Abstract

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Aura™ Communication Manager 5.2 and Nortel Communication Server 1000 using SIP trunks.

For the sample configuration, Avaya Aura™ Session Manager runs on an Avaya S8510 Server, Avaya Aura™ Communication Manager 5.2 runs on an Avaya S8720 Server with Avaya G650 Media Gateway, and Nortel Communication Server 1000 runs on Nortel Communication Server 1000S. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura™ Communication Manager 5.2.
1 Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Aura™ Communication Manager 5.2 and Nortel Communication Server 1000 using SIP trunks.

As shown in Figure 1, the Avaya 9630 IP Telephone (H.323) and 6408D+ Digital Telephone are supported by Avaya Aura™ Communication Manager 5.2. The Nortel i2004 H.323 Telephone and 3904 Digital Telephone are supported by Nortel Communication Server 1000. SIP trunks are used to connect these two systems to Avaya Aura™ Session Manager, using its SM-100 (Security Module) network interface. All inter-system calls are carried over these SIP trunks. Avaya Aura™ Session Manager can support flexible inter-system call routing based on dialed number, calling number and system location, and can also provide protocol adaptation to allow multi-vendor systems to interoperate. It is managed by a separate Avaya Aura™ System Manager, which can manage multiple Avaya Aura™ Session Managers by communicating with their management network interfaces. Configurations supporting SIP telephones still require Avaya SIP Enablement Services, and are not addressed in these application notes.

For the sample configuration, Avaya Aura™ Session Manager runs on an Avaya S8510 Server, Avaya Aura™ Communication Manager 5.2 runs on an Avaya S8720 Server with Avaya G650 Media Gateway, and Nortel Communication Server 1000 runs on Nortel Communication Server 1000S. The results in these Application Notes should be applicable to other Avaya Aura™ servers and Media Gateways.

Figure 1 – Sample Configuration

A five digit Uniform Dial Plan (UDP) is used for dialing between systems. Unique extension ranges are associated with Avaya Aura™ Communication Manager 5.2 (30xxx) and Nortel Communication Server 1000 (53xxx).
These Application Notes will focus on the configuration of the SIP trunks and call routing. Detailed administration of the endpoint telephones will not be described (see the appropriate documentation listed in Section 8).

2 Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Hardware Component</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8510 Server</td>
<td>Avaya Aura™ Session Manager Release 1.1.3.1.18022 Quick Fix “asset-gefanuc-1.1.3.0.18005-1.i386.rpm” Avaya Aura™ System Manager, Release 1.1.3.1.18022</td>
</tr>
<tr>
<td>Avaya S8720 Servers with G650 Media Gateway</td>
<td>Avaya Aura™ Communication Manager 5.2 Load 947.3 Patch 17250</td>
</tr>
<tr>
<td>Avaya 9630 IP Telephone (H.323)</td>
<td>2.0</td>
</tr>
<tr>
<td>Avaya 6408D+ Digital Telephone</td>
<td>-</td>
</tr>
<tr>
<td>Nortel Communication Server 1000S</td>
<td>Nortel Communication Server 1000 Release 450w, Version 2121 sse-4.50.88</td>
</tr>
<tr>
<td>• Call Server</td>
<td></td>
</tr>
<tr>
<td>• Signaling Server</td>
<td></td>
</tr>
<tr>
<td>Nortel 3904 Digital Telephone</td>
<td>NA</td>
</tr>
<tr>
<td>Nortel I2004 H.323 Telephone</td>
<td>C502B41</td>
</tr>
</tbody>
</table>

3 Configure Avaya Aura™ Communication Manager 5.2

This section provides the procedures for configuring Avaya Aura™ Communication Manager 5.2. The procedures include the following areas:

- Verify Avaya Aura™ Communication Manager 5.2 license
- Administer system parameters features
- Administer IP node names
- Administer IP interface
- Administer IP codec set and network region
- Administer SIP trunk group and signaling group
- Administer SIP trunk group members and route patterns
- Administer location and public unknown numbering
- Administer uniform dial plan and AAR analysis

Some administration screens have been abbreviated for clarity.
3.1 Verify Avaya Aura™ Communication Manager 5.2 License

Log into the System Access Terminal (SAT) to verify that the Avaya Aura™ Communication Manager 5.2 license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to Page 2, and verify that there is sufficient remaining capacity for SIP trunks by comparing the Maximum Administered SIP Trunks field value with the corresponding value in the USED column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

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

<table>
<thead>
<tr>
<th>display system-parameters customer-options</th>
<th>Page 2 of 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTIONAL FEATURES</td>
<td></td>
</tr>
<tr>
<td>IP PORT CAPACITIES</td>
<td></td>
</tr>
<tr>
<td>Maximum Administered H.323 Trunks: 800</td>
<td>200</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP Stations: 18000</td>
<td>2</td>
</tr>
<tr>
<td>Maximum Administered Remote Office Trunks: 0</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered Remote Office Stations: 0</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP eCons: 0</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Video Capable H.323 Stations: 0</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Video Capable IP Softphones: 0</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Administered SIP Trunks: 800</td>
<td>47</td>
</tr>
</tbody>
</table>

3.2 Configure System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers. Submit the change.

This feature is needed to be able to transfer an incoming/outgoing call from/to the remote switch back out to the same or another switch. For simplicity, the Trunk-to-Trunk Transfer field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented using Class Of Restriction or Class Of Service levels. Refer to the appropriate documentation in Section 8 for more details.

<table>
<thead>
<tr>
<th>change system-parameters features</th>
<th>Page 1 of 18</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEATURE-RELATED SYSTEM PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>Self Station Display Enabled? y</td>
<td></td>
</tr>
<tr>
<td>Trunk-to-Trunk Transfer: all</td>
<td></td>
</tr>
<tr>
<td>Automatic Callback with Called Party Queuing? n</td>
<td></td>
</tr>
<tr>
<td>Automatic Callback - No Answer Timeout Interval (rings): 3</td>
<td></td>
</tr>
<tr>
<td>Call Park Timeout Interval (minutes): 10</td>
<td></td>
</tr>
<tr>
<td>Off-Premises Tone Detect Timeout Interval (seconds): 20</td>
<td></td>
</tr>
<tr>
<td>DID/Tie/ISDN/SIP Intercept Treatment: attd</td>
<td></td>
</tr>
<tr>
<td>Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred</td>
<td></td>
</tr>
</tbody>
</table>
3.3 Configure IP Node Names

Use the “change node-names ip” command to add entries for the C-LAN that will be used for connectivity, its default gateway, and Avaya Aura™ Session Manager. In this case, “clan2” and “10.1.2.234” are entered as Name and IP Address for the C-LAN, “asm” and “10.1.2.170” are entered for Avaya Aura™ Session Manager Security Module (SM-100) interface, and “Gateway001” and “10.1.2.1” are entered for the default gateway. Note that “Gateway001” will be used in the form used to configure the IP interface for the C-LAN (see Section 3.4). The actual node names and IP addresses may vary. Submit these changes.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>clan2</td>
<td>10.1.2.234</td>
</tr>
<tr>
<td>Gateway001</td>
<td>10.1.2.1</td>
</tr>
<tr>
<td>asm</td>
<td>10.1.2.170</td>
</tr>
</tbody>
</table>

3.4 Configure IP Interface for C-LAN

Add the C-LAN to the system configuration using the “add ip-interface 1a03” command. The actual slot number may vary. In this case, “1a03” is used as the slot number. Enter the C-LAN node name assigned from Section 3.3 into the Node Name field.

Enter proper values for the Subnet Mask and Gateway Node Name fields. In this case, “24” and “Gateway001” are used to correspond to the network configuration in these Application Notes. Set the Enable Interface and Allow H.323 Endpoints fields to “y”. Default values may be used in the remaining fields. Submit these changes.

<table>
<thead>
<tr>
<th>Type: C-LAN</th>
<th>Slot: 01A03</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code/Suffix: TN799 D</td>
<td>Receive Buffer TCP Window Size: 8320</td>
</tr>
<tr>
<td>Enable Interface? y</td>
<td>Gatekeeper Priority: 5</td>
</tr>
<tr>
<td>VLAN: n</td>
<td>Allow H.248 Gateways? y</td>
</tr>
<tr>
<td>Network Region: 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPV4 PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Name: clan2</td>
</tr>
<tr>
<td>Subnet Mask: /24</td>
</tr>
<tr>
<td>Gateway Node Name: Gateway001</td>
</tr>
</tbody>
</table>

Ethernet Link: 2
Network uses 1’s for Broadcast Addresses? y
3.5 Configure IP Codec Sets and Network Regions

Configure the IP codec set to use for calls to the Nortel Communication Server 1000. Use the “change ip-codec-set n” command, where “n” is an existing codec set number to be used for interoperability. Enter the desired audio codec type in the Audio Codec field. Retain the default values for the remaining fields and submit these changes.

In addition to the “G.711MU” codec shown below, “G.729” and “G.729A” have also been verified to be interoperable with Nortel Communication Server 1000 via SIP trunks.

```
change ip-codec-set 1
```

<table>
<thead>
<tr>
<th>Codec Set: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Codec</td>
</tr>
<tr>
<td>1: G.711MU</td>
</tr>
<tr>
<td>2:</td>
</tr>
<tr>
<td>3:</td>
</tr>
</tbody>
</table>

In the test configuration, network region “1” was used for calls to the Nortel Communication Server 1000 via Avaya Aura ™Session Manager. Use the “change ip-network-region 1” command to configure this network region. For the Authoritative Domain field, enter the SIP domain name configured for this enterprise network (See Section 4.1). This value is used to populate the SIP domain in the From header of SIP INVITE messages for outbound calls. It is also must match the SIP domain in the request URI of incoming INVITEs from other systems. Enter a descriptive Name. For the Codec Set field, enter the corresponding audio codec set configured above in this section. Enable the Intra-region IP-IP Direct Audio, and Inter-region IP-IP Direct Audio. These settings will enable direct media between Avaya IP telephones and the far end. Retain the default values for the remaining fields, and submit these changes.

```
change ip-network-region 1
```

<table>
<thead>
<tr>
<th>IP NETWORK REGION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region: 1</td>
</tr>
<tr>
<td>Location:</td>
</tr>
<tr>
<td>Name: ASM to Nortel</td>
</tr>
<tr>
<td>Authoritative Domain: avaya.com</td>
</tr>
<tr>
<td>MEDIA PARAMETERS</td>
</tr>
<tr>
<td>Codec Set: 1</td>
</tr>
<tr>
<td>Intra-region IP-IP Direct Audio: yes</td>
</tr>
<tr>
<td>Inter-region IP-IP Direct Audio: yes</td>
</tr>
<tr>
<td>UDP Port Min: 2048</td>
</tr>
<tr>
<td>UDP Port Max: 10001</td>
</tr>
<tr>
<td>DIFFSERV/TOS PARAMETERS</td>
</tr>
<tr>
<td>Call Control PHB Value: 46</td>
</tr>
<tr>
<td>Audio PHB Value: 46</td>
</tr>
<tr>
<td>Video PHB Value: 26</td>
</tr>
<tr>
<td>RTCP Reporting Enabled? y</td>
</tr>
<tr>
<td>RTCP MONITOR SERVER PARAMETERS</td>
</tr>
<tr>
<td>Use Default Server Parameters? y</td>
</tr>
</tbody>
</table>
3.6 Configure SIP Signaling Group and Trunk Group

3.6.1 SIP Signaling Group

In the test configuration, trunk group “32” and signaling group “32” were used to reach Avaya Aura™ Session Manager. Use the “add signaling-group n” command, where “n” is an available signaling group number. Enter the following values for the specified fields, and retain the default values for all remaining fields. Submit these changes.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** C-LAN node name from Section 3.3.
- **Far-end Node Name:** Avaya Aura™ Session Manager node name from Section 3.3.
- **Near-end Listen Port:** “5061”
- **Far-end Listen Port:** “5061”
- **Far-end Network Region:** Avaya network region number “1” from Section 3.5.
- **Far-end Domain:** SIP domain name from Section 4.1.
- **DTMF over IP:** “rtp-payload”

```plaintext
add signaling-group 32
```

```
SIGNALING GROUP

Group Number: 32
Group Type: sip
Transport Method: tls

Near-end Node Name: clan2
Near-end Listen Port: 5061

Far-end Node Name: asm
Far-end Listen Port: 5061
Far-end Network Region: 1

Far-end Domain: avaya.com

Bypass If IP Threshold Exceeded? n

DTMF over IP: rtp-payload
Direct IP-IP Audio Connections? y
IP Audio Hairpinning? n
Direct IP-IP Early Media? n
Alternate Route Timer(sec): 6

Enable Layer 3 Test? n
Session Establishment Timer(min): 3
```
3.6.2 SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total trunks configure in Section 3.1).

```
add trunk-group 32
```

**TRUNK GROUP**

<table>
<thead>
<tr>
<th>Group Number: 32</th>
<th>Group Type: sip</th>
<th>CDR Reports: y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name: To ASM</td>
<td>COR: 1</td>
<td>TN: 1</td>
</tr>
<tr>
<td>Direction: two-way</td>
<td>TAC: 132</td>
<td></td>
</tr>
<tr>
<td>Dial Access? n</td>
<td>Outgoing Display? y</td>
<td>Night Service:</td>
</tr>
<tr>
<td>Queue Length: 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Type: tie</td>
<td>Auth Code? n</td>
<td></td>
</tr>
<tr>
<td>Signaling Group: 32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Members: 10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Navigate to Page 3, and enter “public” for the **Numbering Format** field as shown below. Use default values for all other fields. Submit these changes.

```
add trunk-group 32
```

**TRUNK FEATURES**

<table>
<thead>
<tr>
<th>ACA Assignment? n</th>
<th>Measured: none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance Tests? y</td>
<td></td>
</tr>
</tbody>
</table>

**Numbering Format: public**

| UUI Treatment: service-provider |
| Replace Restricted Numbers? n |
| Replace Unavailable Numbers? n |
3.7 Configure Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use the “change route-pattern n” command, where “n” is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name**: A descriptive name.
- **Grp No**: The trunk group number from Section 3.6.2.
- **FRL**: Enter a level that allows access to this trunk, with 0 being least restrictive.

```
change route-pattern 32
```

<table>
<thead>
<tr>
<th>Grp</th>
<th>FRL</th>
<th>NPA</th>
<th>Pfx</th>
<th>Hop</th>
<th>Toll No.</th>
<th>Inserted</th>
<th>SCCAN?</th>
<th>n</th>
<th>Secure SIP?</th>
<th>n</th>
<th>DCS/ IXC</th>
<th>n</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>32</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n</td>
<td>user</td>
<td></td>
<td></td>
<td>user</td>
<td></td>
</tr>
<tr>
<td>2:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n</td>
<td>user</td>
<td></td>
<td></td>
<td>user</td>
<td></td>
</tr>
<tr>
<td>3:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n</td>
<td>user</td>
<td></td>
<td></td>
<td>user</td>
<td></td>
</tr>
<tr>
<td>4:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n</td>
<td>user</td>
<td></td>
<td></td>
<td>user</td>
<td></td>
</tr>
<tr>
<td>5:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n</td>
<td>user</td>
<td></td>
<td></td>
<td>user</td>
<td></td>
</tr>
<tr>
<td>6:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n</td>
<td>user</td>
<td></td>
<td></td>
<td>user</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BCC VALUE</th>
<th>TSC</th>
<th>CA-TSC</th>
<th>ITC</th>
<th>BCIE Service/Feature PARM</th>
<th>No. Numbering LAR</th>
<th>Dgts Format</th>
<th>Subaddress</th>
<th>Digits</th>
<th>Intw</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 4 M W</td>
<td>Request</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1: y y y y y n n</td>
<td>rest</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3.8 Configure Location and Public Unknown Numbering

Use the “change locations” command to assign the SIP route pattern for Avaya SIP endpoints to a location corresponding to the Main site. Add an entry for the Main site if one does not exist already, enter the following values for the specified fields, and retain default values for the remaining fields. Submit these changes.

- **Name:** A descriptive name to denote the Main site.
- **Timezone:** An appropriate timezone offset.
- **Rule:** An appropriate daylight savings rule.
- **Proxy Sel. Rte. Pat.:** The Avaya route pattern number from Section 3.7.

<table>
<thead>
<tr>
<th>Loc No</th>
<th>Name</th>
<th>Timezone</th>
<th>Offset</th>
<th>NPA</th>
<th>Proxy Sel Rte Pat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Main</td>
<td>+00:00</td>
<td>0</td>
<td>32</td>
<td>32</td>
</tr>
</tbody>
</table>

Use the “change public-unknown-numbering 0” command, to define the calling party number to be sent to Nortel Communication Server 1000. Add an entry for the trunk group defined in Section 3.6.2 to reach Nortel endpoints. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed to trunk group 32 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header. Submit these changes.

<table>
<thead>
<tr>
<th>Ext Len</th>
<th>Ext Code</th>
<th>Trk Grp(s)</th>
<th>CPN Prefix Len</th>
<th>CPN Len</th>
<th>Total Administered</th>
<th>Maximum Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3</td>
<td>32</td>
<td>5</td>
<td>32</td>
<td>2</td>
<td>9999</td>
</tr>
</tbody>
</table>

ARS Prefix 1 Required For 10-Digit NANP Calls? y
3.9 Administer Uniform Dial Plan and AAR Analysis

This section provides sample Automatic Alternate Routing (AAR) used for routing calls with dialed digits 53xxx to Nortel Communication Server 1000. Note that other methods of routing may be used. Use the “change uniform-dialplan 0” command, and add an entry to specify use of AAR for routing of digits 53xxx. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Matching Pattern**: Dialed prefix digits to match on, in this case “53”.
- **Len**: Length of the full dialed number.
- **Del**: Number of digits to delete.
- **Net**: “aar”

Use the “change aar analysis 0” command, and add an entry to specify how to route the calls to 53xxx. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Dialed String**: Dialed prefix digits to match on, in this case “53”.
- **Total Min**: Minimum number of digits.
- **Total Max**: Maximum number of digits.
- **Route Pattern**: The route pattern number from Section 3.7.
- **Call Type**: “aar”

3.10 Save Translations

Configuration of Avaya Aura™ Communication Manager 5.2 is complete. Use the “save Translations command to save these changes.

4 Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Avaya Aura™ Session Manager. The procedures include adding the following items:
- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities corresponding to the SIP telephony systems and Avaya Aura™ Session Manager
- Entity Links, which define the SIP trunk parameters used by Avaya Aura™ Session Manager when routing calls to/from SIP Entities
- Time Ranges during which routing policies are active
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Avaya Aura™ Session Manager Server to be managed by Avaya Aura™ System Manager.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura™ System Manager, using the URL “http://<ip-address>/IMSM”, where “<ip-address>” is the IP address of Avaya Aura™ System Manager. Log in with the appropriate credentials and accept the Copyright Notice. The menu shown below is displayed. Expand the Network Routing Policy Link on the left side as shown. The sub-menus displayed in the left column below will be used to configure all but the last of the above items (Sections 4.1 through 4.7).
4.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting SIP Domains on the left and clicking the New button on the right. The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., “avaya.com”)
- **Notes:** Descriptive text (optional).

Click **Commit**.

Since the sample configuration does not deal with any other domains, no additional domains need to be added.
4.2 Add Locations
Locations can be used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management. Locations are added for the Avaya and the Nortel environments. To add a location, select Locations on the left and click on the New button on the right. The following screen will then be shown. Fill in the following:

Under General:
- **Name**: A descriptive name.
- **Notes**: Descriptive text (optional).

Under Location Pattern:
- **IP Address Pattern**: A pattern used to logically identify the location.
- **Notes**: Descriptive text (optional).
The screen below shows addition of the Lincroft location, which includes Avaya Aura™ Communication Manager 5.2 and Avaya Aura™ Session Manager. Click **Commit** to save each Location definition.

The following screen shows the addition of a second location based on the subnet used by Nortel Communication Server 1000.
The fields under **General** can be filled in to specify bandwidth management parameters between Avaya Aura™ Session Manager and this location. These were not used in the sample configuration, and reflect default values. Note also that although not implemented in the sample configuration, routing policies can be defined based on location.
4.3 Add SIP Entities

A SIP Entity must be added for Avaya Aura™ Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration a SIP Entity is added for the ASM, the C-LAN board in the Avaya G650 Media Gateway, and the Nortel Communication Server 1000. To add a SIP Entity, select SIP Entities on the left and click on the New button on the right. The following screen is displayed. Fill in the following:

Under General:
- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the ASM or the signaling interface on the telephony system.
- **Type:** “Session Manager” for Avaya Aura™ Session Manager, “CM” for Avaya Communication Manager, and “Other” for Nortel Communication Server 1000.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

Under Port, click Add, and then edit the fields in the resulting new row as shown below:
- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain** The domain used for the enterprise (e.g., “Avaya.com”).

Defaults can be used for the remaining fields. Click Commit to save each SIP Entity definition.
The following screen shows addition of Avaya Aura™ Session Manager. The IP address used is that of the SM-100 Security Module.
The following screen shows addition of Avaya Aura™ Communication Manager 5.2. The IP address used is that of the C-LAN board in the Avaya G650 Media gateway.
The following screen shows addition of Nortel Communication Server 1000. The IP address used is that of the “Voice LAN (TLAN) Node IP address”.
4.4 Add Entity Links

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

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Avaya Aura™ Session Manager.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of the other system.
- **Port:** Port number on which the other system receives SIP requests.
- **Trusted:** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity specified in **Section 4.3** will be denied.

Click **Commit** to save each Entity Link definition. The following screen shows the result of adding the two Entity Links for Avaya Aura™ Communication Manager 5.2 and Nortel Communication Server 1000.
4.5 Add Time Ranges

Before adding routing policies (see next section), time ranges must be defined during which the policies will be active. In the sample configuration, one policy was defined that would allow routing to occur at anytime. To add this time range, select Time Ranges, and click on the left and click on the New button on the right. Fill in the following:

- **Name:** A descriptive name (e.g., “Anytime”).
- **Mo through Su** Check the box under each of these headings
- **Start Time** Enter 00:00.
- **End Time** Enter 23:59

Click **Commit** to save this time range.
4.6 Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in Section 4.3. Two routing policies must be added—one for Avaya Aura™ Communication Manager 5.2 and one for Nortel Communication Server 1000. To add a routing policy, select Routing Policies on the left and click on the New button on the right. The following screen is displayed. Fill in the following:

Under General:
Enter a descriptive name in Name.

Under SIP Entity as Destination:
Click Select, and then select the appropriate SIP entity to which this routing policy applies.

Under Time of Day:
Click Add, and select the time range configured in the previous section.

Defaults can be used for the remaining fields. Click Commit to save each Routing Policy definition. The following screens show the Routing Policy for Avaya Aura™ Communication Manager 5.2 and one for Nortel Communication Server 1000.
4.7 Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 5-digit extensions beginning with “30” reside on Avaya Aura™ Communication Manager 5.2, and 5-digit extensions beginning with “53” reside on Nortel Communication Server 1000. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right. Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Avaya Aura™ Communication Manager 5.2:

Under **General:**
- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **Notes** Comment on purpose of dial pattern.

Under **Originating Locations and Routing Policies:**
Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screens show the dial pattern definitions for Avaya Aura™ Communication Manager 5.2 and Nortel Communication Server 1000.
4.8 Add Session Manager

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

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

**Under Security Module:**
- **Network Mask:** Enter the network mask corresponding to the IP address of Avaya Aura™ Session Manager
• Default Gateway: Enter the IP address of the default gateway for Avaya Aura™ Session Manager

Use default values for the remaining fields. Click **Save** to add this Session Manager.
5 Configure Nortel Communication Server 1000

Nortel Communication Server 1000 uses the Signaling Server to provide SIP and H.323 signaling interfaces to IP networks. The Signaling Server communicates with the NTDK20 Small System Controller card (also referred to as Call Server) over a private Ethernet interface.

There can be one or more Signaling Servers supported per Nortel Communication Server 1000 system. The applications that can run on the Signaling Server include the following:

- **SIP Gateway** Provides SIP signaling for IP networks.
- **Network Routing Service (NRS)** Provides SIP Redirect & Registrar service components.
- **NRS Manager** Provides web interface for NRS management.
- **Element Manager** Provides web interface for system administrative tasks.

The Nortel Communication Server 1000 in the interoperability test configuration contained one Signaling Server connected to a Call Server. The Element Manager was used to configure system resources such as SIP virtual routes and trunks, and the NRS Manager was used to configure the routing for SIP devices. These Application Notes assume that the basic configuration of the Signaling Server with the Call Server is in place and the configuration will not be described.

Furthermore, these Application Notes used the Coordinated Dial Plan (CDP) feature to route calls from the Nortel Communication Server 1000, over the SIP trunks to Avaya Aura™ Session Manager to reach endpoints on Avaya Aura™ Communication Manager 5.2. The CDP feature is assumed to be already enabled on Nortel Communication Server 1000, and therefore will not be described in detail.

The procedures below describe the details of configuring Nortel Communication Server 1000 for SIP trunks:

- Launch Element Manager
- Obtain node and IP addresses
- Administer ISDN
- Administer D-Channel
- Administer zones
- Administer virtual SIP routes and trunks
- Administer route list block and distant steering code
- Administer node SIP parameters
- Launch NRS Manager
- Administer service domain
- Administer SIP gateway endpoints
- Administer routing entry
- Cut over and commit changes
5.1 Launch Element Manager

Access the Nortel Communication Server 1000 web based interface Element Manager by using the URL “http://<ip-address>” in an Internet browser window, where “<ip-address>” is the IP address of the Signaling Server from Section 5.2. Note that the IP address for the Signaling Server may vary, and in this case “192.168.1.30” is used.

The CS 1000 ELEMENT MANAGER screen is displayed. Enter the appropriate credentials, retain the automatically populated value in the Call Server IP Address field, and click Login.

5.2 Obtain Node and IP Addresses

The Home – System Overview screen is displayed. Select IP Telephony > Nodes: Servers, Media Cards > Configuration in the left pane.
The Node Configuration screen is displayed. Click Node: 271 to expand it. Note that the node number and IP address may vary.

The Node Configuration screen is updated with additional details as shown below. Make a note of the Node number “271”, Node IP “192.168.1.33”, and Signaling Server IP address of “192.168.1.30”. These values are used to configure other sections.

Figure 2: Node Configuration
5.3 Administer ISDN

Select Customers in the left pane. The Customers screen is displayed. Click the Edit button associated with the appropriate customer. The system can support more than one customer with different network settings and options. In the sample configuration, only one customer was configured on the system.

The Customer 0 Property Configuration screen is displayed next. Select Feature Packages toward the bottom of the screen.
The screen is updated with a listing of feature packages populated below Feature Packages (not all features shown below). Scroll down the screen, and select Integrated Services Digital Network to edit its parameters.

![Feature Packages](image)

The screen is updated with parameters populated below Integrated Services Digital Network. Check the Integrated Services Digital Network (ISDN) checkbox, and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click Submit (not shown).

![Integrated Services Digital Network](image)

5.4 Administer D-Channel

Select Routes and Trunks > D-Channels from the left pane to display the D-Channels screen. In the Choose a D-Channel Number field, select an available D-channel from the drop-down list (in this case “8”). Click to Add.
The **D-Channels 8 Property Configuration** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields. Select **Basic options (BSCOPT)** toward the bottom of the screen to expand it.

- **D channel Card Type (CTYP):** “D-Channel is over IP (DCIP)”
- **Designator (DES):** A descriptive name.
- **User (USR):** “Integrated Services Signaling Link Dedicated (ISLD)”
- **Interface type for D-channel:** “Meridian Meridian1 (SL1)”
The screen is updated with additional parameters populated below Basic options (BSCOPT). Click Edit, next to Remote Capabilities (RCAP).

The **Remote Capabilities Configuration** screen is displayed next.

Scroll down the screen, and check the **Network name Display method 2 (ND2)** checkbox as shown below, followed by Return – Remote Capabilities. The D-Channels 8 Property Configuration screen is displayed again (not shown below). Click Submit.
5.5 Administer Zones
Select IP Telephony > Zones from the left pane to display the Zones screen. For the Please Choose the field, select an available zone number from the drop-down list (in this case “10”). Click to Add.

The Zone Basic Property and Bandwidth Management screen is displayed next. For the Intrazone Bandwidth (INTRA_BW) and Interzone Bandwidth (INTER_BW) fields, enter the maximum intra-zone and inter-zone bandwidth in Kbits/sec respectively for the network configuration. For the Interzone Strategy (INTER_STGY) field, select “Best Bandwidth (BB)” from the drop-down list. The Call Server considers the best quality codec to be G.711 and the best bandwidth codec to be G.729 or G.723. For the Zone Intent (ZBRN) field, select “VTRK (VTRK)” from the drop-down list. For the Description (ZDES) field, enter descriptive text. Retain the default values for all remaining fields, and click Submit.
5.6  Administer Virtual SIP Routes and Trunks

Select Routes and Trunks > Routes and Trunks from the left pane to display the Routes and Trunks screen. Next to the applicable Customer row, click Add route.

The Customer 0, New Route Configuration screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- Route Number (ROUT): Select an available route number.
- Designator field for trunk (DES): A descriptive text.
- Trunk Type (TKTP): “TIE trunk data block (TIE)”
- Incoming and Outgoing trunk (ICOG): “Incoming and Outgoing (IAO)”
Scroll down the screen, and check the field **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear. For the **Zone for codec selection and bandwidth management (ZONE)** field, enter the zone number from Section 5.5. For the **Node ID of signaling server of this route (NODE)** field, enter the node number from Section 5.2. Select “SIP (SIP)” from the drop-down list for the **Protocol ID for the route (PCID)** field.

Scroll down the screen, check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click **Submit** (not shown).

- **Mode of operation (MODE):** “Route uses ISDN Signaling Link (ISLD)”
- **D channel number (DCH):** D-Channel number from Section 5.4.
- **Network Call Redirection (NCRD):** Check the field.

The **Routes and Trunks** screen is displayed again, and updated with the newly added route. Click the **Add trunk** button next to the newly added route.
The **Customer 0, Route 8, New Trunk Configuration** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click **Submit**. The **Multiple trunk input number (MTINPUT)** field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. The total number of trunks should match the number of trunk group members provisioned in the SIP trunk from Avaya Aura™ Communication Manager 5.2 to Nortel in **Section 3.7**. In the sample configuration, only four trunks were created due to capacity limitation on Nortel Communication Server 1000.

- **Trunk data block (TYPE):** “IP Trunk (IPTI)”
- **Terminal Number (TN):** An available terminal number.
- **Designator field for trunk (DES):** A descriptive text.
- **Extended Trunk (XTRK):** “Virtual trunk (VTRK)”
- **Route number, Member number (RTMB):** Current route number and starting member.
- **Start arrangement Incoming (STRI):** “Wink or Fast Flash (WNK)”
- **Start arrangement Outgoing (STRO):** “Wink or Fast Flash (WNK)”
- **Trunk Group Access Restriction (TGAR):** Desired trunk group access restriction level.
- **Channel ID for this trunk (CHID):** An available starting channel ID.

![Nortel CS 1000 Element Manager](image.png)
5.7 Administer Route List Block and Distant Steering Code

Select Dialing and Numbering Plans > Electronic Switched Network from the left pane to display the Electronic Switched Network (ESN) screen. Select Route List Block (RLB).

The Route List Blocks screen is displayed. In the Please enter a route list index field, enter an available route list block number (in this case “10”). Click to Add.

Figure 3: Route List Blocks
The **Route List Block** screen is updated with a listing of parameters. For the **Route Number (ROUT)** field, select the route number from **Section 5.6**. Retain the default values for the remaining fields, and scroll down to the bottom of the screen and click **Submit** (not shown).

The **Electronic Switched Network (ESN)** screen is displayed again. Select **Distant Steering Code (DSC)** to add an entry to route 33xxx calls to Avaya Communication Manager.

The **Distant Steering Code List** screen is displayed next. In the **Please enter a distant steering code** field, enter the dialed prefix digits to match on (in this case “33”). Click **to Add**.
The **Distant Steering Code** screen is displayed. For the **Route List to be accessed for trunk steering code (RLI)** field, select the route list index in **Figure 3** of **Section 5.7** from the drop-down list. Retain the default values in all remaining fields, and scroll down to the bottom of the screen to click **Submit** (not shown).

### 5.8 Administer Node SIP Parameters

Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the left pane to display the **Node Configuration** screen. Click **Edit**.
The **Edit** screen is displayed next.

Scroll down the screen and click **VGW and IP phone codec profile** to expand it. Check the applicable audio codec checkboxes as shown below, and maintain the default values in all remaining fields.
Scroll down the screen and select **SIP GW Settings** to expand it. For the **Primary Proxy / Redirect IP address** field, enter the Signaling Server IP address from **Section 5.2**. Check the **Primary Proxy Supports Registration** checkbox, and retain the default values in the remaining fields.

Scroll down the screen and select **SIP URI Map** to expand it. For the **Public E.164/National domain name** and **Public E.164/Subscribers domain name** fields, enter the appropriate values for the network configuration. In the test configuration, “1” is the country code and “732” is the area code.
Scroll down the screen and select **Signaling Server** to expand it. Select **Signaling Server 192.168.0.3 Properties** to view a listing of parameters. Note that the displayed IP address for the Signaling Server may vary.

![Signaling Server Properties](image)

A list of parameters appears under **Signaling Server 192.168.0.3 Properties**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Hostname**: Enter a unique host name.
- **Enable IP Peer Gateway (Virtual Trunk TPS)**: “SIP only”
- **SIP Transport Protocol**: “TCP”
- **SIP Domain name**: SIP domain name from Section 4.1.
- **SIP Gateway Endpoint Name**: A descriptive name.
- **SIP Gateway Authentication Password**: A desired password.

Note that the management LAN and voice LAN IP addresses should already be configured as a result of basic configuration of the Signaling Server. **SIP Transport Protocol** and **Local SIP Port** should match the values configured for “Nortel” in Section 4.4.

![Figure 4: Signaling Server Properties](image)

Scroll down to the bottom of the screen, and click **Save and Transfer**.
The message dialog box below is displayed. Click **OK**.

![Image of a message dialog box]

The **Transfer Progress** screen is displayed, and updated with the status on transferring of configuration data to all elements. Click **OK** on the message dialog box that pops up at the end of the transfer.
5.9 Launch NRS Manager

Select Dialing and Number Plans > Network Routing Service from the left pane to launch the NRS Manager.

The Network Routing Service (NRS) screen is displayed. Retain the automatically populated IP address, and click Next to proceed.

A separate Internet browser window is opened with the NETWORK ROUTING SERVICE MANAGER screen. Enter the appropriate credentials and click Login.
The NETWORK ROUTING SERVICE MANAGER screen is displayed. Click the Home tab, followed by NRS Server Settings in the left pane. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click Save (not shown).

- **Host name:** Host name of Signaling Server from Figure 4 of Section 5.8.
- **Primary IP (TLAN):** The Signaling Server IP address from Section 5.2.
- **Mode:** “Redirect”
- **UDP transport enabled:** Check the checkbox.
- **TCP transport enabled:** Check the checkbox.

Click the Configuration tab in the top of the screen.

![Network Routing Service Manager](image)

The message pop up dialog box below is displayed. Click OK.
5.10 Administer Service Domain
The NRS hosts an active and a standby database. The active database is used for runtime queries, and the standby database is used for administrative modifications. Click (set Standby DB view) to switch to the standby database, in order to make administrative changes.

The view changes to Standby DB view, as shown below. The Service Domains option in the left pane is automatically selected, with the Service Domains screen displayed in the right pane. Click Add.

The Add Service Domain screen is displayed. Enter the SIP domain name from Figure 4 of Section 5.8 into the Domain name field, and a descriptive text for the Domain description field. Click Save.
Select **L1 Domains (UDP)** in the left pane to display the **L1 Domains (UDP)** screen. Click **Add** to add a new L1 domain. The L1 and L0 domains are building blocks of the phone context for private addresses. For more information on L1 and L0 domains, refer to the Nortel documentation in **Section 8**.

The **Add L1 Domain (mm.com)** screen is displayed next, as shown below. Enter a descriptive **Domain name** and **Domain description**, and applicable **E.164 country code** and **E.164 area code** for the network configuration. Retain the default value in the remaining fields, and scroll down to the bottom of the screen to click **Save** (not shown).
Select **L0 Domains (CDP)** in the left pane to display the **L0 Domains (CDP)** screen. Click **Add** to add a new L0 domain.

The **Add L0 Domain (mm.com / udp1)** screen is displayed next, as shown below. Enter a descriptive **Domain name** and **Domain description**. Retain the default values in the remaining fields, and scroll down to the bottom of the screen to click **Save** (not shown).
5.11 Administer SIP Gateway Endpoints

Next, configure two SIP gateway endpoints; one for the Avaya SES server, and the other for the Nortel SIP Redirect Server. Select **Gateway Endpoints** in the left pane to display the **Gateway Endpoints** screen. Click **Add** to add a new gateway endpoint for Avaya SES.

Enter a descriptive **Endpoint name** and **Endpoint description**, as shown below. For the **Endpoint authentication enabled** field, select “Authentication off” from the drop-down list.
Scroll down the screen. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click Save.

- **Static endpoint address:** IP address of Avaya Aura™ Session Manager SM-100 Module interface
- **H.323 Support:** “Not RAS H.323 endpoint”
- **SIP support:** “Static SIP endpoint”
- **SIP transport:** “TCP”

Repeat the procedures to add a gateway endpoint for the Nortel SIP Redirect Server as shown below. Select the desired value for **Endpoint authentication enabled**. If the authentication is turned on, then the value entered in the **Authentication password** field must match the authentication password value from Figure 4 of Section 5.8.
Scroll down the screen. For the **SIP support** field, select “Dynamic SIP endpoint” from the drop-down list. For the **SIP transport** field, select “TCP” to match the SIP transport protocol from **Figure 4 of Section 5.8**. Maintain the default values in the remaining fields, and click **Save**.

### 5.12 Administer Routing Entry

Configure two routing entries. The first entry uses the Avaya Aura™ Session Manager gateway endpoint to reach Avaya endpoints with extension digits 33xxx. The second entry uses the Nortel Redirect Server gateway endpoint to reach Nortel endpoints with extension digits 53xxx.

Select **Routing Entries** in the left pane to display the **Routing Entries** screen. Enter the gateway endpoint name for Avaya Aura™ Session Manager (in this case “ASM”), and click **Show**, followed by **Add** to add a routing entry.
The **Add Routing Entry** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Save**.

- **DN type:** “Private level 0 regional (CDP steering code)”
- **DN prefix:** Dialed prefix digits to match on, in this case “30”.
- **Route cost (1 – 255):** An appropriate cost value with 1 being least cost.

Repeat the same procedures to add a routing entry to reach the Nortel Communication Server 1000 endpoints with extension digits 53xxx behind the Nortel SIP Redirect Server gateway endpoint.
5.13 Cut Over and Commit Changes

Select the **Tools** tab at the top of the screen. Select **Database Actions** from the left pane to display the **Database Actions | Database State: Changed** screen. For the **Select database action** field, select “Cut over & Commit” from the drop-down list, and click **Submit**.
6 Verification Steps

This section provides the tests that can be performed on Avaya Aura™ Communication Manager 5.2 and Avaya Aura™ Session Manager to verify proper configuration of Communication Manager, Session Manager, and Nortel Communication Server 1000.

6.1 Verify Avaya Aura™ Communication Manager 5.2

Verify the status of the SIP trunk group by using the “status trunk n” command, where “n” is the trunk group number administered in Section 3.6. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 32

TRUNK GROUP STATUS

<table>
<thead>
<tr>
<th>Member</th>
<th>Port</th>
<th>Service State</th>
<th>Mtce Connected Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>0032/001</td>
<td>T00226</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0032/002</td>
<td>T00227</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0032/003</td>
<td>T00228</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0032/004</td>
<td>T00229</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0032/005</td>
<td>T00230</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0032/006</td>
<td>T00231</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0032/007</td>
<td>T00232</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0032/008</td>
<td>T00233</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0032/009</td>
<td>T00234</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0032/010</td>
<td>T00235</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
</tbody>
</table>
```

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in Section 3.6. Verify the signaling group is “in-service” as indicated in the Group State field shown below.

```
status signaling-group 32

STATUS SIGNALING GROUP

Group ID: 32  Active NCA-TSC Count: 0
Group Type: sip  Active CA-TSC Count: 0
Signaling Type: facility associated signaling
Group State: in-service
```
Make a call between the Avaya 9600 Series IP Telephone and the Nortel i2004 H.323 Telephone. Verify the status of connected SIP trunks by using the “status trunk x/y”, where “x” is the number of the SIP trunk group from Section 3.6.2 to reach Avaya Aura™ Session Manager, and “y” is the member number of a connected trunk. Verify on Page 1 that the Service State is “in-service/active”. On Page 2, verify that the IP addresses of the C-LAN and Avaya Aura™ Session Manager are shown in the Signaling section. In addition, the Audio section shows the G.729 codec and the IP addresses of the Avaya H.323 and Nortel H.323 endpoints. The Audio Connection Type displays “ip-direct”, indicating direct media between the two endpoints.

### status trunk 32/1

<table>
<thead>
<tr>
<th>Trunk Group/Member:</th>
<th>0032/001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port:</td>
<td>T00226</td>
</tr>
<tr>
<td>Service State:</td>
<td>in-service/active</td>
</tr>
<tr>
<td>Maintenance Busy?</td>
<td>no</td>
</tr>
<tr>
<td>Signaling Group ID:</td>
<td>32</td>
</tr>
<tr>
<td>IGAR Connection?</td>
<td>no</td>
</tr>
<tr>
<td>Connected Ports:</td>
<td>S00504</td>
</tr>
</tbody>
</table>

### status trunk 32/1

<table>
<thead>
<tr>
<th>Near-end Signaling Loc:</th>
<th>01A0317</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling IP Address</td>
<td></td>
</tr>
<tr>
<td>Near-end:</td>
<td>10.1.2.234</td>
</tr>
<tr>
<td>Far-end:</td>
<td>10.1.2.170</td>
</tr>
<tr>
<td>H.245 Near:</td>
<td></td>
</tr>
<tr>
<td>H.245 Far:</td>
<td></td>
</tr>
<tr>
<td>H.245 Signaling Loc:</td>
<td></td>
</tr>
<tr>
<td>H.245 Tunneled in Q.931?</td>
<td>no</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audio Connection Type:</th>
<th>ip-direct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Type:</td>
<td>None</td>
</tr>
<tr>
<td>Codec Type:</td>
<td>G.711MU</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audio IP Address</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Near-end:</td>
<td>10.1.2.253</td>
</tr>
<tr>
<td>Far-end:</td>
<td>192.45.100.73</td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Near-end:</td>
<td>6646</td>
</tr>
<tr>
<td>Far-end:</td>
<td>5200</td>
</tr>
</tbody>
</table>

| Video Near:           |         |
| Video Far:            |         |
| Video Port:           |         |
| Video Near-end Codec: |         |
| Video Far-end Codec:  |         |
6.2 Verify Avaya Aura™ Session Manager

Expand the Session Manager menu on the left and click SIP Monitoring. Verify as shown below that none of the links to the defined SIP entities is down, indicating that they are all reachable for all routing.

[Image: Integrated Management System Manager 1.0]

Under All Monitored SIP entities, select the appropriate SIP entities and verify that the connection status is “Up”, as shown below for the Nortel Communication Server 1000.

[Image: Integrated Management System Manager 1.0]

6.3 Verify Nortel Communication Server 1000

Select Services->Logs and Reports->IP Telephony Nodes on the left. Click Status for the “SS_Node” to verify that the signaling server is enabled and operational.
6.4 Verification Scenarios

Verification scenarios for the configuration described in these Application Notes included:

- Basic calls between various telephones on the Avaya Aura™ Communication Manager 5.2 and Nortel Communication Server 1000 can be made in both directions using G.711MU, G.729B, and G.729AB. For G.729 interoperability, the IP codec set on Avaya Communication Manager must include a version of the G.729 that Nortel Communication Manager 1000 supports.

- Proper display of the calling and called party name and number information was verified for all telephones with the basic call scenario.

- Supplementary calling features were verified. The feature scenarios involved additional endpoints on the respective systems, such as performing an unattended transfer of the SIP trunk call to a local endpoint on the same site, and then repeating the scenario to transfer the SIP trunk call to a remote endpoint on the other site. The supplementary calling features verified are shown below. Note that calling/called party name and number display may not be consistent in some cases.

  - Unattended transfer
  - Attended transfer
  - Hold/Unhold
  - Consultation hold
  - Call forwarding
  - Conference
7 Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager 5.2 can interoperate with Nortel Communication Server 1000 using SIP trunks via Avaya Aura™ Session Manager. The following is a list of interoperability items to note:

- For G.729 interoperability, “G.729” or “G.729A” must be included in the codec set in Avaya Aura™ Communication Manager 5.2.
- Audio shuffling between the H.323 IP telephones is supported.
- The entered DTMF digits over the SIP trunks were not recognizable due to support of two different methods for passing DTMF digits. Avaya complies with RFC 2833 while Nortel uses the SIP INFO method, and the two methods are not interoperable. Note that Release 5.0 or later of Nortel Communication Server 1000 supports RFC 2833, but this version has not yet been interoperability tested.
- Calling/called party name and number display may not be consistent for some supplementary calling features.
- Calls from Nortel Communication Server 1000 to Avaya Aura™ Communication Manager 5.2 that are abandoned in the ringing state will continue to ring the destination for a brief period.
- Calls from Nortel Communication Server 1000 to Avaya Aura™ Communication Manager 5.2 that are forwarded back to Nortel Communication Server 1000 are not supported.

8 Additional References

This section references the product documentation relevant to these Application Notes.

Avaya Aura™ Session Manager:

Avaya Aura™ Communication Manager 5.2:
Nortel Communication Server 1000:

©2009 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com