Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server and AcmePacket Net-Net 3800 Session Director with SIP Trunking offering from IntelePeer - Issue 1.0

Abstract

These Application Notes describe the procedure to configure an Enterprise network containing Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server and AcmePacket NetNet3800 Session Director to work with SIP Trunking offering from IntelePeer.

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 present a sample configuration for an Enterprise network that enables Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server and AcmePacket Net-Net 3800 Session Director to access the SIP Trunking solution provided by IntelePeer (Service Provider). This solution allows an Avaya Aura® Enterprise network access to PSTN, Mobile phones and other SIP Trunk customers. An Enterprise customer with an Avaya SIP-based solution can subscribe to a network-based IP communication service from IntelePeer that supports SIP-to-PSTN calls to reduce their long distance and interconnection costs. To accomplish this, customers interconnect their Avaya Aura® Session Manager with AcmePacket Net-Net 3800 SessionDirector.

AcmePacket Net-Net 3800 Session Director is a security appliance that manages and protects the flow of SIP signaling and related media across an un-trusted network. The compliance testing focused on telephony scenarios between the enterprise and IntelePeer connected via SIP trunks across an un-trusted network.

2. General Test Approach and Test Results

The general test approach was to make calls between the Enterprise and the PSTN using various codec settings exercising common and advanced telephony features.

The serviceability testing focused on verifying the ability of solution to recover from adverse conditions, such as network failures.

2.1. Interoperability Compliance Testing

The primary focus of testing is to verify SIP Trunking interoperability between an Avaya SIP-based network secured with an AcmePacket Net-Net 3800 and IntelePeer's voice over IP network. Test cases are selected to exercise a sufficiently broad segment of functionality to have a reasonable expectation of interoperability in production configurations.

Basic Interoperability:

- PSTN calls delivered via the Service Provider's SIP Trunking to an Avaya IP telephony solution
- PSTN calls sent via a Service Provider's SIP Trunking from an Avaya IP telephony solution
- Calling with various Avaya telephone models including IP/SIP models as well as traditional analog and digital TDM phones
- Verify G.711 / G.729 support
- Various PTSN dialing plans including national and international calling, toll-free, operator, directory assistance and direct inward dialed calling
- SIP transport using UDP as supported by IntelePeer

Advanced Interoperability:

- Codec negotiation

- Telephony supplementary features, such as Hold, Call transfer, Conference Calling and Call Forwarding
- DTMF Tone Support
- Voicemail Coverage and Retrieval
- Direct IP-to-IP Media (also known as "Shuffling") over SIP Trunk. Direct IP-to-IP media allows compatible phones to reconfigure the RTP path after call establishment directly between the Avaya phones and the Service Provider and release media processing resources on the Avaya Media Gateway
- EC500 feature support for Avaya Aura® Communication Manager

Service Provider specific:

- Calls from/to PSTN
- Calls from/to Mobile users

Serviceability:

- Recovery from network outage

2.2. Test Results

All test cases passed. During the compliance testing T.38 Fax transmission and receiving was impaired by PSTN service provider outside the scope of lab configuration.

2.3. Support

Technical Support on SIP Trunking offering from IntelePeer can be obtained through the following phone contacts:

- **T: +1.866.780.8639**

3. Reference Configuration

As shown in **Figure 1**, the Avaya enterprise network uses SIP Trunking for call signaling internally and with SIP gateway residing on IntelePeer network. Avaya Aura® Session Manager using its signaling interface, routes the calls between the different entities using SIP Trunks. All inter-system calls are carried over these SIP trunks. Avaya Aura® Session Manager supports flexible inter-system call routing based on the dialed number, the calling number and the system location; it can also provide protocol adaptation to allow multi-vendor systems to interoperate. Avaya Aura® Session Manager is managed by Avaya Aura® System Manager (not displayed here) via the management network interface

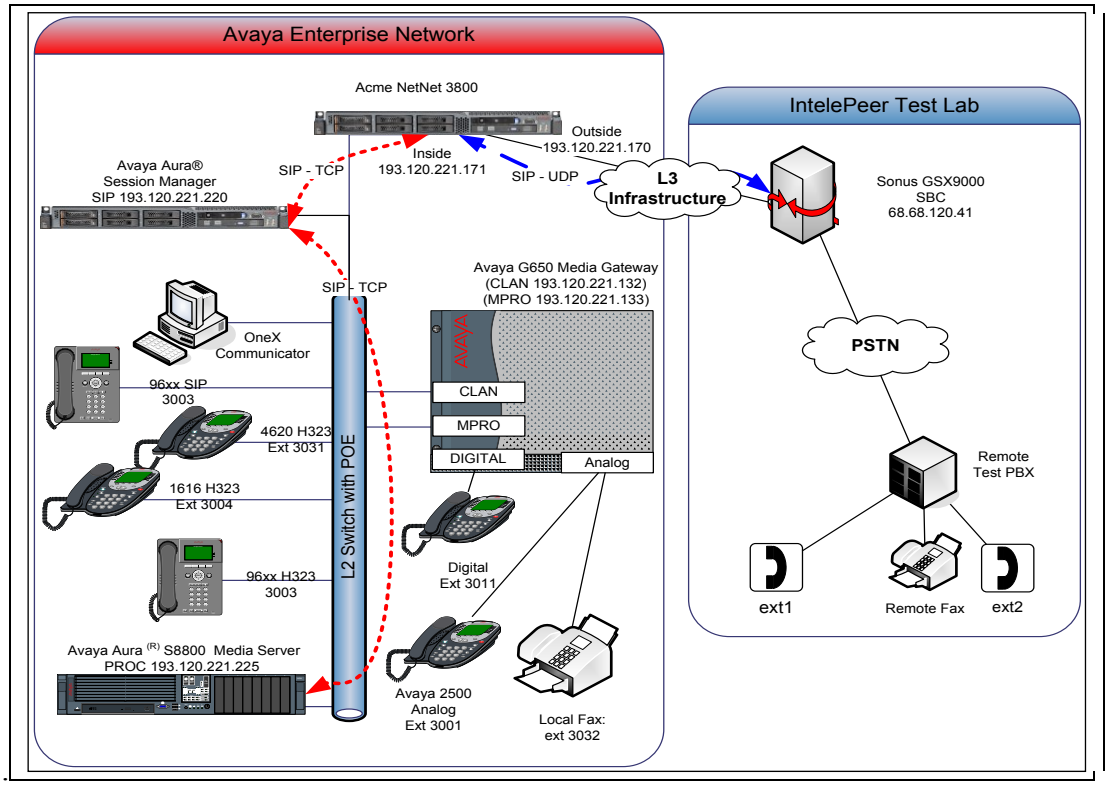


Figure 1 – Sample configuration for Avaya Aura® Communication Manager Avaya Aura® Session Manager and AcmePacket Net-Net performing SIP Trunking with IntelePeer

For the sample configuration shown in **Figure 1**, Avaya Aura® Session Manager runs on an Avaya S8800 Server, Avaya Aura® Communication Manager R6 runs on an Avaya S8800 Server with an Avaya G650 Media Gateway. The results in these Application Notes are applicable to other Avaya Aura® Communication Manager Server and Media Gateway combinations. These Application Notes will focus on the configuration of the SIP trunks and call routing. Detailed administration of the endpoint telephones will not be described. Refer to the appropriate documentation in **Section 10**.

4. Equipment and Software Validated

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

Avaya Product / Hardware Platform	Software Version
Avaya S8800 Server	Avaya Aura® Session Manager R6 SP1 R6.0.1.0.601016
Avaya S8800 Server	Avaya Aura® Communication Manager Evolution Server R601x.00.0.345.0 patch 18444
Avaya G650 Media Gateway • IPSI (TN2312BP) • C-LAN (TN799DP) • IP Media Resource 320 (TN2602AP)	 • TN2312BP HW28 FW0530 • TN799DP HW01 FW0397 • TN2602AP HW08 FW0553

Avaya Product / Hardware Platform	Software Version
• Analog (TN2793B) • Digital line (TN2214CP)	• TN2793B 000005 • TN2214CP HW10 FW015
Avaya IP Telephones: • 9630 & 9620 (SIP) • 9620 (H323) • 1616 (H323) • 4621 (H323) • Avaya Digital Telephones (2420) • Avaya Analog (2500)	 • Release 96x1-IPT-SIP-R6_0-112210 • Release 3.1 • Release 1.3 • Release R2.9 SP1 • N/A • N/A
Avaya One-X Communicator (H323)	Release 6.0.1.16
Acme Packet Net-Net 3800 Session Director	SCX6.2.0 GA
Service Provider - IntelePeer	
Product /Hardware Platform	**Software Version**
• SBC: Sonus Networks GSX9000 Session Border Controller Chassis	• N/A

5. Configure Avaya Aura® Communication Manager Evolution Server

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

- Verify Avaya Aura® Communication Manager License
- Configure IP Node Names
- Verify/List IP Interfaces
- Configure IP Codec Set
- Configure IP Network Region
- Administer SIP Trunks with Session Manager
- Configure Route Pattern
- Configure Public Unknown Numbering
- Administer ARS Analysis
- Save Translations

Throughout this section the administration of Communication Manager is performed by entering the following commands using a System Access Terminal (SAT) 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 **Reference [1]** and **[2]** for more details**.** In these Application Notes, Communication Manager was configured with 4 digit extention **3xxx** for stations. Diaplan analysis can be verified with the **display dialplan analysis** command.

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

      Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
      String   Length Type    String   Length Type     String   Length Type
   3           4    ext
   8           1    dac
   9           1    dac
   *           2    fac
   *           3    dac
```

Other numbers on PSTN (accessible from the SIP trunk offering) are reachable via **ars** table with the use of **feature access code *9**.

5.1. Verify Avaya Aura® 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 highlighted value, as shown below.

```
display system-parameters customer-options                  Page   2 of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                          USED
                     Maximum Administered H.323 Trunks: 100   0
          Maximum Concurrently Registered IP Stations: 18000 2
            Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
             Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 100   0
                   Maximum Video Capable IP Softphones: 100   9
                       Maximum Administered SIP Trunks: 1000  300
```

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.

5.2. Configure IP Node Names

As SIP interaction with Session Manager is carried through the security module SM100 IP interface, this IP address is used when configuring the SIP Trunk. Use the **change node-names ip** command to add the **Name** and **IP Address** for the Session Manager. In the example **SM100** and **193.120.221.220** were used.

```
change node-names ip                                        Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
clan                   193.120.221.132
default                0.0.0.0
```

```
gw                  193.120.221.129
mpro                193.120.221.133
procr               193.120.221.225
procr6              ::
sm100               193.120.221.220
```

Note: In the example some other values (CLAN, MedPro) have been already created as per installation and configuration of Communication Manager.

5.3. Verify/List IP Interfaces

Use the **list ip-interface all** command and note the **PROCR** interface address to be used for SIP trunks between the Communication Manager and the Session Manager.

```
list ip-interface all
                                IP INTERFACES
                                                                  Net
ON Type    Slot  Code/Sfx     Node Name/       Mask              Rgn  VLAN
                             IP-Address/
                             Gateway Node
-- ------ ----- --------     ---------------  ----              ---  ----
y PROCR                      procr            /25                1
                             193.120.221.225
                             193.120.221.129
n PROCR                      procr6           /64                1
                             ::
                             ::
y C-LAN  01A02 TN799  D      clan             /25                1    n
                             193.120.221.132
                             gw
y MEDPRO 01A03 TN2602        mpro             /25                1    n
                             193.120.221.133
                             gw
```

5.4. Configure IP Codec Set

Use the **change ip-codec-set n** command where **n** is codec set used in the configuration. The IntelePeer SIP Trunking offering is based on G.711MU or G.729. Configure the IP Codec Set as follows:

- **Audio Codec** Select **G.711MU** and **G.729**

Retain the default values for the remaining fields.

```
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.729             n          2        20
3:
```

On **Page 2** of the ip-codec-set form, set **FAX Mode** to "**t.38-standard**".

```
 change ip-codec-set 1                                        Page   2 of   2
                           IP Codec Set
                              Allow Direct-IP Multimedia? n

                     Mode               Redundancy
   FAX               t.38-standard      0
   Modem             off                0
   TDD/TTY           off                0
```

5.5. Configure IP Network Region

Use the **change ip-network-region n** command where **n** is the number of the network region used. 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 **Section 5.4**. 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. If a new network region is needed or an existing one is modified, ensure to configure it with the correct parameters.

```
change ip-network-region 1                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Test Lab
MEDIA PARAMETERS                 Intra-region IP-IP Direct Audio: yes
      Codec Set: 1               Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
```

5.6. Administer SIP Trunks with Avaya Aura® Session Manager

To administer a SIP Trunk on Communication Manager, three intermediate steps are required, creation of a signaling group, a trunk group for calls within the enterprise and a trunk group for calls to the Service Provider.

Note: the second trunk group is needed to allow for additional modifications to the SIP messages. See for more information on applying Adaptations to SIP messages for external calls.

5.6.1. 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 the Session Manager, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type:** **sip**
- **Transport Method:** **tcp**
- **Near-end Node Name:** **PROCR** node name from **Section 5.2** (i.e., **procr**)
- **Far-end Node Name:** Session Manager node name from **Section 5.2** (i.e., **SM100**)
- **Near-end Listen Port:** **5060**

- **Far-end Listen Port:** **5060**
- **Far-end Domain:** The SIP domain in use within the enterprise i.e. **avaya.com**
- **DTMF over IP:** **rtp-payload**

```
add signaling-group 100                                         Page   1 of   1
                              SIGNALING GROUP

 Group Number: 100            Group Type: sip
  IMS Enabled? n        Transport Method: tcp
       Q-SIP? n                                        SIP Enabled LSP? n
    IP Video? n                                 Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM

   Near-end Node Name: procr                  Far-end Node Name: sm100
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1

Far-end Domain: avaya.com
                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: allow                     RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y                 Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

5.6.2. Configure a SIP Trunk Group for calls within the Enterprise

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 (i.e**. Enterprise**)
- **TAC:** An available trunk access code (i.e. ***10)**
- **Service Type:** **public-ntwrk**
- **Signaling Group:** Number of the signaling group added in **Section 5.6.1** (i.e. **100**)
- **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 5.1**)

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

```
add trunk-group 100                                          Page   1 of  21
                                TRUNK GROUP
Group Number: 100                 Group Type: sip            CDR Reports: y
  Group Name: Enterprise                COR: 1        TN: 1        TAC: *10
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                        Signaling Group: 100
                                                      Number of Members: 100
```

Navigate to **Page 3** and change **Numbering Format** to **public.** Submit these changes.

```
add trunk-group 100                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y
                      Numbering Format: public
                                              UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n
```

5.6.3. Configure a SIP Trunk Group for calls to IntelePeer Service Provider

Add a second trunk group controlled by the same 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 (i.e**. IntelePeer**)
- **TAC:** An available trunk access code (i.e. ***15)**
- **Service Type:** **public-ntwrk**
- **Signaling Group:** Number of the signaling group added in **Section 5.6.1** (i.e. **100**)
- **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 5.1**)

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

```
add trunk-group 150                                          Page   1 of  21
                                TRUNK GROUP
Group Number: 150                 Group Type: sip            CDR Reports: y
  Group Name: IntelePeer                COR: 1        TN: 1        TAC: *15
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                           Member Assignment Method: auto
                                                     Signaling Group: 100
                                                   Number of Members: 100
```

Navigate to **Page 3** and change **Numbering Format** to **public.**

```
add trunk-group 150                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y
                     Numbering Format: public
                                           UUI Treatment: service-provider

                                             Replace Restricted Numbers? n
                                            Replace Unavailable Numbers? n
```

Navigate to **Page 4** and change **Telephone Event Payload Type** to **101.** Use default values for all other fields. Submit these changes.

```
add trunk-group 150                                          Page   4 of  21
                           PROTOCOL VARIATIONS

                       Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                  Network Call Redirection? n
                     Send Diversion Header? n
                   Support Request History? y
              Telephone Event Payload Type: 101
```

5.7. Configure Route Patterns

Configure two route patterns to correspond to the newly added SIP trunk groups Use **change route pattern n** command, where **n** is an available route pattern.

5.7.1. Route Pattern for Enterprise Calls

When changing the 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., **toEnterprise**)
- **Grp No:** The trunk group number from **Section 5.6.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

```
change route-pattern 2                                        Page   1 of   3
                   Pattern Number: 2   Pattern Name: toEnterprise
                            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: 100  0                                                          n   user
 2:                                                                 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           unre                                     none
 2: y y y y y n  n           rest                                     none
```

5.7.2. Route Pattern for outbound call to IntelePeer

When changing the 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., **IntelePeer**)
- **Grp No:** The trunk group number from **Section 5.6.3**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

```
change route-pattern 3                                        Page   1 of   3
                   Pattern Number: 3   Pattern Name: IntelePeer
                            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: 150  0                                                          n   user
 2:                                                                 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           unre                                     none
 2: y y y y y n  n           rest                                     none
```

5.8. Configure Public Unknown Numbering

Use the **change public-unknown-numbering 0** command to assign number presented by Communication Manager when call is leaving to Session Manager to reach to Service Provider.

Note: IntelePeer requires that the caller id is presented in the From as well in the PAI fields.

Add an entry for the Extensions configured in the dialplan. Enter the following values for the specified fields. Submit these changes.

- **Ext Len:** Number of digits of the station i.e. **4**
- **Ext. Code:** Digits in the station number, i.e. **3011**
- **Trk Group:** Trunk number configured to reach the Service Provider as in **Section 5.6.3** i.e. **150**
- **CPN Prefix:** Configure according to the numbering plan offered by IntelePeer
- **Total CPN Len** Number of digits i.e. **10**

```
change public-unknown-numbering 0                              Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext  Ext             Trk        CPN       CPN
Len  Code            Grp(s)     Prefix    Len
                                                Total Administered: 3
 4   3011            150        3033289131  10       Maximum Entries: 9999
 4   3030            150        3033289130  10
 4   3032            150        3033289132  10   Note: If an entry applies to
                                                 a SIP connection to Avaya
                                                 Aura(tm) Session Manager,
                                                 the resulting number must
                                                  be a complete E.164 number.
```

5.9. Administer ARS Analysis

This section provides sample Automatic Route Selection (ARS) used for routing calls with dialed digits beginning with **0** corresponding to national numbers accessible via the Service Provider. To select ARS routing, a feature access code is required, refer to [1] for additional information.

Use the **change ars 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 **011**
- **Total Min:** Minimum number of digits, in this case **3**
- **Total Max:** Maximum number of digits, in this case **25**
- **Route Pattern:** The route pattern number from **Section 5.7.2** i.e. **3**
- **Call Type:** **pubu**

Note that additional entries may be added for different number destinations.

```
change ars analysis 0                                    Page   1 of   2
                          ARS DIGIT ANALYSIS TABLE
                                Location:  all          Percent Full:    1

          Dialed          Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
            011           3    25   3      pubu   n
```

5.10. Save Translations

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

6. Configure Avaya Aura® Session Manager

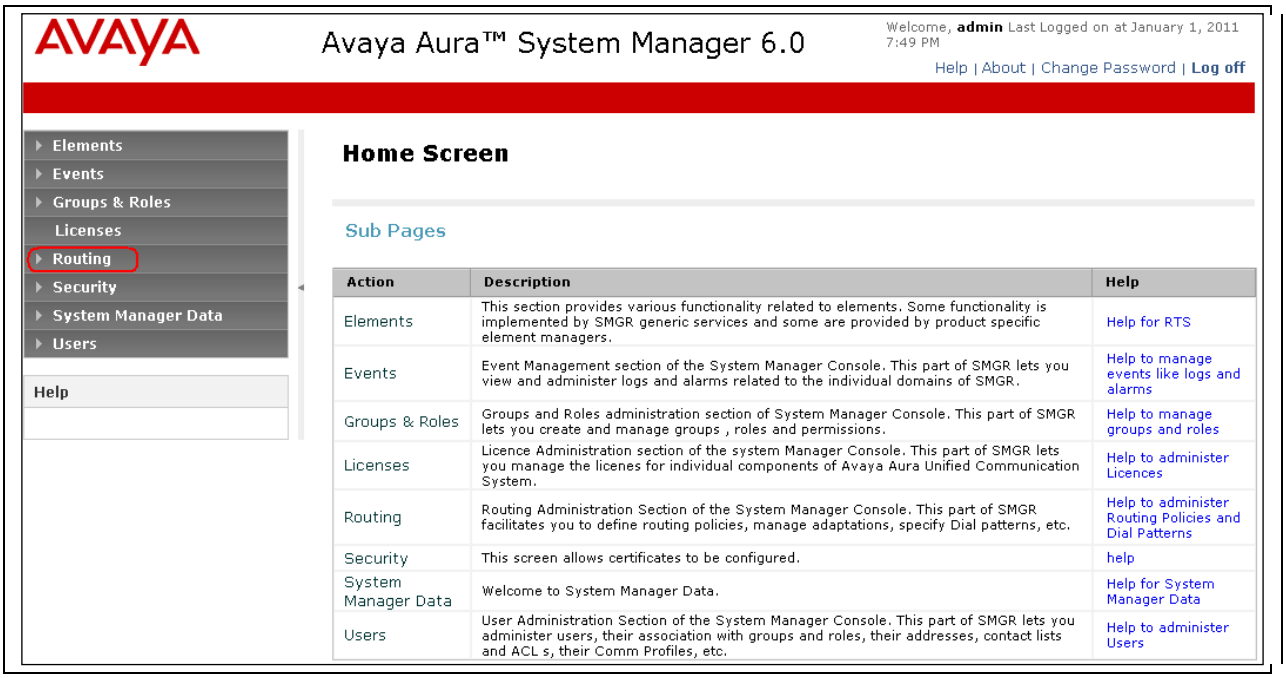
This section provides the procedures for configuring Session Manager, assuming it has been installed and licensed as described in **Reference [3]**. The procedures include adding the following items:

- Specify SIP Domain
- Add Locations
- Add Adaptations
- Add SIP Entities
- Add Entity Links
- Add Routing Policies
- Add Dial Patterns
- Add Session Manager

It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session

Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

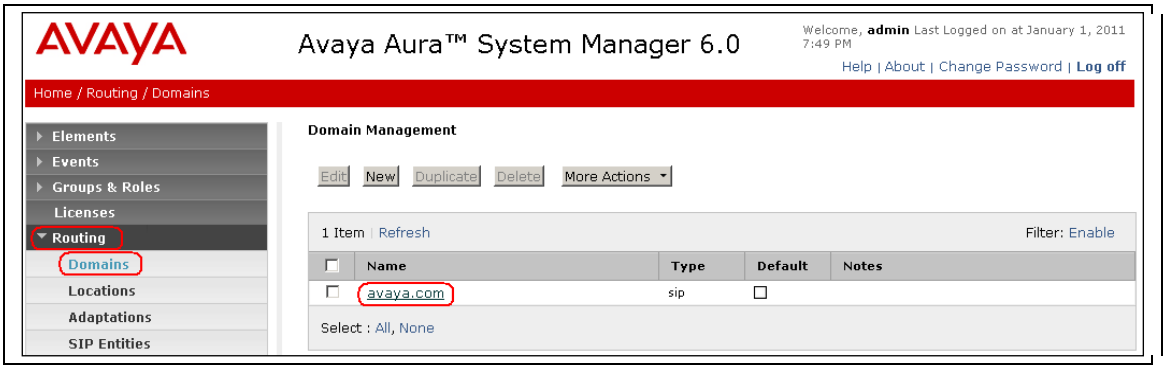
Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials and accept the Copyright Notice. The menu shown below is displayed. Expand the **Routing** Link on the left side as shown.



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. The following screen will then be shown. Fill in the following fields and click **Commit**.

- **Name:** The authoritative domain name (e.g. **avaya.com**)
- **Type** Select **sip**
- **Notes:** Descriptive text (optional)



6.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management. A single location is added to the configuration for Communication Manager and AcmePacket Net-Net Session Director. To add a location, navigate the menu on the left **Routing → Locations** on the left and click on the **New** button on the right (not shown). The following screen will then be shown. Fill in the following:

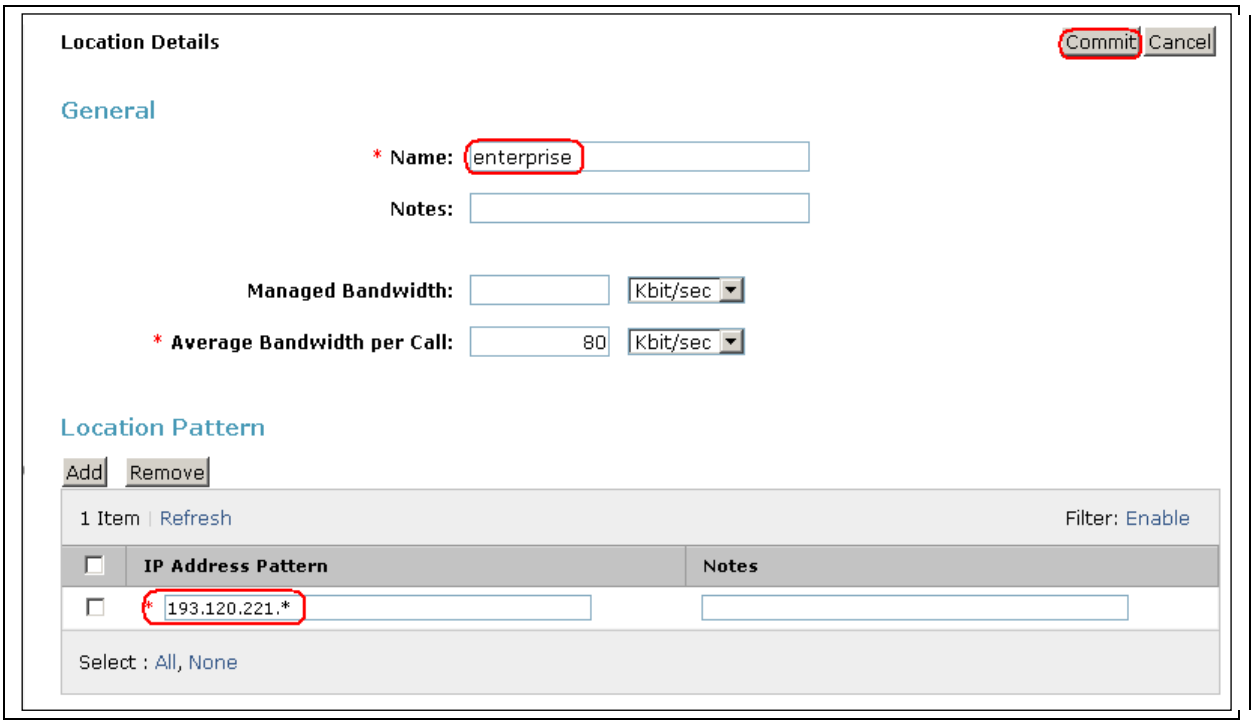
Under **General**:

- **Name:** A descriptive name
- **Notes:** Descriptive text (optional)
- **Managed Bandwidth:** Leave the default or customize as described in **[3]**

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location. In these Application Notes, the pattern selected defined the networks involved e.g. **193.120.221.*** for referring the Enterprise network. **Note:** Other patterns can be used
- **Notes:** Descriptive text (optional)

The screen below shows addition of the **Enterprise** location, which includes all the components of the compliance environment. Click **Commit** to save.

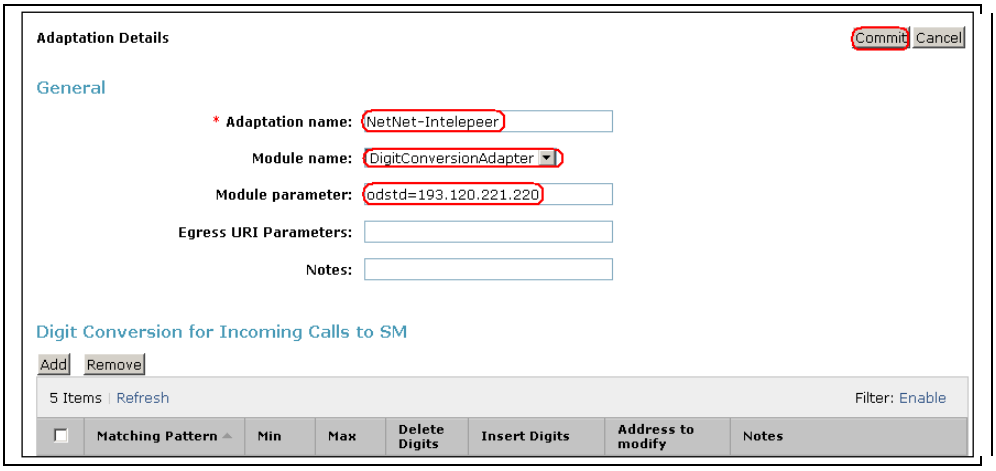


6.3. Add Adaptations

In order to maintain digit manipulation centrally on Session Manager, an adaptation module has to be configured with numbering plan offered from the Service Provider. To add an adaptation, under the **Routing → Adaptations** on the left and click on the **New** button on the right (not shown). The following screen will then be shown. Fill in the following:

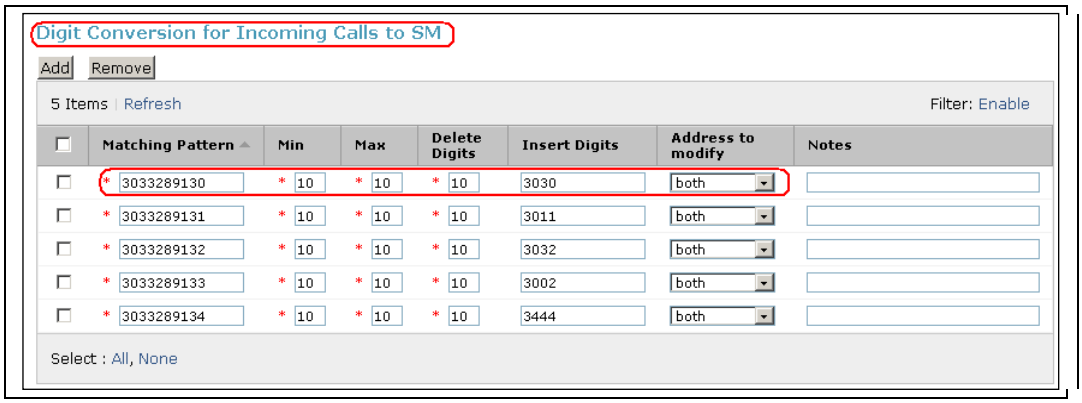
Under **General**:

- **Name:** A descriptive name i.e: **NetNet-Intelepeer**
- **Module Name:** From the dropdown list select **DigitConversionAdapter**
- **Module Parameter:** Enter **odstd=<address>** where address is the IP address of the SIP interface of Session Manager



Under **Digit Conversion for Incoming Calls to SM**:

- **Matching Pattern**: The dialed number from the PSTN i.e. **3033289130**
- **Min/Max**: Minimum/Maximum number of digits i.e. **10**
- **Delete**: Digits to be deleted i.e. **10**
- **Insert Digits**: Digit to be added i.e. **3030**
- **Address to modify**: Select **both**

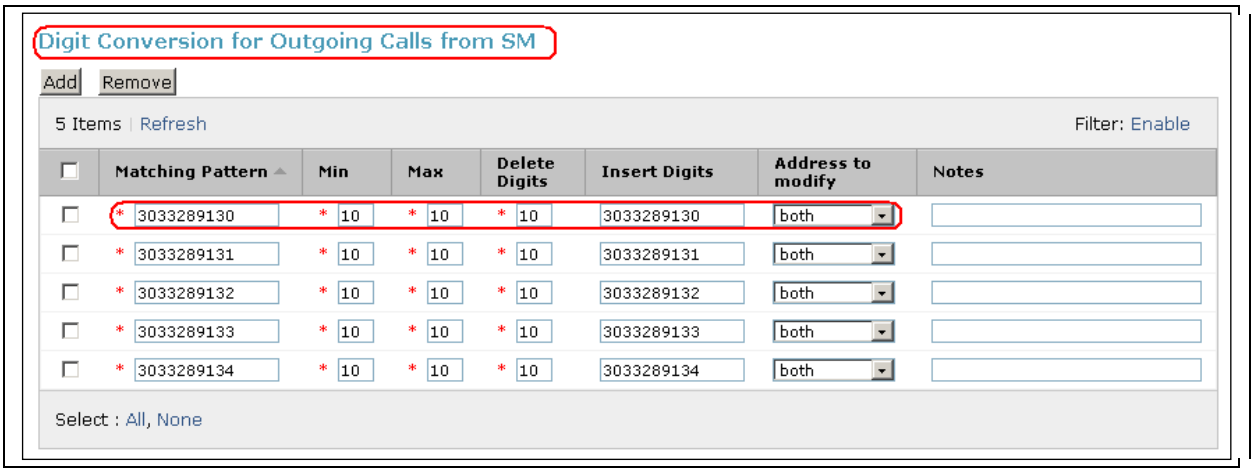


Under **Digit Conversion for Outgoing Calls from SM**:

- **Matching Pattern**: The dialed number from enterprise network i.e.**3033289130**
- **Min:/ Max**: Minimum/ Maximum number of digits i.e. **10**
- **Delete**: Digits to be deleted i.e. **10**
- **Insert Digits**: Digit to be added i.e. **3033289130**
- **Address to modify**: Select **both**

Note: This Digit Conversion rule was used by Session Manager to modify outgoing SIP messages to match the format expected by the Service Provider.

The screen below illustrates the sample configuration. Click **Commit** (shown in first adaptation screen above) to save the changes.



6.4. Add SIP Entities

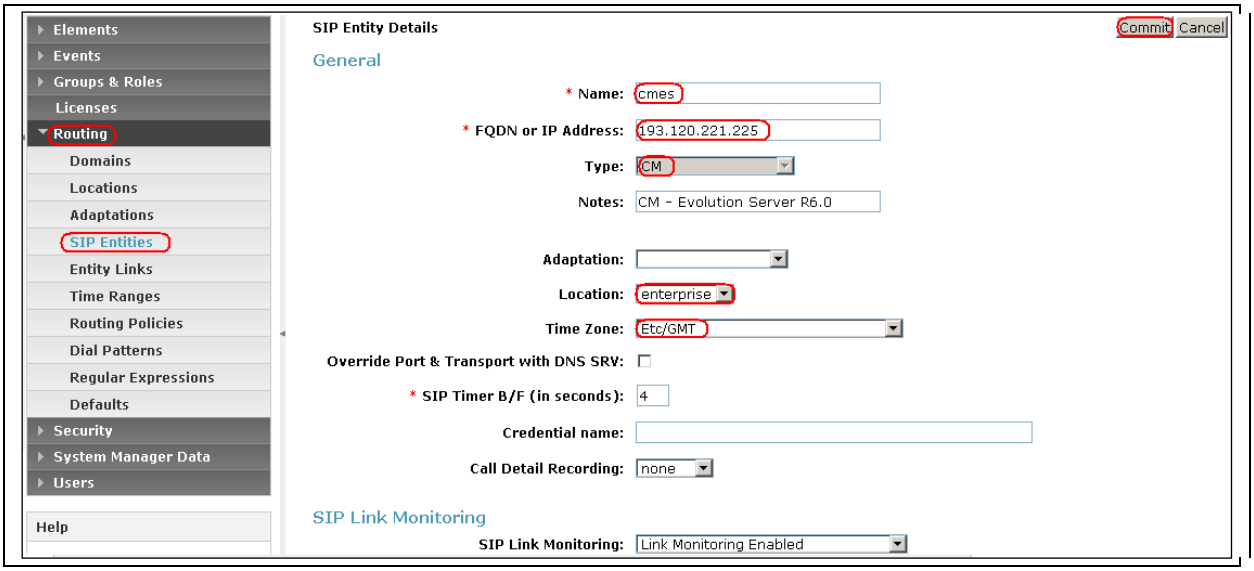
A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration, a SIP Entity is added for the Session Manager, the PROC interface on the Communication Manager and the SIP Trunking for AcmePacket Net-Net which acts as gateway with the Service Provider.

6.4.1. Adding Avaya Aura® Communication Manager Evolution Server SIP Entity

To add a SIP Entity, navigate **Routing → SIP Entities** on the left and click on the **New** button on the right (not shown).
Under **General**:

- **Name:** A descriptive name (i.e. **cmes**)
- **FQDN or IP Address:** IP address of the signaling interface for SIP Trunk defined in **Section 5.6.1** i.e. **193.120.221.225**
- **Type:** Select **CM**
- **Location:** Select one of the locations defined previously i.e. **enterprise**
- **Time Zone:** Time zone for this entity

Defaults can be used for the remaining fields. Click **Commit** to save SIP Entity definition. The following screen shows addition of Communication Manager Evolution Server.

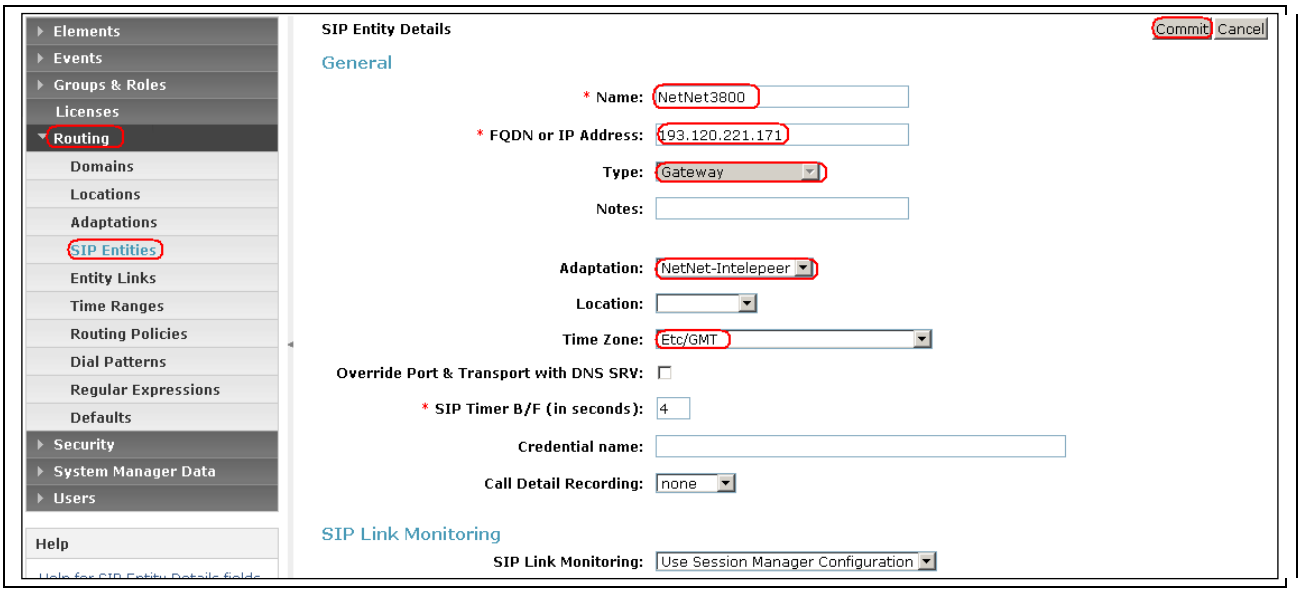


6.4.2. Adding AcmePacket NetNet SIP Entity

Navigate **Routing Policy → SIP Entities** on the left and click on the **New** button on the right. Under **General**:

- **Name:** A descriptive name (i.e. **NetNet3800**)
- **FQDN or IP Address:** IP address of the signaling interface for the inside realm configured on Net-Net, i.e. **193.120.221.171**
- **Type:** Select **Gateway**
- **Adaptation:** Select the adaptation created in **Section 6.3** i.e. **NetNet-IntelePeer**
- **Location:** Select one of the locations defined previously i.e. **enterprise**
- **Time Zone:** Time zone for this entity

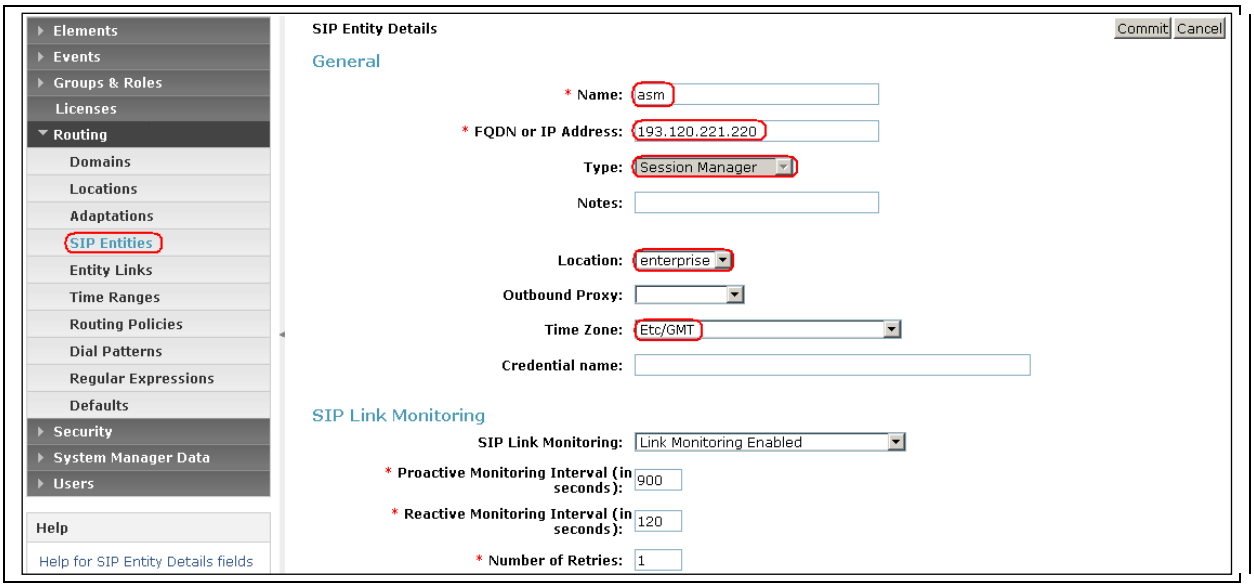
Defaults can be used for the remaining fields. Click **Commit** to save SIP Entity definition. The picture below shows the configuration of the SIP Entity.



6.4.3. Adding Avaya Aura® Session Manager SIP Entity

Navigate **Routing→ SIP Entities** on the left and click on the **New** button on the right.
Under **General**:

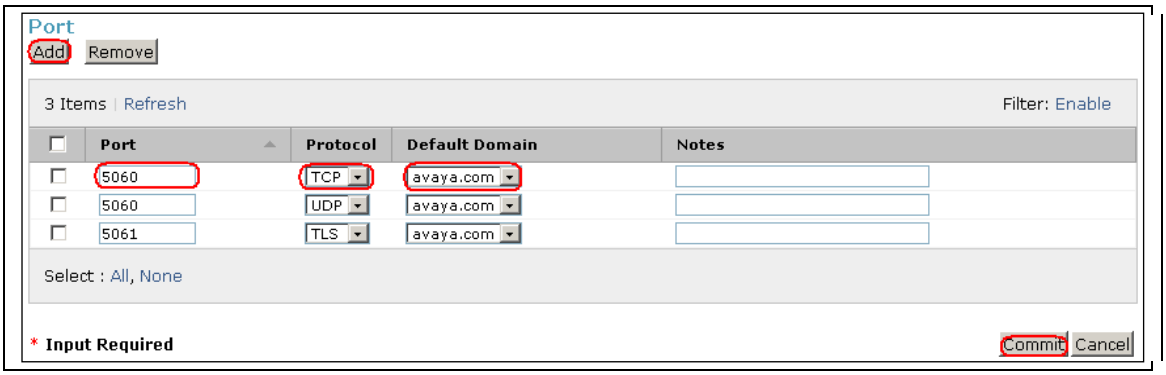
- **Name:** A descriptive name, i.e. **asm**
- **FQDN or IP Address:** IP address of the Session Manager i.e. **193.120.221.220**, the SM-100 software Security Module
- **Type:** Select **Session Manager**
- **Location:** Select one of the locations defined previously
- **Time Zone:** Time zone for this entity



Create a Port definition for **TCP.** 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 (e.g., **avaya.com**)

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition. The following screen shows the addition of Session Manager.

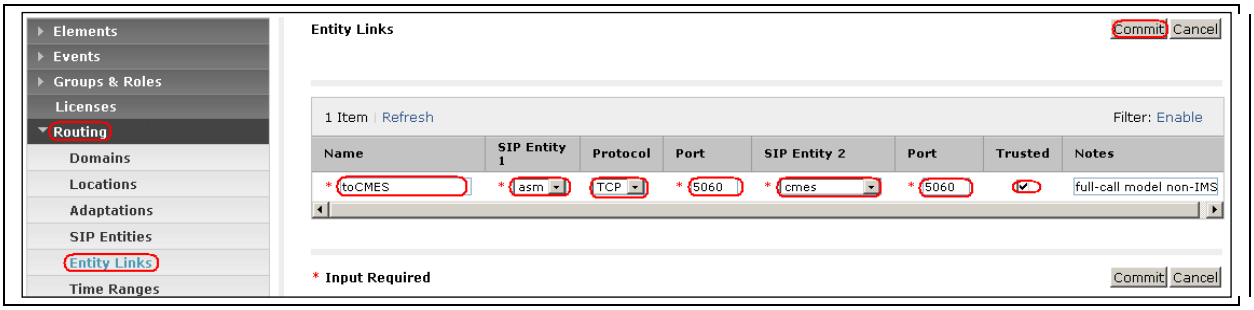


6.5. Add Entity Links

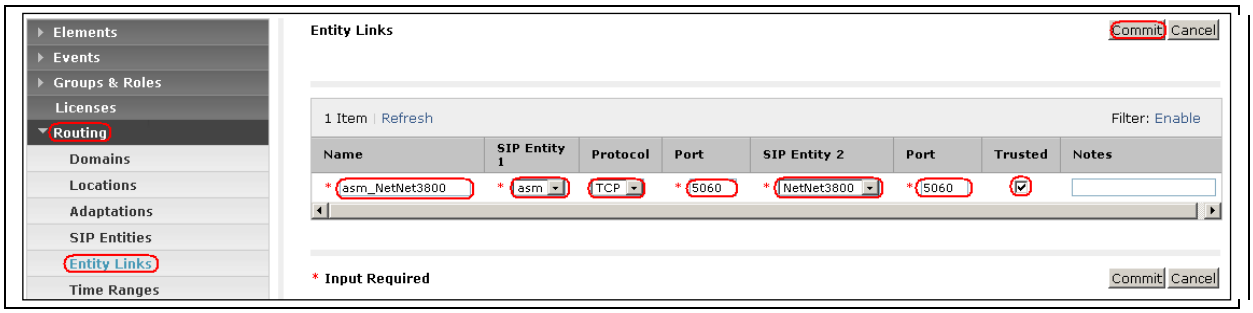
A SIP trunk between Session Manager and a telephony system is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button on the right (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name
- **SIP Entity 1:** Select the **SessionManager** 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
- **Trusted:** Check this box, otherwise calls from the associated SIP Entity specified will be denied
- **Protocol:** Select the transport protocol between **UDP/TCP/TLS** to align with the definition on the **other end o**f the link. In these Application Notes **TCP** was used for **Communication Manager** and **AcmePacket Net-Net Session Director**

Click **Commit** to save each Entity Link definition**.** The following screen illustrates adding the Entity Link for Communication Manager.



The screen below illustrates adding the Entity Link for AcmePacket Net-Net.



6.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.3**. Two routing policies must be added: one for Communication Manager Evolution Server and one for the Net-Net 3800. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right (not shown). The following screen is displayed. Fill in the following:

Under **General:**

- Enter a descriptive name in **Name**

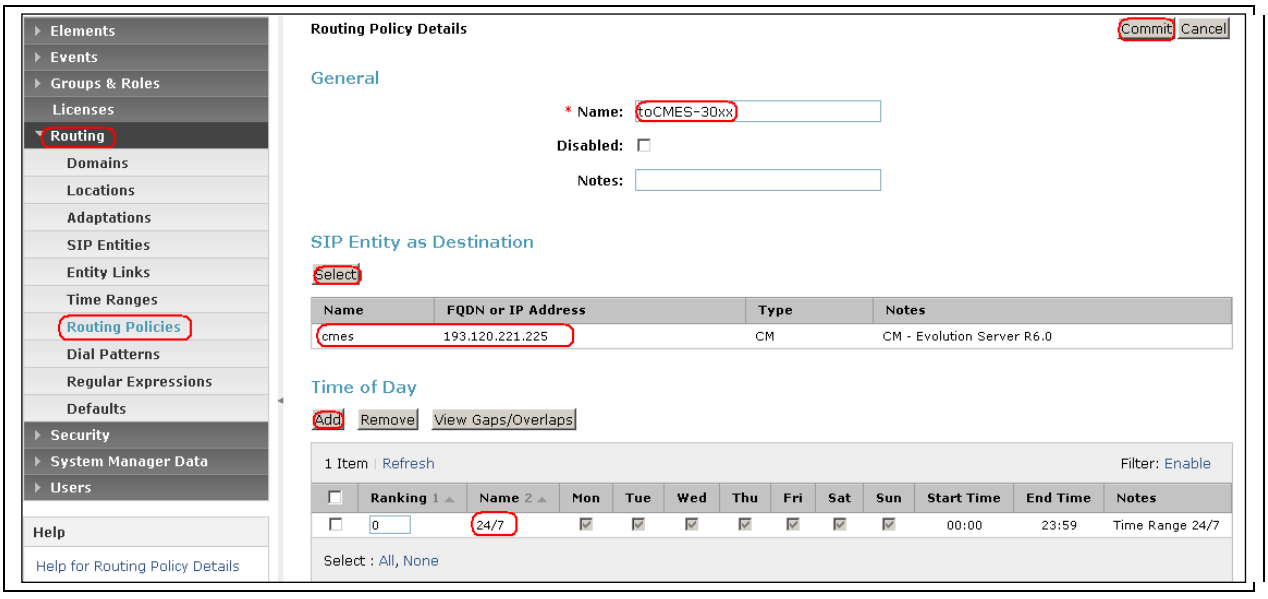
Under **SIP Entity as Destination:**

- Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

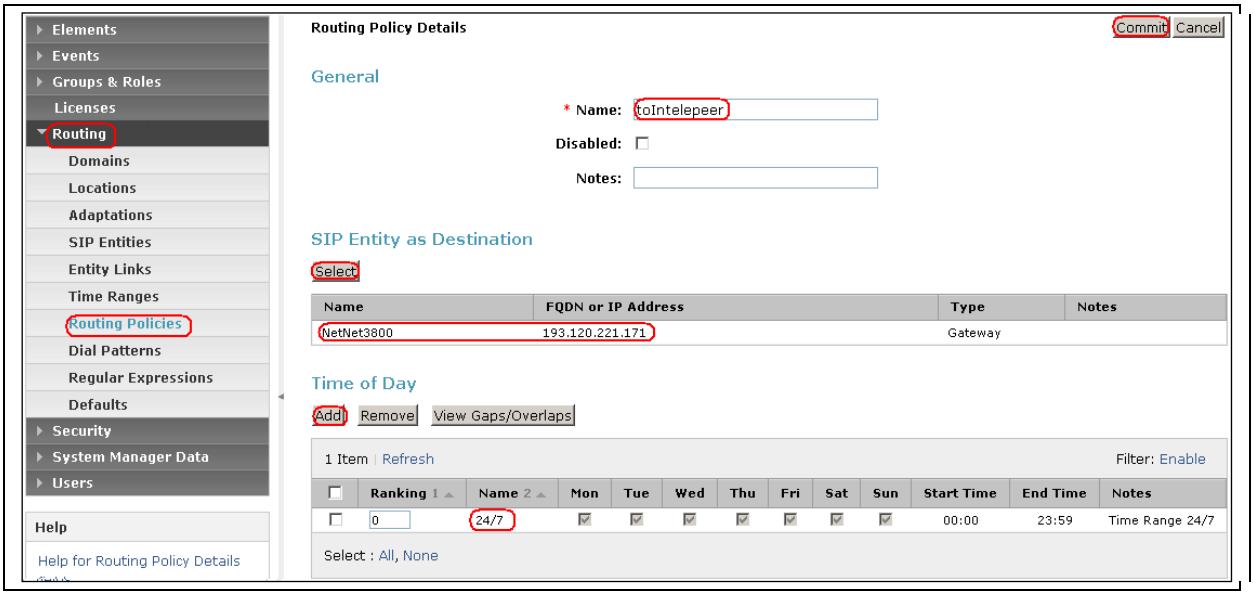
Under **Time of Day:**

- Click **Add**, and select the time range configured. In these Application Notes, the predefined **24/7** Time Range is used.

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



The following screen shows the Routing Policy for AcmePacket Net-Net Session Director.



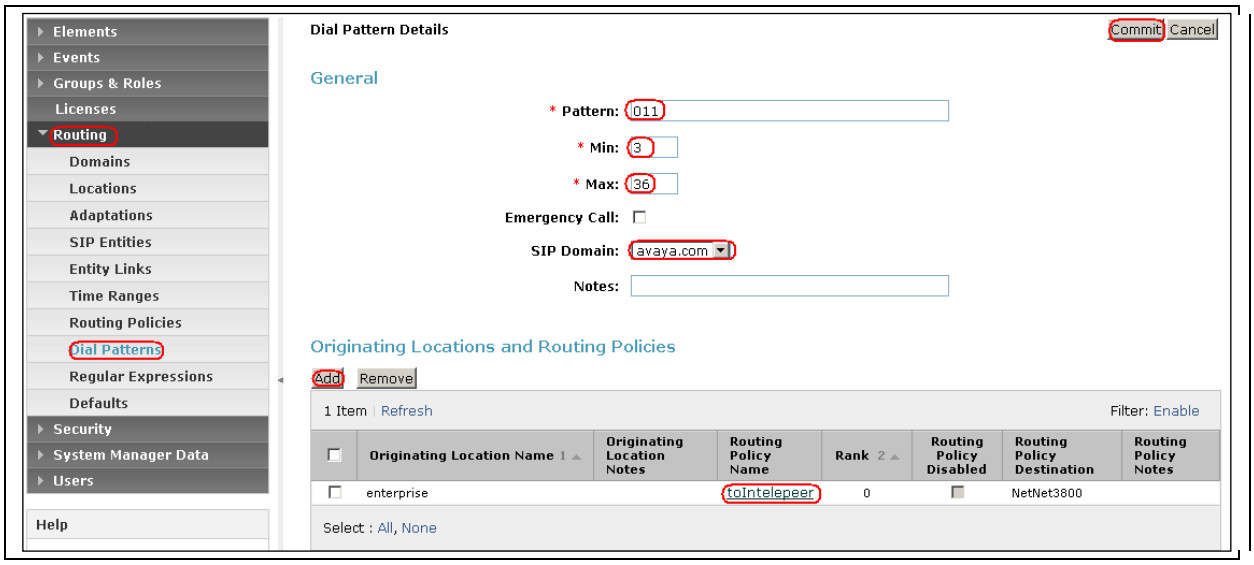
6.7. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 4-digit extensions beginning with **30** reside on Communication Manager and numbers beginning with **011** with 3 to 25 digits reside on the Service Provider.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right (not shown).Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to AcmePacket Net-Net that in turn will be forwarded to the IntelePeer's gateway:
Under **General**:

- **Pattern:** Dialed number or prefix i.e. **011**
- **Min:** Minimum length of dialed number i.e. **3**
- **Max:** Maximum length of dialed number i.e. **24**
- **SIP Domain:** Select **avaya.com**

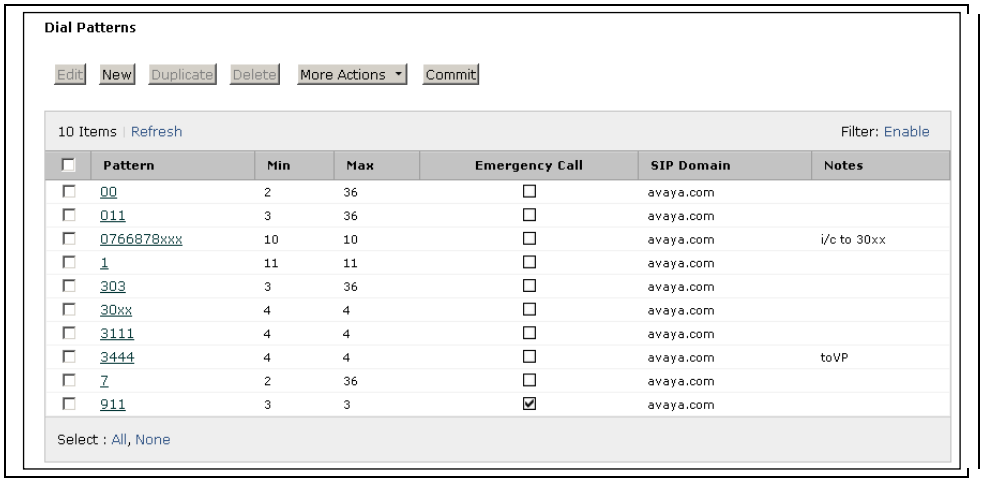
Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list. Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows a sample the dial pattern definition for SIP Trunking service. Create as many dial pattern required for the destination considered.



Repeat the process adding one or more dial patterns for the extensions that reside on Communication Manager. Fill in the following, which corresponds to the dial pattern for routing calls to Communication Manager:
Under **General**:

- **Pattern:** Dialed number or prefix i.e. **30**
- **Min:** Minimum length of dialed number i.e. **4**
- **Max:** Maximum length of dialed number i.e. **4**
- **SIP Domain:** Select **avaya.com**

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 a sample the dial pattern definition for Communication Manager Evolution Server. The figure below summarizes the creation of several dial patterns created for the compliance test bed.



6.8. Add/View Avaya Aura® Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane (**Section 6.1**) and click on the New button in the right pane (not shown). If the Session Manager already exists, click View (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen: In the General:

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

In the **Security Module** section, (not shown) enter the following values:

- SIP Entity IP Address: Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- 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 **Save** to add this Session Manager.

7. Configure Acme Packet Net-Net Session Director

This section describes the configuration of the Acme Packet Session Director necessary for interoperability with Session Manager and with IntelePeer SBC. The Acme Packet Session Director was configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet Session Director. Each of the configuration components is defined in the Acme Packet Session Director configuration file contained in **Appendix A**. However, this configuration file serves multiple purposes and thus not everything in the file pertains to these Application Notes. Also note that

this section does not cover standard Acme Packet Session Director configurations (e.g., *redundancy-config*, *media-manager*, etc.) that are not directly related to the interoperability test. This section will not attempt to describe each component in its entirety but instead will highlight critical fields in each component which relates to the functionality in these Application Notes and the direct connection to Session Manager. The remaining fields are generally the default/standard value used by the Acme Packet Session Director for that field. For additional details on the administration of the Acme Packet Session Director, refer to **Reference [8].**

7.1. Acme Packet Command Line Interface Summary

The Acme Packet Session Director is configured using the Acme Packet Command Line Interface (ACLI). The following are the generic ACLI steps for configuring various elements.

1. Access the console port of the Acme Packet Session Director using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the Session Director for cable connection). Use the following settings for the serial port on the PC.
   - Bits per second: 115200
   - Data bits: 8
   - Parity : None
   - Stop bits: 1
   - Flow control: None
2. Log in to the Acme Packet Session Director with the user password.
3. Enable the Superuser mode by entering the enable command and then the superuser password. The command prompt will change to include a "#" instead of a ">" while in Superuser mode. This level of system access (i.e. at the "acmesystem#" prompt) will be referred to as the *main* level of the ACLI. Specific sub-levels of the ACLI will then be accessed to configure specific *elements* and specific *parameters* of those elements.
4. In Superuser mode, enter the **configure terminal** command. The **configure terminal** command is used to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the *configuration* level.
5. Enter the **name of an element** to be configured (e.g., **system**).
6. Enter the **name of a sub-element**, if any (e.g., **phy-interface**).
7. Enter the **name of an element parameter** followed by its **value** (e.g., **name s0p0**).
8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as necessary to return to the configuration level.
10. Repeat Steps 5 - 9 to configure all the elements.
11. Enter **exit** to return to the main level.
12. Type **save-config** to save the entire configuration.
13. Type **activate-config** to activate the entire configuration.

After accessing different levels of the ACLI to configure elements and parameters, it is necessary to return to the main level in order to run certain tasks such as saving the configuration, activating the configuration, and rebooting the system.

7.2. System Configuration

The system configuration defines system-wide parameters for the Acme Packet Session Director.

The key system configuration (***system-config***) field(s) are:

- **hostname**: a descriptive name for the Session Director i.e. **netnet3800**.
- **default-gateway**: The IP address of the default gateway for the management network (193.120.221.129) from **Figure 1**. In this case, the default gateway is **193.120.221.129**.

```
system-config
        hostname                        netnet3800
        description                     NetNet
        location
        mib-system-contact
        mib-system-name
        mib-system-location

        < text removed for brevity >

        call-trace                      disabled
        internal-trace                  disabled
        log-filter                      all
        default-gateway                 193.120.221.129
        restart                         enabled
        exceptions
        telnet-timeout                  0
        console-timeout                 0
        remote-control                  enabled
        cli-audit-trail                 enabled
        link-redundancy-state           disabled
        source-routing                  disabled
        cli-more                        disabled
        terminal-height                 24
        debug-timeout                   0
        trap-event-lifetime             0
        default-v6-gateway              ::
        ipv6-support                    disabled
```

7.3. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface **slot 0 / port 0** of the Acme Packet Session Director was connected to the external un-trusted network. Ethernet **slot 0 / port 1** was connected to the internal corporate LAN. A network interface was defined for each physical interface to assign it a routable IP address.

The key physical interface (***phy-interface***) fields are:

- **name**: A descriptive string used to reference the Ethernet interface.
- **operation-type**: **Media** indicates both signaling and media packets are sent on this interface.
- **slot / port**: The identifier of the specific Ethernet interface used.

```
phy-interface
        name                            s0p0
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        overload-protection             disabled
        last-modified-by                admin@console
        last-modified-date              2010-11-11 10:07:45
phy-interface
        name                            s0p1
        operation-type                  Media
        port                            1
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        overload-protection             disabled
        last-modified-by                admin@console
        last-modified-date              2010-11-11 11:18:03
```

The key network interface (***network-interface***) fields are:

- **name**: The name of the physical interface (defined previously) that is associated with this network interface.
- **ip-address**: The IP address used for the Session Director services on the specific interface (**i.e. 193.120.221.170**). The Acme Packet Session Director was used in the compliance test as standalone system and not in high availabiliy pair, for further details on redundant configuration please refer to [**8**]
- **pri-utility-addr**: not implemented in a standalone configuration
- **sec-utility-addr**: not implemented in a standalone configuration
- **netmask**: Subnet mask for the IP subnet (i.e. **255.255.255.128**).
- **gateway**: The subnet gateway address (i.e. **193.120.221.129**)
- **hip-ip-list**: The list of virtual IP addresses assigned to the Acme Packet Session Director on this interface. If a single virtual IP address is used, this value would be the same as the value entered for the **ip-address** field above.
- **icmp-address**: The list of IP addresses to which the Acme Packet Session Director will answer ICMP requests on this interface.

```
network-interface
        name                            s0p0
        sub-port-id                     0
        description
        hostname
        ip-address                      193.120.221.170
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.128
        gateway                         193.120.221.129
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     193.120.221.170
        ftp-address
        icmp-address                    193.120.221.170
        snmp-address
        telnet-address
        ssh-address
        last-modified-by                admin@console
        last-modified-date              2010-11-15 11:04:24
```

The settings for the private side network interface are shown below.

```
network-interface
        name                            s0p1
        sub-port-id                     0
        description
        hostname
        ip-address                      193.120.221.171
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.128
        gateway                         193.120.221.129
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     193.120.221.171
        ftp-address                     193.120.221.171
        icmp-address                    193.120.221.171
        snmp-address
        telnet-address
        ssh-address                     193.120.221.171
        last-modified-by                admin@console
        last-modified-date              2010-11-22 11:45:51
```

7.4. Realm

A realm represents a group of related Acme Packet Session Director components. Two realms were defined for the compliance test. The **OUTSIDE** realm was defined for the external network and the **INSIDE** realm was defined for the internal network. The key realm (***realm-config***) fields are:

- **identifier**: A string used as a realm reference. This will be used in the configuration of other components.
- **network interfaces**: The network interfaces located in this realm.
- **out-manipulationid**: **NAT_IP** This name refers to a set of sip-manipulations (defined in **Section 7.8**) that are performed on outbound traffic from the Acme Packet Session Director. These sip-manipulations are specified in each realm. Thus, these sip-manipulations are applied to outbound traffic from the public side of the Acme Packet Session Director as well as to outbound traffic from the private side of the Acme Packet Session Director.

```
realm-config
        identifier                      OUTSIDE
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s0p0:0

        < text removed for brevity >

        out-translationid
        in-manipulationid
        out-manipulationid              NAT_IP

        < text removed for brevity >

realm-config
        identifier                      INSIDE
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s0p1:0

        < text removed for brevity >

        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid              NAT_IP

        < text removed for brevity >
```

7.5. SIP Configuration

The SIP configuration (***sip-config***) defines the global system-wide SIP parameters. The key SIP configuration (***sip-config***) fields are:

- **home-realm-id**: The name of the realm on the private side of the Acme Packet Session Director.
- **nat-mode: None**
- **registrar-domain**: An asterisk (*****) is specified to allow any domain.
- **registrar-host**: An asterisk (*****) is specified to allow any host.
- **registrar-port**: port used for registration, ie. **5060**
- **options max-udp-length=0**: Option required to process long udp invites.
  Note: This setting is used to disable fragmentation of UDP messages.

```
sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id                   INSIDE
        egress-realm-id                 INSIDE
        nat-mode                        None
        registrar-domain                *
        registrar-host                  *
        registrar-port                  5060

        < text removed for brevity >

        options                         max-udp-length=0
```

7.6. SIP Interface

The SIP interface (***sip-interface***) defines the receiving characteristics of the SIP interfaces on the Acme Packet Session Director. Two SIP interfaces were defined; one for each realm. The key SIP interface (***sip-interface***) fields are:

- **realm-id**: The name of the realm to which this interface is assigned.
- **sip port**
  - **address**: The IP address assigned to this sip-interface.
  - **port**: The port assigned to this sip-interface. Port 5060 is used for both UDP and TCP.
  - **transport-protocol**: The transport method used for this interface.
  - **allow-anonymous**: Defines from whom SIP requests will be allowed. On the public side, the value of **agents-only** is used. Thus, SIP requests will only be accepted from session agents (as defined in **Section 7.7**) on this interface. On the private side, the value of all is used. Thus, SIP requests will be accepted from any entity on this interface.

```
sip-interface
        state                           enabled
        realm-id                        INSIDE
        description
        sip-port
                address                         193.120.221.171
                port                            5060
                transport-protocol              TCP
                tls-profile
                allow-anonymous                 all
        carriers
        trans-expire                    0

        < text removed for brevity >

sip-interface
        state                           enabled
        realm-id                        OUTSIDE
        description
        sip-port
                address                         193.120.221.170
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 agents-only
                ims-aka-profile
        carriers
        trans-expire                    0

         < text removed for brevity >
```

7.7. Session Agent

A session agent defines the characteristics of a signaling peer to the Acme Packet Session Director such as Session Manager or the IntelPeer SBC. The key session agent (session-agent) fields are:

- **hostname**: Fully qualified domain name or IP address of this SIP peer.
- **port**: The port used by the peer for SIP traffic.
- **app-protocol: SIP**
- **transport-method: DynamicTCP** or **UDP**
- **realm-id**: The realm id where this peer resides.
- **description:** A descriptive name for the peer.
- **ping-method**: **OPTIONS;hops=0** This setting defines that the SIP OPTIONS message will be sent to the peer to verify that the SIP connection is functional. In addition, this parameter causes the Acme Packet Session Director to set the SIP "Max-Forward" field to 0 in outbound SIP OPTIONS pings generated by the Acme Packet Session Director to this session agent.
- **ping-interval**: Specifies the interval (in seconds) between each ping attempt.

The settings for the session agent on the public side are shown below.

```
session-agent
        hostname                        68.68.120.41
        ip-address
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        OUTSIDE
        egress-realm-id
        description                     IntelepeerSBC
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled

         < text removed for brevity >


        ping-method                     OPTIONS;hops=0
        ping-interval                   60
        ping-send-mode                  keep-alive

         < text removed for brevity >
```

The settings for the session agent on the private side are shown below.

```
session-agent
        hostname                        193.120.221.220
        ip-address                      193.120.221.220
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                DynamicTCP
        realm-id                        INSIDE
        egress-realm-id
        description                     INSIDE_SessionManager
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled

        < text removed for brevity >

        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   60
        ping-send-mode                  keep-alive

        < text removed for brevity >
```

7.8. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages (if necessary) for interoperability. In **Section 7.4**, it was defined that the set of sip-manipulations named **NAT_IP** would be performed on outbound traffic in each realm.

The key SIP manipulation (***sip-manipulation***) fields are:

- **name**: The name of this set of SIP header rules.
- **header-rule**:
  - **name**: The name of this individual header rule.
  - **header-name**: The SIP header to be modified.
  - **action**: The action to be performed on the header.
  - **comparison-type**: The type of comparison performed when determining a match.
  - **msg-type**: The type of message to which this rule applies.
  - **element-rule**:
    - **name**: The name of this individual element rule.
    - **type**: Defines the particular element in the header to be modified.
    - **action**: The action to be performed on the element.
    - **match-val-type**: Element matching criteria on the data type (if any) in order to perform the defined action.
    - **comparison-type**: The type of comparison performed when determining a match.
    - **match-value**: Element matching criteria on the data value (if any) in order to perform the defined action.
    - **new-value**: New value for the element (if any).

The example below shows the **manipFrom** header-rule. It specifies that the "***From***" header in SIP request messages will be manipulated based on the element rule defined. The element rule specifies if the host part of the URI in this header is an IP address, than replace it with the value of ***$LOCAL_IP***. The value of $LOCAL_IP is the IP address of the SIP peer in this realm.
In a similar way it is defined the **manipTo** header roule where the "***To***" header, that in turn will be replaced with ***$REMOTE_IP***.

```
sip-manipulation
        name                            NAT_IP
        description
        header-rule
                name                            manipFrom
                header-name                     From
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods
                match-value
                new-value
                element-rule
                        name                            From
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP
        header-rule
                name                            manipTo
                header-name                     To
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods
                match-value
                new-value
                element-rule
                        name                            To
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $REMOTE_IP
```

7.9. Steering Pools

Steering pools define the range of ports to be used for the RTP voice stream. Two steering pools were defined; one for each realm. The key steering pool (***steering-pool***) fields are:

- **ip-address**: The address of the interface on the Acme Packet Session Director.
- **start-port**: An even number of the port that begins the range.
- **end-port**: An odd number of the port that ends the range.
- **realm-id**: The realm to which this steering pool is assigned.

```
steering-pool
        ip-address                      193.120.221.170
        start-port                      8000
        end-port                        20000
        realm-id                        OUTSIDE
        network-interface
        last-modified-by                admin@console
        last-modified-date              2010-11-15 13:16:13
steering-pool
        ip-address                      193.120.221.171
        start-port                      8000
        end-port                        20000
        realm-id                        INSIDE
        network-interface
        last-modified-by                admin@console
        last-modified-date              2010-11-15 13:16:50
```

7.10. Local Policy

Local policy controls the routing of SIP calls from one realm to another. The key local policy (***local-policy***) fields are:

- **from-address**: A policy filter indicating the originating IP address to which this policy applies. An asterisk (*****) indicates any IP address.
- **to-address**: A policy filter indicating the terminating IP address to which this policy applies. An asterisk (*****) indicates any IP address.
- **source-realm**: A policy filter indicating the matching realm in order for the policy rules to be applied.
- **policy-attribute**:
  - **next-hop**: The IP address where the message should be sent when the policy rules match.
  - **realm**: The realm associated with the next-hop IP address.

In this case, the first policy provides a simple routing rule indicating that messages originating from the INSIDE realm are to be sent to the OUTSIDE realm via IP address **68.68.120.41** (IntelePeer SBC).

```
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        INSIDE
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@console
        last-modified-date              2010-11-15 12:17:28
        policy-attribute
                next-hop                        68.68.120.41
                realm                           OUTSIDE
                action                          none
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
```

7.11. Host Routes

This configuration is needed as the IP address of the IntelePeer SBC and the network interface icmp-address of the Acme Packet Session Director (on either the public or the private side) do not reside in the same IP subnet. In the compliance test, the IP address of the Session Manager (193.120.221.220) and the Acme Packet Session Director private side network interface icmp address (193.120.221.171) reside in the same IP subnet, therefore this configuration is only needed for the public side where the IP address of the Service Provider SBC (ie. **68.68.120.41**) and the Acme Packet Session Director network interface icmp address (193.120.221.170) reside in different IP subnet. The key host-routes fields are:

- **dest-network**: IP address of the IntelePeer SBC to connect to.
- **netmask**: specified as 255.255.255.255 so that only the specified IP of the IntelePeer SBC can be used in the static route.
- **gateway** as specified in the public side network-interface configuration (**Section 7.3**).
- **description**: a descriptive text

```
host-routes
        dest-network                    68.68.120.41
        netmask                         255.255.255.0
        gateway                         193.120.221.129
        description
```

8. Verification Steps

This section provides the verification steps that may be performed to verify that Avaya Enterprise network can establish and receive with IntelePeer SIP gateway.

8.1. Verify Avaya Aura® Communication Manager Evolution Server Trunk Status

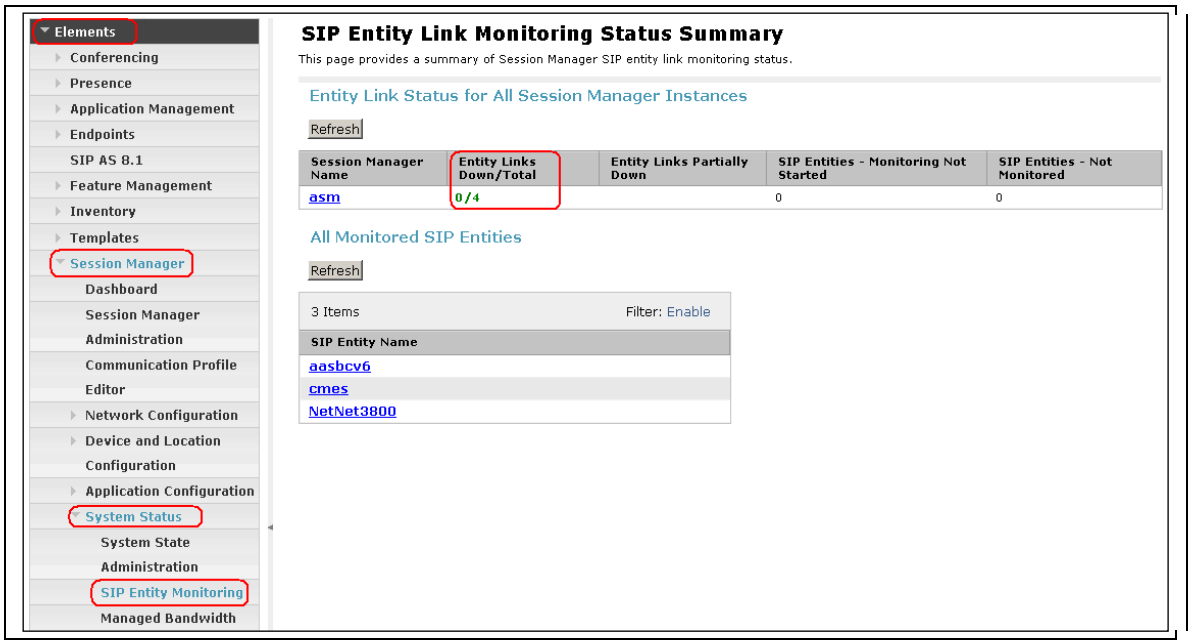
On Communication Manager, ensure that all the signalling groups are **in-service** status, by issuing the command **status signalling-group n** where **n** is the signalling group number, as illustrated by the figure below.

```
status signaling-group 100
                         STATUS SIGNALING GROUP

       Group ID: 100                              Active NCA-TSC Count: 0
     Group Type: sip                              Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
    Group State: in-service
```

8.2. SIP Monitoring on Avaya Aura® Session Manager

Expand the menu on the left and navigate **Elements → Session Manager → System Status → SIP Entity Monitoring**. Verify that none of the links to the defined SIP entities are down, indicating that they are all reachable for call routing. The figure below illustrates the SIP Entity Monitoring Status Summary page.



9. Conclusion

The SIP Trunking solution from IntelePeer passed compliance testing. These Application Notes describe the procedures required to configure a telephony solution based on Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Acme Packet Net-Net 3800 Session Director to interoperate with SIP trunks to IntelePeer.

10. Additional References

The following documentation may be obtained from http://support.avaya.com.

[1] Installing and Configuring Avaya Aura® Communication Manager, Doc ID 03-603558, Release 6.0 June, 2010 available at http://support.avaya.com/css/P8/documents/100089133

[2] Administering Avaya Aura® Communication Manager, Doc ID 03-300509, Issue 6.0 June 2010 available at http://support.avaya.com/css/P8/documents/100089333

[3] Administering Avaya Aura® Session Manager, Doc ID 03-603324, Release 6.0, June 2010 available at http://support.avaya.com/css/P8/documents/100082630

[4] Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473 Release 6.0, June 2010 available at http://support.avaya.com/css/P8/documents/100089152

[5] Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, Release 6.0, June 2010 available at http://support.avaya.com/css/P8/documents/100089154
[6] Administering Avaya Aura® System Manager, Document Number 03-603324, Release 6.0, June 2010 available at http://support.avaya.com/css/P8/documents/100089681

Product documentation for the Session Director can be obtained from Acme Packet's support web site (https://support.acmepacket.com).

[7] Net-Net 3800 System Hardware Installation Guide, Release Version 1.0, Acme Packet Documentation Set.
[8] Net-Net 4000 ACLI Reference Guide, Release Version S-C6.1.0, Acme Packet Documentation Set.

11. Appendix A: Acme Packet Session Director Configuration File

Included below is the Acme Packet Session Director configuration used during the compliance testing. The contents of the configuration can be shown by using the ACLI command **show running-config** at the Acme Packet Session Director.

```
acmesystem# show running-config
authentication
        source-port                     1812
        type                            local
        protocol                        pap
        allow-local-authorization       disabled
        login-as-admin                  enabled
        management-strategy             hunt
        ike-radius-params-name
        management-servers
        last-modified-by                admin@console
        last-modified-date              2010-11-22 06:53:32
host-routes
        dest-network                    68.68.120.0
        netmask                         255.255.255.0
        gateway                         193.120.221.129
        description
        last-modified-by                admin@console
        last-modified-date              2010-11-15 11:17:32
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        OUTSIDE
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@console
```

```
        last-modified-date              2010-11-15 12:16:29
        policy-attribute
                next-hop                        193.120.221.220
                realm                           INSIDE
                action                          none
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        INSIDE
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@console
        last-modified-date              2010-11-15 12:17:28
        policy-attribute
                next-hop                        68.68.120.41
                realm                           OUTSIDE
                action                          none
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
network-interface
        name                            s0p0
        sub-port-id                     0
        description
        hostname
```

```
        ip-address                      193.120.221.170
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.128
        gateway                         193.120.221.129
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     193.120.221.170
        ftp-address
        icmp-address                    193.120.221.170
        snmp-address
        telnet-address
        ssh-address
        last-modified-by                admin@console
        last-modified-date              2010-11-15 11:04:24
network-interface
        name                            s0p1
        sub-port-id                     0
        description
        hostname
        ip-address                      193.120.221.171
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.128
        gateway                         193.120.221.129
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     193.120.221.171
        ftp-address                     193.120.221.171
        icmp-address                    193.120.221.171
        snmp-address
        telnet-address
        ssh-address                     193.120.221.171
        last-modified-by                admin@console
        last-modified-date              2010-11-22 11:45:51
phy-interface
```

```
        name                            s0p0
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        overload-protection             disabled
        last-modified-by                admin@console
        last-modified-date              2010-11-11 10:07:45
phy-interface
        name                            s0p1
        operation-type                  Media
        port                            1
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        overload-protection             disabled
        last-modified-by                admin@console
        last-modified-date              2010-11-11 11:18:03
realm-config
        identifier                      OUTSIDE
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s0p0:0
        mm-in-realm                     disabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid              NAT_IP
        manipulation-string
        manipulation-pattern
```

```
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        ext-policy-svr
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        dyn-refer-term                  disabled
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        xnq-state                       xnq-unknown
        hairpin-id                      0
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
        last-modified-by                admin@console
        last-modified-date              2010-11-11 11:24:46
realm-config
        identifier                      INSIDE
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s0p1:0
        mm-in-realm                     disabled
        mm-in-network                   enabled
```

```
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid              NAT_IP
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        ext-policy-svr
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        dyn-refer-term                  disabled
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
```

```
        xnq-state                       xnq-unknown
        hairpin-id                      0
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
        last-modified-by                admin@193.120.221.208
        last-modified-date              2010-11-22 08:24:21
session-agent
        hostname                        68.68.120.41
        ip-address
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        OUTSIDE
        egress-realm-id
        description                     IntelepeerSBC
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
```

```
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
        last-modified-by                admin@console
        last-modified-date              2010-11-15 11:21:25
session-agent
        hostname                        193.120.221.220
        ip-address                      193.120.221.220
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        INSIDE
        egress-realm-id
        description                     INSIDE_SessionManager
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
```

```
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
        last-modified-by                admin@193.120.221.208
        last-modified-date              2010-11-22 08:02:37
sip-config
        state                           enabled
        operation-mode                  dialog
```

```
        dialog-transparency             enabled
        home-realm-id                   INSIDE
        egress-realm-id                 INSIDE
        nat-mode                        None
        registrar-domain                *
        registrar-host                  *
        registrar-port                  5060
        register-service-route          always
        init-timer                      500
        max-timer                       4000
        trans-expire                    32
        invite-expire                   180
        inactive-dynamic-conn           32
        enforcement-profile
        pac-method
        pac-interval                    10
        pac-strategy                    PropDist
        pac-load-weight                 1
        pac-session-weight              1
        pac-route-weight                1
        pac-callid-lifetime             600
        pac-user-lifetime               3600
        red-sip-port                    1988
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        add-reason-header               disabled
        sip-message-len                 4096
        enum-sag-match                  disabled
        extra-method-stats              disabled
        registration-cache-limit        0
        register-use-to-for-lp          disabled
        options                         max-udp-length=0
        refer-src-routing               disabled
        add-ucid-header                 disabled
        pass-gruu-contact               disabled
        sag-lookup-on-redirect          disabled
        last-modified-by                admin@console
        last-modified-date              2010-12-01 13:06:54
sip-interface
        state                           enabled
        realm-id                        INSIDE
        description
        sip-port
                address                         193.120.221.171
                port                            5060
                transport-protocol              TCP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
        carriers
        trans-expire                    0
        invite-expire                   0
        max-redirect-contacts           0
        proxy-mode
        redirect-action
```

```
        contact-mode                    none
        nat-traversal                   none
        nat-interval                    30
        tcp-nat-interval                90
        registration-caching            disabled
        min-reg-expire                  300
        registration-interval           3600
        route-to-registrar              disabled
        secured-network                 disabled
        teluri-scheme                   disabled
        uri-fqdn-domain
        trust-mode                      all
        max-nat-interval                3600
        nat-int-increment               10
        nat-test-increment              30
        sip-dynamic-hnt                 disabled
        stop-recurse                    401,407
        port-map-start                  0
        port-map-end                    0
        in-manipulationid               NAT_IP
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                 disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns   0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode            pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                  none
        implicit-service-route          disabled
        rfc2833-payload                 101
        rfc2833-mode                    transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                 disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                   none
        add-sdp-invite                  disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by                admin@console
        last-modified-date              2010-11-30 06:22:48
sip-interface
        state                           enabled
```

```
        realm-id                        OUTSIDE
        description
        sip-port
                address                         193.120.221.170
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 agents-only
                ims-aka-profile
        carriers
        trans-expire                    0
        invite-expire                   0
        max-redirect-contacts           0
        proxy-mode
        redirect-action
        contact-mode                    none
        nat-traversal                   none
        nat-interval                    30
        tcp-nat-interval                90
        registration-caching            disabled
        min-reg-expire                  300
        registration-interval           3600
        route-to-registrar              disabled
        secured-network                 disabled
        teluri-scheme                   disabled
        uri-fqdn-domain
        trust-mode                      all
        max-nat-interval                3600
        nat-int-increment               10
        nat-test-increment              30
        sip-dynamic-hnt                 disabled
        stop-recurse                    401,407
        port-map-start                  0
        port-map-end                    0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                 disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns   0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode            pass
        charging-function-address-mode  pass
        ccf-address
        ecf-address
        term-tgrp-mode                  none
        implicit-service-route          disabled
        rfc2833-payload                 101
        rfc2833-mode                    transparent
```

```
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                 disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                   none
        add-sdp-invite                  disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by                admin@console
        last-modified-date              2010-11-30 06:51:14
sip-manipulation
        name                            NAT_IP
        description
        header-rule
                name                            manipFrom
                header-name                     From
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods
                match-value
                new-value
                element-rule
                        name                            From
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP
        header-rule
                name                            manipTo
                header-name                     To
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods
                match-value
                new-value
                element-rule
                        name                            To
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $REMOTE_IP
        last-modified-by                admin@193.120.221.130
        last-modified-date              2010-11-25 10:16:05
steering-pool
        ip-address                      193.120.221.170
```

```
        start-port                      8000
        end-port                        20000
        realm-id                        OUTSIDE
        network-interface
        last-modified-by                admin@console
        last-modified-date              2010-11-15 13:16:13
steering-pool
        ip-address                      193.120.221.171
        start-port                      8000
        end-port                        20000
        realm-id                        INSIDE
        network-interface
        last-modified-by                admin@console
        last-modified-date              2010-11-15 13:16:50
system-config
        hostname                        netnet3800
        description                     NetNet
        location
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                    enabled
        enable-snmp-auth-traps          disabled
        enable-snmp-syslog-notify       disabled
        enable-snmp-monitor-traps       disabled
        enable-env-monitor-traps        disabled
        snmp-syslog-his-table-length    1
        snmp-syslog-level               WARNING
        system-log-level                WARNING
        process-log-level               NOTICE
        process-log-ip-address          0.0.0.0
        process-log-port                0
        collect
                sample-interval                 5
                push-interval                   15
                boot-state                      disabled
                start-time                      now
                end-time                        never
                red-collect-state               disabled
                red-max-trans                   1000
                red-sync-start-time             5000
                red-sync-comp-time              1000
                push-success-trap-state         disabled
        call-trace                      disabled
        internal-trace                  disabled
        log-filter                      all
        default-gateway                 193.120.221.129
        restart                         enabled
        exceptions
        telnet-timeout                  0
        console-timeout                 0
        remote-control                  enabled
        cli-audit-trail                 enabled
        link-redundancy-state           disabled
        source-routing                  disabled
        cli-more                        disabled
```

```
        terminal-height                 24
        debug-timeout                   0
        trap-event-lifetime             0
        default-v6-gateway              ::
        ipv6-support                    disabled
        last-modified-by                admin@console
        last-modified-date              2010-11-22 06:26:56
task done
amesystem#
```

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.