Avaya Solution & Interoperability Test Lab

Configuring SIP Trunks Among Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, and Avaya Aura® Session Border Controller 6.0 – Issue 1.0

Abstract

These Application Notes describe the steps required to configure SIP trunks between Avaya Aura® Session Border Controller 6.0, Avaya Aura® Communication Manager Evolution Server 6.0.1 and Avaya Aura® Session Manager 6.1.

The main function of Avaya Aura® Session Border controller is to protect private network from outside intrusion by topology hiding. It does NAT translations for SIP and Media traffic for inbound and outbound calls. It supports SIP traffic on UDP, TCP and TLS protocols.

©2011 Avaya Inc. All Rights Reserved.

©2011 Avaya Inc. All Rights Reserved.

©2011 Avaya Inc. All Rights Reserved.

1. Introduction

Avaya Aura® Session Border Controller secures the IP border for the real time interactive communications that flow from outside to internal network and is a standard element of Avaya's Communication Architecture. The main features are secure SIP voice, and SIP signaling elements against security threats and overloads.

These Application Notes present a sample configuration for a network that connects Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Manager 6.1 with Avaya Aura® Session Border Controller using SIP trunks.

2. Reference Configuration

In the sample configuration, Avaya Aura® Communication Manager 6.0.1 runs on an Avaya S8800 Server with Avaya G650 Media Gateway, Avaya Aura® Session Manager 6.1, Avaya Aura® System Manager and Avaya Aura® Session Border Controller 6.0 all runs on an Avaya S8800 Server platform. The sample configuration is shown in **Figure 1**.
The test configuration below shows Communication Manager Site and Data Center as part of private enterprise network. Session Border Controller is located on the edge of private network and controls SIP traffic to and from public network. For the sample configuration, Communication Manager was connected via SIP trunk over the enterprise WAN to simulate a SIP Service Provider.
The current configuration shows Communication Manager and Session Manager connected to Session Border Controller via SIP trunk. On public side Session Border Controller has SIP trunk configured to Communication Manager in simulated public network.

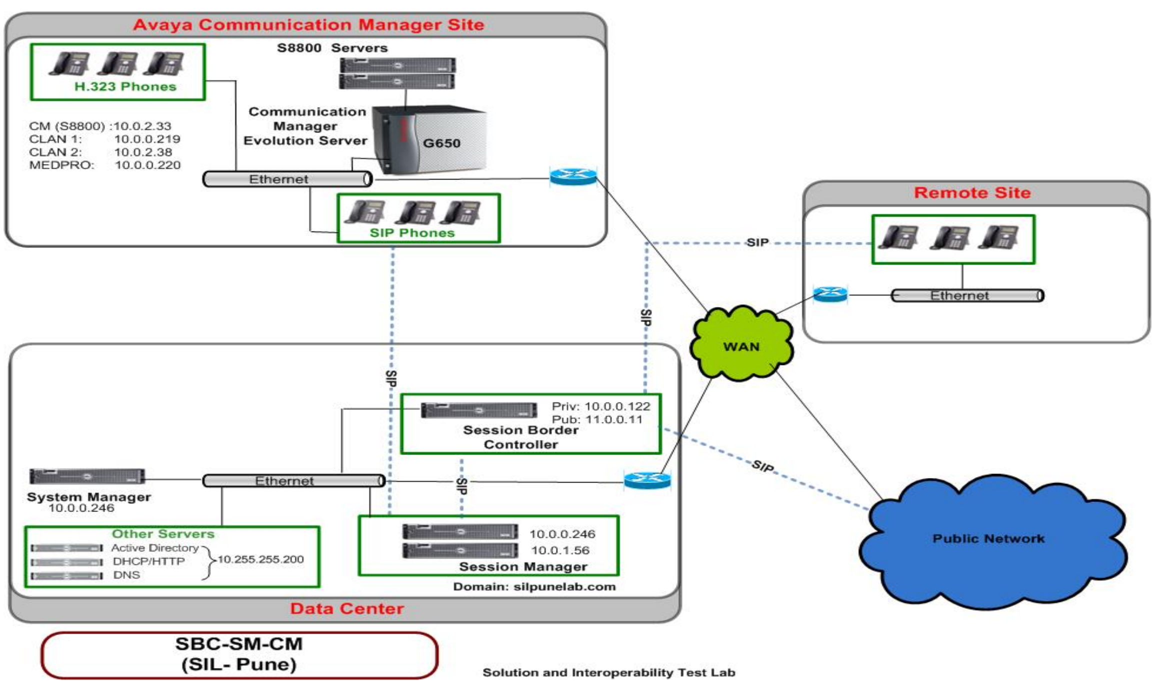


Figure 1: Test configuration

©2011 Avaya Inc. All Rights Reserved.

3. Equipment and Software Validated

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

Hardware Component	Software/Firmware Version
S8800 Media Server	Avaya Aura® Session Manager 6.1.1.0.611023
	Avaya Aura® System Manager 6.1.0 (Build No. - 6.1.0.0.7345-6.1.5.7)
S8800 Server	Avaya Aura® Session Border Controller Release 6.0.0.1.5 (GA build)
S8800 Server with G450 Media Gateway	Avaya Aura® Communication Manager 6.0.1 acting as an Evolution Server. Release: R016x.00.1.510.1
Avaya 9600 Series IP Deskphone.	SIP version 2.6.4 & H.323 version FW3.110b

©2011 Avaya Inc. All Rights Reserved.

4. Configure Avaya Aura® Communication Manager Evolution Server

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

- Verify Communication Manager license
- Configure IP node names
- Verify IP interfaces
- Configure Codec Set
- Configure Network Region
- Administer a SIP Trunk to Session Manager
- Configure Route Pattern Configure Location and Public Unknown Numbering
- View configured Dial Plan analysis
- Administer AAR Analysis
- Add station(s)
- Save Translations

Throughout this section the administration of Communication Manager is performed using a System Access Terminal (SAT). The following commands are entered on the system with the appropriate administrative permissions. Some administration screens have been abbreviated for clarity.

These instructions assume that the Communication Manager has been installed, configured, licensed and provided with a functional dial plan. Refer to the appropriate documentation as described in references for more details**.**

©2011 Avaya Inc. All Rights Reserved.

4.1. Verify Communication Manager License

Use the **display system-parameters customer-options** command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections. Verify the highlighted value, as shown below.

```
display system-parameters customer-options                      Page   2 of 11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 1129
           Maximum Concurrently Registered IP Stations: 18000 14
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 5
                   Maximum Video Capable IP Softphones: 18000 415
                       Maximum Administered SIP Trunks: 24000 2953
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 18
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   4
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

If there is insufficient capacity of SIP Trunks or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

4.2. Configure IP Node Names

All SIP signaling with Session Manager is carried through an IP-interface. When configuring a SIP Trunk in Communication Manager, use the IP-address of the Session Manager’s SIP Entity interface.

Use the **change node-names ip** command to add the **Name** and **IP Address** for the Session Manager. In the sample configuration, **ASMC** and **10.0.0.246** were used.

```
change node-names ip                                       Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASMA                10.0.0.247
ASMC                10.0.0.246
CLAN_1a04           10.0.0.219
Clan_1a09           10.0.2.38
Clan_3a04           10.0.2.126
```


©2011 Avaya Inc. All Rights Reserved.

4.3. Configure IP Codec Sets

Use the command **change ip-codec-set n** command where **n** is the codec set used in the configuration. Enter the following values:

- **Audio Codec** Set for **G.711MU/ G.711A**.
- **Silence Suppression**: Retain the default value **n.**
- **Frames Per Pkt:** Enter **2**.
- **Packet Size (ms):** Enter **20**.

Retain the default values for the remaining fields, and submit these changes.

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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2: G.711A            n          2        20
```

4.4. Configure IP Network Region

Use the **change ip-network-region n** command**,** where **n** is the number of the network region used and set the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields to **yes**. For the **Codec Set** enter the corresponding audio codec set configured in previous section. Set the **Authoritative Domain** to the SIP domain. Retain the default values for the remaining fields, and submit these changes.

Note: In the test configuration, **network region 1** was used. When creating a new network region or modifying another one, ensure to configure it with the correct parameters.

```
change ip-network-region 1                                         Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: silpunelab.com
    Name: default
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
```


©2011 Avaya Inc. All Rights Reserved.

4.5. Verify IP Interface

Use the **change ip-interface procr** command to verify procr interface on Communication Manager to communicate with Session Manager.

```
change ip-interface procr                                   Page   1 of   2
                                  IP INTERFACES
                  Type: PROCR
                                                     Target socket load: 19660
      Enable Interface? y                            Allow H.323 Endpoints? y
                                                     Allow H.248 Gateways? y
      Network Region: 1                              Gatekeeper Priority: 5
                                 IPV4 PARAMETERS
      Node Name: procr                               IP Address:
      Subnet Mask: /24
```

4.6. Add SIP Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number, for one of the SIP trunks to Session Manager, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type:** sip
- **Transport Method:** tcp
- **Peer Detection Enabled?:** y
- **Peer Server:** SM
- **Near-end Node Name:** procr
- **Far-end Node Name:** Session Manager node name from **section 4.2.**
- **Near-end Listen Port:** 5060
- **Far-end Listen Port:** 5060
- **Far-end Network Region:** 1
- **Far-end Domain:** silpunelab.com
- **IMS Enabled?:** n

```
add signaling-group 1                                         Page   1 of   1
                                SIGNALING GROUP
 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                              SIP Enabled LSP? n
     IP Video? y          Priority Video? y      Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM
   Near-end Node Name: procr             Far-end Node Name: ASMC
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1
                                   Far-end Secondary Node Name:
Far-end Domain: silpunelab.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? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                  Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 6
```


©2011 Avaya Inc. All Rights Reserved.

4.7. Configure a SIP Trunk Group

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type:** sip
- **Group Name:** A descriptive name
- **TAC:** An available trunk access code i.e., **#01**
- **Service Type:** tie
- **Signaling Group:** signaling group number added in **section 4.6** i.e., **1**
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total trunks available from licensed verified in **section 4.1**)

Note: the number of members determines how many simultaneous calls can be processed by the trunk through Session Manager.

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

Group Number: 1                  Group Type: sip          CDR Reports: y
  Group Name: To ASMC                  COR: 1        TN: 1        TAC: #01
   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: 1
                                                   Number of Members: 50
```

Navigate to **page 3** and change **Numbering Format** to **public.** Use default values for all other fields. Submit these changes.

```
add trunk-group 1                                     Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                Maintenance Tests? y


                  Numbering Format: public
                                          UUI Treatment: service-provider
```


©2011 Avaya Inc. All Rights Reserved.

4.8. Configure Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use **change route pattern n** command, where **n** is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name:** A descriptive name i.e., **to asmc**
- **Grp No:** The trunk group number from **section 4.7.**
- **FLR:** Enter a level that allows access to this trunk, with **0** being least restrictive.

```
change route-pattern 1                                         Page   1 of   3
                    Pattern Number: 1   Pattern Name: to asmc
                             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: 1    0                    0                                        n   user
 2: 6    0                    0                                        n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC   ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                       Subaddress
 1: y y y y y n  n            rest                                          none
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
```

4.9. View Configured Dial Plan

The system was configured with a 5-digit dialplan. As shown below, dialed strings that begin with 62 with a total length of 4 are assigned to extension numbers. Dialed strings that begin with 61 with a total length of 5 will be routed to Session Border Controller using AAR tables. Dialplan can be verified with the **display dialplan analysis** command. Note extensions used are in the range 6200-6299 and set 61000-61999 to AAR.

```
display dialplan analysis                                      Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 4

    Dialed    Total  Call     Dialed    Total  Call     Dialed    Total  Call
    String    Length Type     String    Length Type     String    Length Type
   4            4   ext
   61           5   aar
   62           4   ext
   8            1   fac
   9            1   fac
   *            3   fac
   #            3   dac
```


©2011 Avaya Inc. All Rights Reserved.

4.10. Configure Public Unknown Numbering

Use the **change public-unknown-numbering 1** command, to define the calling party number to be sent to Session Border Controller. Add an entry for the trunk group defined in **section 4.7.** In the example shown below, all calls originating from a 4-digit extension beginning with "62" and routed to trunk group 1 will result in a 5-digit calling number. The calling party number will be in the SIP "From" header. Submit these changes.

For Communication Manager:

- **Ext Len:** Number of digits for extension. i.e., **4**
- **Trk Grp:** Trunk group number. i.e., 1
- **Ext Code:** Enter range for CM extensions. i.e., 62

```
change public-unknown-numbering 1                                   Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                 Total Administered: 2
 5  62             1                         5       Maximum Entries: 9999
```

4.11. Administer AAR Analysis

This section provides sample Automatic Alternate Routing (AAR) used for routing calls with dialed digits 61xxx to SBC via SM. Note that other methods of routing may be used. Use the **change aar analysis 0** command and add an entry to specify how to route the calls. Enter the following values for the specified fields and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case **61**
- **Total Min:** Minimum number of digits, in this case **5**
- **Total Max:** Maximum number of digits, in this case **5**
- **Route Pattern:** The route pattern number from **section 4.8**. i.e., **1**
- **Call Type:** aar

```
change aar analysis 6                                                Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 1

          Dialed           Total     Route    Call   Node   ANI
          String          Min  Max  Pattern   Type   Num    Reqd
    61                    5    5     1        aar           n
```


©2011 Avaya Inc. All Rights Reserved.

4.12. View Feature Access Code

To view the Feature-access-code configuration, execute **display feature-access-codes** command note “8” is used as AAR the feature-access-code.

```
display feature-access-codes                                  Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code: #35
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *64    Deactivation: *36
Call Forwarding Activation Busy/DA: *91    All: *90    Deactivation: #90
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: #30
                       Call Pickup Access Code: *37
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code: *77
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

4.13. Save Translations

Configuration of Communication Manager is complete. Use the **save translation** command to save these changes.

```
save translation
                               SAVE TRANSLATION

 Command Completion Status                        Error Code          Success
```


©2011 Avaya Inc. All Rights Reserved.

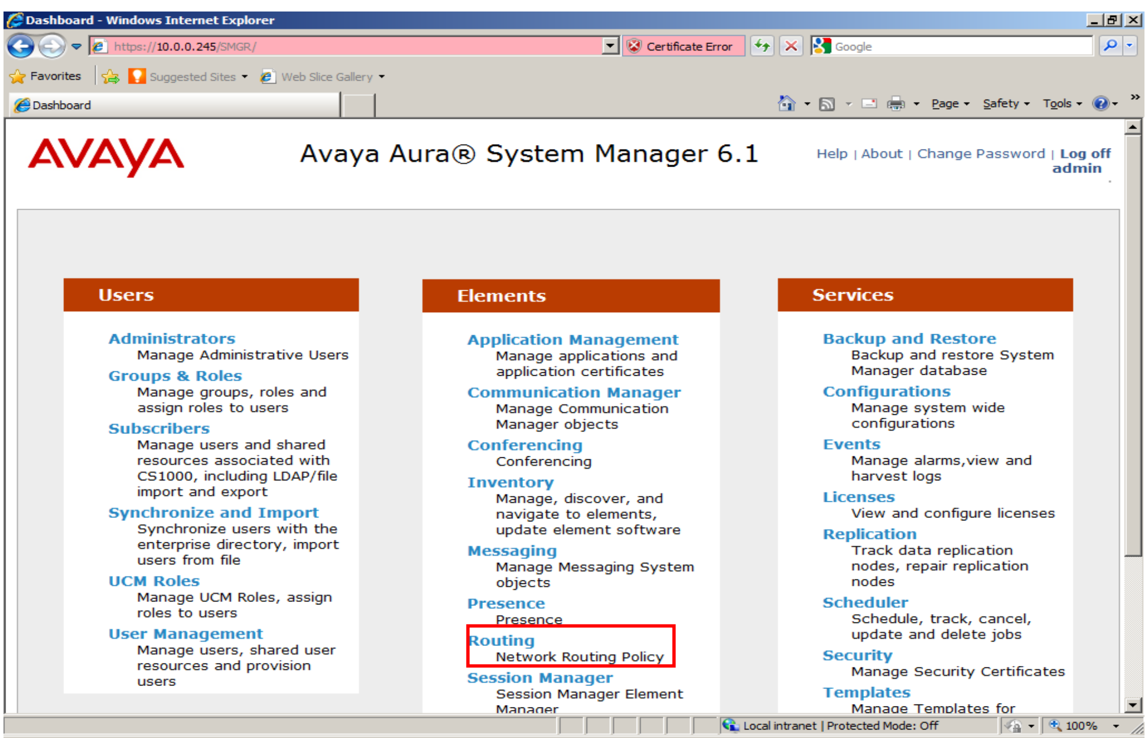
5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, assuming it has been installed and licensed as described in the references. The following steps describe configuration of Session Manager for:

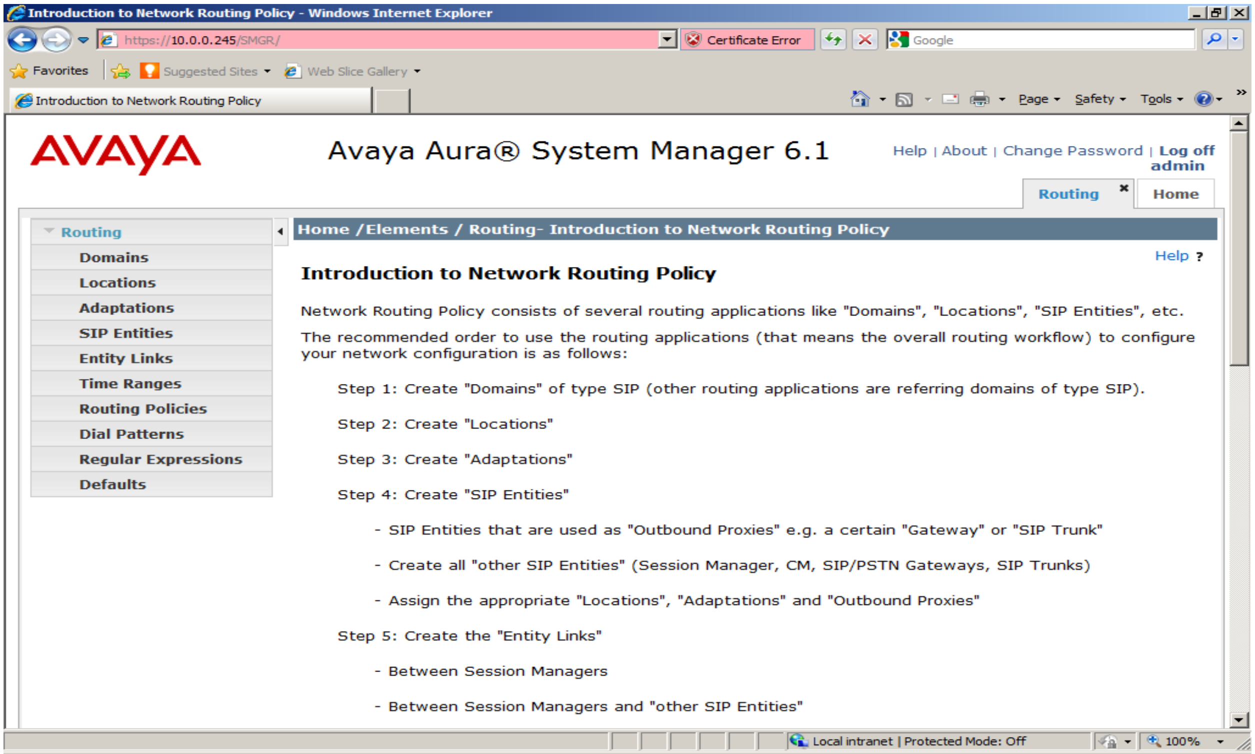
- Access Avaya Aura® Session Manager.
- Add SIP Domain.
- Add Location.
- Administer Avaya Aura® Session Manager SIP Entity.
- Administer Avaya Aura® Communication Manager Evolution Server SIP Entity.
- Administer Avaya Aura® Session Border Controller Entity.
- Administer SIP Entity Link.
- Administer Time ranges.
- Administer Route Policies.
- Administer Dial Pattern.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR** where **<ip-address>** is the IP address of System Manager. Log in to the system with valid credentials. The menu shown below is displayed. Click on the **Routing** link as shown in snapshot below. The sub-menus displayed in the left column below will be used to configure all but the last of the above items

Log in to the system with valid credentials. The menu shown below is displayed. Select the **Routing** link in the **Elements** section as shown.



The sub-menus displayed in the left column below will be used to configure call routing for Session Manager.

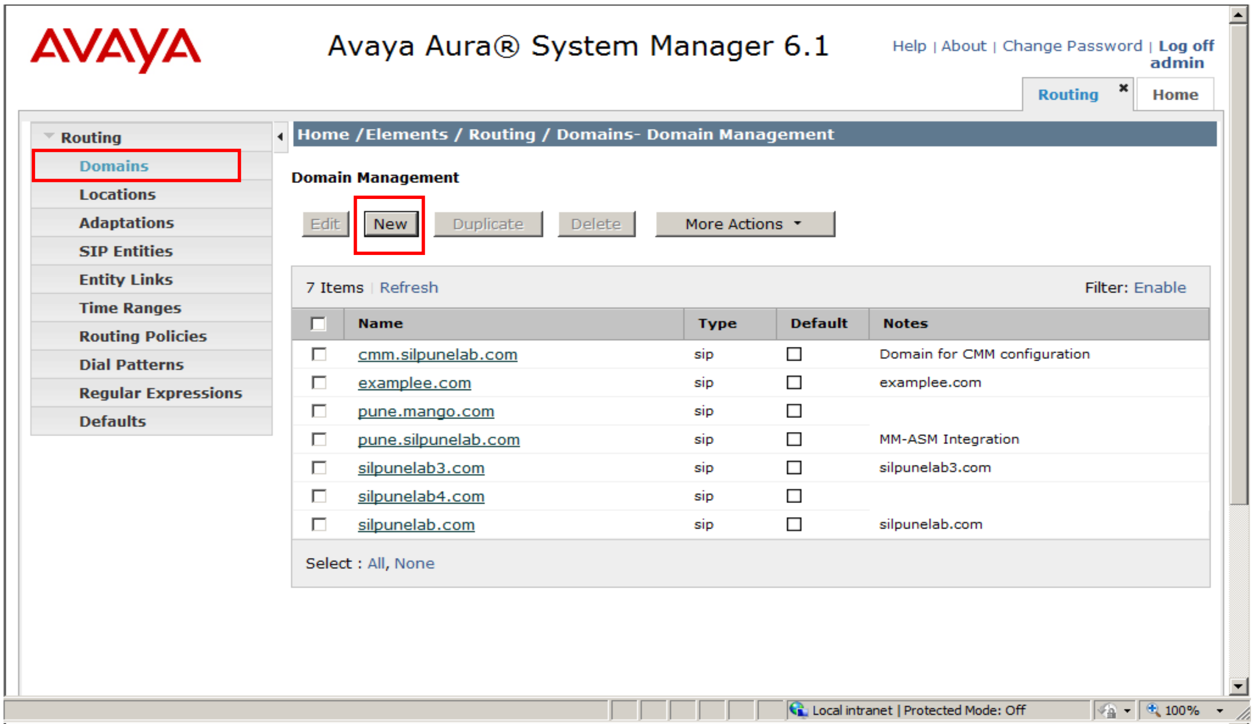


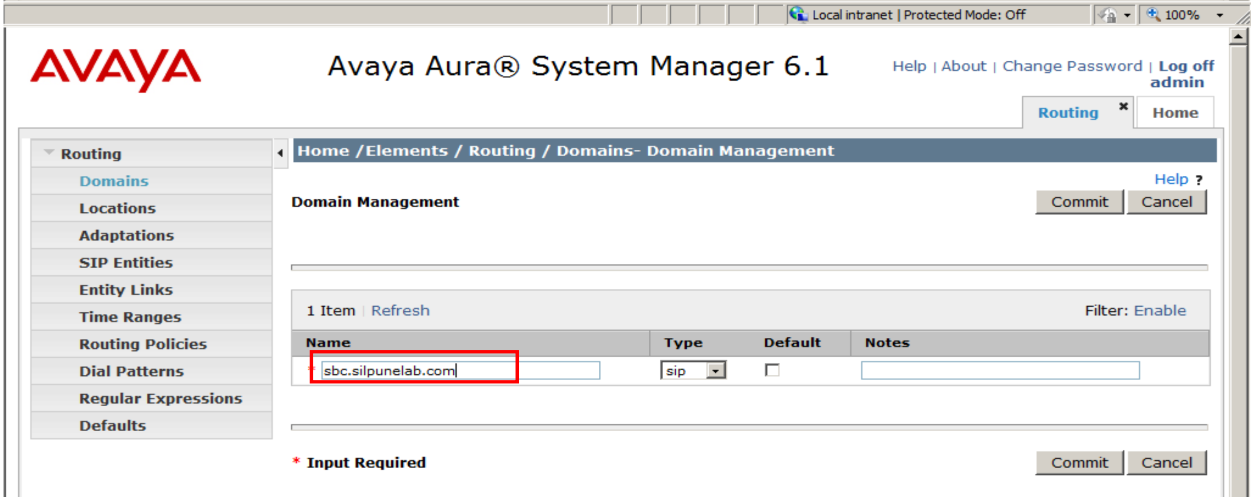
©2011 Avaya Inc. All Rights Reserved.

5.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **Domains** on the left and clicking the **New** button on the right. The following screens will then be shown. Fill in the following fields and click **Commit**.

- **Name:** The authoritative domain name (e.g., sbc.silpunelab.com)
- **Notes:** Descriptive text (optional).





©2011 Avaya Inc. All Rights Reserved.

5.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management. Location is added to the configuration for Communication Manager and Session Border Controller. 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:

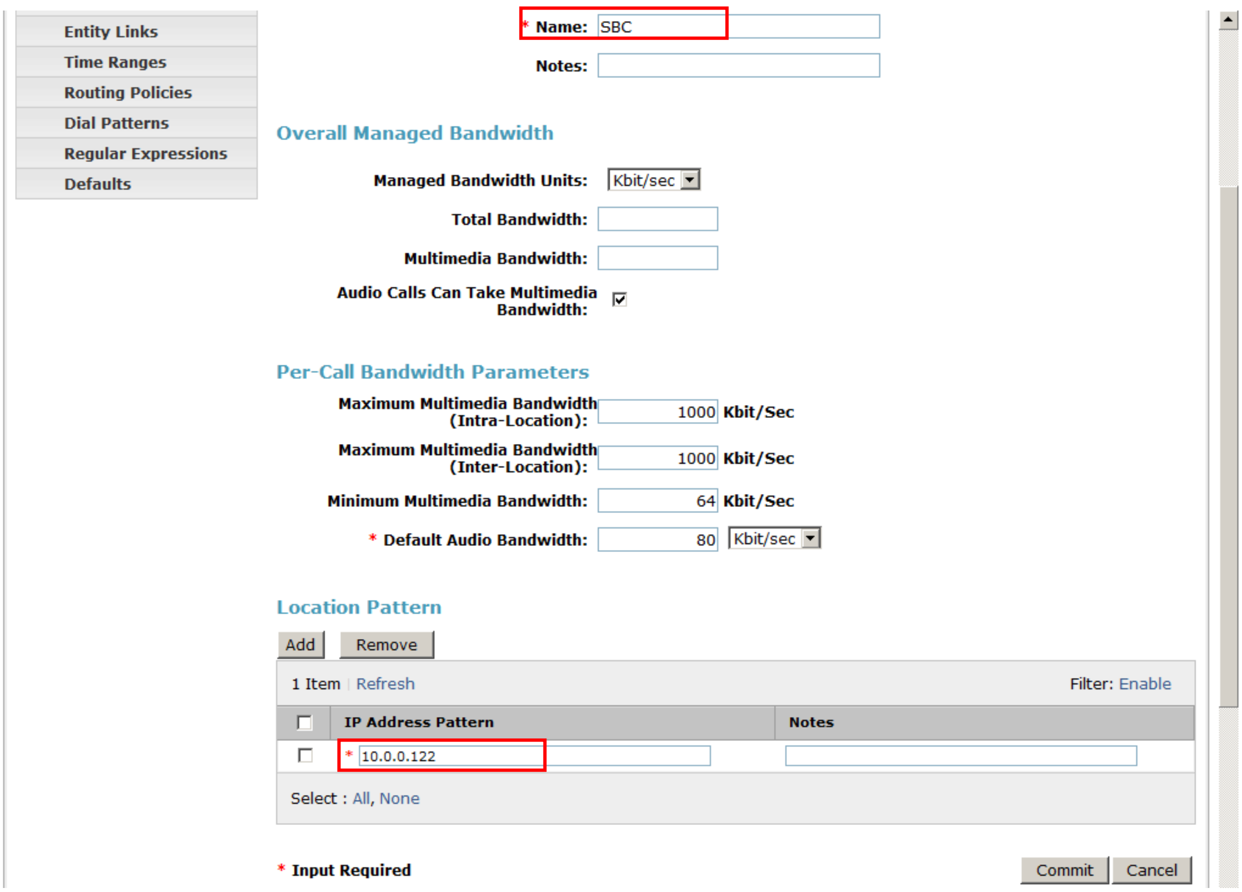
Under ***General***:

- **Name:** A descriptive name for Session Border Controller.
- **Notes:** Descriptive text (optional).
- **Managed Bandwidth:** Use the default value.

Under ***Location Pattern***:

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

After entering the location details for Session Border Controller, click **Commit** button to save.



©2011 Avaya Inc. All Rights Reserved.

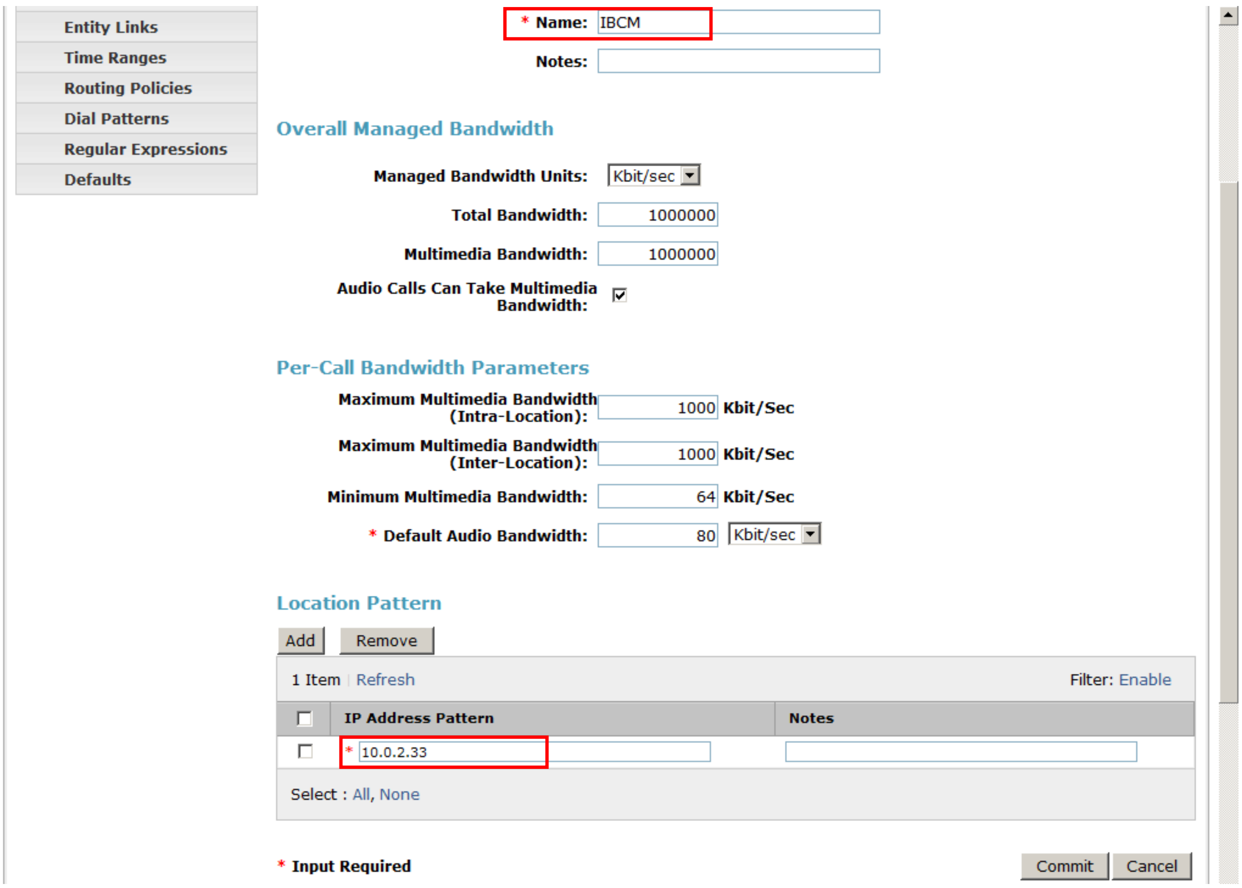
Add Location for Communication Manager.

Under ***General***:

- **Name:** A descriptive name for Communication Manager.
- **Notes:** Descriptive text (optional).
- **Managed Bandwidth:** Use the default value.

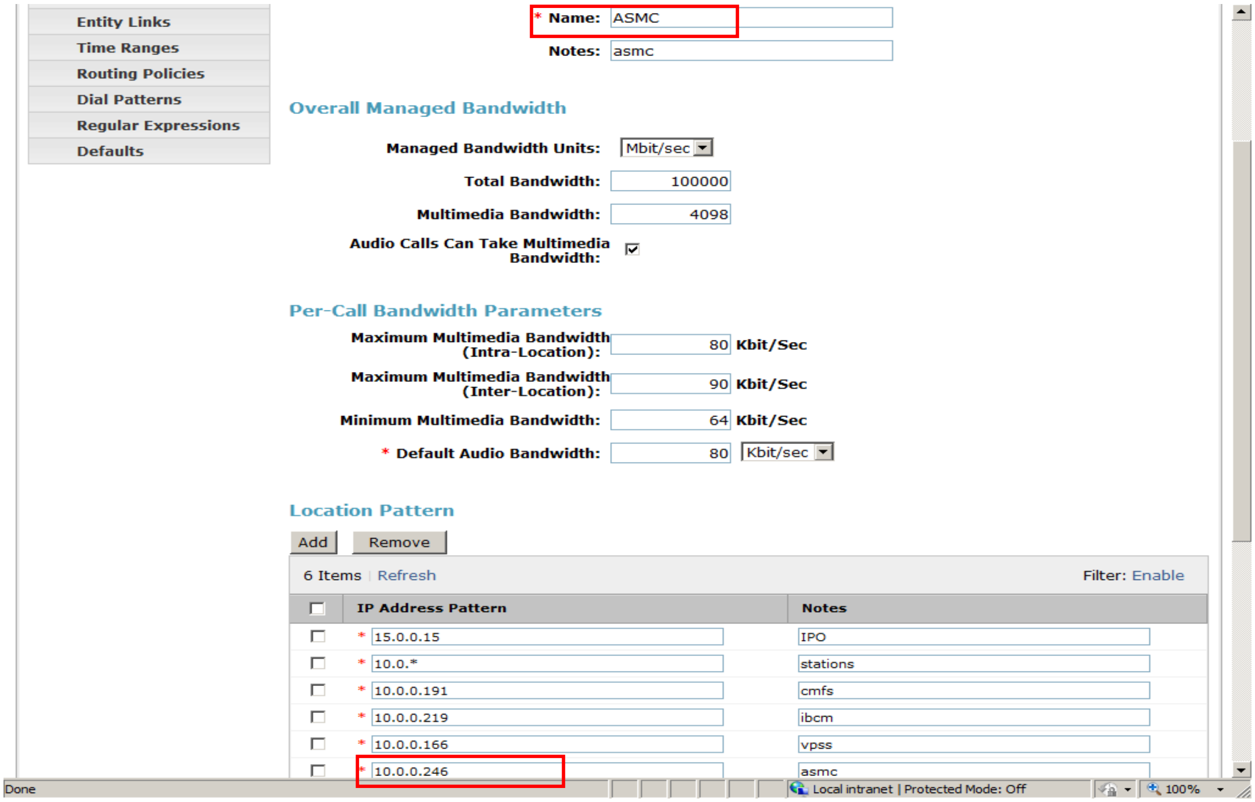
Under ***Location Pattern***:

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



©2011 Avaya Inc. All Rights Reserved.

Verify the Location for Session Manager. Note this configuration is done during installation of Session Manager.



5.3. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system communicating with it using SIP trunks. In the sample configuration, the following SIP entities were added:

- Communication Manager (**IBCM**), and
- Session Border Controller (**SBC**).

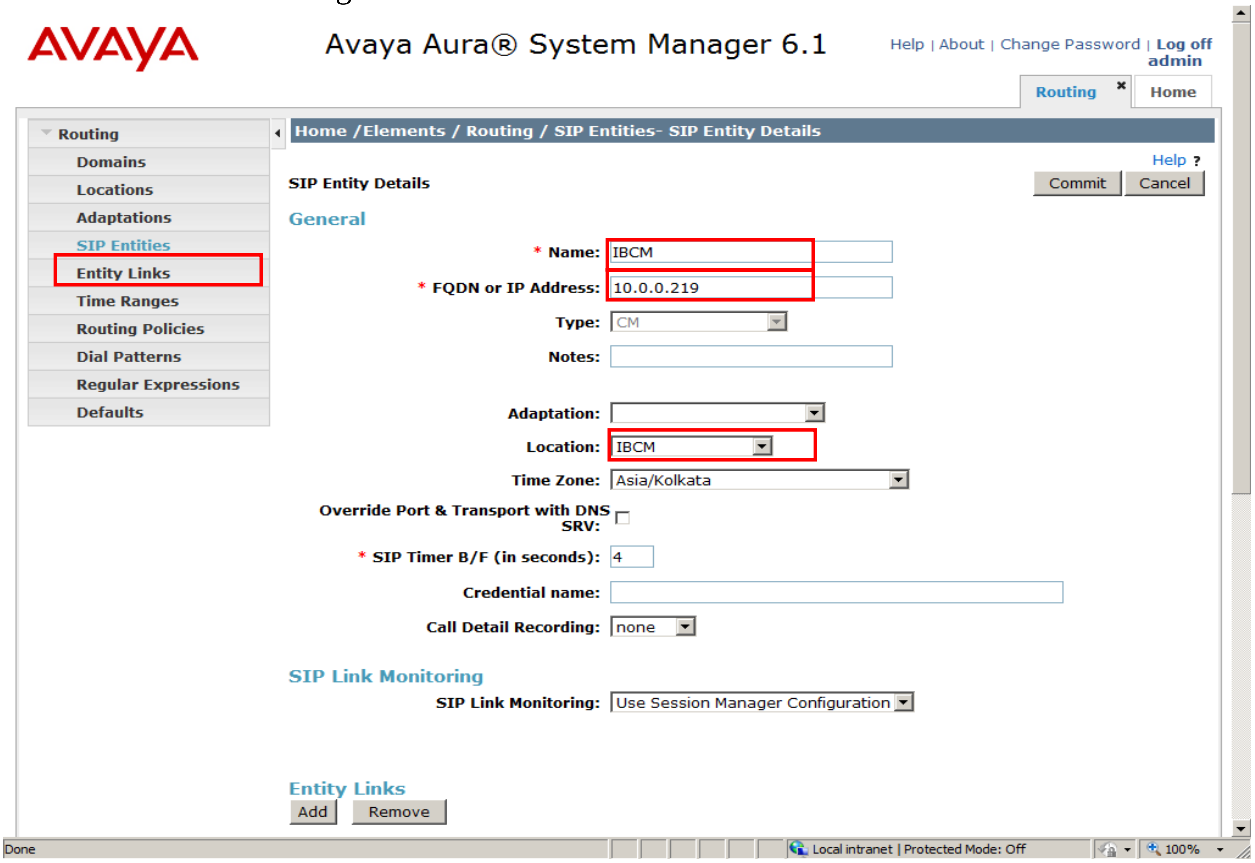
To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:
Under ***General***:

- **Name:** A descriptive name for Communication Manager.
- **FQDN or IP Address:** IP address of the signaling interface
- **Type:** **CM** for Communication Manager
- **Location:** Select one of the locations defined previously. i.e., **IBCM**
- **Time Zone:** Time zone for this location.

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

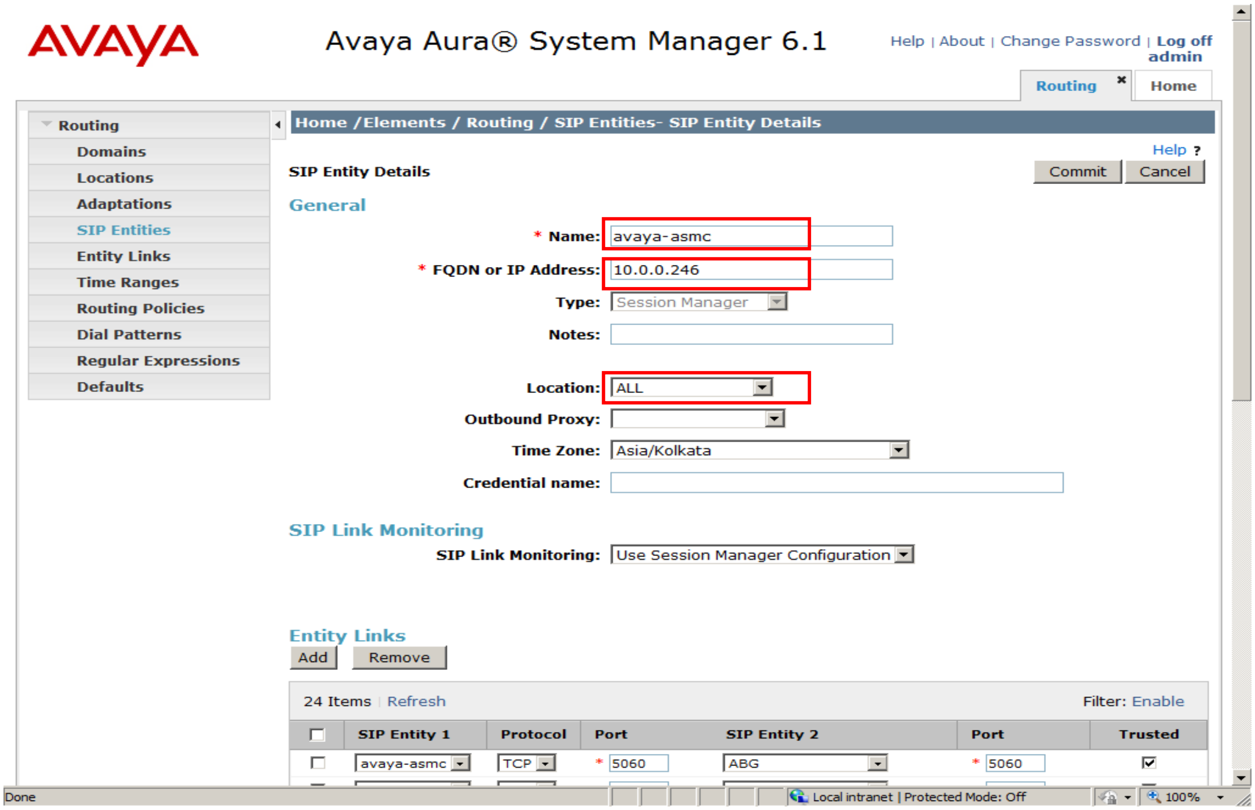
©2011 Avaya Inc. All Rights Reserved.

The following screen shows the addition of Communication Manager. The IP address used is that of the “procr” as configured in **section 4.5**. Keep **Adaptation** as blank. **Location** is IBCM for Communication Manager



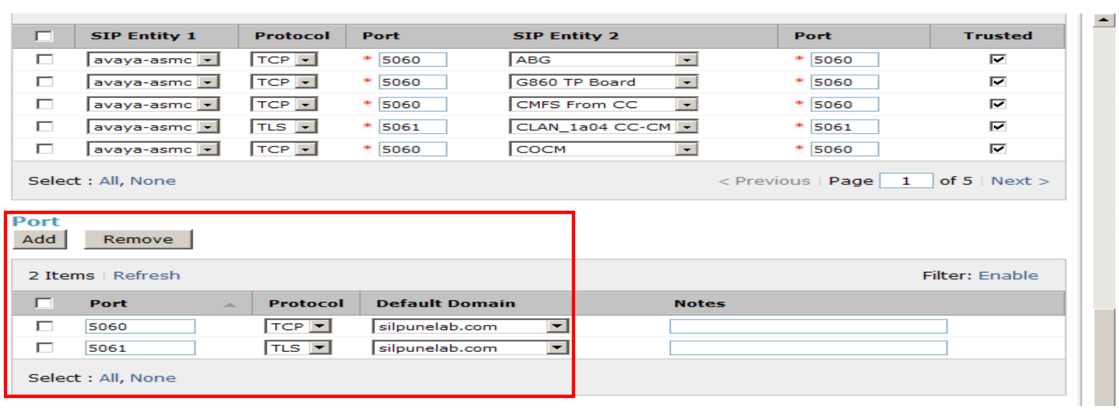
©2011 Avaya Inc. All Rights Reserved.

Note the screen shot below shows configuration of Session Manager. The IP address used is that of the SIP Entity Interface configured on the Session Manager.



For Session Manager, there is additional Port configuration as shown below.

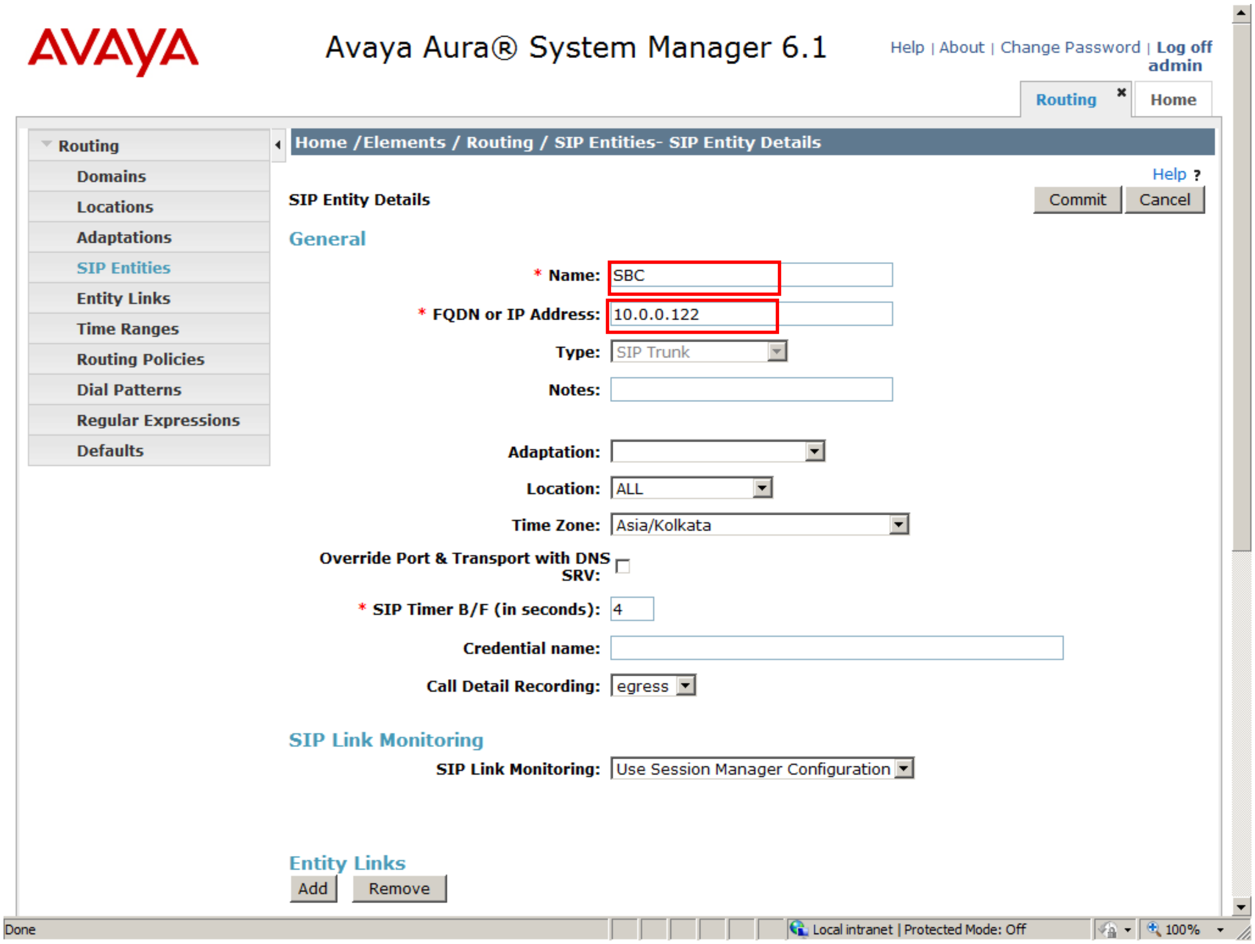
- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests i.e., TCP
- **Default Domain** The domain used for the enterprise



©2011 Avaya Inc. All Rights Reserved.

The following screen shows the addition of Session Border Controller.

- **Name:** A descriptive name for Session Border Controller.
- **FQDN or IP Address:** IP address of the signaling interface
- **Type:** SIP Trunk
- **Location:** Select one of the locations defined previously. i.e., **SBC**
- **Time Zone:** Time zone for this location.



5.4. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

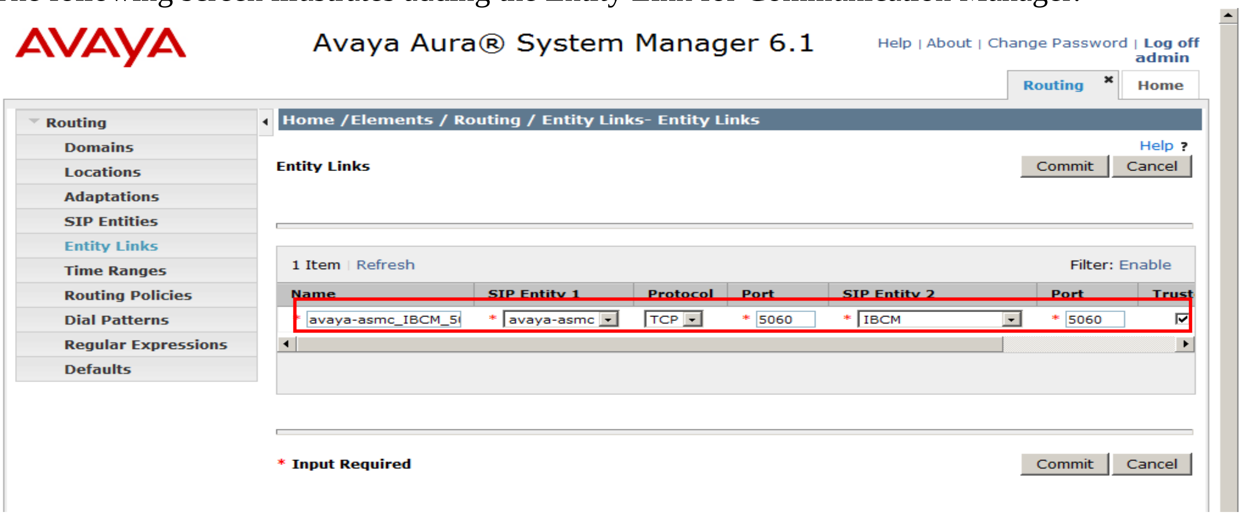
- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager entity.
- **Port:** Port number to which the other system sends SIP requests
- **SIP Entity 2:** Select the name of the other system.
- **Port:** Port number on which the other system receives SIP requests. These ports should match SIP signaling ports.

©2011 Avaya Inc. All Rights Reserved.

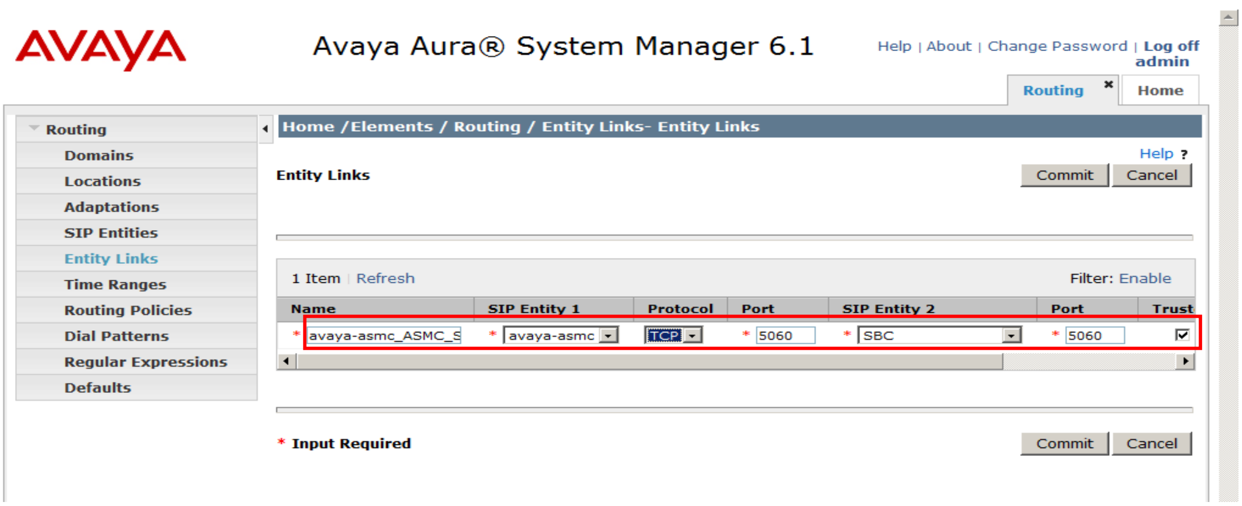
- **Trusted:** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity will be denied.
- **Protocol:** Select the transport protocol among **UDP/TCP/TLS** Check these are aligned with the definition on the other end of the link. In the example, **TCP** is used.

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

The following screen illustrates adding the Entity Link for Communication Manager.



Below is illustrated adding the Entity Link for Session Border Controller.



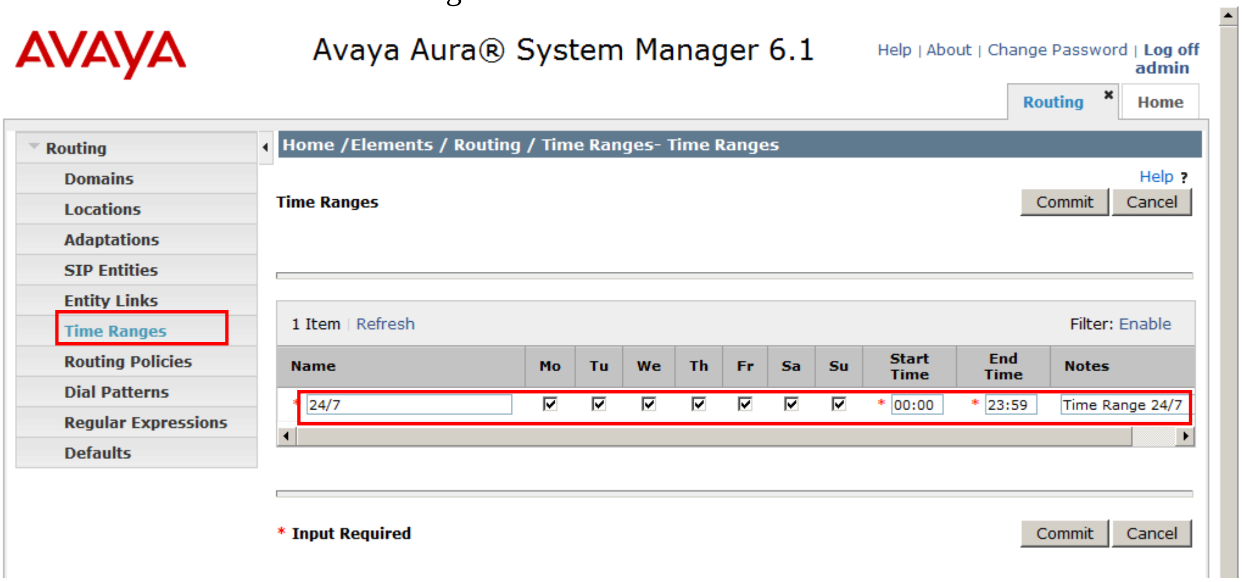
©2011 Avaya Inc. All Rights Reserved.

5.5. Add Time Ranges

Before adding routing policies (see next section), time ranges must be defined during which the policies will be active. In the sample configuration, one policy was defined that would allow routing to occur at anytime. To add this time range, select **Time Ranges** on the center of the Time Ranges page under the heading, click on the **New** button (not shown). Fill in the following:

- **Name:** A descriptive name (e.g., 24/7).
- **Mo** through **Su** Check the box under each of these headings
- **Start Time** Enter **00:00**.
- **End Time** Enter **23:59**

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



5.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **section 5.3**. Two routing policies must be added – first for Communication Manager and second for Session Border Controller.

To add a routing policy, select **Routing Policies** 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**: Enter a descriptive name for the Communication Manager policy.

Under ***SIP Entity as Destination***:

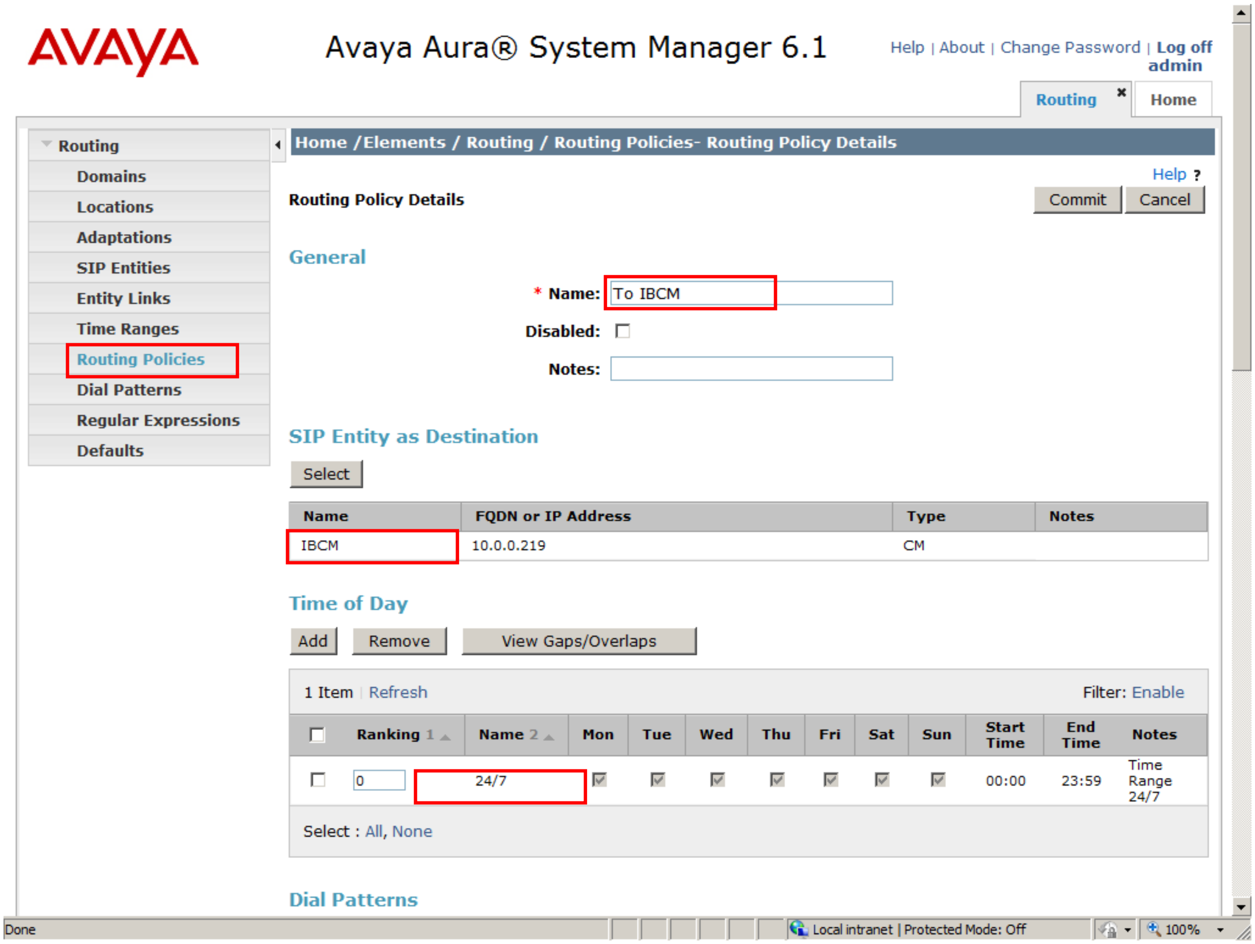
- Click **Select**, and then select the appropriate SIP entity created for Communication Manager.

Under ***Time of Day***:

- Click **Add**, and select the time range configured in the previous section.

©2011 Avaya Inc. All Rights Reserved.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition. The following screen shows the Routing Policy for Communication Manager.



Under ***General***:

- **Name**: Enter a descriptive name for Session Border Controller policy.

Under ***SIP Entity as Destination***:

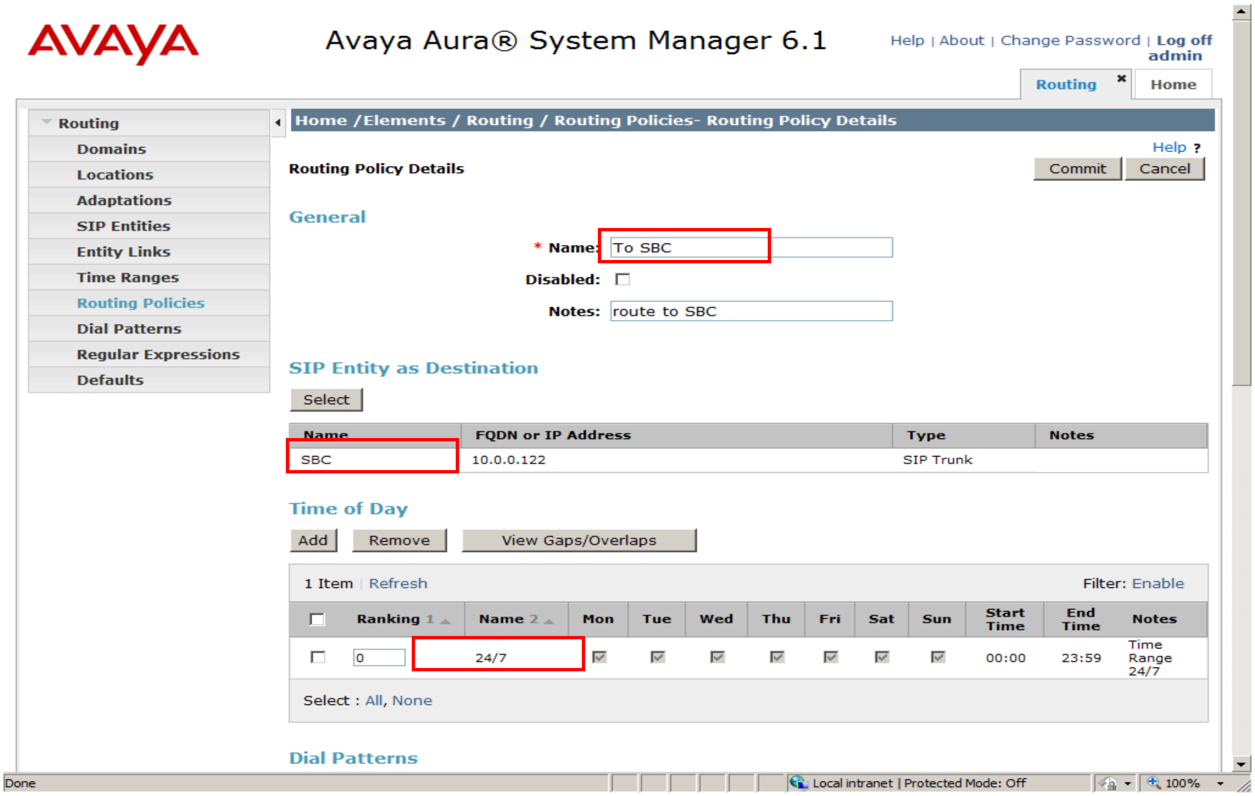
- Click **Select**, and then select the appropriate SIP entity created for Session Border Controller.

Under ***Time of Day***:

- Click **Add**, and select the time range configured in the previous section.

©2011 Avaya Inc. All Rights Reserved.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition. Below is illustrated the Routing Policy for Session Border Controller, configured in these sample application notes.



©2011 Avaya Inc. All Rights Reserved.

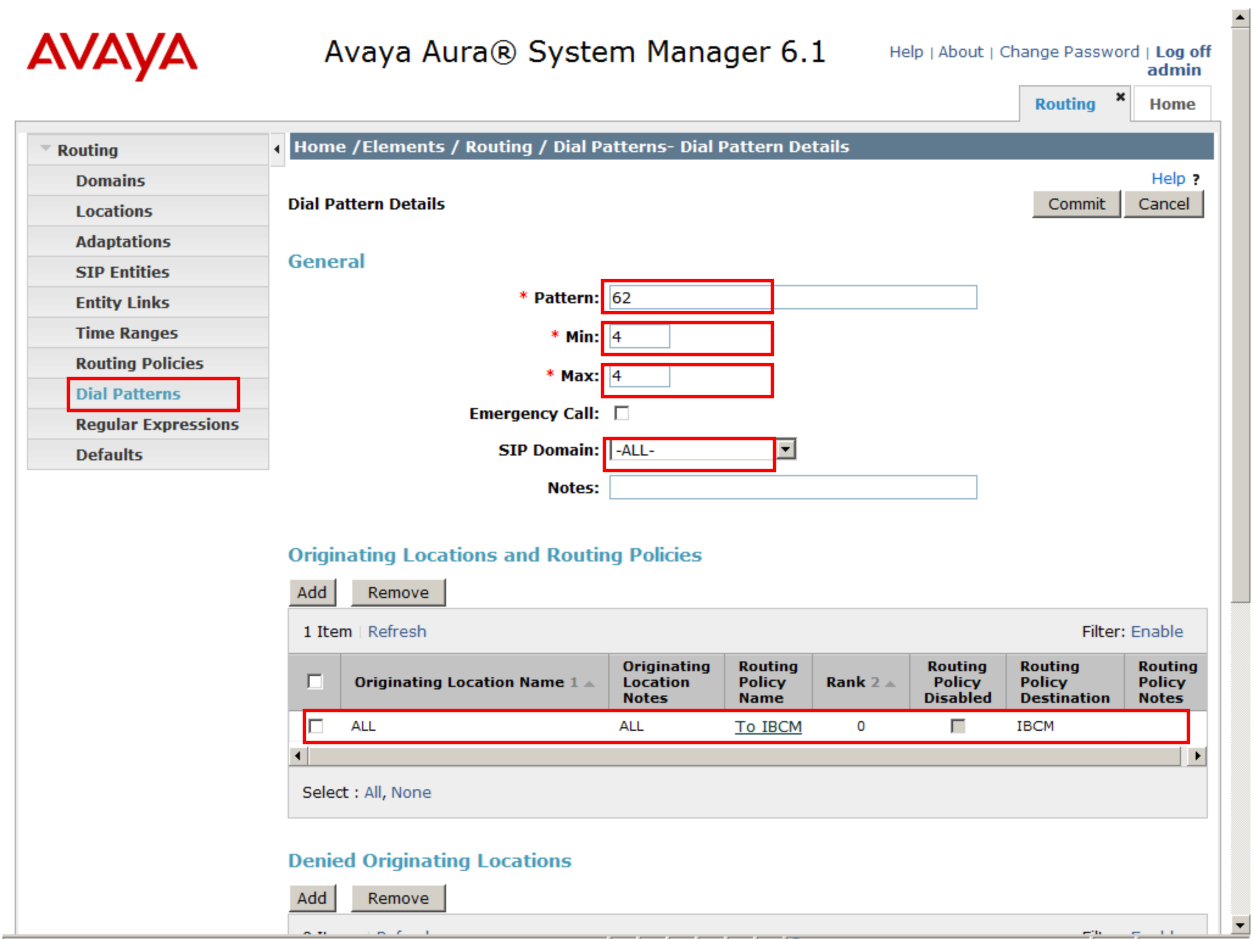
5.7. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 4-digit extensions beginning with **62** reside on Communication Manager and 5-digit starting with **61** will be routed to Session Border Controller. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Communication Manager:

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.

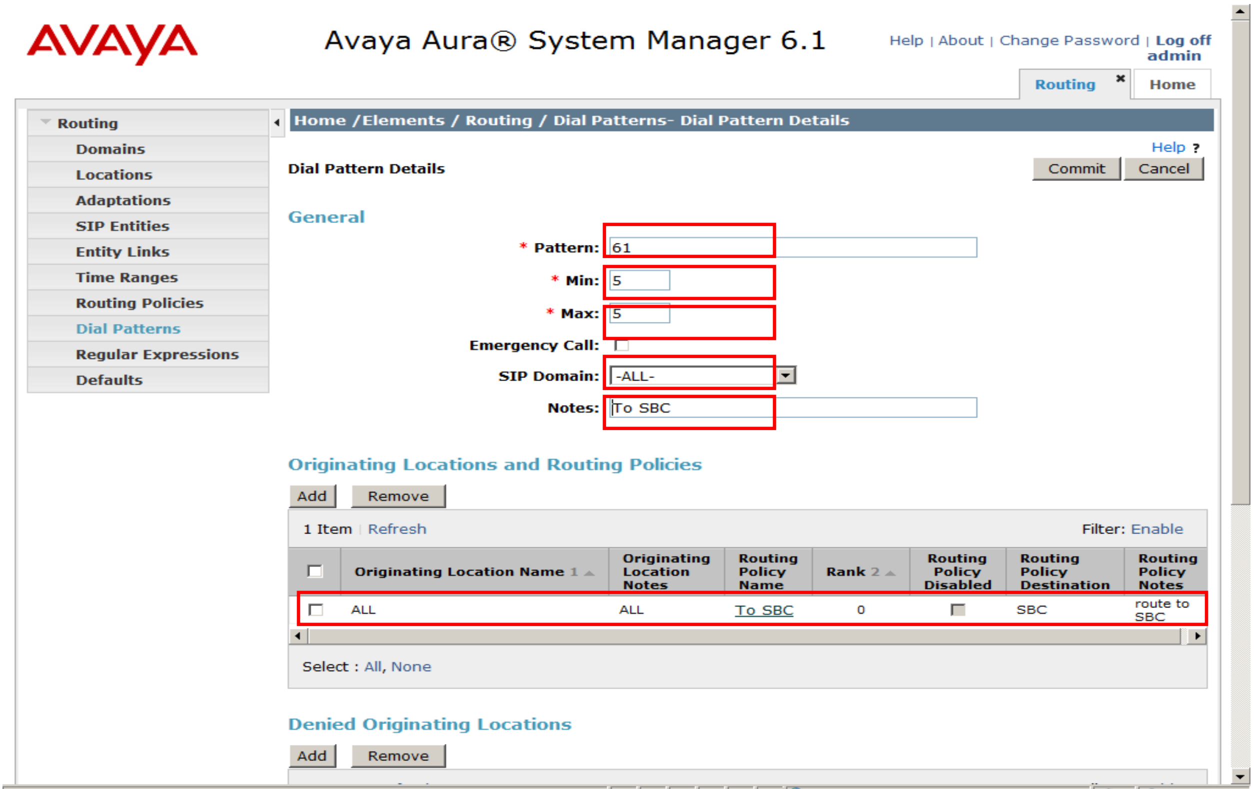
Under ***Originating Locations and Routing Policies***:
Click **Add**, and then select the appropriate location and routing policy from the list.
Default values can be used for the remaining fields. Click **Commit** to save this dial pattern.
The following screen shows the dial pattern definitions for Communication Manager.



©2011 Avaya Inc. All Rights Reserved.

The following screen shows the dial pattern definitions for Session Border Controller.

- **Pattern:** 61
- **Min** 5
- **Max** 5
- **Notes** optional descriptive text.



©2011 Avaya Inc. All Rights Reserved.

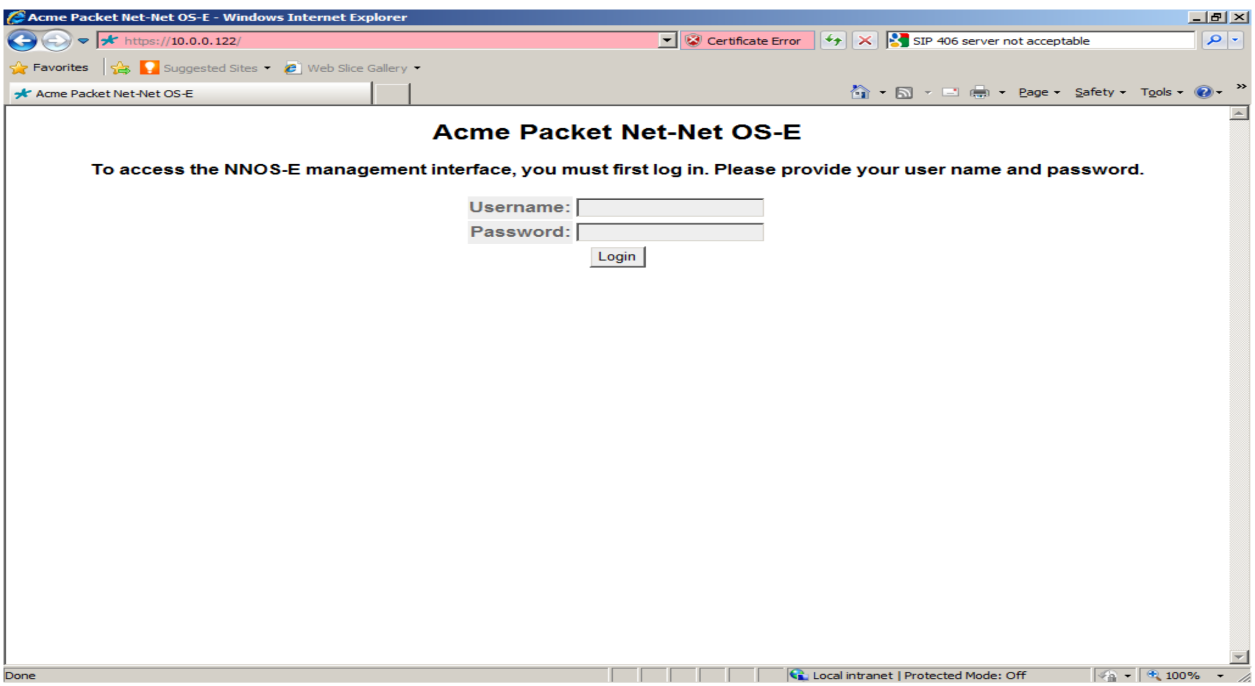
6. Configure Avaya Aura® Session Border Controller

This section provides the procedures for configuring Session Border Controller, assuming it has been installed and licensed as described in the references. The following steps describe configuration of Session Border Controller for:

- Access Avaya Aura® Session Border Controller
- Administer Ethernet Interfaces
    - Administer Ethernet private interface on eth0
    - Administer SIP TCP configuration on eth0
    - Administer public interface on eth2
    - Administer SIP TCP configuration on eth2
- Administer Enterprise PBX server
    - Administer SIP TCP configuration on PBX server
- Administer Enterprise TELCO server
    - Administer SIP TCP configuration on TELCO server

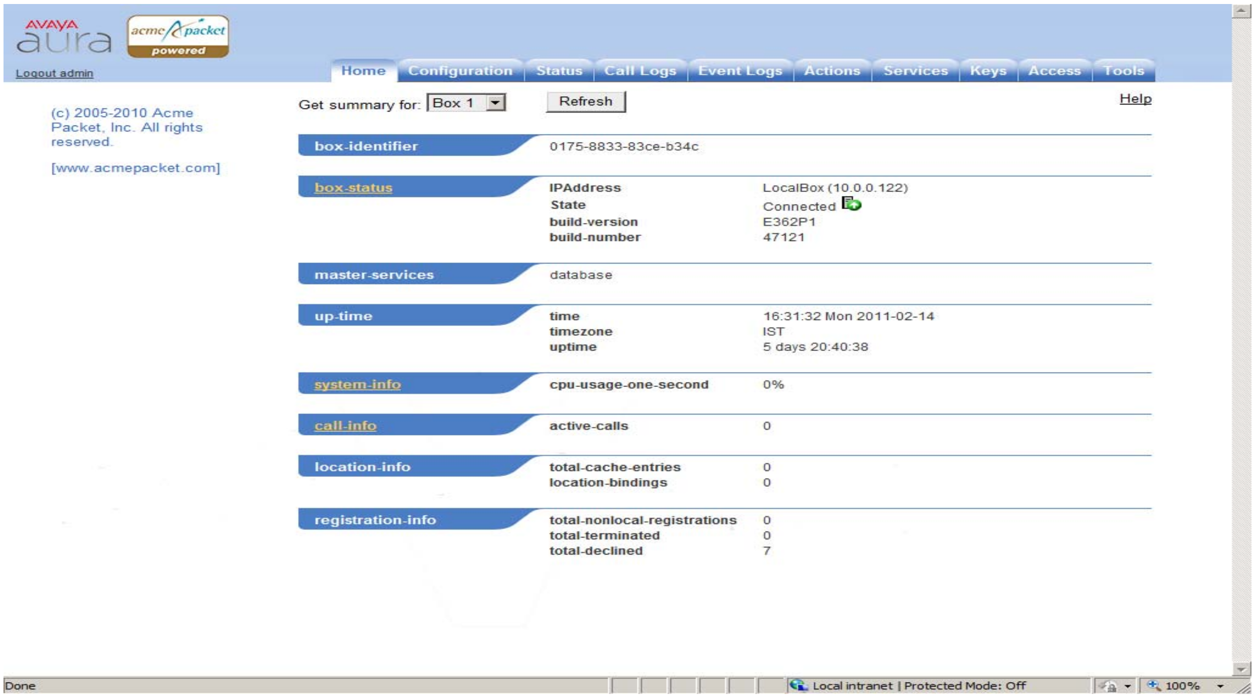
6.1. Accessing Avaya Aura® Session Border Controller

To access the Session Border Controller configuration use the browser-based GUI using the URL http://<ip-address> where **<ip-address>** is the IP-address of Session Border Controller configured on eth0 interface. Log in to the system with valid credentials.



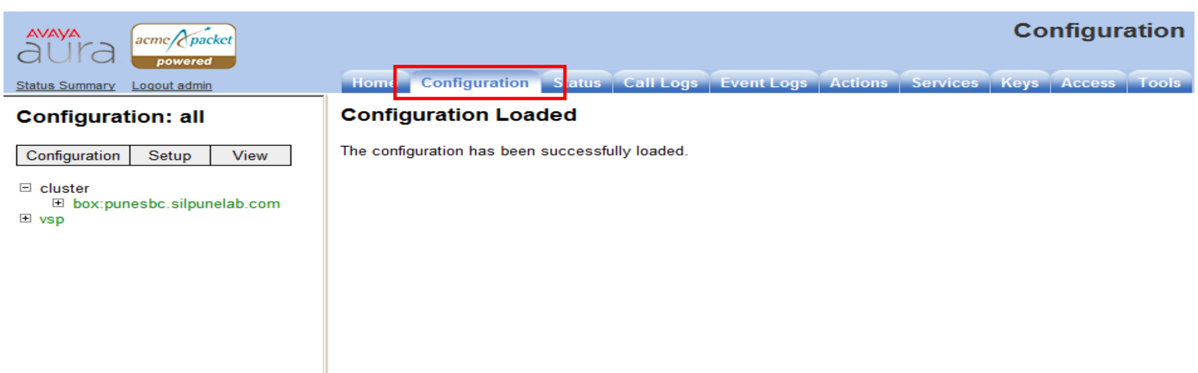
©2011 Avaya Inc. All Rights Reserved.

The Home page for Session Border Controller configuration is shown below.

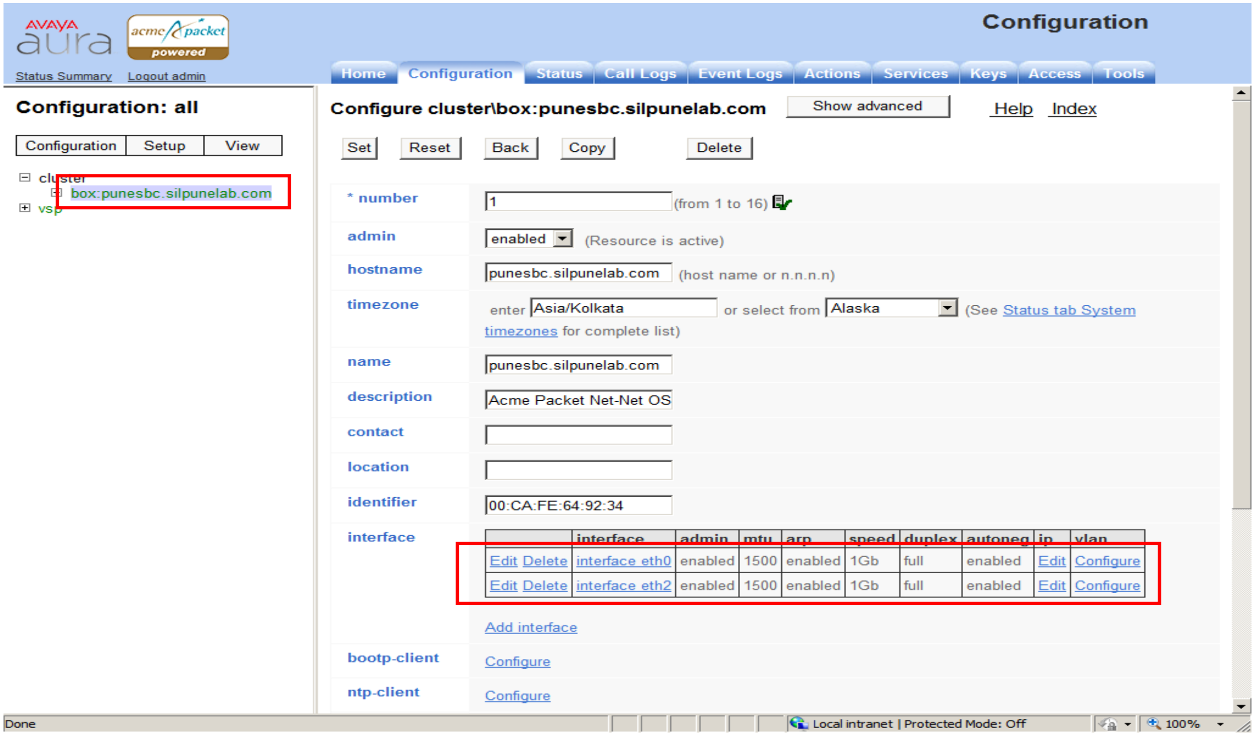


To access the configuration, click on **Configuration** tab. The web page shows two main nodes **cluster** and **vsp** as shown in left frame. By default cluster has single box configured on it. To view box configuration click on it.

Note: To update and save configuration for all the menus, click on **set** button after making changes.



The box configuration is shown below has two Ethernet interfaces configured.



Note: The hostname, timezone and the Ethernet interfaces are configured during installation of the system.

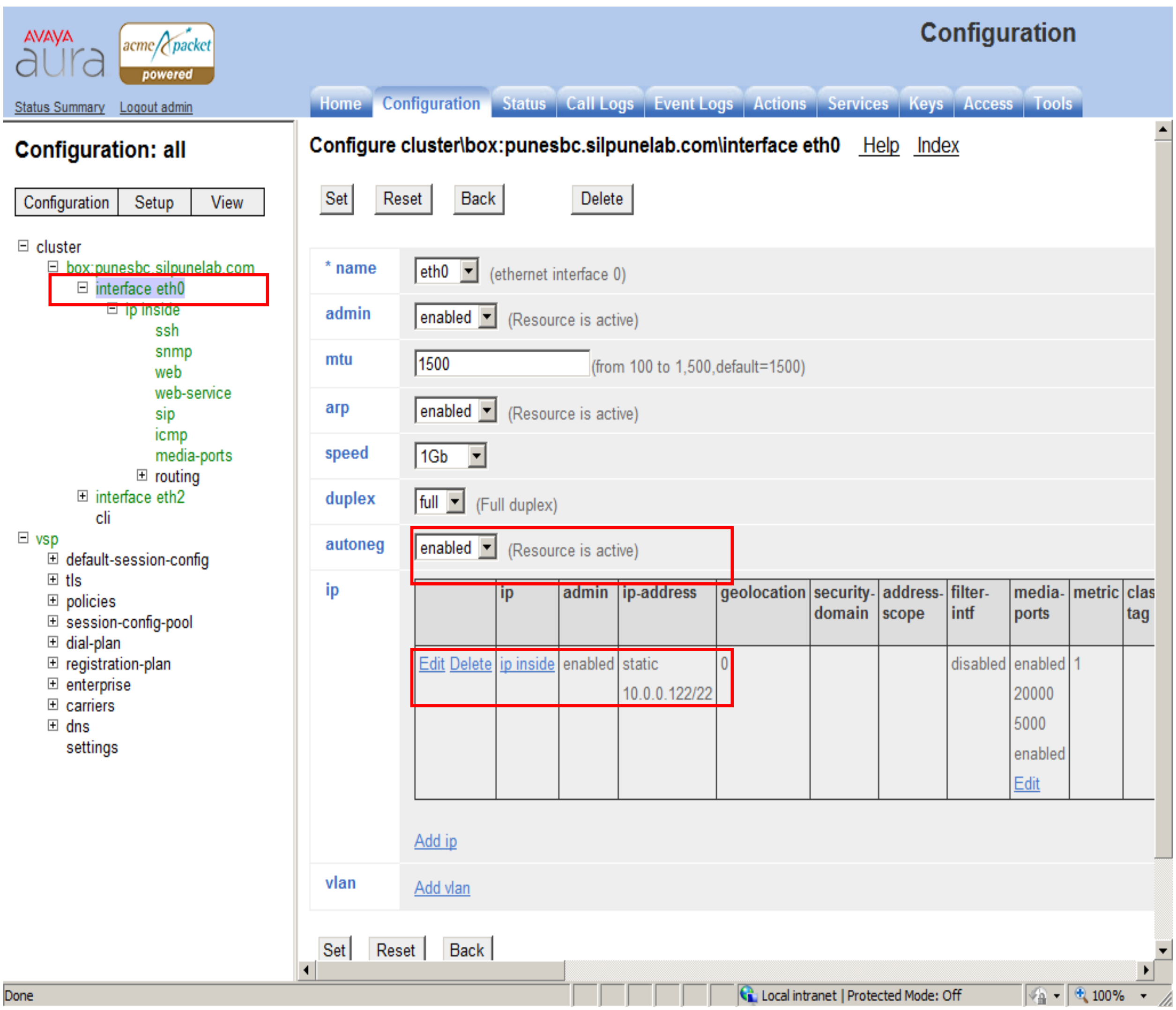
©2011 Avaya Inc. All Rights Reserved.

6.2. Configuring the Ethernet Interface

Session Border Controller sits on the edge of enterprise network. The main functionality is similar to NAT and firewall is to protect private network from intrusion from public network. It has two Ethernet interfaces one configured in private network and other in public network. Session Border Controller performs the network address translation for SIP messages and media translations going from private to public or vice-versa.

6.2.1. Configuring Private Ethernet Interface 0

The private Ethernet interface has an IP-address in the range of addresses in the private network. Verify the IP-address and net-mask assigned to the interface.

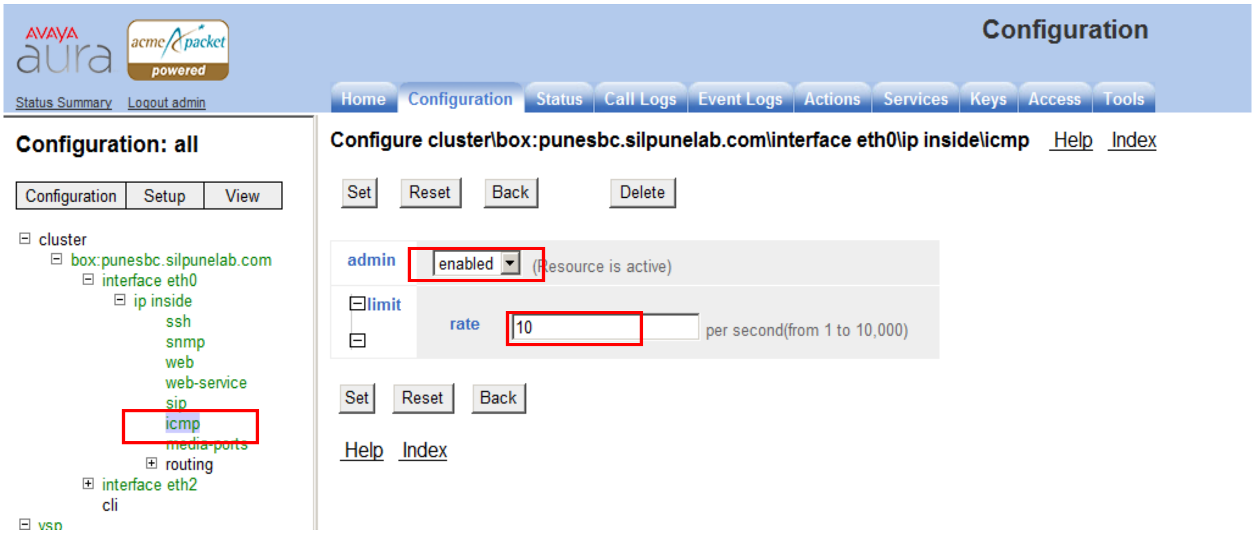


Click on **ip inside** node and configure ICMP protocol. Select ICMP link as shown in snapshot below. Verify the IP-address for private interface is pingable from private network after completing entire configuration for Session Border Controller.

©2011 Avaya Inc. All Rights Reserved.

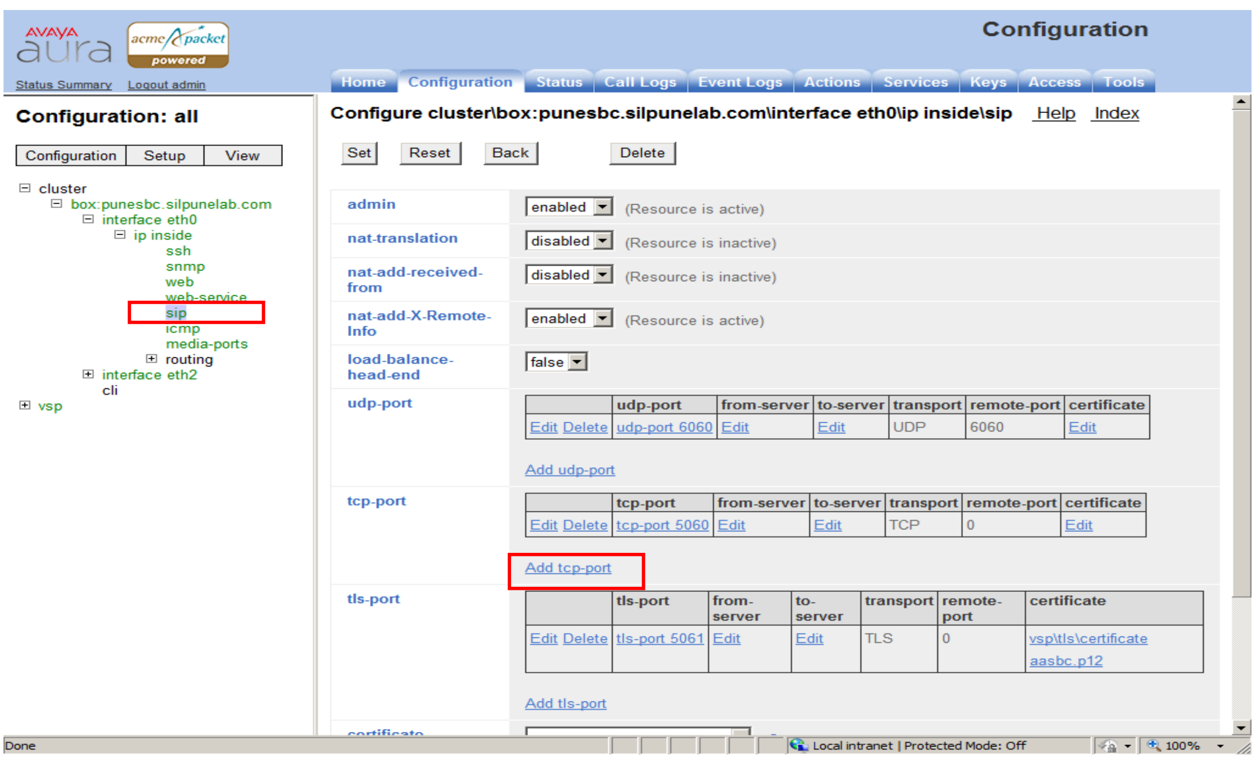
Make following changes to ICMP configuration.

- **admin**: enabled
- **rate:** 10



6.2.2. Administer SIP TCP Configuration On Eth0

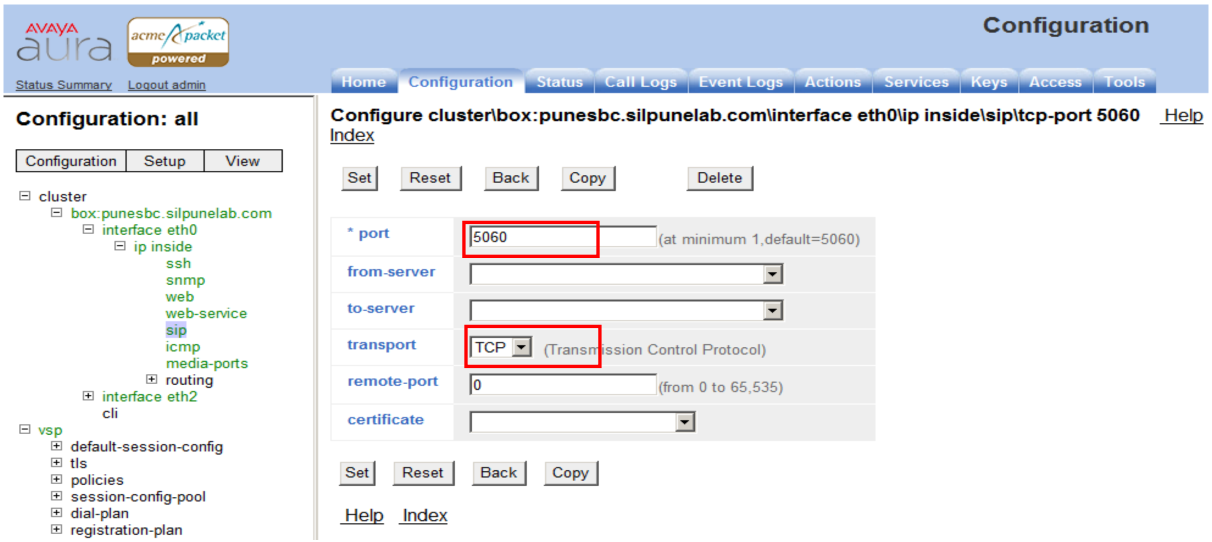
To configure TCP SIP trunk for private interface, click on interface eth0 from left frame and then click on SIP link. Click on add TCP port.



©2011 Avaya Inc. All Rights Reserved.

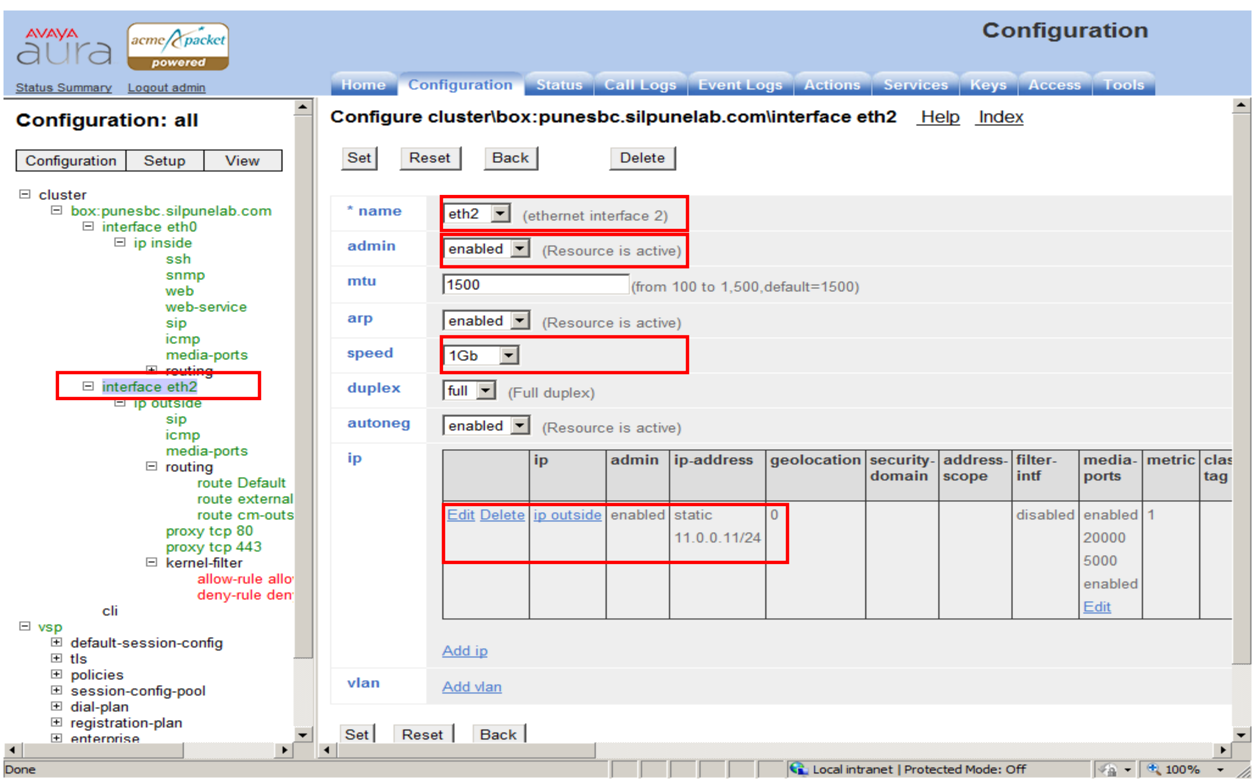
Make following changes to the configuration and click on set to save configuration.

- **Port**: 5060
- **Transport**: TCP



6.2.3. Configuring Public Ethernet Interface 2

The public Ethernet interface eth2 has an IP-address in the range of addresses in the public network. Verify the IP-address and net-mask assigned to the interface.

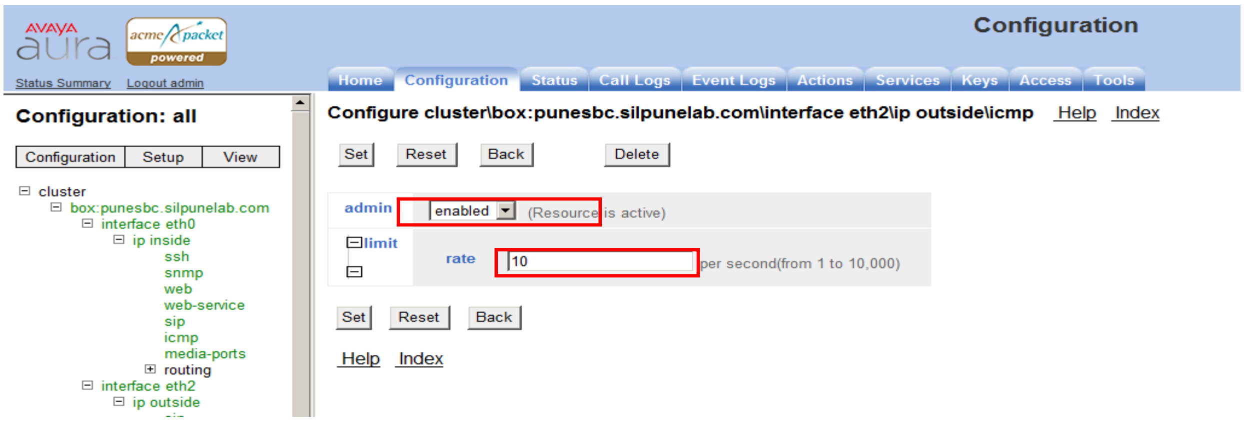


©2011 Avaya Inc. All Rights Reserved.

Click on **ip outside** node and configure ICMP protocol as shown in snapshot below. Verify the IP-address for public interface is pingable from public network. Note the public and private network are configured in different subnets.

Make following changes to ICMP configuration.

- **admin**: enabled
- **rate:** 10

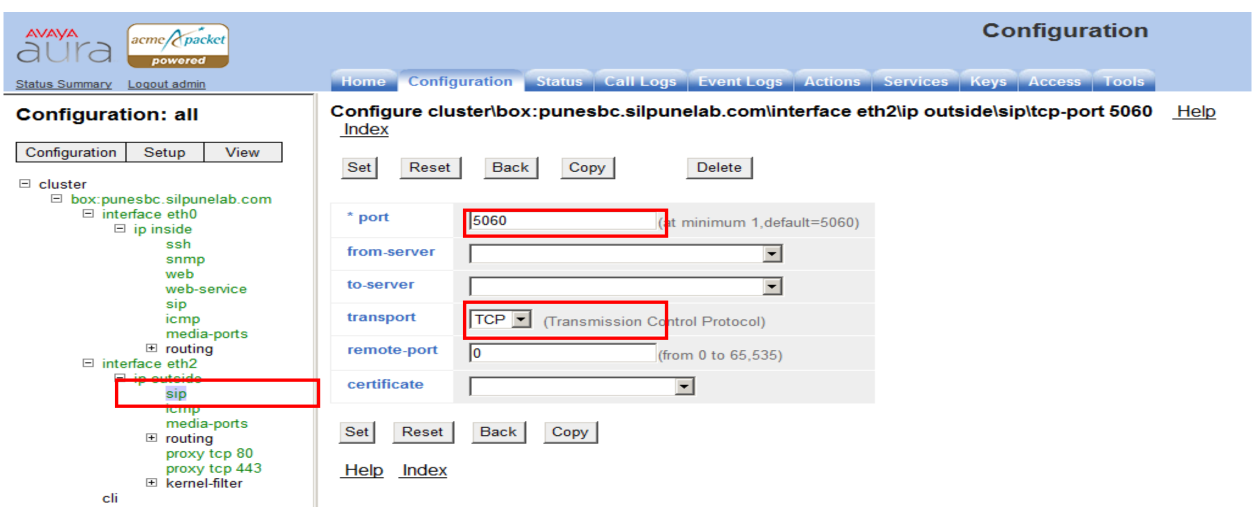


6.2.4. Administer SIP TCP Configuration On Eth2

To configure TCP SIP trunk for public interface, click on interface eth0 from left frame and then click on SIP link. Click on add TCP port.

Make following changes to the configuration and click on set to save configuration.

- **Port**: 5060
- **Transport**: TCP



©2011 Avaya Inc. All Rights Reserved.

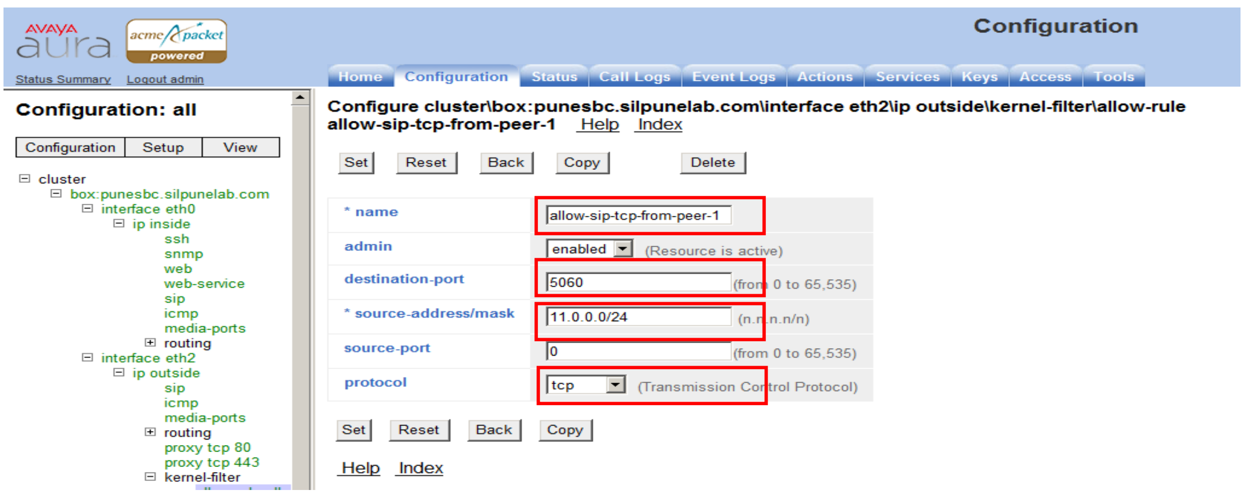
6.2.5. Administer Kernel Filter

Kernel filtering is by default enabled on the outside network to restrict the traffic from the public network entering Session Border Controller. This is similar to Linux kernel firewall **iptables**, which allow or restrict traffic to and from Session Border Controller to public network. There are two types of rules defined in filter Allow and Deny.

Allow rule allows specific type of traffic to enter Session Border Controller based on protocol and port selection. And Deny rule restricts generically all other or specific type of traffic to enter Session Border Controller based on protocol and port selection.

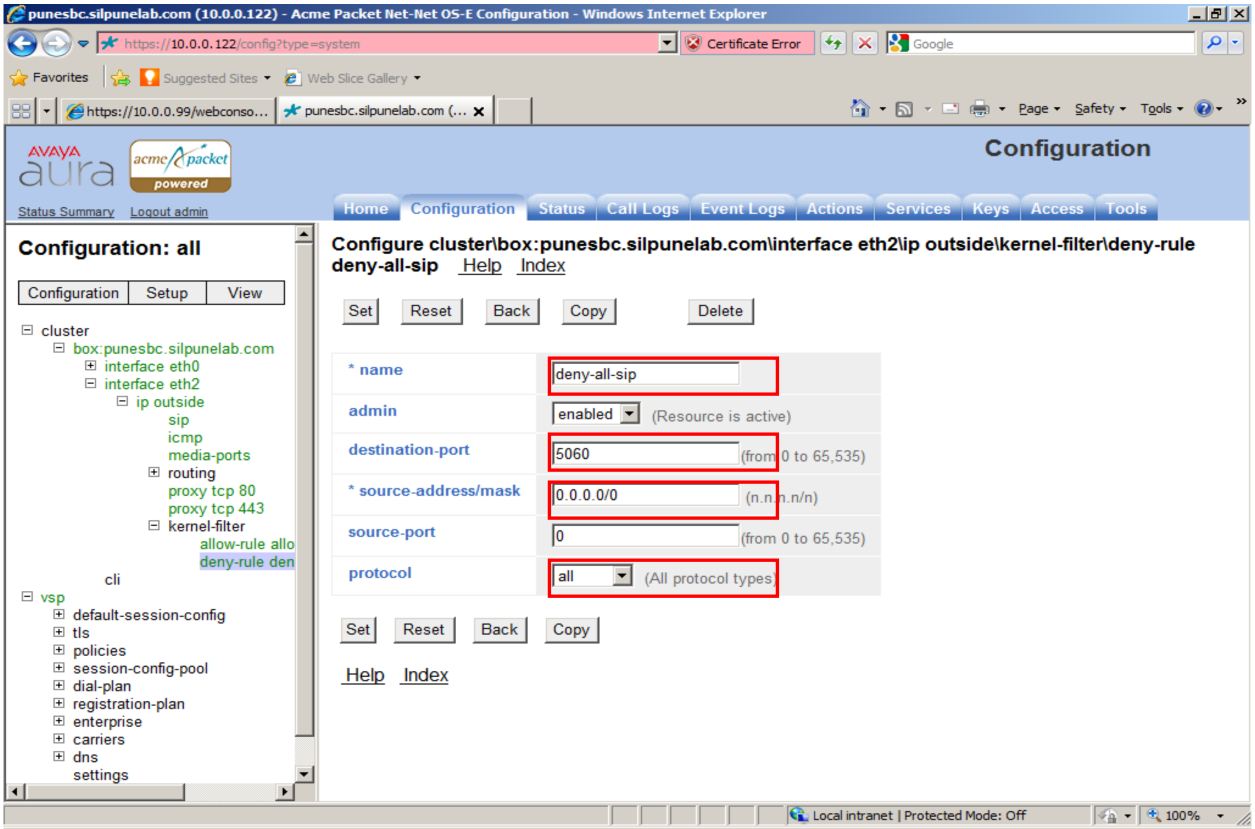
Select kernel-filter node under ip outside and make following changes to Allow rule.

- **Protocol:** This is to make sure all SIP TCP traffic is allowed.
- **Port:** The port configured on Eth2 interface for Telco sip Trunk.
- **Source-address/mask:** Specify the public network range.



©2011 Avaya Inc. All Rights Reserved.

Make following changes to **Deny** rule to restrict any other traffic from entering Session Border Controller from public network.



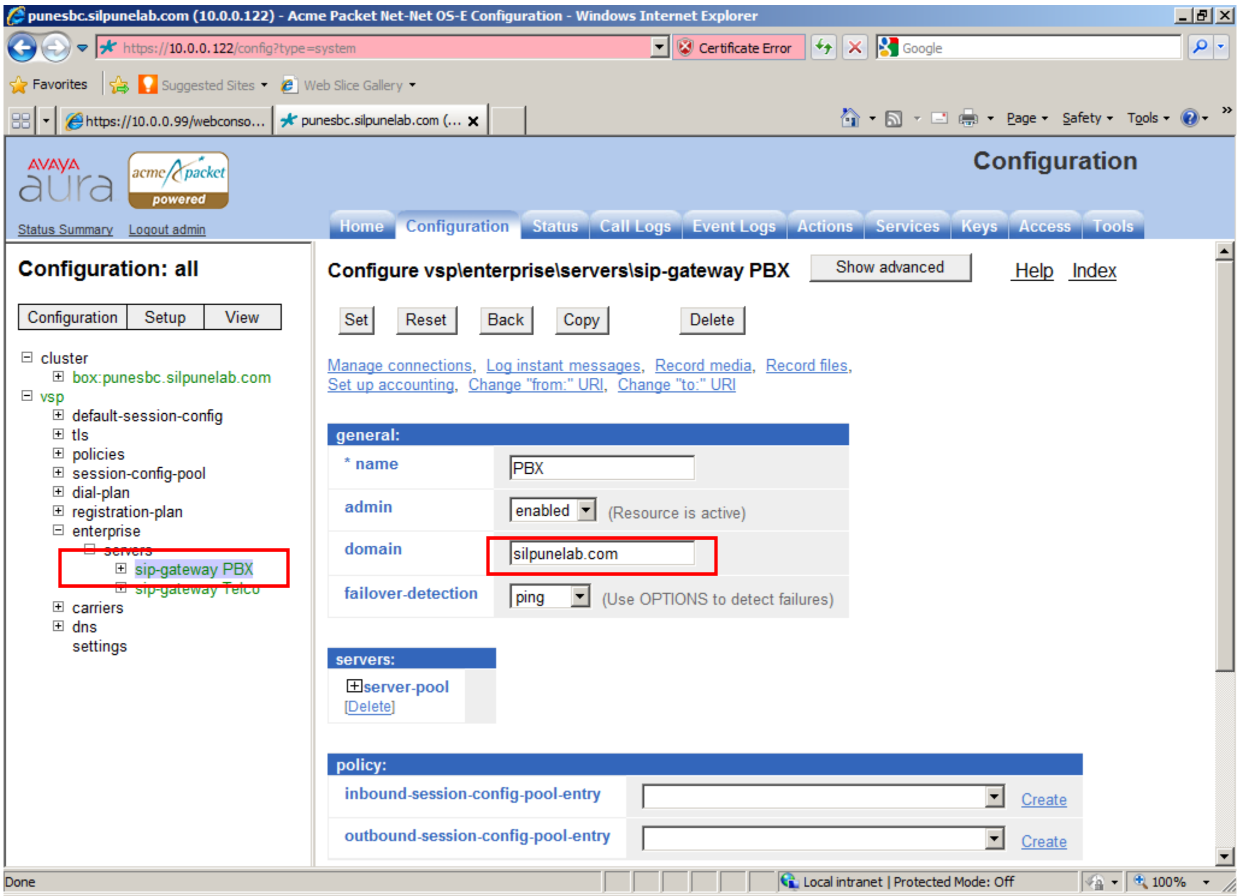
©2011 Avaya Inc. All Rights Reserved.

6.3. Administer Enterprise PBX Server

PBX enterprise server configuration is required to create link to Session Manager. Go to **vsp** node and click on Enterprise. Select sip-gateway PBX to update configuration.

Enter following details:

- **Domain**: Enter domain name as configured in Session Manager.

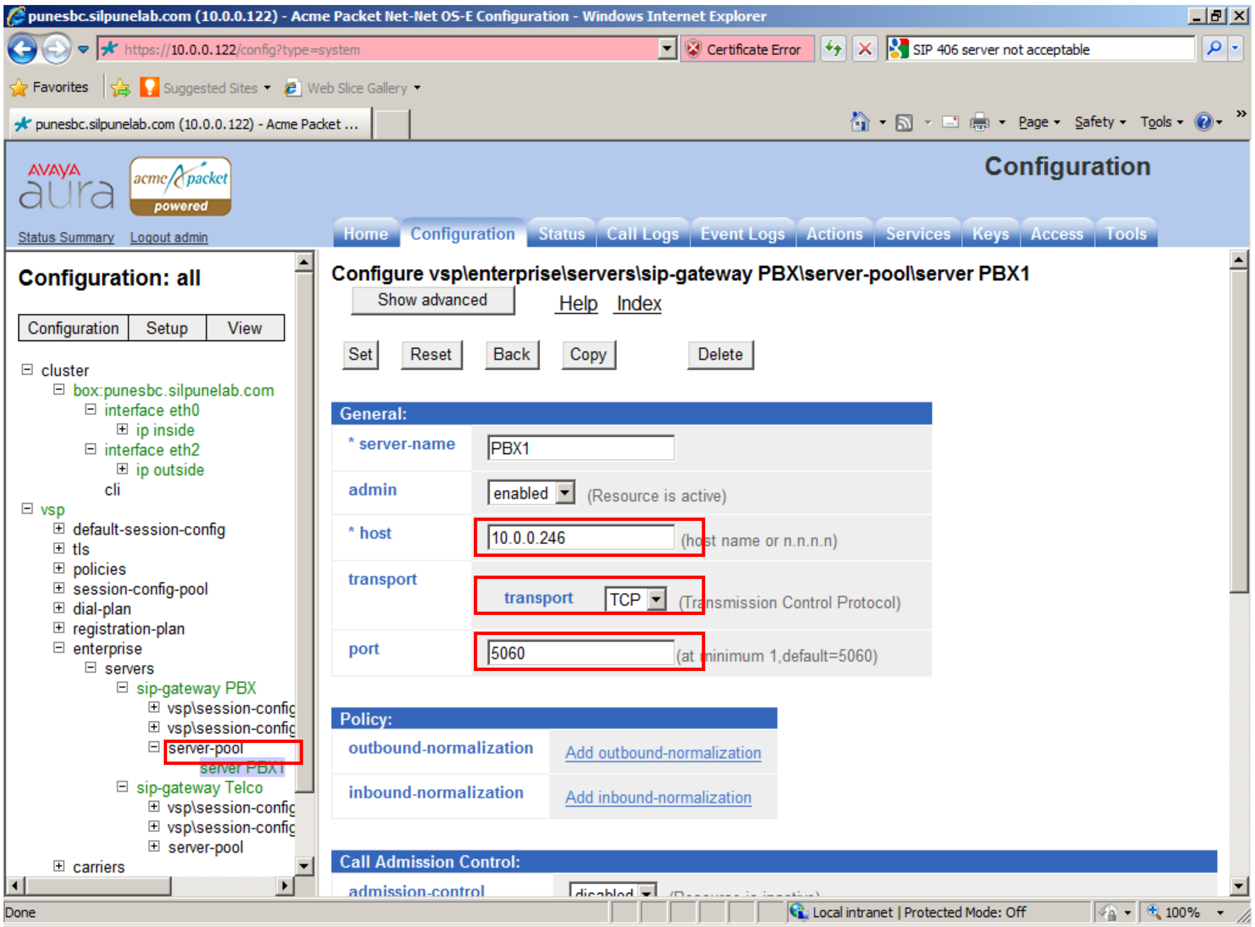


©2011 Avaya Inc. All Rights Reserved.

6.3.1. Administer SIP TCP Configuration On PBX Server

To administer PBX configuration click on server pool and select server **PBX1**. Make the following changes to the configuration. Click on set button after configuration to update it.

- **Host**: Set the value to Session Manager IP-address.
- **Transport**: TCP
- **Port**: 5060

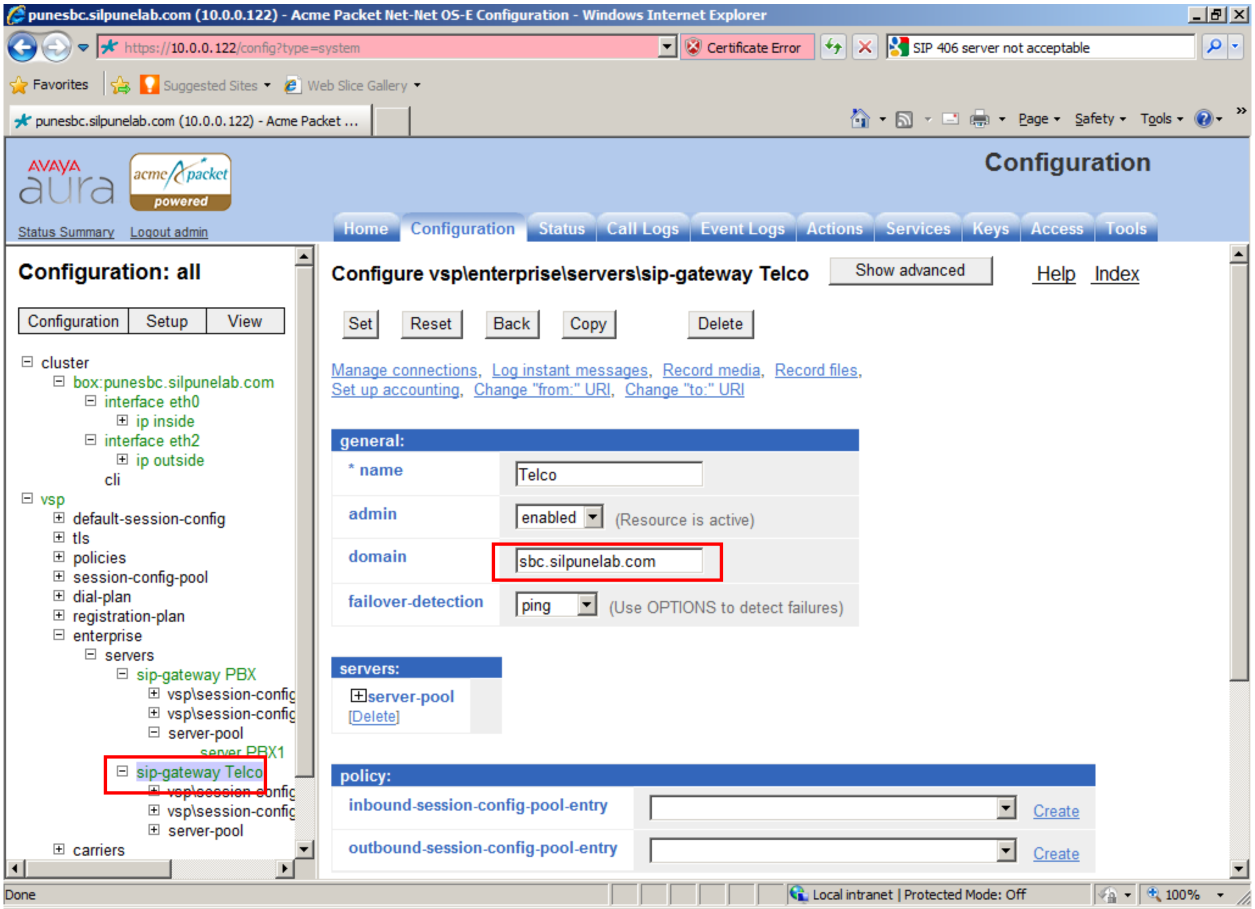


©2011 Avaya Inc. All Rights Reserved.

6.4. Administer Enterprise TELCO Server

Telco server configuration is required to create link to service provider in public network. Go to VSP node and click on **Enterprise**. Select **sip-gateway Telco** to update configuration.
Enter following details:

- **Domain**: Enter domain name for service provider network.

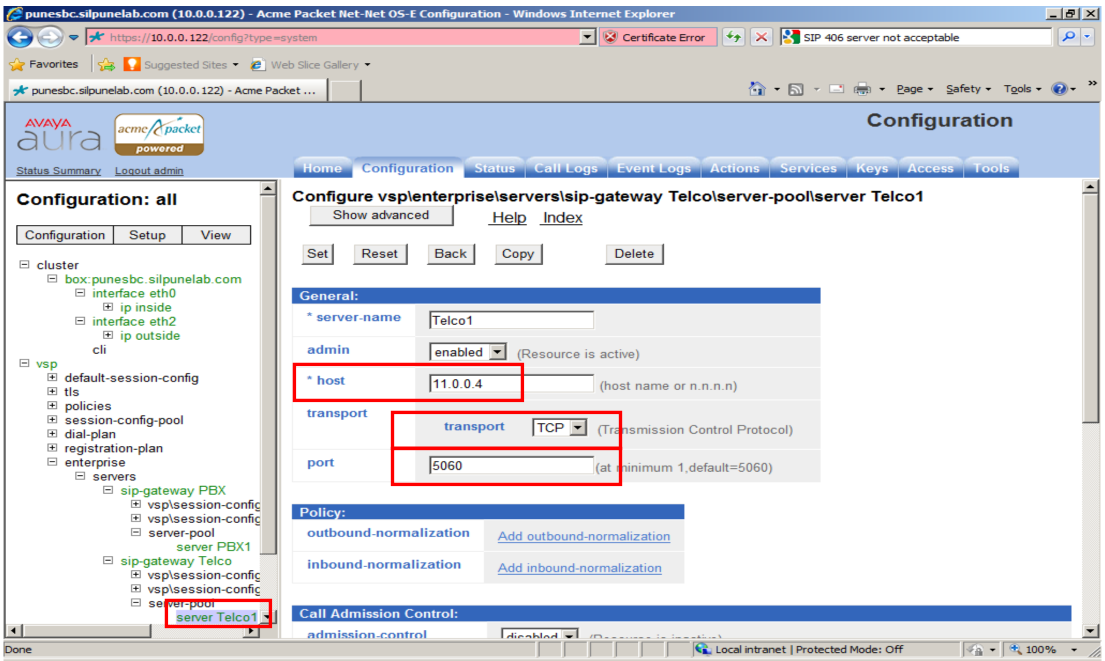


©2011 Avaya Inc. All Rights Reserved.

6.4.1. Administer SIP TCP Configuration On TELCO Server

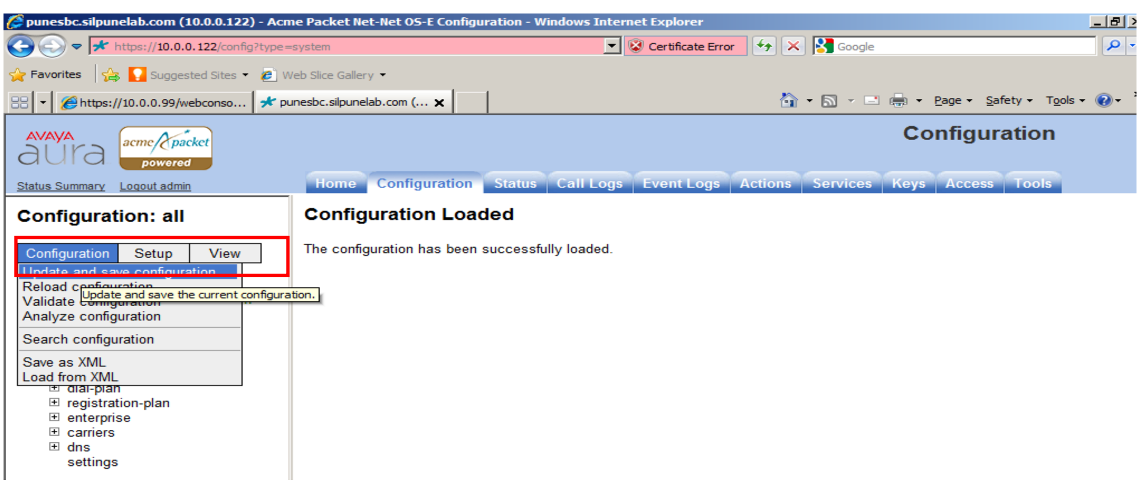
To administer Telco configuration click on server pool and select **server Telco1**. Make the following changes to the configuration. Click on the **set** button after configuration to update it.

- **Host:** Set the value to Server Provider IP-address.
- **Transport**: TCP
- **Port:** 5060



6.5. Save and Update Configuration

After completing configuration on the Session Border Controller, user is required to apply the changes to the current running configuration. Click on Configuration drop down menu button in left frame and select **Update and Save configuration**.



©2011 Avaya Inc. All Rights Reserved.

7. Configure Service Provider

This section provides the information for configuring Service provider in public network. In a customer deployment scenario, a user will configure a SIP trunk with parameters such as IP address and port received from the service provider.

In this lab deployment scenario Avaya Aura® Communication Manager Evolution Server 6.0.1 has been configured in public network to terminate calls to public network. The configuration on Communication Manager is similar to configuration described in **section 4**. Session Border controller is configured as a peer for the SIP trunk with Communication Manager. Avaya endpoints configured with this Communication Manager will act as public users to make and receive calls from private network.

©2011 Avaya Inc. All Rights Reserved.

8. Verification Steps

8.1. Verify Link Status On Communication Manager

To check status of the signaling link on Communication Manager, execute status signaling-group command.

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

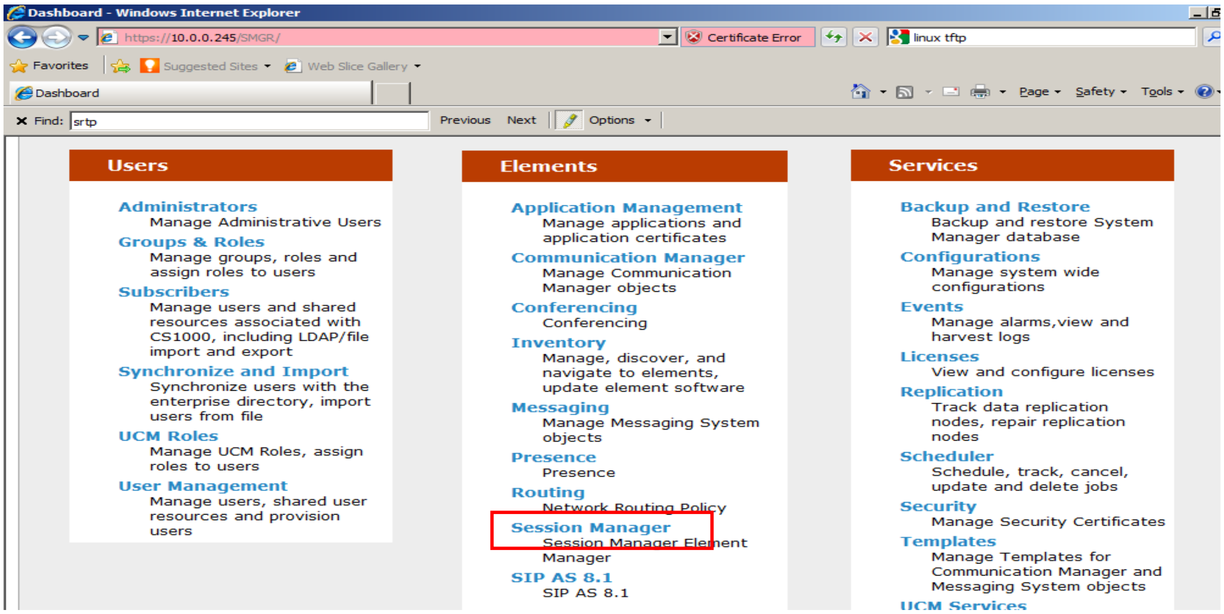
To check the status of trunk group on Communication Manager, execute status trunk command.

```
status trunk 1                                                       Page   1
                             TRUNK GROUP STATUS
Member   Port     Service State      Mtce Connected Ports
                                     Busy
0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
0001/011 T00011   in-service/idle    no
0001/012 T00012   in-service/idle    no
```

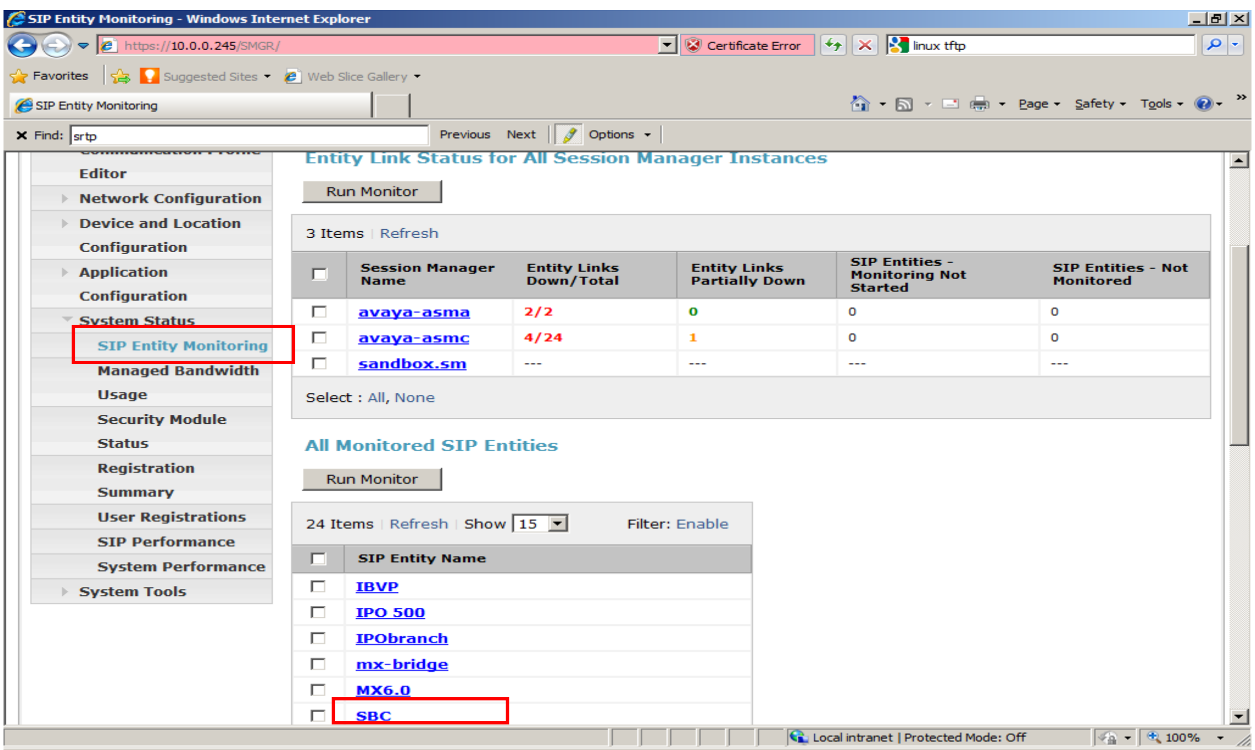

©2011 Avaya Inc. All Rights Reserved.

8.2. Verify Link Status on Session Manager

To verify the status on Session Manager go to the System Manager home page and click on **Session Manager** link in Elements column.

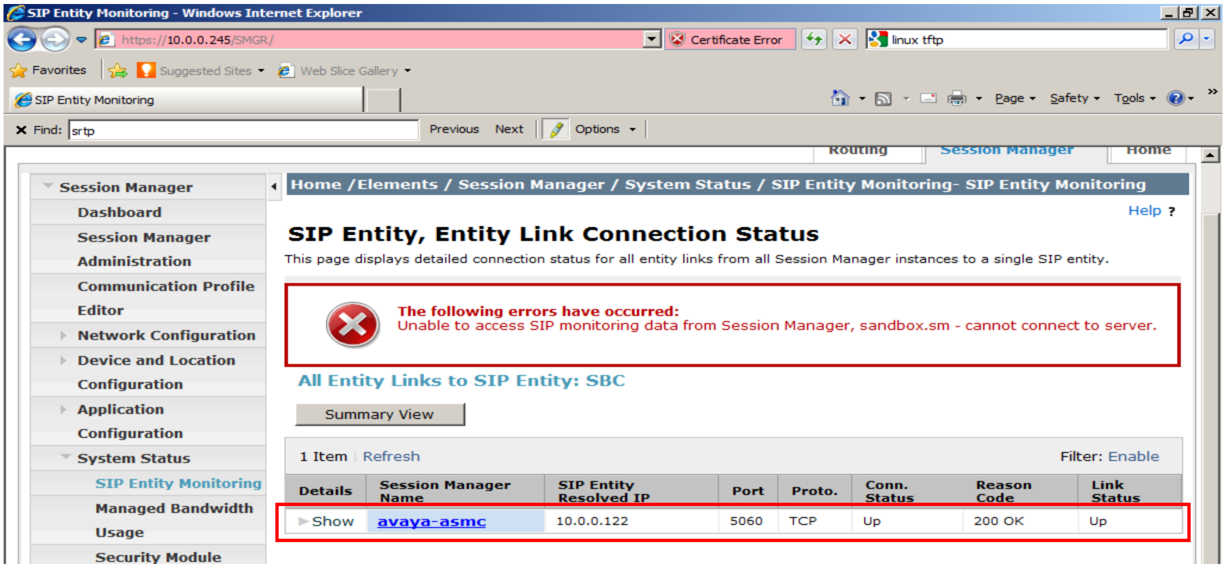


Go to **System Status** and select **SIP Entity Monitoring** from the menu. This shows the entities configured on Session Manager. Click on **Session Border Controller** entity to view its status.

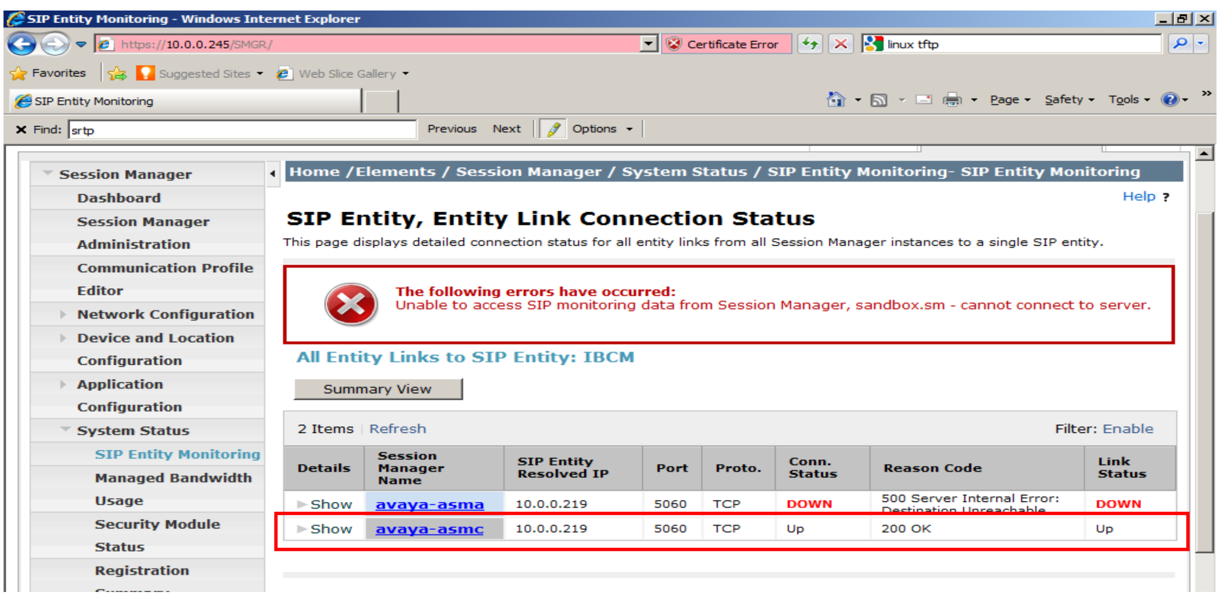


©2011 Avaya Inc. All Rights Reserved.

Check the status for the link configured with **avaya-asmc** in Session Manager. The connection status and link status is UP.

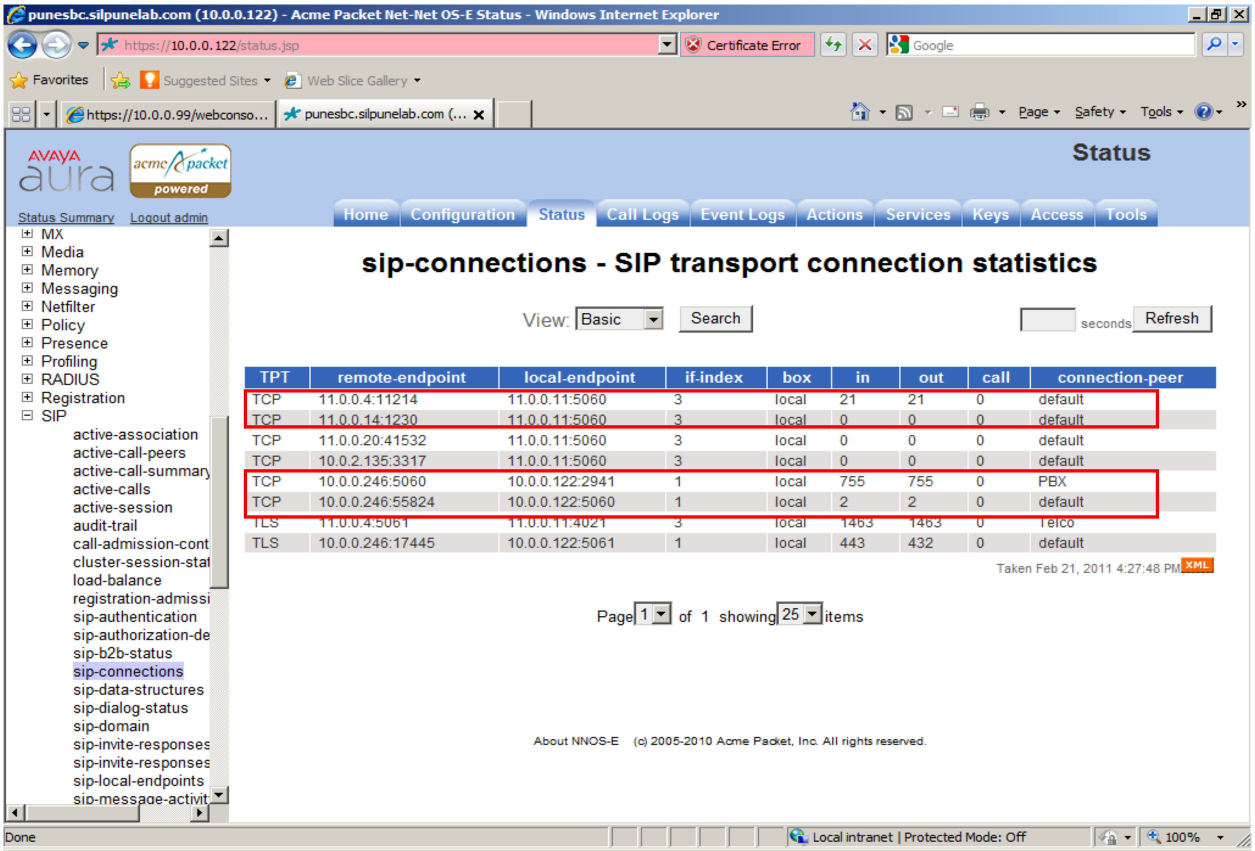


Similarly check the status for SIP link with Communication Manager. Go back to SIP Entity Monitoring and click on **IBCM** link to view its status. Check the status for the link configured with avaya-asmc Session Manager. As shown below, the connection status and link status is UP.



8.3. Verify Private and Public Link Status on Session Border Controller

To verify the status on Session Border Controller go to the home page and click on **Status** tab. Go to the SIP node in the left frame and click on **sip-connections**. The webpage shows statistics for the connections. Check the status of connections to PBX and Telco server.



8.4. Make a Basic TCP Call

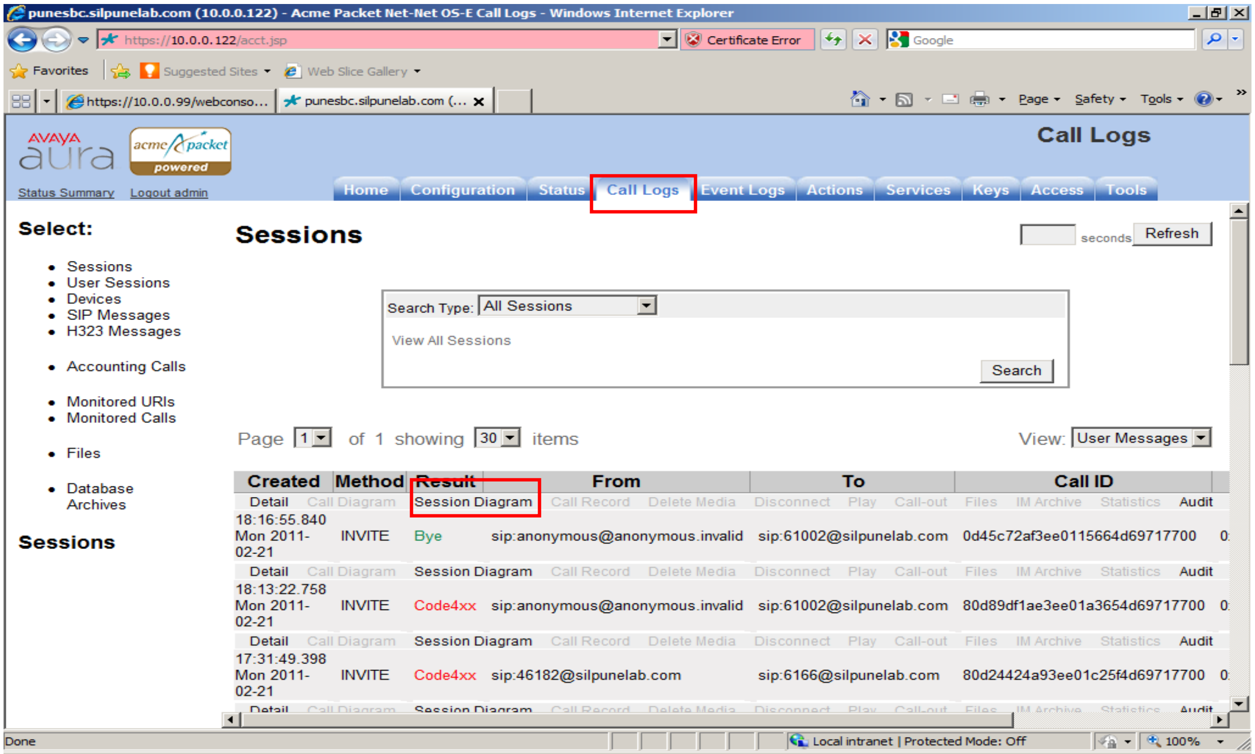
Station 6201 is configured on Communication Manager in the private network and Station 61002 is station on the Communication Manager serving as a simulated Telco server in public network. To make call to public network follow the steps below.

1. User dials 61002 from station 6201.
2. Call is routed to Session Border Controller by Session Manager.
3. Session Border Controller acts as proxy and routes the call to Telco Server.
4. The station registered to Telco Server rings and User answers the call.
5. Verify both party can talk to each other.
6. Called party terminates call. Verify the call logs on Session Border Controller.
7. Also make call from 61002 station to the private extension 6201. To verify public to private calling.

©2011 Avaya Inc. All Rights Reserved.

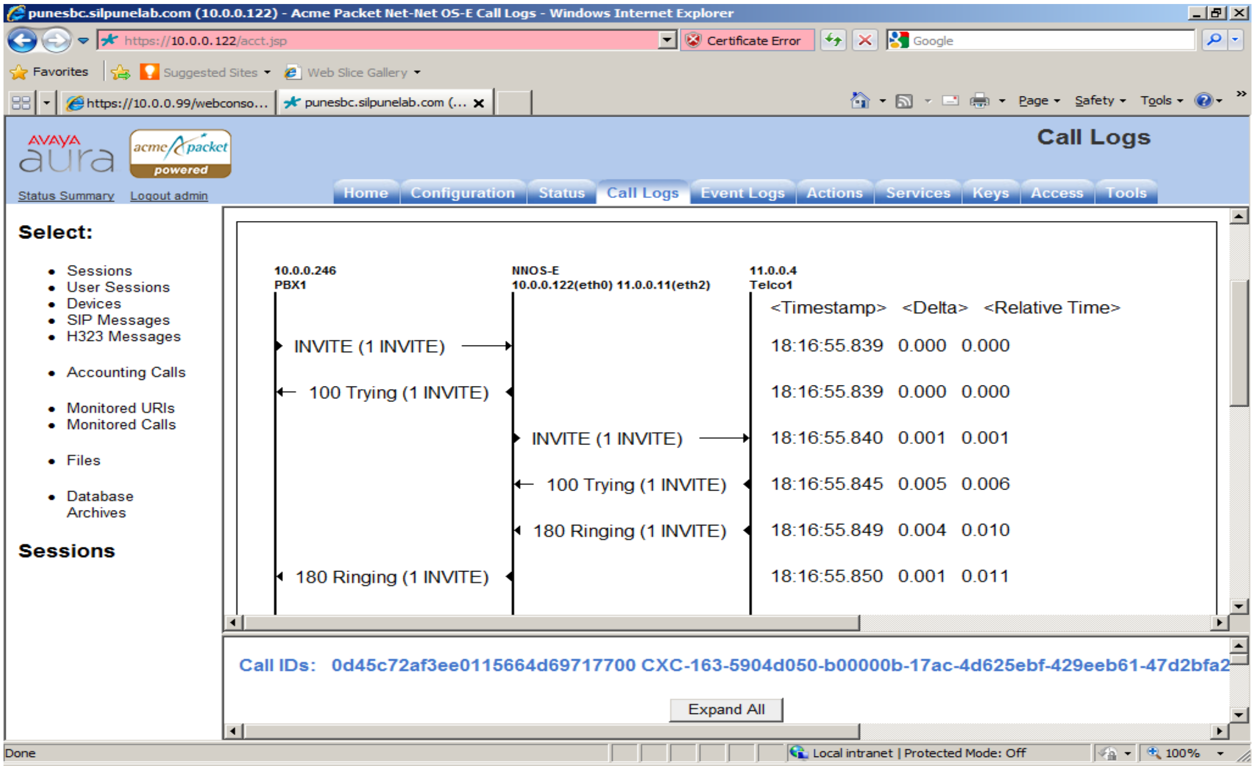
8.5. Verify Call Logs On Session Border Controller

To view the call logs on Session Border Controller go to home page and click on **Call logs** tab and view the first entry in the logs which displays latest session.



Click on **Sesson Diagram link,** this shows the call flow for the session as shown above.

©2011 Avaya Inc. All Rights Reserved.



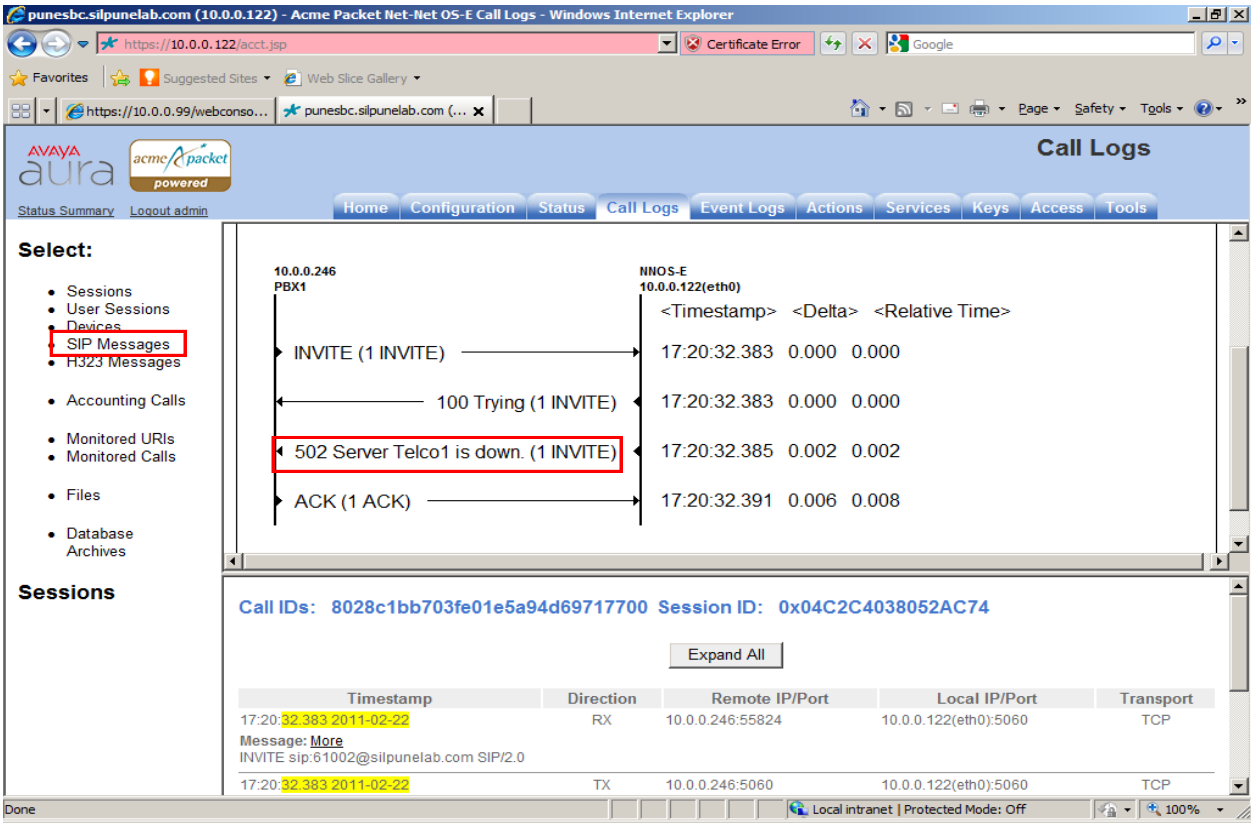
The following are different customer scenarios and call flows verified on the setup:

- Verify basic call flow from public station to private station on Communication Manager over TCP protocols.
- Verify basic call flow from private station to public station using different codec supported by Communication Manager.
- Verify call scenario were user performs call Hold/Un-Hold feature.
- Verify call scenario were user in private network performs Attended and Un-Attended transfers from a one public user to another public station.
- Verify call scenario were user in private network conferences to other stations in public network via Session Border Controller.
- Verify that Call forward feature enabled on Communication Manger on private extension forwards call from public station.
- Verify that basic and call features can be tested using different Avaya Endpoints such as Avaya one-X® Communicator, Avaya one-X® Agent and 9600 Series IP Deskphone.

8.6. Troubleshooting Post Configuration Issues

After completing configuration for Session Border Controller the call failure may occur due different reasons. Following are some of the common failure scenarios and how to troubleshoot.

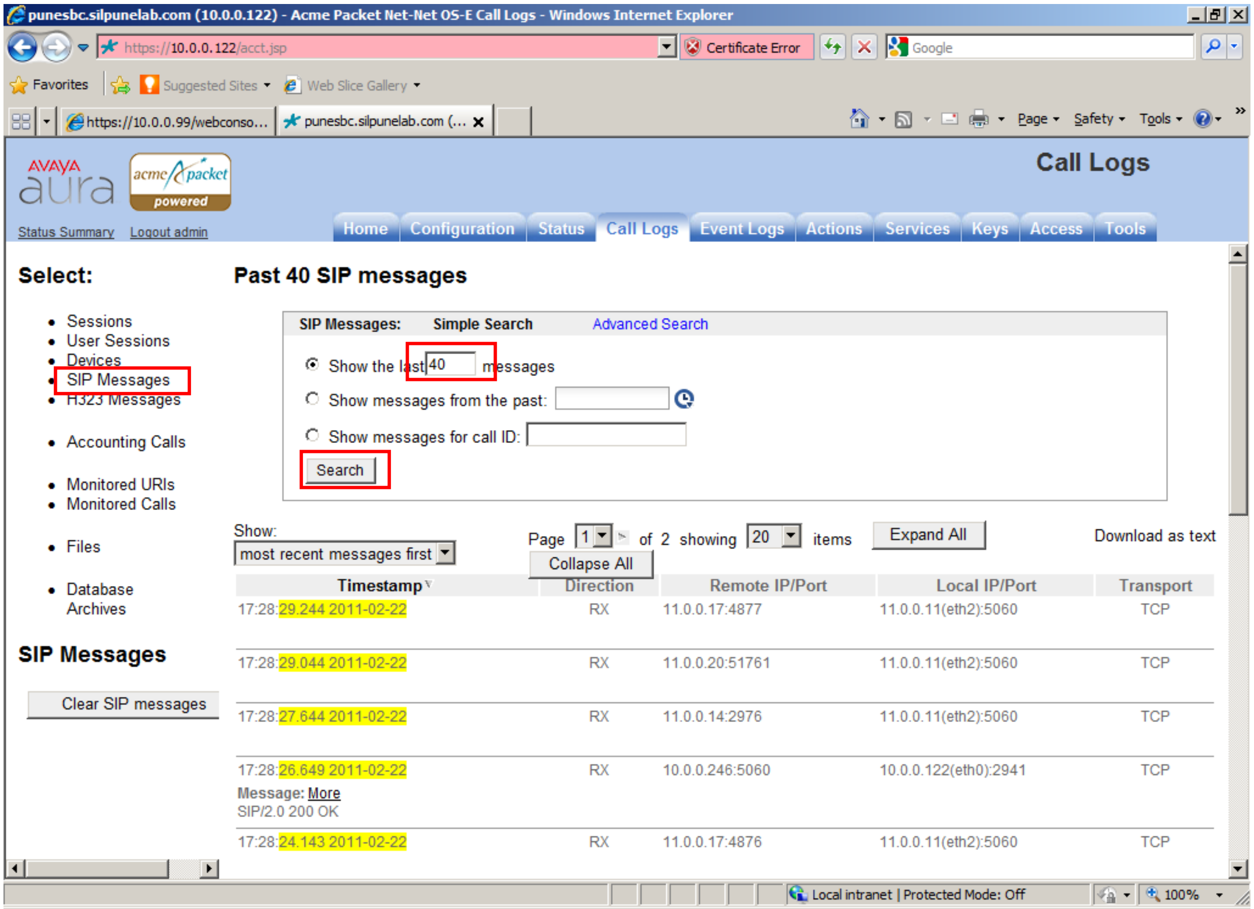
Scenario1: Session Border Controller receives no response from Telco server. Telco server is down.



Troubleshooting steps:

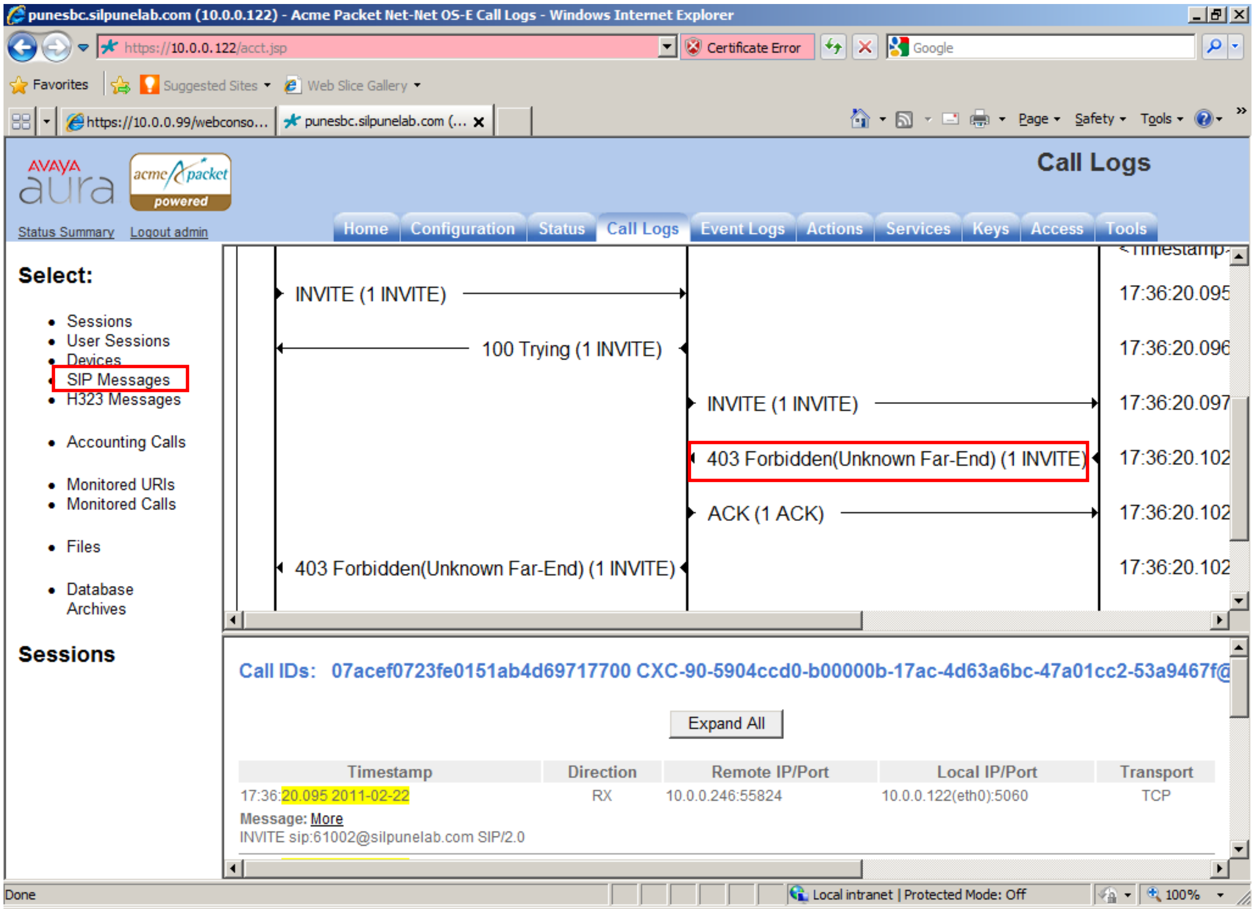
1. Check the status of the SIP trunk from Telco server to Session Border Controller. Go to Call Logs tab and select SIP Messages link.
2. See snapshot below. Enter 40 to see last SIP messages. And check if 200 OK is received for OPTIONS message from Telco IP-address. If 200 OK is not received TELCO server is down.
3. Check the Telco server is reachable and SIP enabled.
4. If the Telco Server is reachable, then check the IP-address and ports are correctly configured on Telco server. The incorrect configuration of IP-address or port may be the reason for Telco server not reachable from Session Border Controller.
5. Also check Kernel-filter configuration in **section 6.2.5**, and verify allow rule is set correctly for **transport** and **network**, to accept SIP traffic from public network.

©2011 Avaya Inc. All Rights Reserved.



©2011 Avaya Inc. All Rights Reserved.

Scenario2: Telco server rejects INVITE from Session Border Controller (Forbidden).



Troubleshooting steps:

1. Check the status of the Telco server trunk to Session Border Controller. Go to Call Logs tab and select SIP Messages link
2. Enter 40 to see last SIP messages. And check if 200 OK is received for OPTIONS message from Telco IP-address.
3. If the Telco Server is reachable, then check configuration on the Session Border Controller for Telco server, Ethernet ETH2 have same transport type (in current configuration TCP). If the Telco server is TLS or UDP i.e., Transport type is mismatch then Telco server rejects call with 403 Forbidden. Update the configuration to correct transport type.

©2011 Avaya Inc. All Rights Reserved.

9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Border Controller can be successfully configured with Avaya Aura® Session Manager 6.0 and Avaya Aura® Communication Manager. Avaya Aura® Session Border Controller allows enterprise network to be connected to public network and provides protection from intrusion and external attacks. The tests calls were made with SIP on TCP and media over RTP. However, for security reasons, it is preferable that SIP with TLS and media over SRTP be used.

10. Additional References

Avaya references, available at http://support.avaya.com
This section references the product documentation relevant to these Application Notes.

Avaya Aura® Session Border Controller

1) Installing and configuring Avaya Aura® Session Border Controller.
2) Avaya Aura® Session Border Controller Release 6.0 Release Notes.
3) Avaya Aura(tm) Session Border Controller System Administration.
4) Avaya Aura(tm) Session Border Controller Objects and Properties Reference.
5) Avaya Aura(tm) Session Border Controller Session Services Guide.

Avaya Aura® Session Manager

6) Avaya Aura™ Session Manager Overview, Doc ID 03-603323.
7) Installing and Upgrading Avaya Aura™ Session Manager 6.0, Doc ID 03-603324.
8) Installing and Upgrading Avaya Aura™ System Manager 6.0.
9) Maintaining and Troubleshooting Avaya Aura™ Session Manager 6.0, Doc ID 03-603325.

Avaya Aura® Communication Manager

10) Installing and Configuring Avaya Aura™ Communication Manager, Doc ID 03-603558
11) Upgrading to Avaya Aura® Communication Manager Release 6.0.1, Doc ID 03-603560.
12) Administering Avaya Aura™ Communication Manager Doc ID 03-300509

©2011 Avaya Inc. All Rights Reserved.

©2011 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com