Avaya Solution & Interoperability Test Lab

Configuring SIP Trunks Among Avaya Aura™ Session Manager 6.0, Avaya Aura™ Communication Manager Evolution Server 6.0, Avaya one-X® Deskphone Edition for 9600 Series SIP IP Telephones, and Avaya Communication Server 1000E 6.0 – Issue 1.0

Abstract

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager 6.0 to connect Avaya Aura™ Communication Manager Evolution Server 6.0, Avaya 96xx SIP telephones and an Avaya (formerly Nortel) Communication Server 1000E 6.0 using SIP trunks.

- Avaya Aura™ Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura™ Communication Manager Evolution Server operates as a feature server for the SIP endpoints which register to Avaya Aura™ Session Manager using the SIP protocol. The Avaya Aura™ Communication Manager Evolution Server also supports traditional telephones such as DCP, analog and H.323.

For the sample configuration, Avaya Aura™ Session Manager runs on an Avaya S8800 Server, Avaya Aura™ Communication Manager Evolution Server runs on duplex Avaya S8800 Servers with an Avaya G650 Media Gateway and the 96xx SIP telephones are registered to Avaya Aura™ Session Manager. The Avaya Communication Server 1000E runs on a co-res CP+PM Server blade, version 6.0. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura™ Communication Manager Evolution Server 6.0 and Avaya Communication Server 1000E 6.0.

(This page intentionally left blank)

Table of Contents

1. Introduction 5
2. Equipment and Software Validated 7
3. High-level List of Tasks 7
4. Configuring Avaya Aura™ Communication Manager Evolution Server 8
   - 4.1 Verify System Capabilities and Licensing 8
     - 4.1.1 SIP Trunk Capacity Check 8
     - 4.1.2 AAR/ARS Routing Check 9
     - 4.1.3 Enable Private Networking and Uniform Dialing Plan 9
     - 4.1.4 Configure Trunk-to-Trunk Transfers 10
   - 4.2 Add Node Name of Avaya Aura™ Session Manager 10
   - 4.3 Configure IP Network Regions 10
     - 4.3.1 Configure IP Network Region 1 11
     - 4.3.2 Configure IP Network Region 2 11
     - 4.3.3 Administer IP Codec Set 12
   - 4.4 Add SIP Signaling Group 13
   - 4.5 Add SIP Trunk Group 14
   - 4.6 Administer Private Numbering 15
   - 4.7 Administer Call Routing 16
     - 4.7.1 Administer DialPlan Analysis 16
     - 4.7.2 Administer Uniform Dialplan 17
     - 4.7.3 Administer AAR table 17
     - 4.7.4 Administer Route Pattern 18
   - 4.8 Configure Stations 18
   - 4.9 Verify Off-Pbx Telephone Station-Mapping 20
   - 4.10 Save Translation 21
5. Configure Avaya Aura™ Session Manager 22
   - 5.1 Administer SIP Domains 23
   - 5.2 Define Locations 24
   - 5.3 Add SIP Entities 25
     - 5.3.1 Define Avaya Aura™ Session Manager as a SIP Entity 25
     - 5.3.2 Define Ports for Use by Avaya Aura™ Session Manager 25
     - 5.3.3 Add Avaya Aura™ Session Manager to System Manager 26
     - 5.3.4 Define a SIP Entity for Avaya Aura™ Communication Manager Evolution Server28
     - 5.3.5 Define a SIP Entity for the CS1000E 28
   - 5.4 Create Entity Links 29
   - 5.5 Add Routing Policies 30
   - 5.6 Add Dial Patterns 32
   - 5.7 Define Avaya Aura™ Communication Manager Evolution Server as an Administrable Entity 34
     - 5.7.1 Add Avaya Aura™ Communication Manager as an Administerable Element 34
     - 5.7.2 Synchronize Communication Manager with System Manager 36
   - 5.8 Define an Application Sequence for Avaya Aura™ Communication Manager Evolution Server 37
   - 5.9 Add SIP Users 39

6. Configure 96xx SIP Deskphone....44
6.1 Configure IP Address, Subnet Mask & Default Gateway 44
6.2 Configure SIP Global and Proxy Settings 46
6.3 Login Phone to Avaya Aura™ Session Manager 49
7. Configure the Avaya Communication Server 1000E 50
7.1 Launch Unified Communications Manager.... 51
7.2 Obtain Node and IP Addresses 51
7.3 Administer ISDN 53
7.4 Administer a Virtual D-Channel.... 56
7.5 Administer Zones.... 58
7.6 Administer Virtual SIP Routes and Trunks 59
7.7 Administer Route List Block and Distant Steering Code 63
7.8 Administer Node SIP Parameters 66
7.9 Launch NRS Manager.... 72
7.10 Administer Service Domain.... 74
7.11 Administer SIP Gateway Endpoints 77
7.12 Administer Routing Entries 80
7.13 Cut Over and Commit Changes 83
8. Verification Steps....84
8.1 Verify Avaya Aura™ Communication Manager.... 84
8.2 Verify Avaya Aura™ Session Manager 86
8.3 Verify 96xx SIP Phones are Registered.... 87
8.4 Verify Avaya Communication Server 1000 87
8.4.1 Verify Status of the Signaling Server 87
8.4.2 Verify Status of an Active Call.... 87
8.5 Verification Scenarios.... 88
9. Conclusion 89
10. Additional References....89

1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager 6.0 to connect Avaya Aura™ Communication Manager Evolution Server 6.0, Avaya 96xx SIP telephones and an Avaya Communication Server 1000E 6.0 using SIP trunks.

The Avaya Aura™ Communication Manager Evolution Sever is a new concept for the 6.0 release. Like Avaya Aura™ Communication Manager Feature Server introduced in release 5.2.1, it can support 96xx SIP endpoints, however it can also support traditional telephones such as DCP and H.323. In addition, unlike the Avaya Aura™ Communication Manager Feature Server, the Avaya Aura™ Communication Manager Evolution Server communicates with Avaya Aura™ Session Manager via a non-IMS SIP signaling group and associated SIP trunk group.

- Avaya Aura™ Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura™ Communication Manager Evolution Server operates as a feature server for the SIP endpoints which register to Avaya Aura™ Session Manager using the SIP protocol. The Avaya Aura™ Communication Manager Evolution Server also supports traditional telephones such as DCP, analog and H.323.

For the sample configuration, Avaya Aura™ Session Manager runs on an Avaya S8800 Server, Avaya Aura™ Communication Manager Evolution Server runs on duplex Avaya S8800 Servers with an Avaya G650 Media Gateway and the 96xx SIP telephones are registered to Avaya Aura™ Session Manager. The Avaya Communication Server 1000E runs on a co-res CP+PM Server blade, version 6.0. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura™ Communication Manager 6.0 Evolution Server and Avaya Communication Server 1000E 6.0.

As shown in **Figure 1** below, the Avaya 96xx SIP telephones are registered to Avaya Aura™ Session Manager but supported by the Avaya Aura™ Communication Manager Evolution Server.

The Avaya 1140e/1165e UNIstim and 3903/3904 Digital Telephones are supported by the Avaya Communication Server 1000E (CS1000E) PBX. SIP trunks are used to connect these two systems to Avaya Aura™ Session Manager, using its SM-100 (Security Module) network interface. All inter-system calls are carried over these SIP trunks. Avaya Aura™ Session Manager can support flexible inter-system call routing based on dialed number, calling number and system location, and can also provide protocol adaptation to allow multi-vendor systems to interoperate. It is managed by a separate Avaya Aura™ System Manager, which can manage multiple Avaya Aura™ Session Managers by communicating with their management network interfaces.

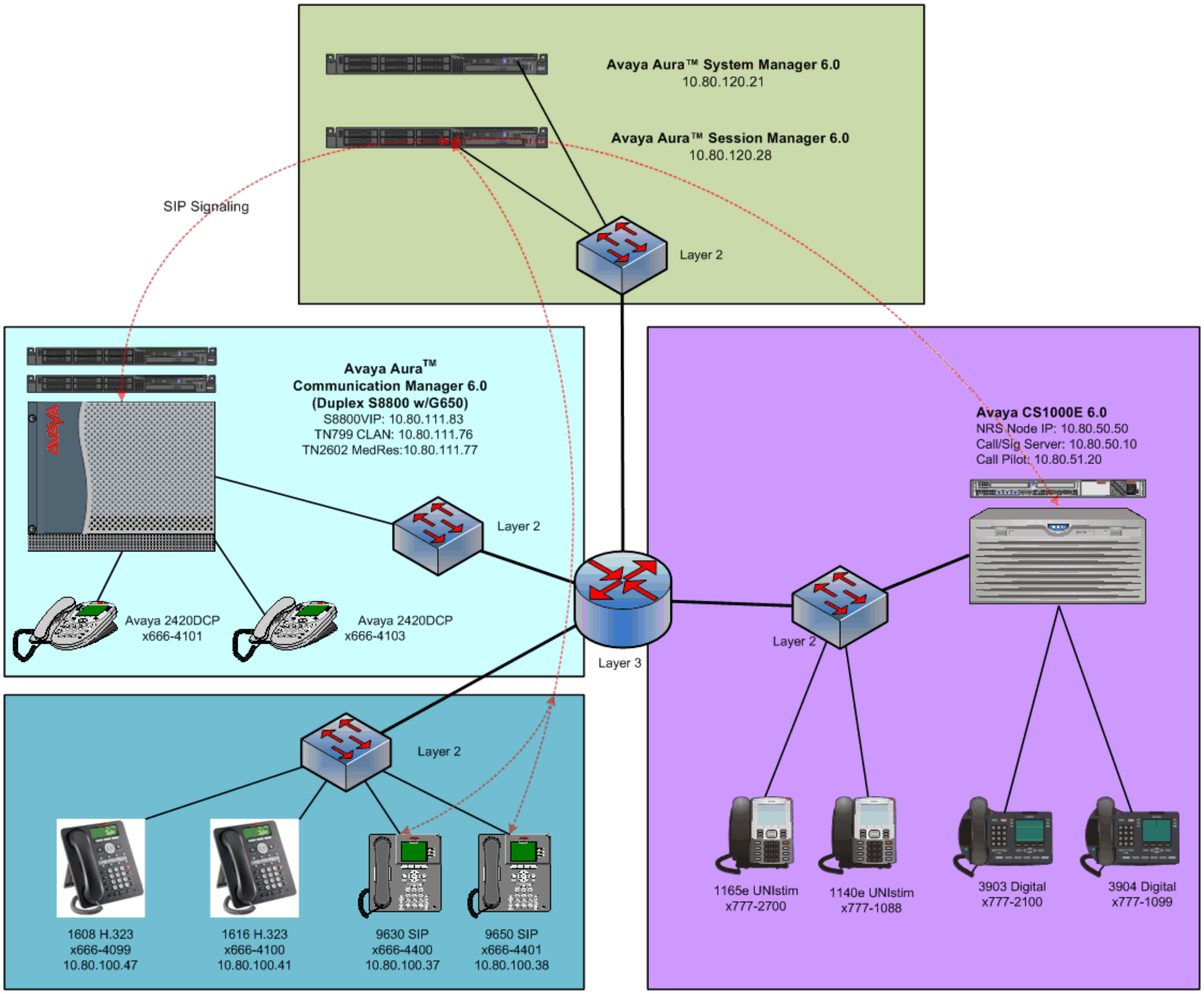


Figure 1 – Sample Configuration

Avaya Aura™ Communication Manager's Uniform Dial Plan (UDP) and AAR tables in conjunction with the Avaya Communication Server 1000E Coordinated Dial Plan (CDP) feature are used to implement extension-extension 7-digit dialing between systems. Unique extension ranges are associated with Avaya Aura™ Communication Manager telephones (666xxxx) and Avaya Communication Server 1000E phones (777xxxx).

These Application Notes focus on configuration of the SIP trunks, configuration of the 96xx SIP phones as 'users' on Avaya Aura™ Session Manager and call routing between the two systems. It's important to understand that the 96xx phones are registered directly to Avaya Aura™ Session Manager with Avaya Aura™ Communication Manager supplying 'call features' via Avaya Aura™ Session Manager's **Sequenced Application** capability.

2. Equipment and Software Validated

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

Hardware Component	Software/Firmware Version
Avaya S8800 Server	Avaya Aura™ Session Manager R6.0
	Avaya Aura™ System Manager R6.0
Avaya S8800 Server (duplex)	Avaya Aura™ Communication Manager 6.0+SP1*
Avaya G650 Media Gateway	n/a
Avaya 9630/9650 one-X®Deskphone (SIP)	2.6
Avaya 1608/1616 one-X® Deskphone Value Edition (H.323)	1.22
Avaya 2420 DCP Telephone	6
Avaya Communication Server 1000E CP+PM	Release 6.0.18
Avaya Network Routing Service (NRS)	6.0
Avaya 3903/3904 Digital Telephones	NA
Avaya 1140e UNIstim Telephone	0625C7J
Avaya 1165e UNIstim Telephone	0626C7J
***NOTE:** CM 6.0 SP1 is required for basic interoperability between Communication Manager 6.0 and the CS1000E 6.0	

3. High-level List of Tasks

The following is a high-level list of tasks that will be covered in this document.

1) Configure Communication Manager Evolution Server to communicate with Session Manager using the SIP protocol.
2) Configure Communication Manager and the CS1000E as SIP nodes in Session Manager via System Manager.
3) Configure SIP routing in Session Manager.
4) Configure Communication Manager in System Manager as an administrable element.
5) Add SIP users/endpoints to Session Manager using System Manager.
6) Configure 96xx SIP phones to register to Session Manager.
7) Configure the CS1000E Network Routing Service (NRS) to communicate with the CS1000E Signaling Server and Call Server.
8) Configure the CS1000E Call Server to route calls to 666xxxx to the NRS.
9) Configure the NRS to route 666xxxx calls to Session Manager

4. Configuring Avaya Aura™ Communication Manager Evolution Server

This section describes the administration of Communication Manager using a System Access Terminal (SAT). Alternatively, some of the station administration could be performed using the Communication System Management application on System Manager. These instructions assume the G650 Media Gateway is already configured on Communication Manager. Some administration screens have been abbreviated for clarity.

- Verify System Capabilities and Communication Manager Licensing
- Administer network regions
- Administer IP node names
- Administer IP interface
- Administer SIP trunk group and signaling group
- Administer route patterns
- Administer numbering plan

After completing these steps, the "**save translation**" command should be performed.

4.1 Verify System Capabilities and Licensing

This section describes the procedures to verify the correct system capabilities and licensing have been configured. If there is insufficient capacity or a required feature is not available, contact an authorized Avaya sales representative to make the appropriate changes.

4.1.1 SIP Trunk Capacity Check

Issue the **display system-parameters customer-options** command to verify that an adequate number of SIP trunk members are licensed for the system as shown below.

```
display system-parameters customer-options                 Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                               USED
                     Maximum Administered H.323 Trunks: 500   0
           Maximum Concurrently Registered IP Stations: 18000 4
             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: 100   0
                        Maximum Video Capable Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 50    20
```

4.1.2 AAR/ARS Routing Check

Verify that the **ARS** and **ARS/AAR Dialing without FAC** options are enabled (on Page 3 of system-parameters customer options).

```
display system-parameters customer-options                    Page   3 of  11
                                OPTIONAL FEATURES

 A/D Grp/Sys List Dialing Start at 01? n                            CAS Main? n
Answer Supervision by Call Classifier? n                   Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                         DCS (Basic)? y
          ASAI Link Core Capabilities? y                   DCS Call Coverage?
```

4.1.3 Enable Private Networking and Uniform Dialing Plan

Use the **display system-parameters customer-options** command to verify that **Private Networking** and **Uniform Dialing Plan** are enabled as shown below:

```
display system-parameters customer-options               Page   5 of  11
                                OPTIONAL FEATURES

               Multinational Locations? y            Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n     Station as Virtual Extension? y
                    Multiple Locations? y
                                           System Management Data Transfer? n
         Personal Station Access (PSA)? y              Tenant Partitioning? n
                       PNC Duplication? n      Terminal Trans. Init. (TTI)? y
                  Port Network Support? n              Time of Day Routing? n
                       Posted Messages? n      TN2501 VAL Maximum Capacity? y
                                                      Uniform Dialing Plan? y
                    Private Networking? y    Usage Allocation Enhancements? y
              Processor and System MSP? y
                    Processor Ethernet? y              Wideband Switching? n
                              Wireless? y
```

4.1.4 Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable 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: This feature can pose a significant security risk by increasing the risk of toll fraud and must be used with caution. To minimize the risk, a COS can be defined to allow trunk-to-trunk transfers for a specific trunk group(s). For more information regarding how to configure a Communication Manager to minimize toll fraud, see **Reference [9].**

```
change system-parameters features                                   Page   1 of  18
                                FEATURE-RELATED SYSTEM PARAMETERS
                                   Self Station Display Enabled? n
                                        Trunk-to-Trunk Transfer: all
                 Automatic Callback with Called Party Queuing? n
     Automatic Callback - No Answer Timeout Interval (rings): 3
```

4.2 Add Node Name of Avaya Aura^{TM} Session Manager

Using the **change node-names ip** command, add the node-name and IP address for the Session Manager SM-100 interface, if not previously added during the initial install of the solution. This same screen shows the node-name for the C-LAN interface which will be used in administering a SIP signaling-group in **Section 4.4**.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASM1-SM100          10.80.120.28
ASM2-SM100          10.80.120.30
VAL01a08            10.80.111.90
clan-1a04           10.80.111.76
default             0.0.0.0
gateway1            10.80.111.1
procr               10.80.111.73
xfire-1a02          10.80.111.77
```

4.3 Configure IP Network Regions

In the sample configuration shown in **Figure 1**, calls to/from Session Manager will be viewed by Communication Manager as calls to/from ip-network-region 2. Communication Manager and its endpoints are in ip-network-region 1. To enable communication between the two network regions requires additional administration of the **ip-network-region** and **signaling-group** forms as shown in the next few sections.

4.3.1 Configure IP Network Region 1

Using the **change ip-network-region 1** command, set the **Authoritative Domain** to the correct SIP domain for the configuration. Verify the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields are set to **yes**.

```
change ip-network-region 1                                Page   1 of  19
                                IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: avaya.com
    Name:
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: 16585
```

Navigate to Page 4 and connect ip-network-region 1 to ip-network-region 2 by typing a **y** under the **direct WAN** column for **dst rgn 2**. Select an ip **codec set** to be used for negotiating audio between the two regions as well. In this case ip-codec-set **2** was used. See **Section 4.3.3** for additional information on the ip-codec-set form.

```
change ip-network-region 1                                        Page   4 of  20

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    1                                                               all
 2    2     y    NoLimit                                             n       t
```

4.3.2 Configure IP Network Region 2

Using the **change ip-network-region 2** command, set the **Authoritative Domain** to the correct SIP domain for the configuration. Verify the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields are set to **yes**.

```
change ip-network-region 2                                Page   1 of  19
                                IP NETWORK REGION
  Region: 2
Location: 1        Authoritative Domain: avaya.com
    Name:
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: 16585
```

Navigate to Page 4 and verify that ip-network-region 1 and 2 are directly connected and use ip **codec set 2** as shown below.

```
change ip-network-region 2                                      Page   4 of  20

 Source Region: 2     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst  codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    2     y    NoLimit                                             n       t
 2    2                                                                all
 3
```

4.3.3 Administer IP Codec Set

In **Section 4.3.1 ip-codec-set 2** was chosen as the inter-region codec to be used for call between ip-network-region's 1 and 2. In the sample configuration G.711MuLaw was the preferred codec to be used for RTP audio between Communication Manager and the CS1000E, therefore ip-codec-set 2 will be configured to prefer this codec as well. Use the command **change ip-codec-set 2** to administer this codec-set.

- **Audio Codec** **G.711MU** is entered as the first choice. Optionally enter in a secondary **Codec l**ike **G.729A** to help ensure there will be two-way audio in most cases.

Leave all other fields at their defaults.

```
change ip-codec-set 2                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 2

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2: G.729A            n          2        20
 3:
```

4.4 Add SIP Signaling Group

Issue the **add signaling-group n** command, where **n** is an available signaling group number, for one of the SIP trunks to the Session Manager, and fill in the indicated fields. In the sample configuration, trunk group **10** and signaling group **10** were used to connect to Session Manager. Default values can be used for the remaining fields.

- **Group Type:** **sip**
- **Transport Method:** **tcp***(1)*
- **IMS Enabled?:** **n**
- **Peer Detection Enabled?** **y**
- **Near-end Node Name:** C-LAN node-name from **Section 4.2**
- **Far-end Node Name:** Session Manager SM-100 node name from **Section 4.2**
- **Near-end Listen Port:** **5060**
- **Far-end Listen Port:** **5060**
- **Far-end Network Region:** **2**
- **Far-end Domain:** Authoritative Domain from **Section 4.3.1**
- **Enable Layer 3 Test:** **y**
- **Session Estab. Timer:** **3***(2)*

```
display signaling-group 10
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                                   SIP Enabled LSP? n
     IP Video? n                                         Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: clan-1a04             Far-end Node Name: ASM1-SM100
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 2

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? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

(1) TCP was used for the sample configuration. However, TLS would typically be used in production environments.
(2) If any call originating from the SIP phone is not expected to be answered within 3 minutes such would happen if the call is made to a VDN and agents are not available within 3 minutes, this value may need to be increased.

4.5 Add SIP Trunk Group

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where "n" is an available trunk group number and fill in the indicated fields.

- **Group Type:** **sip**
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code
- **Direction** **two-way** for both incoming and outgoing calls
- **Service Type:** **tie**
- **Signaling Group:** The number of the signaling group added in **Section 4.4**
- **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 number of trunks configured in **Section 4.1.1**)

```
add trunk-group 10                                             Page   1 of  21
                                TRUNK GROUP

Group Number: 10                   Group Type: sip           CDR Reports: y
  Group Name: to ASM1                     COR: 1        TN: 1        TAC: #10
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 10
                                                     Number of Members: 25
```

Once the add command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

On **Page 2**, set the **Preferred Minimum Session Refresh Interval** to **1200**.

Note: To avoid extra SIP messages, all SIP trunks connected to Session Manager should be configured with a minimum value of 1200.

```
add trunk-group 10                                             Page   2 of  21
                                     Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                                 Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 1200
```

On **Page 3**, set **Numbering Format** to be **private**. Use default values for all other fields.

```
add trunk-group 10                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n             Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                  UUI Treatment: service-provider

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

4.6 Administer Private Numbering

SIP Users registered to Session Manager need to be added to either the private or public numbering table on the Communication Manager Evolution Server. For the sample configuration, **private** numbering was used and all extension numbers were unique within the private network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in **References [5]** and **[6]**.

To enable SIP endpoints to send their caller ID number when dialing over a trunk you must define their extension pattern on either the **private** or **public-numbering** table. In **Section 4.5** trunk-group 10 was configured as **private**. Use the command **change private-numbering 7** to define the caller ID number which will be sent out with the call. For the sample configuration, extension numbers in the range of 666xxxx are used on the Evolution Server.

- **Ext Len:** Enter the extension length allowed by the dial plan
- **Ext Code:** Enter leading digit (s) from extension number
- **Trunk Grp:** Enter the SIP Trunk Group number for the SIP trunk between the Evolution Server and Session Manager
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix

```
change private-numbering 7                                        Page   1 of  2
                            NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 7  6                10                          7     Total Administered: 1
                                                       Maximum Entries: 540
```

4.7 Administer Call Routing

There are several administration screens one must edit in order to enable 7-digit dialing from Communication Manager to Session Manager (and ultimately to the CS1000) without the need to dial a Feature Access Code (FAC) like **9** or ***9**. These steps are shown in the next few sections.

4.7.1 Administer DialPlan Analysis

In the screenshot below, the following entries we added using the **change dialplan analysis** command:

- **Dialed String** ‘**666**’ was added for extensions local to Communication Manager
  ‘**777**’ was added for extensions on the CS1000E
- **Total Length** ‘**7**’.
- **Call Type** ‘**Ext**’

```
change dialplan analysis                                           Page   1 of  12
                              DIAL PLAN ANALYSIS TABLE
                                    Location: all          Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   0           1   attd
   1           2   dac
   2           2   fac
   666         7   ext
   777         7   ext
   8           1   fac
   9           1   fac
   *           3   dac
   #           3   dac
```

4.7.2 Administer Uniform Dialplan

Using the command **change uniform-dialplan 7** make the following changes:

- **Matching Pattern** **777**
- **Len** **7** Length of digit string
- **Del** **0** Number of digits to delete
- **Net** **aar**

```
change uniform-dialplan 7                                         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
                                             n
```

4.7.3 Administer AAR table

In the sample configuration the AAR table is used for two purposes: To route calls to 777xxx (calls to the CS1000E) from Communication Manager to Session Manager as well as to route calls to 96xx SIP telephones which are registered to Session Manager and are in the 666xxxx extension range. Using the command **change aar analysis 6**, make the following changes which instruct Communication Manager to use the appropriate route-patern for a given digit string.

- **Dialed String** **777** & **666**
- **Total Min** **7** Minimum number of dialed digits
- **Total Max** **7** Maximum number of dialed digits
- **Route Pattern** **10** (route-pattern admin shown in next section)
- **Call type** **unku** Unknown numbering plan

```
change aar analysis 6                                             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     10       unku         n
    666                    6    6     10       unku         n
```

4.7.4 Administer Route Pattern

The final step for enabling 7-digit dialing to Session Manager is to add the trunk group created in **Section 4.5** to a route pattern. Use the command **change route-pattern 10** to add trunk-group 10 to the route pattern.

- **Pattern Name** Use a descriptive name for the route pattern
- **Grp No** **10** Trunk-group number created in **Section 4.5**
- **FRL** **0** Restriction Level with '0' being the least restrictive

```
change route-pattern 10                                        Page   1 of   3
                    Pattern Number: 10  Pattern Name: ASM1-6.0
                             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: 10   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
```

4.8 Configure Stations

For each SIP user to be defined in Session Manager, add a corresponding station on the Communication Manager Evolution Server.

Note: Instead of manually defining each station using the Communication Manager SAT interface, an alternative option is to automatically generate the SIP station when adding a new SIP user in System Manager. See **Section 5.9** for more information on adding SIP users.

The phone number defined for the station will be the number the SIP user enters to register to Session Manager. Use the "**add station x**" command where x is a valid extension number defined in the system. On **Page 1** of the change station form:

- **Phone Type:** Set to **9630SIP**
- **Name:** Display name for user
- **Security Code:** Numeric password used when user logs into station. **Note:** this code should match the **Shared Communication Profile Password** field defined when adding this user in Session Manager. See **Section 4.9**

```
add station 6664400                                        Page   1 of   6

                                   STATION

Extension: 666-4400                         Lock Messages? n            BCC: 0
     Type: 9630SIP                          Security Code: 123456        TN: 1
     Port: S00006                         Coverage Path 1: 1            COR: 1
     Name: John Smith                     Coverage Path 2:              COS: 1
                                          Hunt-to Station:
STATION OPTIONS
                                              Time of Day Lock Table:
              Loss Group: 19
                                                    Message Lamp Ext: 666-4400
        Display Language: english                     Button Modules: 0
          Survivable COR: internal
   Survivable Trunk Dest? y                             IP SoftPhone? n

                                                            IP Video? n
```

On **Page 6**, set the following:

-**SIP Trunk :** **AAR** which corresponds to the '666' entry from **Section 4.7.3**

```
change station 6664400                                     Page   6 of   6

                                   STATION
SIP FEATURE OPTIONS
         Type of 3PCC Enabled: None
                    SIP Trunk: AAR
```

4.9 Verify Off-Pbx Telephone Station-Mapping

Use the **display off-pbx-telephone station-mapping** command for each extension associated with SIP users defined in Session Manager to verify settings:

```
display off-pbx-telephone station-mapping 6664400              Page   1 of  3

                STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk      Config  Dual
 Extension                 Prefix                     Selection  Set     Mode
 666-4400         OPS          -      6664400          AAR          1
                               -
                               -
```

On **Page 2**, verify the following values:

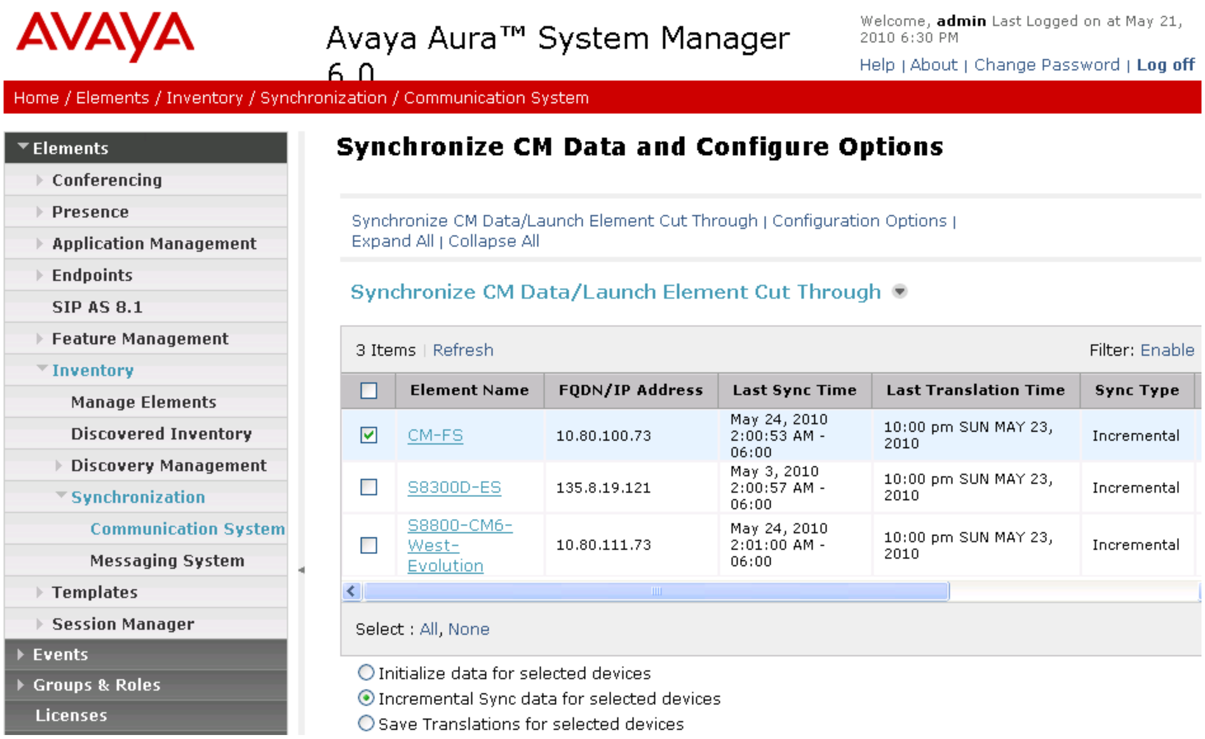
- **Mapping Mode**: **both**
- **Calls Allowed:** **all**

```
change off-pbx-telephone station-mapping 6664400              Page   2 of  3

                STATIONS WITH OFF-PBX TELEPHONE INTEGRATION


 Station       Appl    Call         Mapping    Calls      Bridged     Location
 Extension     Name    Limit        Mode       Allowed    Calls
 666-4400      OPS      3           both       all         none
                               -
```

4.10 Save Translation

Configuration of Communication Manager Evolution Server is complete. Use the **save translation** command to save these changes

Note: After a change on Communication which alters the dial plan, synchronization between Communication Manager and Session Manager needs to be completed and SIP phones must be re-registered. To request an on demand synchronization, log into the System Manager console, navigate to **Elements → Inventory → Synchronization → Communication System** and initiate an incremental syncronization of Communication Manager as shown below:

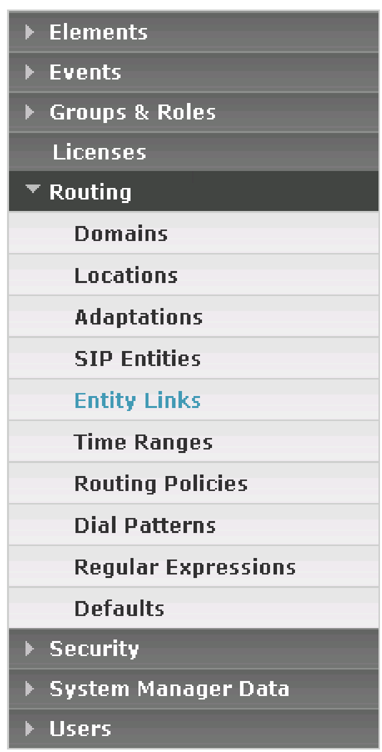


5. Configure Avaya Aura™ Session Manager

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

- Administer SIP domain
- Define Logical/physical Locations that can be occupied by SIP Entities
- Add Session Manager to System Manager
- For each SIP Entity in the sample configuration:
  - Define SIP Entity
  - Define Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
  - Define Routing Policies, which control call routing between the SIP Entities
  - Define Dial Patterns, which govern to which SIP Entity a call is routed
- Administer CM-ES as a 'Sequenced Application'.
- Define the Communication Manager Evolution Server as an administrable entity
- Adding SIP Endpoints/SIP users in System Manager

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. Expand the **Routing** link on the left side of Navigation Menu. Select a specific item such as **SIP Entities**. When the specific item is selected, the color of the item will change to blue as shown below:

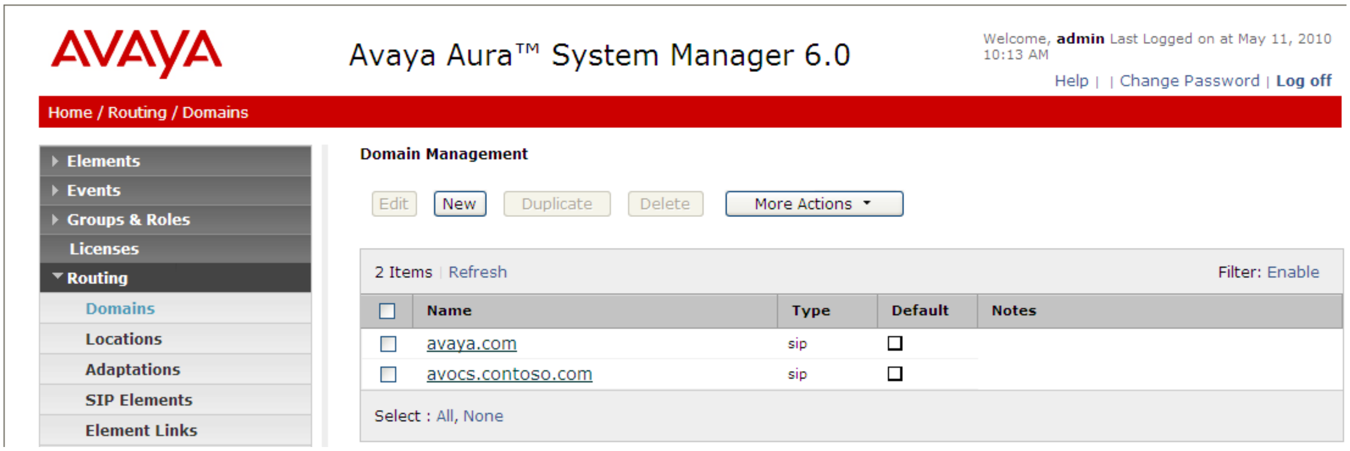


5.1 Administer SIP Domains

Expand **Routing** as described above and select **Domains**.

- Click **New**
- In the **General** Section, under **Name** add a domain name. Under **Notes** add a brief description
- Click **Commit** to save.

The screen below shows the information for the sample configuration.

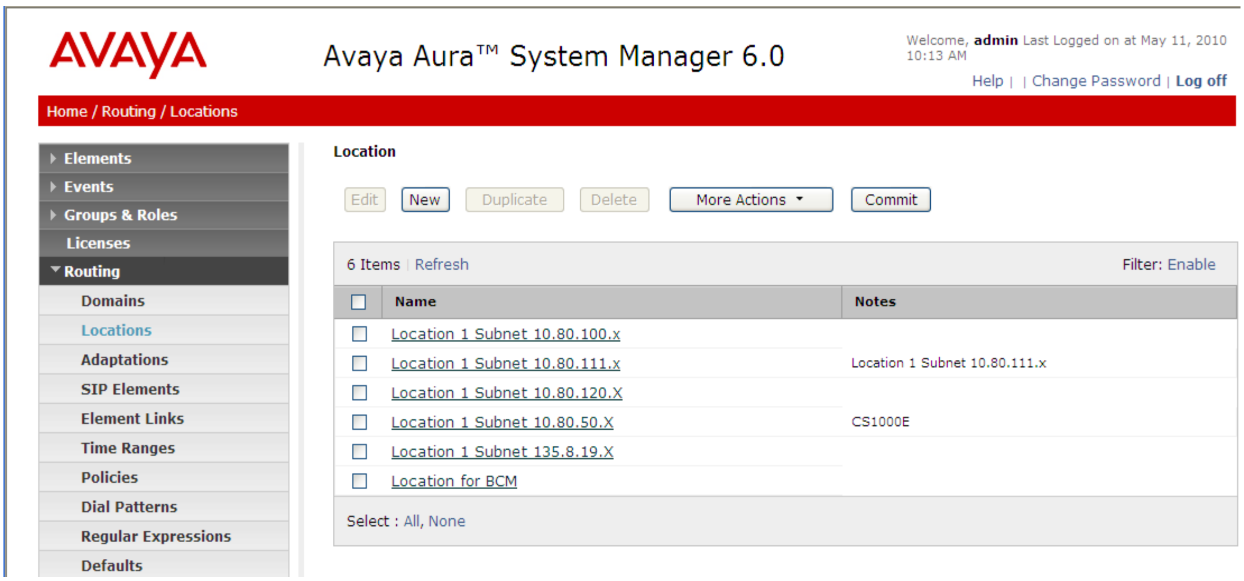


5.2 Define Locations

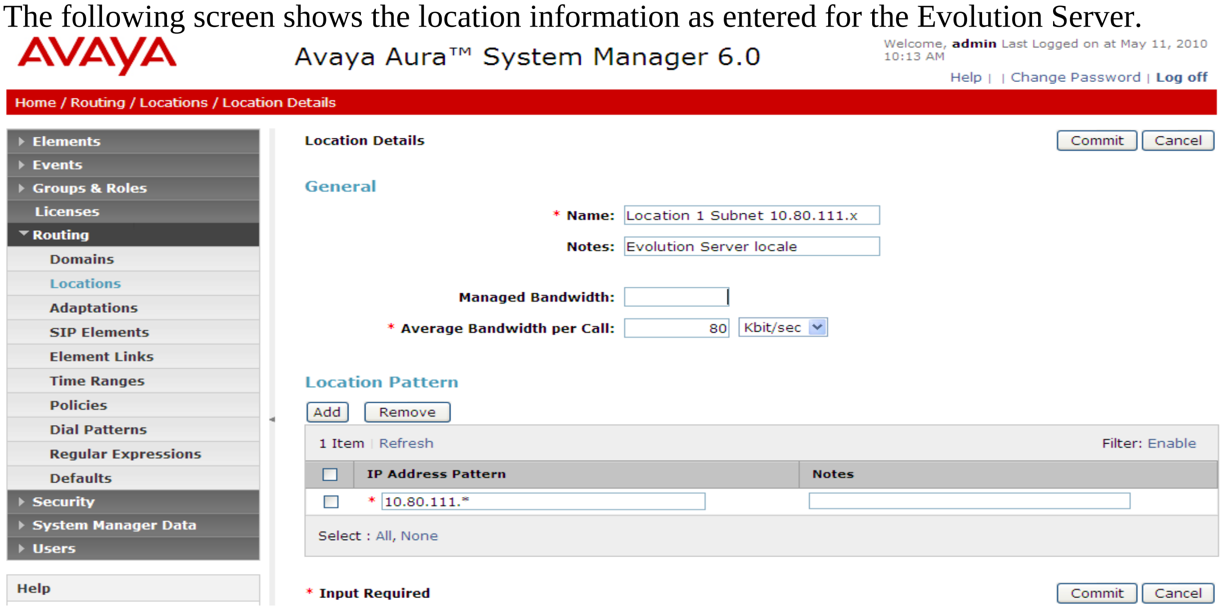
Expand **Routing** and select **Locations.** Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing. Click **New** to create a new location.

- **Name** Add a descriptive name for the location
- **Notes** Add a brief description
- **IP Address Pattern** Enter pattern used to logically identify the location Under **Notes** add a brief description

The screen below shows the information for the CS1000E in the sample configuration.



The following screen shows the location information as entered for the Evolution Server.

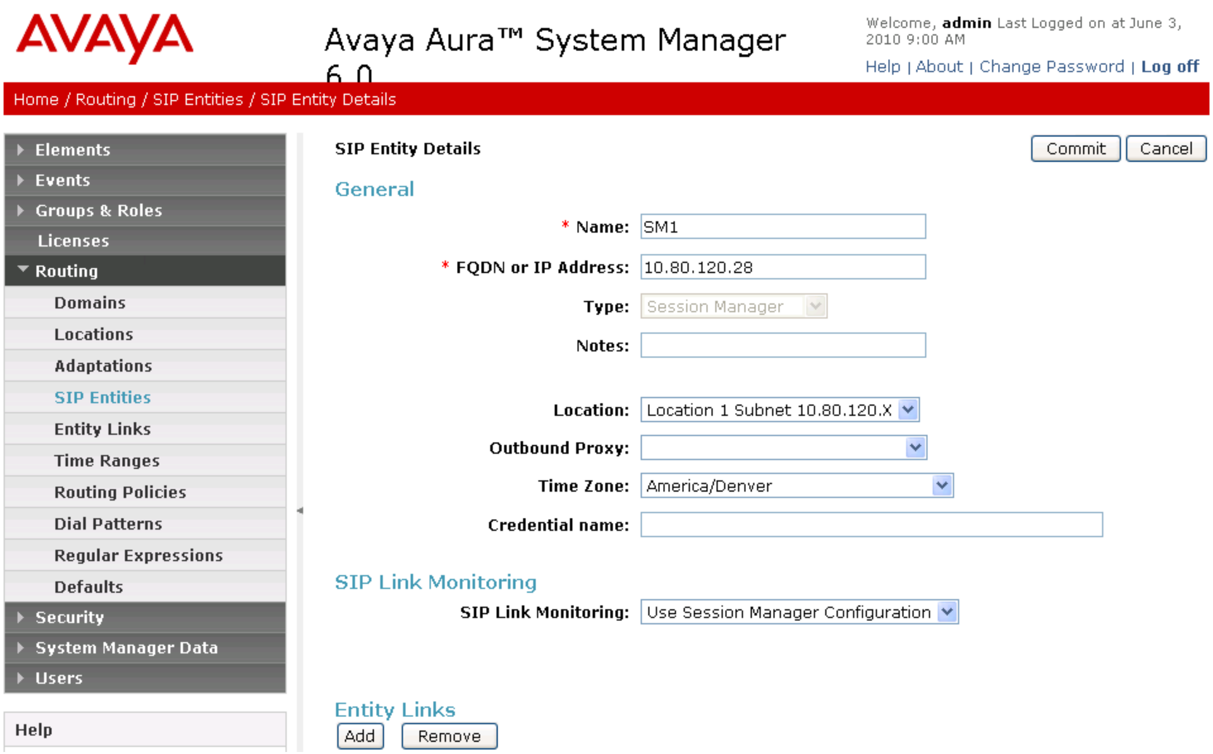


5.3 Add SIP Entities

5.3.1 Define Avaya Aura™ Session Manager as a SIP Entity

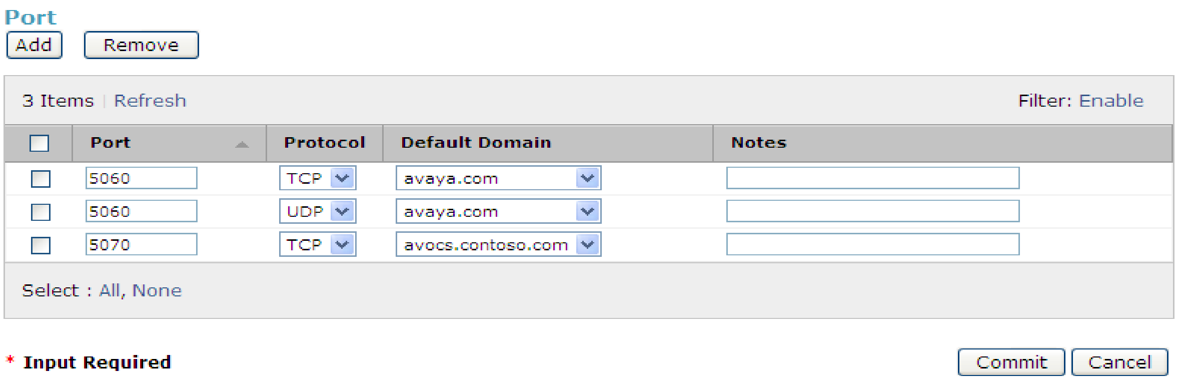
One of the first steps in properly setting up Session Manager and System Manager is to add Session Manager as SIP Entity. Generally this is done during the initial installation of Session Manager and System manager. To do this, log in to System Manager and from the left-side navigation pane, expand the **Routing** link by selecting it, and then select **SIP Entities**. Fill in the fields as described and shown below. Click **Commit** to complete:

- **Name** A descriptive name
- **FQDN or IP Addr** Hostname or IP address of the SM-100 interface in Session Mgr.
- **Type** **Session Manager**
- **Notes** Free-form text
- **Location** Appropriate location created in **Section 5.2**
- **Oubound Proxy** Leave blank
- **Time Zone** Time zone value appropriate for the physical location
- **Sip Link Mon** Usually set to **Use Session Mgr Config** though it can be customized on a per-element basis



5.3.2 Define Ports for Use by Avaya Aura™ Session Manager

Session Manager has the ability to translate communication between two SIP entities that 'talk' using different ports and protocols. However to do so, it's necessary to define the ports and protocols that Session Manager will need to communicate with. The screen shot shown below is the lower half of the same screen used to add/edit Session Manager as a SIP Entity and discussed in the previous section. As shown below, two ports (**5060** & **5070**) and 2 protocols (**TCP** & **UDP**) are defined for one instance of Session Manager. TLS can also be configured.



5.3.3 Add Avaya Aura™ Session Manager to System Manager

To complete the linkage between System Manager and Session Manager it's necessary to identify the SIP Entity created in the previous section as an instance of Session Manager to System Manager. Generally this is done during the initial installation of System Manager and Session Manager.

As shown below, expand the **Elements** menu on the left pane then select **Session Manager** then **Session Manager Administration**. Then click **New** (not shown), and fill in the fields as described below and shown in the following screen:

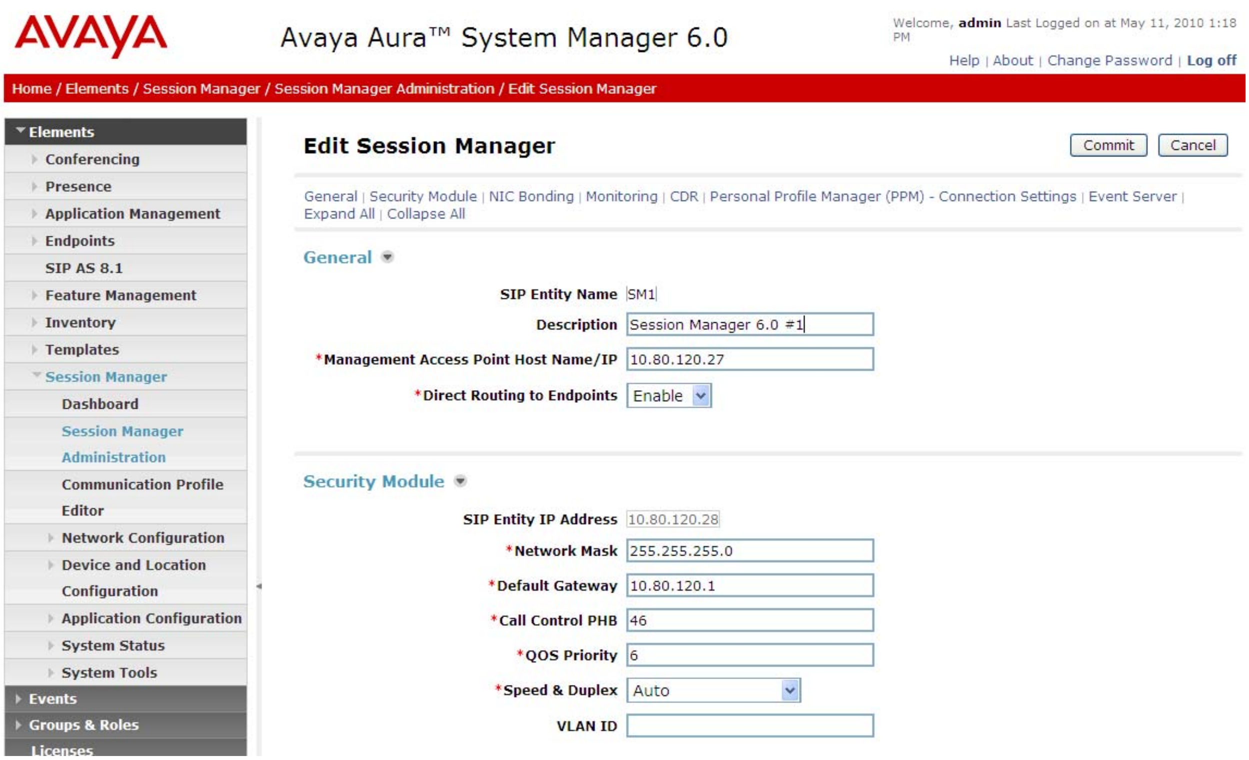
Under *General*:

- **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 (not the SIP Entity address).

Under *Security Module*:

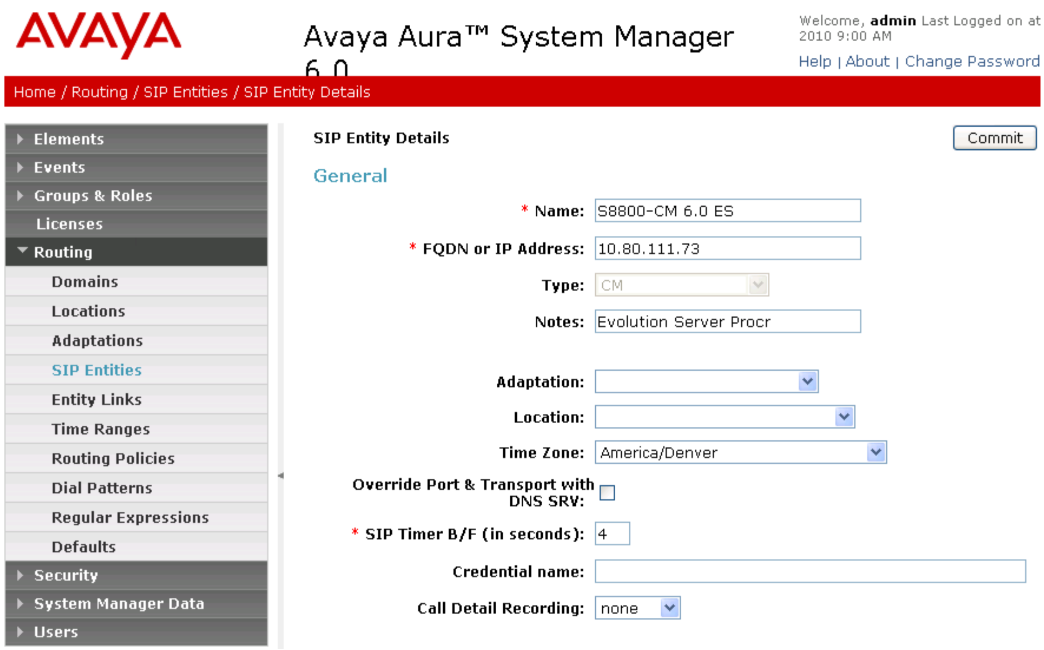
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager. The screen below shows the resulting Session Manager definition.



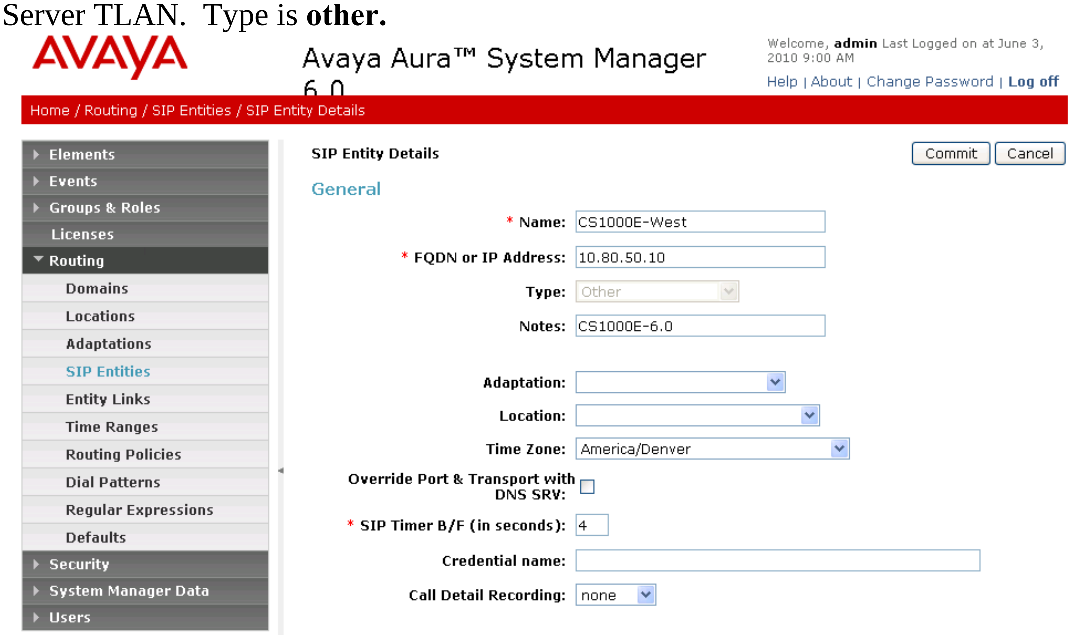
5.3.4 Define a SIP Entity for Avaya Aura™ Communication Manager Evolution Server

The following screen shows the addition of Communication Manager Evolution Server as a SIP Entity. The IP address shown below is that of the near-end node used on the signaling-group form from **Section 4.2**.



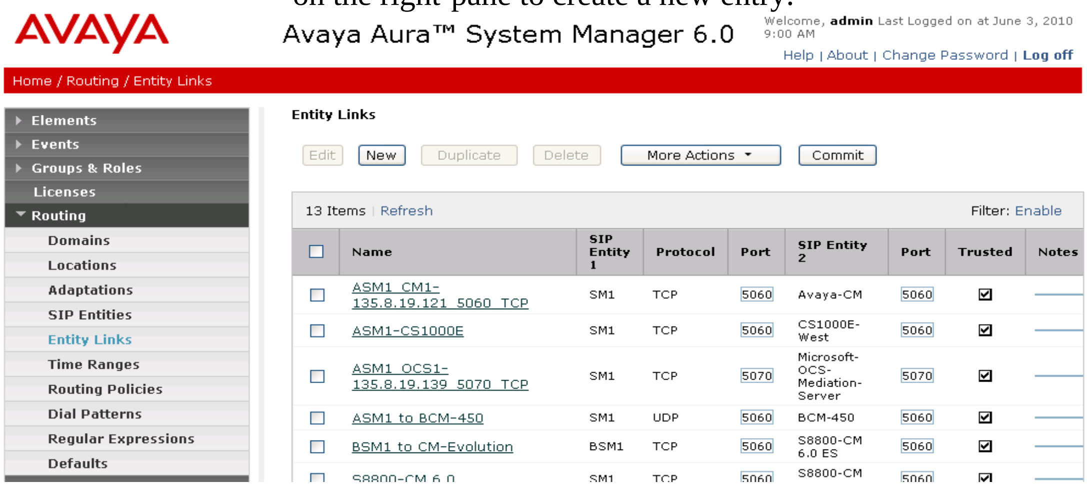
5.3.5 Define a SIP Entity for the CS1000E

The following screen shows the addition of the CS1000E as a SIP Entity. The IP address is that of the Signaling Server TLAN. Type is **other.**



5.4 **Create Entity Links**

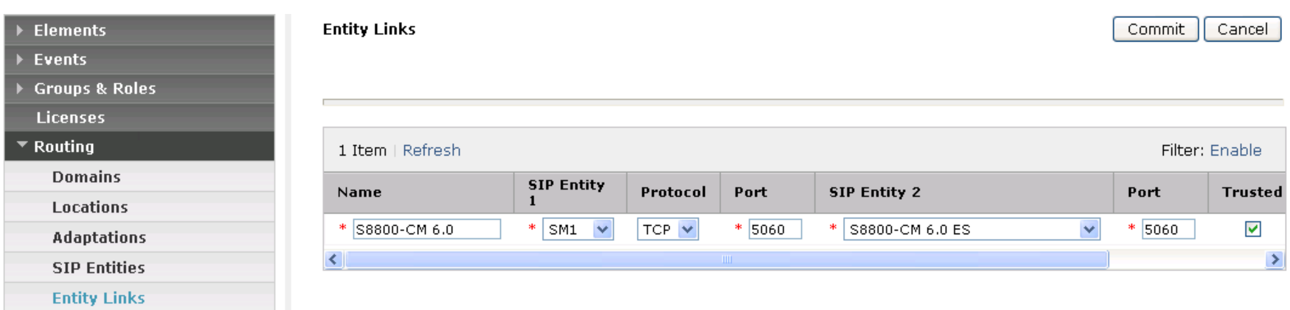
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. To add an Entity Link, expand **Routing** from the left-pane then select **Entity Links**. Click on the **New** button on the right-pane to create a new entry.

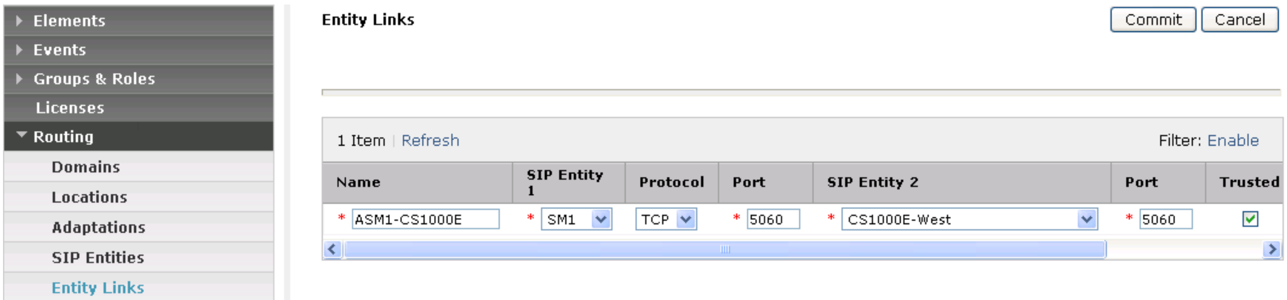


Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1** Select the **Session Manager.**
- **Protocol** Select **TCP**, **TLS** or **UDP** from the dropdown
- **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 5.3** will be denied.

Click **Commit** to save each Entity Link definition. The following screens illustrate the Entity Links for Communication Manager Evolution Server and the CS1000, both of which use port 5060 and TCP to communicate with Session Manager.





5.5 Add Routing Policies

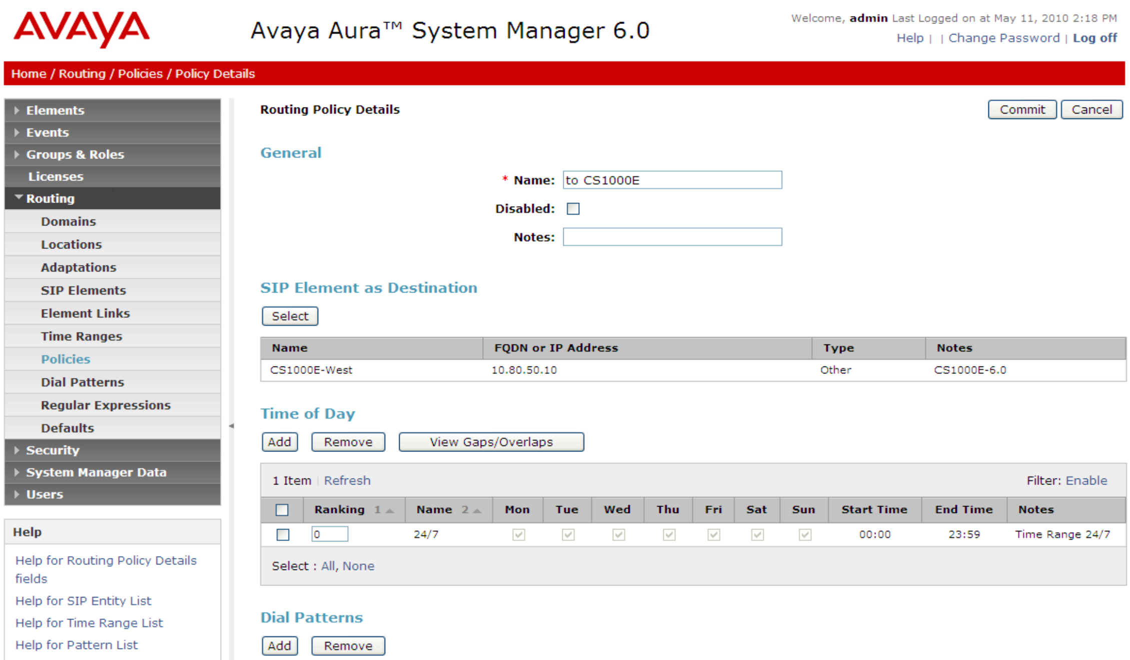
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 5.3**. Routing policies for Communication Manager and the CS1000 need to be added. For 96xx SIP telephones registered to Session Manager, the necessary SIP communication between Session Manager and Evolution Server happens as a result of administering a 'Sequenced Application' shown in **Section 5.7**.

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:

- **General** Enter a descriptive name in **Name**.
- **SIP Entity as Destination** Click **Select**, and then select the appropriate SIP Entity to which this routing policy applies**.**
- **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 screen shows the Routing Policy to send calls to the Communication Server 1000.



5.6 Add Dial Patterns

Define dial patterns to direct calls to the appropriate SIP Entity. Calls to 7-digit extensions beginning with “777xxxx” should be routed to the Communication Server 1000. Calls to 7-digit extensions beginning with “666xxx” should be routed to Communication Manager.

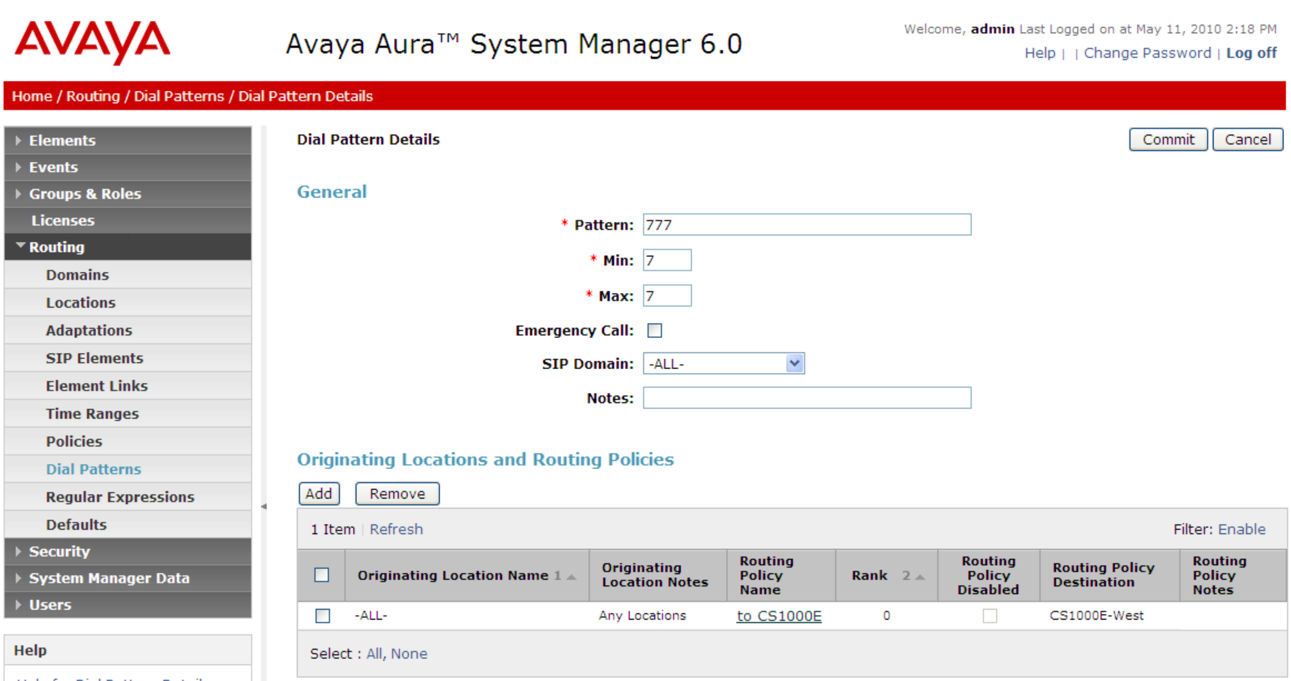
Note: Calls to 96xx SIP phones do not rely on a dial pattern for call routing. Since these phones are registered directly to Session Manager they utilize a “Sequenced Application” to make use of Communication Manager’s call features. This administration is shown in **Section 5.8**. To add a dial pattern, 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**:

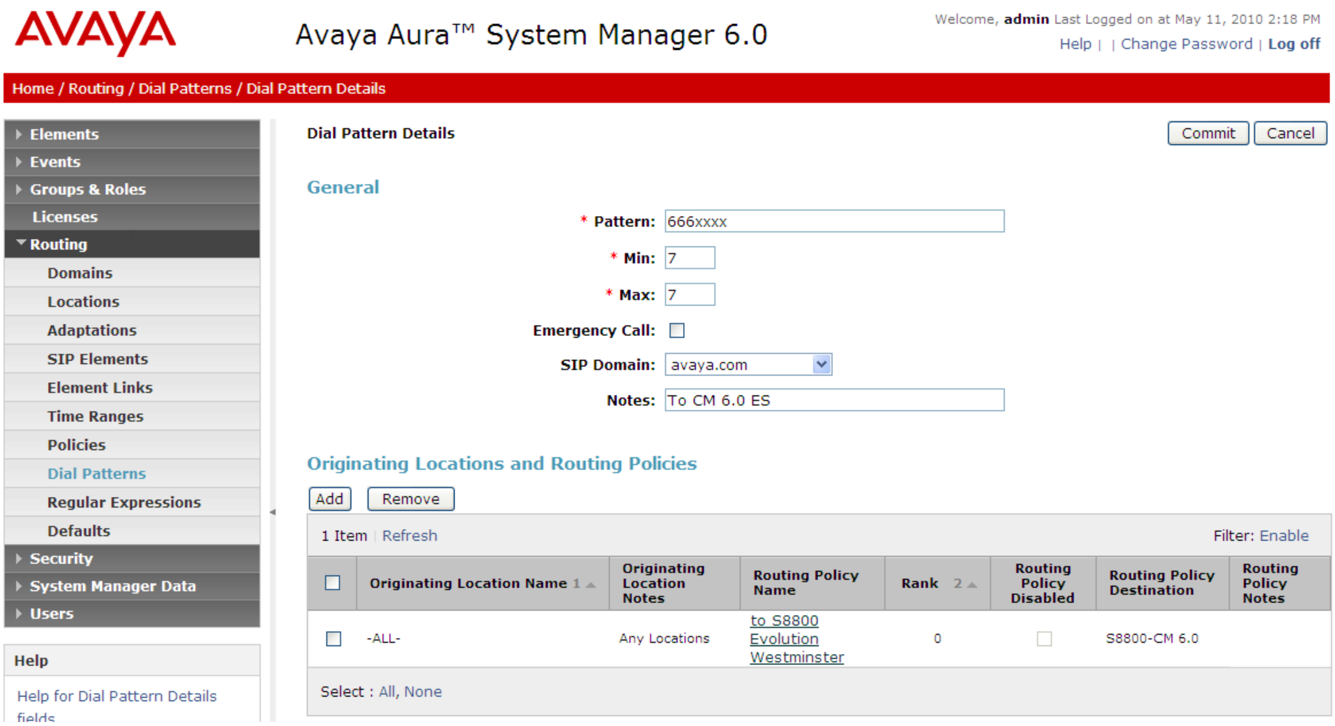
- **Pattern:** Dialed number or prefix
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **SIP Domain:** SIP domain specified in **Section 4.1**
- **Notes:** Comment on purpose of dial pattern.

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 the dial pattern. The following screenshot shows the dial pattern for routing calls to the Communication Server 1000.



The following screenshot shows the dial pattern for routing calls to the Communcation Manager Evolution Server.


AVAYA
Avaya Aura™ System Manager 6.0
Welcome, admin Last Logged on at May 11, 2010 2:18 PM
Help | | Change Password | Log off
Home / Routing / Dial Patterns / Dial Pattern Details
Elements
Events
Groups & Roles
Licenses
Routing
Domains
Locations
Adaptations
SIP Elements
Element Links
Time Ranges
Policies
Dial Patterns
Regular Expressions
Defaults
Security
System Manager Data
Users
Help
Help for Dial Pattern Details fields
Dial Pattern Details
Commit
Cancel
General
* Pattern: 666xxxx
* Min: 7
* Max: 7
Emergency Call:
SIP Domain: avaya.com
Notes: To CM 6.0 ES
Originating Locations and Routing Policies
Add
Remove
1 Item | Refresh
Filter: Enable
Originating Location Name
Originating Location Notes
Routing Policy Name
Rank
Routing Policy Disabled
Routing Policy Destination
Routing Policy Notes
-ALL-
Any Locations
to S8800 Evolution Westminster
0
S8800-CM 6.0
Select : All, None

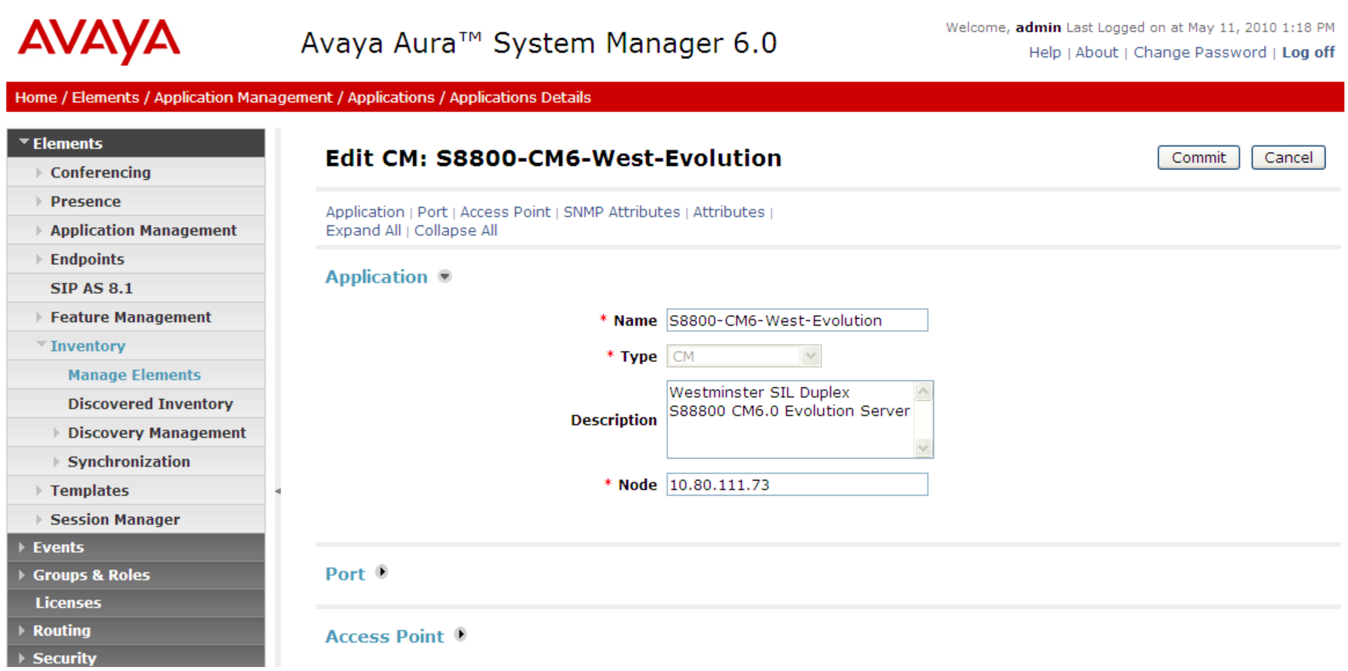
5.7 Define Avaya Aura™ Communication Manager Evolution Server as an Administrable Entity

Before adding SIP users, the Communication Manager Evolution Server must be added to System Manager as an administrable entity. This action allows System Manager to access Communication Manager over its administration interface similar to how other administration tools such as Avaya Site Administration access Communication Manager. Using this administration interface, System Manager will notify the Communication Manager Evolution Server when new SIP users are added.

5.7.1 Add Avaya Aura™ Communication Manager as an Administerable Element

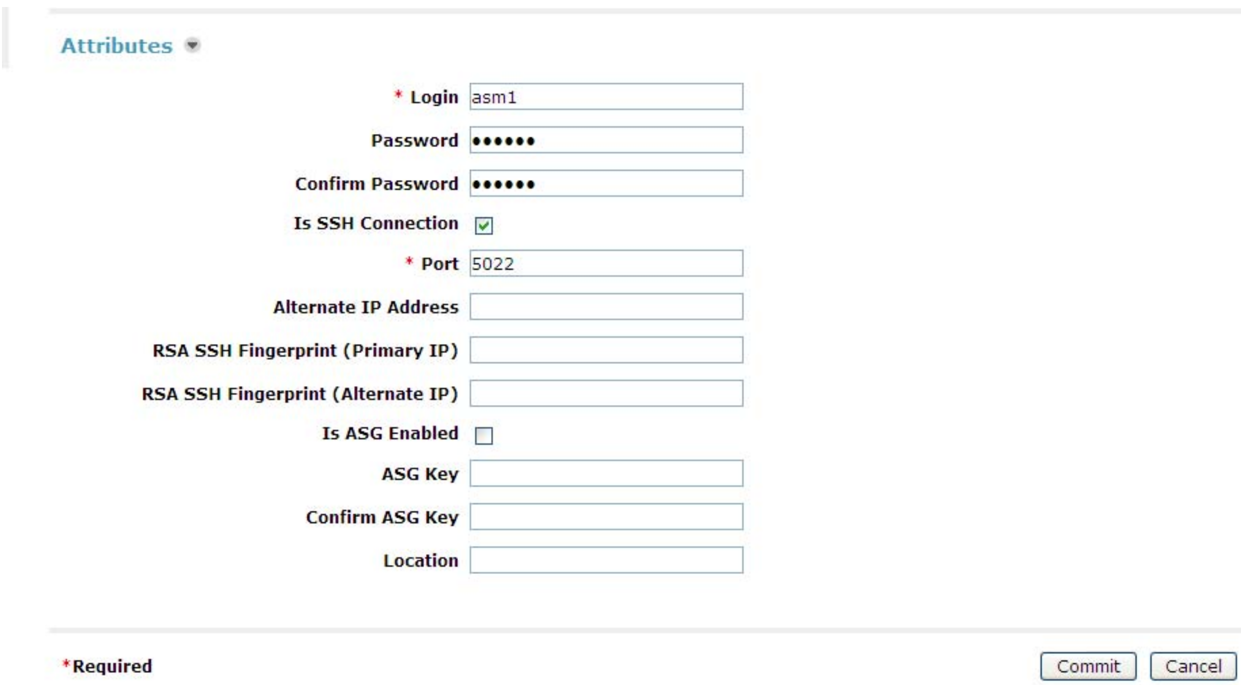
To define the Communication Manager Evolution Server as an administrable entity go to **Elements → Inventory → Manage Elements** and select **New** (not shown). In the section titled **Application** enter in the following information:

- **Type** Select **CM** from the drop-down
- **Name** Enter an identifier for the Communication Manager Evolution Server.
- **Node** Enter the IP address of the administration interface for the Evolution Server



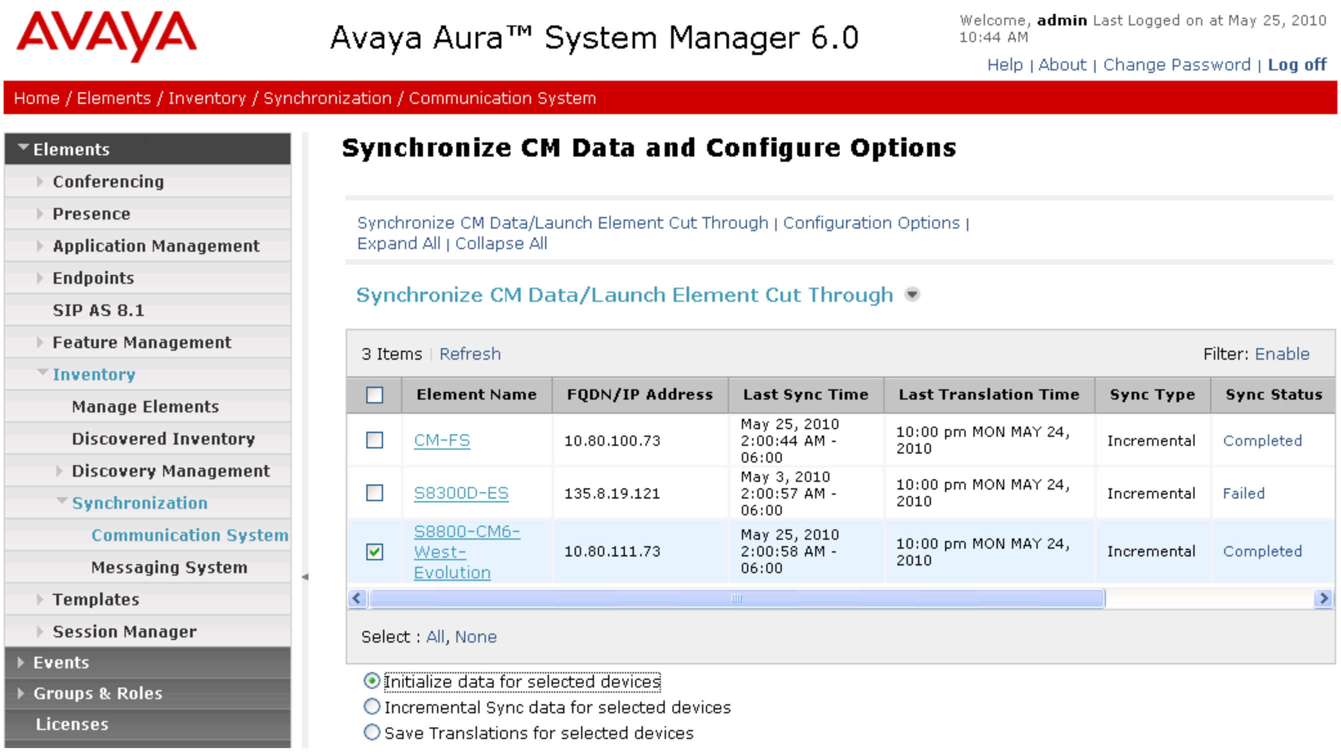
Scroll down to the section titled **Attributes** and enter the following login information for Communication Manager:

- **Login** — Enter a login ID that System Manager will use to login to a **SAT** **s**ession on Communication Manager.
  NOTE: This login ID should be dedicated for System Manager's use only.
- **Password/Confirm** — Password for the login used in the above field
- **Is SSH Connection** — Check this box if SSH access has been enbabled for SAT access to Communication Manager. SSH is enabled by default on Communication Manager.
- **Port** — **5022** if SSH is enabled (default). 5023 if Telnet is enabled.



5.7.2 Synchronize Communication Manager with System Manager

Select **Elements → Inventory → Manage Elements → Synchronization → Communication System** on the left. Check the appropriate **Element Name**, click **Initialize data for selected devices** and click **Now**. This may take some time to complete while System Manager examines the entire configuration on Communication Manager.



5.8 Define an Application Sequence for Avaya Aura™ Communication Manager Evolution Server

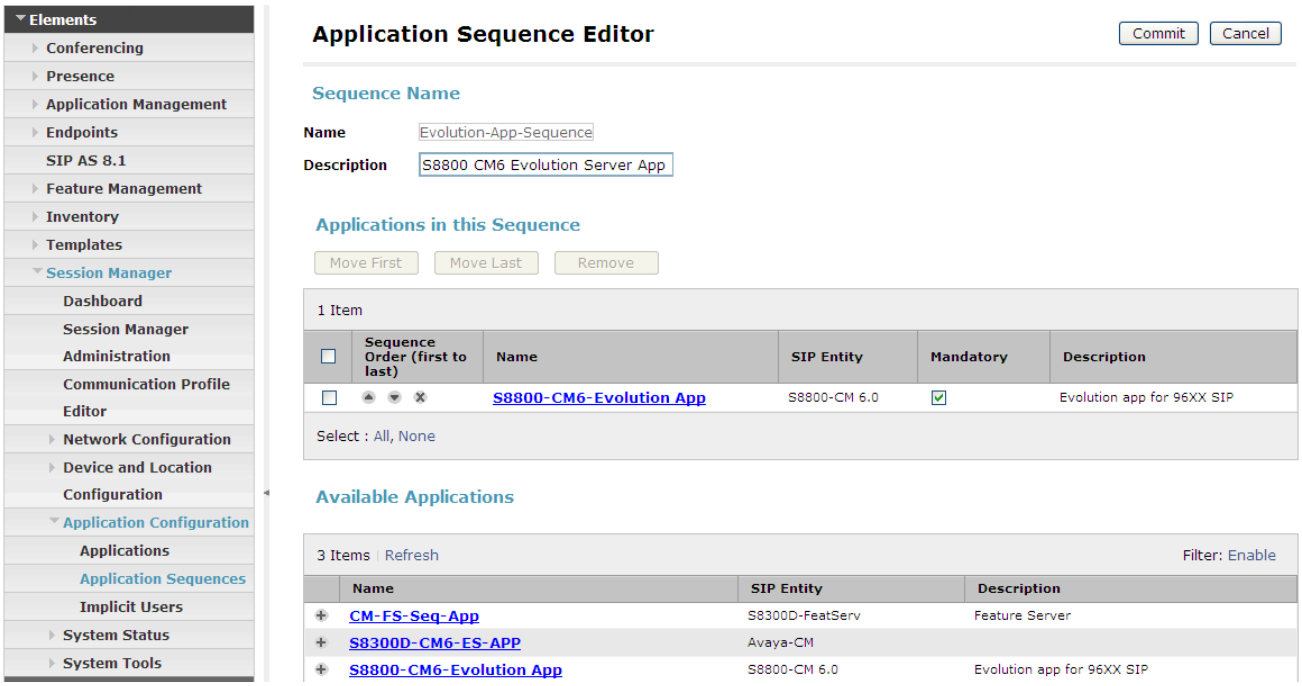
In order for 96xx SIP telephones registered to Session Manager to get call features from a Communication Manager instance, it's necess to define the Communication Manager Evolution Server as a Sequenced Application.To administer this, from the menu on the left select, **Elements → Session Manager → Application Configuration → Applications**

Select **NEW** (not shown) to define an application for Communication Manager Evolution Server. Fill in the following information as shown below:

- **Name** A descriptive name for the Application
- **SIP Entity** Select the appropriate SIP Entity (Element) from the drop-down
- **CM System for SIP Entity** Select CM System added in **Section 5.7**
- **Description** Any additional information about the Application

Next select **Application Sequences** and define an application sequence for the Communication Manager Evolution Server as shown below:

- **Name** — A name for the Application Sequence
- **Description** — More descriptive info for the same Application Sequence
- **Applications in this Sequence** — Select the + symbol next to the **Available Application** to be used in this sequence. This will add the Application to the **Applications in this Sequence** section as shown below



5.9 Add SIP Users

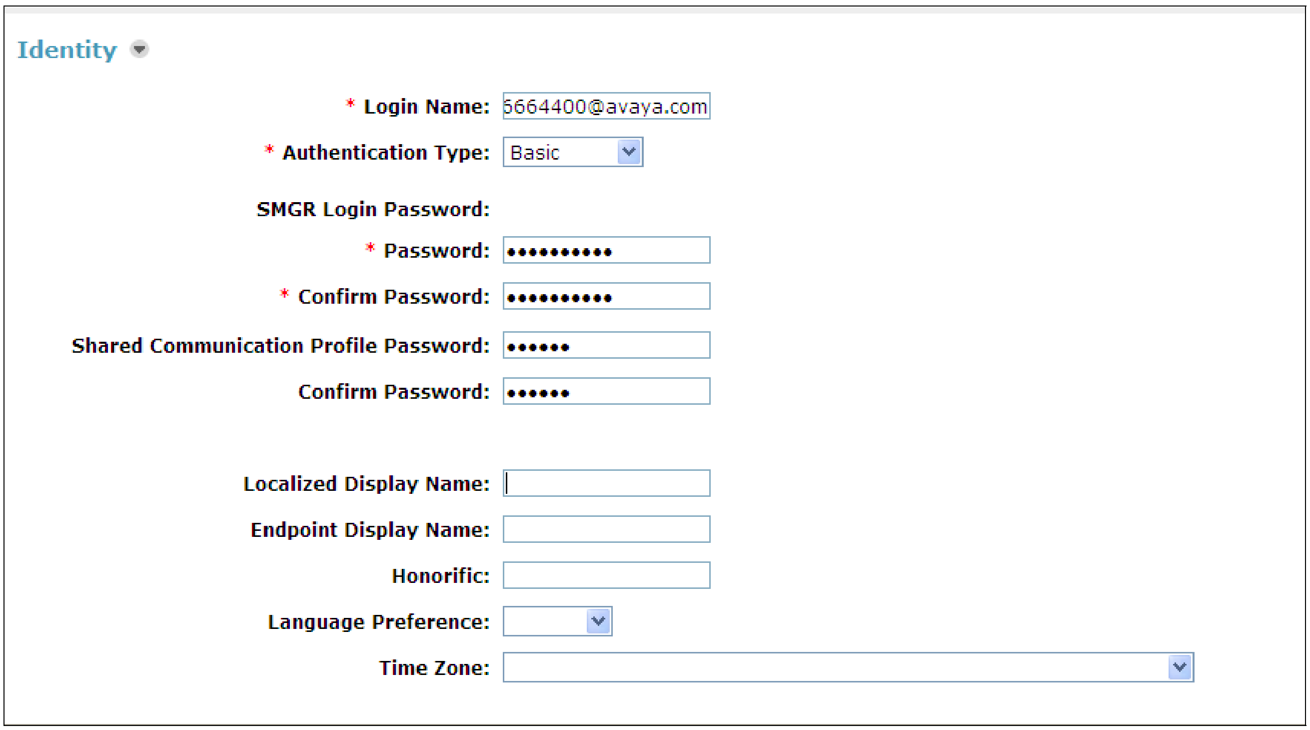
Add SIP users corresponding to the 96xx SIP stations defined in **Section 4.7.** Alternatively, use the option to automatically generate the SIP stations on Communication Manager Evolution Server when adding a new SIP user. To begin entering user info, from the left pane navigate to **Users → Manage Users** and select **New** (not shown).

Step 1: Enter values for the following required attributes for a new SIP user in the **General** section of the new user form.

- **Last Name:** Enter last name of user
- **First Name:** Enter first name of user

Step 2: Enter values for the following required attributes in the **Identity** section.

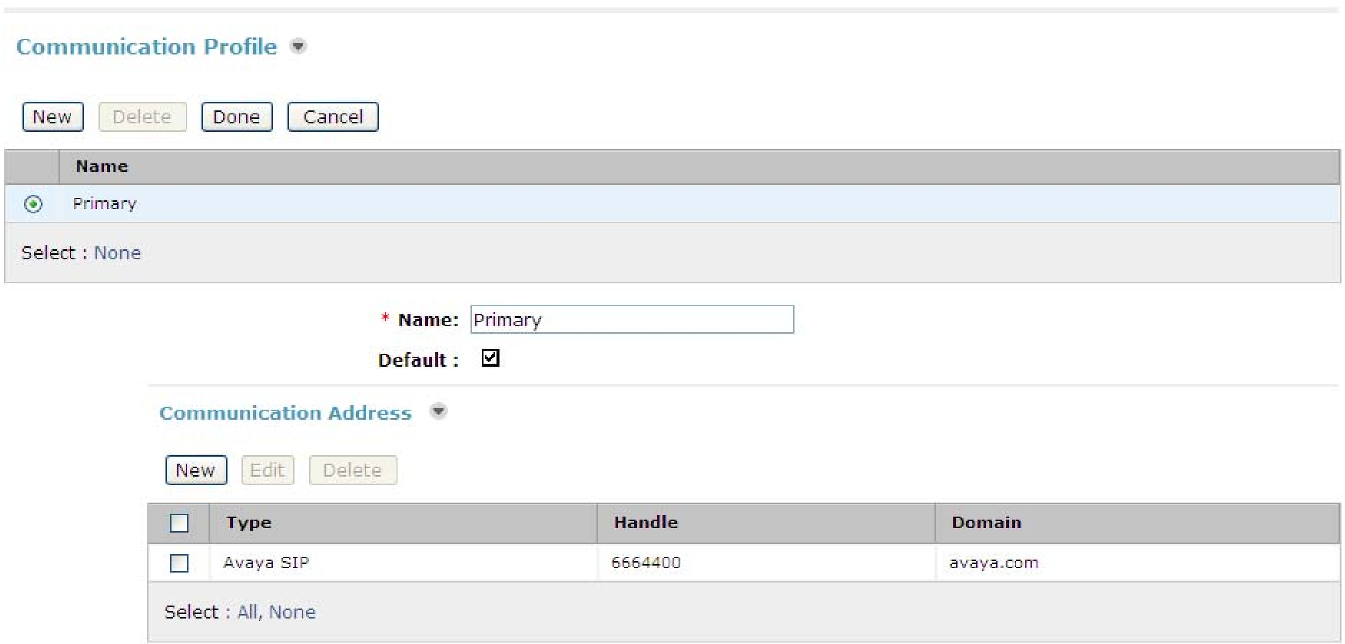
- **Login Name:** Enter extension xxx@sip domain defined in **Section 5.1**. This field is the primary handle of the user
- **Authentication Type:** Select **Basic**
- **SMGR Login Password:** Enter an alphanumeric password which will be used to log into the System Manager application
- **Confirm Password:** Repeat value entered above
- **Shared Comm. Profile Pass.:** Enter a numeric value which will be used by the SIP phone to login to Session Manager. *Note*: this field must match the **Security Code** field on the station form defined in **Section 4.7.**
- **Confirm Password:** Repeat numeric password



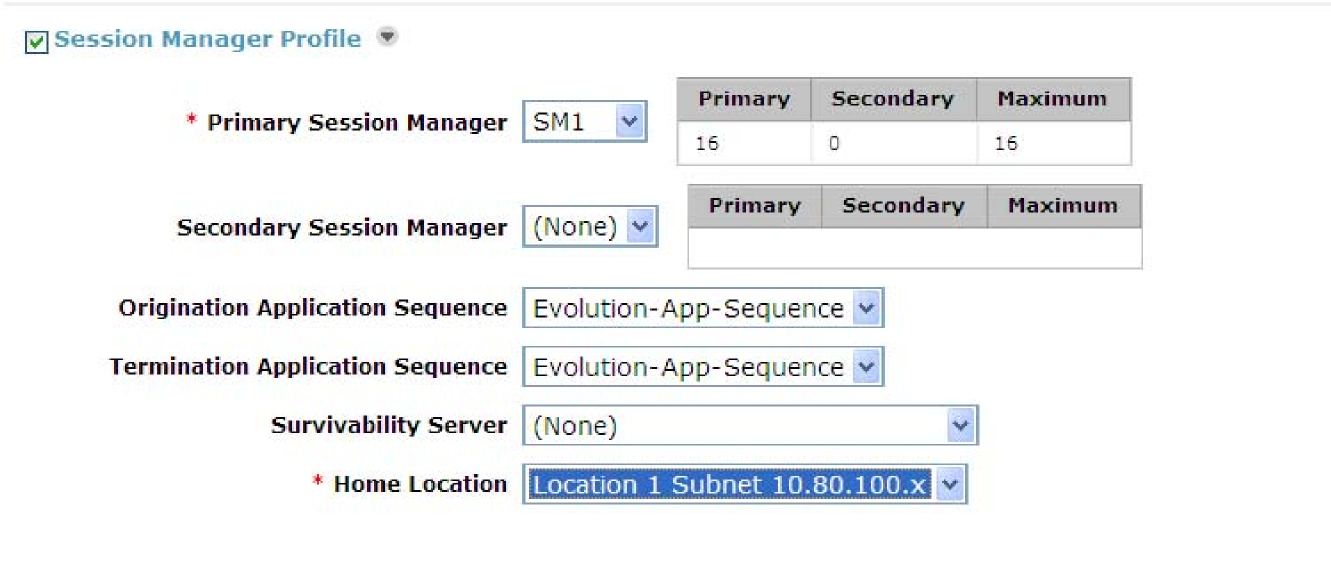
Step 3: Scroll down to the **Communication Profile** section and expand the view by selecting the icon. There should already be one profile called **Primary** which is already defined as the default. Select **New** to define a **Communication Address** for the new SIP user. Enter values for the following required attributes:

- **Type:** Select **SIP**
- **SubType:** Select username
- **Handle:** Enter extension number
- **Domain:** Enter SIP domain defined in **Section 5.1**

Once the above information is entered select **Add** to create the new Communication Address. The screen below shows the completed information when adding a new SIP user to the sample configuration.



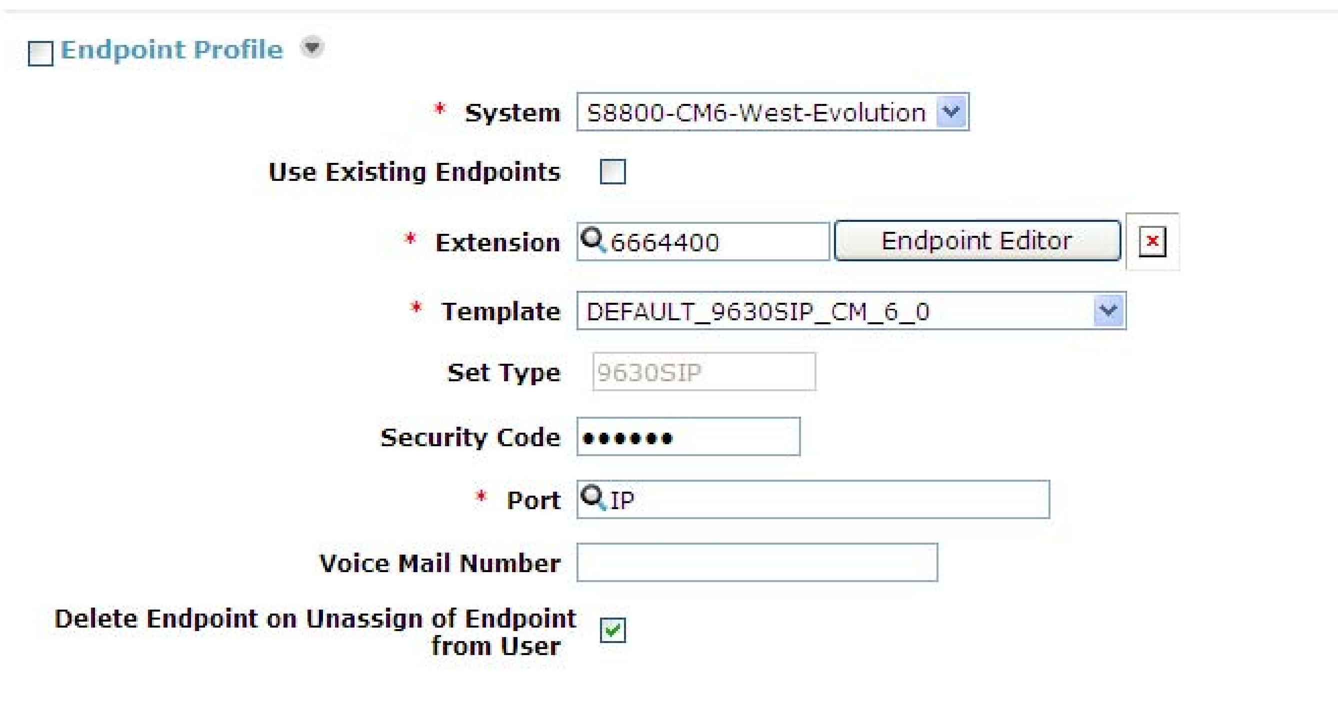
Step 4: Scroll down to the **Session Manager Profile** section and expand the view by selecting the icon. Assign the user to a **Primary Session Manager** instance and the **Application Sequence** defined in **Section 5.8** for Communication Manager Evolution Server. The **Application Sequence** must be used for both the originating and terminating sequence. Select the appropriate Location value from the drop-down.



Step 5: Scroll down to the **Endpoint Profile** section and expand the view by selecting the icon. Enter values for the following required attributes of the **Endpoint Profile** section:

- **System:** From the drop-down select the managed instance of the Communication Manager defined in **Section 5.8.**
- **Use Existing Endpoints:** Enter checkmark if station was already created per **Section 4.4**. Else, station will automatically be created
- **Extension**: Enter extension number
- **Template:** Select template for type of SIP phone.
- **Security Code:** Enter numeric value which will be used to logon to SIP phone
  Note: this field must match the value entered for the **Shared Communication Profile Password** field.
- **Port**: Select **IP** from the drop-down
- **Delete Endpoint on Unassign of Endpoint from User**: Enter checkmark to automatically delete station from Communication Manager when the User Profile is removed in System Manager

The screen below shows the information when adding a new SIP user to the sample configuration.



6. Configure 96xx SIP Deskphone

Before configuring the 96xx SIP Deskphone, please refer to **reference [7]** for a more complete explanation on setting up these telephones. Also it's important to realize that the 96xx phones support both H.323 and SIP firmware so it is necessary to ensure that SIP firmware has been loaded on the phone. At a minimum, the following parameters must be set.

- IP address, subnet mask, default gateway of the phone itself.
- SIP domain
- SIP Proxy Server Address (in this case: Session Manager)
- Username (usually the extension number like 666-4400)
- Password

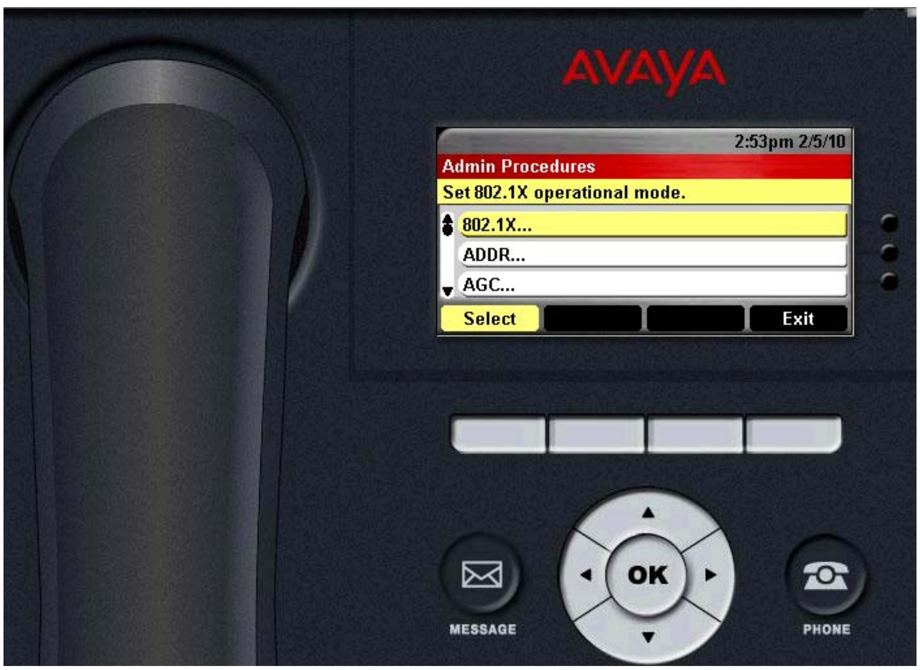
All but the last two values can configured with a combination of DHCP and the **46xxsettings.txt** file or by manually programming these values directly on the phone itself.

The following sections illustrate how to set these values manually on the phone itself via the keypad.

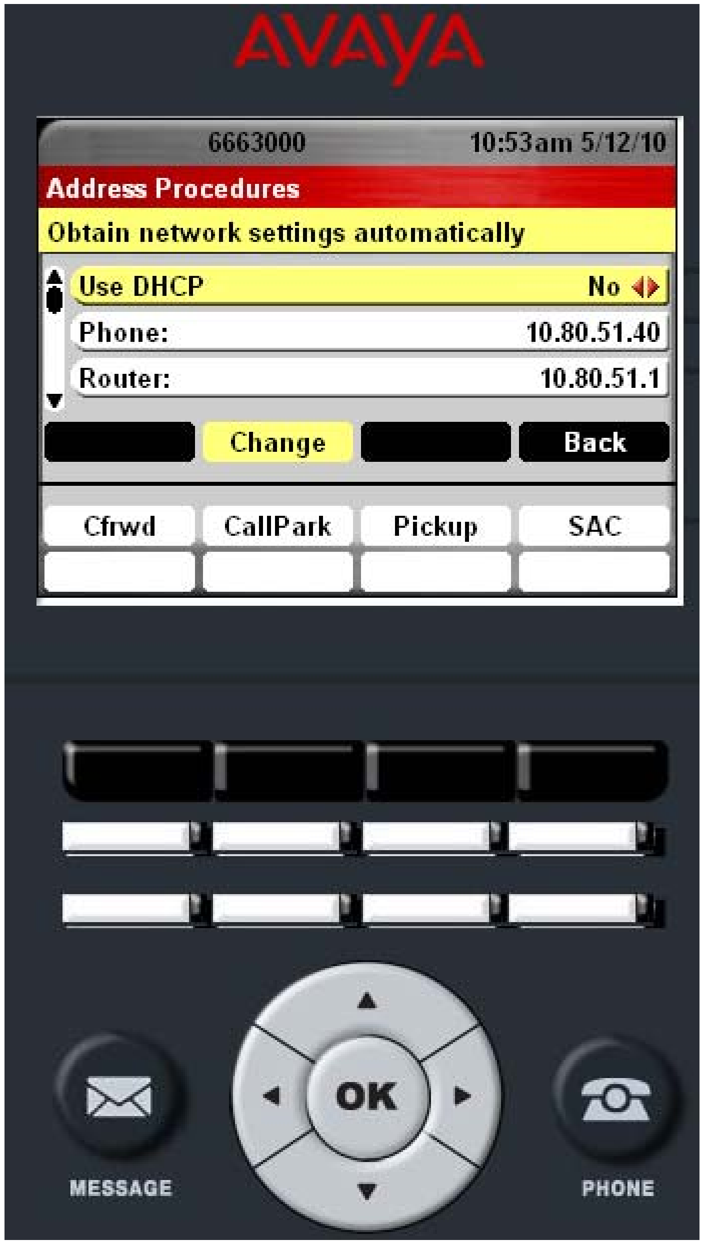
6.1 Configure IP Address, Subnet Mask & Default Gateway

To access the 96xx setup screens shown below press the following keys on the keypad:
Mute-c-r-a-f-t # (mute-2-7-2-3-8-#). The screen shown below will appear on the phone.

Note: These screenshots are from a 9650C telephone though all 96xx phones use the same basic settings.

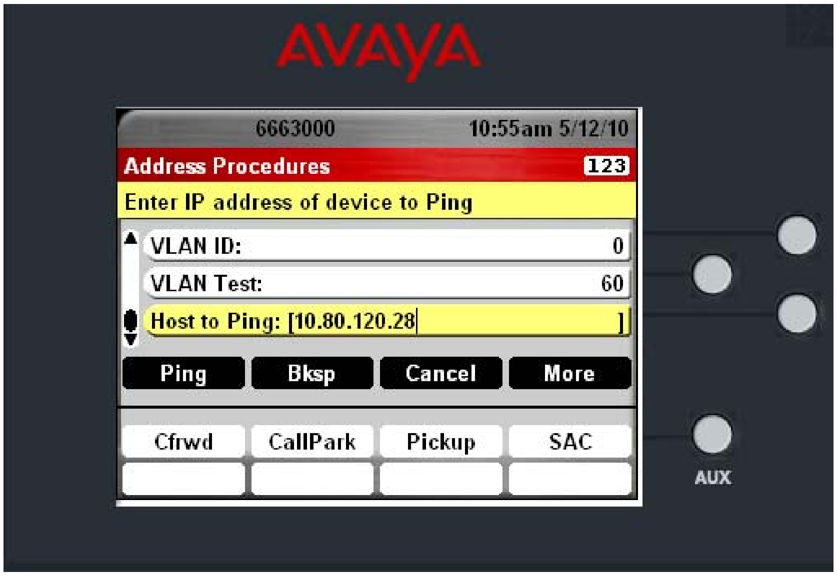


Using the phone's down arrow, scroll down one row and select **ADDR…**. The following screen appears:



Using the up and down scroll buttons, select the appropriate fields for editing, pressing the **Change** button to edit each field. Scroll down further to see the fields for Mask (subnet mask), HTTPS & HTTP File Server, DNS Server, 802.1Q, VLAN ID, and VLAN Test.

The last row on this screen is **Host To Ping**. If needed, enter in an IP address and press the **PING** key to test network connectivity. Press the **Bksp** button when the test is complete to remove the IP address.

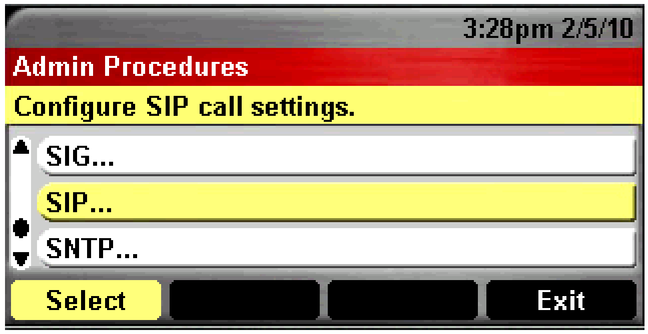


Shown below is a screenshot of a successful test to 10.80.120.28:

Once programming is completed on the above screens be sure to press **Save** to get back to the main screen and save your configuration.

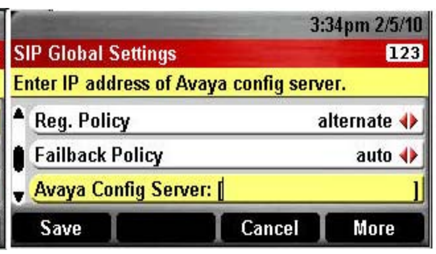
6.2 Configure SIP Global and Proxy Settings

The next steps are to configure the SIP Domain and the SIP Proxy server address. From the main admin screen, scroll down and select **SIP…**

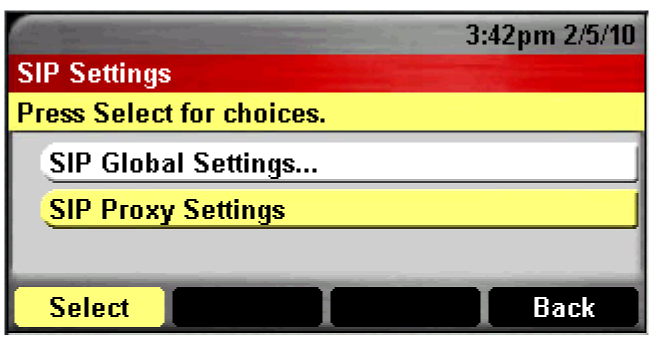


In the screen that appears select **SIP Global Settings**, The options as shown in the image below will appear. Verify the following are set:

- **Sip Mode** **Proxied**
- **SIP Domain** In this case set to **avaya.com**
- **Avaya Environment** **Auto**
- **Registration Policy** **alternate** or simultaneous
- **Failback Policy** **auto**
- **User ID Field** **No**

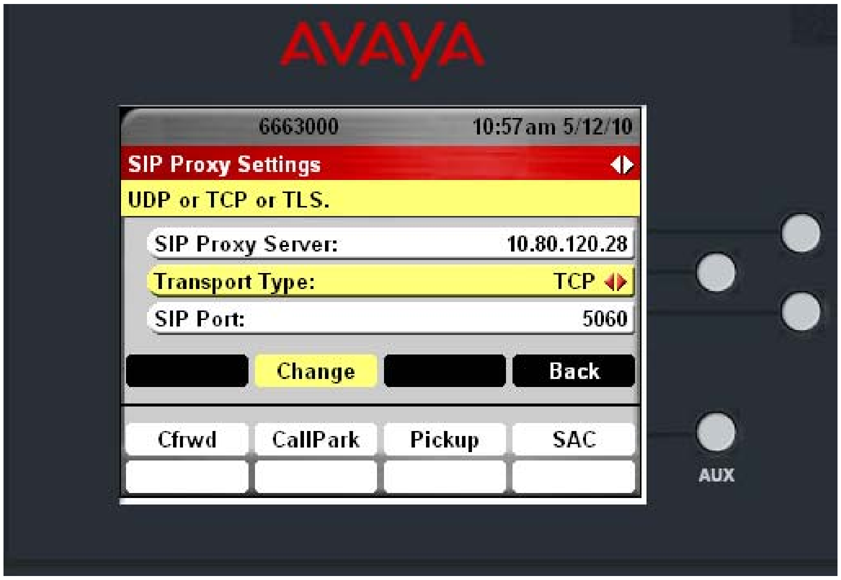


Select the **Save** button when complete. Next, select **SIP Proxy Settings.**



Select **NEW** and the following screen appears. Set fields according to your configuration. In this case:

- **SIP Proxy Server** Address of Session Manager SM-100 interface
- **Transport Type** **TCP** (can be TLS or UDP as well)
- **SIP Port** **5060** for TCP & UDP, 5061 for TLS

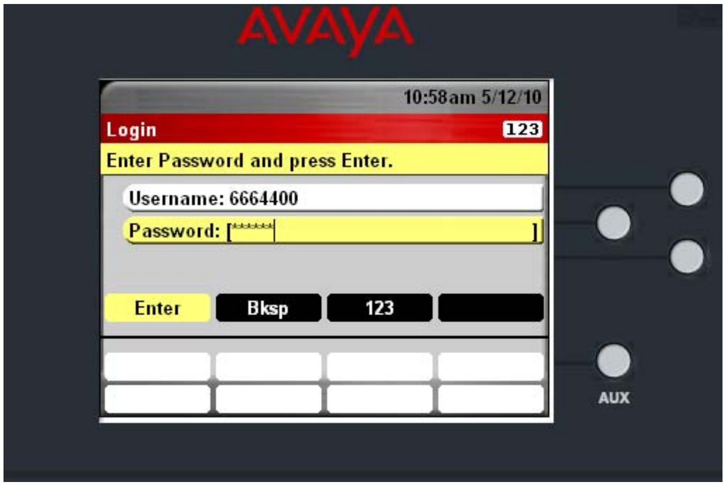


Select **Save** when complete. Select **Back** two times to get back to the main menu. Select **Exit** to complete the configuration. The phone will reboot.

6.3 Login Phone to Avaya Aura™ Session Manager

Once the phone has rebooted, a login screen will be presented. Enter the following information:

- **Username** Extension number/User created in **Section 5.9**
- **Password** Password as it was programmed when creating a SIP user in **Section 5.9**



Select Enter and the phone will login to Session Manager immediately. Shown below is a successfully logged in 9650C phone.

7. Configure the Avaya Communication Server 1000E

Avaya Communication Server 1000 uses the Network Routing Server (NRS) to provide SIP and H.323 signaling interfaces to IP networks. The NRS communicates with the CS1000E Signaling Server over a private Ethernet interface. There can be one or more NRS supported CS1000E instance. The applications that can run on the CS1000E's CP+PM proccessing module include the following:

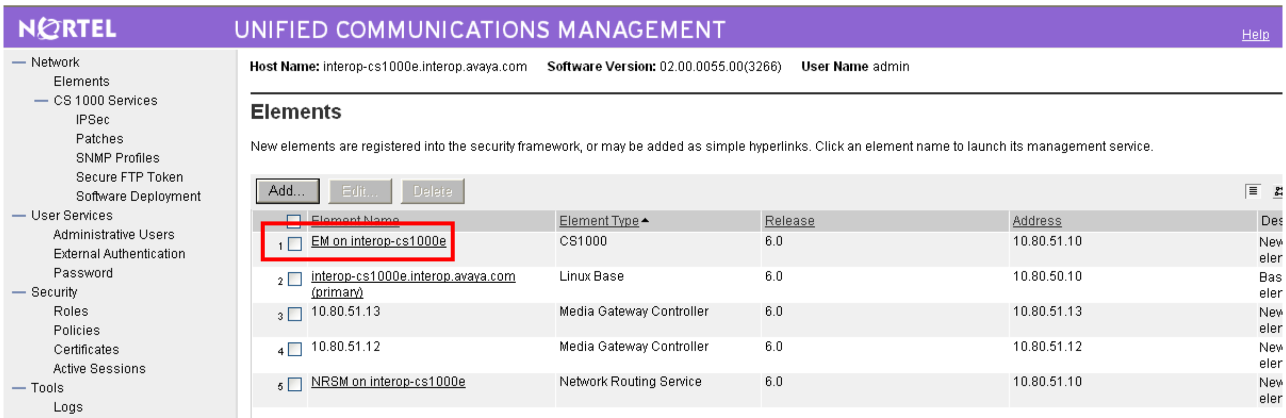
- **Call Server** — Provides the primary PBX functionality.
- **SIP Signaling Gateway (SSG)** — Provides SIP signaling for IP networks.
- **H.323 Gateway** — Provides H323 Redirect & Registrar service components**.**
- **NRS Server** — Provides routing information for SIP calls to/from the CS1000
- **NRS Manager** — Provides web interface for NRS management.
- **Element Manager** — Provides web interface for system administrative tasks

The Communication Server 1000 used in the interoperability test configuration contained one NRS and Call Server co-resident on the same CS1000E server blade. The Element Manager web interface 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 used the Coordinated Dial Plan (CDP) feature to route calls from the Communication Server 1000, over the SIP trunks to Session Manager to reach the 96xx endpoints registered to Session Manager. The procedures below describe the details of configuring Communication Server 1000E for SIP trunks:

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

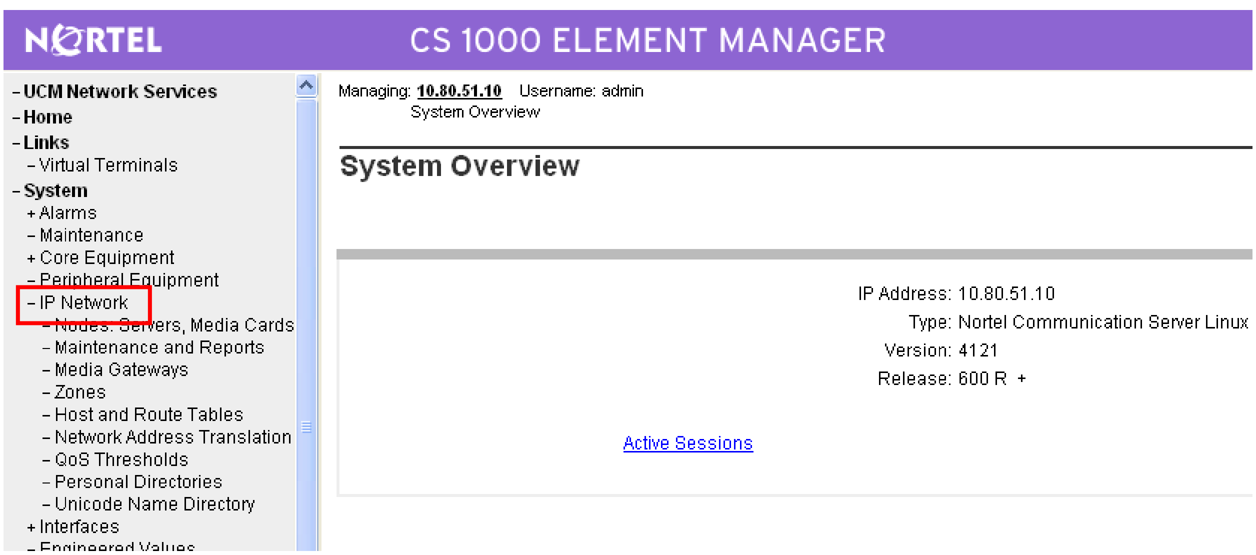
7.1 Launch Unified Communications Manager

Access the Communication Server 1000 web based interface by using the URL "**https://<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**.

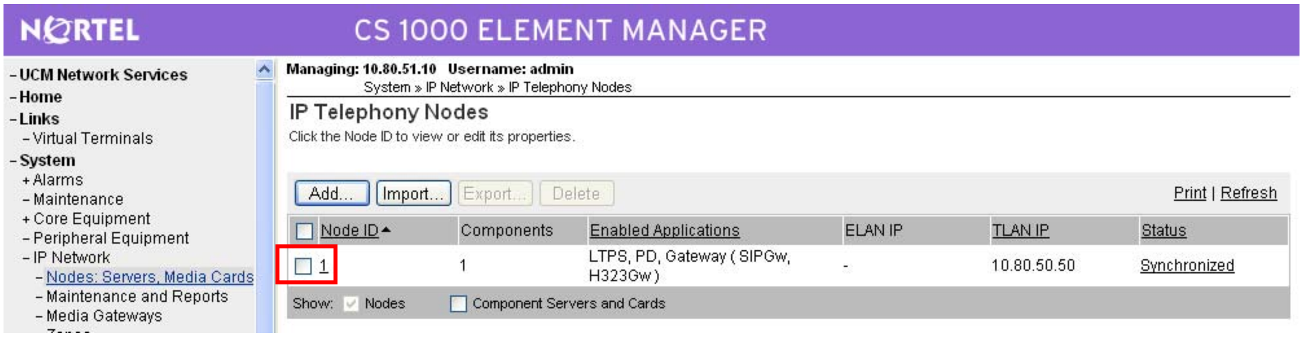


7.2 Obtain Node and IP Addresses

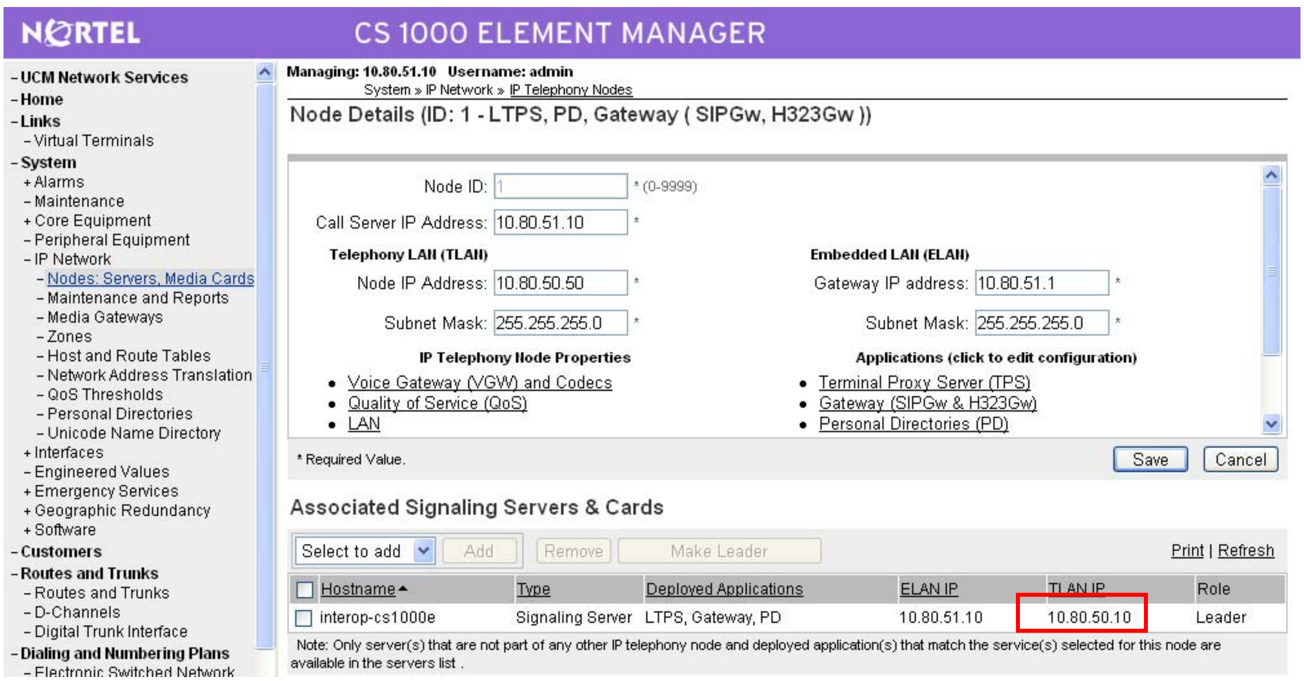
The Element Manager **System Overview** screen is displayed. Expand the **IP Network** menu on the left pane and select **Nodes: Servers, Media Cards**.



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



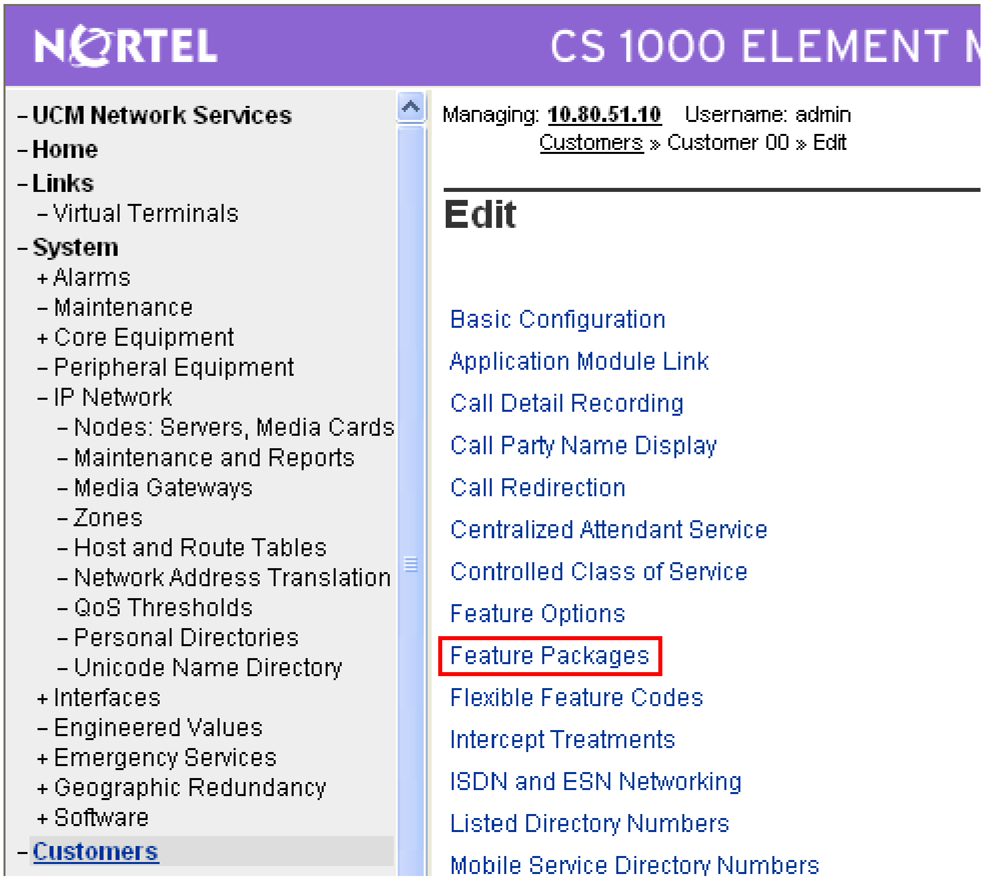
The **Node Details** screen is updated with additional details as shown below. Make a note of the Signaling Server **TLAN IP** address of **10.80.50.10**. This value is used to configure other sections.



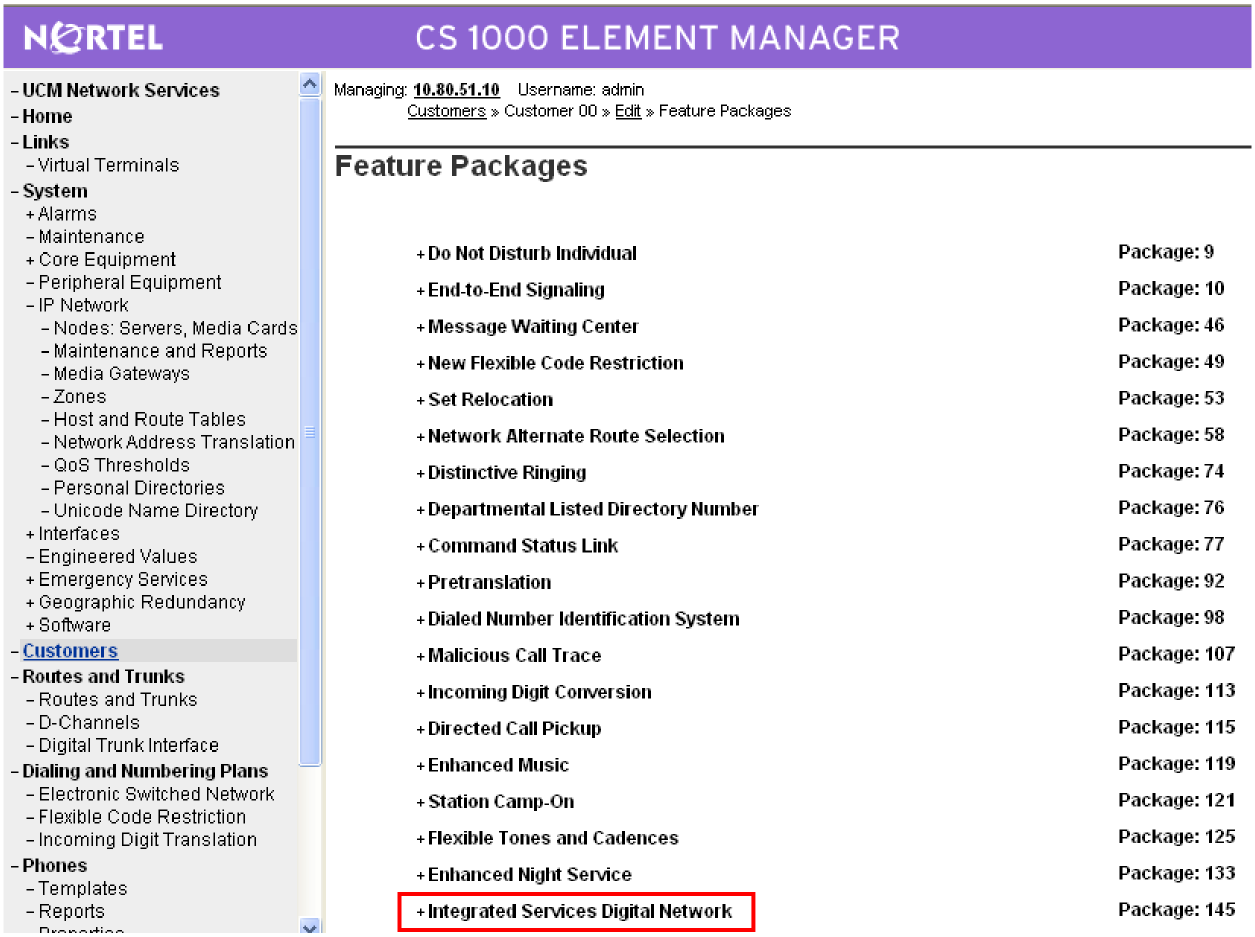
7.3 Administer ISDN

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. In the sample configuration, only one customer was configured on the system.

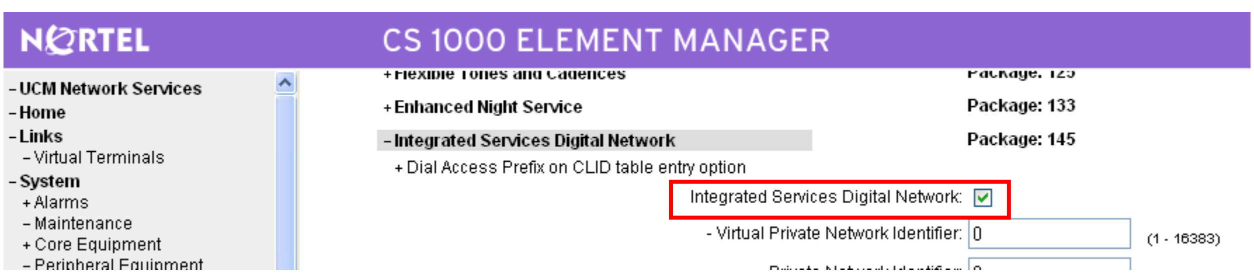
The **Customer 00 Property Configuration** screen is displayed next. Select **Feature Packages**.



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.

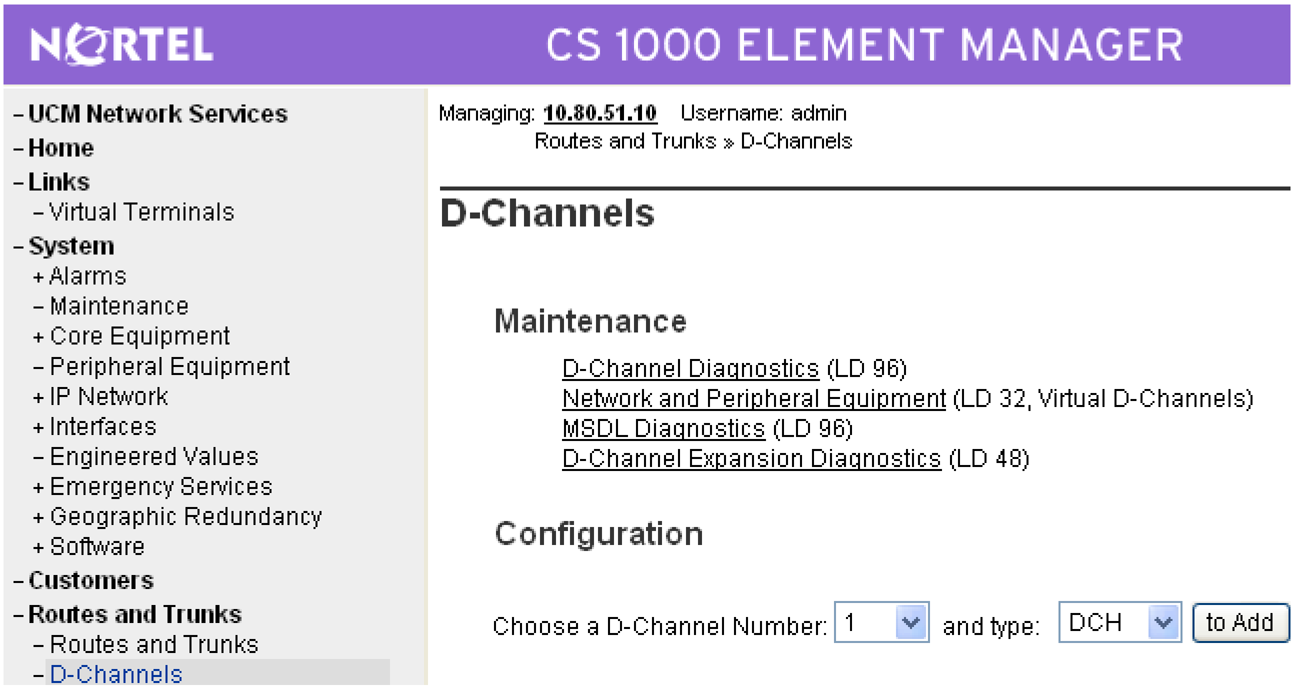


The screen is updated with parameters populated below Integrated Services Digital Network. Check the **Integrated Services Digital Network** checkbox, and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click Save (not shown).



7.4 Administer a Virtual D-Channel

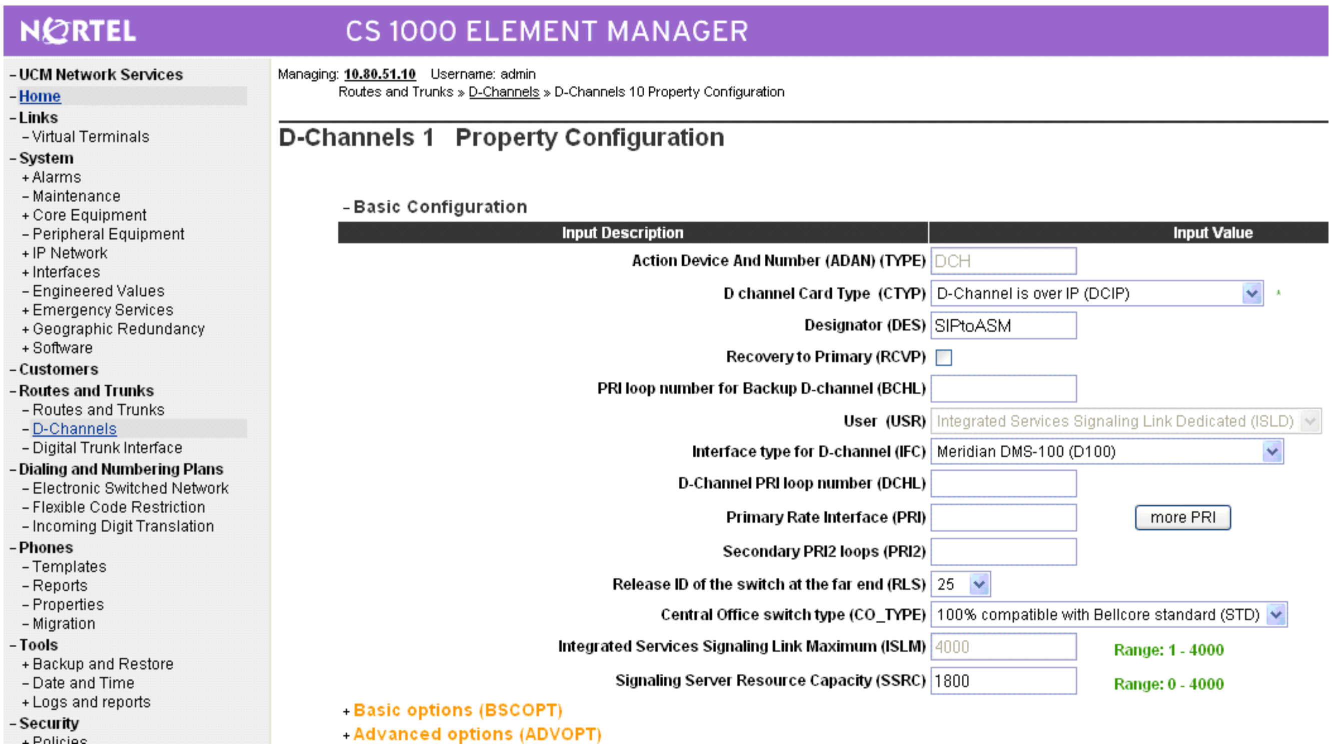
Select **Routes and Trunks → D-Channels** from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list (in this case **1**). Click **to Add**.



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.

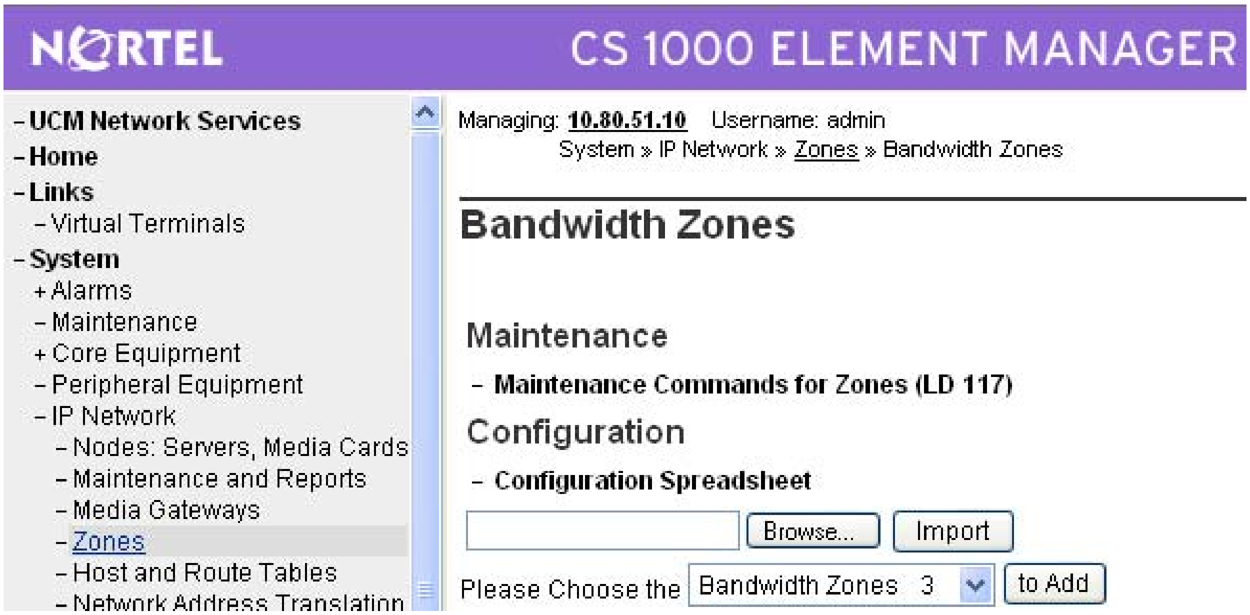
- **D channel Card Type (CTYP):** D-Channel is over IP (DCIP)”
- **Designator (DES):** A descriptive name.

Click **Submit**.

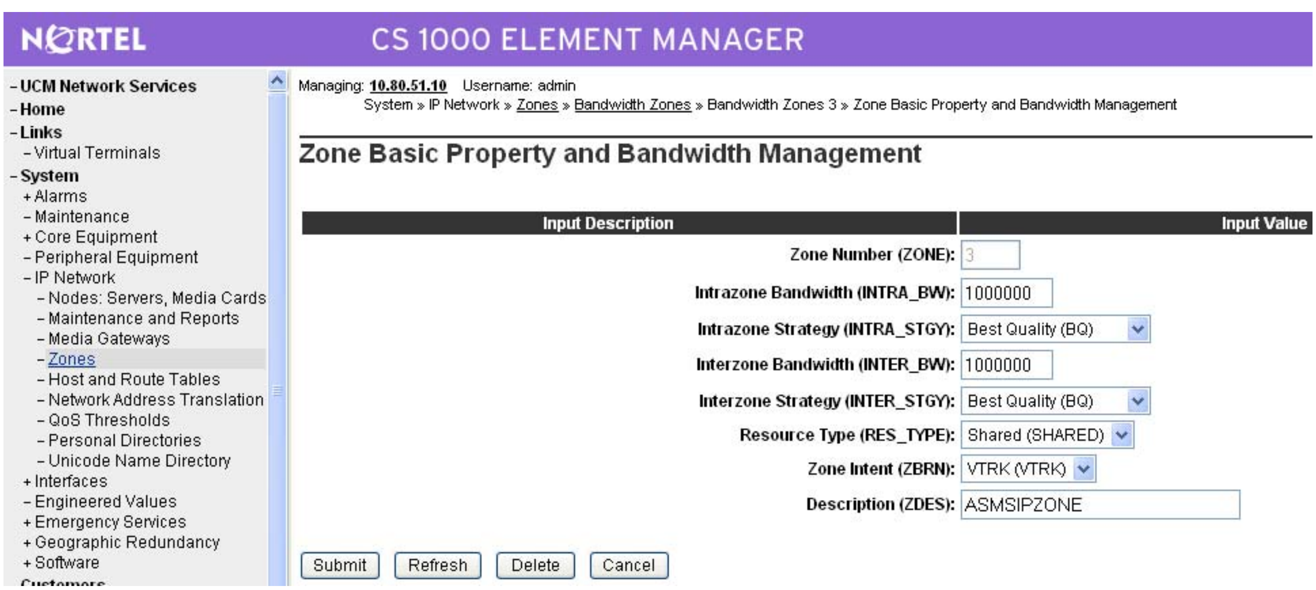


7.5 Administer Zones

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 **Bandwidth Zones 3**). Click **to Add**.

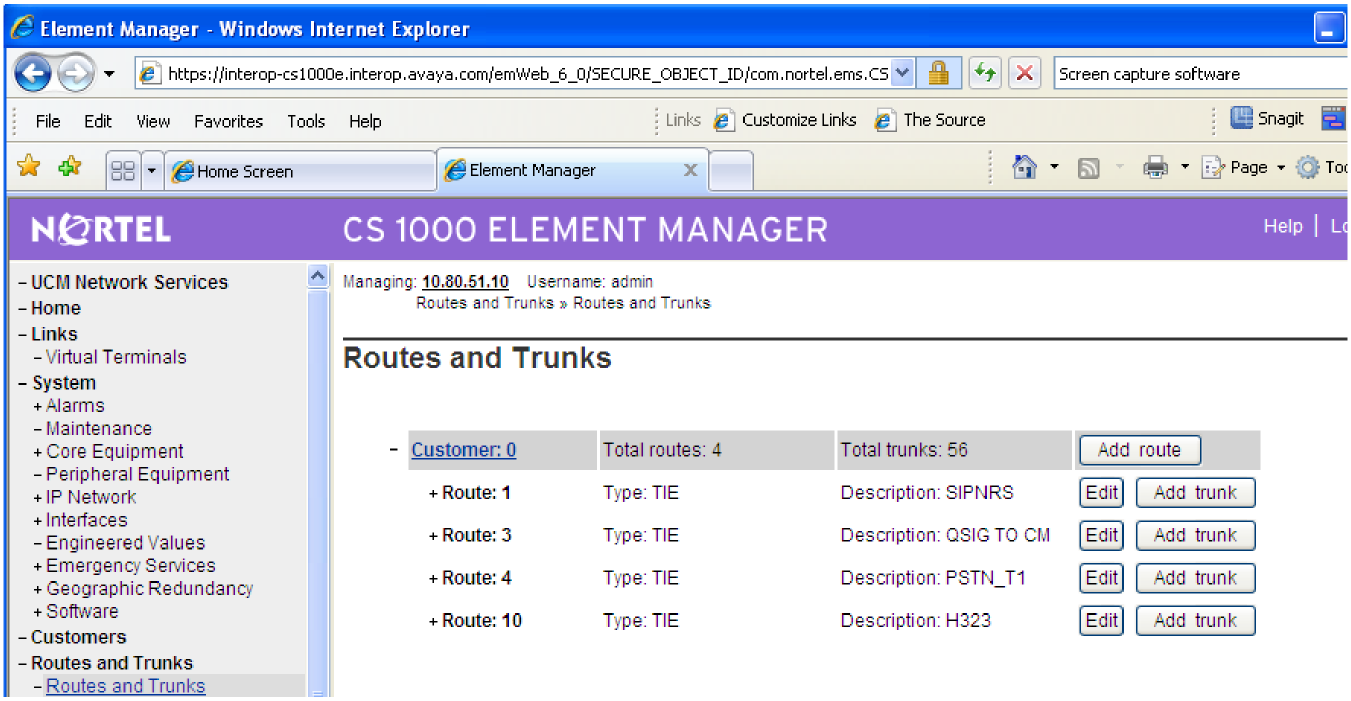


The **Zone Basic Property and Bandwidth Management** screen is displayed next. For the **Zone Intent (ZBRN)** field, select **VTRK (VTRK)** from the drop-down list. For the Description (ZDES) field, enter descriptive text. Retain the default values for all remaining fields, and click **Submit.**



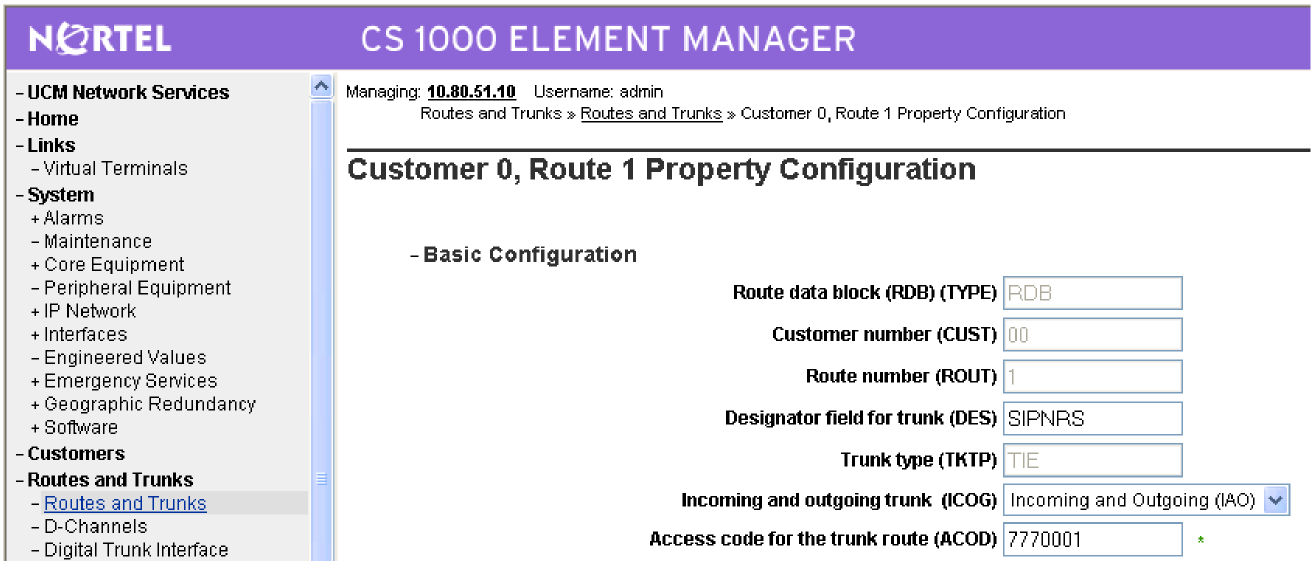
7.6 Administer Virtual SIP Routes and Trunks

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

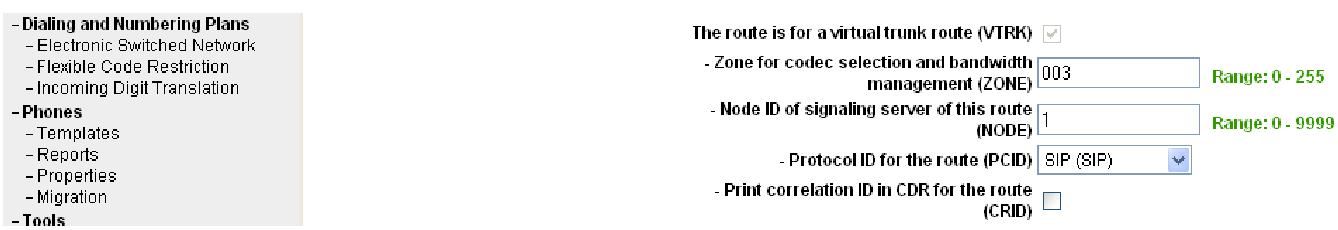


The **Customer 0, Route 1 Configuration** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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.

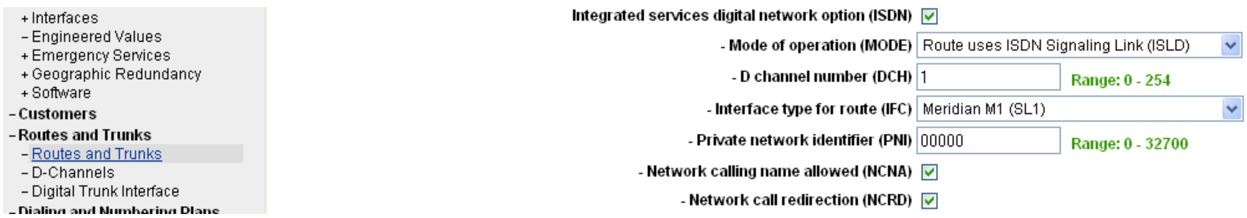


Scroll down the screen, and check the field **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear. For the **Zone for codec selection and bandwidth management (ZONE)** field, enter the zone number from **Section 7.5**. For the **Node ID of signaling server of this route (NODE)** field, enter the node number from **Section 7.2**. Select **SIP (SIP)** from the drop-down list for the **Protocol ID for the route (PCID)** field.

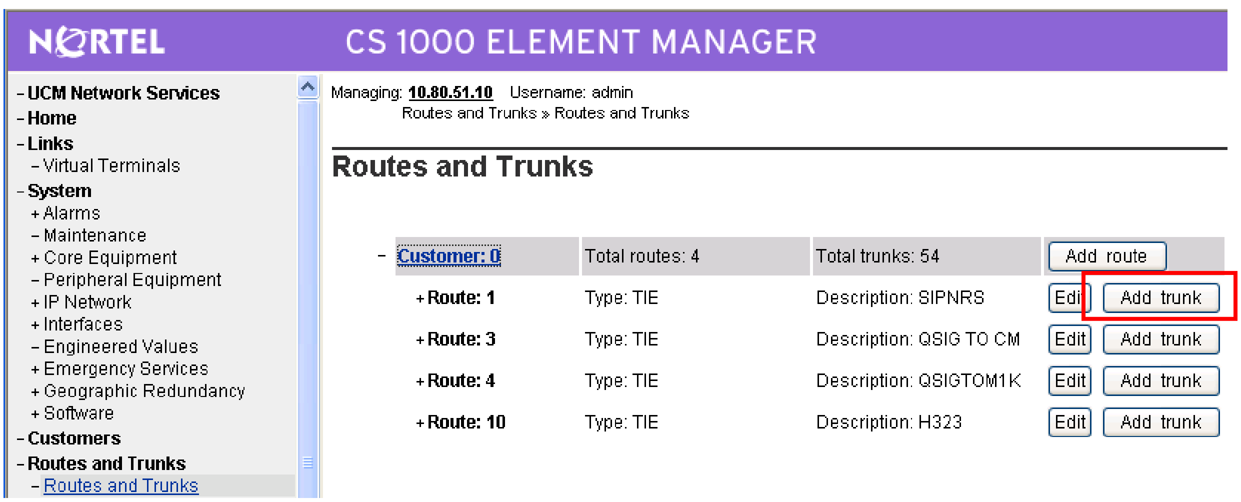


Scroll down the screen and check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click **Submit**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

- **Mode of operation (MODE):** **Route uses ISDN Signaling Link (ISLD)**
- **D channel number (DCH):** D-Channel number from **Section 7.4**
- **Network calling name allowed (NCNA):** Check the field
- **Network call redirection (NCRD):** Check the field

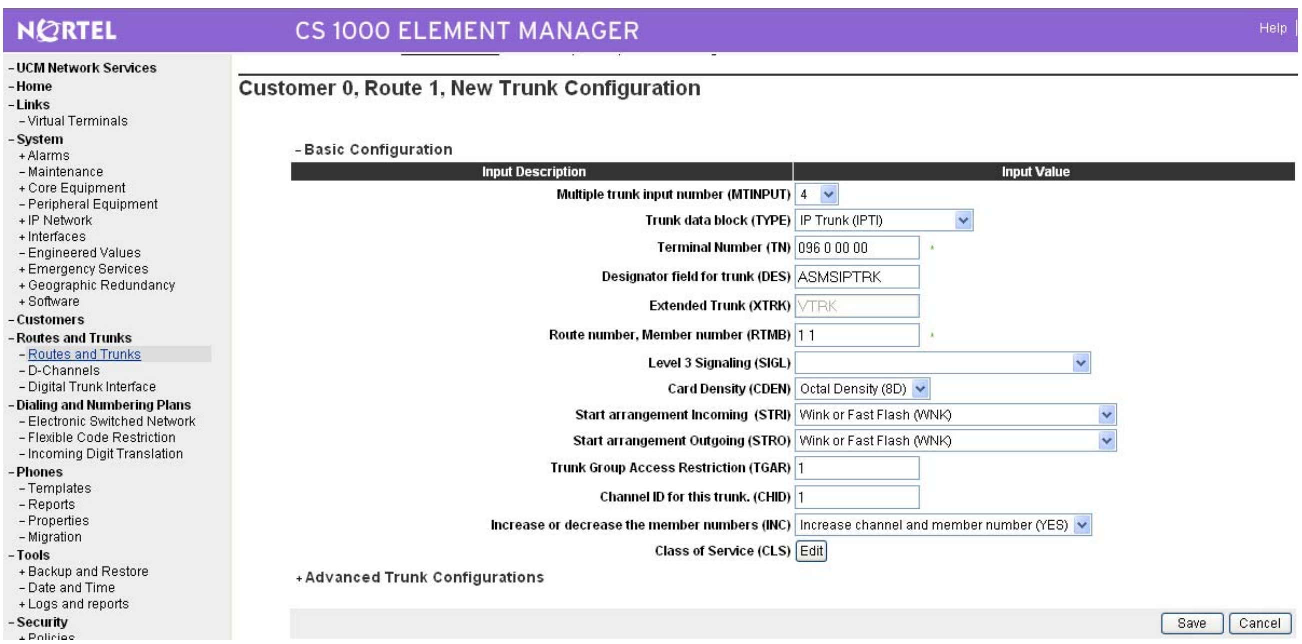


The **Routes and Trunks** screen is displayed again, and updated with the newly added route. Click the **Add trunk** button next to the newly added route.



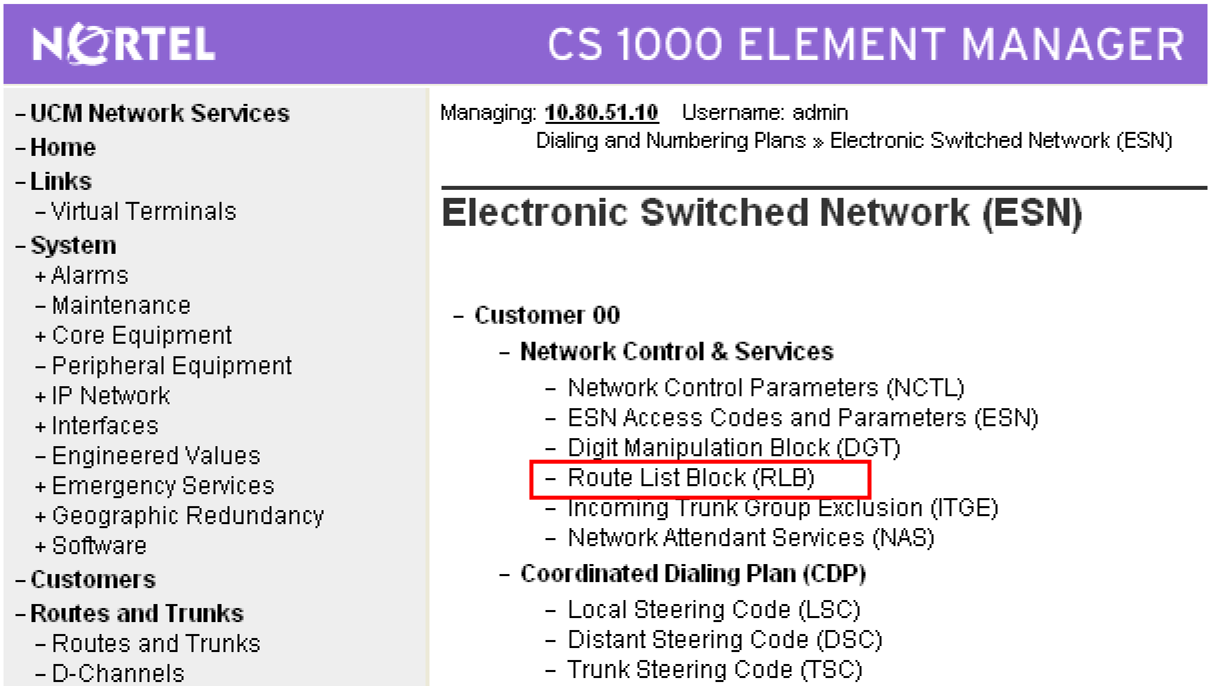
The **Customer 0, Route 1, New Trunk Configuration** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click **Save**. The **Multiple trunk input number (MTINPUT)** field may be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

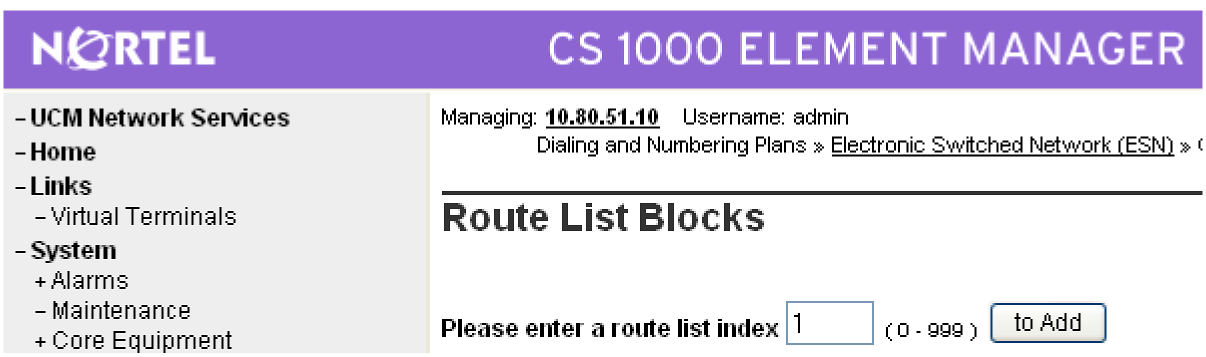


7.7 Administer Route List Block and Distant Steering Code

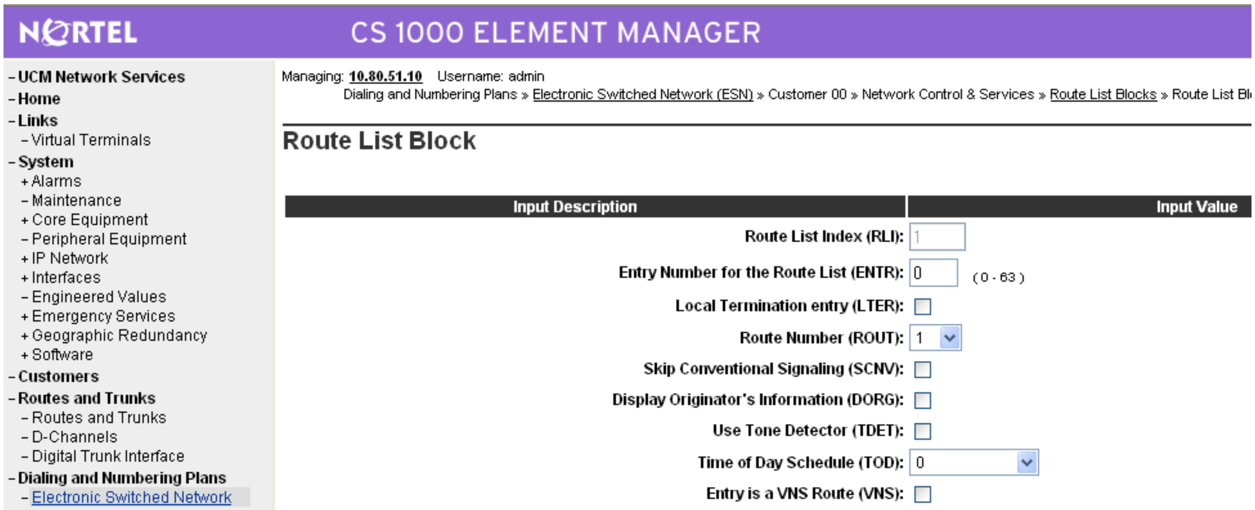
Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block (RLB)**.



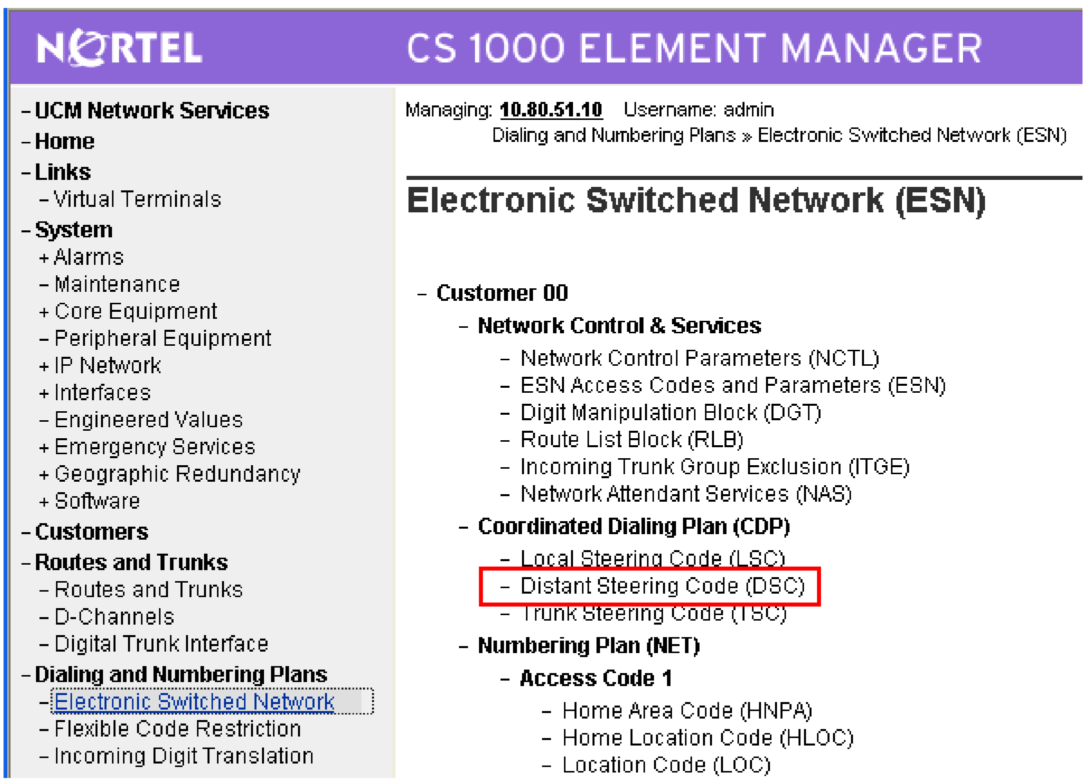
The **Route List Blocks** screen is displayed. In the **Please enter a route list index** field, enter an available route list block number (in this case **1**). Click **to Add**.



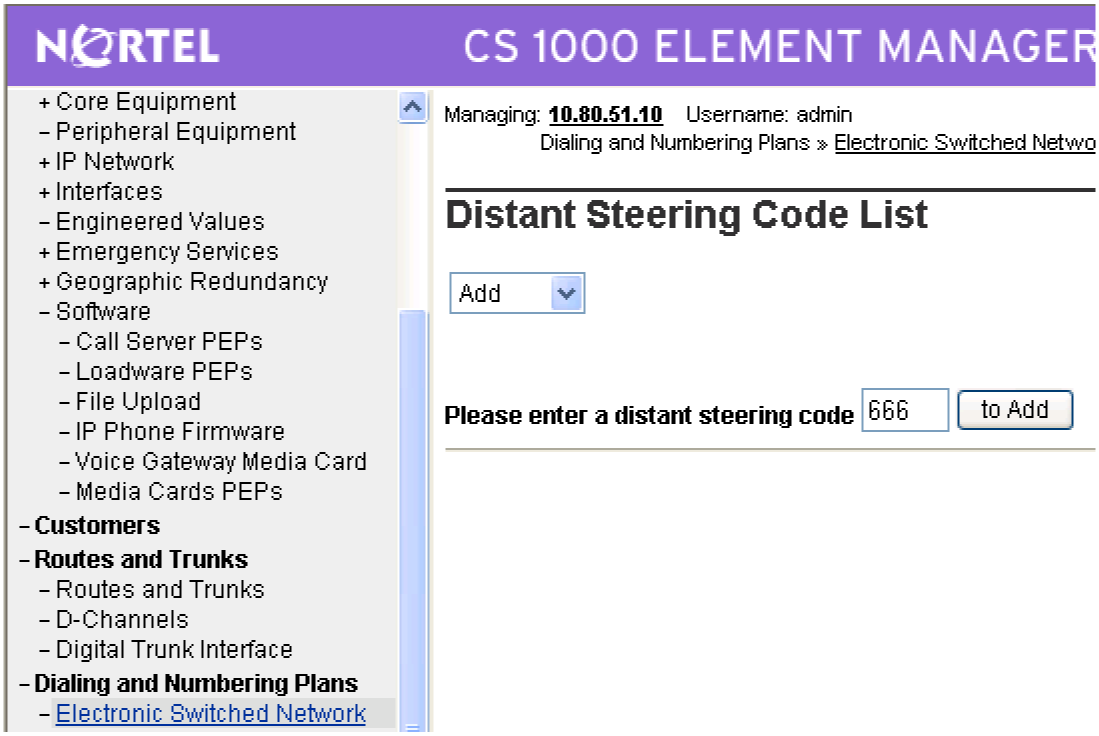
The **Route List Block s**creen is displayed with a listing of parameters. For the **Route Number (ROUT)** field, select the route number from **Section 7.6**. Retain the default values for the remaining fields, and scroll down to the bottom of the screen and click **Submit** (not shown).



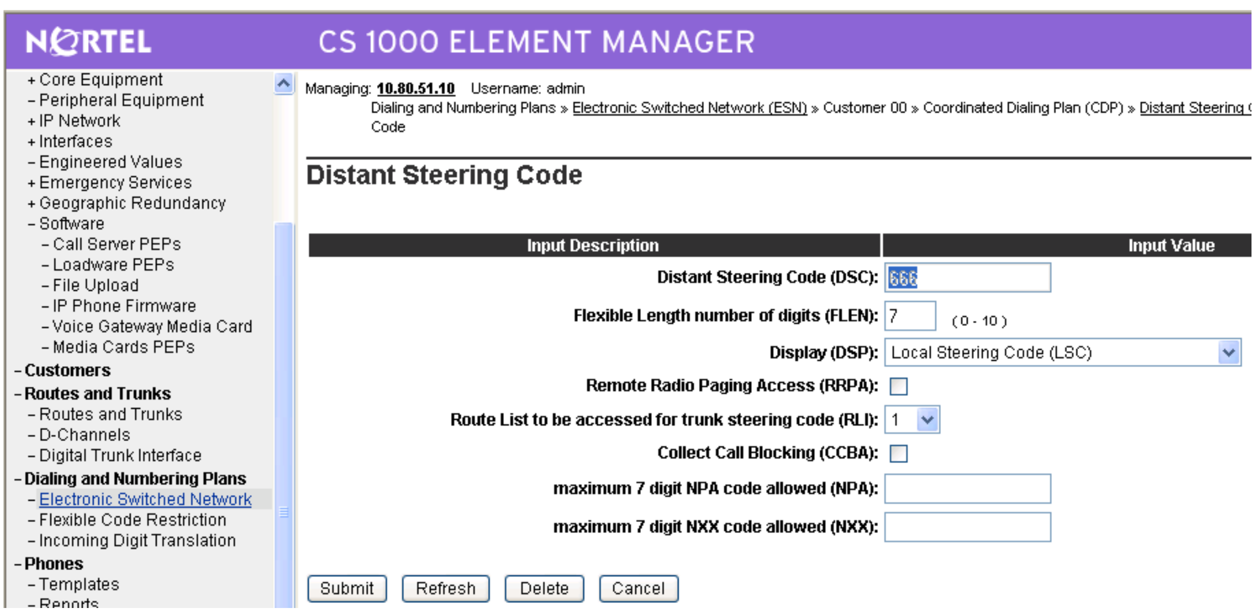
Select **Dialing and Numbering Plans → Electronic Switched Network** again from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Distant Steering Code (DSC)** to add an entry to route 666xxxx calls to Session Manager.



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 **666**). Click **to Add**.

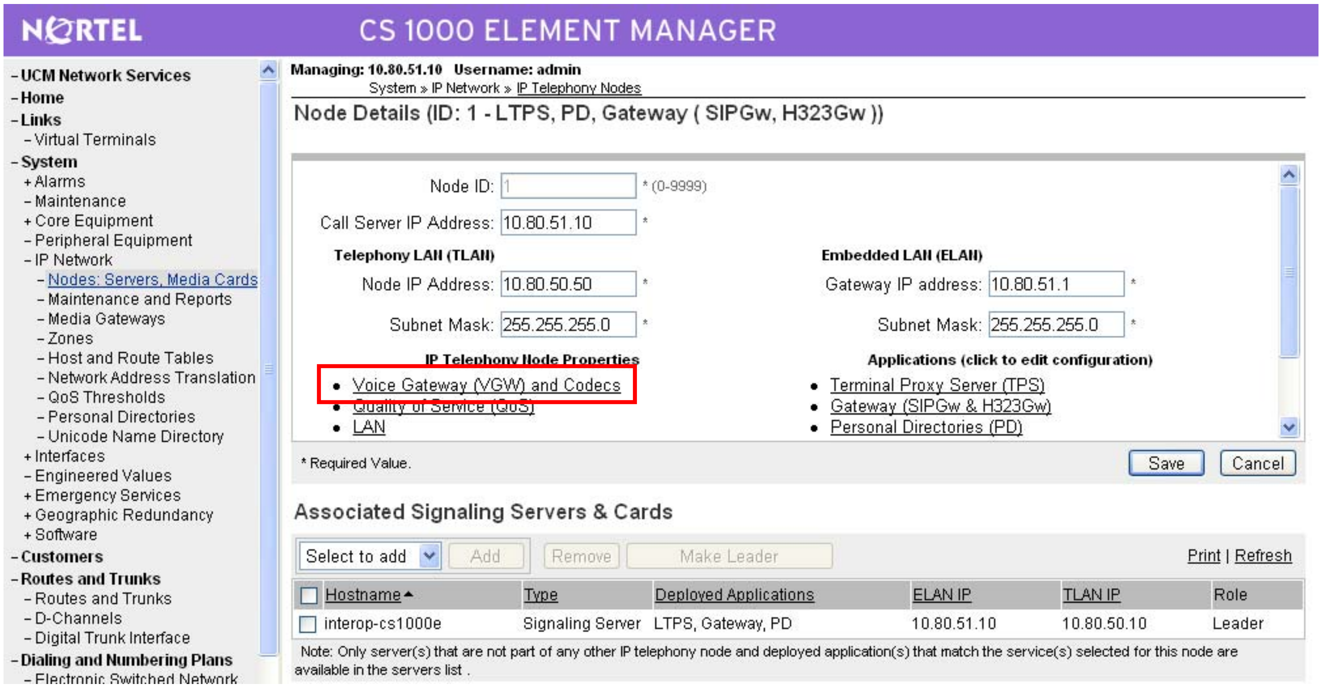


The **Distant Steering Code** screen is displayed. For the **Route List to be accessed for trunk steering code (RLI)** field, select the route list index **shown in Section 7.7** from the drop-down list. Retain the default values in all remaining fields and click on **Submit**.

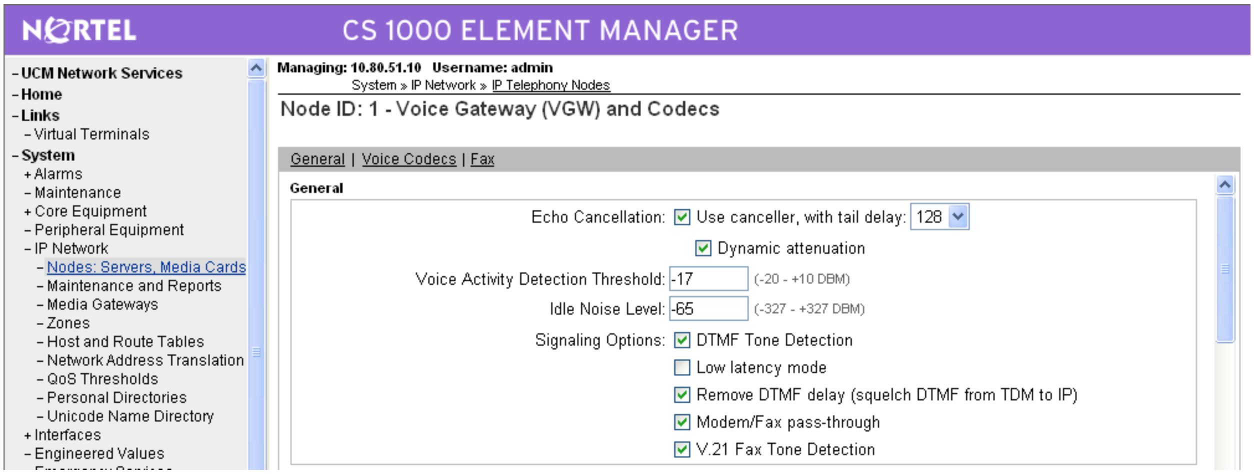


7.8 Administer Node SIP Parameters

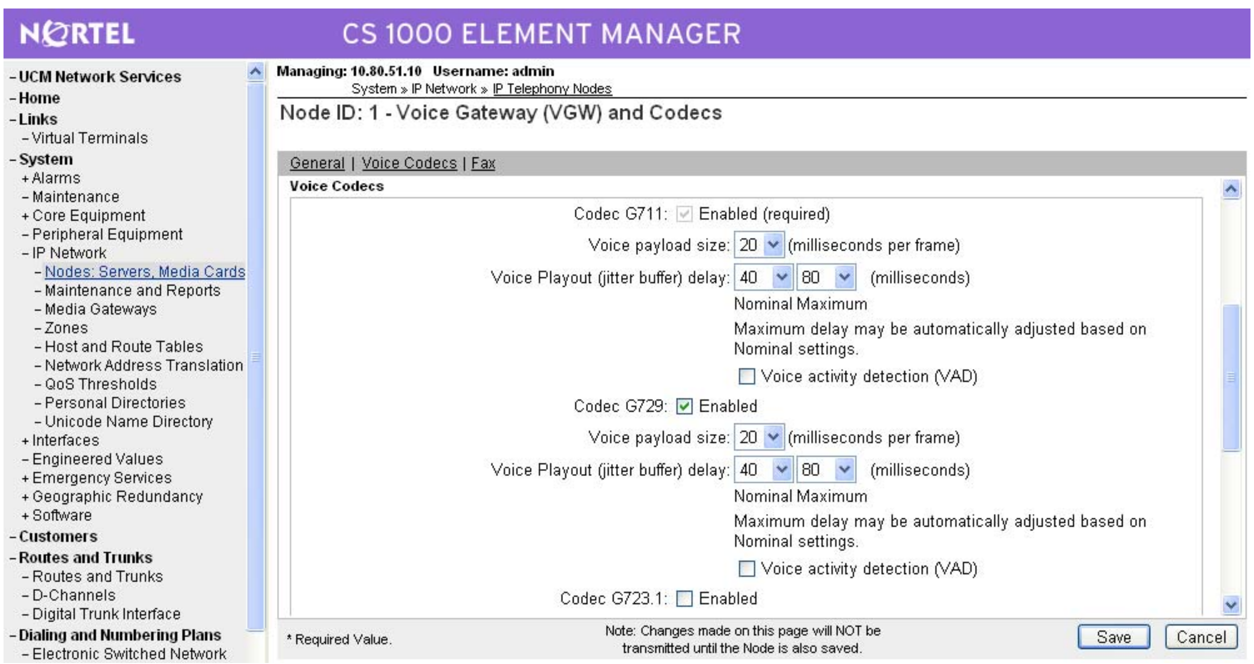
Select **IP Network → Nodes: Servers, Media Cards → Configuration** from the left pane, and in the **IP Telephony Nodes** screen displayed (not shown), select the node ID of this CS1000 system (see **Section 7.2**). The **Node Details** screen is displayed. It is assumed that the TLAN and ELAN IP addresses 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**.

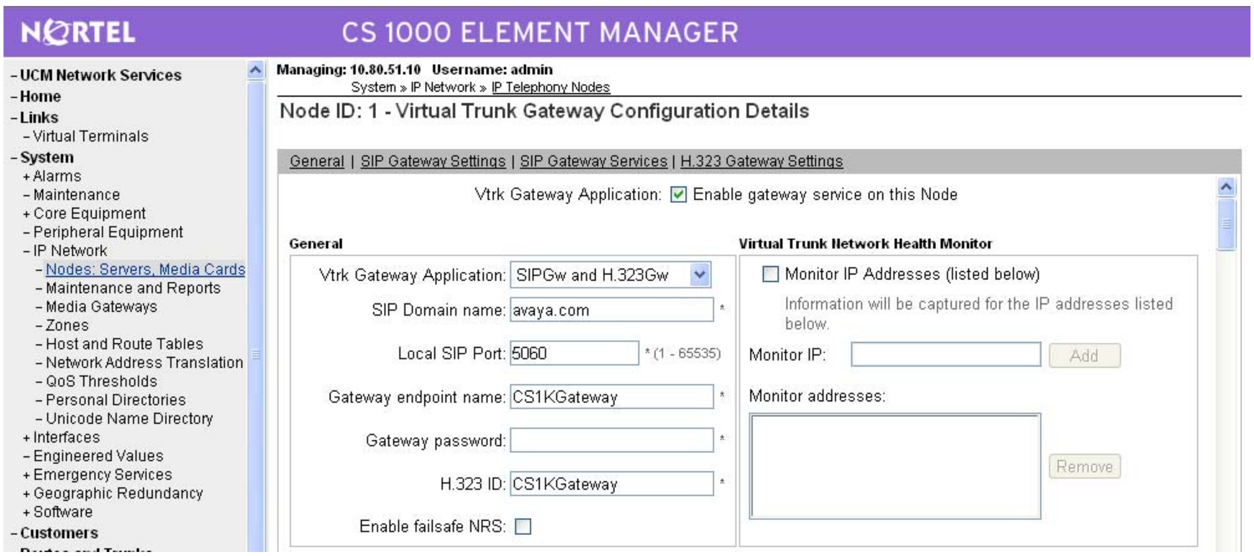


Scroll down the parameters box and check the desired codecs under **Voice Codecs**. Note that G.711 and G.729 were verified for the sample configuration. G.711 is checked by default and cannot be unchecked. Click on **Save**.



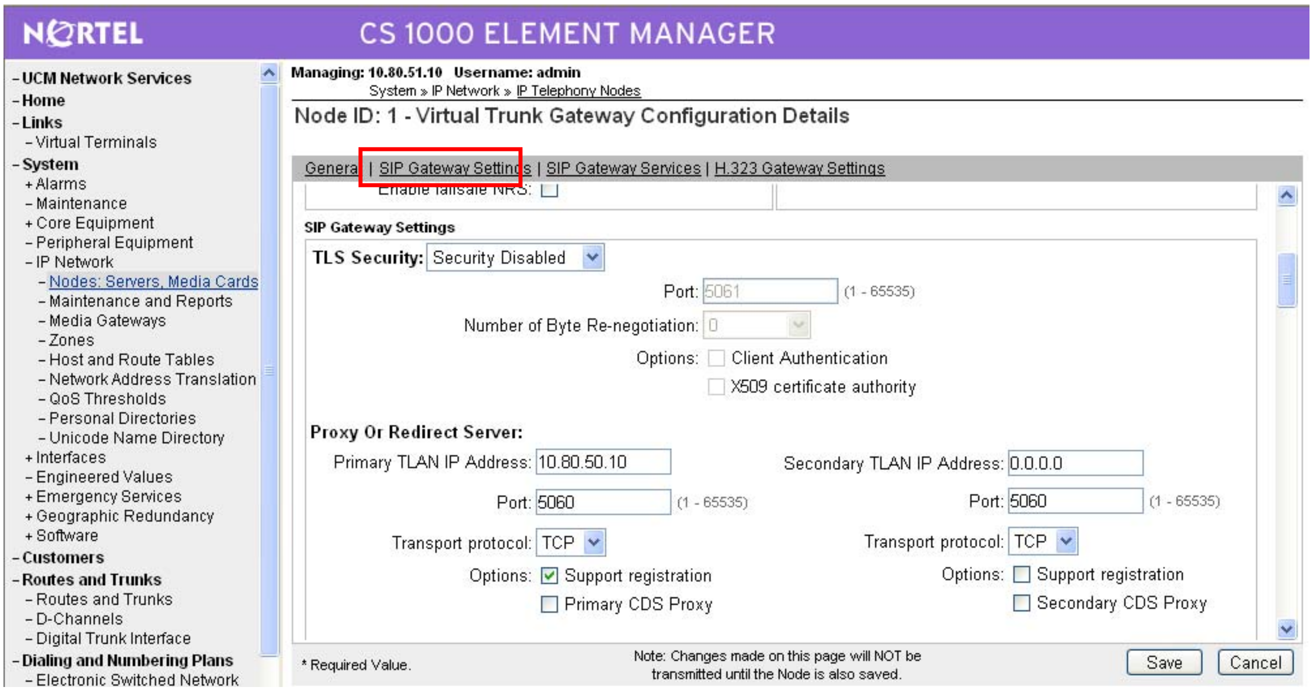
When the **Node Details** screen is displayed, click on **Gateway (SIPGw and H.323Gw)**. Under **General** on the **Virtual Trunk Gateway Configuration Details** screen, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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 5.1**
- **Local SIP Port** **5060**
- **Gateway endpoint name** A descriptive name. Record this name for use in **Section 7.11**
- **Gateway password** Enter a password if desired.
  Note: this password is only used when the SSG is configured as a SIP Proxy (as opposed to SIP Redirect Server) and then only when registration is required. See **Section 10**, **Reference [13]**

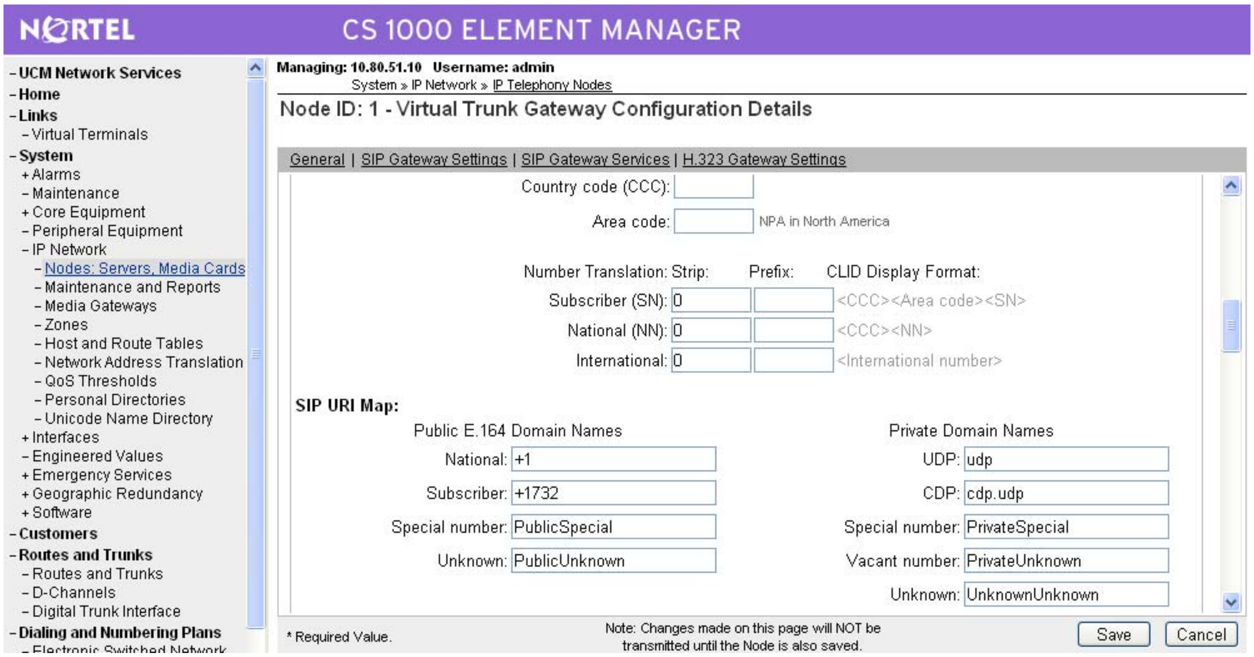


Click on **SIP Gateway Settings** and under **Proxy or Redirect Server**, enter the following values for the specified fields, and retain the default values for the remaining fields.

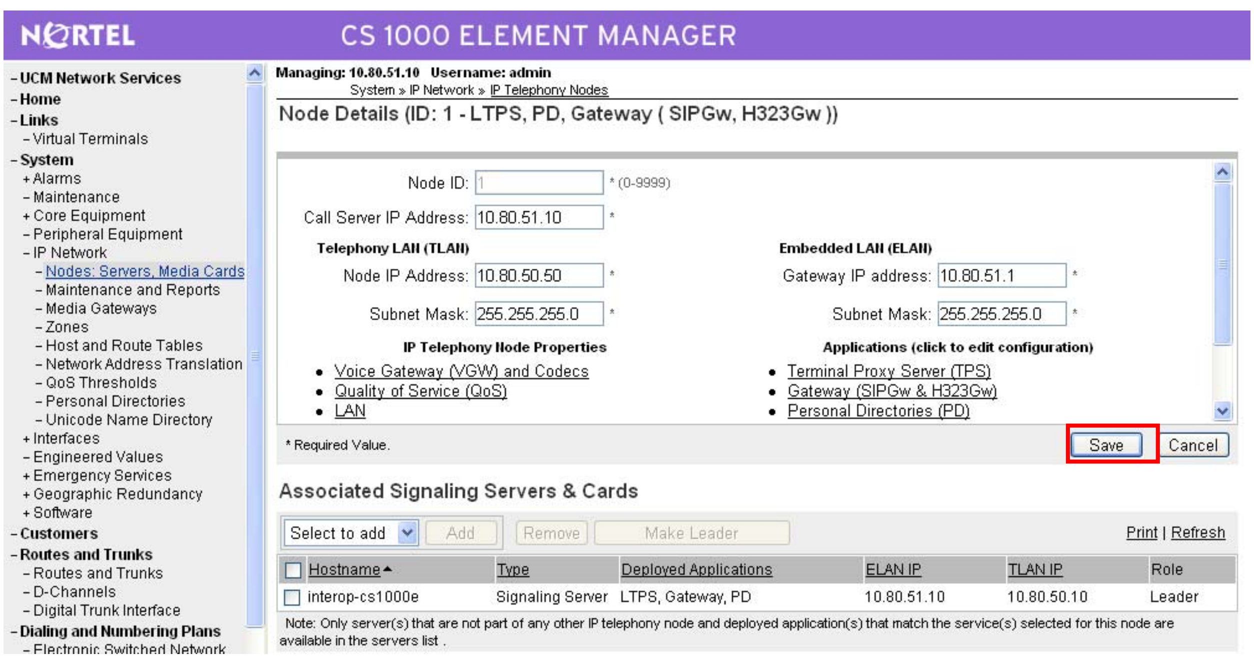
- **Primary TLAN IP Address:** The IP address of the Signaling Server noted in **Section 7.2**.
- **Port** **5060**
- **Transport Protocol** **TCP**
- **Options** Check **Support registration**



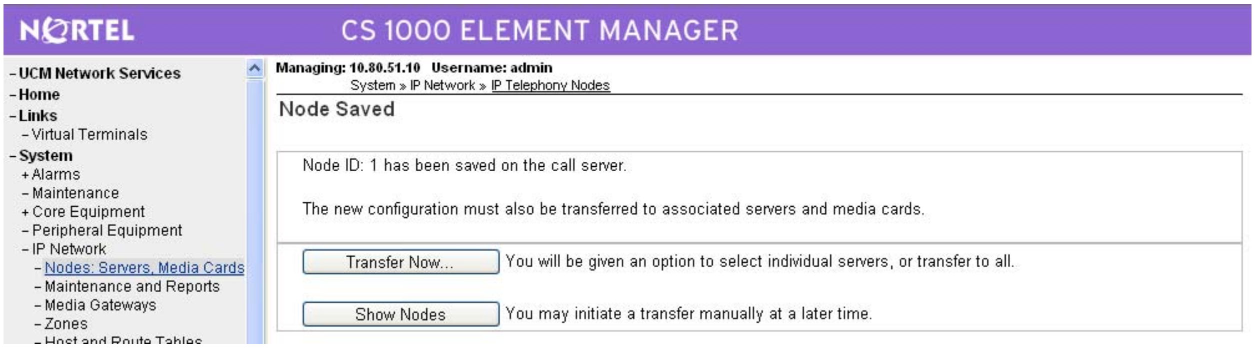
Scroll down the parameters box to the **SIP URI Map** section. Under **Public E.164 Domain Names,** enter the appropriate **National** and **Subscriber** values for the network configuration. In the test configuration, **1** is the country code and **732** is the area code. The remaining fields can be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



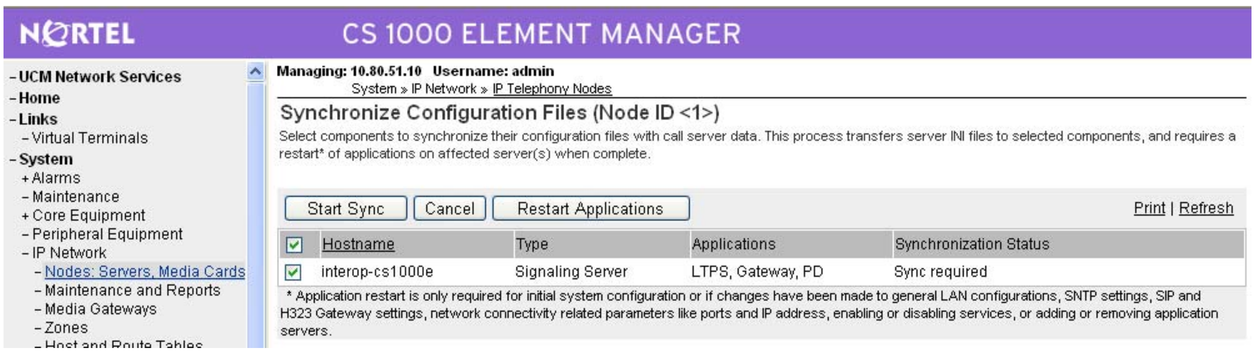
Return to the **Node Details** screen and click **Save**, as shown below.



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

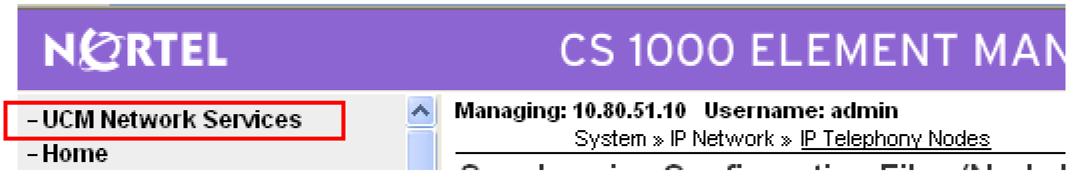


The **Synchronize Configuration Files** screen is displayed. Select the Signaling Server and click on **Start Sync**. When the synchronization completes, click on **Restart Applications**.

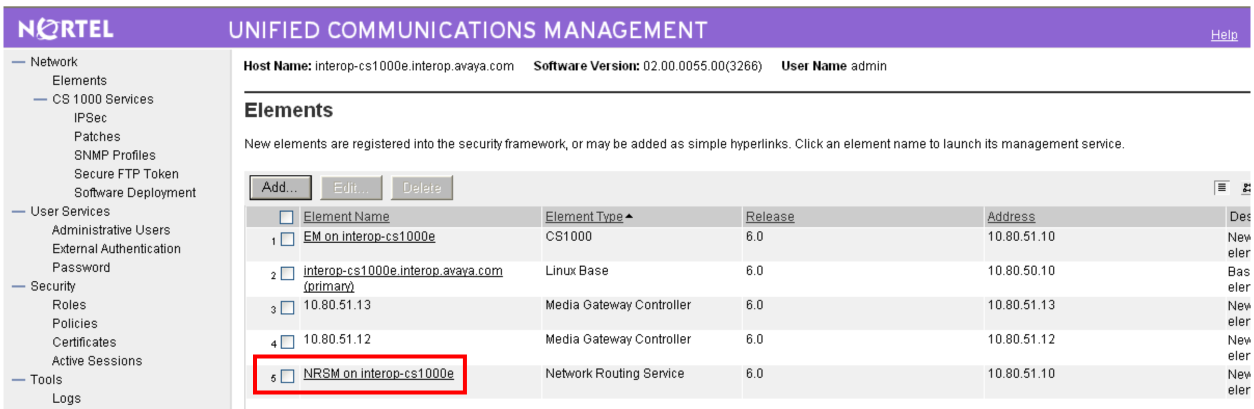


7.9 Launch NRS Manager

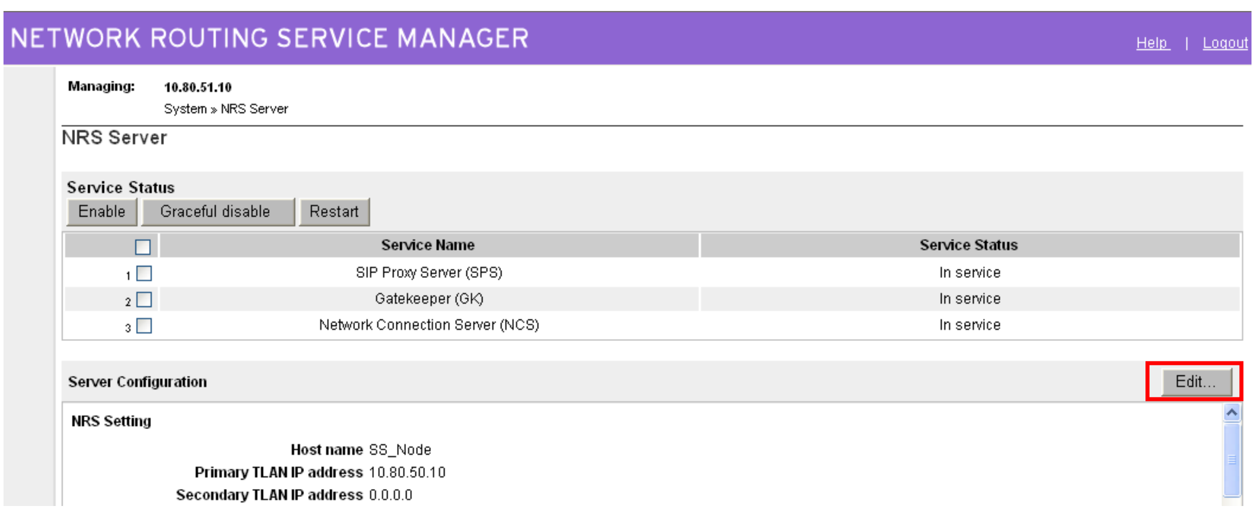
Select **UCM Network Services** from the left pane, which will display the high level **Unified Communications Management** screen.



Click on the **Element Name** with **Element Type** is **Network Routing Service**.



The **NETWORK ROUTING SERVICE MANAGER** screen is displayed. Click **EDIT**.

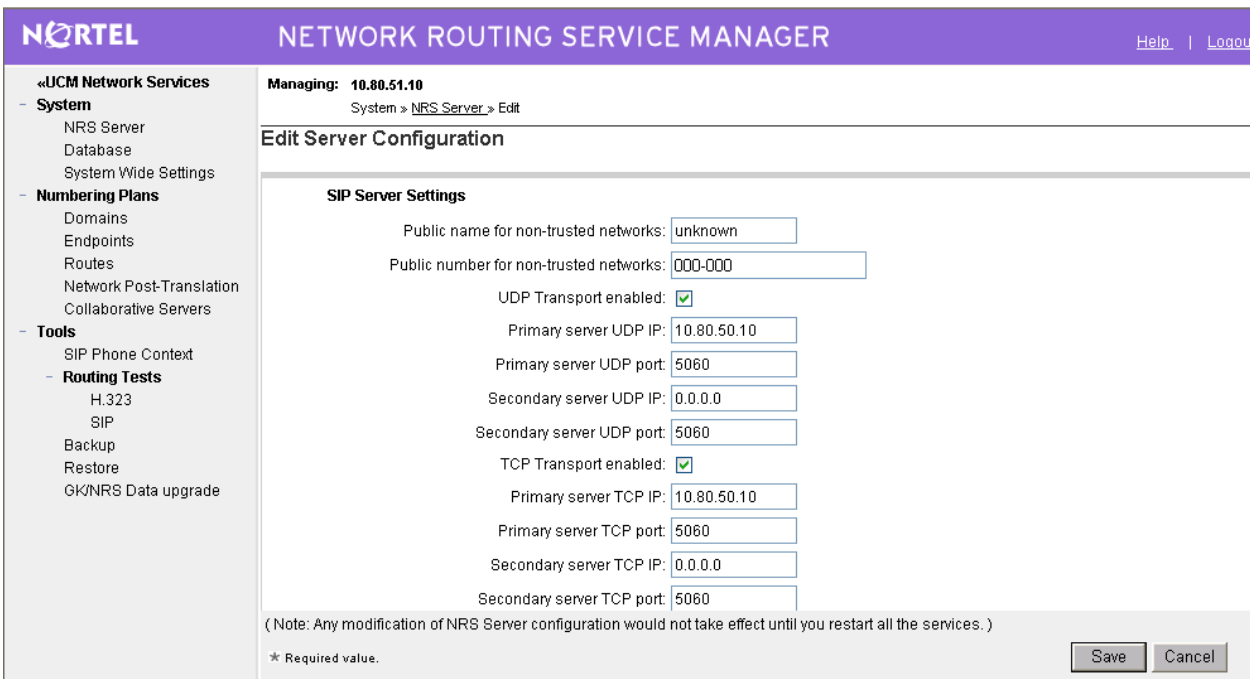


Under **SIP Server Settings**, enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click **Save** (not shown).

NOTE: For the scenario described in these Application Notes, SIP communication between the CS1000E and Session Manager utilizes TCP. The screenshot below enables UDP at a global level though it's possible to configure individual 'Endpoints' to use only TCP. See **Section 7.11**.

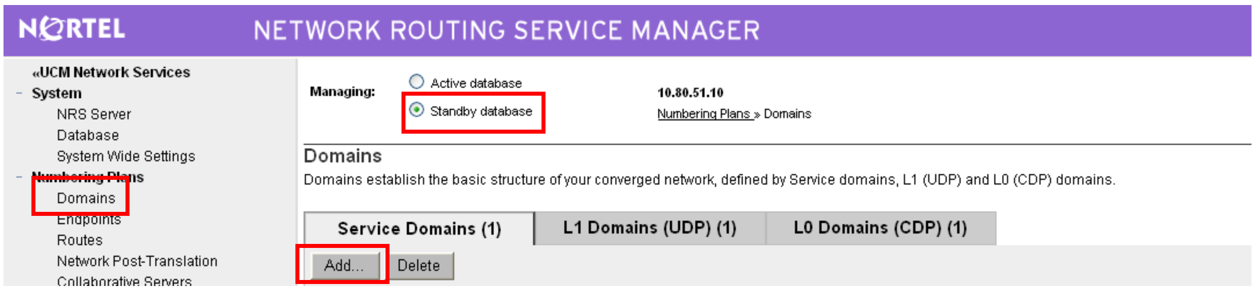
- **UDP transport enabled:** Check the checkbox
- **Primary Server UDP IP:** The Sig Server IP address from **Section 7.2**
- **Primary Server UDP port:** **5060**
- **TCP transport enabled:** Check the checkbox
- **Primary Server TCP IP:** The Sig Server IP address from **Section 7.2**
- **Primary Server TCP port:** **5060**

Click on **Save**.

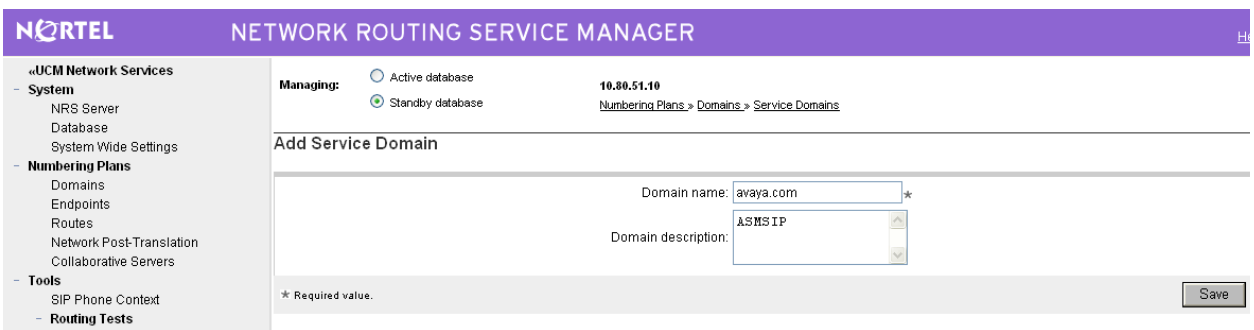


7.10 Administer Service Domain

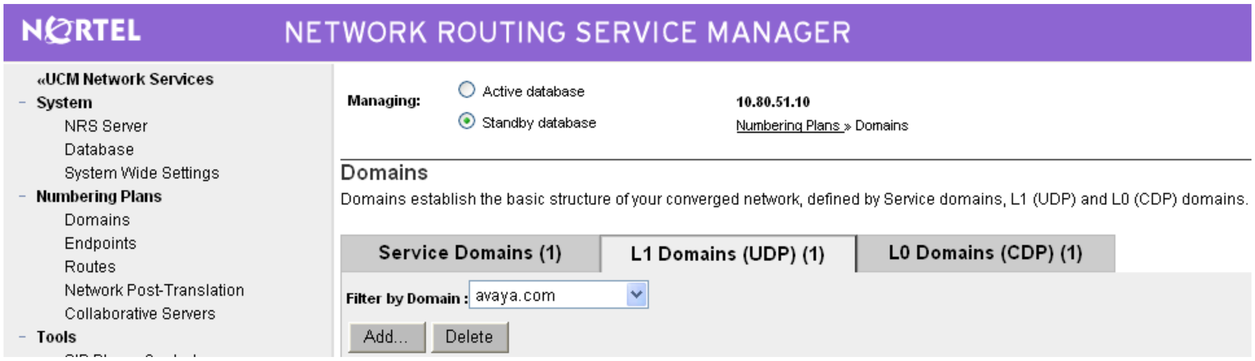
The NRS hosts an active and a standby database. The active database is used for runtime queries, and the standby database is used for administrative modifications. Under **Numbering Plans** on the left, click on **Domains**, and the **Domains** screen will be displayed. To add a domain, first click on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



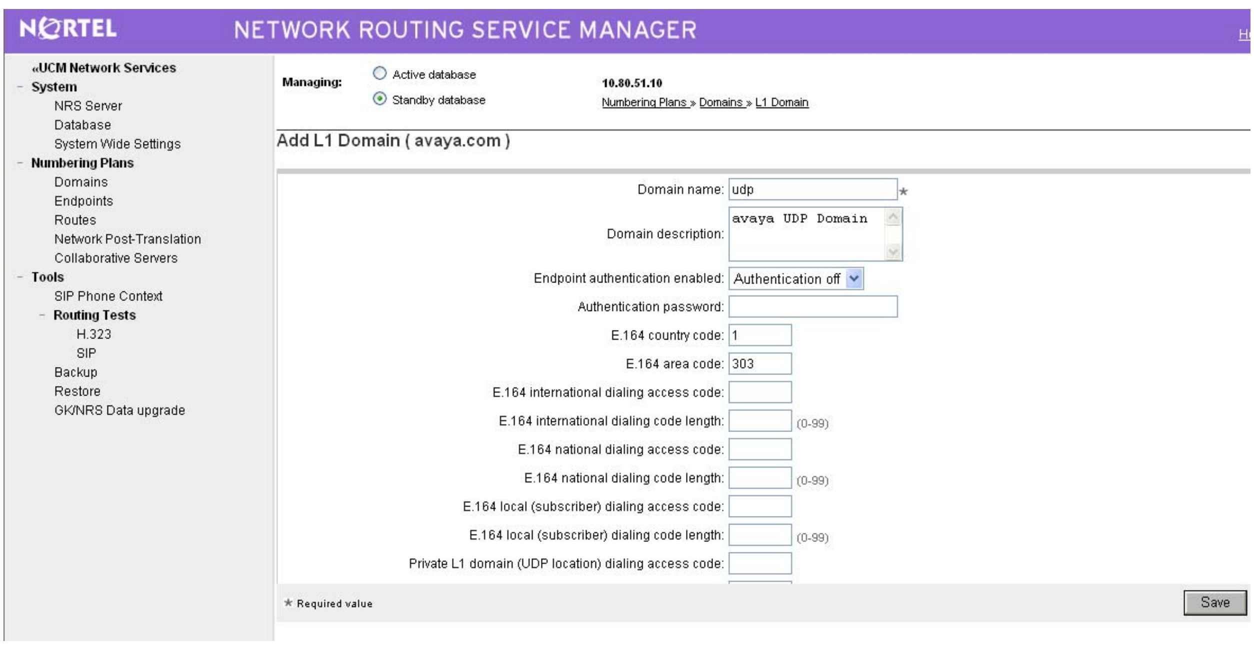
The **Add Service Domain** screen is displayed. Enter the SIP domain name as shown in **Section 7.8** into the **Domain name** field, and a descriptive text for the **Domain description** field. Click **Save**.



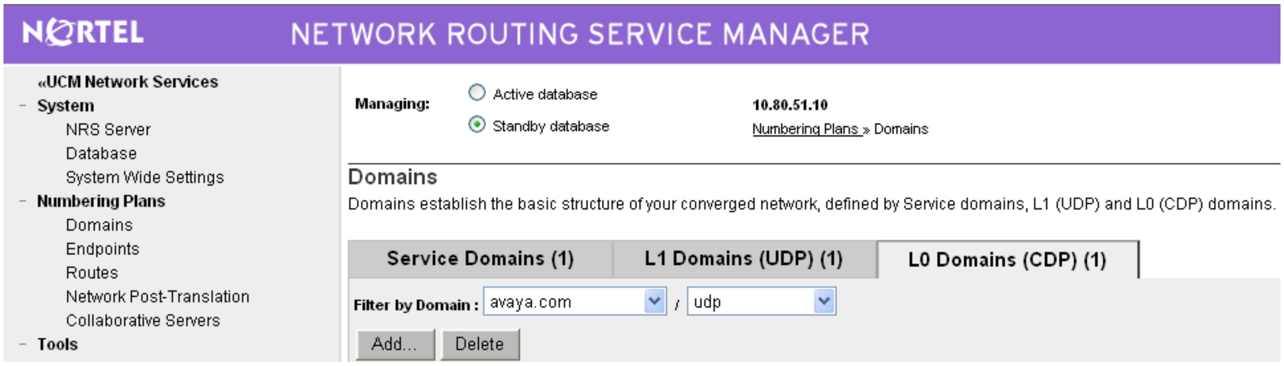
Select the **L1 Domains (UDP)** tab to display the **L1 Domains (UDP)** screen. Select the service domain just created for **Filter by Domain**, and click on **Add** to add a new L1 domain. The L1 and L0 domains are building blocks of the phone context for private addresses. For more information on L1 and L0 domains, refer to the Nortel documentation in **Section 10**.



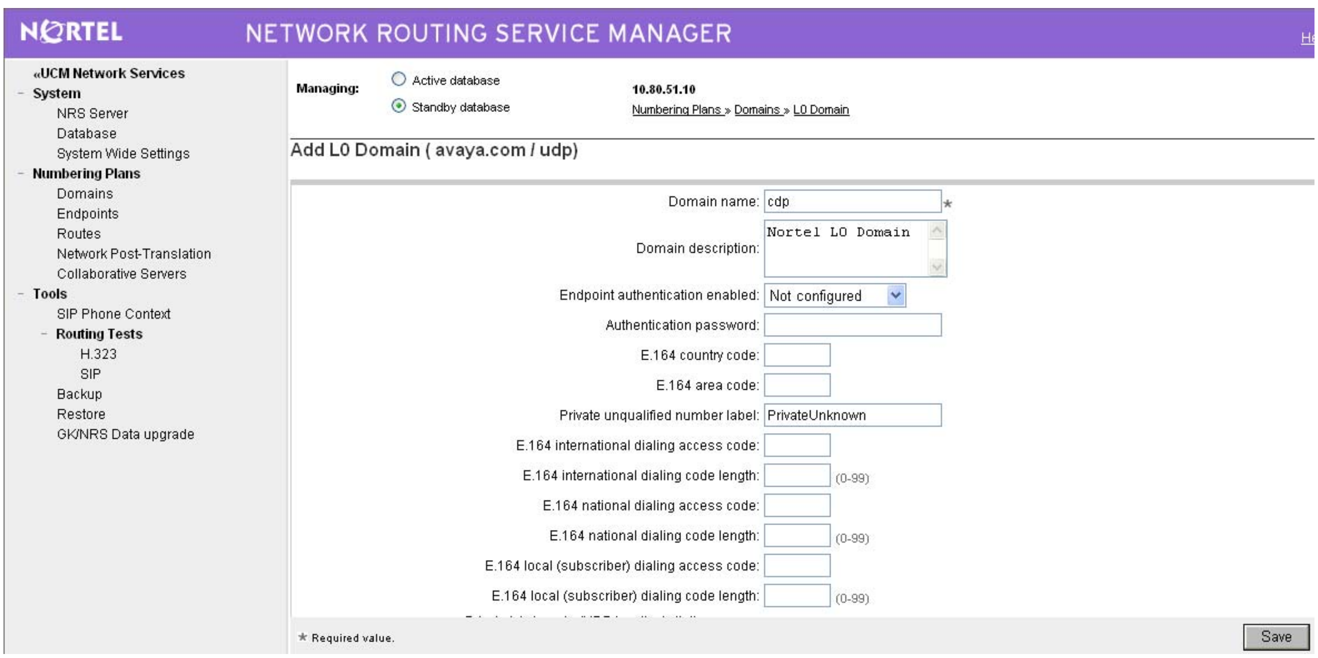
The **Add L1 Domain (avaya.com)** screen is displayed next, as shown below. Enter a descriptive **Domain name** and **Domain description**, and applicable **E.164 country code** and **E.164 area code** for the network configuration. Retain the default value in the remaining fields, and select **Save**.



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.

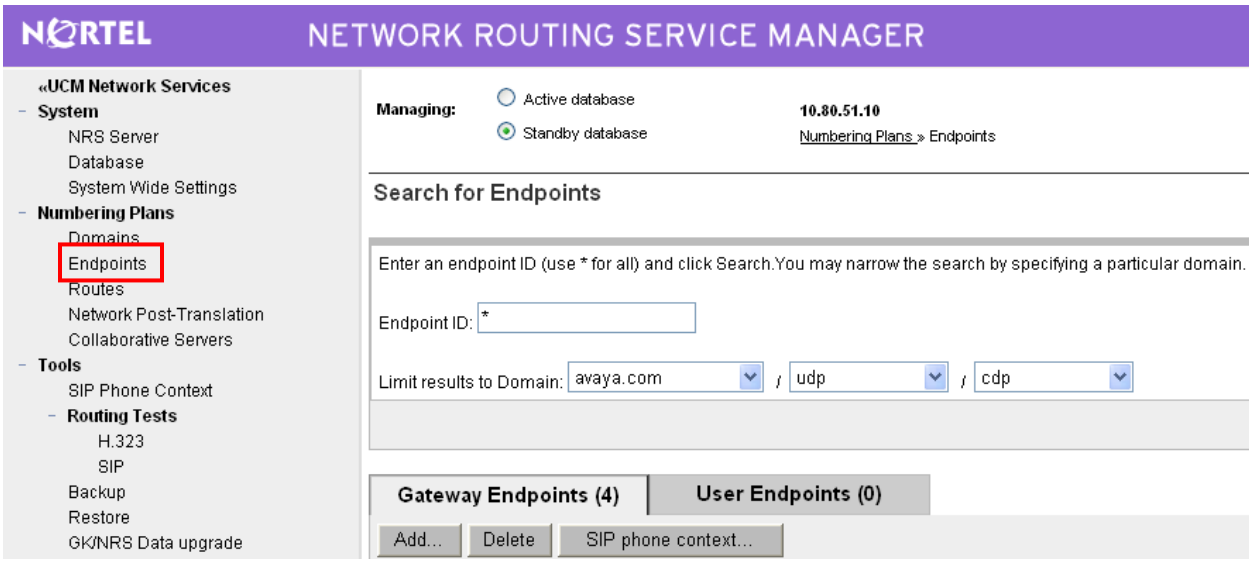


The **Add L0 Domain (avaya.com /udp)** screen is displayed next, as shown below. Enter a descriptive **Domain name** and **Domain description**. Retain the default values in the remaining fields and click **Save**.

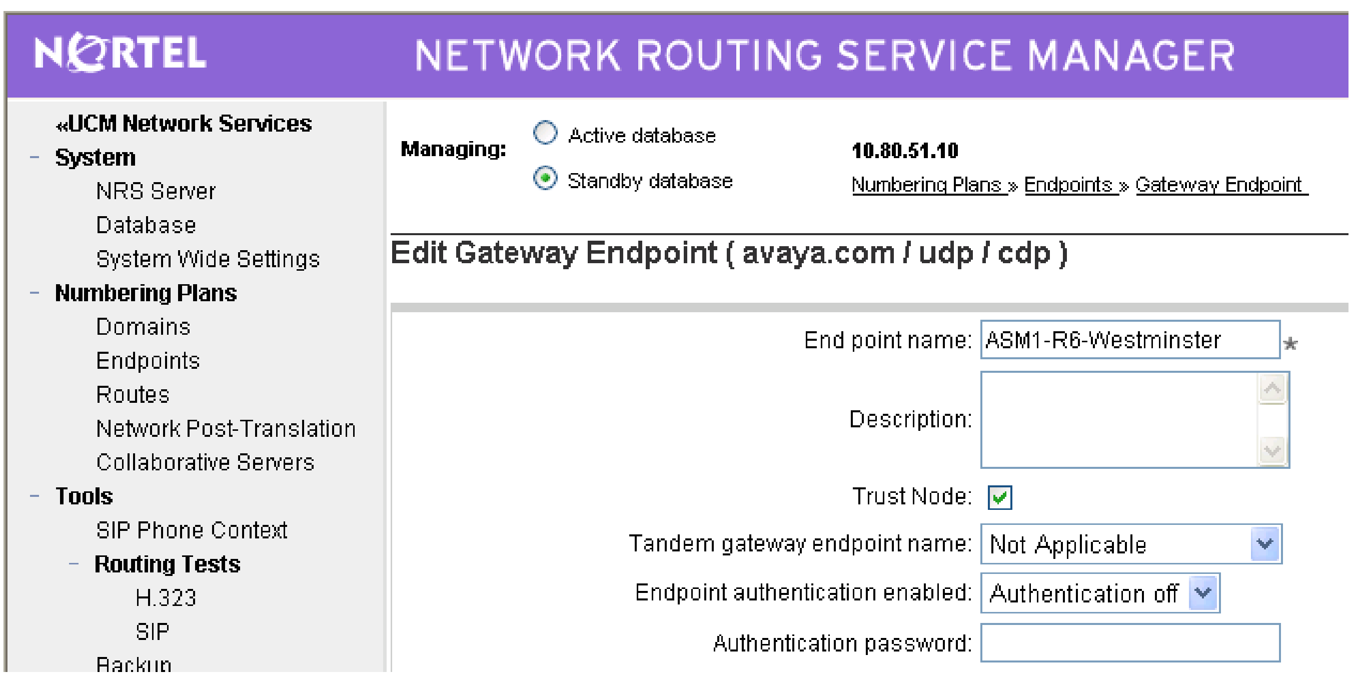


7.11 Administer SIP Gateway Endpoints

Next, configure two SIP gateway endpoints - one for the Session Manager server, and the other for the CS1000E Signaling 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.

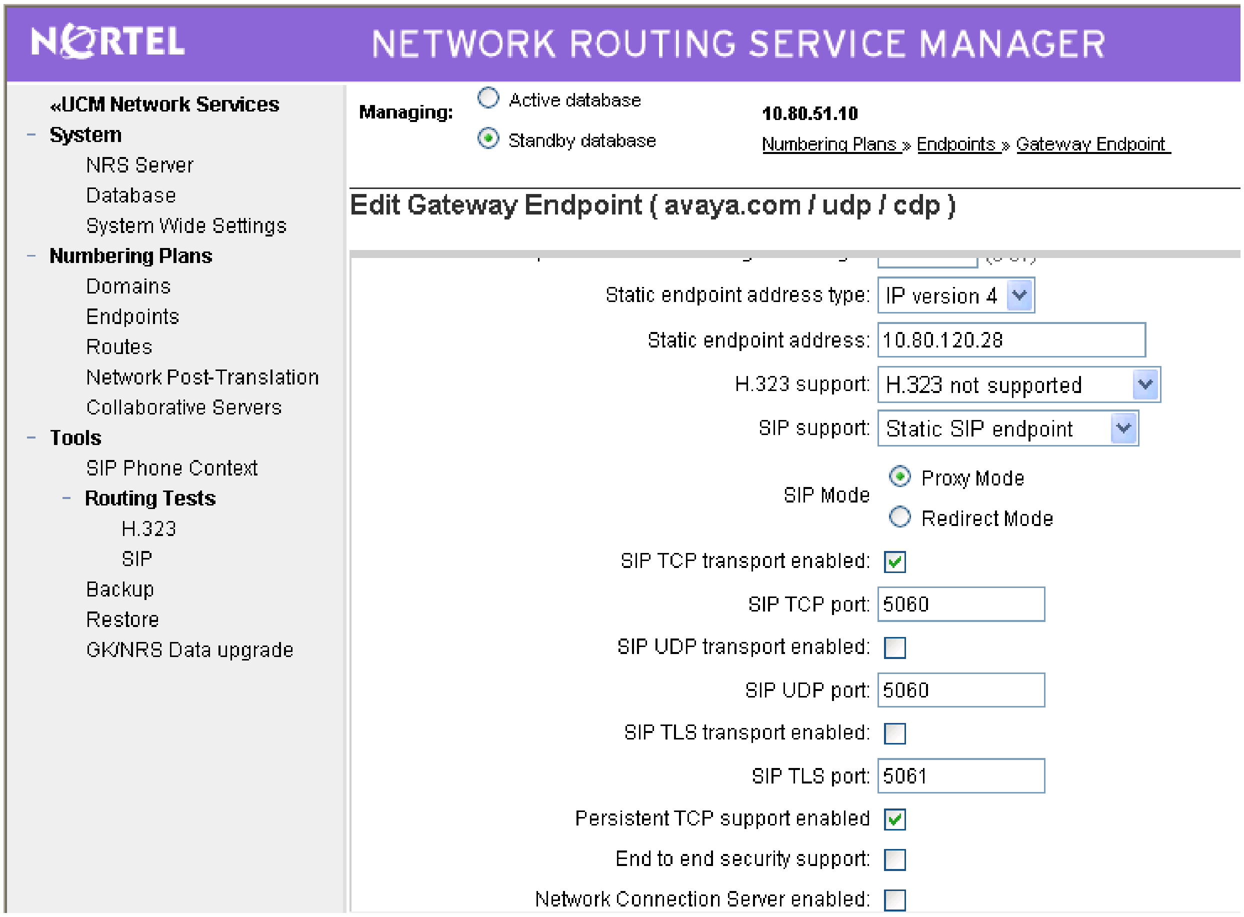


Enter a descriptive **End point name** and **Description**

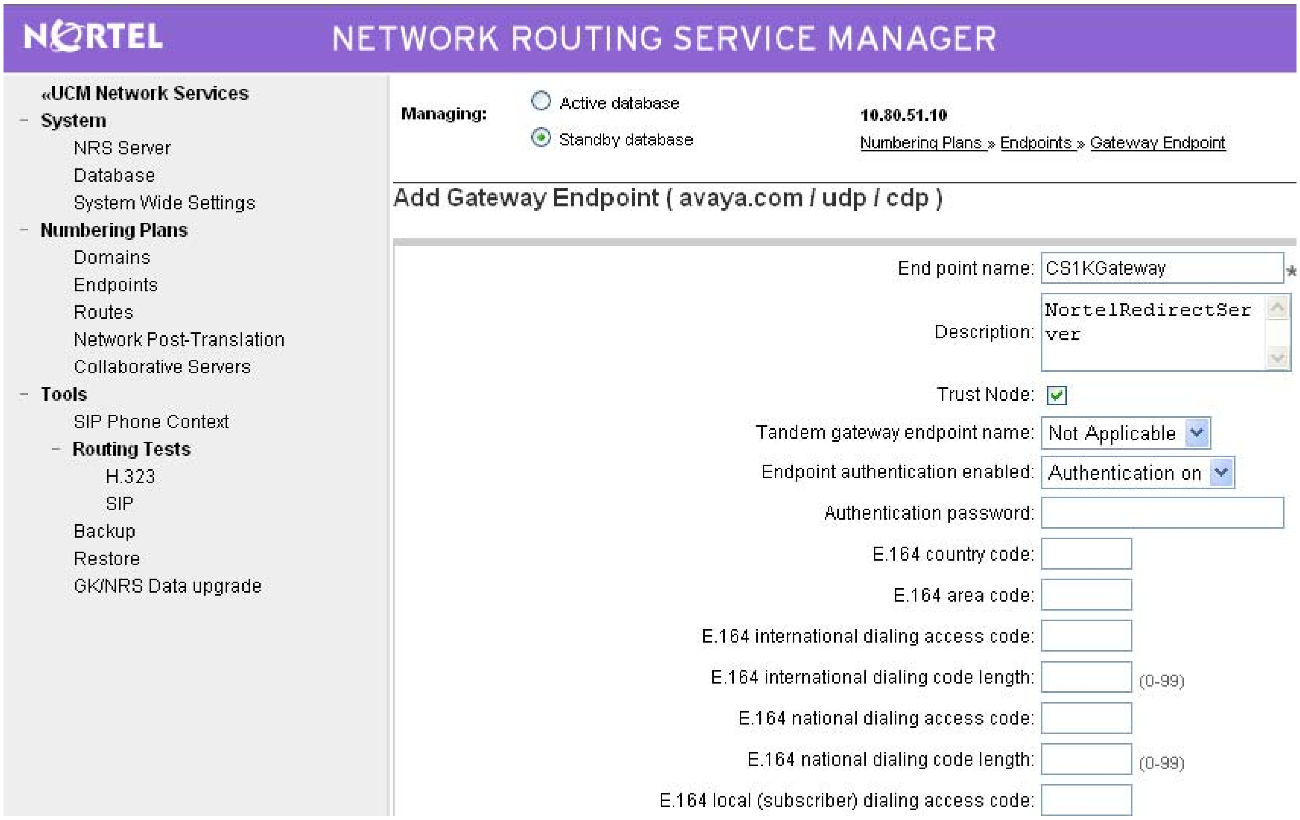


Scroll down the screen. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Save**.

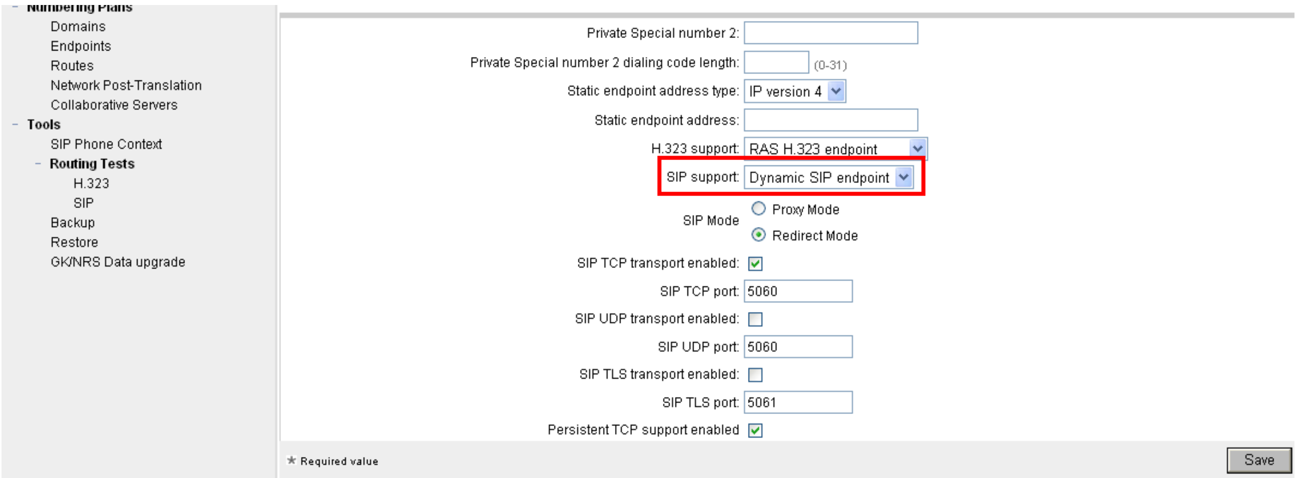
- **Static endpoint address:** IP address of the Session Manager SM-100 interface
- **H.323 Support:** **H.323 not supported**
- **SIP support:** **Static SIP endpoint**
- **SIP TCP transport enabled:** TCP SIP checkbox



Repeat the procedures to add a gateway endpoint for the CS1000 Signaling 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 **as shown in Section 7.8**. Note that the value in the **End Point name** field (**CS1Kgateway**) must be the same that was used in the **End point name** field in the **General** node config screen shown in **Section 7.8**.

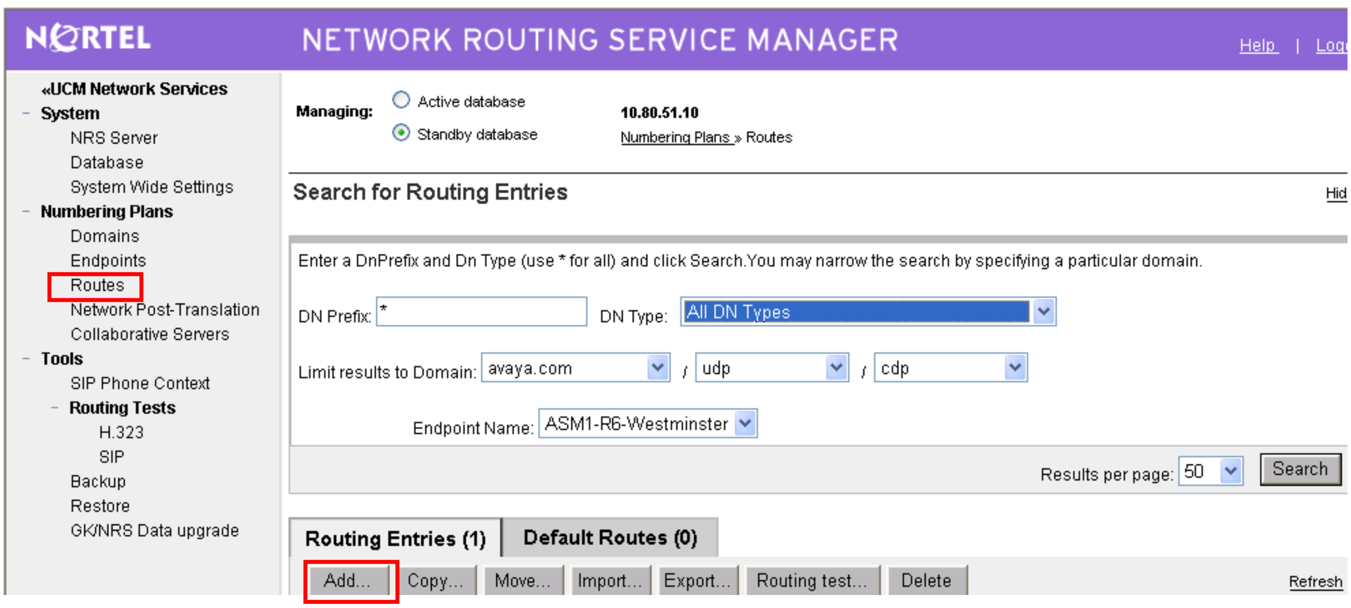


Scroll down the screen. For the **SIP support** field, select **Dynamic SIP endpoint** from the drop-down list. Check the **SIP TCP transport enabled** field to match the SIP transport protocol as shown in **Section 7.8**. Maintain the default values in the remaining fields, and click **Save**.



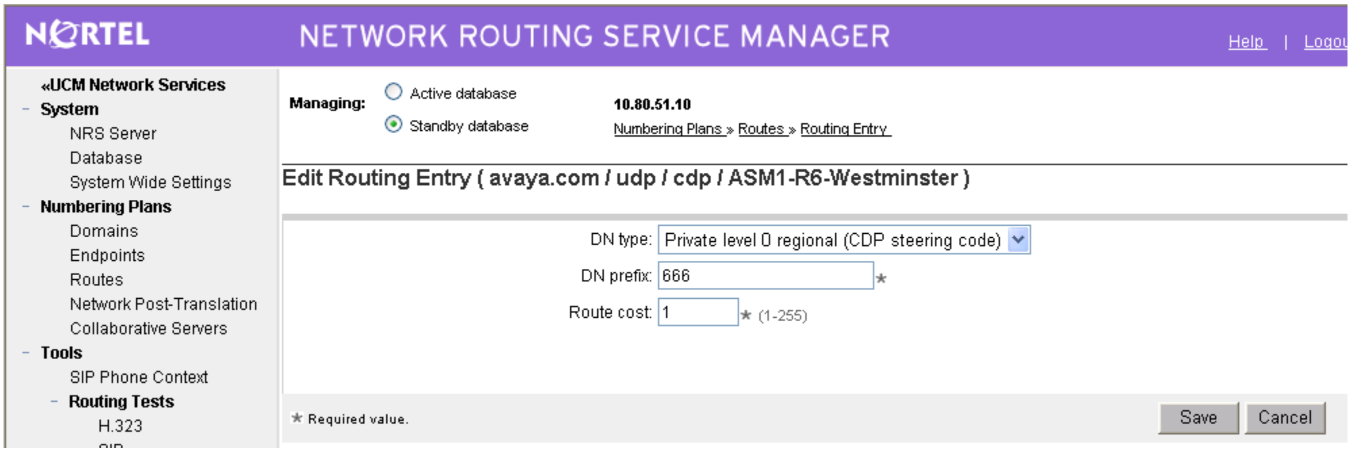
7.12 **Administer Routing Entries**

Configure two routing entries. The first entry uses the Session Manager gateway endpoint to reach the Session Manager and ultimately to Communicatin Manager endpoints with extension digits 666xxxx. The second entry uses the CS1000 Signaling Server to reach CS1000E endpoints who's extensions start with 777xxxx. 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**.

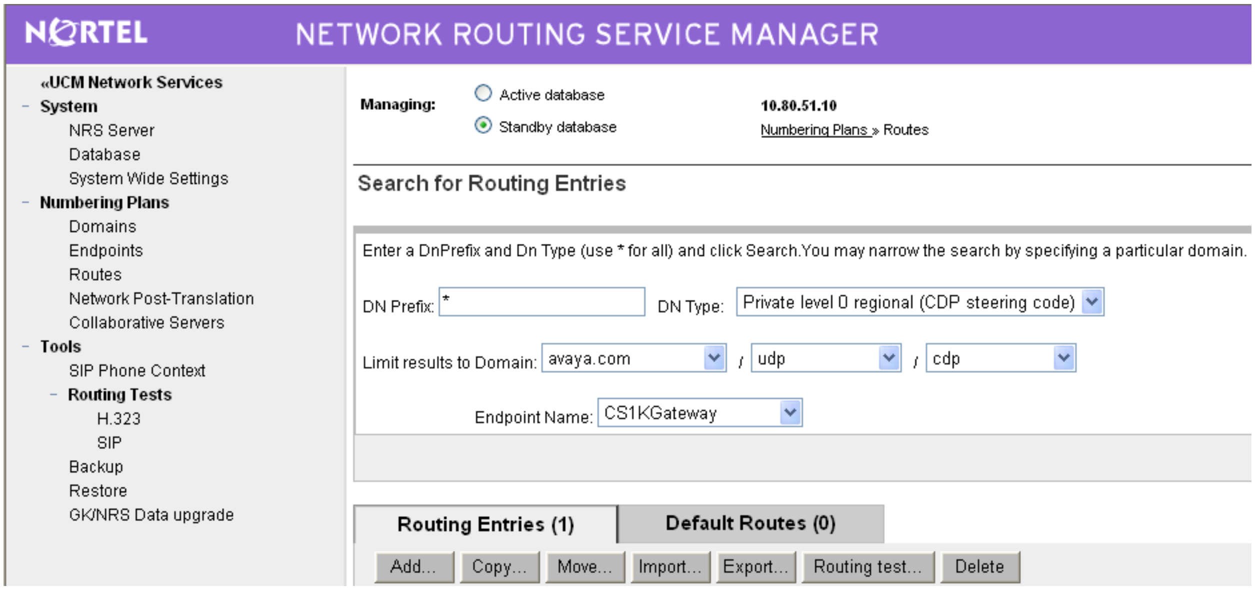


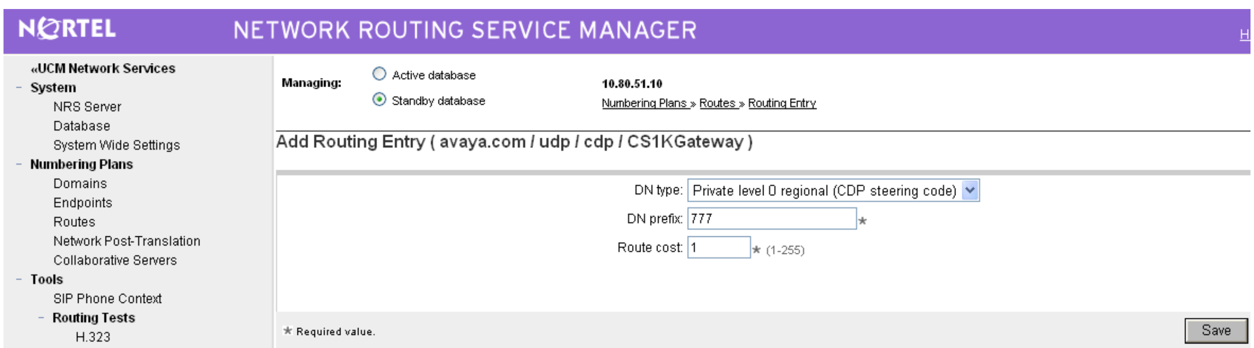
The **Add Routing Entry** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Save**.

- **DN type:** **Private level 0 regional (CDP steering code)**
- **DN prefix:** Dialed prefix digits to match on, in this case **666**
- **Route cost (1 – 255)**: An appropriate cost value with **1** being least cost.



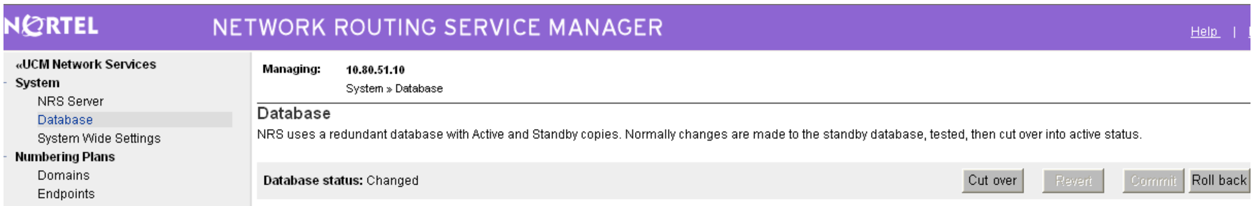
Repeat the same procedures to add a routing entry to reach the CS1000E endpoints with extension digits 777xxxx behind the SIP Redirect Server gateway endpoint.



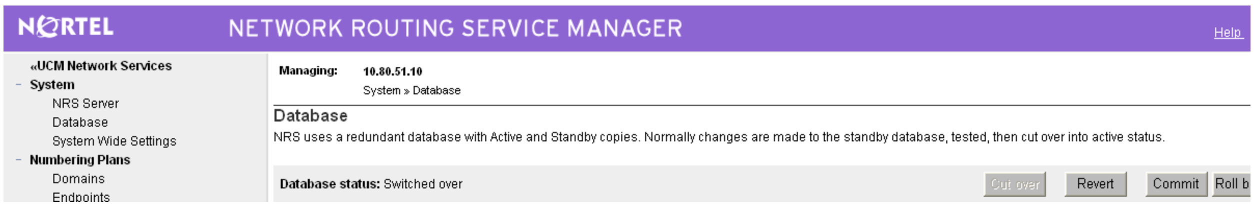


7.13 Cut Over and Commit Changes

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**.



8. Verification Steps

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

8.1 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 4.5**. Verify that all trunks are in the **in-service/idle** state as shown below.

```
status trunk 10

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0010/001 T00226   in-service/idle    no
0010/002 T00227   in-service/idle    no
0010/003 T00228   in-service/idle    no
0010/004 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 4.4**. Verify the signaling group is **in-service** as indicated in the **Group State** field shown below.

```
status signaling-group 10
                         STATUS SIGNALING GROUP

        Group ID: 10                                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 Communication Manager and the CS1000E. Verify which trunks are in use by running the command **status trunk x** where **x** is the number of the SIP trunk group created in **Section 4.5**.

```
status trunk 10

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0010/018 T00018   in-service/idle    no
0010/019 T00019   in-service/idle    no
0010/020 T00020   in-service/idle    no
0010/021 T00021   in-service/idle    no
0010/022 T00022   in-service/idle    no
0010/023 T00023   in-service/idle    no
0010/024 T00024   in-service/idle    no
0010/025 T00025   in-service/active  no   01A1201
```

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 4.5** to reach Session Manager, and **y** is the member number of a connected trunk. As shown above trunk member 25 is in use.

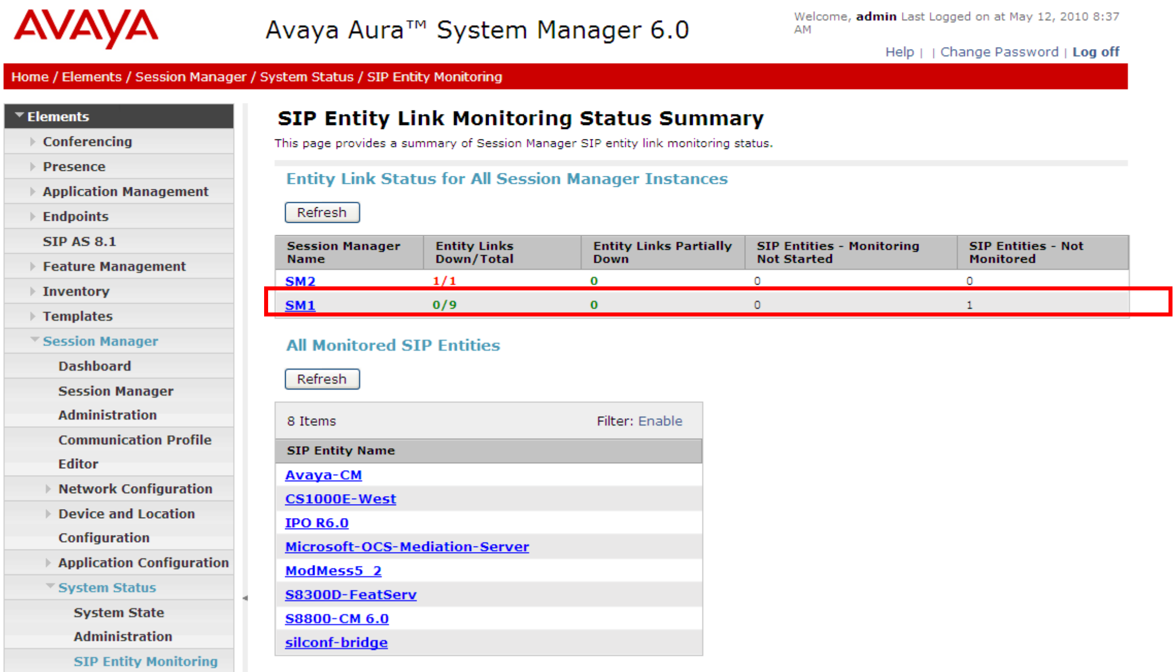
Verify on Page 1 that the **Service State** is **in-service/active**. On Page 2, verify that the IP addresses of the C-LAN and Session Manager are shown in the **Signaling** section. In addition, the **Audio** section shows the G.711 codec and the IP addresses of the Communication Manager and CS1000E endpoints. The **Audio Connection Type** displays **ip-direct**, indicating direct (or 'shuffled') media between the two endpoints.

```
status trunk 10/25                                            Page   1 of   4
                              TRUNK STATUS

 Trunk Group/Member: 0010/025             Service State: in-service/active
               Port: T00025            Maintenance Busy? no
 Signaling Group ID: 10

   IGAR Connection? no

    Connected Ports: 01A1201
```

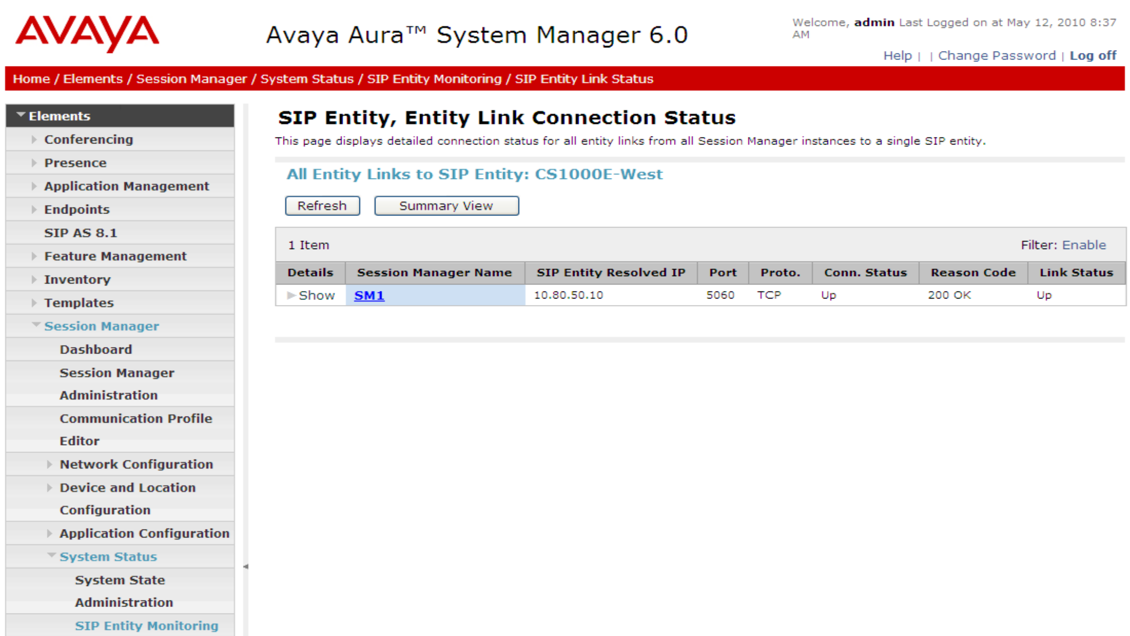
```
status trunk 10/25                                            Page   2 of   4
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: 01A0417
  Signaling   IP Address                               Port
   Near-end:  10.80.111.76                           : 5060
    Far-end:  10.80.120.28                           : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-tdm        Authentication Type: None
    Near-end Audio Loc: 01A0201                Codec Type: G.711
   Audio      IP Address                               Port
   Near-end:  10.80.111.77                           : 25808
    Far-end:  10.80.100.39                           : 5004
```

8.2 Verify Avaya Aura™ Session Manager

Log in to System Manager. From the left-pane navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** to verify that none of the links to the defined SIP entities are down.

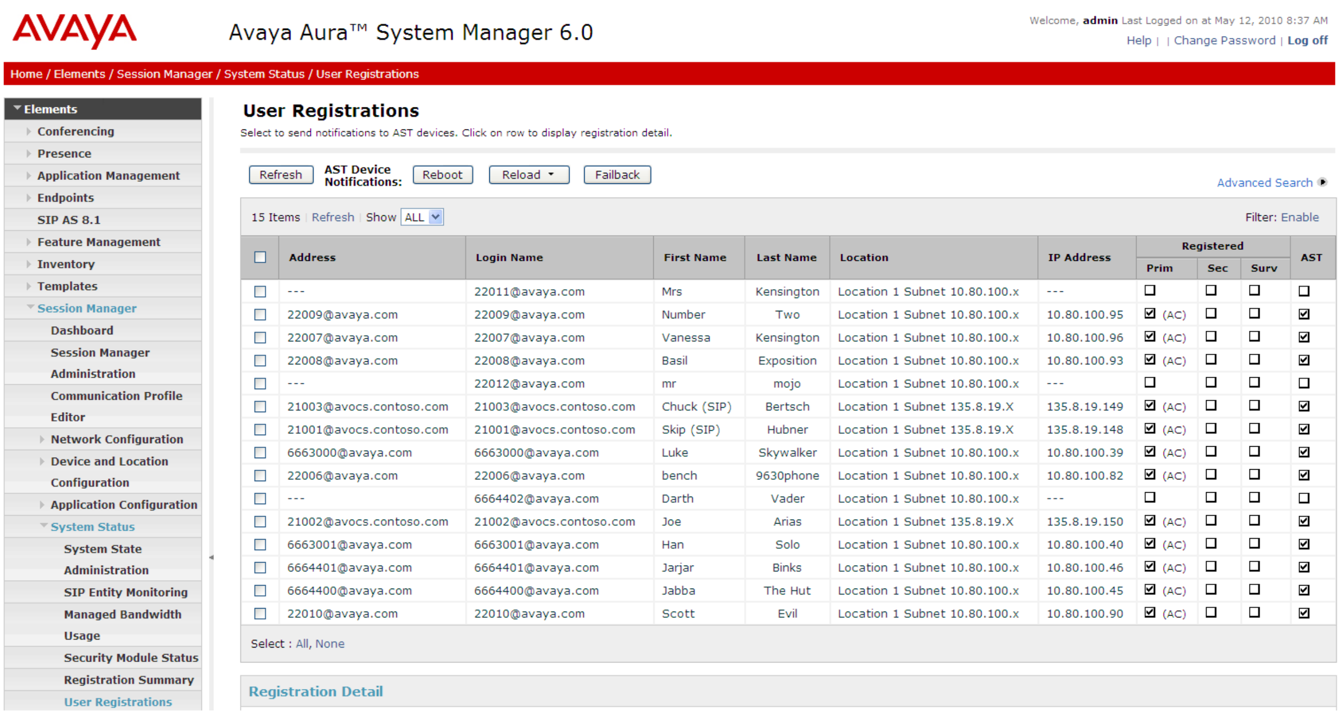


Under **All Monitored SIP entities**, select the appropriate SIP Entity Name and verify that the connection status is **Up**, as shown below for the Communication Server 1000.



8.3 Verify 96xx SIP Phones are Registered

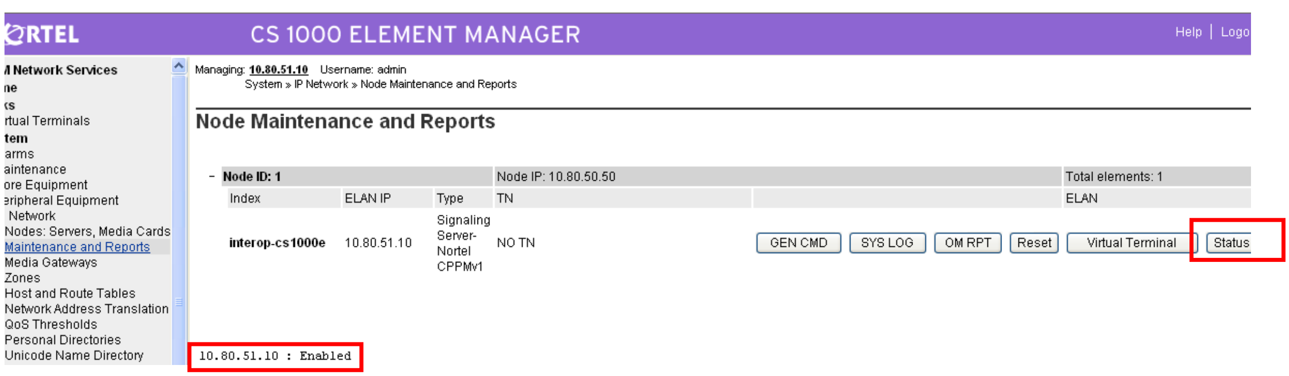
Log in to System Manager. Navigate to **Elements → Session Manager → System Status → User Registrations** on the left-pane to verify which endpoints are registered with Session Manager.



8.4 Verify Avaya Communication Server 1000

8.4.1 Verify Status of the Signaling Server

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.



8.4.2 Verify Status of an Active Call

To verify the status of an active call on the CS1000, first login to the CPPM Linux shell via SSH. Next, make a phone call between the CS1000E and Communication Manager. From the Linux shell run the command **SIPGwShow tSSG all** (additional variations of this command can be found by running **SIPGwShow** without any additional qualifiers). The results as displayed below indicate, among other things, an active call on extension **7771088** that's using **G.711MuLaw** and is talking to another endpoint with the IP address of **10.80.48.200**. Chan **1** of the **VTRK** is in use.

```
[admin@interop-cs1000e ~]$ SIPGwShow tSSG all

=== VTRK ===
SIPNPM Status                : Active
Primary   Proxy IP address   : 10.80.50.10
Primary   Proxy port         : 5060
Primary   Proxy Transport    : TCP
Secondary Proxy IP address   : 0.0.0.0
Secondary Proxy port         : 5060
Secondary Proxy Transport    : TCP
Active    Proxy              : Primary  :Registered
Time To Next Registration    : 12 Seconds
Channels Busy / Idle / Total : 1 / 5 / 6
Stack version              : 4.0.0.30
TLS Security Policy          : Security Disabled
SIP Gw Registration Trace    : OFF
Output Type Used             : RPT
Channel tracing          : -1
There are 1 sessions.
Handle     Chan Type        Direction CallState SIPState          RxState   TxState
---------- ---- ----------- --------- --------- ----------------- --------- -------
--
0x9677300    1 VTRK        Terminate BUSY      Ringing Sent      Connected
Connected
Codec                 AirTime FS  MS Fax DestNum RemoteIP        URI Scheme
--------------------- ------- --- -- --- ------- --------------- ------------
G_711_u_law_20MS_NOVAD      78 yes m  no  7771088 10.80.48.200    SIP
```

8.5 Verification Scenarios

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

- Basic calls between various telephones on the Session Manager and 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

- o Conference
- o Calling number block

- During testing an issue was discovered such that if a CS1000E endpoint is forwarded to Communication Manager Feature Server, a call from a SIP endpoint to the forwarded CS1000E endpoint will fail. A SIP trace reveals Communication Manager sends a "404 originating user not found" back to the CS1000E thus preventing the call from completing. This issue is currently being investivated.

9. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager can interoperate with the Avaya (formerly 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 IP telephones, including SIP endpoints, on Communication Manager and the CS1000 telephones is supported.
- Calling/called party name and number display may not be consistent for some supplementary calling features such as call transfers, call forwarding and call conferencing.

10. Additional References

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

Avaya Aura™ Session Manager 6.0:

[1] *Avaya Aura™ Session Manager Overview*, Doc ID 03-603323, available at http://support.avaya.com.

[2] *Installing and Upgrading Avaya Aura™ Session Manager 6.0*, Doc ID 03-603324, available at http://support.avaya.com.

[3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager 6.0*, Doc ID 03-603325, available at http://support.avaya.com.

Avaya Aura™ Communication Manager 6.0:

[4] *Administering Avaya Aura™ Communication Manager as a Feature Server*, Doc # 03-603479, Issue 1.2, Release 5.2 January 2010, available at http://support.avaya.com.

[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, June 2010, available at http://support.avaya.com.

[7] *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones: Administrator Guide*, Release 2.6, Doc ID 16-601944 Issue 5. June 2010. http://support.avaya.com

[8] *Avaya Toll Fraud Security Guide*, Doc ID 555-025-600, February 2010, available at http://support.avaya.com

Avaya Application Notes:

[9] *Front-Ending Nortel Communication Server 1000 with an AudioCodes Mediant 1000Modular 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.

[10] *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.

[11] *Configuring 96xx SIP Phones with Avaya Aura™ Session Manager, 5.2* – Issue 1.0 available at http://www.avaya.com

Nortel CS1000E 6.0 Support Documents:

[12] *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

[13] *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

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