Avaya Solution & Interoperability Test Lab

Configuring SIP Trunks among Avaya Communication Server 1000E 6.0, Avaya Aura™ Session Manager 5.2 and Avaya Meeting Exchange Enterprise Edition 5.2 – Issue 1.0

Abstract

These Application Notes present a sample configuration for a network that uses SIP trunks to connect the Avaya Communication Server 1000E (formerly known as Nortel CS1000E) to Avaya Meeting Exchange Enterprise Edition via Avaya Aura™ Session Manager 5.2.

For the sample configuration, Avaya Communication Server 1000E runs the SIP Proxy NRS hosted co-resident with the Signaling Server on a single CPPM card while the Avaya Meeting Exchange Application and Media Server run on two separate S8510 servers.

1. Introduction

These Application Notes present a sample configuration for a network that uses SIP trunks to connect the Avaya Communication Server 1000E (formerly known as Nortel CS1000E) to Avaya Meeting Exchange Enterprise Edition via Avaya Aura™ Session Manager 5.2.

As shown in **Figure 1**, the Avaya 2050 IP Softphone (UNIStim), Avaya M3820 Digital Telephone, Avaya 1120E UNIStim IP Telephone and Avaya 1140E SIP Telephone are supported by Avaya Communication Server 1000E. The Avaya 1140E SIP phones are registered to the SIP Line Gateway (SIPL) which is a SIP Registrar running on the Signaling Server component of the Communication Server 1000E. SIP trunks are used to connect Avaya Aura™ Session Manager to Communication Server 1000E and Avaya Meeting Exchange Enterprise over the LAN. Signaling messages are carried over the TCP-based SIP trunks while DTMF is transmitted within the RTP stream using RFC2833 compliant messages. An analogue phone is attached to a PSTN simulator which is connected with an E1 PRI trunk to the sample telephony network. This configuration enables PSTN users to participate in a conference with other enterprise users on the private network. The Telephones are configured in the 3xxx extension range, while the conference access number (DNIS) on the Avaya Meeting Exchange is set to 11111.

For the sample configuration, Avaya Communication Server 1000E runs on a single CPPM card while the Avaya Meeting Exchange Enterprise Application and Media Server run on two separate Avaya S8510 servers.

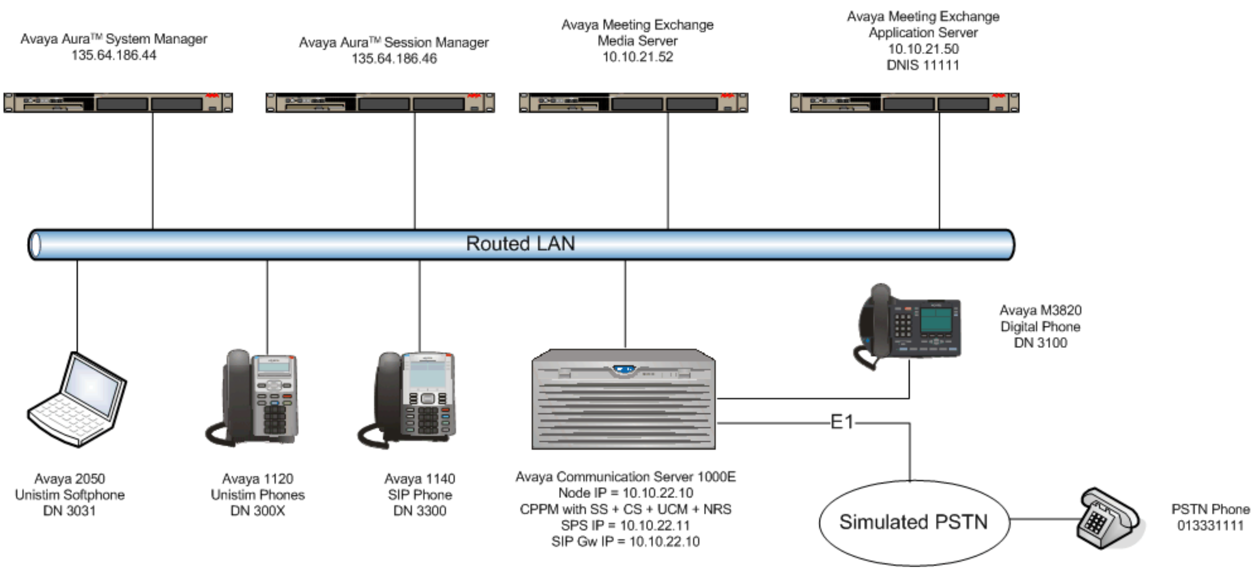


Figure 1 – Sample Configuration

These Application Notes will focus on the configuration of the SIP trunks and call routing. Detailed administration of the endpoint telephones and E1 PRI trunk will not be described (see the appropriate documents listed in **Section 9**).

2. Equipment and Software Validated

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

Equipment	Software Version
Avaya S8510 Server	Avaya Aura™ Session Manager 5.2.0.1 VSP 1.1.0.0.8 with patch 1.1.0.4.8
Avaya S8510 Server	Avaya Aura™ System Manager 5.2.0.7.11
Avaya Communication Server 1000E	Release 600R, Version 4121
Avaya 1140 IP Phone	SIP 02.02.21.00
Avaya 1120E IP Phone	UNIStim 0624C60
Avaya IP SoftPhone2050	UNIStim 3.04.0003
Avaya M3820 Digital Phone	N/A
Avaya S8510 Server	Avaya Meeting Exchange Enterprise Edition Application Server S6200 R5.2 Build 5.2.0.0.22 (GA) and MX Patch Group 5.2.1.2.1
Avaya S8510 Server	Avaya Meeting Exchange Enterprise Edition Media Server S6200 R5.2 Build 5.2.0.0.22 (GA) and MX Patch Group 5.2.1.2.1

Table 1: Version Numbers of Equipment and Software

3. Configure Avaya Communication Server 1000E

The sample network uses a single CPPM card within the Avaya MG1000E gateway which runs all the software services necessary to route calls, administer the dial plan and provide signaling interfaces to external nodes (telephones and trunks). Avaya Communication Server 1000E uses the Signaling Server and Network Routing Service (NRS) to provide SIP, H.323 and UNIStim (Avaya proprietary) signaling interfaces to IP networks. The Call Server is another software component that resides on the CPPM card within the Avaya MG1000E gateway and controls the telephony features. Avaya provides a single web GUI which runs on the CPPM called Unified Communications Management (UCM) for the provisioning of the various telephony software components.

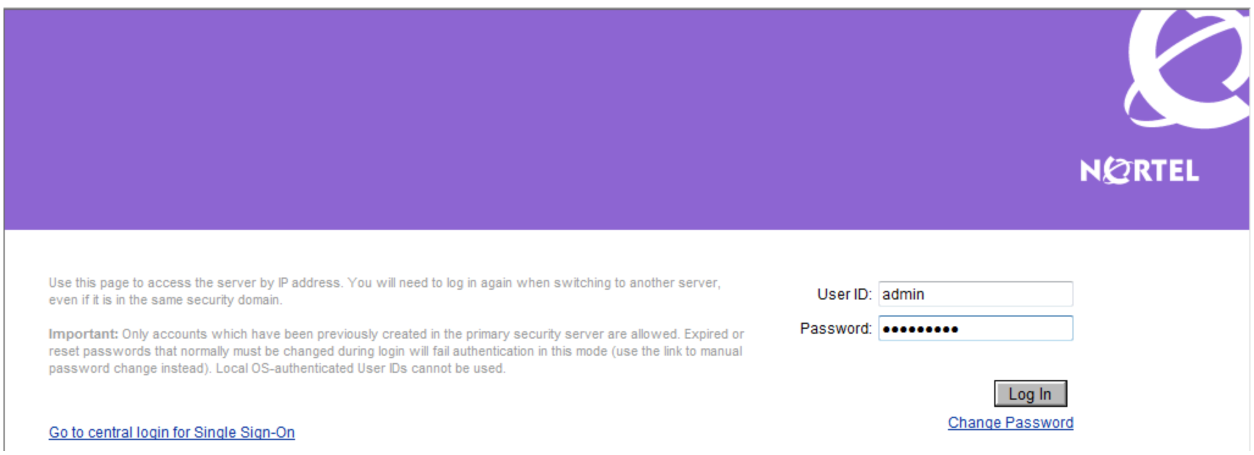
These Application Notes used the Coordinated Dial Plan (CDP) feature to route calls from the Avaya Communication Server 1000E, over a SIP trunk to Session Manager. The CDP feature is assumed to be already enabled on Avaya Communication Server 1000E, and therefore will not be described in detail.

All configurations in this section are administered using a web browser. These Application Notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000E, please consult reference **[1]**. The procedures below describe the details of configuring Avaya Communication Server 1000 with a SIP trunk to Session Manager:

- Login to the Unified Communications Management GUI
- Obtain Node IP address
- Administer ISDN
- Administer D-Channel
- Administer virtual SIP routes and trunks
- Administer route list block and distant steering code
- Administer Node Media and SIP parameters
- Launch NRS Manager
- Administer service domain
- Administer SIP Signaling Gateway endpoints
- Administer routing entries
- Cut over and commit changes

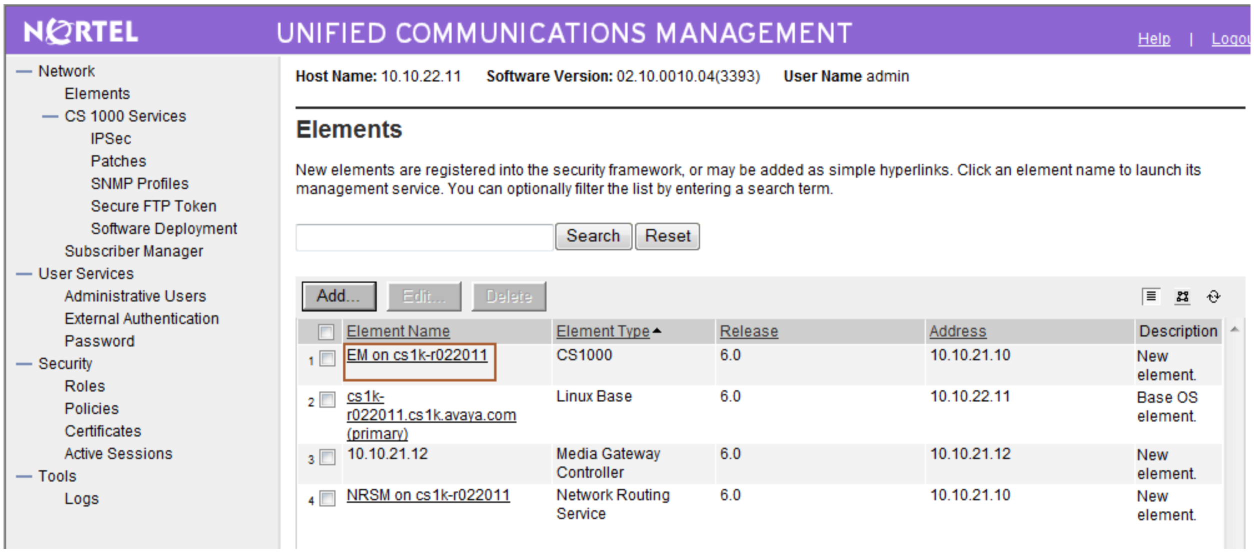
3.1. Log in to the Unified Communications Management GUI

Open an instance of a web browser and connect to the UCM GUI at the following address: http://<node IP address>. Log in using an appropriate Username and Password.

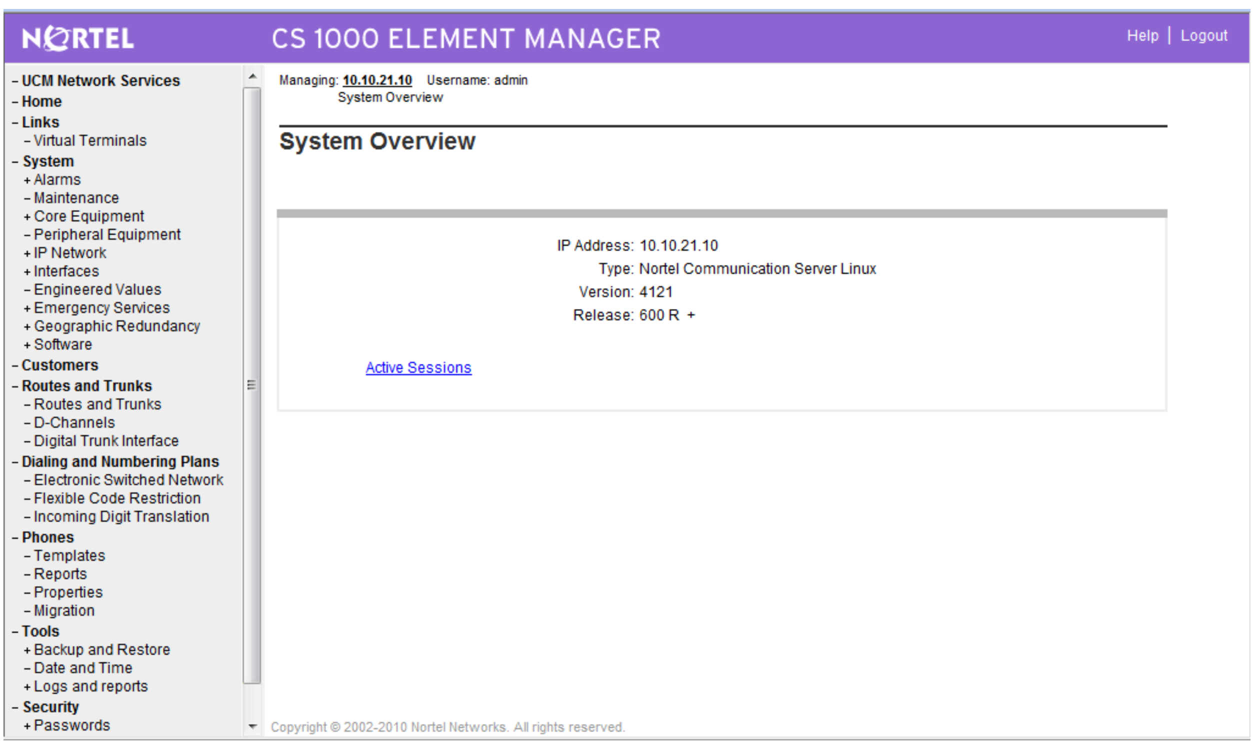


3.2. Obtain Node IP Address

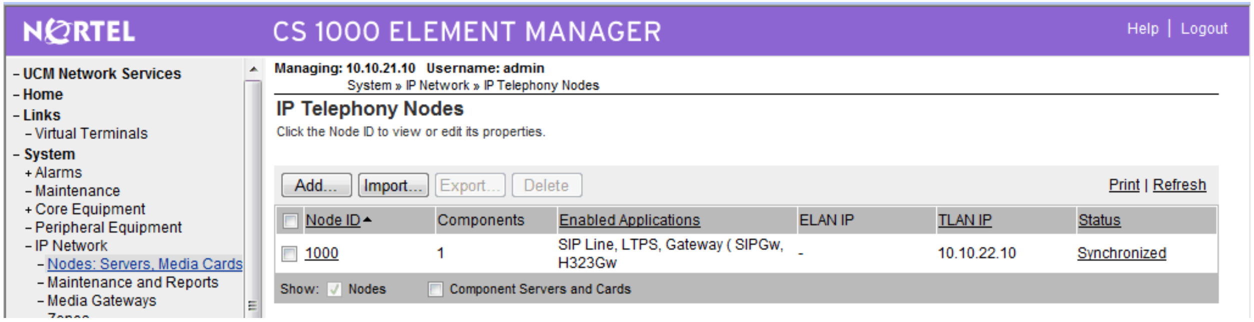
The **Elements** screen is displayed. Click on the **Element Name** of the CS1000 Element.



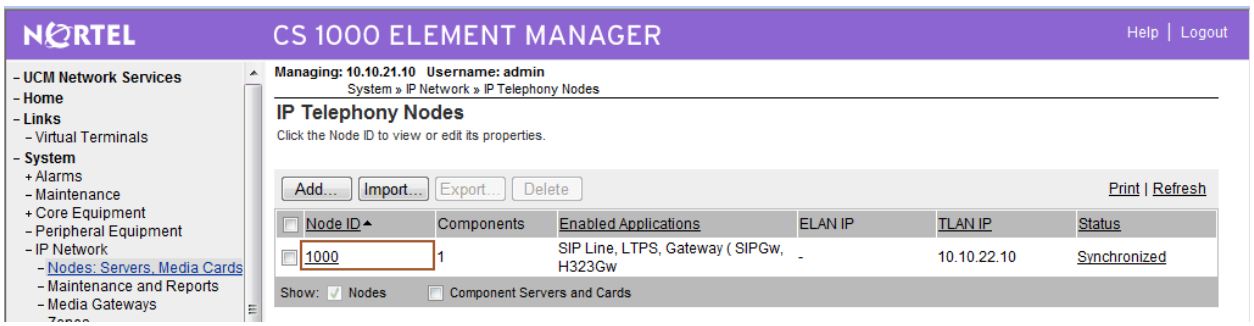
The CS 1000 Element Manager **System Overview** page is displayed.



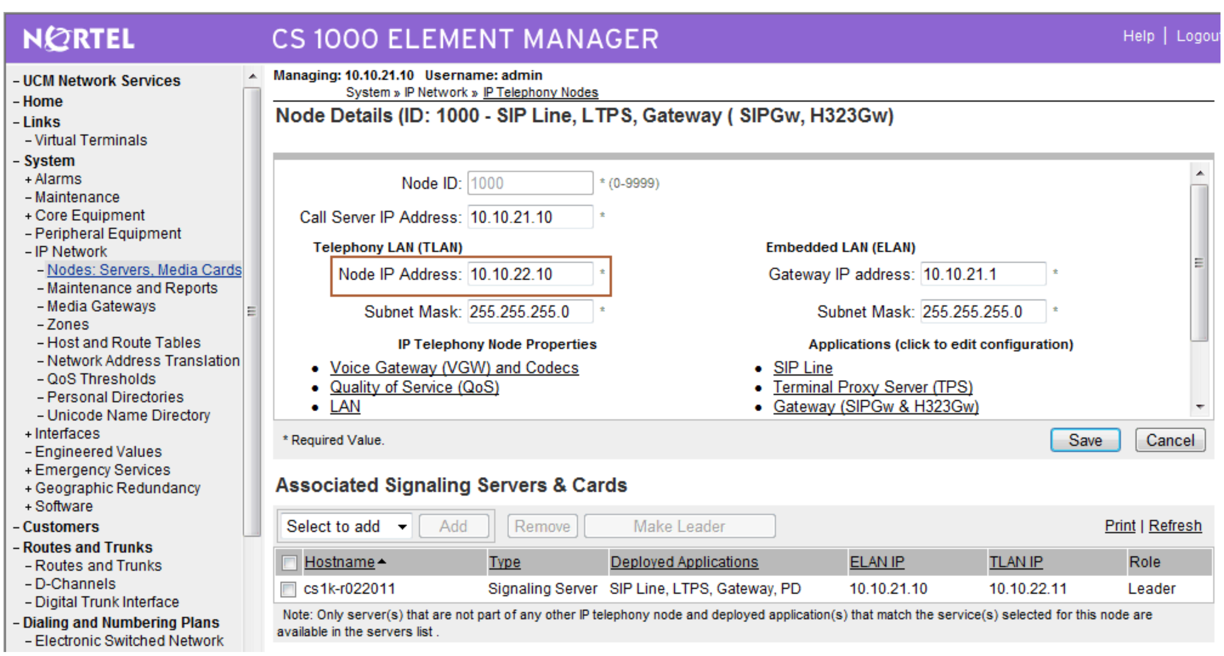
Select IP Network → Nodes: Servers, Media Cards



Click on the **Node ID** of your CS1000 Element.

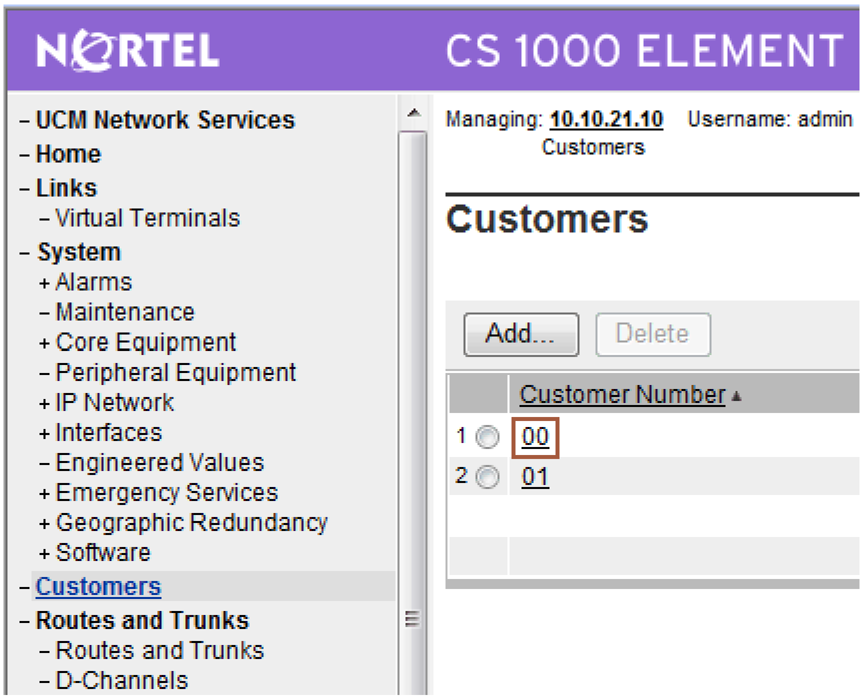


The **Node Details** screen is displayed with the IP address of the CS1000 node. The **Node IP Address** is a virtual address which corresponds to the IP address of the Call Server, Signaling Server, SIP Signaling Gateway and UCM interface. The SIP Signaling Gateway uses the **Node IP Address** as a source address when registering with the SIP Proxy Server (SPS).

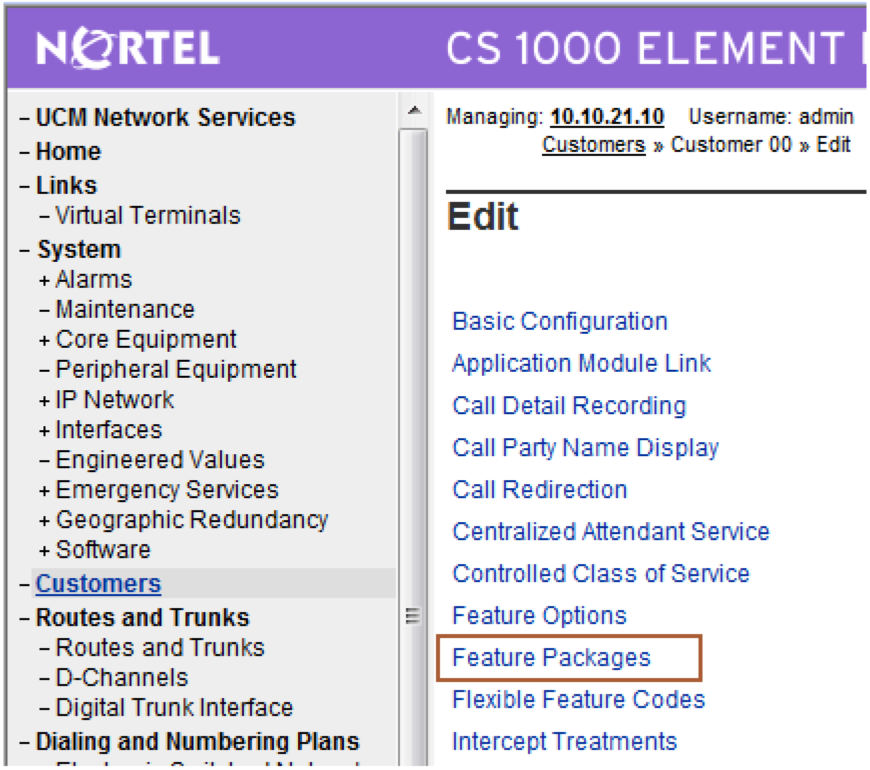


3.3. Administer ISDN

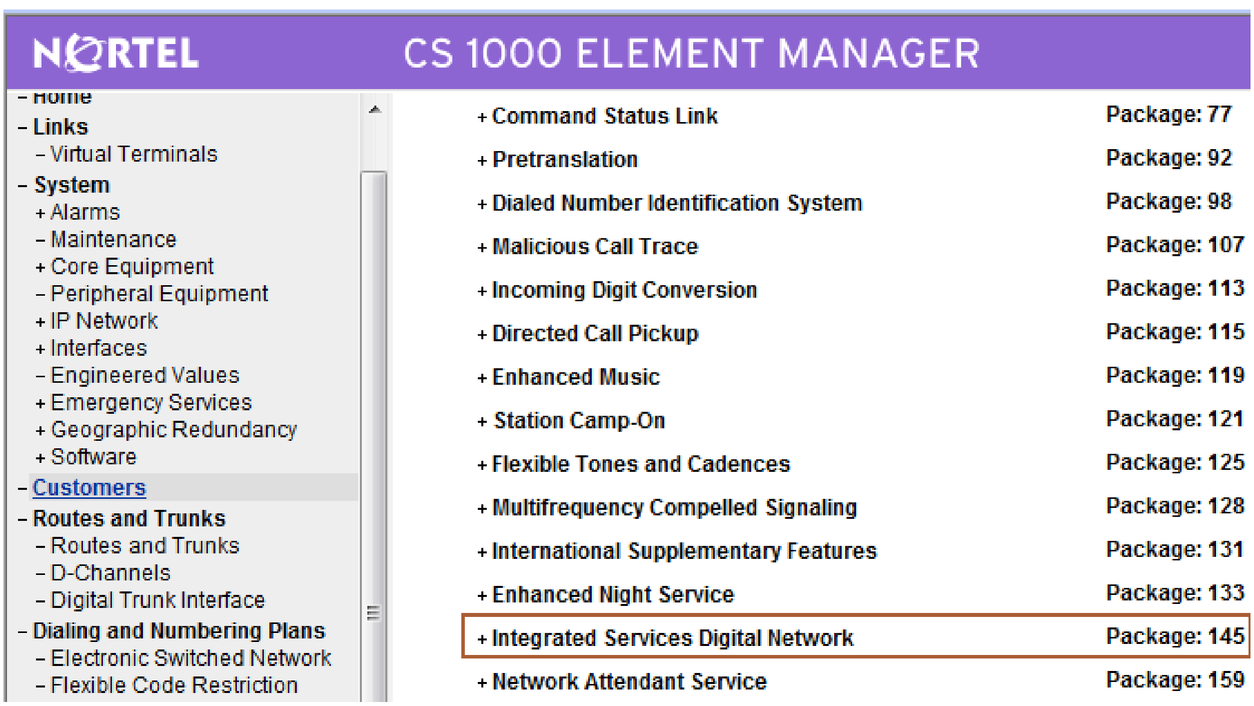
Select **Customers** in the left pane. The **Customers** screen is displayed. Click the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options.



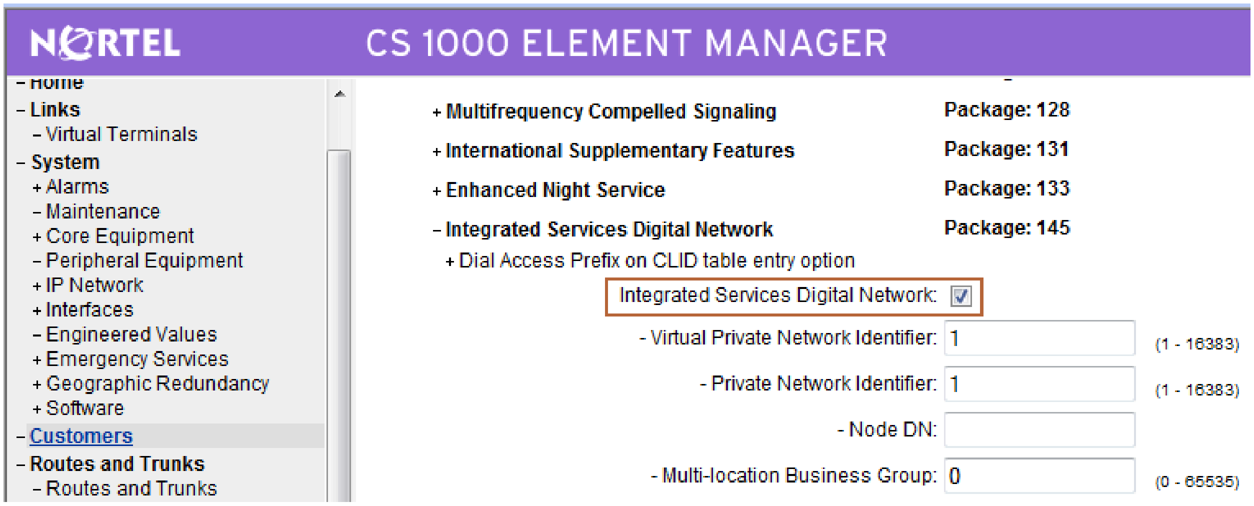
The **Customer 00** screen is displayed next. Select **Feature Packages**.



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.

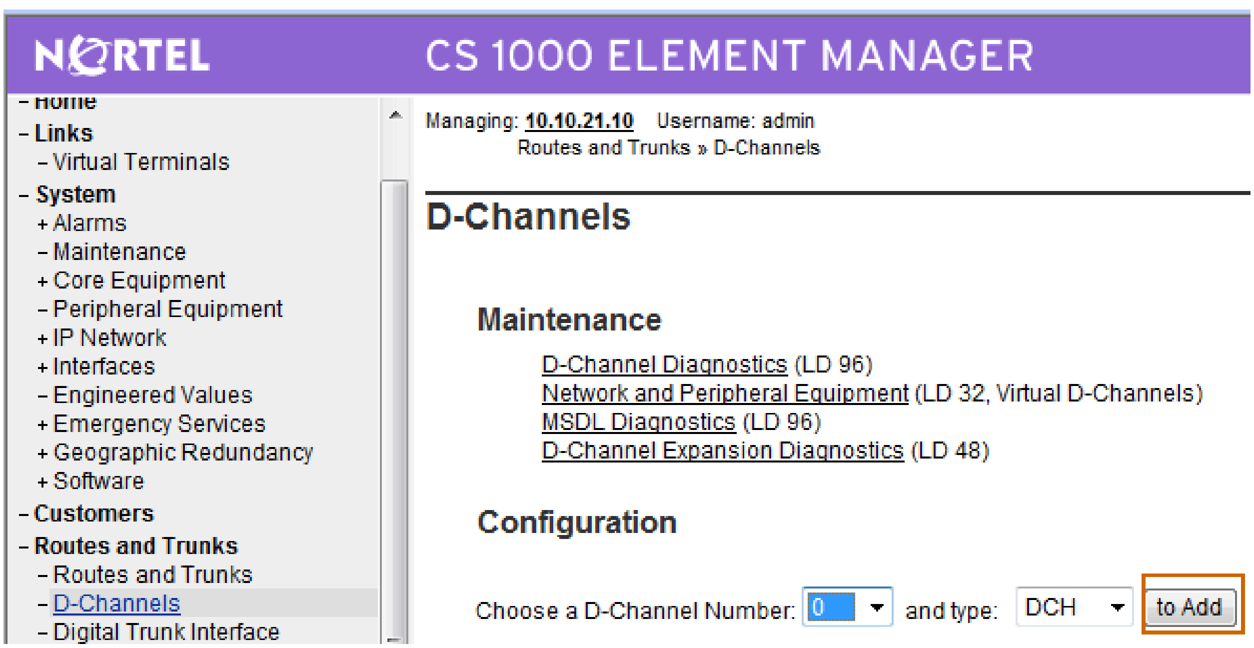


The screen is updated with parameters populated below **Integrated Services Digital Network**. Check the **Integrated Services Digital Network (ISDN)** checkbox, and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click **Save** (not shown).



3.4. Administer a Virtual D-Channel

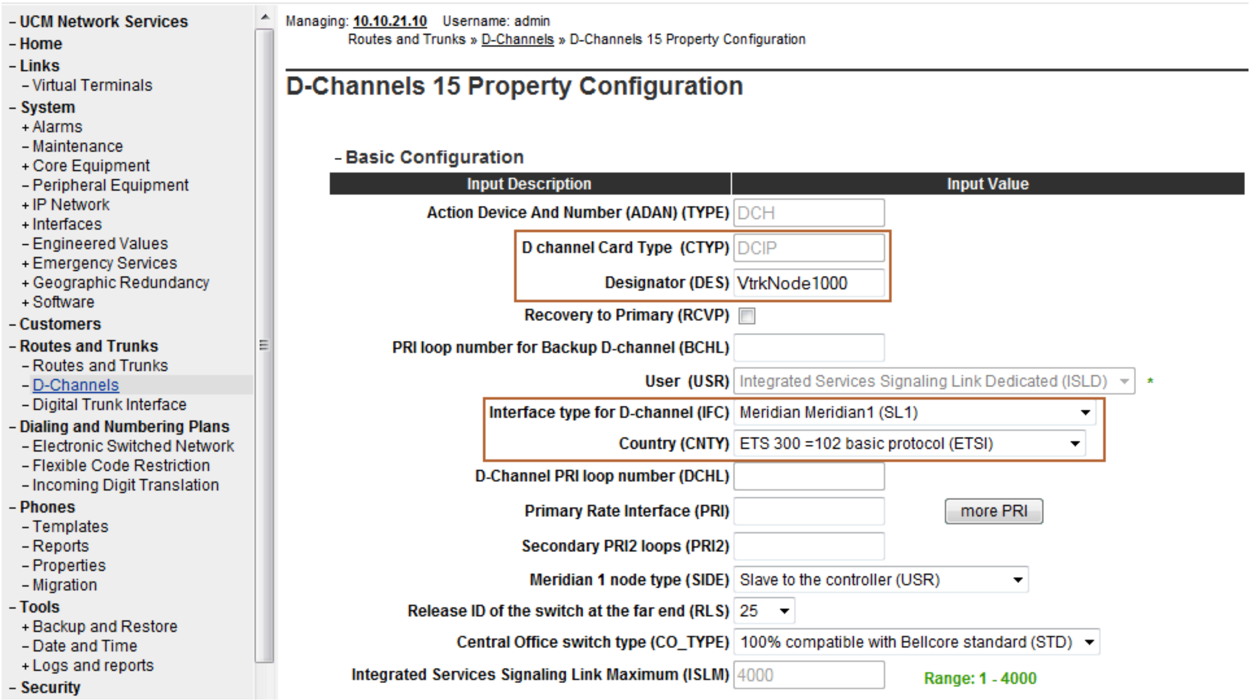
Select **Routes and Trunks → D-Channels** from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list. Click **to Add**.



The **D-Channels 15 Property Configuration** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

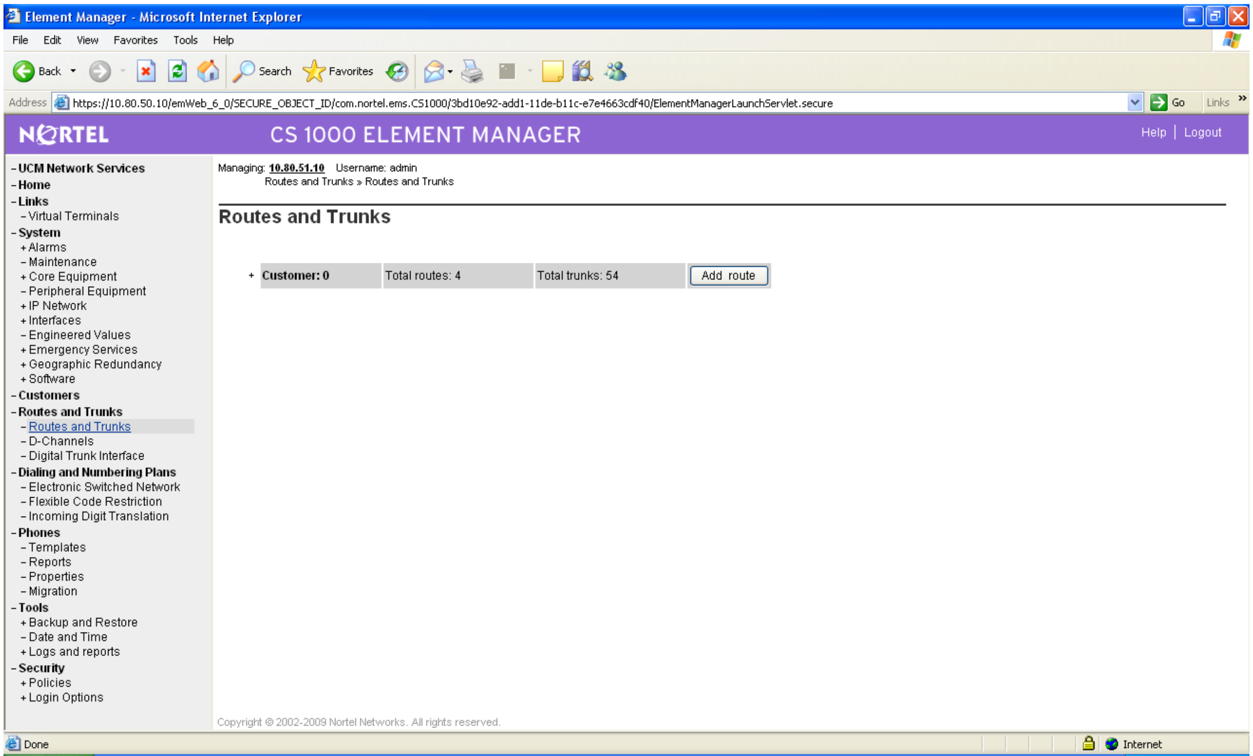
D channel Card Type (CTYP): D-Channel is over IP (**DCIP**)
Designator (DES): A descriptive name.
Interface type for D-channel (IFC): Meridian Meridian1 (SL1)
Country (CNTY): ETS 300 = 102 basic protocol (ETSI)

Click **Submit** (not shown).



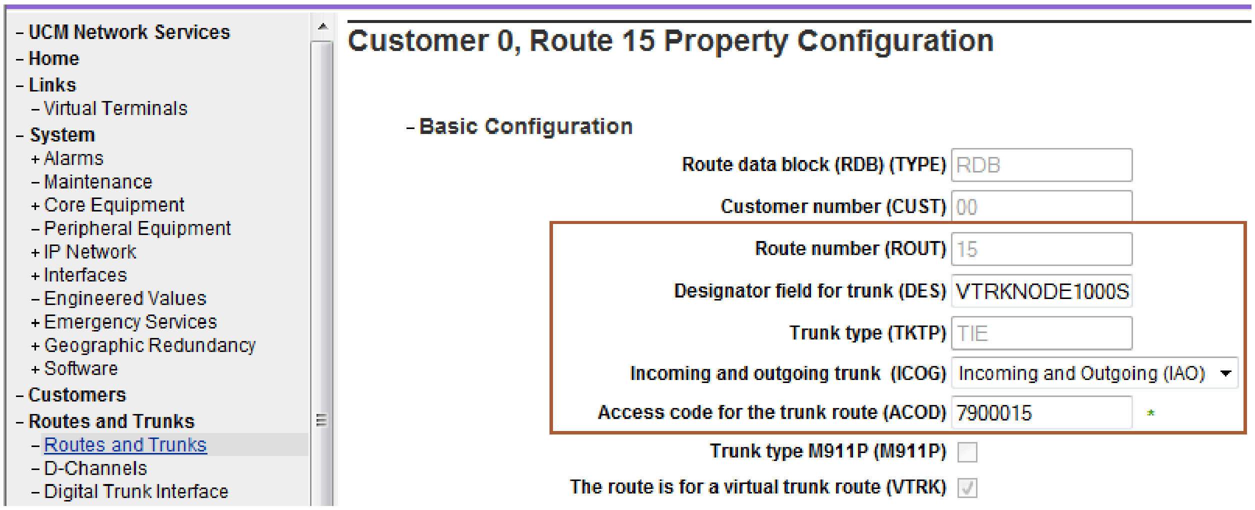
3.5. Administer Virtual SIP Routes and Trunks

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**.

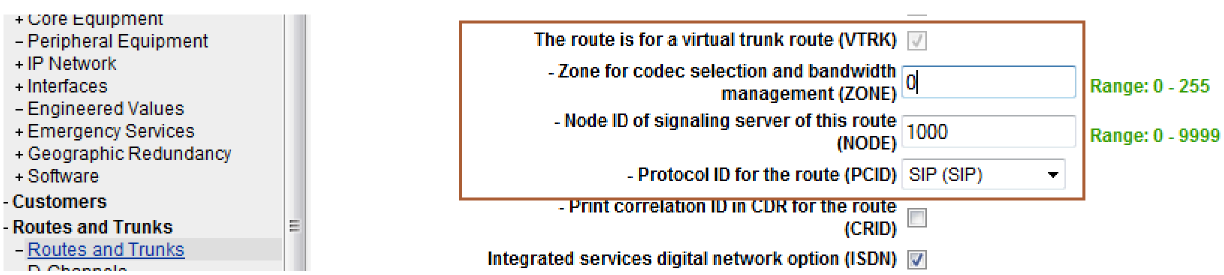


The **Customer 0, New Route Configuration** screen is displayed next. Scroll down until the **Basic Configuration** section is displayed and enter the following values for the specified fields, and retain the default values for the remaining fields.

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

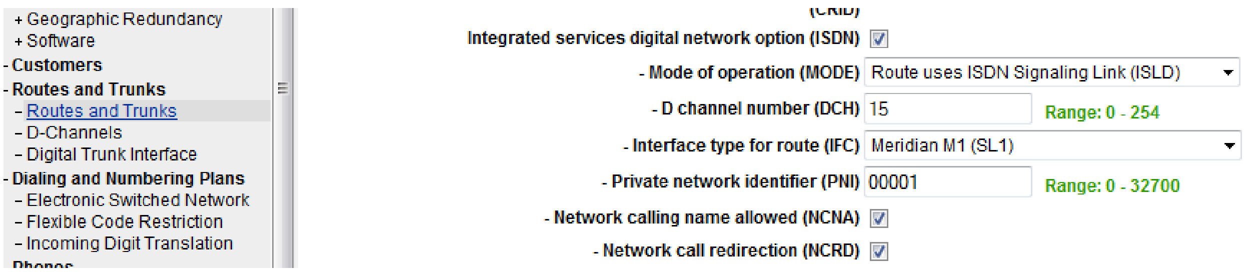


Scroll down the screen, and check the field **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear. For the **Zone for codec selection and bandwidth management (ZONE)** field, enter the default zone number (in this case **0**). For the **Node ID of signaling server of this route (NODE)** field, enter the node number from **Section 3.3**. Select **SIP (SIP)** from the drop-down list for the **Protocol ID for the route (PCID)** field.

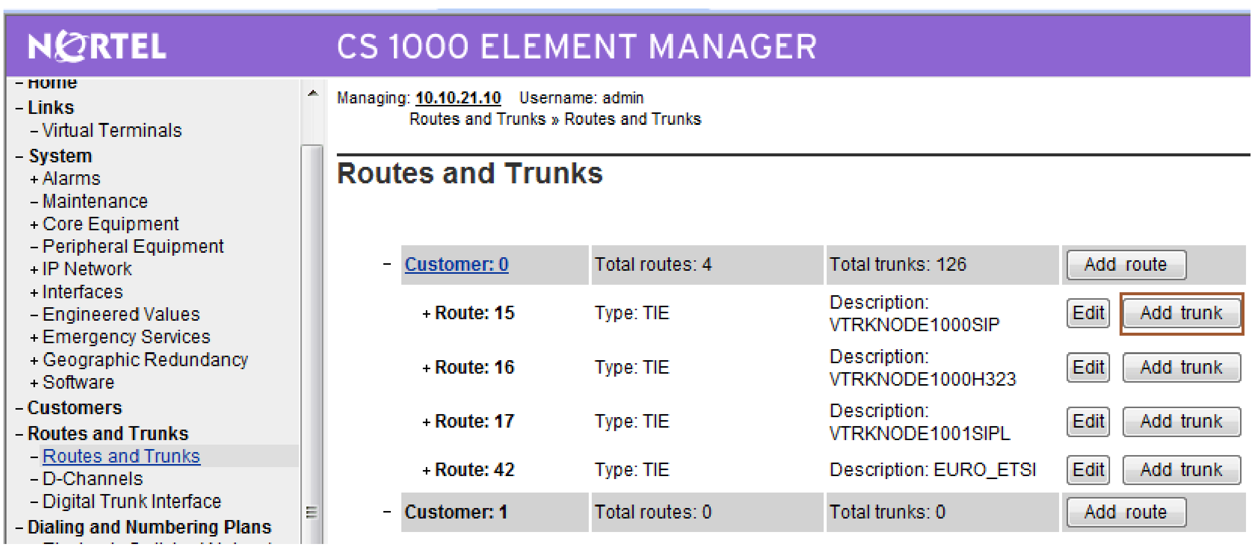


Scroll down the screen, check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click **Submit**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

Mode of operation (MODE):	**Route uses ISDN Signaling Link (ISLD)**
D channel number (DCH):	D-Channel number from **Section 3.4**
Network calling name allowed (NCNA):	Check the field
Network call redirection (NCRD):	Check the field

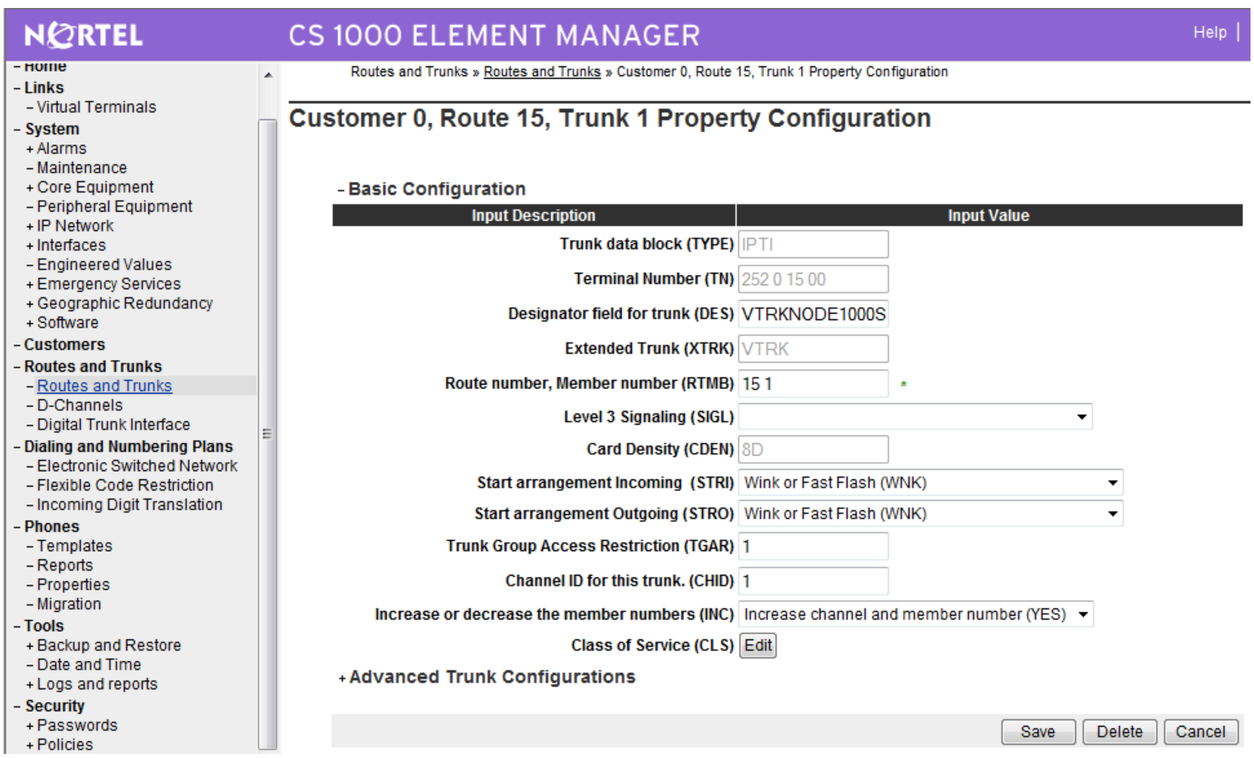


The **Routes and Trunks** screen is displayed again, and updated with the newly added route. Click the **Add trunk** button next to the newly added route.



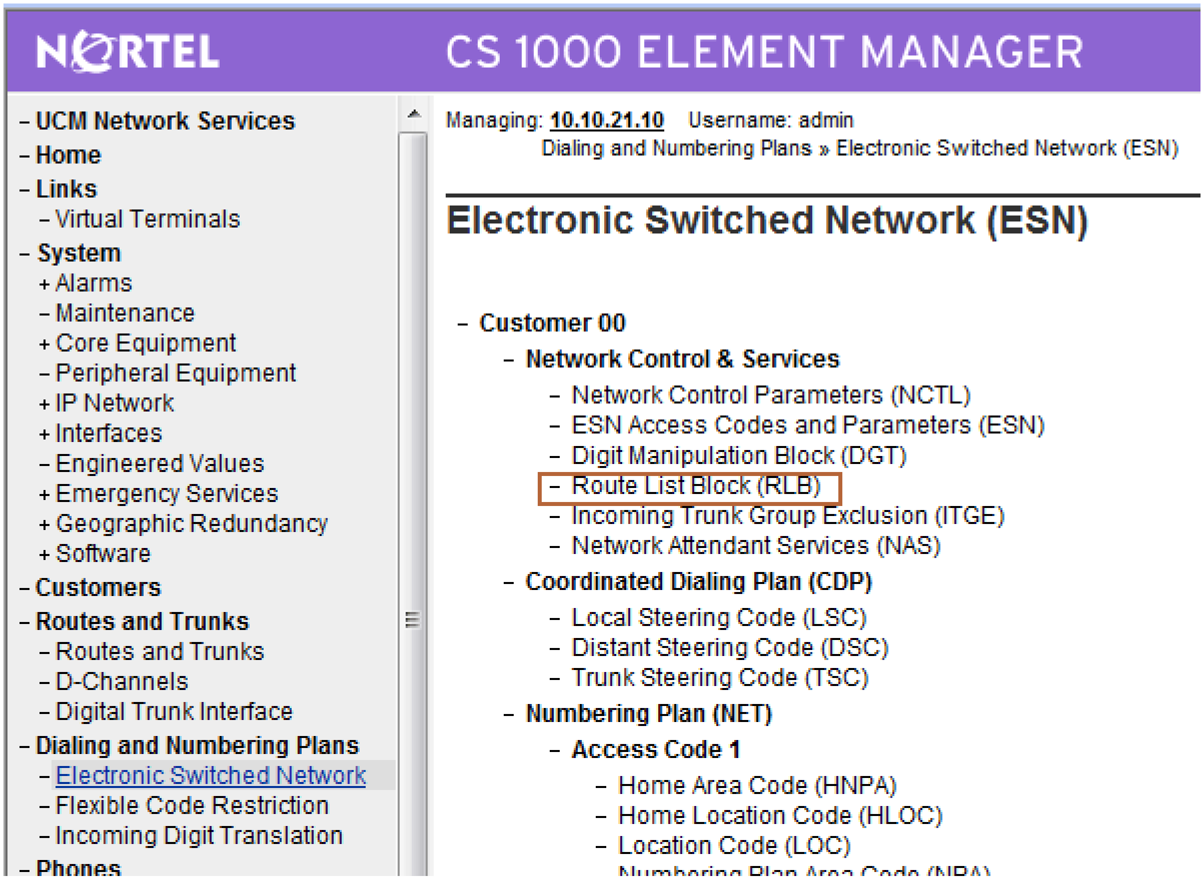
The **Customer 0, Route 15, Trunk 1 Property Configuration** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click **Save**. The **Multiple trunk input number (MTINPUT)** field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. 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
Card Density:	Select **8D**
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.

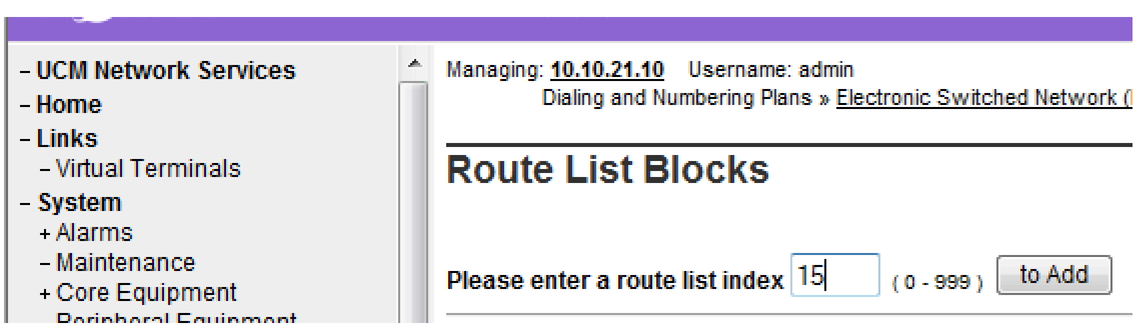


3.6. Administer Route List Block and Distant Steering Code

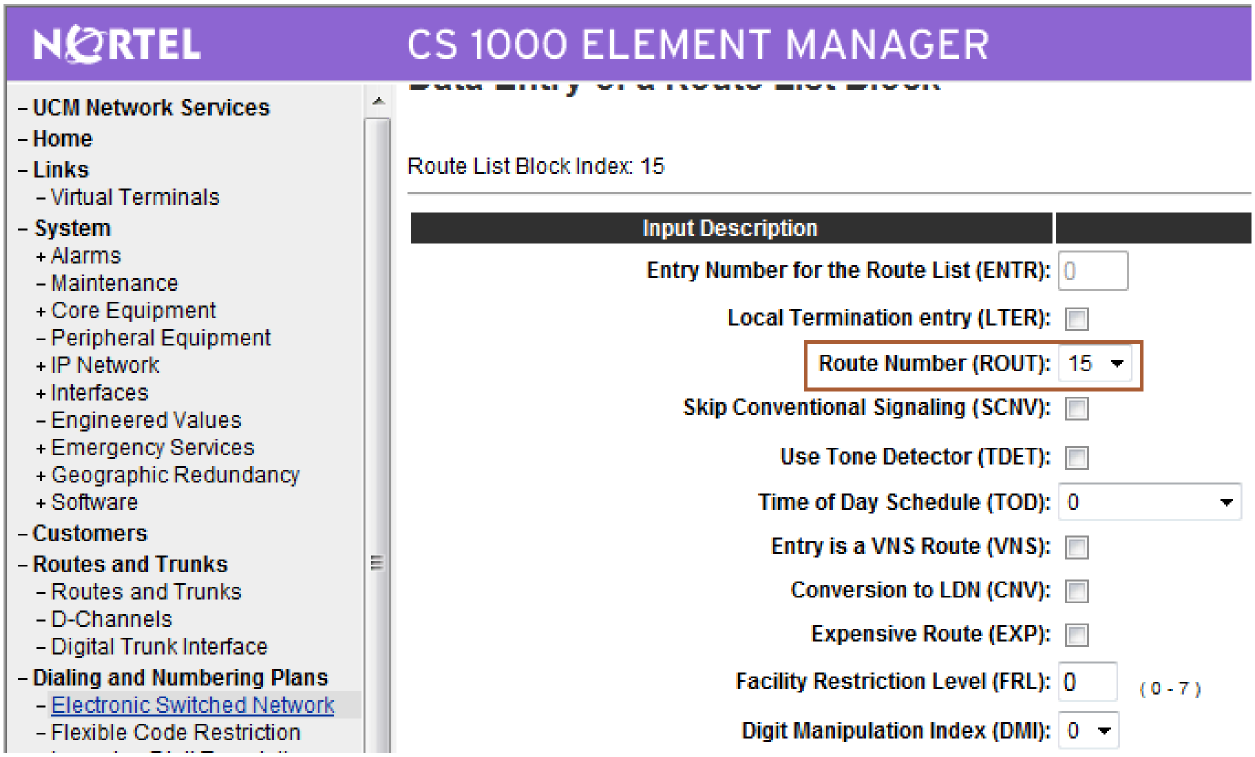
Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block (RLB)**.



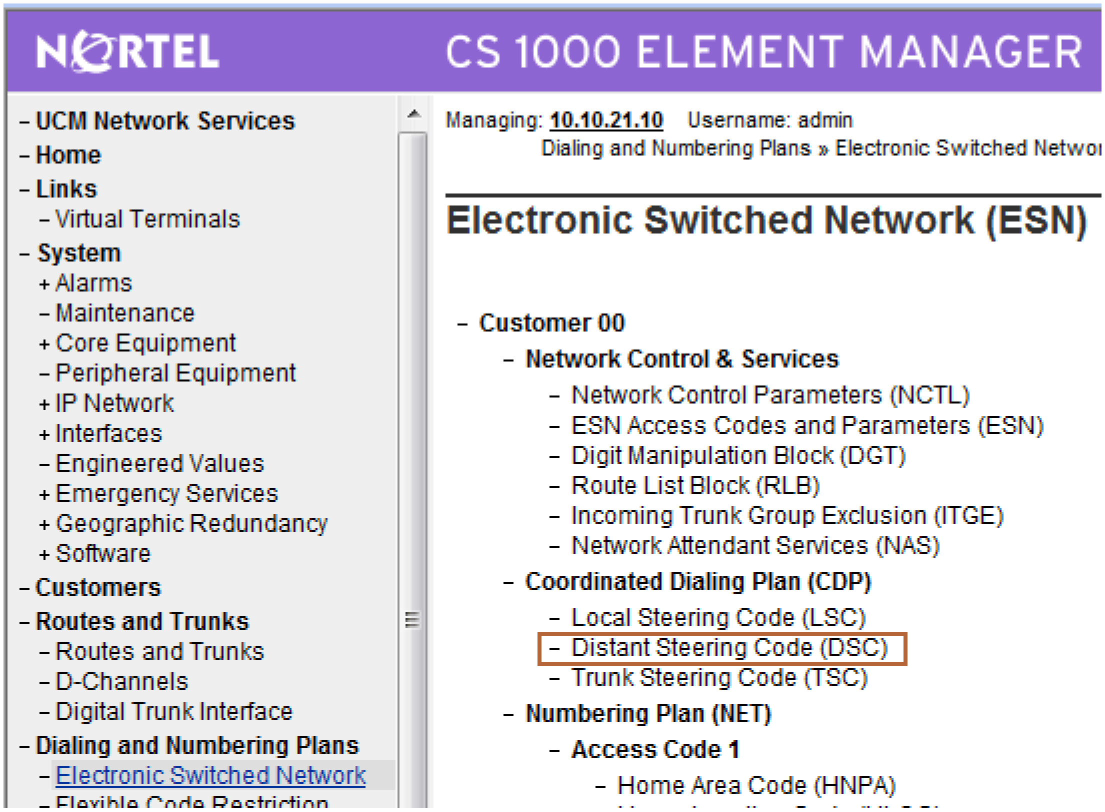
The **Route List Blocks** screen is displayed. In the **Please enter a route list index** field, enter an available route list block number (in this case **15**). Click **to Add**.



The **Route List Block** screen is displayed with a listing of parameters. For the **Route Number (ROUT)** field, select the route number from **Section 3.6**. Retain the default values for the remaining fields, and scroll down to the bottom of the screen and click **Submit** (not shown).



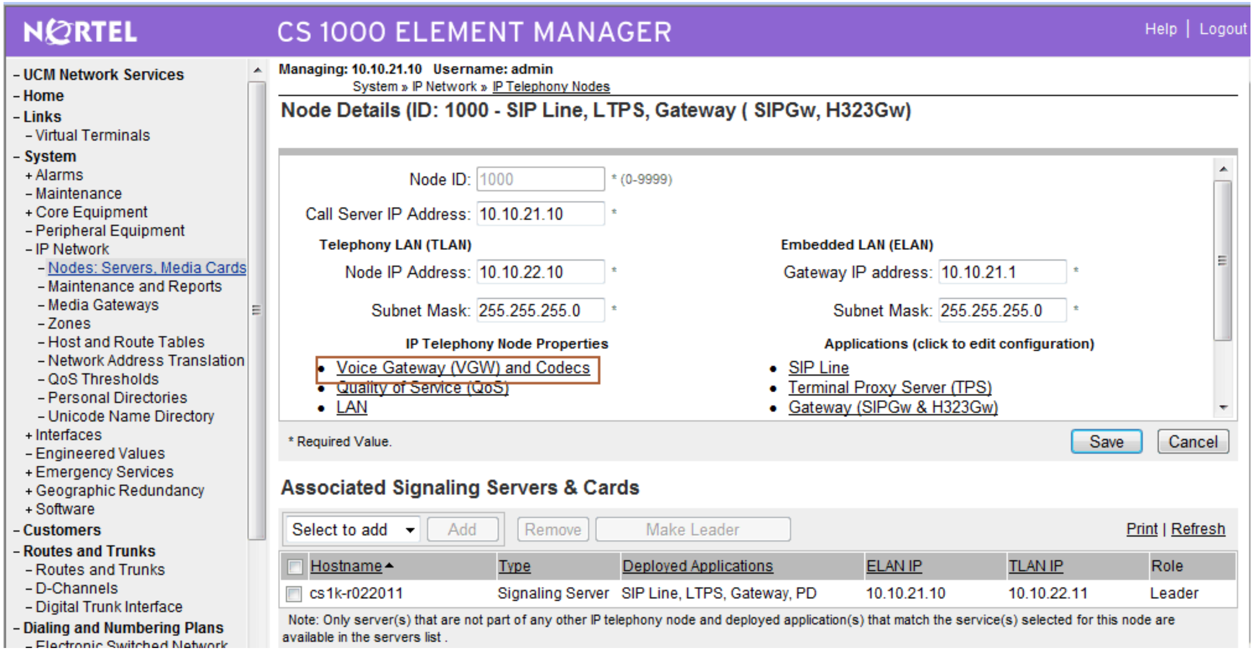
Select **Dialing and Numbering Plans → Electronic Switched Network** again from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Distant Steering Code (DSC)** to add an entry to route 11111 calls to Avaya Meeting Exchange Application Server.



The **Distant Steering Code List** screen is displayed next (not shown). In the **Please enter a distant steering code** field, enter the dialed prefix digits to match on (in this case **111**) as the conference access number is 44444. Click **to Add**.

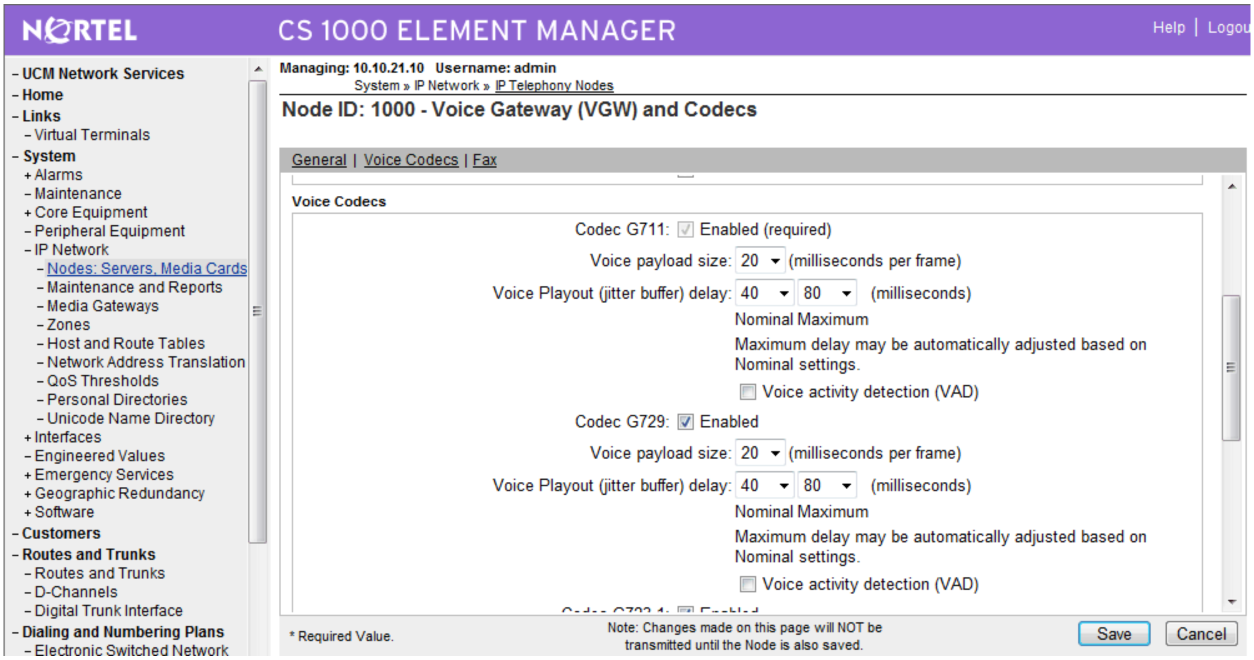
3.7. Administer Node SIP and Media Parameters

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 3.2**). The **Node Details** screen is displayed. Click on **Voice Gateway (VGW) and Codecs**.

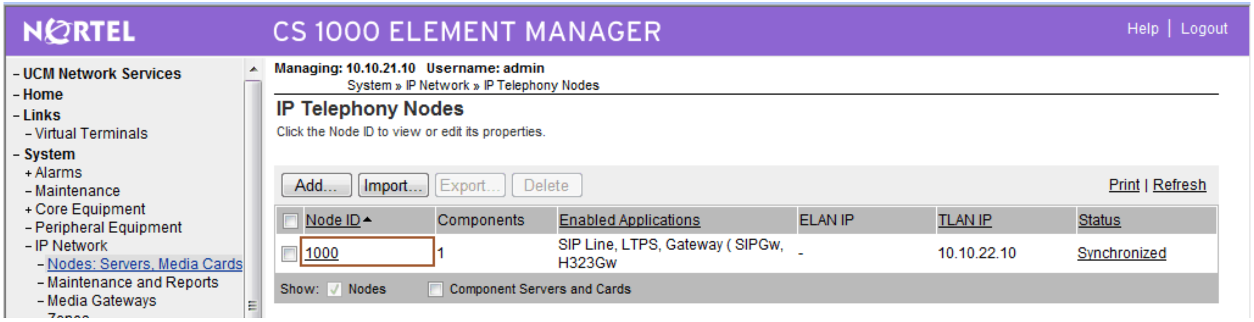


Solution & Interoperability Test Lab Application Notes

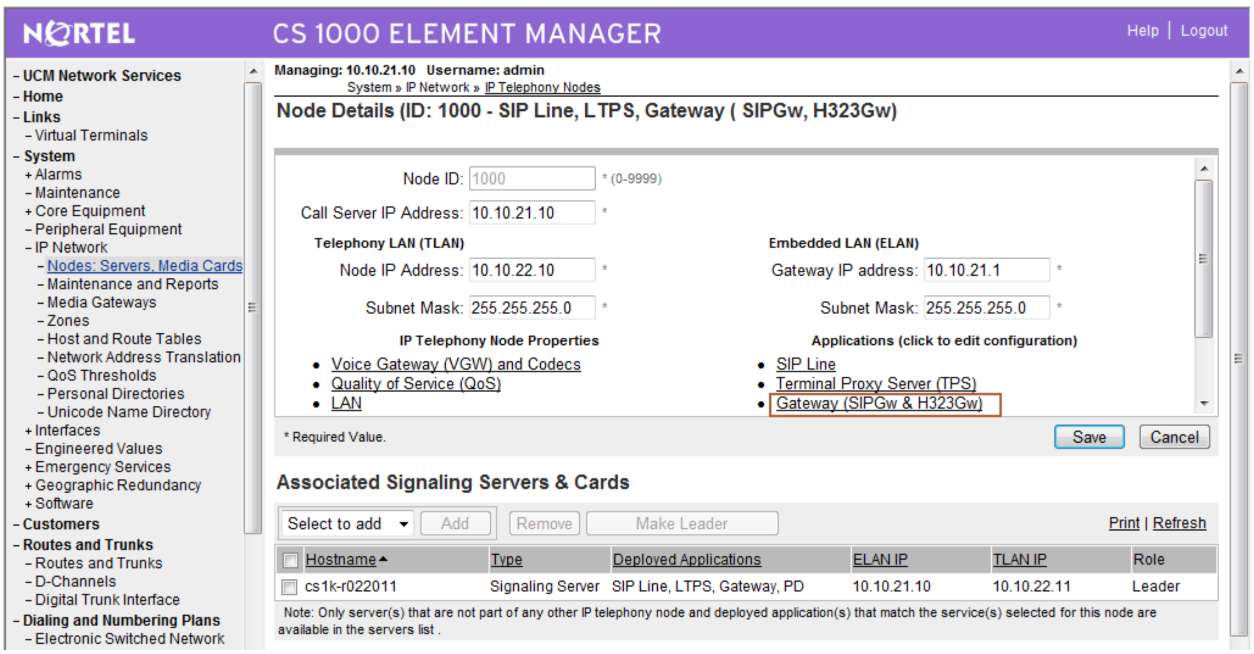
In the following screen scroll down the parameters box and check the desired codecs under **Voice Codecs.** Note that G.711 and G.729 were verified for the sample configuration. G.711 is checked by default and cannot be unchecked. Click on **Save**.



Select **IP Network → Nodes: Servers, Media Cards.** Click the **Node ID** of the Avaya CS1000 Element (in this case **1000**).

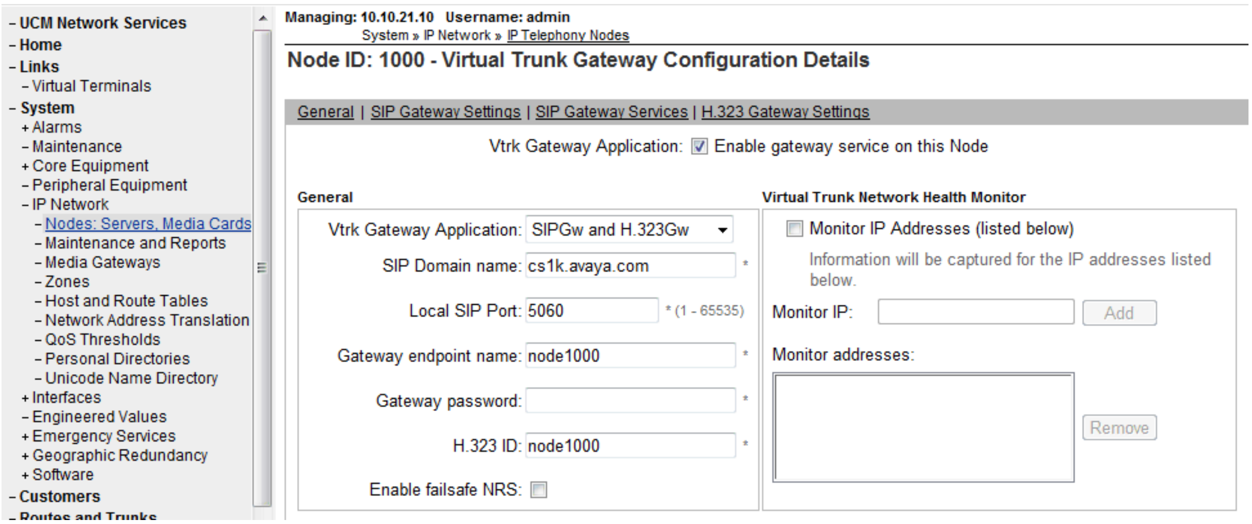


On the **Node Details** screen select **Gateway (SIPGw & H323Gw)**



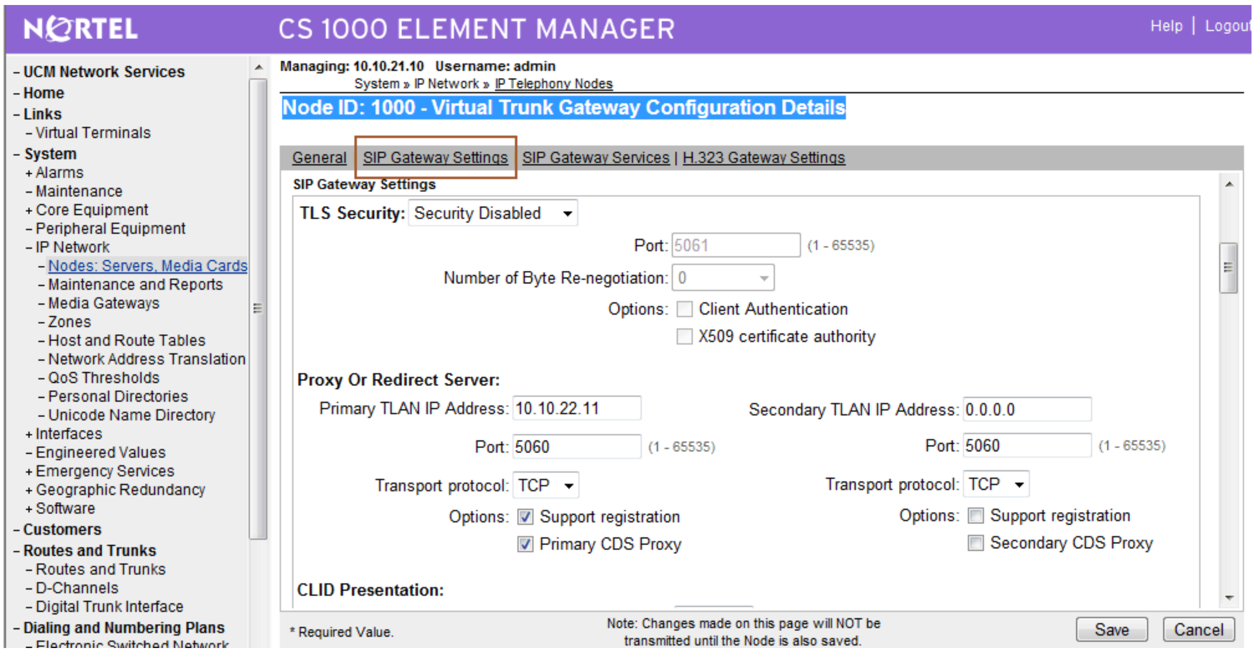
Under **General** of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values for the specified fields, and retain the default values for the remaining fields.

Vtrk Gateway Application:	Select **SIPGw and H.323Gw**
SIP Domain Name	Domain name used for constructing the SIP URI in SIP messages (in this case **cs1k.avaya.com**)
Local SIP Port	**5060**
Gateway endpoint name	An appropriate name



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.

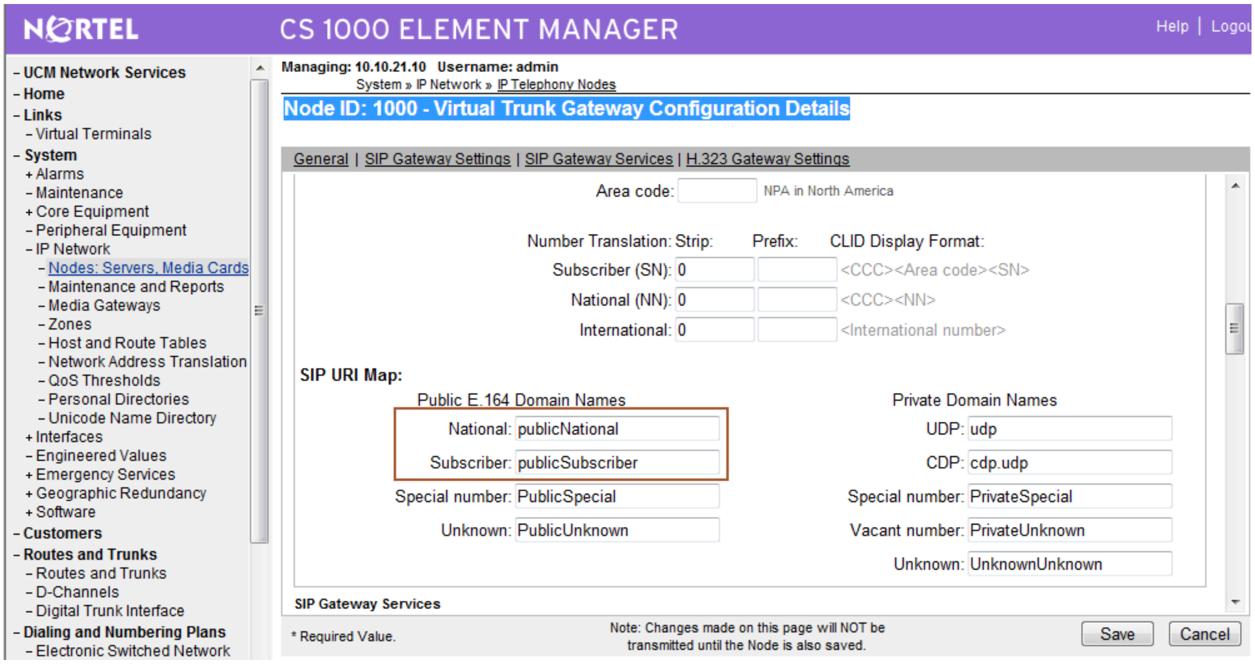
Primary TLAN IP Address:	The IP address of the Signaling Server noted in **Section 3.2**.
Port	**5060**
Transport Protocol	**TCP**
Options	Check **Support registration** and **Primary CDS Proxy**



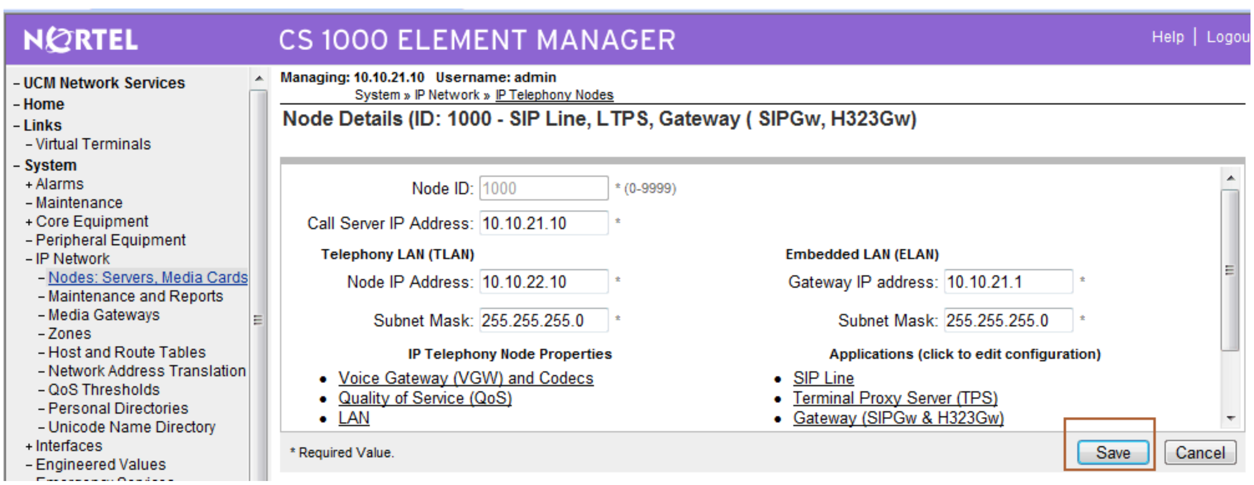
Scroll down the parameters box to the **SIP URI Map** section. Under **Public E.164 Domain Names** heading**,** for

National Enter **publicNational**
Subscriber Enter **publicSubscriber**

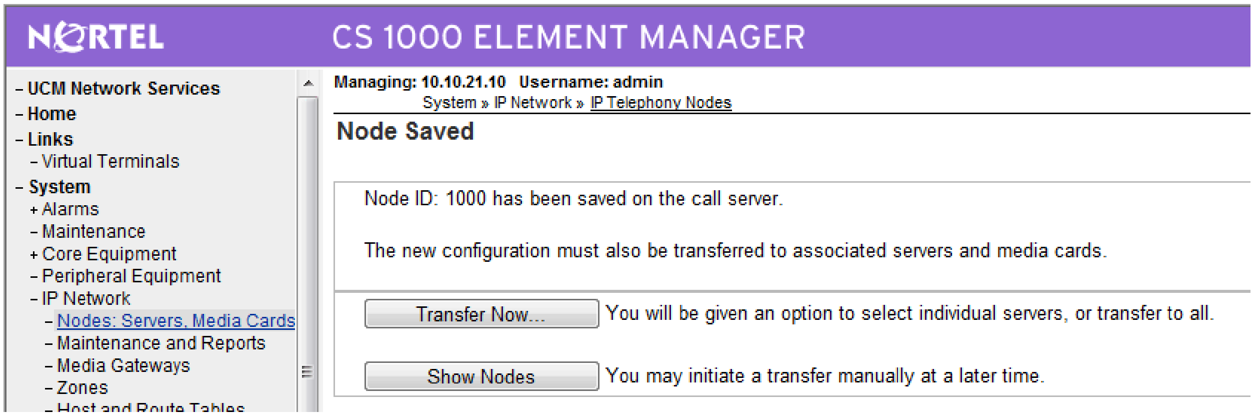
The remaining fields can be left at their default values. Click on **Save**.



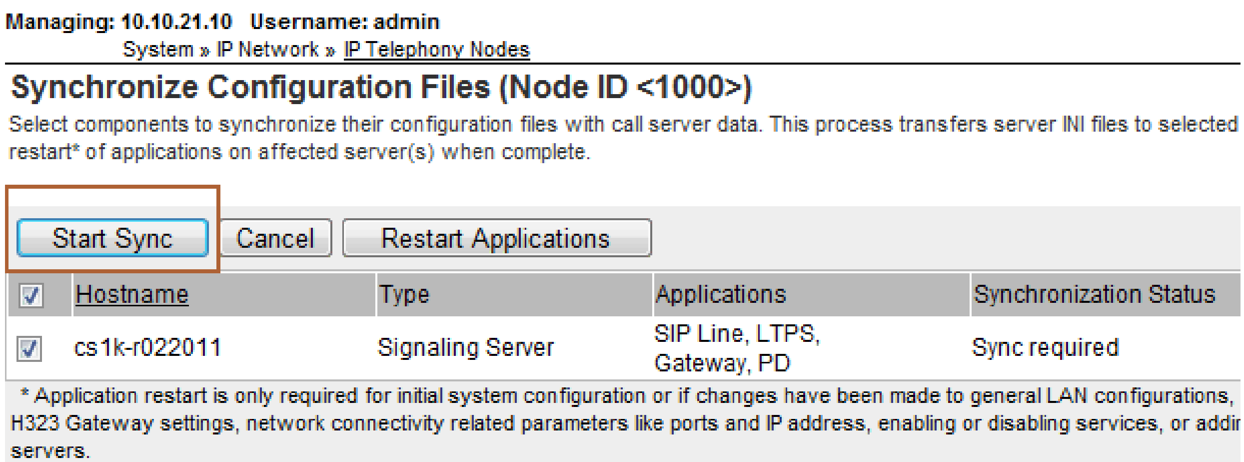
Return to the **Node Details** screen and click **Save**, as shown below.



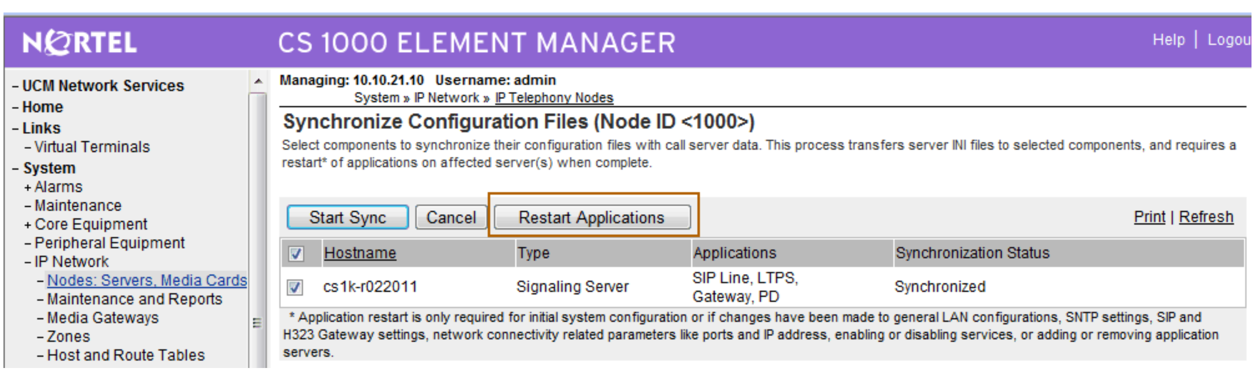
The **Node Saved** screen is displayed. Click **Transfer Now…**



The **Synchronize Configuration Files** screen is displayed. Select the Signaling Server and click on **Start Sync**.

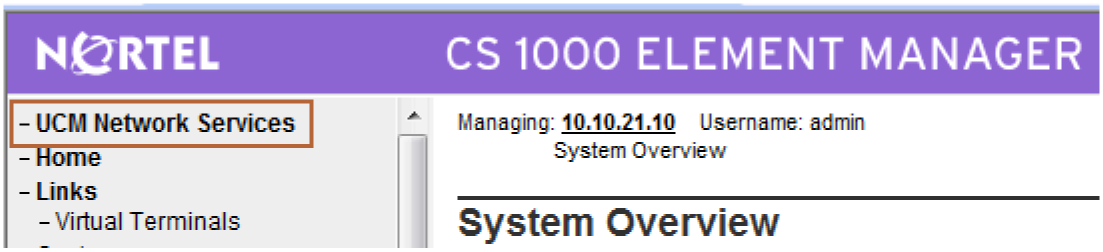


When the synchronization completes, click on **Restart Applications**.

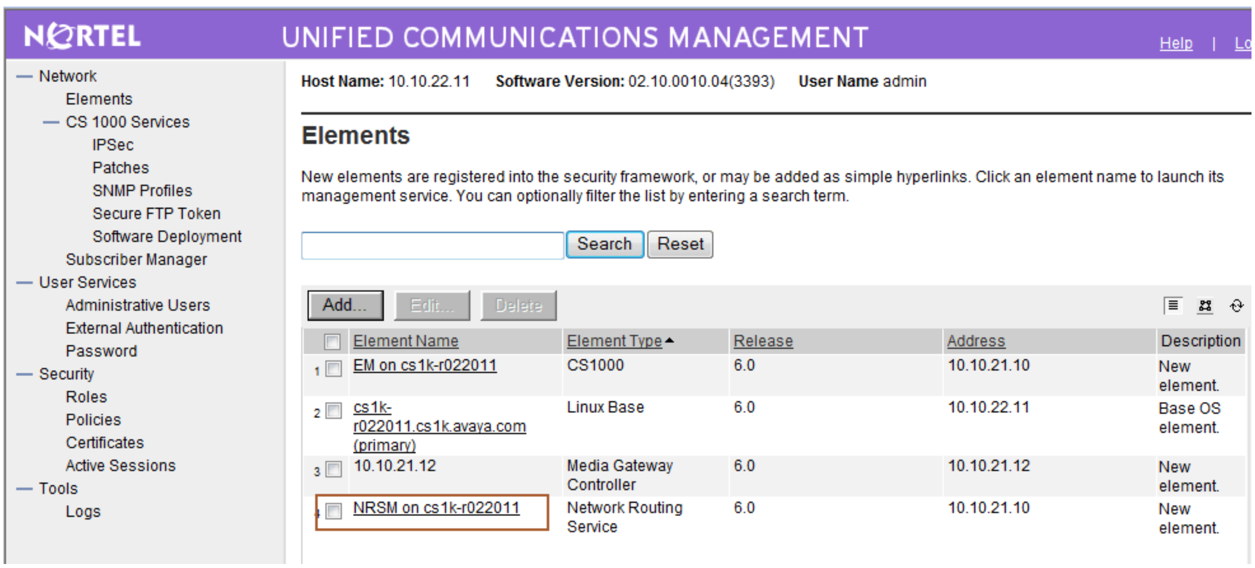


3.8. Launch NRS Manager

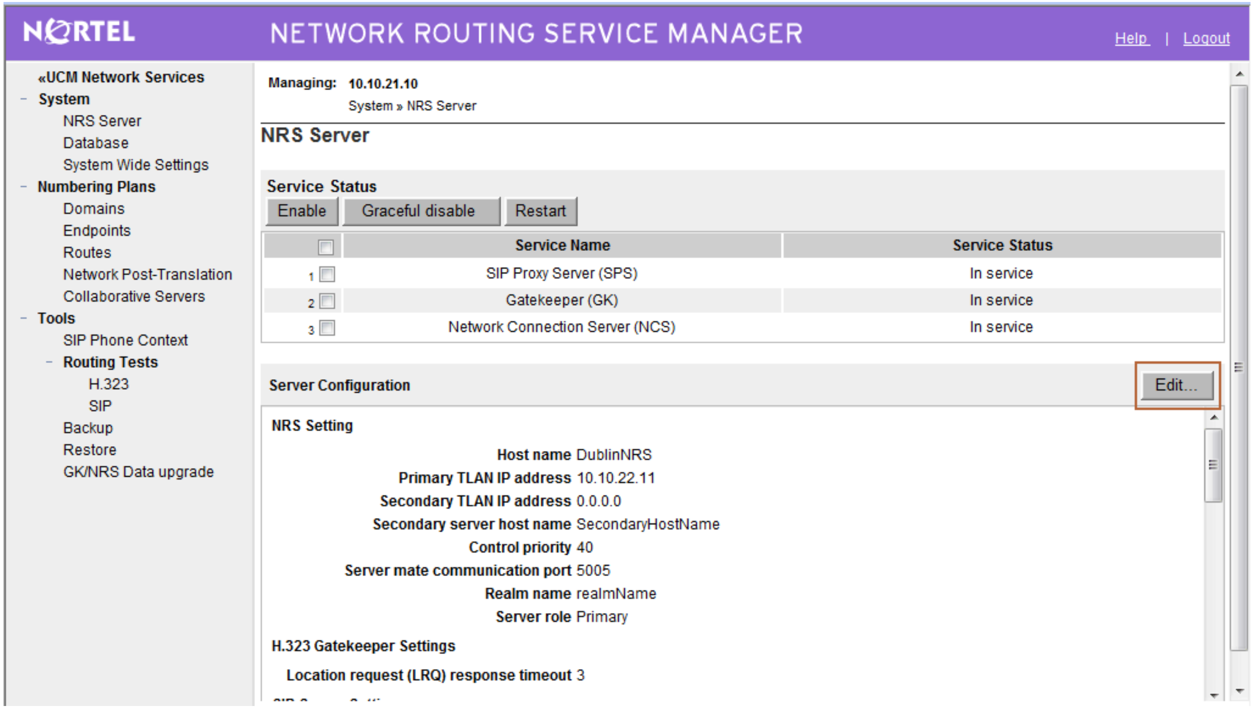
Select **UCM Network Services** from the left pane, which will display the high level **Unified Communications Management** screen.



Click on the **Element Name** with **Element Type** “Network Routing Service”



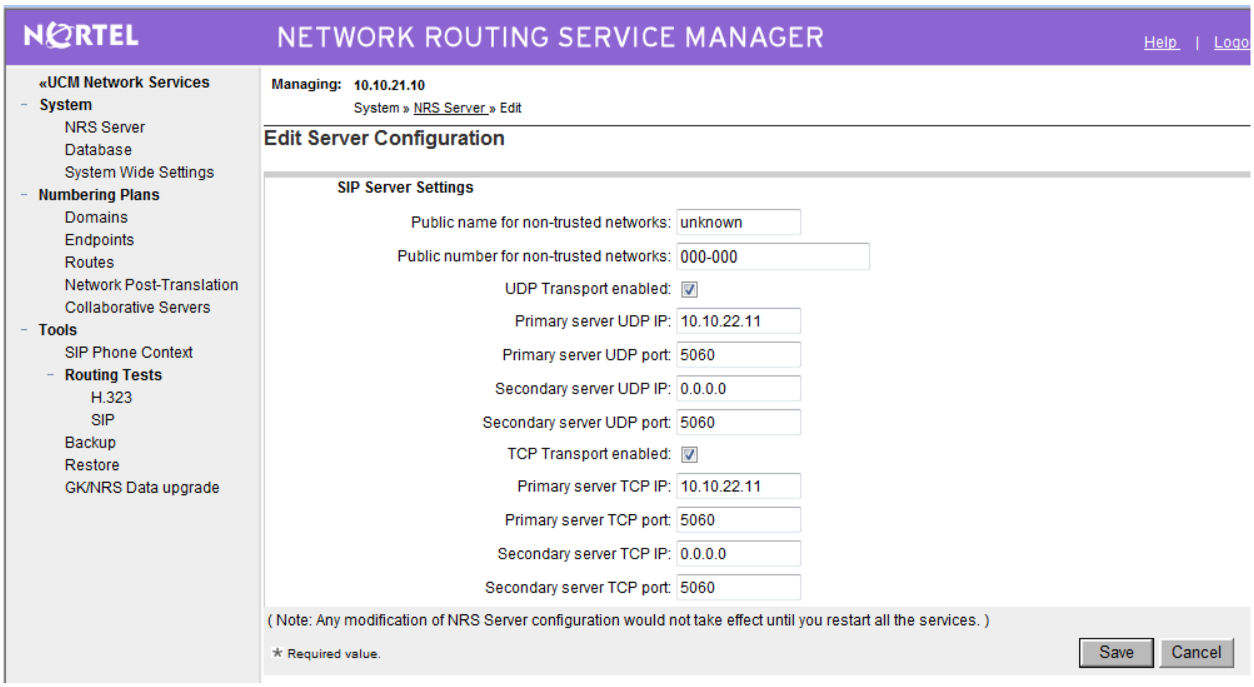
The **NRS Server** screen is displayed. Click **Edit**.



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).
NOTE: For the scenario described in these Application Notes, SIP communication between the CS1000E and Meeting Exchange utilizes TCP.

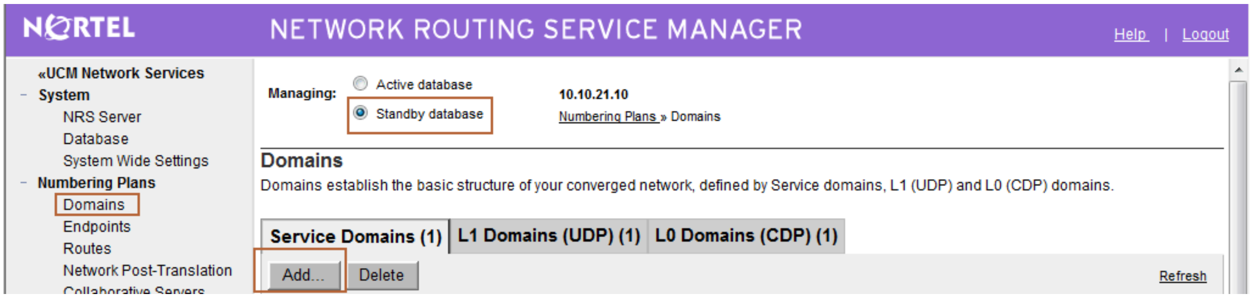
TCP transport enabled:	Check the checkbox
Primary Server TCP IP:	Type the IP address of the Avaya SPS/NRS **.** All outgoing SIP messages from the Avaya SPS/NRS will use this address in the source field of the IP Header
Primary Server TCP port:	**5060**

Click on **Save**.

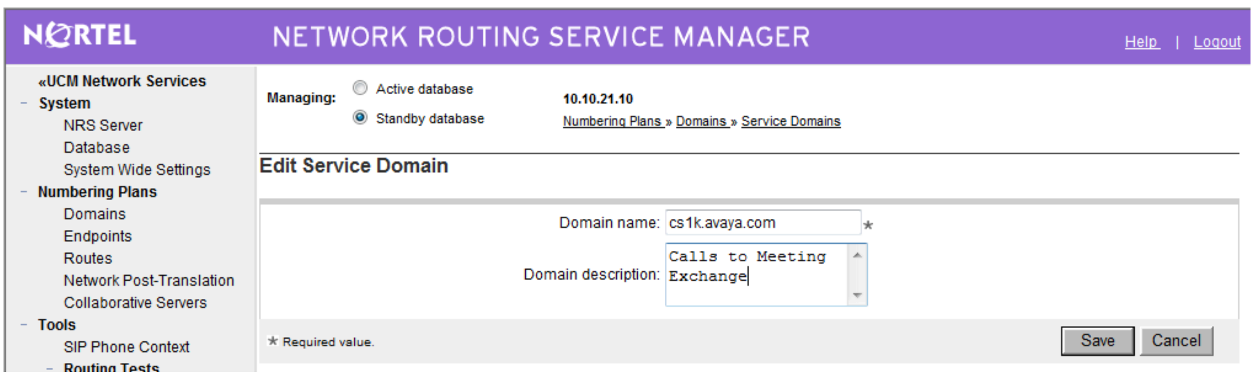


3.9. Administer Service Domain

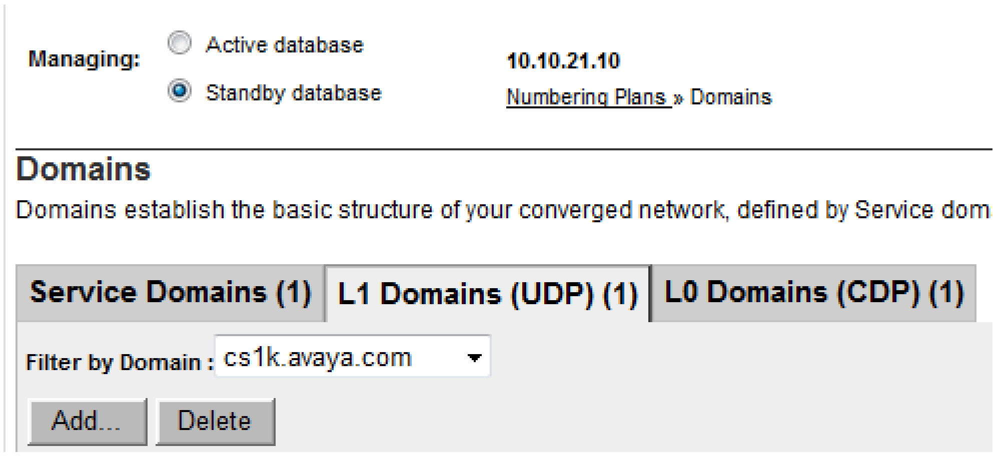
The NRS hosts an active and a standby database. The active database is used for runtime queries, and the standby database is used for administrative modifications. Under **Numbering Plans** on the left, click on **Domains**, and the **Domains** screen will be displayed. To add a domain, first click on 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.



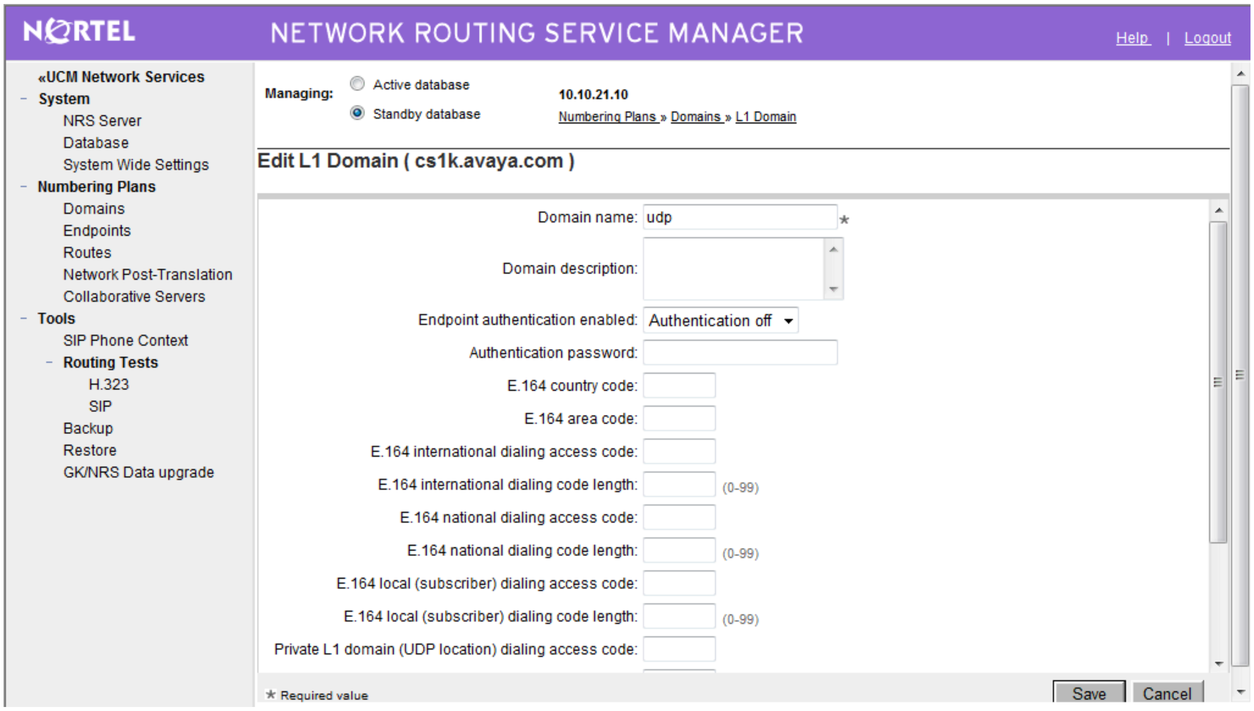
The **Add Service Domain** screen is displayed. Enter the SIP domain name from **Section 3.8** into the **Domain name** field, and a descriptive text for the **Domain description** field. Click **Save**.



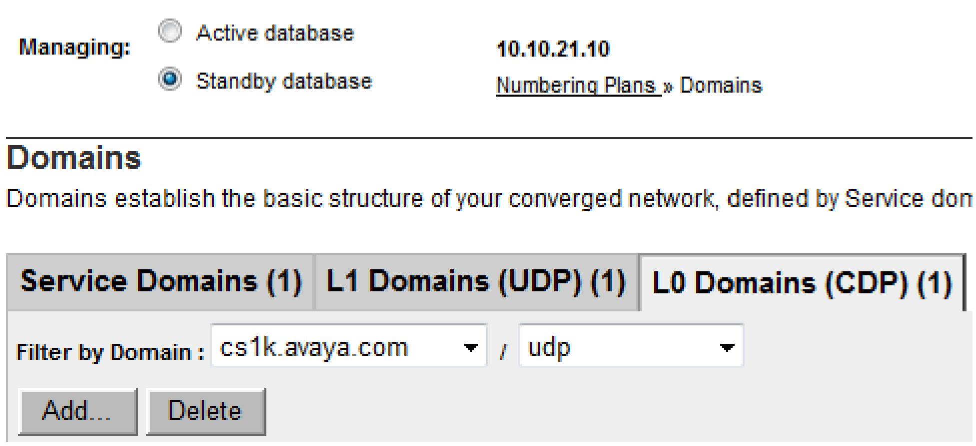
Select the **L1 Domains (UDP)** tab. Select the service domain just created for **Filter by Domain**, and click on **Add** to add a new L1 domain. The L1 and L0 domains are building blocks of the phone context for private addresses. For more information on L1 and L0 domains, refer to the Nortel documentation in **Section 9**.



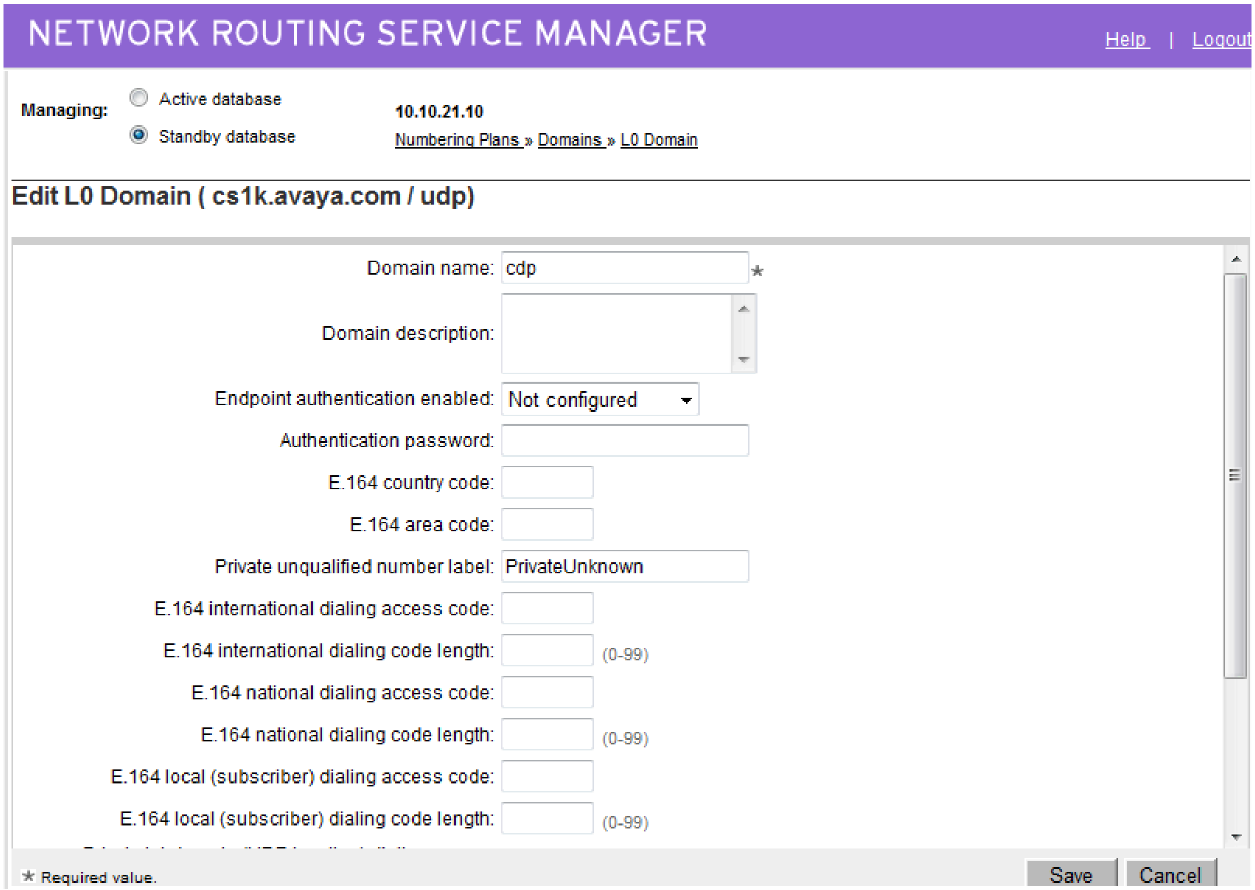
The **Add L1 Domain (cs1k.avaya.com)** screen is displayed next (not shown). Enter a descriptive **Domain name** and **Domain description**. Retain the default value in the remaining fields, and click on S**ave**.



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

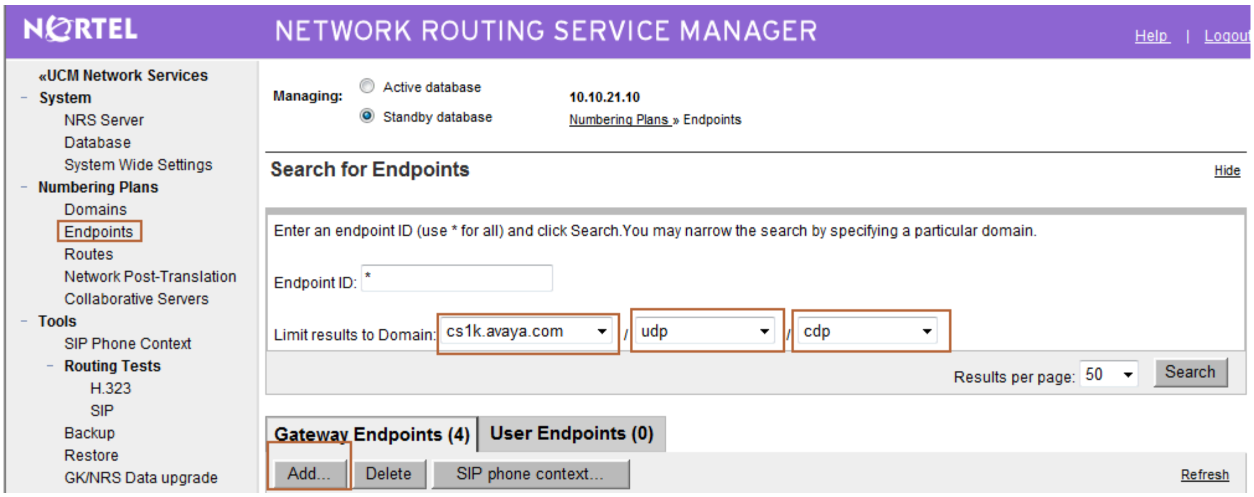


The **Add L0 Domain (cs1k.avaya.com /udp)** screen is displayed next, (not shown). Enter a descriptive **Domain name** and **Domain description**. Retain the default values in the remaining fields and click **Save**.

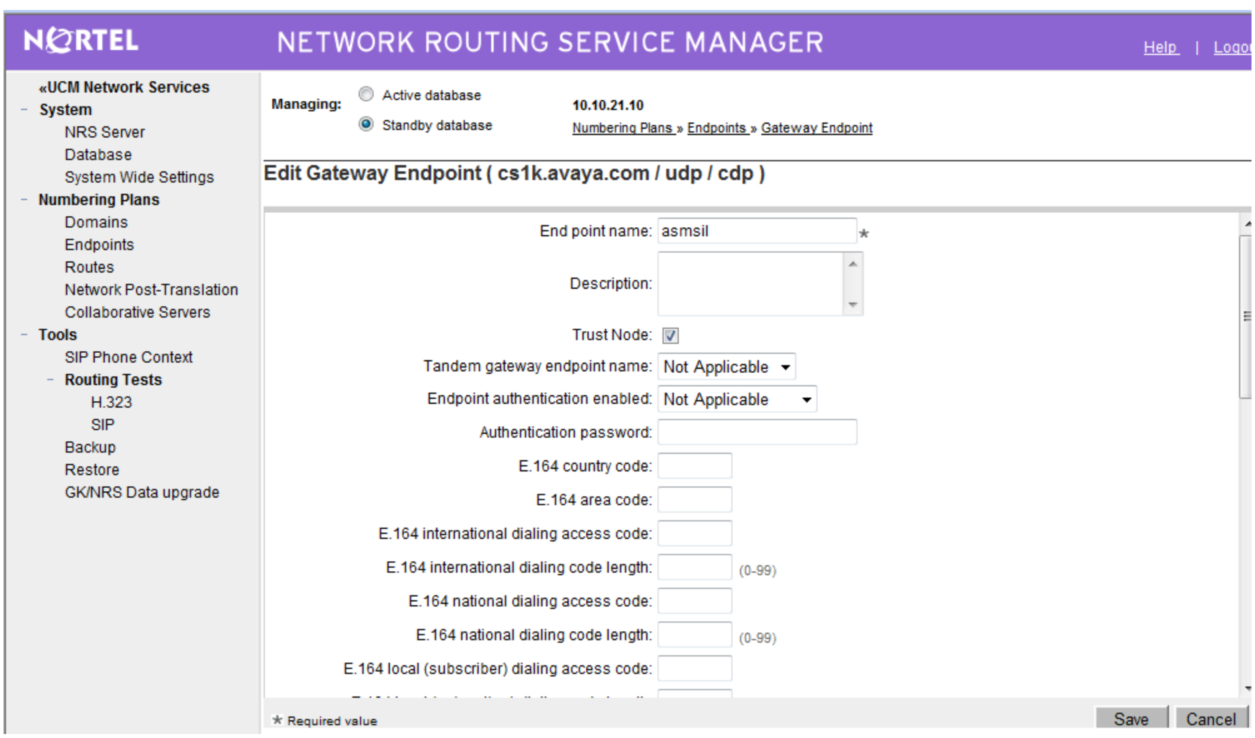


3.10. Administer SIP Signaling Gateway Endpoints

Next, configure two SIP Signaling Gateway endpoints - one for the Avaya Meeting Exchange Application Server and another for the Avaya SIP Signaling Gateway. 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 (**cs1k.avaya.com**), **udp** and **cdp**. Click **Add** to add a new gateway endpoint for Meeting Exchange Application Server.



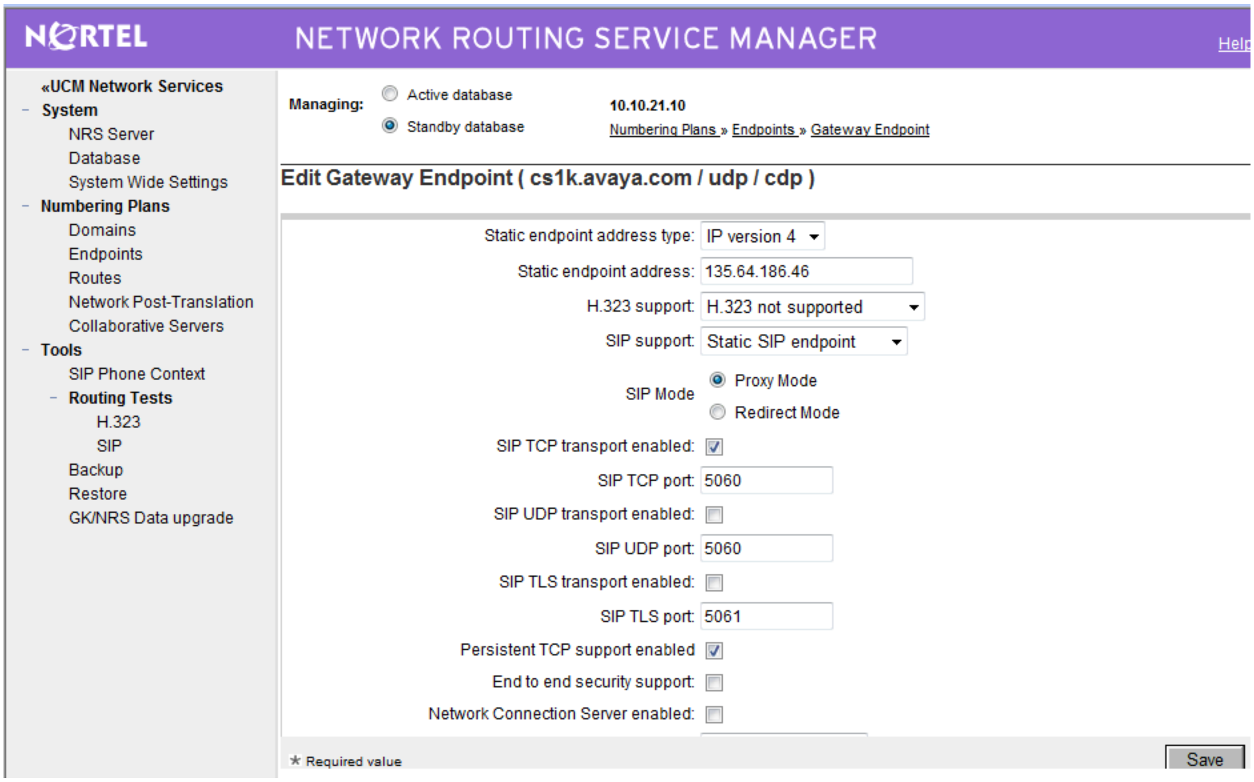
Enter a descriptive **End point name** and **Description**.



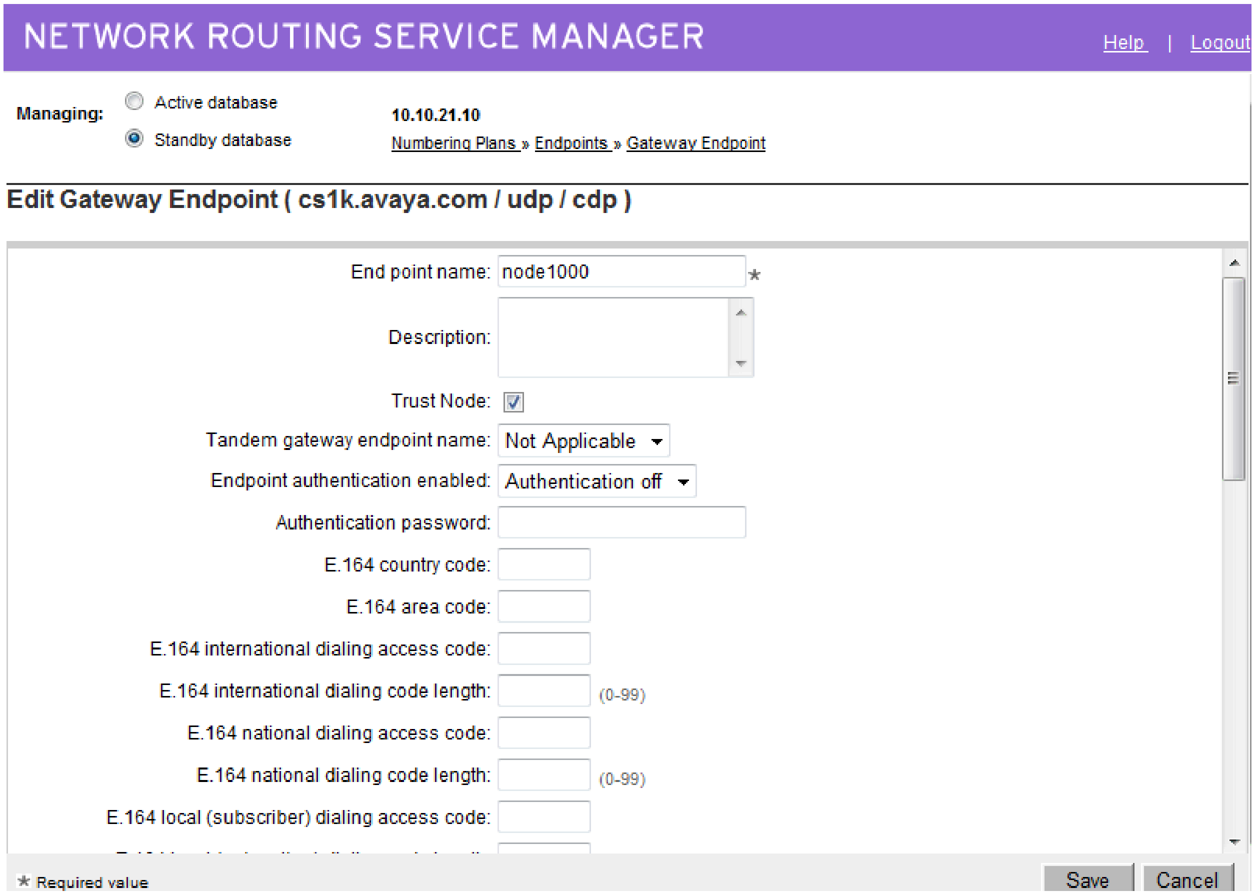
Scroll down the screen. Enter the following values for the specified fields, and retain the default values for the remaining fields.

Static endpoint address: IP address of the Meeting Exchange Application Server
SIP support: **Static SIP endpoint**

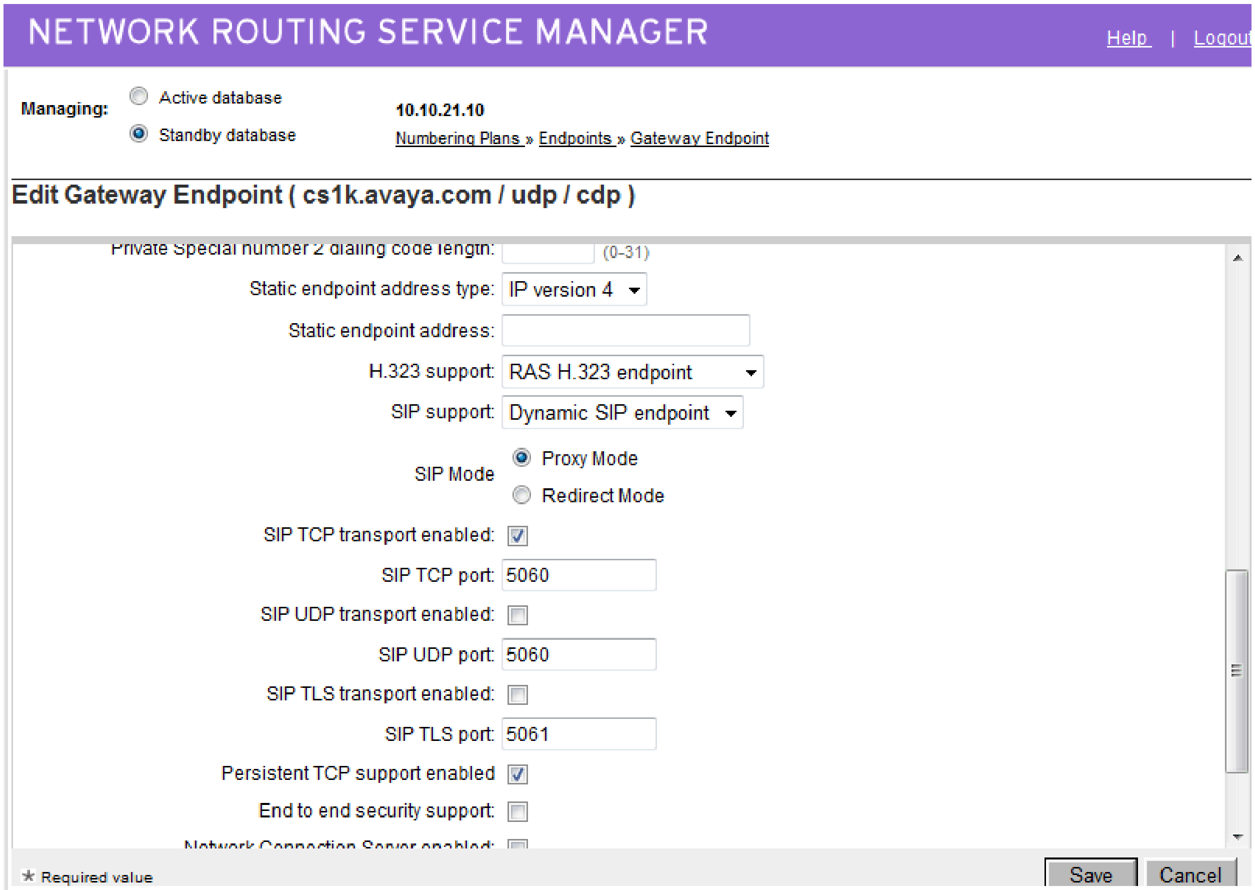
Select the **SIP TCP transport enabled** checkbox. Retain the default values in the remaining fields and click **Save**.



Repeat the procedures to add a **Gateway Endpoint** for the Avaya SIP Signaling Gateway as shown below.

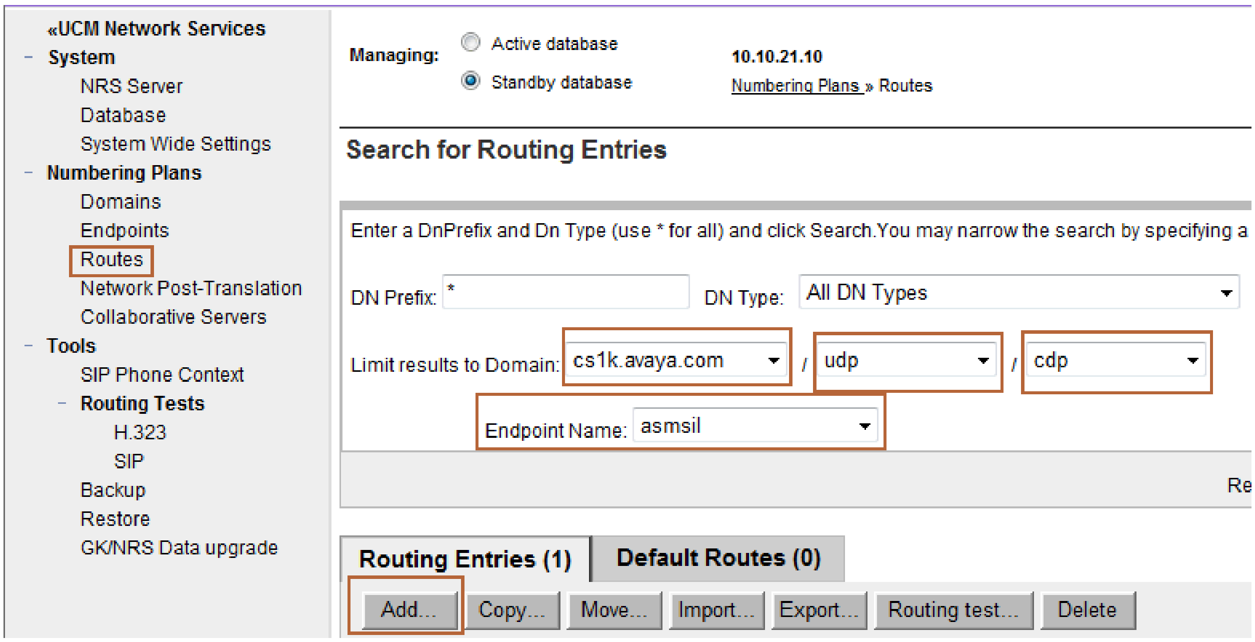


Scroll down the screen. For the **SIP support** field, select **Dynamic SIP endpoint** from the drop-down list. Check the **SIP TCP transport enabled** field to match the SIP transport protocol from **Section 3.8**. Maintain the default values in the remaining fields, and click **Save**.



3.11. Administer Routing Entries

A single routing entry is required for Session Manager in order to reach the conference access number (DNIS=11111) on Meeting Exchange. 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**.



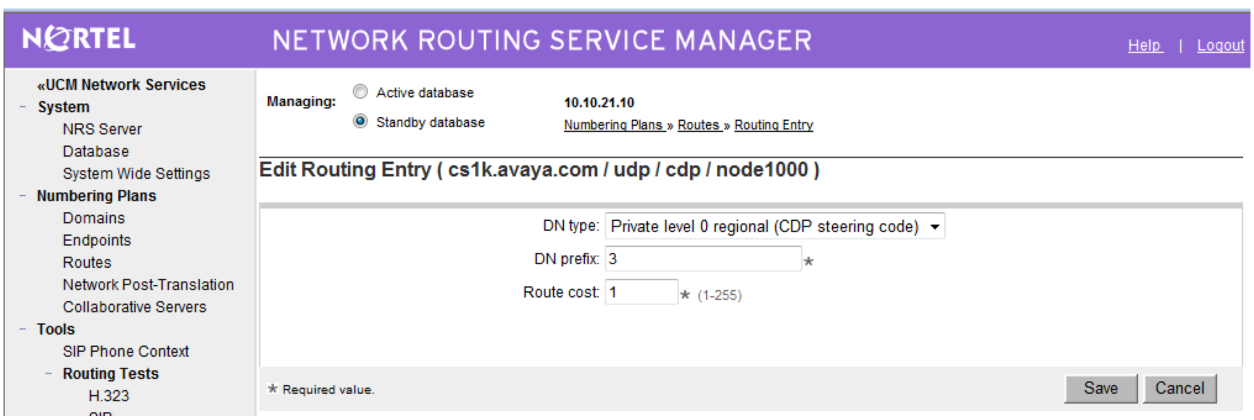
The **Add Routing Entry** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Save**.

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

DN prefix: Dialed prefix digits to match on, in this case **11**. **11111** is the conference access number.

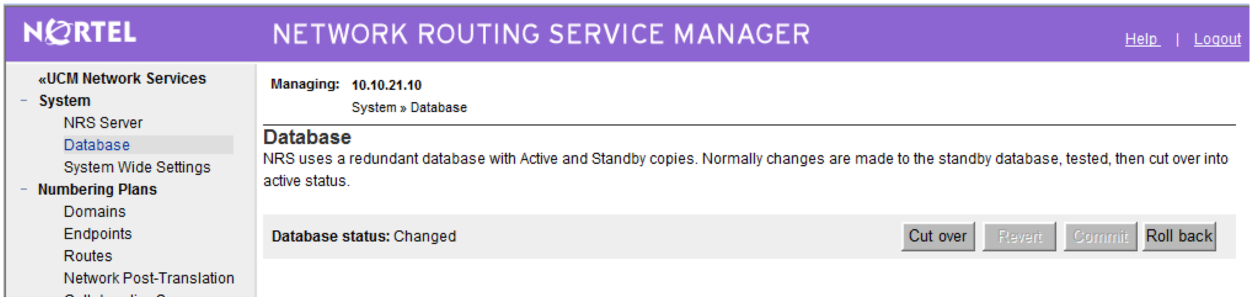
Route cost (1 – 255): An appropriate cost value with 1 being least cost.

Repeat the same procedures to add a routing entry to reach the CS1000E endpoints with extension digits 3xxx behind the Avaya SIP Signaling Gateway Endpoint.

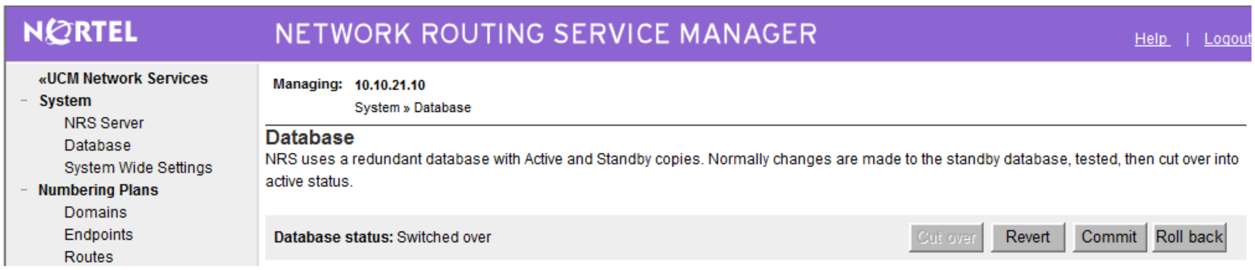


3.12. Cut Over and Commit Changes

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**.



4. Configure Avaya Meeting Exchange Enterprise Application Server

This section describes the steps for configuring a SIP trunk between Meeting Exchange Enterprise Application Server and Session Manager. This configuration will allow both moderators and participants to access a conference and also for operators to dial participants who have difficulties accessing a conference. It's assumed, that Meeting Exchange is installed, configured and licensed as per **[3].** The following steps describe the administrative procedures for configuring Meeting Exchange Enterprise Application Server:

- Configure SIP Listener
- Configure Dialout
- Configure DNIS Mappings
- Configure Incoming SIP URI Conversion Rules
- Restart the Conference Bridge

The following instructions assume the user is logged in to the Meeting Exchange Enterprise Application Server Linux console using SSH.

4.1. Configure SIP Listener

The SIP signaling messages in the sample configuration are transmitted between the Avaya Meeting Exchange Enterprise Application Server and Session Manager over a TCP channel. Configure the following settings to enable SIP connectivity on the Meeting Exchange Enterprise Application Server:

- Edit **/usr/ipcb/config/system.cfg** using the Linux vi tool or download the file to your local machine using a Secure Copy Protocol (SCP) client (i.e.: WinSCP) for editing.
  - Add the IP address of the Meeting Exchange Enterprise Application Server: **IPAddress=10.10.21.50** as shown below
  - Add a line to populate the From Header Field in SIP INVITE messages. The following SIP URI will be displayed when the conference operator calls a participant: **MyListener=sip:6000@10.10.21.50**
  - Add a line to provide a SIP Device Contact address to use for acknowledging SIP messages: **respContact=sip:6000@10.10.21.50**

```
# ip address of the server
IPAddress=10.10.21.50

# request we will be listening to
MyListener=sip:6000@10.10.21.50

# if this setting is populated will Overwrite the contact field in responses
respContact=<sip:6000@10.10.21.50:5060;transport=tcp>
```

4.2. Configure Dialout

The FQDN of the Session Manager must be configured on Meeting Exchange Enterprise Application Server for dialout to work. The Application Server must be able to resolve the FQDN to an IP address, by either using its own hosts file or an external DNS server. For the sample configuration an external DNS server was authoritative for the **cs1k.avaya.com** zone and had the following entry in its zone file:

```
cs1k.avaya.com      IN     A      135.64.186.46
```

Edit **/usr/ipcb/config/telnumToUri.tab** file with a text editor.

Add the following line to the file to route outbound calls from the Meeting Exchange Enterprise Application Server to the extension range administered on the CS1000's dial plan.

```
       3*               sip:$0@cs1k.avaya.com:5060;transport=tcp   default
```

4.3. Configure DNIS Mappings

The DNIS is the number that the phone users dial to access a conference. To map DNIS entries, run the **cbutil** utility on Meeting Exchange Enterprise Application Server as follows:

- Add 11111 as a new DNIS entry using the following command:

```
[mx6200-a ~]# cbutil add 11111 0 247 1 N SCAN
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.
```

At the command prompt, enter **cbutil list** to verify the DNIS entries provisioned.

```
[mx6200-a ~]# cbutil list
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.

DNIS   Grp Msg PS  CP Function On Failure Line Name Company Name Room Start  Room End
------ --- --- --- -- -------- ---------- --------- ------------ ----------- --------
11111   0   247 1   N  SCAN     ENTER                             0           0
```

4.4. Configure Incoming SIP URI Conversion Rules

The Meeting Exchange Enterprise Application Server rejects incoming SIP calls from the CS1000 SIP Proxy Server when CDP is used for call routing, because the CS1000 SIP Signaling Gateway includes a "phone-context=" and “user=phone” parameter in the SIP INVITE messages. In the sample configuration the To: field of the incoming INVITE includes the following values:

To: <sip:11111;phone-context=cdp.udp@cs1k.avaya.com;user=phone

The purpose of the **Incoming SIP URI Conversion Rule** is to extract the DNIS from the To: field and discard the **phone-context=cdp.udp@cs1k.avaya.com** and **user=phone** parameters.

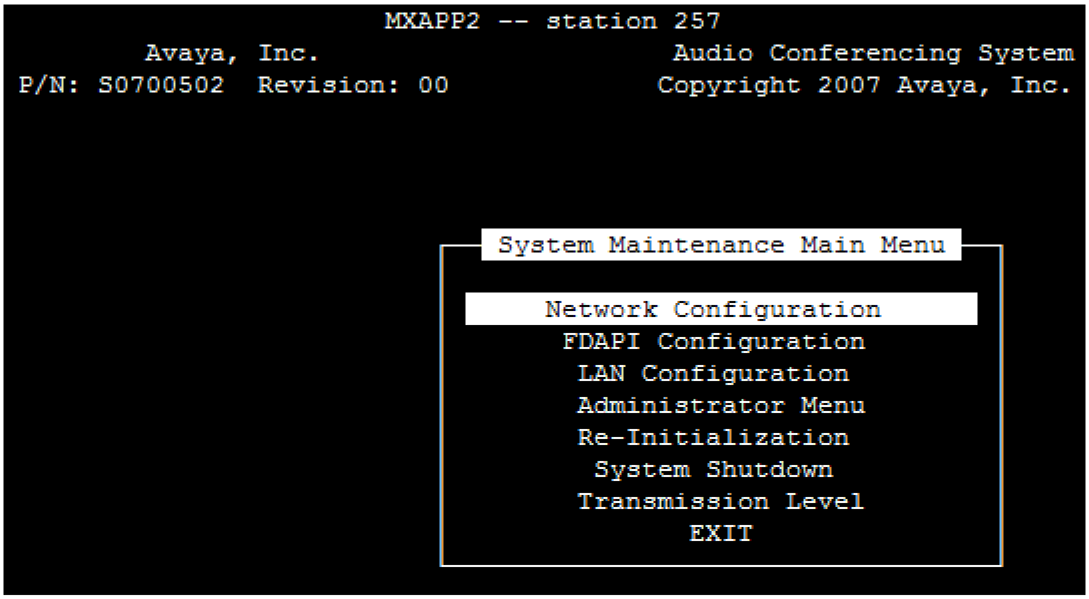
Edit the /usr/ipcb/config/UriToTelnum.tab file with a text editor. Enter the following two rules at the top of the list:

```
TelnumPattern    TelnumConversion        comment
"*sip:*;*@*"    $2
"sip:*;*@*"     $1
```

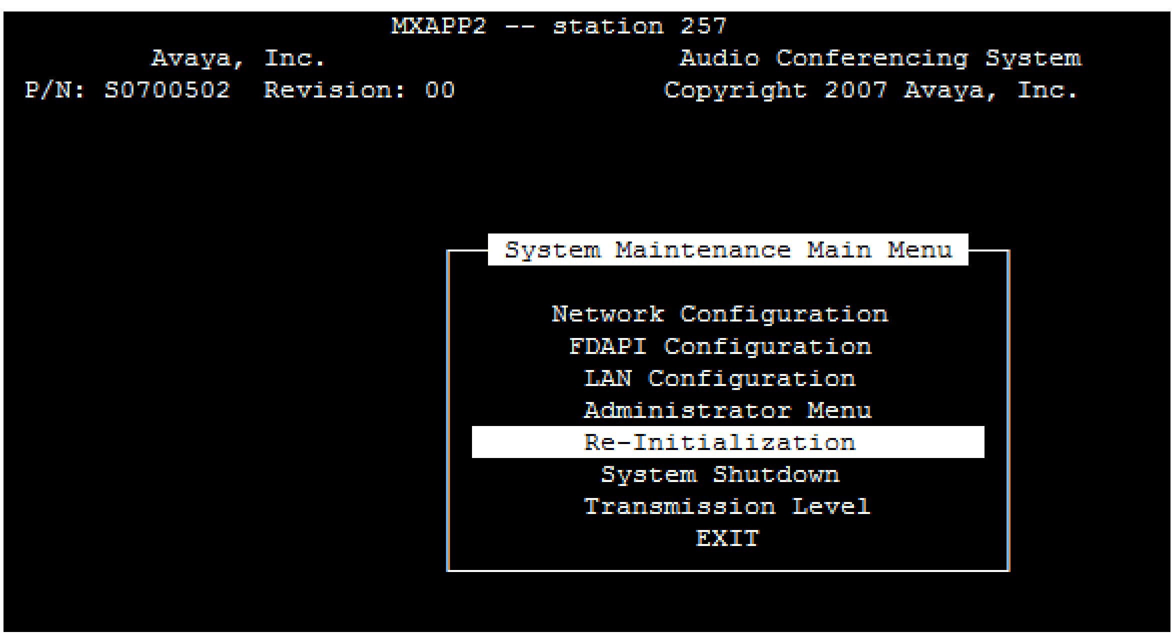
4.5. Restart the Conference Bridge

After the configuration changes are made, restart the Meeting Exchange Enterprise Application Server:

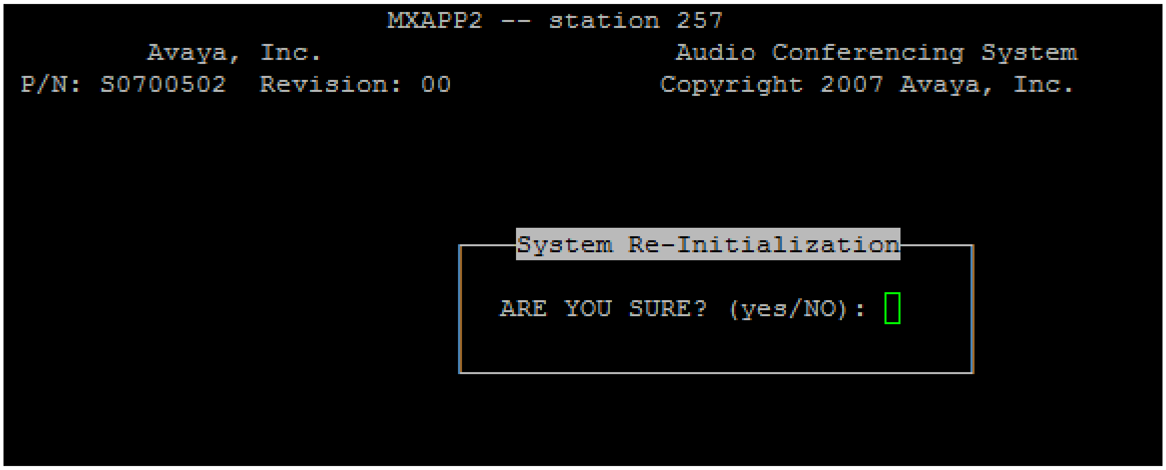
- Log in to the MX Application Server using the **dcbmaint** account.
- Issue the **dcbmaint** command. The **System Maintenance Main Menu** screen is displayed.



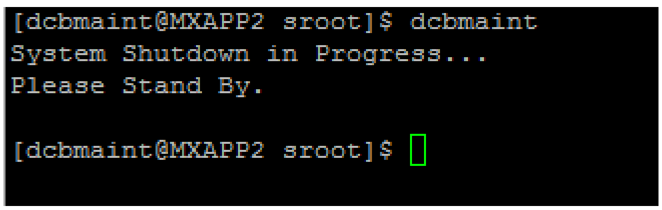
- Navigate to **Re-Initialization**.



- Press **Enter** and at the prompt type **yes**.



- The **dcbmaint** utility terminates and the following message is displayed:



5. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring the Session Manager and includes the following items:

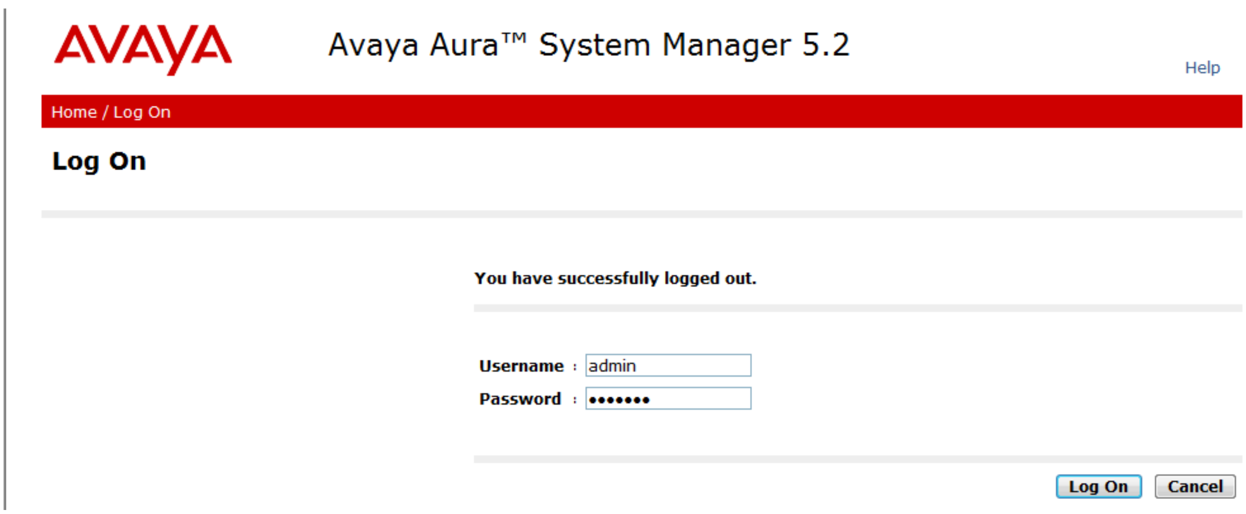
- Log in to Avaya Aura™ System Manager using the GUI
- Administer SIP domain
- Define Locations for SIP Entities

For each SIP entity in the sample configuration:

- Define SIP Entity
- Define Entity Links
- Define Routing Policies
- Define Dial Patterns

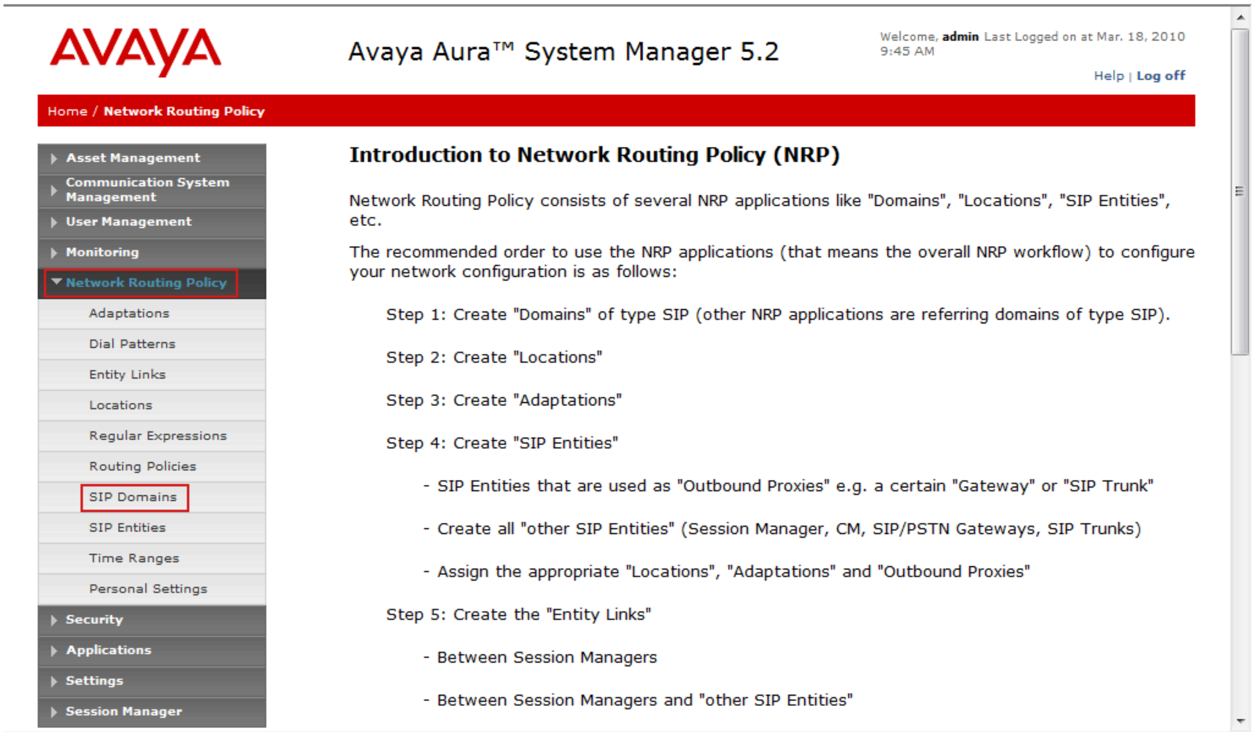
5.1. Log in to Avaya Aura™ System Manager using the GUI

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "**https://<ip-address>/SMGR**", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials.

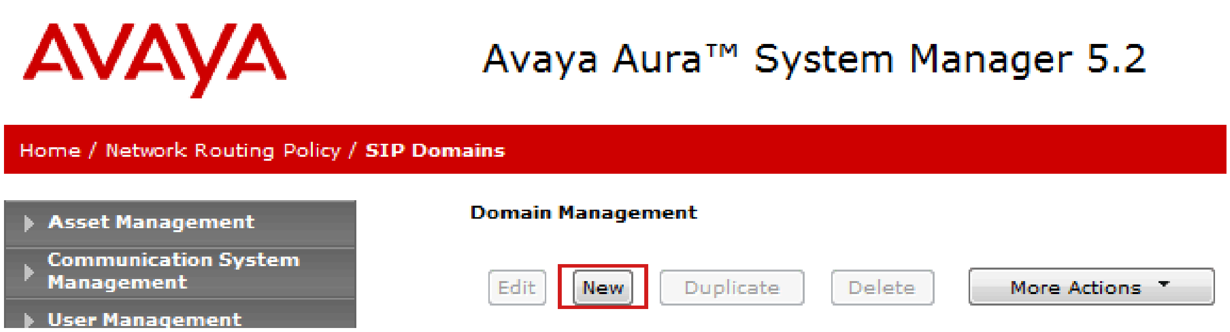


5.2. Administer SIP Domain

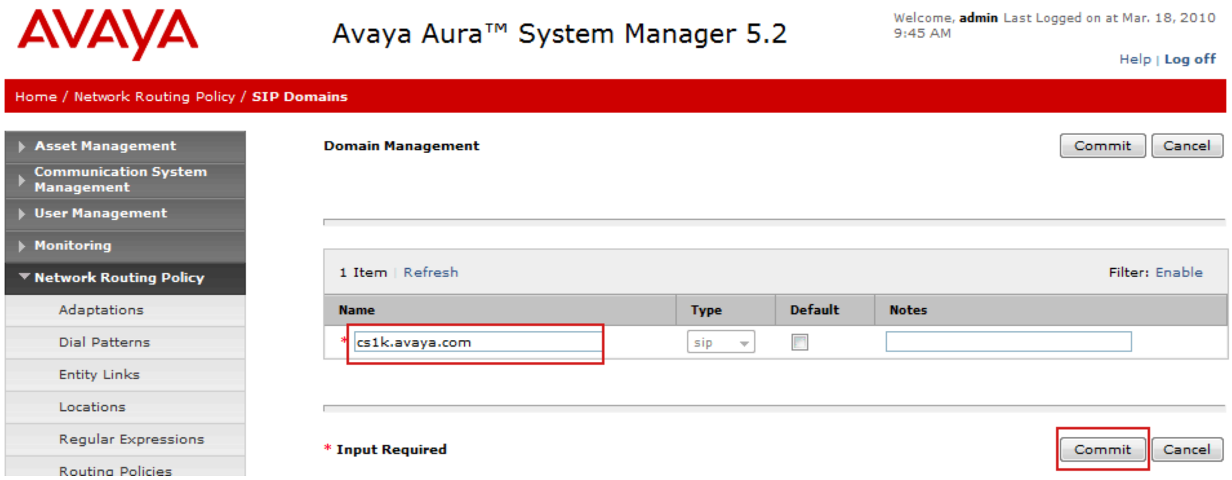
Expand Network Routing Policy and select **SIP Domains**.



Click **New.**

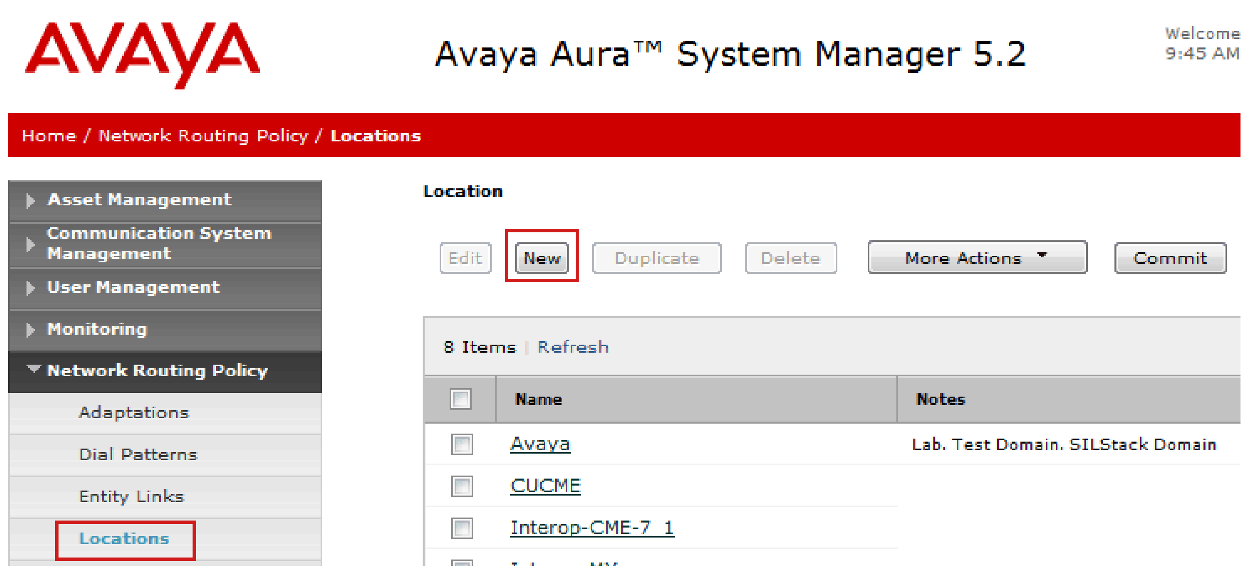


On the **Domain Management** screen under **Name** add a descriptive name (in this case **cs1k.avaya.com**). Retain the default values for the remaining fields. Click **Commit** to save.

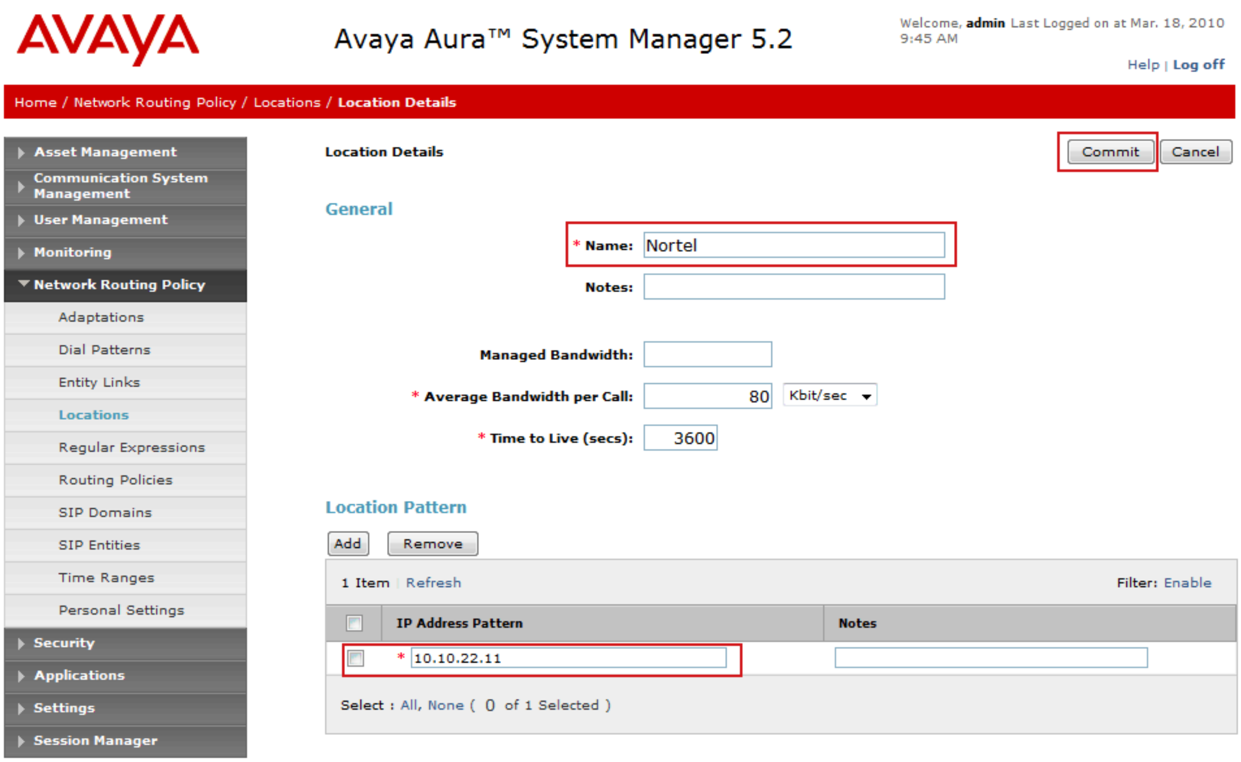


5.3. Define Locations for SIP Entities

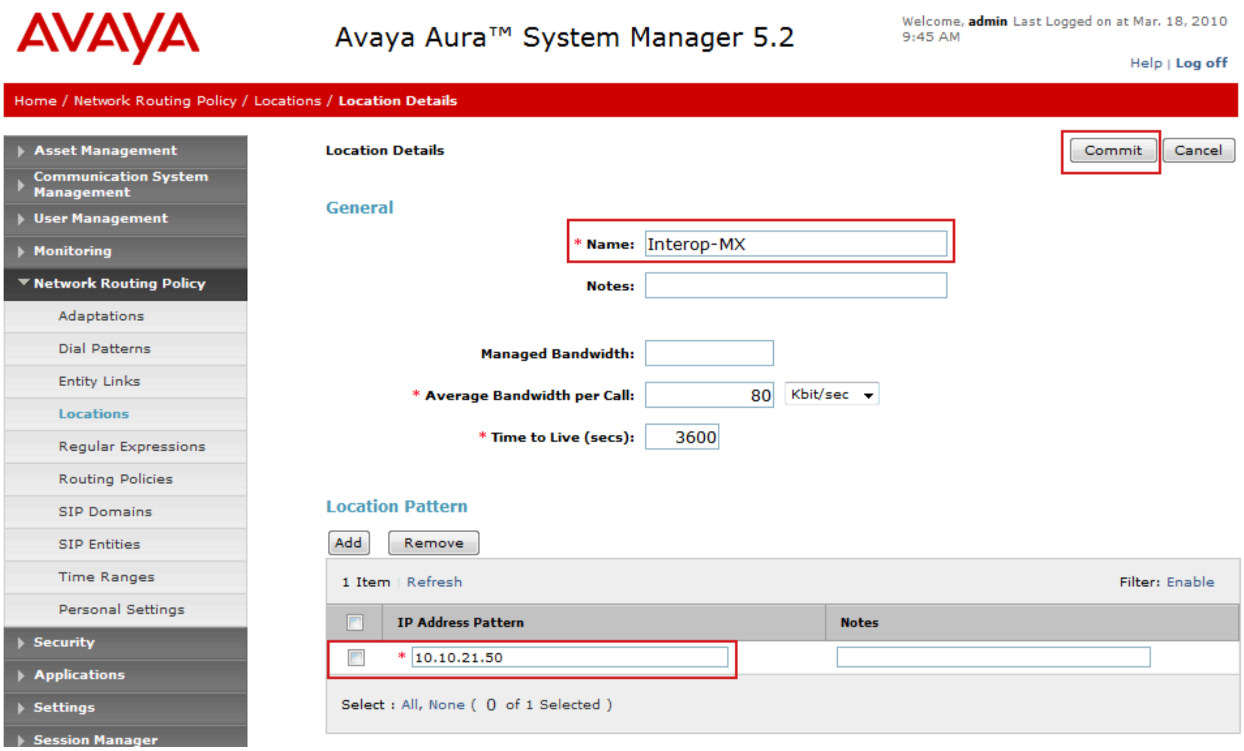
Expand Network Routing Policy and select **Locations.** Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing. Click **New.**



In the **General** Section, under **Name** add a descriptive name. Click on **Add**. In the **Location Pattern** Section under **IP Address Pattern** enter the IP Address of the SIP Proxy Server (SPS) of the CS1000E. In **Section 3.11** the SIP Mode of the Session Manager Endpoint was set to Proxy. This means that the SIP messages will be sourced from the IP address of the NRS/SPS. Click **Commit** to save.

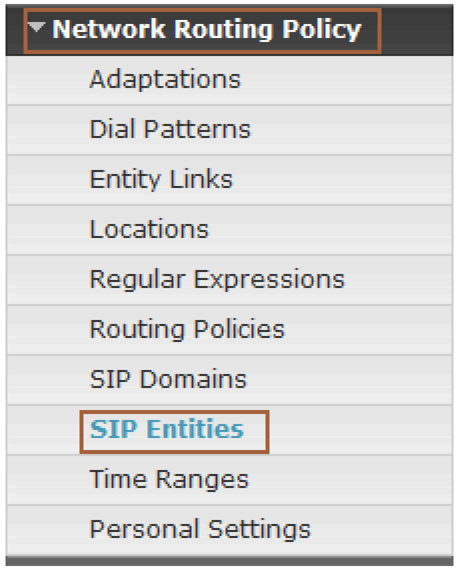


Repeat the above steps for adding a **Location** for the Meeting Exchange Enterprise Application Server. Under **IP Address Pattern** enter the IP Address of the Meeting Exchange Enterprise Application Server as per **Figure 1**. Click **Commit** to save.

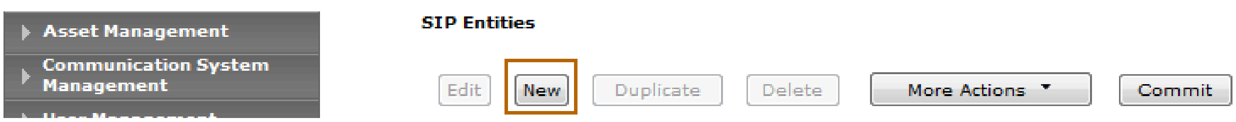


5.4. Define a SIP Entity for the Avaya CS1000E

Under **Network Routing Policy** in the left pane click **SIP Entities**.

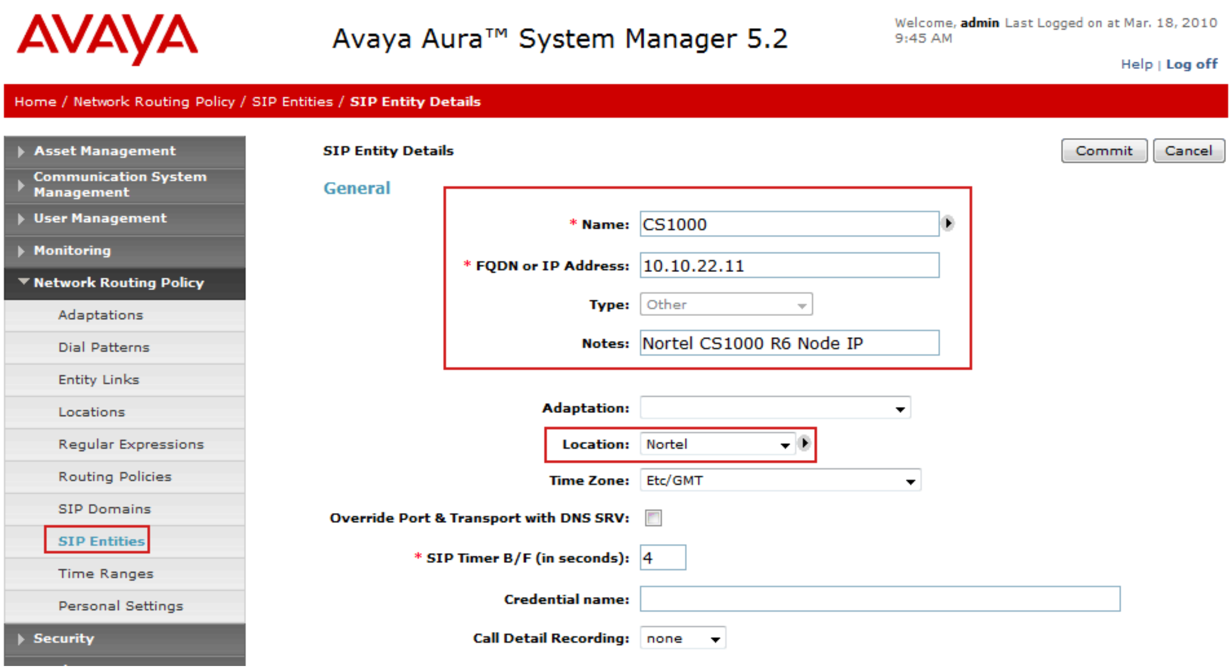


The **SIP Entities** screen is displayed. Click **New**.



The following screen shows addition of the CS1000E as a SIP entity.
Under **General**:

Name	Type in a descriptive name for the CS1000E
FQDN or IP Address	Type IP address of the NRS/SPS
Type	Select **Other**
Notes (Optional)	Type in description
Location	Select the Location created in **Section 5.3**.

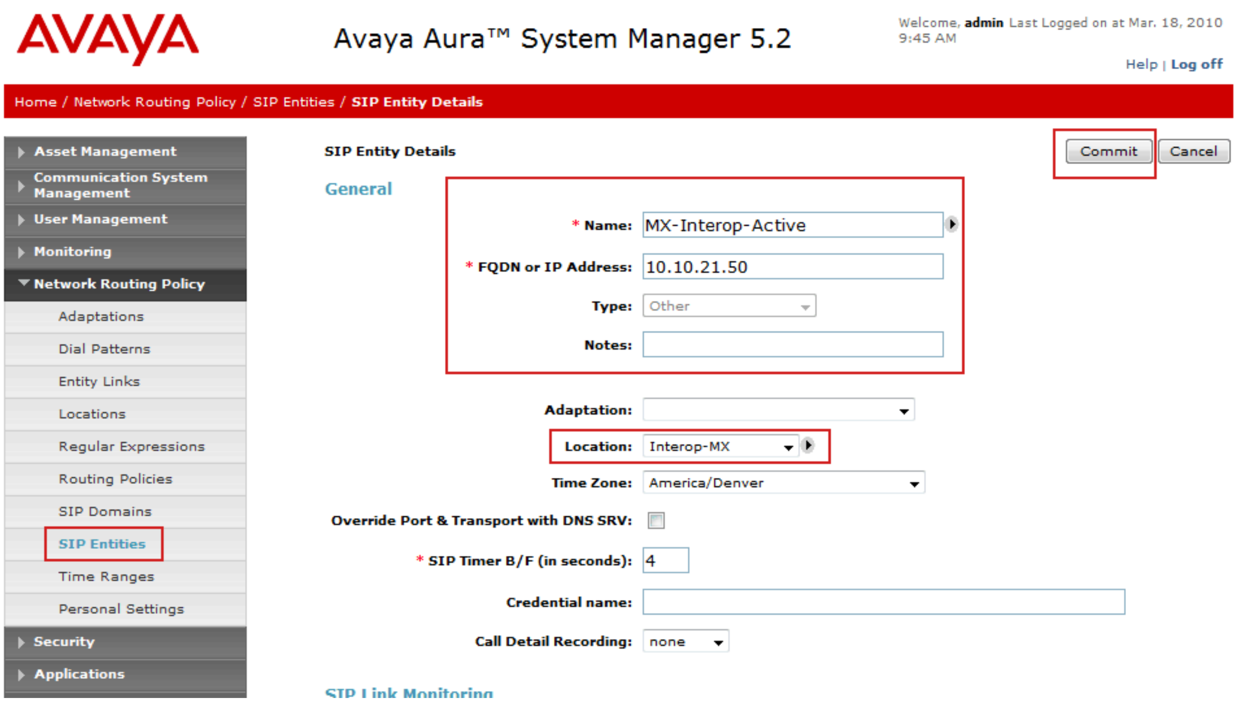


5.5. Define a SIP Entity for Avaya Meeting Exchange Application Server

Repeat the steps from the previous section. Click **New** on the **SIP Entities** page. The following screen shows addition of the Meeting Exchange as a SIP entity. Under **General**:

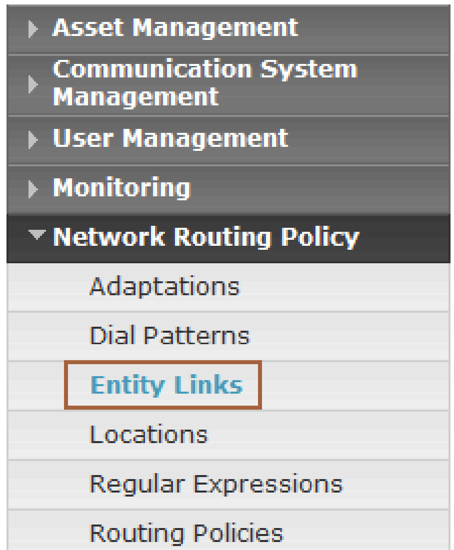
Name	Type in a descriptive name for the Meeting Exchange
FQDN or IP Address	Type IP address of the Meeting Exchange Application Server
Type	Select **Other**
Notes (Optional)	Type in description

Location	Select the Location we created in **Section 5.3**



5.6. Create Entity Link for CS1000E

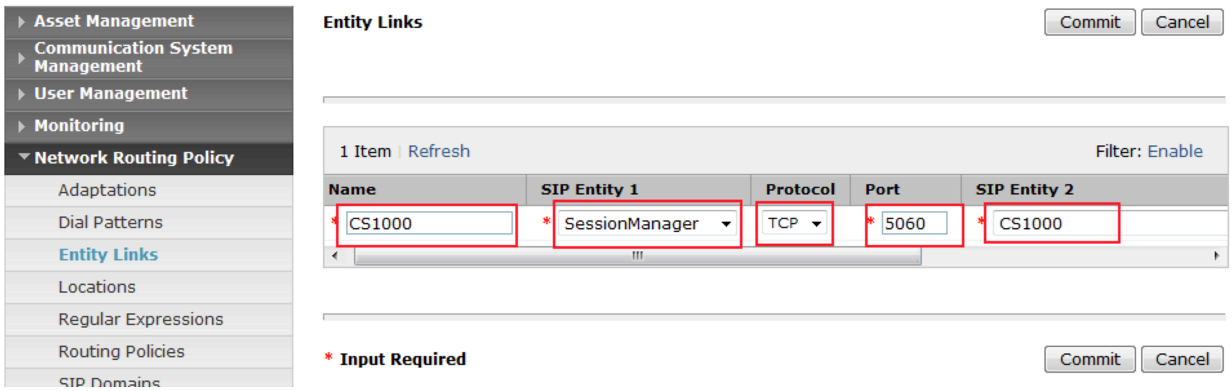
A SIP trunk between Session Manager and the NRS/SPS is described by an Entity Link. Entity Links are not required for SIP user-agent (IP Telephones). To add an Entity Link, select **Entity Links** on the left pane.



Click **New**.

The **Entity Links** screen is displayed. Fill in the following fields in the new row that is displayed:

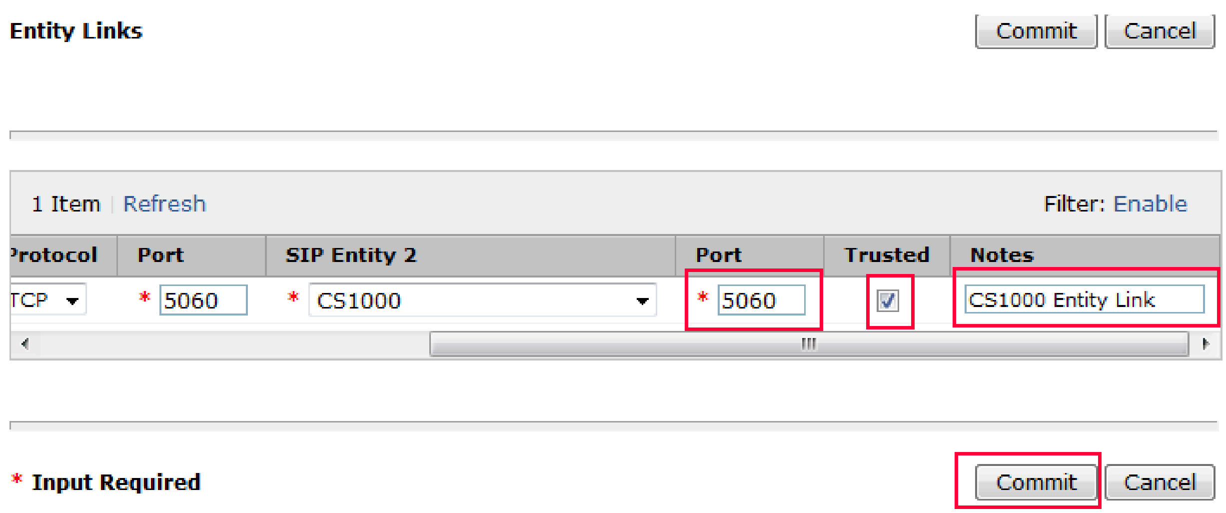
Name: A descriptive name, i.e. **CS1000**.
SIP Entity 1: Select the **Session Manager**.
Protocol: Select **TCP**.
Port: Type **5060**. The Session Manager will listen for SIP requests on TCP port 5060.
SIP Entity 2: Select the SIP Entity we created in **Section 5.4**



Move the scroll bar to the right and fill in the remaining fields.

Protocol: Select **TCP**
Port: Type **5060**. The NRS/SPS will listen for SIP requests on TCP port 5060.**Trusted:** Check this box, otherwise SIP calls will be denied to/from the NRS/SPS
Notes (Optional): A description for the Entity Link.

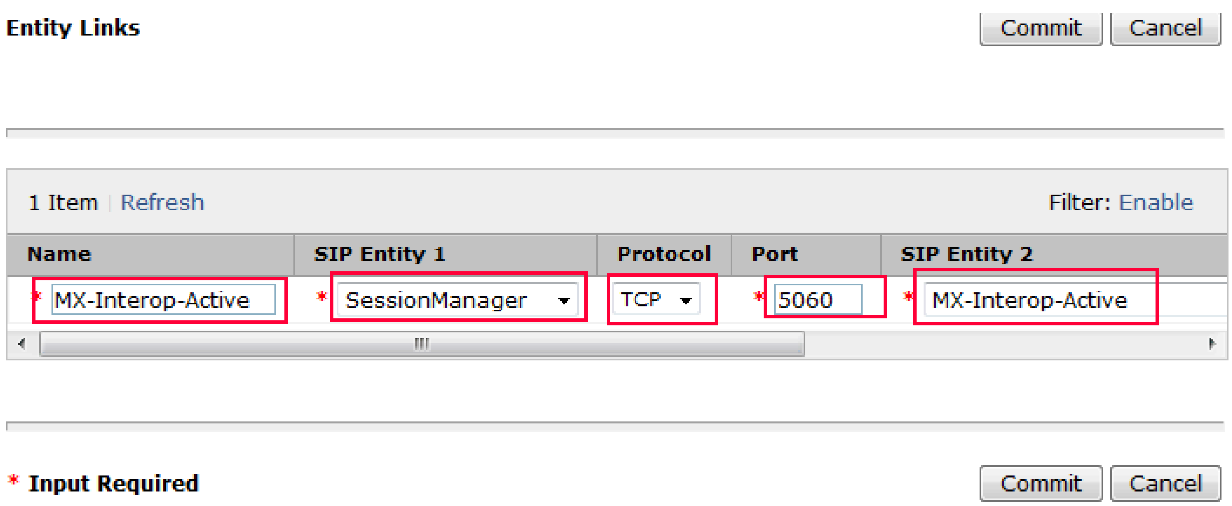
Click **Commit**.



5.7. Create Entity Link for Avaya Meeting Exchange Enterprise Application Server

Repeat the steps from the previous section. Click **New** on the **Entity Links** page. The **Entity Links** screen is displayed. Fill in the following fields in the new row that is displayed:

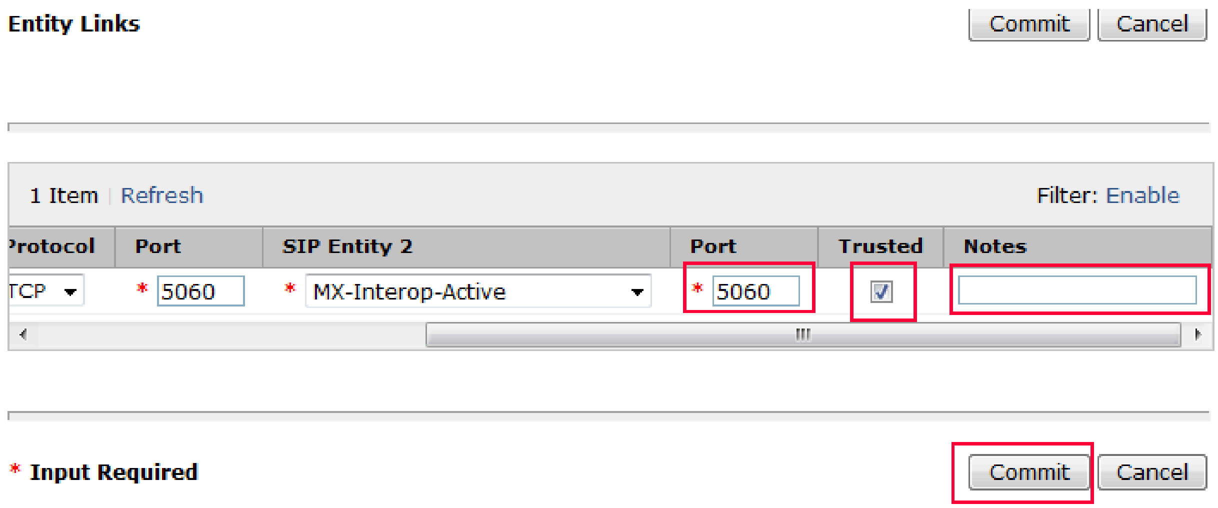
Name:	A descriptive name. In this case **MX-Interop-Active**
SIP Entity 1:	Select the **Session Manager**
Protocol:	Select **TCP**
Port:	Type **5060**. The Session Manager will listen for SIP requests on TCP port 5060
SIP Entity 2:	Select the SIP Entity we created in **Section 5.5**



Move the scroll bar to the right and fill in the remaining fields.

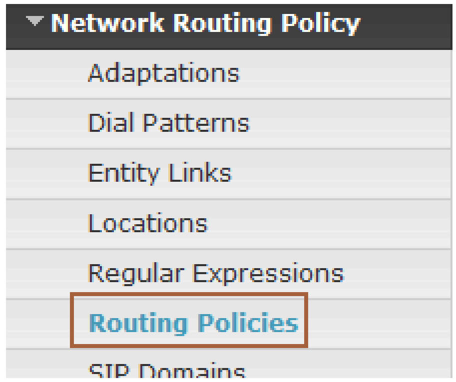
Protocol:	Select **TCP**.
Port:	Type **5060**. The Meeting Exchange Application Server will listen for SIP requests on TCP port 5060.
Trusted:	Check this box, otherwise SIP calls will be denied to/from the Meeting Exchange Application Server.
Notes (Optional):	A description for the Entity Link.

Click **Commit**.

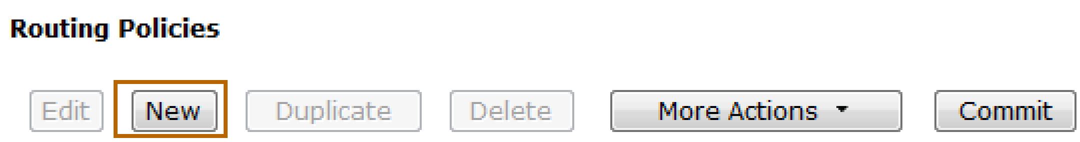


5.8. Add Routing Policy for CS1000E

A routing policy describes the conditions under which calls will be routed to the CS1000E. To add a routing policy, select **Routing Policies** on the left pane.



Click **New.**

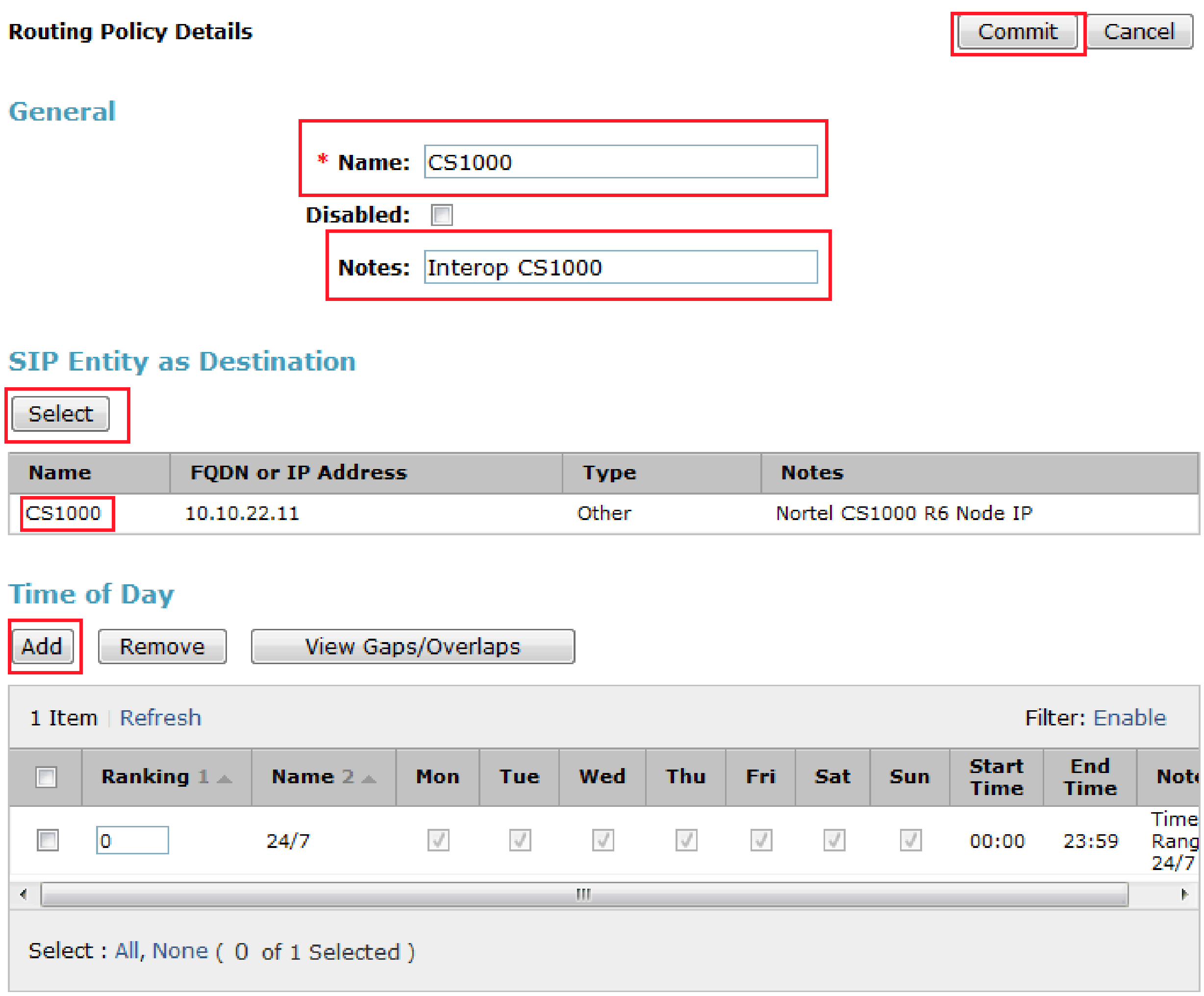


The **Routing Policy Details** screen is displayed. Fill in the following under **General**:

Name	Descriptive name. In this case **CS1000**.
Notes (Optional)	Brief description.

Under **SIP Entity as Destination**:
Click **Select**, and then select the CS1000E SIP Entity we created in **Section 5.4** 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.**



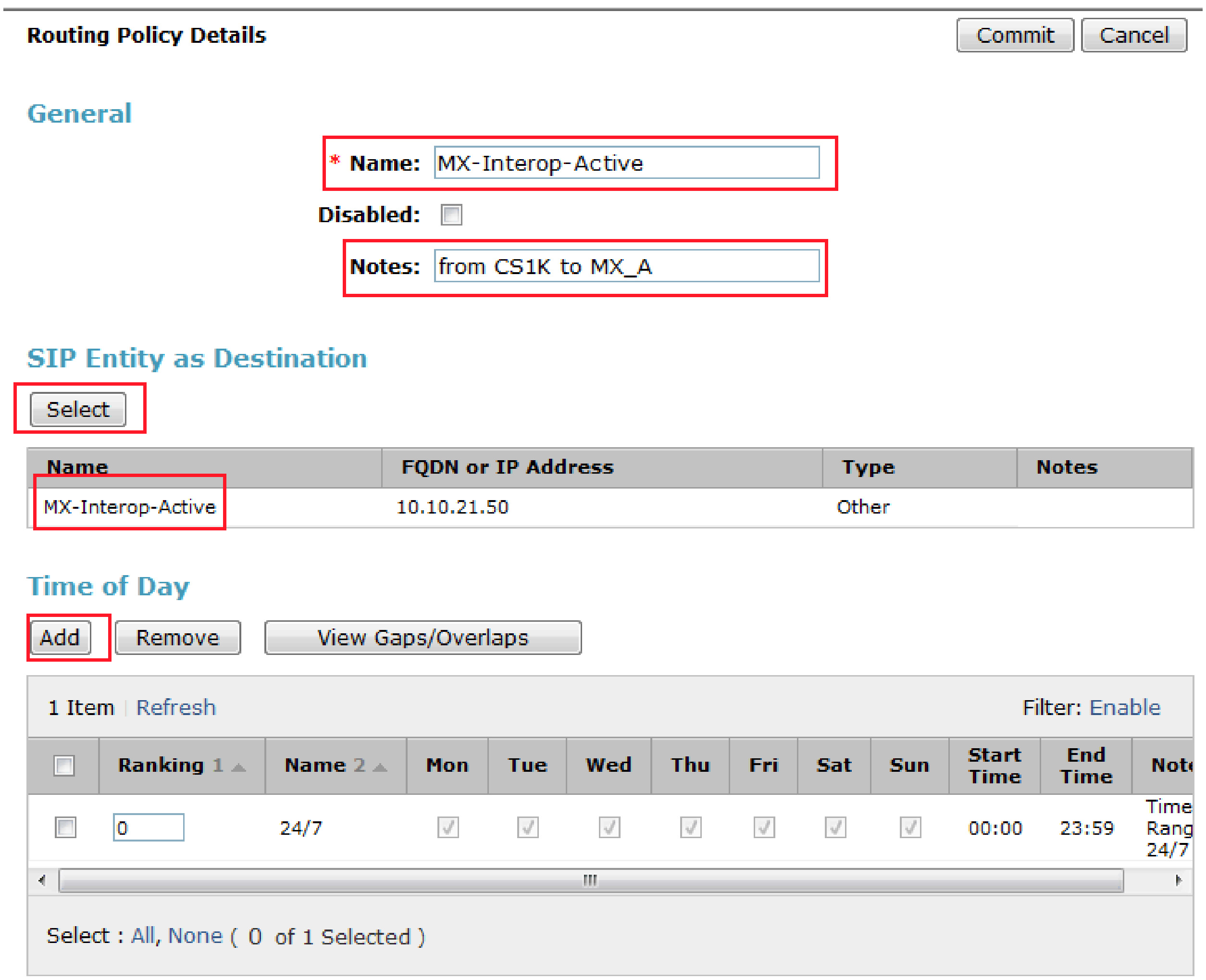
5.9. Add Routing Policy for Avaya Meeting Exchange Enterprise Application Server

Repeat the steps from the previous section until the **Routing Policy Details** screen is displayed. Fill in the following under **General**:

Name	Descriptive name. In this case MX-Interop-Active.
Notes (Optional)	Brief description.

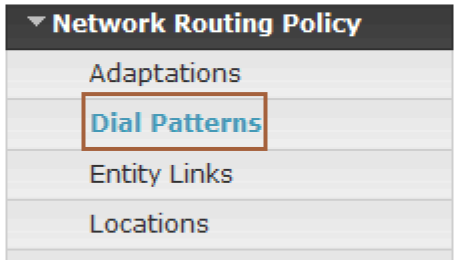
Under **SIP Entity as Destination**:
Click **Select**, and then select the Meeting Exchange SIP Entity we created in **Section 5.5** to which this routing policy applies. In this case **MX-Interop-Active**.

Under **Time of Day**:
Click **Add**, and select the default **24/7** time range. Defaults can be used for the remaining fields. Click **Commit.**

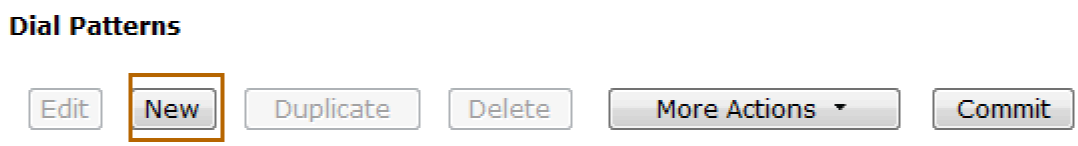


5.10. Add Dial Pattern for CS1000E

Define dial patterns to direct calls to the appropriate SIP Entity. Calls to 4-digit extensions beginning with **3** should be routed to the NRS/SPS. To add a dial pattern, select **Dial Patterns** on the left pane.



Click **New.**



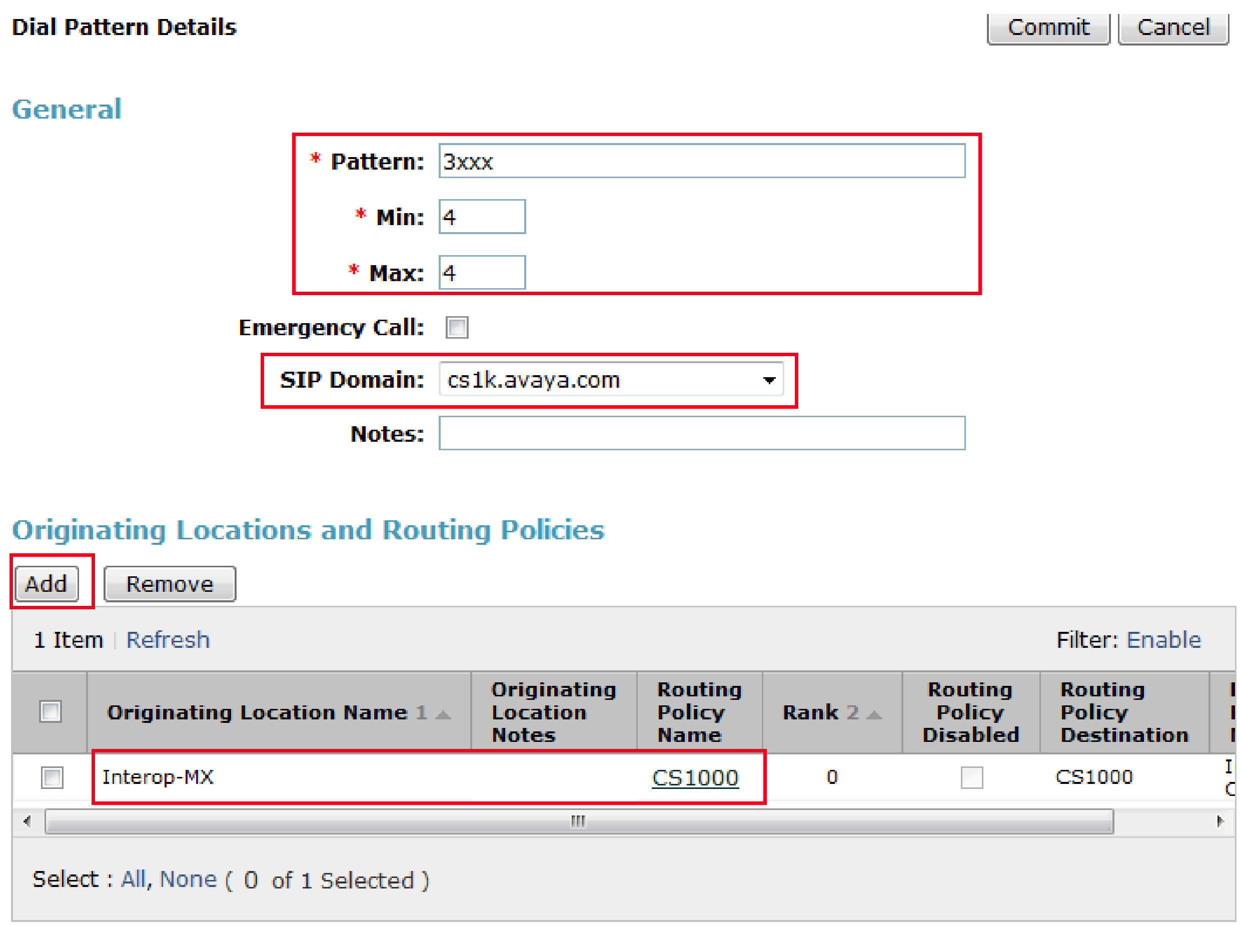
The **Dial Pattern Details** screen is displayed. Under **General** fill in the following fields:

Pattern:	Type **3xxx** as four digit extensions are used on the IP and Digital phones beginning with **3**.
Min:	Minimum length of dialled number. Type **4**
Max:	Maximum length of dialled number. Type **4**
SIP Domain:	SIP domain specified in **Section 5.2**

Under **Originating Locations and Routing Policies:**
Click **Add**. Select the following entries:

Originating Location Name	Select the Location created in **Section 5.3**
Routing Policy Name	Select the Routing Policy created in **Section 5.8**

Default values can be used for the remaining fields. Click **Commit** to save the dial pattern. The following screenshot shows the dial pattern for the CS1000E.



5.11. Add Dial Pattern for Avaya Meeting Exchange Enterprise Application Server

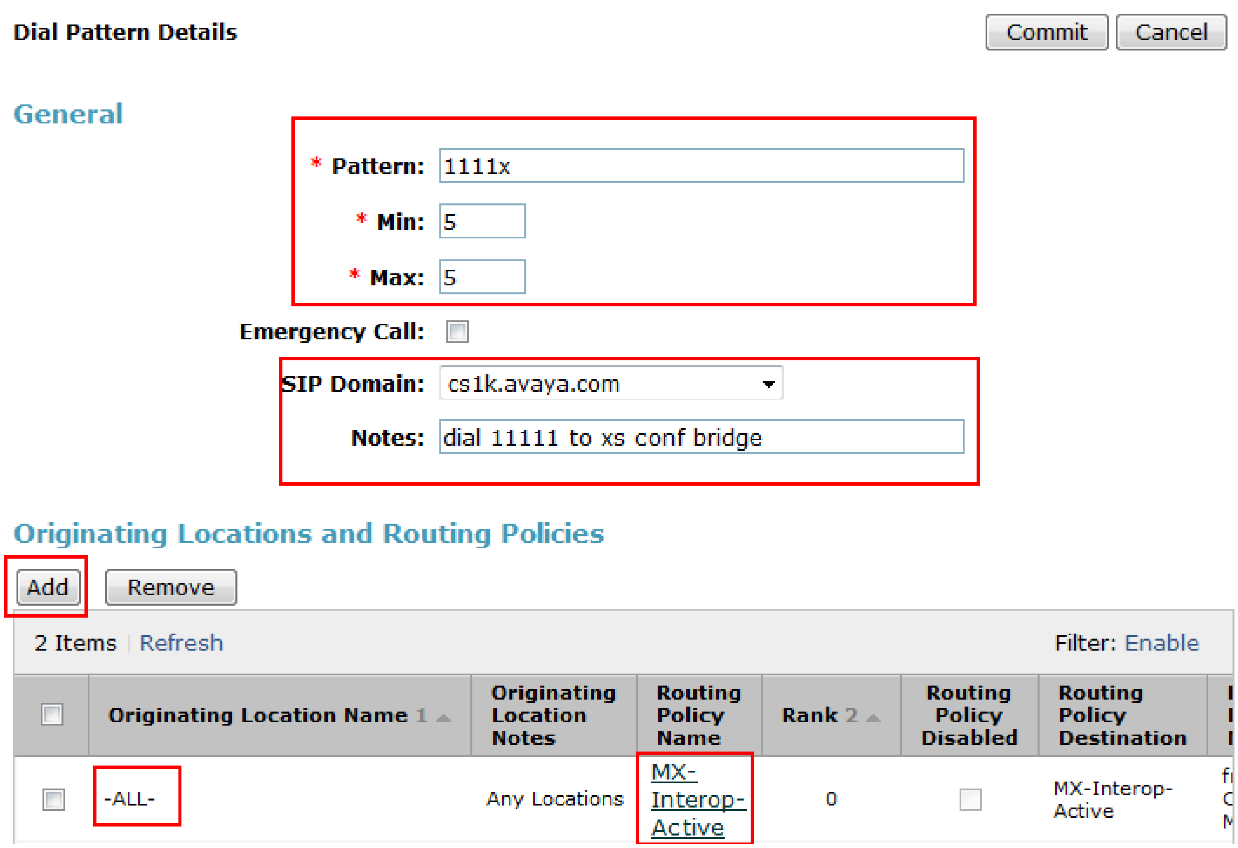
Repeat the steps from the previous section until the **Dial Pattern Details** screen is displayed. Under **General** fill in the following fields:

Pattern:	Type **11111** as the DNIS (conference access number) on the Meeting Exchange is set to 11111.
Min:	Minimum length of dialled number. Type **5**
Max:	Maximum length of dialled number. Type **5**
SIP Domain:	SIP domain specified in **Section 5.2**

Under **Originating Locations and Routing Policies**:
Click **Add**. Select the following entries:

Originating Location Name	Select **All**
Routing Policy Name	Select the Routing Policy we created in **Section 5.9**. In this case **MX-Interop-Active**.

Default values can be used for the remaining fields. Click **Commit** to save the dial pattern. The following screenshot shows the dial pattern for the Meeting Exchange.

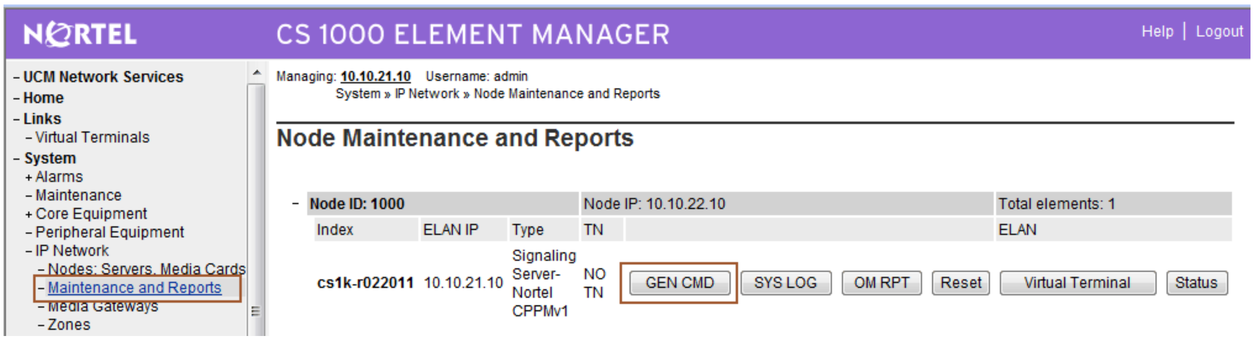


6. Verification Steps

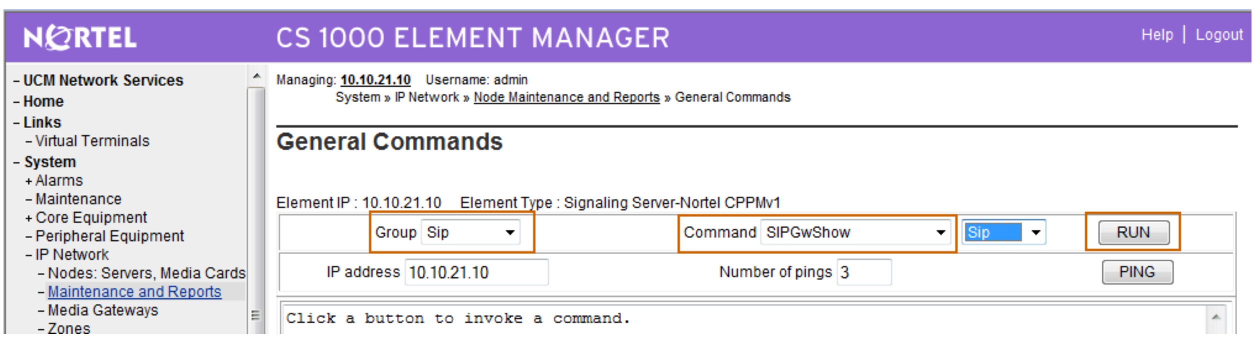
This section provides the tests that can be performed to verify proper configuration of Avaya Communication Server 1000E and Avaya Meeting Exchange Enterprise Edition.

6.1. Verify Avaya Communication Server 1000E

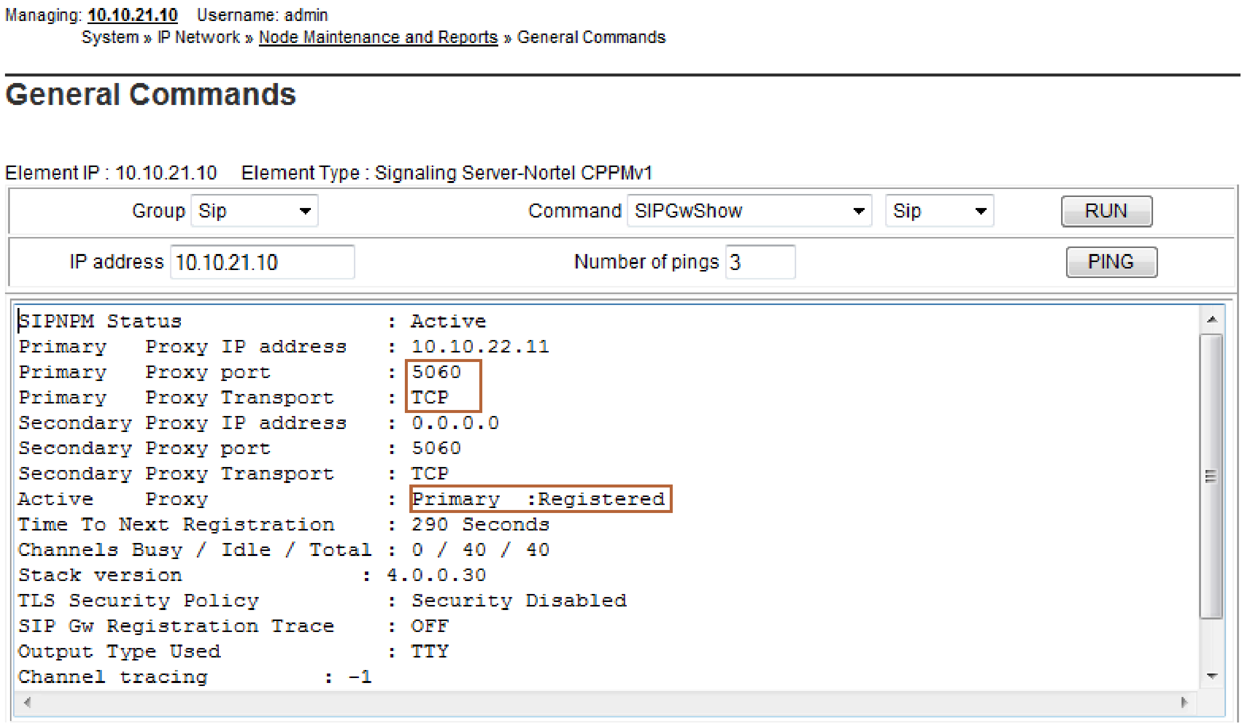
Select **IP Network → Nodes: Servers, Media Cards → Maintenance and Reports** on the left pane. Click **GEN CMD**.



The **General Commands** page is displayed. Click on **Group** and from the drop-down list box select **Sip**. From the **Command** list box select **SIPGwShow** and click on **RUN**.



Confirm that the SIP Signaling Gateway is registered to the SIP Proxy Server and that the SPS uses TCP port 5060 for SIP message transport.



6.2. Verify Avaya Meeting Exchange Enterprise Edition

Verify that the **sipagent** process is running and that number **1** or number **2** is displayed after **/usr/dcb/bin/sipagent** in the following command output on the MX Application Server:

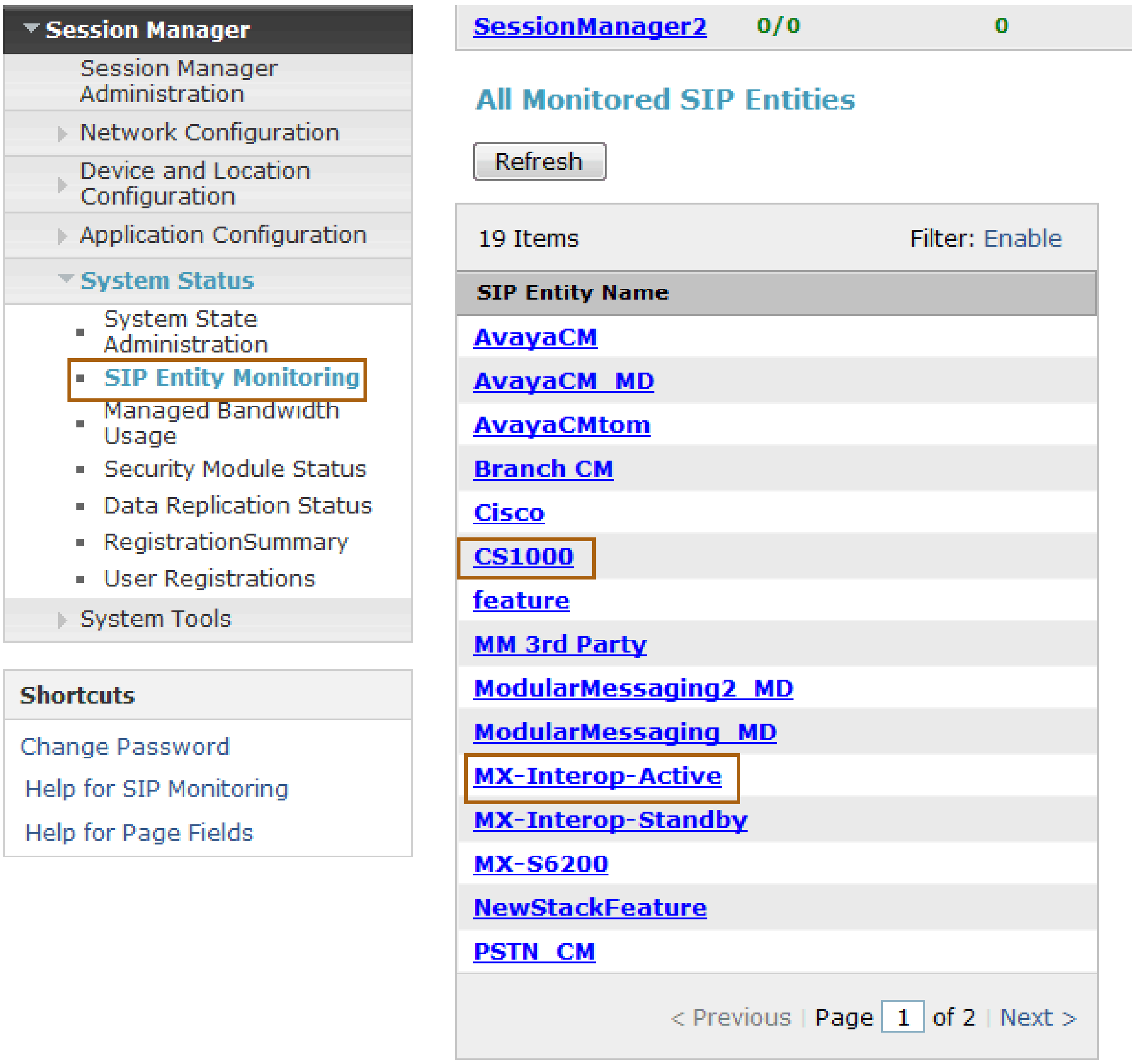
```
[craft@MXAPP1 ]$ ps -ef | grep -i sipagent
sroot    11079 10966  0 Feb18 ?        00:00:21 /usr/dcb/bin/sipagent 1
craft    25946 25926  0 14:00 pts/1    00:00:00 grep -i sipagent
```

Verify that the MX Application Server is listening for SIP requests on TCP port 5060:

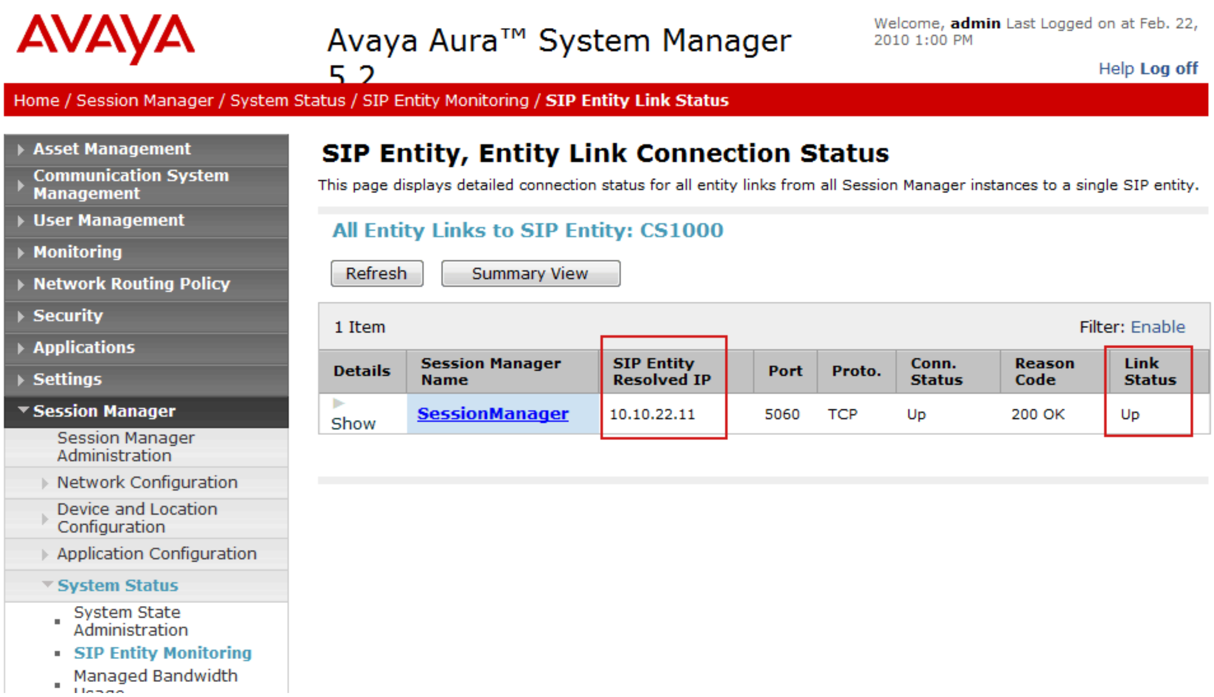
```
[craft@MXAPP1 ]$ netstat -antu | grep 506
tcp        0      0 0.0.0.0:5060                0.0.0.0:*                   LISTEN
```

6.3. Verify Avaya Aura™ Session Manager

Log in to System Manager. Navigate to **Session Manager → System Status → SIP Entity Monitoring** on the left pane to verify that none of the links to the defined SIP entities are down. The **SIP Entity Monitoring** screen is displayed. Click on the individual SIP Entities to check their status. In this sample configuration, **CS1000** and **MX-Interop-Active** were used.



The following screenshot displays the **SIP Entity Link Connection Status** of the CS1000 Entity. The **SIP Entity Resolved IP** column displays the IP address of the NRS/SPS. Check the **Link Status** column and make sure it displays **Up**. Repeat these steps for the Meeting Exchange Entity Link.



7. Verification Scenarios

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

- Conference calls between various telephones on the Avaya Communication Server 1000E can be made using G.711MU/A, G.729 and G.722.
- Proper display of the calling and called party name and number information was verified for all telephones.
- Dialout from the Operator phone to conference participants was verified.

8. Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000E (formerly known as Nortel CS1000E) can interoperate with Avaya Meeting Exchange Enterprise Edition via Avaya Aura™ Session Manager using SIP trunks. The following is a list of interoperability items to note:

- MX Patch Group 5.2.1.2.1 needs to be applied on the Meeting Exchange Application Server for this configuration to work.
- The UriToTelnum.cfg file on the Avaya Meeting Exchange Application Server must contain the required regular expression entries in order to remove the **phone-context** and **user=phone** parameter from the incoming INVITE on the Avaya Meeting Exchange Application Server.

9. Additional References

Avaya CS1000E Support Documents:

[1] *Network Routing Service Fundamentals*, Nortel Communication Server 1000 Release 6, Document Number NN43001-130, Version 1.03, May, 2009, available on the Nortel Communication Server Electronic Reference Library CD. http://support.nortel.com

[2] *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. http://support.nortel.com

Avaya Meeting Exchange Support Documents:

[3] *Administering Meeting Exchange™ 5.2 Servers*, Doc ID 04-603419, 16-Nov-2009, available at http://support.avaya.com/css/P8/documents/100068644

[4] *Administering Meeting Exchange™ 5.2 Applications*, Doc ID 04-603420, 16-Nov-2009, available at http://support.avaya.com/css/P8/documents/100068646

Avaya Aura™ Session Manager:

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

[6] *Installing and Upgrading Avaya Aura™ Session Manager*, Doc ID 03-603324, available at http://support.avaya.com.

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

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