Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura™ Communication Manager, Avaya Modular Messaging, Avaya Aura™ Session Manager and Avaya Aura™ System Manager to Support IPC Alliance MX using QSIG - Issue 1.0

Abstract

These Application Notes describe the procedure to configure Avaya Aura™ Communication Manager, Avaya Modular Messaging, Avaya Aura™ Session Manager and Avaya Aura™ System Manager to support IPC Alliance MX using QSIG (Q Signaling Protocol) connectivity between the two enterprises.

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

The objective of this compliance test is to verify the solution provided by IPC can interoperate with Avaya Enterprise when connected by QSIG.
The Avaya solution will consist of the following:

- Avaya Aura™ Communication Manager
- Avaya Modular Messaging
- Avaya Aura™ Session Manager
- Avaya Aura™ System Manager

The IPC solution will consist of the following:

- IPC Alliance MX
- IPC System Center
- IPC turrets

The Avaya Aura™ Communication Manager will be connected via a QSIG trunk to the Alliance MX. The Alliance MX is a voice technology product designed to provide a high resiliency platform for provision of telephony and other associated services to financial traders. The Alliance MX provides its users with connectivity to various telephone transport services. Included in the transport services is E1 connectivity for connection within the private telephony network where the signaling protocol is QSIG. Based on IPC support policy there is no IPC configuration documented in this Application Notes. IPC engineers will be responsible for the installation and maintenance of Alliance MX products. These Application Notes describe the required configuration steps for Avaya enterprise components.

1.1. Interoperability Compliance Testing

The interoperability compliance test focused on the ability for the IPC solution to interoperate with the Avaya solution. The following is a summary of the feature and serviceability testing that was undertaken.

- Basic Calls, which including calling/connected party name/number display and restriction
- Codec Negotiation
- Hold
- Conference
- Call Transfer including calling/connected party name/number display and restriction at the primary and secondary party of the transfer
- Call forward with tests for call forward unconditional, call forward busy and call forward no reply
- Multiple call forward including calling/connected party name/number display at the calling and the diverted to party of the call forward.
- Call forward, loop avoidance
- Mail box access and message retrieval
- Message waiting indication activation and deactivation

1.2. Support

Technical support for the Avaya products can be obtained from Avaya. See the support link at support.avaya.com for contact information.

Technical support for the IPC products can be obtained from IPC. See the support link at www.ipc.com for contact information.

2. Reference Configuration

Figure 1 illustrates the network topology of the lab environment used for compliance testing.

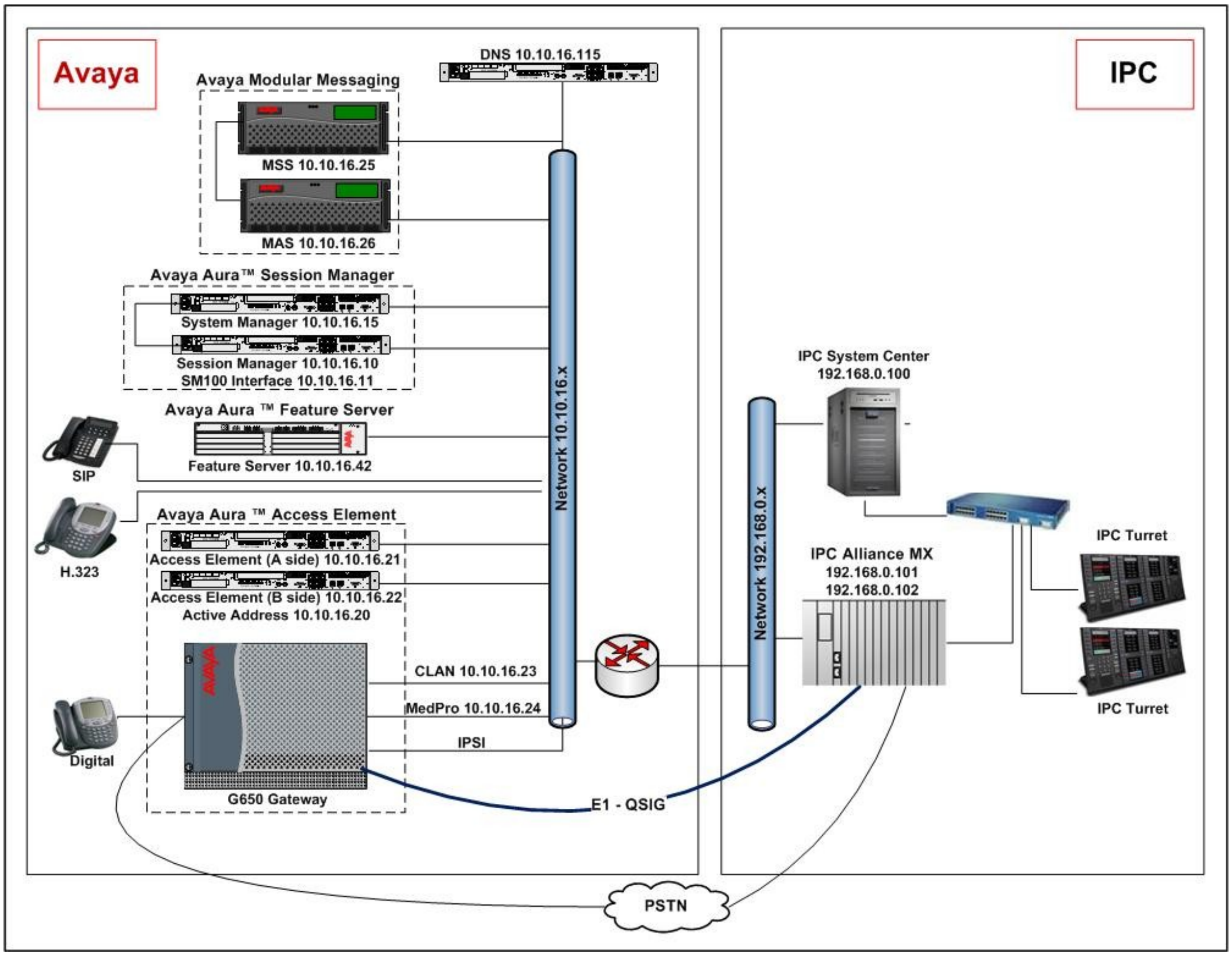
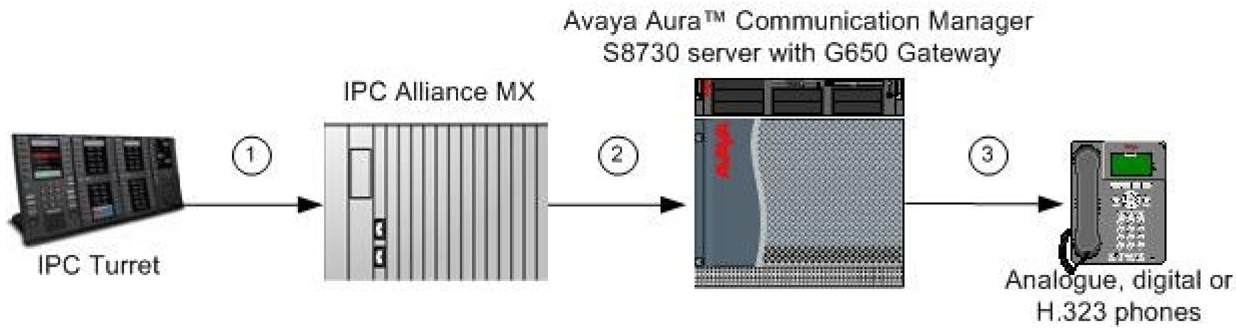


Figure 1: Test Environment Network Topology

Note: Although the Avaya and IPC IP networks are connected, all voice traffic is carried between the two enterprises via the QSIG connection represented by the blue line toward the bottom of **Figure 1.**

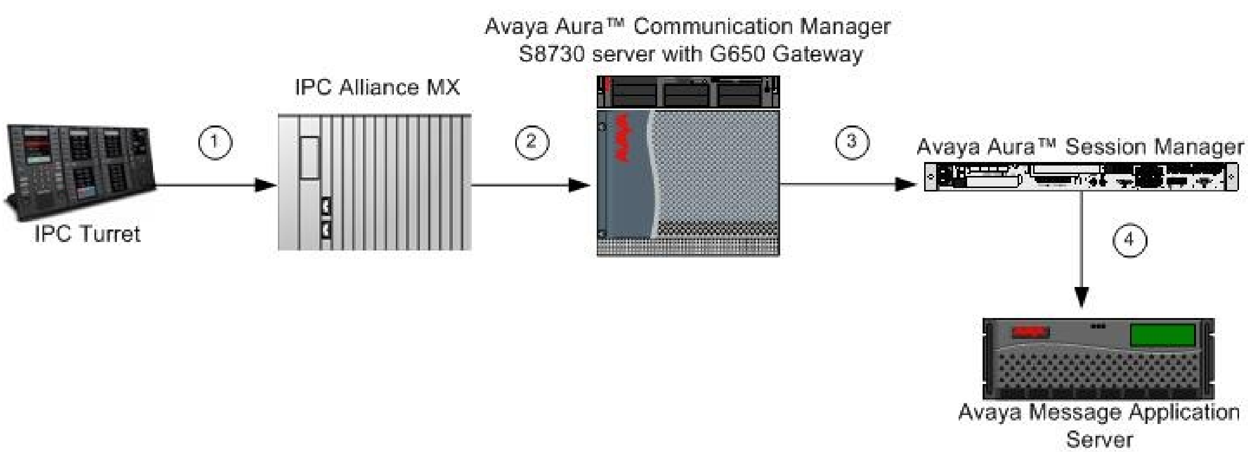
To better understand how calls are routed between the two enterprise solutions shown in **Figure 1,** four call flows are described in this section. The first call scenario is an incoming call from IPC to an Avaya H.323, digital or analog extension on a Communication Manager Access Element.

1. An IPC user dials a number which is assigned to an Avaya telephone.
2. IPC Alliance routes the call via the QSIG trunk to Communication Manager
3. Communication Manager rings the analog, digital, or H.323 telephone.



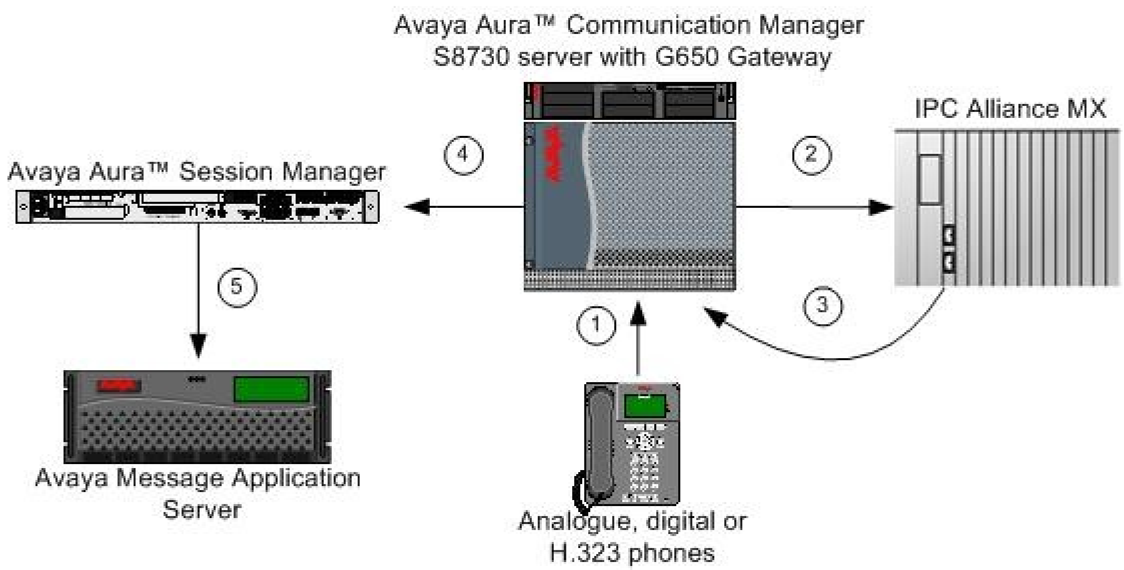
The second call scenario is an incoming call from an IPC user to an Avaya H.323, digital or analog extension on a Communication Manager Access Element that is diverting to voicemail provided by Modular Messaging.

1. An IPC user dials a number which is assigned to an Avaya telephone
2. IPC Alliance routes the call via the QSIG trunk to Communication Manager
3. Communication Manager rings the Avaya telephone and upon no answer, diverts the call to voicemail using its dial plan configuration to route the call to Session Manager
4. Session Manager routes the call to Modular Messaging via a SIP trunk configured to the MAS (Message Application Server)



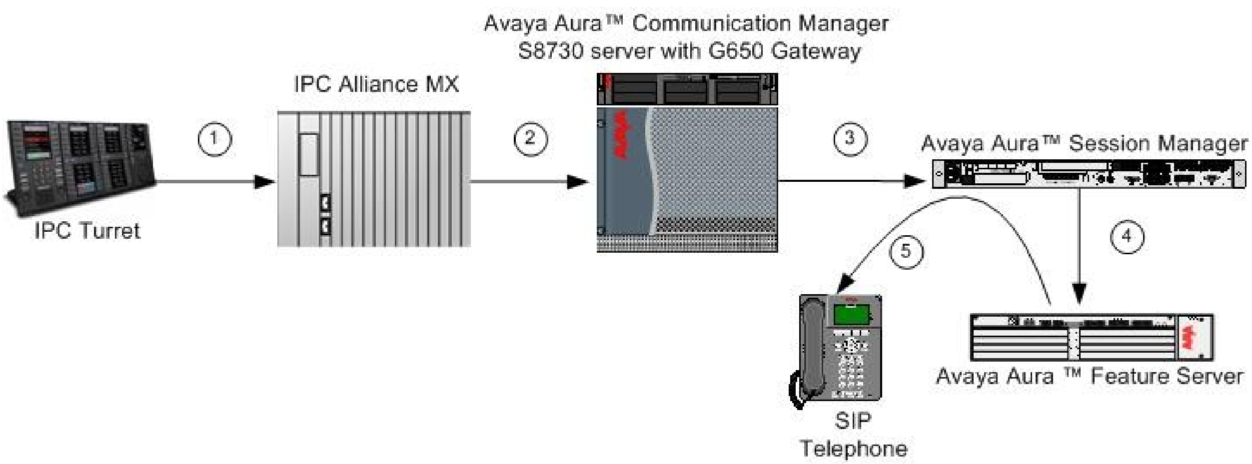
The third call scenario is an outgoing call to IPC from Avaya extension where the IPC extension is diverting to voicemail. The Avaya phone dials a number provided by IPC which is assigned to a turret where this turret line is diverted to voicemail.

1. An Avaya station dials a number provided by IPC which is assigned to a turret line appearance
2. Based on the dialed number Communication Manager routes the call to the IPC Alliance MX via QSIG trunk
3. IPC Alliance MX diverts the call to voicemail and sends the call back to Communication Manager. When a call is diverted after transiting the QSIG trunk a QSIG re-route request is sent to the switch that initiated the QSIG call, this re-route request allows the initiating switch to tear down the original leg of the call and create a new call leg to the diverted to number. In this example the diverted to number resides within the Avaya enterprise so upon completion of the re-route request no call leg will be active to the Alliance MX
4. Based on the diverted to number Communication Manager uses its dial plan configuration to route the call to Session Manager via a SIP trunk
5. Session Manager routes the call to Modular Messaging via a SIP trunk configured on the MAS (Message Application Server)



The fourth call scenario is an incoming call from an IPC user to an Avaya SIP extension. SIP extensions register with Session Manager and use the Feature Server for their feature and configuration settings.

1. An IPC user dials a number which is assigned to an Avaya SIP telephone
2. IPC Alliance routes the call via the QSIG trunk to Communication Manager Access Element.
3. Communication Manager Access Element uses its dial plan configuration to route the call to Session Manager
4. Session Manager uses an application sequence to route the call to the Feature Server via an IMS enabled SIP trunk.
5. As the SIP extension is registered with the Session Manager, Feature Server uses the IMS enabled SIP trunk to inform the Session Manager to terminate the call to the SIP end point.



3. Equipment and Software Validated

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

Equipment	Software
Avaya™ S8510 Server	Avaya Aura™ System Manager 5.2 Service Pack 1
Avaya™ S8510 Server	Avaya Aura™ Session Manager 5.2 Service Pack 1
Avaya™ S8730 Server's	Avaya Aura™ Communication Manager 5.2.1 – S8730-15-02.1.016.4. Service Pack 0
Avaya™ G650 Media Gateway - CLAN - TN799DP - MedPro - TN 2602AP	 HW16 FW032 .(35) HW08 FW048. (51)
Avaya S8300D Server & Avaya G450 Media Gateway	Avaya Aura™ Communication Manager 5.2.1, R015x02.1.016.4. Service Pack 0 (Feature Server)
Avaya ™ 3500 Server	Avaya Modular Messaging, Message Application Server 5.1. Service Pack 1 Patch 2
Avaya ™ 3500 Server	Avaya Modular Messaging, Message Storage Server 5.1. Service Pack 1 Patch 2
Avaya 9630 IP Telephones	SIP: 2.5.0.0 H.323: R3.0
IPC Information Systems Alliance MX IPC System Center (Sun ULTRA 25) IPC IQ/MAX Turrets	15.03.00 Patch 2

4. Configure Avaya Aura^{TM} Communication Manager as Access Element

This section describes the steps for configuring the Communication Manager as an Access Element. All configurations in the section are administered using the System Access Terminal (SAT). These Application Notes assume that the basic Communication Manager configuration has already been administered. The procedures include the following areas:

- Confirm Necessary Features
- Confirm Special Applications
- Confirm Call forwarding Configuration
- Administer Feature Access Codes
- Administer IP Node Names
- Administer IP Network Region
- Administer IP Codec Set
- Administer SIP Signaling Group
- Administer SIP Trunk Group
- Administer DS1
- Administer QSIG Signaling Group
- Administer QSIG Trunk Group
- Administer Public Numbering
- Administer Private Numbering
- Administer Route patterns
- Administer Dialplan Analysis
- Administer Uniform Dialplan
- Administer AAR
- Administer Modular Messaging Hunt Group
- Administer Modular Messaging Coverage Path

4.1. Confirm Necessary Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Log into the Communication Manager SAT interface and use the **display system-parameters customer-options** command to determine these values. On **Page 2** verify that the available **Maximum Administered SIP Trunks** is equal to or greater than the desired number of simultaneous SIP trunk connections.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 200   0
           Maximum Concurrently Registered IP Stations: 1800  1
             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: 0     0
                        Maximum Video Capable Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 200   78
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
```

On **Page 3** verify the fields **ARS** and **ARS/AAR Partitioning** are set to **y.**

```
display system-parameters customer-options                      Page   3 of  10
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? n
        Access Security Gateway (ASG)? n              Authorization Codes? n
        Analog Trunk Incoming Call ID? n                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? n                         CAS Main? n
Answer Supervision by Call Classifier? n                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? n
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                      DCS (Basic)? n
          ASAI Link Core Capabilities? n                DCS Call Coverage? n
```

On **Page 4** verify the fields **ISDN-PRI** and **IP Trunks** are set to **y**

```
display system-parameters customer-options                         Page   4 of  10
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                          IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                    ISDN Feature Plus? y
                  Enhanced EC500? y       ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                      ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                             ISDN-PRI? y
              ESS Administration? n              Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? n                 Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? n                 Multifrequency Signaling? y
      Global Call Classification? n          Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y       Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? n              Multimedia IP SIP Trunking? y
                       IP Trunks? y
```

On **Page 5** verify the fields **Private Networking** and **Uniform Dialing Plan** are set to **y.**

```
display system-parameters customer-options                         Page   5 of  10
                                OPTIONAL FEATURES

                Multinational Locations? y           Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? y      Station as Virtual Extension? n
                     Multiple Locations? y
                                            System Management Data Transfer? n
          Personal Station Access (PSA)? y              Tenant Partitioning? n
                       PNC Duplication? n       Terminal Trans. Init. (TTI)? y
                   Port Network Support? y              Time of Day Routing? n
                       Posted Messages? y       TN2501 VAL Maximum Capacity? y
                                                       Uniform Dialing Plan? y
                     Private Networking? y     Usage Allocation Enhancements? y
               Processor and System MSP? n
                     Processor Ethernet? y                 Wideband Switching? n
```

On **Page 8**, verify that **Basic Call Setup**, **Basic Supplementary Services**, **Centralized Attendant**, **Supplementary Services with Rerouting** and **Transfer into QSIG Voice Mail** are all set to **y.**

```
 display system-parameters customer-options                        Page   8 of  10
                             QSIG OPTIONAL FEATURES

                                     Basic Call Setup? y
                         Basic Supplementary Services? y
                                Centralized Attendant? y
                                Interworking with DCS? n
                Supplementary Services with Rerouting? y
                        Transfer into QSIG Voice Mail? y
                                   Value-Added (VALU)? y
```

Use the **display system-parameters features** command to verify the following system features are defined. On **Page 1** verify **DID/Tie/ISDN/SIP Intercept Treatment** is set to **attd** to route calls to unassigned numbers to the attendant console. For simplicity, the **Trunk-to-Trunk Transfer** field was set to **all** to enable all trunk-to-trunk transfers on asystem 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

```
display 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
```

On **Page 8** confirm **QSIG/ETSI TSC Extension** and **QSIG Path Replacement Extension** fields are configured with valid extensions and that the **MWI – Number of Digits Per Voice Mail Subscriber** is configured with the appropriate extension length.

```
display system-parameters features                              Page   8 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS
ISDN PARAMETERS
                                                          PARAMETERS FOR CREATING
 Send Non-ISDN Trunk Group Name as Connected Name? y      QSIG SELECTION NUMBERS
 Display Connected Name/Number for ISDN DCS Calls? y        Network Level:
       Send ISDN Trunk Group Name on Tandem Calls? y         Level 2 Code:
                Send Custom Messages Through QSIG? y         Level 1 Code:

                          QSIG/ETSI TSC Extension: 6666
 MWI - Number of Digits Per Voice Mail Subscriber: 4
                                Feature Plus Ext:
                             National CPN Prefix:
                        International CPN Prefix:
                               Pass Prefixed CPN: ASAI? n   VDN/Vector? n
    Unknown Numbers Considered Internal for AUDIX? y         Maximum Length: 5
             USNI Calling Name for Outgoing Calls? n
               Path Replacement with Measurements? y
                  QSIG Path Replacement Extension: 6667
   Send QSIG Path Replacement Conf. Event to ASAI? y
```

On **Page 9** confirm that **CPN/ANI/ICLID PARAMETERS** have a relevant text string configured

```
display system-parameters features                              Page   9 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: restricted
```

On **Page 15** confirm that **Chained Call-forwarding** is set to **y.** This feature enables the ability to alter the number of allowed QSIG re-routes covered in **Section 4.3**

```
display system-parameters features                               Page  15 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS
SPECIAL TONE
                                  Special Dial Tone? n
          Special Dial Tone for Digital/IP Stations: none

REDIRECTION NOTIFICATION
                           Display Notification for Do Not Disturb? n
                           Display Notification for Send All Calls? n
                             Display Notification for Call Forward? n
                    Display Notification for Enhanced Call Forward? n
                         Display Notification for a locked Station? n
         Display Notification for Limit Number of Concurrent Calls? n
                          Display Notification for Posted Messages? n
                                Scroll Status messages Timer(sec.):

Chained Call Forwarding? y
```

On **Page 18** confirm that **Direct IP-IP Audio Connections** is set to **y.**

```
display system-parameters features                              Page  18 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

IP PARAMETERS

                   Direct IP-IP Audio Connections? y
                             IP Audio Hairpinning? n
```

4.2. Special Applications

Use the **display system-parameters special-applications** command. On **Page 3**, verify that **(SA8440) - Unmodified QSIG Reroute Number?** is set to **y**. When a call that arrives on a QSIG trunk is then diverted off net, a facility message is sent back toward the switch that originated the call to allow the originating switch to pick a better route to reach the diverted-to party. The facility message contains the number of the diverted-to party. This number is normally processed by Communication Manager so that the digits in the facility message are not the same digits as those entered when the call forwarding feature was activated. When SA8440 feature is active, the number in the facility message will not be processed by Communication Manager so it will exactly match the number entered when call forwarding was activated. If this option is not set, please contact Avaya sales team or business partner for the appropriate license file.

```
display system-parameters special-applications                    Page   3 of   9
                              SPECIAL APPLICATIONS

                   (SA8141) - LDN Attendant Queue Priority? n
       (SA8143) - Omit Designated Extensions From Displays? n
            (SA8146) - Display Update for Redirected Calls? n
              (SA8156) - Attendant Priority Queuing by COR? n
               (SA8157) - Toll Free Vectoring until Answer? n
  (SA8201) - Start Time and 4-Digit Year CDR Custom Fields? n
                         (SA8202) - Intra-switch CDR by COS? n
                     (SA8211) - Prime Appearance Preference? n
                       (SA8240) - Station User Admin of FBI? n
                                  (SA8312) - Meet-Me Paging? n
                   (SA8323) - Idle Call Preference Display? n
                         (SA8339) - PHS X-Station Mobility? n
                  (SA8348) - Map NCID to Universal Call ID? n
               (SA8428) - Station User Button Ring Control? n
             (SA8434) - Delay PSTN Connect on Agent Answer? n
                          (SA8439) - Forward Held-Call CPN? n
                 (SA8440) - Unmodified QSIG Reroute Number? y

                                           (SA8475) - SOSM? n
```

4.3. Confirm Call Forwarding Configuration

Use the **display system-parameters coverage-forwarding** command to verify on **Page 2** that the **Maximum Number Of Call Forwarding Hops** is set to a value mutually agreed with IPC**.** This feature determines the number of QSIG re-route requests the Communication Manager will accept. If this value is lower than the value used by IPC then the Communication Manager will reject any QSIG re-route requests from the Alliance MX once the specified value has been reached. This will force the Alliance MX to forward switch any further diversions.

```
display system-parameters coverage-forwarding                    Page   2 of   2
                SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING

COVERAGE OF CALLS REDIRECTED OFF-NET (CCRON)

                       Coverage Of Calls Redirected Off-Net Enabled? y
 Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point? y
                                  Ignore Network Answer Supervision? n
                 Disable call classifier for CCRON over ISDN trunks? n
                  Disable call classifier for CCRON over SIP trunks? n

CHAINED CALL FORWARDING
                             Maximum Number Of Call Forwarding Hops: 6
                Station Coverage Path For Coverage After Forwarding: principal
```

4.4. Administer Feature Access Codes

Use the **display feature-access-codes** command to verify the following feature access codes are defined. On **Page 1** confirm that **Auto Alternate Routing (AAR) Access Code** is set to a valid feature access code according to the dial plan.

```
 display 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: #3
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 1
    Auto Route Selection (ARS) - Access Code 1: *7    Access Code 2:
                 Automatic Callback Activation: *4     Deactivation: #4
Call Forwarding Activation Busy/DA: *2     All: *3     Deactivation: #2
   Call Forwarding Enhanced Status:        Act: 622    Deactivation: 623
                         Call Park Access Code: #5
                       Call Pickup Access Code: *6
CAS Remote Hold/Answer Hold-Unhold Access Code: #6
```

On **Page 3**, Verify a **Per Call CPN Blocking Code Access Code** is assigned

```
display feature-access-codes                                      Page   3 of   8
                               FEATURE ACCESS CODE (FAC)
             Leave Word Calling Send A Message:
           Leave Word Calling Cancel A Message:
   Limit Number of Concurrent Calls Activation:        Deactivation:
               Malicious Call Trace Activation:        Deactivation:
         Meet-me Conference Access Code Change:
          Message Sequence Trace (MST) Disable:

 PASTE (Display PBX data on Phone) Access Code:
  Personal Station Access (PSA) Associate Code:        Dissociate Code:
        Per Call CPN Blocking Code Access Code: *34
      Per Call CPN Unblocking Code Access Code: *35
                  Posted Messages Activation:          Deactivation:
                  Priority Calling Access Code: *30
                           Program Access Code:
```

4.5. Administer IP Node Names

Use the **change node-names ip** command to add the IP address of the Session Manager interface, also make note of the CLAN name as this will be used to configure the SIP signaling groups.

```
 change node-names ip
                                 IP NODE NAMES
    Name              IP Address
CLAN1               10.10.16.23
Gateway             10.10.16.1
MedPro1             10.10.16.24
SM100               10.10.16.11
default             0.0.0.0
procr               10.10.16.20
```

4.6. Administer IP Network Region

Use the **change ip-network-region n** command, where **n** is the network region number to configure. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise, a descriptive **Name** for this ip-network-region and set the **Codec Set** to the number of the codec set that will be used. **Intra-region IP-IP Direct Audio** and **Intra-region IP-IP Direct Audio** should be set to **yes** to enable IP shuffling. Although not highlighted, note also that the **IP Network Region** form is used to set the QoS packet parameters that provide priority treatment for signaling and audio packets over other data traffic. These parameters may need to be aligned with the specific values expected by the IP network.

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Default Region
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
```

4.7. Administer IP Codec Sets

Use the **change ip-codec-set n** command, where **n** is the codec set specified in the **IP Network Region** form. Enter the codecs eligible to be used; In the sample configuration Modular Messaging uses the G.711A codec, this codec must be included.

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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.711A           n          2        20
 3: G.729            n          2        20
 4:
 5:
```

4.8. Administer SIP Signaling Group

Use the **add signaling-group n** command, where **n** is the number of the SIP signaling-group to create.

- Set the **Group Type** field to be **SIP**
- Set the **Transport Method** to the desired transport method; either **TCP** (Transport Control Protocol) or TLS (Transport Layer Security). For transparency, **TCP** was used during this compliance test but the recommended method is TLS
- The **Near-end Node Name** is set to the name of the CLAN that will be used to process the signaling. The clan name is assigned in the IP Node-names form
- The **Far-end Node Name** is set to the name of the Session manager that was entered into the IP Node-names form
- The **Far-end network Region** to the region configured in **Section 4.6**
- The **Far-end Domain** is set to the name of the domain name that is used by Session Manager and Modular Messaging

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

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


   Near-end Node Name: CLAN1                 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: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                      Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

4.9. Administer SIP Trunk Group

Use the **add trunk-group n** command where **n** is the number of the SIP trunk group to create. This trunk will be used to connect Communication Manager to Session Manager.

- Set the **Group Type** field to be **sip**
- Add a descriptive name into the **Group Name** field
- Set the **TAC** field to a valid dial access code (dac) according to the dial plan configuration
- Set the **Service Type** field to **tie**
- Set the **Signaling Group** field to the signaling group set up in **Section 4.8**
- Set the **Number of Members** field to the number of channels required on the trunk group

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

Group Number: 2                    Group Type: sip          CDR Reports: y
  Group Name: SIP Trunk                COR: 1        TN: 1        TAC: 502
   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: 48
```

On **Page 3** of the trunk-group form set the **Numbering Format** field to **public**.

```
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


 Show ANSWERED BY on Display? y
```

On **Page 4** of the trunk-group form ensure the **Support Request History** field is set to **y** as MM relies on the History Info headers to select an appropriate mail box.

```
add trunk-group 1                                             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:
```

4.10. Administer DS1

Use the **add ds1 n** command where **n** is the board location of the DS1, to configure the DS1 Circuit Pack that will be used for the QSIG connection between Avaya Communication Manager and the Alliance MX. The values used should be agreed with IPC prior to configuration. The screen output below shows the values used during this compliance test, modified fields are shown in bold all other fields were left as default.

```
add ds1 01a06                                                 Page   1 of   1
                                DS1 CIRCUIT PACK

            Location: 01A06                           Name: QSIG-IPC
            Bit Rate: 2.048                    Line Coding: hdb3

      Signaling Mode: isdn-pri
             Connect: pbx                        Interface: peer-master
   TN-C7 Long Timers? n                      Peer Protocol: Q-SIG
Interworking Message: PROGress                        Side: a
Interface Companding: alaw                            CRC? y
           Idle Code: 11111111           Channel Numbering: timeslot
                              DCP/Analog Bearer Capability: 3.1kHz

                                           T303 Timer(sec): 4
                                          Disable Restarts? n

      Slip Detection? n                Near-end CSU Type: other

   Echo Cancellation? n
```

4.11. Administer QSIG Signaling Group

Use the **add signaling-group n** command, where **n** is the number of the signaling-group to create.

- Set the **Group Type** field to be **isdn-pri**
- The **Primary D-Channel** is set to channel 16 of the DS1 circuit pack configured in **Section 4.10**
- The **TSC Supplementary Service Protocol** is set to **b**

The **Max number of NCA, Trunk Group for NCA TSC** and **Trunk Group for Channel Selection** must all be set after the trunk group has been added by running the command **change signaling-group 3.** The **Max number of NCA TSC** must be at least 2, one for Communication Manager and one for Alliance MX.

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

 Group Number: 3             Group Type: isdn-pri
                   Associated Signaling? y          Max number of NCA TSC: 5
                      Primary D-Channel: 01A0616     Max number of CA TSC: 5
                                                  Trunk Group for NCA TSC: 3
       Trunk Group for Channel Selection: 3
      TSC Supplementary Service Protocol: b          Network Call Transfer? n
```

4.12. Administer QSIG Trunk Group

Use the command **add trunk-group n** where **n** is the number of the QSIG trunk group to create. This trunk will be used to connect Communication Manager to Alliance MX.

- Set the **Group Type** field to be **isdn**
- Add a descriptive name into the **Group Name** field
- Set the **TAC** field to a valid dial access code (dac) according to the dial plan configuration
- Set the **Carrier Medium** field to **PRI/BRI**
- Set the **Service Type** field to **tie**

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

Group Number: 3                   Group Type: isdn          CDR Reports: y
  Group Name: IPC QSIG                   COR: 1        TN: 1        TAC: 503
   Direction: two-way       Outgoing Display? n        Carrier Medium: PRI/BRI
 Dial Access? y             Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n            TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
```

On **Page 2** of the trunk group form set the **Supplementary Service Protocol** to **b. The Digit Handling (in/out)** field should be set to a value mutually agreed with IPC, in the sample configuration **overlap/enbloc** is used.

```
add trunk-group 3                                              Page   2 of  21
      Group Type: isdn

TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6
        Max Message Size to Send: 260   Charge Advice: none
  Supplementary Service Protocol: b     Digit Handling (in/out): overlap/enbloc
       Digit Treatment:                                         Digits:
            Trunk Hunt: cyclical
                                                    Digital Loss Group: 13
Incoming Calling Number - Delete:     Insert:                  Format:
              Bit Rate: 1200         Synchronization: async    Duplex: full
 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 0
          Administer Timers? n        CONNECT Reliable When Call Leaves ISDN? n
```

On **Page 3** of the trunk group form set **Send Name** and **Send Calling Number** to **y.** Set the **Format** field to **private** so that calls will reference the private numbering table. Set the **Replace Restricted Numbers?, Replace Unavailable Numbers**? and **Send Connected Number** to **y**. **Modify Reroute Number** is the administrative control for special application SA8440 (covered in **Section 4.2**) and should be set to **n.**

```
add trunk-group 3                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                 Internal Alert? n       Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member: 1
                                      Send Name: y      Send Calling Number: y
            Used for DCS? n             Hop Dgt? n     Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: private
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y
                                                      Send Connected Number: y
                                                  Hold/Unhold Notifications? y
             Send UUI IE? y                   Modify Tandem Calling Number? n
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                         Ds1 Echo Cancellation? n
                                                      Modify Reroute Number? n
    Apply Local Ringback? n
 Show ANSWERED BY on Display? y
                              Network (Japan) Needs Connect Before Disconnect? n
 DSN Term? n
```

On **Page 4** of the trunk group form set **Diversion by Reroute, Path Replacement** and **Display Forwarding Party Name** to **y.**

```
add trunk-group 3                                              Page   4 of  21
                       QSIG TRUNK GROUP OPTIONS




   TSC Method for Auto Callback: drop-if-possible
           Diversion by Reroute? y
               Path Replacement? y
Path Replacement with Retention? n
        Path Replacement Method: better-route
                           SBS? n
  Display Forwarding Party Name? y
    Character Set for QSIG Name: eurofont
               QSIG Value-Added? n
```

4.13. Administer Public Numbering

To ensure that the caller number is correctly presented, the SIP trunk group set up in **Section 4.9** references the public numbering table, use the command **change public-unknown-numbering n**. The following values should be set:

- Set **Ext Len** field to **4** as this is the length of the extensions that will be using the table
- Set **Ext Code** to match the leading digits of extension ranges to be used
- Set **Trk Grp(s)** to **2** for the number of the trunk group that will use this entry
- Set **Total Len** to **4** as this is the total length of the calling number that will be presented by the trunk group

```
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  66               2                          4          Maximum Entries: 9999
 4  31               2                          4
```

4.14. Administer Private Numbering

To ensure that the caller number is correctly presented, the QSIG trunk group set up in **Section 4.12** references the private numbering table, use the command **change private-numbering n** where **n** is the number of the private numbering table to be edited. The following values should be set:

- Set **Ext Len** field to **4** this is the length of the extensions that will be using the table
- Set **Ext Code** to match the leading digits of extension ranges to be used
- Set **Trk Grp(s)** to **3** this is the number of the trunk group that will use this entry
- Set **Total Len** to **4** this is the total length of the calling number that will be presented by the trunk group

```
change private-numbering 0                                        Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext             Trk         Private          Total
Len Code            Grp(s)      Prefix           Len
 4  1                                            4     Total Administered: 4
 4  31              3                            4        Maximum Entries: 540
 4  37                                           4
 4  66              3                            4
```

4.15. Administer Route Patterns

Use the **change route-pattern n** command to add the route pattern that will direct calls to the SIP trunk group. AAR will select this route pattern for calls to Modular Messaging. In this configuration trunk group **2** is added under the **Grp No** field.

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

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

Use the **change route-pattern n** command to add the route pattern that will direct calls to the QSIG trunk group. AAR will select this route pattern for calls to IPC. In this configuration trunk group **3** is added under the **Grp No** field. Set **TSC** to **y**, **CA TSC Request** to **none** and the **Numbering Format** field to **unk-unk**

```
change route-pattern 3                                              Page   1 of   3
                   Pattern Number: 3   Pattern Name: IPC_QSIG
                            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
3:                                                                     n   user
4:                                                                     n   user
5:                                                                     n   user
6:                                                                     n   user

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

4.16. Administer Dialplan Analysis

Use the **change dialplan analysis** command to administer the dialplan. In this configuration extensions in the range 31xx are assigned to IPC turrets and are configured as **udp** to send calls via the UDP (uniform dial plan). Extensions ranges 66xx, 89xx and 88xx are Communication Manager extensions and are configured as **ext.**

```
change 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
     0             1    ext     663          4    udp
     1             1    fac     7            4    ext
     2             4    udp     88           4    ext
     30            9    udp     89           4    ext
     3005          8    udp     972          5    udp
     31            4    udp     99           4    ext
     33            4    udp     *            2    fac
     37            4    udp     #            2    fac
     38            5    aar
     4             4    aar
     4             5    ext
     5             3    dac
     6             3    fac
     61            4    ext
     66            4    ext
```

4.17. Administer Uniform Dialplan

Use the **change uniform-dialplan** command to administer the UDP routing. It is possible to use the UDP to manipulate the dialed digits but in this configuration UDP is used to direct the matching calls to AAR (alternate access routing). Extensions beginning 31 are used by IPC turrets and extensions beginning 663 are SIP extension on the Feature Server, both are directed to the AAR for routing. Extension 8889 is directed to the AAR as it is the Modular Messaging pilot number

```
change uniform-dialplan

                      UNIFORM DIAL PLAN TABLE

 Matching Pattern   Len   Del   Insert Digits   Net    Conv   Node Num

 31                  4     0                    aar     n
 33                  4     0                    aar     n
 37                  4     0                    aar     n
 663                 4     0                    aar     n
 8889                4     0                    aar     n
 972                 5     0                    aar     n
```

4.18. Administer AAR

Use the **change aar analysis n** command to specify which route pattern to use based upon the number dialed. In this example, **Route Pattern 3** is used for IPC extensions beginning **31** and **Route Pattern 2** is used for SIP extensions that begin with **663** as well as the Modular Messaging pilot number **8889.**

```
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
    31                     4    4     3        aar          n
    33                     4    4     2        aar          n
    37                     4    4     7        aar          n
    663                    4    4     2        aar          n
    8889                   4    4     2        aar          n
    972                    5    5     4        aar          n
```

4.19. Administer Avaya Modular Messaging Hunt Group

Use the **add hunt-group n** command where **n** is the number of the hunt-group to add. Give the hunt group a descriptive name and a valid extension according to the dial plan. Set **ISDN/SIP Caller Display** to **grp-name.**

```
add hunt-group 2                                              Page   1 of  60
                                    HUNT GROUP

            Group Number: 2                                    ACD? n
              Group Name: Modular Messaging                  Queue? n
         Group Extension: 8999                              Vector? n
              Group Type: ucd-mia                   Coverage Path:
                      TN: 1          Night Service Destination:
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display: grp-name
```

On **Page 2** of the hunt group form set the **Message Center** to be **sip-adjunct** and enter a **Voice Mail Number** and **Voice Mail Handle**, in this configuration both are set to **8889**. Enter the AAR access code as defined in the feature access codes form (**Section 4.4)** for **Routing Digits.**

```
add hunt-group 2                                              Page   2 of  60
                                    HUNT GROUP


                        Message Center: sip-adjunct

     Voice Mail Number         Voice Mail Handle          Routing Digits
                                                     (e.g., AAR/ARS Access Code)
     8889                      8889                       1
```

4.20. Administer Avaya Modular Messaging Coverage Path

Use command **change coverage path n** where **n** is the number of the coverage path to administer. Set **Point 1** to **h2** to send covered calls using this coverage path to hunt group 2.

```
change coverage path 2                                          Page   1 of   1
                                 COVERAGE PATH

                   Coverage Path Number: 2
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA

    Station/Group Status    Inside Call     Outside Call
             Active?            n               n
               Busy?            y               y
       Don't Answer?            y               y        Number of Rings: 2
                All?            n               n
 DND/SAC/Goto Cover?            y               y
   Holiday Coverage?            n               n

COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h2            Rng:    Point2:
  Point3:                       Point4:
```

Use the **change station n** command to add the coverage path to a station where **n** is the extension number of the station to administer. Enter the coverage path number in the **Coverage Path 1** field.

```
change station 6621                                             Page   1 of   5
                                     STATION

Extension: 6621                         Lock Messages? n             BCC: 0
     Type: 9630                         Security Code: ****           TN: 1
     Port: S00002                     Coverage Path 1: 2             COR: 1
     Name: IP2nd                      Coverage Path 2:               COS: 1
                                      Hunt-to Station:
```

4.21. Save Configuration

Use the **save translation** command to save the Communication Manager configuration. The following screen shows the output of a successful save translation command.

```
save translation

                               SAVE TRANSLATION

           Command Completion Status                           Error Code

           Success                                             0
```

5. Configure Avaya Aura™ Communication Manager as Feature Server

This section describes the steps for configuring the Communication Manager as an Feature Server to support SIP handsets. All Configurations in the section are administered using the System Access Terminal (SAT). These Application notes assume that the basic Communication Manager configuration has already been completed. The procedures covered, include the following areas:

- Administer IP Node Names
- Administer IP Network Region
- Administer IP Codec Set
- Administer SIP Signaling Group
- Administer SIP Trunk Group

5.1. Administer IP Node Names

Use the **change node-names ip** command to add the IP address of the Session Manager interface, also make note of the procr name as this will be used to configure the SIP signaling groups.

```
change node-names ip
                                  IP NODE NAMES
    Name              IP Address
DefGW               10.10.16.1
procr               10.10.16.42
default             0.0.0.0
medpro              10.10.16.43
procr               10.10.16.17
sm100               10.10.16.11
```

5.2. Administer IP Network Region

Use the **change ip-network-region n** command, where **n** is the network region number to configure. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise, a descriptive **Name** for this ip-network-region and set the **Codec Set** to the number of the codec set that will be used. **Intra-region IP-IP Direct Audio** and **Intra-region IP-IP Direct Audio** should be set to **yes** to enable IP shuffling.

Although not highlighted, note also that the **IP Network Region** form is used to set the QoS packet parameters that provide priority treatment for signaling and audio packets over other data traffic. These parameters may need to be aligned with the specific values expected by the IP network.

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: SIP IPNR
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
```

5.3. Administer IP codec sets

Use the **change ip-codec-set n** command, where **n** is the codec set specified in the IP Network Region form. Enter the codecs eligible to be used. In the sample configuration Modular Messaging uses the G.711A codec, this codec must be included

```
change ip-codec-set 1                                           Page   1 of   2
                          IP Codec Set
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.711A           n          2        20
 3: G.729            n          2        20
 4:
 5:
```

5.4. Administer SIP Signaling Group

Use the **add signaling-group n** command, where **n** is the number of the signaling-group being added to the system.

- Set the **Group Type** field to be **SIP**
- Set the **Transport Method** to the desired transport method; TCP (Transport Control Protocol) or TLS (Transport Layer Security). For transparency **TCP** was used during this compliance test but the recommended method is TLS
- The **Near-end Node Name** is set to the name of the CLAN that will be used to process the signaling. The **clan** name is assigned in the IP Node-names form
- The **Far-end Node Name** is set to the name of the Session Manager that was entered into the IP Node-names form
- The **Far-end network Region** is set to the region configured in **Section 5.2**
- The **Far-end Domain** is set to the name of the domain name that is used by Session Manager
- Set the **IMS Enabled** field to **y**

```
add signaling-group 200                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 200              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? y



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

5.5. Administer SIP Trunk Group

To create a SIP trunk group use the command **add trunk-group n** where **n** is the number of the trunk group to create.

- Set the **Group Type** field to be **sip**
- Add a descriptive name into the **Group Name** field
- Set the **TAC** field to a valid dial access code (dac) according to the dial plan configuration
- Set the **Service Type** field to **tie**
- Set the **Signaling Group** field to the signaling group set up in **Section 5.4**
- Set the **Number of Members** field to the number of channels required on the trunk group

```
add trunk-group 200                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 200                   Group Type: sip           CDR Reports: y
  Group Name: toASM                        COR: 1        TN: 1        TAC: *20
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                      Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                         Signaling Group: 200
                                                       Number of Members: 30
```

On **Page 3** of the trunk-group form set the **Numbering Format** field to **private** and ensure the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields are set to **y.**

```
add trunk-group 200                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                            Maintenance Tests? y

                     Numbering Format: private
                                                   UUI Treatment: service-provider

                                                    Replace Restricted Numbers? y
                                                   Replace Unavailable Numbers? y
```

On **Page 4** of the trunk-group form set the **Support Request History** field to **y**.

```
add trunk-group 200                                               Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n

                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type:
```

5.6. Administer Private Numbering

To ensure that the caller number is correctly presented, the SIP trunk group set up in **Section 5.5** references the private numbering table, use the command **change private-numbering n** where **n** is the number of the private numbering table to be edited. The following values should be set:

- Set **Ext Len** field to **4** this is the length of the extensions that will be using the table
- Set **Ext Code** to match the leading digits of extension ranges to be used
- Set **Trk Grp(s)** to **200** this is the number of the trunk group that will use this entry
- Set **Total Len** to **4** this is the total length of the calling number that will be presented by the trunk group

```
change private-numbering 0                                    Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext Ext              Trk         Private           Total
Len Code             Grp(s)      Prefix            Len
 4  6                200                           4     Total Administered: 1
                                                            Maximum Entries: 540
```

5.7. Save Configuration

Use the **save translation** command to save the Communication Manager configuration. The following screen shows the output of a successful save translation command.

```
save translation

                              SAVE TRANSLATION

           Command Completion Status                              Error Code

           Success                                                0
```

6. Configuring Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured via the System Manager. The procedures include the following areas:

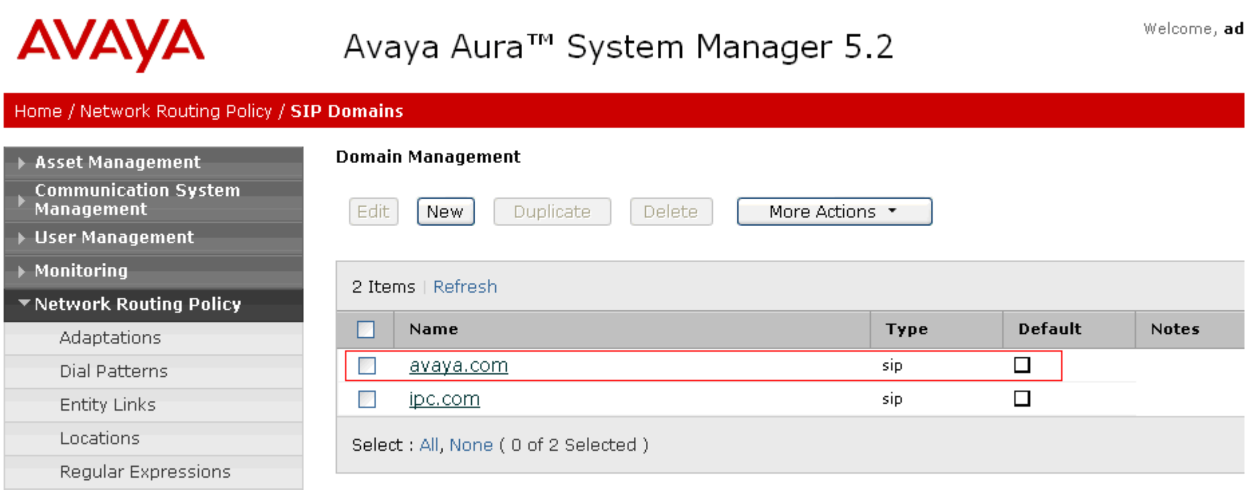
- Log in to Avaya Aura™ System Manager
- Administer SIP domain
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns
- Administer Session Manager

6.1. Log in to Avaya Aura™ System Manager

Access the Avaya Aura™ System Manager using a Web Browser and entering **http://<ip-address>/SMGR**, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials and accept the subsequent Copyright Legal Notice.

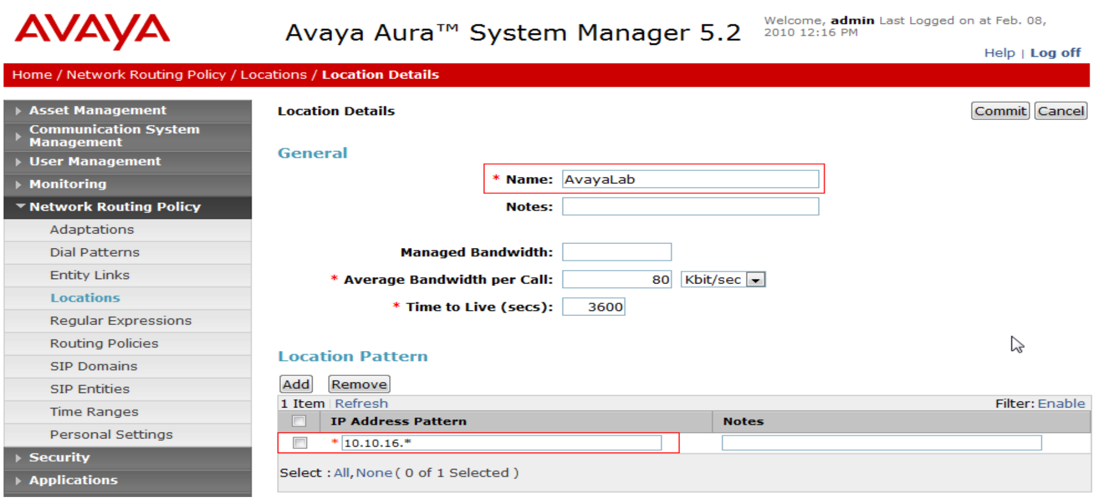
6.2. Administer SIP domain

Add the SIP domains that will be used with Session Manager. Select **SIP Domains** on the left panel menu and click the **New** button (not shown) to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **avaya.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes.



6.3. Administer Locations

To add a Location select **Locations** on the left panel menu and then click on the **New** button (not shown).Under **General,** In the **Name** field enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add,** then enter an **IP Address Pattern** in the resulting new row, '*' is used to specify any number of allowed characters at the end of the string. The following screen shows the location for the Avaya enterprise.

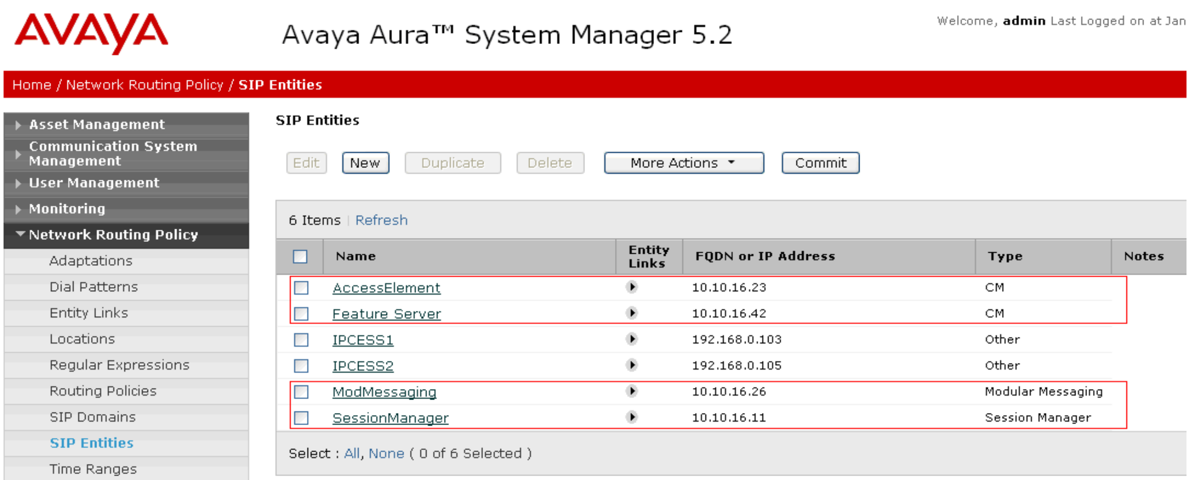


6.4. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity Under **General:**

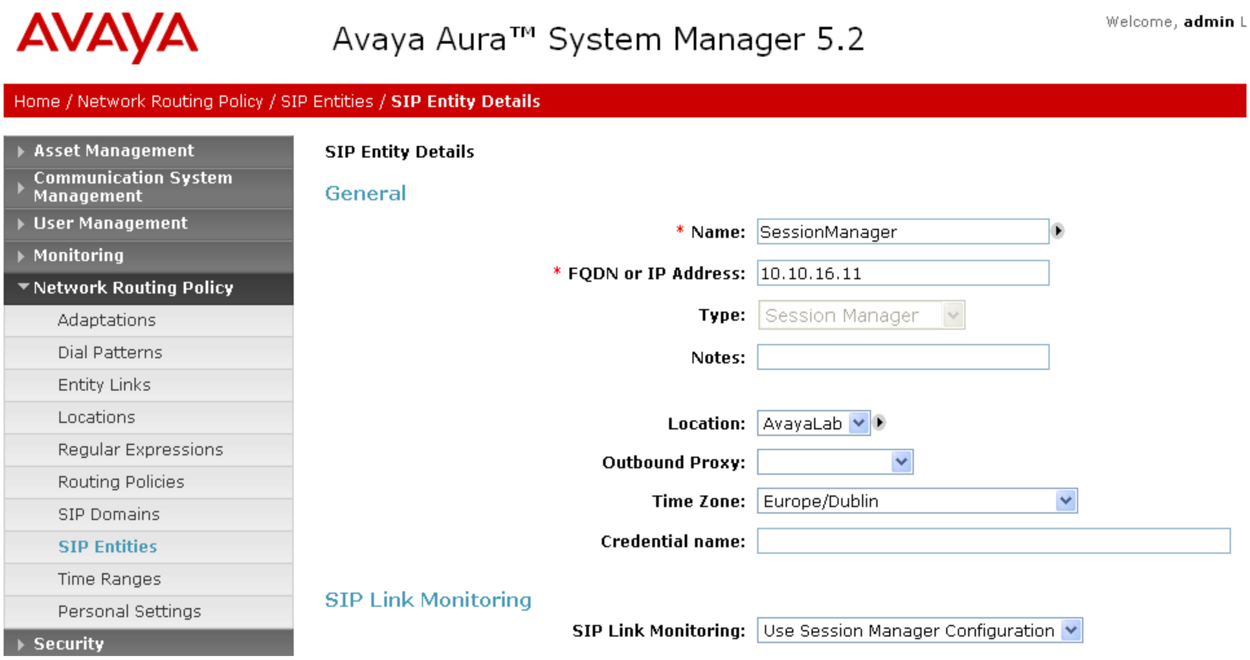
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter an IP address of the SM or the signaling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity or **Modular Messaging** for a Modular Messaging SIP entity
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for this location

In this configuration there are four SIP Entities required which are highlighted below.



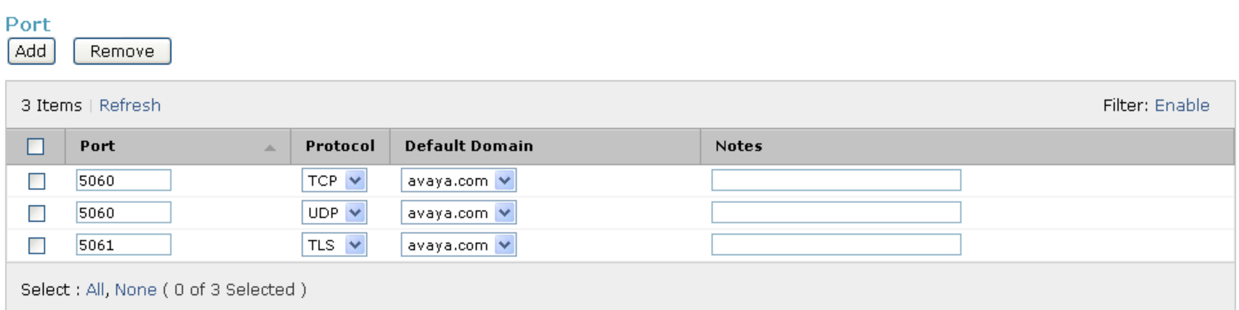
6.4.1. Avaya Aura™ Session Manager SIP Entity

The following screens show the SIP entity for Session Manager.



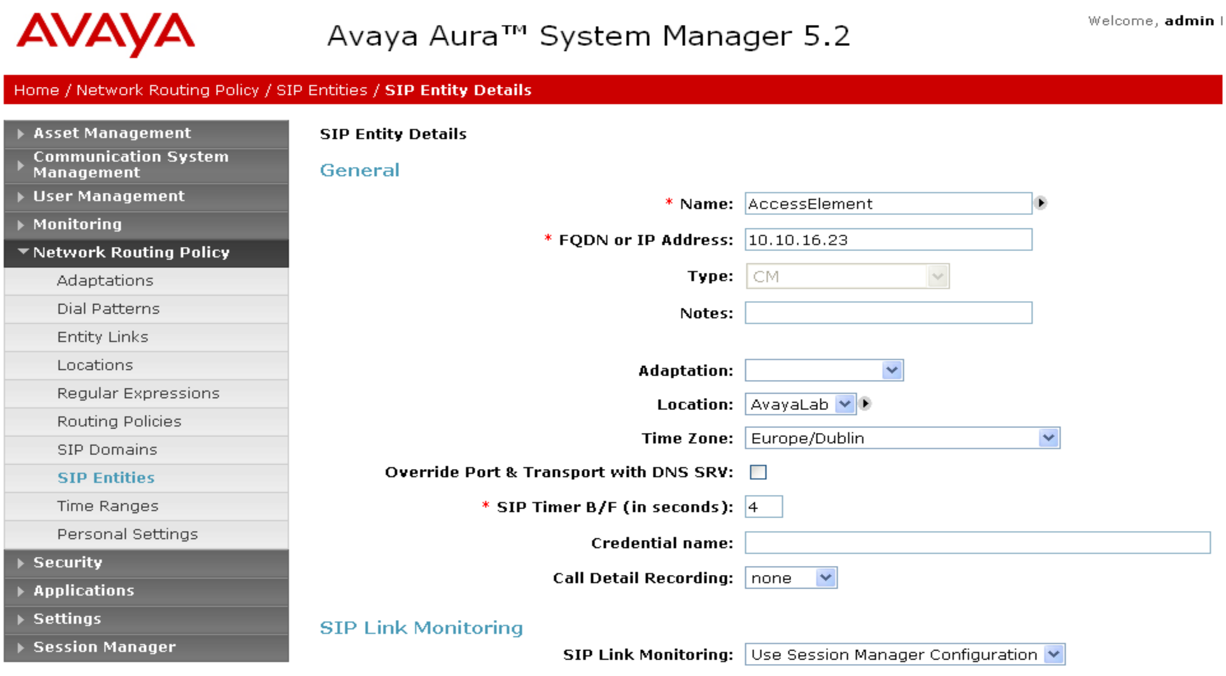
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add,** then edit the fields in the resulting new row

- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field select from the drop down menu the Avaya domain as the default domain

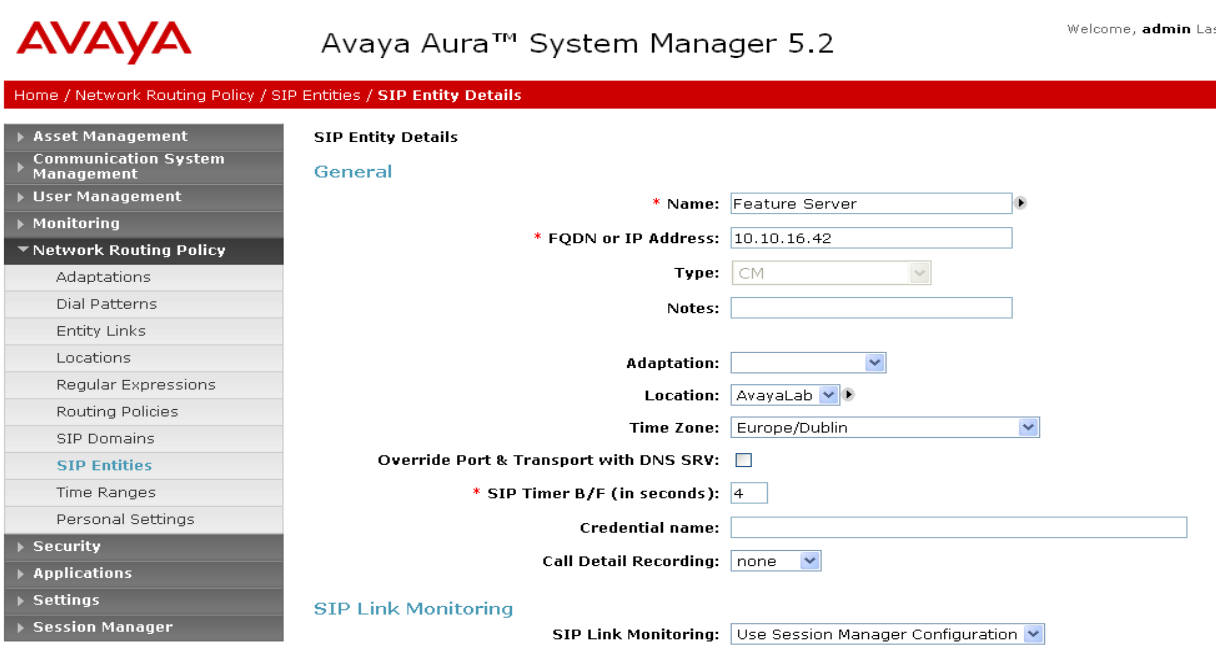


6.4.2. Avaya Aura™ Communication Manager SIP Entities

In this configuration two Communication Manager SIP entities are required. The first SIP entity is for an Access Element, the second SIP entity is for a Feature Server, the Feature Server is only required to service SIP handsets. The following screen shows the SIP Entity for the Access Element.

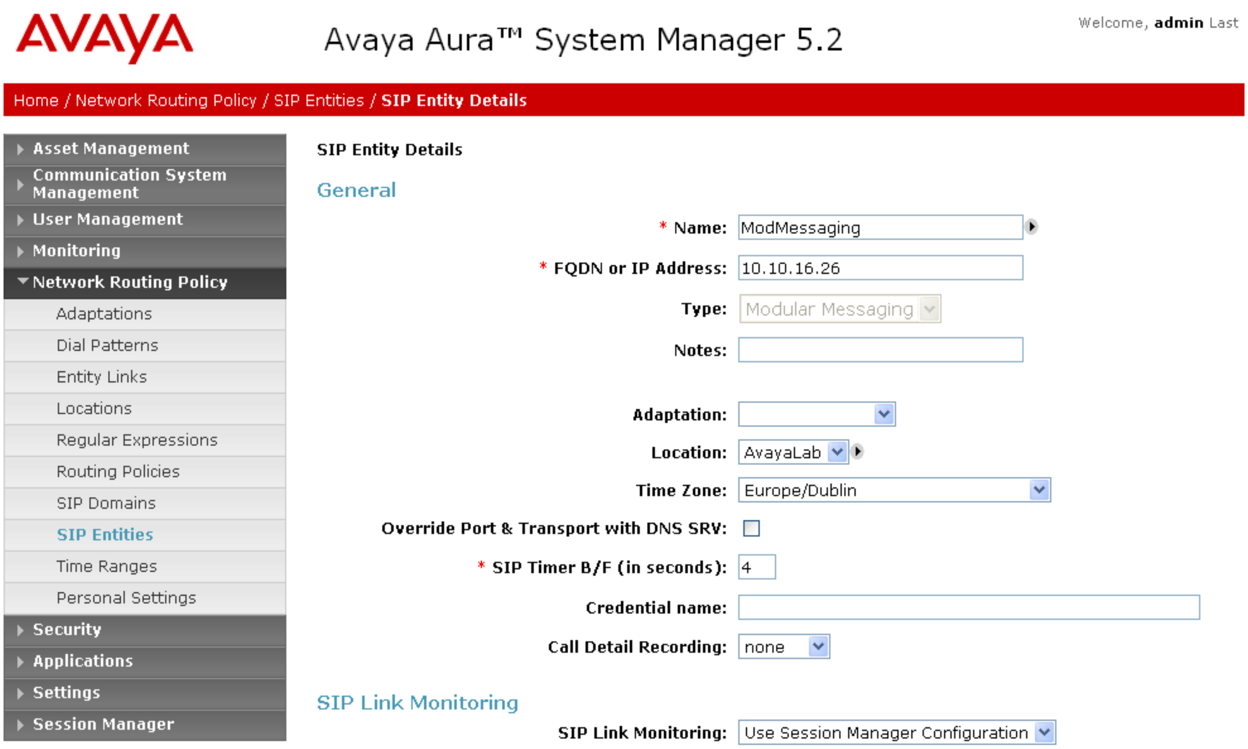


The following screen shows the SIP Entity for the Feature Server Communication Manager.



6.4.3. Avaya Modular Messaging SIP Entity

The following screen shows the SIP Entity for Modular Messaging

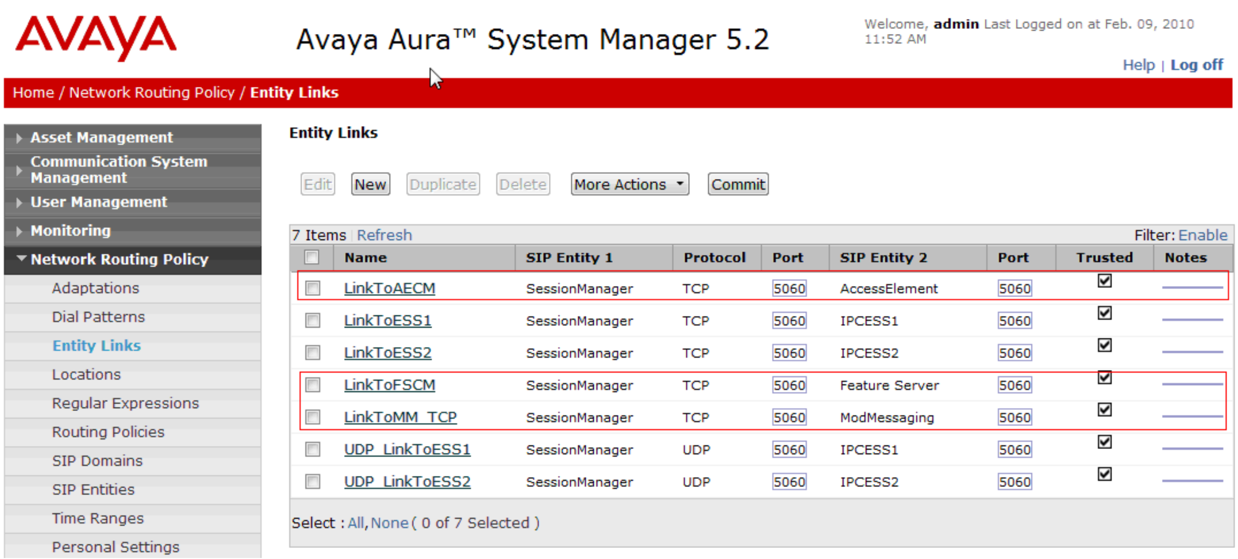


6.5. Administer Entity Links

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

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **SessionManager**
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.4**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- In the **Trusted** field specify whether to trust the other system
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration. An individual entity link must be set up for each combination of port and protocol. In this configuration for transparency during testing port **5060** and **TCP** is used for all entity links, however TLS is recommended for production use.

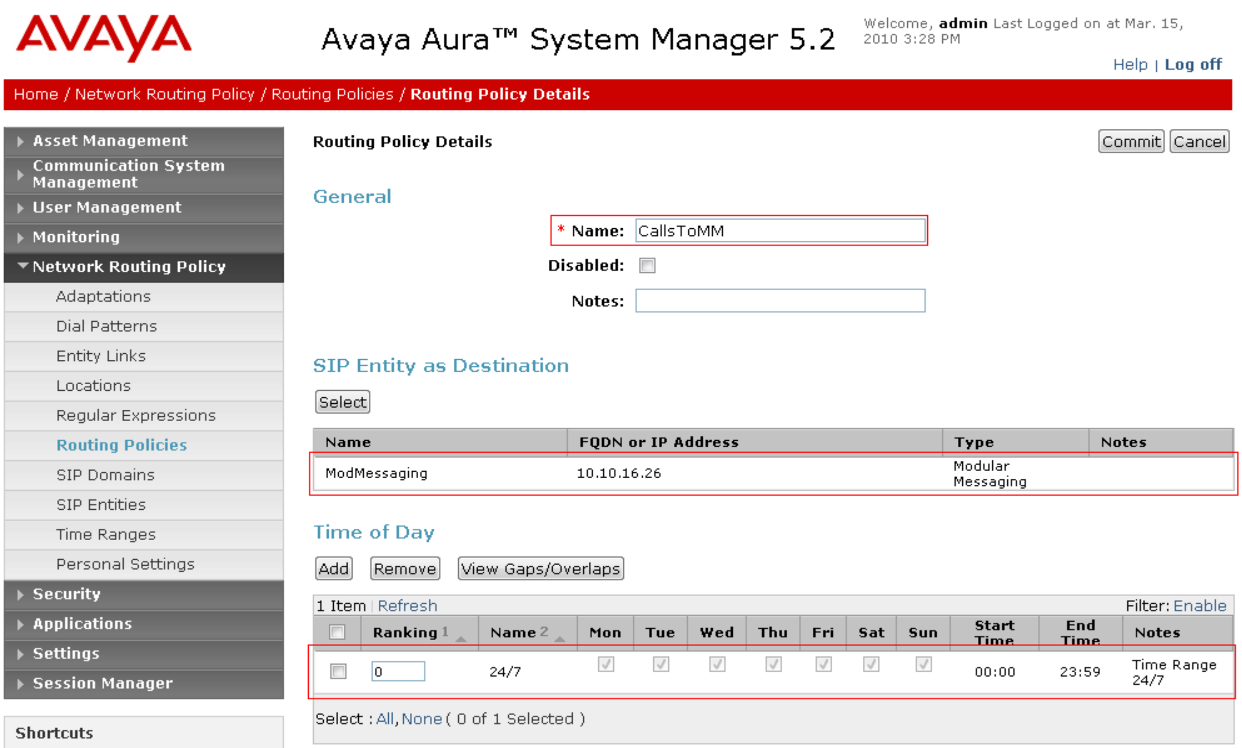


6.6. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

- Under **General** enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies
- Under **Time of Day**, click **Add**, and then select the time range

As an example the following screen shows the routing policy for Modular Messaging



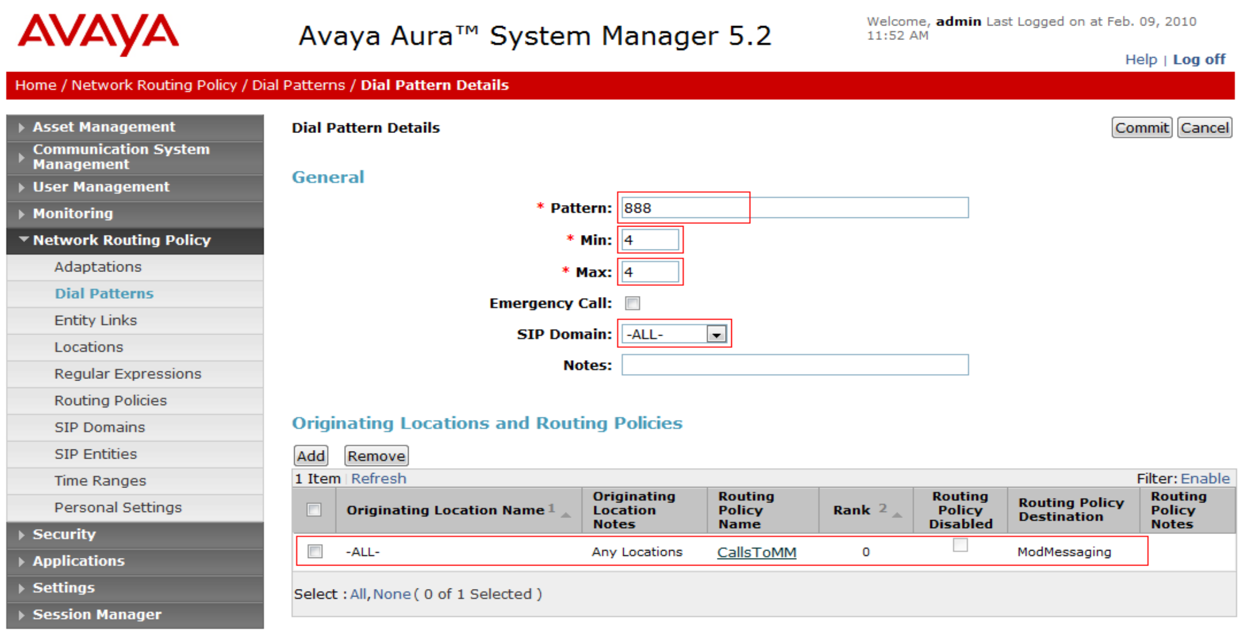
6.7. Administer Dial Patterns

A dial pattern must be defined that will direct calls to the appropriate telephony system. A dial pattern is not needed for SIP extensions as they are registered with the Session Manager and are routed to via an application sequence. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

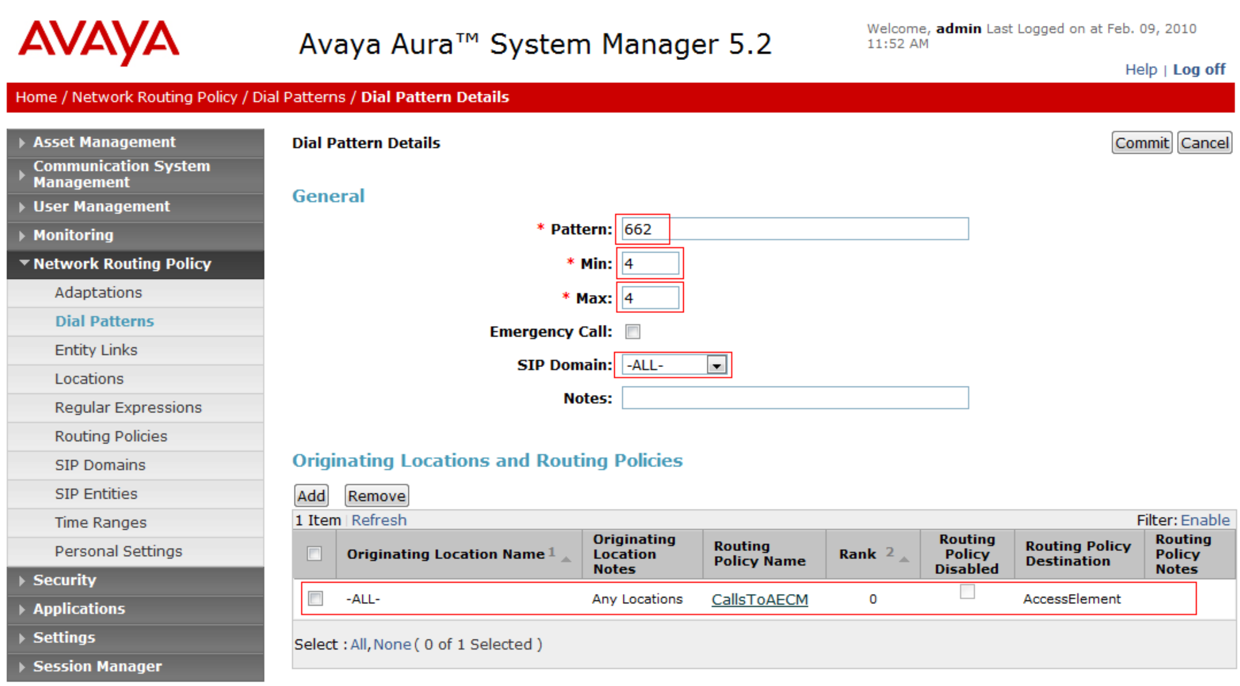
Under **General:**

- In the **Pattern** field enter a dialed number or prefix to be matched
- In the **Min** field enter the minimum length of the dialed number
- In the **Max** field enter the maximum length of the dialed number
- In the **SIP Domain** field select **ALL**

Navigate to **Originating Locations and Routing Policies** and select **Add**, in the resulting screen (not shown). Under **Originating Location** select **ALL** and under **Routing Policies** select **AvayaCM.** Click **Select** button to save. The following screen shows the dial pattern configured for the Modular Messaging pilot number.



The following screen shows the dial pattern configured for the Access Element extensions.



6.8. Administer Feature Server as an Application

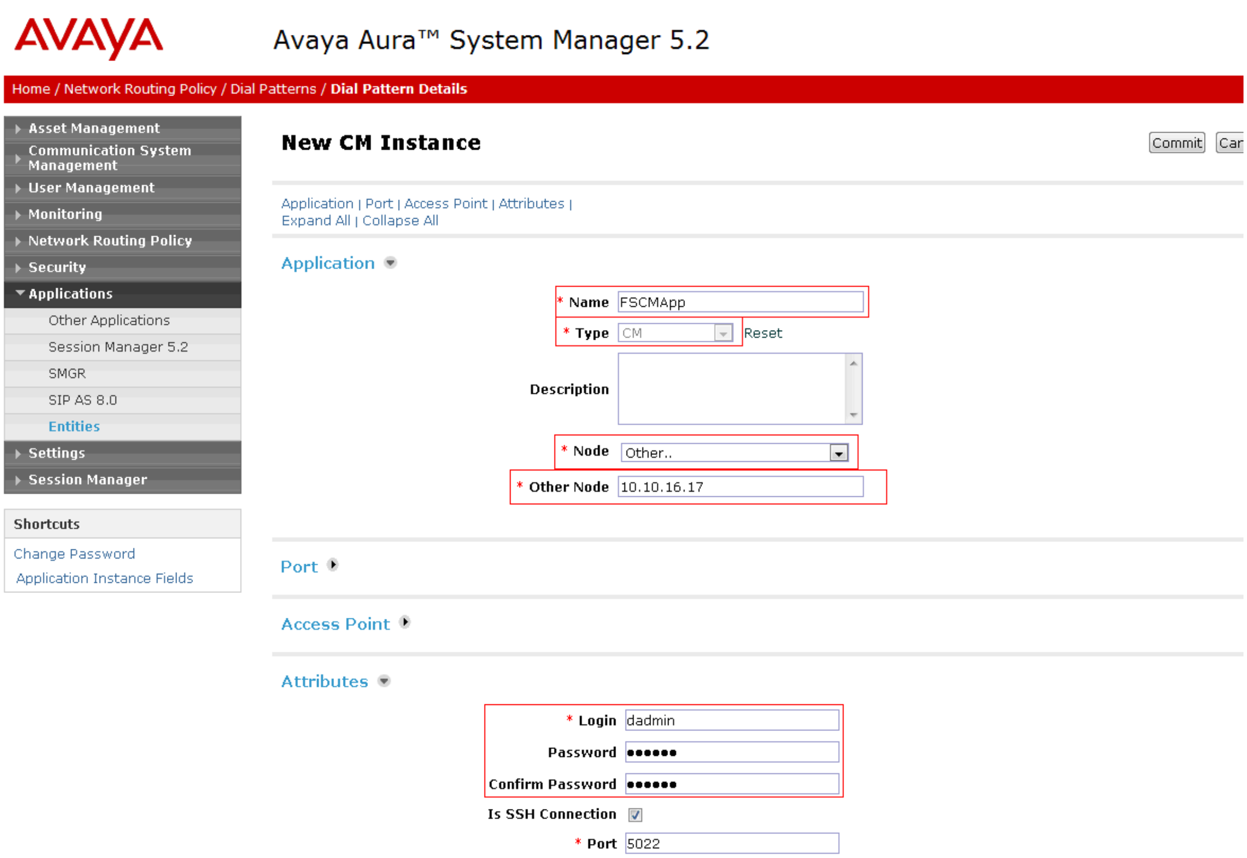
In order for Communication Manager to provide configuration and Feature Server support to SIP phones when they register to Session Manager, the Feature Server must be added as an application. From the left panel menu select **Applications → Entities** and click **New.** Select **CM** for the type of application from the drop down menu (not shown) in the resulting screen under the **Application** heading, enter values in the following fields and use defaults for the remaining fields:

- In the **Name** field enter a descriptive name
- In the **Node** field select **Other** from the drop-down menu
- In the resulting **Other Node field** enter the IP address of the Communication Manager (the IP address that is used for the SAT login).

Under the **Attributes** heading enter values in the following fields and use defaults for the remaining fields:

- In the **Login** field enter a login name for Communication Manager (SAT SSH login)
- In the **Password** field enter Password for Communication Manager (SAT SSH password)

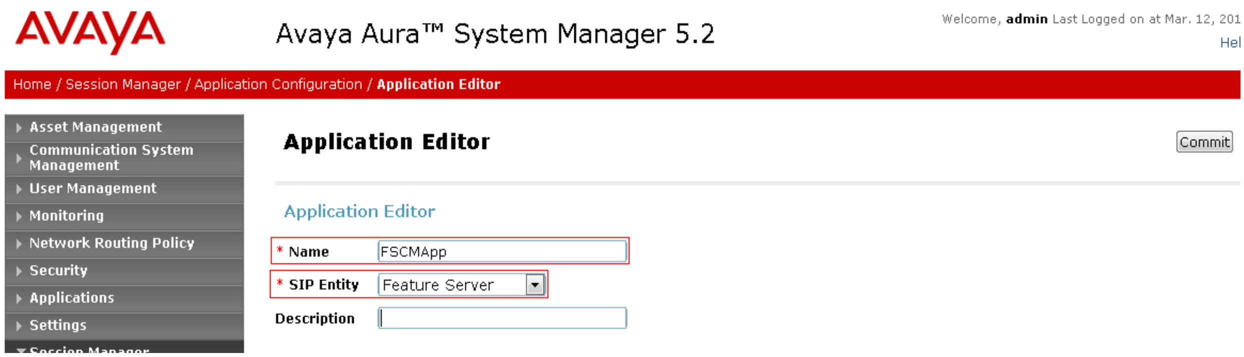
Select **Commit**, this causes System Manager to synchronize with the Communication Manager in the background.



6.9. Create a Feature Server Application

From the left panel menu select **Session Manager → Application Configuration → Applications** and click on **New.** Enter the following fields and use defaults for the remaining fields:

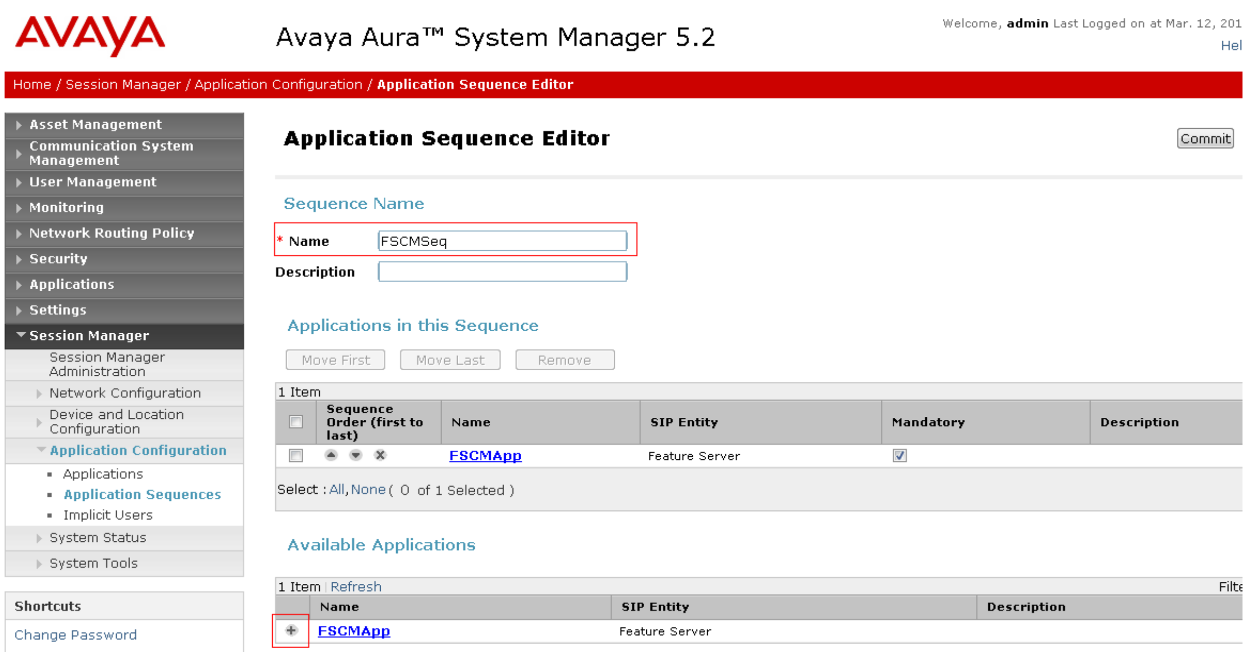
- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Feature Server Communication Manager.
- Select **Commit.**



6.10. Administer Feature Server Application sequence

From the left panel menu select **Session Manager → Application Configuration → Application Sequences** and click on **New.**

- In the **Name** field enter a descriptive name
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes select **Commit**

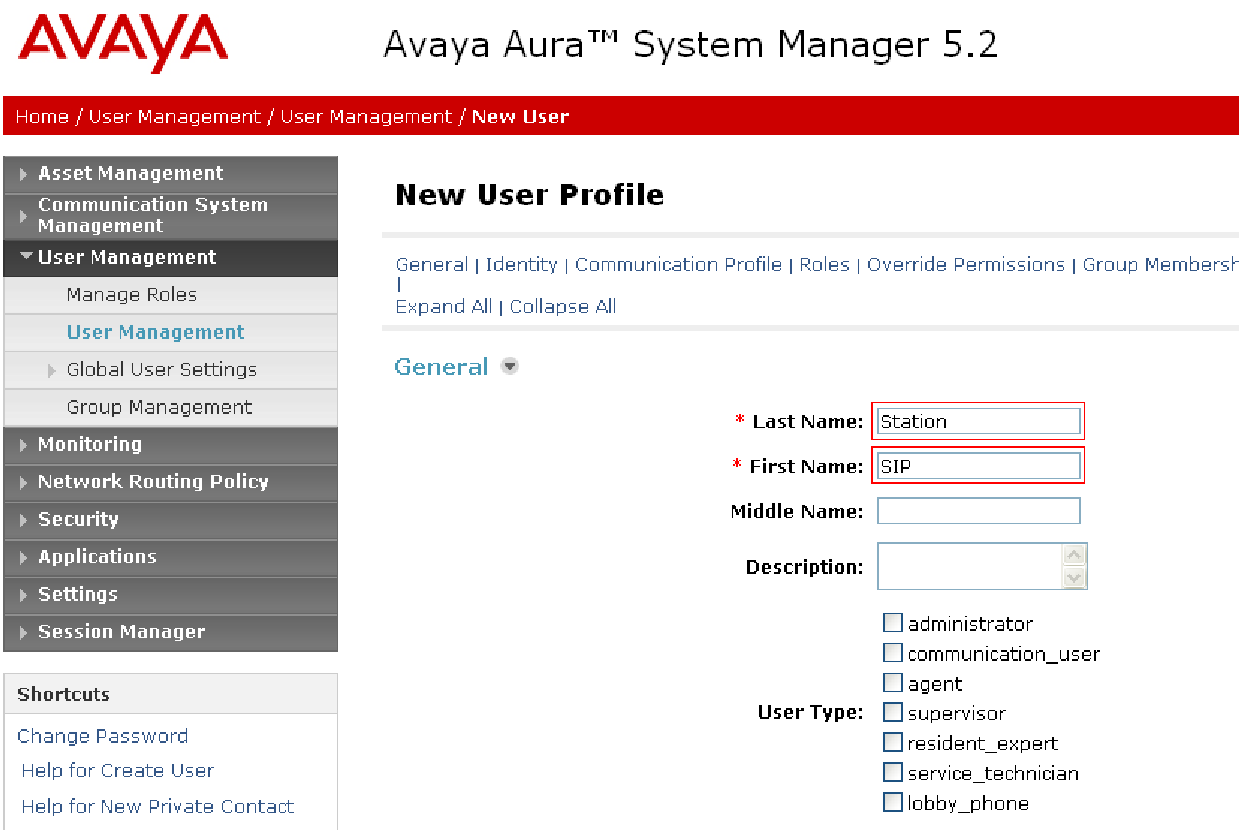


6.11. Administer SIP Extensions

SIP extensions are registered with the Session Manager and use the Feature Server for their feature and configuration settings. To add a SIP user select **User Management → User Management** and select **New**.

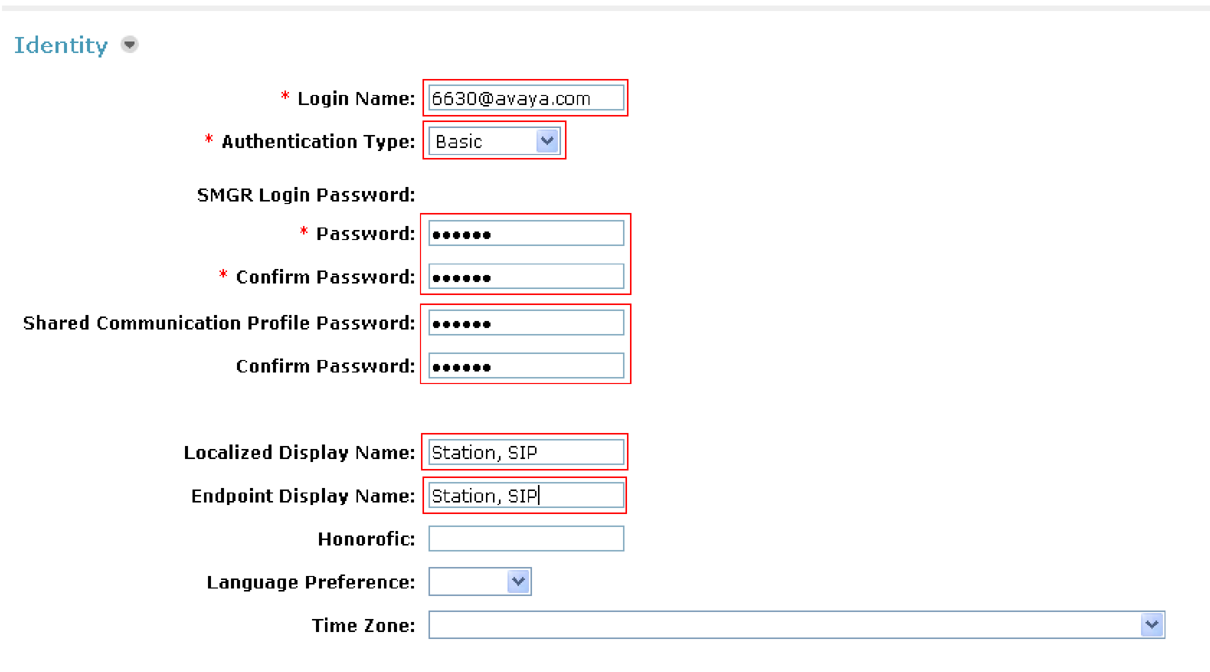
Under the **General** section,

- Enter the user's name in the **Last Name** and **First Name** fields.



Under the **Identity** section,

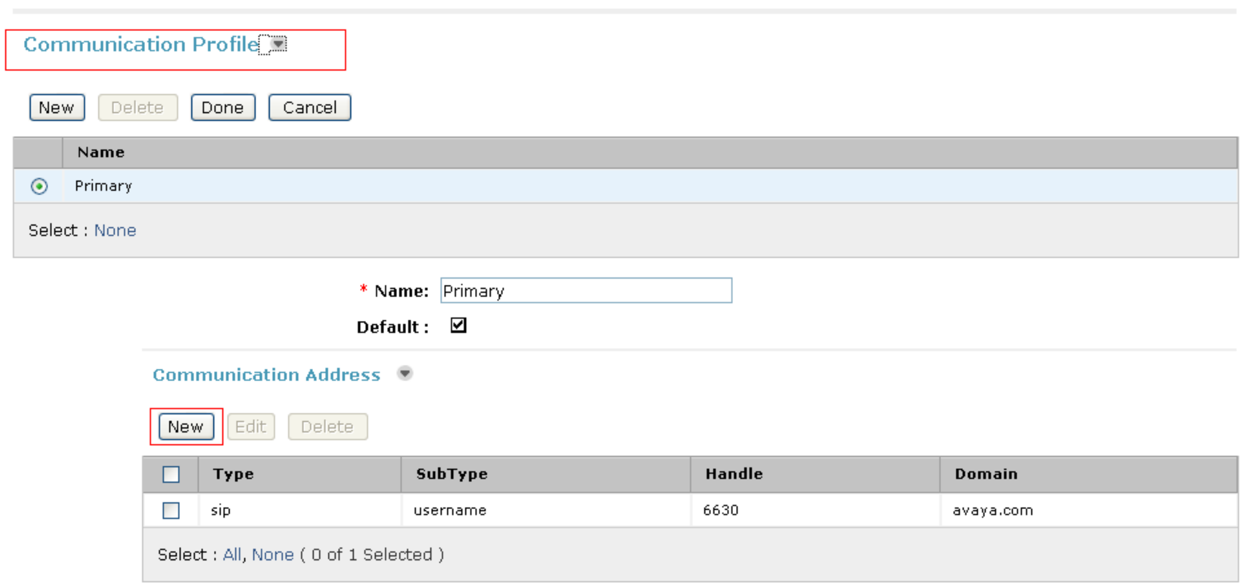
- In the **Login Name** field enter a unique system login name in the form of user@domain (e.g. "6630@avaya.com") where the extension is used to log into the SIP phone.
- The **Authentication Type** should be Basic
- In the **SMGR Login Password** field enter an alphanumeric password and confirm it
- In the **Shared Communication Profile Password** enter a numeric password; this is the password that is used when logging in to the phone
- In the **Localized Display Name** field enter the name to be displayed as the calling party
- Re-enter the name of the user for **Endpoint Display Name**



Click on the show/hide button for **Communication Profile** then Click on the show/hide button for **Communication Address.**

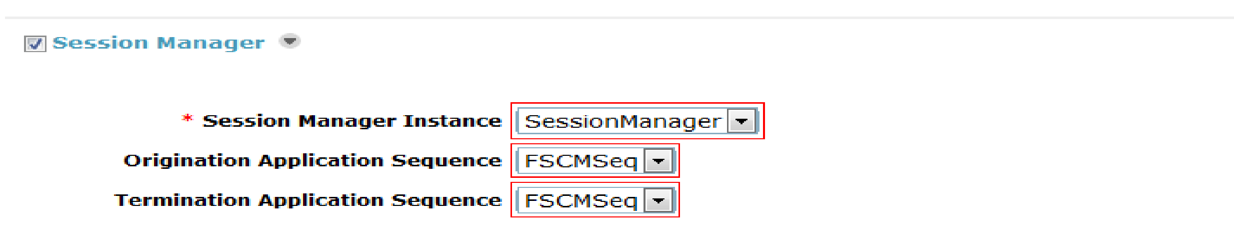
- Select **New** and in the **SubType** field, select username from the drop-down menu
- Click the **New**.button.and in the resulting fields (not shown)
- Select **sip** from the drop-down menu for **Type** if it is not set already
- In the **SubType** field, select **username** from the drop-down menu
- In the **Fully Qualified Address** field, enter an extension number
- Click the **Add** button to commit

The following screen displays a Communication Address once it had been added.



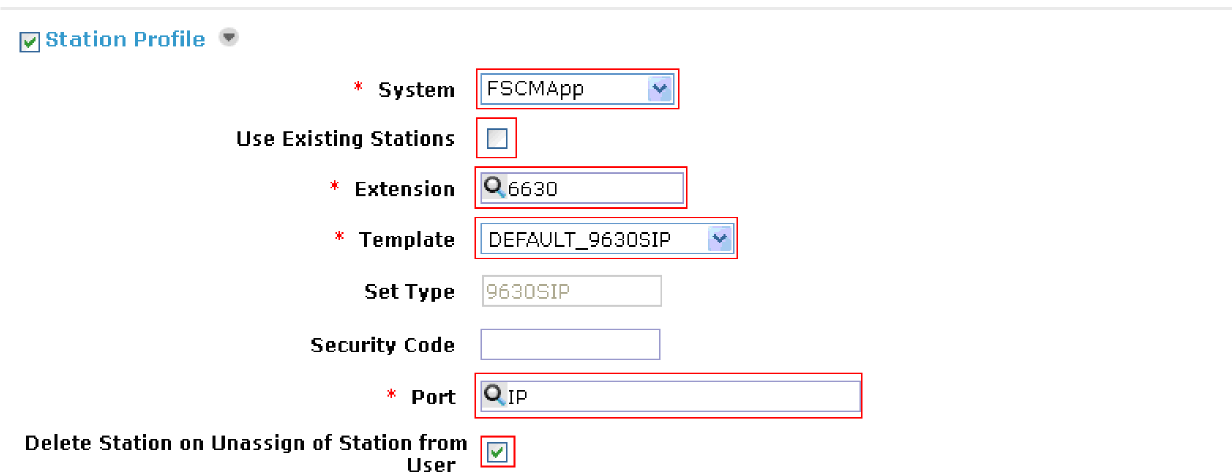
Click the show/hide button next to **Session Manager:**

- Make sure the **Session Manager** check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Session Manager Instance** field
- Select the appropriate application name from the drop-down menu in the **Origination Application Sequence** field
- Select the appropriate application name from the drop-down menu in the **Termination Application Sequence** field



Click the show/hide button next to **Station Profile** and Make sure the **Station Profile** check box is checked.

- Select the Communication Manager application from the **System** drop-down menu
- Ensure that the **Use Existing Stations** check box is not selected
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select IP
- Select the **Delete Station on Unassign of Station from User** box
- Select **Commit** to save changes and the System Manager will add the Communication Manager Feature Server configuration automatically



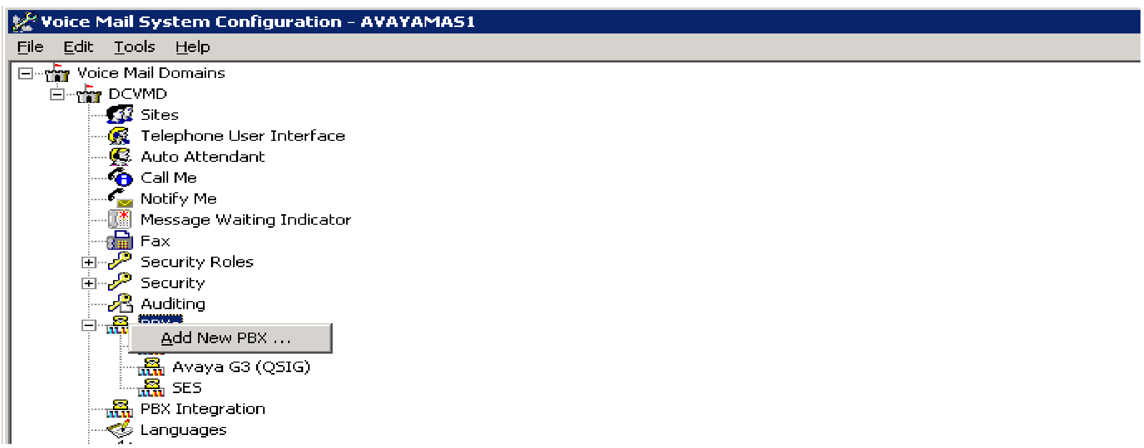
7. Configure Avaya Modular Messaging

This section provides the procedures for configuring Modular Messaging. The procedures include the following areas:

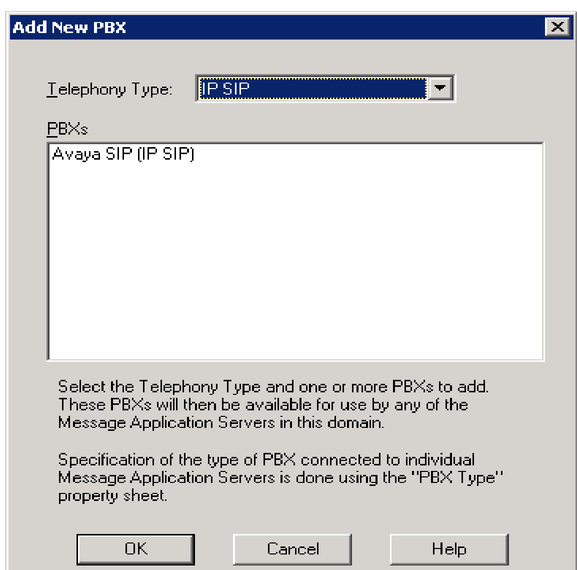
- Configure Avaya Message Application Server
- Configure Avaya Message Storage Server

7.1. Configure Avaya Message Application Server

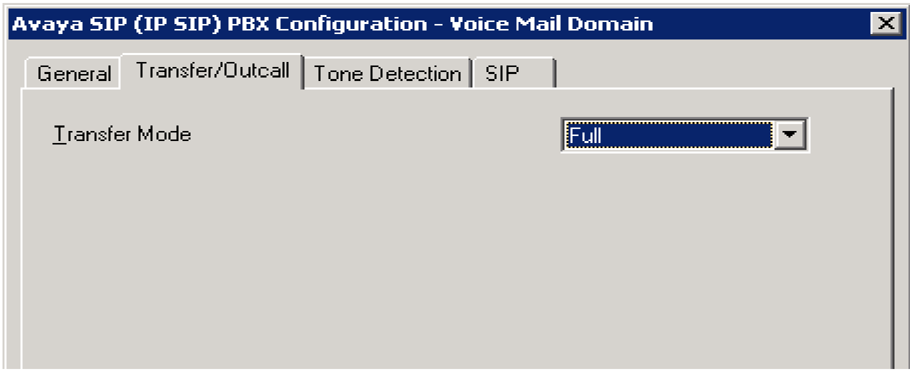
Select **Start** → **Programs** → **Avaya Modular Messaging** →**Voice Mail System Configuration – AVAYAMAS1**. Expand **Voice Mail Domains** and the administered domain name (**DCVMD** in the screenshot below). Right-click on **PBXs** and select **Add New PBX Type…**



On the **Add New PBX** screen, select **IP SIP** from the **Telephony Type** drop down box, then select **Avaya SIP (IP SIP)** from the **PBXs** box. Select **OK** when completed.

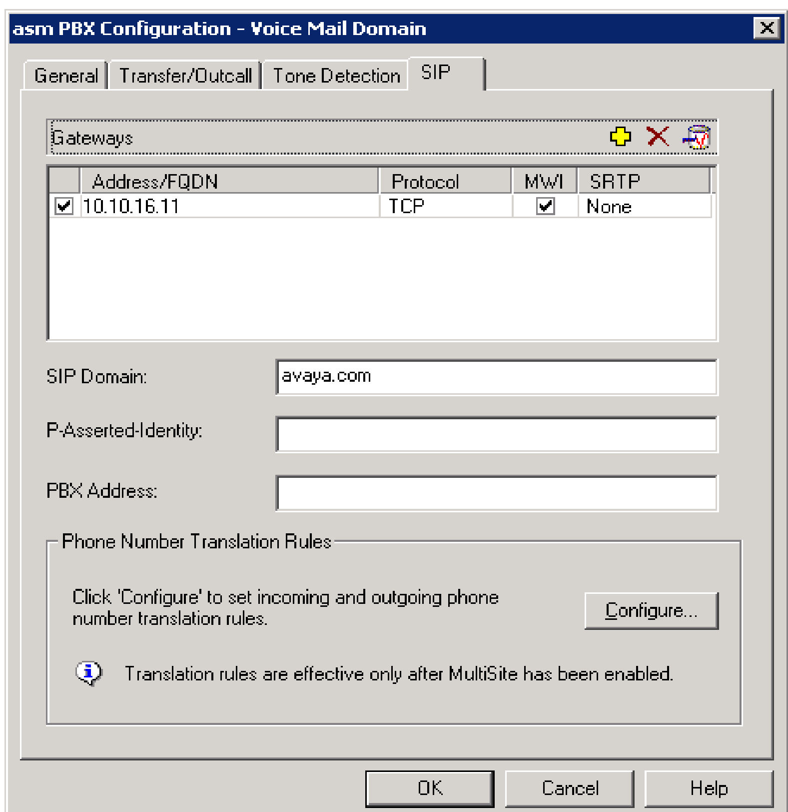


On the **Voice Mail System Configuration – AVAYAMAS1** screen double-click on **PBXs**. On the **Avaya SIP (IP SIP) PBX Configuration** screen, select the **Transfer/Outcall** tab, in the **Transfer Mode** field select **Full** from the drop down menu.

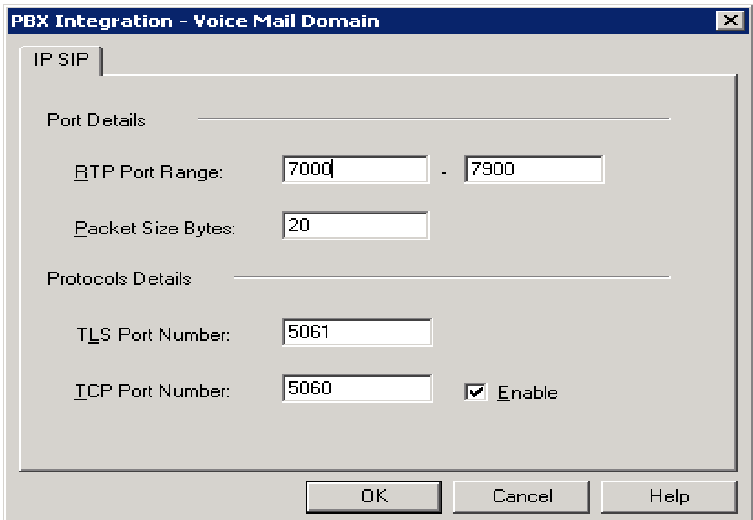


Select the **SIP** tab and enter the following fields.

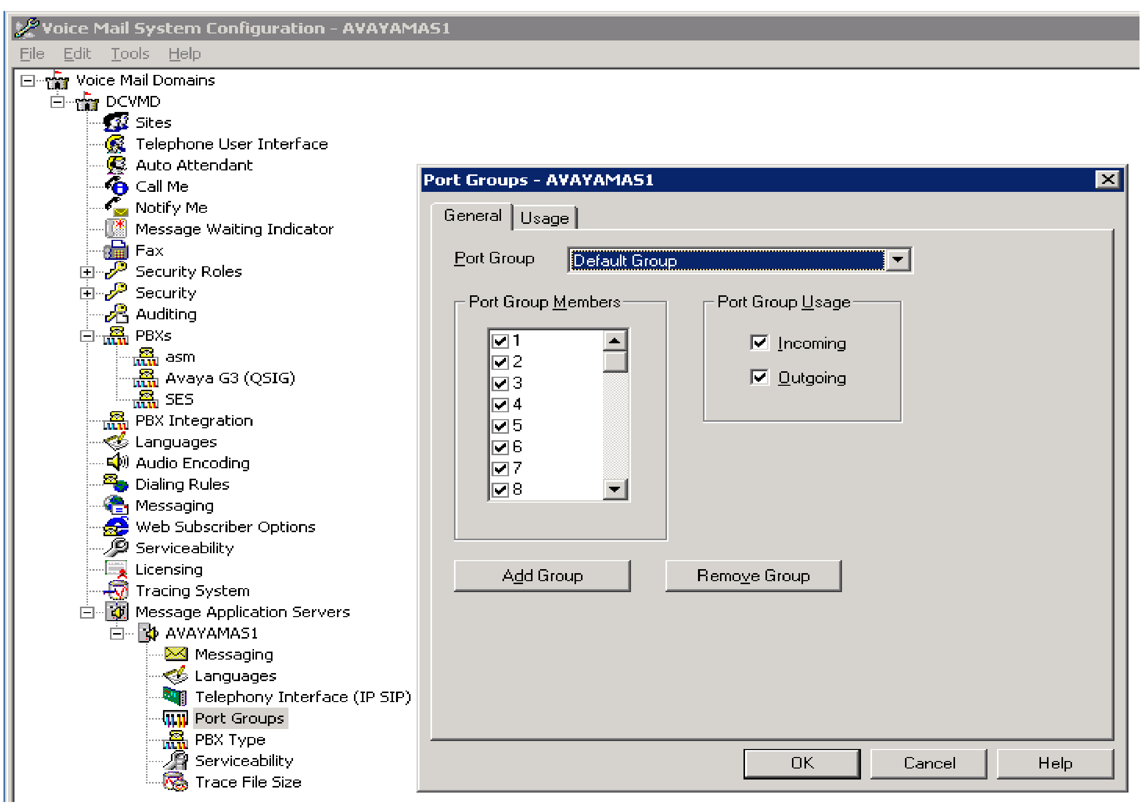
- In the **Address/FQDN** field enter the IP address of the Session Manager interface
- In the **Protocol** field select the protocol Modular Messaging will use for communication to the session Manager
- Select the **MWI** check box
- In the **SIP Domain** field enter the sip domain that is being used by Session Manager and that Modular Messaging will become part of.



On the **Voice Mail System Configuration – AVAYAMAS1** screen, double-click on **PBX Integration**. Confirm the default settings below and check the **Enable** check box if TCP is to be used. Click **OK** when completed.

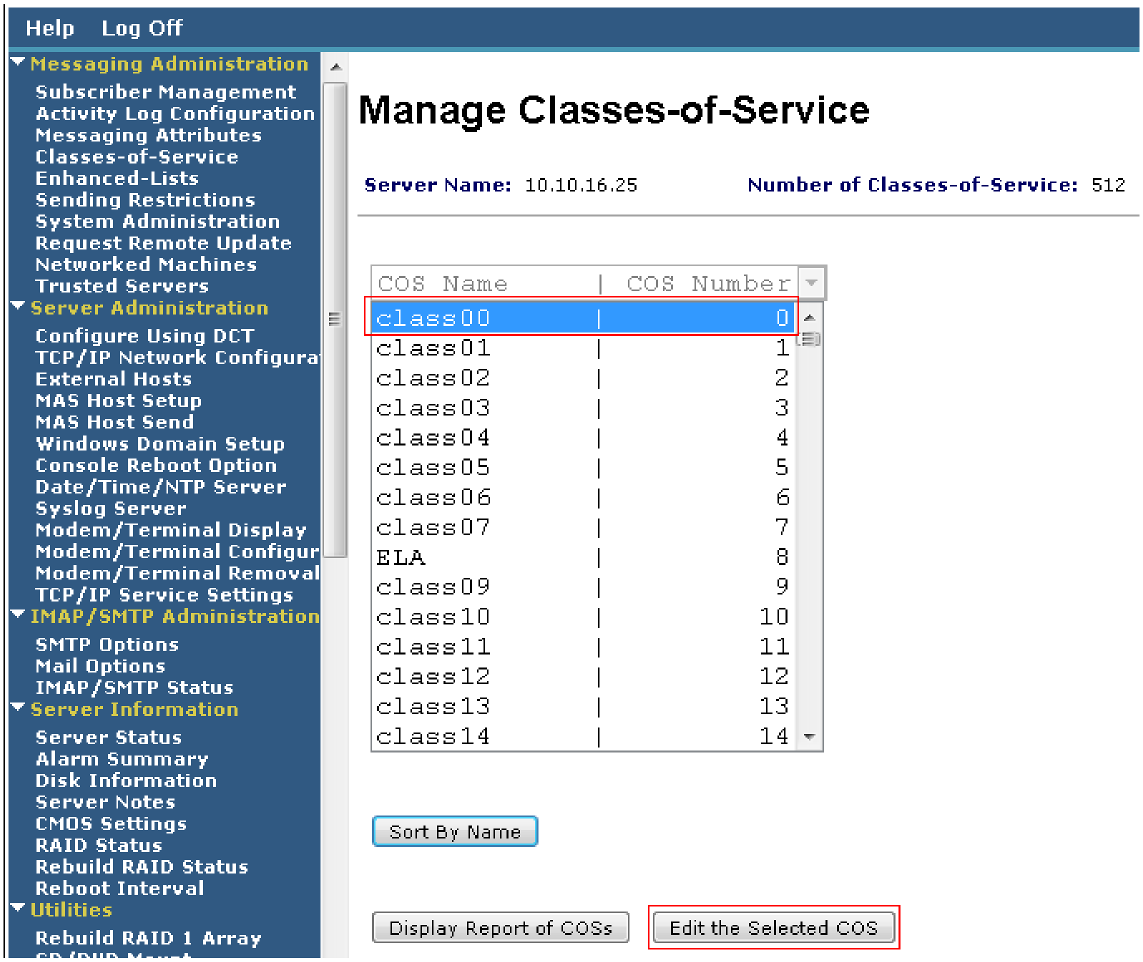


On the **Voice Mail System Configuration – AVAYAMAS1** screen, expand **Message Application Servers** and expand the appropriate MAS server. Double click **Port Groups** and confirm all the **Port Group Members** and both the **Incoming** and **Outgoing** check boxes are selected.

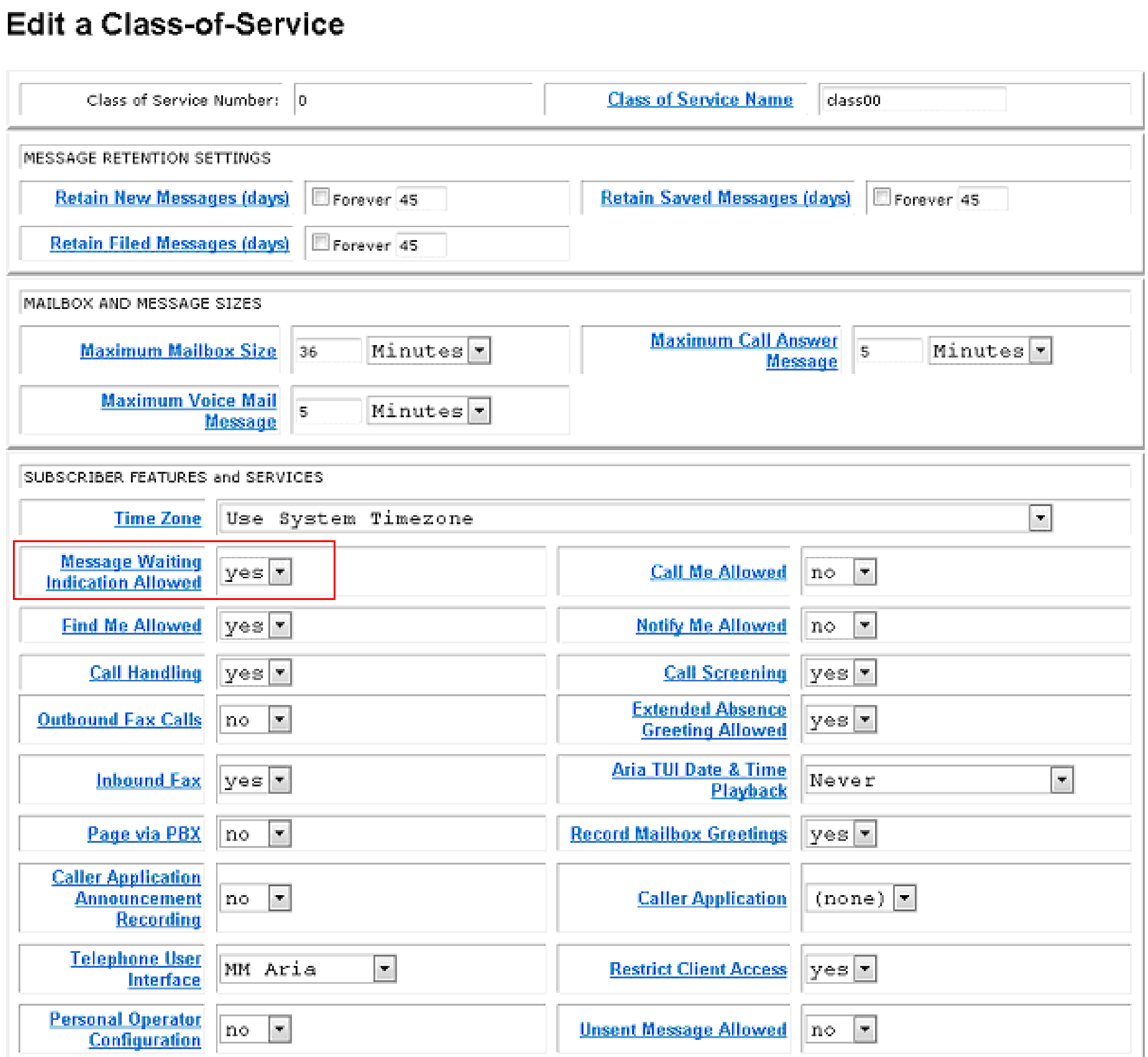


7.2. Configure Avaya Message Storage Server

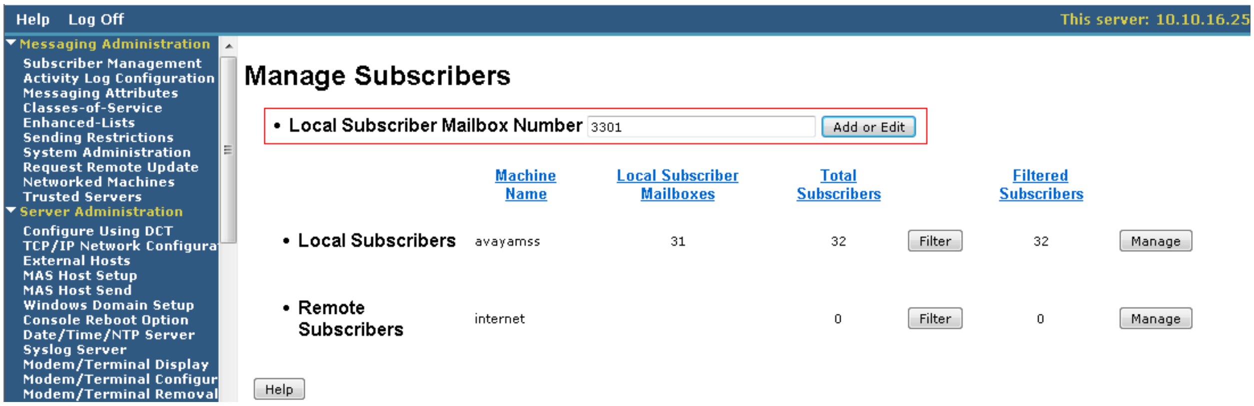
From a Web browser, navigate to **http://<ip-addr>** where **<ip-addr>** is the IP address of the Avaya MSS. After logging in with an appropriate login and password, the main page appears. (not shown). Select **Messaging Administration → Classes-of-Service** from the left pane. From the **Manage Classes-of-Service** screen that is presented, select a Class of Service (COS) that will be used by subscribers using IPC turrets (in this example **class00** is selected).



Click **Edit the Selected COS** button on **Step 2**. In the **Edit a Class-of-Service** screen that follows, select **yes** from the drop-down menu for the **Message Waiting Indication Allowed** field. Scroll down to the bottom of the screen and click the **Save** button (not shown).



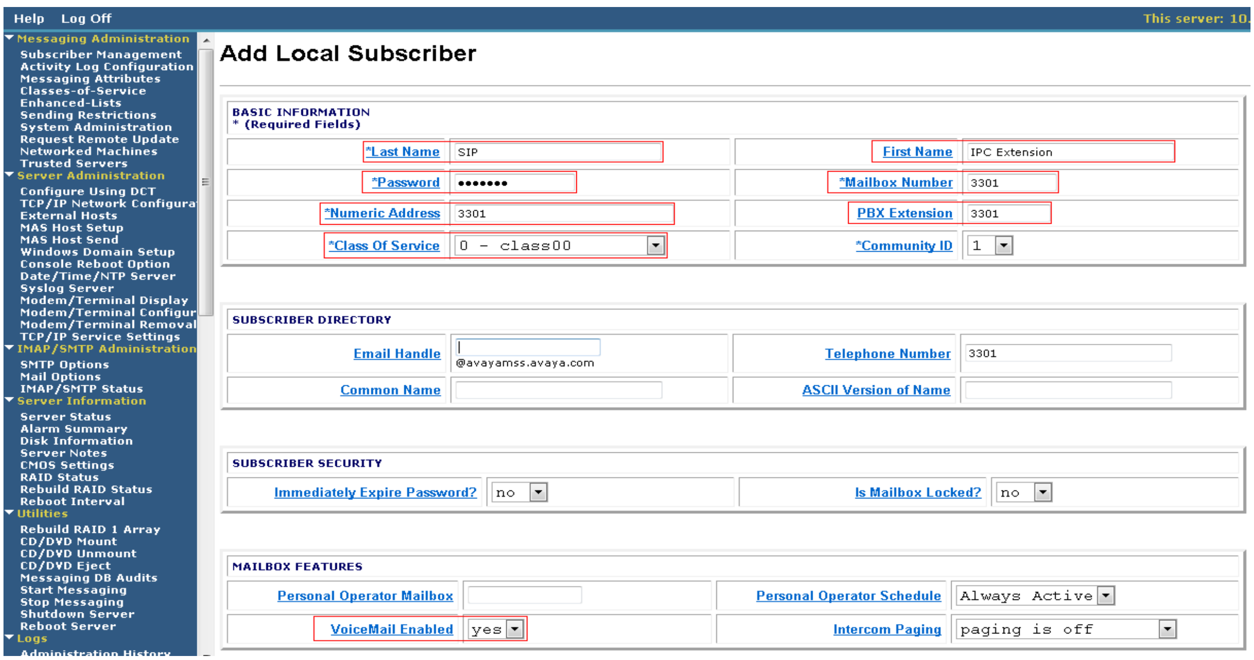
Select **Messaging Administration → Subscriber Management** in the left pane. The **Manage Subscribers** page appears, as shown below. In the **Local Subscriber Mailbox Number** field, enter the extension of the desired IPC turret or Avaya extension and click the **Add or Edit** button.



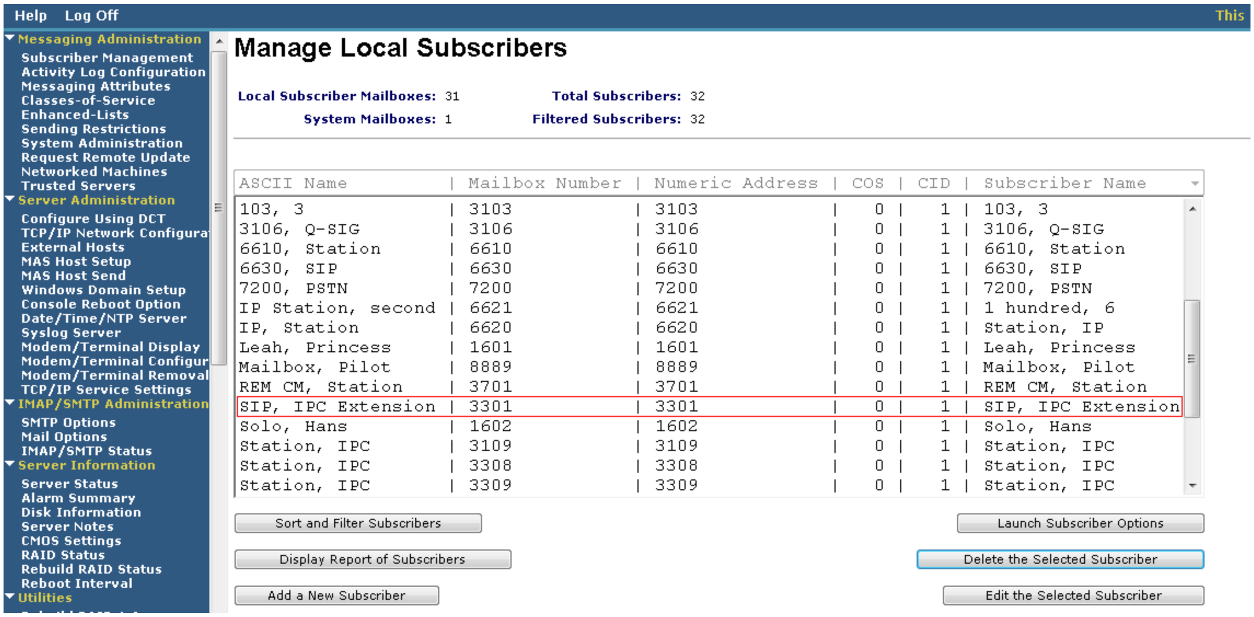
In the **Add Local Subscriber** screen, fill in the required fields, in this example, IPC extension 3301 is used:

- For **Last Name** and **First Name** fields enter values appropriate for the user
- **Password**: Enter a default password for accessing the subscriber's mailbox, from 1 to 15 digits
- **Mailbox Number**: Enter a number, from 2 to 10 digits in length, which uniquely identifies the mailbox for the purpose of logging in or addressing messages. It must be within the range of Mailbox Numbers assigned to this system and be a valid length on the local machine
- **Numeric Address**: Enter a unique address in the voice mail network
- **Class of Service**: Select the Class of Service
- **VoiceMail Enabled**: verify it is set to **yes**

Repeat this step for all IPC extensions.



To verify that mailboxes have been created, select **Messaging Administration → Subscriber Management**, click the **Manage** button to the right of the **Local Subscribers** entry. In the resulting **Manage Subscribers** screen that is presented (see below), verify that the mailboxes created appear in the list of subscribers.



8. General Test Approach and Test Results

A simulated enterprise site using an Avaya IP telephony solution was connected to IPC via an E1-QSIG connection provisioned between Communication Manager and IPC's Alliance MX. The compliance test included the following:

- Incoming calls to the Avaya telephones, calls were made from IPC turrets to Avaya SIP, H.323, digital and analog telephones within the enterprise.
- Outgoing calls from the Avaya telephones, calls were made from Avaya SIP, H.323, digital and analog telephones to IPC turrets
- Calls using G.729A, G.711MU, and G.711A codecs.
- DTMF transmission using RFC 2833 with successful Voice Mail navigation
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones.
- Voicemail coverage and retrieval for endpoints at the enterprise sites.

The following is a list of items that were observed during compliance testing:

- Occasional failures were encountered when diverting a call to Modular Messaging, where the diverting party is a Communication Manager SIP user. This is being investigated by the Avaya team.
- In some instances of the more complex call scenarios for multiple diversions and/or transfers between the two enterprises where the final diversion is to Modular Messaging,

inconsistencies were encountered regarding which mailbox terminates the call. For example, depending on the specific scenario being run, the mailbox for the last called party mail box is reached, while in other scenarios, the mail box for the initial called party is reached. These inconsistencies are being investigated by the Avaya team.

- Connected name/number privacy is lost when invoked by called party, where the calling party is a Communication Manager SIP user. SIP user sees the connected name and number. This is being investigated by the Avaya team.
- Occasional failures of Communication Manager User screen display updates were encountered when various transfers scenarios between the two enterprise solutions where executed. This is being investigated by the Avaya team.
- Issues were encountered when using the Auto attendant function provided by Modular Messaging. Call failures were seen when Auto attendant transferred calls between two enterprise users. This is being investigated by the Avaya team

These items were not deemed significant to fail the solution, and are listed here for user awareness. Testing of the sample configuration was completed with successful results for the IPC QSIG architecture.

9. Verification Steps

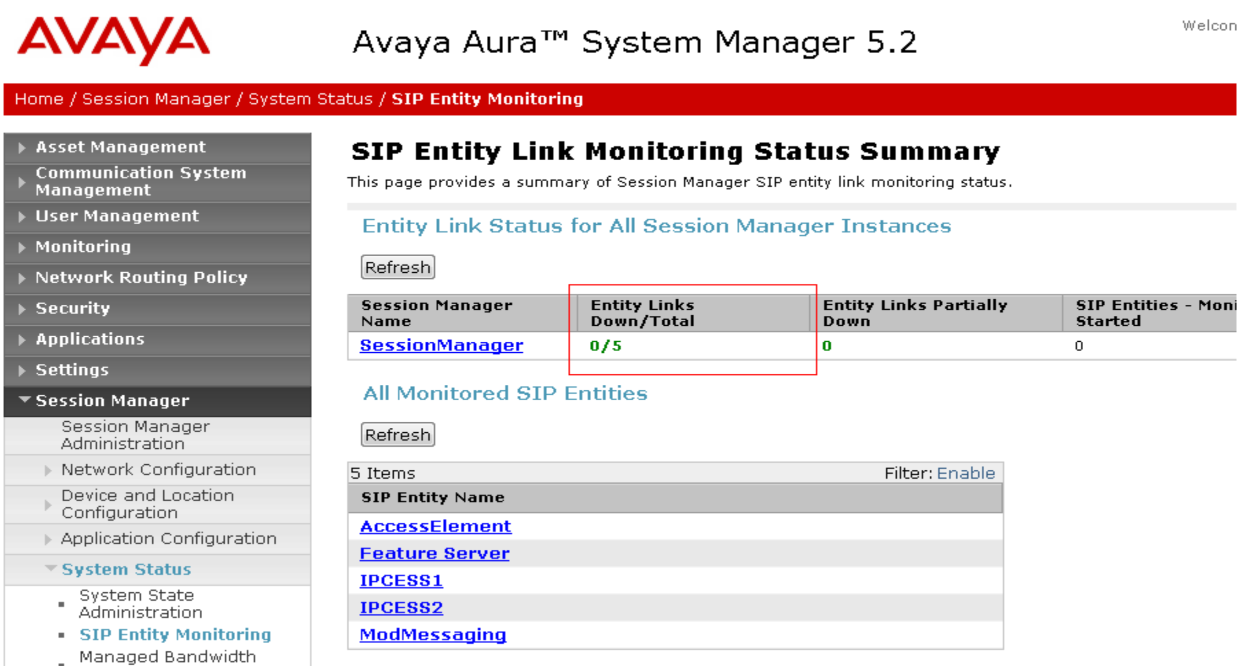
The following steps can be used to verify that the required configuration has been correctly administered to support IPC QSIG architecture. To verify that any of the trunk groups are up, from the Avaya Communication Manager SAT use the **status trunk n** command, where **n** is the number of the trunk group. (Refer to **Sections 4.8, 4.9** and **5.5** for trunk details). Verify for each trunk, that the **Service State** shows in-service/idle.

```
                              TRUNK GROUP STATUS

Member    Port      Service State       Mtce Connected Ports
                                        Busy

0003/001 01A0601   in-service/idle      no
0003/002 01A0602   in-service/idle      no
0003/003 01A0603   in-service/idle      no
```

To ensure that all of the configured SIP entites and their associated links are in service from the system manager web interface click on **Session Manager → System Status → SIP entity monitoring.** Check that zero links are reported down under the **Entity Links Down/Total** heading.



To confirm routing between all devices a number of calls should be made.

- Make a call from an Access Element extension to Feature Server extension and vice versa to confirm routing between them
- Make a call from an Access Element extension to and IPC extension and vice versa to confirm routing between them

- Make a call from a Feature Server extension to an IPC extension and vice versa to confirm routing between them
- Make a call from an Access Element extension to Feature Server extension and vice versa to confirm routing between them
- Make a call from an Access Element extension to Modular Messaging to confirm routing between them
- Make a call from a Feature Server extension to Modular Messaging to confirm routing between them
- Make a call from an IPC extension to Modular Messaging to confirm routing between them

10. Conclusion

These Application Notes describe the steps required to successfully configure the Avaya components to successfully interoperate with IPC QSIG architecture using QSIG as the transport method between the two enterprises. The Avaya Enterprise components include Avaya Aura™ Communication Manager Access Element, Avaya Aura™ Communication Manager Feature Server, Avaya Modular Messaging, Avaya Aura™ System Manager and Avaya Aura™ Session Manager.

11. Additional References

This section references the Avaya and other external documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Avaya Aura™ Communication Manager Special Application Features, 10-Nov-2009*

[2] *Administering Avaya Aura™ Communication Manager, 04-May-2009,* Document Number 03-300509

[3] *SIP Support in Avaya Aura™ Communication Manager Running on the Avaya S8xxx Servers 04-May-2009*, Document Number 555-245-206

[4] *Administering Avaya Aura™ Communication Manager as a Feature Server, 29-Jan-2010*

[5] *Administering Avaya Aura™ Session Manager, 20-Noc-2009*

[6] *Modular Messaging Release 5.1 with the Avaya MSS - Messaging Application Server (MAS) Administration Guide, 29-Jun-2009*

[7] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/

[8] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

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.