Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Aura™ Session Manager, Avaya Aura™ Communication Manager Access Element and Avaya Aura™ Communication Manager Feature Server with the SIP Trunking offerings from Opal Telecom - Issue 1.0

Abstract

These Application Notes describe the procedure to configure an Enterprise network made of Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager Access Element and Avaya Aura™ Communication Manager Feature Server to work with SIP Trunking products from Opal Telecom.

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, consisting of Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager Access Element and Avaya Aura™ Communication Manager Feature Server as SIP infrastructure, to access the SIP trunking solution provided by Opal Telecom (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 Opal Telecom that supports SIP-to-PSTN calls to reduce their long distance and interconnection costs.

To accomplish this, customers interconnect their Avaya SIP-enabled networks to a Service Provider's IP network via the Public Internet (or other forms of IP connectivity) and use SIP transport to establish calls to the PSTN. Calls from the customer site to the PSTN transit the Service Provider's network where a Session Board Controller (SBC) and SIP-to-PSTN gateway usually resides.

1.1. Interoperability Compliance Testing

The primary focus of testing is to verify SIP trunking interoperability between an Avaya SIP-based network and Opal Telecom'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 support
- Various PTSN dialing plans including national and international calling, toll-free, operator, directory assistance and direct inward dialed calling
- SIP transport using UDP and TCP

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 for Avaya Aura™ Communication Manager

Service Provider specific:

- Calls from/to PSTN
- Calls from/to Mobile users
- Calls from to other SIP trunks.

1.2. Support

Technical Support on Sip Trunk offering from Opal Telecom can be obtained through the following phone contacts:

- +44(0) 800 840 6778

2. Reference Configuration

As shown in **Figure 1**, the Avaya enterprise network uses SIP trunking for call signaling internally and with the SIP gateway provided by Opal Telecom. Session Manager using its SM-100 (Security Module) network interface, routes the calls between the different entities using SIP Trunks. All inter-system calls are carried over these SIP trunks. 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. Session Manager is managed by System Manager via the management network interface.

For security reasons all Service Provider IP Addresses have been removed.

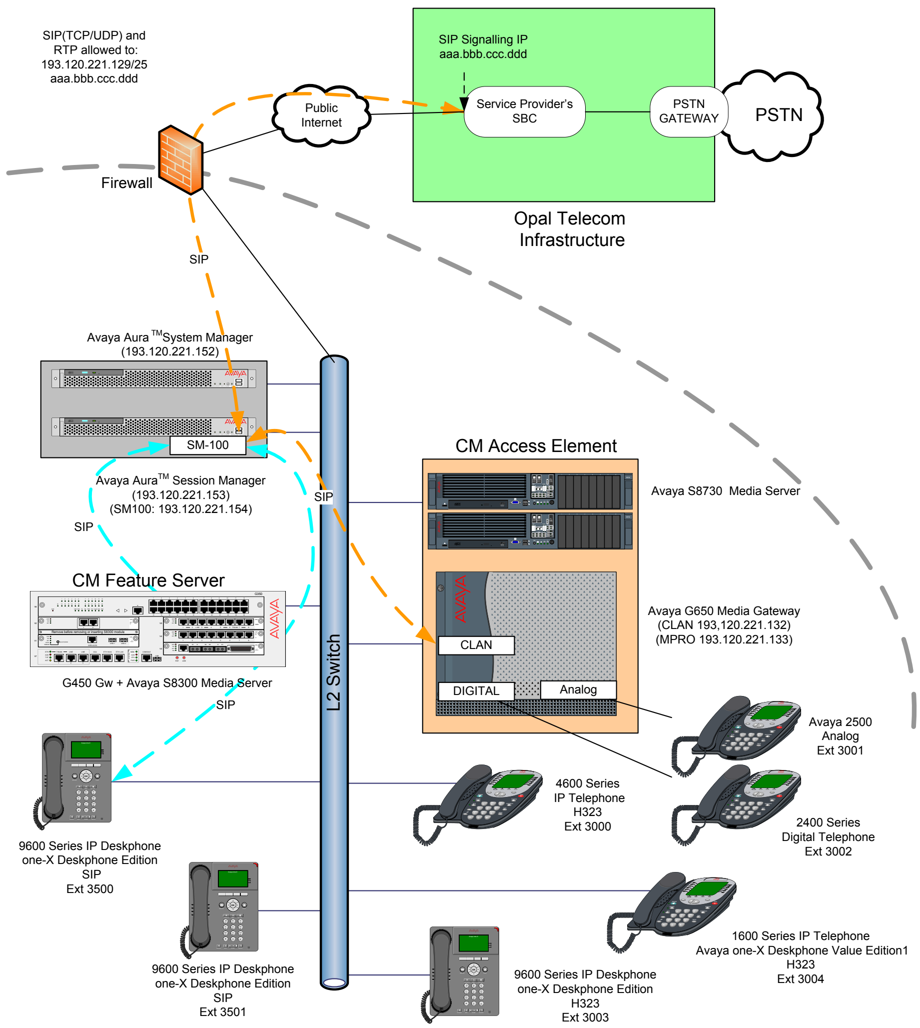


Figure 1 – Sample configuration for Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager with Sip Trunking

For the sample configuration shown in **Figure 1**, Session Manager runs on an Avaya S8510 Server, Communication Manager Access Element 5.2 runs on an Avaya S8730 Server with an Avaya G650 Media Gateway, and Communication Manager Feature Server 5.2 runs on an Avaya S8300D inside an Avaya G450 Media Gateway. For the Communication Manager Access Element, the results in these Application Notes are applicable to other 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**.

3. Equipment and Software Validated

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

Avaya Product / Hardware Platform	**Software Version**
Avaya Aura TM Session Manager on Avaya S8510 Server	Avaya Aura TM Session Manager 5.2.1.1.521012 – 5.2.1 SP1
Avaya Aura TM System Manager Template running on Avaya System Platform	Avaya Aura TM System Manager 5.2.1.0.521001 - 05_02_GA_01_Dec10
Avaya System Platform on Avaya S8510 Server	Version 1.1.1.0.2
Avaya Aura TM Communication Manager - Access Element – Avaya Media Server S8730	Avaya Aura TM Communication Manager R015x.02.1.016.4 – patch 17959
Avaya Aura TM Communication Manager – Feature Server – Avaya Media Server S8300C	Avaya Aura TM Communication Manager R015x.02.1.016.4 – patch 17959
Avaya Media Gateway G450	Firmware 30 .11 .3
Avaya G650 Media Gateway • IPSI (TN2312BP) • C-LAN (TN799DP) • IP Media Resource 320 (TN2602AP) • Analog (TN2793B) • Digital line (TN2214CP)	 • TN2312BP HW28 FW050 • TN799DP HW01 FW037 • TN2602AP HW08 FW053 • TN2793B 000005 • TN2214CP HW10 FW015
Avaya IP Telephones: • 9630 & 9620 (SIP) • 9620 (H323) • 1616 (H323) • 4621 (H323) Avaya Digital Telephones (2420) Avaya Analog (2500)	 • Avaya one-X TM Deskphone SIP 2.5.0 • Avaya one-X TM Deskphone S3.1 • Release 1.2.2 • Release R2.9 SP1 N/A N/A
Service Provider -Opal Telecom	
Product /Hardware Platform	**Software Version**
SBC: Sonus Networks Network Border Switch	n/a

4. Configure Avaya Aura™ Communication Manager Access Element

This section provides the procedures for configuring Communication Manager as Access Element. 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 AAR Analysis
- Administer ARS Analysis
- Save Translations

Throughout this section the administration of Communication Manager is performed using a System Access Terminal (SAT), the following commands are entered on the system with the appropriate administrative permissions. Some administration screens have been abbreviated for clarity. These instructions assume that the Communication Manager has been installed, configured, licensed and provisioned with a functional dial plan. Refer to the appropriate documentation as described in **Reference [9]** and **[10]** for more details**.** In these Application Notes, Communication Manager was configured with 4 digit extensions **30xx** for stations. The sip endpoints **35xx**, administrated by Session Manager, are reachable with **aar**. 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
     30            4    ext
     35            4    aar
     8             3    dac
     9             1    fac
```

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

4.1. 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.

4.2. Configure IP Node Names

As SIP interaction with Session Manager is carried through the security module SM100 interface, in configuring the SIP Trunk on Communication Manager it is necessary to refer to the SM100 IP address using a **node-name**. Use the **change node-names ip** command to add the **Name** and **IP Address** for the Session Manager. In the example, **SM100** and **193.120.221.154** were used.

```
change node-names ip                                         Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
Gateway001          193.120.221.129
SM100               193.120.221.154
clan                193.120.221.132
default             0.0.0.0
mpro                193.120.221.133
procr               0.0.0.0
```

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

4.3. Verify/List IP Interfaces

Use the **list ip-interface all** command and note the **C-LAN** 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  Gateway Node     Rgn VLAN
                            IP-Address
-- ------ ----- --------    ---------------  ----  ---------------  ---  ----
 y C-LAN  01A02 TN799  D     clan             /25   Gateway001       1    n
                             193.120.221.132
 y MEDPRO 01A03 TN2602       mpro             /25   Gateway001       1    n
                             193.120.221.133
```

4.4. Configure IP Codec Set

Use the **change ip-codec-set n** command where **n** is codec set used in the configuration. The Opal Telecom SIP trunking offering is based on G.711A. Configure the IP Codec Set as follows:

- **Audio Codec** Set **G.711A**

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.711A            n         2        20
 2:
 3:
```

4.5. 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 4.4**. 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
```

4.6. Administer SIP Trunks with Avaya Aura™ Session Manager

Two SIP trunks are needed for the configuration presented in these notes: one for calls with Service Provider and another one for calls within the Enterprise. To administer a SIP Trunk on Communication Manager, two intermediate steps are required; the creation of a signaling group and a trunk group.

4.6.1. Add SIP Signaling Group for Service Provider

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:** **tls**
- **Near-end Node Name:** C-LAN node name from **Section 4.2** (i.e., **clan**)
- **Far-end Node Name:** Session Manager node name from **Section 4.2** (i.e., **SM100**)
- **Near-end Listen Port:** **5061**
- **Far-end Listen Port:** **5061**
- **Far-end Domain:** The IP address of the SIP gateway with the Service Provider i.e**. aaa.bbb.ccc.ddd**
- **DTMF over IP:** **rtp-payload**
- **Direct IP-IP Audio Connection:** **y**

```
add signaling-group 2                                           Page   1 of   1
                                SIGNALING GROUP
Group Number: 2              Group Type: sip
                        Transport Method: tls
  IMS Enabled? n
     IP Video? n

   Near-end Node Name: clan                    Far-end Node Name: SM100
 Near-end Listen Port: 5061                  Far-end Listen Port: 5061
                                          Far-end Network Region: 1
Far-end Domain: aaa.bbb.ccc.ddd

                                         Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate              RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                  IP Audio Hairpinning? n
         Enable Layer 3 Test? n                  Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n        Alternate Route Timer(sec): 15
```

4.6.2. Configure a SIP Trunk Group for Service Provider

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**. To AuraSM**)
- **TAC:** An available trunk access code (i.e. **802**)
- **Service Type:** **tie**
- **Signaling Group:** Number of the signaling group added in **Section 4.6.1** (i.e. **2**)
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager (**must be within the limits of the total trunks available from licensed verified in **Section 4.1**)

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

```
add trunk-group 2                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip          CDR Reports: y
  Group Name: To AuraSM                   COR: 1       TN: 1      TAC: 802
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                               Signaling Group: 2
                                             Number of Members: 30
```

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

```
add trunk-group 2                                          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
```

4.6.3. Add SIP Signaling Group for Calls within the Enterprise

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:** **tls**
- **Near-end Node Name:** C-LAN node name from **Section 4.2** (i.e., **clan**).
- **Far-end Node Name:** Session Manager node name from **Section 4.2** (i.e., **SM100**).
- **Near-end Listen Port:** **5061**
- **Far-end Listen Port:** **5061**
- **Far-end Domain:** **avaya.com**
- **DTMF over IP:** **rtp-payload**
- **Direct IP-IP Audio Connections:** **y**

Submit these changes.

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

 Group Number: 3             Group Type: sip
                       Transport Method: tls
  IMS Enabled? n
     IP Video? n

   Near-end Node Name: clan                  Far-end Node Name: SM100
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
Far-end Domain: avaya.com

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

4.6.4. 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**. To AuraSM**)
- **TAC:** An available trunk access code (i.e. **803**)
- **Service Type:** **tie**
- **Signaling Group:** The number of the signaling for intra-enterprise calls (i.e. **3**)
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager (**must be within the limits of the total trunks available from licensed verified in **Section 4.1**)

```
add trunk-group 3                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 3                   Group Type: sip          CDR Reports: y
  Group Name: To AuraSM                  COR: 1       TN: 1       TAC: 803
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                             Signaling Group: 3
                                           Number of Members: 30
```

Navigate to **Page 3** and change **Numbering Format** to **public.** Use default values for all other fields.

```
add trunk-group 3                                             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
```

4.7. 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.

4.7.1. Route Pattern for Service Provider 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., **toSessionManager**)
- **Grp No:** The trunk group number from **Section 4.6.2**
- **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: toSessionManager
                             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: 2    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
```

4.7.2. 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., **toSessionManager**)
- **Grp No:** The trunk group number from **Section 4.6.4**
- **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: toSessionManager
                             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: 3    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
```

4.8. Configure Public Unknown Numbering

Use the **change public-unknown-numbering 0** command to assign the number presented by Communication Manager when call is leaving to Session Manager. Add an entry for the Extensions configured in the dialplan. Enter the following values for the specified fields, and retain default values for the remaining fields. Submit these changes.

- **Ext Len:** Number of digits of the Extension i.e. **4**
- **Ext. Code:** Digits beginning the Extension number, i.e. **30**
- **Trk Group:** Leave it blank (meaning any trunk)
- **CPN Prefix:** Leave it blank
- **Total CPN Len** Number of digits i.e. **4**

```
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: 1
 4  30                                      4           Maximum Entries: 9999
```

4.9. Administer AAR Analysis

This section provides sample Automatic Alternate Routing (AAR) used for routing calls with dialed digits **35xx** corresponding to SIP endpoint registered on Session Manager. Use the **change aar analysis 0** command and add an entry to specify how to route the calls to **35xx**. 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 **35**
- **Total Min:** Minimum number of digits, in this case **4**
- **Total Max:** Maximum number of digits, in this case **4**
- **Route Pattern:** The route pattern number from **Section 4.7.2** i.e. **3**
- **Call Type:** **aar**

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

       Dialed          Total     Route    Call   Node   ANI
       String        Min  Max  Pattern    Type   Num    Reqd

       35             4    4     3       aar
```

4.10. Administer ARS Analysis

This section provides sample Auto Route Selection (ARS) used for routing calls with dialed digits beginning with **0** corresponding to national numbers accessible via the Service Provider. 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 **0**
- **Total Min:** Minimum number of digits, in this case **3**
- **Total Max:** Maximum number of digits, in this case **24**
- **Route Pattern:** The route pattern number from **Section 4.7.2** i.e. **2**
- **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
             0            3    25     2         pubu         n
```

4.11. Save Translations

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

5. Configure Avaya Aura™ Communication Manager Feature Server

This section shows the configuration in Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). These Application Notes assumed that the basic configuration has already been administered. For further information on Communication Manager, please consult with **References [10]** and **[13].** The procedures include the following areas:

- Verify Avaya Aura™ Communication Manager License
- Administer System Parameters Features
- Administer IP Node Names
- Administer IP Network Region and Codec set
- Administer SIP Signaling Group and Trunk Group
- Administer Route Pattern
- Administer Private Numbering
- Administer Dial Plan and AAR analysis
- Administer ARS analysis
- Administer Feature Access Codes
- Save Changes

5.1. Verify Avaya Aura™ Communication Manager License

Use the **display system-parameter customer options** command to verify whether 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.

Note: The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

```
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: 450   0
             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   0
                       Maximum Administered SIP Trunks: 100   50
```

5.2. Administer System Parameters Features

Use the **change system-parameters features** command to allow for trunk-to-trunk transfers. This feature is needed to allow for transferring an incoming/outgoing call from/to a remote switch back out to the same or different switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to **all** to enable all trunk-to-trunk transfers on a system wide basis.

Note: This feature poses significant security risk and must be used with caution. As an alternative, the trunk-to-trunk feature can be implemented using Class Of Restriction or Class Of Service levels.

```
change system-parameters features                                Page   1 of  18
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
                             Music/Tone on Hold: none
              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n
```

5.3. Administer IP Node Names

Use the **change node-names ip** command to add an entry for Session Manager that will be used for connectivity. In the sample network, the processor Ethernet interface **procr** and **193.120.221.180** are entered as **Name** and **IP Address** for the signaling in Communication Manager running on the Avaya S8300 Server. In addition, **SM100** and **193.120.221.154** are entered for Session Manager.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address

default             0.0.0.0
procr               193.120.221.180
sm100               193.120.221.154
```

5.4. Administer IP Network Region and Codec Set

Use the **change ip-network-region n** command, where **n** is the network region number to configure the network region being used. In the sample network, ip-network-region 1 is used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise and a descriptive **Name** for this ip-network-region. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec Set** to **1** to use ip-codec-set 1.

```
change ip-network-region 1                                         Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Enterprise
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
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Use the **change ip-codec-set n** command where **n** is codec set used in the configuration. The Opal Telecom SIP trunking offering is based on G.711A. Configure the IP Codec Set as follows:

- **Audio Codec** Set **G.711A**

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.711A           n          2        20
 2:
 3:
```

Note: G.711A is the only codec supported for the current SIP Trunking offering from Opal Telecom.

5.5. Administer SIP Trunks with Avaya Aura^{TM} Session Manager

In the test configuration, since Communication Manager acts as a Feature Server in this case, trunks with Session Manager must be IMS enabled. Two SIP trunks are needed for the configuration presented in these notes: one for calls with Service Provider and another one for calls within the Enterprise. To administer a SIP Trunk on Communication Manager, two intermediate steps are required; the creation of a signaling group and a trunk group.

5.5.1. Add SIP Signaling Group for Calls within the Enterprise

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:** **tls**
- **IMS Enabled:** **y**
- **Near-end Node Name:** **procr**
- **Far-end Node Name:** Session Manager node name from **Section 5.3** (i.e. **sm100**)
- **Near-end Listen Port:** **5061**
- **Far-end Listen Port:** **5061**
- **Far-end Domain:** **avaya.com**
- **DTMF over IP:** **rtp-payload**
- **Direct IP-IP Audio Connections:** **y**

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

 Group Number: 1             Group Type: sip
                       Transport Method: tls
  IMS Enabled? y
     IP Video? n


   Near-end Node Name: procr                 Far-end Node Name: sm100
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
Far-end Domain: avaya.com

                                           Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload          Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                   IP Audio Hairpinning? n
         Enable Layer 3 Test? n                   Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n       Alternate Route Timer(sec): 30
```

5.5.2. 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**. with-SessionManager**)
- **TAC:** An available trunk access code (i.e. **101**)
- **Service Type:** **tie**
- **Signaling Group:** The number of the signaling group associated (i.e. **1**)
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager (**must be within the limits of the total trunks available from licensed verified in **Section 5.1**)

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

Group Number: 1                  Group Type: sip          CDR Reports: y
  Group Name: with-SessionManager       COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                       Signaling Group: 1
                                                     Number of Members: 20
```

Navigate to **Page 3** and change **Numbering Format** to **private.** Use default values for all other fields.

```
add trunk-group 1                                             Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y
                     Numbering Format: private
                                              UUI Treatment: service-provider
                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n
```

5.5.3. Add SIP Signaling Group for Service Provider

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:** **tls**
- **IMS Enabled:** **y**
- **Near-end Node Name:** **procr**
- **Far-end Node Name:** Session Manager node name from **Section 5.3** (i.**e** **sm100**)
- **Near-end Listen Port:** **5061**
- **Far-end Listen Port:** **5061**
- **Far-end Domain:** The IP address of the SIP gateway with the Service Provider i.e. **aaa.bbb.ccc.ddd**
- **DTMF over IP:** **rtp-payload**
- **Direct IP-IP Audio Connection:** **y**

```
add signaling-group 2                                          Page   1 of   1
                               SIGNALING GROUP

 Group Number: 2             Group Type: sip
                       Transport Method: tls
  IMS Enabled? y
     IP Video? n


   Near-end Node Name: procr                    Far-end Node Name: sm100
 Near-end Listen Port: 5061                   Far-end Listen Port: 5061
                                           Far-end Network Region: 1
Far-end Domain: aaa.bbb.ccc.ddd

                                          Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate               RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload          Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                  IP Audio Hairpinning? n
         Enable Layer 3 Test? n                   Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n       Alternate Route Timer(sec): 30
```

5.5.4. Configure a SIP Trunk Group for Service Provider

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**. OUTSIDE CALL**)
- **TAC:** An available trunk access code (i.e. **102**)
- **Service Type:** **tie**
- **Signaling Group:** The number of the signaling group associated (i.e. **2**)
- **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 2                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip          CDR Reports: y
  Group Name: OUTSIDE CALL                  COR: 1       TN: 1      TAC: 102
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                      Auth Code? n

                                              Signaling Group: 2
                                             Number of Members: 30
```

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

```
add trunk-group 2                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                 Maintenance Tests? y

                     Numbering Format: private
                                              UUI Treatment: service-provider

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

5.6. Configure Route Patterns

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

5.6.1. 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. **toSessionManager**)
- **Grp No:** The trunk group number from **Section 5.5.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: toSessionManager
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
    No          Mrk Lmt List Del  Digits                            QSIG
                             Dgts                                   Intw
 1: 1    0                                                          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
```

5.6.2. Route Pattern for Service Provider 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. **toGW**)
- **Grp No:** The trunk group number from **Section 5.5.4**
- **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: toGW
                             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: 2    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. Administer Private Numbering

Use the **change private-numbering** command to define the calling party number to be sent out through the SIP trunk. In the sample network configuration below, all calls originating from a **4**-digit extension (**Ext Len**) beginning with **35** (**Ext Code**) will result in a **4**-digit calling number (**Total Len**). The calling party number will be in the SIP "From" header.

```
change private-numbering 0
                           NUMBERING - PRIVATE FORMAT

Ext Ext             Trk        Private          Total
Len Code            Grp(s)     Prefix           Len
 4  35                                          4     Total Administered: 1
                                                         Maximum Entries: 540
```

5.8. Administer Dial Plan and AAR analysis

Configure the dial plan for dialing 4-digit extensions beginning with **30** from stations registered with Communication Manager Access Element . Use the **change dialplan analysis** command to define **Dialed String 30** as an **aar Call Type**.

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                  Location:  all          Percent Full:    2

       Dialed    Total  Call     Dialed    Total  Call      Dialed    Total  Call
       String    Length Type     String    Length Type      String    Length Type
     1             3    dac
     30            4    aar
     35            4    ext
     9             1    fac
     *             1    fac
```

Use the **change aar analysis n** command where **n** is the dial string pattern to configure an **aar** entry for **Dialed String 30** (Extensions on Communication Manager Access Element**)** to use **Route Pattern 1** (defined in **Section 5.6.1**).

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

          Dialed           Total     Route     Call    Node   ANI
          String         Min  Max   Pattern    Type    Num    Reqd
    30                   4    4      1         aar            n
    35                   4    4      1         aar            n
```

5.9. Administer ARS Analysis

This section provides sample Auto Route Selection (ARS) used for routing calls with dialed digits beginning with **0** corresponding to national numbers accessible via the Service Provider. 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 **0**
- **Total Min:** Minimum number of digits, in this case **3**
- **Total Max:** Maximum number of digits, in this case **24**
- **Route Pattern:** The route pattern number from **Section 5.6.2** i.e. **2**
- **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
    0                      3    25     2         pubu          n
```

5.10. Administer Feature Access Code

Configure a feature access code to use for AAR routing. Use the **change feature access code** command to define an **Auto Alternate Routing (AAR) Access Code** and for **Auto Route Selection (ARS).** In these notes, **9** and ***** were used.

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

5.11. Save Changes

Use the **save translation** command to save all changes.

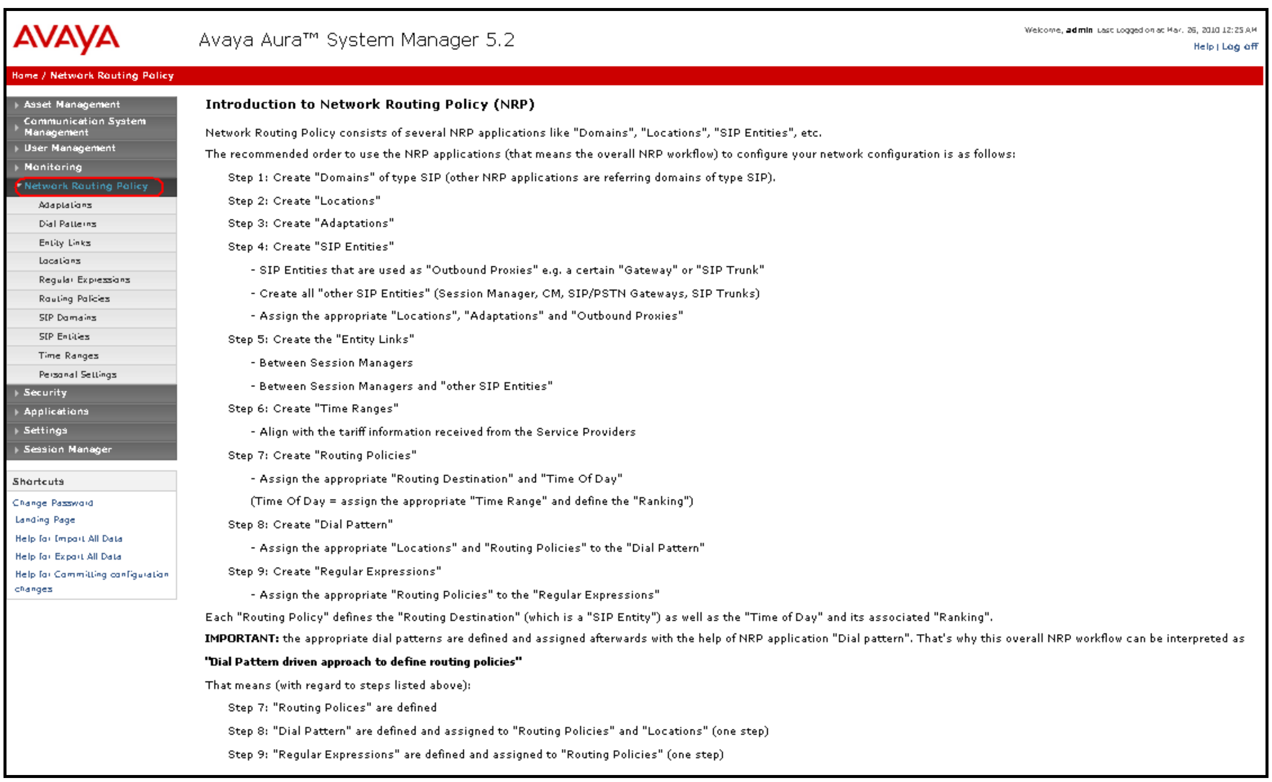
```
save translation

                              SAVE TRANSLATION

          Command Completion Status                              Error Code

          Success                                                  0
```

6. Configure Avaya Aura^{TM} 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
- Add Communication Manager as Feature Server
- Add Users for Sip Phones

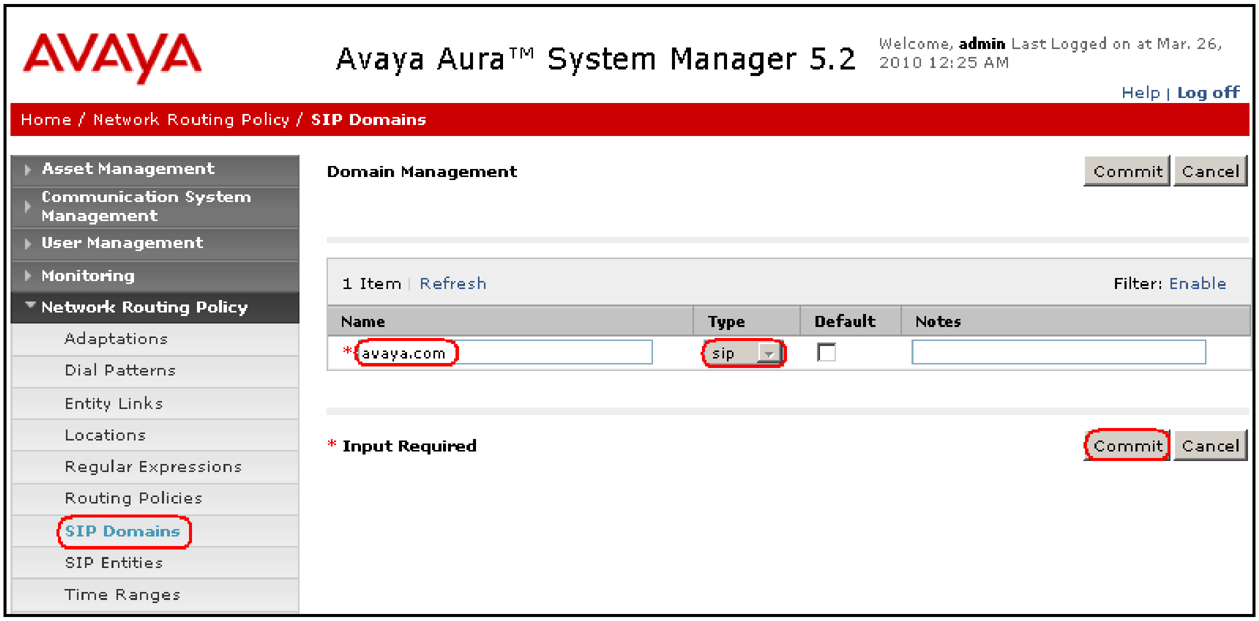
Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials and accept the Copyright Notice. The menu shown below is displayed. Expand the **Network Routing Policy** 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 **SIP 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 Access Element, Feature Server and Service Provider SIP gateway. To add a location, select **Locations** on the left and click on the **New** button on the right. The following screen will then be shown. Fill in the following:

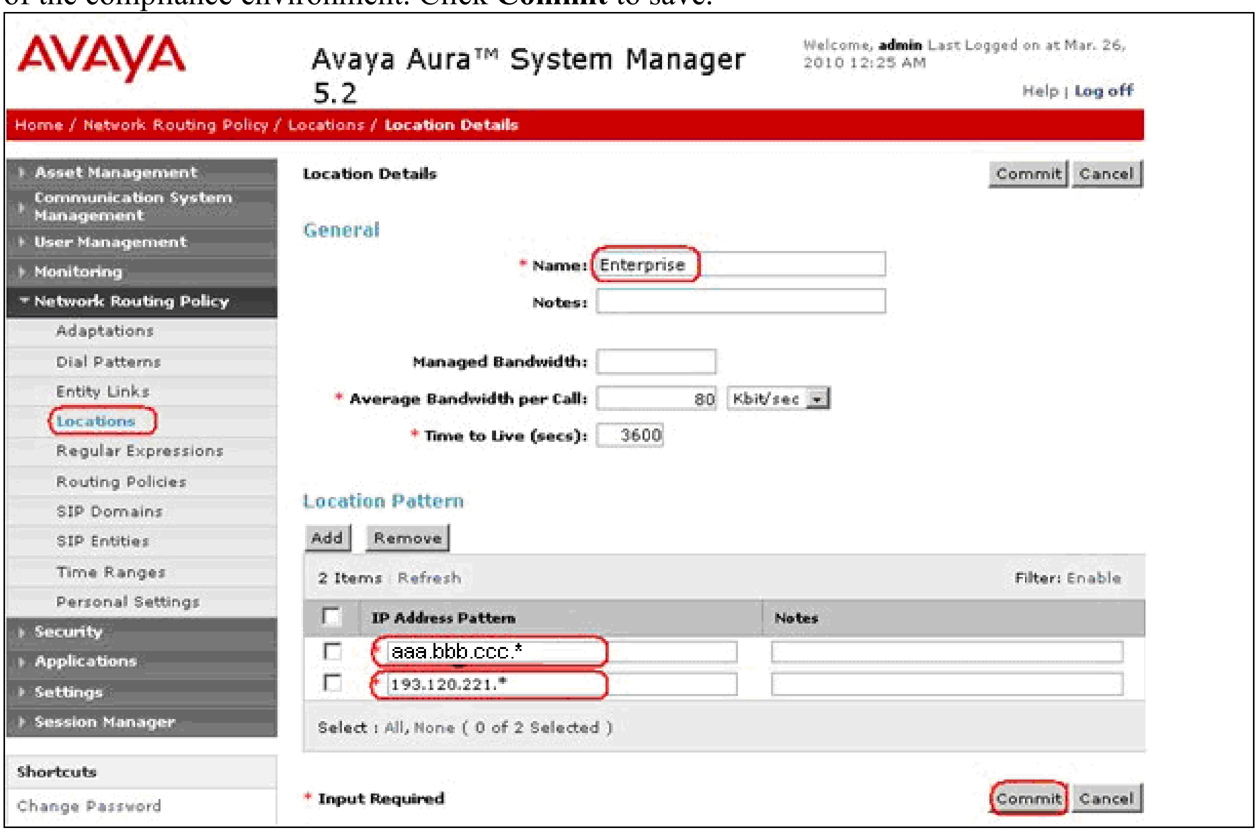
Under **General**:

- **Name:** A descriptive name
- **Notes:** Descriptive text (optional)
- **Managed Bandwidth:** Leave the default or customize as described in **[5]**

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 and **aaa.bbb.ccc.*** for the SIP Trunking gateway offered by the Service Provider. 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 a numbering plan offered from the Service Provider. To add an adaptation, under the **Network Routing Policy,** select **Adaptations** on the left and click on the **New** button on the right. The following screen will then be shown. Fill in the following:

Under **General**:

- **Name:** A descriptive name i.e: **DigitConversionAdapter**
- **Module Name:** From the dropdown list select **DigitConversionAdapter**
- **Module Parameter:** Enter **odstd=<GW address>** where GW address is the IP address of the SIP gateway within the Opal, i.e. **aaa.bbb.ccc.ddd**

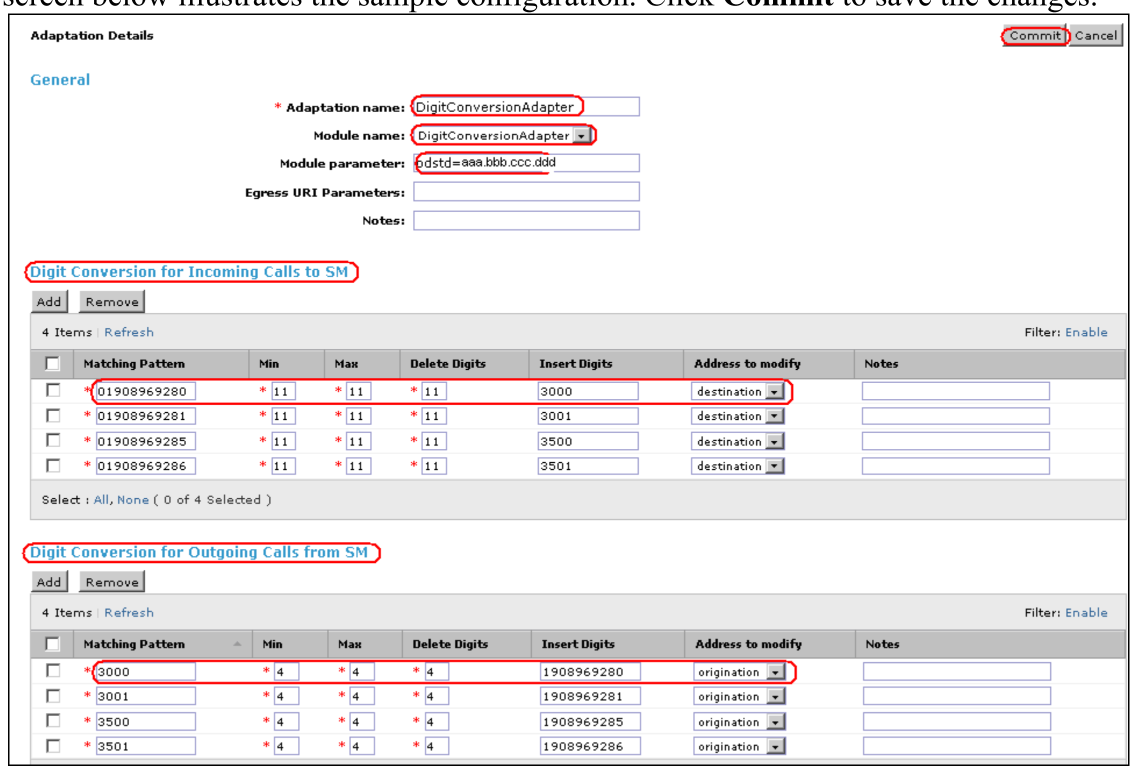
Under **Digit Conversion for Incoming Calls to SM**:

- **Matching Pattern**: The dialed number from the PSTN i.e. 01908969280
- **Min/Max**: Minimum/Maximum number of digits
- **Delete**: Digits to be deleted i.e. 11
- **Insert Digits**: Digit to be added i.e. 3000
- **Address to modify**: Select **destination**

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

- **Matching Pattern**: The dialed number from enterprise network i.e. 3000
- **Min:/ Max**: Minimum/ Maximum number of digits i.e. 4
- **Delete**: Digits to be deleted i.e. 4
- **Insert Digits**: Digit to be added i.e. 1908969280
- **Address to modify**: Select **origination**

The screen below illustrates the sample configuration. Click **Commit** 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 C-LAN board in the Avaya G650 Media Gateway for the Communication Manager Access Element, the Proc interface for the Communication Manager Feature Server and the SIP Trunking gateway on the Service Provider.

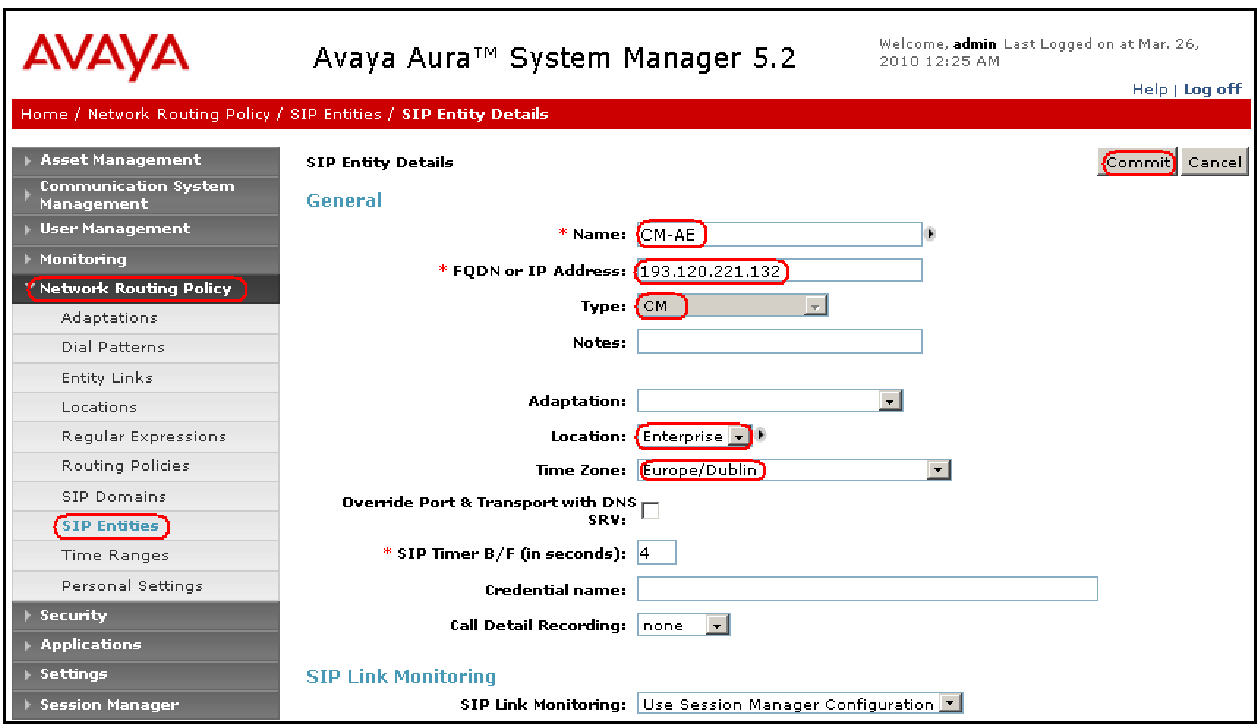
6.4.1. Adding Avaya Aura™ Communication Manager Access Element SIP Entity

To add a SIP Entity, navigate **Network Routing Policy → SIP Entities** on the left and click on the **New** button on the right.

Under **General**:

- **Name:** A descriptive name (i.e. **CM-AE**)
- **FQDN or IP Address:** IP address of the signaling interface of CLAN board in the G650 Media gateway, i.e. **193.120.221.132**
- **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 Access Element.



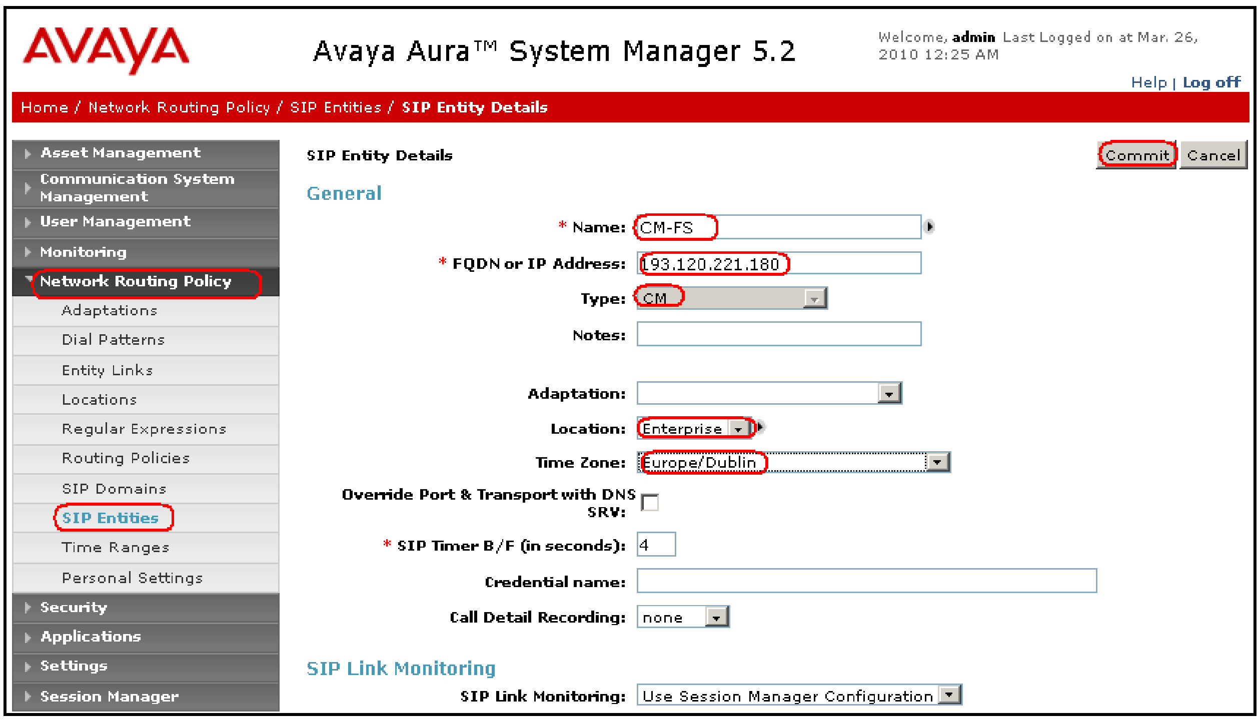
6.4.2. Adding Avaya Aura™ Communication Manager Feature Server SIP Entity

To add a SIP Entity, navigate **Network Routing Policy → SIP Entities** on the left and click on the **New** button on the right.

Under **General**:

- **Name:** A descriptive name (i.e. **CM-FS)**
- **FQDN or IP Address:** IP address of the Proc interface of S8300 Server, i.e. **193.120.221.180**
- **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 Feature Server.



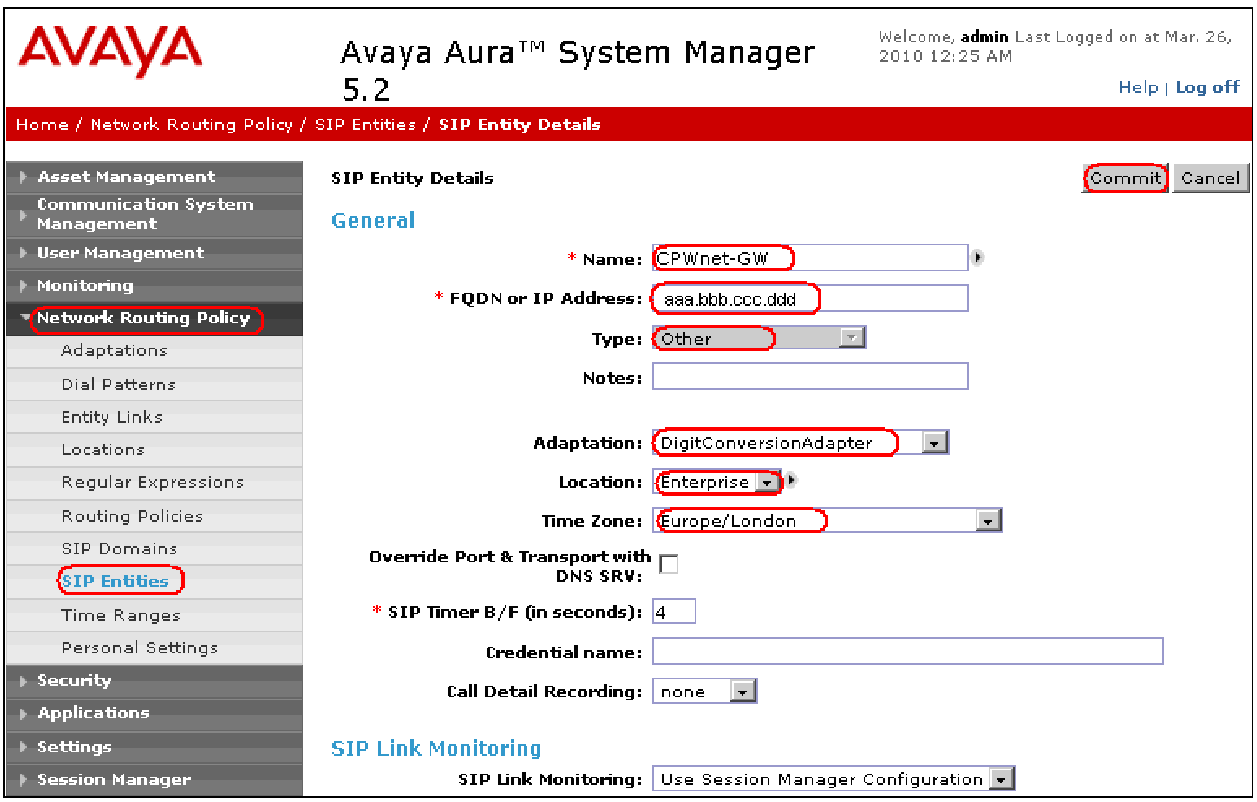
6.4.3. Adding Opal Telecom Gateway SIP Entity

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

Under **General**:

- **Name:** A descriptive name (i.e. **CPWnet-GW**)
- **FQDN or IP Address:** IP address of the signaling interface provided by the Service Provider, i.e. **aaa.bbb.ccc.ddd**
- **Type:** Select **Other**
- **Adaptation:** Select the adaptation created in **Section 6.3** i.e. **DigitConversionAdapter**
- **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 related to Opal Telecom SIP Gateway.



6.4.4. Adding Avaya Aura™ Session Manager SIP Entity

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

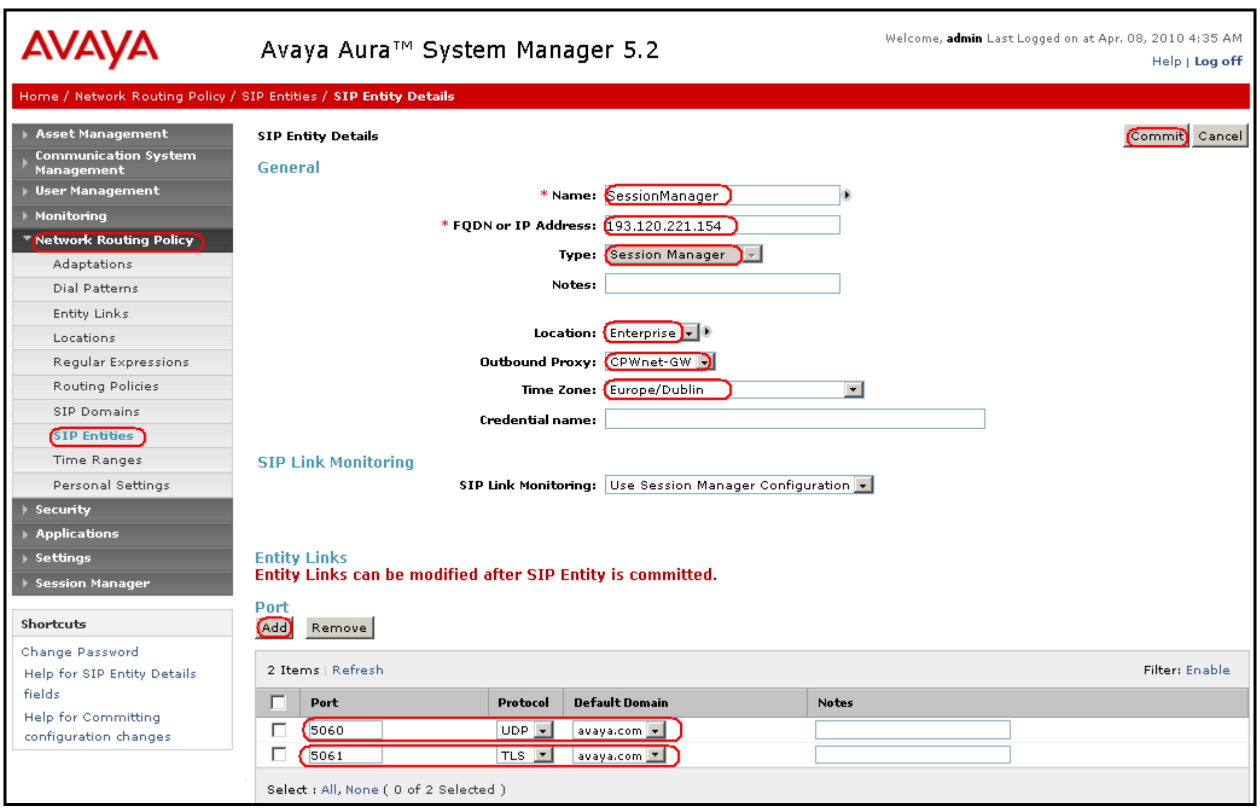
Under **General**:

- **Name:** A descriptive name, i.e. **SessionManager**
- **FQDN or IP Address:** IP address of the Session Manager i.e. **193.120.221.154**, the SM-100 Security Module
- **Type:** Select **Session Manager**
- **Location:** Select one of the locations defined previously
- **Outbound Proxy:** Select the SIP Entity defined previously as Opal Telecom SIP gateway, i.e. **CPWnet-GW**
- **Time Zone:** Time zone for this entity

Create two Port definitions, one for **TLS** and one for **UDP**. 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.

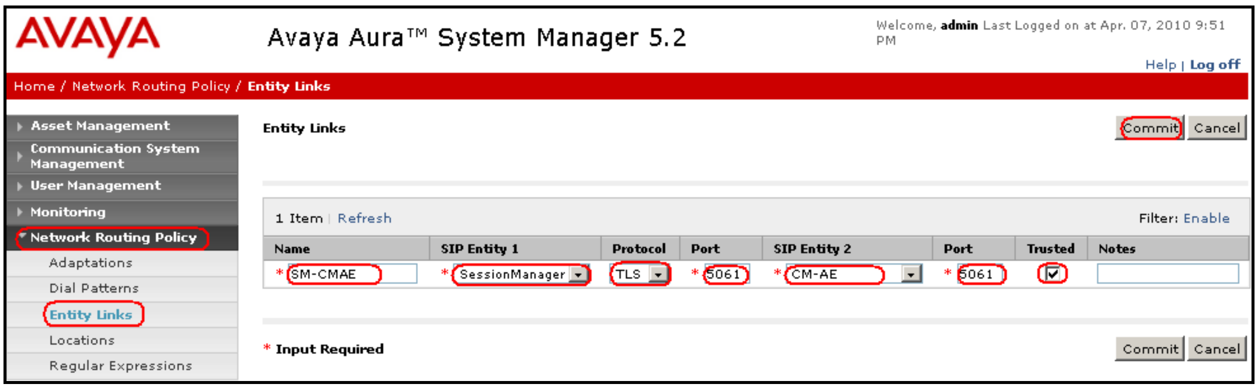


6.5. Add Entity Links

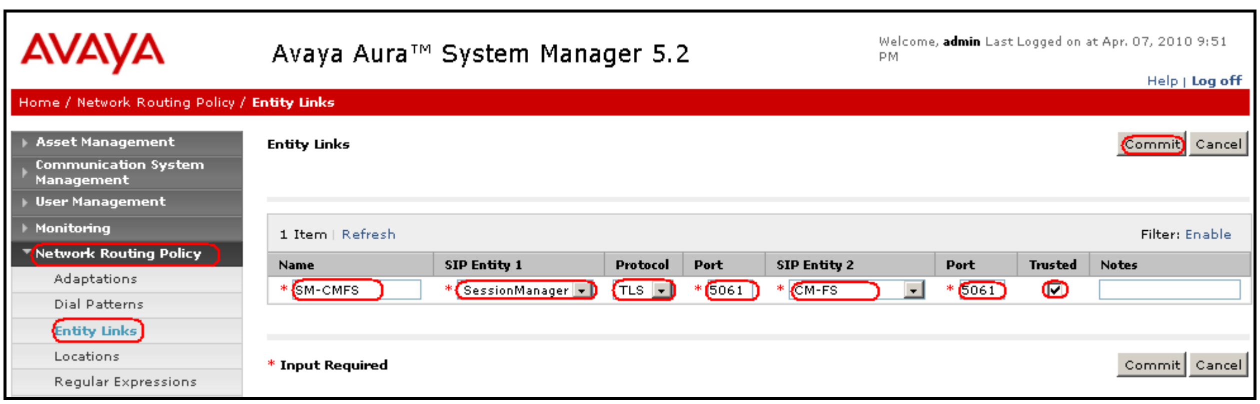
A SIP trunk between Session Manager and a telephony system is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button on the right. Fill in the following fields in the new row that is displayed:

- **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 **TLS** was used for **Communication Manager Access Element** and **Feature Server** while **UDP** for **Opal Telecom SIP Trunk Gateway**

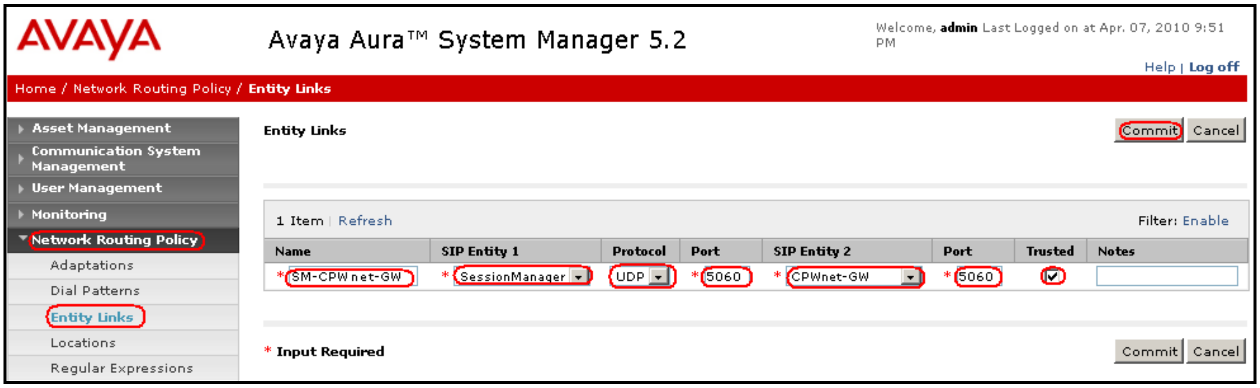
Click **Commit** to save each Entity Link definition**.** The following screen illustrates adding the Entity Link for Communication Manager Access Element.



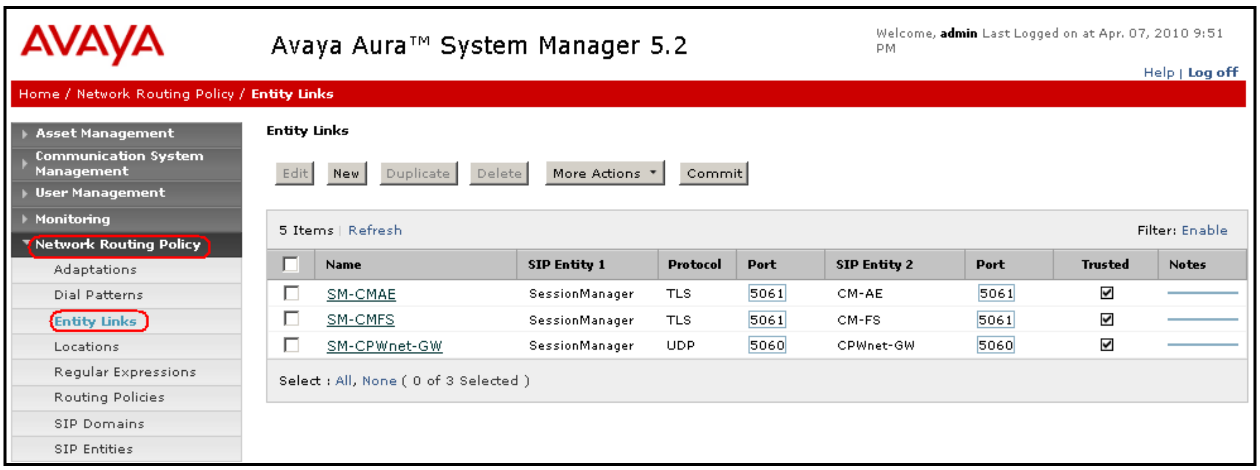
The screen below illustrates adding the Entity Link for Communication Manager Feature Server.



The screen below illustrates adding the Entity Link for Opal Session Border Controller.



The screen below summarizes the Entity Links view after the insertion of the three Entity Links.



6.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies must be added: one for Communication Manager Access Element and one for the Service Provider Gateway. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under **General:**

- Enter a descriptive name in **Name**

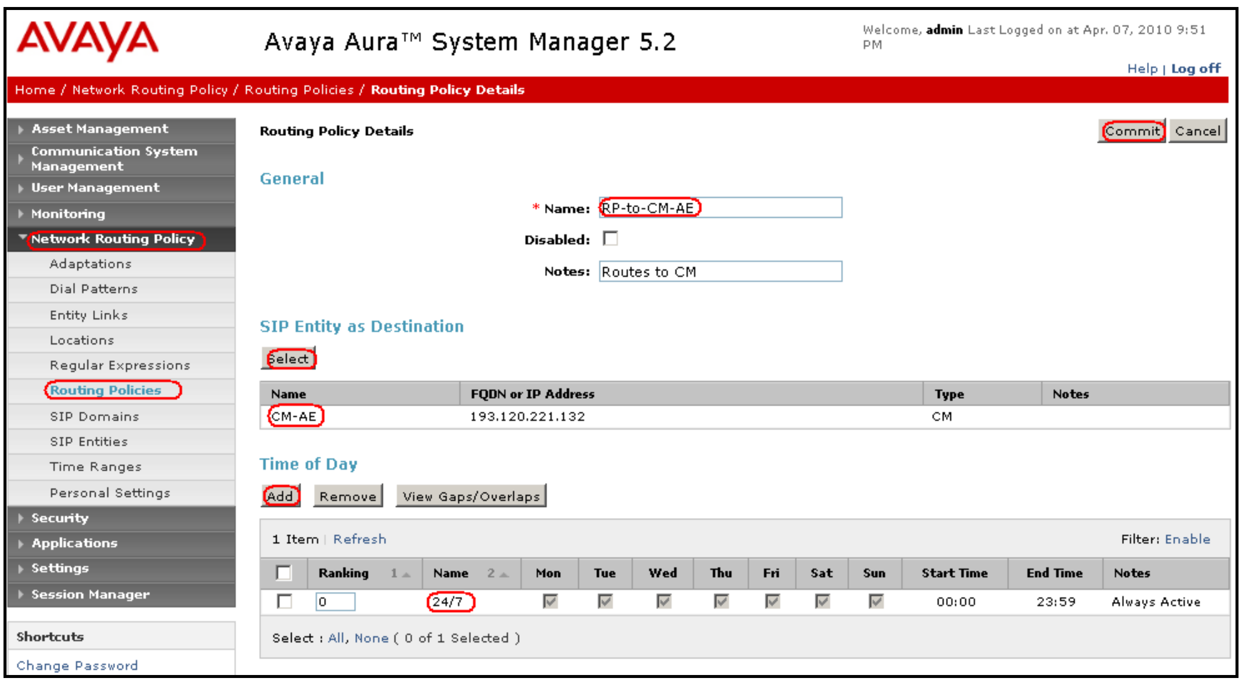
Under **SIP Entity as Destination:**

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

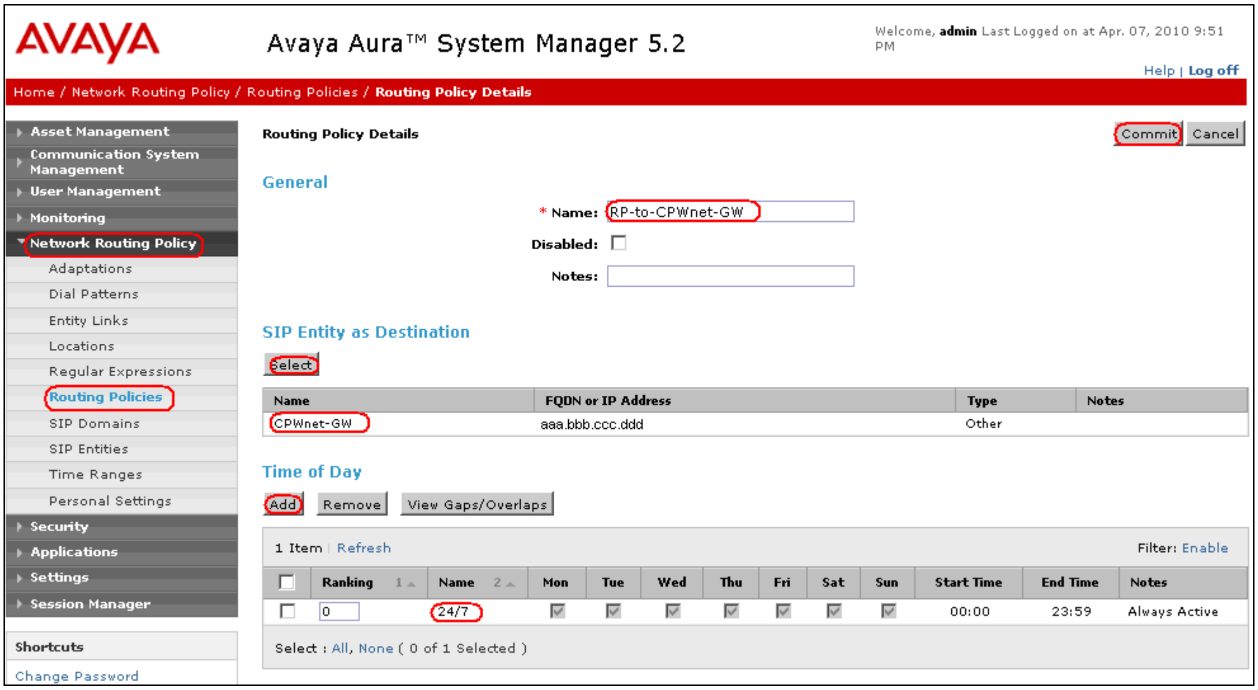
Under **Time of Day:**

- 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 picture shows the Routing Policy for Communication Manager Access Element.



The following picture shows the Routing Policy for Opal Telecom Gateway.



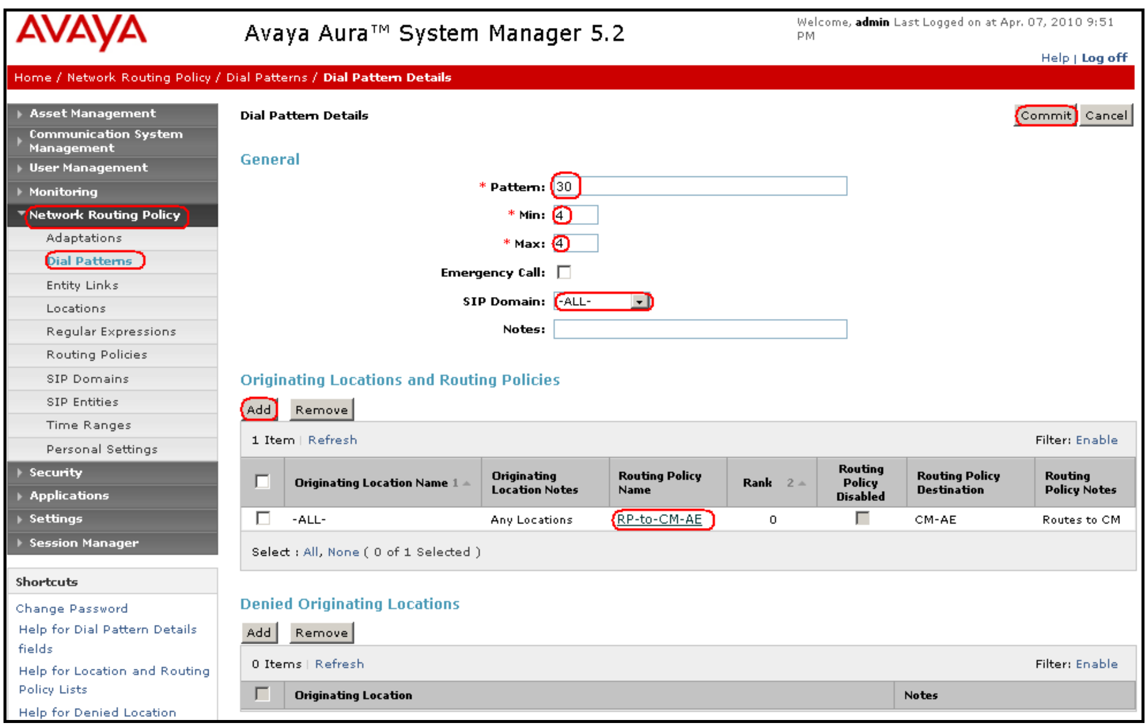
6.7. Add Dial Patterns

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 Access Element,and numbers beginning with **0** with 3 to 24 digits are accessible trough Opal Telecom Gateway. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right. Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Communication Manager Access Element:

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 **ALL**

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 Access Element.

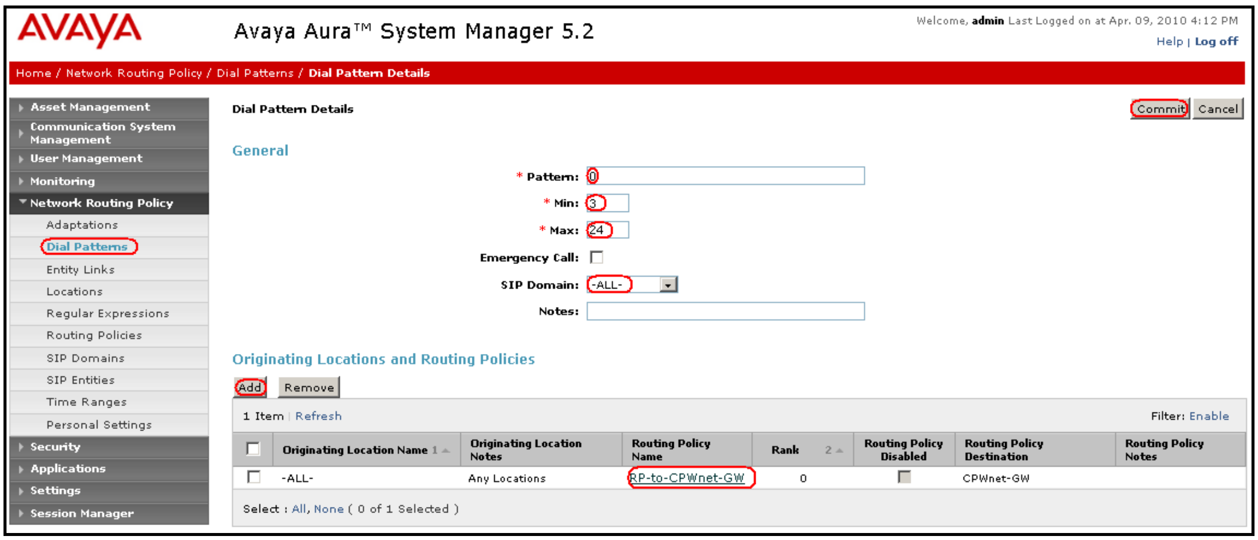


Repeat the process adding one or more dial patterns for the trunking services offered by the Service Provider. Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Opal Telecom gateway:

Under **General**:

- **Pattern:** Dialed number or prefix i.e. **0**
- **Min:** Minimum length of dialed number i.e. **3**
- **Max:** Maximum length of dialed number i.e. **24**
- **SIP Domain:** Select **ALL**

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 Opal Telecom SIP service.



6.8. Add Avaya Aura™ Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add**, and fill in the fields as described below and shown in the following screen:

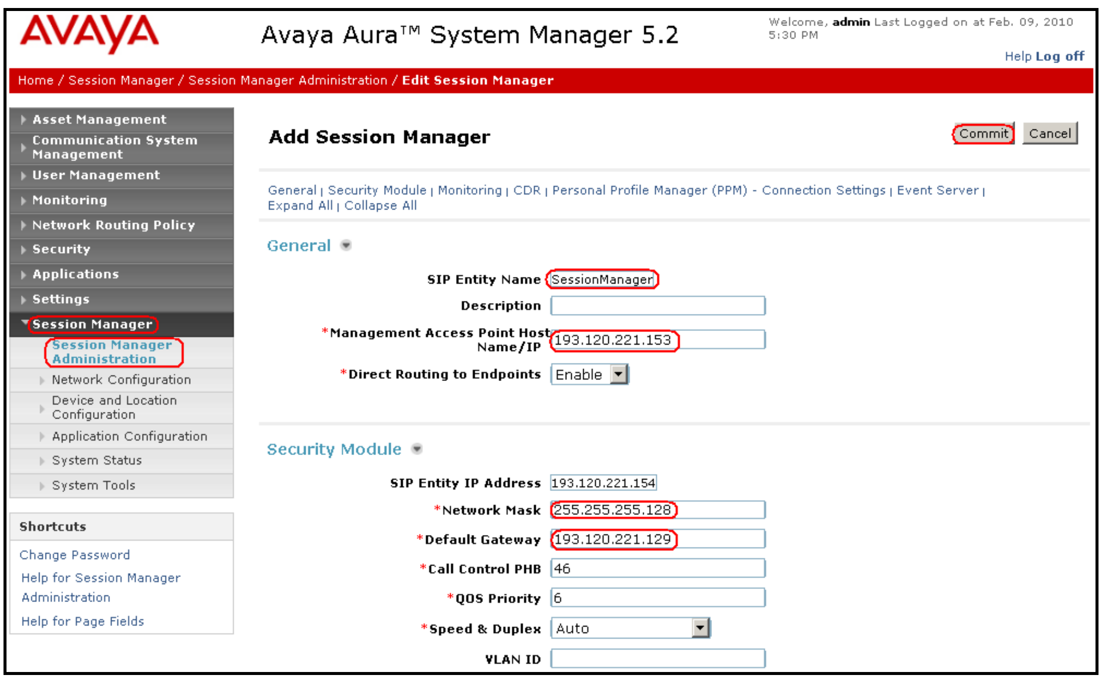
Under **General**:

- **SIP Entity Name**: Select the name of the SIP Entity added for Session Manager
- **Description**: Descriptive comment (optional)
- **Management Access Point Host Name/IP**: Enter the IP address of the Session Manager management interface

Under **Security Module**:

- **Network Mask**: Enter the network mask corresponding to the IP address of the SM100 interface (i.e., **255.255.255.128**)
- **Default Gateway**: Enter the IP address of the default gateway for SM100 interface (i.e., **193.120.221.129**)

Use default values for the remaining fields. Click **Save** to add this Session Manager.



6.9. Add Avaya Aura™ Communication Manager as a Feature Server

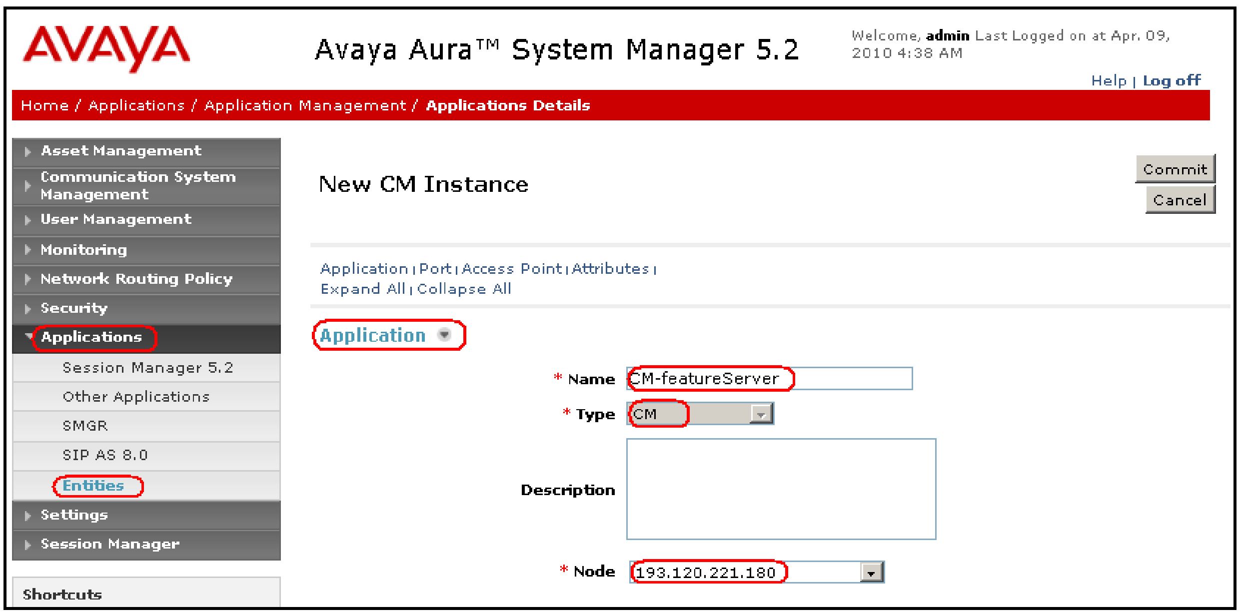
In order for Communication Manager to provide configuration and Feature Server support to SIP phones when they register to Session Manager, Communication Manager must be added as an application.

6.9.1. Create an Application Entry

Expand **Application** menu, select **Entities** on left, click on **New** (not shown). Enter the following fields and retain defaults for the remaining fields.

Under **Application**:

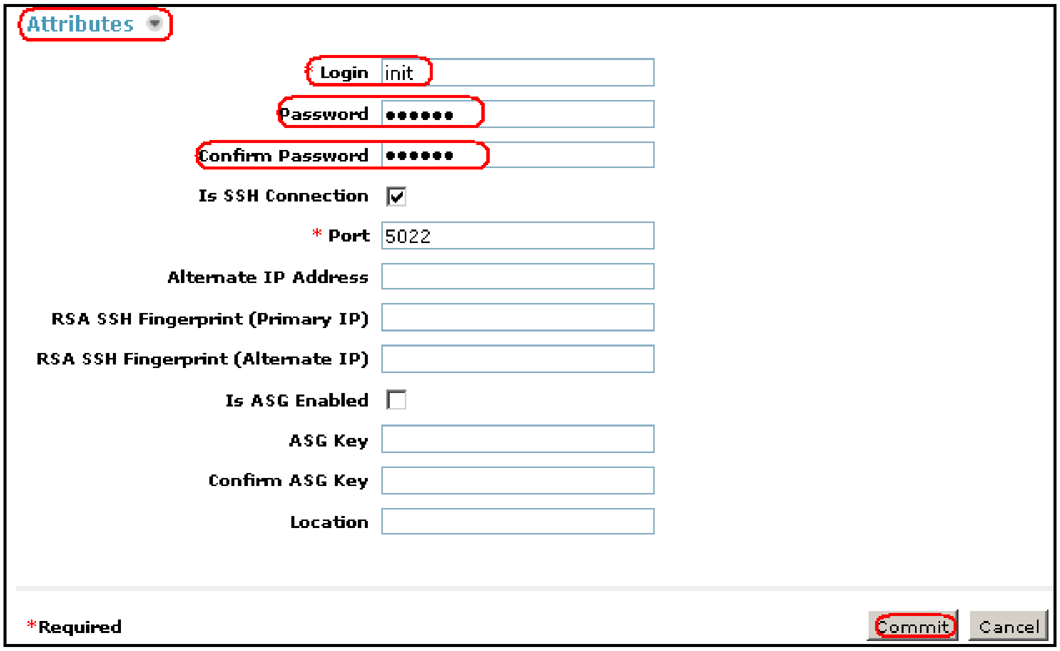
- **Name**: Enter a descriptive name i.e. **CM-featureServer**
- **Type**: Select **CM**
- **Node**: Select **Other..** and enter the IP address for CM SAT access i.e. **193.120.221.180**



Navigate to the **Attributes** section and enter the following:

- **Login**: Login used for SAT access
- **Password**: Password used for SAT access
- **Confirm Password**: Password used for SAT access

Retain default values for the remaining fields. Click **Commit** to save.

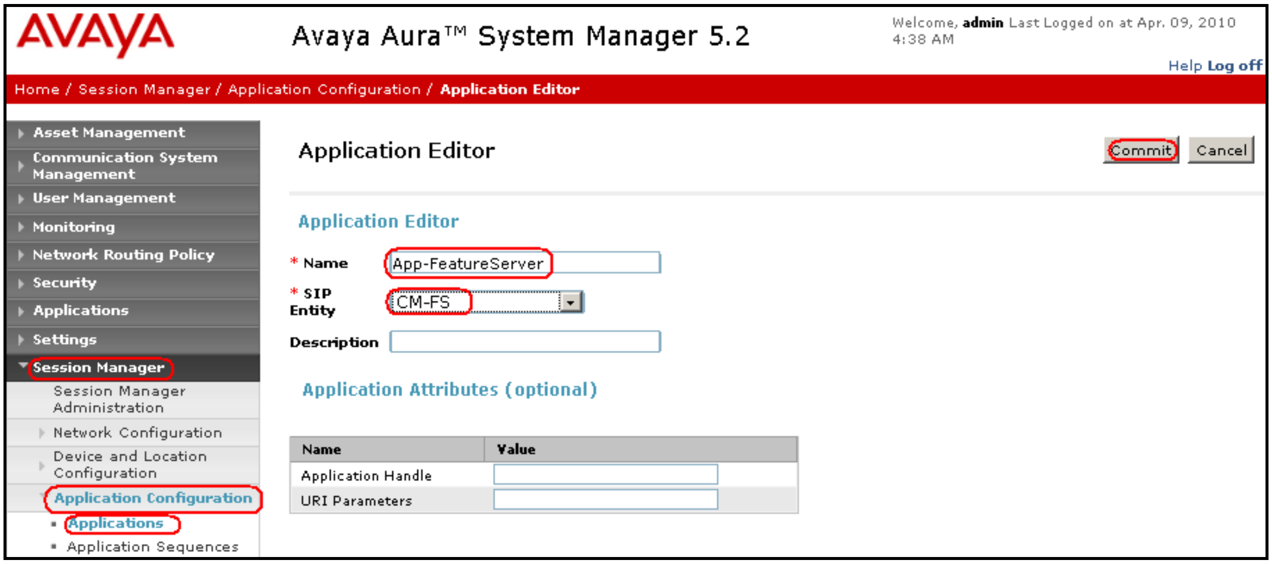


6.9.2. Create a Feature Server Application

Navigate to **Session Manager → Application Configuration → Applications** on the left menu. Click on **New** (not shown). Enter following fields and use defaults for the remaining fields:

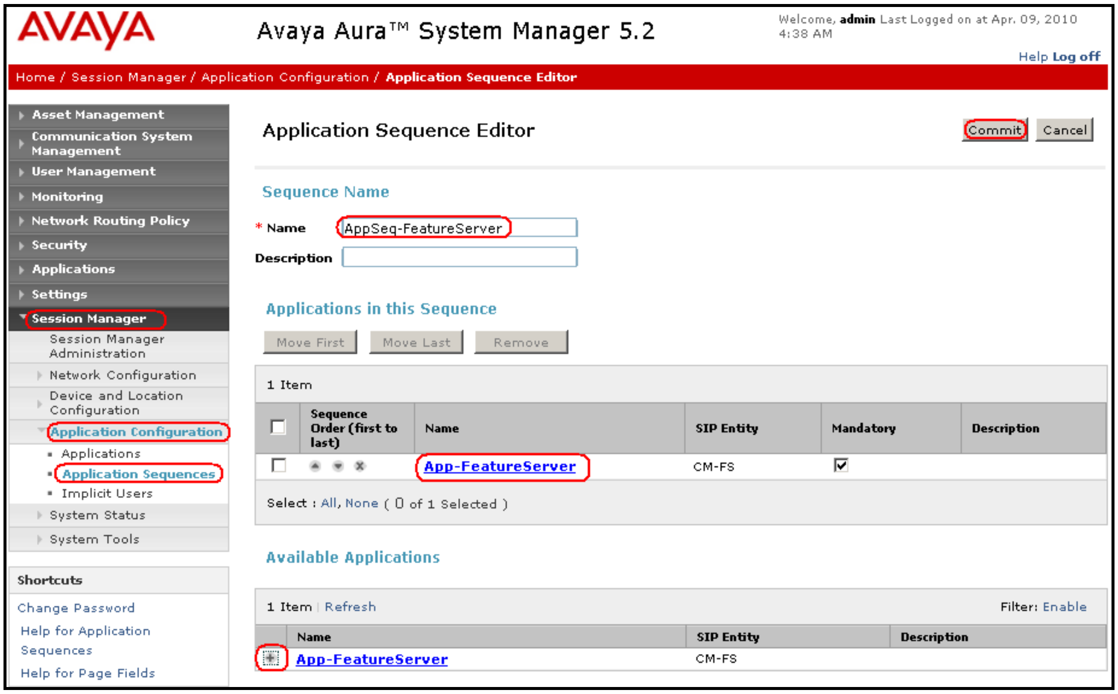
- **Name** A descriptive name
- **SIP Entity** Select the CM SIP Entity defined in **Section 6.4.2**

Click on **Commit** to save.



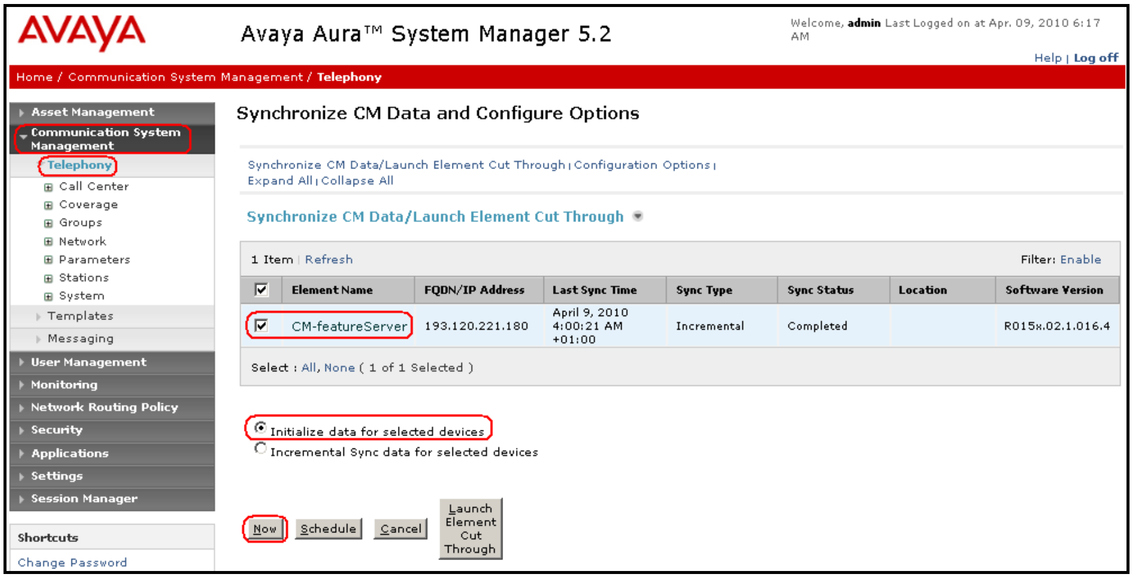
6.9.3. Create a Feature Server Application Sequence

From the left menu, navigate to **Application Sequences** under **Session Manager → Application Configuration**. Click on **New** (not shown). Enter a descriptive **Name**. Click on the + sign next to the appropriate **Available Applications** and they will move up to the **Applications in this Sequence** section. Click on **Commit** to save.



6.9.4. Synchronize Avaya Aura™ Communication Manager Data

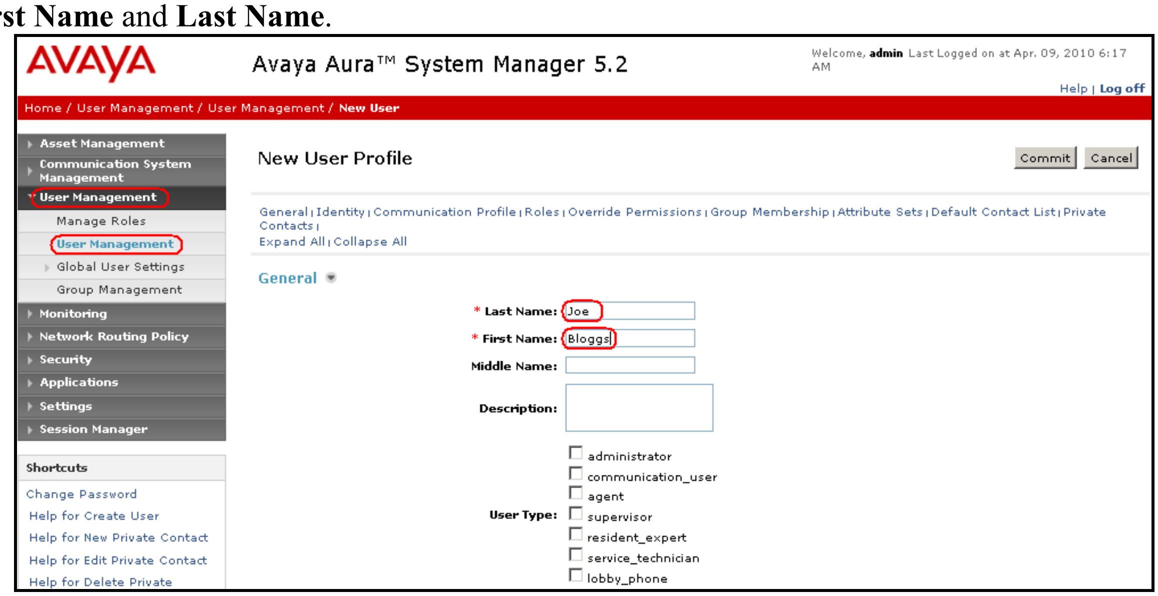
Select **Communications System Management → Telephony** on the left. Select the appropriate **Element Name**. Select **Initialize data for selected devices**. Then click on **Now**. This may take some time.



Use the menus on the left under **Monitoring → Scheduler** to determine when the task is complete.

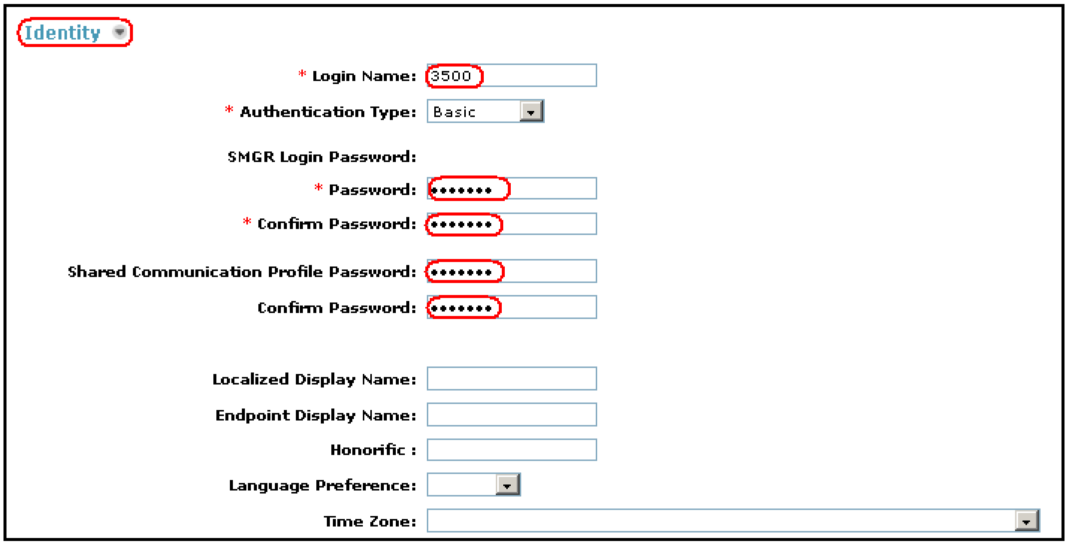
6.10. Add Users for SIP Phones

Users must be added via Session Manager and the details will be updated on the CM. Select **User Management → User Management** on the left. Then click on **New** (not shown). Enter a **First Name** and **Last Name**.



Navigate to the **Identity** section and enter the following and use defaults for other fields:

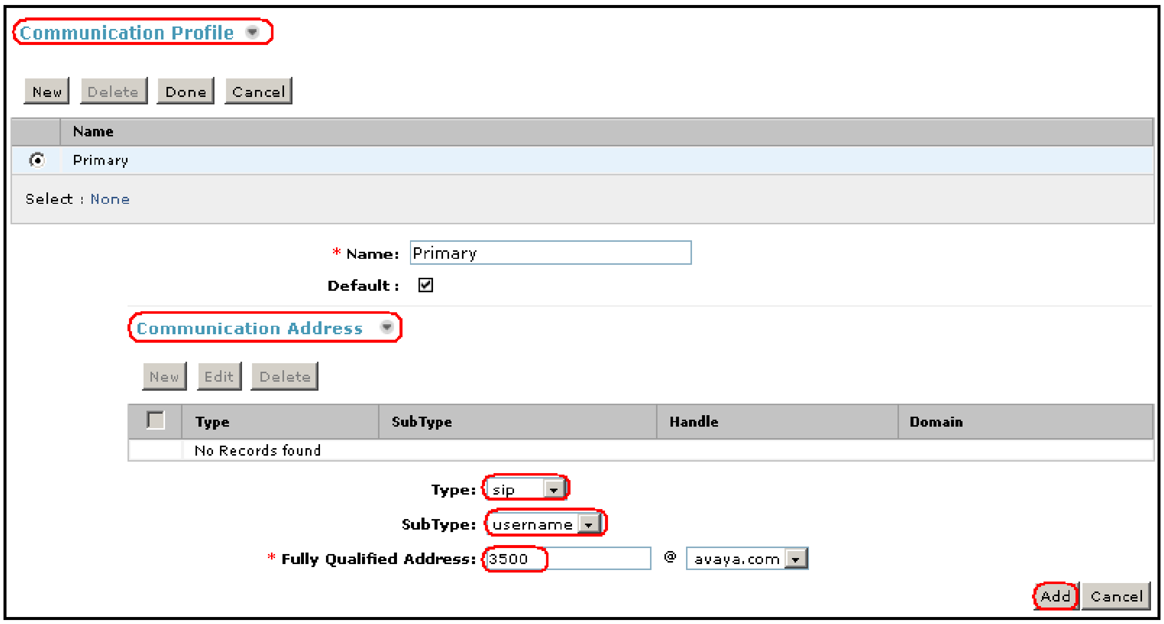
- **Login Name** The desired phone extension number belonging to the domain defined in **Section 6.1**
- **Password** Password for user to log into SMGR
- **Shared Communication Profile Password**
  Password to be entered by the user when logging into the phone



Navigate to and click on **Communication Profile** section to expand. Then click on **Communication Address** to expand that section. Enter the following and defaults for the remaining fields:

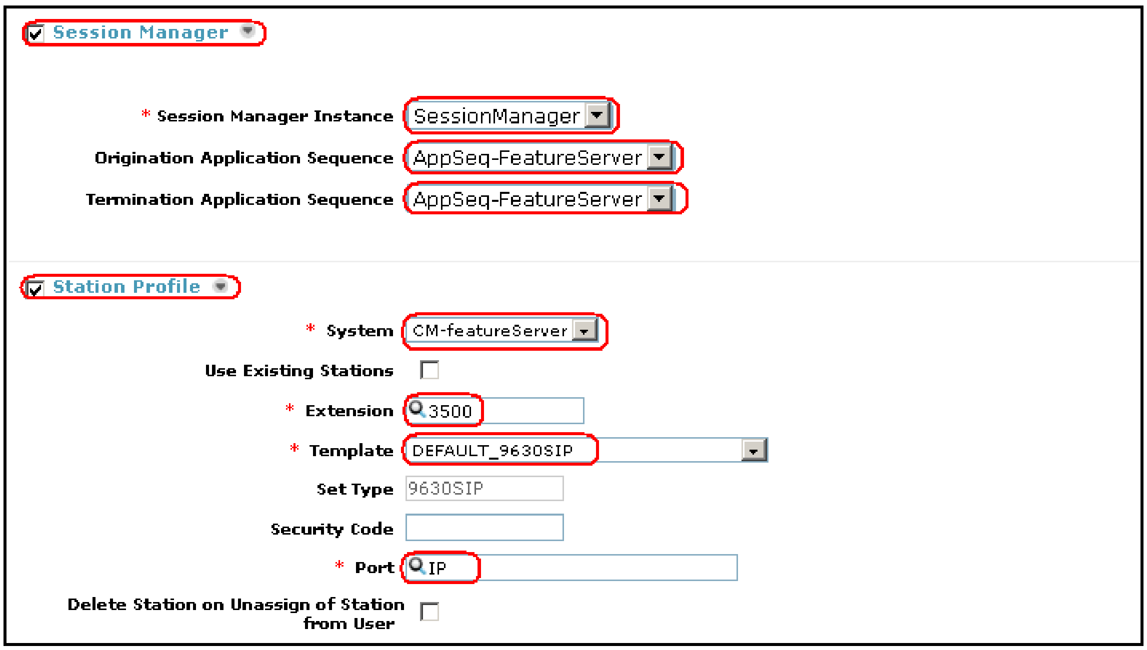
- **Type** Select **SIP**
- **SubType** Select **username**
- **Fully Qualified Address** Enter the extension number i.e. **3500**

Click on **Add**.



Navigate to and click on the **Session Manager** section to expand. Select the appropriate Session Manager server for **Session Manager Instance**. For **Origination Application Sequence** and **Termination Application Sequence** select the application sequence created in **Section 6.9.3**. Click on **Station Profile** to expand that section. Enter the following fields and use defaults for the remaining fields:

- **System**: Select the CM Entity
- **Extension**: Enter a desired extension number i.e. **3500**
- **Template**: Select a telephone type template
- **Port**: Select **IP**



Click on **Commit** to save (not shown).

7. Verification Steps

This section provides the verification steps that may be performed to verify that Avaya Aura^{TM} enterprise network can place and receive with Opal Telecom SIP gateway.

7.1. Verify Avaya Aura^{TM} Communication Manager Access Element Signaling Group Status

On Communication Manager Access Element, ensure that all the signaling groups are in-service status, by issuing the command status **signaling-group n** where **n** is the signaling group number.

```
status signaling-group 2
                         STATUS SIGNALING GROUP

        Group ID: 2                              Active NCA-TSC Count: 0
      Group Type: sip                             Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

```
status signaling-group 3
                         STATUS SIGNALING GROUP

        Group ID: 3                              Active NCA-TSC Count: 0
      Group Type: sip                             Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

7.2. Verify Avaya Aura^{TM} Communication Manager Feature Server Signaling Group Status

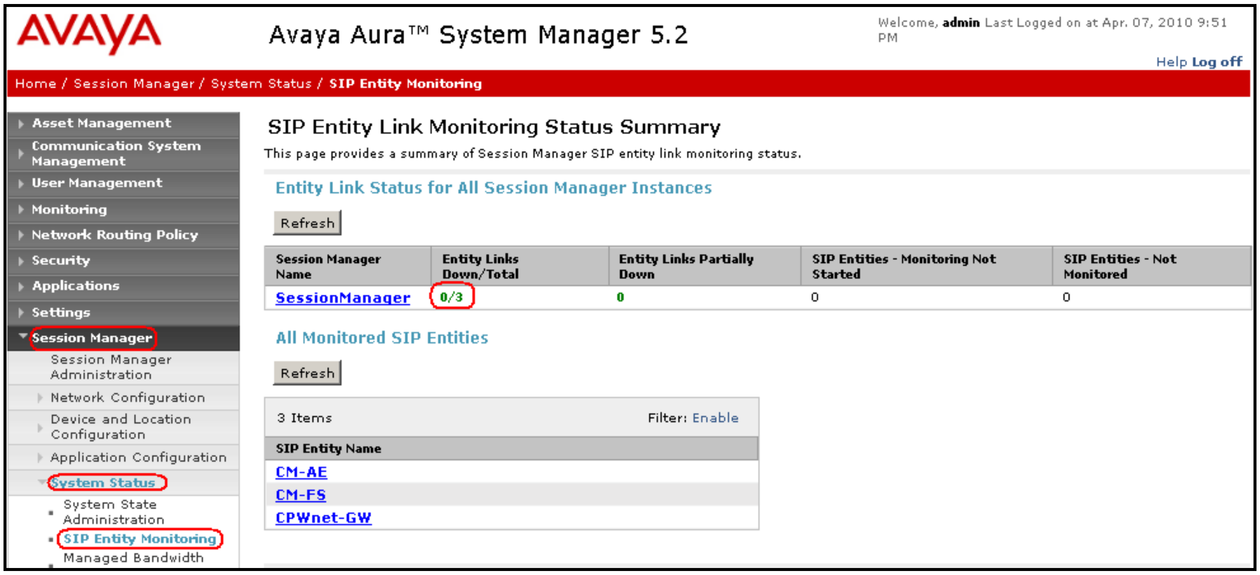
On Communication Manager Feature Server, ensure that all the signaling groups are in-service status, by issuing the command status **signaling-group n** where **n** is the signaling group number.

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1                              Active NCA-TSC Count: 0
      Group Type: sip                             Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

```
status signaling-group 2
                         STATUS SIGNALING GROUP

        Group ID: 2                              Active NCA-TSC Count: 0
      Group Type: sip                             Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

7.3. SIP Monitoring on Avaya Aura™ Session Manager

Expand the menu on the left and navigate **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.



8. General Test Approach

The interoperability compliance test included feature and serviceability test cases. The feature testing focused on verifying the following:

Basic Interoperability:

- PSTN calls from and to Avaya IP endpoint
- Calling with various Avaya telephone models including IP/SIP models as well as traditional analog and digital TDM phones
- Support G.711A
- Various PTSN dialing plans including national and international calling, toll-free, operator, directory assistance and direct inward dialed calling
- SIP transport using UDP and TCP

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
- EC500 for Avaya Aura™ Communication Manager

Service Provider specific:

- Calls from/to PSTN
- Calls from/to Mobile users
- Calls from/to other SIP trunks.

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

8.1. Test Results and Remarks

All test cases passed. DTMF test cases were deferred because lack of hardware resources in the test lab. During the execution of the tests, it was noted that on the Opal Telecom equipment that it is necessary to set **No Port Number 5060** and **SIP Maximum PDU SIZE to 3K**, in order to have successful interoperability.

9. Conclusion

As illustrated in these Application Notes, the SIP Trunking offering from Opal Telecom interoperates with Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager using SIP trunks.

10. Additional References

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

[1] "Avaya Aura™ Session Manager Overview", Document Number 03-603323, Issue 2, Release 5.2, November 2009

[2] "Installing and Upgrading Avaya Aura™ Session Manager", Document Number 03-603473, Issue 2, Release 5.2, November 2009

[3] "Administering Avaya Aura™ Session Manager", Document Number 03-603324, Issue 2.1, Release 5.2, August 2010

[4] "Avaya Aura™ Session Manager Case Studies", Document Number 03-603478, Issue 3, Release 6.0, June 2010

[5] "Maintaining and Troubleshooting Avaya Aura™ Session Manager, Document Number 03-603325, Issue 1.3, Release 5.2, January 2010

[6] "Installing and Configuring Avaya Aura™ System Platform", Release 1.1, November 2009

[7] "Installing and Upgrading Avaya Aura™ System Manager", Release 5.2, January 2010

[8] "Avaya Aura™ Communication Manager Overview", Document Number 03-300468, Issue 6, Release 5.2, May 2009

[9] "Administering Avaya Aura™ Communication Manager", Document Number 03-300509, Issue 5.0, Release 5.2, May 2009

[10] "Avaya Aura™ Communication Manager Feature Description and Implementation", Document Number 555-245-205, Issue 7.0, Release 5.2, May 2009

[11] "Administering Network Connectivity on Avaya Aura™ Communication Manager", Document Number 555-233-504, Issue 14, May 2009

[12] "SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers", Document Number 555-245-206, Issue 9, May 2009

[13] "Administering Avaya Aura™ Communication Manager as a Feature Server", Document Number 03-603479, Issue 1.2, Release 5.2, January 2010

[14] "Configuring 9600-Series SIP Phones with Avaya Aura™ Session Manager Release 5.2 – Issue 1.0", Application Note, Febrary 2010

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.