Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunking Using Nectar Services Enterprise Session Management and Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services Within the Midsize Business Template – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the Nectar Services Enterprise Session Management and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura™ SIP Enablement Services and Avaya Aura™ Communication Manager as part of the Midsize Business Template. The Midsize Business Template is a packaging of several Avaya applications running on a single server including Communication Manager and SIP Enablement Services. These Application Notes are also applicable for Communication Manager and SIP Enablement Services running on standalone servers.

Nectar Services is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Nectar Services Enterprise Session Management (ESM) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura™ SIP Enablement Services (SES) and Avaya Aura™ Communication Manager as part of the Midsize Business Template (MBT). The Midsize Business Template is a packaging of several Avaya applications running on a single server including Communication Manager and SES. These Application Notes are also applicable for Communication Manager and SES running on standalone servers.

Customers using this Avaya SIP-enabled enterprise solution with ESM are able to place and receive PSTN calls via a dedicated broadband Internet connection and the SIP protocol. This converged network solution is an alternative to traditional analog and digital PSTN trunks generally resulting in lower cost for the enterprise.

1.1. Interoperability Compliance Testing

A simulated enterprise site using Communication Manager and SES was connected to the public Internet using a dedicated broadband connection. The enterprise site was configured to connect to ESM.

To verify SIP trunking interoperability, the following features and functionality were covered during the compliance test:

- Incoming PSTN calls to various phone types.
  Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types.
  Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator soft clients.
  Avaya one-X Communicator supports both H.323 and SIP, as well as Road Warrior and Telecommuter modes. Clients using each protocol in each mode were tested.
- Various call types were tested including: local, long distance, international, and outbound toll-free.
- Calls using G.729A, G.711MU, and G.711A codecs.
- Caller ID presentation and Caller ID restriction.
- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and Extension to Cellular (EC500).
- T.38 Fax.

- Direct IP-to-IP media (also known as “media shuffling”) with SIP and H.323 telephones. This allows IP endpoints to send audio (RTP) packets directly to each other without using media resources on the Avaya Media Gateway.

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls (911) are supported but were not tested as part of the compliance test.
- Operator services and directory assistance calls are not supported.

This solution requires media shuffling be disabled on the SIP trunk to the service provider to support the Communication Manager Extension to Cellular (EC500) feature and the Avaya one-X Communicator SIP client in Telecommuter mode.

Please refer to Section 8 for complete test results, observations and any necessary workarounds.

1.2. Support

For technical support on ESM, contact Nectar Services using the contact link at www.nectarcorp.com.

2. Reference Configuration

Figure 1 illustrates an example Avaya SIP-enabled enterprise connected to ESM. This was the configuration used for compliance testing.

The Avaya components used to create a simulated customer site included:

- Avaya S8510 Server running the Midsize Business Template
  - Avaya Aura™ Communication Manager
  - Avaya Aura™ SIP Enablement Services
  - Avaya Aura™ Communication Manager Messaging (voicemail)
  - Media Services (media resources for IP endpoints)
- Avaya G450 Media Gateway (no S8300 Server)
- Avaya 1600 Series IP Telephones (H.323)
- Avaya 4600 Series IP Telephones (H.323)
- Avaya 9600 Series IP Telephones (H.323 and SIP)
- Avaya one-X Communicator (H.323 and SIP soft client)
- Avaya analog and digital telephones
- Fax machines

In **Figure 1**, the H.323 endpoints register to Communication Manager and get their media resources from Media Services. The Avaya G450 Media Gateway is only needed to provide connectivity to the analog and digital endpoints. The SIP endpoints register with the SES.

For the purposes of the compliance test, the simulated enterprise site was configured using all public IP addresses so that all devices could communicate directly with the public IP address of the service provider. However, in these Application Notes, these public IP addresses have been replaced with private addresses for security reasons. Any references to real routable PSTN numbers have also been changed to numbers that can not be routed by the PSTN.

In an actual customer configuration, the enterprise site may also include additional network components between the SES and the service provider, such as a session border controller or data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that traffic must be allowed to pass between the service provider and the following enterprise components:

- SIP traffic to/from the SES
- RTP traffic to/from VOIP media resources in the Midsize Business Template Media Services or Avaya Media Gateways (e.g. MedPro circuit packs in the Avaya G650 Media Gateway or on-board integrated VOIP resources in the smaller gateways)
- RTP traffic to/from H.323 and SIP telephones and soft clients

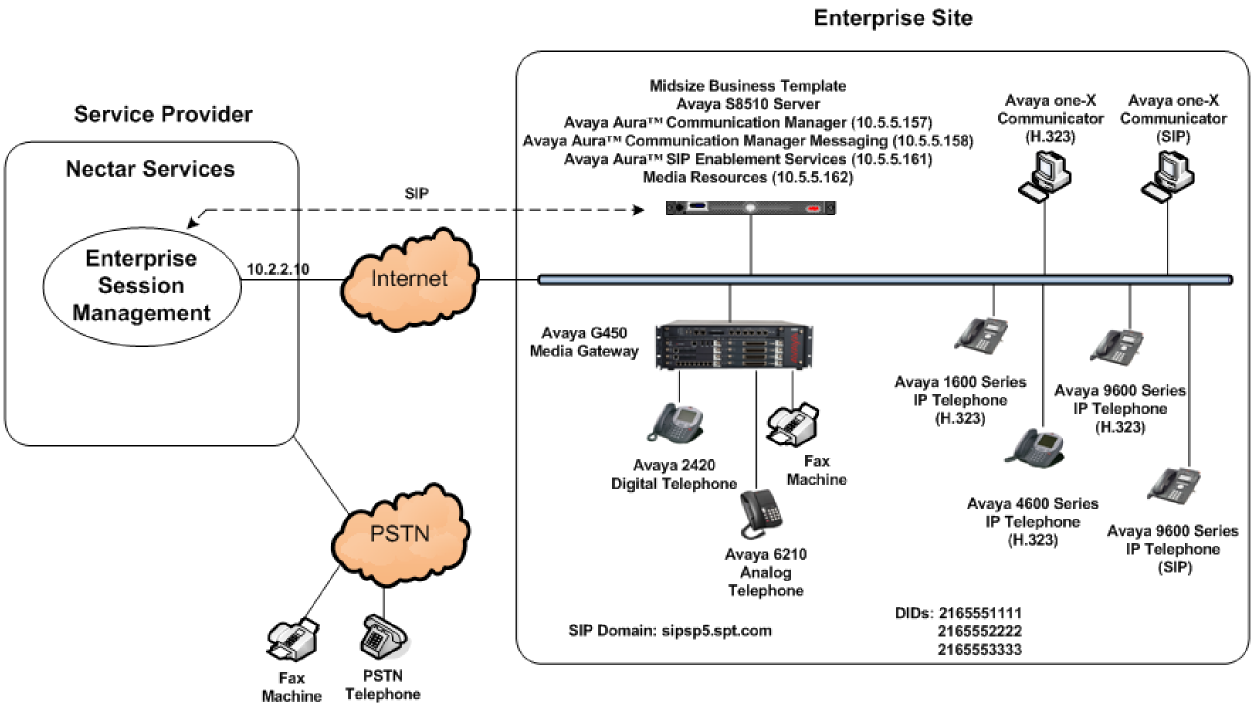

Enterprise Site
Service Provider
Nectar Services
Enterprise Session Management
10.2.2.10
SIP
Internet
PSTN
Fax Machine
PSTN Telephone
Midsize Business Template
Avaya S8510 Server
Avaya Aura™ Communication Manager (10.5.5.157)
Avaya Aura™ Communication Manager Messaging (10.5.5.158)
Avaya Aura™ SIP Enablement Services (10.5.5.161)
Media Resources (10.5.5.162)
Avaya one-X Communicator (H.323)
Avaya one-X Communicator (SIP)
Avaya G450 Media Gateway
Avaya 2420 Digital Telephone
Fax Machine
Avaya 6210 Analog Telephone
Avaya 1600 Series IP Telephone (H.323)
Avaya 9600 Series IP Telephone (H.323)
Avaya 4600 Series IP Telephone (H.323)
Avaya 9600 Series IP Telephone (SIP)
SIP Domain: sipsp5.spt.com
DIDs: 2165551111
2165552222
2165553333

Figure 1: Nectar Services ESM Test Configuration

For incoming calls, the SES uses address maps to direct the incoming SIP messages to Communication Manager, as shown in **Section 5.2.2**. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signaling is routed to the SES. The SES directs the outbound SIP messages to the Nectar Services network.

The dial plan for the configuration described in these Application Notes requires the user to use 1+10 digit dialing for PSTN calls within the North American Numbering Plan (NANP). All 11 digits are sent in the To header of the outbound SIP INVITE message and 10 digits are sent in the From header. For inbound calls, the network sends 11 digits in both the To and From headers in the inbound SIP INVITE message. Communication Manager routes all calls to the Nectar Services network using Automatic Route Selection (ARS).

3. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Midsize Business Template running on an Avaya S8510 Server	5.2.1.2.5 with System Platform 1.1.1.02 patch 1.1.1.4.2
• Avaya Aura™ Communication Manager	5.2.1 (R015x.02.1.016.4)
• Avaya Aura™ SIP Enablement Services	5.2.1 (SES-5.2.1.0-016.4)
• Avaya Aura™ Communication Manager Messaging	5.2.1 (R015x.02.1.016.4)
• Media Services	1.1.0.2.1
Avaya G450 Media Gateway	30.10.4
Avaya 9640 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.0 SP1 (s3.002)
Avaya 9620 IP Telephone (SIP)	Avaya one-X Deskphone Edition SIP 2.4.2
Avaya 1608 IP Telephone (H.323)	Avaya one-X Deskphone Value Edition 1.2.1.1
Avaya 4621SW IP Telephone (H.323)	2.9.1
Avaya one-X Communicator (H.323)	5.2.0.10
Avaya one-X Communicator (SIP)	5.2.0.10
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Nectar Services Enterprise Session Management Components	
Component	Release
Genband S3 Session Border Controller	4.6m5

Table 1: Equipment and Software Tested

The specific configuration above was used for the compatibility testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and SIP Enablement Services.

4. Configure Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and SIP Enablement Services (SES). One trunk is created as part of the initial SES installation and is meant to carry SIP signaling between SIP endpoints within the SES domain. A second trunk is created specifically to carry SIP signaling between the SES domain and ESM.

It is assumed the general installation of the System Platform and Midsize Business Template (with Communication Manager and SES) and Avaya G450 Media Gateway has been previously completed and is not discussed here. In addition, it is assumed that any initial SIP configuration on Communication Manager that is required to support the SES installation has also been completed. For more information on these installation procedures, refer to **[1]**, **[3]** and **[7]**.

This section is divided into two parts. **Section 4.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. This section will not attempt to show the installation procedures in their entirety.

Section 4.2 will describe the procedures beyond the initial SIP installation that are necessary to configure SIP trunking to ESM.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

4.1. Summarize Initial SIP Configuration

This section summarizes the Communication Manager configuration in the test environment **prior** to adding SIP trunking to ESM.

4.1.1. Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and SES. Use the **change node-names ip** command to create a mapping between a logical name and an IP address. In the test environment, node name ***procr*** is mapped to IP address ***10.5.5.157*** (the IP address of Communication Manager) and node name ***ses1*** is mapped to ***10.5.5.161*** (the IP address of the SES). In other Avaya configurations with an Avaya G650 Media Gateway, a CLAN circuit pack can also be used as the SIP signaling interface to SES, as well as the **procr** interface.

```
change node-names ip                                        Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
CMM                 10.5.5.158
MedSvcsMedpro1      10.5.5.194
MedSvcsMedpro2      10.5.5.195
MedSvcsMedpro3      10.5.5.196
MedSvcsMedpro4      10.5.5.197
aeserver1           10.5.5.160
default             0.0.0.0
procr               10.5.5.157
ses1                10.5.5.161
vspGateway          10.5.5.129
```

4.1.2. IP Network Regions

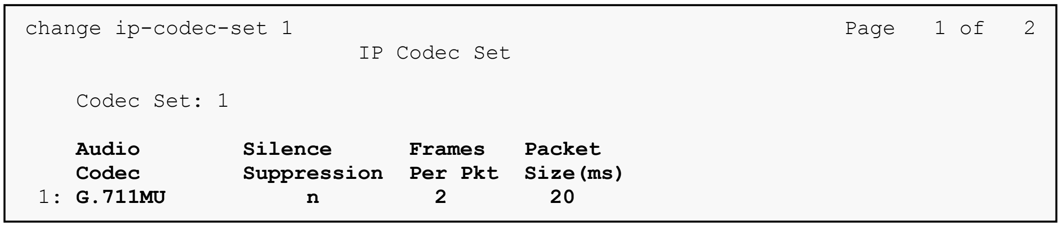
In the test environment, Communication Manager, Media Services, Avaya Media Gateway, SES, and IP (H.323/SIP) endpoints are located in a single IP network region. These components are located in the default IP network region 1. The **change ip-network-region 1** command was used to configure the region with the parameters described below.

- Set the **Authoritative Domain** field to match the domain name configured on SES. In this configuration, the domain name is ***sipsp5.spt.com***. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name for the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. This was done for both **Intra-region** and **Inter-region IP-IP Direct Audio.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.
- Default values may be used for all other fields.

```
change ip-network-region 1                                  Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: sipsp5.spt.com
    Name: Default
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? 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
```

4.1.3. Codecs

Use the **change ip-codec-set 1** command to define the codec(s) contained in this set which is used for calls within the enterprise as defined in the previous section. The codecs selected and their order of preference is defined by the end customer. The example below uses only G.711MU.

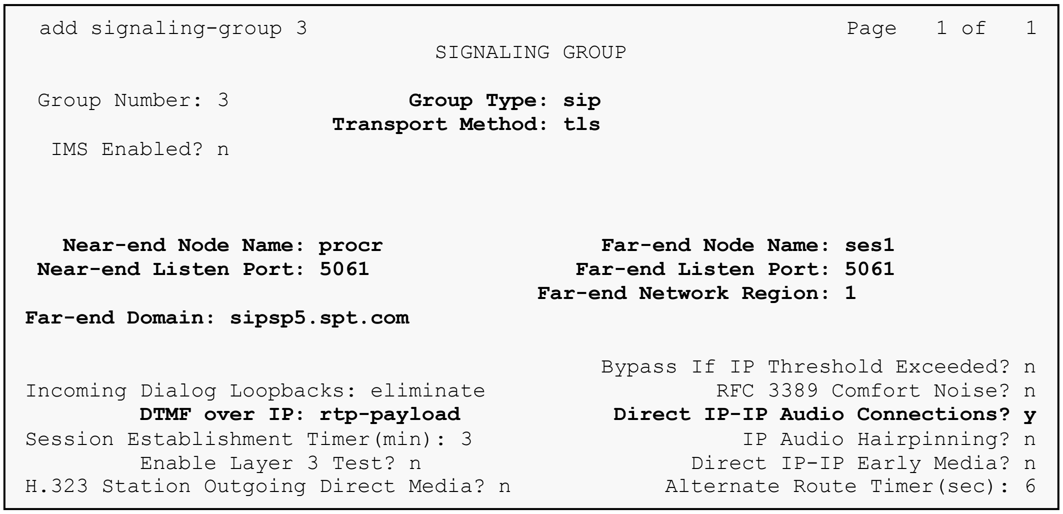


```
change ip-codec-set 1                                          Page   1 of   2
                          IP Codec Set

    Codec Set: 1

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

4.1.4. Signaling Group

The **add signaling-group** command was used to create a signaling group between Communication Manager and the SES for use by intra-site traffic. For the compliance test, signaling group 3 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5061.***
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of Communication Manager. Node names are defined using the **change node-names ip** command.
- Set the **Far-end Node Name** to ***ses1***. This node name maps to the IP address of SES as defined using the **change node-names ip** command.
- Set the **Far-end Network Region** to the IP network region defined **Section 4.1.2**.
- Set the **Far-end Domain** to the domain of the SES.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

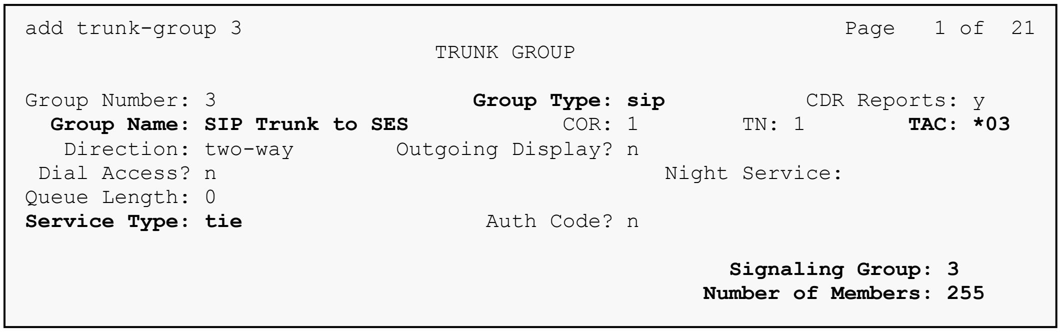


```
 add signaling-group 3                                          Page   1 of   1
                                SIGNALING GROUP

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



   Near-end Node Name: procr                 Far-end Node Name: ses1
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
Far-end Domain: sipsp5.spt.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
```

4.1.5. Trunk Group

The **add trunk-group** command was used to create a trunk group for the signaling group created in the previous section. For the compliance test, trunk group 3 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***tie***.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group up to a maximum of 255. This value determines how many simultaneous SIP calls can be supported by this trunk.
- The default values were used for all other fields.



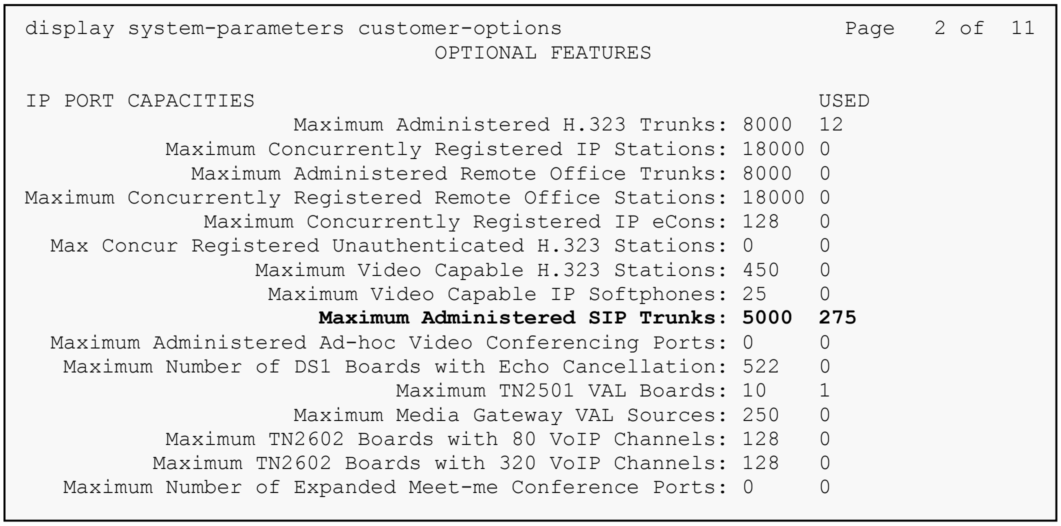
```
add trunk-group 3                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 3                    Group Type: sip           CDR Reports: y
  Group Name: SIP Trunk to SES            COR: 1        TN: 1        TAC: *03
   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: 255
```

4.2. Nectar Services Specific Configuration

This section describes the Communication Manager configuration specific to the SIP connection to ESM. Connection to ESM requires separate outbound and inbound trunks. This is necessary because the destination SIP domain required in outbound SIP INVITE messages differs from the originating SIP domain received in the PAI header of inbound INVITE messages.

4.2.1. Licensing and Capacity

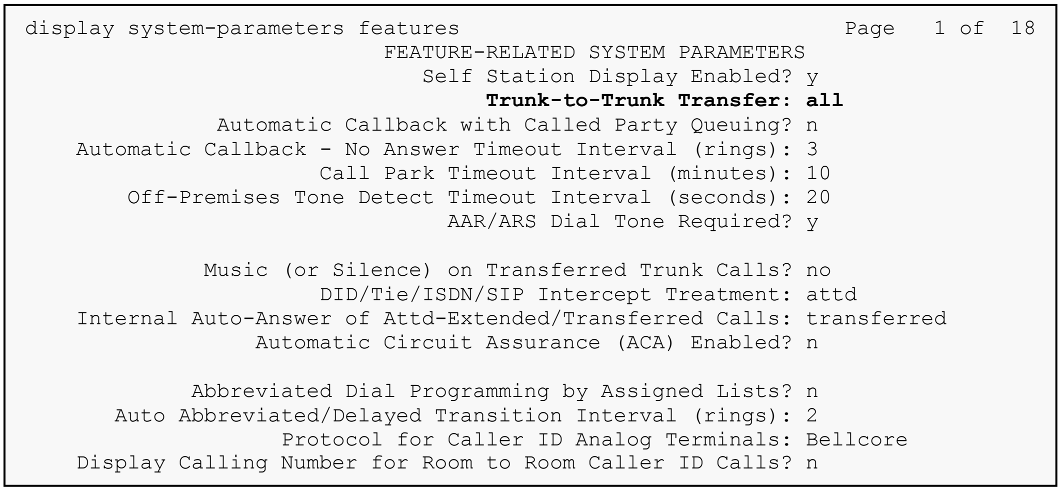
Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunk** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. Each Avaya SIP telephone on a 2-party call with the SIP service provider uses two SIP trunks for the duration of the call. Each non-SIP telephone (i.e., analog, digital, H.323) on a 2-party call with SIP service provider uses one SIP trunk. The example shows that ***5000*** licenses are available and ***275*** are in use. 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.



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

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 8000  12
           Maximum Concurrently Registered IP Stations: 18000 0
             Maximum Administered Remote Office Trunks: 8000  0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 450   0
                   Maximum Video Capable IP Softphones: 25    0
                       Maximum Administered SIP Trunks: 5000  275
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

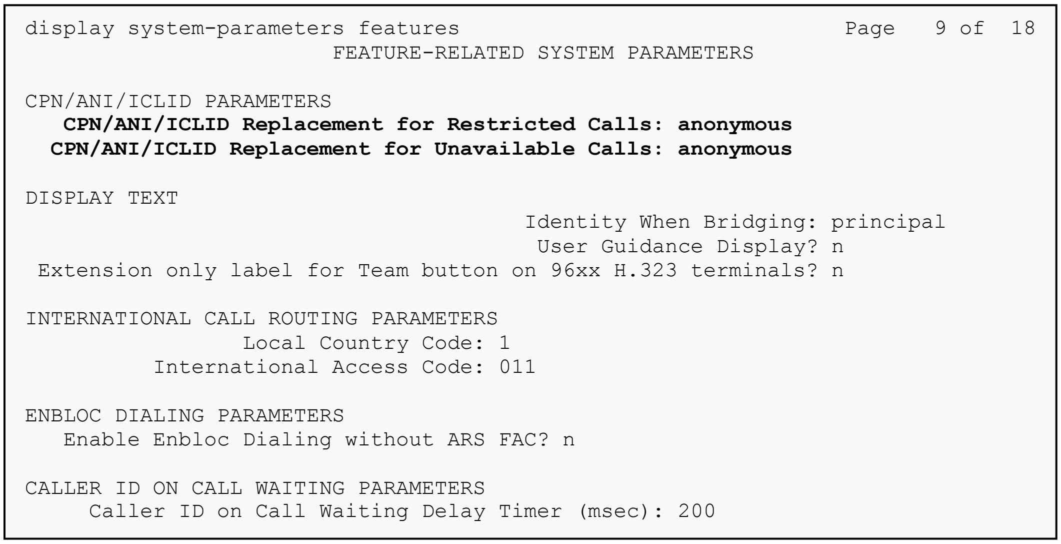
4.2.2. System Features

Use the **change system-parameters feature** command to set the **Trunk-to-Trunk Transfer** field to ***all*** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to ***none***.



```
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 (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

             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

On **Page 9,** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the default value of ***anonymous*** for both fields**.**

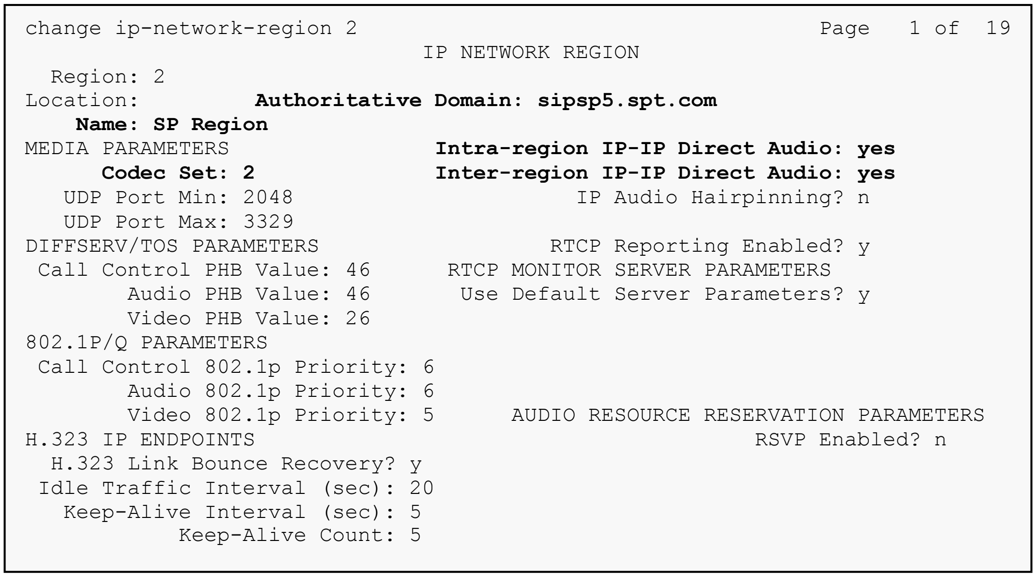


```
display system-parameters features                              Page   9 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

DISPLAY TEXT
                                       Identity When Bridging: principal
                                        User Guidance Display? n
 Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code: 1
          International Access Code: 011

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200
```

4.2.3. IP Network Region

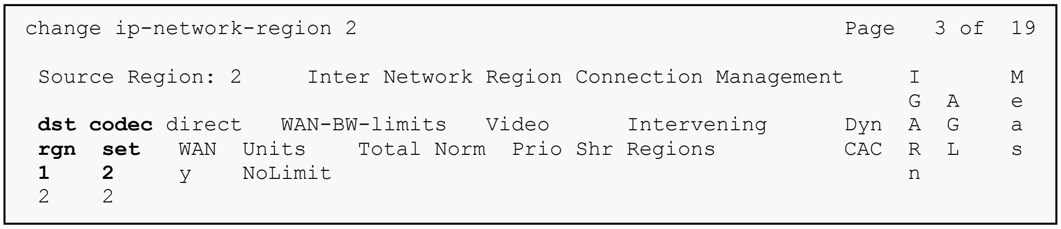
Create a separate IP network region for the service provider trunk(s). This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 2 was chosen for the service provider trunk(s). Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the domain name configured on SES. In this configuration, the domain name is ***sipsp5.spt.com***. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to ***yes*.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 2 was selected.
- Default values can be used for all other fields.



```
change ip-network-region 2                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 2
Location:         Authoritative Domain: sipsp5.spt.com
    Name: SP Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              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
```

On **Page 2**, define the IP codec set to be used for traffic between region 2 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).



```
change ip-network-region 2                                     Page   3 of  19

 Source Region: 2     Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    2     y    NoLimit                                             n
 2    2
```

4.2.4. Codecs

Use the **change ip-codec-set 2** command to define the codec(s) contained in this set which is used for calls between the enterprise and the service provider as defined in the previous section.

ESM supports G.729A, G.711A, and G.711MU. Thus, these codecs were included in this set in order of preference. The order of preference is defined by the end customer. Enter ***G.729A***, ***G.711MU, and G.711A*** in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

                          IP Codec Set

    Codec Set: 2

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

On **Page 2**, set the **Fax Mode** field to ***t.38-standard***.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                    Mode                 Redundancy
    FAX             t.38-standard         0
    Modem           off                   0
    TDD/TTY         US                    3
    Clear-channel   n                     0
```

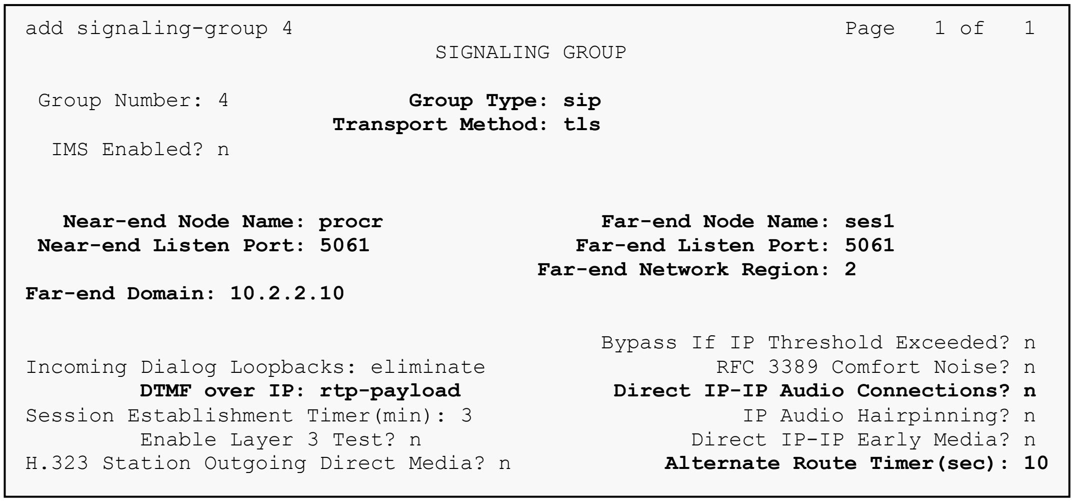
4.2.5. Outbound Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the SES for use by the service provider outbound trunk. For the compliance test, signaling group 4 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5061.***
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address Communication Manager. Node names are defined using the **change node-names ip** command.
- Set the **Far-end Node Name** to ***ses1***. This node name maps to the IP address of SES as defined using the **change node-names ip** command.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 4.2.3**.
- Set the **Far-end Domain** to the domain of the service provider. This may be a fully qualified domain name or an IP address but it must match the domain that the service

provider expects to see in the SIP Request URI and the “To” header of outbound INVITE messages. If a fully qualified domain name is used, then a DNS server must be present in the network that can resolve the name to the appropriate IP address. In the case of the compliance test, this field was set to the IP address of the Session Border Controller (SBC) at the edge of the Nectar Services network.

- Set **Direct IP-IP Audio Connections** to ***n***. This field will disable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to ***10***. This timer determines how many seconds to wait for a response other than “100 Trying” after sending an INVITE. If no response other than 100 Trying is received before this time, then the call will be terminated. The default value of 6 was not always long enough for the Nectar Services network.
- Default values may be used for all other fields.



```
add signaling-group 4                                           Page   1 of   1
                                SIGNALING GROUP

 Group Number: 4              Group Type: sip
                        Transport Method: tls
  IMS Enabled? n


   Near-end Node Name: procr                 Far-end Node Name: ses1
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 2
Far-end Domain: 10.2.2.10

                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 10
```

4.2.6. Outbound Trunk Group

Use the **add trunk-group** command to create an outbound trunk group for the signaling group created in **Section 4.2.5**. For the compliance test, trunk group 4 was configured using the parameters highlighted below.

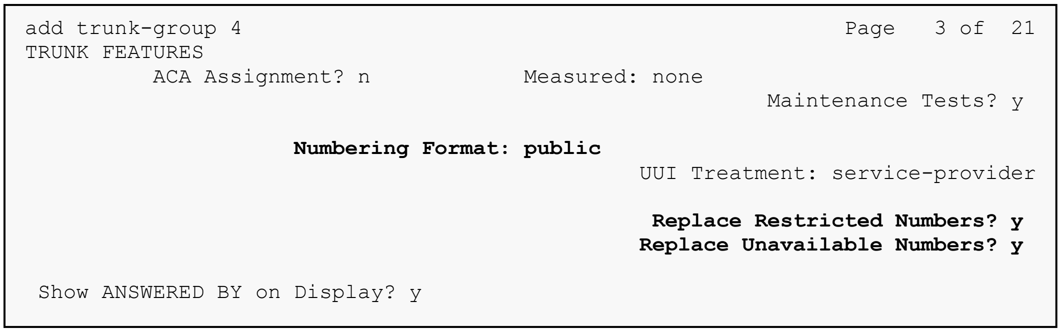
- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set the **Signaling Group** to the signaling group shown in the previous section.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- The default values were used for all other fields.

```
add trunk-group 4                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 4                   Group Type: sip          CDR Reports: y
  Group Name: Nectar                     COR: 1        TN: 1        TAC: 7004
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                     Signaling Group: 4
                                                   Number of Members: 10
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For ESM, the value of ***600*** seconds was used.

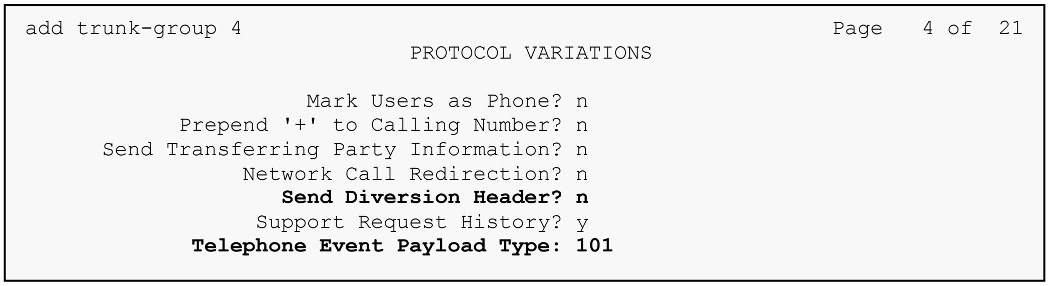
```
add trunk-group 4                                              Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                             Redirect On OPTIM Failure: 5000

            SCCAN? n                                 Digital Loss Group: 18
                       Preferred Minimum Session Refresh Interval(sec): 600
```

On **Page 3**, set the **Numbering Format** field to ***public***. This field specifies the format of the calling party number (CPN) sent to the far-end. Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 4.2.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.



```
add trunk-group 4                                                  Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                             Maintenance Tests? y

                     Numbering Format: public
                                                  UUI Treatment: service-provider

                                                   Replace Restricted Numbers? y
                                                  Replace Unavailable Numbers? y

 Show ANSWERED BY on Display? y
```

On **Page 4**, the **Send Diversion Header** field may be set to ***n***. This field provides information about the re-directing party if the call has been re-directed. The service provider may use this field to authenticate the caller of these re-directed calls. This is often needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. However, the Diversion Header is not needed by ESM since it does not authenticate on the originating number. Set the **Telephone Event Payload Type** to the value used by ESM (***101***).

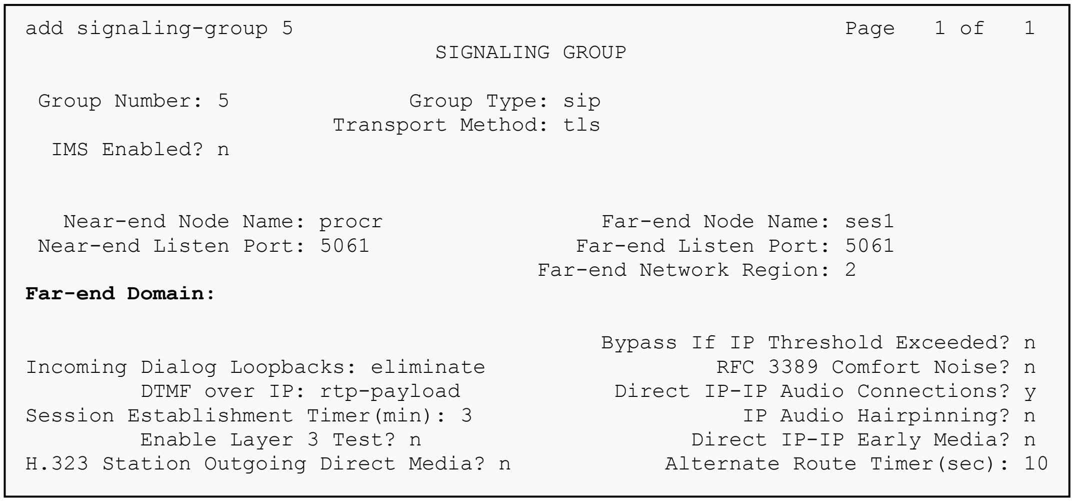


```
add trunk-group 4                                                  Page   4 of  21
                              PROTOCOL VARIATIONS

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

4.2.7. Inbound Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the SES for use by the service provider inbound trunk. For the compliance test, signaling group 5 was used for this purpose. This signaling group is configured the same as the outbound signaling group in **Section 4.2.5** except were noted below.

- Leave the **Far-end Domain** blank. This value must match the domain received in the PAI or From header (if no PAI present) of inbound INVITE messages. If this value is blank then it will match on any domain. The domain sent by ESM varies based on the network PSTN gateway where the call originates so this field must be left blank.

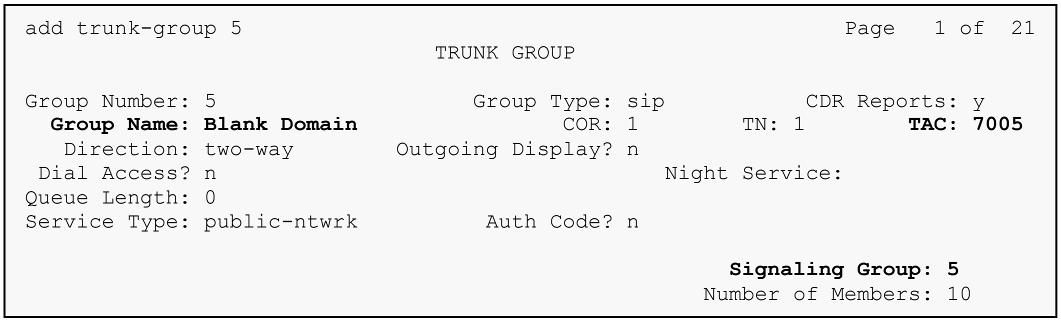


```
add signaling-group 5                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 5             Group Type: sip
                       Transport Method: tls
  IMS Enabled? n


   Near-end Node Name: procr                  Far-end Node Name: ses1
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 2
Far-end Domain:

                                           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): 10
```

4.2.8. Inbound Trunk Group

Use the **add trunk-group** command to create an inbound trunk group for the signaling group created in **Section 4.2.7**. For the compliance test, trunk group 5 was configured using the parameters highlighted below. This trunk group is configured the same as the outbound trunk group in **Section 4.2.6** except were noted below.

- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Signaling Group** to the signaling group shown **Section 4.2.6**.



```
add trunk-group 5                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 5                   Group Type: sip          CDR Reports: y
  Group Name: Blank Domain               COR: 1        TN: 1        TAC: 7005
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                     Signaling Group: 5
                                                   Number of Members: 10
```

4.2.9. Calling Party Information

Public unknown numbering defines the calling party number to be sent to the far-end. This calling party number is sent in the SIP "From" header. Use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider.

In the sample configuration, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions 30001, 30002 and 30003. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 3
 5  30001         4         2165551111      10          Maximum Entries: 9999
 5  30002         4         2165552222      10
 5  30003         4         2165553333      10
```

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single public unknown numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 3 will send the calling party number as the **CPN Prefix** plus the extension number.

```
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
 5  3             4        21655           10          Maximum Entries: 9999
```

4.2.10. Outbound Routing

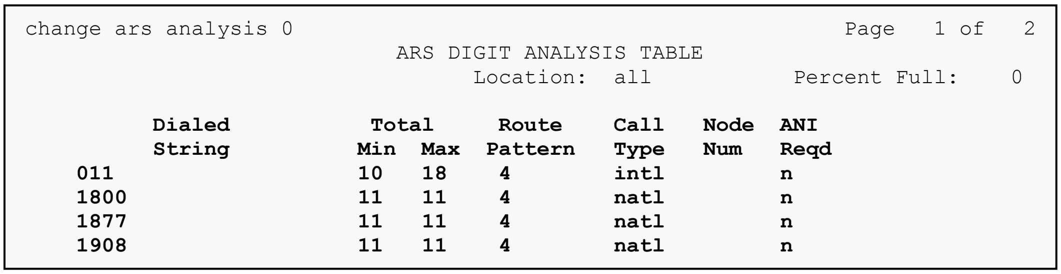
In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1 as a feature access code (**fac**).

```
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    attd
     19           5    ext
     3            5    ext
     7            5    ext
     70           4    dac
     8            5    ext
     9            1    fac
     *            3    dac
     #            3    dac
```

Use the **change feature-access-codes** command to configure ***9*** as the **Auto Route Selection (ARS) – Access Code 1**.

```
change feature-access-codes                                    Page   1 of   9
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *10
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *14
                      Announcement Access Code: *19
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *33    Deactivation: #33
Call Forwarding Activation Busy/DA: *30    All: *31    Deactivation: #30
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: *40
```

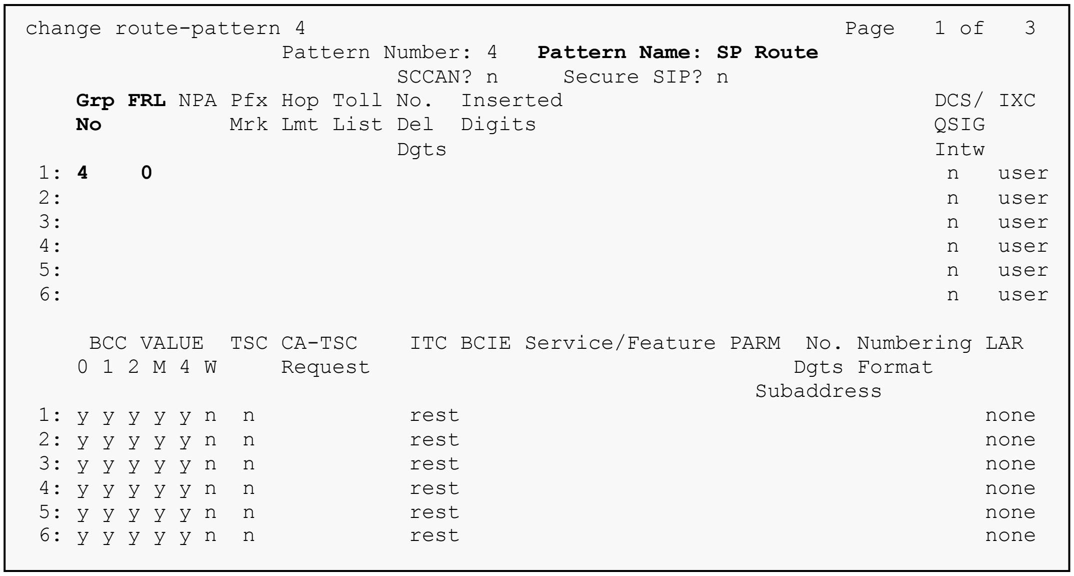
Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 1.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 4 which contains the SIP trunk to the service provider (as defined below).



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

          Dialed            Total     Route     Call    Node  ANI
          String          Min  Max  Pattern    Type    Num   Reqd
    011                   10   18     4        intl          n
    1800                  11   11     4        natl          n
    1877                  11   11     4        natl          n
    1908                  11   11     4        natl          n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 4 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 4 was connected to ESM.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.



```
change route-pattern 4                                          Page   1 of   3
                    Pattern Number: 4   Pattern Name: SP Route
                             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: 4    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                                              none
 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
```

4.2.11. Inbound Routing

Incoming call handling treatment is applied to inbound calls to direct them to the proper destination. Use the **change inc-call-handling-trmt trunk-group *x*** command (where ***x*** is the service provider trunk group) to define the proper digit manipulation for each DID number to map it to an internal extension. The example below shows the DID numbers used in the compliance test.

```
change inc-call-handling-trmt trunk-group 5                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    11 12165551111      11  30001
 public-ntwrk    11 12165552222      11  30002
 public-ntwrk    11 12165553333      11  30003
```

5. Configure SIP Enablement Services

This section covers the configuration of SES. With the MBT, the SES is accessed through the System Platform Web Console using an Internet browser. The SES is then configured using the SES System Management Interface. It is assumed that the SES software and the license file have already been installed on the server. During the software installation, the MBT Installation Wizard is run which allows the user to enter SES parameters to initially configure the SES. For additional information on these installation tasks, refer to **[3]** and **[10]**.

Each SIP endpoint at the enterprise used in the compliance test requires that a user and media server extension be created on SES. This configuration is not directly related to SIP Trunking so it is not included here. These procedures are covered in **[9]** and **[10]**.

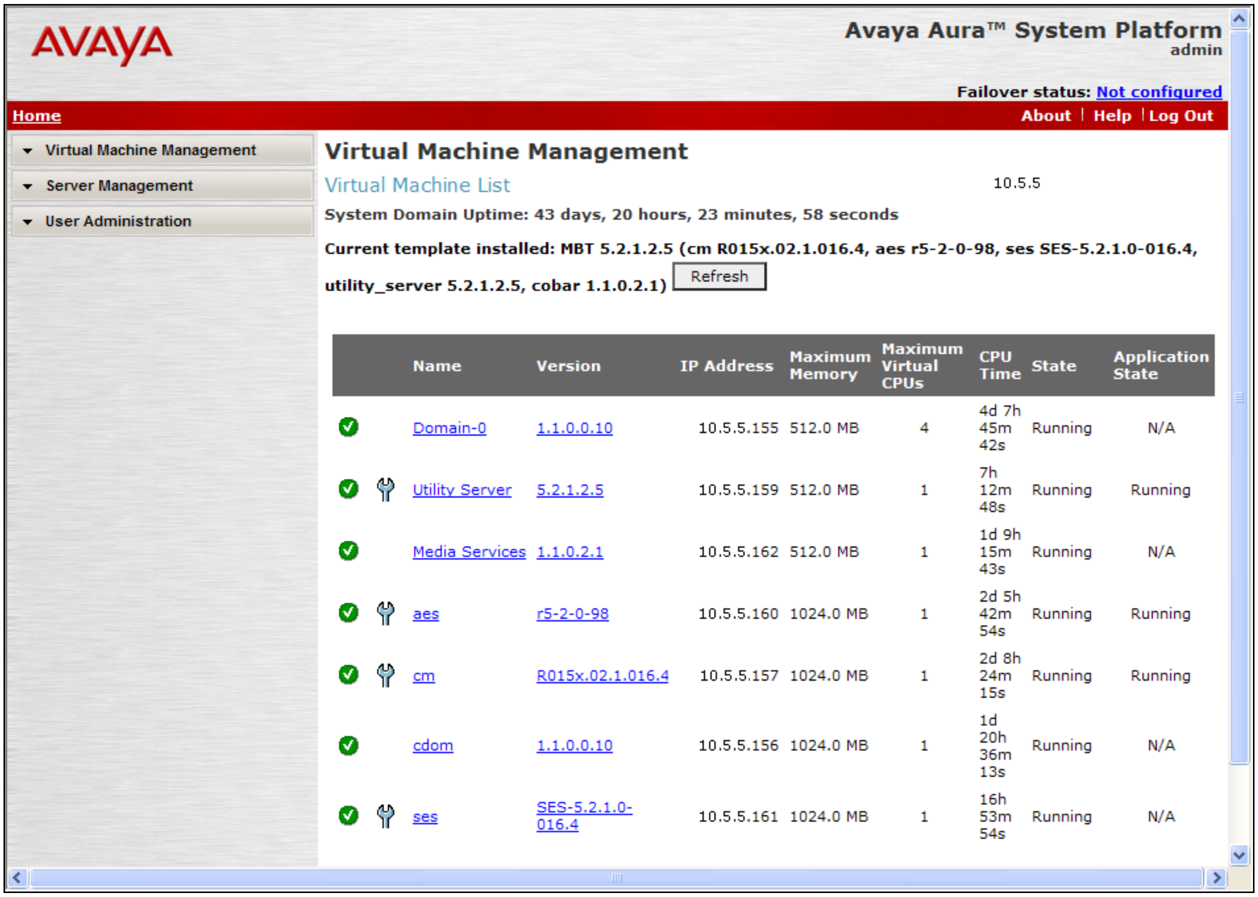
This section is divided into two parts. **Section 5.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. This section will not attempt to show the installation procedures in their entirety. It will describe any deviations from the standard procedures, if any. **Section 5.2** will describe procedures beyond the initial SIP installation procedures that are necessary to support ESM.

5.1. Summarize Initial Configuration Parameters

This section summarizes the applicable user-defined parameters used during the SES installation procedures.

5.1.1. System Platform Console Login

To access the System Platform Web Console, enter https://<ip-addr>/webconsole as the URL in an Internet browser, where *<ip-addr>* is the IP address of the System Platform Console Domain. Log in with the appropriate credentials and then click the wrench icon next to the SES host name to access the SES System Management Interface.


AVAYA
Avaya Aura™ System Platform
admin
Failover status: Not configured
Home
About | Help | Log Out
Virtual Machine Management
Server Management
User Administration
Refresh

Virtual Machine Management

Virtual Machine List 10.5.5

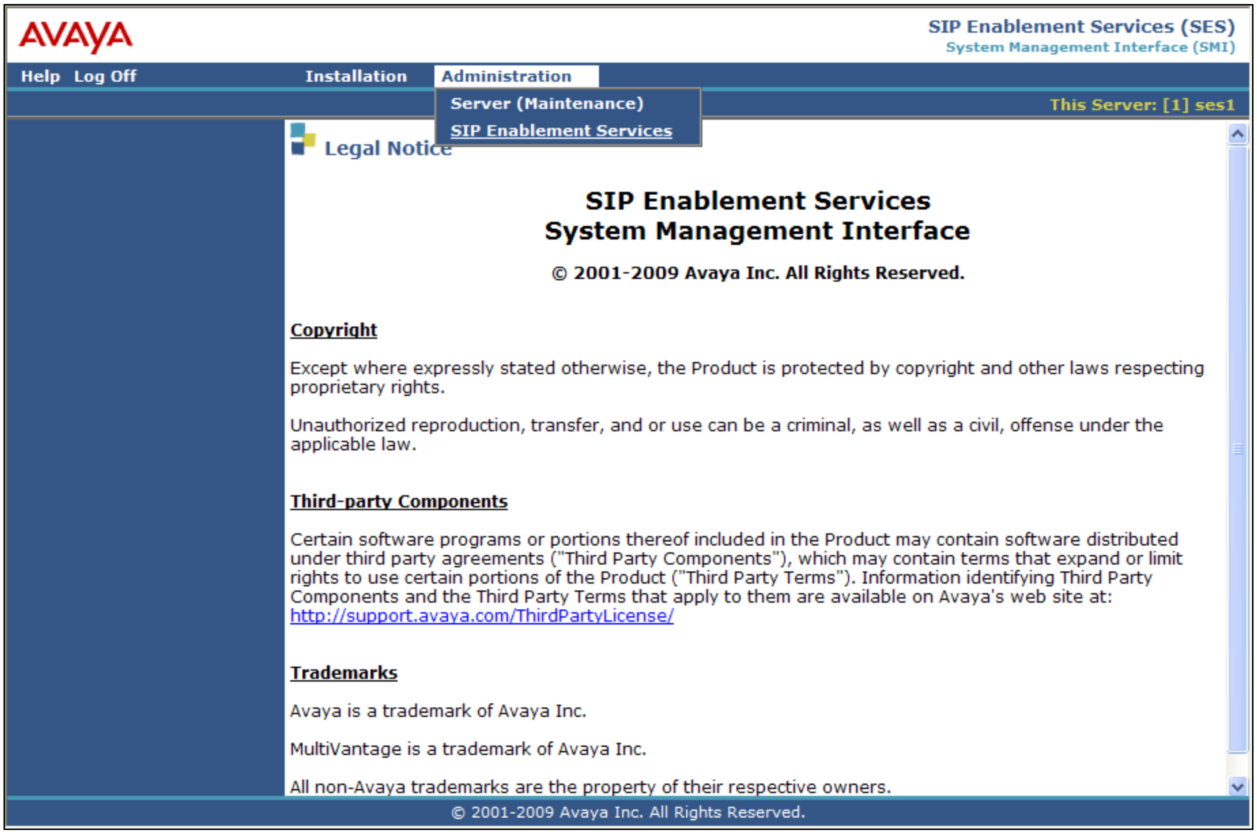
System Domain Uptime: 43 days, 20 hours, 23 minutes, 58 seconds

Current template installed: MBT 5.2.1.2.5 (cm R015x.02.1.016.4, aes r5-2-0-98, ses SES-5.2.1.0-016.4, utility_server 5.2.1.2.5, cobar 1.1.0.2.1)

		Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓		Domain-0	1.1.0.0.10	10.5.5.155	512.0 MB	4	4d 7h 45m 42s	Running	N/A
✓	🔧	Utility Server	5.2.1.2.5	10.5.5.159	512.0 MB	1	7h 12m 48s	Running	Running
✓		Media Services	1.1.0.2.1	10.5.5.162	512.0 MB	1	1d 9h 15m 43s	Running	N/A
✓	🔧	aes	r5-2-0-98	10.5.5.160	1024.0 MB	1	2d 5h 42m 54s	Running	Running
✓	🔧	cm	R015x.02.1.016.4	10.5.5.157	1024.0 MB	1	2d 8h 24m 15s	Running	Running
✓		cdom	1.1.0.0.10	10.5.5.156	1024.0 MB	1	1d 20h 36m 13s	Running	N/A
✓	🔧	ses	SES-5.2.1.0-016.4	10.5.5.161	1024.0 MB	1	16h 53m 54s	Running	N/A

5.1.2. Login

On the SES System Management Interface, log in with the appropriate credentials and then navigate to the **Administration→ SIP Enablement Services** link from the main page shown below.



SIP Enablement Services
System Management Interface

© 2001-2009 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

Trademarks

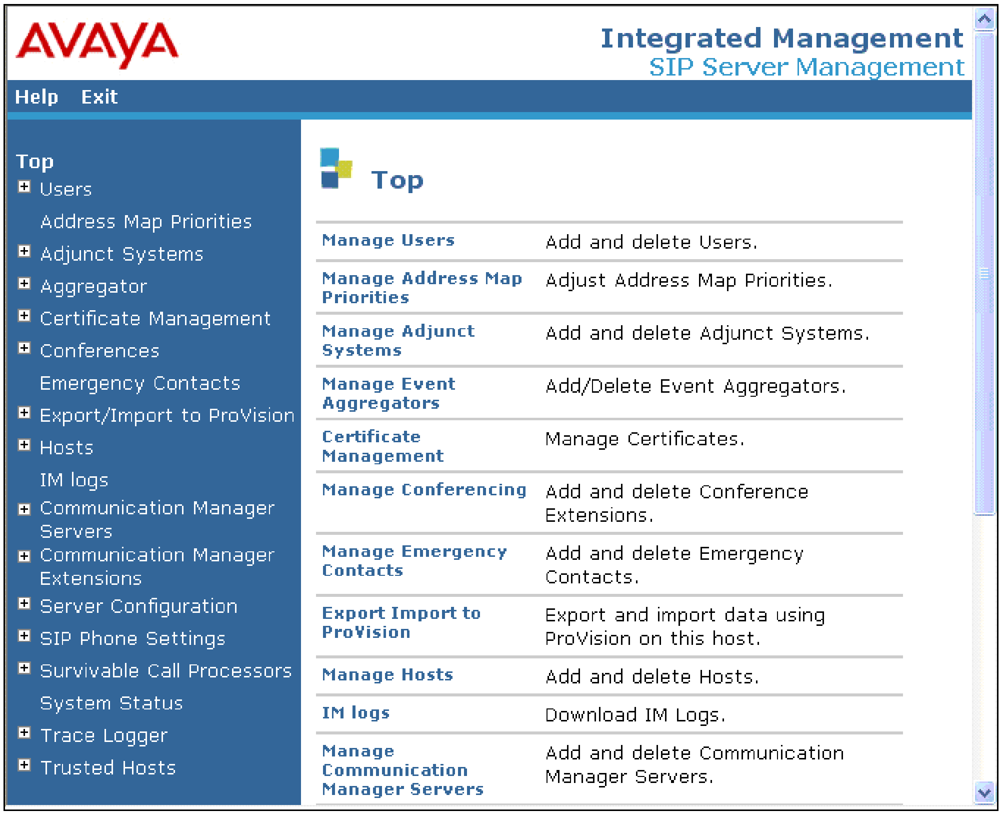
Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

© 2001-2009 Avaya Inc. All Rights Reserved.

The SES **Top** page will be displayed as shown below.



Manage Users	Add and delete Users.
Manage Address Map Priorities	Adjust Address Map Priorities.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Event Aggregators	Add/Delete Event Aggregators.
Certificate Management	Manage Certificates.
Manage Conferencing	Add and delete Conference Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Export Import to ProVision	Export and import data using ProVision on this host.
Manage Hosts	Add and delete Hosts.
IM logs	Download IM Logs.
Manage Communication Manager Servers	Add and delete Communication Manager Servers.

5.1.3. Initial Configuration Parameters

As part of the SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each group of parameters is a brief description of how to view the values for that group from the SES **Top** page shown in the previous step.

- SIP Domain: ***sipsp5.spt.com***

  (To view, navigate to **Server Configuration→System Parameters**)

- Host IP Address (SES IP address): ***10.5.5.161***
- Host Type: ***SES combined home-edge***

  (To view, navigate to **Host→List**; click **Edit**)

- Communication Manager Server Interface Name: ***CM***
- SIP Trunk Link Type: ***TLS***
- SIP Trunk IP Address (Communication Manager IP address): ***10.5.5.157***

  (To view, navigate to **Communication Manager Servers→List**; click **Edit**)

5.2. Nectar Services Specific Configuration

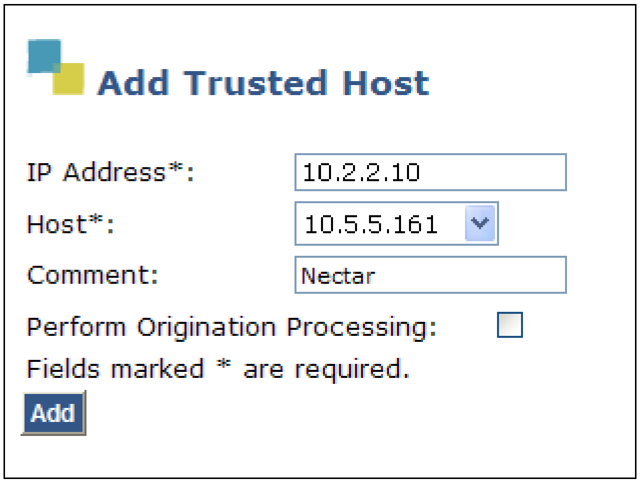
This section describes additional SES configuration necessary for supporting ESM.

5.2.1. Trusted Host

Define the ESM SBC to be a trusted host. Navigate to **Trusted Hosts→Add** in the left pane (see **Section 5.1.1**). In the **Add Trusted Host** window that appears, configure the following:

- **IP Address**: Enter the IP address of the Nectar Services SBC.
- **Host**: Select the SES IP address from the drop-down menu.
- **Comment**: Enter a description of the trusted host being added.

Click the **Add** button.



Add Trusted Host

IP Address*: 10.2.2.10

Host*: 10.5.5.161

Comment: Nectar

Perform Origination Processing: □

Fields marked * are required.

5.2.2. Communication Manager Address Map

A Communication Manager address map is needed to route calls from the PSTN via the SIP trunk to the enterprise. This is necessary because the caller or the called party may not be a registered user on the SES with a media server extension assigned to it. As a result, the SES may not know how to route this call to Communication Manager. Thus to accomplish this task, a Communication Manager address map is needed.

Each map defines a call matching criteria based on the contents of the SIP Request-URI of the call. If a call matches the map, then the call is directed to the specified destination or contact. The URI usually takes the form of *sip:user@domain*, where *user* is the destination number and *domain* is a domain name or an IP address.

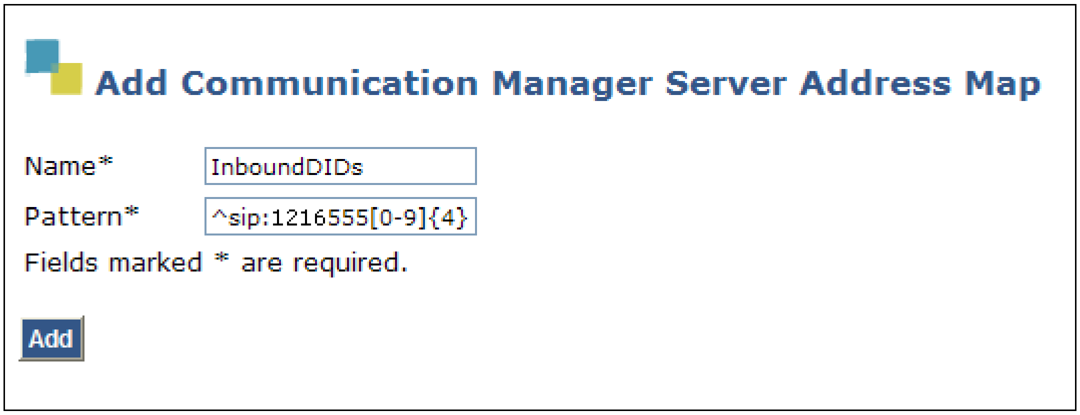
To configure a **Communication Manager Server Address Map**:

- Navigate to **Communication Manager Servers→List** in the left navigation pane of the System Management Interface.
- Click on the **Map** link associated with the appropriate server.
- Click on the **Add Map In New Group** link. If other maps exist that point to the correct destination (contact) then click on **Add Another Map**.

In either case, the **Add Communication Manager Server Address Map** window appears as shown below. Configure the address map as follows:

- **Name**: Enter any descriptive name.
- **Pattern**: Enter an expression to define the matching criteria for calls to be routed from the PSTN to Communication Manager. For the address map named ***InboundDIDs***, the expression will match any URI that begins with ***sip:1216555*** followed by any digit between ***0-9*** for the next ***4*** digits. Additional information on the syntax used for address map patterns can be found in **[9]**.

Click **Add**.



Add Communication Manager Server Address Map

Name* InboundDIDs

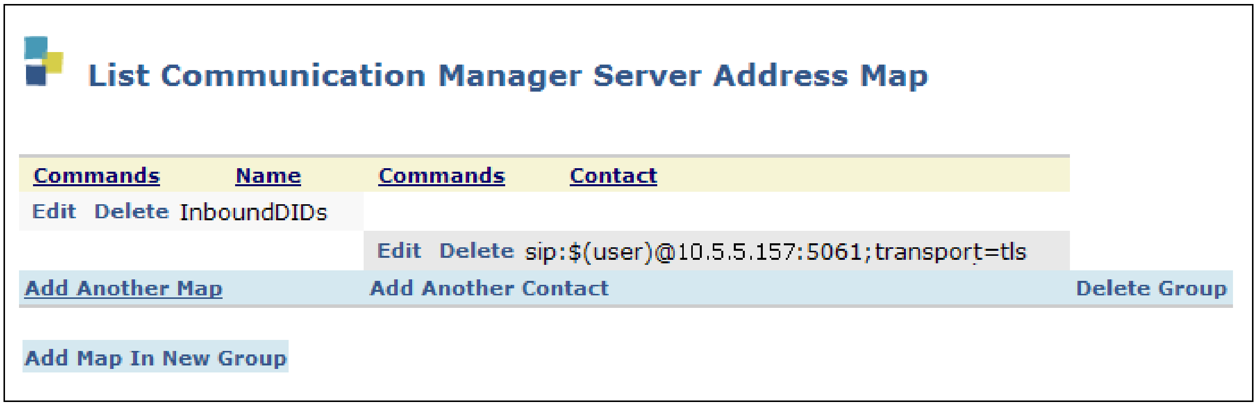
Pattern* ^sip:1216555[0-9]{4}

Fields marked * are required.

After adding the address map, the **List Communication Manager Server Address Map** screen will appear, as shown below. When the first **Communication Manager Server Address Map** is added, a **Contact** is created automatically. For the **Communication Manager Server Address Map** previously added, the following contact was created:

sip:$(user)@10.5.5.157:5061;transport=tls

This contact directs the calls to Communication Manager via IP address (***10.5.5.157***) using port ***5061*** and ***TLS*** as the transport protocol. The incoming DID number sent in the user part of the original request URI is substituted for **$(user)** in the **Contact** expression.



Commands	Name	Commands	Contact
Edit Delete	InboundDIDs		
		Edit Delete	sip:$(user)@10.5.5.157:5061;transport=tls

6. Nectar Services Enterprise Session Management Configuration

Nectar Services is responsible for the configuration of ESM. The customer will need to provide the public IP address used to reach the SES at the enterprise as well as any IP addresses and ports used for media that will need to be granted access to the service provider network.

Nectar Services will provide the customer the necessary information to configure the SIP Trunking connection to ESM, which includes:

- IP address of SIP Trunking SIP proxy/SBC
- Network SIP Domain (if necessary)
- Supported codecs
- DID numbers
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

7. Avaya IP Telephones Configuration

The preferred DTMF payload header value can be set in the phone configuration file (46xxsettings.txt). Not all phone types support this setting. It is used by the Avaya 9600 Series and 16cc Series Telephones running the SIP protocol. Other Avaya H.323 and SIP phone types will ignore this value and use a fixed preferred DTMF payload header value which may vary between phone types. The Avaya 16cc Telephone was not used in the compliance test.

This value should be set to the value recommended by Nectar Services (101) to minimize the need to renegotiate the DTMF payload header value during a call (See **Section 8**). This will only affect calls involving phones that support the DTMF payload setting in the 46xxsettings.txt file.

To set this value, edit the 46xxsettings.txt file on the HTTP server that downloads the file to the Avaya IP Telephones. Add the following line to the file:

```
SET DTMF_PAYLOAD_TYPE 101
```

8. General Test Approach and Test Results

This section describes the general test approach used during compliance testing and the test results.

The general test approach was to configure a simulated enterprise site using Communication Manager and SES within the Midsize Business Template to connect to ESM. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 1.1**.

Interoperability testing of the sample configuration with ESM was completed with successful results. The following observations were made during the compliance test:

- **Calling Party Number (CPN) Block**: Inbound PSTN calls from Nectar Services with CPN block enabled that terminate on an Avaya 9600 SIP Telephone, inadvertently have the calling party number displayed. This can be observed only if the parameter DISPLAY_NAME_NUMBER is set to 1 in the phone settings file; otherwise, the Avaya 9600 SIP Telephone will not attempt to display a caller's number even for the majority of calls that have CPN block disabled.

- **Unsuccessful calls due to the timing of Re-INVITE messages**: When the problem occurs, the network sends a re-INVITE to the SES at approximately the same time that the SES has sent (or in the process of sending) a Re-INVITE. The SES sends a 491 Request Pending response to the network. The combined Avaya/Nectar solution should be able to handle this condition but instead the call gets torn down. This was observed with the following call scenarios, each has a workaround to avoid the underlying problem.

- **Transfer an inbound call back to the PSTN**. In this scenario, re-INVITEs may be sent to re-negotiate the DTMF payload header value from the value chosen during the initial call set-up. The workaround is to avoid these re-INVITEs by configuring the Communication Manager (see **Section 4.2.6 and 4.2.8**) and Avaya IP Telephones where possible (see **Section 7**) to use the value preferred by ESM.

- **Inbound call to an enterprise extension with EC500 enabled that is later extended to the remote phone.** In this scenario, when the enterprise extension is hung up, the extended call to the remote phone is also dropped. Re-INVITEs are generated when re-directing the media from the Communication Manager media resources to the endpoints. The workaround is to avoid these re-INVITEs by disabling Direct IP-IP media on the trunks connected to ESM (**Section 4.2.6 and 4.2.8**).

- **One-way audio when bridging on a stable EC500 call:** An inbound call is placed from an EC500 associated remote phone to an internal enterprise extension. If the user bridges on to this stable call at the EC500 host station, the call results in one-way audio with the EC500 associated remote phone. This problem can also be avoided by disabling Direct IP-IP media on the trunks connected to ESM (**Section 4.2.6 and 4.2.8**).

- **One-X Communicator (SIP) in Telecommuter mode**: Inbound calls to the SIP version of one-X Communicator in telecommuter mode result in no audio. This problem can also be avoided by disabling Direct IP-IP media on the trunks connected to ESM (**Section 4.2.6 and 4.2.8**).

9. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

- From the Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

10. Conclusion

Nectar Services Enterprise Session Management passed compliance testing with the observations/limitations described in **Section 8**. These Application Notes describe the procedures necessary to configure the SIP Trunking connectivity of Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services to Enterprise Session Management.

11. References

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

[1] *Installing and Configuring Avaya Aura™ System Platform,* November 2009.

[2] *Administering Avaya Aura™ System Platform,* November 2009.

[3] *Installing and Configuring Avaya Aura™ Solution for Midsize Enterprises,* November 2009.

[4] *Administering Avaya Aura™ Solution for Midsize Enterprises,* November 2009.

[5] *Avaya Aura™ Communication Manager Feature Description and Implementation,* May 2009, Document Number 555-245-205.

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

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

[8] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide*, June 2005, Document Number 210-100-500.

[9] *Avaya Aura™ SIP Enablement Services Implementation Guide*, May 2009, Document Number 16-300140.

[10] *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura™ SIP Enablement Services,* November 2009, Document Number 03-600768.

[11] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.2.x*, February 2010, Document Number 03-601443.

[12] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.

[13] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Release 3.0 Administrator Guide,* November 2009, Document Number 16-300698.

[14] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Release 2.4 Administrator Guide,* Dec 2008, 16-601944.

[15] *Avaya one-X Communicator Getting Started*, November 2009.

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

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

[18] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, 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.