



## **Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager 5.2, and Nortel Communication Server 1000 – Issue 1.1**

### **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.

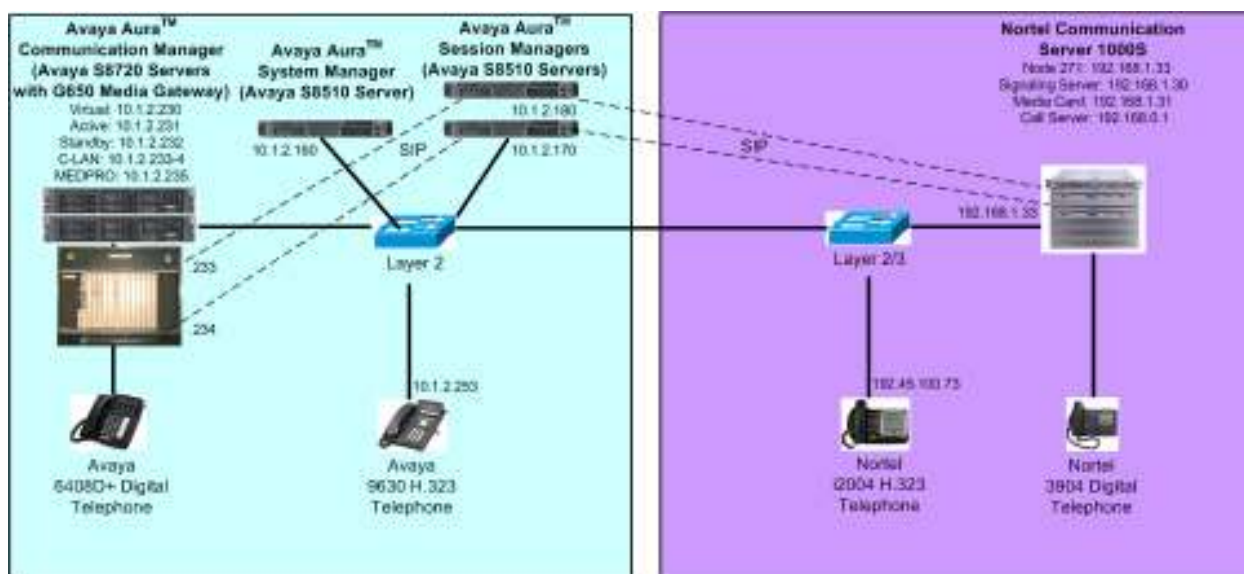
For the sample configuration, Avaya Session Manager runs on an Avaya S8510 Server, Avaya Communication Manager 5.2 runs on an Avaya S8720 Server with Avaya G650 Media Gateway, and Nortel Communication Server 1000 runs on Nortel Communication Server 1000S. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya 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 Communication Manager. 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 Session Manager, using its SM-100 (Security Module) network interface. All inter-system calls are carried over these SIP trunks. Avaya 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 Session Managers by communicating with their management network interfaces. As shown in the figure, two Avaya Aura Session Managers were configured to support “active-active” failover and “route-through”, which are alternate call routing features that are employed during network failures (see **Section 6**). Configurations supporting SIP telephones still require Avaya SIP Enablement Services, and are not addressed in these application notes.

For the sample configuration, Avaya Session Manager runs on an Avaya S8510 Server, Avaya Communication Manager runs on an Avaya S8720 Server with Avaya G650 Media Gateway, and Nortel Communication Server 1000 runs on Nortel Communication Server 1000S. These Application Notes should apply 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 Communication Manager (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 9**).

## 2 Equipment and Software Validated

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

| Hardware Component   | Software Version  |
|--|---|
| Avaya S8510 Server   | Avaya Session Manager Release 1.1.3.1.18022<br>Quick Fix “asset-gefanuc-1.1.3.0.18007-1.i386.rpm” |
|  | Avaya Aura™ System Manager, Release 1.1.3.1.18022   |
| Avaya S8720 Servers with G650 Media Gateway  | Avaya Communication Manager Load 947.3 Patch 17250  |
| Avaya 9630 IP Telephone (H.323)  | 2.0   |
| Avaya 6408D+ Digital Telephone   | -   |
| Nortel Communication Server 1000S <ul style="list-style-type: none"><li>• Call Server</li><li>• Signaling Server</li></ul> | Nortel Communication Server 1000 Release 450w, Version 2121 sse-4.50.88                           |
| Nortel 3904 Digital Telephone  | NA  |
| Nortel I2004 H.323 Telephone   | C502B41   |

## 3 Configure Avaya Communication Manager

This section describes configuring Avaya Communication Manager in the following areas. Some administration screens have been abbreviated for clarity.

- Verify Avaya Communication Manager 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

### 3.1 Verify Avaya Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Avaya Communication Manager 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.

| display system-parameters customer-options                |      | Page 2 of 10 |
|---|------|--------------|
| OPTIONAL FEATURES   |      |              |
| IP PORT CAPACITIES  | USED |              |
| Maximum Administered H.323 Trunks: 800                    | 200  |              |
| Maximum Concurrently Registered IP Stations: 18000        | 2    |              |
| Maximum Administered Remote Office Trunks: 0              | 0    |              |
| Maximum Concurrently Registered Remote Office Stations: 0 | 0    |              |
| Maximum Concurrently Registered IP eCons: 0               | 0    |              |
| Max Concur Registered Unauthenticated H.323 Stations: 0   | 0    |              |
| Maximum Video Capable H.323 Stations: 0                   | 0    |              |
| Maximum Video Capable IP Softphones: 0                    | 0    |              |
| Maximum Administered SIP Trunks: 800                      | 47   |              |

### 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 9** for more details.

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

### 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, “clan1” and “10.1.2.233” are entered as **Name** and **IP Address** for the C-LAN, “sm1” and “10.1.2.170” are entered for Avaya 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 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.

|                      |            |      |      |   |
|----------------------|------------|------|------|---|
| change node-names ip |            | Page | 1 of | 2 |
| IP NODE NAMES        |            |      |      |   |
| Name                 | IP Address |      |      |   |
| clan1                | 10.1.2.233 |      |      |   |
| Gateway001           | 10.1.2.1   |      |      |   |
| sm1                  | 10.1.2.170 |      |      |   |

### 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.

|   |  |   |  |
|---|--|---|--|
| add ip-interface 1a02                       |  | Page 1 of 3                               |  |
| IP INTERFACES                               |  |   |  |
| Type: C-LAN                                 |  |   |  |
| Slot: 01A02                                 |  | Target socket load and Warning level: 400 |  |
| Code/Suffix: TN799 D                        |  | Receive Buffer TCP Window Size: 8320      |  |
| Enable Interface? y                         |  | Allow H.323 Endpoints? y                  |  |
| VLAN: n                                     |  | Allow H.248 Gateways? y                   |  |
| Network Region: 1                           |  | Gatekeeper Priority: 5                    |  |
| IPV4 PARAMETERS                             |  |   |  |
| Node Name: clan1                            |  |   |  |
| Subnet Mask: /24                            |  |   |  |
| Gateway Node Name: Gateway001               |  |   |  |
| 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 |                     |                |                  |  | Page 1 of 2 |
|-----------------------|---------------------|----------------|------------------|--|-------------|
| IP Codec Set          |                     |                |                  |  |             |
| Codec Set: 1          |                     |                |                  |  |             |
| Audio Codec           | Silence Suppression | Frames Per Pkt | Packet Size (ms) |  |             |
| 1: G.711MU            | n                   | 2              | 20               |  |             |
| 2:                    |                     |                |                  |  |             |
| 3:                    |                     |                |                  |  |             |

In the test configuration, network region “1” was used for calls to the Nortel Communication Server 1000 via Avaya Aura <sup>TM</sup>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 |                                      | Page 1 of 19 |
|----------------------------|--------------------------------------|--------------|
| IP NETWORK REGION          |                                      |              |
| Region: 1                  |                                      |              |
| Location:                  | Authoritative Domain: avaya.com      |              |
| Name: ASM to Nortel        |                                      |              |
| MEDIA PARAMETERS           | Intra-region IP-IP Direct Audio: yes |              |
| Codec Set: 1               | Inter-region IP-IP Direct Audio: yes |              |
| UDP Port Min: 2048         | IP Audio Hairpinning? n              |              |
| UDP Port Max: 10001        |                                      |              |
| DIFFSERV/TOS PARAMETERS    | RTCP Reporting Enabled? y            |              |
| Call Control PHB Value: 46 | RTCP MONITOR SERVER PARAMETERS       |              |
| Audio PHB Value: 46        | Use Default Server Parameters? y     |              |
| Video PHB Value: 26        |                                      |              |

## 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 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 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”

|                                     |                                   |             |
|-------------------------------------|-----------------------------------|-------------|
| add signaling-group 32              |                                   | Page 1 of 1 |
| SIGNALING GROUP                     |                                   |             |
| Group Number: 32                    | Group Type: sip                   |             |
|                                     | Transport Method: tls             |             |
| IMS Enabled? n                      |                                   |             |
|                                     |                                   |             |
| Near-end Node Name: clan1           | Far-end Node Name: sml            |             |
| Near-end Listen Port: 5061          | Far-end Listen Port: 5061         |             |
|                                     | Far-end Network Region: 1         |             |
| Far-end Domain: avaya.com           |                                   |             |
| Bypass If IP Threshold Exceeded? n  |                                   |             |
| DTMF over IP: rtp-payload           | Direct IP-IP Audio Connections? y |             |
|                                     | IP Audio Hairpinning? n           |             |
| Enable Layer 3 Test? n              | Direct IP-IP Early Media? n       |             |
| Session Establishment Timer(min): 3 | Alternate Route Timer(sec): 6     |             |

### 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 configured in **Section 3.1**).

|                           |                        |                             |                 |
|---------------------------|------------------------|-----------------------------|-----------------|
| <b>add trunk-group 32</b> |                        | Page 1 of 21                |                 |
| TRUNK GROUP               |                        |                             |                 |
| Group Number: 32          | <b>Group Type: sip</b> | CDR Reports: y              |                 |
| <b>Group Name: To SM1</b> | COR: 1                 | TN: 1                       | <b>TAC: 132</b> |
| Direction: two-way        | Outgoing Display? y    | Night Service:              |                 |
| Dial Access? n            |                        |                             |                 |
| Queue Length: 0           |                        |                             |                 |
| <b>Service Type: tie</b>  | Auth Code? n           |                             |                 |
|                           |                        | Signaling Group: 32         |                 |
|                           |                        | <b>Number of Members: 4</b> |                 |

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.

|                                 |                |                                 |  |
|---------------------------------|----------------|---------------------------------|--|
| <b>add trunk-group 32</b>       |                | Page 3 of 21                    |  |
| TRUNK FEATURES                  |                |                                 |  |
| ACA Assignment? n               | Measured: none | Maintenance Tests? y            |  |
|                                 |                |                                 |  |
| <b>Numbering Format: public</b> |                |                                 |  |
|                                 |                | UUI Treatment: service-provider |  |
|                                 |                | Replace Restricted Numbers? n   |  |
|                                 |                | Replace Unavailable Numbers? n  |  |



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                    |     |         |        |          |      |                 |          |      |      |     |           |        | Page 1 of 3 |      |  |
| Pattern Number: 32    Pattern Name: To ASM |     |         |        |          |      |                 |          |      |      |     |           |        |             |      |  |
| SCCAN? n    Secure SIP? n                  |     |         |        |          |      |                 |          |      |      |     |           |        |             |      |  |
| Grp  | FRL | NPA     | Pfx    | Hop      | Toll | No.             | Inserted |      |      |     |           |        | DCS/        | IXC  |  |
| No   |     |         | Mrk    | Lmt      | List | Del             | Digits   |      |      |     |           |        | QSIG        |      |  |
|  |     |         |        |          |      |                 |          | Dgts |      |     |           |        |             | Intw |  |
| 1:   | 32  | 0       |        |          |      |                 |          |      |      |     |           |        | n           | user |  |
| 2:   |     |         |        |          |      |                 |          |      |      |     | n         | user   |             |      |  |
| 3:   |     |         |        |          |      |                 |          |      |      |     | n         | user   |             |      |  |
| 4:   |     |         |        |          |      |                 |          |      |      |     | n         | user   |             |      |  |
| 5:   |     |         |        |          |      |                 |          |      |      |     | n         | user   |             |      |  |
| 6:   |     |         |        |          |      |                 |          |      |      |     | n         | user   |             |      |  |
|  |     |         |        |          |      |                 |          |      |      |     |           |        |             |      |  |
| BCC VALUE                                  |     | TSC     | CA-TSC | ITC BCIE |      | Service/Feature |          |      | PARM | No. | Numbering | LAR    |             |      |  |
| 0 1 2 M 4 W                                |     | Request |        |          |      |                 |          |      |      |     | Dgts      | Format |             |      |  |
|  |     |         |        |          |      |                 |          |      |      |     |           |        | Subaddress  |      |  |
| 1:   | y   | y       | y      | y        | y    | n               | n        | rest |      |     |           |        | none        |      |  |

### 3.8 Configure Location and Public Unknown Numbering

Use the “change locations” command to specify the SIP route pattern to be used as a “default SIP route” for the location corresponding to the Main site. Calls to non-numeric users or unknown domains will still be routed to Avaya Session Manager. 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**.

|  |      |          |      |     |             |     |  |
|--|------|----------|------|-----|-------------|-----|--|
| change locations                                 |      |          |      |     | Page 1 of 1 |     |  |
| LOCATIONS  |      |          |      |     |             |     |  |
| ARS Prefix 1 Required For 10-Digit NANP Calls? y |      |          |      |     |             |     |  |
| Loc  | Name | Timezone | Rule | NPA | Proxy       | Sel |  |
| No   |      | Offset   |      |     | Rte         | Pat |  |
| 1:   | Main | + 00:00  | 0    |     |             | 32  |  |

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.

|                                   |      |        |        |     |                       |
|-----------------------------------|------|--------|--------|-----|-----------------------|
| change public-unknown-numbering 0 |      |        |        |     | Page 1 of 2           |
| NUMBERING - PUBLIC/UNKNOWN FORMAT |      |        |        |     |                       |
| Total                             |      |        |        |     |                       |
| Ext                               | Ext  | Trk    | CPN    | CPN |                       |
| Len                               | Code | Grp(s) | Prefix | Len |                       |
| 5                                 | 3    | 32     |        | 5   | Total Administered: 2 |
|                                   |      |        |        |     | Maximum Entries: 9999 |

### 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”

| change uniform-dialplan 0 |     |     |                  |     |      | Page            | 1 of | 2 |
|---------------------------|-----|-----|------------------|-----|------|-----------------|------|---|
| UNIFORM DIAL PLAN TABLE   |     |     |                  |     |      | Percent Full: 0 |      |   |
| Matching<br>Pattern       | Len | Del | Insert<br>Digits | Net | Conv | Node<br>Num     |      |   |
| 53                        | 5   | 0   |                  | aar | n    |                 |      |   |

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”

| change aar analysis 0    |              |              |                  |              |             | Page            | 1 of | 2 |
|--------------------------|--------------|--------------|------------------|--------------|-------------|-----------------|------|---|
| AAR DIGIT ANALYSIS TABLE |              |              |                  |              |             | Percent Full: 1 |      |   |
| Location: all            |              |              |                  |              |             |                 |      |   |
| Dialed<br>String         | Total<br>Min | Total<br>Max | Route<br>Pattern | Call<br>Type | Node<br>Num | ANI<br>Reqd     |      |   |
| 53                       | 5            | 5            | 32               | aar          |             | n               |      |   |

### 3.10 Save Translations

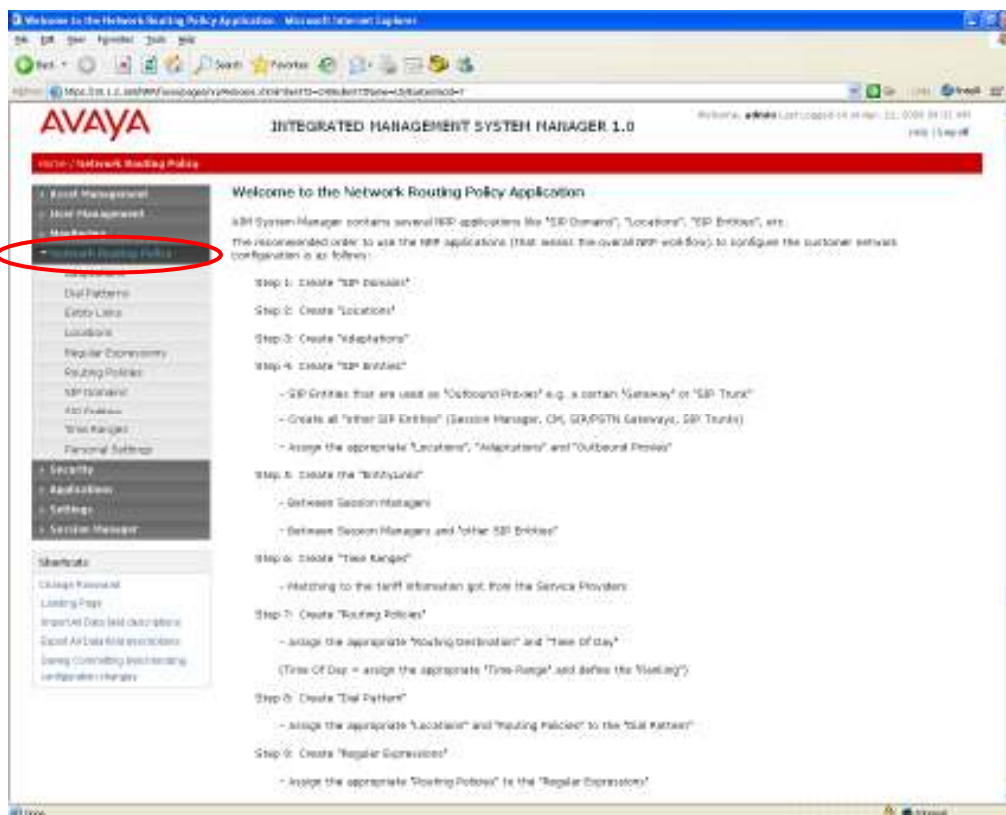
Configuration of Avaya Communication Manager is complete. Use the “save Translations command to save these changes.

## 4 Configure Avaya Session Manager

This section provides the procedures for configuring Avaya 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 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 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**).



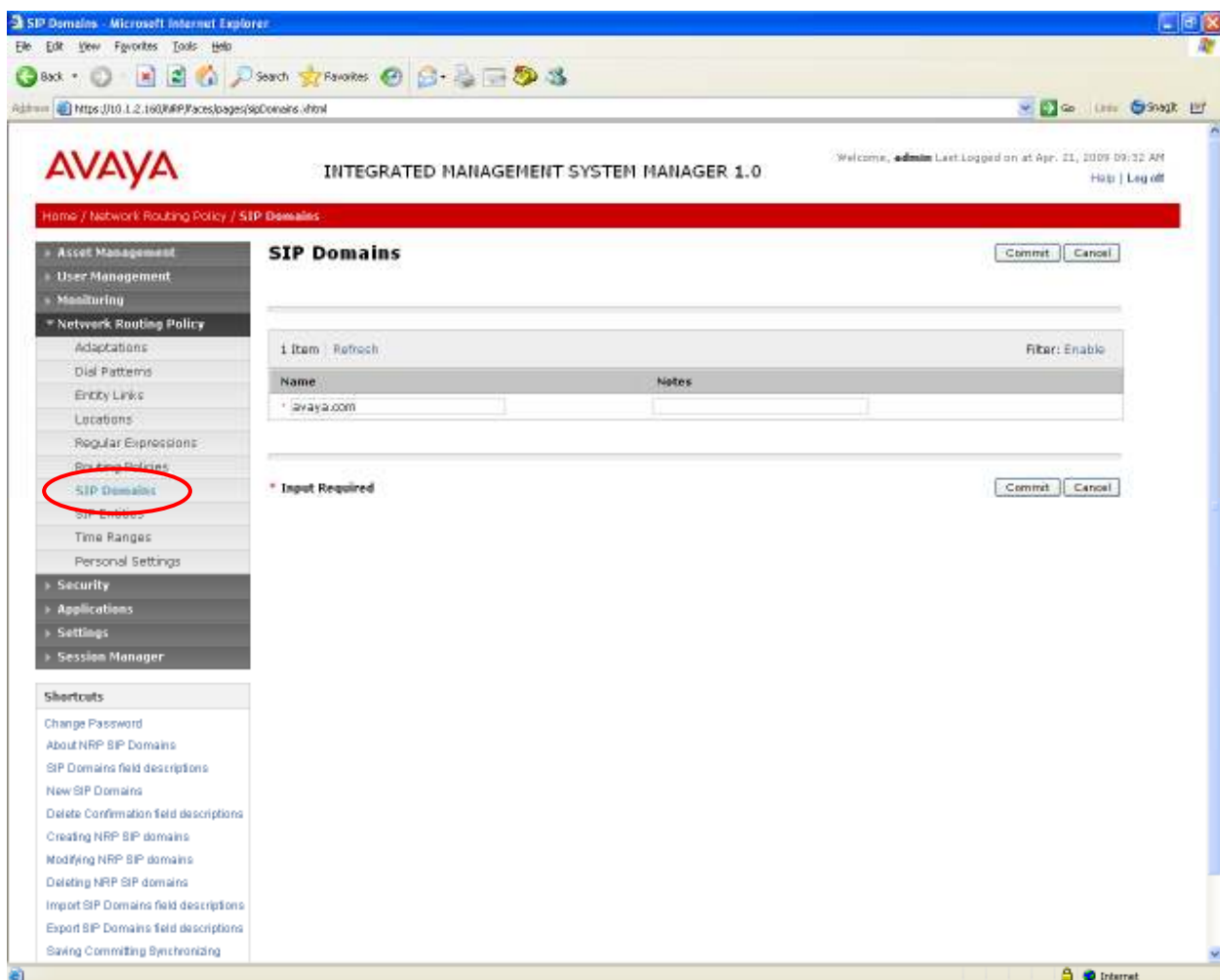
## 4.1 Specify SIP Domain

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 Communication Manager and Avaya Session Manager. Click **Commit** to save each Location definition.

The screenshot displays the 'Location Details' page in the Avaya Integrated Management System Manager 1.0. The left sidebar shows a navigation menu with 'Locations' highlighted. The main content area is divided into two sections: 'General' and 'Location Pattern'. The 'General' section includes fields for 'Name' (Lincroft), 'Notes' (Session Manager and ACM), 'Managed Bandwidth' (Kbit/sec), 'Average Bandwidth per Call' (Kbit/sec), and 'Time to Live (secs)' (3000). The 'Location Pattern' section includes an 'Add' button, a 'Remove' button, and a table with one row showing an 'IP Address Pattern' of '10.1.2.\*' with 'Notes' (Session Manager and ACM). The 'Commit' and 'Cancel' buttons are visible at the bottom right of the form.

The following screen shows the addition of a second location based on the subnet used by Nortel Communication Server 1000.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Apr. 21, 2009 09:32 AM  
Help | Log off

Home / Network Routing Policy / Locations / Location Details

**Location Details** [Commit] [Cancel]

**General**

| Name    | Notes         |
|---------|---------------|
| Toronto | Nortel CS1000 |

Managed Bandwidth: [ ] Kbit/sec

\* Average Bandwidth per Call: [ 80 ] Kbit/sec

\* Time to Live (secs): [ 3000 ]

**Location Pattern**

[Add] [Remove]

1 Item [Refresh] Filter: Enable

| IP Address Pattern | Notes         |
|--------------------|---------------|
| 192.168.*          | Nortel CS1000 |

Select: All, None ( 0 of 1 Selected )

\* Input Required [Commit] [Cancel]

**Shortcuts**

- Change Password
- Locations Details field descriptions
- Saving/Committing/Synchronizing configuration changes

The fields under *General* can be filled in to specify bandwidth management parameters between Avaya 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 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. Two *Port* entries are added. TCP (well-known port 5060) is used for communicating with Nortel Communication Server 1000, and TLS (well-known port 5061) is used for communication with other Avaya Session Managers and Avaya Communication Manager.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at May 20, 2009 13:44 PM  
Help | Log off

Home / Network Routing Policy / SIP Entities / SIP Entity Details

**SIP Entity Details** [Commit] [Cancel]

**General**

| Name  | FQDN or IP Address | Type            | Notes |
|-------|--------------------|-----------------|-------|
| * SM1 | * 10.1.2.170       | Session Manager |       |

**Entity Links \***

Adaptation: [dropdown]  
 Location: [Lincoln] [dropdown]  
 Outbound Proxy: [dropdown]  
 Time Zone: [America/New\_York] [dropdown]  
 Override Port & Transport with DNS SRV: ☐  
 SIP Timer B/F (secs): \* 4  
 Credential name: [text field]

**Monitoring**

Monitoring on/off: [Use Session Manager configuration] [dropdown]  
 [Monitoring on/off] [button]

**Port**

[Add] [Remove]

2 Items / Refresh [Filter: Enable]

| Port                          | Protocol       | Default Domain       | Notes |
|-------------------------------|----------------|----------------------|-------|
| <input type="checkbox"/> 5060 | TCP [dropdown] | avaya.com [dropdown] |       |
| <input type="checkbox"/> 5061 | TLS [dropdown] | avaya.com [dropdown] |       |

Select: All, None ( 0 of 2 Selected )

\* Input Required [Commit] [Cancel]

The following screen shows addition of Avaya Communication Manager. The IP address used is that of the C-LAN board in the Avaya G650 Media gateway.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on: 01 Jun. 02, 2009 10:27 AM  
Help | Log off

Home / Network Routing Policy / SIP Entities / SIP Entity Details

**SIP Entity Details** [Commit] [Cancel]

**General**

| Name                    | FQDN or IP Address | Type | Notes |
|-------------------------|--------------------|------|-------|
| * Cell Center ACM CLAN1 | * 10.1.2.233       | CM   |       |

**Entity Links \***

Adaptation: [Select]  
Location: [Lincoln]  
Time Zone: [America/New\_York]  
Override Port & Transport with DNS SRV: ☐  
SIP Timer B/F (secs): \* 4  
Credential name: [Text Field]  
Call Detail Recording: [egress]

**Monitoring**

Monitoring on/off: Use Session Manager configuration [Select]

\* Input Required [Commit] [Cancel]

**Shortcuts**

- Change Password
- SIP Entity Details field descriptions
- Saving/Committing/Synchronizing configuration changes

The following screen shows addition of Nortel Communication Server 1000. The IP address used is that of the “Voice LAN (TLAN) Node IP address”.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, admin Last Logged on 01 Jun 02, 2009 10:27 AM  
Help | Log off

Home / Network Routing Policy / SIP Entities / SIP Entity Details

**SIP Entity Details** [Commit] [Cancel]

General

| Name          | FQDN or IP Address | Type  | Notes |
|---------------|--------------------|-------|-------|
| Nortel CS1000 | 192.168.1.33       | Other |       |

Entity Links \*

Adaptation: [Select]

Location: Toronto

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

SIP Timer B/F (secs): 4

Credential name: [Text]

Call Detail Recording: egress

Monitoring

Monitoring on/off: Use Session Manager configuration

\* Input Required [Commit] [Cancel]

## 4.4 Add Entity Links

A SIP trunk between Avaya 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 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 screens illustrate adding the two Entity Links for Avaya Communication Manager and Nortel Communication Server 1000. Since this version of Nortel Communication Server 1000 does not support TLS, TCP (well-known port (5060) was used. TLS (well-known port 5061) is used for Avaya Communication Manager.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome: admin Last Logged on at Jun. 02, 2009 1 Help

Home / Network Routing Policy / Entity Links

Entity Links

1 Item Refresh Filter: Enable

| Name      | SIP Entity 1 | Port | SIP Entity 2          | Port | Trusted                             | Protocol | Notes |
|-----------|--------------|------|-----------------------|------|-------------------------------------|----------|-------|
| SM1 CLAN1 | SM1          | 5061 | Call Center ACM CLAN1 | 5061 | <input checked="" type="checkbox"/> | TLS      |       |

\* Input Required

Commit Cancel

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome: admin Last Logged on at Jun. 02, 2009 Help

Home / Network Routing Policy / Entity Links

Entity Links

1 Item Refresh Filter: Enable

| Name              | SIP Entity 1 | Port | SIP Entity 2  | Port | Trusted                             | Protocol | Notes |
|-------------------|--------------|------|---------------|------|-------------------------------------|----------|-------|
| SM1 Nortel CS1000 | SM1          | 5060 | Nortel CS1000 | 5060 | <input checked="" type="checkbox"/> | TCP      |       |

\* Input Required

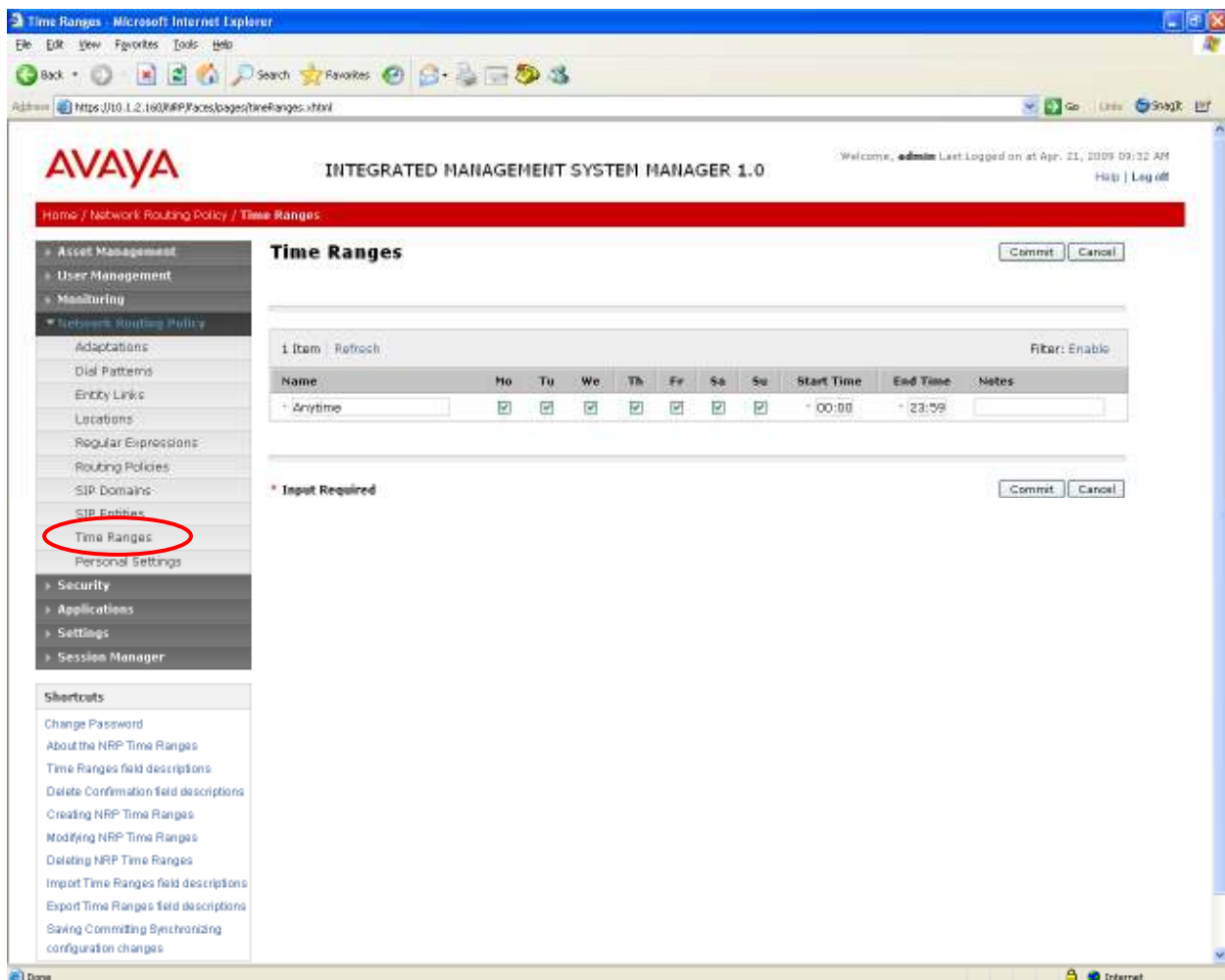
Commit Cancel

## 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 Communication Manager 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**.

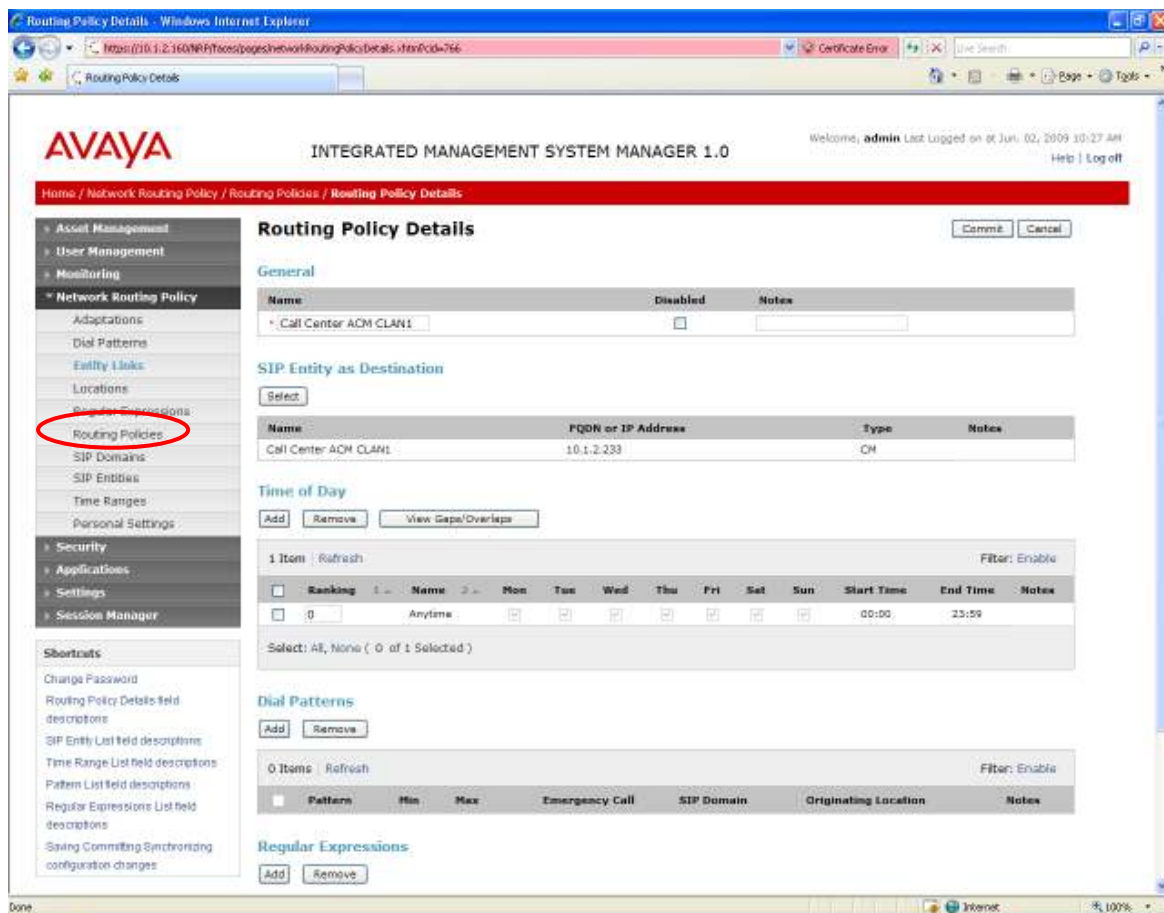
Under *SIP Entity as Destination*:

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 Communication Manager and one for Nortel Communication Server 1000.





Routing Policy Details - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address: https://10.1.2.160/IMP/Faces/pages/networkRoutingPolicyDetails.xhtml?\_afid=110

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, admin Last Logged on at Apr. 21, 2009 09:32 AM Help | Log off

Home / Network Routing Policy / Routing Policies / Routing Policy Details

Routing Policy Details

Commit Cancel

General

| Name          | Disabled                 | Notes |
|---------------|--------------------------|-------|
| Nortel CS1000 | <input type="checkbox"/> |       |

SIP Entity as Destination

Select

| Name          | FQDN or IP Address | Type  | Notes |
|---------------|--------------------|-------|-------|
| Nortel CS1000 | 192.168.1.33       | Other |       |

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

| Ranking | Name    | Mon                                 | Tue                                 | Wed                                 | Thu                                 | Fri                                 | Sat                                 | Sun                                 | Start Time | End Time | Notes |
|---------|---------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-------|
| 0       | Anytime | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 00:00      | 23:59    |       |

Select: All, None ( 0 of 1 Selected )

Dial Patterns

Add Remove

0 Items Refresh Filter: Enable

| Pattern | Min | Max | Emergency Call | SIP Domain | Originating Location | Notes |
|---------|-----|-----|----------------|------------|----------------------|-------|
|---------|-----|-----|----------------|------------|----------------------|-------|

Regular Expressions

Add Remove

0 Items Refresh Filter: Enable

Shortcuts

- Change Password
- Routing Policy Details field descriptions
- SIP Entity List field descriptions
- Time Range List field descriptions
- Pattern List field descriptions
- Regular Expressions List field descriptions
- Saving/Committing/Synchronizing configuration changes

## 4.7 Add Dial Patterns

Define dial patterns to direct calls to the appropriate SIP Entity. 5-digit extensions beginning with “30” reside on Avaya Communication Manager, 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 Communication Manager:

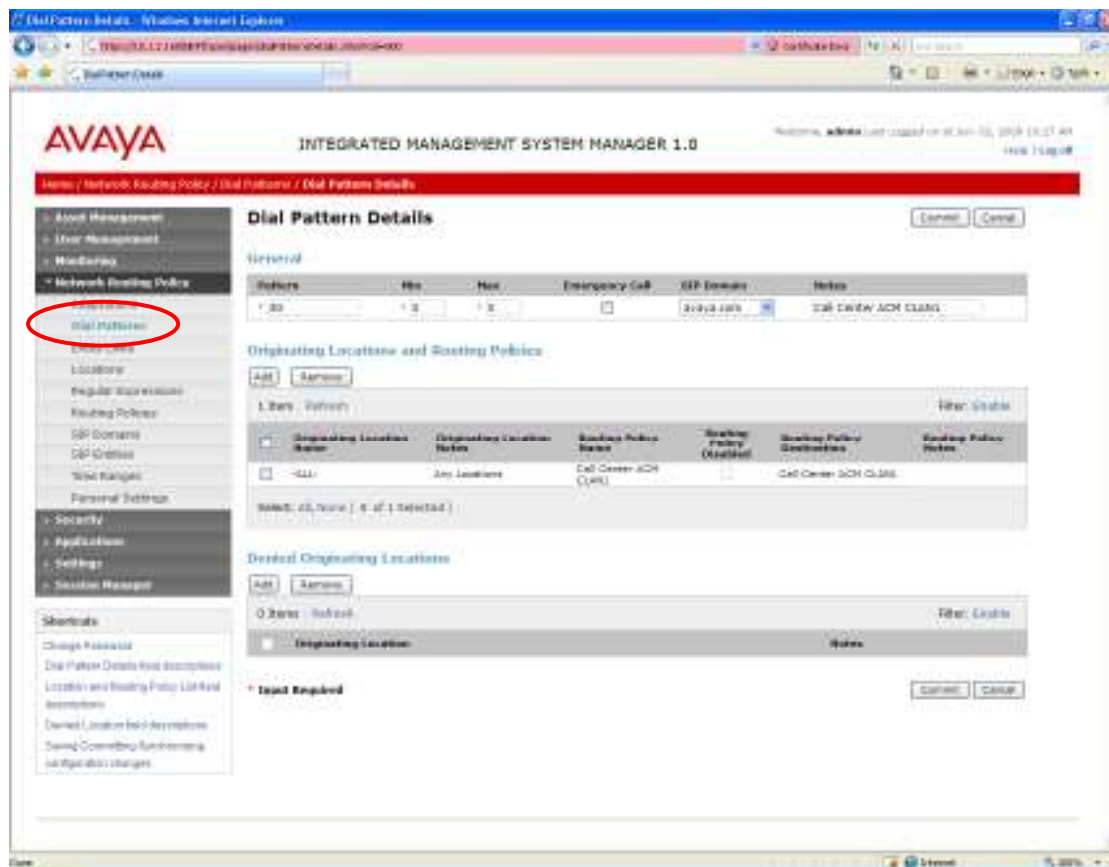
Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain specified in **Section 4.1**
- **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 Communication Manager and Nortel Communication Server 1000.





Dial Pattern Details - Windows Internet Explorer

https://10.1.2.160/NR/Tools/pages/dialPatternsDetails.xhtml?cid=662

Certificate Error

Live Search

Dial Pattern Details

AVAYA

INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, admin Last Logged on at Jun 02, 2009 10:27 AM

Help | Log off

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

Commit Cancel

**Dial Pattern Details**

General

| Pattern | Min | Max | Emergency Call           | SIP Domain | Notes         |
|---------|-----|-----|--------------------------|------------|---------------|
| * 53    | * 5 | * 5 | <input type="checkbox"/> | avaya.com  | Nortel CS1000 |

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name | Routing Policy Disabled  | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|---------------------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | -ALL-                     | Any Locations              | Nortel CS1000       | <input type="checkbox"/> | Nortel CS1000              |                      |

Select: All, None ( 0 of 1 Selected )

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

| <input type="checkbox"/> | Originating Location | Notes |
|--------------------------|----------------------|-------|
|--------------------------|----------------------|-------|

\* Input Required

Commit Cancel

Shortcuts

- Change Password
- Dial Pattern Details field descriptions
- Location and Routing Policy List field descriptions
- Denied Location field descriptions
- Saving Commencing Refreshing configuration changes

## 4.8 Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between Avaya Aura™ System Manager and Avaya 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 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.

The screenshot displays the 'Add Session Manager' configuration page in the Avaya Aura System Manager web interface. The left sidebar shows the 'Session Manager Administration' menu item highlighted. The main content area has tabs for General, Security Module, Monitoring, and CDR. The General tab is active, showing fields for SIP Entity Name (SM1), Description (Session Manager 1), and Management Access Point Host Name/IP (10.1.2.171). The Security Module tab is also visible, showing fields for SIP Entity IP Address (10.1.2.170), Network Mask (255.255.255.0), Default Gateway (10.1.2.1), Call Control PHB (46), VLAN ID, and QoS Priority (6). The Monitoring tab shows 'Enable Monitoring' checked and 'Proactive cycle time (secs)' set to 900.

## 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 Session Manager to reach endpoints on Avaya Communication Manager. 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

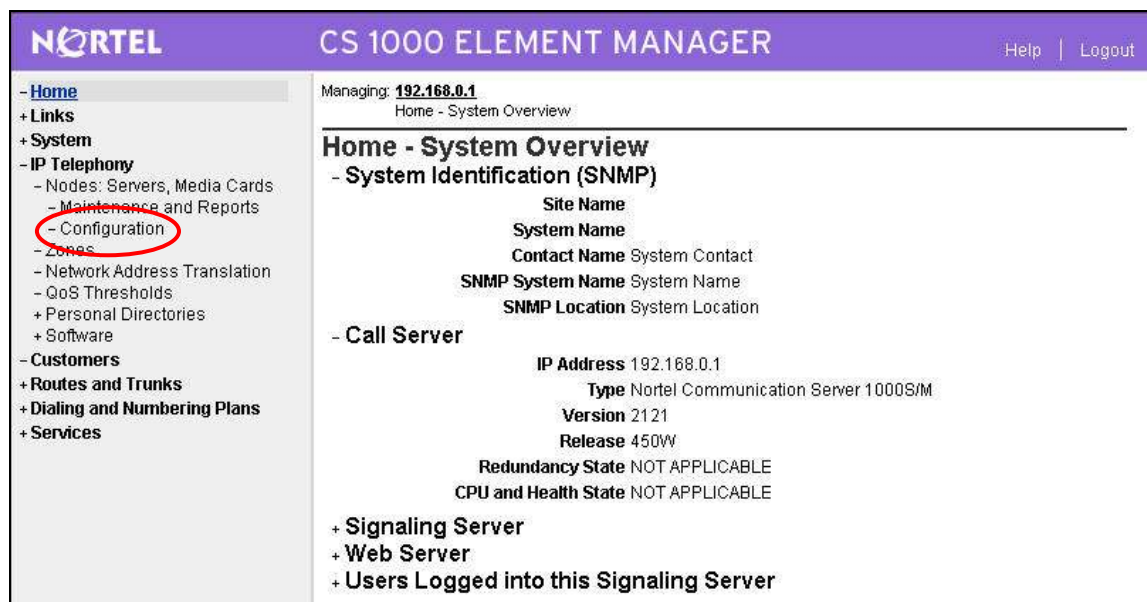
Access the Nortel Communication Server 1000 web based interface Element Manager by using the URL “http://<ip-address>” in an Internet browser window, where “<ip-address>” is the IP address of the Signaling Server from **Section 5.2**. Note that the IP address for the Signaling Server may vary, and in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



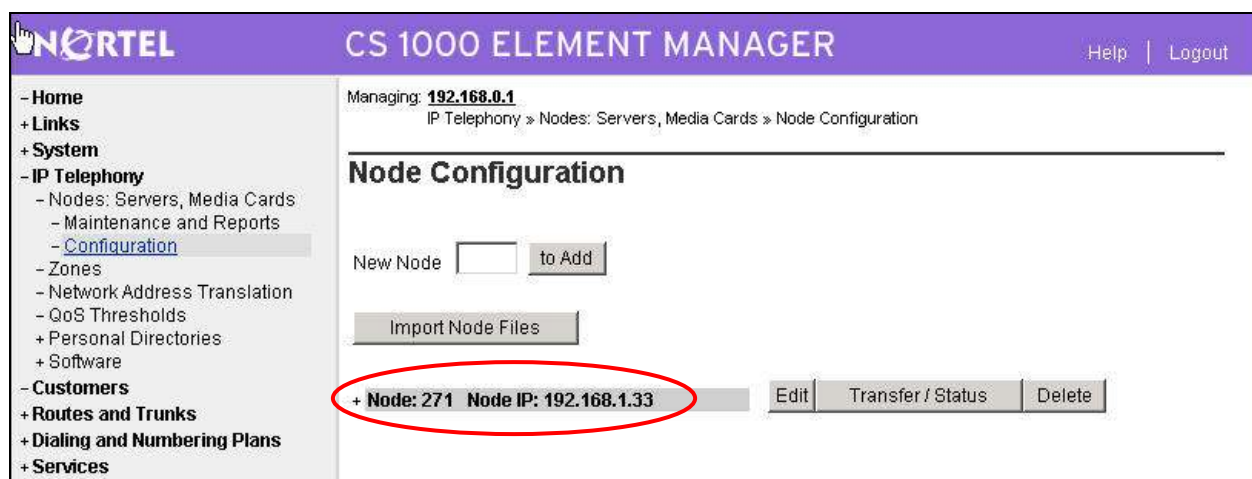
## 5.2 Obtain Node and IP Addresses

The **Home – System Overview** screen is displayed. Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** in the left pane.

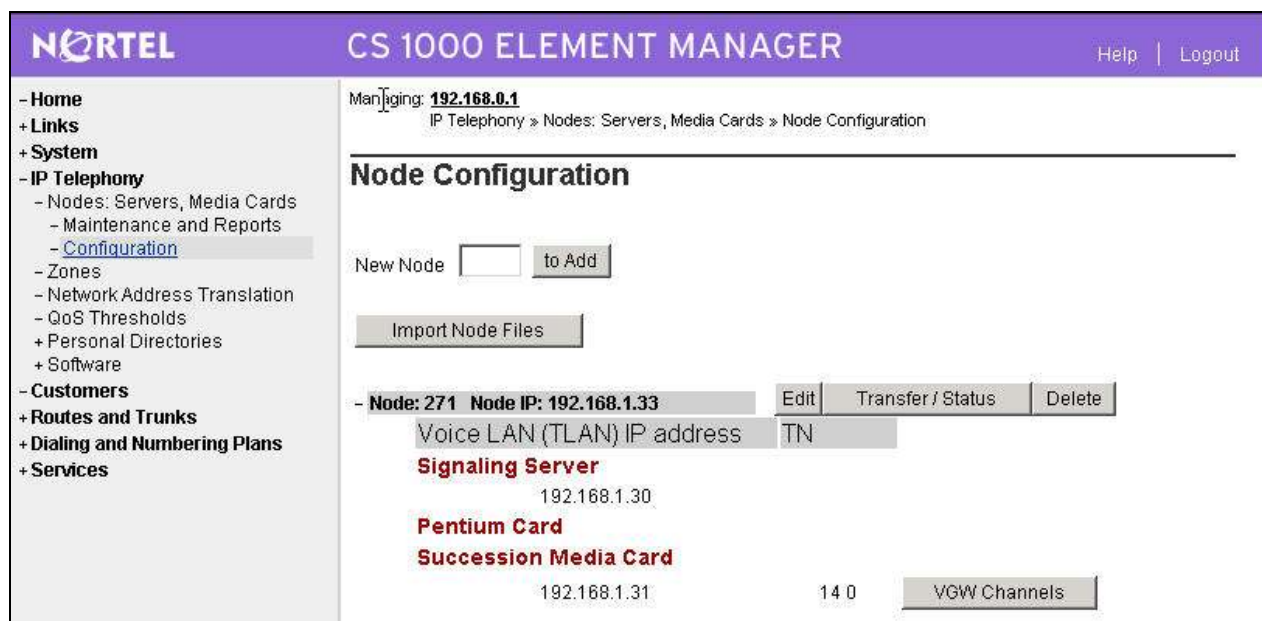


| Home - System Overview                           |                                     |
|--|-------------------------------------|
| <b>- System Identification (SNMP)</b>            |                                     |
| Site Name  |                                     |
| System Name                                      |                                     |
| Contact Name                                     | System Contact                      |
| SNMP System Name                                 | System Name                         |
| SNMP Location                                    | System Location                     |
| <b>- Call Server</b>                             |                                     |
| IP Address                                       | 192.168.0.1                         |
| Type   | Nortel Communication Server 1000S/M |
| Version  | 2121                                |
| Release  | 450W                                |
| Redundancy State                                 | NOT APPLICABLE                      |
| CPU and Health State                             | NOT APPLICABLE                      |
| <b>+ Signaling Server</b>                        |                                     |
| <b>+ Web Server</b>                              |                                     |
| <b>+ Users Logged into this Signaling Server</b> |                                     |

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 screenshot shows the 'Customers' screen in the CS 1000 ELEMENT MANAGER. The left sidebar contains a navigation menu with options: Home, Links, System, IP Telephony, Customers (highlighted), Routes and Trunks, Dialing and Numbering Plans, and Services. The main content area has a header 'Managing: 192.168.0.1 Customers'. Below this is a section titled 'Customers'. It includes a form to 'Choose a Customer Number' with a dropdown menu showing '1' and a 'to Add' button. Below the form is a table with one row: 'Customer: 0', 'Total routes: 25', 'Total trunks: 27', and an 'Edit' button.

| Customer    | Total routes | Total trunks | Action |
|-------------|--------------|--------------|--------|
| Customer: 0 | 25           | 27           | Edit   |

The **Customer 0 Property Configuration** screen is displayed next. Select **Feature Packages** toward the bottom of the screen.

The screenshot shows the 'Customer 0 Property Configuration' screen. The left sidebar is the same as the previous screen, but 'Customers' is now expanded, showing sub-items: Virtual Terminals, Bookmarks, Maintenance, Loops, Superloops, SNMP, Software, Nodes: Servers, Media Cards, Zones, Network Address Translation, QoS Thresholds, Personal Directories, Software, Routes and Trunks, Dialing and Numbering Plans, and Services. The main content area has a header 'Managing: 192.168.0.1 Customers > Customer 0 Property Configuration'. Below this is a section titled 'Customer 0 Property Configuration'. It includes a 'Basic Configuration' section with a table of input fields: 'Customer Data Block (CDB) (TYPE)' with value 'CDB', 'Customer number (CUST)' with value '0', 'ANI Attendant Billing number (ANAT)' with value '111', and 'ANI Listed Directory Number (ANLD)' with value '1111'. There is also an 'Options (OPT)' button. Below the table are several expandable sections: 'Flexible Feature Codes (FFC\_DATA)', 'Feature options (FTR\_DATA)', 'Listed Directory Number options (LDN\_DATA)', 'ISDN and ESN Networking options (NET\_DATA)', 'Night service options (NIT\_DATA)', and 'Feature Packages'.

| Input Description                   | Input Value |
|-------------------------------------|-------------|
| Customer Data Block (CDB) (TYPE)    | CDB         |
| Customer number (CUST)              | 0           |
| ANI Attendant Billing number (ANAT) | 111         |
| ANI Listed Directory Number (ANLD)  | 1111        |

Options (OPT) Edit

- > Flexible Feature Codes (FFC\_DATA)
- > Feature options (FTR\_DATA)
- > Listed Directory Number options (LDN\_DATA)
- > ISDN and ESN Networking options (NET\_DATA)
- > Night service options (NIT\_DATA)
- > Feature Packages



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.

The screenshot shows the 'CS 1000 ELEMENT MANAGER' interface. On the left is a navigation menu with 'Home', 'Links' (Virtual Terminals, Bookmarks), 'System' (Maintenance, Loops, Superloops, SNMP), and 'IP Telephony' (Nodes: Servers, Media Cards, Maintenance and Reports). The main area displays a list of feature packages:

| Feature Package                     | Package ID   |
|-------------------------------------|--------------|
| Enhanced Night Service              | Package: 133 |
| Integrated Services Digital Network | Package: 145 |
| Flexible Services                   | Package: 152 |
| Network Attendant Service           | Package: 159 |
| Flexible Numbering Plan             | Package: 160 |

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).

The screenshot shows the configuration page for 'Integrated Services Digital Network' (Package: 145). The left navigation menu is the same as in the previous screenshot. The main area contains the following configuration options:

| Input Description   | Input Value                         | Range            |
|---|-------------------------------------|------------------|
| <b>+ Dial Access Prefix on CLID table entry option (DAPC)</b> |                                     |                  |
| Integrated Services Digital Network (ISDN)                    | <input checked="" type="checkbox"/> |                  |
| - Virtual Private Network Identifier (VPNI)                   | <input type="text" value="0"/>      | Range: 1 - 16383 |
| - Private Network Identifier (PNI)                            | <input type="text" value="0"/>      | Range: 1 - 16383 |

## 5.4 Administer D-Channel

Under *Routes and Trunks*, select **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 screenshot shows the Nortel CS 1000 Element Manager interface. The top header is purple with the Nortel logo and the text "CS 1000 ELEMENT MANAGER". Below the header, the left sidebar contains a navigation menu with the following items: Home, Links (Virtual Terminals, Bookmarks), System (Maintenance, Loops, Superloops, SNMP, Software), IP Telephony (Nodes: Servers, Media Cards, Maintenance and Reports, Configuration, Zones, Network Address Translation, QoS Thresholds, Personal Directories, Software), Customers, Routes and Trunks (Routes and Trunks, **D-Channels**, Digital Trunk Interface). The main content area is titled "D-Channels" and shows the IP address "192.168.0.1" and the path "Routes and Trunks » D-Channels". Under the "Maintenance" section, there are links for "D-Channel Diagnostics (LD 96)", "Network and Peripheral Equipment (LD 32, Virtual D-Channels)", "MSDL Diagnostics (LD 96)", "TMDI Diagnostics (LD 96)", and "D-Channel Expansion Diagnostics (LD 48)". Under the "Configuration" section, there is a form with the label "Choose a D-Channel Number:" followed by a dropdown menu showing "8", the text "and type:", a dropdown menu showing "DCH", and a button labeled "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)”

**NORTEL CS 1000 ELEMENT MANAGER**

Managing: 192.168.8.1  
Routes and Trunks > D-Channels > D-Channels 8 Property Configuration

### D-Channels 8 Property Configuration

**- Basic Configuration**

| Input Description                                 | Input Value   |
|---|---|
| Action Device And Number (ADAN) (TYPE)            | CCH   |
| D channel Card Type (CTYP)                        | DCIP  |
| Designator (DES)                                  | ASM   |
| Necessary to Primary (DCVP)                       | <input type="checkbox"/>                            |
| User (USR)  | Integrated Services Signaling Link Dedicated (ISLD) |
| Interface type for D-channel (IFC)                | Meridian Meridian1 (SL1)                            |
| D-Channel PRI loop number (DCHL)                  |   |
| Primary Rate Interface (PRI)                      | <input type="button" value="more PRI"/>             |
| Secondary PRI2 loops (PRI2)                       |   |
| Meridian 1 node type (SIDE)                       | Slave to the controller (USR)                       |
| Release ID of the switch at the far end (RLS)     | 25  |
| Central Office switch type (CO_TYPE)              | 100% compatible with Bellcore standard (STD)        |
| Integrated Services Signaling Link Maximum (ISLM) | 4000<br>Range: 1 - 4000                             |
| Signaling Server Resource Capacity (SSRC)         | 1800<br>Range: 0 - 4000                             |

**+ Basic options (BSCOPT)**  
**+ Advanced options (ADVOPT)**  
**+ Feature Packages**

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.

| Input Description                                      | Input Value              |
|--|--------------------------|
| Basic rate interface (BRI)                             | <input type="checkbox"/> |
| Call completion on busy using integer value (CCB)      | <input type="checkbox"/> |
| Call completion on busy using object identifier (CCBO) | <input type="checkbox"/> |

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 “8”). Click to **Add**.

The screenshot shows the Nortel CS 1000 Element Manager interface. The left navigation pane includes links for Home, Links, System, and IP Telephony. The IP Telephony section is expanded, showing options like Nodes, Maintenance and Reports, Configuration, and Zones. The main content area is titled 'Zones' and shows a 'Please Choose the' dropdown menu with 'Zone 8' selected. There are buttons for 'Browse...', 'Import', and '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**.

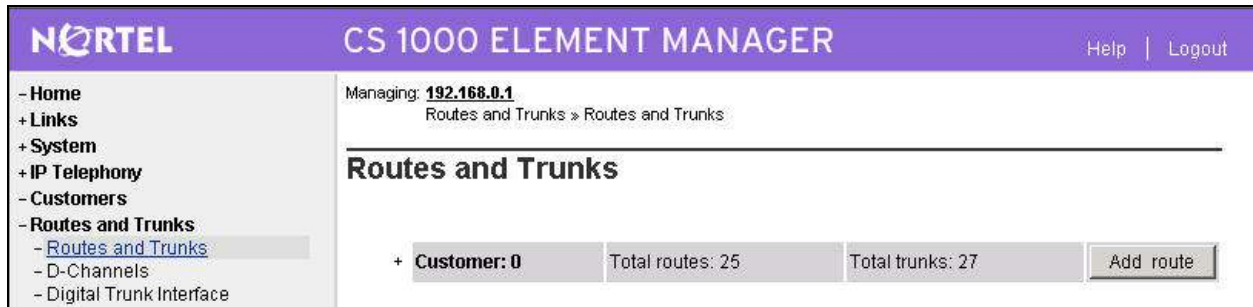
The screenshot shows the 'Zone Basic Property and Bandwidth Management' screen. The left navigation pane is the same as the previous screen. The main content area has a title bar and a table with two columns: 'Input Description' and 'Input Value'. The table contains the following fields:

| Input Description                | Input Value         |
|----------------------------------|---------------------|
| Zone Number (ZONE):              | 8                   |
| Intrazone Bandwidth (INTRA_BW):  | 1000000             |
| Intrazone Strategy (INTRA_STGY): | Best Quality (BQ)   |
| Interzone Bandwidth (INTER_BW):  | 1000000             |
| Interzone Strategy (INTER_STGY): | Best Bandwidth (BB) |
| Resource Type (RES_TYPE):        | Shared (SHARED)     |
| Zone Intent (ZBRN):              | VTRK (VTRK)         |
| Description (ZDES):              | ASMSIPZONE          |

At the bottom of the screen are buttons for 'Submit', 'Refresh', 'Delete', and 'Cancel'.

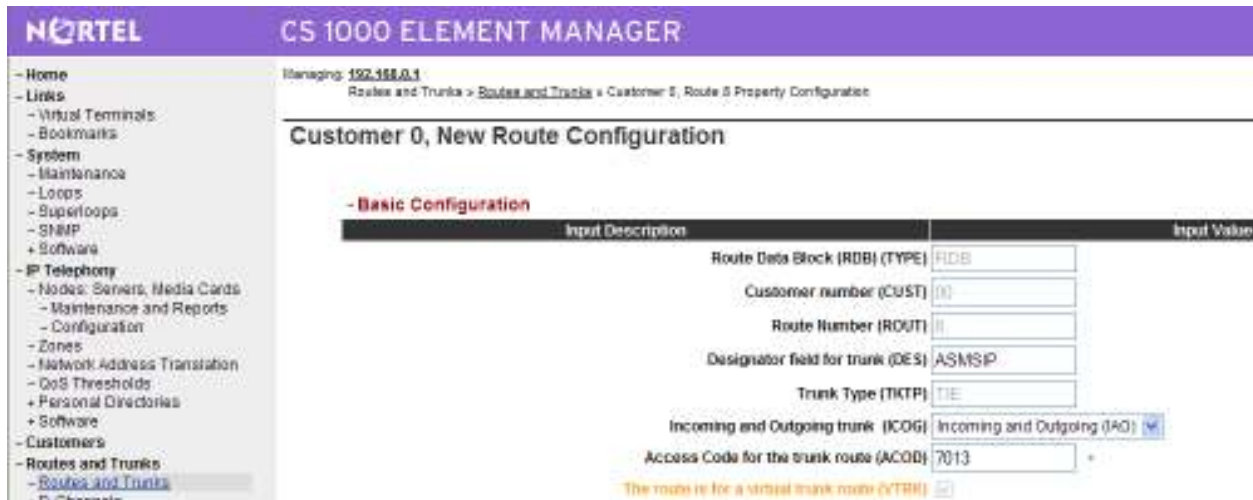
## 5.6 Administer Virtual SIP Routes and Trunks

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**.

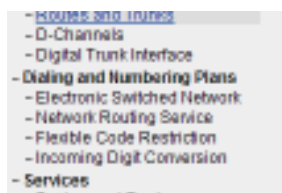


The **Customer 0, New Route Configuration** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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)”
- **Access Code for the trunk route (ACOD):** An available access code.



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.



The route is for a virtual trunk route (VTRK) ☒

- Zone for codec selection and bandwidth management (ZONE)  Range: 0 - 255

- Node ID of signaling server of this route (NODE)  Range: 0 - 9999

- Protocol ID for the route (PCID)

- Print Correlation ID in CDR for the route (CRID) ☐

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.



Integrated Services Digital Network option (ISDN) ☒

- Mode of operation (MODE)

- D channel number (DCH)

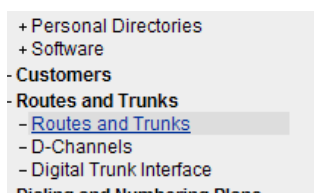
- Interface type for route (IFC)

- Private Network Identifier (PNI)  Range: 0 - 32767

- Network Calling Name Allowed (NCNA) ☒

Network Call Redirection (NCRD) ☒

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.



|             |           |                        |      |           |
|-------------|-----------|------------------------|------|-----------|
| + Route: 8  | Type: TIE | Description: ASMSIP    | Edit | Add trunk |
| - Route: 9  | Type: WAT | Description: NONE      | Edit | Add trunk |
| - Route: 10 | Type: TIE | Description: SIP TRUNK | Edit | Add trunk |
| + Route: 11 | Type: TIE | Description: SUCC      | Edit | Add trunk |



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 Communication Manager to Avaya Session Manager in **Section 3.6.2**. In the sample configuration, only four trunks were created due to capacity limitation on the 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**

Managing: 192.168.0.1  
Routes and Trunks > Routes and Trunks > Customer 0, Route 8, New Trunk Configuration

### Customer 0, Route 8, New Trunk Configuration

**- Basic Configuration**

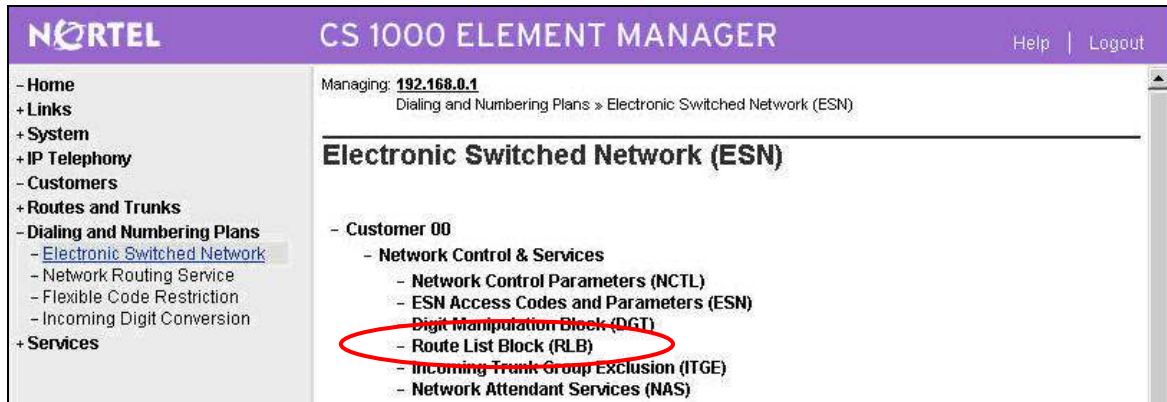
| Input Description                             | Input Value                              |
|---|--|
| Multiple trunk input number (MTINPUT)         | 4  |
| Trunk data block (TYPE)                       | IP Trunk (IPTI)                          |
| Terminal Number (TN)                          | 003 0 00 00                              |
| Designator field for trunk (DES)              | ASMSIPTRK                                |
| Extended Trunk (XTRK)                         | Virtual trunk (VTRK)                     |
| Customer number (CUST)                        | 0  |
| Route number, Member number (RTMB)            | 8 1                                      |
| Start arrangement Incoming (STRI)             | Wink or Fast Flash (WNK)                 |
| Start arrangement Outgoing (STRO)             | Wink or Fast Flash (WNK)                 |
| Trunk Group Access Restriction (TGAR)         | 1  |
| Channel ID for this trunk (CHID)              | 1  |
| Increase or decrease the member numbers (INC) | Increase channel and member number (YES) |
| Class of Service (CLS)                        | Edit                                     |

**+ Advanced Trunk Configurations**

Submit Cancel

## 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 “8”). Click to **Add**.

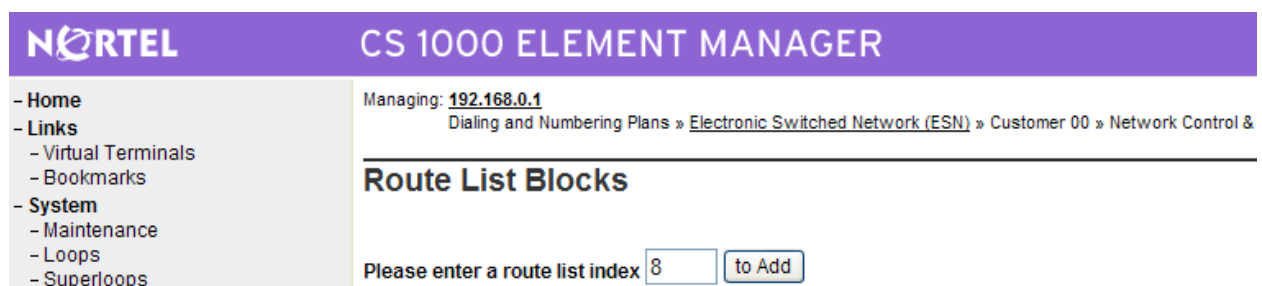


Figure 3: Route List Blocks

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).

**NORTEL CS 1000 ELEMENT MANAGER**

Managing: 192.168.0.1  
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Ro

### Route List Block

| Input Description  |
|--|
| Route List Index (RLI): <input type="text" value="8"/>                 |
| Entry Number for the Route List (ENTR): <input type="text" value="0"/> |
| Local Termination entry (LTER): <input type="checkbox"/>               |
| Route Number (ROUT): <input type="text" value="8"/>                    |

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.

**NORTEL CS 1000 ELEMENT MANAGER**

Help | Logout

### Electronic Switched Network (ESN)

- Customer 00
  - Network Control & Services
    - Network Control Parameters (NCTL)
    - ESN Access Codes and Parameters (ESN)
    - Digit Manipulation Block (DGT)
    - Route List Block (RLB)
    - Incoming Trunk Group Exclusion (ITGE)
    - Network Attendant Services (NAS)
  - Coordinated Dialing Plan (CDP)
    - Local Steering Code (LSC)
    - **Distant Steering Code (DSC)**
    - Trunk Steering Code (TSC)

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 “30”). Click to **Add**.

**NORTEL CS 1000 ELEMENT MANAGER**

Managing: 192.168.0.1  
Dialing and Numbering Plans » Electronic Switched Network (ESN) » C

### Distant Steering Code List

Please enter a distant steering code



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 click **Submit**.

The screenshot shows the 'Distant Steering Code' configuration page in the Nortel CS 1000 Element Manager. The left sidebar contains a navigation tree with options like Home, Links, System, IP Telephony, and Customers. The main content area has a breadcrumb trail: 'Managing: 192.168.0.1 > Dialing and Numbering Plan > Electronic Switched Network (ESN) > Customer DE > Coordinated Dialing Plan (CDP) > Distant Steering Code List'. The page title is 'Distant Steering Code'. Below the title is a table with two columns: 'Input Description' and 'Input Value'. The table contains the following fields:

| Input Description  | Input Value               |
|--|---------------------------|
| Distant Steering Code (DSC):                             | 30                        |
| Flexible Length number of digits (FLEN):                 | 5                         |
| Display (DSP):   | Local Steering Code (LSC) |
| Remote Radio Paging Access (RRPA):                       | <input type="checkbox"/>  |
| Route List to be accessed for trunk steering code (RLI): | 8                         |
| Collect Call Blocking (CCBA):                            | <input type="checkbox"/>  |
| maximum 7 digit NPA code allowed (NPA):                  |                           |
| maximum 7 digit NXX code allowed (NXX):                  |                           |

At the bottom of the form are four buttons: 'Submit', 'Refresh', 'Delete', and 'Cancel'.

## 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 screenshot shows the 'Node Configuration' page in the Nortel CS 1000 Element Manager. The left sidebar contains a navigation tree with options like Home, Links, System, IP Telephony, and Customers. The main content area has a breadcrumb trail: 'Managing: 192.168.0.1 > IP Telephony > Nodes: Servers, Media Cards > Node Configuration'. The page title is 'Node Configuration'. Below the title, there is a 'New Node' field with a 'to Add' button and an 'Import Node Files' button. At the bottom, there is a table with one row:

| Node ID     | Node IP               | Actions   |
|-------------|-----------------------|---|
| + Node: 271 | Node IP: 192.168.1.33 | <a href="#">Edit</a> <a href="#">Transfer / Status</a> <a href="#">Delete</a> |

The 'Edit' button for the first node is circled in red.

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 / Re-direct 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.

**- SIP GW Settings**

Primary Proxy / Re-direct IP address: 192.168.1.30

Primary Proxy / Re-direct IP Port: 5060

Primary Proxy Supports Registration: ☒

Primary CDS Proxy or Re-direct server flag: ☐

Secondary Proxy / Re-direct IP address: 0.0.0.0

Secondary Proxy / Re-direct IP Port: 5060

Secondary Proxy Supports Registration: ☐

Secondary CDS Proxy or Re-direct server flag: ☐

**CLID Parameters**

Country Code:

Area Code:

Subscriber / Number of digits to strip: 0

Subscriber / Prefix to insert:

National / Number of digits to strip: 0

National / Prefix to insert:

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. Both codes must be preceded by a “+”.

**- SIP URI Map**

Public E.164/National domain name: +1 \*

Public E.164/Subscribers domain name: +1732 \*

Public E.164/Unknown domain name:

Public E.164/Special Number domain name:

Private/UDP domain name:

Private/CDP domain name:

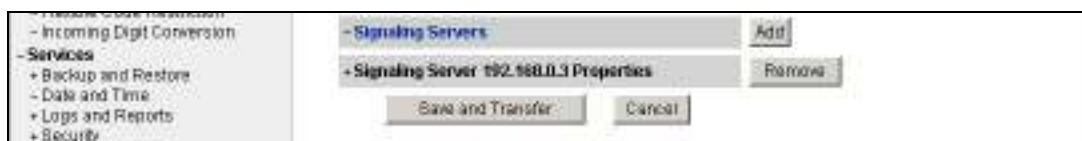
Private/Special Number domain name:

Private/Unknown (vacant number routing) domain name:

Unknown/Unknown domain name:

**+ SIP CD Services**

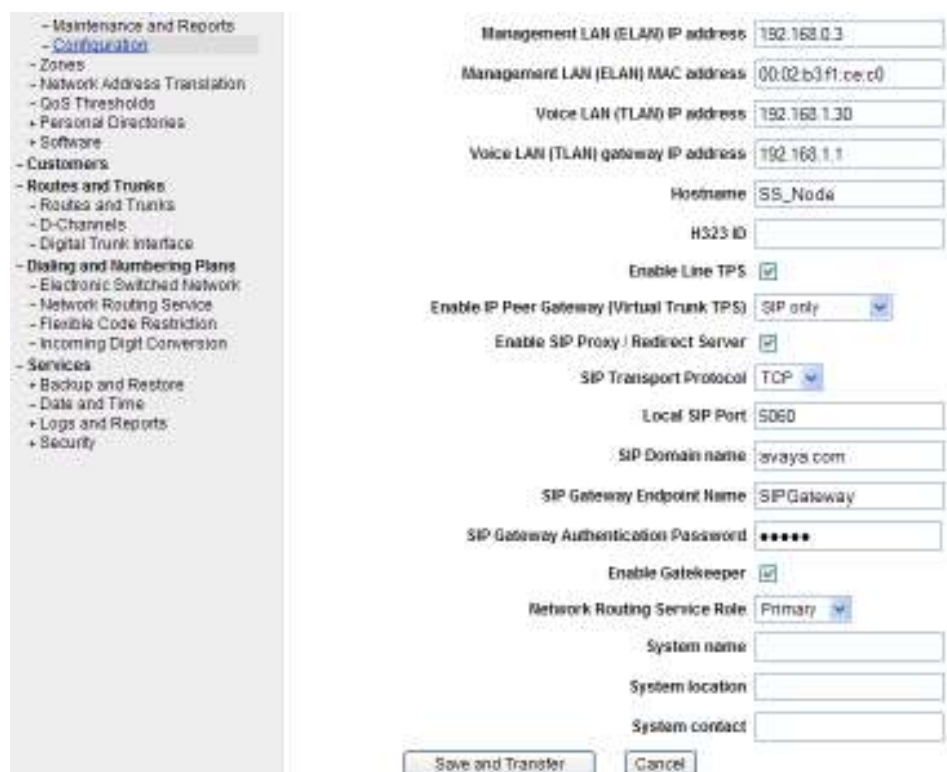
Scroll down the screen and select **Signaling Server** to expand it. Select **Signaling Server 192.168.0.3 Properties** to view a listing of parameters. Note that the displayed IP address for the Signaling Server may vary.



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**

Scroll down to the bottom of the screen, and click **Save and Transfer**.

The message dialog box below is displayed. Click **OK**.



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.

**NORTEL**

CS 1000 ELEMENT MANAGER

Help | Logout

Home

Links

System

IP Telephony

- Nodes: Servers, Media Cards
  - Maintenance and Reports
  - Configuration
- Zones
- Network Address Translation
- QoS Thresholds

Personal Directories

Software

Customers

Routes and Trunks

Dialing and Numbering Plans

Services

Managing: **192.168.0.1**

IP Telephony » Nodes: Servers, Media Cards » [Node Configuration](#) » IP Telephony: Node ID 271 » [Edit](#) » Transfer Progress

Transfer Progress

| Card        | Status   | bootp                               | config                              |
|-------------|----------|-------------------------------------|-------------------------------------|
| 192.168.0.3 | Complete | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 192.168.0.4 | Complete | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Microsoft Internet Explorer

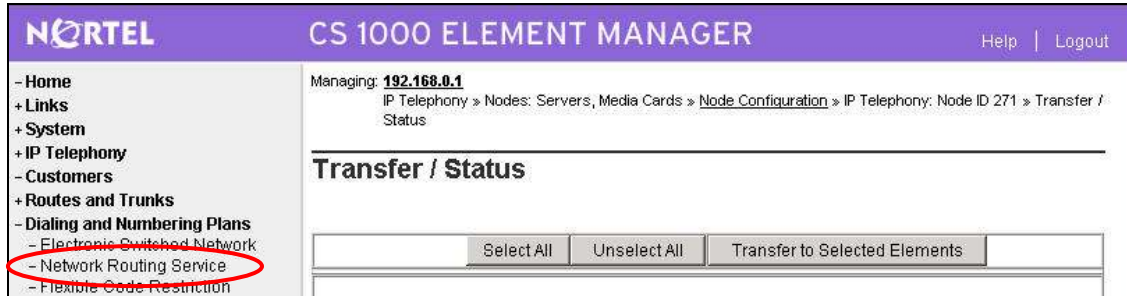
Transfer succesful to all elements in the node

OK

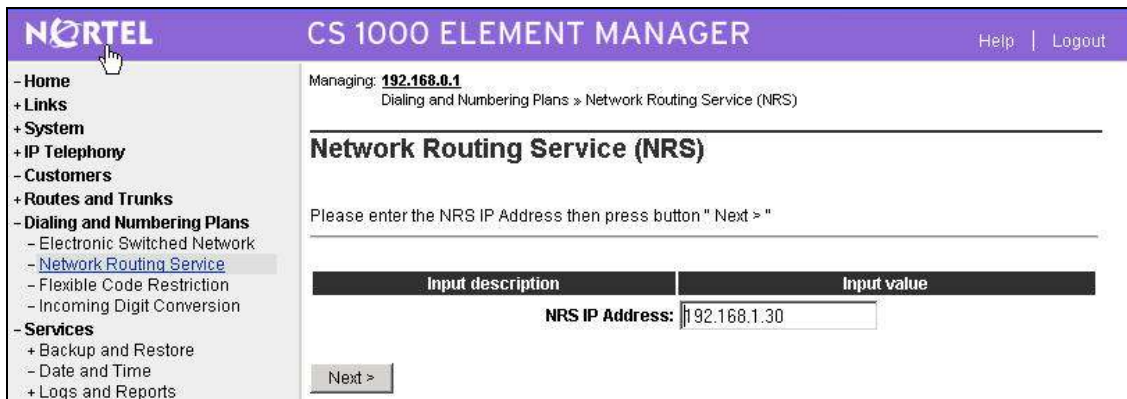


## 5.9 Launch NRS Manager

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.



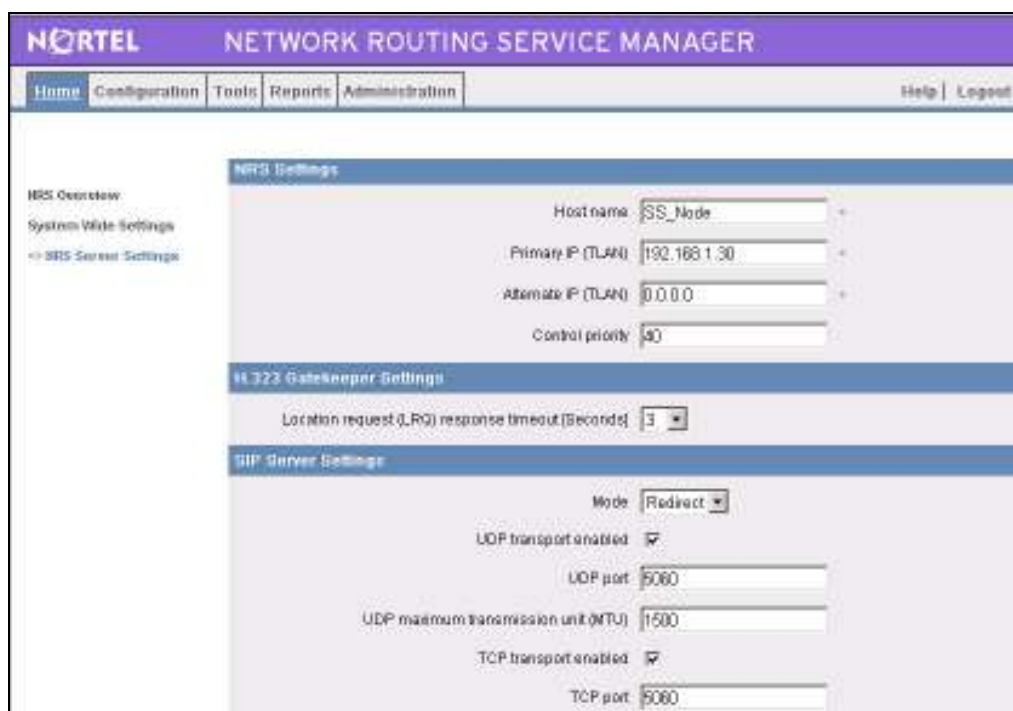
A separate Internet browser window is opened with the **NETWORK ROUTING SERVICE MANAGER** screen. Enter the appropriate credentials and click **Login**.



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.



The screenshot shows the Nortel Network Routing Service Manager (NRS) Configuration page. The page has a purple header with the Nortel logo and the title "NETWORK ROUTING SERVICE MANAGER". Below the header is a navigation bar with tabs: Home, Configuration, Tools, Reports, and Administration. The "Configuration" tab is selected. On the left side, there is a sidebar with "NRS Overview" and "System Wide Settings". Under "System Wide Settings", there is a link for "NRS Server Settings". The main content area is titled "NRS Settings" and contains several sections: "Host name" (SS\_Node), "Primary IP (TLAN)" (192.168.1.30), "Alternate IP (TLAN)" (0.0.0.0), "Control priority" (90), "H.323 Gatekeeper Settings" (Location request (LRQ) response timeout (Seconds) set to 3), and "SIP Server Settings" (Mode set to Redirect, UDP transport enabled checked, UDP port 5060, UDP maximum transmission unit (MTU) 1500, TCP transport enabled checked, TCP port 5060).

The message pop up dialog box below is displayed. Click **OK**.



## 5.10 Administer Service Domain

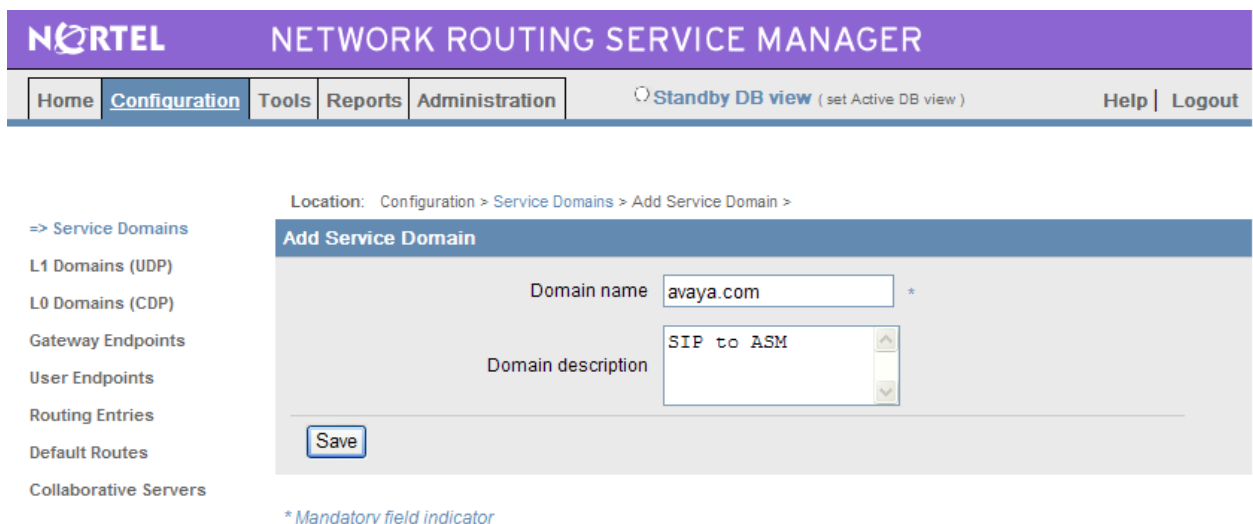
The NRS hosts an active and a standby database. The active database is used for runtime queries, and the standby database is used for administrative modifications. Click **(set Standby DB view)** to switch to the standby database, in order to make administrative changes.



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 9**.

The screenshot shows the Nortel Network Routing Service Manager interface. The top navigation bar includes 'Home', 'Configuration', 'Tools', 'Reports', and 'Administration'. The 'Configuration' tab is active, and a 'Standby DB view' link is present. The left sidebar lists 'Service Domains' with a sub-link '=> L1 Domains (UDP)'. The main content area is titled 'L1 Domains (UDP)' and shows the 'Show L1 Domains for (Service Domain):' section with a dropdown menu set to 'avaya.com' and a 'Show' button. Below this is an 'Add...' button.

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).

The screenshot shows the 'Add L1 Domain (avaya.com)' screen in the Nortel Network Routing Service Manager. The top navigation bar is the same as the previous screenshot. The left sidebar lists 'Service Domains' with a sub-link '=> L1 Domains (UDP)'. The main content area is titled 'Add L1 Domain (avaya.com)' and shows the 'View L1 Domain Property' section. The form includes the following fields: 'Domain name' (udp1), 'Domain description' (Avaya UDP L1 Domain), 'Endpoint authentication enabled' (Authentication off), 'Authentication password' (empty), 'E.164 country code' (1), 'E.164 area code' (732), and 'E.164 international dialing access code' (empty).

Select **L0 Domains (CDP)** in the left pane to display the **L0 Domains (CDP)** screen. Click **Add** to add a new L0 domain.

The screenshot shows the Nortel Network Routing Service Manager interface. The top navigation bar includes 'Home', 'Configuration', 'Tools', 'Reports', and 'Administration'. The 'Configuration' tab is active, and the 'Standby DB view' is selected. The left sidebar lists 'Service Domains', 'L1 Domains (UDP)', '=> L0 Domains (CDP)', 'Gateway Endpoints', 'User Endpoints', and 'Routing Entries'. The main content area shows the 'L0 Domains (CDP)' screen. The location path is 'Configuration > L0 Domains (CDP) >'. The title is 'L0 Domains (CDP)'. Below the title, it says 'Show L0 Domains for (Service Domain / L1 Domain):'. There are two dropdown menus: 'avaya.com' and 'udp1', followed by a 'Show' button. Below these is an 'Add...' button.

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).

The screenshot shows the Nortel Network Routing Service Manager interface. The top navigation bar includes 'Home', 'Configuration', 'Tools', 'Reports', and 'Administration'. The 'Configuration' tab is active, and the 'Standby DB view' is selected. The left sidebar lists 'Service Domains', 'L1 Domains (UDP)', '=> L0 Domains (CDP)', 'Gateway Endpoints', 'User Endpoints', 'Routing Entries', 'Default Routes', and 'Collaborative Servers'. The main content area shows the 'Add L0 Domain (avaya.com / udp1)' screen. The location path is 'Configuration > L0 Domains (CDP) > View L0 Domain Property >'. The title is 'Add L0 Domain (avaya.com / udp1)'. The form contains the following fields: 'Domain name' (text input with 'cdp1'), 'Domain description' (text input with 'Nortel L0 Domain'), 'Endpoint authentication enabled' (dropdown menu with 'Not configured'), 'Authentication password' (text input), 'E.164 country code' (text input), 'E.164 area code' (text input), 'Private unqualified number label' (text input), and 'E.164 international dialing access code' (text input).

## 5.11 Administer SIP Gateway Endpoints

Next, configure two SIP gateway endpoints; one for the Avaya Session Manager 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 Session Manager.

The screenshot shows the 'Gateway Endpoints' configuration page. The top navigation bar includes 'Home', 'Configuration', 'Tools', 'Reports', and 'Administration'. The 'Configuration' tab is active, and a 'Standby DB view' link is present. The left sidebar lists 'Service Domains', 'L1 Domains (UDP)', 'L0 Domains (CDP)', '=> Gateway Endpoints', and 'User Endpoints'. The main content area shows the breadcrumb 'Location: Configuration > Gateway Endpoints >'. Below this is a section titled 'Gateway Endpoints' with a sub-header 'Show Gateway Endpoints for (Service Domain / L1 Domain / L0 Domain):'. Three dropdown menus are set to 'avaya.com', 'udp1', and 'cdp1', followed by a 'Show' button. An 'Add...' button is located at the bottom left of the main content area.

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.

The screenshot shows the 'View Gateway Endpoint Property' page for the endpoint 'avaya.com / udp1 / cdp1'. The top navigation bar is the same as the previous screenshot. The left sidebar lists 'Service Domains', 'L1 Domains (UDP)', 'L0 Domains (CDP)', '=> Gateway Endpoints', 'User Endpoints', 'Routing Entries', 'Default Routes', and 'Collaborative Servers'. The main content area shows the breadcrumb 'Location: Configuration > Gateway Endpoints > View Gateway Endpoint Property >'. Below this is a section titled 'View Gateway Endpoint Property (avaya.com / udp1 / cdp1)'. It contains four fields: 'Endpoint name' with the value 'ASM1', 'Endpoint description' with the value 'Avaya SM1 (SM-100)', 'Tandem gateway endpoint name' which is empty, and 'Endpoint authentication enabled' with a dropdown menu set to 'Authentication off'. A 'Look up' link is next to the 'Tandem gateway endpoint name' field.

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 Session Manager SM-100 Module interface
- **H.323 Support:** “Not RAS H.323 endpoint”
- **SIP support:** “Static SIP endpoint”
- **SIP transport:** “TCP”

Static endpoint address type: IP version 4

Static endpoint address: 10.1.2.170

H.323 Support: H.323 not supported

SIP support: Static SIP endpoint

SIP transport: TCP

SIP port: 5060

Network Connection Server enabled: ☐

Buttons: Save, Delete

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**.

**NORTEL** NETWORK ROUTING SERVICE MANAGER

Home Configuration Tools Reports Administration Standby DB view (set Active DB view) Help Logout

Location: Configuration > Gateway Endpoints > View Gateway Endpoint Property >

Add Gateway Endpoint (avaya.com / udp1 / cdp1)

Endpoint name: SIPGateway \*

Endpoint description: NortelRedirect server

Tandem gateway endpoint name: Look up

Endpoint authentication enabled: Authentication on

Service Domains

L1 Domains (UDP)

L0 Domains (CDP)

=> Gateway Endpoints

User Endpoints

Routing Entries

Default Routes

Collaborative Servers

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**.

Static endpoint address

H.323 Support

SIP support

SIP transport

SIP port

Network Connection Server enabled ☐

## 5.12 Administer Routing Entry

Configure two routing entries. The first entry uses the Avaya 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 Session Manager (in this case “ASM1”), and click **Show**, followed by **Add** to add a routing entry.

**NORTEL** NETWORK ROUTING SERVICE MANAGER

Home Configuration Tools Reports Administration Standby DB view ( set Active DB view ) Help Logout

Location: Configuration > Routing Entries >

**Routing Entries**

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)  
Select domains and enter a gateway endpoint name to show specified routing entries.  
Use the wildcard \* by itself for all gateway endpoints :

avaya.com / udp1 / cdp1 /

Gateway Endpoint:  [Look up](#)

With DN Type:

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.

The screenshot shows the 'View Routing Entry Property' screen in the Nortel Network Routing Service Manager. The breadcrumb trail is 'Configuration > Routing Entries > View Routing Entry Property >'. The title bar indicates the view is for 'avaya.com / udp1 / cdp1 / ASM1'. The form contains three fields: 'DN type' set to 'Private level 0 regional (CDP steering code)', 'DN prefix' set to '30', and 'Route cost (1 -255)' set to '1'. There are 'Save' and 'Delete' buttons at the bottom. A sidebar on the left lists navigation options like 'Service Domains', 'L1 Domains (UDP)', 'L0 Domains (CDP)', 'Gateway Endpoints', 'User Endpoints', and 'Routing Entries' (highlighted). A footer note states '\* Mandatory field indicator'.

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.

The screenshot shows the 'Routing Entries' screen in the Nortel Network Routing Service Manager. The breadcrumb trail is 'Configuration > Routing Entries >'. The title bar indicates the view is for 'avaya.com / udp1 / cdp1 / ASM1'. The form contains three dropdown menus for 'avaya.com', 'udp1', and 'cdp1', followed by a comma. Below these is a 'Gateway Endpoint' field set to 'SIPGateway' with a 'Look up' button. There is also a 'With DN Type' dropdown set to '< All DN Types >' and a 'Show' button. An 'Add...' button is at the bottom left. A sidebar on the left lists navigation options like 'Service Domains', 'L1 Domains (UDP)', 'L0 Domains (CDP)', 'Gateway Endpoints', 'User Endpoints', and 'Routing Entries' (highlighted).

**NORTEL** NETWORK ROUTING SERVICE MANAGER

Home Configuration **Tools** Reports Administration Standby DB view ( set Active DB view ) Help | Logout

Location: Configuration > Routing Entries > View Routing Entry Property >

**Add Routing Entry (avaya.com / udp1 / cdp1 / SIPGateway)**

DN type: Private level 0 regional (CDP steering code) ▼

DN prefix: 53 \*

Route cost (1 -255): 1 \*

Save Delete

\* Mandatory field indicator

Service Domains  
L1 Domains (UDP)  
L0 Domains (CDP)  
Gateway Endpoints  
User Endpoints  
=> Routing Entries  
Default Routes  
Collaborative Servers

### 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**.

**NORTEL** NETWORK ROUTING SERVICE MANAGER

Home Configuration Tools **Reports** Administration Help | Logout

Location: Tools > Database Actions >

**Database Actions [ Database State: Changed ]**

Select database action: Cut over & Commit ▼ Submit

H.323 Routing Test  
SIP Routing Test  
Server Actions  
=> Database Actions



## 6 Configuration Steps for Alternate Routing Operation

The following sections describe the configuration steps for implementing alternate call routing features to handle network failures:

1. Avaya Aura Communication Manager 5.2 and the Nortel Communication Server 1000 are configured to route calls to a second Avaya Aura Session Manager, should there be no response from the first. This is known as “Active-Active” operation, in which either Avaya Aura Session Manager can accept calls at any time.
2. A “route-through” link is configured between the two Avaya Aura Session Managers. If a call from the first Avaya Aura Session Manager to Avaya Aura Communication Manager 5.2 on the primary SIP trunk via *clan1* fails, the call will be routed through this link to the other Avaya Aura Session Manager, which can then route the call to the secondary trunk via *clan2*.

### 6.1 Configure Avaya Aura Communication Manager 5.2

Repeat the steps in **Section 3.3**, adding node names and IP addresses for the second C-LAN interface and second Avaya Aura Session Manager SM-100 interface.

| change node-names ip |                   | Page 1 of 2 |
|----------------------|-------------------|-------------|
| IP NODE NAMES        |                   |             |
| Name                 | IP Address        |             |
| clan1                | 10.1.2.233        |             |
| Gateway001           | 10.1.2.1          |             |
| sm1                  | 10.1.2.170        |             |
| <b>clan2</b>         | <b>10.1.2.234</b> |             |
| <b>sm2</b>           | <b>10.1.2.180</b> |             |

Repeat the steps in **Section 3.4**, adding the second C-LAN interface.

| add ip-interface 1a03                       |   | Page 1 of 3 |
|---|---|-------------|
| IP INTERFACES                               |   |             |
| Type: C-LAN                                 | Target socket load and Warning level: 400 |             |
| Slot: 01A03                                 | Receive Buffer TCP Window Size: 8320      |             |
| Code/Suffix: TN799 D                        |   |             |
| <b>Enable Interface? y</b>                  | <b>Allow H.323 Endpoints? y</b>           |             |
| VLAN: n                                     | Allow H.248 Gateways? y                   |             |
| Network Region: 1                           | Gatekeeper Priority: 5                    |             |
| IPV4 PARAMETERS                             |   |             |
| Node Name: clan2                            |   |             |
| Subnet Mask: /24                            |   |             |
| Gateway Node Name: Gateway001               |   |             |
| Ethernet Link: 2                            |   |             |
| Network uses 1's for Broadcast Addresses? y |   |             |

Repeat the steps in **Section 3.6**, adding the second signaling and trunk groups for the second Avaya Aura Session Manager.

|                                     |                                    |             |
|-------------------------------------|------------------------------------|-------------|
| <b>add signaling-group 33</b>       |                                    | Page 1 of 1 |
| SIGNALING GROUP                     |                                    |             |
| Group Number: 33                    | Group Type: sip                    |             |
|                                     | Transport Method: tls              |             |
| IMS Enabled? n                      |                                    |             |
| Near-end Node Name: clan2           | Far-end Node Name: sm2             |             |
| Near-end Listen Port: 5061          | Far-end Listen Port: 5061          |             |
|                                     | Far-end Network Region: 1          |             |
| Far-end Domain: avaya.com           |                                    |             |
|                                     | Bypass If IP Threshold Exceeded? n |             |
| DTMF over IP: rtp-payload           | Direct IP-IP Audio Connections? y  |             |
|                                     | IP Audio Hairpinning? n            |             |
| Enable Layer 3 Test? n              | Direct IP-IP Early Media? n        |             |
| Session Establishment Timer(min): 3 | Alternate Route Timer(sec): 6      |             |

|                           |                       |                |
|---------------------------|-----------------------|----------------|
| <b>add trunk-group 33</b> |                       | Page 1 of 21   |
| TRUNK GROUP               |                       |                |
| Group Number: 33          | Group Type: sip       | CDR Reports: y |
| Group Name: To SM2        | COR: 1                | TN: 1 TAC: 133 |
| Direction: two-way        | Outgoing Display? y   |                |
| Dial Access? n            | Night Service:        |                |
| Queue Length: 0           |                       |                |
| Service Type: tie         | Auth Code? n          |                |
|                           | Signaling Group: 33   |                |
|                           | Number of Members: 10 |                |

Add this second trunk group to the routing pattern for calls to the Nortel Communications System 1000 (see **Section 3.7**). Set the Look Ahead Routing (**LAR**) field to “next” corresponding to the first trunk group. This will permit routing to the second Avaya Aura Session Manager if the initial attempt to the first one fails.

|   |     |     |     |     |      |     |          |      |  |  |   |             |      |      |
|---|-----|-----|-----|-----|------|-----|----------|------|--|--|---|-------------|------|------|
| change route-pattern 32   |     |     |     |     |      |     |          |      |  |  |   | Page 1 of 3 |      |      |
| Pattern Number: 32    Pattern Name: To ASM  |     |     |     |     |      |     |          |      |  |  |   |             |      |      |
| SCCAN? n    Secure SIP? n   |     |     |     |     |      |     |          |      |  |  |   |             |      |      |
| Grp   | FRL | NPA | Pfx | Hop | Toll | No. | Inserted |      |  |  |   | DCS/        | IXC  |      |
| No  |     |     | Mrk | Lmt | List | Del | Digits   |      |  |  |   | QSIG        |      |      |
|   |     |     |     |     |      |     |          |      |  |  |   | Intw        |      |      |
| 1:  | 32  | 0   |     |     |      |     |          |      |  |  |   | n           | user |      |
| 2:  | 33  | 0   |     |     |      |     |          |      |  |  |   | n           | user |      |
| 3:  |     |     |     |     |      |     |          |      |  |  | n | user        |      |      |
| 4:  |     |     |     |     |      |     |          |      |  |  | n | user        |      |      |
| 5:  |     |     |     |     |      |     |          |      |  |  | n | user        |      |      |
| 6:  |     |     |     |     |      |     |          |      |  |  | n | user        |      |      |
| BCC VALUE    TSC    CA-TSC    ITC    BCIE    Service/Feature    PARM    No.    Numbering    LAR |     |     |     |     |      |     |          |      |  |  |   |             |      |      |
| 0 1 2 M 4 W    Request    Dgts    Format    Subaddress  |     |     |     |     |      |     |          |      |  |  |   |             |      |      |
| 1:  | y   | y   | y   | y   | y    | n   | n        | rest |  |  |   |             |      | next |
| 2:  | y   | y   | y   | y   | y    | n   | n        | rest |  |  |   |             |      | none |

Add the second trunk group to the public-unknown-numbering table (see **Section 3.8**).

|                                   |      |        |        |     |                       |  |  |  |  |             |  |
|-----------------------------------|------|--------|--------|-----|-----------------------|--|--|--|--|-------------|--|
| change public-unknown-numbering 0 |      |        |        |     |                       |  |  |  |  | Page 1 of 2 |  |
| NUMBERING - PUBLIC/UNKNOWN FORMAT |      |        |        |     |                       |  |  |  |  |             |  |
| Total                             |      |        |        |     |                       |  |  |  |  |             |  |
| Ext                               | Ext  | Trk    | CPN    | CPN |                       |  |  |  |  |             |  |
| Len                               | Code | Grp(s) | Prefix | Len |                       |  |  |  |  |             |  |
| 5                                 | 3    | 32,33  |        | 5   | Total Administered: 2 |  |  |  |  |             |  |
|                                   |      |        |        |     | Maximum Entries: 9999 |  |  |  |  |             |  |

## 6.2 Configure Avaya Aura Session Manager

Repeat the steps in Sections 4.3 and 4.8 to add a second Avaya Aura Session Manager.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on 01 Jun 02, 2009 10:51 AM  
Help | Log off

Home / Network Routing Policy / SIP Entities / SIP Entity Details

**SIP Entity Details** [Commit] [Cancel]

**General**

| Name  | FQDN or IP Address | Type            | Notes |
|-------|--------------------|-----------------|-------|
| * SM2 | * 10.1.2.180       | Session Manager |       |

**Entity Links \***

Adaptation: [Select]  
Location: [Lincoln] \*  
Outbound Proxy: [Select]  
Time Zone: [America/New\_York]  
Override Port & Transport with DNS SRV: ☐  
SIP Timer B/F (secs): \* 4  
Credential name: [Text Box]

**Monitoring**

Monitoring on/off: Use Session Manager configuration [Select]

**Port**

[Add] [Remove]

2 Items | Refresh Filter: Enable

| Port                          | Protocol | Default Domain | Notes |
|-------------------------------|----------|----------------|-------|
| <input type="checkbox"/> 5060 | TCP      | avaya.com      |       |
| <input type="checkbox"/> 5061 | TLS      | avaya.com      |       |

Select: All, None ( 0 of 2 Selected )

\* Input Required [Commit] [Cancel]

Repeat the steps in Section 4.3 to create a SIP Entity corresponding to the second SIP trunk to Avaya Aura Communication Manager 5.2 via *clan2*.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, admin Last Logged on at Jun. 02, 2009 10:51 AM  
Help | Log off

Home / Network Routing Policy / SIP Entities / SIP Entity Details

**SIP Entity Details** [Commit] [Cancel]

**General**

| Name                    | FQDN or IP Address | Type | Notes |
|-------------------------|--------------------|------|-------|
| * Call Center ACM CLAN2 | * 10.1.2.234       | CM   |       |

**Entity Links \***

Adaptation: [dropdown]  
Location: [Lincoln] [dropdown]  
Time Zone: [America/New\_York] [dropdown]  
Override Port & Transport with DNS SRV: ☐  
SIP Timer B/F (secs): \* 4  
Credential name: [text field]  
Call Detail Recording: [egress] [dropdown]

**Monitoring**

Monitoring on/off: [Use Session Manager configuration] [dropdown]

\* Input Required [Commit] [Cancel]

**Shortcuts**

- Change Password
- SIP Entity Details field descriptions
- Saving/Committing/Synchronizing configuration changes

Repeat the steps in **Section 4.4** to create Entity Links from *clan2* and the Nortel Communication Server 1000 to the second Avaya Aura Session Manager.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Jun. 02, 2009 1

Home / Network Routing Policy / Entity Links

**Entity Links**

1 Item Refresh Filter: Enable

| Name          | SIP Entity 1 | Port | SIP Entity 2          | Port | Trusted                             | Protocol | Notes |
|---------------|--------------|------|-----------------------|------|-------------------------------------|----------|-------|
| SM2 ACM CLAN2 | SM2          | 5061 | Call Center ACM CLAN2 | 5061 | <input checked="" type="checkbox"/> | TLS      |       |

\* Input Required

Commit Cancel

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Jun. 02, 2009 1

Home / Network Routing Policy / Entity Links

**Entity Links**

1 Item Refresh Filter: Enable

| Name              | SIP Entity 1 | Port | SIP Entity 2  | Port | Trusted                             | Protocol | Notes |
|-------------------|--------------|------|---------------|------|-------------------------------------|----------|-------|
| SM2 Nortel CS1000 | SM2          | 5060 | Nortel CS1000 | 5060 | <input checked="" type="checkbox"/> | TCP      |       |

\* Input Required

Commit Cancel

To support route-through between the Avaya Aura Session Managers, create an Entity Link between them.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Jun. 01, 2009

Home / Network Routing Policy / Entity Links

**Entity Links**

1 Item Refresh Filter: Enable

| Name    | SIP Entity 1 | Port | SIP Entity 2 | Port | Trusted                             | Protocol | Notes |
|---------|--------------|------|--------------|------|-------------------------------------|----------|-------|
| SM1 SM2 | SM1          | 5061 | SM2          | 5061 | <input checked="" type="checkbox"/> | TLS      |       |

\* Input Required

Commit Cancel

Repeat the steps in **Section 4.6** to add a Routing Policy for the second SIP trunk to Avaya Aura Communication Manager 5.2.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Jun. 02, 2009 10:51 AM  
Help | Log off

Home / Network Routing Policy / Routing Policies / Routing Policy Details

**Routing Policy Details** [Comm] [Cancel]

**General**

| Name                  | Disabled                 | Notes |
|-----------------------|--------------------------|-------|
| Call Center ACM CLAN2 | <input type="checkbox"/> |       |

**SIP Entity as Destination**

[Select]

| Name                  | FQDN or IP Address | Type | Notes |
|-----------------------|--------------------|------|-------|
| Call Center ACM CLAN2 | 10.1.2.234         | CH   |       |

**Time of Day**

[Add] [Remove] [View Gaps/Overlaps]

1 Item | Refresh Filter: Enable

| Ranking | Name    | Mon                      | Tue                      | Wed                      | Thu                      | Fri                      | Sat                      | Sun                      | Start Time | End Time | Notes |
|---------|---------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------|----------|-------|
| 0       | Anytime | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 00:00      | 23:59    |       |

Select: All, None ( 0 of 1 Selected )

**Dial Patterns**

[Add] [Remove]

1 Item | Refresh Filter: Enable

| Pattern | Min | Max | Emergency Call           | SIP Domain | Originating Location | Notes |
|---------|-----|-----|--------------------------|------------|----------------------|-------|
| 30      | 5   | 5   | <input type="checkbox"/> | avaya.com  | -ALL-                |       |

Select: All, None ( 0 of 1 Selected )



## 6.3 Configure Nortel Communication Server 1000

Repeat the Steps in **Section 5.11** to add a SIP gateway corresponding to the second Avaya Aura Session Manager.

The screenshot displays the Nortel Network Routing Service Manager web interface. The top navigation bar includes the Nortel logo and the title "NETWORK ROUTING SERVICE MANAGER". Below this is a secondary navigation bar with tabs for Home, Configuration, Tools, Reports, and Administration. The Configuration tab is active, and a link for "Standby DB view" is visible. On the left side, a sidebar menu lists various configuration options, with "Gateway Endpoints" selected. The main content area shows the "View Gateway Endpoint Property" page for the endpoint named "ASM2". The page includes fields for the endpoint name, description, tandem gateway endpoint name, and authentication status. Below these, there are settings for static endpoint address type, address, H.323 support, SIP support, SIP transport, and SIP port. A checkbox for "Network Connection Server enabled" is also present. At the bottom, there are "Save" and "Delete" buttons.

Location: Configuration > Gateway Endpoints > View Gateway Endpoint Property >

**View Gateway Endpoint Property (avaya.com / udp1 / cdp1)**

Endpoint name:  \*

Endpoint description:

Tandem gateway endpoint name:  [Look up](#)

Endpoint authentication enabled:

Static endpoint address type:

Static endpoint address:

H.323 Support:

SIP support:

SIP transport:

SIP port:

Network Connection Server enabled: ☐

Repeat the Steps in **Section 5.12** to add a second route entry with more expensive weight for the second Avaya Aura Session Manager. This gateway will be chosen after an attempt to route using the lower cost gateway (ASM1) has failed.

**NETWORK ROUTING SERVICE MANAGER**

[Home](#)
[Configuration](#)
[Tools](#)
[Reports](#)
[Administration](#)

Standby DB view ( set Active DB view )

[Help](#) | [Logout](#)

Service Domains
L1 Domains (UDP)
L0 Domains (CDP)
Gateway Endpoints
User Endpoints
=> Routing Entries
Default Routes
Collaborative Servers

Location: Configuration > Routing Entries >

**Routing Entries**

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)  
Select domains and enter a gateway endpoint name to show specified routing entries.  
Use the wildcard \* by itself for all gateway endpoints :

avaya.com

udp1

cdp1

Gateway Endpoint:

ASM2

[Look up](#)

With DN Type:

< All DN Types >

Show

Add...

| #                 | DN Prefix | DN Type | Route Cost | SIP URI Phone Context |
|-------------------|-----------|---------|------------|-----------------------|
| <div>Add...</div> |           |         |            |                       |

**NETWORK ROUTING SERVICE MANAGER**

[Home](#)
[Configuration](#)
[Tools](#)
[Reports](#)
[Administration](#)

Standby DB view ( set Active DB view )

[Help](#) | [Logout](#)

Service Domains
L1 Domains (UDP)
L0 Domains (CDP)
Gateway Endpoints
User Endpoints
=> Routing Entries
Default Routes
Collaborative Servers

Location: Configuration > Routing Entries > Add Routing Entry >

**Add Routing Entry (avaya.com / udp1 / cdp1 / ASM2)**

DN type

Private level 0 regional (CDP steering code)

DN prefix

30

\*

Route cost (1 -255)

2

\*

Save

\* Mandatory field indicator

## 7 Verification Steps

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

### 7.1 Verify Avaya Communication Manager

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 |        |                 |                              |
|--------------------|--------|-----------------|------------------------------|
| Member             | Port   | Service State   | Mtce Connected Ports<br>Busy |
| 0032/001           | T00226 | in-service/idle | no                           |
| 0032/002           | T00227 | in-service/idle | no                           |
| 0032/003           | T00228 | in-service/idle | no                           |
| 0032/004           | T00229 | in-service/idle | no                           |
| 0032/005           | T00230 | in-service/idle | no                           |
| 0032/006           | T00231 | in-service/idle | no                           |
| 0032/007           | T00232 | in-service/idle | no                           |
| 0032/008           | T00233 | in-service/idle | no                           |
| 0032/009           | T00234 | in-service/idle | no                           |
| 0032/010           | T00235 | in-service/idle | no                           |

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 |                         |
| <b>Group State: in-service</b>                |                         |

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 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 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.

|                              |   |             |
|------------------------------|---|-------------|
| <b>status trunk 32/1</b>     |   | Page 1 of 3 |
| TRUNK STATUS                 |   |             |
| Trunk Group/Member: 0032/001 | <b>Service State: in-service/active</b> |             |
| Port: T00226                 | Maintenance Busy? no                    |             |
| Signaling Group ID: 32       |   |             |
| IGAR Connection? no          |   |             |
| Connected Ports: S00504      |   |             |

|   |                      |                             |
|---|----------------------|-----------------------------|
| <b>status trunk 32/1</b>                |                      | Page 2 of 3                 |
| CALL CONTROL SIGNALING                  |                      |                             |
| Near-end Signaling Loc: 01A0217         |                      |                             |
| <b>Signaling</b>                        | <b>IP Address</b>    | <b>Port</b>                 |
| <b>Near-end:</b>                        | <b>10.1.2.233</b>    | <b>: 5060</b>               |
| <b>Far-end:</b>                         | <b>10.1.2.170</b>    | <b>: 5060</b>               |
| H.245 Near:                             |                      |                             |
| H.245 Far:                              |                      |                             |
| H.245 Signaling Loc:                    |                      | H.245 Tunneled in Q.931? no |
| <b>Audio Connection Type: ip-direct</b> |                      | Authentication Type: None   |
| Near-end Audio Loc:                     |                      | Codec Type: G.711MU         |
| <b>Audio</b>                            | <b>IP Address</b>    | <b>Port</b>                 |
| <b>Near-end:</b>                        | <b>10.1.2.253</b>    | <b>: 6646</b>               |
| <b>Far-end:</b>                         | <b>192.45.100.73</b> | <b>: 5200</b>               |
| Video Near:                             |                      |                             |
| Video Far:                              |                      |                             |
| Video Port:                             |                      |                             |
| Video Near-end Codec:                   |                      | Video Far-end Codec:        |

## 7.2 Verify Avaya Session Manager

Expand the **Session Manager** menu on the left and click **SIP Monitoring**. Verify that none of the links to the defined SIP entities are down, indicating that they are all reachable for call routing. In the sample screen below, the SIP trunk to SM1 has been busied out on Avaya Aura Communication Manager 5.2, so one of the links is shown as down.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Jun. 02, 2009 1:00 PM

Home / Session Manager / SIP Monitoring

**SIP Entity Link Monitoring Status Summary**

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

Refresh

| Session Manager Name | Entity Links Down/Total | Entity Links Partially Down | SIP Entities - Monitoring Not Started | SIP Entities - Not Monitored |
|----------------------|-------------------------|-----------------------------|---------------------------------------|------------------------------|
| SM1                  | 1/8                     | 0                           | 0                                     | 0                            |
| SM2                  | 0/5                     | 0                           | 0                                     | 0                            |

**All Monitored SIP Entities**

Refresh

10 Items Filter: Enable

| SIP Entity Name       |
|-----------------------|
| AcmePacket            |
| Avaya-G430            |
| Avaya-S8500           |
| Call Center ACM-CLAN1 |
| Call Center ACM-CLAN2 |
| CiscoUCM-2            |
| CiscoUCME             |
| Nortel CS1000         |
| SM1                   |
| SM2                   |

Select the corresponding Avaya Aura Session Manager (**SM1** in this example) to view the Entity Link that is down and the Reason Code. The Reason Code reflects the result of Avaya Aura Session Manager sending a SIP OPTIONS message to that SIP Entity.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Jun. 02, 2009 1:00 PM

Home / Session Manager / SIP Monitoring / ASM Entity Link Status

**Session Manager Entity Link Connection Status**

This page displays detailed connection status for all entity links from a Session Manager where at least one connection is currently down.

All Entity Links with Down Connections for Session Manager: SM1

Refresh Summary View

1 Item Filter: Enable

| Details | SIP Entity Name       | SIP Entity Resolved IP | Port | Proto | Conn. Status | Reason Code               | Link Status |
|---------|-----------------------|------------------------|------|-------|--------------|---------------------------|-------------|
| Show    | Call Center ACM-CLAN1 | 10.1.2.233             | 5061 | TLS   | DOWN         | 300 Server Internal Error | DOWN        |

## 7.3 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.

Managing: 192.168.0.1  
Services > Logs and Reports > Node Maintenance and Reports

### Node Maintenance and Reports

| Index         | ELAN IP     | Type                  | TH    |
|---------------|-------------|-----------------------|-------|
| SS_Node       | 192.168.0.3 | Signaling Server      | NO TN |
| Media-Card-14 | 192.168.0.4 | Succession Media Card | 14 0  |

Buttons: GEN CMD, RPT LOG, OM RPT, Reset, Virtual Terminal, Status

Status bar: 192.168.0.3 : Enabled

## 7.4 Verify Alternate Routing

The following tests can verify proper alternate routing operation::

- Disconnect the SM-100 network interface on the first Avaya Aura Session Manager (SM1). Make a call from Nortel Communication Server 1000 and Avaya Aura Communication Manager 5.2. Verify using a network sniffer that the call is successfully routed to SM2 and on to the second SIP trunk via clan2.
- Busy out the signaling group for the first SIP trunk on Avaya Aura Communication Manager 5.2. Make a call from Nortel Communication Server 1000 and Avaya Aura Communication Manager 5.2. Verify using the **list trace tac SAT** command that the call is routed to the second SIP trunk via clan2, which means that SM1 routed the call through SM2. Make a call in the opposite direction and verify that the call is routed to SM2 on the second SIP trunk via clan2.

## 7.5 Verification Scenarios

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

- Basic calls between various telephones on the Avaya Communication Manager 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
- Alternate routing scenarios:
  - Nortel Communication Server 1000 routes to an alternate Avaya Aura Session Manager.
  - Avaya Aura Communication Manager routes to an alternate Avaya Aura Session Manager.
  - “Route-through” routing between Avaya Aura Session Managers

## 8 Conclusion

As illustrated in these Application Notes, Avaya Communication Manager can interoperate with Nortel Communication Server 1000 using SIP trunks via Avaya Session Manager. Alternate routing features can be implemented to handle network failures. 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 Communication Manager.
- 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 Communication Manager that are forwarded back to Nortel Communication Server 1000 are not supported.



## 9 Additional References

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

### Avaya Session Manager:

- [1] Avaya Aura™ Session Manager Overview, Doc ID 03-603323, available at <http://support.avaya.com>.
- [2] Installing and Administering Avaya Aura™ Session Manager, Doc ID 03-603324, available at <http://support.avaya.com>.
- [3] Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>.

### Avaya Communication Manager:

- [4] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc ID 555-245-206, May, 2009, available at <http://support.avaya.com>.
- [5] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, May 2009, available at <http://support.avaya.com>.

### Nortel Communication Server 1000:

- [6] *IP Peer Networking Installation and Configuration*, Nortel Communication Server 1000 Release 4.5, Document Number 553-3001-332, available on the Nortel Communication Server Electronic Reference Library CD.

---

**©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](mailto:interoplabnotes@list.avaya.com)