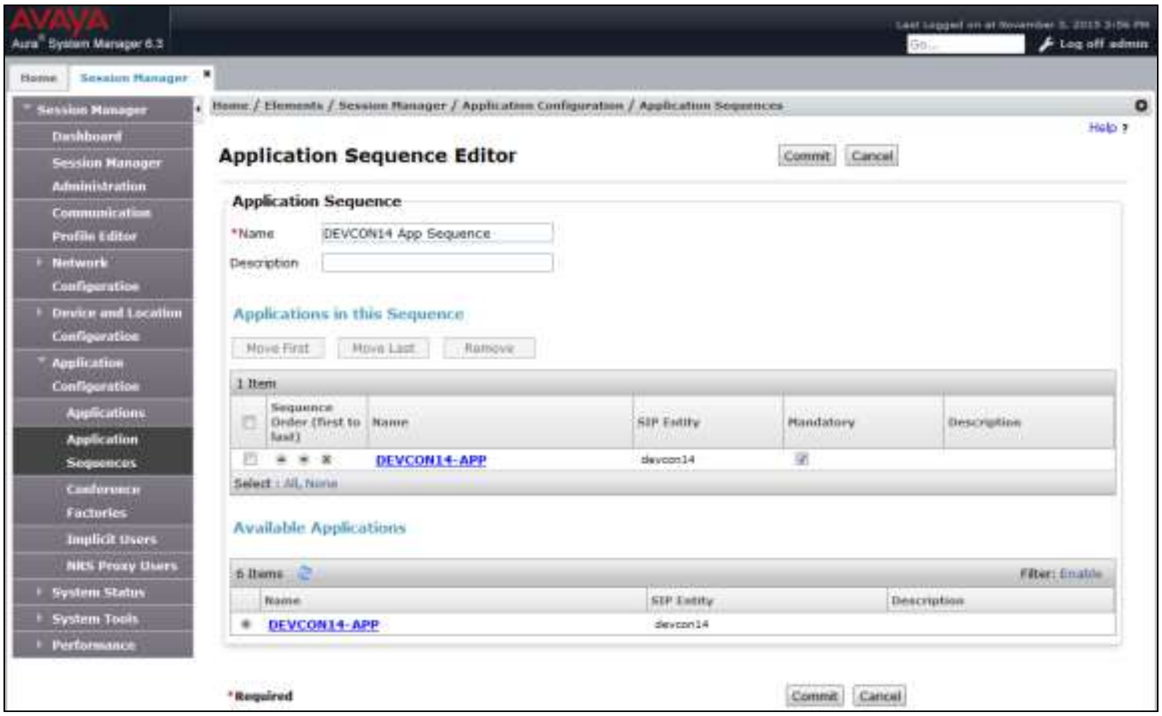
Click **Commit** to save the Application definition.



Next, define the Application Sequence for Communication Manager as shown below.

Verify a new entry is added to the **Applications in this Sequence** table and the **Mandatory** column is ☑ as shown below.

Note: The Application Sequence defined for Communication Manager Evolution Server can only contain a single Application.



6.7 Add SIP Users

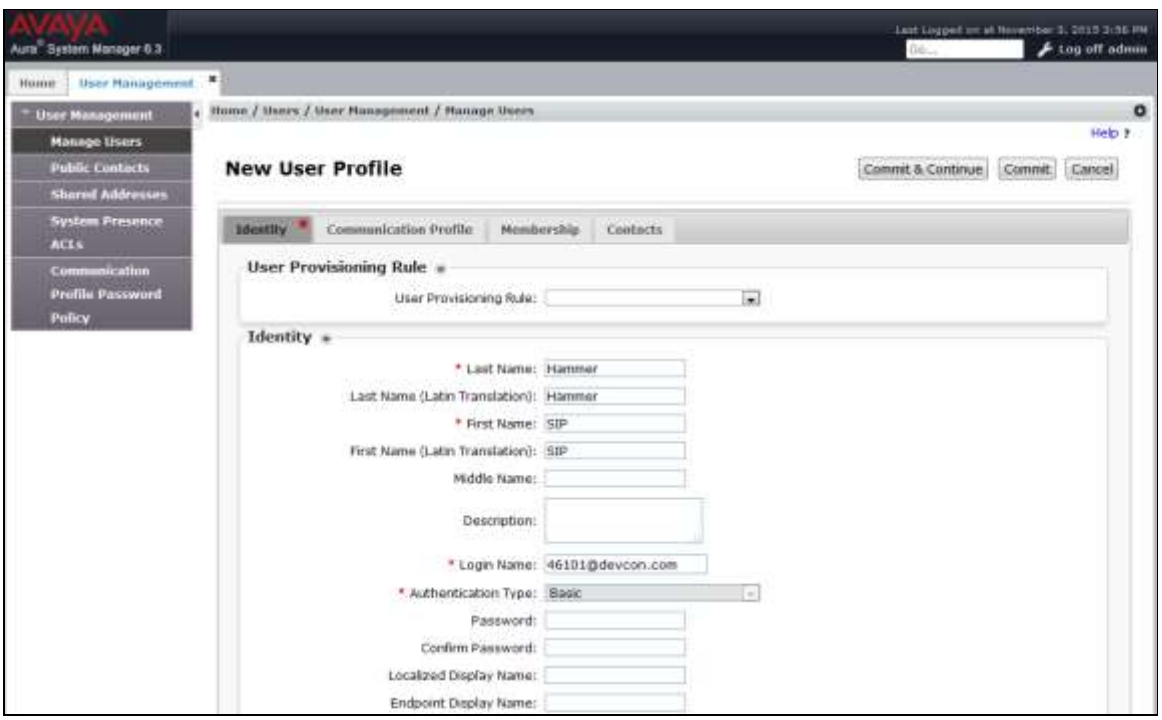
Add a SIP user for each SIP endpoint channel on Hammer IP as defined in **Section 5.5.** Alternatively, use the option to automatically generate the SIP stations on Communication Manager Evolution Server when adding a new SIP user.

To add new SIP users, expand **Users** and select **Manage Users** from left and select **New** button (not shown) on the right.

Enter values for the following required attributes for a new SIP user in the **Identity** section of the new user form.

- **Last Name:** Enter the last name of the user.
- **First Name:** Enter the first name of the user.
- **Login Name:** Enter *<extension>@<sip domain>* of the user (e.g., *46101@devcon.com*).
- **Authentication Type:** Select *Basic*.

The screen below shows the information when adding a new SIP user to the sample configuration.



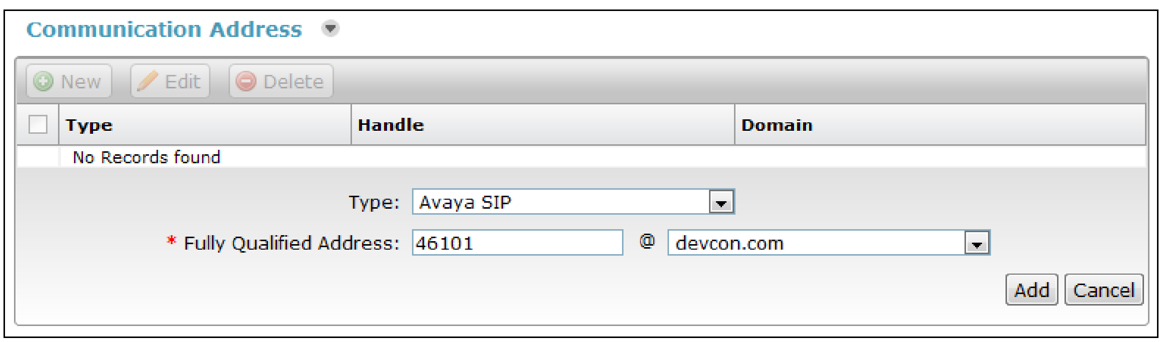
Select the **Communication Profile** tab and configure the following fields:

- **Communication Profile Password:** Enter the password which will used by Hammer IP to log into Session Manager.
- **Confirm Password:** Re-enter the password from above.

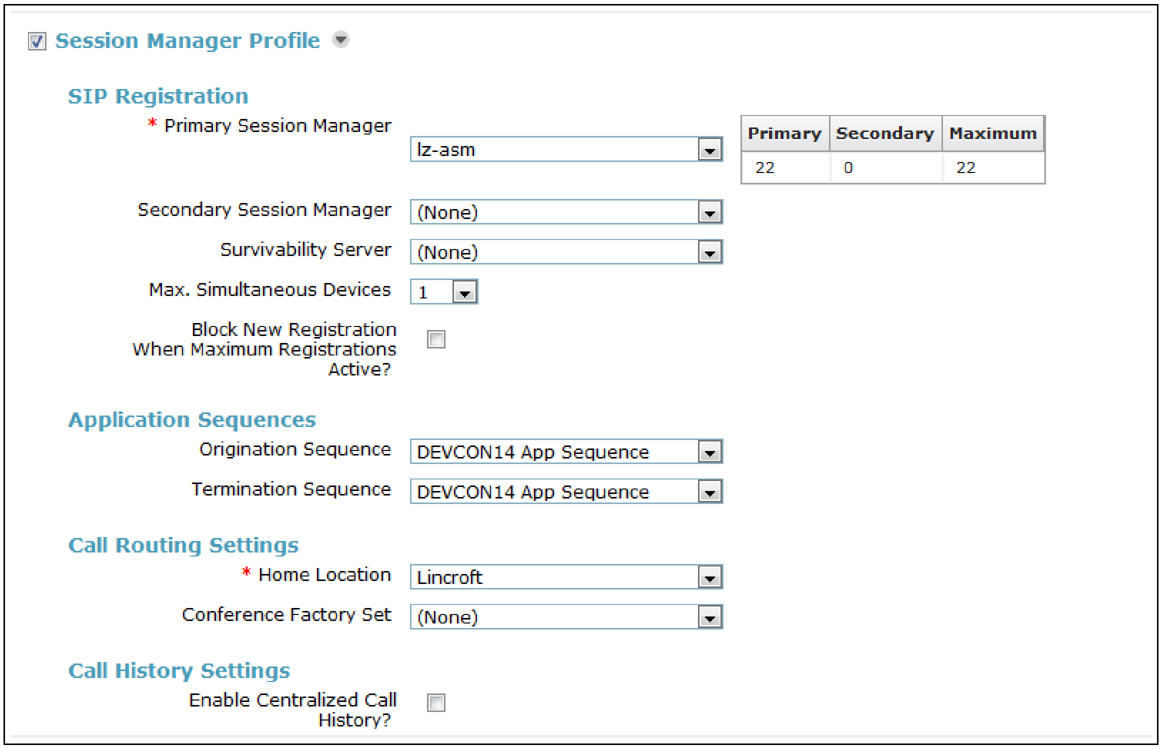
Click **New** to define a **Communication Address** for the new SIP user. Enter values for the following required fields:

- **Type:** Select *Avaya SIP*.
- **Fully Qualified Address:** Enter extension number and select SIP domain.

The screen below shows the information when adding a new SIP user to the sample configuration. Click **Add**.



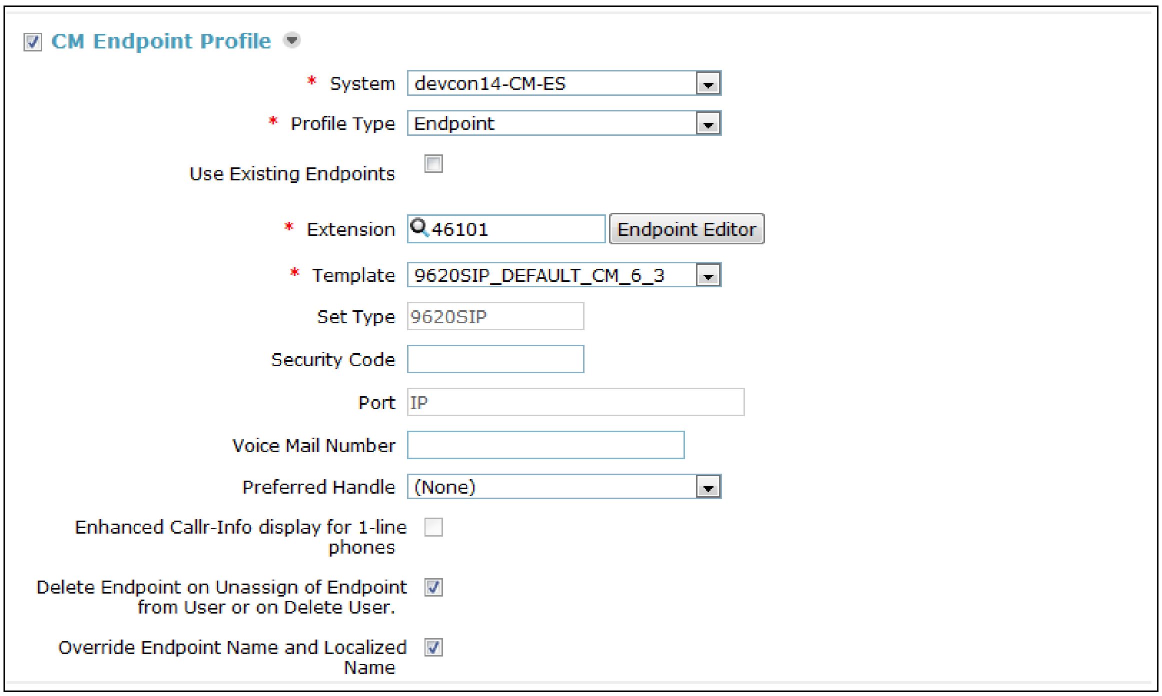
In the *Session Manager Profile* section, specify the Session Manager entity from **Section 6.3.1** for **Primary Session Manager** and assign the **Application Sequence** defined in **Section 6.6** to both the originating and terminating sequence fields. Set the **Home Location** field to the **Location** configured in **Section 6.2**.



In the **CM Endpoint Profile** section, fill in the following fields:

- **System:** Select the managed element corresponding to Communication Manager.
- **Profile Type:** Select *Endpoint*.
- **Use Existing Stations:** If field is not selected, the station will automatically be added in Communication Manager.
- **Extension:** Enter extension number of SIP user.
- **Template:** Select template for 9620 or 9630 SIP phone.
- **Port:** Enter *IP*.

The screen below shows the information when adding a new SIP user to the sample configuration. Click **Commit** (not shown) to add the SIP user.



6.8 Add 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** (not shown), and fill in the fields as described below and shown in the following screen:

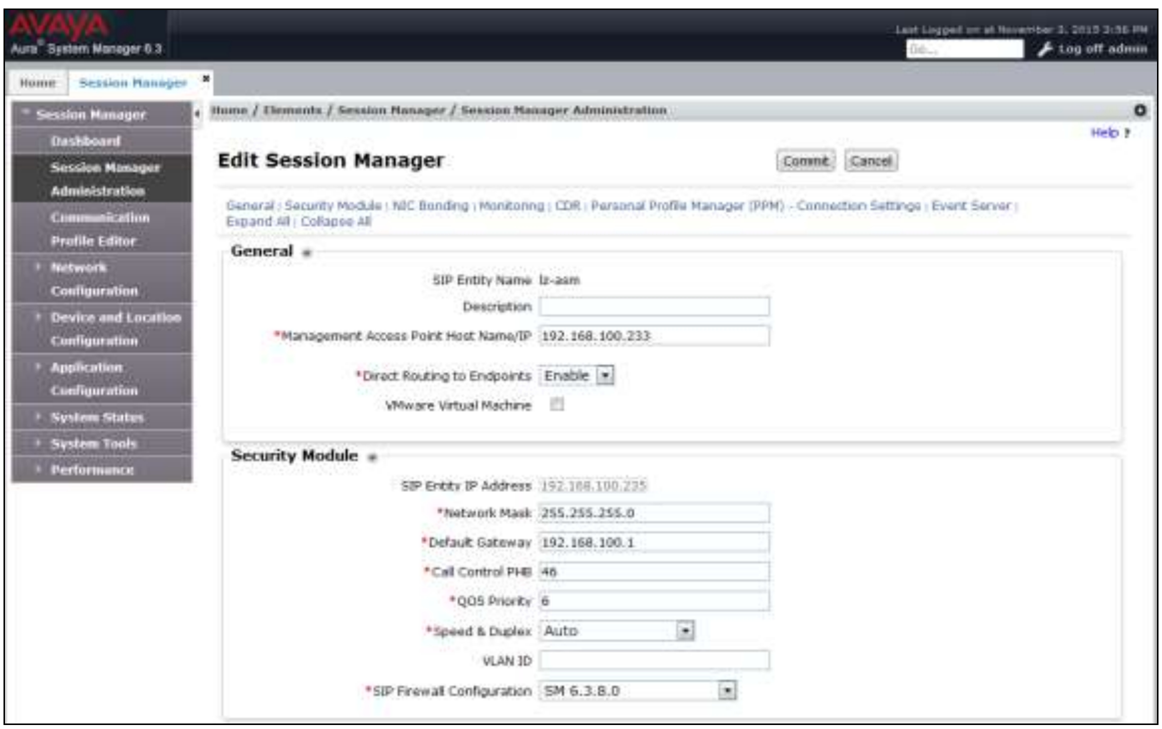
Under *General*:

- **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.



7 Managing and Creating TLS Certificates

This section covers how to manage and create the TLS certificates required to support TLS over SIP trunks between Communication Manager and Session Manager and to support TLS for the emulated SIP endpoints in Hammer IP. For this solution, Avaya Aura® System Manager is used as a certificate authority. For additional information on managing TLS certificates, refer to **[2].** The steps are required include:

- Export the System Manager CA Certificate
- Add the System Manager CA to Communication Manager
- Install Enhanced Validation Certificates for Session Manager
- Create TLS Certificate and Private Key for Hammer IP

7.1 Export the System Manager CA Certificate

To export the System Manager CA, follow these steps:

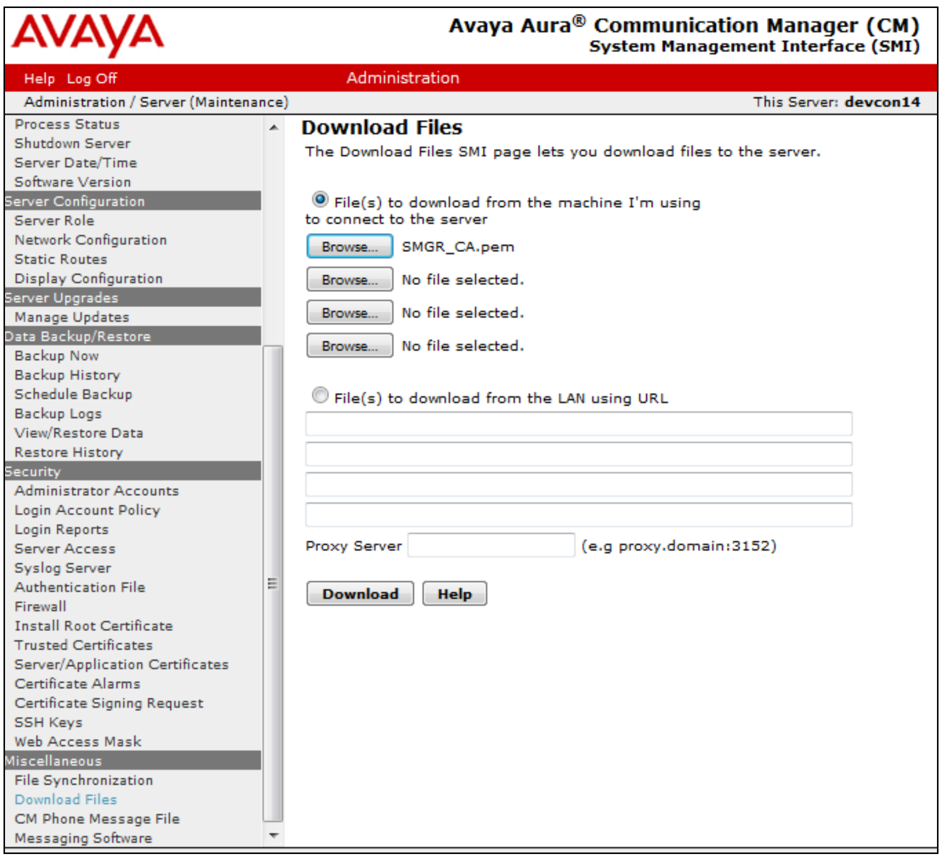
1. On the home page of the System Manager Web Console, under **Services**, select **Security→Certificates→Authority**.
2. On the CA Functions page, click **Download pem file**.

3. Save the file. In this example, the filename was `SMGR_CA.pem`.

7.2 Add the System Manager CA to Communication Manager

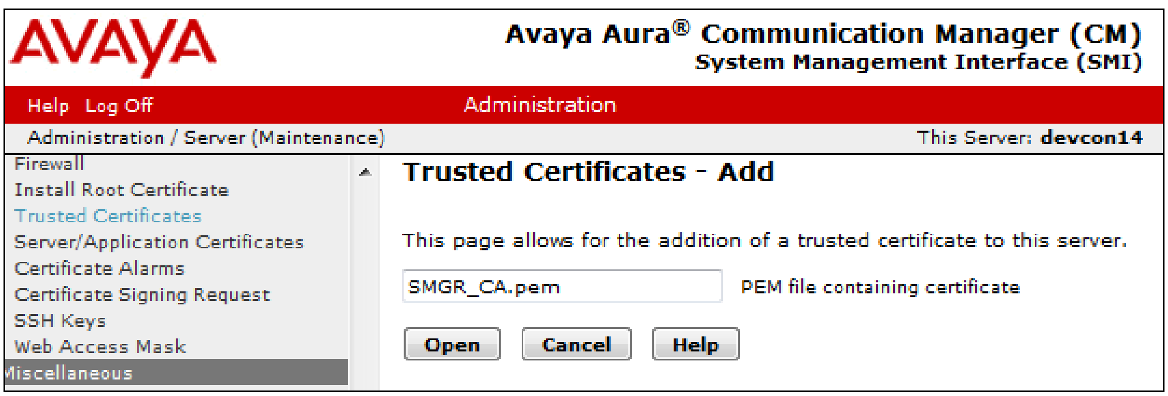
Use the following procedure to make Communication Manager trust the System Manager CA certificate.

1. Verify the System Manager CA certificate downloaded in **Section 7.1** can be accessed.
2. Log into the Communication Manager server web interface.
3. Click **Administration** and select **Service (Maintenance)**.
4. In the left pane, under **Miscellaneous**, click **Download Files**.
5. Select **File(s) to download from the machine I'm using to connect to the server** and click **Browse**.
6. Select the System Manager CA certificate to download as shown below and click **Download**.



7. In the left pane, under **Security**, click **Trusted Certificates** and click **Add**.

8. Enter the name of the downloaded System Manager CA certificate as shown below and click **Open**.



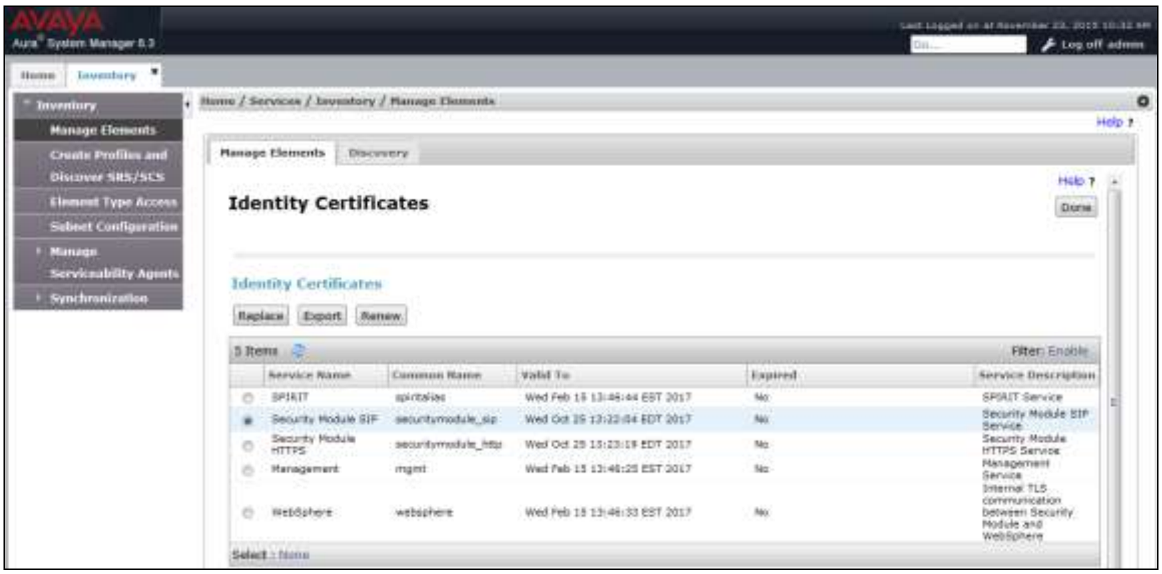
9. Enter the file name again in the text box and select the Communication Manager checkbox as shown below and click **Add**.

10. Restart Communication Manager.

7.3 Install Enhanced Validation Certificates for Session Manager

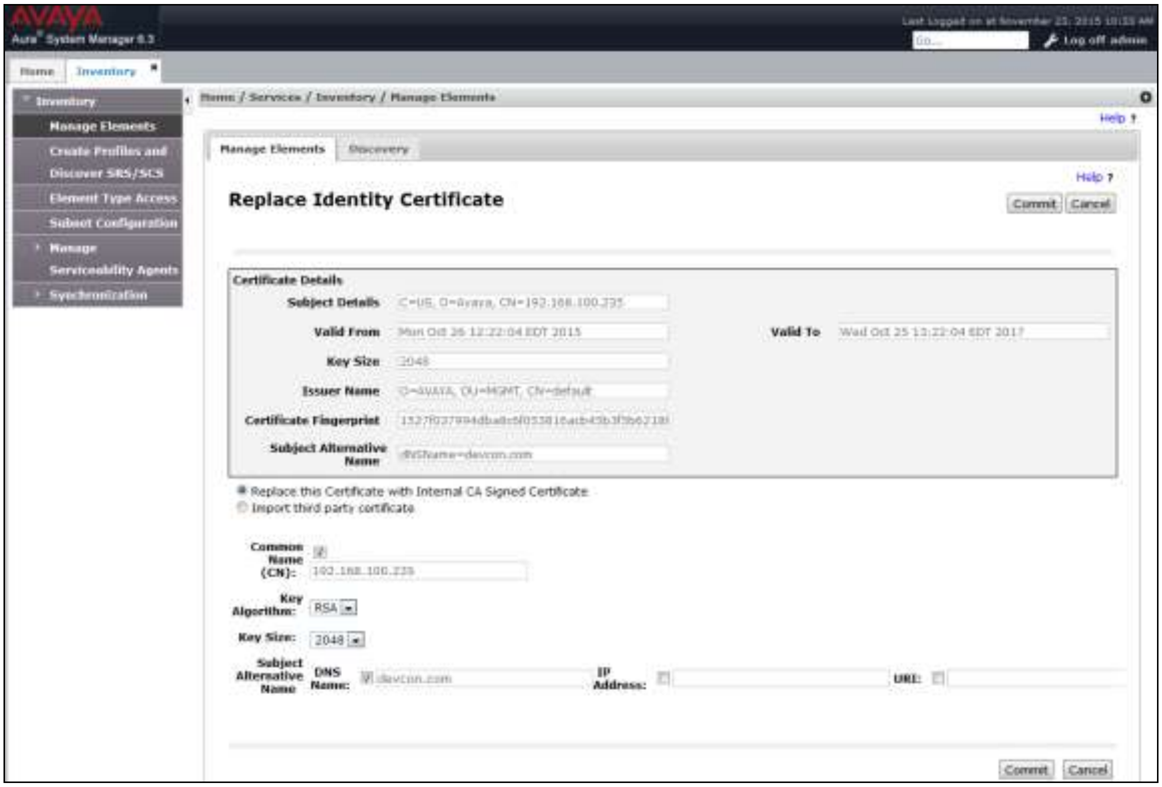
Perform this procedure to populate the **Common Name** and **Subject Alternate Name** of the certificate in Session Manager.

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory→Manage Elements**.
2. Select the appropriate Session Manager Web Console from the list and click **More Actions**.
3. Select **Configure Identity Certificates** from the drop-down menu.
4. On the **Identity Certificates** page, select **Security Module SIP** and click **Replace**.



5. On the **Replace Identity Certificate** page, select **Replace this Certificate with Internal CA Signed Certificate**.
6. Select the **Common Name (CN)** checkbox and enter the host name or IP address of the Security Module. The address is the same as the SIP Entity address.
7. Select **RSA** for the **Key Algorithm**.
8. Select **2048** as the **Key Size**.

9. Select the **DNS Name** checkbox and enter the SIP domain (e.g., *devcon.com*) and click **Commit**.



10. On the **Identity Certificate** page, select **Security Module HTTP** and click **Replace**. The following steps are similar to the ones covered for **Security Module SIP** above.
11. On the **Replace Identity Certificate** page, select **Replace this Certificate with Internal CA Signed Certificate**.
12. Select the **Common Name (CN)** checkbox and enter the host name or IP address of the Security Module. The address is the same as the SIP Entity address.
13. Select **RSA** for the **Key Algorithm**.
14. Select **2048** as the **Key Size**.
15. Select the **DNS Name** checkbox and enter the SIP domain (e.g., *devcon.com*) and click **Commit**.
16. Click **Commit**.

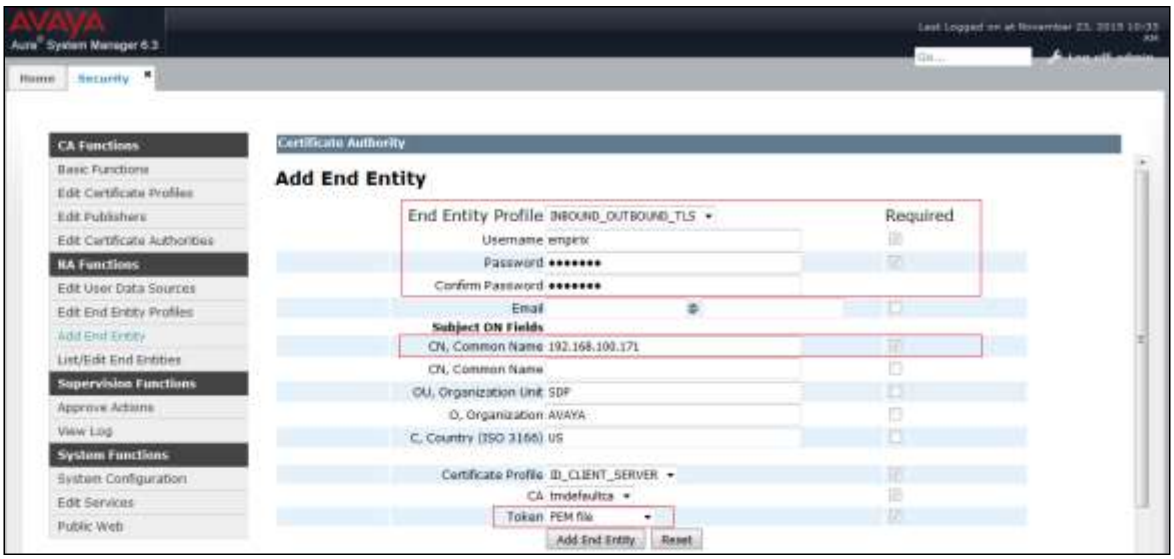
7.4 Create TLS Certificate and Private Key for Hammer IP

This section covers the procedures for creating TLS Certificate and Private Key files for Hammer IP. Refer to **[2]** for more information on creating TLS Certificate and Private Key files.

7.4.1 Create Avaya Private Key Certificates

Follow the following procedure to add Hammer IP as an end entity.

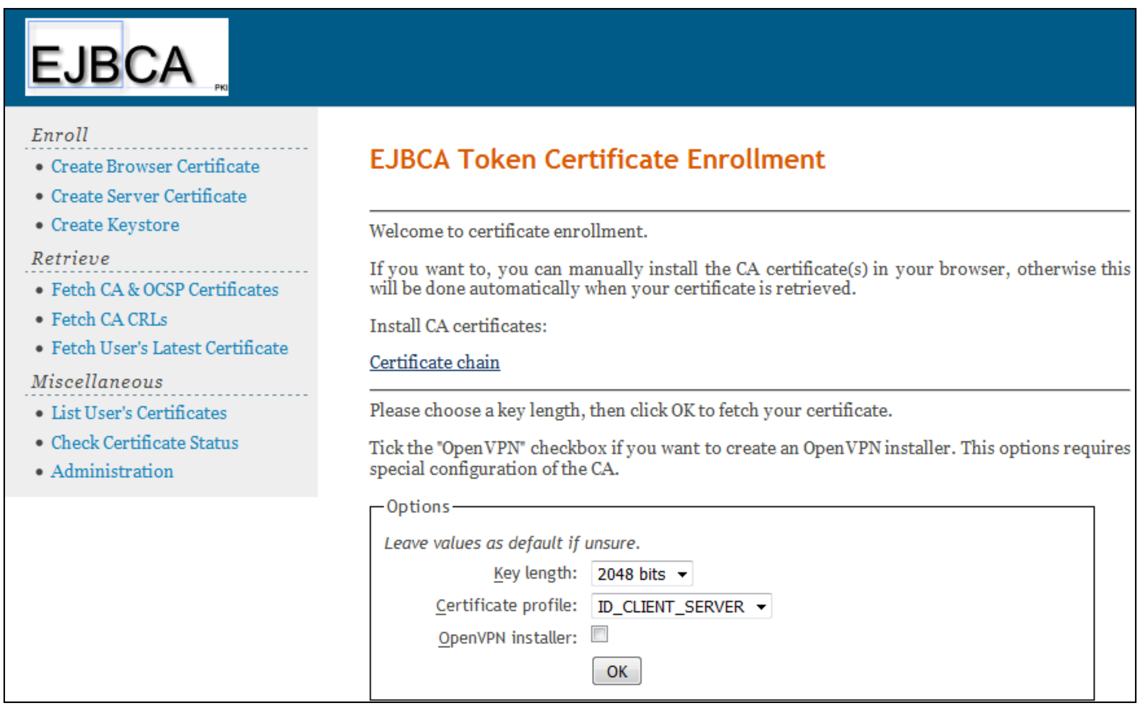
1. Create **End Entity** for Hammer IP. From the System Manager home page, navigate to **Security→Certificates→Authority→RA Functions** and select **Add End Entity**.
2. Enter the following values and use the default values for the remaining fields. For the **CN, Common Name** field, any IP address associated with Hammer IP may be used. Click **Add End Entity** to submit.



3. Navigate to **Security→Certificates→Authority→Public Web**. The EJBCA window is displayed.
4. Click on **Create Keystore**.

5. Under the **Authentication** section, enter the user name and password that were defined in Step 2, and then click OK.

6. In the **Options** section of the **EJBCA Token Certificate Enrollment** page, select *2048 bits* for the **Key length** field and click **OK** to continue.



7. In the next window, click **Save** to save to the file to the local PC. This file will contain a Private Key, Server Certificate, and Trusted Root Certificate.

7.4.2 Create TLS Certificates and Private Key Files for Hammer IP

The following procedure describes how to create a TLS Certificate and TLS Private Key file for Hammer IP.

1. Using a Text Editor, open the Private Key Certificate file created in the previous section.

```
Bag Attributes
    friendlyName: 192.168.100.170
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDKDk9O2J/fwk/c
A7sPM+fFZ7JKQrjyXa8Yye3vQwJLUMptlMgmDP+LuJhDKicxBFpkqS2yhP7xGIO3
                  . . .
NIPZmEhDPRBQfGeY27pq1H+kcv+GsV+ogMn+r2IQ/tiYNkBhLGCRkq+f2VVQ+4R6
7zJI2WvYqRVjc/Hv8z6wH3mu+8aI3E/6Z6wmJuKJelvuWK0i/7gLZqhBFXqhCPHl
LRvylJQkVjBnZqoDeEFmr+o7
-----END PRIVATE KEY-----
Bag Attributes
    friendlyName: 192.168.100.170
subject=/CN=192.168.100.170/OU=SDP/O=AVAYA/C=US
issuer=/CN=default/OU=MGMT/O=AVAYA
-----BEGIN CERTIFICATE-----
MIIC9jCCAl+gAwIBAgIIL67fE/hqP0AwDQYJKoZIhvcNAQELBQAwMTEQMA4GA1UE
AwwHZGVmYXVsdDENMAsGA1UECwwETUdNVDEOMAwGA1UECgwFQVZBWUEwHhcNMTUx
                  . . .
+vIRd58OoxvZvdltMjw1M17GPf6xNrGGnxPpjKQ29kRC1hfxQEjHVBFjXcwXy0vU
X8MSqDrrg8b4Mdv93OUMwvk62IzPmrrJfH3NuyjWoRVjqI35KVX6hIF6
-----END CERTIFICATE-----
Bag Attributes
    friendlyName: default
subject=/CN=default/OU=MGMT/O=AVAYA
issuer=/CN=default/OU=MGMT/O=AVAYA
-----BEGIN CERTIFICATE-----
MIICQjCCAaugAwIBAgIIDBlg8Zh4CWMwDQYJKoZIhvcNAQEFBQAwMTEQMA4GA1UE
AwwHZGVmYXVsdDENMAsGA1UECwwETUdNVDEOMAwGA1UECgwFQVZBWUEwHhcNMTAw
                  . . .
QrlRzEDot5Ep9d+SxWJOLptvmV6efHZ4ChSPyhyERDqcJNmi13vcEoINsW6GOBRx
V+OX1IlAXSJBoxyakR0OTL37pKnk8+1ywRx9JjMqPzSj5TUljCT20BeI8MWk4LZP
D07sRnER
-----END CERTIFICATE-----
```

2. Copy the Private Key part of the file (i.e., the yellow highlighted lines starting with BEGIN PRIVATE KEY and ending with END PRIVATE KEY) and store it in a file. In this example, the file name was `empirix_PrivateKey.pem`.
3. Copy the Idenity Certificate part of the file (i.e., the green highlighted lines starting with the first instance of BEGIN CERTIFICATE and ending with END CERTIFICATE) and store it in a file. In this example, the file name was `empirix_Cert1.pem`.
4. The `empirix_PrivateKey.pem` and `empirix_Cert1.pem` files must be used to configure the **TLS Certificate** and **TLS Private Key** of the originating and terminating

Hammer channels in the **Signaling** tab configured in **Sections 8.2.1** and **8.2.2.1**, respectively.

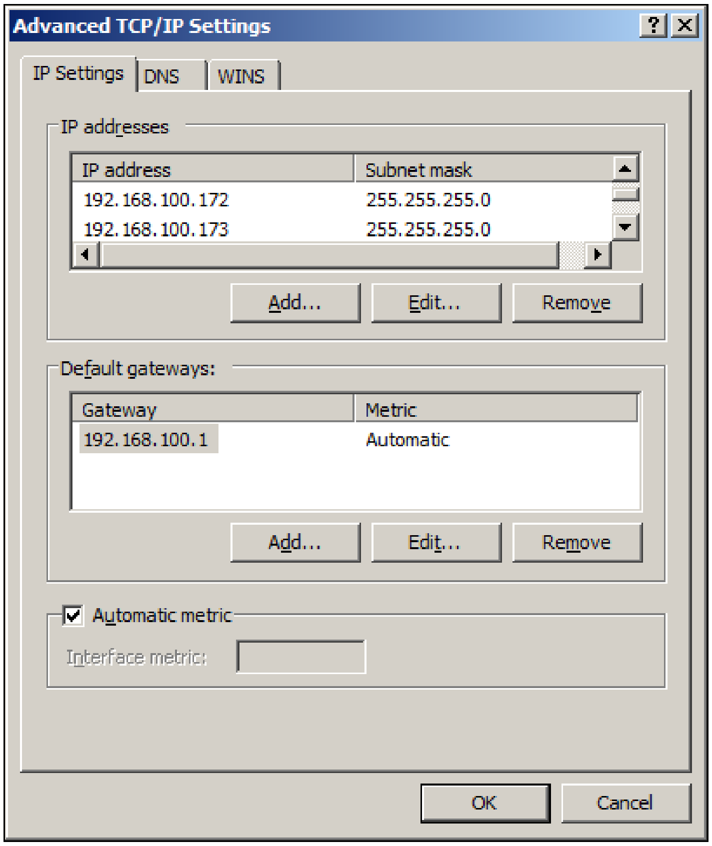
8 Configure Empirix Hammer IP

This section provides the procedures for configuring the Empirix Hammer IP. The procedures fall into the following areas:

- Assign IP addresses to each Hammer IP channel.
- Configure the system, including the originating and terminating channels and the PhoneBook, using the **Hammer Configurator**.
- Save and apply the Hammer configuration and start the Hammer server.
- Create and run the test script using the **Hammer TestBuilder**.

8.1 Configure IP Addresses on Hammer IP Server

The Hammer IP server needs to be configured with IP addresses for each channel. During the compliance test, 20 SIP endpoint channels were used. 10 channels were used to originate calls and 10 channels were used to terminate calls. This requires a block of 20 IP addresses, which must be contiguous. The 20 IP addresses used were from 192.168.100.171 to 192.168.100.190. These IP addresses are configured in the **Advanced TCP/IP Settings** under Network Connections (not shown) in Windows Server 2008.



8.2 Configure System

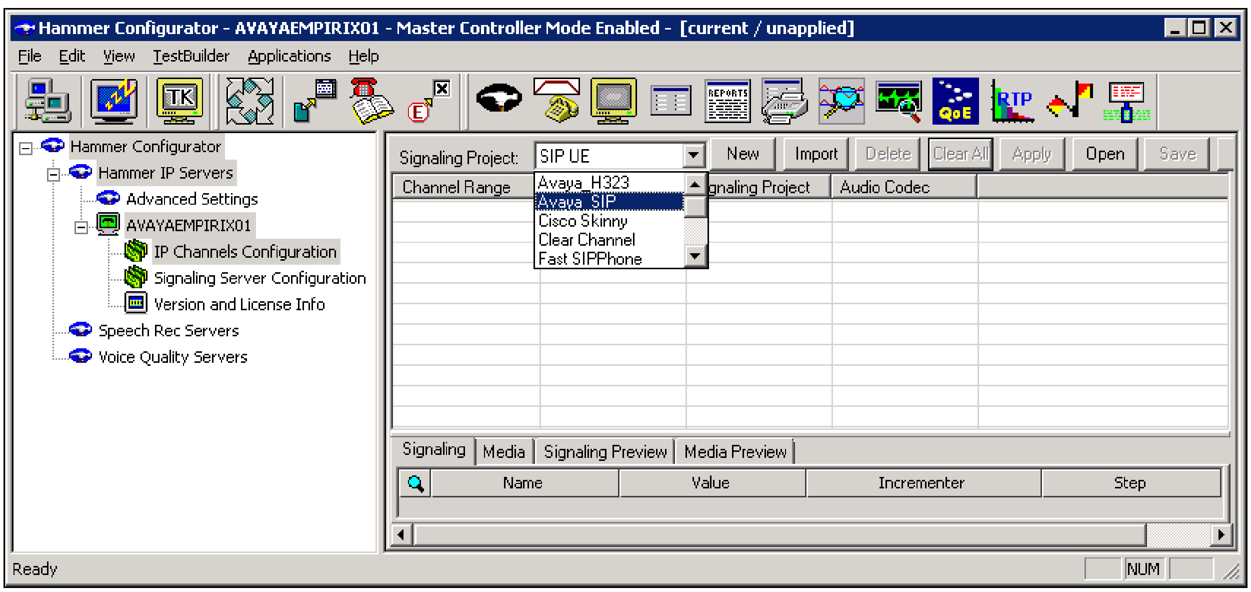
This section covers the configuration of originating and terminating channels and the PhoneBook on Hammer IP. In this configuration, the originating channels emulate SIP endpoints (described in **Section 6.7**). The terminating channels can emulate SIP endpoints or SIP trunks. These Application Notes will explicitly describe the configuration for terminating calls to SIP endpoints in **Section 8.2.2.1**. In addition, it will provide a reference to other Application Notes for configuring terminating channels as SIP trunks in **Sections 8.2.2.2**.

8.2.1 Configure Originating Channels – SIP Endpoints

The Empirix Hammer IP is configured through the **Hammer Configurator**, a graphical user interface, residing on the Hammer IP server. From the Hammer IP server, run the **Hammer Configurator**. The following screen is displayed.

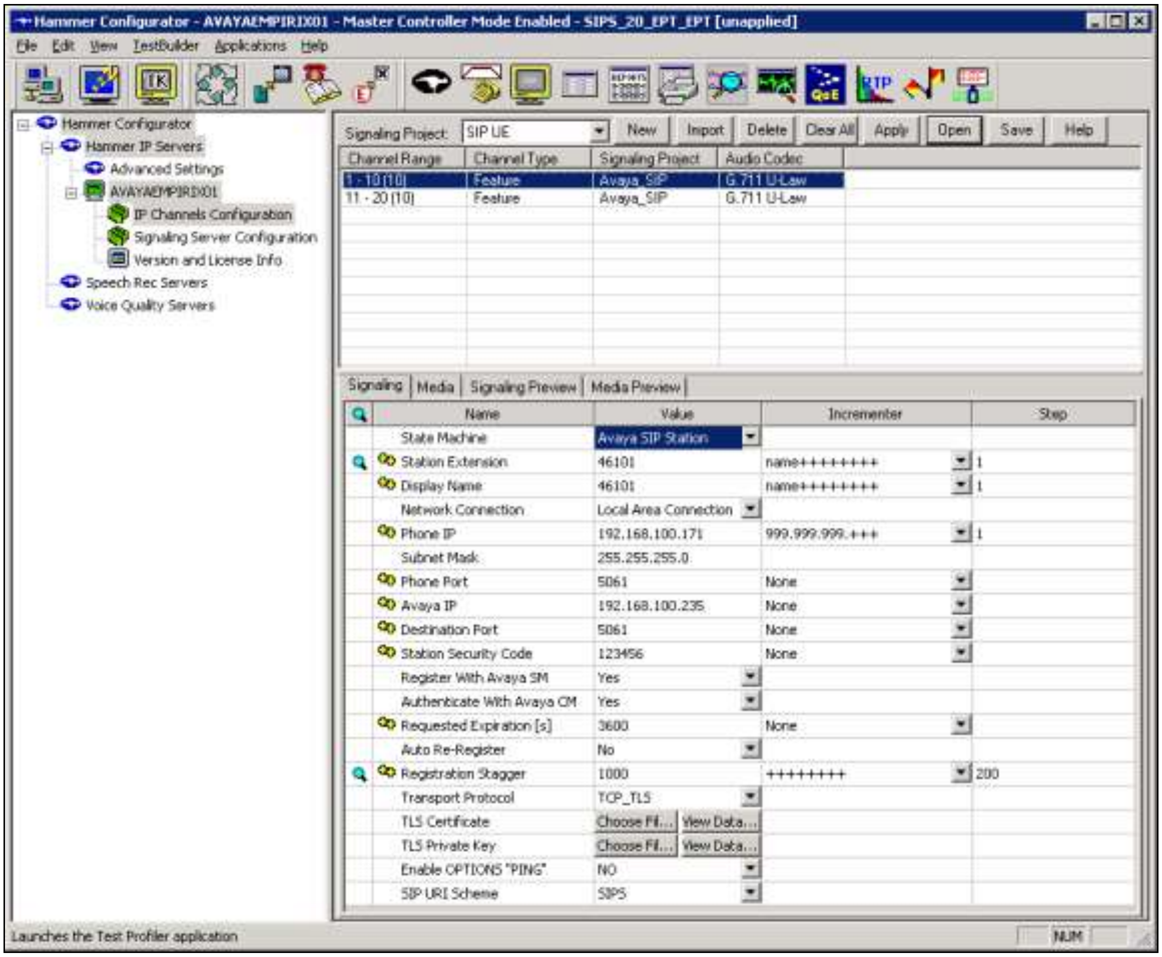
Note: It is assumed that Hammer IP is already in **Master Controller Mode**. To verify, check that the title bar of the **Hammer Configurator** indicates *Master Controller Mode Enabled* as shown below. It is also assumed that a system was already added to the configuration. In this configuration, the system name is *AVAYAEMPIRIX01*, which corresponds to the server name.

In the **Hammer Configurator**, the server name will appear in the left pane of the **Hammer Configurator**. Expand the server name (e.g., *AVAYAEMPIRIX01*) in the left pane and click on **IP Channels Configuration.** The following window will be displayed. Select *Avaya_SIP* for the **Signaling Project** and then click **New**.



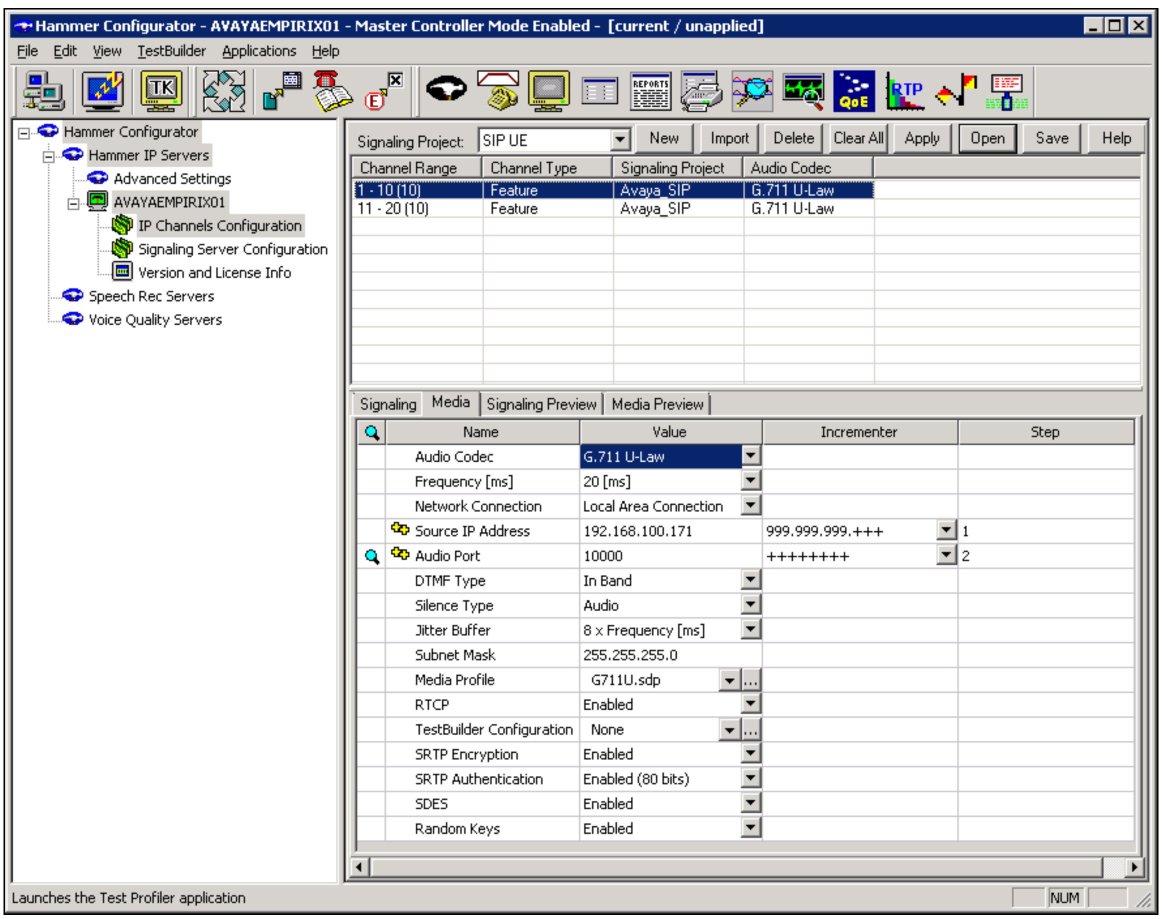
The first line in the grid that is highlighted in the figure below corresponds to the 10 originating channels. To set the number of channels in the group, click on the **Channel Range** cell in the grid and enter the number *10*. The following fields in the **Signaling** tab should be set as follows:

- **State Machine** should be set to *Avaya SIP Station*.
- **Station Extension** should be set to the first extension in the group (e.g., *46101*) and the **Incrementer** and **Step** fields should be set as shown so that the extension of the subsequent channels are incremented by one. This covers extensions from *46101* to *46110*.
- **Display Name** may be set to the first extension in the group (e.g., *46101*) and the **Incrementer** and **Step** fields should be set as shown so that the extension of the subsequent channels are incremented by one. This covers extensions from *46101* to *46110*.
- **Network Connection** should be set to the appropriate network interface.
- **Phone IP** should be set to the IP address of the first channel in the group and the **Incrementer** and **Step** fields should be set as shown so that the last of octet of the IP address is incremented by one. Note that this requires a block of contiguous IP addresses. This covers IP addresses from *192.168.100.171* to *192.168.100.180*.
- **Subnet Mask** should be set to the network mask (e.g., *255.255.255.0*).
- **Phone Port** should be set to TLS port *5061*.
- **Avaya IP** should be set to the Session Manager SIP interface (e.g., *192.168.100.235*).
- **Destination Port** should be set to TLS port *5061*.
- **Station Security Code** should match the one configured under the Communication Profile tab of the **SIP User** in Session Manager described in **Section 6.7**.
- **Register with Avaya SES** should be set to *Yes*.
- **Authenticate with Avaya CM** should be set to *Yes*.
- **Transport Protocol** should be set to *TCP_TLS*. See **Section 7.4** for instructions on managing and creating TLS certificates.
- **TLS Certificate** should be imported by clicking the **Choose File** button. Creating the TKS Certificate file is described in **Section 7.4**.
- **TLS Private Key** should be imported by clicking the **Choose File** button. Creating the TKS Private Key file is described in **Section 7.4**.
- **SIP URI Scheme** should be set to *SIPS*.
- The default values for other fields may be used as shown.



In the **Media** tab of the 10 originating channels, configure the fields as follows:

- **Audio Codec** should be set to the appropriate codec for the test. G711 U-Law, G729AB, and G.729A were used during the compliance testing.
- **Frequency [ms]** should be set to the appropriate value for the specified codec. It should match the Packet Size [ms] field in the **IP Codec Set** form on Communication Manager for the specified codec.
- **Network Connection** should specify the appropriate network interface.
- **Source IP Address** should be set to the IP address of the first channel in the group. The **Incrementer** and **Step** fields should be set as shown so that the last octet of the IP address is incremented for the subsequent channels. Note that the IP addresses for the channels need to be contiguous.
- **Media Profile** should be set to one that specifies the codec configured in the **Audio Codec** field. See **Appendix A** for instructions on configuring a **Media Profile**.
- **SRTP Encryption** should be enabled. Disable SRTP if not required for test.
- **SRTP Authentication** should be set to **Enabled (80 bits)**.
- **SDES** should be enabled.
- **Random Keys** should be enabled.
- The default values for the remaining fields may be used as shown.



8.2.2 Configure Terminating Channels

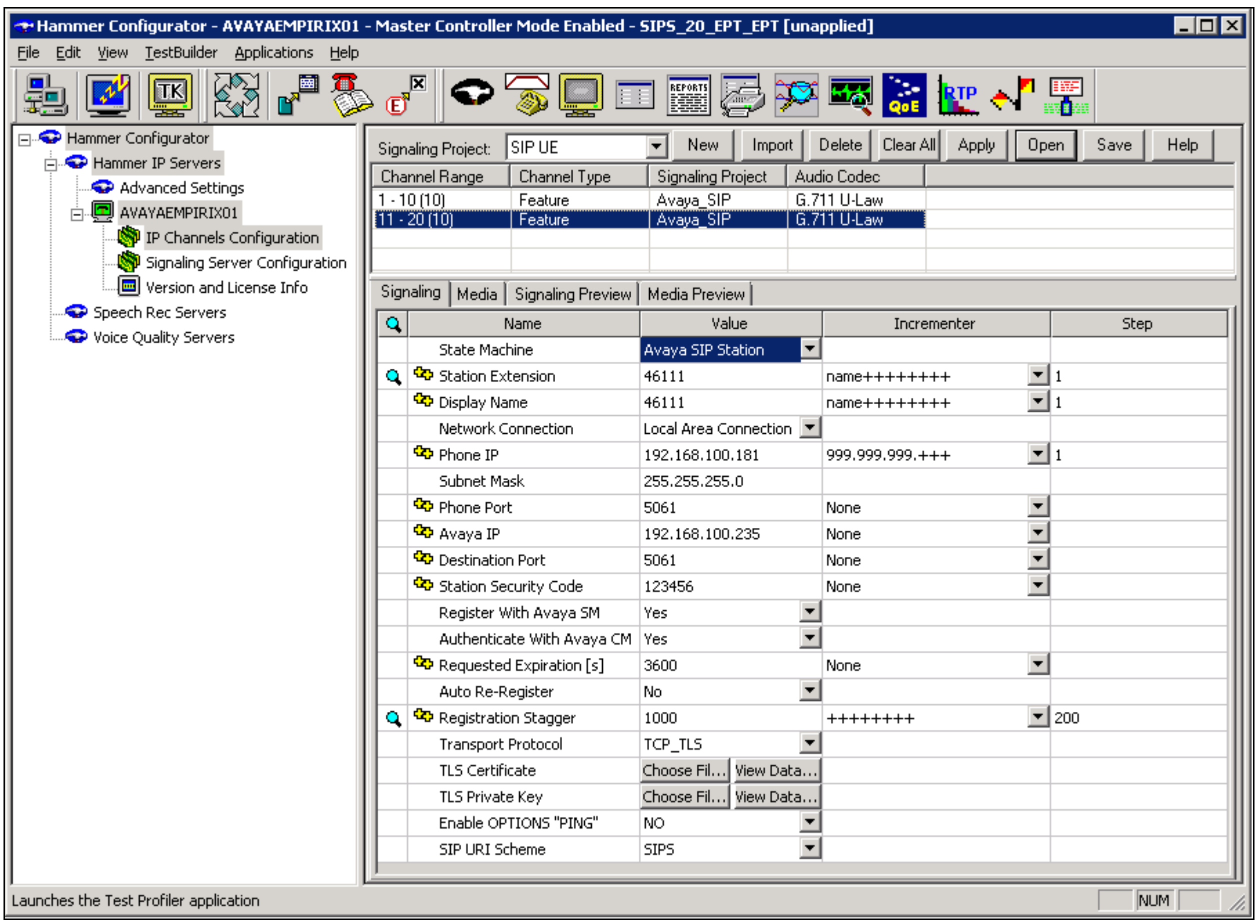
During the compliance test, the originating channels emulated SIP endpoints with the calls terminating on SIP endpoints and SIP trunks. Select one of the following subsections depending on the configuration desired.

- **Section 8.2.2.1** for terminating calls on SIP endpoints.
- **Section 8.2.2.2** for terminating calls on SIP trunks.

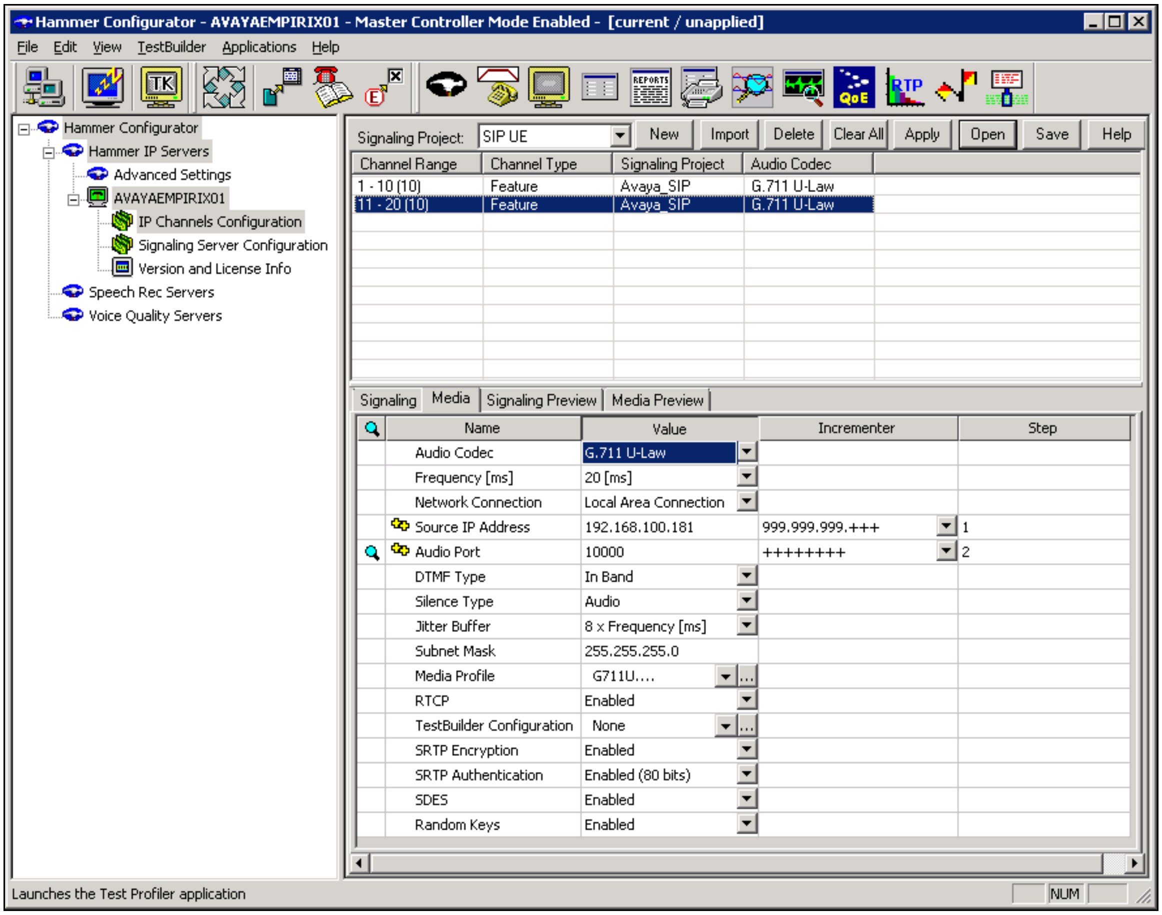
Note: Ensure that the originating and terminating channels are assigned unique IP addresses.

8.2.2.1 Configure Terminating Channels – SIP Endpoints

The second line in the grid that is highlighted in the figure below corresponds to the second group of channels that will terminate calls. Set the **Channel Range** cell to the number of channels in this group. The configuration of the **Signaling** tab is similar to the one for the group of originating channels in **Section 8.2.1** with the exception that the **Station Extension** and **Phone IP** fields will be different. This group of channels will be assigned extensions *46111* to *46120* and IP addresses from *192.168.100.181* to *192.168.100.190*. Again, the IP addresses for this group of channels need to be contiguous.



The **Media** tab for the group of terminating channels is shown below. The configuration is similar to the one for the group of originating channels except for the **Source IP Address** field.



8.2.2.2 Configure Terminating Channels – SIP Trunks

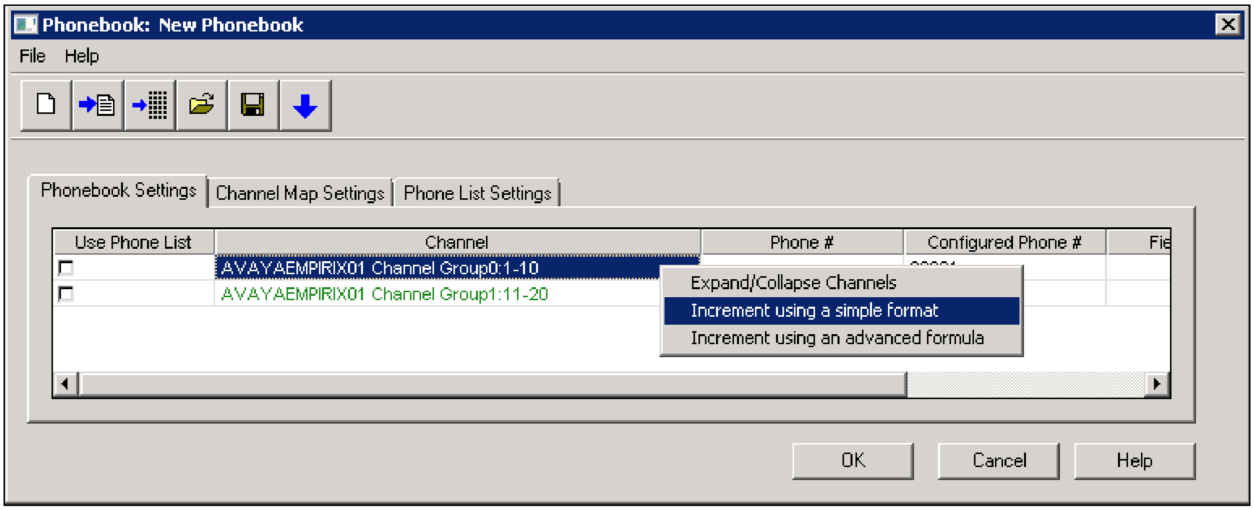
To terminate the calls to SIP trunks follow the instructions described in **[4]**, specifically:

- **Section 5** describes how to configure call routing on Communication Manager.
- **Section 6** describes how to configure SIP trunks to Hammer IP on Session Manager.
- **Section 7.2.2.1** describes how to configure terminating SIP trunks on Hammer IP.
- **Section 7.4** describes how to specify the dialed digits when running a test script.

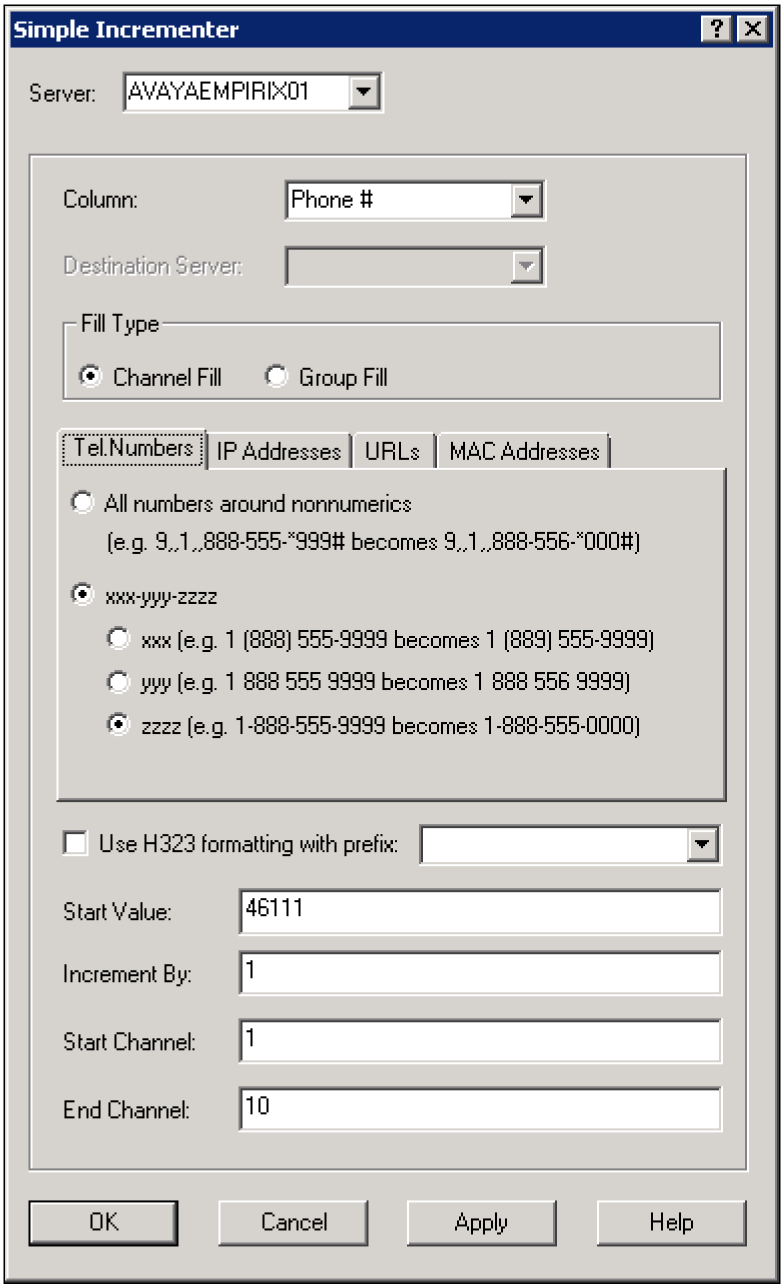
The configuration described in all the aforementioned sections of **[4]** must be completed for terminating calls to SIP trunks.

8.2.3 Configure the PhoneBook

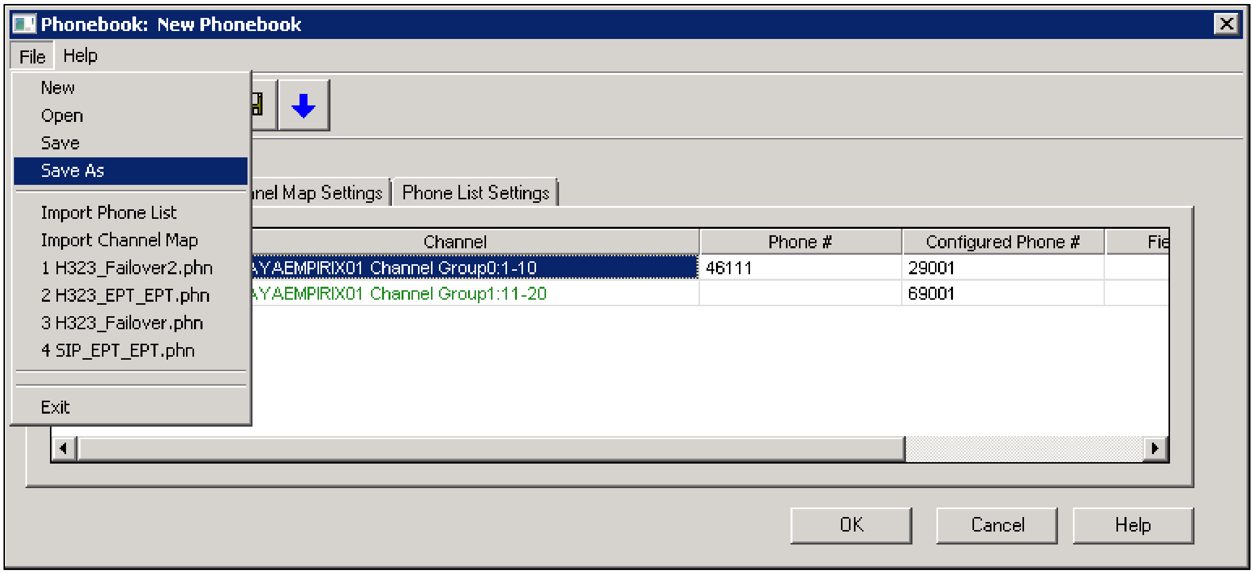
The **PhoneBook** is used to specify which number each originating channel should dial when placing a call. Click on the **PhoneBook** icon (not shown) in the **Hammer Configurator**. The **PhoneBook** window is displayed below. The **Channel** column is automatically displayed with the appropriate channel groups. Right-mouse click on the first line corresponding to the group of originating channels (channels 1-10) and select the **Increment using a simple format** option as shown below.



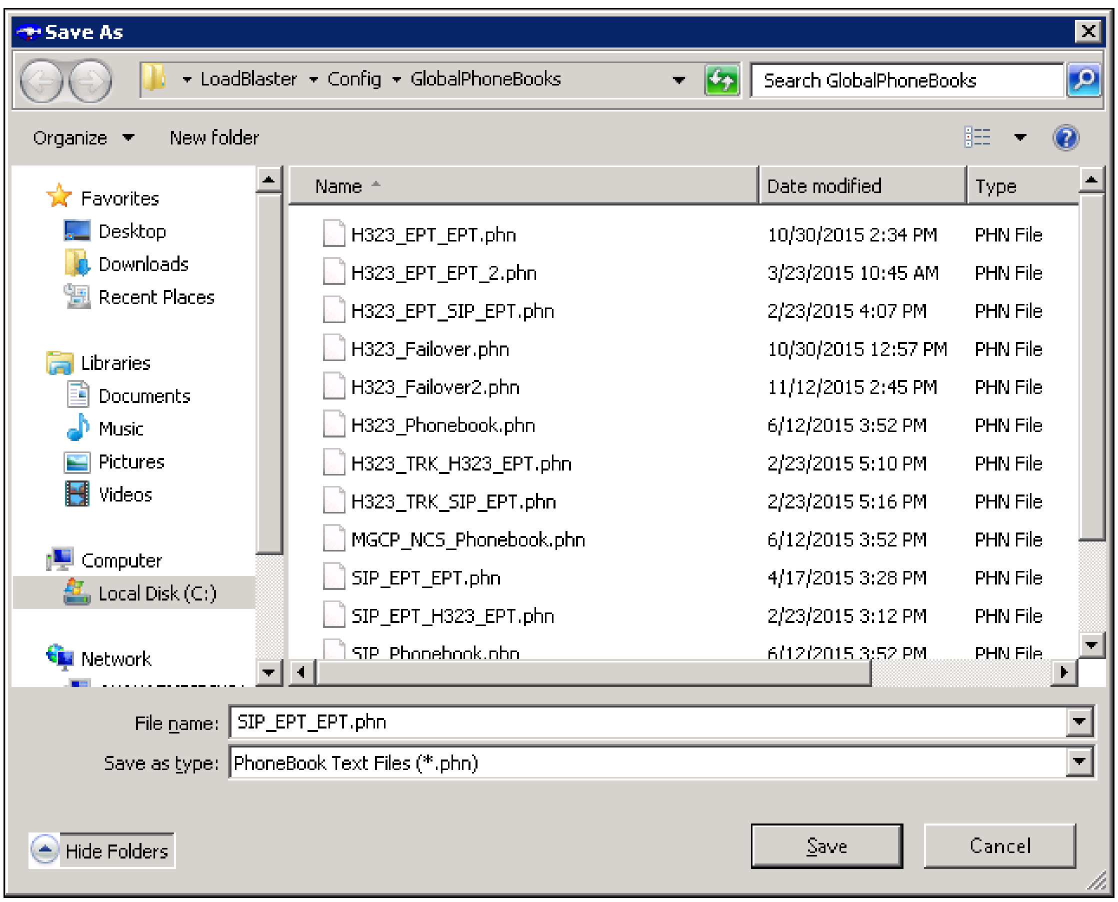
In the **Simple Incrementer** window, specify the number that the first originating channel should dial in the **Start Value** field. In this example, the first channel will dial *46111*, which corresponds to channel 11. Set the **Increment By** field to *1*. This specifies that the subsequent channels should increment the dialed number by one. For example, channel 1 will dial 46111, channel 2 will dial 46112, and so on. The **Start Channel** field should be set to the first channel number and the **End Channel** field should be set to the last originating channel number, which is 10. Click **OK**.



Once the **PhoneBook** is configured, select **File→Save As** to save the PhoneBook.

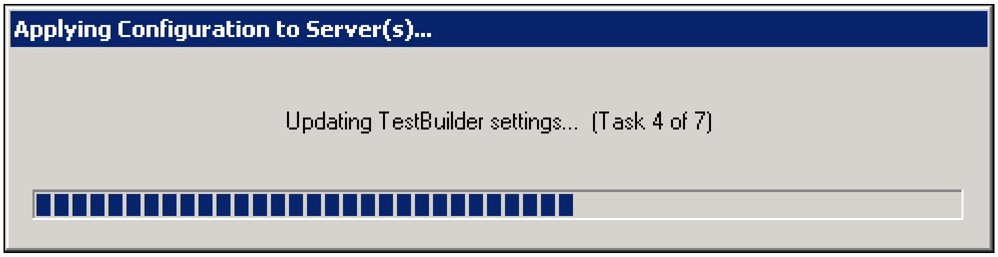


The PhoneBook is saved as *SIP_EPT_EPT.phn* in the following window. This PhoneBook will be used when running the test.

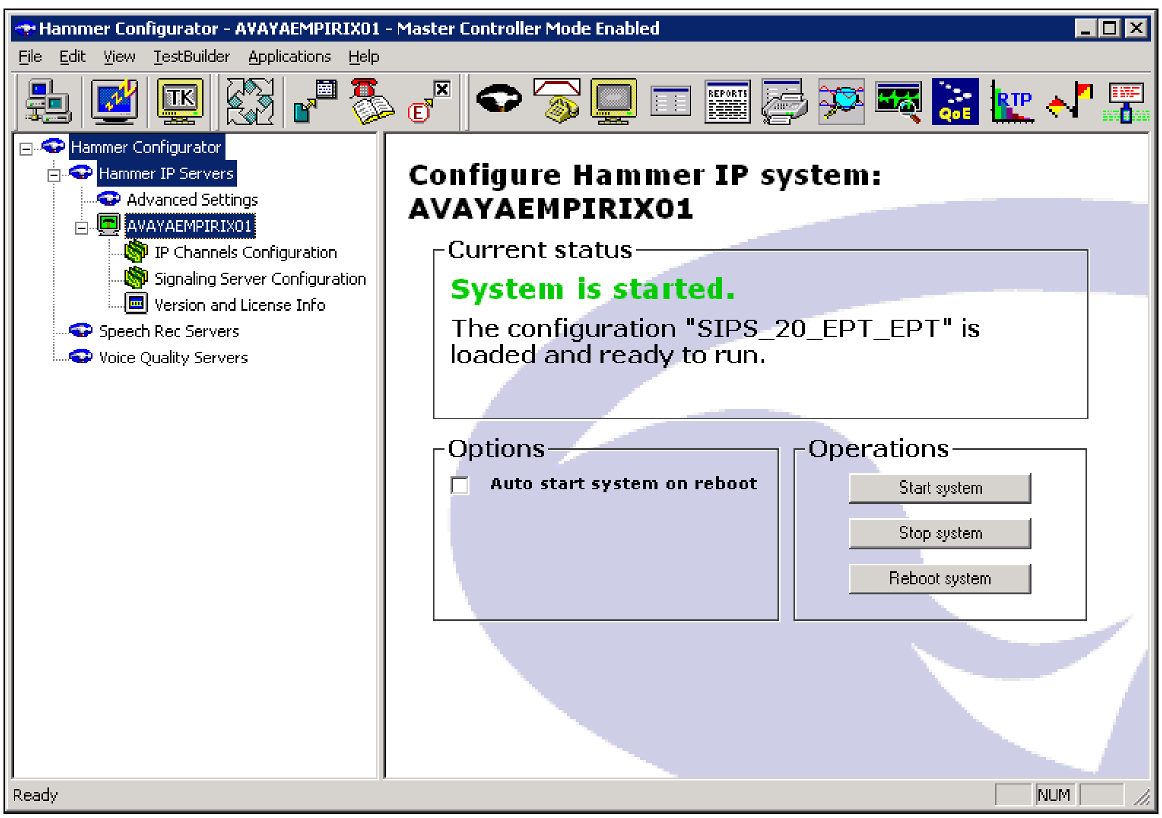


8.3 Applying the Hammer IP Configuration

This completes the configuration of Hammer IP. This configuration should be saved by clicking the **Save** button (not shown) on the **Hammer Configurator** window. The configuration needs to be applied to the server for the changes to take effect. Click on the **Apply** button (not shown) in the **Hammer Configurator** window. The following window is displayed as the configuration is being applied to the server.



Check that the system has been started by clicking on the server name (e.g., *AVAYAEMPIRIX01*) in the left pane of the **Hammer Configurator**. If the current status is *System Is Stopped*, click the **Start system** button to start the system. When the system is started, it should appear as shown below and should also specify which configuration has been applied. The configuration performed above was saved as *SIPS_20_EPT_EPT*. When the system is started, the Hammer IP will register SIP endpoints with Session Manager.

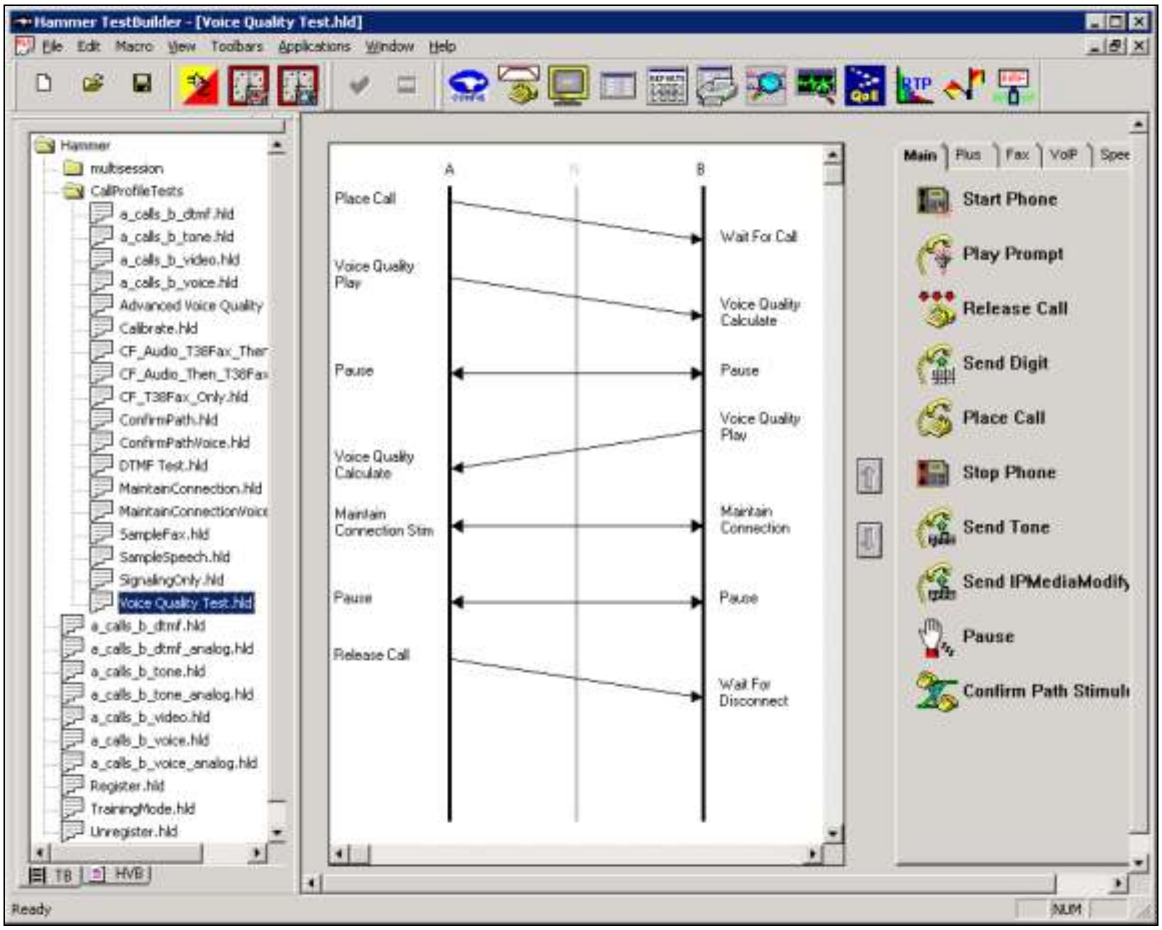


8.4 Configure and Run the Test Script

For the compliance test, two default test scripts were used:

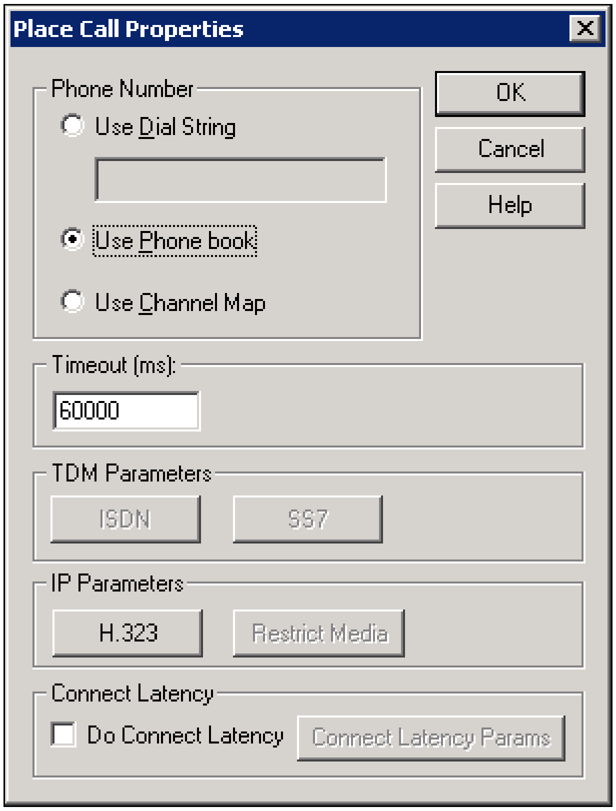
- `a_calls_b_dtmf.hld` to verify DTMF
- `Voice Quality Test.hld` to verify voice quality

The sample test script, `Voice Quality Test.hld`, establishes a VoIP call between two SIP endpoints on the Hammer IP, followed by the originating side playing an audio prompt to the far-end so that voice quality metrics (e.g., PESQ score) can be obtained. The test script is configured with the **Hammer TestBuilder** application and can be displayed in a ladder diagram as shown below by double-clicking on the test script name.

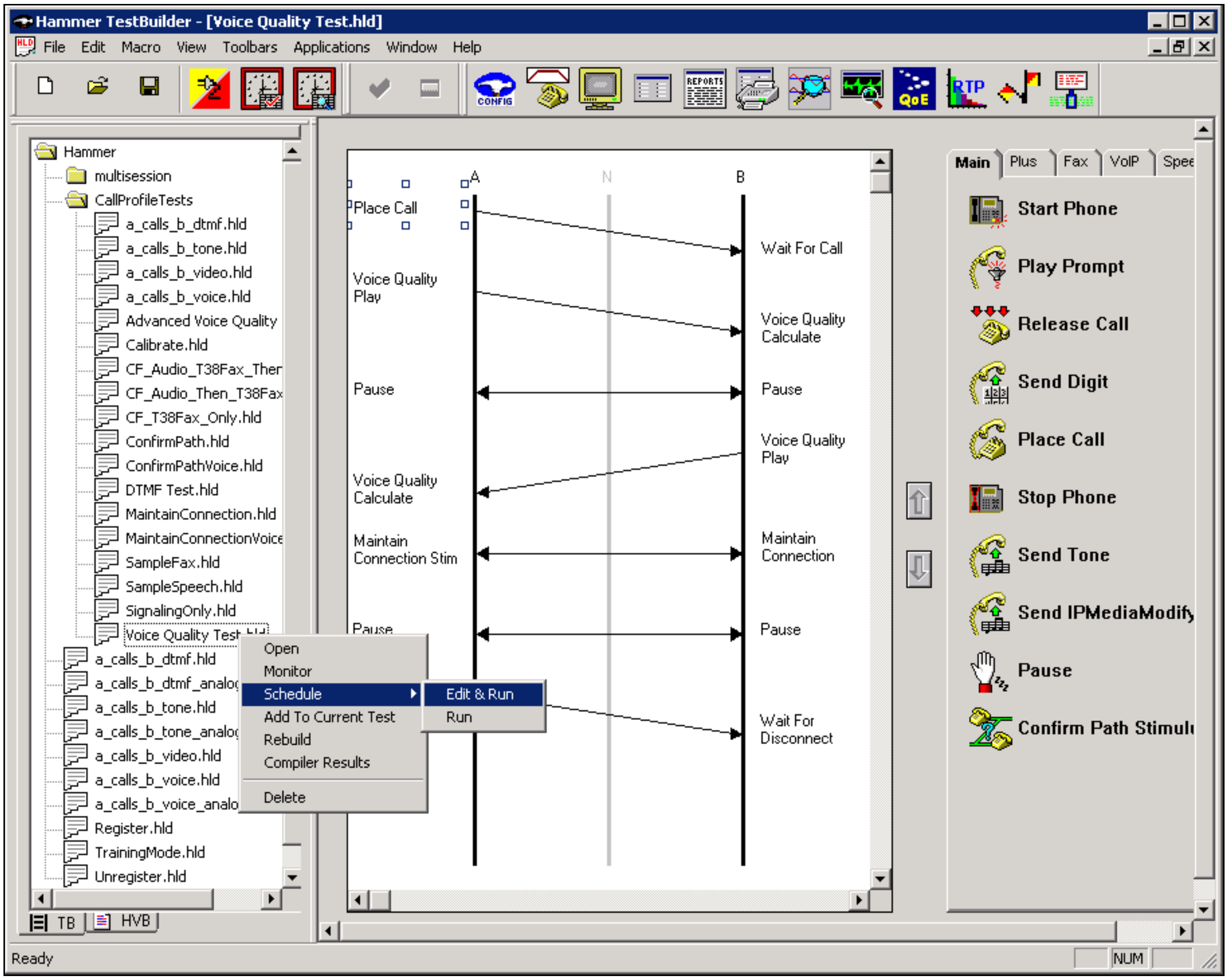


In the sample test script configured above, the A-side (originating SIP endpoint) places a call to the B-side (terminating SIP endpoint) using the **Place Call** action. The **Place Call** properties can be configured by double-clicking on the action in the ladder diagram. The **Place Call Properties** is configured to use the PhoneBook as shown below.

Note: Disable the **Do Connect Latency** option in the **Place Call Properties** window.

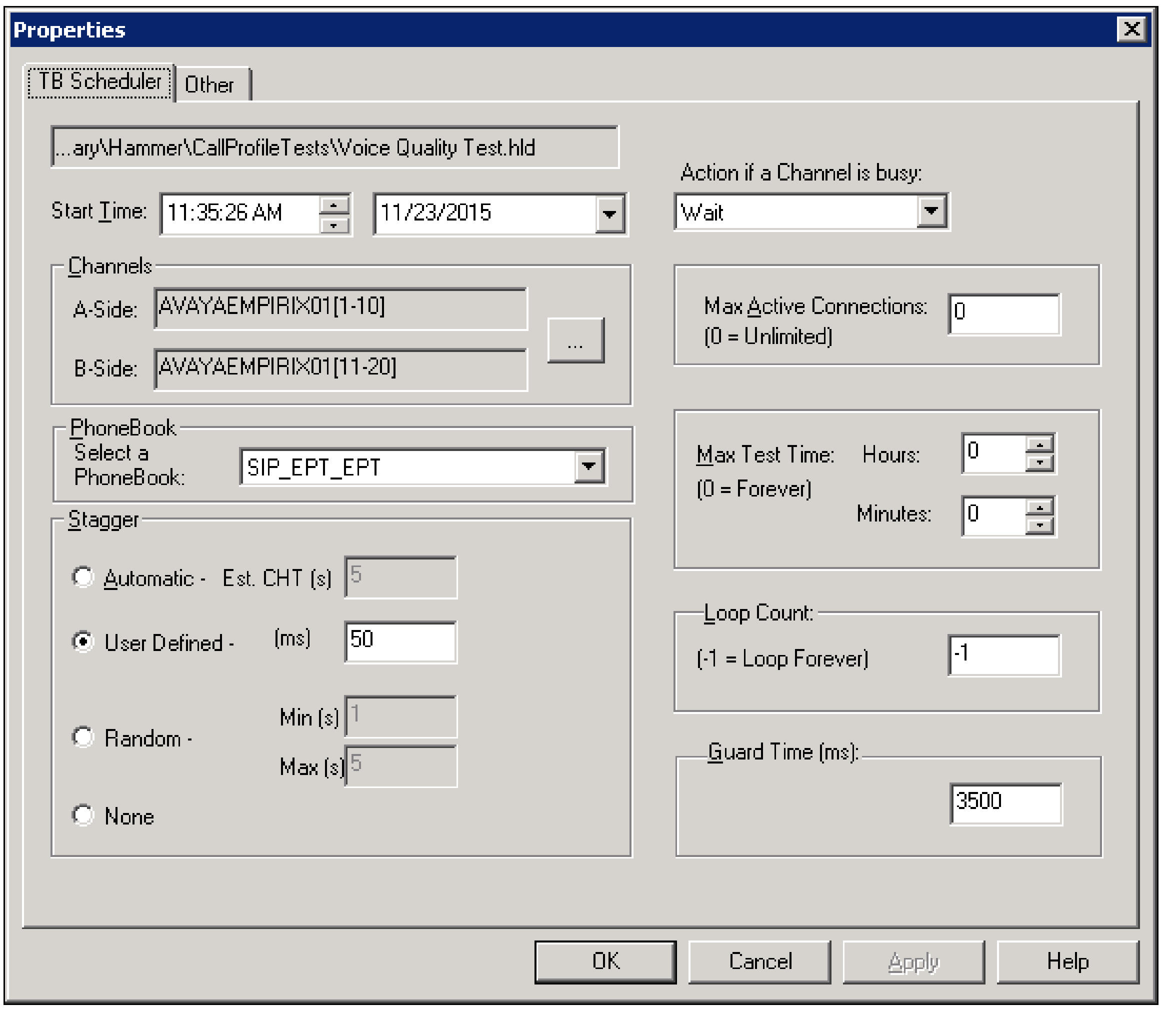


To run the test, right-mouse click on the test script in the left pane of the **Hammer TestBuilder** window and navigate to **Schedule→Edit & Run**. To re-run the test, the user can simply select **Schedule→Run**, if no changes are required.



In the **Properties** window, click on the ellipses button (…) in the **Channels** section and assign channels to the **A-Side** and **B-Side**. Next, select the appropriate PhoneBook (e.g., *SIP_EPT_EPT*). The SIP_EPT_EPT PhoneBook was configured above. Set the **Loop Count** to the appropriate value to control the number of iterations the test should run. Setting this field to *-1* will allow the test to run forever. Setting this field to a specific number will run the test for the many iterations and then stop. The **Guard Time (ms)** field specifies how long to wait before the test is run again on the same channel. The minimum setting should be *3500*. The **Stagger** section allows the user to specify how long to wait before the test is run on the next channel. For the compliance test, the **Stagger** time was set to *50 ms*.

Important Note: The **Guard Time** and **Stagger** parameters should be carefully considered for every test. A test script could fail because the configuration under test cannot handle the load generated by the Hammer IP. These parameters can slow down the test to a rate that can be reasonably handled by the test configuration.



9 Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Empirix Hammer IP.

9.1 Verify Avaya Aura® Communication Manager

When the Hammer IP is running a test script, the **status trunk** command may be used to view the active call status. The trunk being monitored here is the trunk to Session Manager. This command should specify the trunk group and trunk member used for the call be specified.

```
status trunk 60/1                                              Page   1 of   4
                              TRUNK STATUS

 Trunk Group/Member: 0060/001              Service State: in-service/active
               Port: T00044             Maintenance Busy? no
 Signaling Group ID: 60

   IGAR Connection? no

    Connected Ports: T00046
```

Page 2 of the **status trunk** command indicates the codec being used for the call and whether the call is shuffled. If the call is shuffled, the **Audio Connection Type** field would be set to *ip-direct*, if it isn't, the field would be set to *ip-tdm* as shown below. Also, note that TLS port 5061 is being used.

```
status trunk 60/1                                              Page   2 of   4
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                               Port
   Near-end:  192.168.100.10                         : 5061
    Far-end:  192.168.100.235                        : 5061
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-tdm        Authentication Type: None
    Near-end Audio Loc: MG1                    Codec Type: G.711MU
   Audio      IP Address                               Port
   Near-end:  192.168.100.15                         : 2054
    Far-end:  192.168.100.172                        : 10002

 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:               Video Far-end Codec:
```

Page 4 of the **status trunk** command indicates that SRTP is being used for the call.

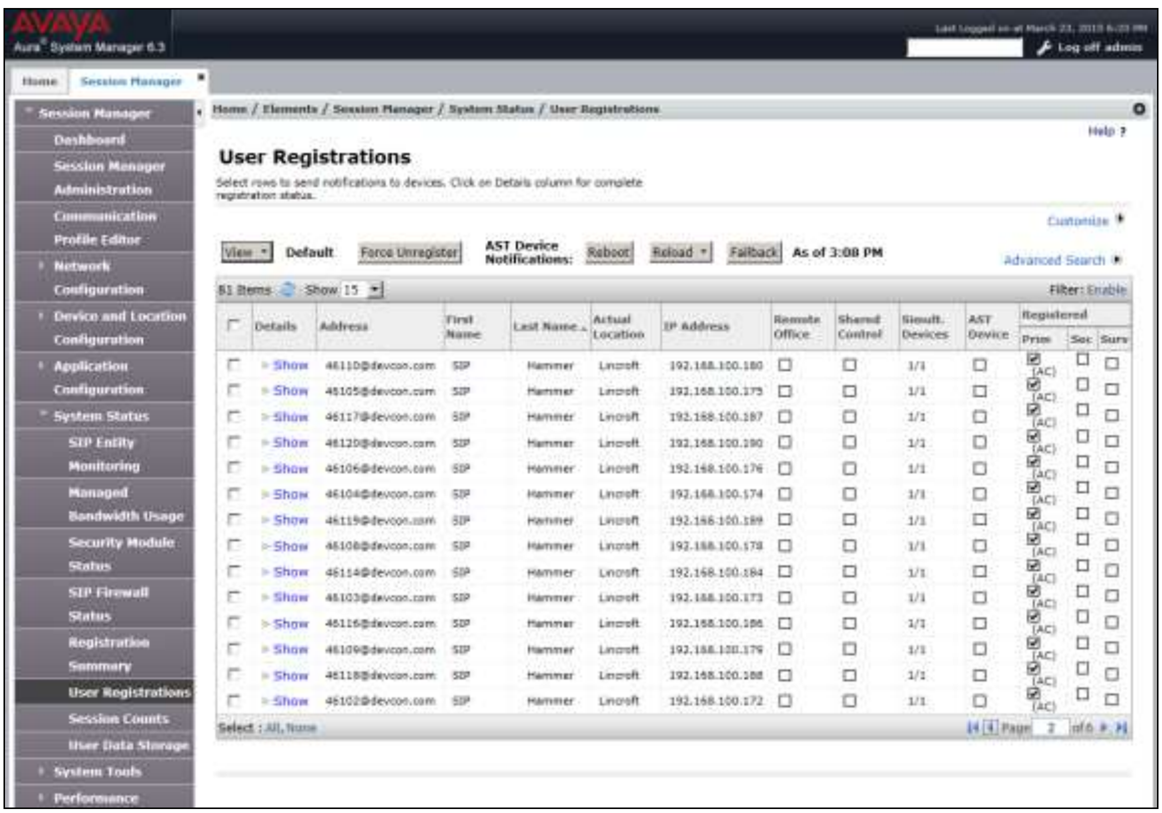
```
status trunk 60/1                                              Page    4 of    4
                             SRC PORT TO DEST PORT TALKPATH
src port: T00044
T00044:TX:192.168.100.173:10004/g711u/20ms/1-srtp-aescm128-hmac80
001V048:RX:192.168.100.15:2084/g711u/20ms/1-srtp-aescm128-hmac80:TX:ctxID:333
001V046:RX:ctxID:333:TX:192.168.100.15:2088/g711u/20ms/1-srtp-aescm128-hmac80
T00137:RX:192.168.100.183:10004/g711u/20ms/1-srtp-aescm128-hmac80

dst port: T00137
```

9.2 Verify Avaya Aura® Session Manager

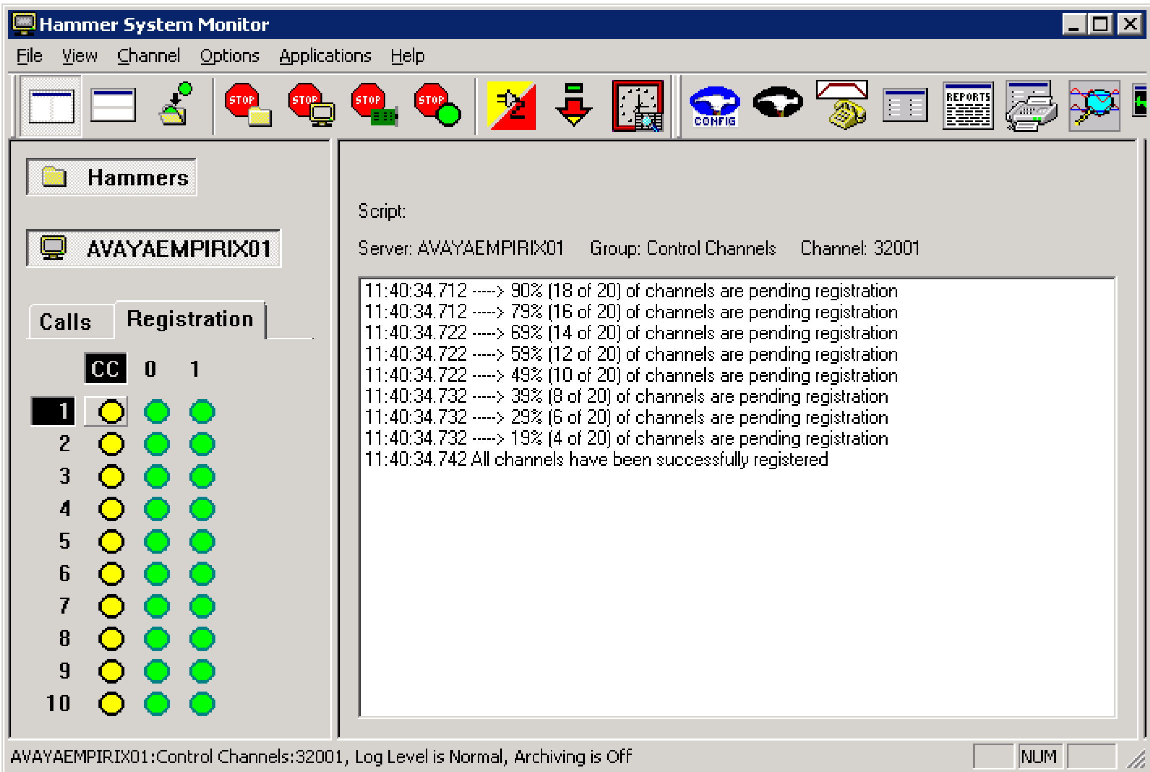
The registered SIP endpoints can also be viewed from Session Manager by navigating to **Home→Elements→Session Manager→System Status→User Registrations**.

Note: Make sure that all registered SIP endpoints associated with the Hammer IP only have one IP address.

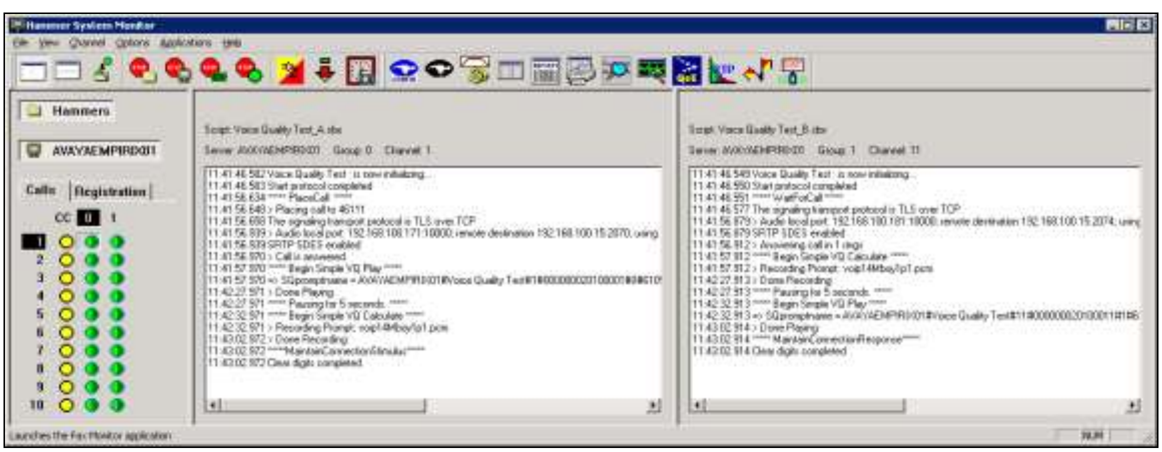


9.3 Verify Empirix Hammer IP

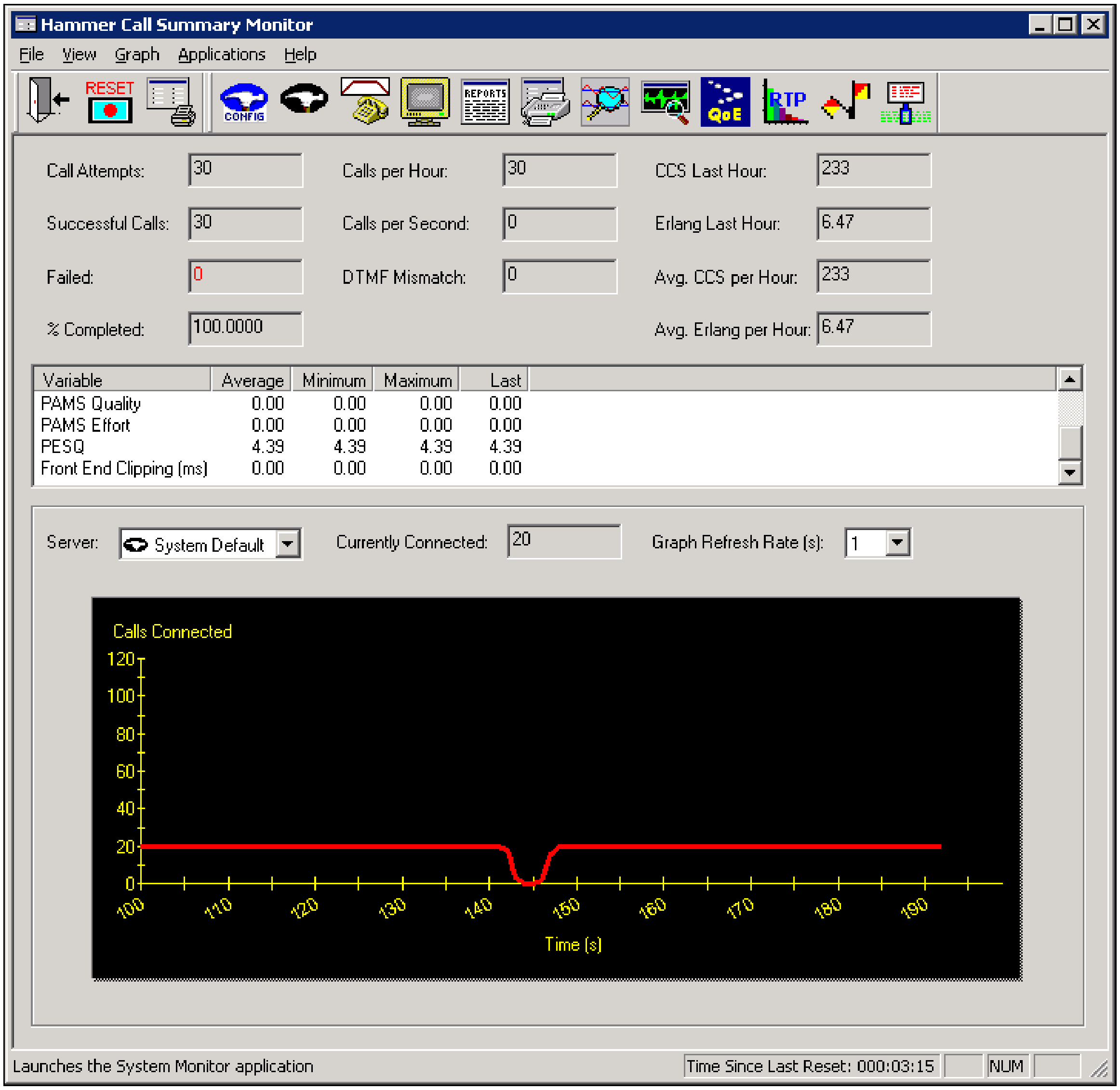
To view the SIP registration status from the Hammer IP, make sure that the **Hammer System Monitor** is running before starting the system. Select the **Registrations** tab and click on the yellow circle under the CC column and row 1. The Hammer IP will indicate when all of the channels have successfully registered.



Call progress can be monitored in the **Hammer System Monitor**. The call log for an originating channel may be logged to the left window and the call log for a terminating channel may be logged to the right window. In the following System Monitor screen, it indicates that TLS over TCP and SRTP were being used for the test calls.



The **Hammer Call Summary Monitor** may be used to get a test status overview, including the number of call attempts, number of failed calls, PESQ scores, amongst other useful metrics.



10 Conclusion

These Application Notes describe the configuration steps required to integrate the Empirix Hammer IP with an Avaya SIP telephony network using SIP endpoint emulation. Hammer IP was able to register with Avaya Aura® Session Manager, successfully establish calls through Avaya Aura® Communication Manager to SIP endpoints/trunks, generate voice quality metrics, monitor the calls, and generate reports. Furthermore, this solution was able to use SIPS to secure the SIP signaling using TLS (Transport Layer Security) and Secure Real-time Transport Protocol (SRTP) to protect the RTP data. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

11 References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 10, August 2015, Document Number 03-300509.

[2] *Administering Avaya Aura® System Manager for Release 6.3.13 through 6.3.15*, Release 6.3, Issue 8, December 2015.

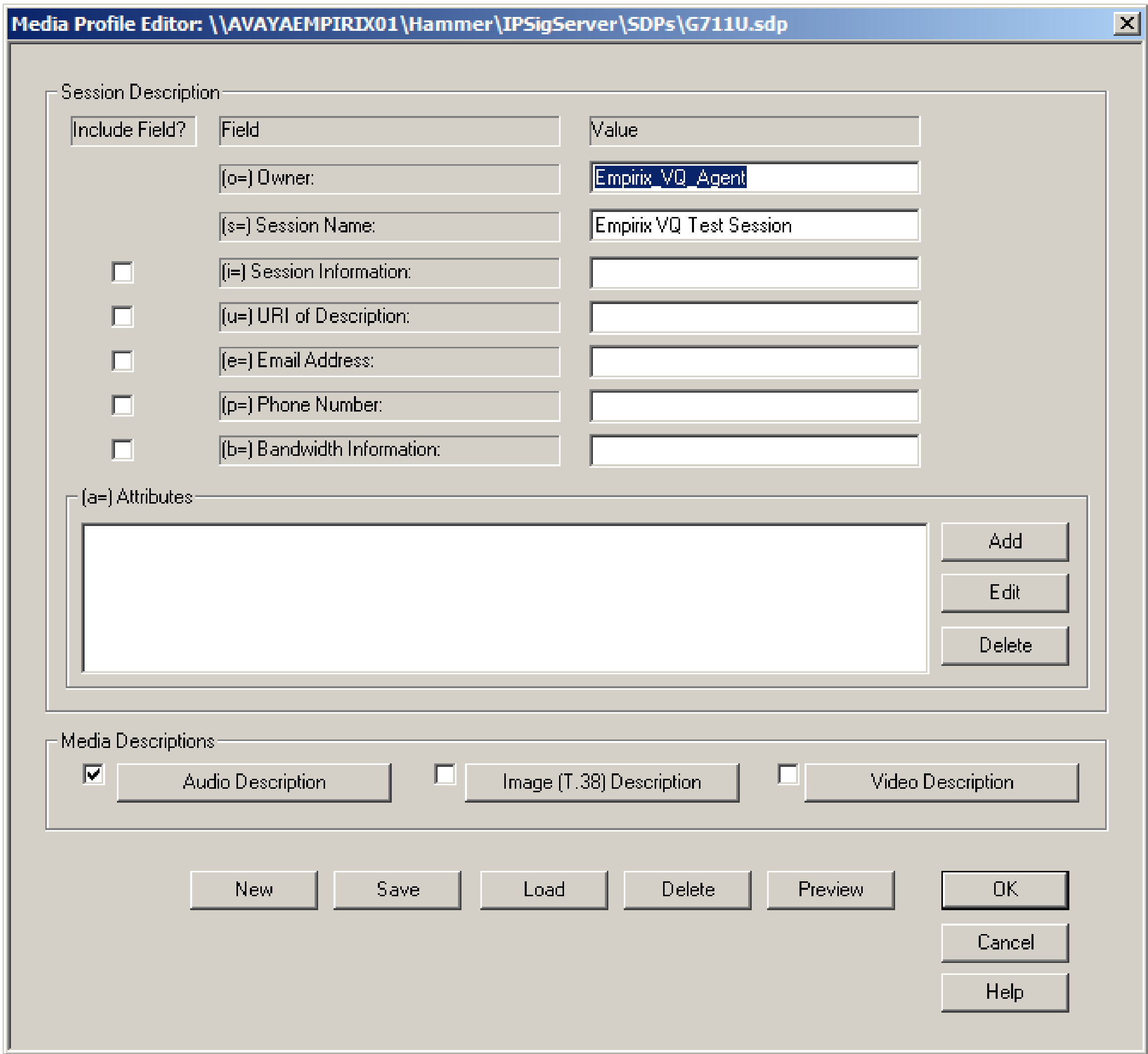
[3] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 7, September 2014.

[4] *Application Notes for Empirix Hammer IP with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunk Emulation with Secure SIP (SIPS) / Transport Layer Security (TLS)*, Issue 1.0, available at http://www.avaya.com.

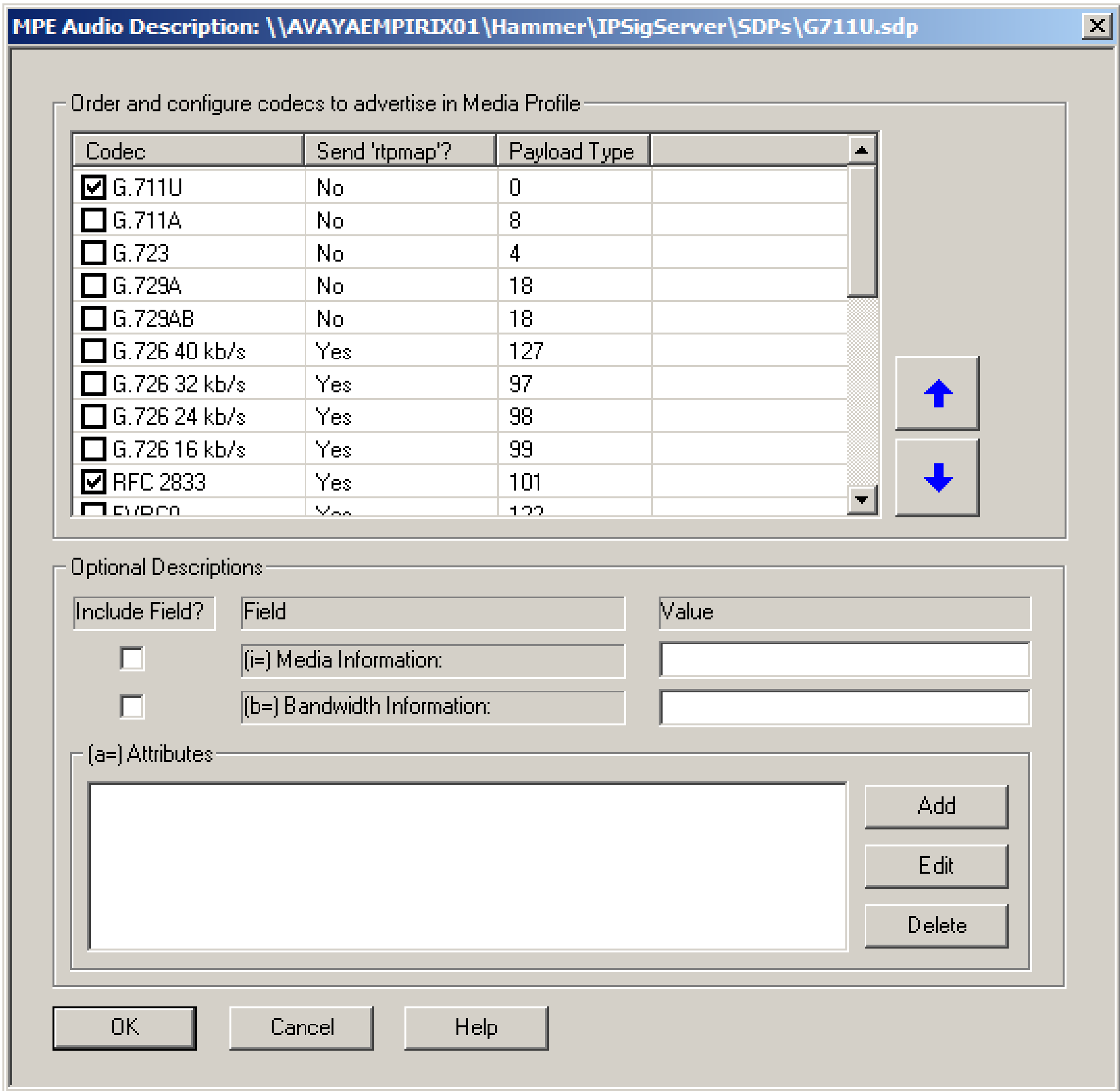
[5] *Empirix Hammer IP Installation Guide,* Release 6.2, October 2015, Revision A, available from Empirix.

APPENDIX A: Configure Media Profile on Empirix Hammer IP

The following windows show the configuration of the **Media Profile** used in the **Media** tab for the originating and terminating channel groups. To access this window, click on the ellipses button (…) by the **Media Profile** field in the **Media** tab. Click on the **Audio Description** button to view the codecs that will be advertised by the Hammer IP when placing a call.



The following window shows the codecs selected for this profile. This **Media Profile** was already created and named *G711U.sdp*. It specifies G.711U and RFC 2833. When done, click **OK** to return to the previous window. Additional media profiles can be created and saved by selecting the desired codecs in this window and then clicking the **Save** button in the previous window.



Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.