Abstract

These Application Notes describe the steps for configuring SIP trunking with the Telcordia Service Interconnection Registry and an Avaya SIP trunking solution using Avaya Communication Manager and Avaya SIP Enablement Services.

The Telcordia Service Interconnection Registry uses SIP trunking to perform directory lookups to determine if a telephone number can be reached using wide-area Internet connections. If the number being called is registered in the Telcordia SIR, a SIP redirection is returned allowing the telephone call to be completed via the SIP trunk. Otherwise, when no match is found, the Telcordia SIR response permits Avaya Communication Manager to complete the telephone call using alternate routing such as a PSTN trunk group.

Telcordia 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 with remote access to the Telcordia Service Interconnection Registry.
1. Introduction

These Application Notes describe the steps for configuring SIP trunking with the Telcordia Service Interconnection Registry (SIR) and an Avaya SIP trunking solution using Avaya Communication Manager and Avaya SIP Enablement Services.

SIP (Session Initiation Protocol) is a standards-based communications protocol designed to provide a common framework to support multimedia communication. RFC 3261 [8] is the primary specification governing this protocol. SIP manages the establishment and termination of connections and the transfer of related information such as the desired codec, calling party identity, etc. Within these Application Notes, SIP is used as the signaling protocol between the Avaya components and the SIR offered by Telcordia.

The Telcordia Service Interconnection Registry uses SIP trunking to perform directory lookups to determine if a telephone number can be reached using wide-area Internet connections. If the number being called is registered in the Telcordia SIR, a SIP redirection is returned allowing the telephone call to be completed via the SIP trunk. Otherwise, when no match is found, the Telcordia SIR response permits Avaya Communication Manager to complete the telephone call using alternate routing such as a PSTN trunk group.

1.1. Illustrative Telcordia Service Interconnection Registry Solution

Figure 1 illustrates a representative customer location using an Avaya Communication Manager based SIP trunking solution with the Telcordia Service Interconnection Registry.

This representative configuration includes:

- A simulated “Acme Corp.” customer location using the Avaya SIP trunking solution in addition to ISDN PRI trunks to their local PSTN carrier. This configuration consists of:
  - Avaya Communication Manager providing the communication services for this customer location.
  - Avaya SIP Enablement Services (in the combined home/edge configuration) serving as the SIP proxy with the Telcordia SIR via the Internet.
  - An ISDN PRI trunk to the local PSTN.
  - Various Avaya telephones and other endpoints.
- Several other simulated locations connected with either SIP trunks to the Internet and/or traditional PSTN trunks.
  - XYZ Corp – another business that has subscribed to the Telcordia SIR. They are able to send or receive SIP trunk calls via the Internet with other subscribed businesses such as Acme Corp. XYZ can have PSTN connections for other communication purposes but they are not shown.
  - Unknown Inc. – another business that has NOT subscribed to the Telcordia SIR. Their SIP trunking connections are unknown to Acme Corp. Thus, while they may be technically able to send and receive SIP trunk calls, all calls will use the PSTN.
• Traditional Inc. and Smith Home represent locations that have no SIP trunking connections and all calls must use the PSTN.
• The Telcordia Service Interconnection Registry providing a SIP directory lookup and redirection functions necessary to permit subscribers to reach each other using SIP trunking.

![Diagram](image)

**Figure 1 – Illustrative SIP Trunking Configuration Using the Telcordia SIR**

### 1.2. Telcordia SIR Configuration Information

These Application Notes provide an illustrative example of how the Avaya SIP trunking solution is configured to work with the Telcordia Service Interconnect Registry.

The specific values provided below are illustrative only. *Each customer uses their specific values obtained from Telcordia at the time of service provisioning.*

<table>
<thead>
<tr>
<th>Telcordia Service Interconnection Registry Information</th>
<th>Value Used in these Application Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telcordia – SIR IP Address</td>
<td>225.132.6.98</td>
</tr>
</tbody>
</table>
2. Equipment and Software Validated

The following equipment and software was used during the DevConnect compliance testing with the Telcordia SIR. This compliance testing is extensible to all other Avaya S8xxx series servers and Avaya Media Gateway platforms running the same version of Avaya Communication Manager and Avaya SIP Enablement Services.

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avaya</strong></td>
<td></td>
</tr>
<tr>
<td>Avaya S8500 Server</td>
<td>Avaya Communication Manager 4.0.1 (R014x.00.0.730.5)</td>
</tr>
<tr>
<td>Avaya G650 Media Gateway</td>
<td></td>
</tr>
<tr>
<td>TN2312BP IP Server Interface (IPSI)</td>
<td>HW03 FW022</td>
</tr>
<tr>
<td>TN799DP Control-LAN (C-LAN)</td>
<td>HW01 FW017</td>
</tr>
<tr>
<td>TN2602AP IP Media Processor (Medpro)</td>
<td>HW02 FW031</td>
</tr>
<tr>
<td>TN2224CP Digital Line</td>
<td>HW08 FW015</td>
</tr>
<tr>
<td>TN793CP Analog Line</td>
<td>HW09 FW09</td>
</tr>
<tr>
<td>TN464GP DS1 Interface</td>
<td>HW06 FW017</td>
</tr>
<tr>
<td>Avaya 4621SW IP (H.323) Telephone</td>
<td>Release 2.8.3</td>
</tr>
<tr>
<td>Avaya 4621 SIP Telephone</td>
<td>Release 2.2.2</td>
</tr>
<tr>
<td>Avaya 6416D+M Digital Telephone</td>
<td>n/a</td>
</tr>
<tr>
<td>Avaya S8500B Server</td>
<td>Avaya SIP Enablement Services 4.0 (SES-4.0.0.0-033.6)</td>
</tr>
<tr>
<td><strong>Telcordia</strong></td>
<td></td>
</tr>
<tr>
<td>Service Interconnection Registry</td>
<td>Version 2.0.1</td>
</tr>
</tbody>
</table>

Table 1 – Equipment and Version

3. Configure Avaya Communication Manager

Avaya Communication Manager was installed and configured for basic station to station calling prior to beginning the configuration shown in these Application Notes. In addition, this configuration assumes that an existing PSTN trunk group (e.g., trunk group 3) exists that is capable of placing outbound calls and receiving inbound Direct Inward Dialed calls to the assigned numbers.
These basic configuration details are outside the scope of this SIP trunking application and are not included here.

3.1. SIP Trunk Configuration

3.1.1. Verify System Capacity and Required Features

The Avaya Communication Manager license controls the customer options. Contact an authorized Avaya sales representative for assistance if insufficient capacity exists or a required feature is not enabled.

Verify that there is sufficient remaining Avaya Communication Manager SIP trunk capacity available for the SIP Trunks using the Telcordia SIR, taking into consideration other applications that may require Avaya Communication Manager SIP trunk resources.

This is done by displaying Page 2 of the System-Parameters Customer-Options form. The number of SIP trunks available to add to new or existing trunk groups is the difference between the Maximum Administered SIP Trunks and the USED value.

```
display system-parameters customer-options

OPTIONAL FEATURES

IP PORT CAPACITIES

Maximum Administered H.323 Trunks: 0 0
Maximum Concurrently Registered IP Stations: 5 2
Maximum Administered Remote Office Trunks: 0 0
Maximum Concurrently Registered Remote Office Stations: 0 0
Maximum Concurrently Registered IP eCons: 0 0
Max Concur Registered Unauthenticated H.323 Stations: 0 0
Maximum Video Capable H.323 Stations: 0 0
Maximum Video Capable IP Softphones: 0 0

Maximum Administered SIP Trunks: 100 50

Maximum Number of DS1 Boards with Echo Cancellation: 0 0
Maximum TN2501 VAL Boards: 10 1
Maximum Media Gateway VAL Sources: 0 0
Maximum TN2602 Boards with 80 VoIP Channels: 128 2
Maximum TN2602 Boards with 320 VoIP Channels: 128 0
Maximum Number of Expanded Meet-me Conference Ports: 0 0

(NOTE: You must logoff & login to effect the permission changes.)
```

Figure 2: System-Parameters Customer-Options Form – Page 2
Verify that the Automatic Route Selection (ARS) feature is enabled on Page 3 of the **System-Parameters Customer-Options** form.

### Figure 3: System-Parameters Customer-Options Form – Page 3

#### 3.1.2. Determine Node Names

Use the “change node-names ip” command to view (or assign) the node names to be used in this configuration.

- “ses” and “150.100.100.130” are the **Name** and **IP Address** respectively of the Avaya SIP Enablement Services server interface where Avaya Communication Manager SIP trunk messages are sent.

- “clan_01a03” and “150.100.100.113” are the **Name** and **IP Address** respectively of the TN799DP C-LAN interface used for the SIP signaling group.

### Figure 4: IP Node Names

#### 3.1.3. Define IP Codec Set for SIP Trunk Calls

This configuration uses IP codec set 2 to assign G.729B, G729A and G.711mu codecs (in that priority) for voice calls. T.38 will be used for group 3 fax calls to PSTN connected fax machines.
Using “change ip-codec-set 2” command, enter “G.729B”, “G.729A” and “G.711MU” as the Audio Codec values on Page 1 of the form. Retain the defaults for the remaining fields. On Page 2 of the form, enter “t.38-standard” for FAX and “off” for Modem and TTD/TTY fields.

<table>
<thead>
<tr>
<th>Audio Codec</th>
<th>Silence Suppression</th>
<th>Frames Per Pkt</th>
<th>Packet Size(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.729B</td>
<td>n</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>G.729A</td>
<td>n</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>G.711MU</td>
<td>n</td>
<td>2</td>
<td>20</td>
</tr>
</tbody>
</table>

**Figure 5: IP Codec Set 2 – Audio Codec Settings**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Redundancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAX</td>
<td>t.38-standard</td>
</tr>
<tr>
<td>Modem</td>
<td>off</td>
</tr>
<tr>
<td>TDD/TTY</td>
<td>off</td>
</tr>
<tr>
<td>Clear-channel</td>
<td>n</td>
</tr>
</tbody>
</table>

**Figure 6: IP Codec Set 2 – Fax, Modem, and TTD/TTY Mode Settings**

### 3.1.4. Verify Near End IP Network Region

These Application Notes use IP network region 1 (the normal default) for the G650 Media Gateway, the IP telephones, the C-LAN (in slot 01a03) used for IP telephone registration and
3.1.5. Verify the C-LAN IP Network Region Assignment

In these Application Notes, the C-LAN was previously installed as part of the initial Avaya Communication Manager basic installation (using the procedures as described in [2]) and assigned the Node Name shown in Figure 4.

Using the “display ip-interface 01a03” command (where 01 is the cabinet, a is the carrier, and 03 is the slot of the respective C-LAN), verify the C-LAN is assigned to **Network Region 1**.

---

**display ip-interface 01a03**

<table>
<thead>
<tr>
<th>Type: C-LAN</th>
<th>Slot: 01A03</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code/Suffix:</td>
<td>TN799 D</td>
</tr>
<tr>
<td>Node Name:</td>
<td>clan_01a03</td>
</tr>
<tr>
<td>IP Address:</td>
<td>150.100.100.113</td>
</tr>
<tr>
<td>Subnet Mask:</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway Address:</td>
<td>150.100.100.1</td>
</tr>
<tr>
<td>Enable Ethernet Port?</td>
<td>y</td>
</tr>
<tr>
<td>Allow H.323 Endpoints?</td>
<td>y</td>
</tr>
<tr>
<td>Network Region:</td>
<td>1</td>
</tr>
<tr>
<td>Allow H.248 Gateways?</td>
<td>y</td>
</tr>
<tr>
<td>VLAN: n</td>
<td>Gatekeeper Priority: 5</td>
</tr>
<tr>
<td>Target socket load and Warning level: 400</td>
<td></td>
</tr>
<tr>
<td>Receive Buffer TCP Window Size: 8320</td>
<td></td>
</tr>
<tr>
<td>Auto? n</td>
<td>Speed: 100Mbps</td>
</tr>
<tr>
<td>Duplex: Full</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 7: IP Interface of C-LAN 01a03 used for SIP Signaling Group 3**
3.1.6. Define IP Network Region

IP network regions set various IP network properties for SIP trunk groups and other IP elements (such as IP telephones, media processor cards, etc.) assigned to the region.

In these Application Notes,

- IP network region 1 defines the properties for the main Avaya Communication Manager site previously configured during installation.
- IP network region 11 is assigned to Telcordia SIR to allow codec preferences different from network region 1 to be used.
- IP network region 1 and 11 are defined to be directly connected with 512 Kbps of bandwidth.
- IP codec-set 2 (defined in Section 3.1.3) will be used for calls between IP network region 1 and 11.

Using the “change ip-network-region 1” command, enter on Page 1:

- **Name:** a descriptive string such as “Avaya CM Main Location”.
- **Authoritative Domain:** the SIP domain of the Avaya SES (in this case “customer-sipdomain.com” as defined in Section 4.1.2).
- **Codec Set:** the value “1” corresponding to the ip-codec-set (defined during initial configuration) for local calls between telephones on Avaya Communication Manager.
- **Intra-region IP-IP Direct Audio:** the value “yes” (the default).
- **Inter-region IP-IP Direct Audio:** the value “yes” (the default).

The IP-IP Direct Audio settings ensure the most efficient use of TN2602AP Media Processor resources.

Defaults for the remaining values are used.

<table>
<thead>
<tr>
<th>change ip-network-region 1</th>
<th>Page 1 of 19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region: 1</td>
<td>IP NETWORK REGION</td>
</tr>
<tr>
<td>Location: 1</td>
<td>Authoritative Domain: customer-sipdomain.com</td>
</tr>
<tr>
<td>Name: Avaya CM Main Location</td>
<td>Cord Set: 1</td>
</tr>
<tr>
<td>Intra-region IP-IP Direct Audio: yes</td>
<td></td>
</tr>
<tr>
<td>Inter-region IP-IP Direct Audio: yes</td>
<td></td>
</tr>
<tr>
<td>UDP Port Min: 2048</td>
<td>IP Audio Hairpinning? n</td>
</tr>
<tr>
<td>UDP Port Max: 3329</td>
<td>RTCP Reporting Enabled? y</td>
</tr>
<tr>
<td>Call Control PHB Value: 46</td>
<td>RTCP MONITOR SERVER PARAMETERS</td>
</tr>
<tr>
<td>Audio PHB Value: 46</td>
<td>Use Default Server Parameters? y</td>
</tr>
<tr>
<td>Video PHB Value: 26</td>
<td>AUDIO RESOURCE RESERVATION PARAMETERS</td>
</tr>
<tr>
<td>802.1P/Q PARAMETERS</td>
<td>H.323 Link Bounce Recovery? y</td>
</tr>
<tr>
<td>Call Control 802.1p Priority: 6</td>
<td>RSVP Enabled? n</td>
</tr>
<tr>
<td>Audio 802.1p Priority: 6</td>
<td>H.323 Link Bounce Recovery? y</td>
</tr>
<tr>
<td>Video 802.1p Priority: 5</td>
<td>Idle Traffic Interval (sec): 20</td>
</tr>
<tr>
<td>802.3P FRAME RELAY</td>
<td>Keep-Alive Interval (sec): 5</td>
</tr>
<tr>
<td>H.323 IP ENDPOINTS</td>
<td>Keep-Alive Count: 5</td>
</tr>
</tbody>
</table>

**Figure 8: IP Network Region 1 – Page 1**
Page 3 of the IP network region form is used to define the codec set and connectivity characteristics between IP network regions.

On Page 3, configure the “src rgn 1 dst rgn 11” row as follows:
- **codec set**: enter “2”, to use the codec choices defined in Section 3.1.3.
- **direct WAN**: enter “y” to indicate that regions 1 and 11 are directly connected.
- **WAN-BW-limits**: enter “Kbits” and “512” to indicate that the WAN access between IP network region 1 and 11 is limited to 512 Kbps of the available bandwidth.

<table>
<thead>
<tr>
<th>src</th>
<th>dst</th>
<th>codec</th>
<th>direct</th>
<th>WAN-BW-limits</th>
<th>Video</th>
<th>Dyn</th>
</tr>
</thead>
<tbody>
<tr>
<td>rgn</td>
<td>rgn</td>
<td>set</td>
<td>WAN</td>
<td>Units</td>
<td>Total</td>
<td>Norm</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>11</td>
<td>2</td>
<td>y</td>
<td>Kbits</td>
<td>512</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 9: IP Network Region 1 – Page 3**
Configure IP Network Region 11, using the “change ip-network-region 11” command. Enter:

- **Name**: a descriptive string such as “SIP PSTN Trks”
- **Authoritative Domain**: the SIP domain of the Avaya SES (in this case “customer-sipdomain.com” as defined in Section 4.1.2).
- **Codec Set**: the value “2” corresponding to the ip-codec-set defined in Section 3.1.3.
- **Intra-region IP-IP Direct Audio**: the value “yes” (the default).
- **Inter-region IP-IP Direct Audio**: the value “yes” (the default).

```
change ip-network-region 11                                         Page   1 of  19
Region: 11
Location: Authoritative Domain: customer-sipdomain.com
Name: SIP PSTN Trks

MEDIA PARAMETERS
Codec Set: 2
Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
UDP Port Min: 20000
UDP Port Max: 20999

DIFFSERV/TOS PARAMETERS
RTCP Reporting Enabled? y

Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26

802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5

Figure 10: IP Network Region 11 – Page 1
```

Verify that Page 3 of the “change ip-network-region 11” command appears as shown below. The codec set and inter-region connectivity characteristics for the **src rgn 11 dst rgn 1** row were established during the configuration of IP network region 1.

```
change ip-network-region 11                                         Page   3 of  19
Inter Network Region Connection Management

src dst codec direct WAN-BW-limits Video Dyn
rgn rgn set WAN Units Total Norm Prio Shr Intervening-regions CAC IGAR
11 1 2 y Kbits 512 0 0 y n

Figure 11: IP Network Region 11 – Page 3
```

### 3.1.7. Define Outbound SIP Trunk Group

One SIP trunk group is defined for outbound calls using the Telcordia SIR (routed via the Avaya SES). This SIP trunk group requires a corresponding SIP signaling group to define the characteristics of the signaling relationship.
3.1.7.1 Establish the SIP Signaling Group

Using the “add signaling-group 11” command, configure signaling group 11 as follows:

- **Group Type**: set to “sip”.
- **Transport Method**: automatically set to “tls”. The Transport Layer Security (TLS) transport protocol is used between Avaya Communication Manager and the Avaya SES. Note this is not the transport protocol used to communicate between the Avaya SES and the Telcordia SIR.
- **Near-end Node Name**: set to the C-LAN node name (defined in Section 3.1.2) used for the respective signaling group. In these Application Notes, “clan_01a03” is used for signaling group 11.
- **Far-end Node Name**: set to the Avaya SES. In these Application Notes, the node name “ses” is used as defined in Section 3.1.2
- **Near-end Listen Port**: set to “5061”, the default port for SIP signaling using tls transport.
- **Far-end Listen Port**: set to “5061”.
- **Far-end Network Region**: set to “11”, the network region defined in Section 3.1.6.
- **Far-end Domain**: set to the IP address provided by Telcordia as their SIR IP address. In these Application Notes, the IP address “225.132.6.98” will be used.
- **Direct IP-IP Audio Connections**: set to “y”, indicating the RTP paths should be optimized to reduce the use of media processing resources when possible.
- **DTMF over IP**: set to “rtp-payload”. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833 [9].

The default values for the other fields are used.

The resulting form for signaling group 11 is shown below.

```
add signaling-group 11
SIGNALING GROUP
Group Number: 11             Group Type: sip
Transport Method: tls

Near-end Node Name: clan_01a03            Far-end Node Name: ses
Near-end Listen Port: 5061                Far-end Listen Port: 5061
Far-end Network Region: 11
Far-end Domain: 225.132.6.98
Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload
Direct IP-IP Audio Connections? y
IP Audio Hairpinning? n
Enable Layer 3 Test? n
Session Establishment Timer(min): 3
```

Figure 12: Signaling Group 11
3.1.7.2 Establish the SIP Trunk Group

Using the “add trunk-group 11” command, configure trunk group 11 as follows.

On Page 1 of the Trunk Group form:
- **Group Type**: set to “sip”.
- **Group Name**: enter a descriptive string such as “SIP OB PSTN TRKS”.
- **TAC**: enter a trunk access code such as “#011”.
- **Service Type**: set to “public-ntwrk” for trunks to the PSTN.
- **Signaling Group**: set to “11” as defined within Section 3.1.7.1.
- **Number of Members**: set to the maximum number of simultaneous calls permitted for each trunk group. Within these Application Notes, “10” was used.

The default values are used on the remaining pages of the trunk-group form. The resulting form for trunk-group 11 is shown below.

```
add trunk-group 11

TRUNK GROUP
Group Number: 3                  Group Type: sip
Group Name: SIP OB PSTN TRKS     CDR Reports: y
COR: 1                           TAC: #011
Direction: two-way                Night Service:
Outgoing Display? n
Dial Access? n                    Queue Length: 0
Service Type: public-ntwrk       Auth Code? n
Signaling Group: 11
Number of Members: 10
```

Figure 13: SIP Trunk Group 11

3.1.8. Define Inbound SIP Trunk Group

A second SIP trunk group is defined for incoming calls from other customers who used the Telcordia SIR to determine routing information. These customers may have an unknown far-end domain.

The SIP trunk group configured here implements the recommended Avaya practice of configuring at least one signaling-group with a blank “Far-end Domain” as specified in the SIP trunk engineering notes section of Reference [4]. This permits Avaya Communication Manager Release 4.0 and later to accept incoming SIP calls from unknown domains.

3.1.8.1 Establish the SIP Signaling Group

Using the “add signaling-group 1” command, configure signaling group 1 as follows:
- **Group Type**: set to “sip”.
- **Transport Method**: automatically set to “tls”. The Transport Layer Security (TLS) transport protocol is used between Avaya Communication Manager and the Avaya SES. Note this is not the transport protocol used to communicate between the Avaya SES and the Telcordia SIR.
• **Near-end Node Name**: set to the C-LAN node name (defined in Section 3.1.2) used for the respective signaling group. In these Application Notes, “clan_01a03” is used for signaling group 1.

• **Far-end Node Name**: set to the Avaya SES. In these Application Notes, the node name “ses” is used as defined in Section 3.1.2.

• **Near-end Listen Port**: set to “5061”, the default port for SIP signaling using tls transport.

• **Far-end Listen Port**: set to “5061”.

• **Far-end Network Region**: set to “11”, the network region defined in Section 3.1.6.

• **Far-end Domain**: leave blank. This permits incoming calls from unknown domains to be accepted.

• **Direct IP-IP Audio Connections**: set to “y”, indicating the RTP paths should be optimized to reduce the use of media processing resources when possible.

• **DTMF over IP**: set to “rtp-payload”. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833 [9].

The default values for the other fields are used.

The resulting form for signaling group 1 is shown below.

```
add signaling-group 1

SIGNALING GROUP
Group Number: 1
Group Type: sip
Transport Method: tls

Near-end Node Name: clan_01a03
Near-end Listen Port: 5061

Far-end Node Name: ses
Far-end Listen Port: 5061
Far-end Network Region: 11
Far-end Domain: 
Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload
Direct IP-IP Audio Connections? y
IP Audio Hairpinning? n
Enable Layer 3 Test? n
Session Establishment Timer(min): 3
```

**Figure 14: Signaling Group 11**

### 3.1.8.2 Establish the SIP Trunk Group

Using the “add trunk-group 1” command, configure trunk group 1 as follows.

On Page 1 of the Trunk Group form:

• **Group Type**: set to “sip”.

• **Group Name**: enter a descriptive string such as “SIP IB TRK”.

• **TAC**: enter a trunk access code such as “#001”.

• **Service Type**: set to “public-ntwrk” for trunks to the PSTN.
• **Signaling Group**: set to “1” as defined within Section 3.1.8.1.
• **Number of Members**: set to the maximum number of simultaneous calls permitted for each trunk group. Within these Application Notes, “10” was used.

The default values are used on the remaining pages of the trunk-group form. The resulting form for trunk-group 1 is shown below.

```
add trunk-group 1

TRUNK GROUP

Group Number: 1          Group Type: sip
Group Name: SIP IB TRKS   CDR Reports: y
Direction: two-way        COR: 1
Dial Access? n            TN: 1
Queue Length: 0           TAC: #001
Service Type: public-ntwrk Night Service:
Auth Code? n

Signaling Group: 1
Number of Members: 10
```

**Figure 15: SIP Trunk Group 1**

### 3.1.9. Configure Calling Party Number Information

The SIP “From” header shown below contains information about the calling party. The header contains the calling party number (e.g., “19085561000”) in the userinfo segment and a domain (or IP address) in the hostname segment separated by an “@” sign.

```
From: "Jane Smith" <sip:19085561000@customer-sipdomain.com>;tag=80f839da25
```

The “public-unknown-numbering” command controls the calling party number sent in the userinfo segment. The Authoritative Domain field of the near-end IP Network Region form completed in Figure 10 associated with the SIP trunk group sets the hostname segment.

Public-unknown-numbering must always be setup. In these Application Notes the public-unknown-numbering is configured to send an 11 digit number corresponding to the assigned DID numbers.

Using the “change public-unknown-numbering n” command (where “n” is the leading digit of the extension range), specify the calling party number information as follows:

• **Ext Len**: set to “4”, the length of the extensions used.
• **Ext Code**: set to the leading digit of the extension used. In these Application Notes “60” is entered to cover the assigned extensions of 60xx.
• **Trk Grp(s)**: by default, leave blank to perform the same conversion across all SIP (and ISDN) trunk groups.
- **CPN Prefix**: set to the leading digits (e.g., “190855610”) that are to be sent as the calling party number.
- **Total CPN Len**: set to the total length (e.g., “11”) of the calling party number to be sent. The extension number will be appended to the **CPN Prefix** to form complete calling party number of **Total CPN Len** digits.

The completed public-unknown-numbering form is shown below.

<table>
<thead>
<tr>
<th>Ext Len Code</th>
<th>Trk Grp(s)</th>
<th>CPN Prefix</th>
<th>Total CPN Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 60</td>
<td></td>
<td>190855610</td>
<td>11</td>
</tr>
</tbody>
</table>

**Figure 16: Public Unknown Numbering**

### 3.1.10. Configure Call Routing

#### 3.1.10.1 Outbound Calls

In these Application Notes, Automatic Route Selection (ARS) is used to route outbound calls via the SIP trunk group to the Telcordia SIR. The Telcordia SIR (and the subscribed XYZ Corp.) expects to receive the following digits in the SIP INVITE message.

<table>
<thead>
<tr>
<th>Type of Call</th>
<th>Digits Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local and Long Distance in North American Numbering Plan</td>
<td>Digit 1 plus any 10 digits</td>
</tr>
</tbody>
</table>

**Table 2: Outbound Dialing Rule**

Here, the configuration of one outbound calling pattern supporting calls to 1-908-xxx-xxx is shown. A typical installation will generally require additional ARS dial string and route pattern entries but that is beyond the scope of these Application Notes. Further information on ARS administration is discussed in References [1] and [3].

ARS administration begins by verifying the availability of the feature as shown in Section 3.1.1.

Following the verification, use the “change dialplan analysis” command to create a feature access code (fac) for ARS use.

- **Dialed String**: enter “9” that will become the user dialed prefix for outbound calls.
- **Total Length**: enter “1” as the length of the prefix.
- **Call Type**: enter “fac” as the type of prefix.
### Figure 17: Dial Plan Analysis

Use the “change feature-access-codes” command to assign the feature access code “9” to **Auto Route Selection (ARS) - Access Code 1** as shown below.

### Figure 18: ARS Feature Access Code

Use the “change ars analysis nn” command to configure the ARS route pattern selection rules as follows. Here “nn” is “19”, the first two digits of the dialed number after the ARS access code.

- **Dialled String**: enter the leading digits (e.g., “1908”) necessary to uniquely select the desired route pattern.
- **Total Min**: enter the minimum number of digits (e.g., “11”) expected for this PSTN number.
- **Total Max**: enter the maximum number of digits (e.g., “11”) expected for this PSTN number.
• **Route Pattern**: enter the route pattern number (e.g., “3”) to be used. The route pattern (to be defined next) will specify the trunk group(s) to be used for calls matching the dialed number.

• **Call Type**: enter “fnpa”, the call type for North American 1+10 digit calls.

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Min</th>
<th>Total Max</th>
<th>Route Pattern</th>
<th>Call Type</th>
<th>Node Num</th>
<th>ANI Reqd</th>
</tr>
</thead>
<tbody>
<tr>
<td>1908</td>
<td>11</td>
<td>11</td>
<td>3</td>
<td>fnpa</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 19: ARS Digit Analysis Entries**

Next the route pattern used for the Telcordia SIR calls is specified. This route pattern must contain at least two choices:

- the SIP trunk group used to reach the Telcordia SIR
- a second trunk group used as a next choice in the event the dialed number is not subscribed to the Telcordia SIR.

Use the “change route-pattern n” command (where “n” is the **Route Pattern** number used above) to specify the SIP trunk groups selected for the outbound call.

In the form:

- **Pattern Name**: enter a descriptive string such as “Telcordia SIR LD” to describe the routing pattern.
- **Secure SIP?**: leave as “n”, the default.
- **Grp No**: enter the trunk groups to be used in priority order. Trunk group 11 is the first choice SIP trunk group to the Telcordia SIR. A second trunk group 7 (not shown) is used to provide a second choice route when the Telcordia SIR returns the subscriber not found status.
- **FRL**: enter the minimum facility restriction level (e.g., 1) necessary to use this trunk group, with 0 being the least restrictive. The FRL within the Class of Restriction (COR) assigned to the station must be greater than or equal to 1 in this case to use these trunk groups.
- **Pfx Mrk**: enter “1”, to always send the prefix 1 on 10 digit calls.
The defaults values for the remaining fields are used. The completed route pattern form is shown below.

<table>
<thead>
<tr>
<th>Pattern Number: 3</th>
<th>Pattern Name: Telcorida SIR LD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grp FRL NPA Pfx</td>
<td>Hop Toll No. Inserted DCS/IXC</td>
</tr>
<tr>
<td>No Mrk Lmt List Del Digits QSIG</td>
<td></td>
</tr>
<tr>
<td>1: 11 1 1 n user</td>
<td></td>
</tr>
<tr>
<td>2: 7 1 1 n user</td>
<td></td>
</tr>
<tr>
<td>3: n user</td>
<td></td>
</tr>
<tr>
<td>4: n user</td>
<td></td>
</tr>
<tr>
<td>5: n user</td>
<td></td>
</tr>
<tr>
<td>6: n user</td>
<td></td>
</tr>
<tr>
<td>BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR</td>
<td></td>
</tr>
<tr>
<td>0 1 2 M 4 W Request Dgts Format Subaddress</td>
<td></td>
</tr>
<tr>
<td>1: y y y y y n n rest next</td>
<td></td>
</tr>
<tr>
<td>2: y y y y y n n rest none</td>
<td></td>
</tr>
<tr>
<td>3: y y y y y n n rest none</td>
<td></td>
</tr>
<tr>
<td>4: y y y y y n n rest none</td>
<td></td>
</tr>
<tr>
<td>5: y y y y y n n rest none</td>
<td></td>
</tr>
<tr>
<td>6: y y y y y n n rest none</td>
<td></td>
</tr>
</tbody>
</table>

Figure 20: Route Pattern 3

Use the “change locations” command to designate the SIP trunk route pattern (route pattern 3 below) in the Proxy Sel. Rte. Pat. field if not previously set.

<table>
<thead>
<tr>
<th>Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARS Prefix 1 Required For 10-Digit NANP Calls? y</td>
</tr>
<tr>
<td>Loc Name</td>
</tr>
<tr>
<td>No Offset FAC FAC Parm</td>
</tr>
<tr>
<td>1: Main + 00:00</td>
</tr>
<tr>
<td>2:</td>
</tr>
</tbody>
</table>

Figure 21: Location Form Administration

3.1.10.2 Incoming Calls

This step configures the routing of incoming DID numbers to the associated Avaya Communication Manager extensions.

In these Application Notes, the incoming PSTN DID numbers 1-908-556-1000 through 1001 are configured. They are assigned to extensions as shown in Table 3.

<table>
<thead>
<tr>
<th>Dialed PSTN Number</th>
<th>Digits Received (within SIP INVITE message)</th>
<th>Extension Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>908 556 1000</td>
<td>908 556 1000</td>
<td>6000</td>
</tr>
<tr>
<td>908 556 1001</td>
<td>908 556 1001</td>
<td>6001</td>
</tr>
</tbody>
</table>

Table 3 - Incoming Number Assignments
Use the “change inc-call-handling-trmt trunk-group n” command (where “n” is the SIP trunk group number “1”) to administer the incoming number routing. This administration must be done for each incoming trunk group.

- **Called Len**: enter the total number of incoming digits received (e.g., “10”).
- **Called Number**: enter the specific digit pattern to be matched.
- **Del**: enter the number of leading digits that should be deleted
- **Insert**: enter the specific digits to be inserted at the beginning of the adjusted incoming digit string (to form what should be the complete number).

The completed inc-call-handling-trmt form for trunk group 1 is shown below.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Called Len</th>
<th>Called Number</th>
<th>Del</th>
<th>Insert</th>
</tr>
</thead>
<tbody>
<tr>
<td>public-ntwrk</td>
<td>10</td>
<td>9085561000</td>
<td>10</td>
<td>6000</td>
</tr>
<tr>
<td>public-ntwrk</td>
<td>10</td>
<td>9085561001</td>
<td>10</td>
<td>6001</td>
</tr>
</tbody>
</table>

3.1.11. **Save Avaya Communication Manager Changes**

This completes the configuration of Avaya Communication Manager.

Use the “save translation” command to make the changes permanent.

4. **Configure Avaya SIP Enablement Services**

This section covers the administration of Avaya SIP Enablement Services. Avaya SIP Enablement Services is configured via an Internet browser using SIP Server Management screens. It is assumed that Avaya SIP Enablement Services software and the license file have been previously installed. During the software installation, the “initial_setup” installation script was run to specify the IP network properties of the server including DNS server address(es). For additional information on these installation tasks, refer to Reference [6].
For reference purposes, Figure 22 illustrates the IP Network Configuration entered into the Avaya SES during installation.

![Figure 22 - Avaya SES Initial Setup Information](image)

### 4.1. SIP Connection to the Telcordia SIR

#### 4.1.1. Log in to Avaya SIP Enablement Services

Access the Avaya SES SIP Server Management pages by entering “http://<ip-addr>/admin” as the URL in an Internet browser, where “<ip-addr>” is the IP address of Avaya SIP Enablement Services server. In these Application Notes, the URL “http://150.100.100.130/admin” is used.

Log in with the appropriate credentials and then select the **Launch Administration Web Interface** link from the main page as shown in Figure 23.

![Figure 23: Avaya SES Main Page](image)
The Avaya SES administration home page shown in Figure 24 is displayed.

4.1.2. Verify System Properties

From the left pane of any SIP Server Management page, expand the Server Configuration option and select System Properties. This page displays the Avaya SES Version and the Network Properties entered via the install script during the installation process.
In the **Edit System Properties**, page note the **SIP Domain** was entered during the initial installation. The **SIP Domain** “customer-sipdomain.com” is used in these Application Notes.

Note that throughout the SES administration screens, the Help link may be used at anytime for further information regarding the meaning of any fields.

![System Properties](image)

**Figure 25: System Properties**
4.1.3. Verify the Avaya SES Host Information

Verify the Avaya SES Host information using the Edit Host page. In these Application Notes the Avaya SES Host Type is a combined “home/edge”. This means that a single Avaya SES routes SIP messages between the Telcordia SIR and Avaya Communication Manager. (Note that separate Avaya SES home and edge servers may exist in other configurations. Communications with the Telcordia SIR will always occur via the edge Avaya SES.)

Navigate to the Edit Host page (Figure 26) by following the Hosts link in the left navigation pane and then clicking on the Edit option under the Commands section of the List Hosts screen.

On the Edit Host screen:
- Verify that the IP address of this combined Avaya SES Home/Edge server is in the Host IP Address field.
- Do not modify the DB Password or Profile Service Password fields. If these fields are changed, exit the form without using the Update button. These values must match the values entered during the Avaya SES installation; incorrect changes may disable the Avaya SES.
- Verify that the UDP, TCP and TLS checkboxes are enabled as Listen Protocols.
- Verify that TLS is selected as the Link Protocol.
- Ensure that the Outbound Proxy and Outbound Direct Domains fields are left blank.
- Default values for the remaining fields may be used.
- Click the Update button only if changes are necessary. Otherwise, exit the Edit Host page by selecting the Top link on the left navigation bar.
4.1.4. Add Avaya Communication Manager Media Server Interface

In these Application Notes, one media server signaling interface named “CLAN-1A03-5061” is used with Avaya Communication Manager.

Expand the Media Servers option within any Avaya SES SIP Server Management page, and select Add to display the Add Media Server page (Figure 27).
In the Add Media Server Interface page, enter information corresponding to the signaling group “11” entry performed in Section 3.1.7.1.

- Enter “CLAN-1A03-5061” as the descriptive name in the Media Server Interface Name field.
- Select the Avaya SES home/edge IP address in the Host field.
- Select “TLS” (Transport Link Security) for the SIP Trunk Link Type. TLS provides encryption at the transport layer between Avaya Communication Manager and the Avaya SES.
- Enter the IP address of the “clan-1a03” interface in the SIP Trunk IP Address field as defined in Figure 4. Note: This may be the IP address of the “Processor Ethernet” interface in other Avaya Communication Manager configurations.

After completing the Add Media Server Interface page, click on the Add button.

![Figure 27: Add Media Server Interface for Voice Calls](image)

When these operations are completed, the List Media Servers page will appear as shown in Figure 28.
4.1.5. Configure Call Routing

4.1.5.1 Background

Avaya SIP Enablement Services functions as a SIP proxy for the SIP trunking with the Telcordia SIR. The Avaya SES examines the SIP Request URI of an incoming SIP INVITE message, modifies the SIP Request URI and certain SIP headers and then forwards the message to the appropriate destination.

The SIP Request URI generally takes the form of `sip:user@domain`, where `domain` can be a fully qualified domain name or an IP address. The `user` part for SIP trunking in these Application Notes contains the called number digits identifying the telephone number being called.

The SIP messages are routed to the IP address associated with the `domain` part when the `domain` does not match the SIP domain of the Avaya SES (Figure 25) and the outbound proxy is not specified. This rule applies to all outbound calls to the Telcordia SIR in these Application Notes.

The Avaya SES address maps are used to route SIP Messages when the `domain` part matches the Avaya SES SIP domain. In this case, the `user` part is compared to address map patterns specified in the Avaya SES and when a pattern match is found the SIP messages are routed to the
corresponding signaling contact address destination. The address map patterns are specified using Linux regular expression syntax. Patterns are designed to match a collection of called numbers that require identical SIP message routing and must be specific enough to direct each unique called number to the proper signaling contact. Appendix A provides a detailed description of the Linux regular expression syntax used within the address map patterns.

The media server address maps are used to route all incoming SIP trunk calls to Avaya Communication Manager in these Application Notes.

4.1.5.2 Outbound Calls Using the Telcordia SIR
In these Application Notes, the domain value of the SIP Request URI for outbound calls to the Telcordia SIR is specified by the Far-end Domain field of the signaling group 11 form (Section 3.1.7.1) of the outbound SIP trunk.

Since this domain value specifies the Telcordia SIR, no additional administration is necessary in the Avaya SES for outbound calls.

4.1.5.3 Inbound Direct Inward Dialed Calls
SIP messages for incoming calls directed by the Telcordia SIR are sent to the Avaya SES. The Avaya SES then routes these messages to the appropriate Avaya Communication Manager using Avaya SES media server address maps.

In these Application Notes, the incoming PSTN calls use media server address map patterns matching the 10-digit called number in the user part of the SIP Request URI.

An example of a SIP Request URI in an INVITE message received for the DID number 908-556-1000 is:

```
sip:9085561000@150.100.100.130
```

The user part in this case is the 10-digit number “9085561000”.

Table 4 below summarizes the media server address map strategy used in these Application
Notes for incoming calls.

<table>
<thead>
<tr>
<th>Dialed PSTN Number</th>
<th>SIP Request URI User Part</th>
<th>SES Media Server Address Map Pattern</th>
<th>Media Server Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>908-556-1000 through 908-556-1001</td>
<td>9085561000 through 9085561001</td>
<td>^sip:908556100[01]</td>
<td>CLAN-1A03-5061</td>
</tr>
</tbody>
</table>

**Table 4: Incoming DID Address Map Rules Used**

To configure the media server address map for voice calls:

- Expand the **Media Servers** link in the left navigation menu of any SIP Server Management page. Select **List** to display the List Media Servers screen shown in **Figure 29**.
- Click on the **Map** link to display the List Media Server Address Map screen associated with the “CLAN-1A03-5061” **Interface**.

![Figure 29: List Media Servers](image)

- Since no previous media server address map exists, click on the **Add Map In New Group** link as shown in **Figure 30**.

![Figure 30 - List Media Server Address Map](image)

The Add Media Server Address Map page shown in **Figure 31** is displayed.
- Enter a descriptive name in the **Name** field, such as “DID-908556100x”.

JSR; Reviewed: Solution & Interoperability Test Lab Application Notes
SPOC 4/25/2008 ©2008 Avaya Inc. All Rights Reserved. Telcordia-SIR
• Enter the **Address Map Pattern** for incoming DID calls (from **Table 4** ) into the **Pattern** field.

The pattern specification for these DID numbers is:

```
^sip:908556100[01]
```

This means that URIs beginning with “sip:908556100” followed either 0 or 1 will match the pattern and be routed to the interface defined as “CLAN-1A03-5061”.

• Click the **Add** button once the form is completed.

![Add Media Server Address Map](image)

**Figure 31: Incoming DID Calls - Media Server Address Map**

After configuring the media server address maps, the **List Media Server Address Map** page appears as shown in **Figure 32**.

![List Media Server Address Map](image)

**Figure 32: List Media Server Address Map**
Note that after the first media server address map is created, a corresponding media server Contact entry is created automatically.

```
sip:$(user)@150.100.100.113:5061;transport=tls
```

This Contact entry contains the IP address of the “CLAN-1A03” interface on Avaya Communication Manager, the port (5061) and the transport protocol (tls) to be used. The incoming digits sent in the user part of the original request URI will replace the $(user) string when the message is sent.

### 4.1.6. Specify the Telcordia SIR as a Trusted Host

The Telcordia SIR IP address (e.g., 225.132.6.98) must be added as a trusted host entry in the Avaya SES. As a trusted host, the Avaya SES will not attempt to authenticate incoming requests from the designated IP address.\(^1\)

To add the trusted host entry:

- Expand the **Trusted Hosts** link in the left navigation menu of any SIP Server Management page. Select **Add** to display the Add Trusted Host screen shown in **Figure 33**.
- Enter the Telcordia SIR IP address (e.g., “225.132.6.98”) into the **IP Address** field.
- Select “150.100.100.130” (the address of the Avaya SES) as the value of the **Host** field.
- Enter a description (e.g. “Telcordia SIR”) in the **Comment** field.
- Click the **Add** button once the form is completed.

![Figure 33 - Add Trusted Host](image)

The resulting List Trusted Hosts page should appear as shown in **Figure 34**.

---

\(^1\) If the trusted host step is not done, authentication challenges to incoming SIP messages (such as INVITEs and BYEs) will be issued by Avaya SES. This may cause call setup to fail, active calls to be disconnected after timeout periods, and/or SIP protocol errors.
4.1.7. Save the Avaya SES Changes

After making any changes within Avaya SES, commit the database changes by using the Update link.

Perform this step by clicking on either Update link on any SIP Server Management page as shown in Figure 35.

5. Verification Steps

5.1. Verification Tests

This section provides steps that may be performed to verify the operation of the SIP trunking configuration described in the Application Notes.
• Outbound Calls
  o Verify that calls placed to a telephone number registered in the Telcordia SIR are routed via the assigned SIP outbound trunk group. Verify that the talk-path exists in both directions and that calls remain stable and disconnect properly.

  Examining the SIP traces of this call should indicate a SIP INVITE message sent to Telcordia SIR with a resulting 302 redirect. A “list trace station” should show the call is using the first choice SIP trunk group.

  o Verify that a call placed to a telephone number not subscribed within the Telcordia SIR is routed via the second choice trunk group.

  Examining the SIP traces of this call should indicate a SIP INVITE message sent to Telcordia SIR with a resulting 406 final status returned. A “list trace station” should show the overflow to the second choice route trunk group.

• Inbound Calls
  o Verify that an incoming call from another known Telcordia SIR subscriber (who attempts to call via the Internet) is successfully received via the incoming SIP trunk group.

  Examining a SIP trace should show an incoming call from the far end subscriber. A “list trace station” or “list trace tac” should show the expected SIP trunk group being used.

  o Verify that an incoming call from a normal PSTN telephone (not a Telcordia SIR subscriber) is received over the expected trunk group.

• Direct IP-IP Connections – This applies if IP and/or SIP telephones and Direct IP-IP are used. Verify that stable calls are using Direct IP-IP talk paths using the “status station” or “status trunk-group” commands. When Direct IP-IP is used, the Audio Connection field will indicate “ip-direct” instead of “ip-tdm”.

5.2. Troubleshooting Tools
The Avaya Communication Manager “list trace station”, “list trace tac”, “status station” and/or “status trunk commands are helpful diagnostic tools to verify correct operation and to troubleshoot problems. Diagnostic traces (performed by Avaya support) can be helpful in understanding the specific SIP interoperability issues.

The “Trace Logger” function within the Avaya SES Administration Web Interface may be used to capture SIP traces between Avaya SES and the Telcordia SIR. These traces can be instrumental in understanding SIP protocol issues resulting from configuration problems.
If port monitoring is available, a SIP protocol analyzer such as WireShark (a.k.a., Ethereal) to monitor the SIP messaging at the various interfaces is a very powerful tool for troubleshooting. Note that SIP messaging between Avaya Communication Manager and Avaya SES uses TLS encryption and cannot be viewed using WireShark.

6. Conclusion

These Application Notes describe the steps for configuring SIP trunking between an Avaya Communication Manager based SIP telephony solution and Telcordia SIR.

The configuration shown in these Application Notes is representative of a typical enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

Further information on the Avaya DevConnect program can be found at http://www.avaya.com/devconnect.
7. References


Several Internet Engineering Task Force (IETF) RFC documents were referenced within these Application Notes. The RFC documents may be obtained at: http://www.rfc-editor.org/rfcsearch.html.

APPENDIX A: Specifying Pattern Strings in Address Maps

The syntax for the pattern matching used within the Avaya SES is a Linux regular expression used to match against the URI string found in the SIP INVITE message.

Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special metacharacters, which may represent items like quantity, location or types of character(s).

In the pattern matching string used in the Avaya SES:

- Normal text characters and numbers match themselves.
- Common metacharacters used are:
  - A period . matches any character once (and only once).
  - An asterisk * matches zero or more of the preceding characters.
  - Square brackets enclose a list of any character to be matched. Ranges are designated by using a hyphen. Thus the expression \[12345\] or \[1-5\] both describe a pattern that will match any single digit between 1 and 5.
  - Curly brackets containing an integer ‘n’ indicate that the preceding character must be matched exactly ‘n’ times. Thus 5\{3\} matches ‘555’ and \[0-9\]{10} indicates any 10 digit number.
  - The circumflex character ^ as the first character in the pattern indicates that the string must begin with the character following the circumflex.

Putting these constructs together as used in this document, the pattern to match the SIP INVITE string for any valid 1+ 10 digit number in the North American dial plan would be:

\(^\text{sip:1[0-9]}\{10\}\)

This reads as: “Strings that begin with exactly \text{sip:1} and having any 10 digits following will match.

A typical INVITE request below uses the shaded portion to illustrate the matching pattern.

```plaintext
INVITE sip:17325551638@20.1.1.54:5060;transport=udp SIP/2.0
```