Avaya Solution & Interoperability Test Lab

Configuring SIP Trunks among Avaya Aura™ Session Manager 5.2, Avaya Aura™ Communication Manager 5.2.1, and Nortel Communication Server 1000 6.0 – Issue 1.0

Abstract

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

For the sample configuration, Avaya Aura™ Session Manager runs on an Avaya S8510 Server, Avaya Aura™ Communication Manager runs on an Avaya S8720 Server with Avaya G650 Media Gateway, and Nortel Communication Server 1000 runs on Nortel Communication Server 1000e. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura™ Communication Manager 5.2.1 and later.

1 Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura ™ Session Manager to connect Avaya Aura™ Communication Manager 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 Communication Manager, which serves as an *Access Element* within the Session Manager architecture. 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 Session Manager, using its SM-100 (Security Module) network interface. All inter-system calls are carried over these SIP trunks. 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 Session Managers by communicating with their management network interfaces. Session Manager also supports SIP telephones, but this configuration is not addressed in these application notes.[1]

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

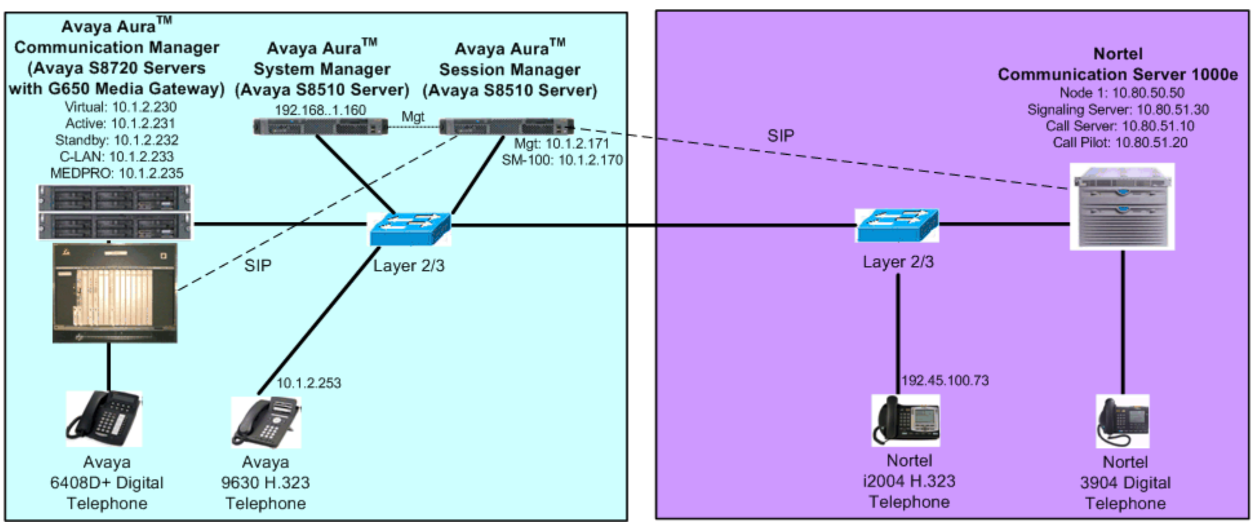


Figure 1 – Sample Configuration

Communication Manager Uniform Dial Plan (UDP) and Nortel Communication Server 1000 Coordinated Dial Plan (CDP) features are used to implement extension-extension dialing

[1] See Reference [7] for application notes on configuring Session Manager and Communication Manager as a Feature Server to support SIP telephones.

between systems. Unique extension ranges are associated with Communication Manager (3xxxx) and Nortel Communication Server 1000 (777xxxx).

These Application Notes will focus on configuration of the SIP trunks and call routing. Detailed administration of the endpoint telephones will not be described except where it affects specific feature operations, e.g., telephone name/number display (see the appropriate documentation listed in **Section 8**).

2 Equipment and Software Validated

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

Hardware Component	Software Version
Avaya S8510 Servers	Avaya Aura™ Session Manager R5.2 Load 5.2.0.0.520011 (GA)
	Avaya Aura™ System Manager R5.2 Load 5.2.0.0.520008 (GA) VSP patch 1.1.0.4.8
Avaya S8720 Servers with G650 Media Gateway	Avaya Aura™ Communication Manager 5.2.1, Load 16.4 (GA)
Avaya 9630 IP Telephone (H.323)	2.0
Avaya 6408D+ Digital Telephone	-
Nortel Communication Server 1000e	Release 600R, Version 4121
Nortel 3904 Digital Telephone	NA
Nortel I2004 H.323 Telephone	C502B41

3 Configure Avaya Aura™ Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Avaya Aura™ Communication Manager license
- Configure system parameters features
- Configure IP node names
- Configure IP interface for C-LAN
- Configure IP codec set and network region
- Configure SIP signaling group and trunk group
- Configure route pattern
- Configure location and public unknown numbering
- Configure uniform dial plan and AAR analysis
- Save Translations

Some administration screens have been abbreviated for clarity.

3.1 Verify Avaya Aura™ Communication Manager License

Log in to the System Access Terminal (SAT) to verify that the 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   57
```

3.2 Configure System Parameters Features

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

```
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
                                  AAR/ARS Dial Tone Required? y
```

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 Session Manager. In this case, "clan1" and "10.1.2.233" are entered as **Name** and **IP Address** for the C-LAN, "asm" and "10.1.2.170" are entered for the Session Manager Security Module (SM-100) interface, and "Gateway001" and "10.1.2.1" are entered for the default gateway. Note that "Gateway001" will be used in the form used to configure the IP interface for the C-LAN (see **Section 3.4**). The actual node names and IP addresses may vary. Submit these changes.

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

3.4 Configure IP Interface for C-LAN

Add the C-LAN to the system configuration using the "add ip-interface 1a02" command. The actual slot number may vary. In this case, "1a02" 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.

```
change 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: 1
         Network uses 1's for Broadcast Addresses? y
```

3.5 Configure IP Codec Set and Network Region

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 has 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        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  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 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 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 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:** "clan1" C-LAN node name from **Section 3.3**.
- **Far-end Node Name:** "asm" Session Manager node name from **Section 3.3**.
- **Near-end Listen Port:** "5061"
- **Far-end Listen Port:** "5061"
- **Far-end Network Region:** Network region number "1" from **Section 3.5**.
- **Far-end Domain:** "avaya.com" SIP domain name from **Section 4.1**.

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

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"
- **Signaling Group** The signaling group number defined in the previous section
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total trunks configure in **Section 3.1**).

```
add trunk-group 32                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 32                   Group Type: sip          CDR Reports: y
  Group Name: To ASM                      COR: 1        TN: 1        TAC: 132
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                     Signaling Group: 32
                                                   Number of Members: 4
```

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

```
add trunk-group 32                                                Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

3.7 Configure Route Pattern

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

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

```
change route-pattern 32                                         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. In this way, calls to non-numeric users or unknown domains will still be routed to 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
                                                     Total Administered: 2
 5  3                                       5           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 777xxxx 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 777xxxx. 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 "777".
- **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                          Insert              Node
  Pattern        Len Del            Digits     Net Conv Num
  777            7   0                        aar   n
```

Use the "change aar analysis 0" command, and add an entry to specify how to route the calls to 777xxxx. 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 digts.
- **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
                                   Location:  all          Percent Full:    1

          Dialed           Total     Route     Call   Node   ANI
          String          Min  Max  Pattern    Type   Num    Reqd
          777             7    7     32        aar           n
```

3.10 Save Translations

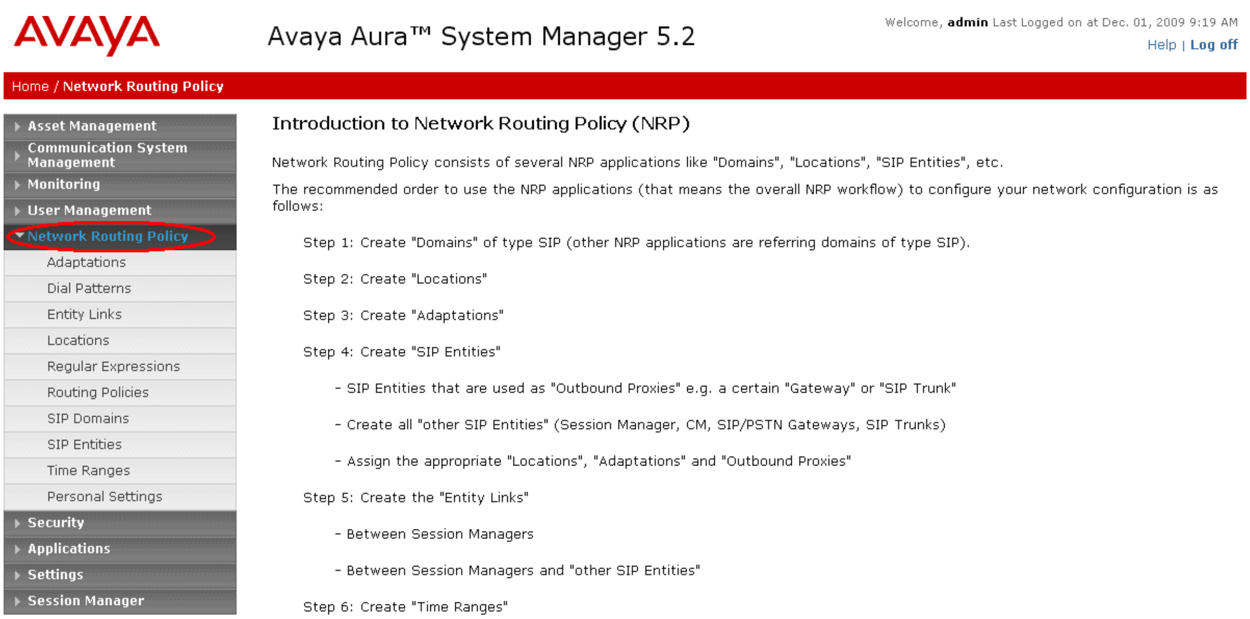
Configuration of Communication Manager is complete. Use the save Translations command to save these changes.

4 Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring 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 Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- 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 Session Manager Server to be managed by System Manager.
- Local host name resolution entries corresponding to fully qualified domain names (FQDN's) referenced in the previous steps.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "http://<ip-address>/SMGR", where "<ip-address>" is the IP address of 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 two of the above items (**Sections 4.1** through **4.6**).

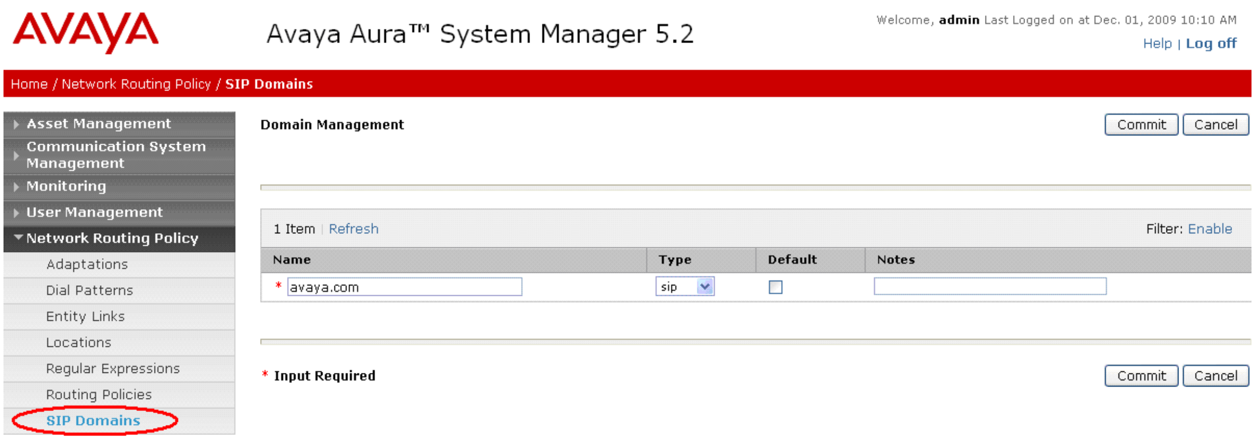


4.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **SIP Domains** on the left and click the **New** button (not shown) on the right. Fill in the following:

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

Click **Commit**.



4.2 Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. Under *General*, enter:

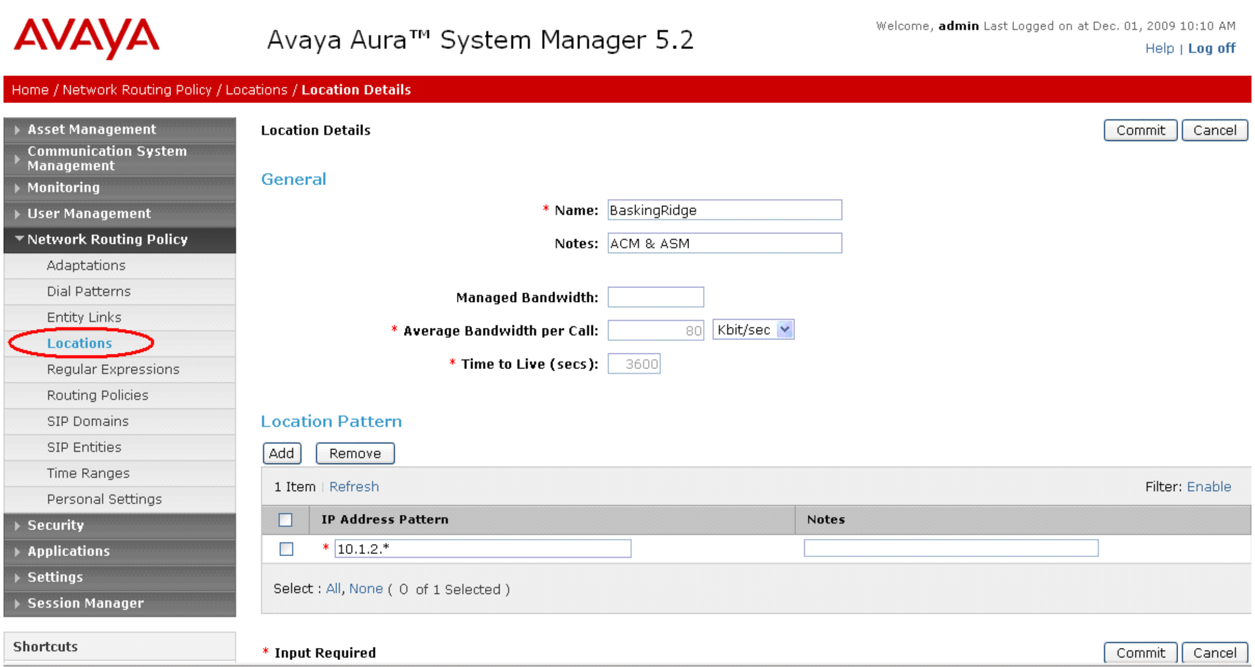
- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

The remaining fields under *General* can be filled in to specify bandwidth management parameters between 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.

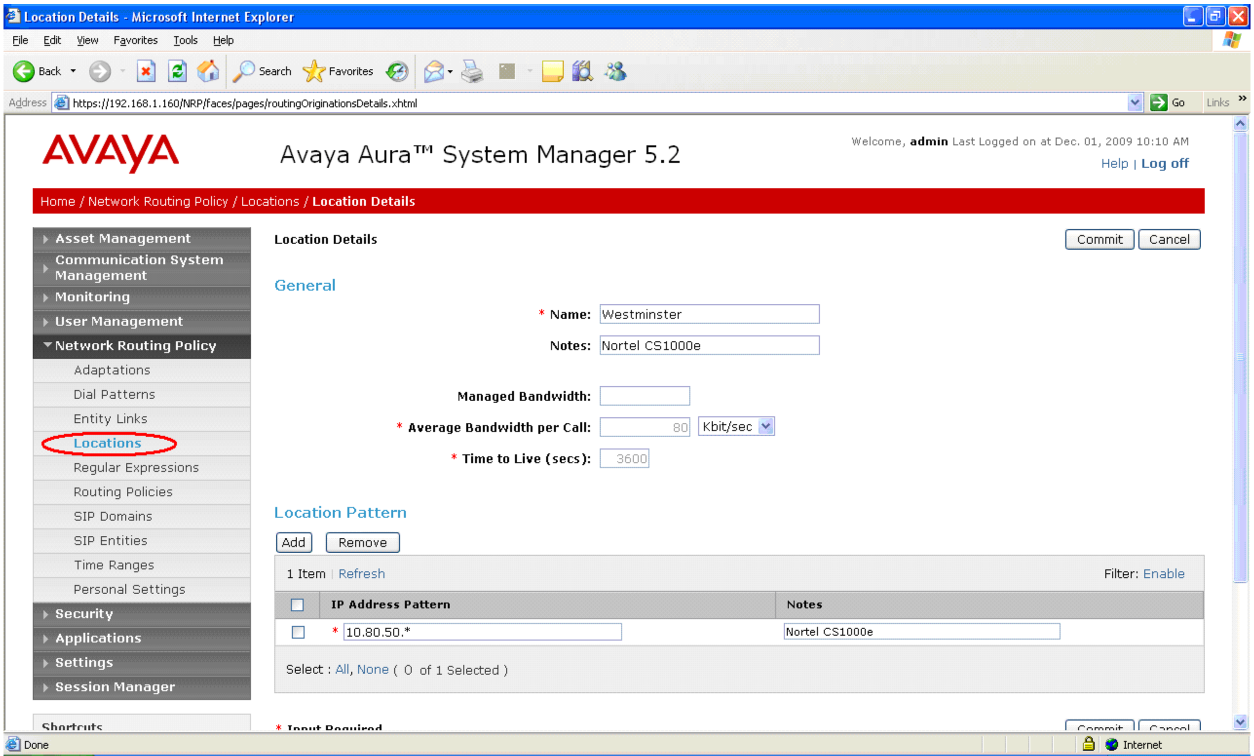
Under *Location Pattern*:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows addition of the Basking Ridge location, which includes Communication Manager and Session Manager in the 10.1.2 subnet. Click **Commit** to save the Location definition.



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



The fields under *General* can be filled in to specify bandwidth management parameters between Session Manager and this location. These were not used in the sample configuration, and reflect default values. Note also that although not implemented in the sample configuration, routing policies can be defined based on location.

4.3 Add SIP Entities

A SIP Entity must be added for Avaya Aura™ Session Manager and for each SIP telephony system supported by it using SIP trunks: the C-LAN board in the Avaya G650 Media Gateway, and the Nortel Communication Server 1000. Select **SIP Entities** on the left and click on the **New** button (not shown) on the right. Under *General*, fill in:

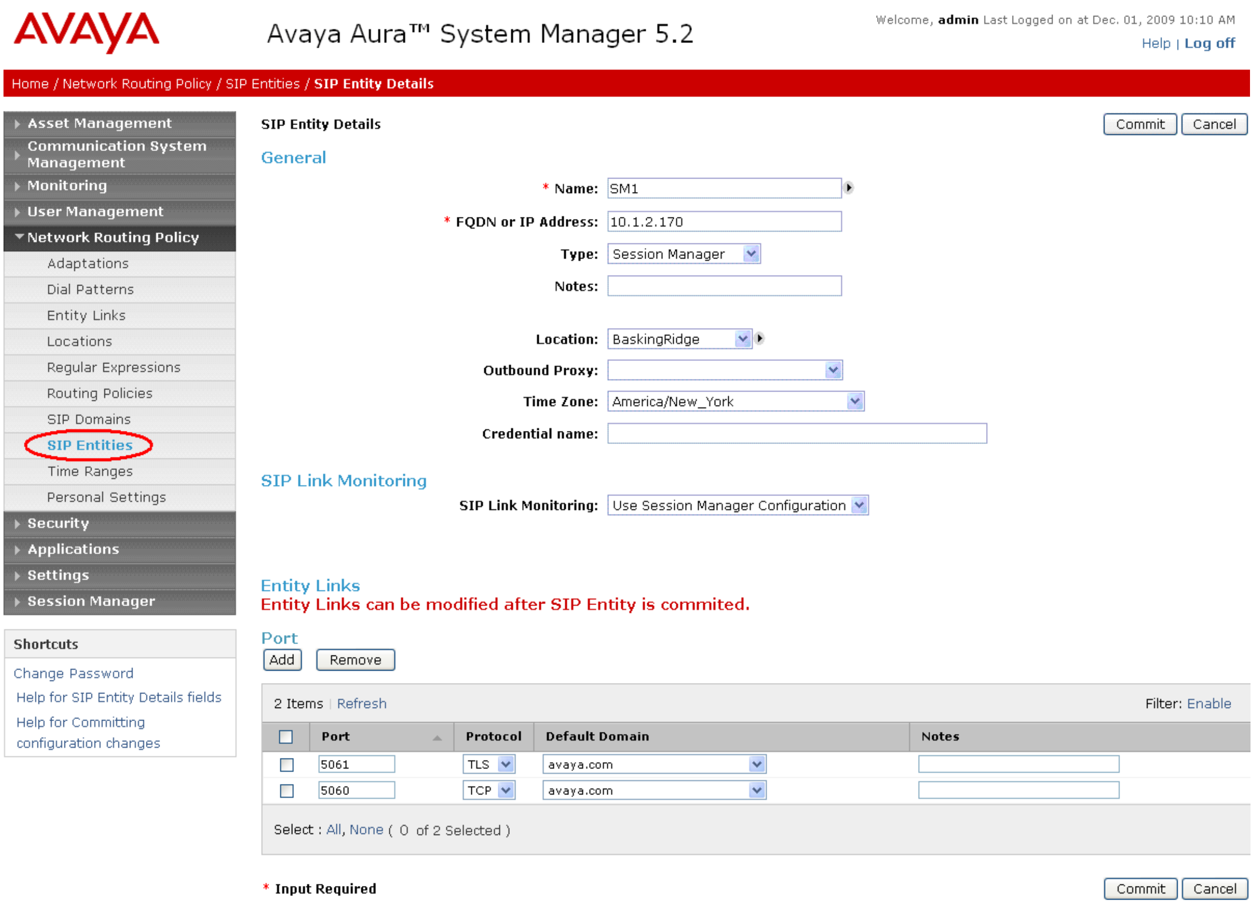
- **Name:** A descriptive name.
- **FQDN or IP Address:** FQDN or IP address of the Session Manager or the signaling interface on the telephony system.
- **Type:** "Session Manager" for Session Manager, **"**CM" for Communication Manager**,** "Other" for the Nortel Communication Server 1000.
- **Location:** 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:

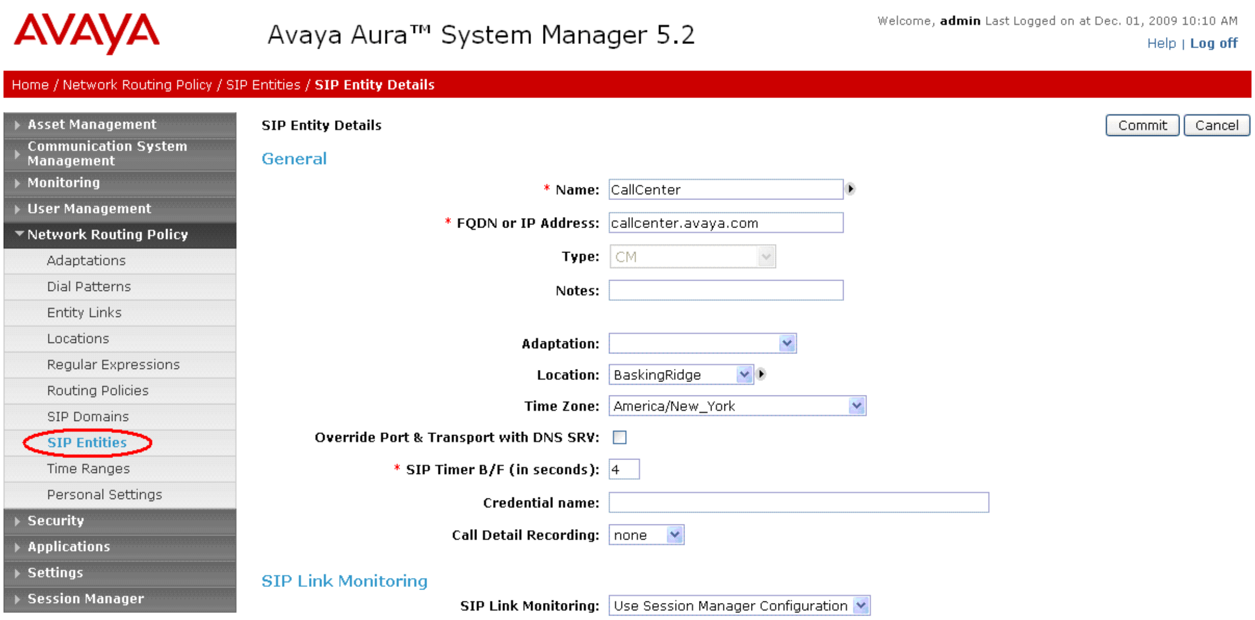
- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise (e.g., "avaya.com").

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

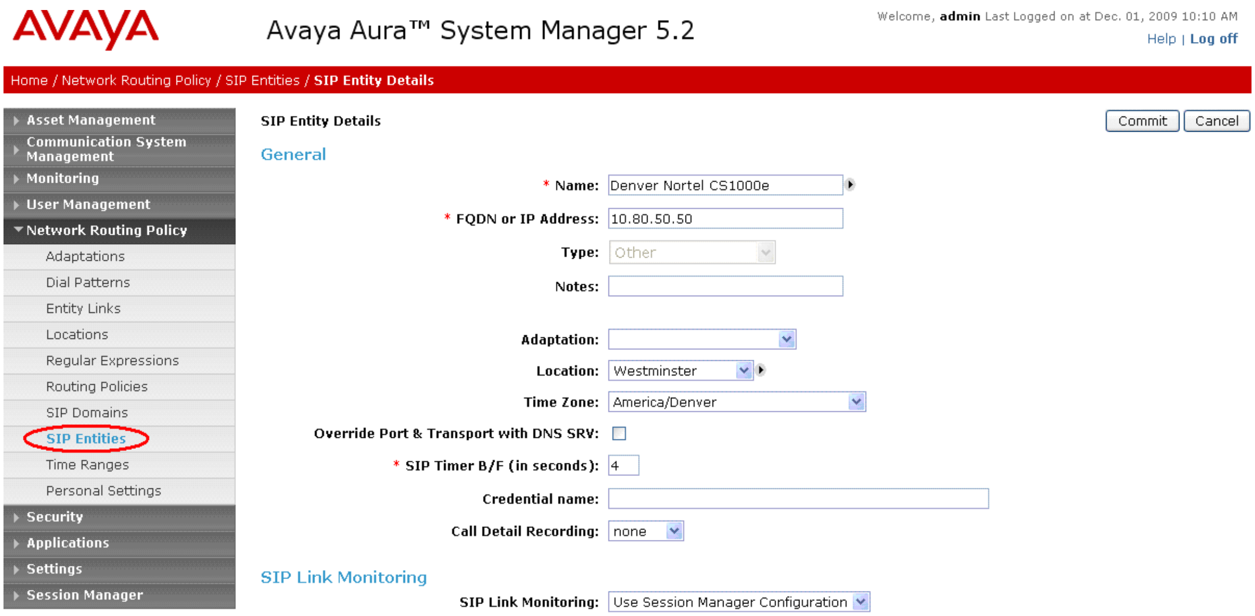
The following screen shows addition of Session Manager. The IP address of the SM-100 Security Module is entered for **FQDN or IP Address**. Two *Port* entries are added. TCP port 5060 is used for communicating with the Nortel Communication Server 1000, and TLS port 5061 is used for communication with Communication Manager.



The following screen shows the results of adding Communication Manager. In this case, **FQDN or IP Address** is the Fully Qualified Domain Name (FQDN) of the C-LAN board in the Avaya G650 Media gateway. Note that although not shown in the sample configuration, definition of multiple IP addresses (e.g., C-LANs) for the same FQDN (see **Section 4.8**) will cause Session Manager to load balance call traffic among those addresses.



The following screen shows addition of Nortel Communication Server 1000. The IP address used is that of the "Voice LAN (TLAN) Node IP address" (See **Figure 2** in **Section 5.2**).

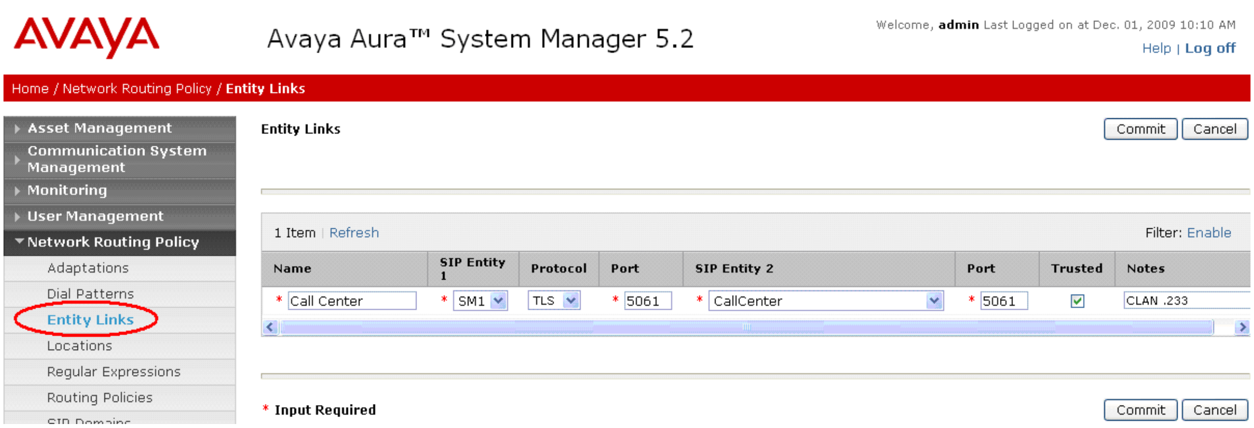


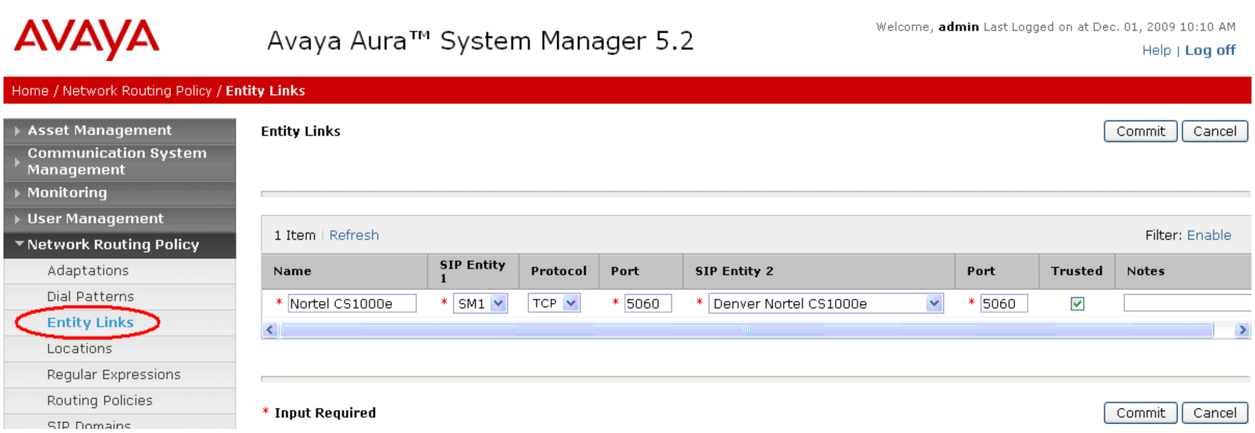
4.4 Add Entity Links

A SIP trunk between 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 (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the 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 Entity Links for Communication Manager and the Nortel Communication Server 1000.





4.5 Add Routing Policies

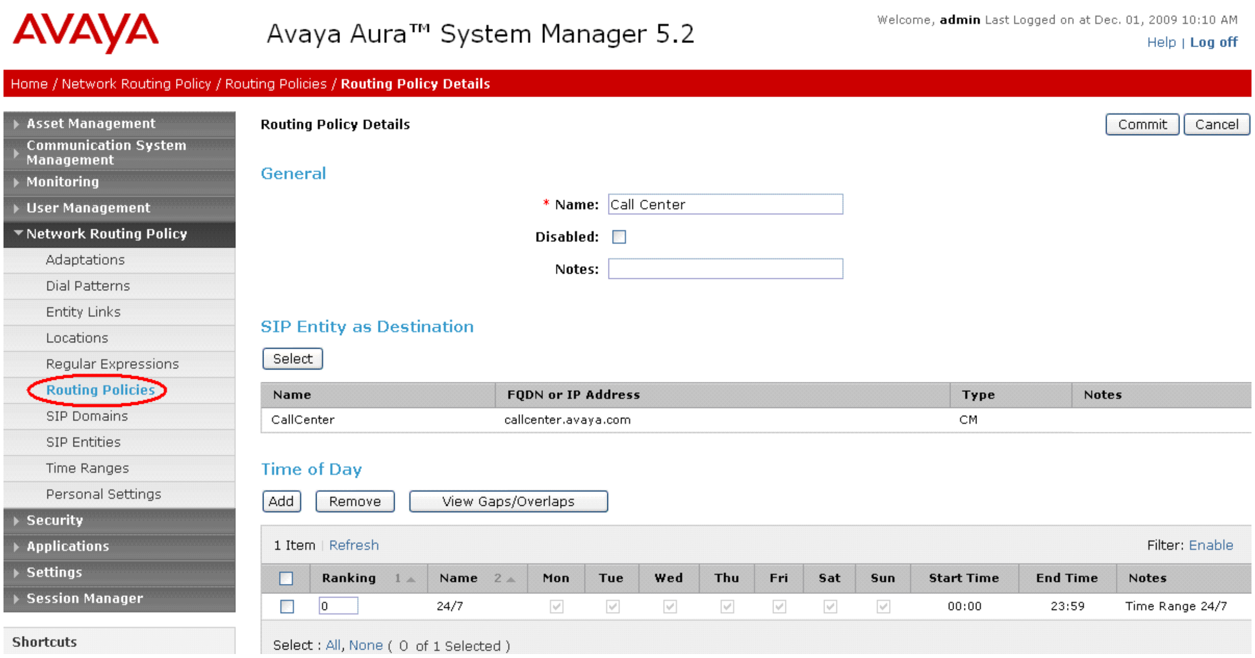
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 4.3**. Two routing policies must be added for Communication Manager and the Nortel Communication Server 1000. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

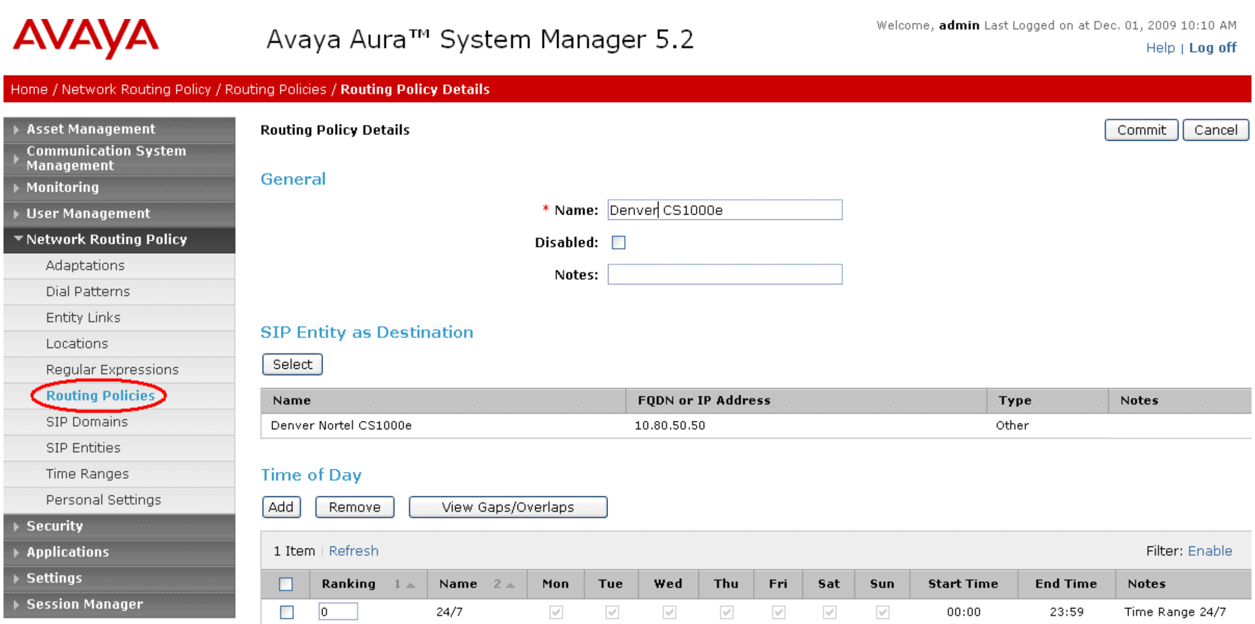
Under *General*:
Enter a descriptive name in **Name**.

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 default “24/7” time range.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screens show the Routing Policies for Communication Manager and the Nortel Communication Server 1000.





4.6 Add Dial Patterns

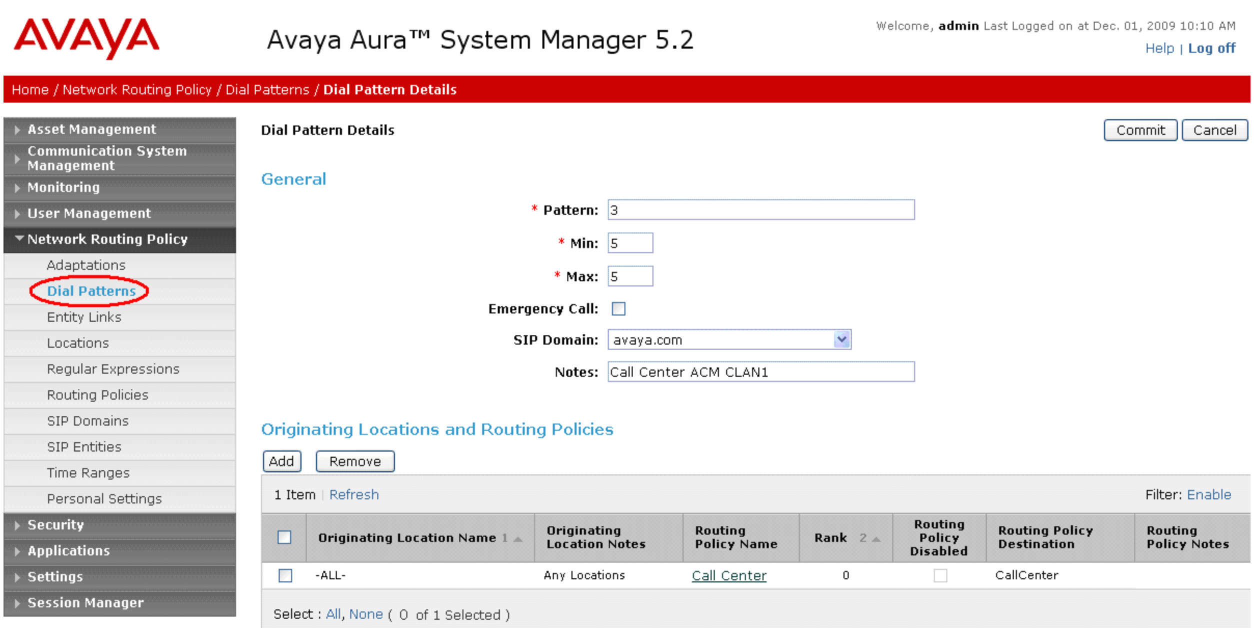
Define dial patterns to direct calls to the appropriate SIP Entity. Calls to 5-digit extensions beginning with "3" should be routed to Communication Manager. Calls to 7-digit extensions beginning with "777" should be routed to the Nortel Communication Server 1000. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under *General*:

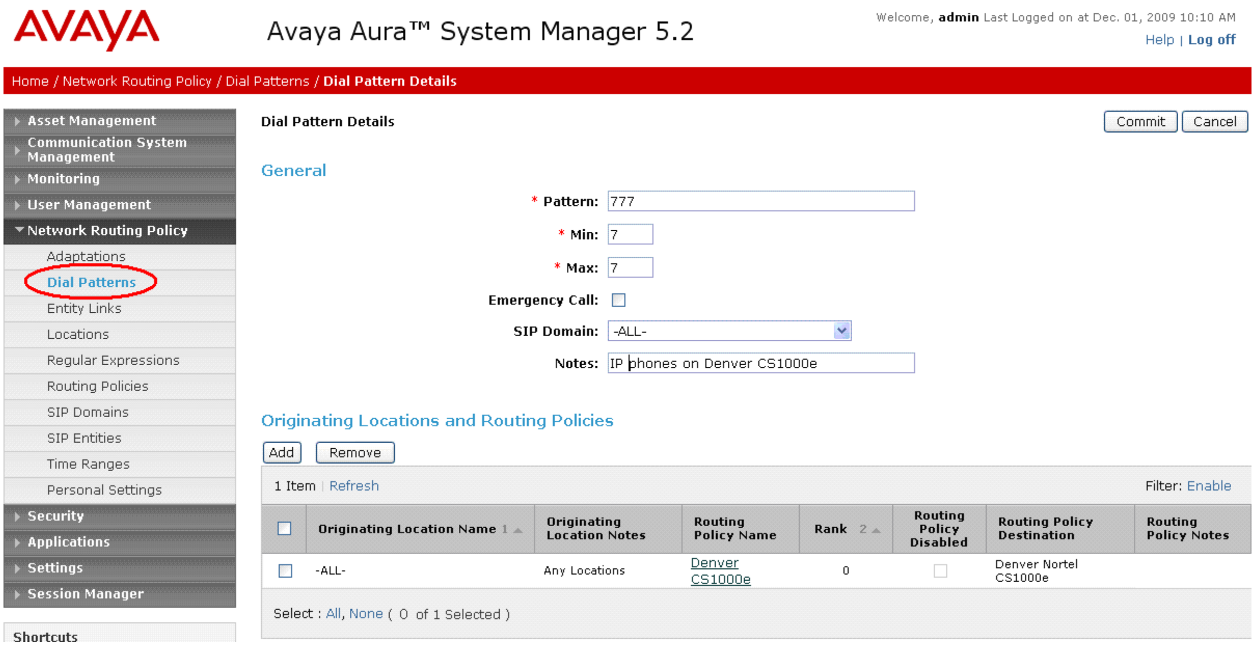
- **Pattern:** Dialed number or prefix.
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **SIP Domain:** SIP domain specified in **Section 4.1**
- **Notes:** Comment on purpose of dial pattern.

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

Default values can be used for the remaining fields. Click **Commit** to save each dial pattern. The following screens show the resulting two dial pattern definitions.



The following screenshot shows the dial pattern for Nortel Communication Server 1000.



4.7 Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

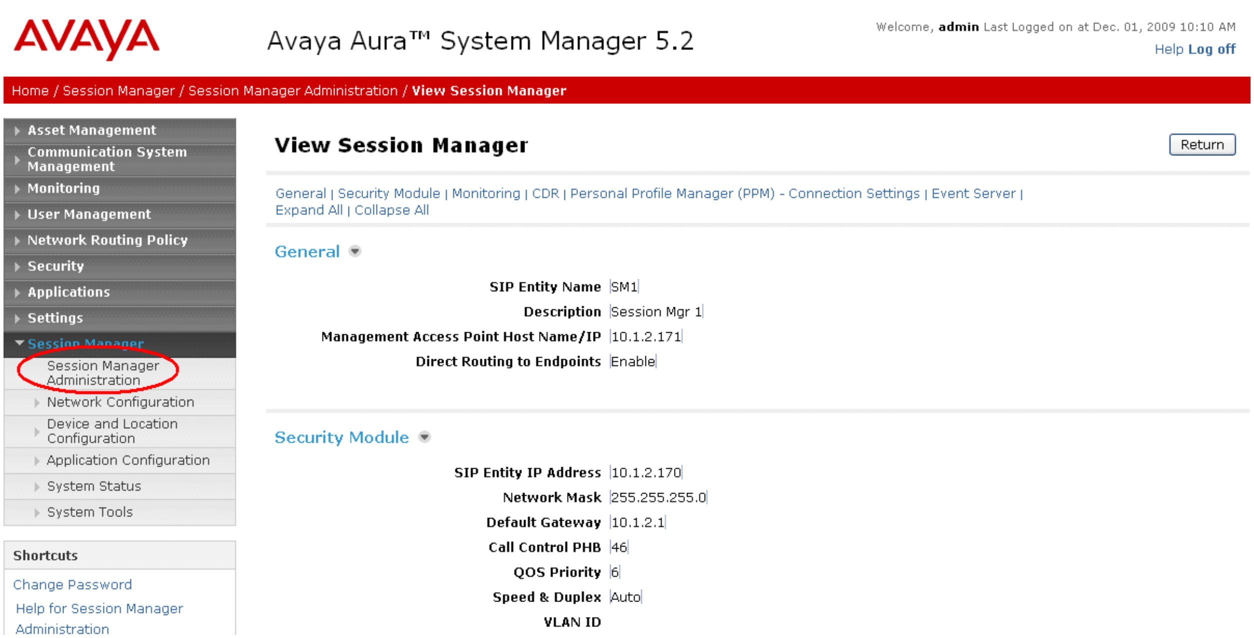
Under *General*:

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

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the resulting Session Manager definition.

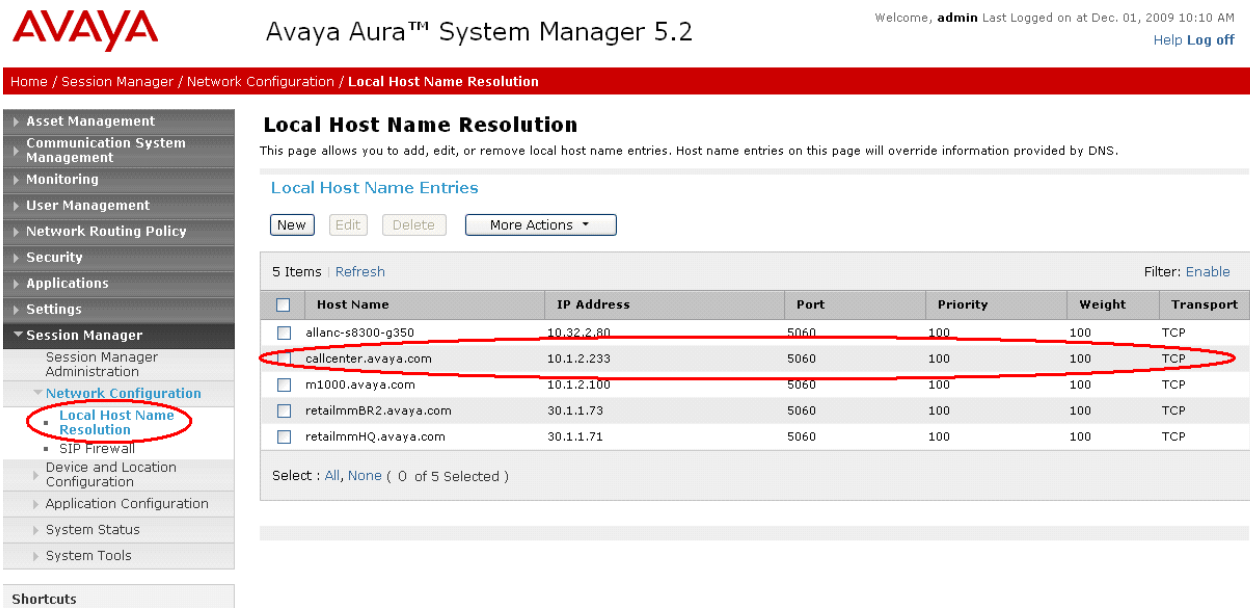


4.8 Define Local Host Names

The host name (FQDN) used for Communication Manager in **Section 4.3** must be defined. To do so, Select **Session Manager → Network Configuration → Local Host Name Resolution** on the left. Click **New** and enter the following:

- **Host Name:** The FQDN used for the host
- **IP Address**: IP address of the host's network interface
- **Port:** Port number to which SIP requests are sent
- **Transport:** Transport to be used for SIP requests

Defaults can be used for the remaining fields. The **Priority** and **Weight** fields are used when multiple IP addresses are defined for the same host. The following screen shows the host name resolution entry used in the sample configuration (circled).



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 a 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 and Call Server co-resident on the same CS1000e 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.

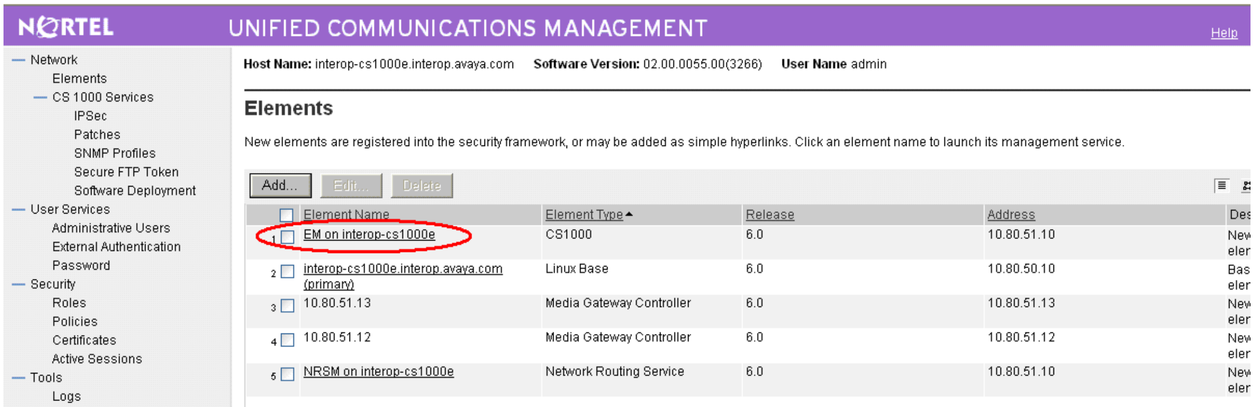
Furthermore, these Application Notes used the Coordinated Dial Plan (CDP) feature to route calls from the Nortel Communication Server 1000, over the SIP trunks to Session Manager to reach endpoints on Communication Manager. The CDP feature is assumed to be already enabled on Nortel Communication Server 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 Unified Communications Manager
- Obtain node and IP addresses
- Configure ISDN
- Configure D-Channel
- Configure zones
- Configure virtual SIP routes and trunks
- Configure route list block and distant steering code
- Configure node SIP parameters
- Launch NRS Manager
- Configure service domain
- Configure SIP gateway endpoints
- Configure routing entries
- Cut over and commit changes

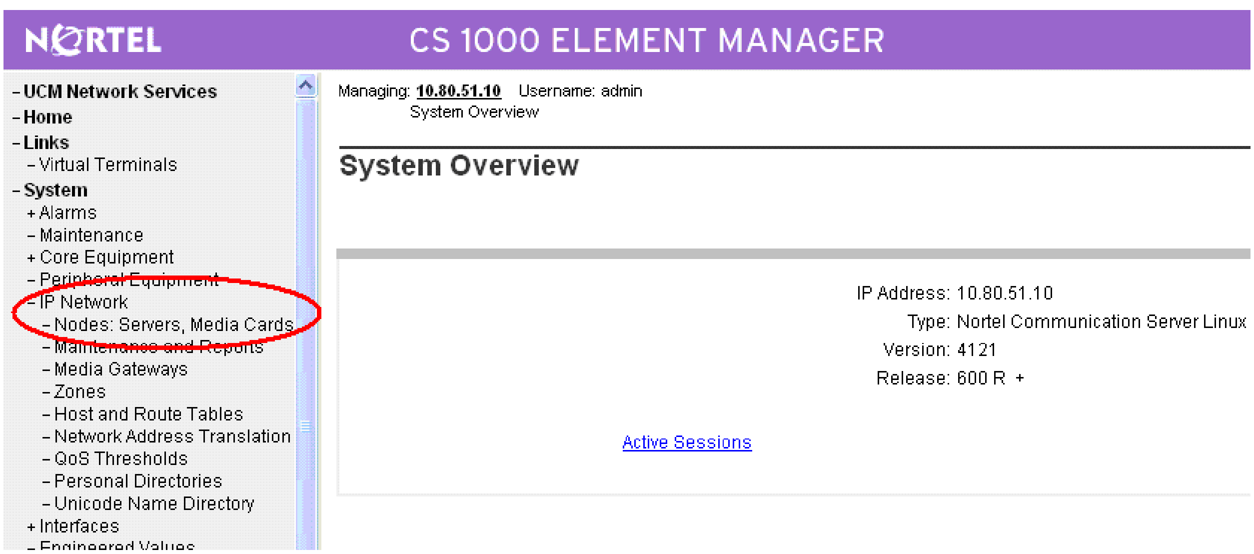
5.1 Launch Unified Communications Manager

Access the Nortel Communication Server 1000 web based interface by using the URL “http://<ip-address>” in an Internet browser window, where “<ip-address>” is the IP address of the Call Server. Note that the IP address for the Call Server may vary, and in this case “10.80.51.10” is used. Log in with the appropriate user name and password. The following Unified Communications Management screen will be displayed. Click on the **Element Name** corresponding to the element of type *CS1000*.

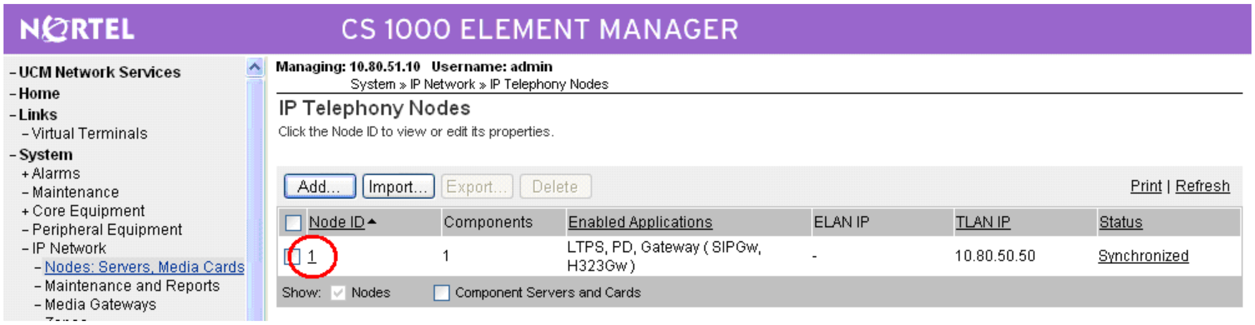


5.2 Obtain Node and IP Addresses

The Element Manager System Overview screen is displayed. Expand the **IP Network** menu on the left pane and select **Nodes: Servers, Media Cards**.



The Node Configuration screen is displayed. Click **Node ID** *1* to expand it. Note that the node number and IP address may vary.



The Node Details screen is updated with additional details as shown below. Make a note of the **Node IP Address** "10.80.50.50", and Signaling Server **TLAN IP** address of "10.80.50.10". These values are used to configure other sections.

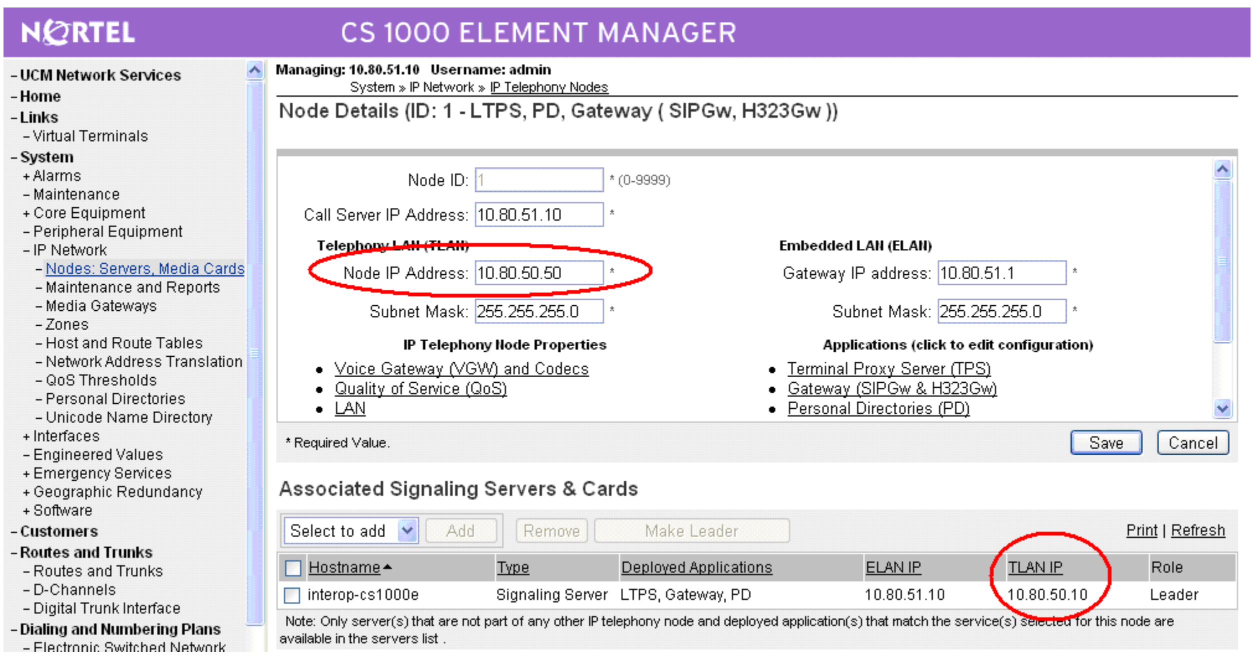
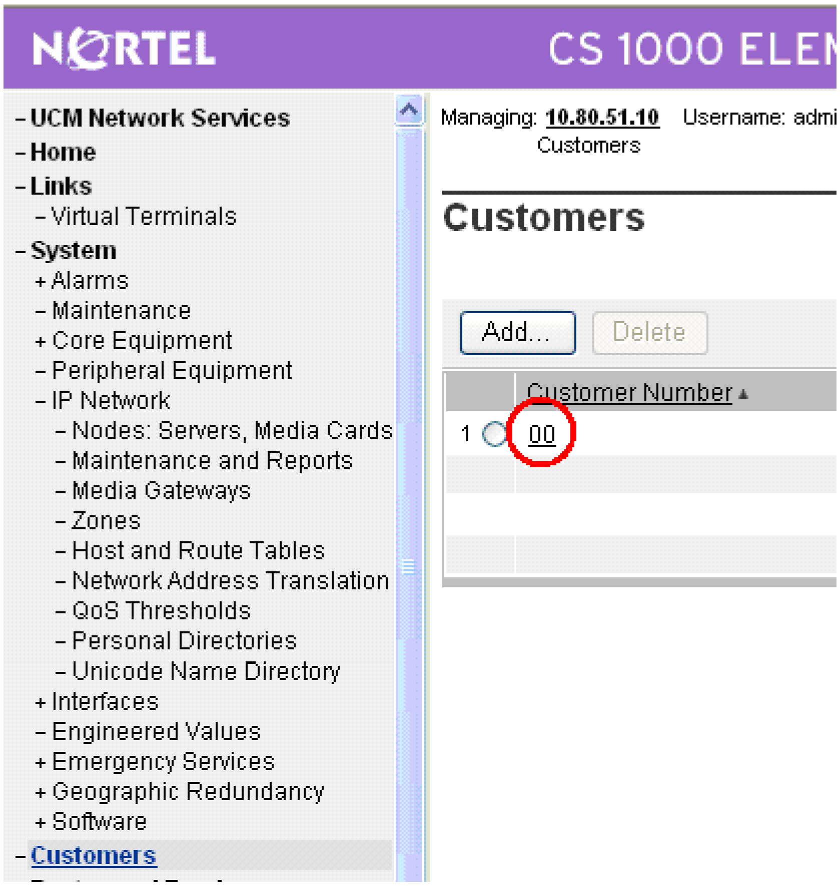


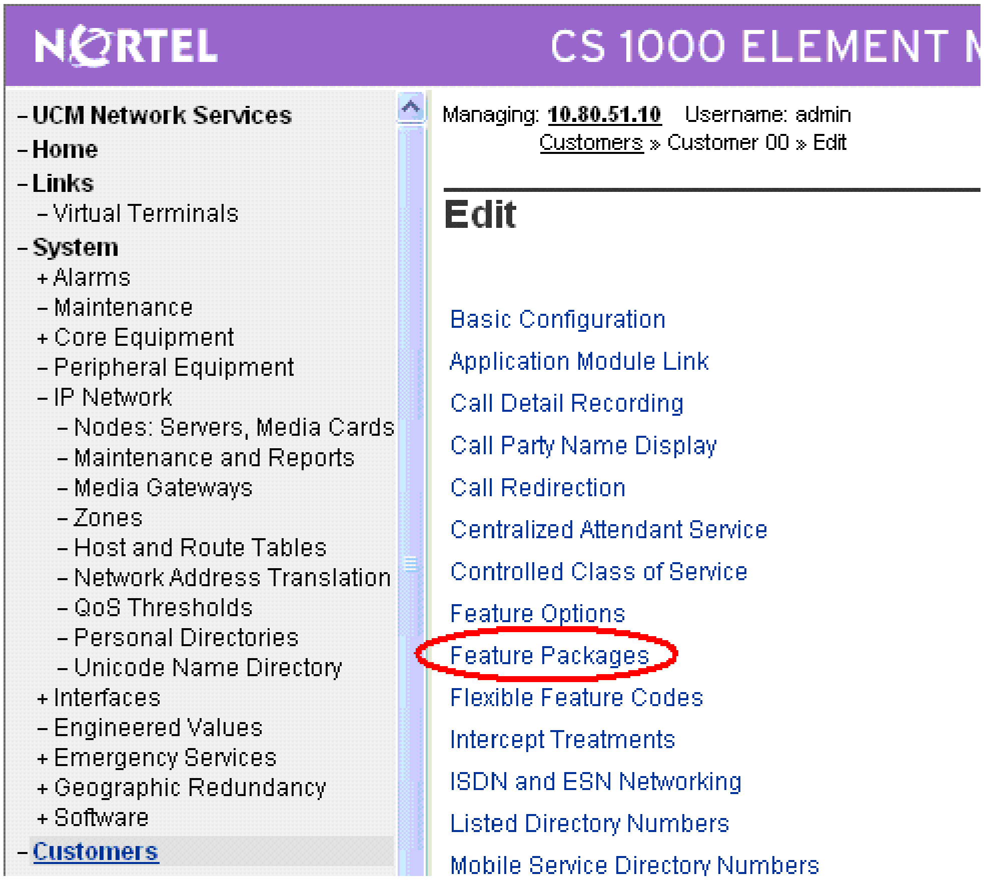
Figure 2: Node Configuration

5.3 Configure ISDN

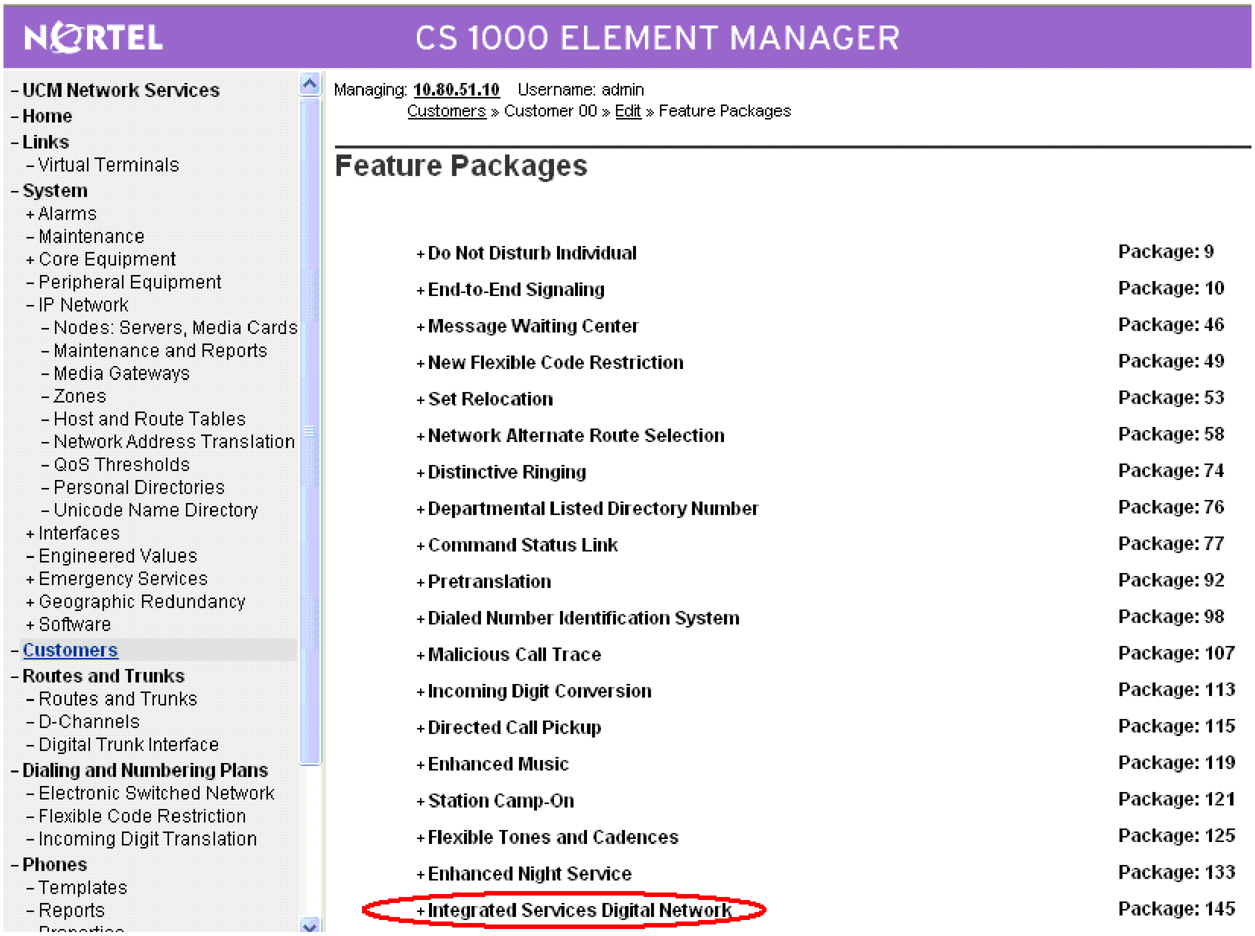
Select **Customers** in the left pane. The **Customers** screen is displayed. Click the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options. In the sample configuration, only one customer was configured on the system.



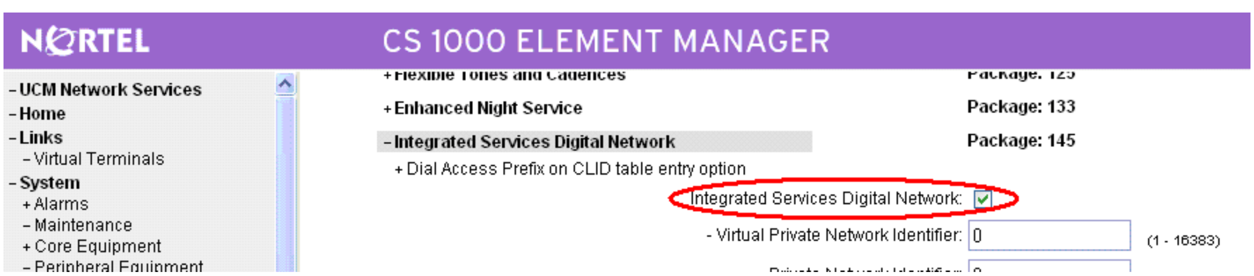
The Customer 00 Property Configuration screen is displayed next. Select **Feature Packages**.



The screen is updated with a listing of feature packages populated below **Feature Packages** (not all features shown below). Select **Integrated Services Digital Network** to edit its parameters.

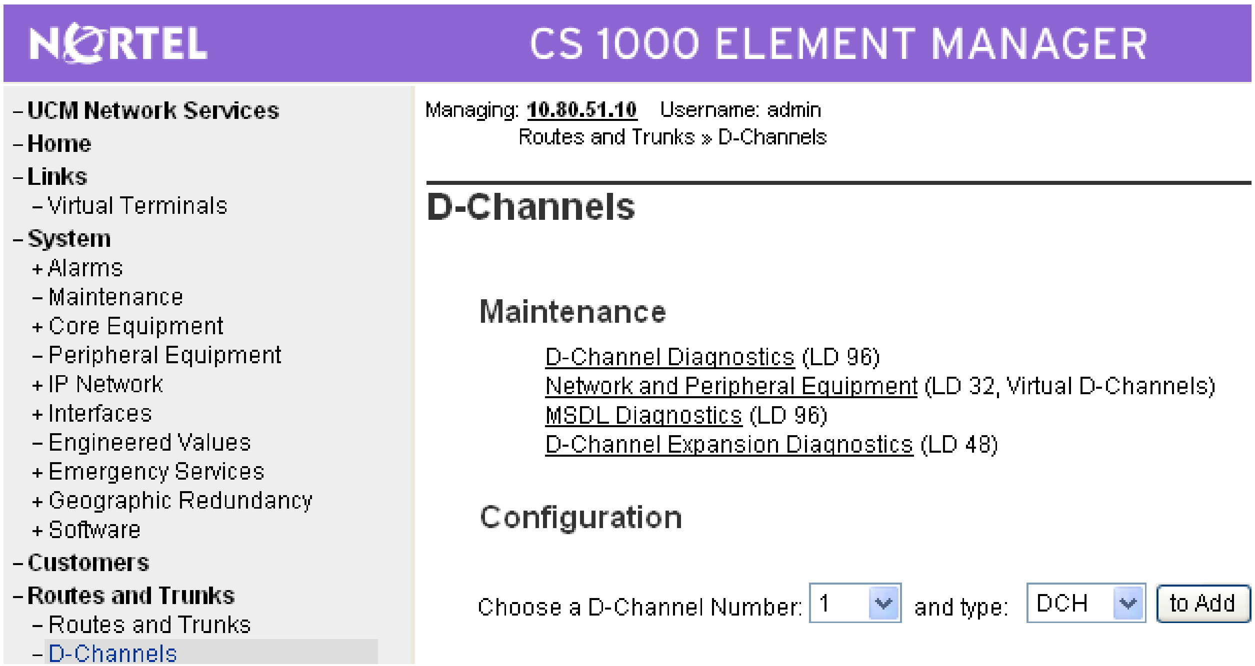


The screen is updated with parameters populated below **Integrated Services Digital Network**. Check the **Integrated Services Digital Network (ISDN)** checkbox, and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click **Save** (not shown).



5.4 Configure D-Channel

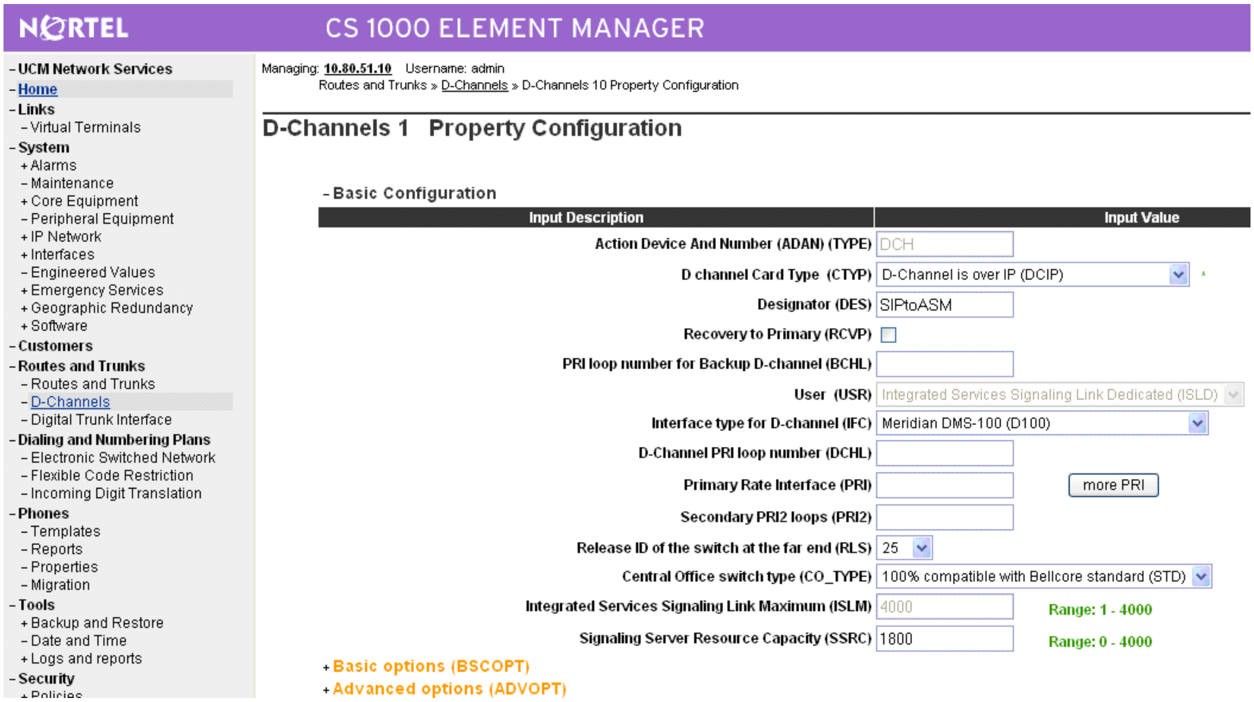
Select **Routes and Trunks → D-Channels** from the left pane to display the D-Channels screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list (in this case "1"). Click **to Add**.



The D-Channels 1 Property Configuration screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

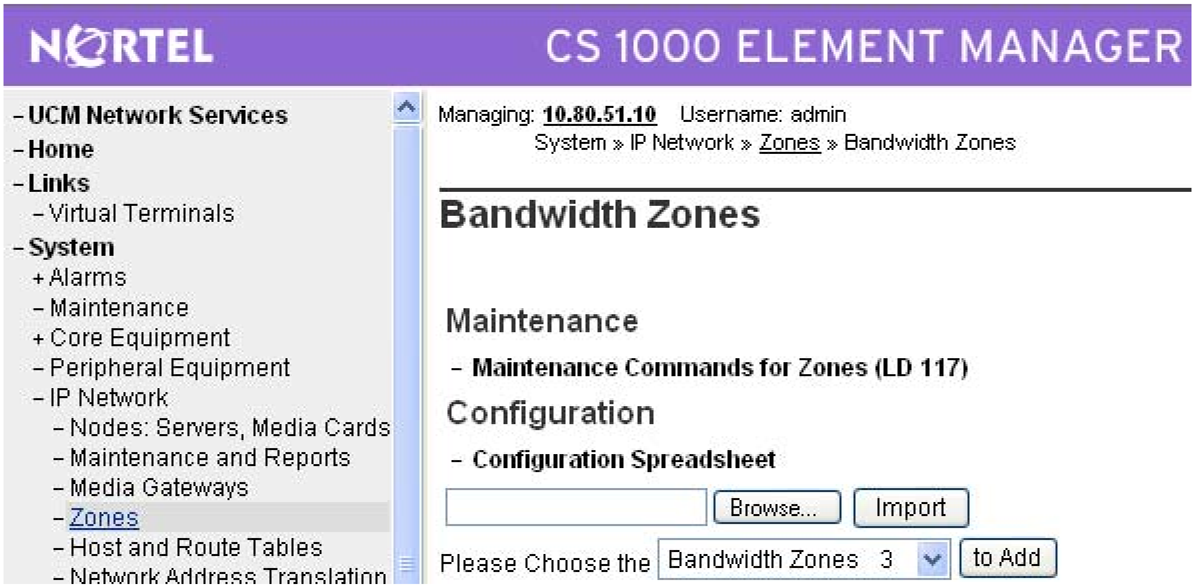
- **D channel Card Type (CTYP):** "D-Channel is over IP (DCIP)"
- **Designator (DES):** A descriptive name.

Click **Submit**.

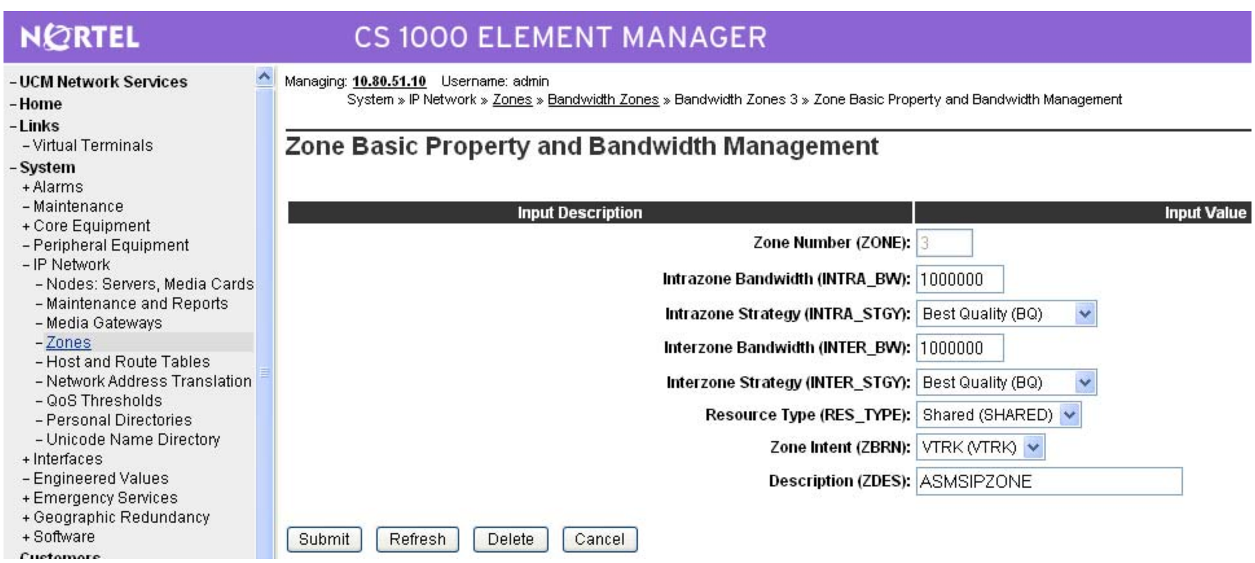


5.5 Configure Zones

Select **IP Network → Zones** from the left pane to display the Zones screen, and then select **Bandwidth Zones** (not shown). For the **Please Choose the** field, select an available zone number from the drop-down list (in this case "3"). Click **to Add**.

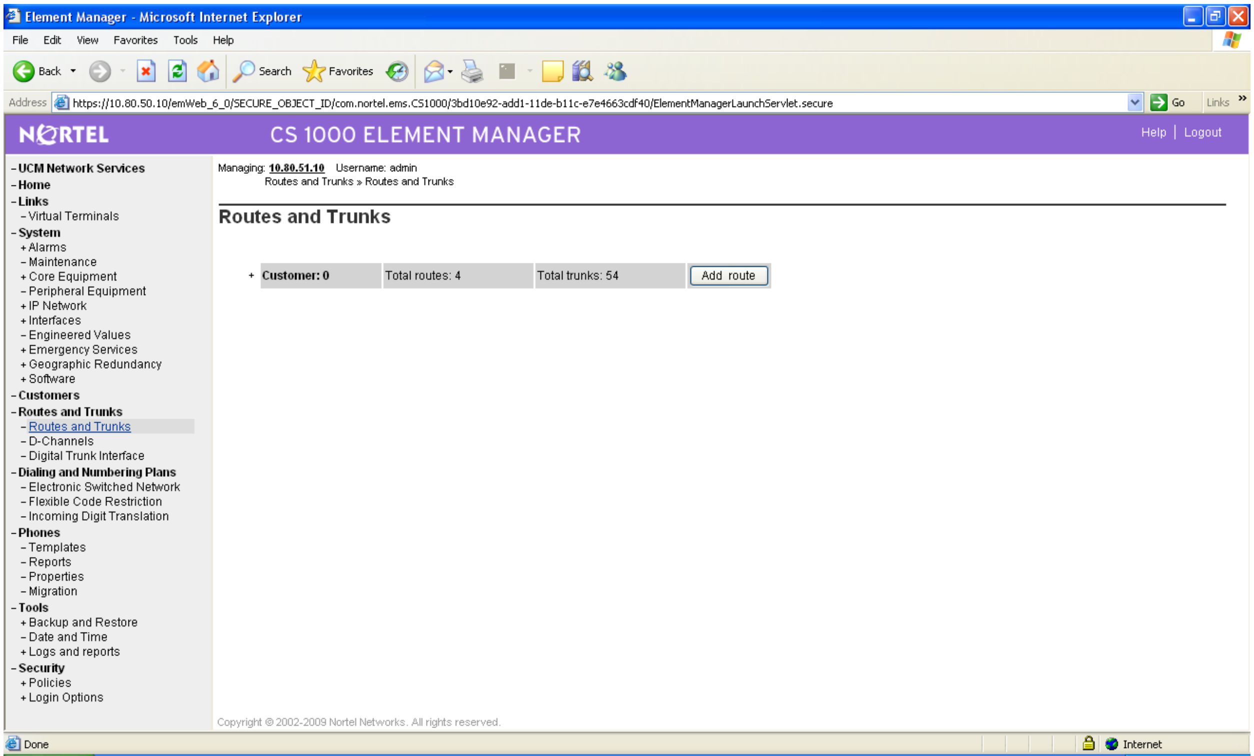


The Zone Basic Property and Bandwidth Management screen is displayed next. For the **Zone Intent (ZBRN)** field, select "VTRK (VTRK)" from the drop-down list. For the Description (ZDES) field, enter descriptive text. Retain the default values for all remaining fields, and click **Submit.**



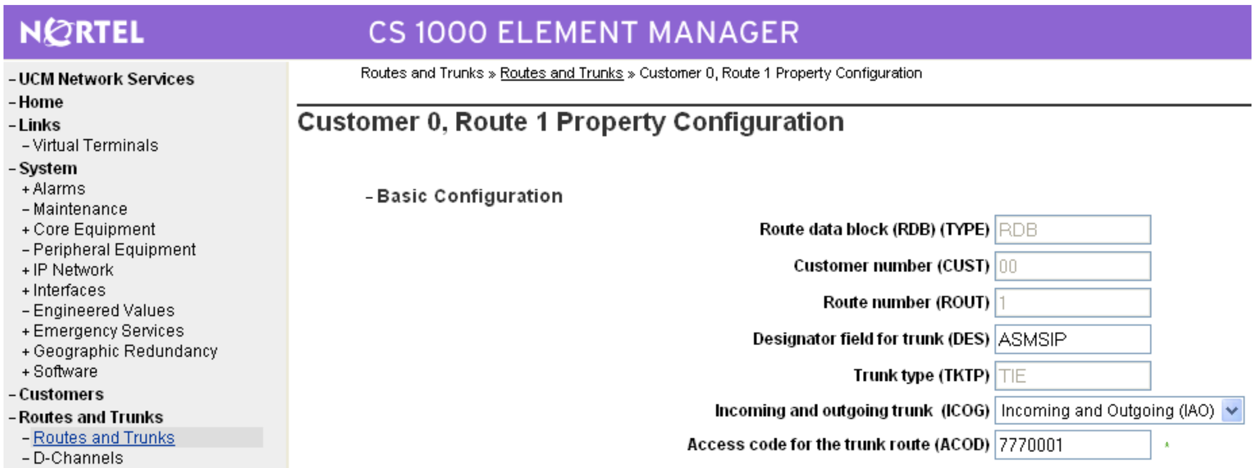
5.6 Configure Virtual SIP Routes and Trunks

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**.

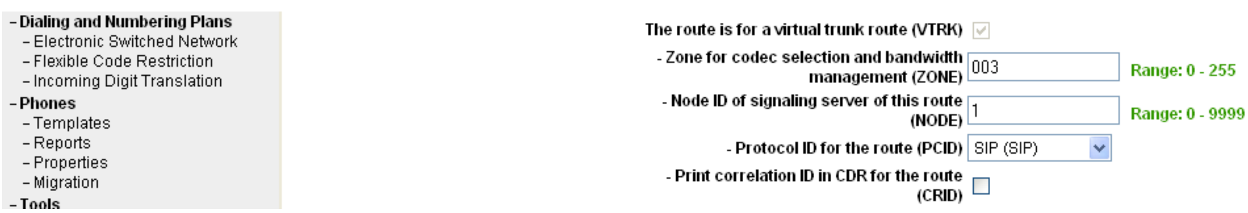


The Customer 0, Route 1 Property Configuration screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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.

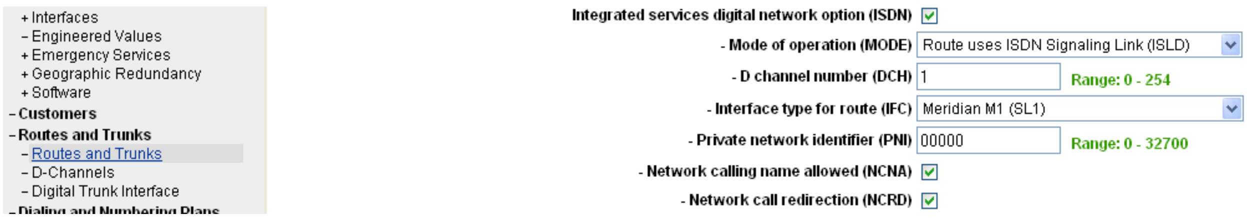


Scroll down the screen, and check the field **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear. For the **Zone for codec selection and bandwidth management (ZONE)** field, enter the zone number from **Section 5.5**. For the **Node ID of signaling server of this 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.

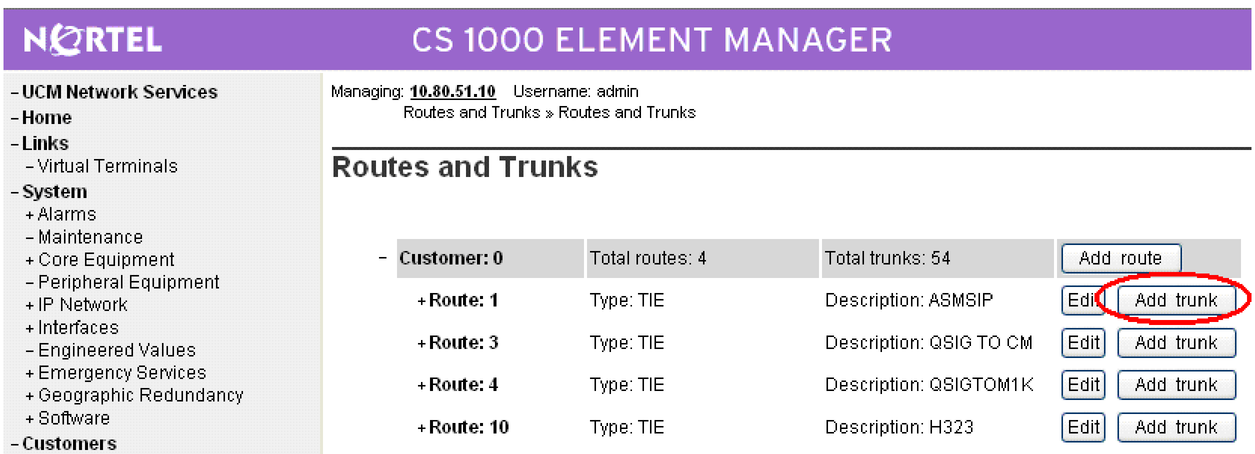


Scroll down the screen, check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click **Submit**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

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

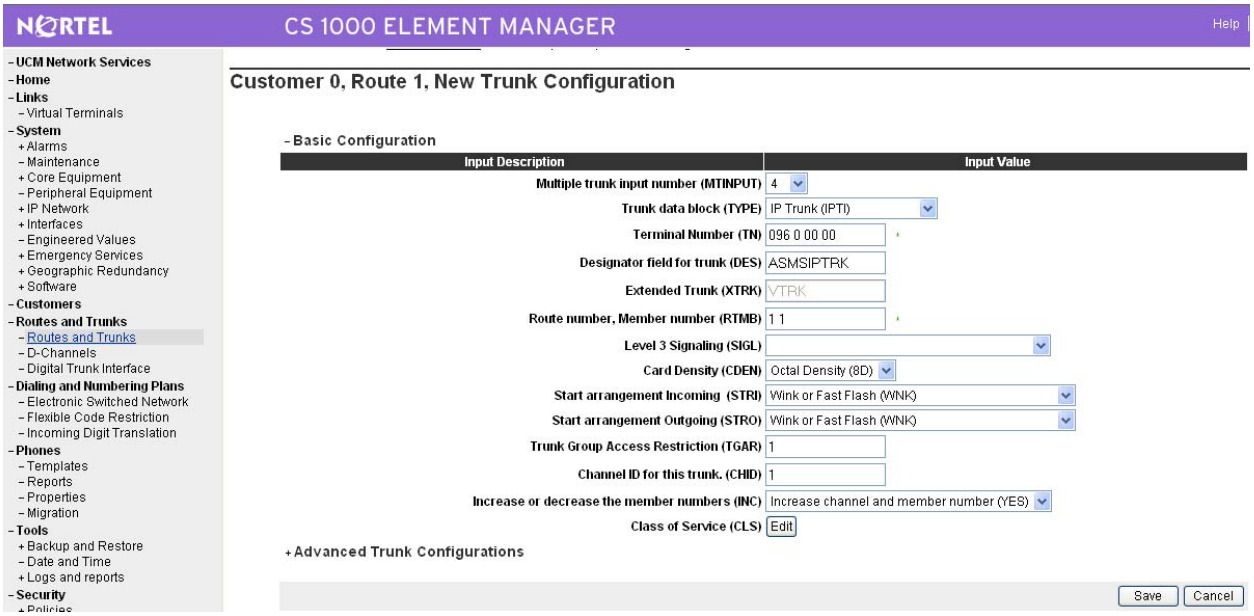


The **Routes and Trunks** screen is displayed again, and updated with the newly added route. Click the **Add trunk** button next to the newly added route.



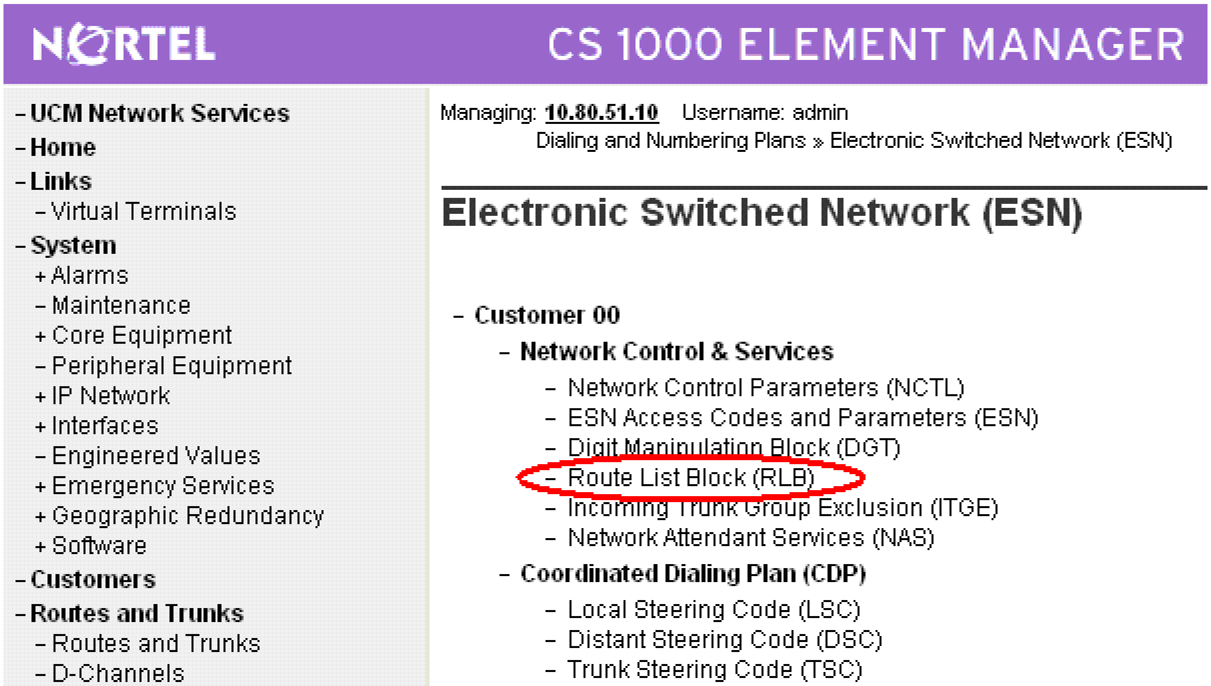
The Customer 0, Route 1, New Trunk Configuration screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click **Save**. The **Multiple trunk input number (MTINPUT)** field may be used 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 Communication Manager 5.2.1 to Nortel in **Section 3.7**. In the sample configuration, four trunks were created.

- **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)"
- **Card Density** Select Octal Density (8D)
- **Trunk Group Access Restriction (TGAR):** Desired trunk group access restriction level.
- **Channel ID for this trunk (CHID):** An available starting channel ID.



5.7 Configure Route List Block and Distant Steering Code

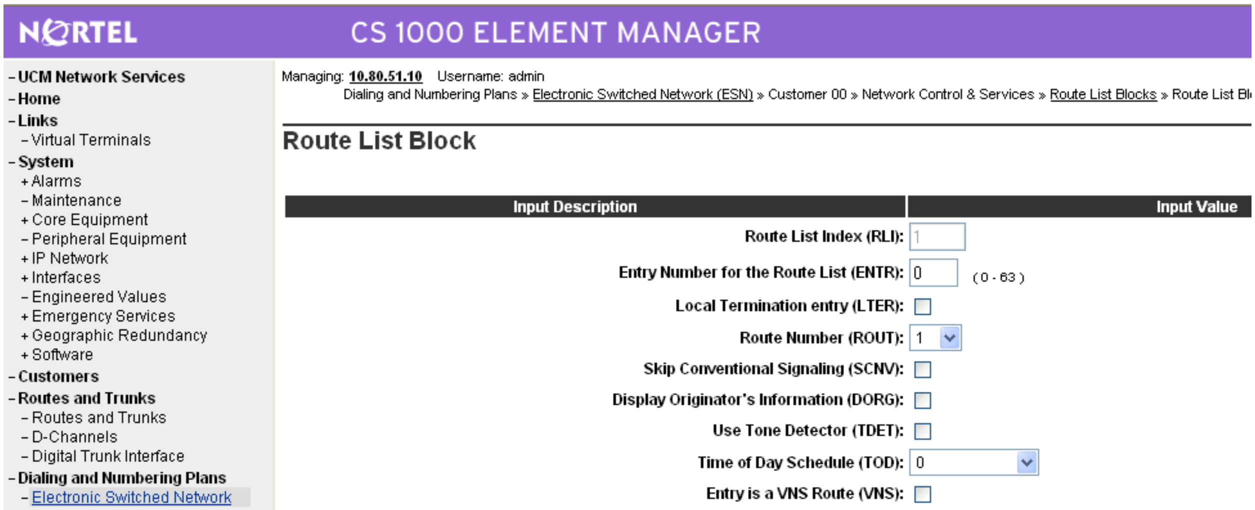
Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the Electronic Switched Network (ESN) screen. Select **Route List Block (RLB)**.



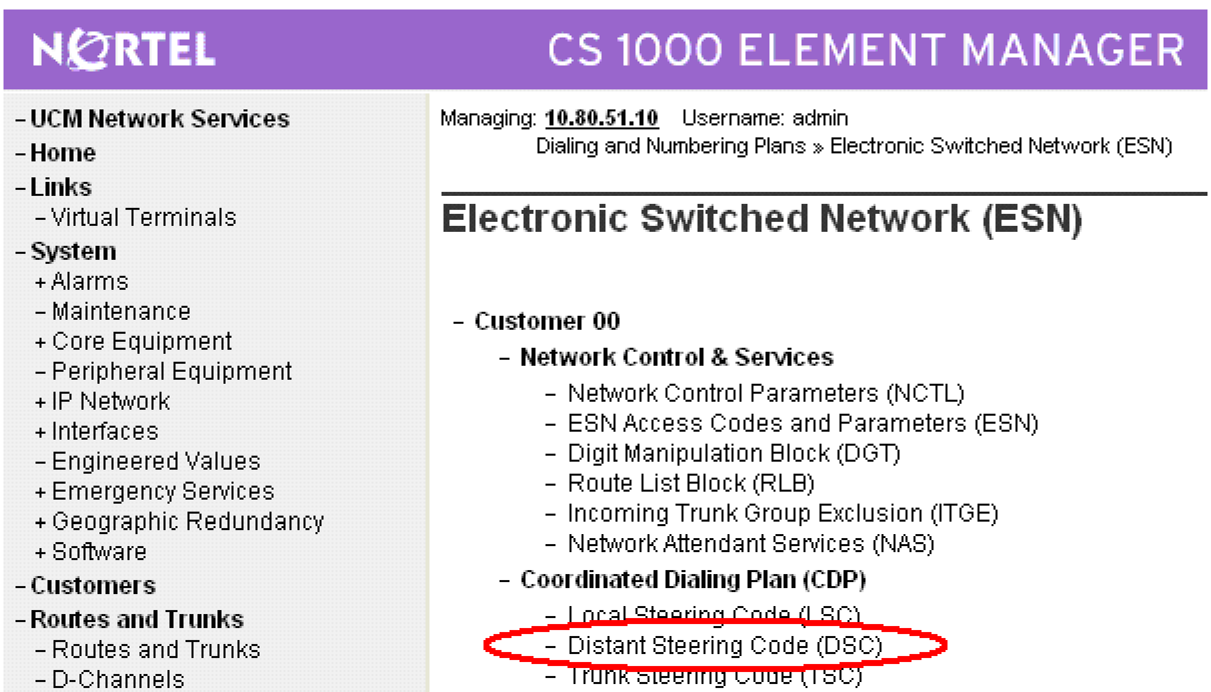
The *Route List Blocks* screen is displayed. In the **Please enter a route list index** field, enter an available route list block number (in this case "1"). Click **to Add**.

Figure 3: Route List Blocks

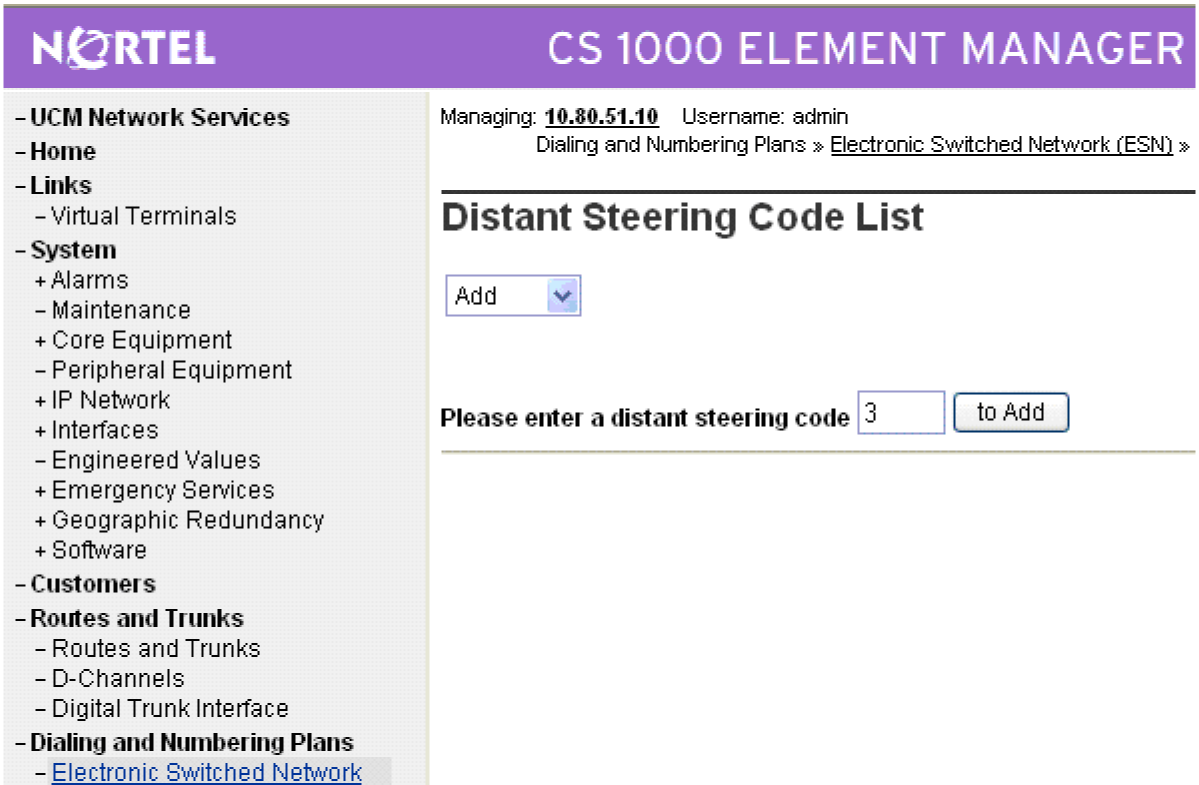
The Route List Block screen is displayed with a listing of parameters. For the **Route Number (ROUT)** field, select the route number from **Section 5.6**. Retain the default values for the remaining fields, and scroll down to the bottom of the screen and click **Submit** (not shown).



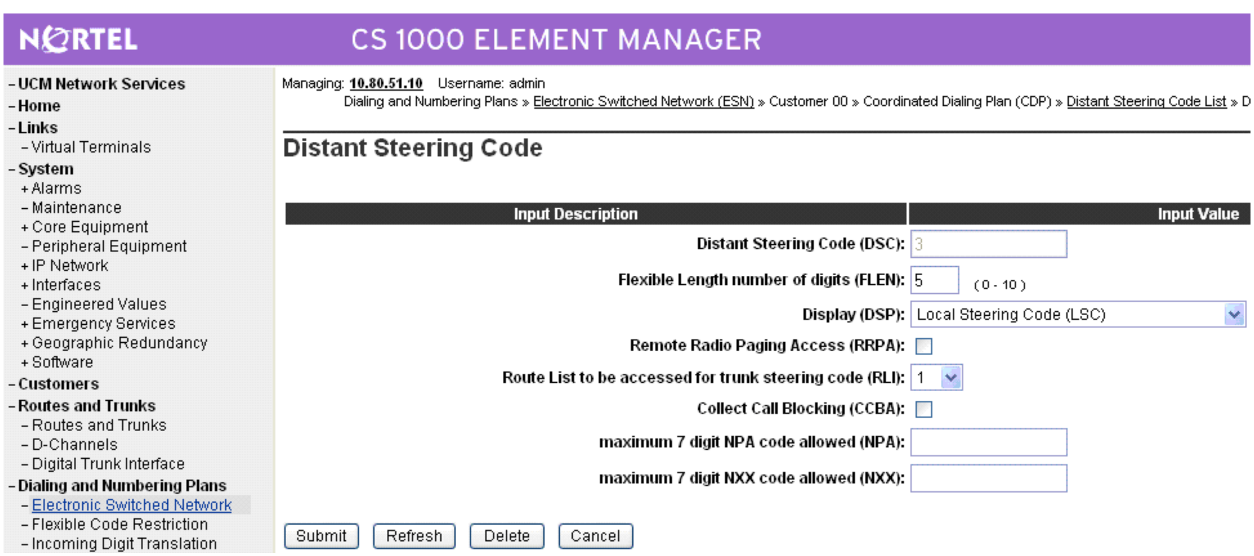
Select **Dialing and Numbering Plans → Electronic Switched Network** again from the left pane to display the Electronic Switched Network (ESN) screen. Select **Distant Steering Code (DSC)** to add an entry to route 3xxxx calls to Communication Manager.



The Distant Steering Code List screen is displayed next. In the **Please enter a distant steering code** field, enter the dialed prefix digits to match on (in this case “30”). Click **to Add**.

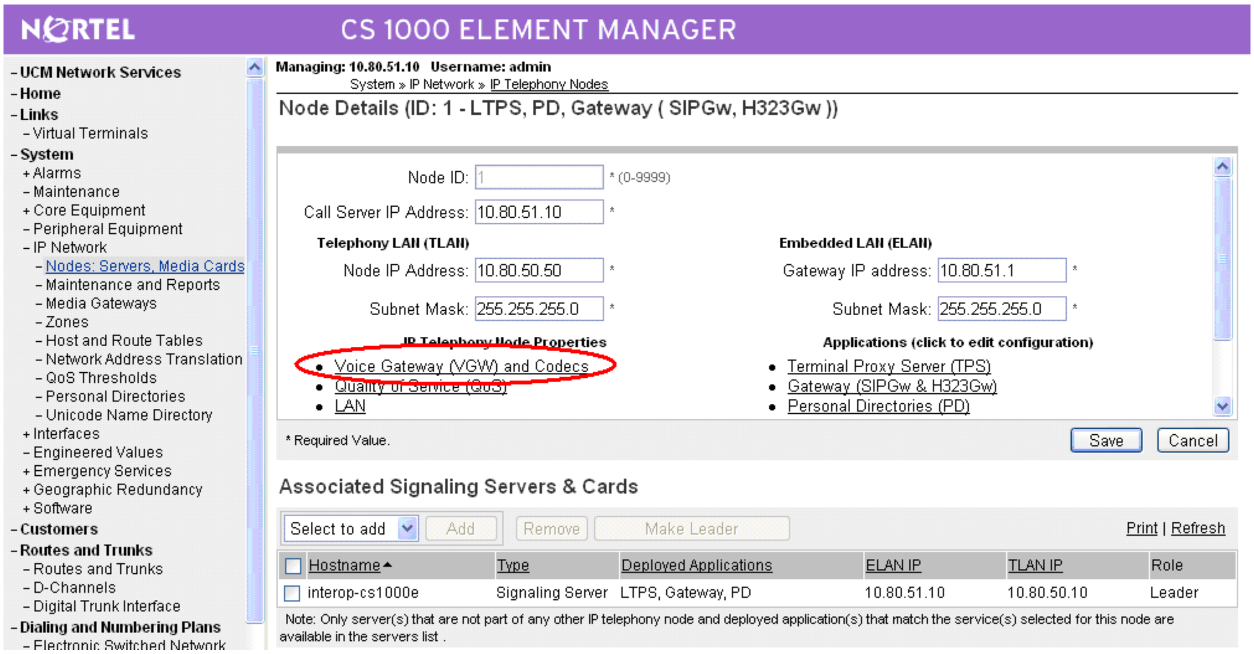


The Distant Steering Code screen is displayed. For the **Route List to be accessed for trunk steering code (RLI)** field, select the route list index in **Figure 3** of **Section 5.7** from the drop-down list. Retain the default values in all remaining fields and click on **Submit**.

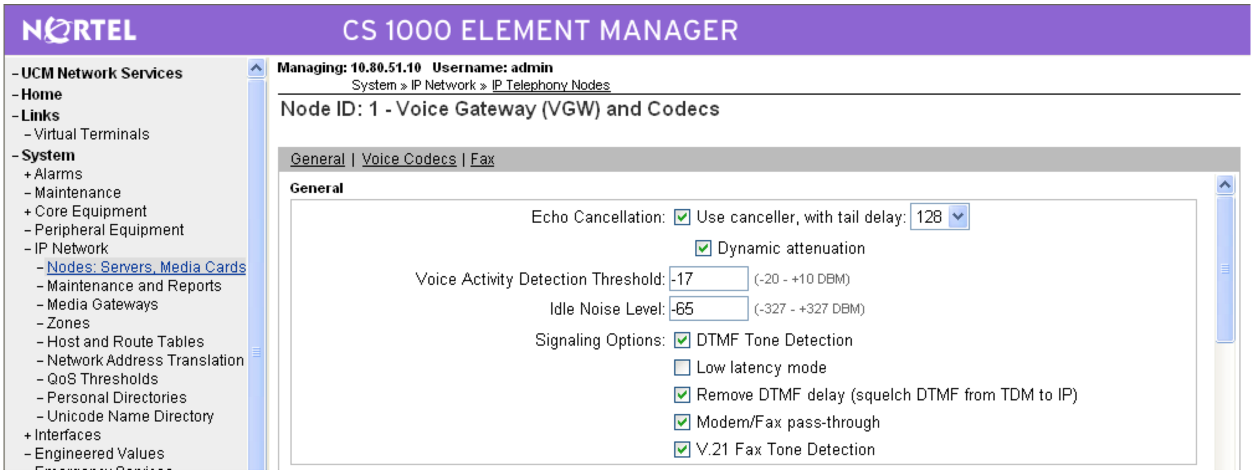


5.8 Configure Node SIP Parameters

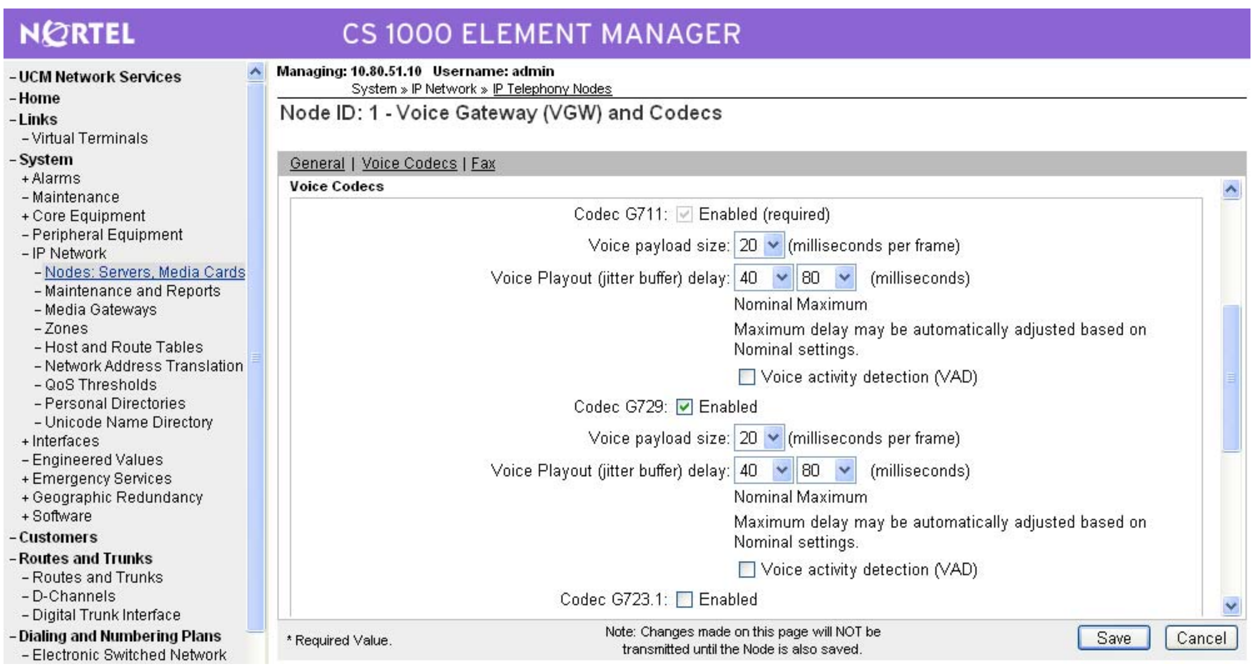
Select **IP Network → Nodes: Servers, Media Cards → Configuration** from the left pane, and in the IP Telephony Nodes screen displayed (not shown), select the node ID of this CS1000 system (see **Section 5.2**). The Node Details screen is displayed. It is assumed that the TLAN and ELAN IP addresses have already been configured as a result of basic configuration of the Signaling Server. Click on **Voice Gateway (VGW) and Codecs**.



In the following screen, verify the default options shown under *General*.



Scroll down the parameters box and check the desired codecs under *Voice Codecs*. Note that G.711 and G.729 were verified for the sample configuration. G.711 is checked by default. Click on **Save**.



When the Node Details screen is displayed, click on **Gateway (SIPGw and H.323Gw)**. Under *General* on the Virtual Trunk Gateway Configuration Details screen, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Vtrk Gateway Application:** Select "SIP Gateway (SIPGw)"; or select "SIPGw and H.323Gw" if both protocols will be supported on this system.
- **SIP Domain Name** Domain name used in **Section 4.1**
- **Local SIP Port** "5060"
- **Gateway endpoint name** An appropriate name
- **Gateway password** Enter a password

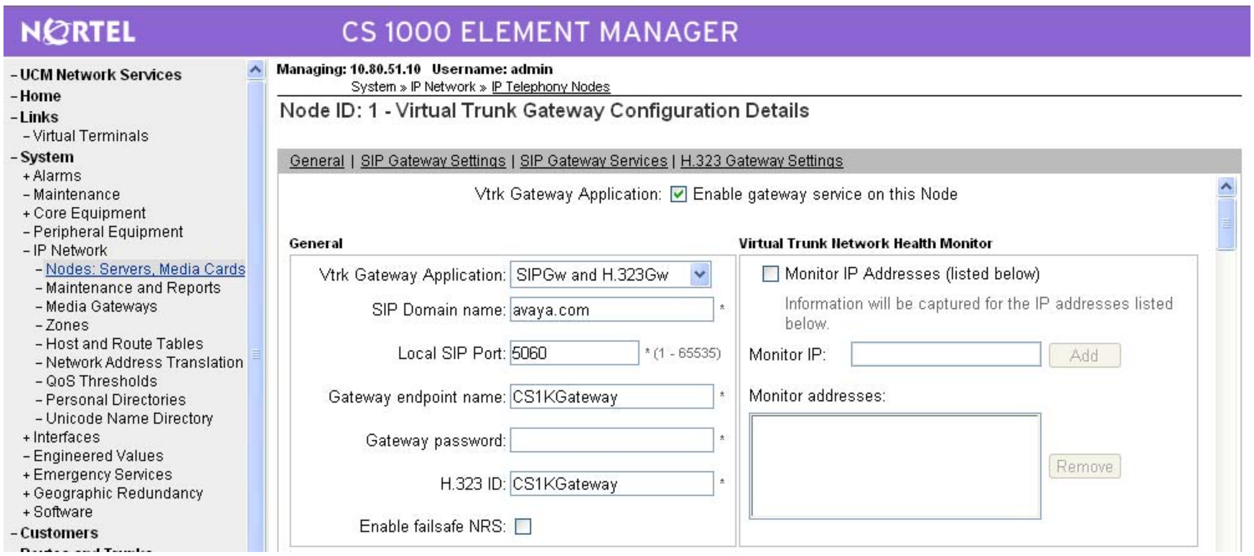
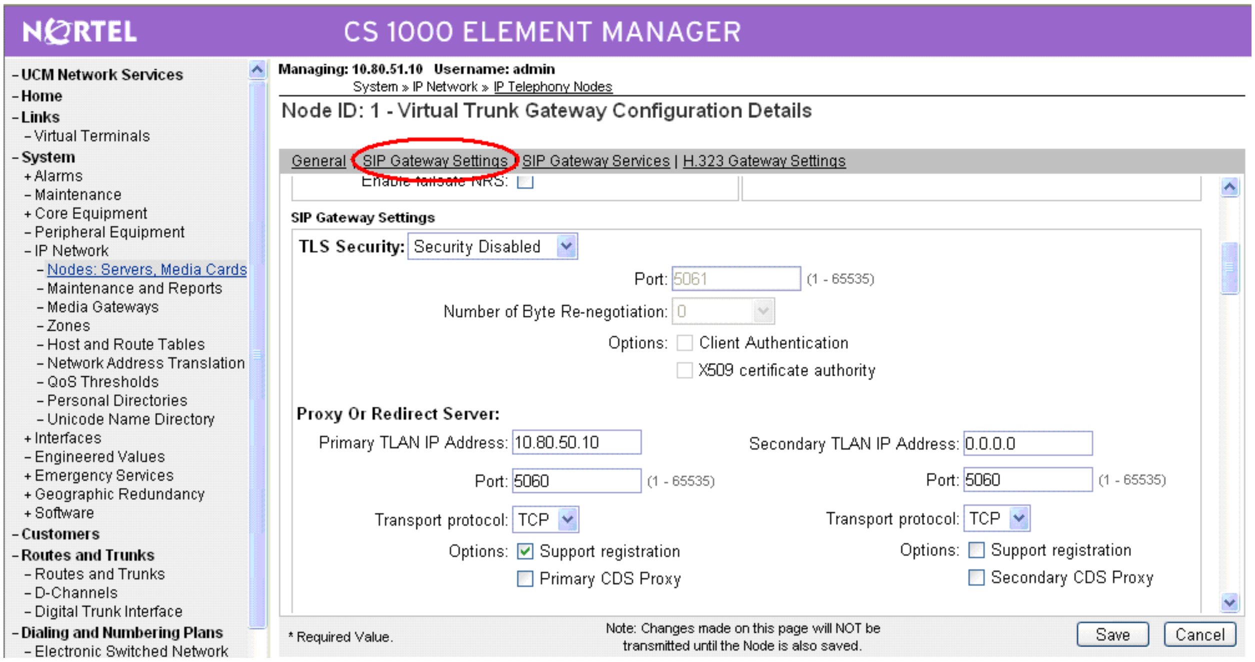


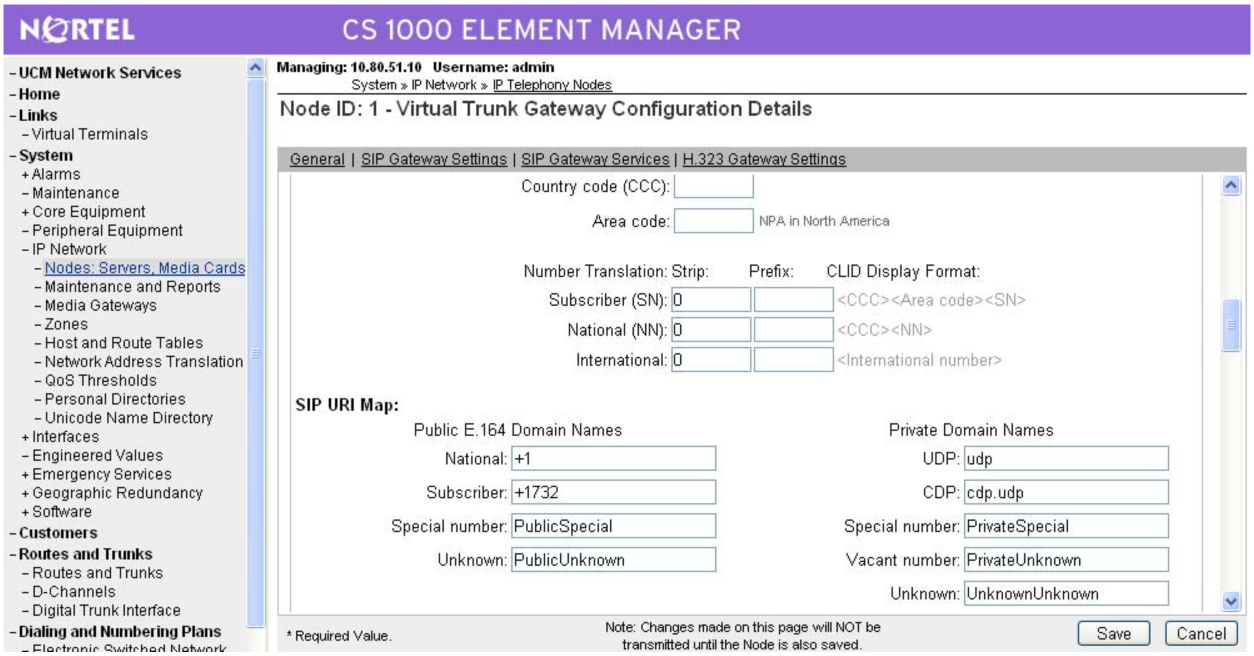
Figure 4: Node Details

Click on **SIP Gateway Settings**, and under *Proxy or Redirect Server*, enter the following values for the specified fields, and retain the default values for the remaining fields.

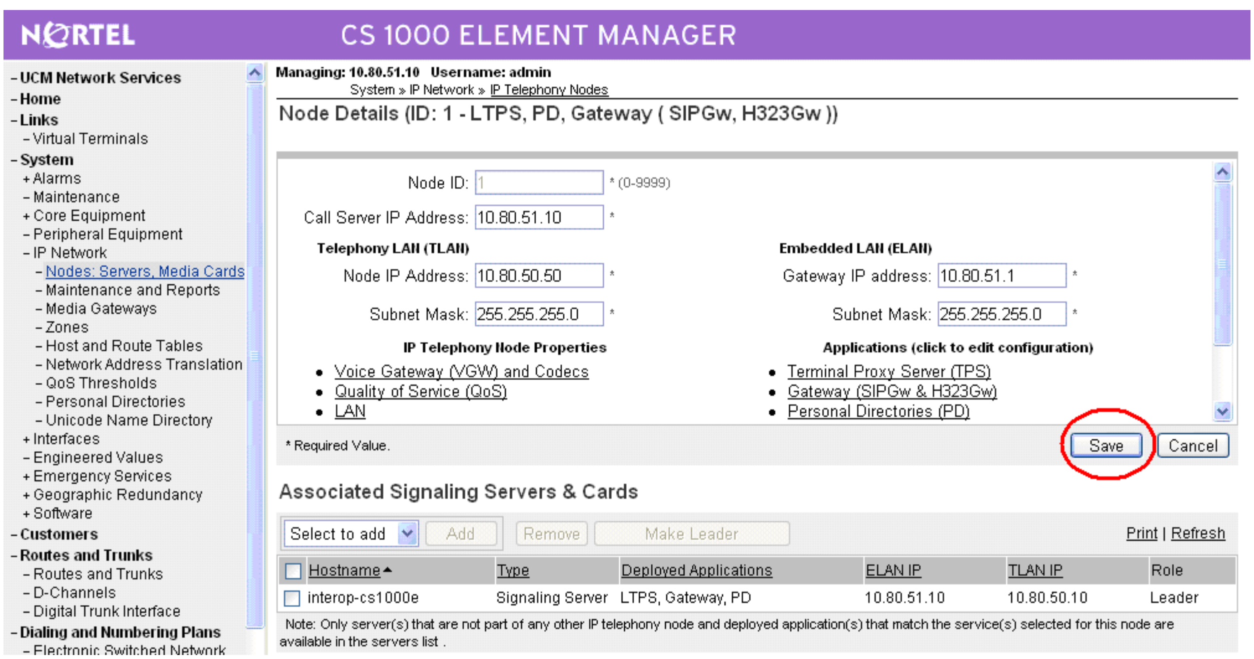
- **Primary TLAN IP Address:** The IP address of the Signaling Server noted in **Figure 2** in **Section 5.2**.
- **Port** "5060"
- **Transport Protocol** "TCP"
- **Options** Check "Support registration"



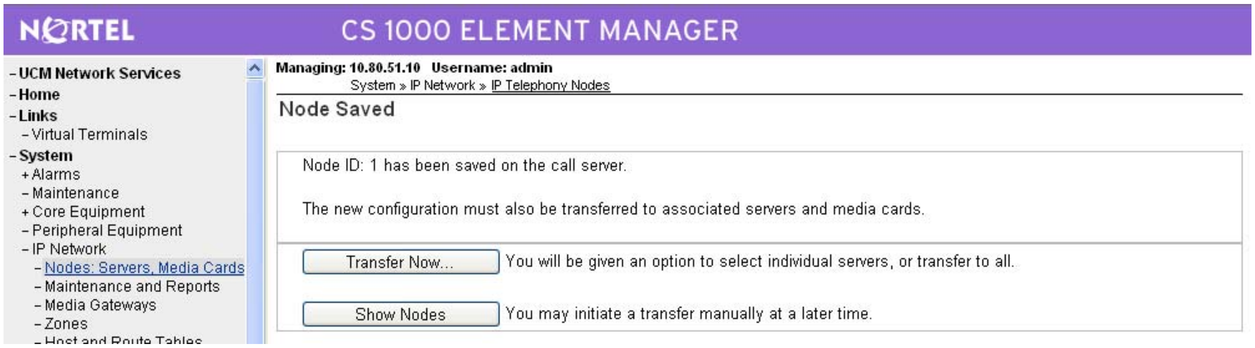
Scroll down the parameters box to the *SIP URI Map* section. Under *Public E.164 Domain Names***,** enter the appropriate **National** and **Subscriber** values for the network configuration. In the test configuration, “1” is the country code and “732” is the area code. The remaining fields can be left at their default values. Click on **Save**.



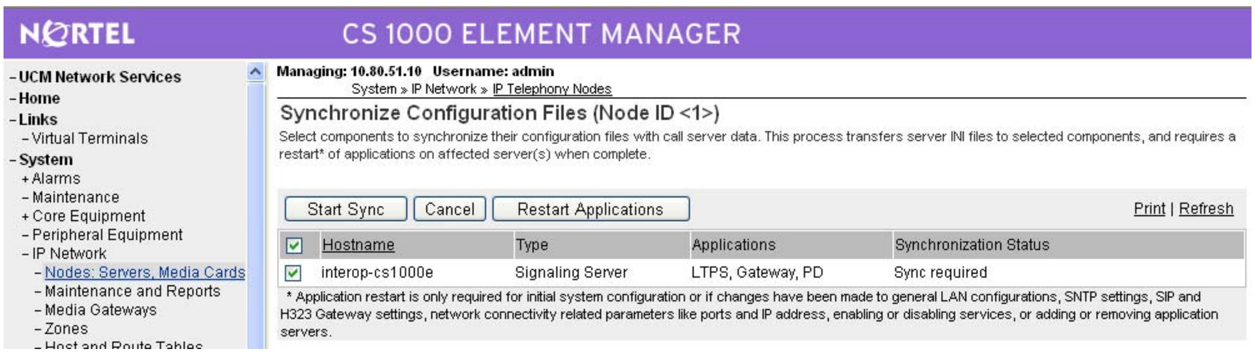
Return to the *Node Details* screen and click **Save**, as shown below.



The Node Saved screen is displayed. Click **Transfer Now…** .

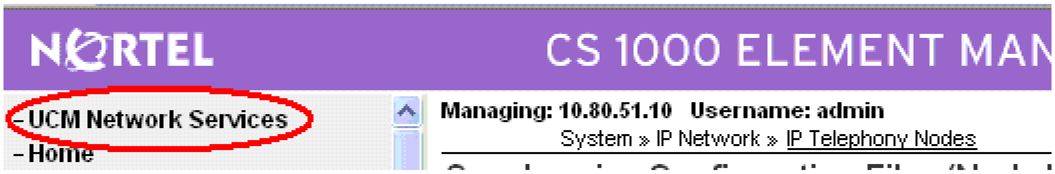


The Synchronize Configuration Files screen is displayed. Select the Signaling Server and click on **Start Sync**. When the synchronization completes, click on **Restart Applications**.

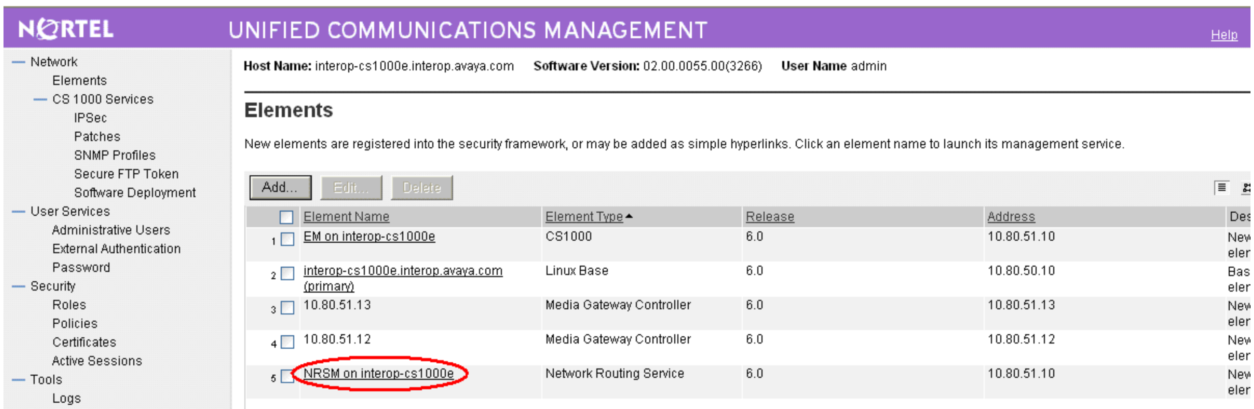


5.9 Launch NRS Manager

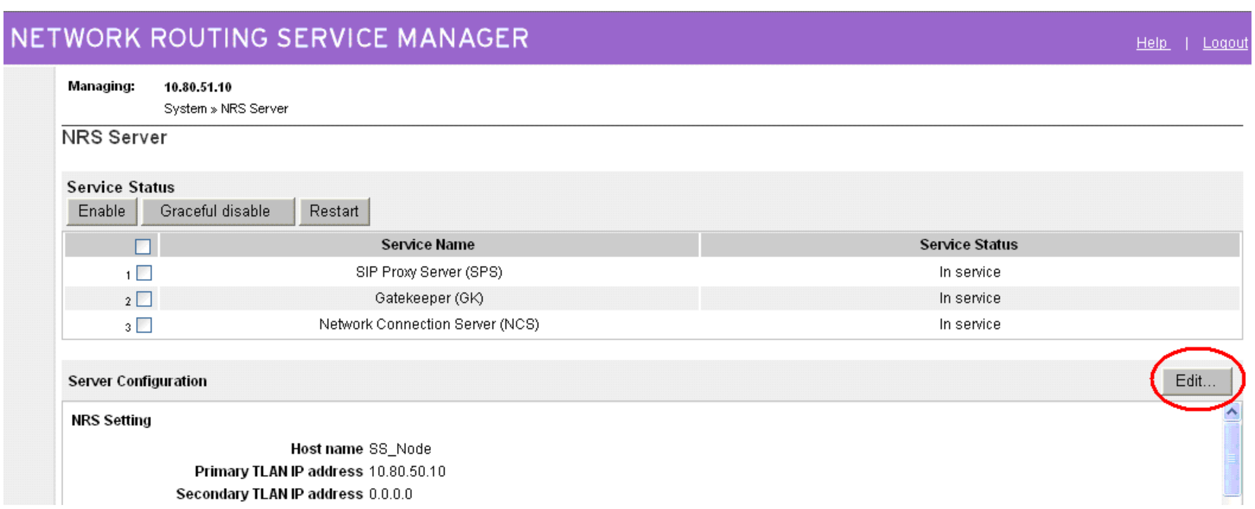
Select **UCM Network Services** from the left pane, which will display the high level Unified Communications Management screen.



Click on the *Element Name* with *Element Type* "Network Routing Service"



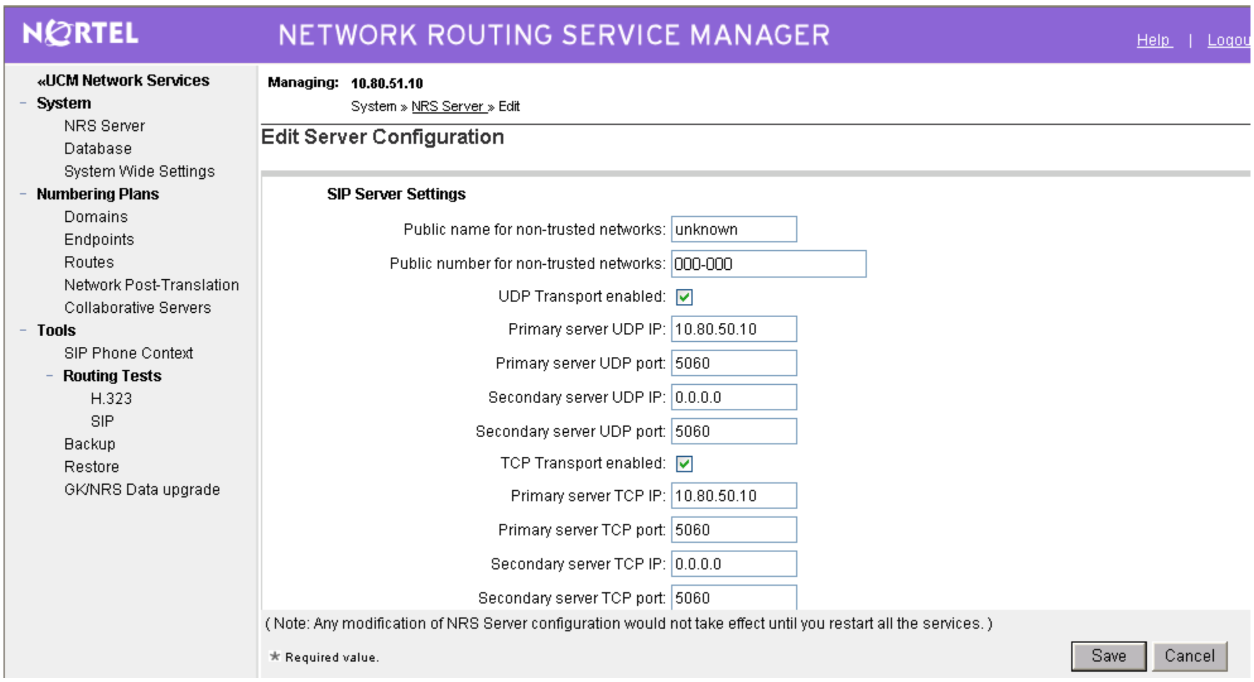
The Network Routing Service Manager screen is displayed. Click **EDIT**.



Under *SIP Server Settings*, 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).

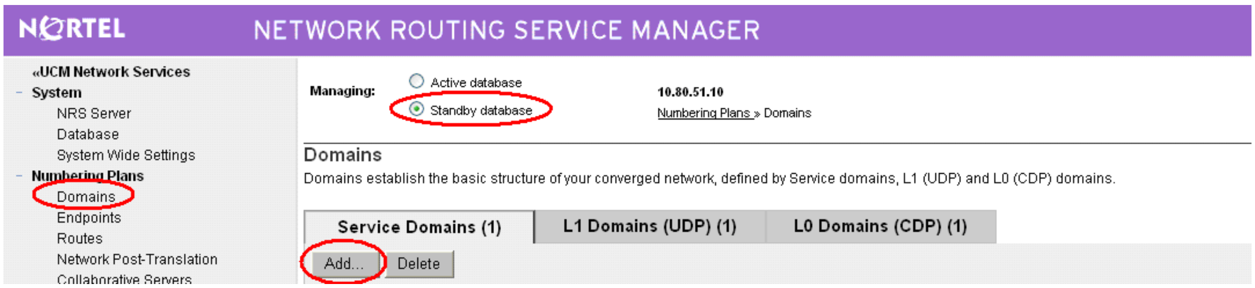
- **UDP transport enabled:** Check the checkbox
- **Primary Server UDP IP:** The Call Server IP address from **Section 5.2**
- **Primary Server UDP port:** “5060”
- **TCP transport enabled:** Check the checkbox
- **Primary Server TCP IP:** The Call Server IP address from **Section 5.2**
- **Primary Server TCP port:** “5060”

Click on **Save**.

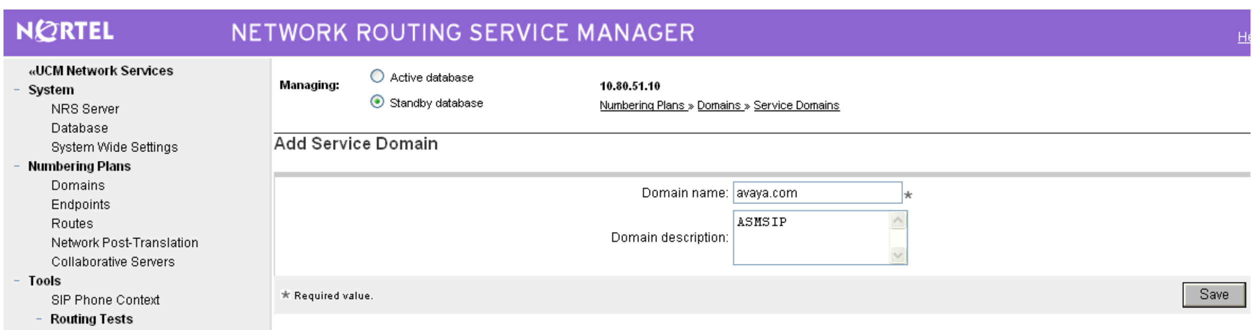


5.10 Configure Service Domain

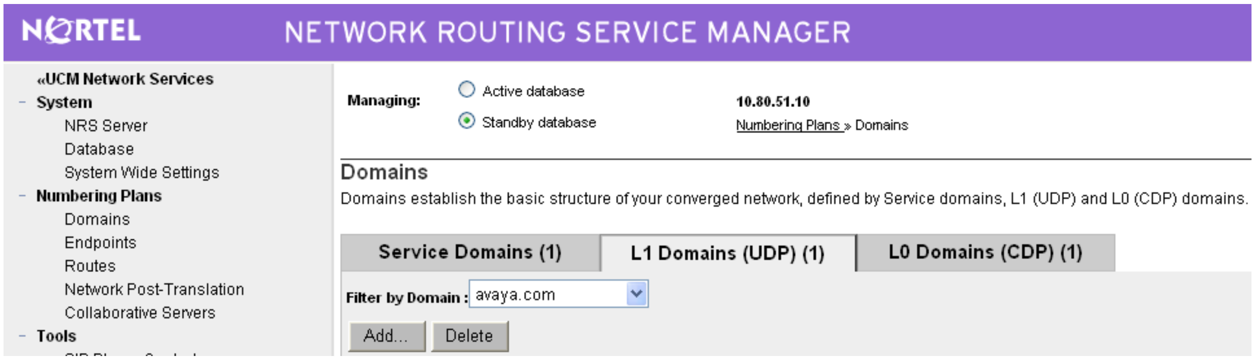
The NRS hosts an active and a standby database. The active database is used for runtime queries, and the standby database is used for administrative modifications. Under *Numbering Plans* on the left, click on **Domains**, and the Domains screen will be displayed. To add a domain, first click on the **Standby database** radio button to switch to the standby database. Then the **Add** button will be added to the display. Click on it to add a domain.



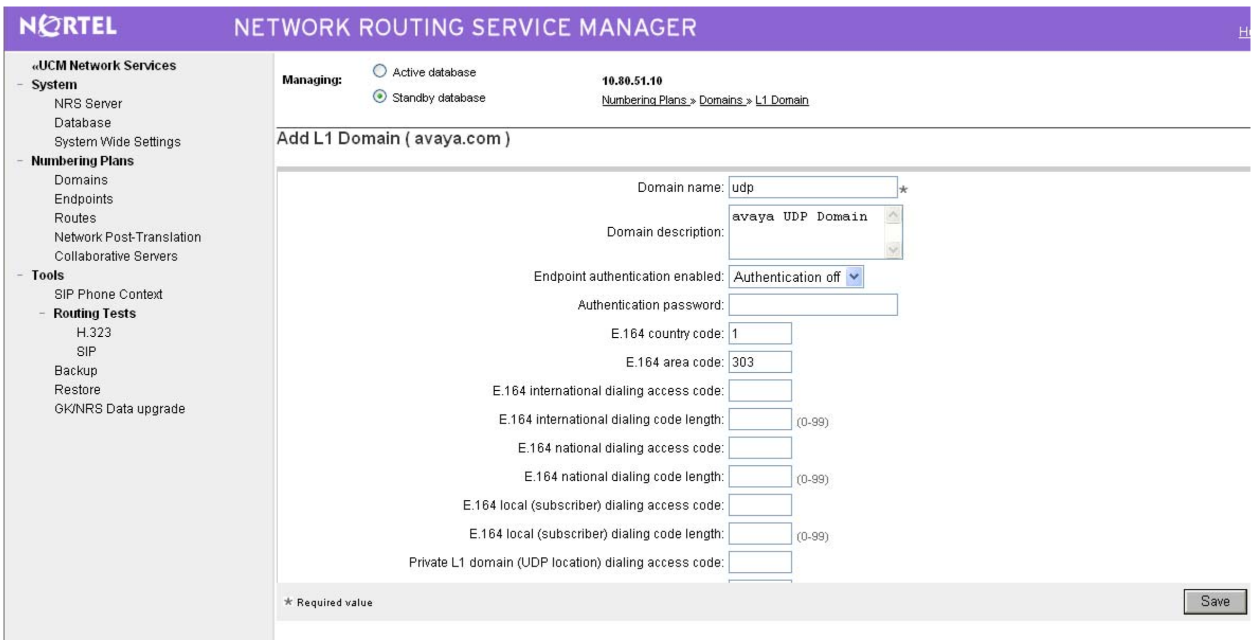
The Add Service Domain screen is displayed. Enter the SIP domain name from **Figure 4** of **Section 5.8** into the **Domain name** field, and a descriptive text for the **Domain description** field. Click **Save**.



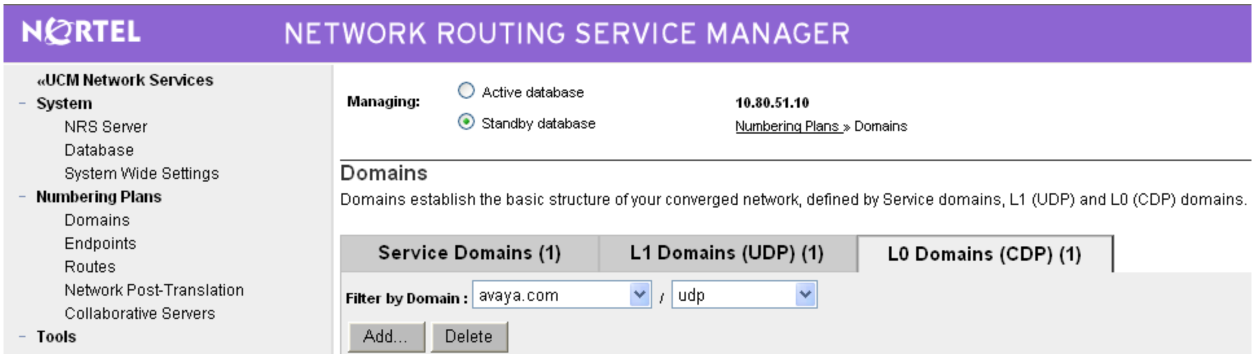
Select the **L1 Domains (UDP)** tab to display the L1 Domains (UDP) screen. Select the service domain just created for **Filter by Domain**, and click on **Add** to add a new L1 domain. The L1 and L0 domains are building blocks of the phone context for private addresses. For more information on L1 and L0 domains, refer to the Nortel documentation in **Section 8**.



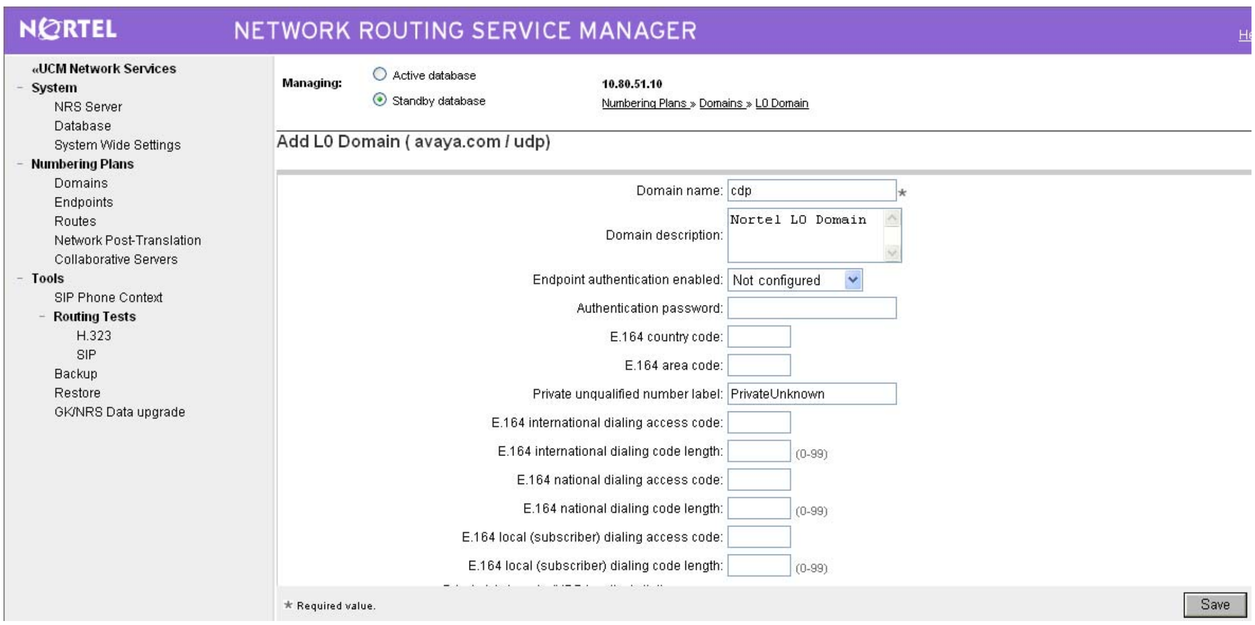
The Add L1 Domain (avaya.com) screen is displayed next, as shown below. Enter a descriptive **Domain name** and **Domain description**, and applicable **E.164 country code** and **E.164 area code** for the network configuration. Retain the default value in the remaining fields, and on **Save**.



Select the **L0 Domains (CDP)** tab to display the L0 Domains (CDP) screen. Select the service domain just created for **Filter by Domain** and "udp", and click on **Add** to add a new L0 domain.

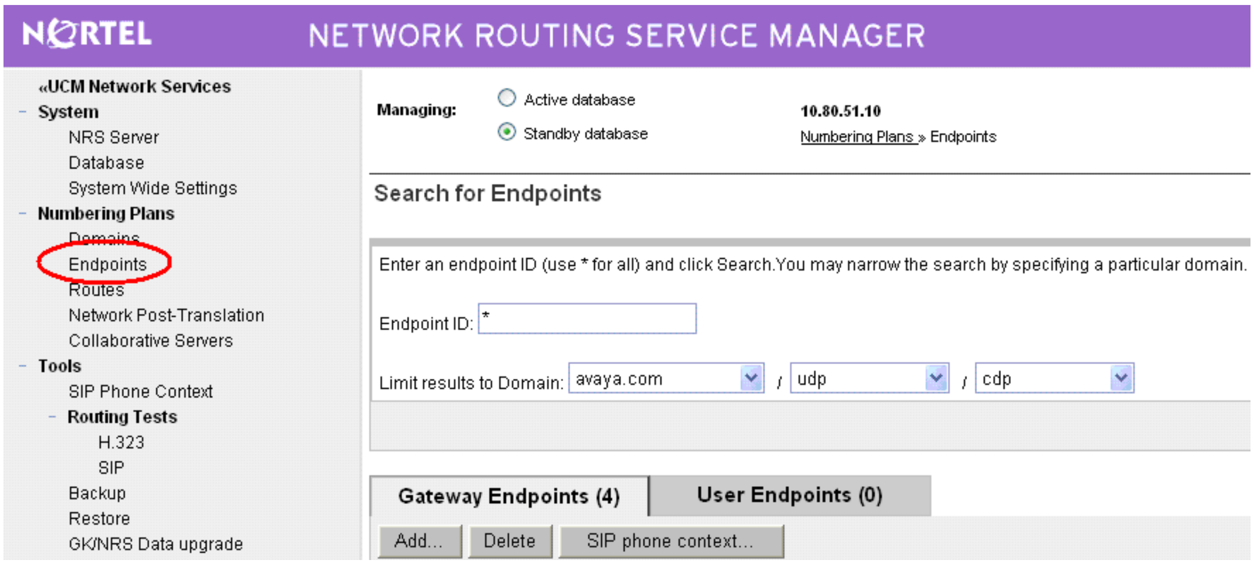


The Add L0 Domain (avaya.com /udp) screen is displayed next, as shown below. Enter a descriptive **Domain name** and **Domain description**. Retain the default values in the remaining fields and click **Save**.

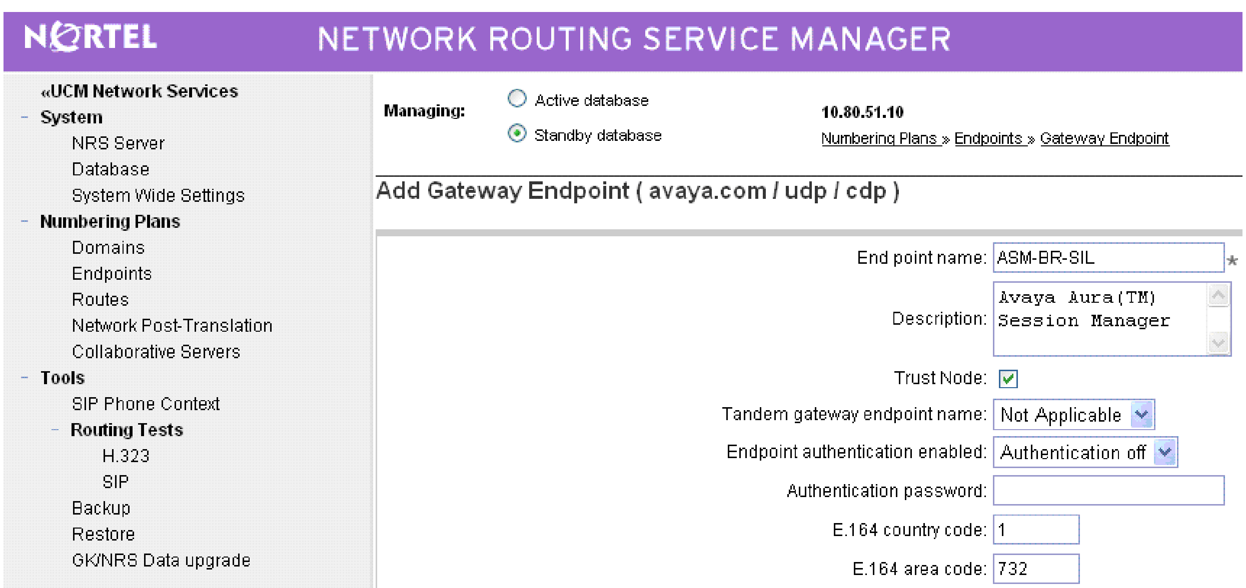


5.11 Configure SIP Gateway Endpoints

Next, configure two SIP gateway endpoints - one for the Session Manager server, and the other for the Nortel SIP Redirect Server. Under *Numbering Plans* on the left, click on **Endpoints**, and the Search for Endpoints screen will be displayed. For **Limit results to Domain**, select the service domain just created, "udp" and "cdp". Click **Add** to add a new gateway endpoint for Session Manager.

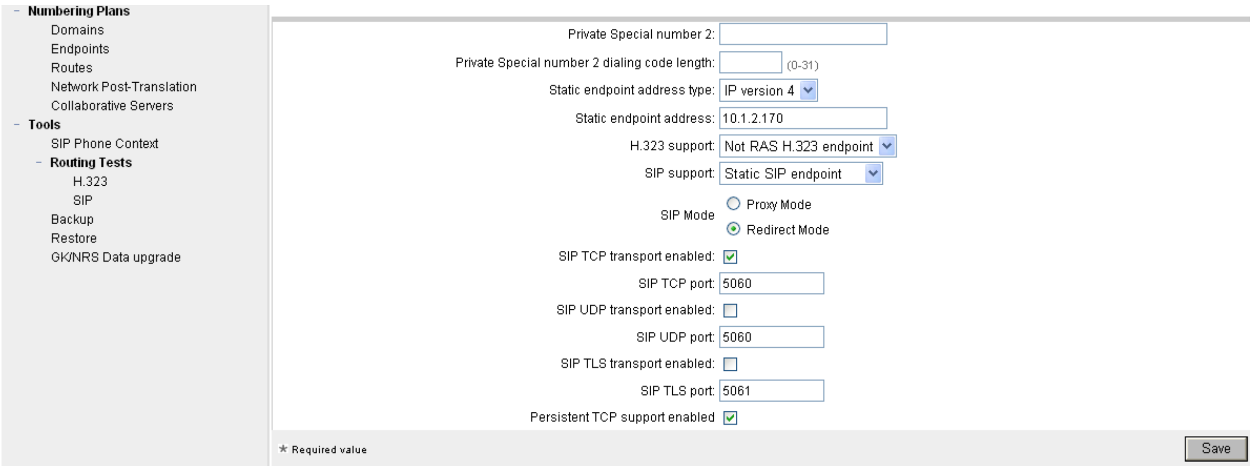


Enter a descriptive **End point name** and **Description**, as shown below and applicable **E.164 country code** and **E.164 area code** for the network configuration.

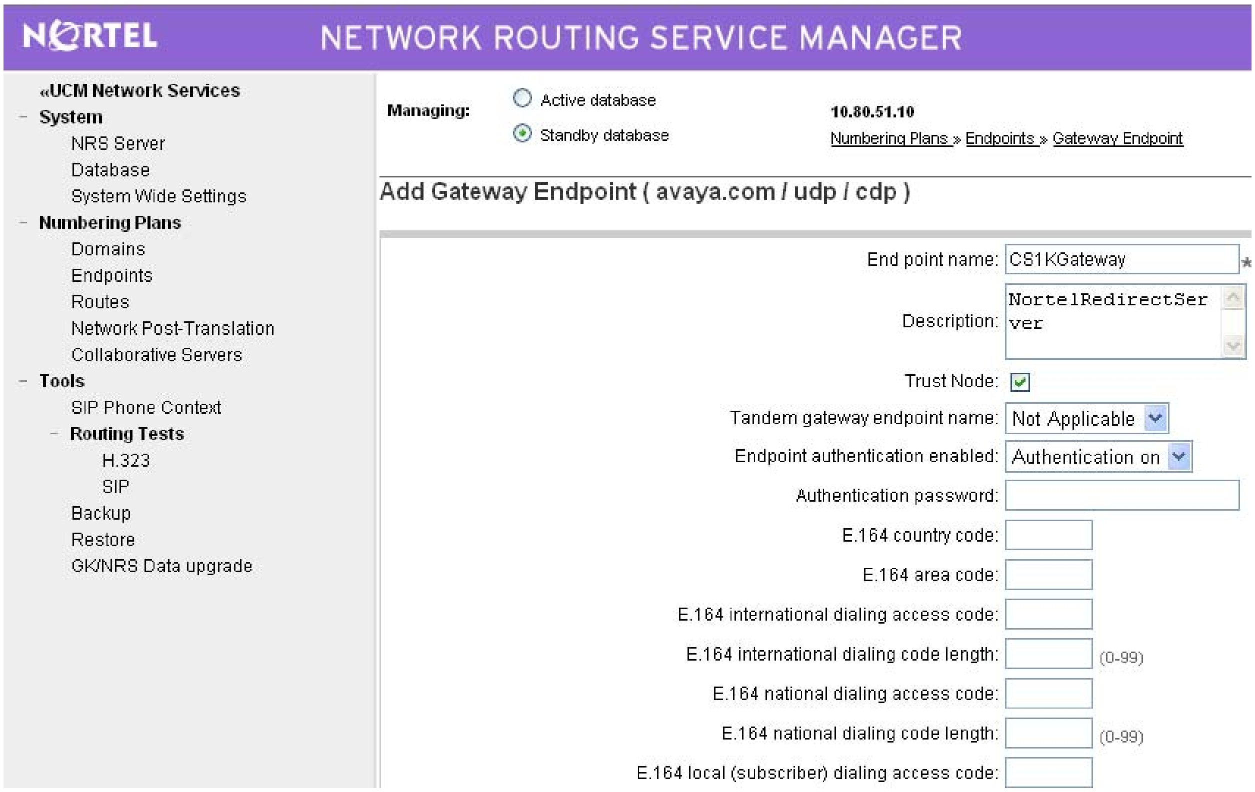


Scroll down the screen. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Save**.

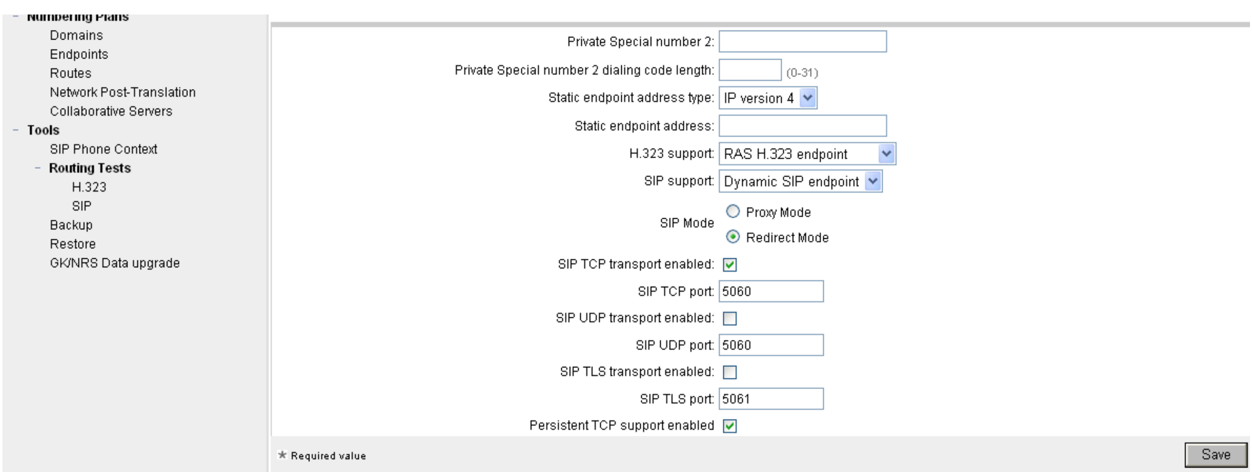
- **Static endpoint address:** IP address of Avaya Aura™ Session Manager SM-100 Module interface
- **H.323 Support:** "Not RAS H.323 endpoint"
- **SIP support:** "Static SIP endpoint"
- **SIP TCP transport enabled:** "TCP"



Repeat the procedures to add a gateway endpoint for the Nortel SIP Redirect Server as shown below. Select the desired value for **Endpoint authentication enabled**. If the authentication is turned on, then the value entered in the **Authentication password** field must match the **Gateway password** value from **Figure 4** of **Section 5.8**.



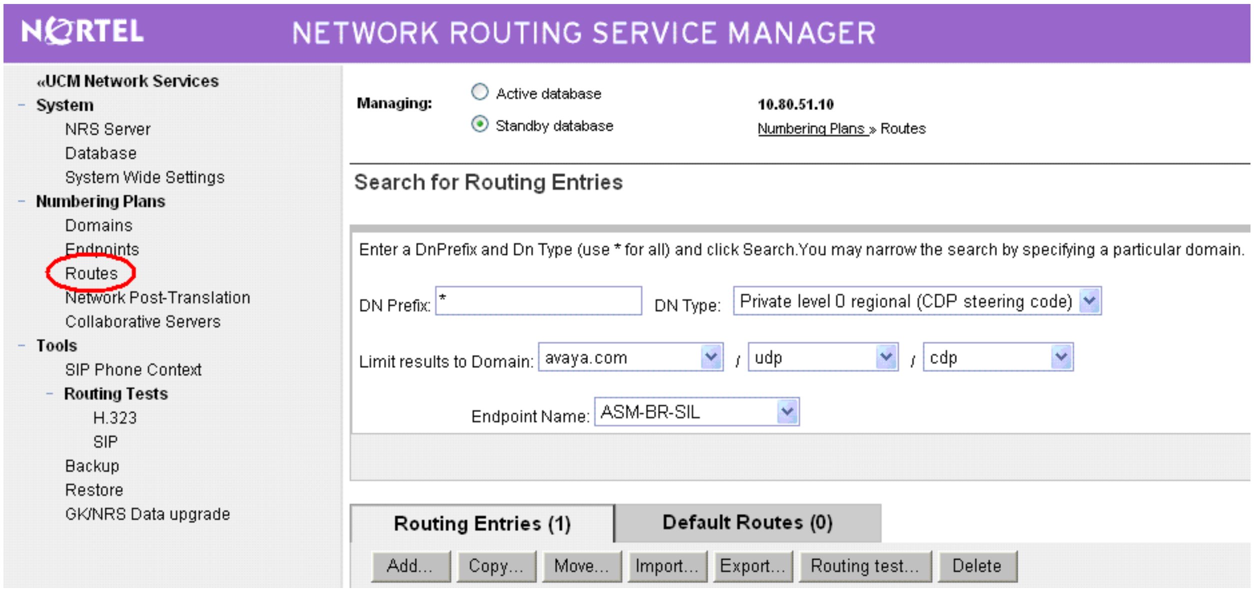
Scroll down the screen. For the **SIP support** field, select "Dynamic SIP endpoint" from the drop-down list. Check the **SIP TCP transport enabled** field to match the SIP transport protocol from **Figure 4** of **Section 5.8**. Maintain the default values in the remaining fields, and click **Save**.



5.12 Configure Routing Entries

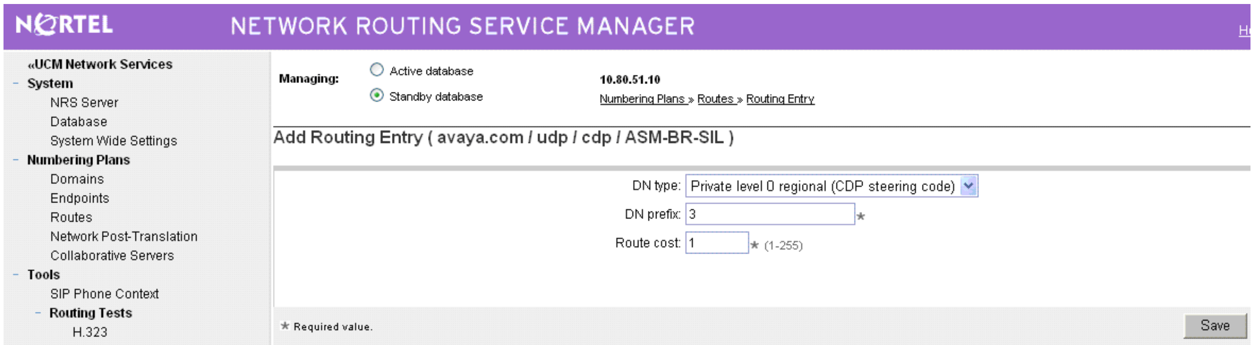
Configure two routing entries. The first entry uses the Session Manager gateway endpoint to reach Avaya endpoints with extension digits 3xxxx. The second entry uses the Nortel Redirect Server gateway endpoint to reach Nortel endpoints with extension digits 777xxx.

Under *Numbering Plans* on the left, click on **Routes**, and the Search for Endpoints screen will be displayed. For **Limit results to Domain**, select the service domain just created, "udp" and "cdp". Enter the **Endpoint name** corresponding to Session Manager. Click on **Add**.

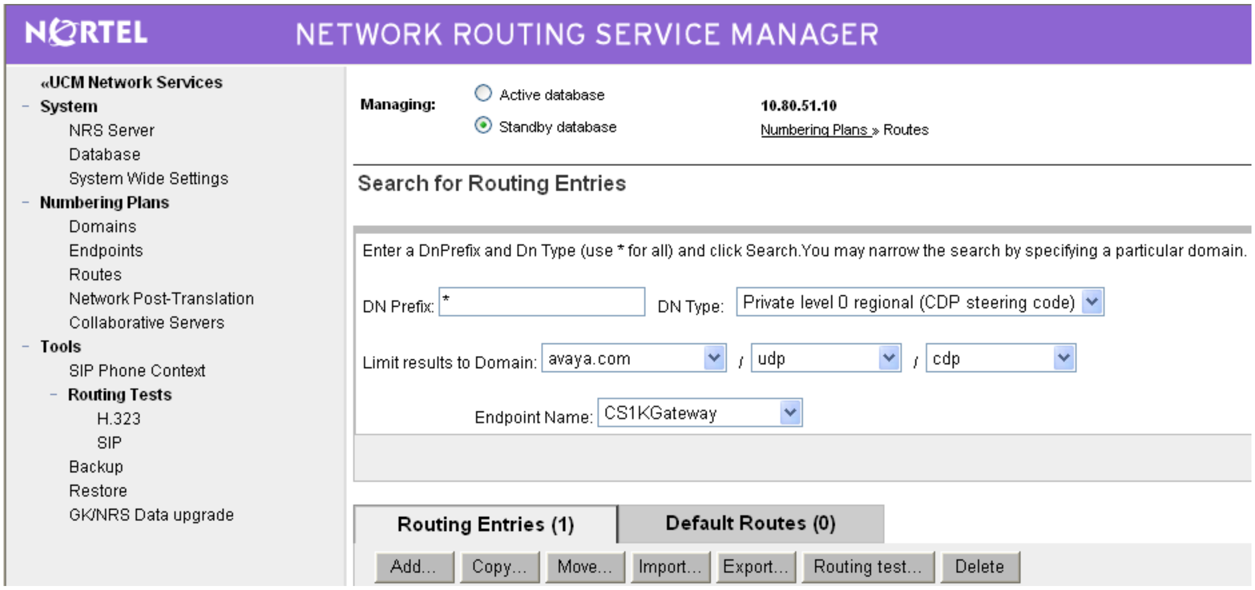


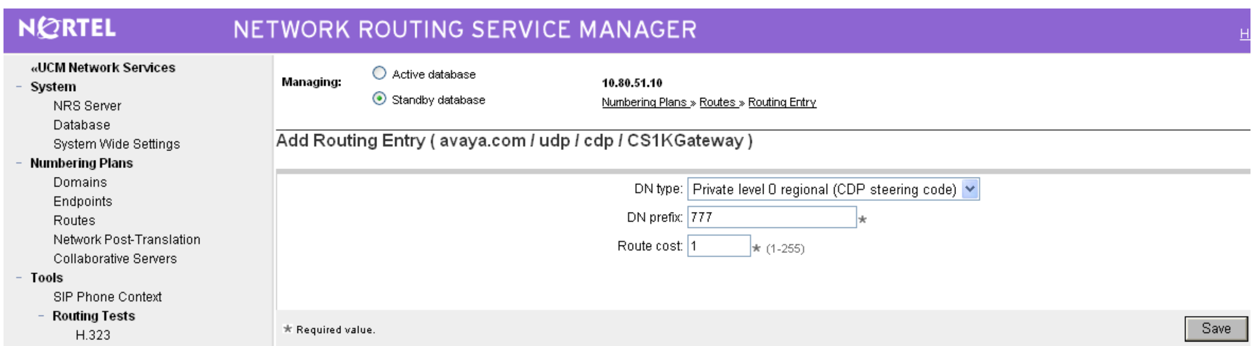
The Add Routing Entry screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Save**.

- **DN type:** "Private level 0 regional (CDP steering code)"
- **DN prefix:** Dialed prefix digits to match on, in this case "3".
- **Route cost (1 – 255)**: An appropriate cost value with 1 being least cost.



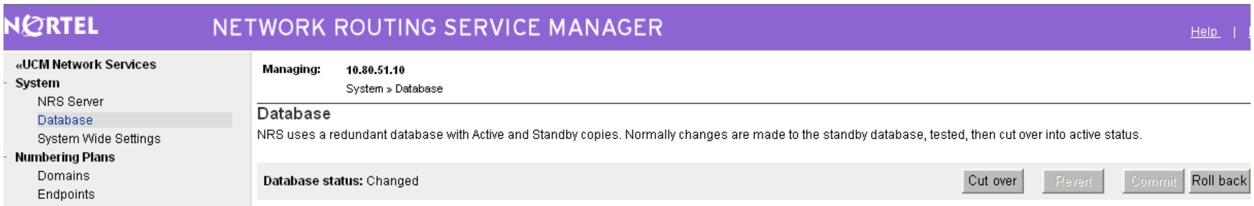
Repeat the same procedures to add a routing entry to reach the Nortel Communication Server 1000 endpoints with extension digits 777xxxx behind the Nortel SIP Redirect Server gateway endpoint.



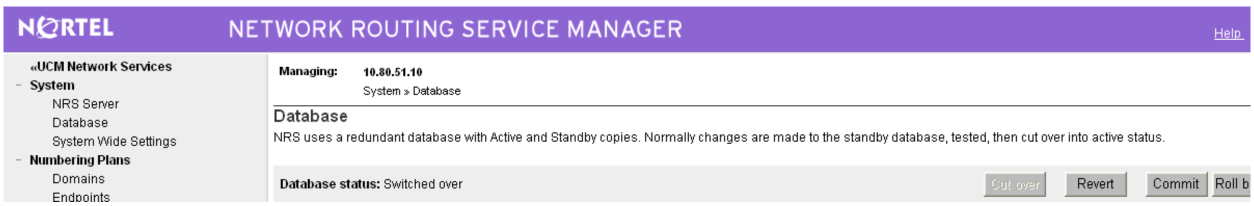


5.13 Cut Over and Commit Changes

Under *System* on the left, select **Database** to display the Database screen. Click on **Cut over**.



The **Database status** will change to "Switched over" and the **Commit** button will be enabled. Click on **Commit**.



6 Verification Steps

This section provides the tests that can be performed on Communication Manager 5.2.1 and Session Manager to verify proper configuration of Communication Manager, Session Manager, and Nortel Communication Server 1000.

6.1 Verify Avaya Aura™ 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
                                      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
```

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

```
status signaling-group 32
                         STATUS SIGNALING GROUP

        Group ID: 32                             Active NCA-TSC Count: 0
      Group Type: sip                             Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

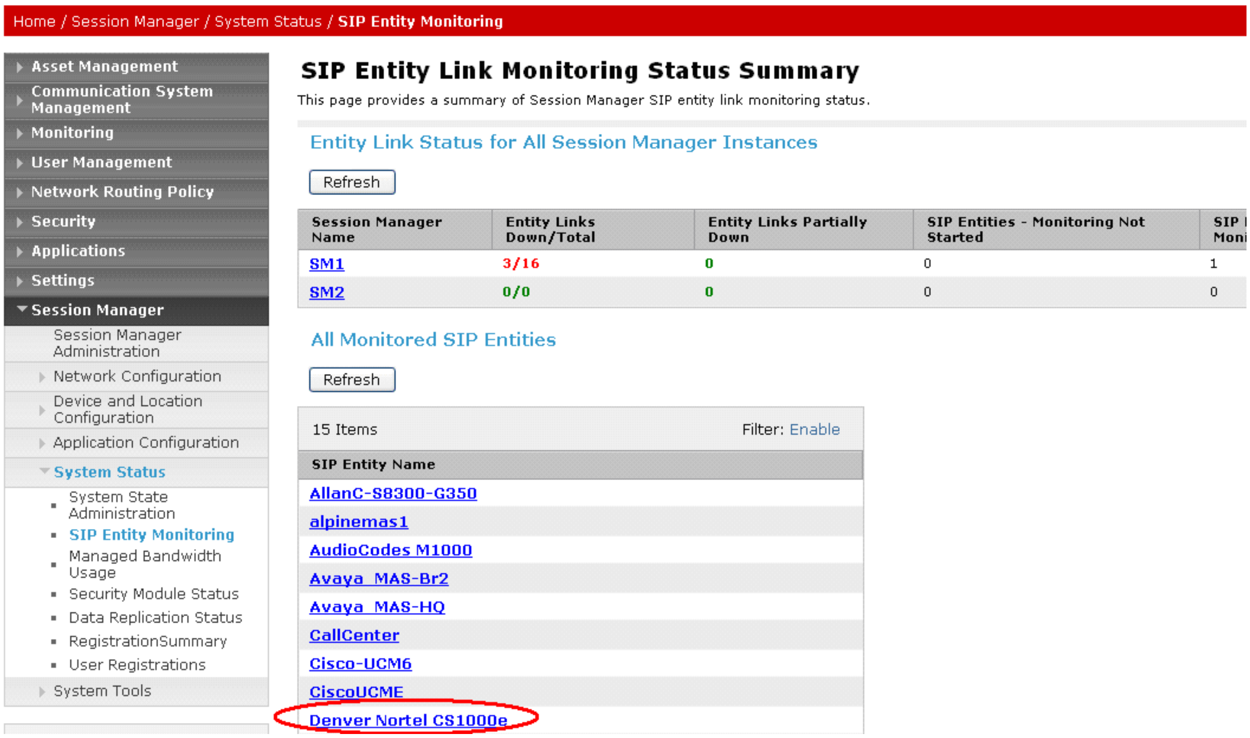
Make a call between the Avaya 9600 Series IP Telephone and the Nortel i2004 H.323 Telephone. Verify the status of connected SIP trunks by using the "status trunk x/y", where "x" is the number of the SIP trunk group from **Section 3.6.2** to reach Session Manager, and "y" is the member number of a connected 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 Session Manager are shown in the **Signaling** section. In addition, the **Audio** section shows the G.729 codec and the IP addresses of the Avaya H.323 and Nortel H.323 endpoints. The **Audio Connection Type** displays "ip-direct", indicating direct media between the two endpoints.

```
  status trunk 32/1                                                Page   1 of   3
                                TRUNK STATUS

   Trunk Group/Member: 0032/001              Service State: in-service/active
                 Port: T00226             Maintenance Busy? no
   Signaling Group ID: 32

     IGAR Connection? no

      Connected Ports: S00504
```

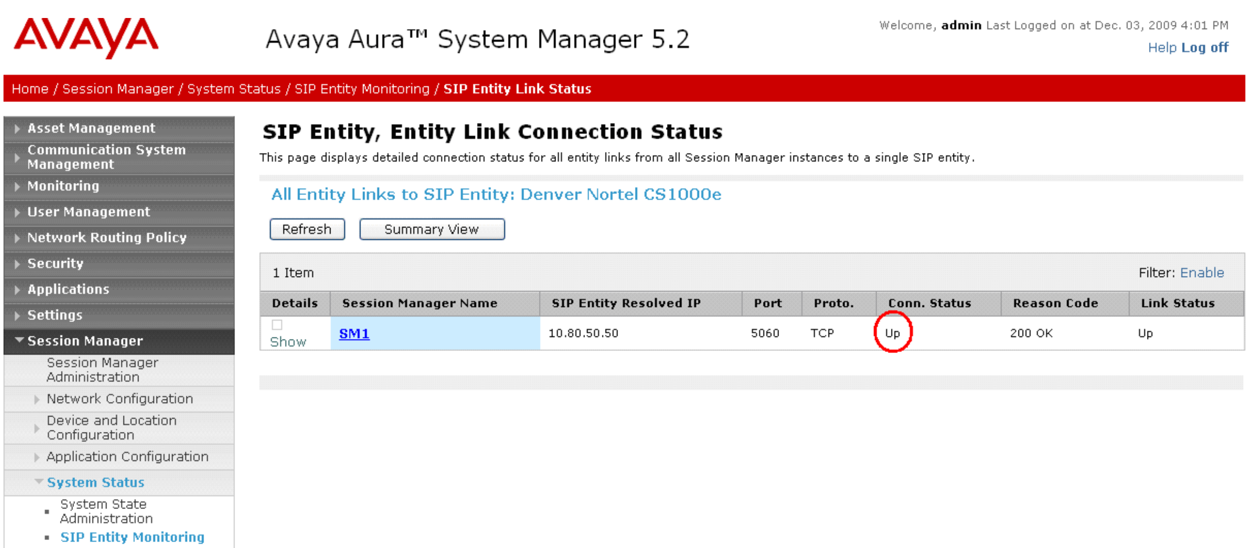
```
status trunk 32/1                                                Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: 01A0217
  Signaling   IP Address                             Port
   Near-end:  10.1.2.233                           : 5060
    Far-end:  10.1.2.170                           : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:          H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.711MU
   Audio      IP Address                             Port
   Near-end:  10.1.2.253                           : 6646
    Far-end:  10.80.50.253                           : 5200

 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:               Video Far-end Codec:
```

6.2 Verify Avaya Aura™ Session Manager

Navigate to *Session Manager* → *System Status* → *SIP Entity Monitoring* on the left to verify that none of the links to the defined SIP entities is down.

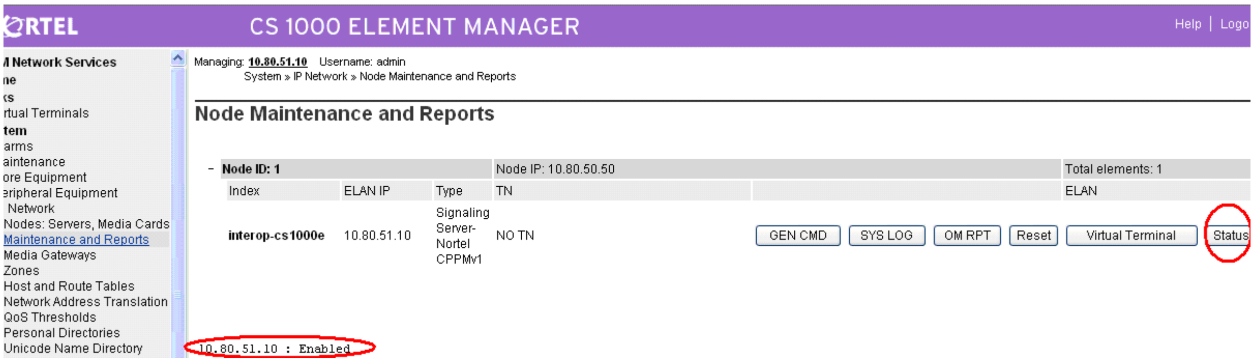


Under *All Monitored SIP entities*, select the appropriate SIP entities and verify that the connection status is "Up", as shown below for the Nortel Communication Server 1000.



6.3 Verify Nortel Communication Server 1000

Select **IP Network→Nodes: Servers, Media Cards→Maintenance and Reports** on the left. Click **Status** for the Signaling Server node to verify that it is enabled and operational.



6.4 Verification Scenarios

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

- Basic calls between various telephones on the Communication Manager and Nortel Communication Server 1000 can be made in both directions using G.711MU, and G.729.
- 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
  - Calling number block

7 Conclusion

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

- For G.729 interoperability, “G.729” must be included in the codec set in Communication Manager.
- Audio shuffling between the H.323 IP telephones is supported.
- Calling/called party name and number display may not be consistent for some supplementary calling features.

8 Additional References

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

Avaya Aura™ Session Manager:

[1] Avaya Aura™ Session Manager Overview, Doc ID 03-603473, available at http://support.avaya.com.

[2] Installing and Upgrading 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.

[4] Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325, available at http://support.avaya.com.

Avaya Aura™ Communication Manager 5.2.1:

[5] *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.

[6] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, May 2009, available at http://support.avaya.com.

Avaya Application Notes:

[7] *Front-Ending Nortel Communication Server 1000 with an AudioCodes Mediant 1000 Modular Media Gateway to Support SIP Trunks to Avaya Aura™ Session Manager with Avaya Aura™ Communication Manager 5.2 as a Feature Server – Issue 1.0*, available at http://www.avaya.com.

[8] *Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager 5.2, and Nortel Communication Server 1000 – Issue 1.1*, available at http://www.avaya.com.

Nortel Communication Server 1000:

[9] *IP Peer Networking Installation and Commissioning*, Nortel Communication Server 1000 Release 6, Document Number NN43001-313, Version 3.02, May, 2009, available on the Nortel Communication Server Electronic Reference Library CD.

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