Avaya Solution Interoperability Test Lab

Configuring SIP Trunks among Avaya Aura® Session Manager Release 6.1, Avaya Communication Server 1000E Release 7.5 and Cisco Unified Communications Manager Release 8.0(3) – Issue 1.0

Abstract

These Application Notes describe a sample configuration of a network that uses SIP trunks among Avaya Aura® Session Manager Release 6.1, Avaya Communication Server 1000E Release 7.5 and Cisco Unified Communications Manager Release 8.0(3).

- Avaya Aura Aura® Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and adaptations to resolve SIP protocol differences across different telephony systems.
- Avaya Communication Server 1000E 7.5 runs on a co-resident server platform and supports digital and UNIstim (IP) telephones.
- Cisco Unified Communications Manager provides SIP trunks for connecting to other telephony systems and supports SCCP (IP) and SIP endpoints.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested on this solution.

TABLE OF CONTENTS

1. Introduction

These Application Notes describe a sample configuration of a network that uses SIP trunks among Avaya Aura Aura® Session Manager Release 6.1, Avaya Communication Server 1000E Release 7.5 and Cisco Unified Communications Manager Release 8.0(3).

As shown in **Figure 1**, Avaya Communication Server 1000E Release 7.5 runs on the Common Processor Pentium Mobile (CP+CM) server as a co-resident configuration and supports 1100 series UNIstim (IP) telephones, 2050 UNIStim Softphone, and M3904 Digital telephones. Avaya Communication Server 1000E is connected over a SIP trunk to Avaya Aura® Session Manager Release 6.1, using the SIP Signaling network interface on Session Manager.

Cisco 7965 IP Telephones (SCCP) and 7975 IP Telephones (SIP) are supported by Cisco Unified Communications Manager Release 8.0(3). Cisco Unified Communications Manager is also connected over a SIP trunk to Session Manager. An Adaptation Module designed for Cisco Unified Communications Manager was configured on Session Manager to resolve SIP protocol differences between Cisco Unified Communications Manager and Avaya Communication Server 1000E.

All inter-system calls are carried over these SIP trunks. To support interoperability testing in a heterogeneous network, all telephony systems are deployed in the same network domain.

Avaya Aura® Session Manager is managed by Avaya Aura® System Manager. For the sample configuration, Avaya Aura® System Manager and Avaya Aura® Session Manager each run on an Avaya S8800 server.

These Application Notes will focus on the configuration of the SIP trunks and call routing. Detailed administration of other aspects of Cisco Unified Communications Manager, Avaya Communication Server 1000E or Session Manager will not be described. For more information on these other administration actions, see the appropriate documentation listed in **Section 9.**

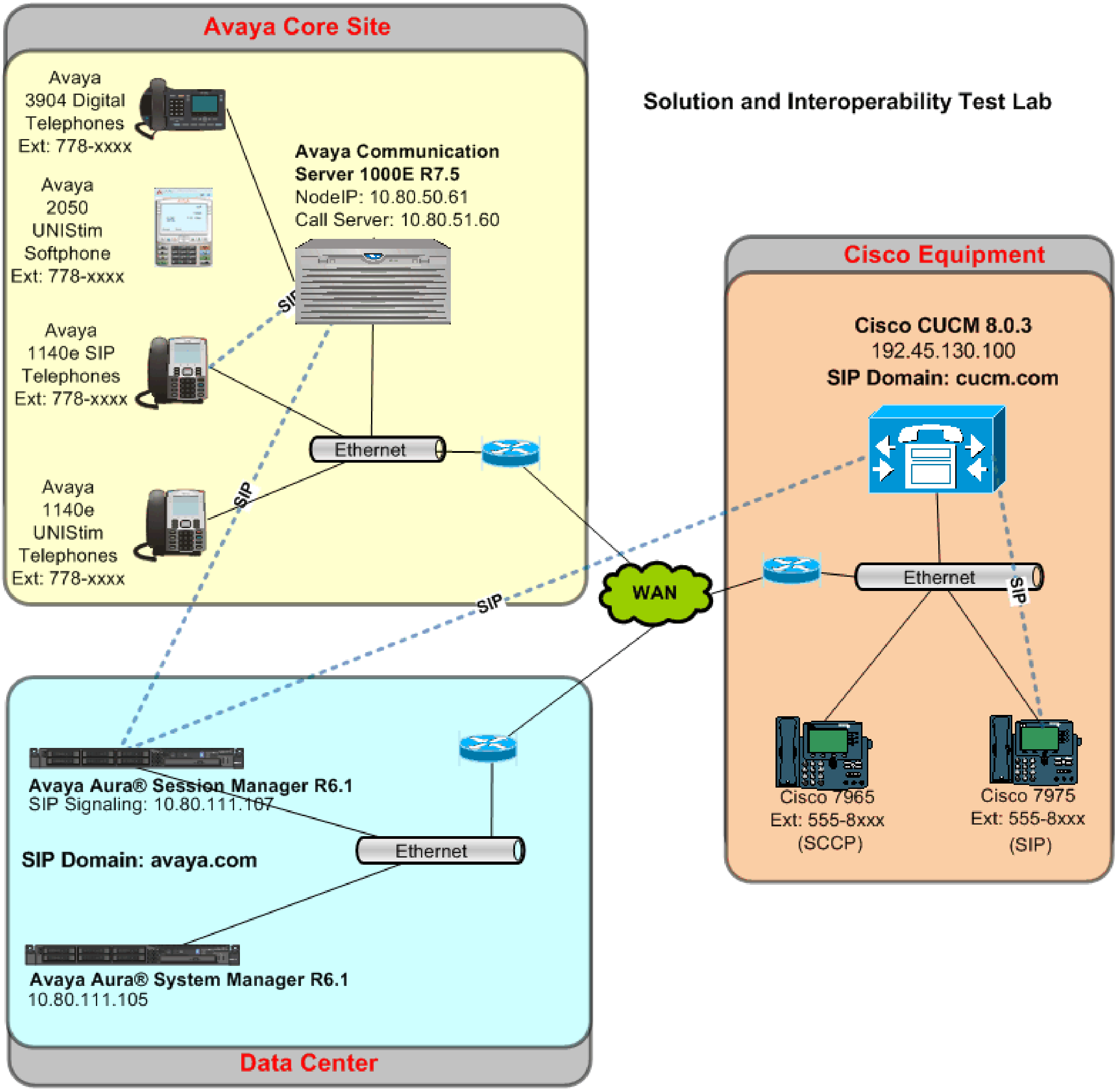


Figure 1 – Sample Configuration

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Provider	Hardware Component	Software Version
Avaya	S8800 Server	Avaya Aura® Session Manager Release 6.1 Build 6.1.0.0.610016
		Avaya Aura® System Manager Release 6.1, Load: 6.1.0.4.5072 Service Pack 0
Avaya	CS1000E CP+PM co-resident server	Release 7.5, Version 7.50.17 Service Update: 7.50_17Nov30 Deplist: X21 07.50Q
Avaya	1 – Avaya 2050 IP Softphone (UNIStim)	4.0.4.1
Avaya	1 – Avaya 1140E IP Telephone (UNIStim)	0625C88
Avaya	1 – Avaya 1140E IP Telephone (SIP)	4.0.0.4
Avaya	1 – Avaya M3904 Digital Telephone	n/a
Cisco	7816I4-K9 CMD1 Appliance (IBM)	Cisco Unified Communications Manager (CUCM) Product Version: 8.0.3.20000-2 Platform Version : 4.0.0.0-43
Cisco	1 - 7975G IP Telephone (SIP)	Phone Load: SIP75.9-0-3S
Cisco	1 - 7965G IP Telephone (SCCP)	Phone Load: SCCP45.9-0-3S

3. Configure Avaya Communication Server 1000E

This section describes the details for configuring Avaya Communication Server 1000E to route calls to Session Manager over a SIP trunk. In the sample configuration, Avaya Communication Server 1000E Release 7.5 was deployed as a co-resident system with the SIP Signaling Server and Call Server applications all running on the same CP+PM server platform.

Note: Avaya Aura® Session Manager Release 6.1 provides all the SIP Proxy Service (SPS) and Network Connect Services (NCS) functions previously provided by the Network Routing Server (NRS) application. As a result, the Network Routing Server application is no longer needed to configure a SIP trunk between Avaya Communication Server 1000E Release 7.5 and Session Manager Release 6.1.

These instructions assume Avaya Aura® System Manager has already been configured as the Primary Security Server for the Avaya Unified Communications Management application and Avaya Communication Server 1000E is registered as a member of the System Manager Security framework. For more information on how to configure System Manager to integrate with the Avaya Unified Communications Management application, see **Reference [7]** in **Section 9.**

In addition, these instructions also assume the configuration of the Call Server and SIP Signaling Server applications has been completed and Avaya Communication Server 1000E is configured to support the 1140e (SIP &UNIStim), 2050Softphone UNIStim (IP) telephones, and M3904 Digital telephones. For information on how to administer these functions of Avaya Communication Server 1000E, see **References [6]** through **[10]** in **Section 9.**

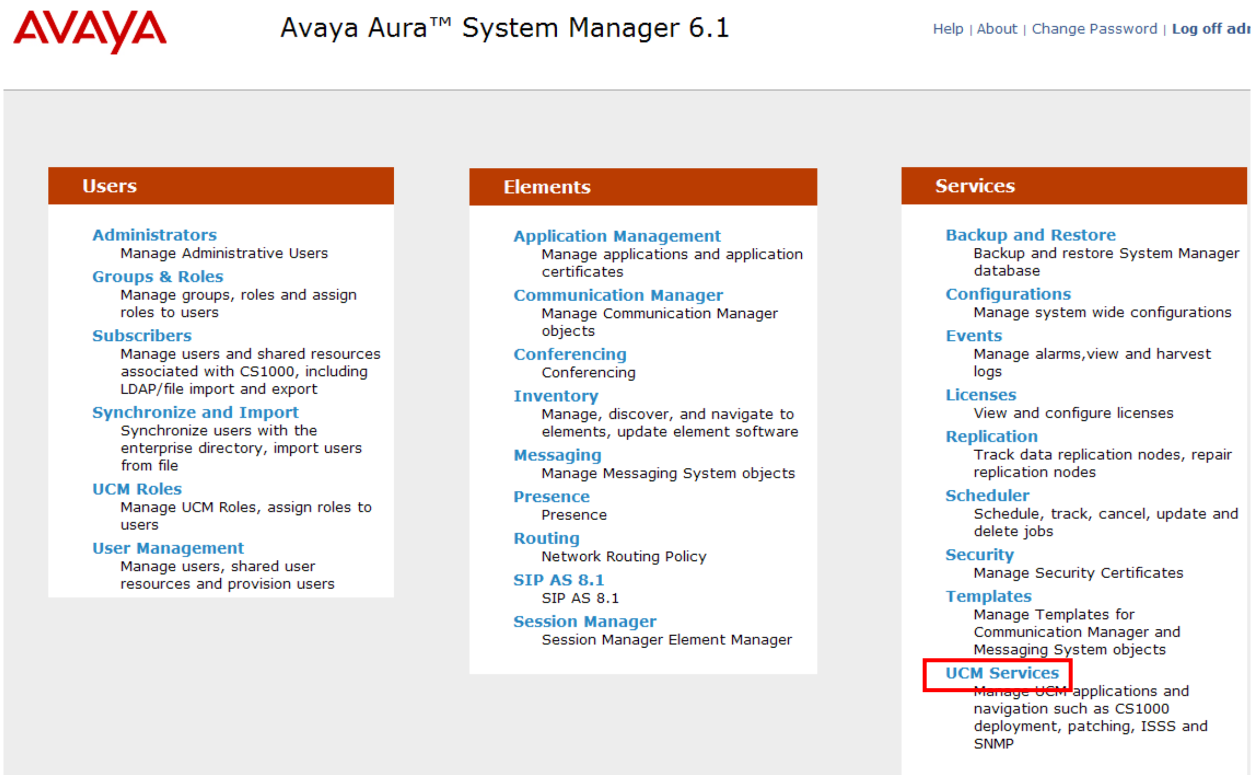
Using the Avaya Unified Communications Management web interface, the following administration steps will be described:

- Launch Avaya Unified Communications Management web interface from System Manager
- Confirm Node and IP addresses
- Confirm Virtual Trunks and D-Channel
- Configure SIP Trunk to Session Manager
- Administer Route List Block and Distant Steering Code
- Commit changes

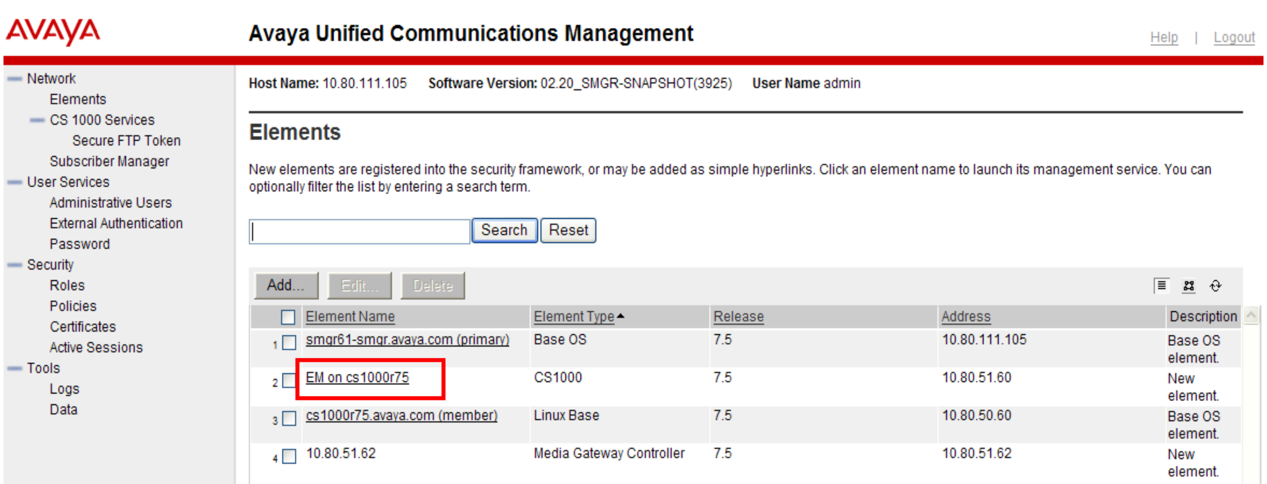
Note: Some administration screens have been abbreviated for clarity.

Access the web based GUI of Avaya Aura® System Manager by using the URL **"http://<ip-address>/SMGR"**, where **<ip-address>** is the IP address of Avaya Aura® System Manager. Login with the appropriate credentials.

The Avaya Aura® System Manager Home Page will be displayed. Under **Services** category on the right side of the page, click on **UCM Services** link.



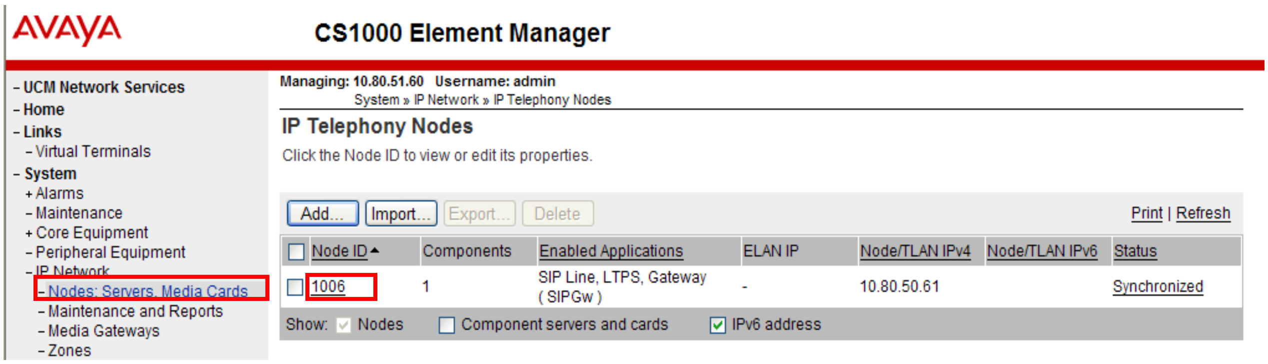
The Avaya Unified Communications Management **Elements** page will open in a new browser window. Click on the **Element Name** corresponding to **"CS1000"** in the **Element Type** column.



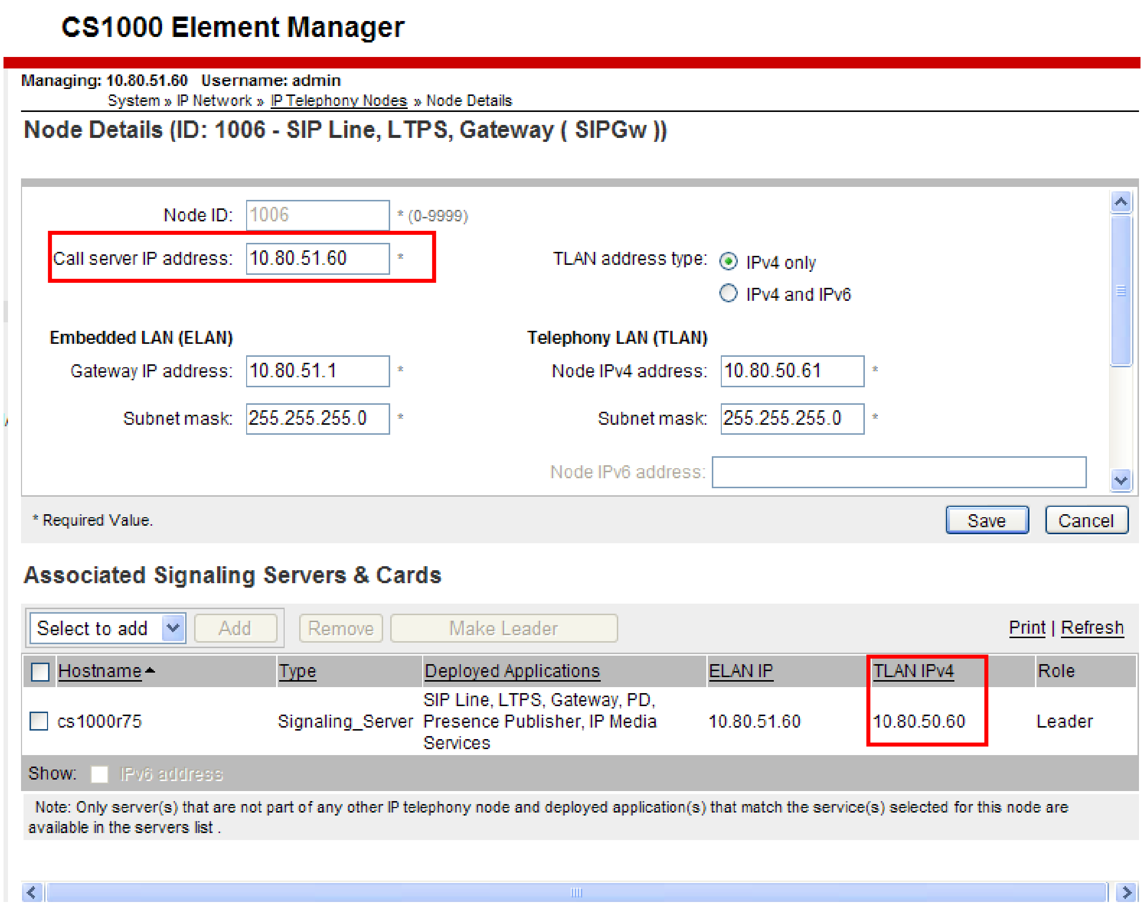
3.1. Confirm Node and IP Addresses

Expand **System → IP Network** on the left panel and select **Nodes: Servers, Media Cards**.

The **IP Telephony Nodes** page is displayed as shown below. Click "**<Node id>**" in the **Node ID** column to view details of the node. In the sample configuration, "**1006**" was used.



The **Node Details** screen is displayed with additional details as shown below. Make a note of the **Call server IP address** and Signaling Server **TLAN IPv4** address fields highlighted below as these values are used to configure other sections.

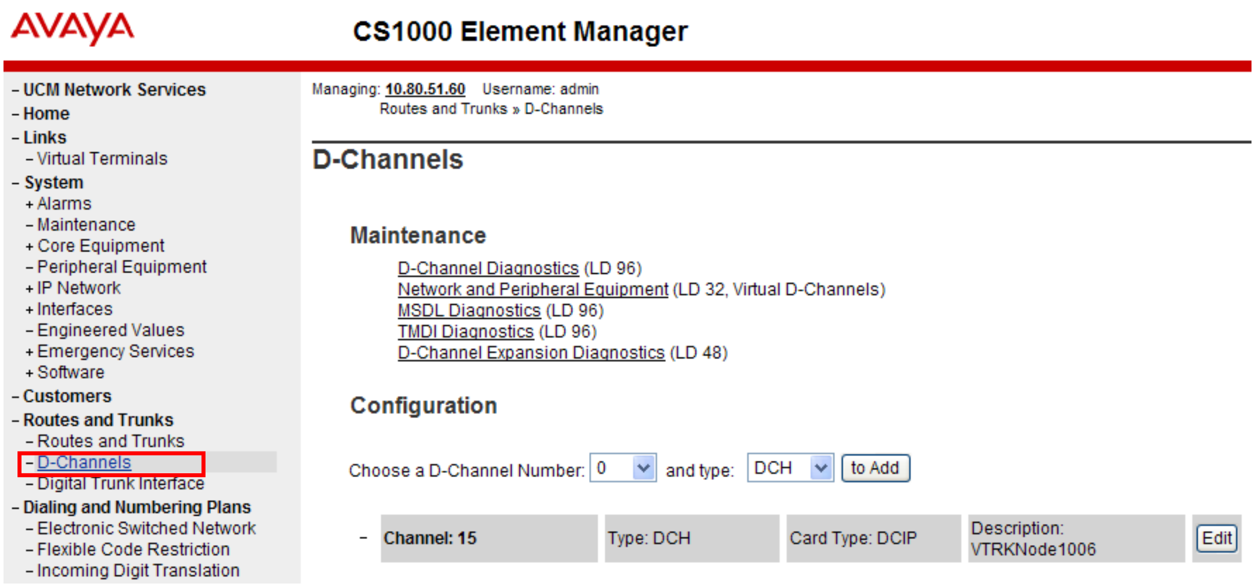


3.2. Confirm Virtual D-Channel, Routes and Trunks

Avaya Communication Server 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server. This section describes the steps to verify that this administration has already been completed.

3.2.1. Confirm Virtual D-Channel Configuration

Expand **Routes and Trunks** on the left navigation panel and select **D-Channels**. The screen below shows all the D-channels administered on the sample configuration.



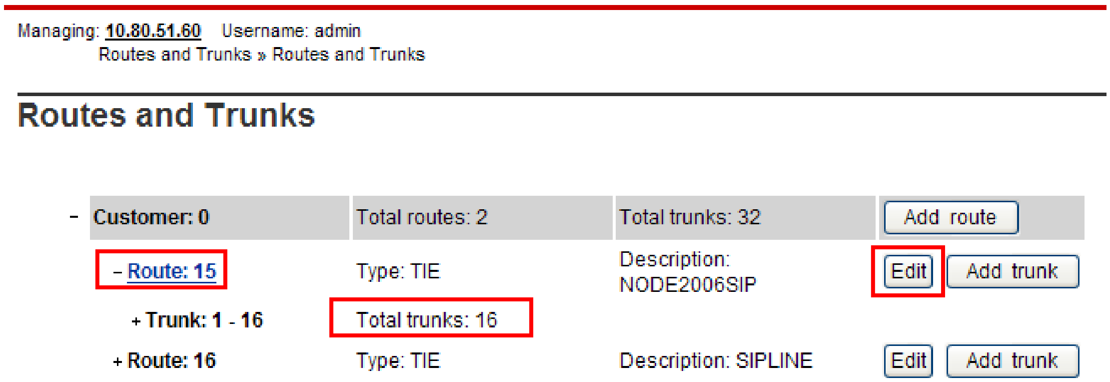
In the sample configuration, there is a single D-channel assigned to "**Channel: 15"** with "**Card Type: DCIP".** Specifying **"DCIP"** as the type of channel indicates the D-channel is a virtual D-channel.

3.2.2. Confirm Routes and Trunks Configuration

In addition to configuring a virtual D-channel, a **Route** and its associated **Trunks** need to be administered.

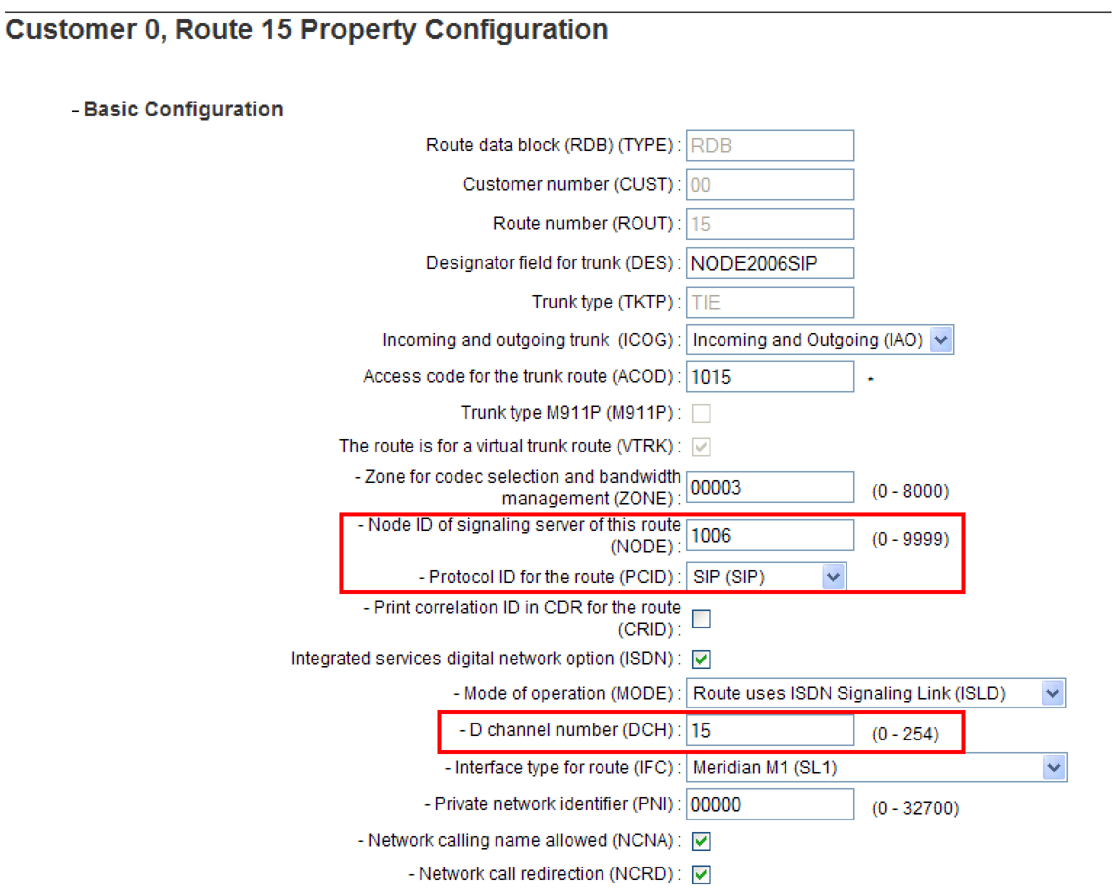
Expand **Routes and Trunks** on the left navigation panel and select **Routes and Trunks** (not shown) to verify a route with enough trunks to handle the expect number of simultaneous calls has been configured.

As shown in the screen below, “**Route 15”** has been configured with 16 trunks which indicates the system can handle 16 simultaneous calls.



Select **Edit** to verify the configuration.

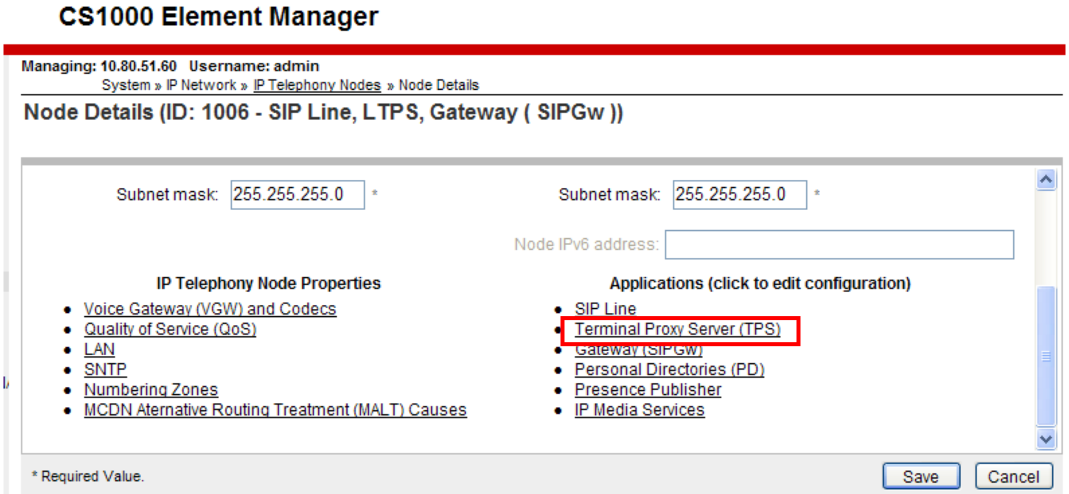
The details of the virtual Route defined for sample configuration is shown below. Verify “**SIP (SIP)”** has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** and **D channel number (DCH)** fields match the values identified in the previous section.



3.3. Configure SIP Trunk to Avaya Aura® Session Manager

Expand **System → IP Network → Nodes: Servers, Media Cards**.
Click "**1006**" in the **Node ID** column (not shown) to edit configuration settings of node.

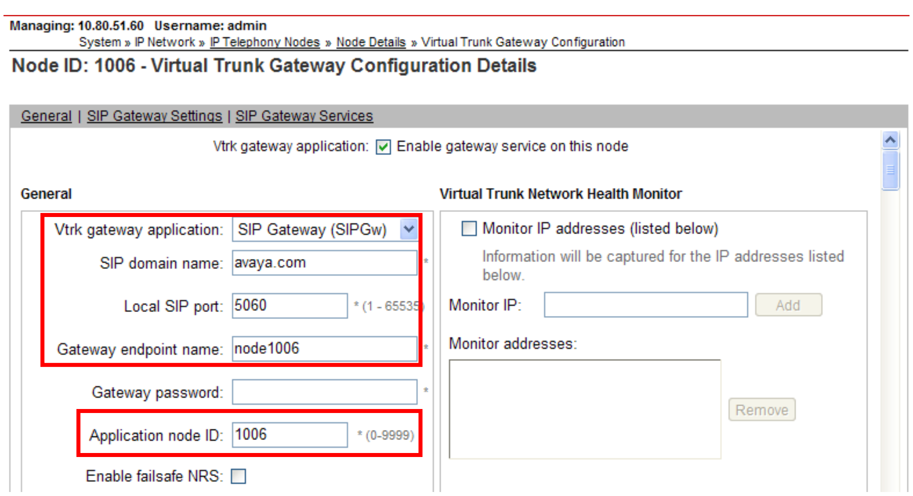
Using the scroll bar on the right side of the screen, navigate to the **Applications** section on the screen and select the **Gateway (SIPGw)** link as highlighted below.



On the **Node ID: 1006 - Virtual Trunk Gateway Configuration Details** page, enter the following values and use default values for remaining fields**.**

- **SIP domain name:** Enter name of domain. In the sample configuration, "**avaya.com**" was used.
- **Local SIP port:** Enter "**5060**"
- **Gateway endpoint name:** Enter descriptive name
- **Application node ID:** Enter "**<Node id>**". In the sample configuration, "**1006**" was used.

The values defined for the sample configuration are shown below.

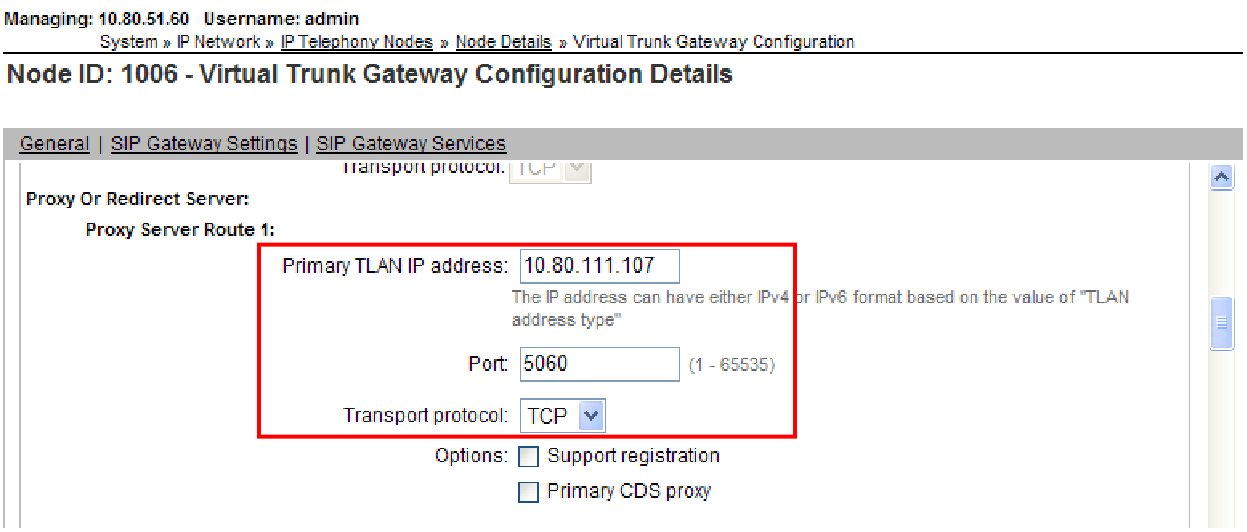


Scroll down to **SIP Gateway Settings → Proxy or Redirect Server**: section of the page.

Under **Proxy Server Route 1:** section, enter the following values and use default values for remaining fields**.**

- **Primary TLAN IP address:** Enter IP address of the Session Manager SIP signaling interface
- **Port:** Enter "**5060**"
- **Transport protocol:** Select "**TCP**"
  Note: TCP was used for the sample configuration. However, TLS would typically be used in production environments.

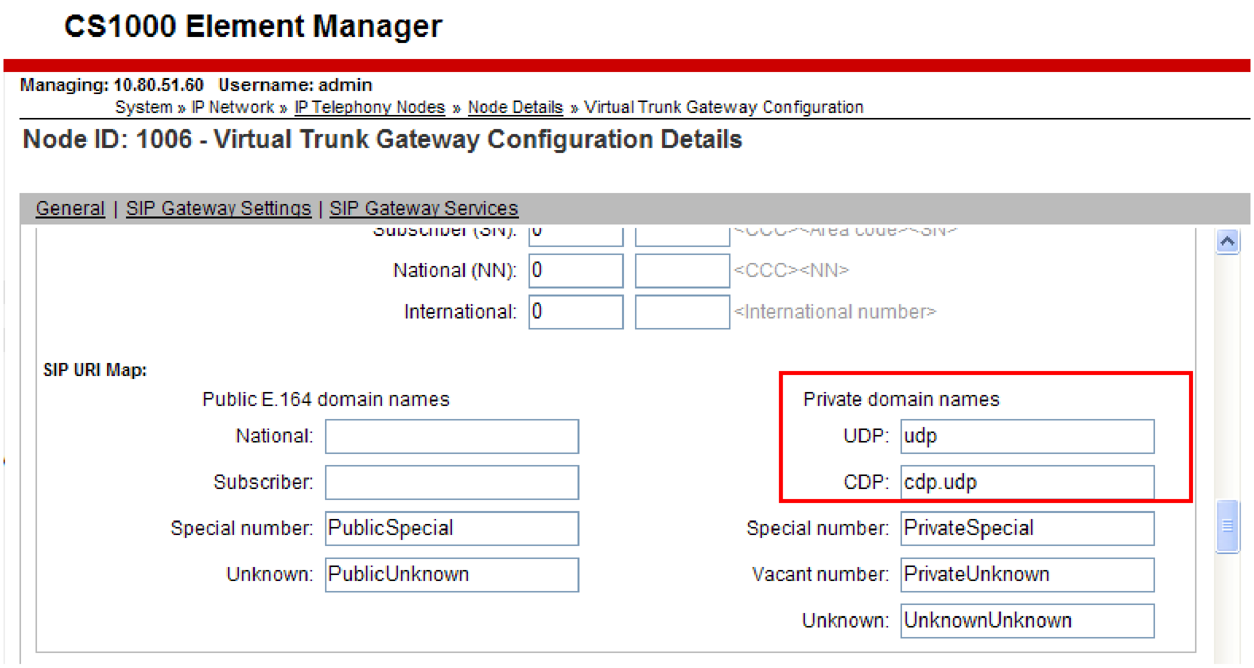
The values defined for the sample configuration are shown below.



Repeat these steps for the **Proxy Server Route 2** section (not shown).

Scroll down to the **SIP URI Map** section of the page and enter the appropriate names for the **UDP** and **CDP Private domain names** fields.

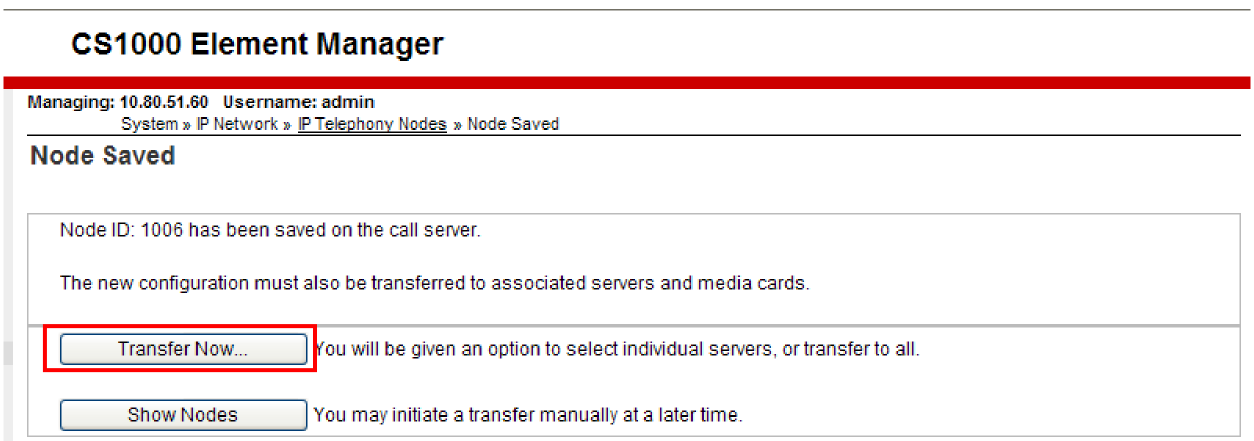
The values defined for the sample configuration are shown below.



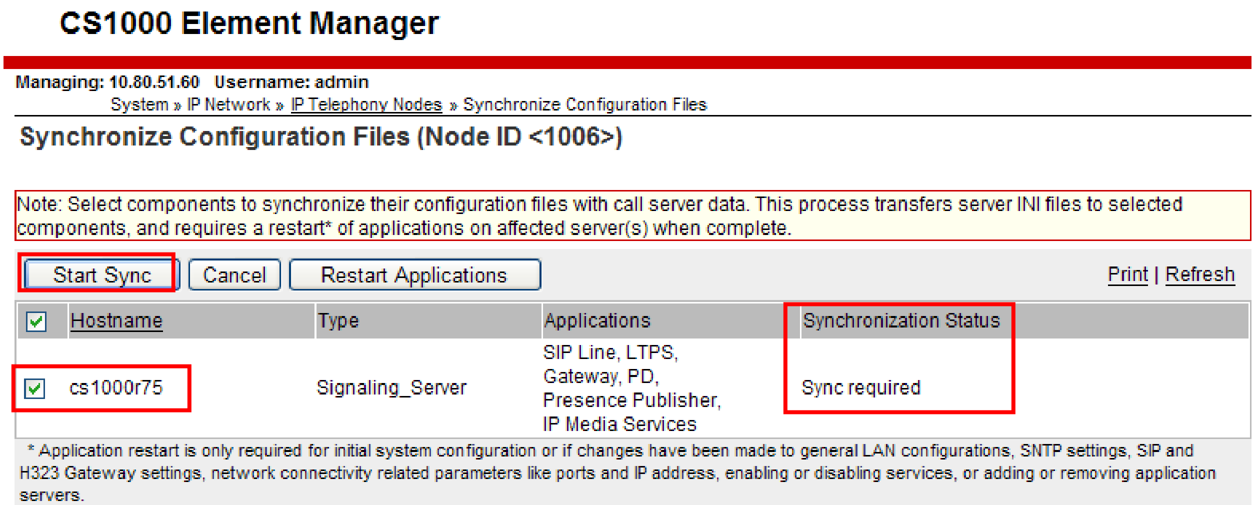
Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings.

Click **Save** on the **Node Details** screen (not shown).

Select **Transfer Now** on the **Node Saved** page as shown below.



Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.



Enter ☑ associated with the appropriate Call Server and click **Start Sync.** The screen will automatically refresh until the synchronization is finished. The **Synchronization Status** field will update from **Sync required** (as shown) to **Synchronized** (not shown).

After synchronization completes, click **Restart Applications** to use new SIP Gateway settings.

3.4. Configure Route List Index and Distant Steering Code

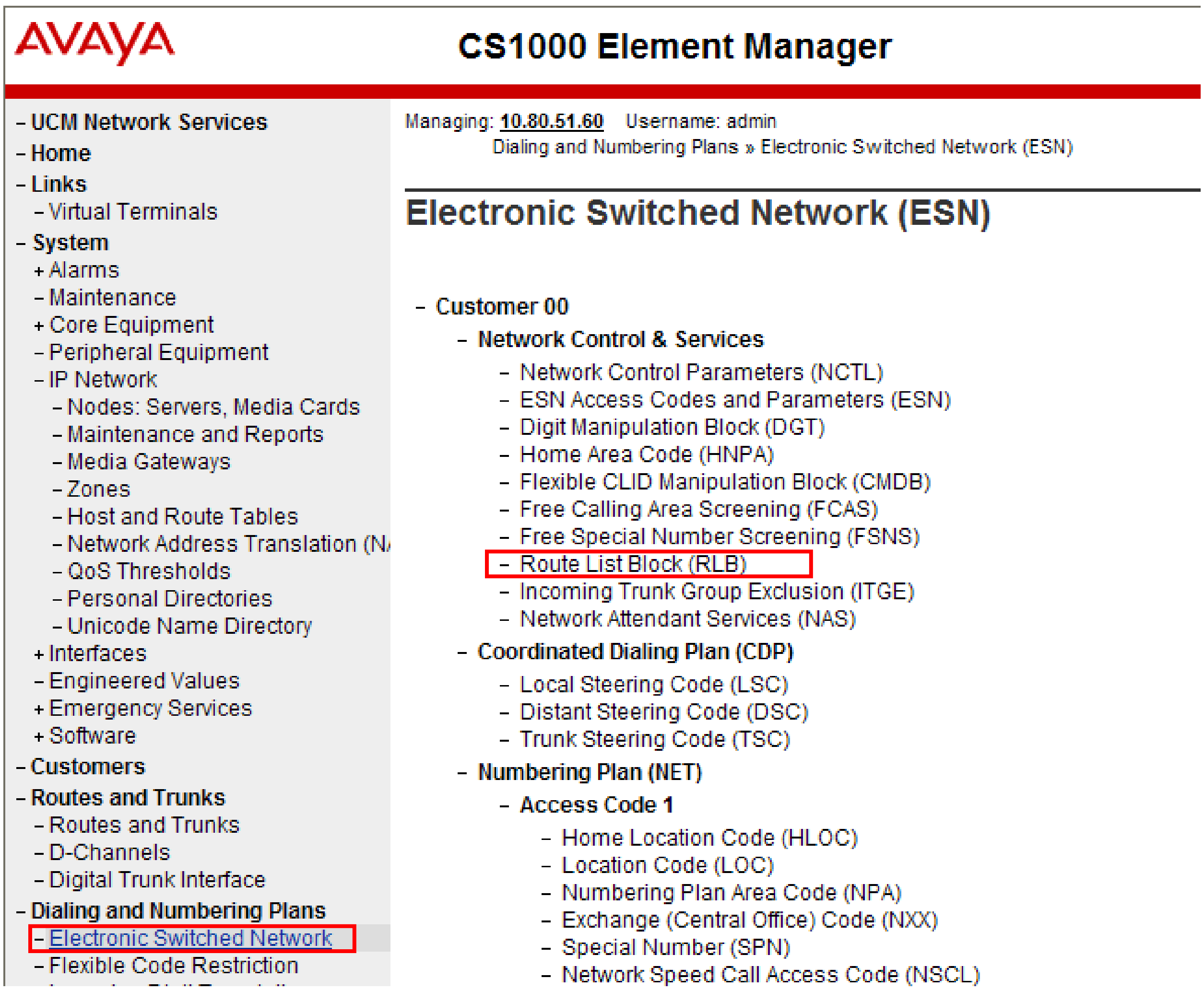
This section provides the configuration of the routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server and Session Manager.

Note: The routing rule defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

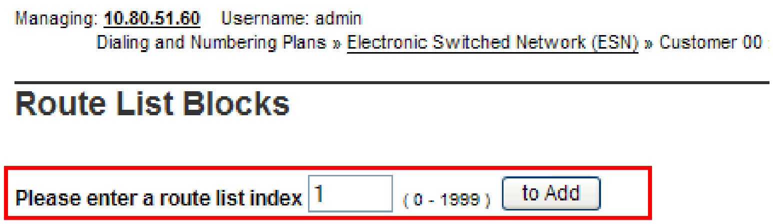
Step 1: Create Route List Index

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network.**

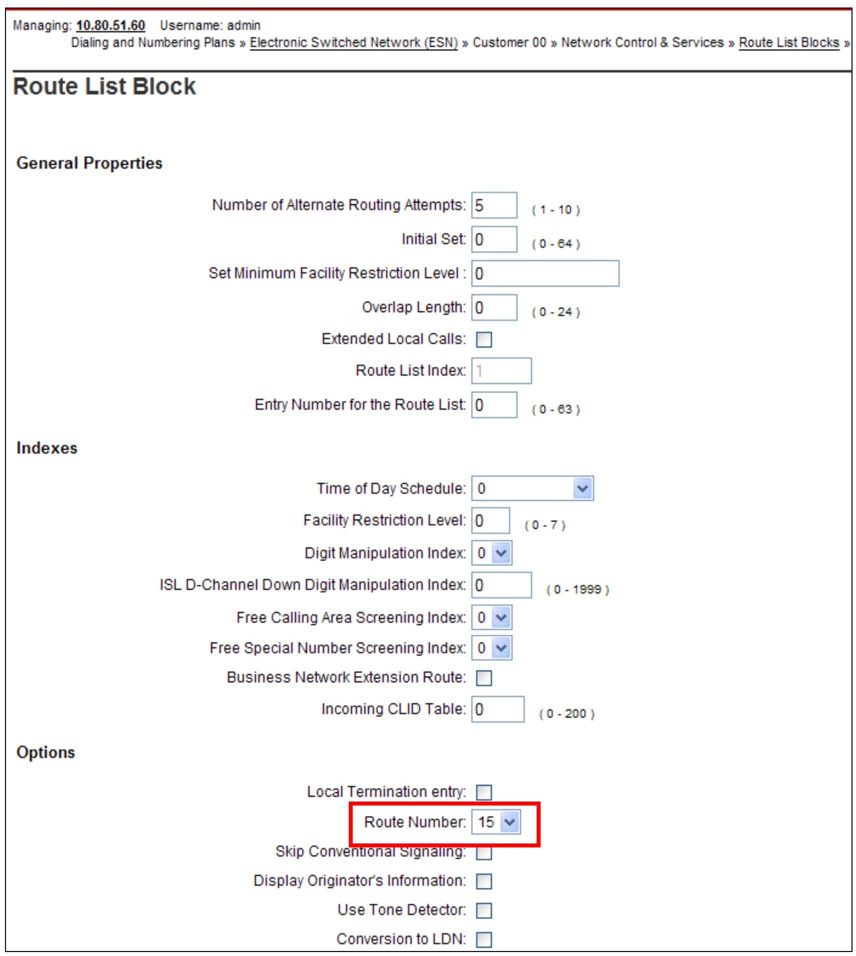
Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown below.



The **Route List Blocks** screen is displayed. Enter an available route list index number in the **Please enter a route list index** field and click **to Add** as shown below.



Under the **Options** section, select **“<Route id>”** of the route identified in **Section 3.2.2** in the **Route Number** field and use default values for remaining fields as shown below.

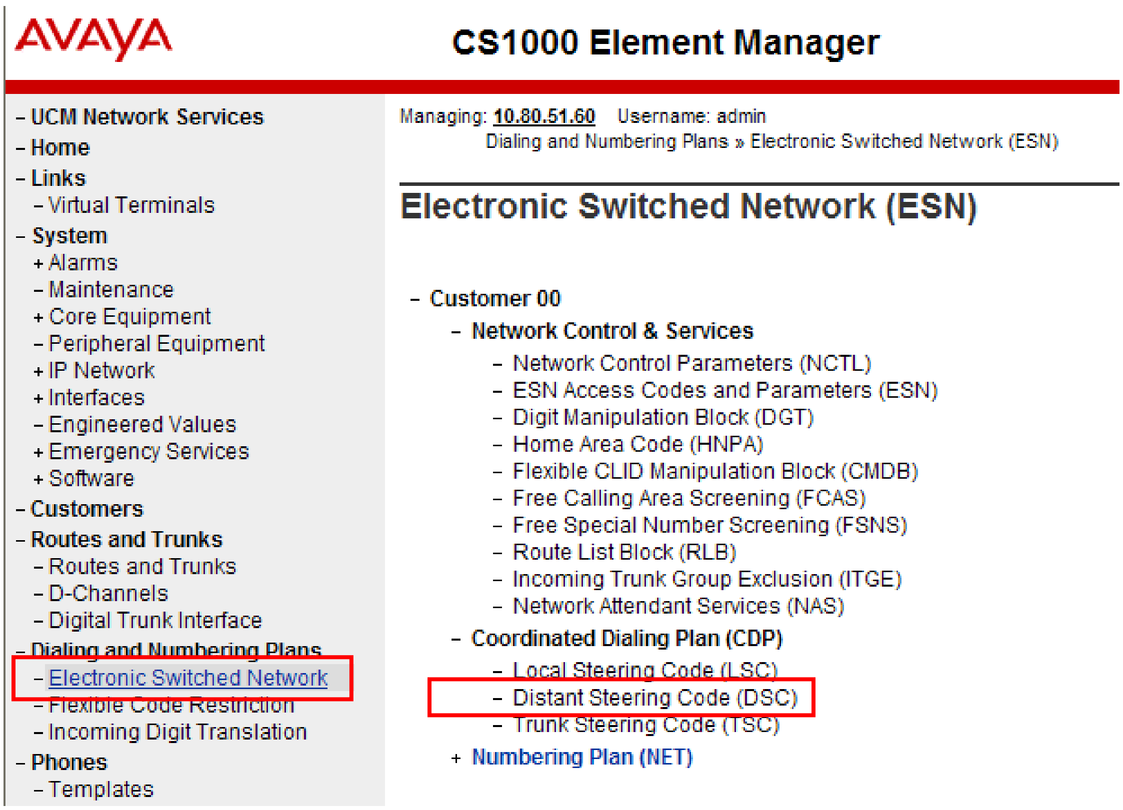


Click **Save** (not shown) to save new Route List Block definition.

Step 2: Create Distant Steering Code

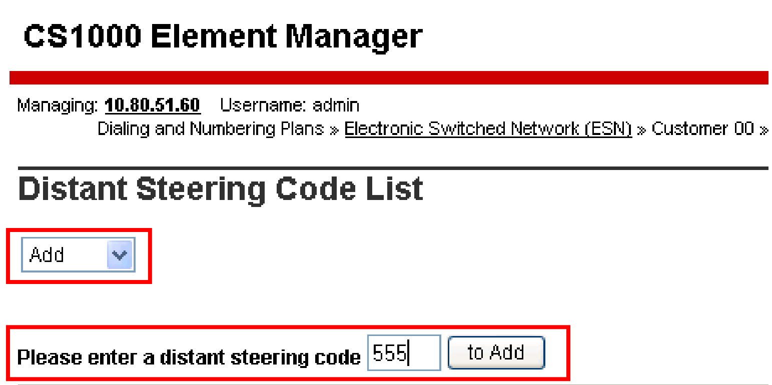
Expand **Dialing and Numbering Plans** on the left and select **Electronic Switched Network.**

Select **Distant Steering Code (DSC)** under the **Coordinated Dialing Plan (CDP)** section on the **Electronic Switched Network (ESN)** page as shown below.



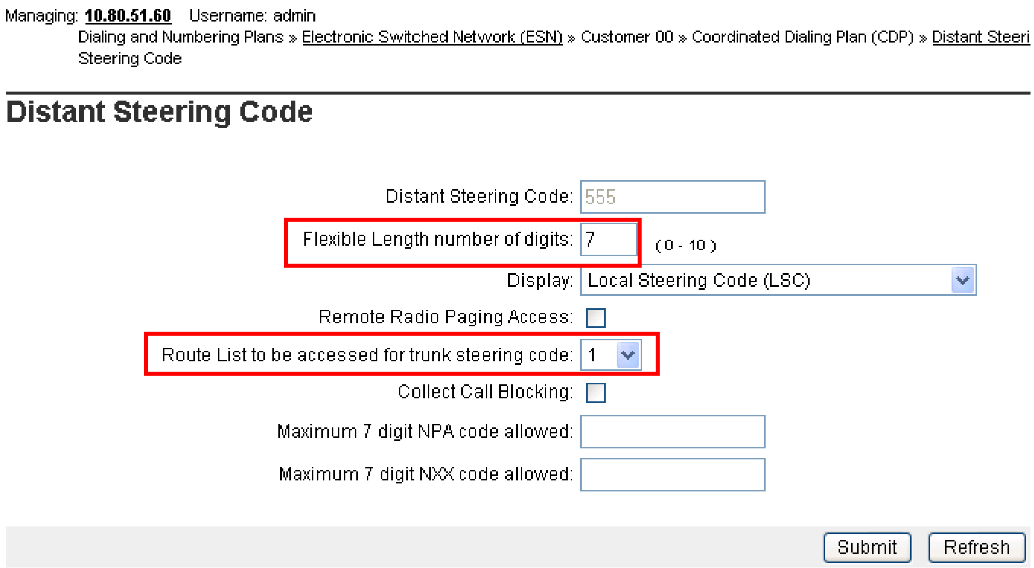
Select "**Add"** from the drop-down menu and enter the dialed prefix for external calls to be routed over SIP trunk to Session Manager in the **Please enter a distant steering code** field.

For the sample configuration, "**555**" was used since SIP endpoints registered to Session Manager were assigned extensions starting with "**555**". Click **to Add** as shown below.



Enter the following values and use default values for remaining fields.

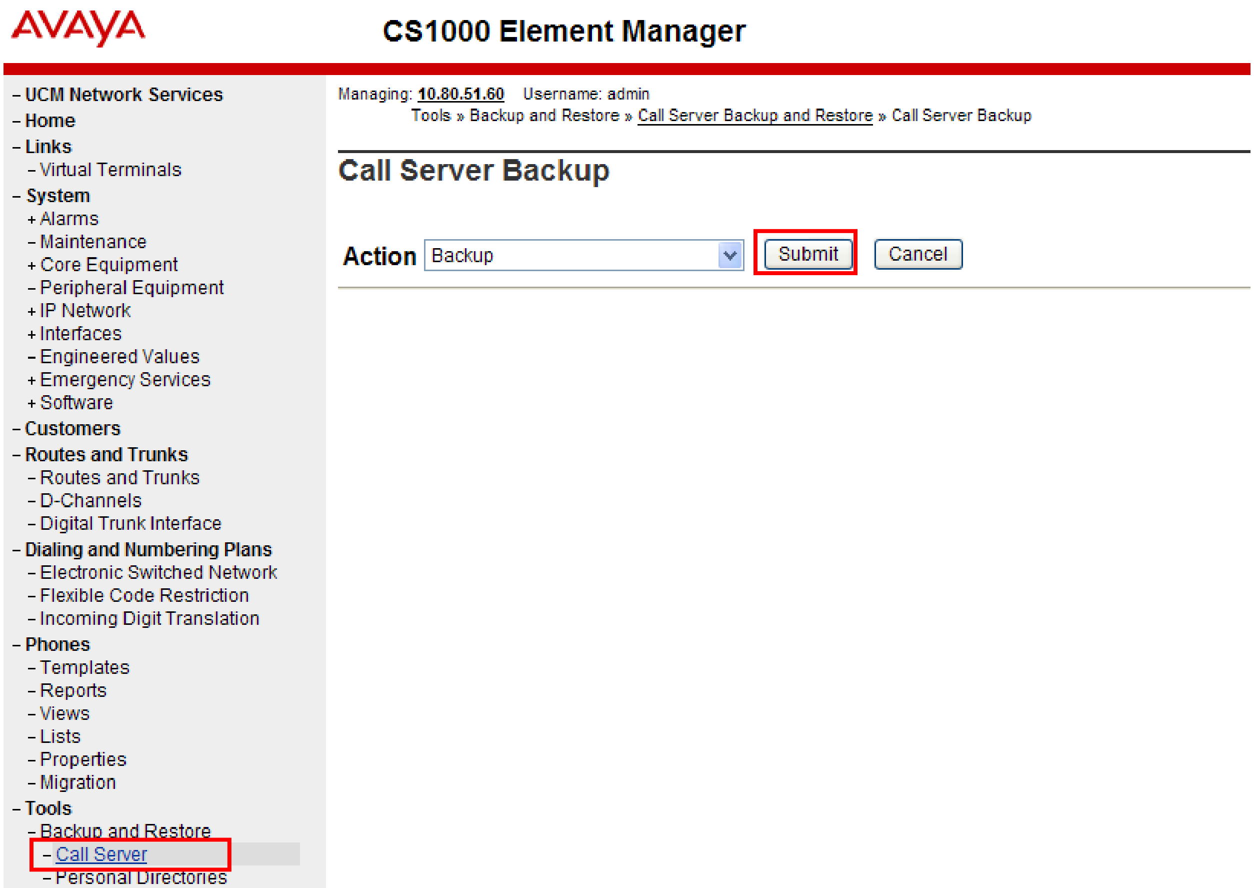
- **Flexible Length number of digits:** Enter number of digits in dialed numbers. In the sample configuration, **“7”** was used.
- **Route List to be accessed for trunk steering code:** Select **“<id>”** of Route List Index created in **Step 1**.



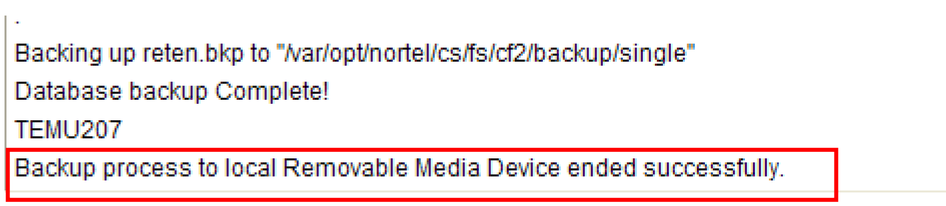
Click **Submit** to save new Distant Steering Code definition

3.5. Save Configuration

Expand **Tools → Backup and Restore** on the left navigation panel and select **Call Server.** Select **Backup** (not shown) and click **Submit** to save configuration changes as shown below.



Backup process will take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.



Configuration of Avaya Communication Server 1000E is complete.

4. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager to route calls between Avaya Communication Server 1000E and Cisco Unified Communications Manager.

The following administration activities will be described:

- Define SIP Domains for **avaya.com** and **cucm.com**
- Define locations for the different subnets
- Configure an Adaptation Module designed for Cisco UCM to resolve SIP protocol differences between Cisco UCM and Avaya Communication Server 1000E
- Configure an Adaptation Module for the CS1000E.
- Define SIP Entities corresponding to each SIP telephony system and Session Manager.
- Define Entity Links, which describe 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.

In addition to the steps described in this section, other administration activities will be needed such a defining the network connection between System Manager and Session Manager. For more information on these additional actions, see **References [2]** through **[5]** in **Section 9.** Some administration screens have been abbreviated for clarity

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL "**http://<ip-address>/SMGR**", where <ip-address> is the IP address of Avaya Aura® System Manager. Login with the appropriate credentials.

4.1. Define SIP Domains

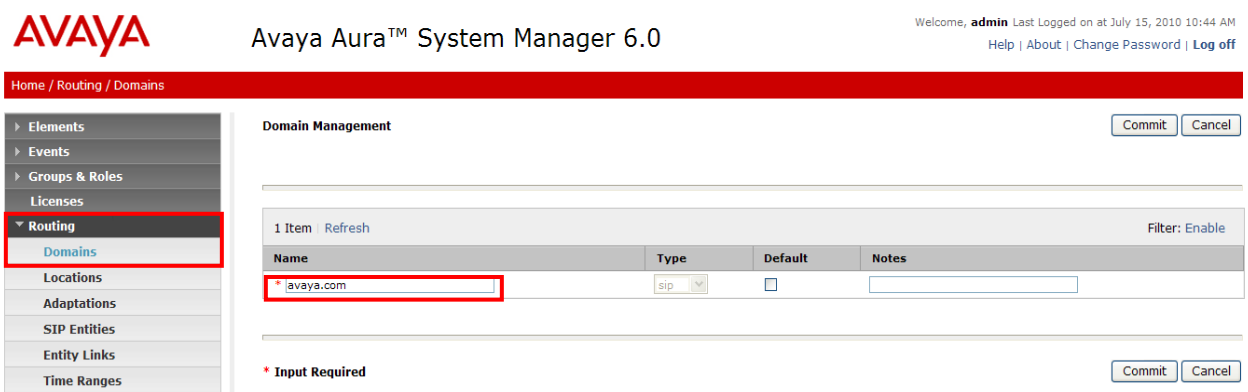
Expand **Routing** and select **Domains** from the left navigation menu.

Click **New** (not shown)**.** Enter the following values and use default values for remaining fields**.**

- **Name** Enter the Authoritative Domain Name specified in **Section 3.1.** In the sample configuration, "**avaya.com**" and "**cucm.com**" were used.
- **Type** Verify "**SIP**" is selected.
- **Notes** Add a brief description. [Optional]

Repeat these same steps for the SIP domain **cucm.com** as well.

Click **Commit** to save. The screen below shows the SIP Domain defined for the avaya.com domain.



4.2. Define Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

Expand **Elements → Routing** and select **Locations** from the left navigational menu.

Click **New** (not shown)**.** In the **General** section**,** enter the following values and use default values for remaining fields**.**

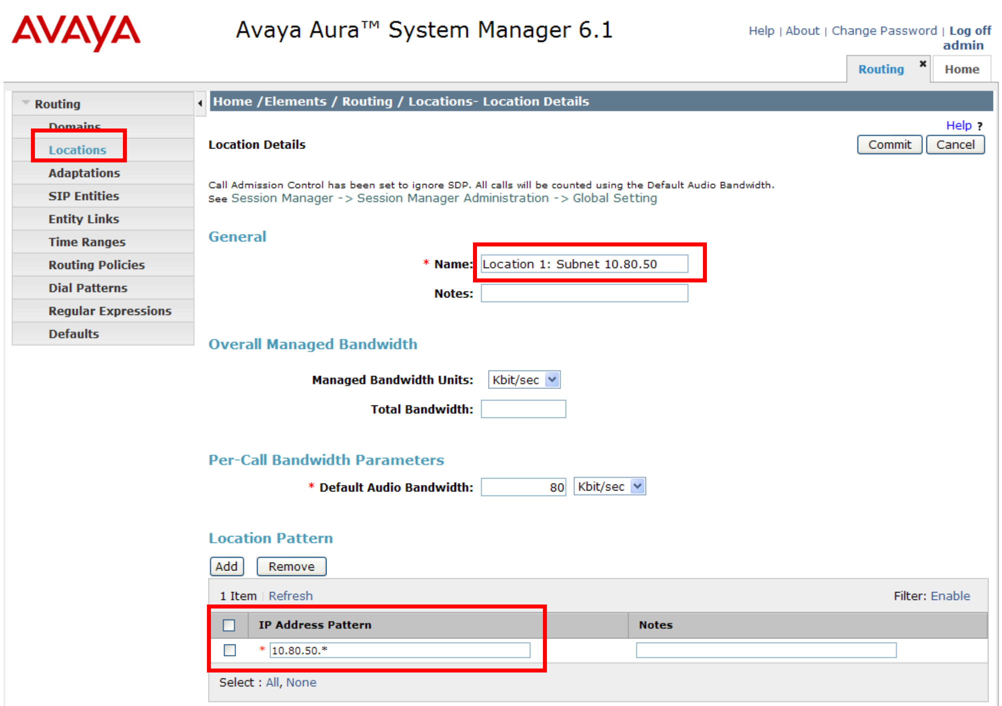
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

In the **Location Pattern** section, click **Add** and enter the following values.

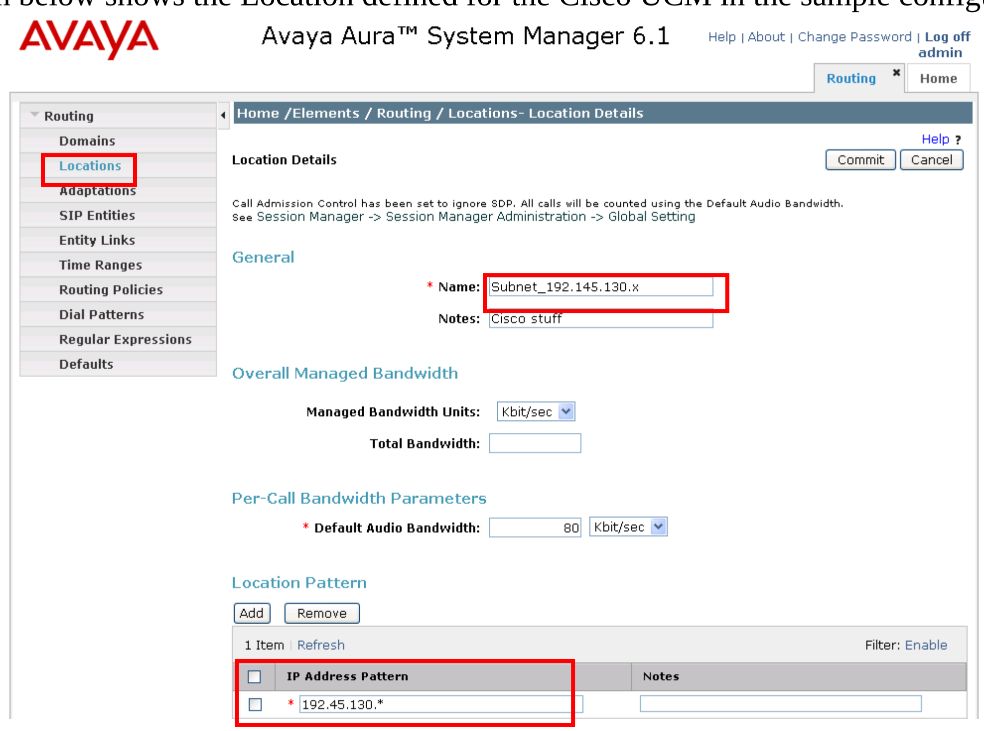
- **IP Address Pattern** Enter the logical pattern used to identify the location. For the sample configuration, "**10.80.50.***" was used.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows the Location defined for Avaya Communication Server 1000E in the sample configuration.



The screen below shows the Location defined for the Cisco UCM in the sample configuration



4.3. Configure Adaptation Modules

To enable calls between stations on Avaya Communication Server 1000E and Cisco Unified Communications Manager, Session Manager should be configured to use an Adaptation Module designed for Cisco Unified Communications Manager and one for the CS1000E which resolve SIP protocol differences between the two telephony systems.

The Cisco Adapter provides two basic header manipulations: converting between Diversion and History-Info headers and converting between P-Asserted-Id and Remote-Party-Id headers. The Diversion and Remote-Party-Id headers have not been accepted by the IETF. They are replaced by History-Info and P-Asserted-Identity respectively, but are still used in the Cisco products. The Cisco Adapter also performs all the conversions available by the Digit Conversion Adapter

4.3.1. Create an Adaptation Module for Cisco UCM

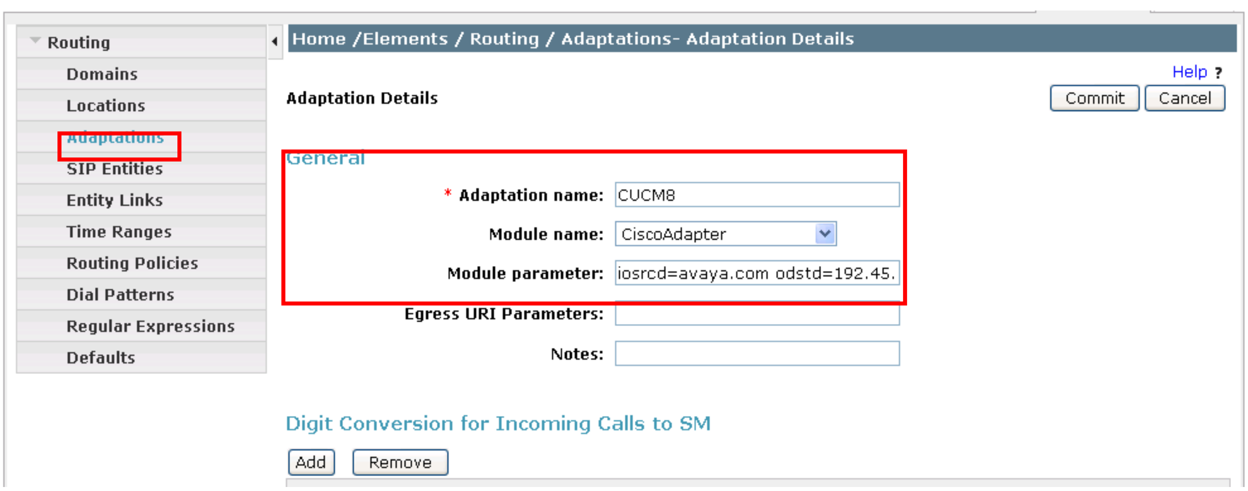
Expand **Routing** and select **Adaptations** from the navigational menu on left side of the page. Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Adaptation Name:** Enter an identifier for the Adaptation Module
- **Module Name:** Select "**CiscoAdapter**" from drop-down menu
- **Module parameter**: Enter **"iosrcd=avaya.com"**the domain defined in **Section 4.1**.
  Enter **"odstd=192.45.130.100"** which is the IP address for Cisco UCM system.

Note: *iosrcd* is the abbreviation for **Ingress Override Source Domain** parameter and *odstd* is the abbreviation for **Override Destination Domain** parameter. For more information on use of module parameters, see **Reference [5]** in **Section 9**.

- **Notes:** Enter a brief description. [Optional]

Click **Commit** to save. The screen below shows the Adaptation Module specified for the sample configuration. **Note:** Digit conversion was not required for sample configuration.



4.3.2. Create an Adaptation for Communication Server 1000E

To enable calls between stations on Avaya Communication Server 1000E and other SIP entities registered to Session Manager, Session Manager should be configured to use an Adaptation Module designed for Avaya Communication Server 1000E. This adaptation module takes over much of the functionality of the CS1000E's Network Routing Service (NRS).

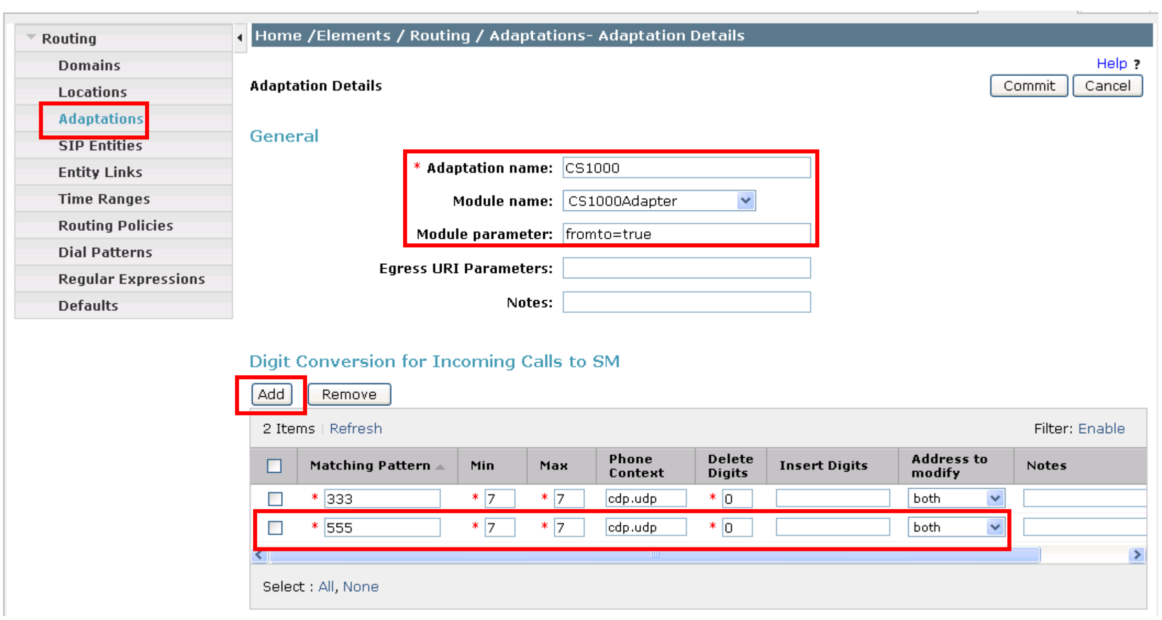
Expand **Elements → Routing** and select **Adaptations** from the left navigational menu. Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Adaptation Name:** Enter an identifier for the Adaptation Module
- **Module Name:** Select "**CS1000Adapter**" from drop-down menu
- **Module Parameter** Enter **"fromto=true.** This will modify the FROM and TO headers in the SIP messages.

In the **Digit Conversion for Incoming Calls to SM** section, click **Add** and enter the following values.

- **Matching Pattern** Enter dialed prefix for calls to SIP endpoints registered to Session Manager. In sample configuration, "**555**" was used *(As shown below "**333**" is not used for the sample config)*
- **Min** Enter minimum number of digits that must be dialed
- **Max** Enter maximum number of digits that may be dialed In the sample configuration, "**7**" was used.
- **Phone Context** Enter value of **Private CDP domain name** defined in **Section 3.3.**
- **Delete Digits** Enter "**0**", unless digits should be removed from dialed number before call is routed by Session Manager
- **Address to modify** Select **"both"**

Click **Commit.** The Adaptation Module defined for sample configuration is shown below.



4.4. Define SIP Entities

A SIP Entity must be added for each telephony system connected to Session Manager over SIP trunk.

Expand **Elements → Routing** and select **SIP Entities** from the left navigation menu.

Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

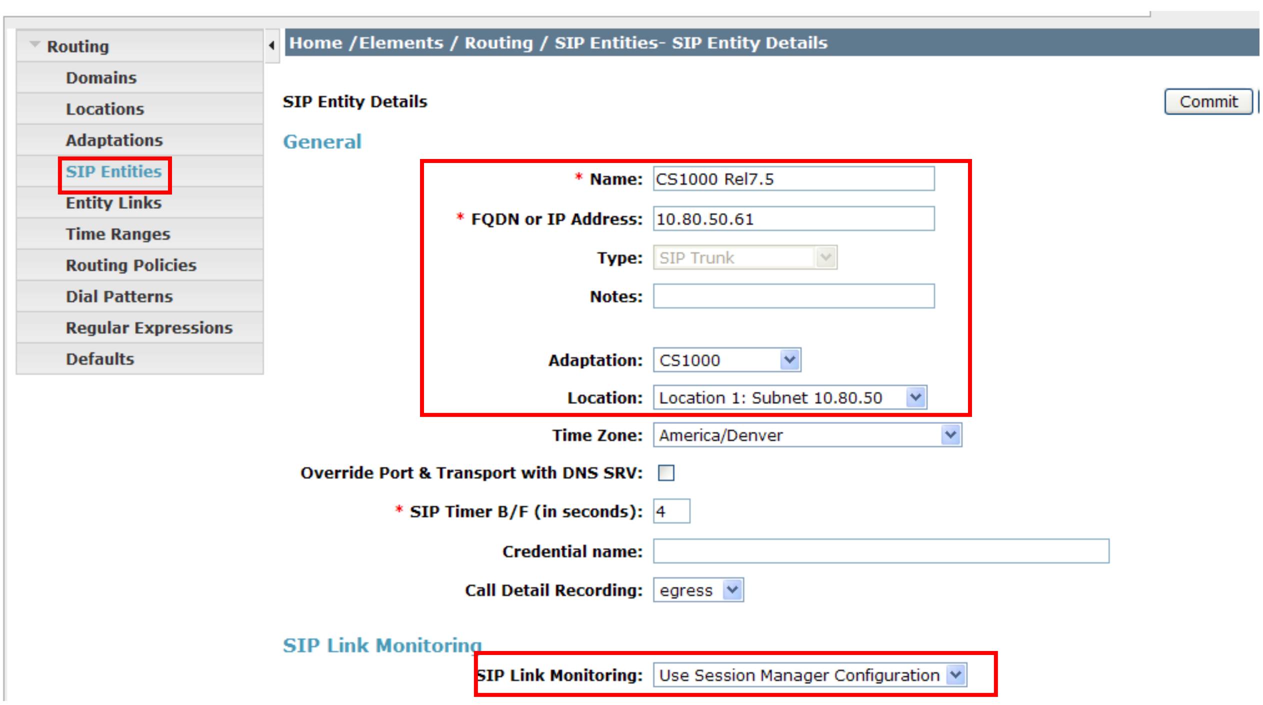
- **Name:** Enter an identifier for the SIP Entity
- **FQDN or IP Address:** Enter TLAN IP address of Avaya Communication Server 1000E Node identified in **Section 3.2**
- **Type:** Select "**SIP Trunk**"
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the Adaptation Module defined in **Section 4.3**
- **Location:** Select the Location defined for Avaya Communication Server 1000E in **Section 4.2**

In the **SIP Link Monitoring** section:

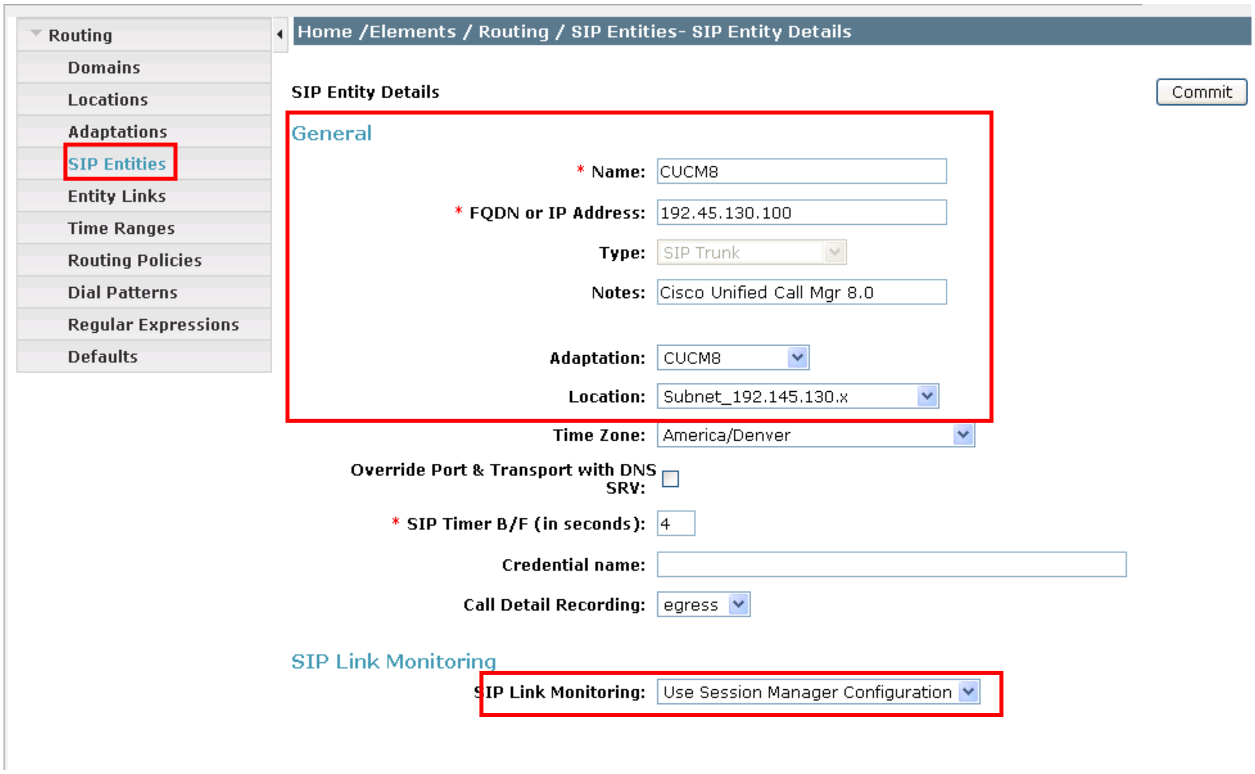
- **SIP Link Monitoring:** Select "**Use Session Manager Configuration**"

Click **Commit** to save the definition of the new SIP Entity.

The following screen shows the SIP Entity defined for Avaya Communication Server 1000E in the sample configuration.



The following screen shows the SIP Entity defined for Cisco Unified Communications Manager.



4.5. Define Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. In the sample configuration, SIP Entity Links were added between Session Manager and each telephony system.

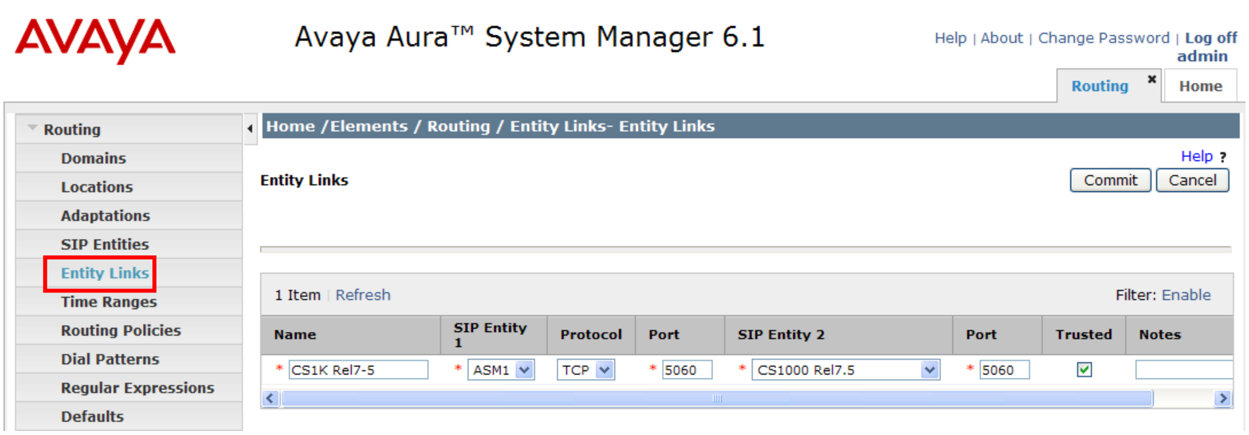
Expand **Elements → Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

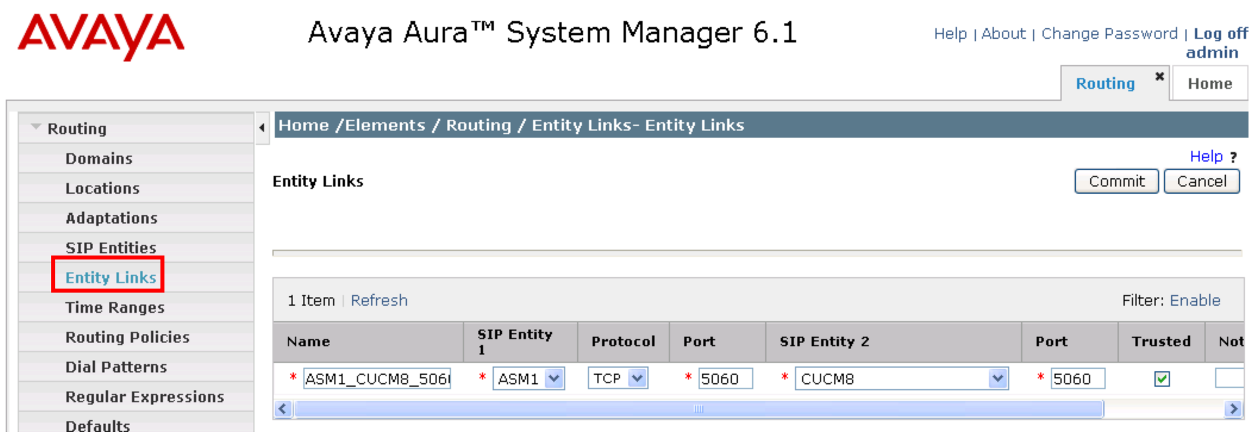
- **Name** Enter an identifier for the link to each telephony system.
- **SIP Entity 1** Select SIP Entity defined for Session Manager
- **SIP Entity 2** Select the SIP Entity defined for Avaya Communication Server 1000E in **Section 4.4**
- **Protocol** After selecting both SIP Entities, select "**TCP"** as the required protocol.
- **Port** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is "**5060**".
- **Trusted** Enter
- **Notes** Enter a brief description. [Optional]

Click **Commit** to save **Entity Link** definition.

The following screen shows the entity link defined for the SIP trunk between Session Manager and Avaya Communication Server 1000E.



The following screen shows the entity link defined for the SIP trunk between Session Manager and Cisco Unified Communications Manager.



4.6. Define Routing Policy

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 4.3.** Two routing policies must be added, one for Avaya Communication Server 1000E and one for Cisco Unified Communications Manager.

To add a routing policy, Expand **Elements → Routing** and select **Routing Policies.**

Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional]

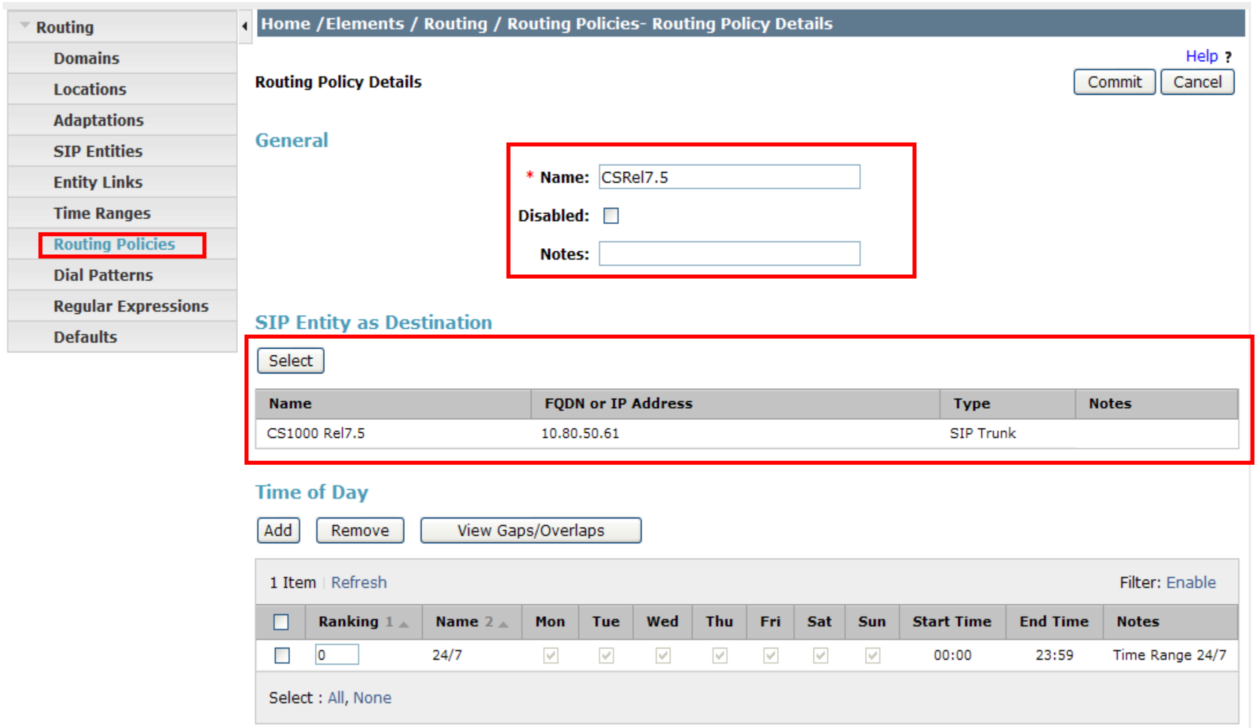
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with Avaya Communication Server 1000E defined in **Section 4.4** and click **Select.**
- The selected SIP Entity displays on the **Routing Policy Details** page.

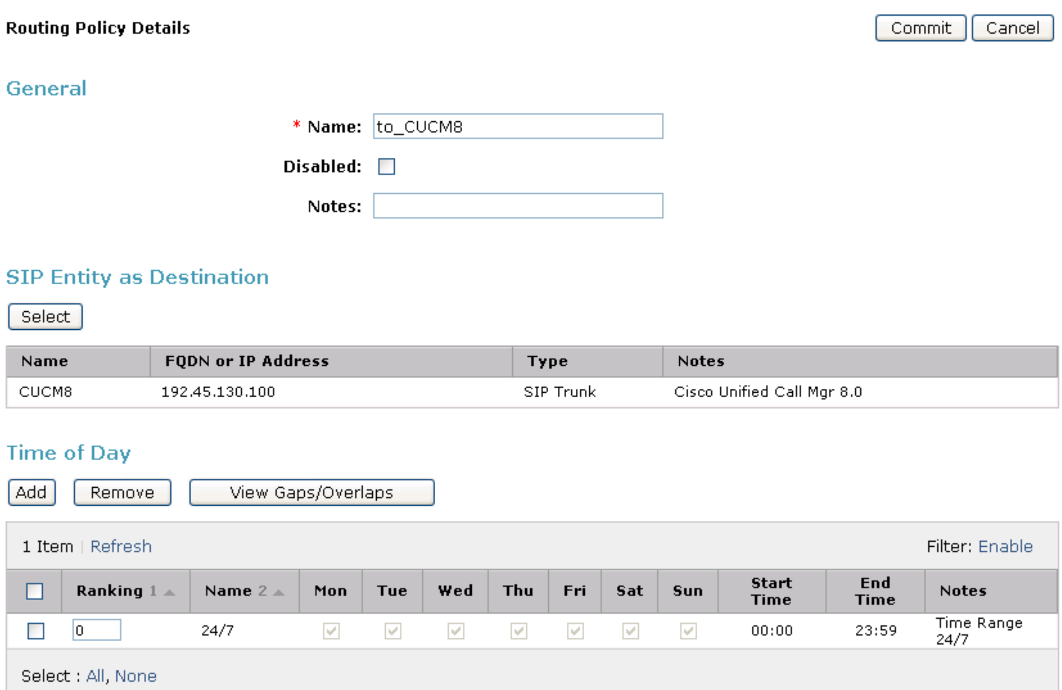
Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

Note: The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

The following screen shows the Routing Policy for Avaya Communication Server 1000E.



The following screen shows the routing policy defined for routing calls to the Cisco Unified Communications Manager.



4.7. Define Dial Pattern

Define dial patterns to direct calls to the appropriate telephony system. In the sample configuration, 7-digit extensions beginning with "**778**" reside on Communication Server 1000E and 7-digit extensions beginning with "**5558**" reside on Cisco Unified Communications Manager.

To define a dial pattern, expand **Routing** and select **Dial Patterns** (not shown).

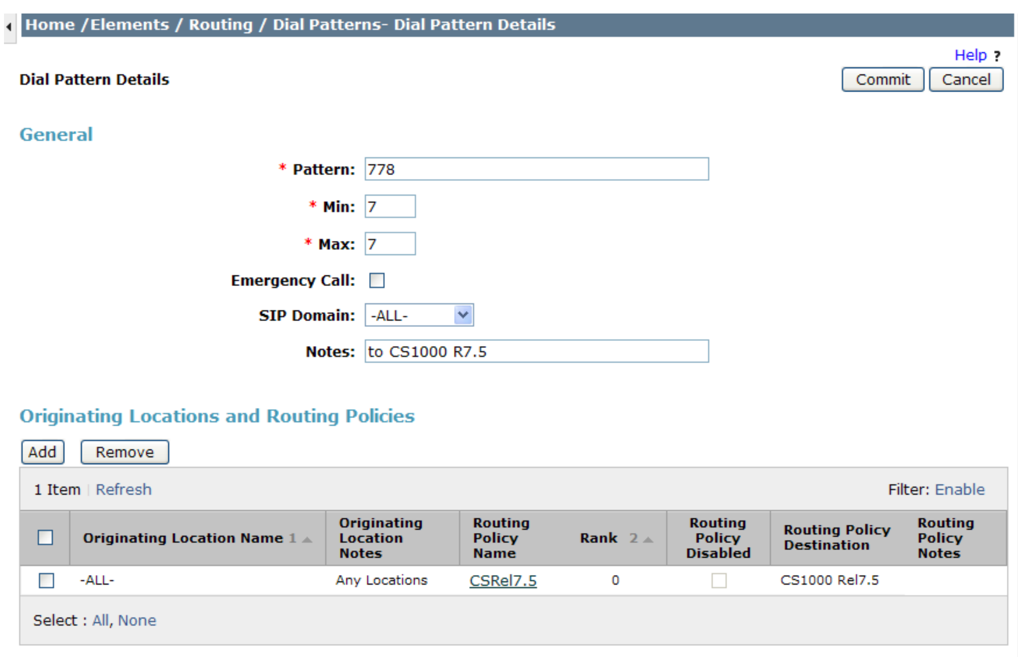
Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to Avaya Communication Server 1000E
- **Min:** Enter the minimum number digits that must to be dialed.
- **Max:** Enter the maximum number digits that may be dialed.
- **SIP Domain:** Select the SIP Domain from drop-down menu or select **"All"** if Session Manager should accept incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

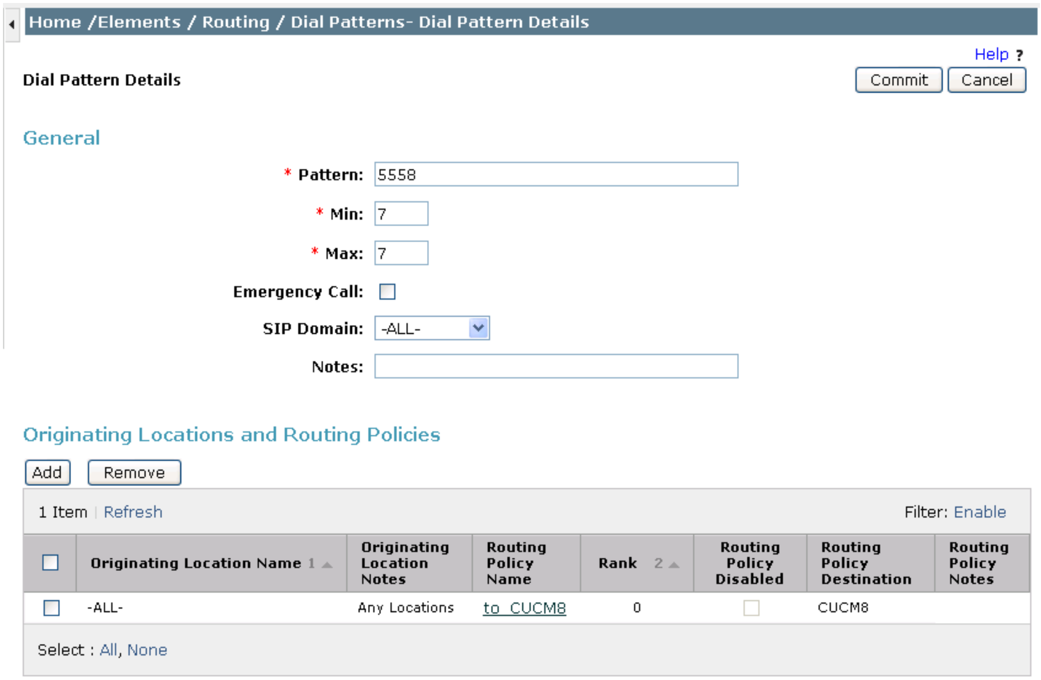
In the **Originating Locations and Routing Policies** section, click **Add.**
The **Originating Locations and Routing Policy List** page opens (not shown).

- In **Originating Locations** table, select "**ALL**"
- In **Routing Policies** table, select the Routing Policy defined for Avaya Communication Server 1000E in **Section 4.6.**
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save. The following screen shows the Dial Pattern defined for sample configuration.



The following screen shows the Dial Pattern defined for routing calls to Cisco UCM.



5. Configure Cisco Unified Communications Manager

This section describes the relevant configuration of the SIP Trunk and call routing between the Cisco Unified Communications Manager (UCM) and Session Manager.

The following administration activities will be described:

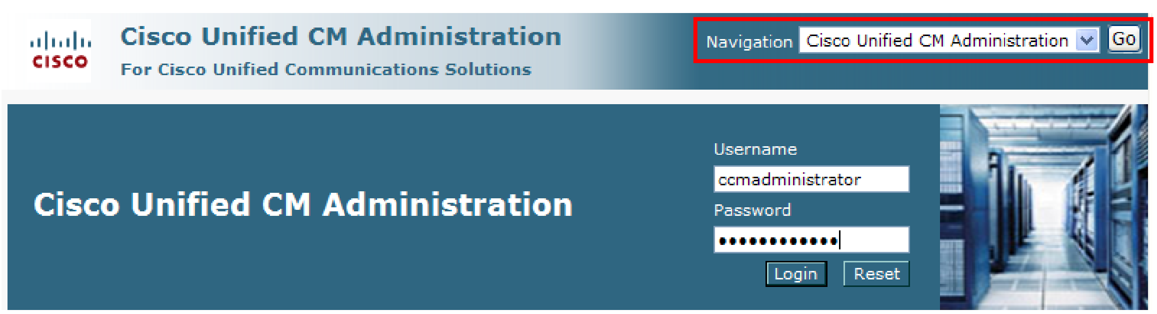
- Verify Audio Codec Configuration
- Configure Media Resources
- Configure Default Device Pool
- Configure SIP Trunk Security Profile
- Define Avaya SIP Profile
- Define SIP Trunk
- Define Routing Pattern

These instructions assume the basic configuration of the Cisco Unified Communications Manager has already been completed and the system is configured to support the SCCP (IP) and SIP telephones, including defining an external phone number mask so calls between Cisco stations and Communication Server 1000E stations use a 7-digit dialing plan starting with "5558xxx". For information on how to administer these other aspects of Cisco Unified Communications Manager, see the appropriate documentation in **Section 9.**

Note: Some administration screens have been abbreviated for clarity.

Cisco Unified Communications Manager is configured using Cisco Unified CM Administration GUI using the URL "**http://<IP Address>:8443/ccmadmin/showHome.do**" where **<ip-address>** is the IP address of Cisco Unified Communications Manager.

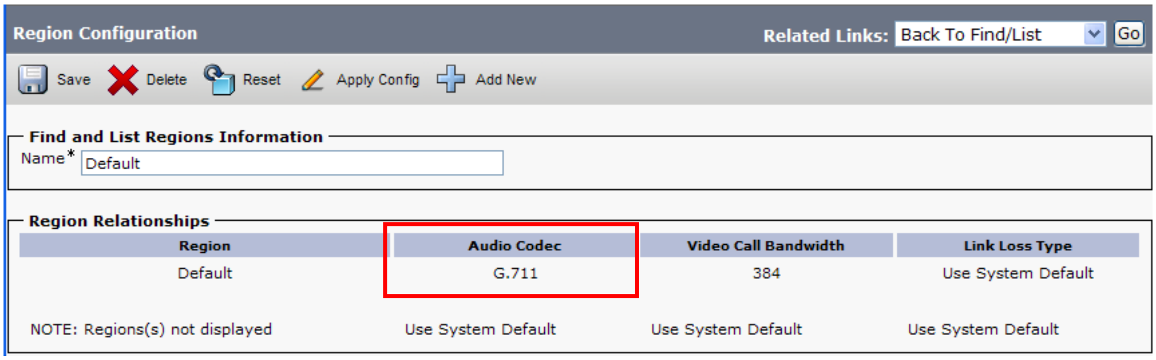
Select the "**Cisco Unified CM Administration"** application from the **Navigation** drop-down menu. Click **Go** and login with the appropriate credentials as shown below.



5.1. Configure Audio Codec

Expand **System** menu and select **Region.** Click **Find** (not shown) and select **Default** region.

Verify **Audio Codec** is set to **"G.711"** as shown below.



5.2. Configure Media Resources

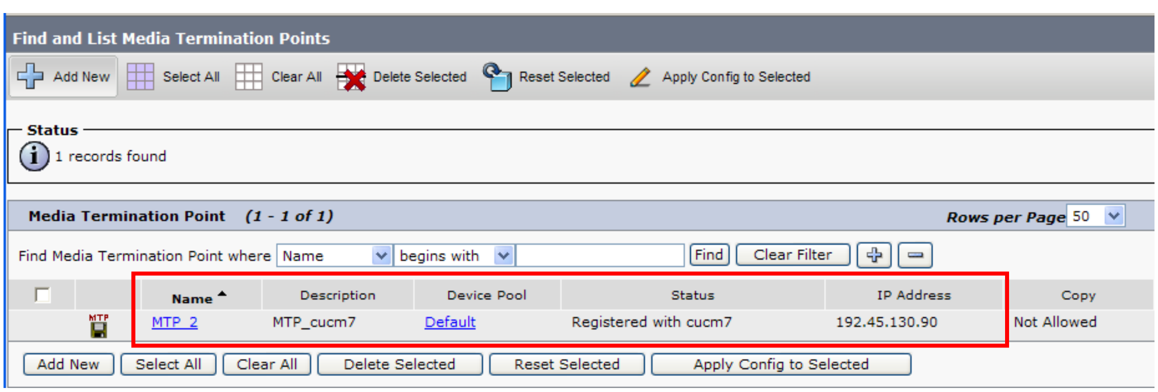
5.2.1. Configure Media Termination Point

Media Termination Points extend supplementary services, such as hold, transfer, call park, and conferencing that are otherwise not available when a call is routed to a SIP endpoint.

Expand **Media Resources** and select **Media Termination Point.** Click **Find** to list available Media Termination Points. Verify at least one media termination points has been defined and verify the following fields:

- **Device Pool** — "**Default**"
- **Status** — "**Registered with <name>**" where <name> is name of Cisco Unified Communications Manager system
- **IP address** — IP address of Cisco Unified Communications Manager system

In the sample configuration, the name of Cisco Unified Communications Manager system is "**cucm7**" and the default media termination point is "**MTP_2**" as shown below.



5.2.2. Add Media Resource Group

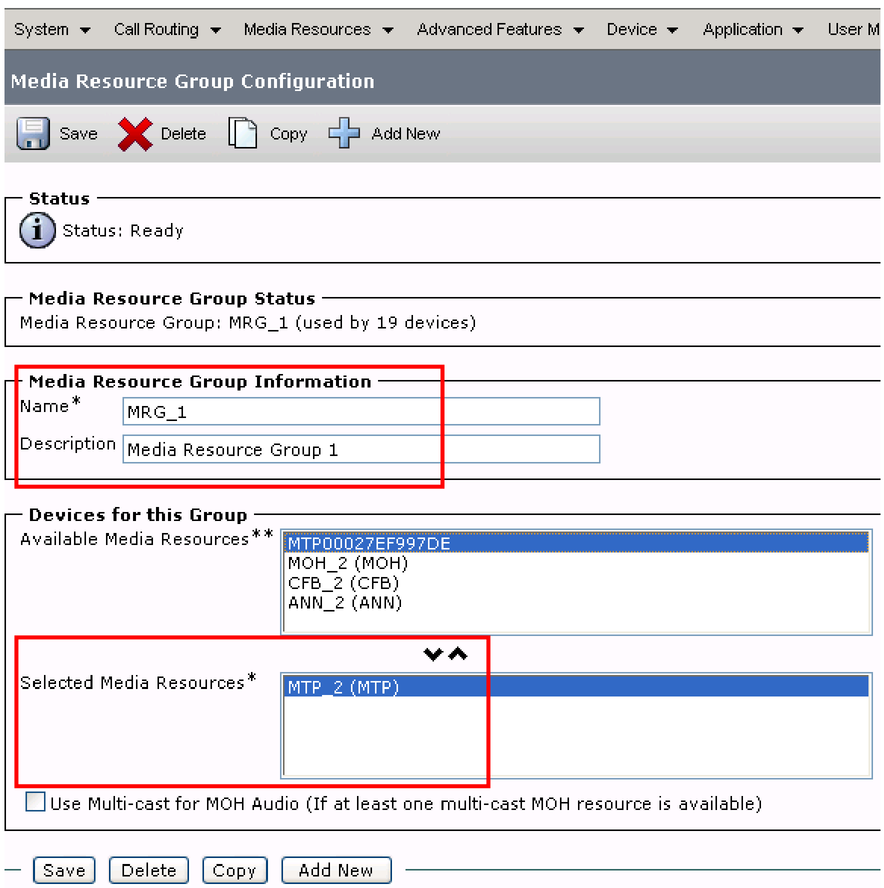
A Media Resource Group is used to group different types of media resources such as annunicators, media termination points, and conference bridges into a single group.

Expand **Media Resources** and select **Media Resource Group.** Click Add New to define a Media Resource Group. Enter the following values:

- **Name** Enter name of Resource Group.
  In the sample configuration, "**MRG_1**" was used.
- **Description** Enter brief description name

Under **Devices for this Group** section, select a set of media resources from the **Available Media Resources** table by using the ∨ (down arrow) to move the selected media resources to the **Selected Media Resources** table.

Click Save to save new group definition. The screen below shows the Media Resource Group defined for the sample configuration.



5.2.3. Add Media Resource Group List

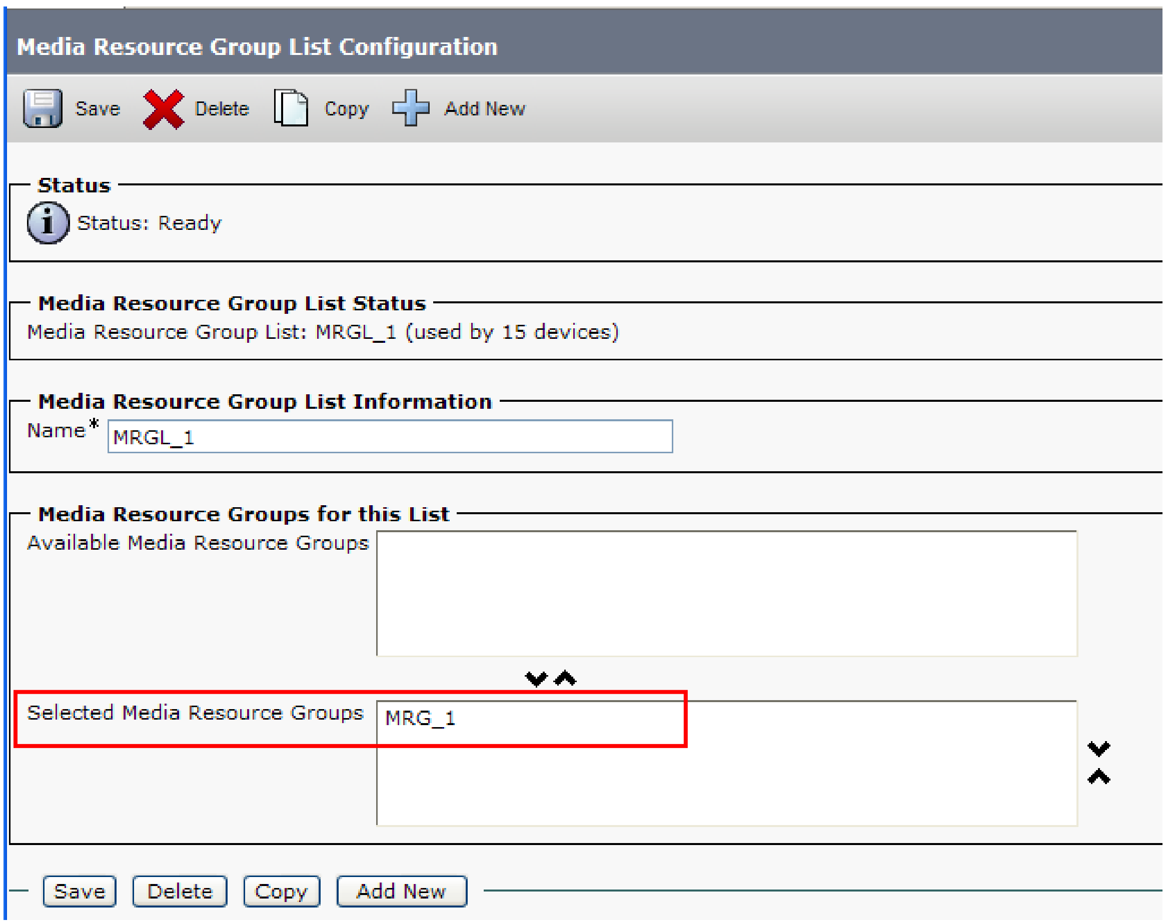
A Media Resource Group List is used to group different types of media resources such as annuncicators, media termination points, etc into a single group.

Expand **Media Resources** and select **Media Resource Group List.** Click Add New to define a Media Resource Group List. Enter the following values:

- **Name** Enter name of Resource Group List. In the sample configuration, "**MRGL_1**" was used.

Under **Media Resource Groups for this List** section, select the Media Resource Group defined in **Section 5.2.2** from the **Available Media Resource Groups** table by using the ⋎ (down arrow) to move the selected media resources to the **Selected Media Resource Groups** table.

Click Save to save new list. The screen below shows the Media Resource Group List defined for the sample configuration.



5.3. Configure Default Device Pool

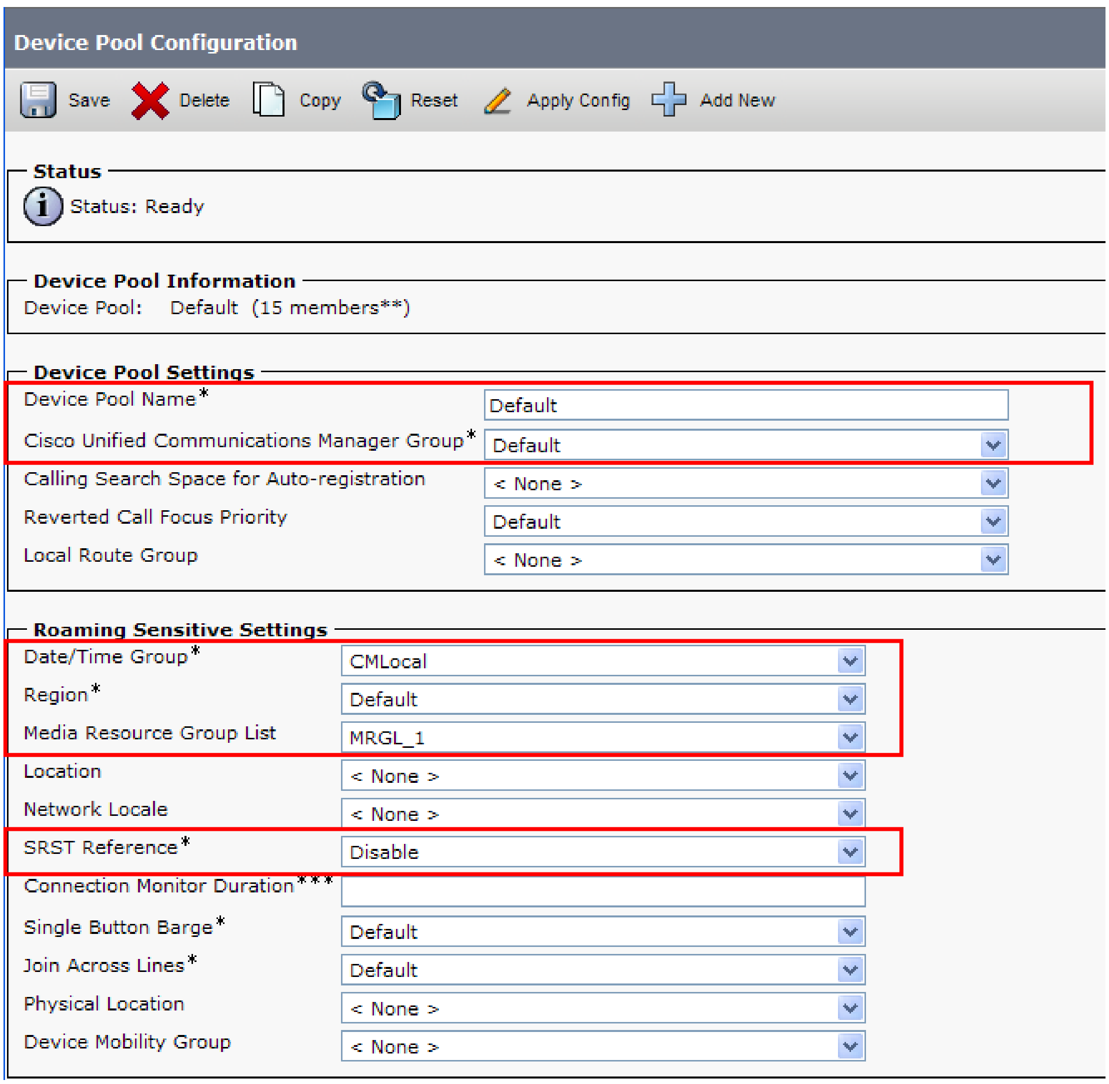
Expand **System** and select **Device Pool.** Click 

to configure a default Device Pool. Enter the following values and use defaults for remaining fields:

• **Device Pool Name**	Enter "**Default**"
• **Cisco Unified Communications Manager Group**	Select **"Default"**
• **Date/Time Group**	Select **"CMLocal"**
• **Region**	Select **"Default"**
• **Media Resource Group List**	Select the Media Resource Group List defined in **Section 5.2.3**
• **SRST Reference**	Select **"Disable**"

Click 

. The screen below shows the default Device Pool for the sample configuration.



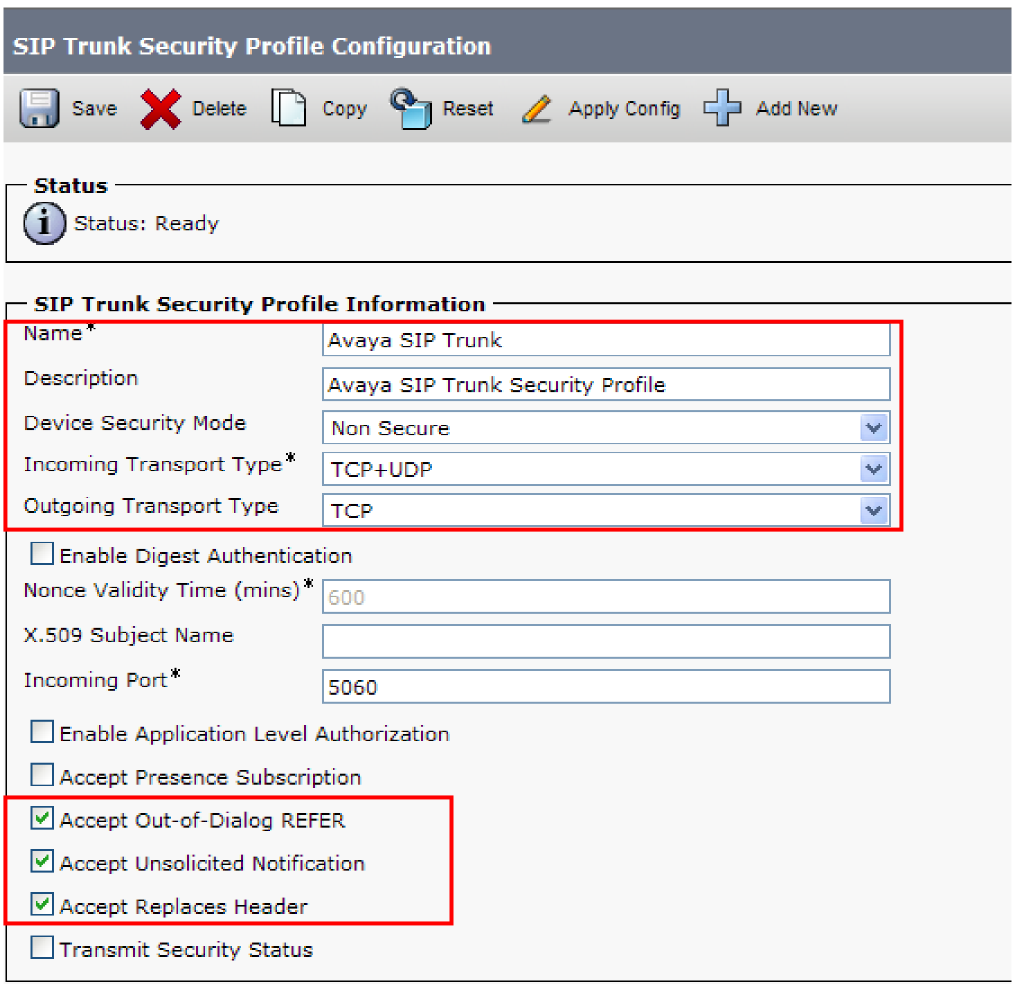
5.4. Define SIP Trunk Security Profile

Expand **System → Security Profile** and select **SIP Trunk Security Profile.** Click Add New to configure a SIP Trunk Security Profile.

Enter the following values and use defaults for remaining fields:

• **Name**	Enter name
• **Description**	Enter a brief description
• **Incoming Transport Type**	Verify **"TCP+UDP"** is selected
• **Outgoing Transport Type**	Verify "**TCP**" is selected
• **Accept Out-of-Dialog REFER**	Enter ☑
• **Accept Unsolicited Notification**	Enter ☑
• **Accept Replaces Header**	Enter ☑

Click Save. The screen below shows SIP Trunk Security Profile for the sample configuration



5.5. Define SIP Profile

Expand **Device → Device Settings** and select **SIP Profile.** Click Add New to configure a SIP Profile.

Under **SIP Profile Information** section, enter the following values and use defaults for remaining fields:

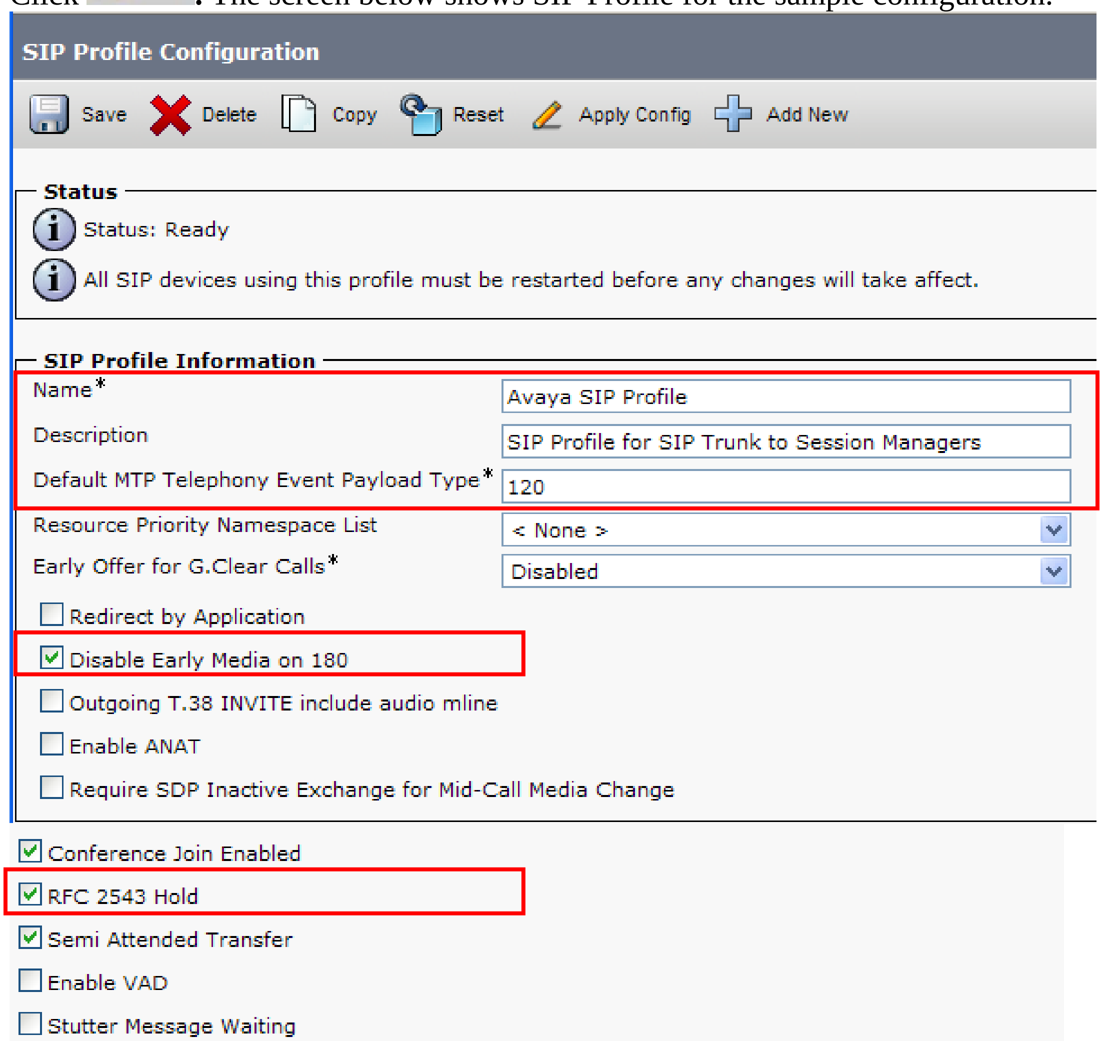
- **Name** Enter name
- **Description** Enter a brief description
- **Default MTP Telephony Event Payload Type** Enter **"120"**
- **Disable Early Media on 180** Enter ☑

  Note: Disabling Early Media allows local ringback to be used.

Under **Parameters used in Phone** section, scroll to end of section and enter the following values and use defaults for remaining fields:

- **RFC 2543 Hold** Enter ☑

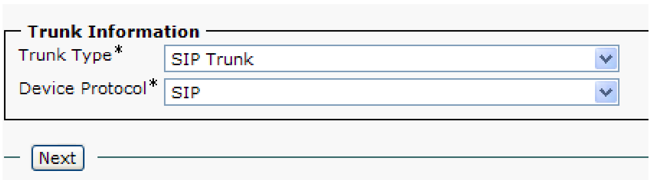
Click Save**.** The screen below shows SIP Profile for the sample configuration.



5.6. Define SIP Trunk to Avaya Aura® Session Manager

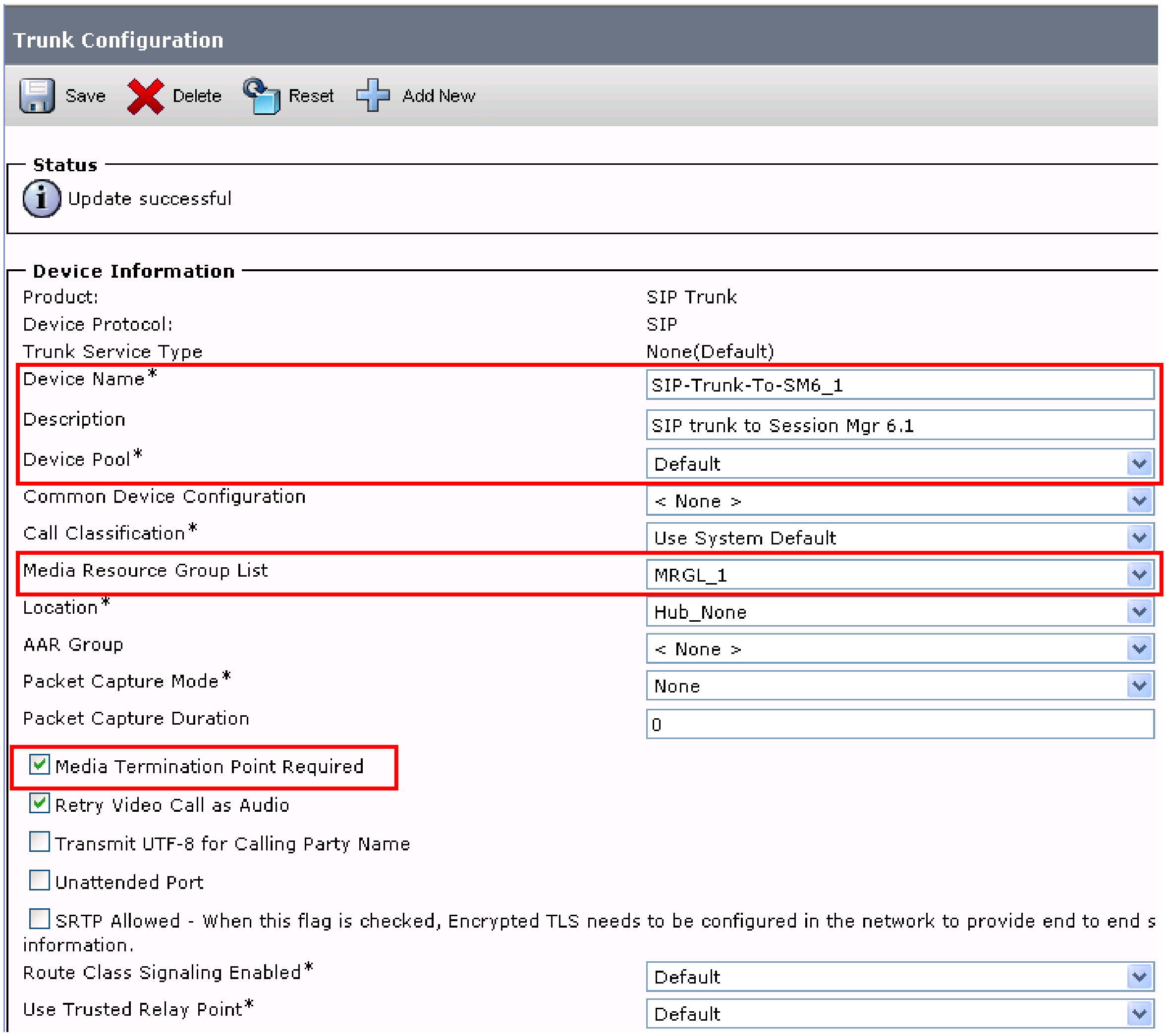
Expand **Device** select **Trunk.** Click Add New to define a SIP Trunk to Session Manager.
Under **Trunk Information** section, enter the following values as shown below and click **Next.**

- **Truck Type** Select **"SIP Trunk"**
- **Device Protocol** Select **"SIP"**



Under **Device Information** section, enter the following values and use defaults for remaining fields as shown below:

- **Device Name** Enter name
- **Description** Enter a brief description
- **Device Pool** Select **"Default"**
- **Media Resource Group List** Select the Media Resource Group List defined in **Section 5.2.3**
- **Media Termination Point Required** Enter ☑

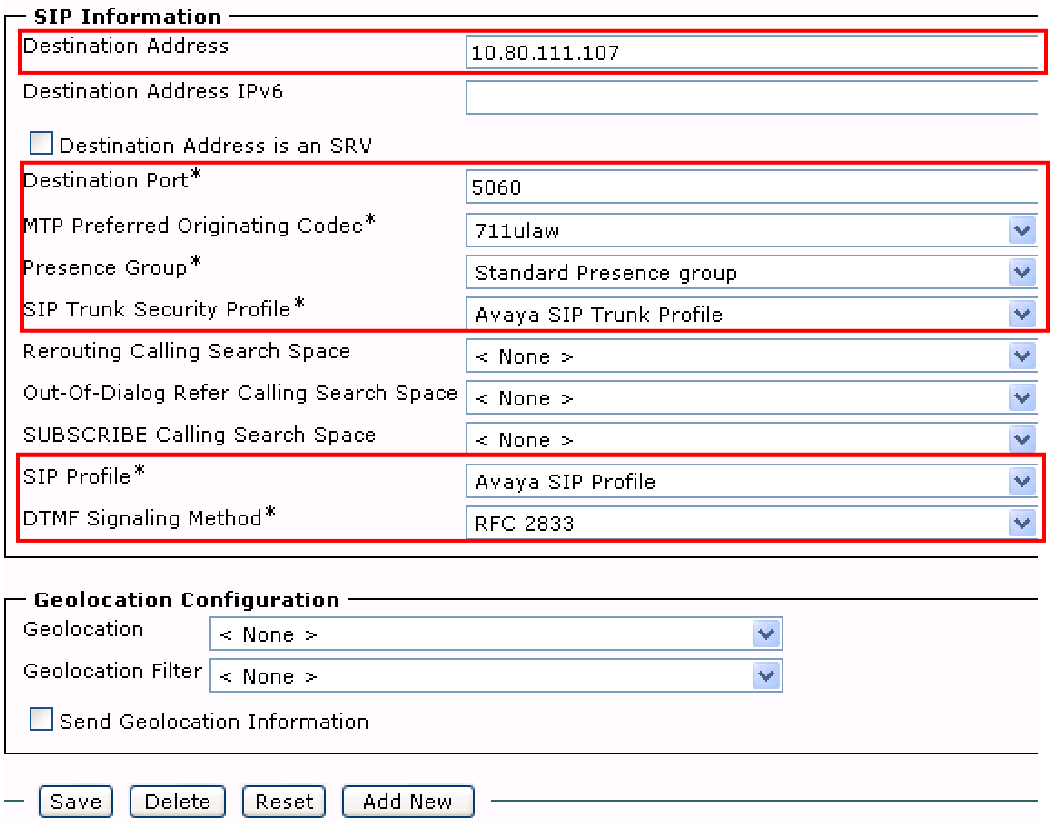


Trunk Configuration
Save
Delete
Reset
Add New
Status
Update successful
Device Information
Product:
SIP Trunk
Device Protocol:
SIP
Trunk Service Type
None(Default)
Device Name*
SIP-Trunk-To-SM6_1
Description
SIP trunk to Session Mgr 6.1
Device Pool*
Default
Common Device Configuration
< None >
Call Classification*
Use System Default
Media Resource Group List
MRGL_1
Location*
Hub_None
AAR Group
< None >
Packet Capture Mode*
None
Packet Capture Duration
0
Media Termination Point Required
Retry Video Call as Audio
Transmit UTF-8 for Calling Party Name
Unattended Port
SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end s
information.
Route Class Signaling Enabled*
Default
Use Trusted Relay Point*
Default

Scroll to **SIP Information** section, enter the following values and use defaults for remaining fields:

- **Destination Address** Enter IP address of SIP signaling interface for Session Manager
- **Destination Port** Enter **“5060”**
- **MTP Preferred Originating Codec** Select **“711ulaw”**
- **SIP Trunk Security Profile** Select SIP Trunk Security Profile defined in **Section 5.4**
- **SIP Profile** Select SIP Profile defined in **Section 5.5**
- **DTMF Signaling Method** Select **“RFC 2833”**

Click **Save.** The screen below shows SIP Information defined for SIP Trunk to Session Manager for the sample configuration.



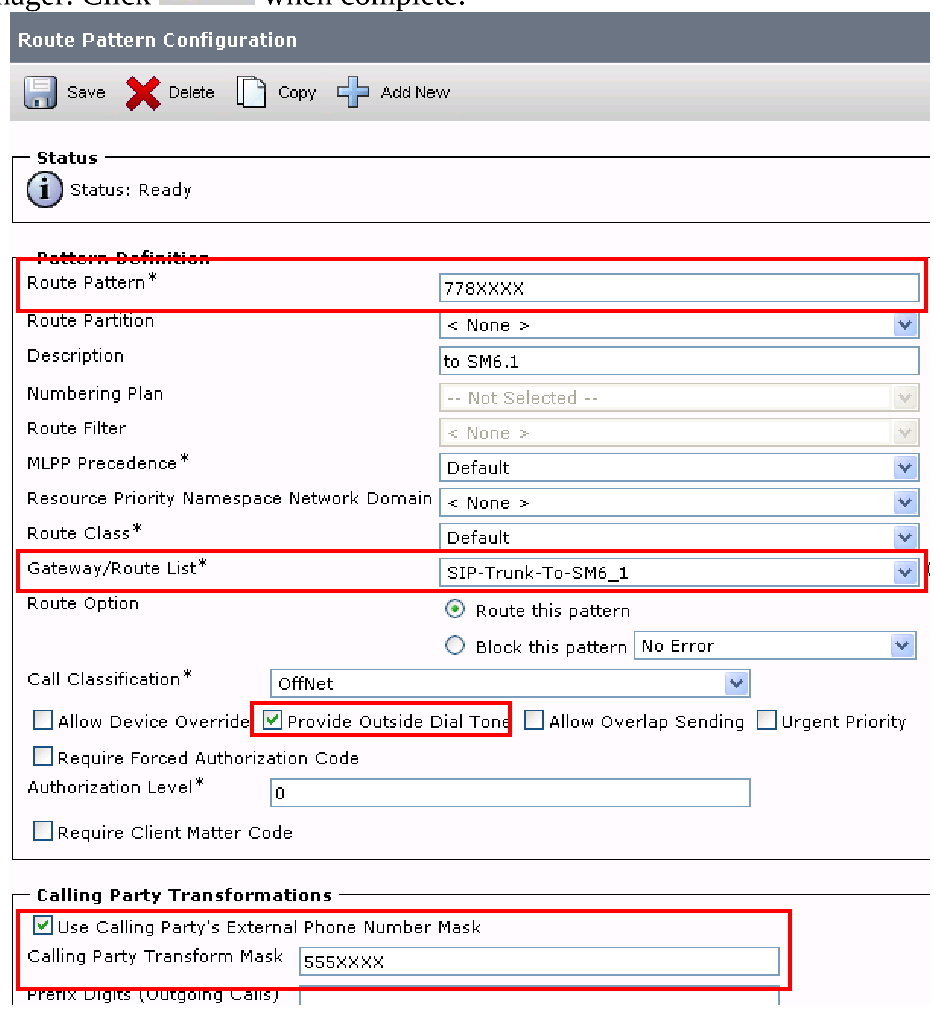
5.7. Define Routing Pattern

Expand **Call Routing → Route/Hunt** select **Route Pattern.**

Click Add New to configure new Route Pattern. Enter the following values as shown below and use defaults for remaining fields.

- **Route Pattern** — Enter dialed digits for calls routed to Session Manager For sample configuration, **"778XXXX"** was used.
- **Description** — Enter brief description [Optional]
- **Gateway/Route List** — Select **"SIP Trunk"** defined in **Section 5.6**
- **Provide Outside Dial Tone** — Enter ☑
- **Use Calling Party's External Phone Number Mask** — Enter ☑
- **Calling Party Transform Mask** — Enter **555xxxx** Which will add a 555 prefix to any 4-digit extension on CUCM that dials off-net**.**

The screen below shows Route Pattern defined for the sample configuration to route calls to Session Manager. Click Save when complete.

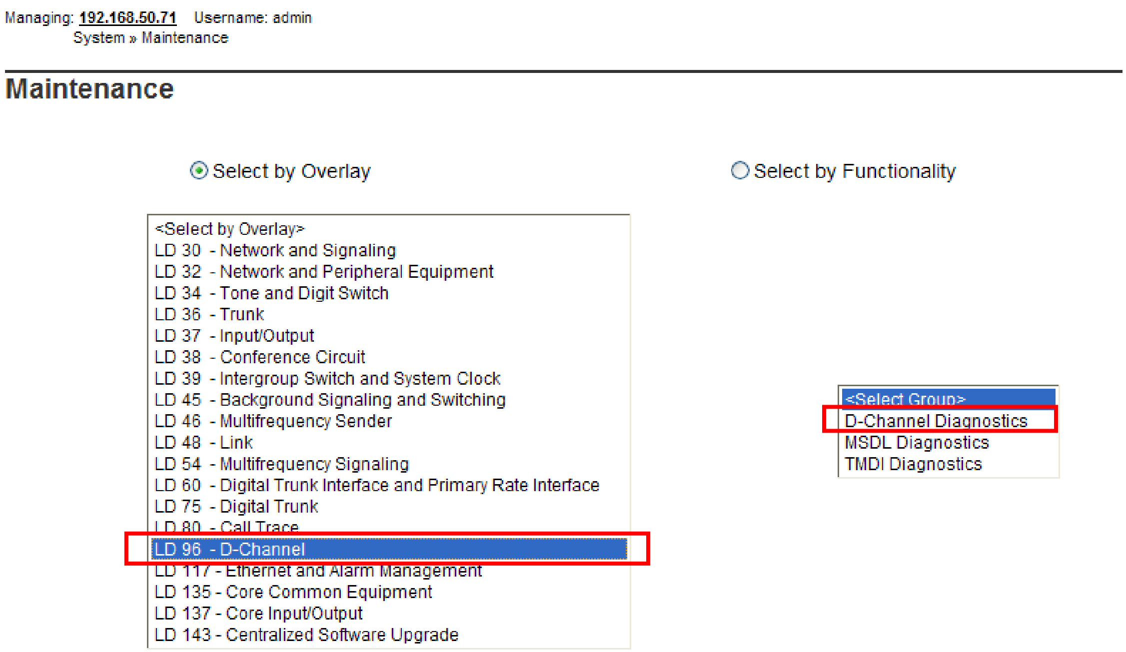


6. Verification Steps

6.1. Verify Avaya Communication Server 1000E Operational Status

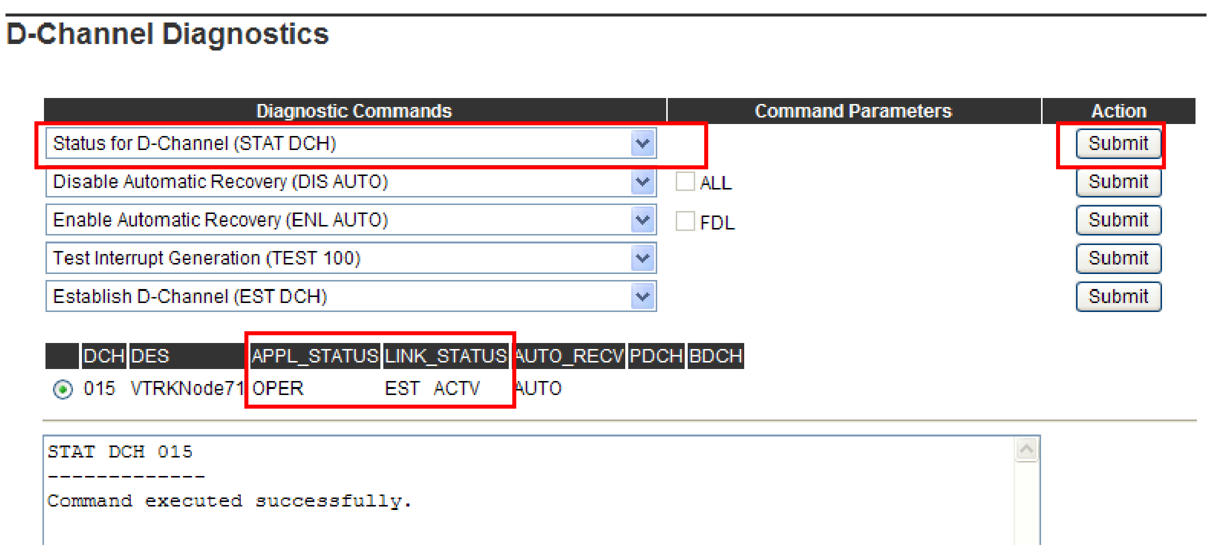
Expand **System** on the left navigation panel and select **Maintenance.**

Select **"LD 96 - D-Channel"** from the **Select by Overlay** table and the "**D-Channel Diagnostics"** function from the **Select Group** table as shown below.



Select **"Status for D-Channel (STAT DCH)"** command and click **Submit** to verify status of virtual D-Channel as shown below. Verify the status of the following fields:

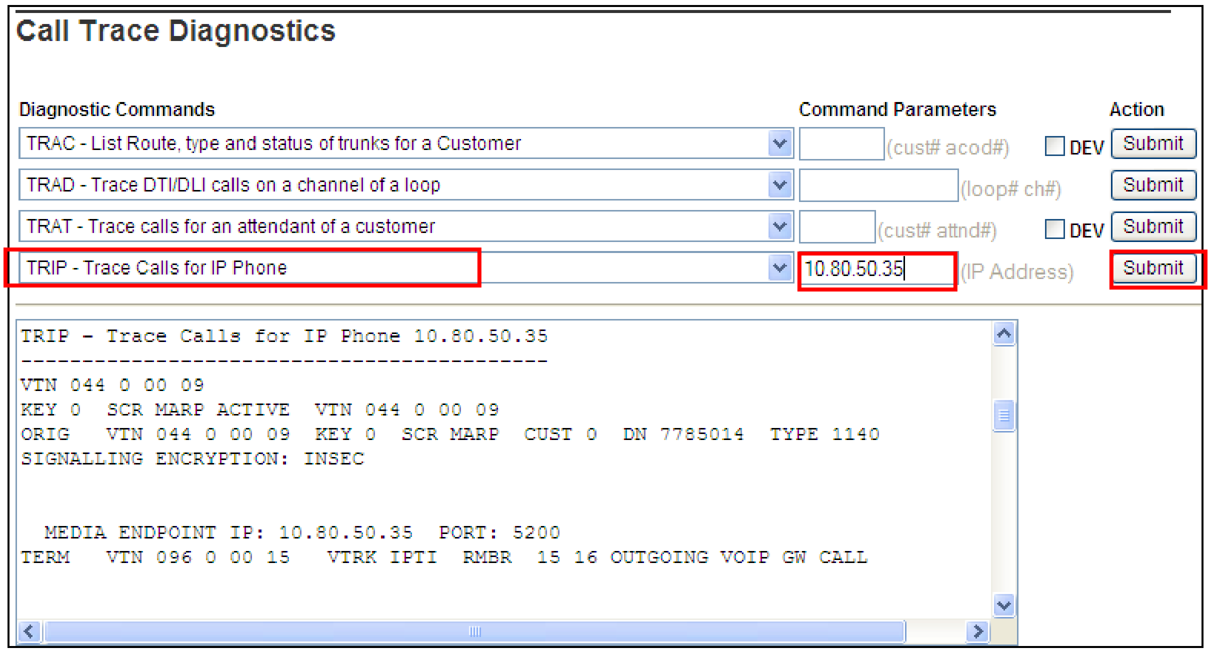
- **Appl_Status** Verify status is **"OPER"**
- **Link_Status** Verify status is **"EST ACTV"**



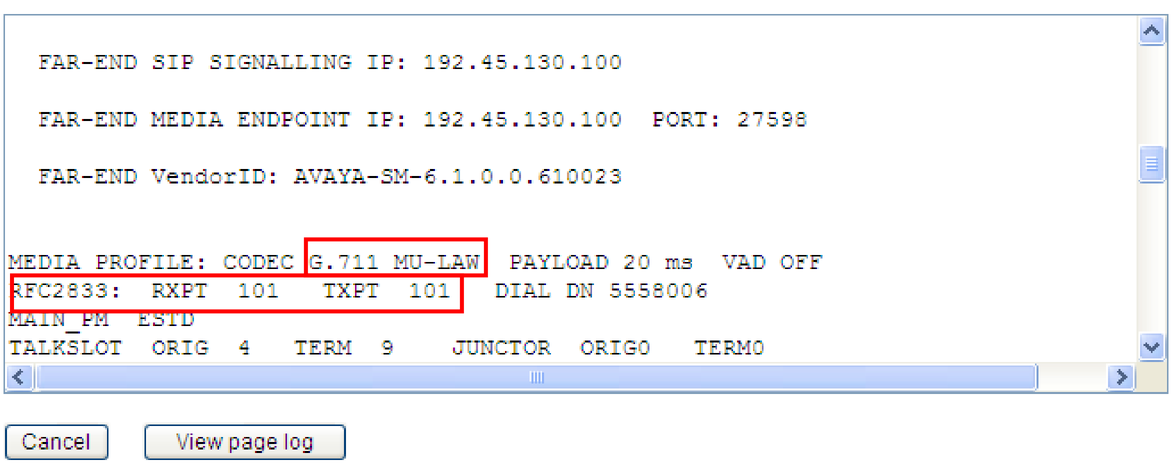
Select "**LD 80 – Call Trace**" command from the **Select by Overlay** table (not shown) to trace a call from IP telephone registered to Communication Server 1000E to a station on Cisco Unified Communications Manager.

On the **Call Trace Diagnostics** page, select "**TRIP – Trace Calls for IP Phone**" command, enter IP address for IP telephone and click **Submit** as shown below.

In the example, IP station with Directory Number "**778-5014**" and IP address "**10.80.50.35**" is calling a station on Cisco Unified Communications Manager with Dialed Number "**555-8006**".



Scrolling down further reveals additional information about the call such as the fact that the **G.711MU-LAW** codec is being used and **RFC2833 payload type 101** is being used for DTMF signaling in both directions. Select the **View page log** button to display the entire contents of the command output in separate window.



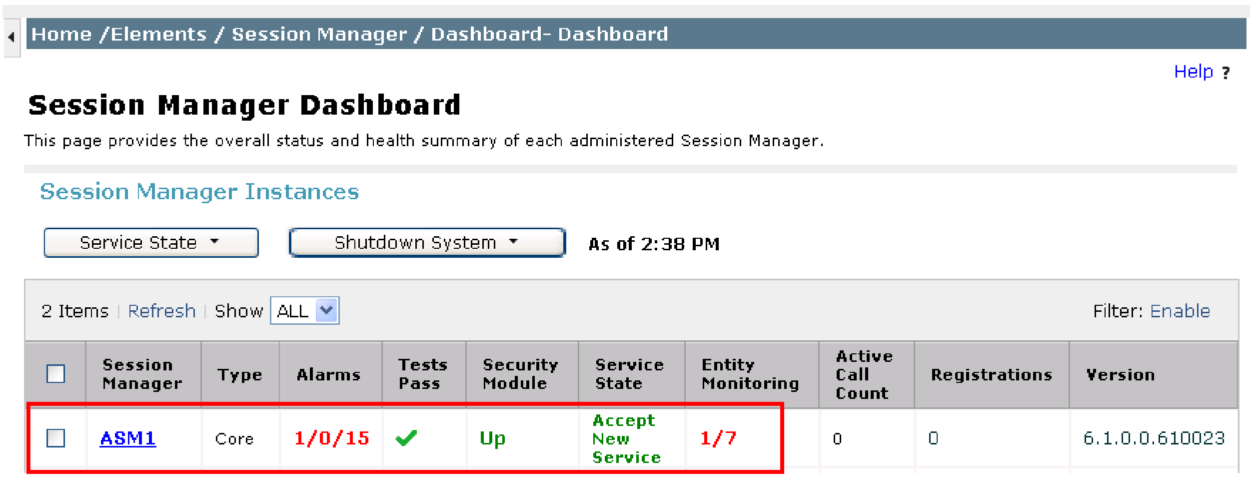
6.2. Verify Avaya Aura® Session Manager Operational Status

6.2.1. Verify Avaya Aura® Session Manager is Operational

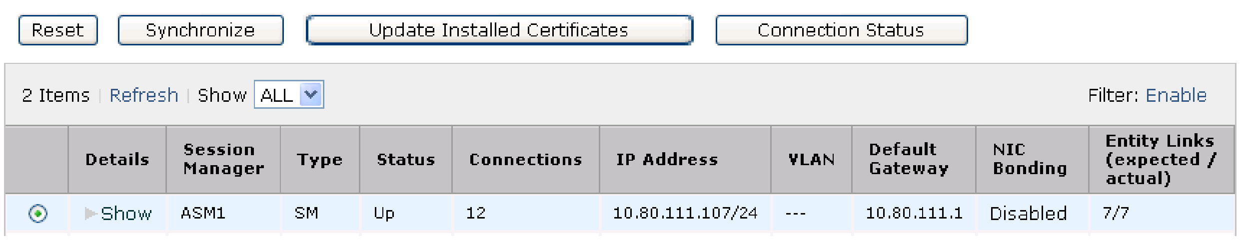
Navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager.

Specifically, verify the status of the following fields as shown below:

- **Tests Pass** ✔
- **Security Module** Up
- **Service State** Accept New Service



Navigate to **Elements → Session Manager → System Status → Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays "**Up**" as shown below.



6.2.2. Verify SIP Entity Link Status

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** (not shown) to view more detailed status information for one of the SIP Entity Links.

Select the SIP Entity for Avaya Communication Server 1000E from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

In the **All Entity Links to SIP Entity: CS1000 Rel7.5** table, verify the **Conn. Status** for the link is "**Up**" as shown below.

All Entity Links to SIP Entity: CS1000 Rel7.5

Summary View

1 Item | Refresh Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶Show	ASM1	10.80.50.61	5060	TCP	Up	200 OK	Up

Select the SIP Entity for Cisco Unified Communications Manager from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

In the **All Entity Links to SIP Entity: CUCM8** table, again verify the **Conn. Status** for the link is "**Up**" as shown below.

All Entity Links to SIP Entity: CUCM8

Summary View

1 Item | Refresh Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶Show	ASM1	192.45.130.100	5060	TCP	Up	200 OK	Up

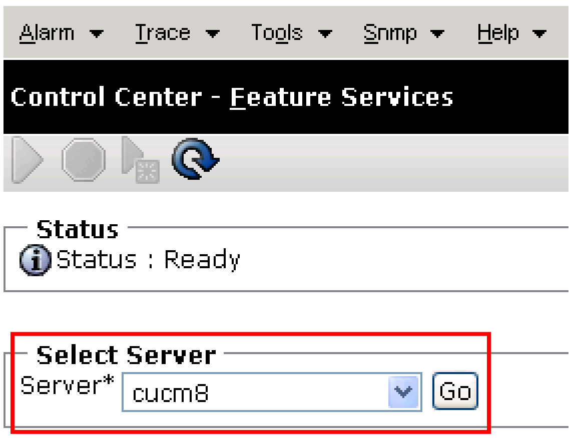
6.3. Verify Cisco Unified Communications Manager Operational Status

From the Cisco Unified CM Administration Home Page described in **Section 5**, select the "**Cisco Unified Serviceability**" application (not shown) to verify status of the Cisco system.

Expand **Tools** (not shown) and select **Control Center – Feature Services**.

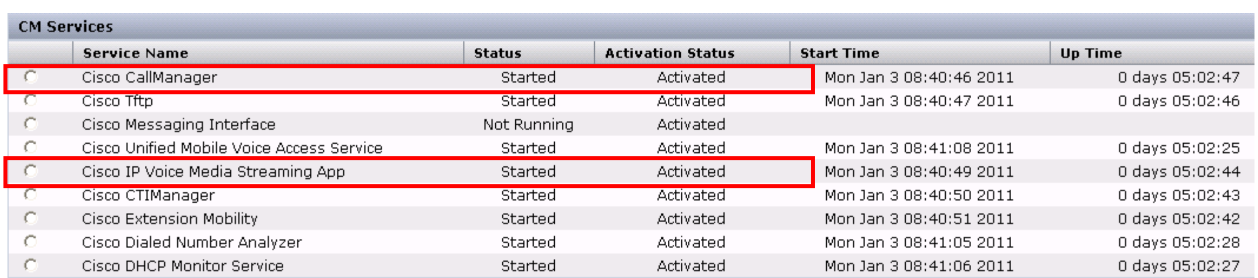
Under **Select Server** section, select **" <name>"** where <name> is name of Cisco Unified Communications Manager system and click **Go** to view status of the system.

In sample configuration, "**cucm8**" is name of system as shown below.



Under **CM Services** section, verify the status of the **Cisco CallManager** and **Cisco IP Voice Media Streaming** services as shown below. Verify the following fields:

- **Status** Verify status is **"Started**"
- **Activation Status** Verify status is **"Activated**

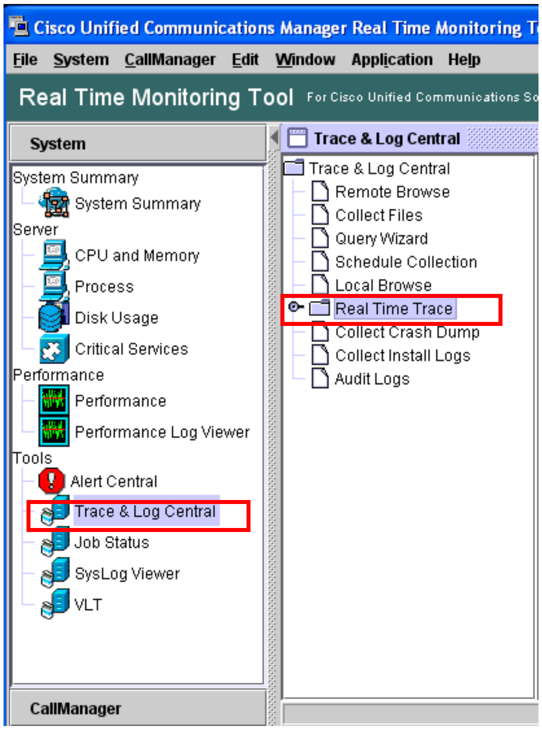


CM Services

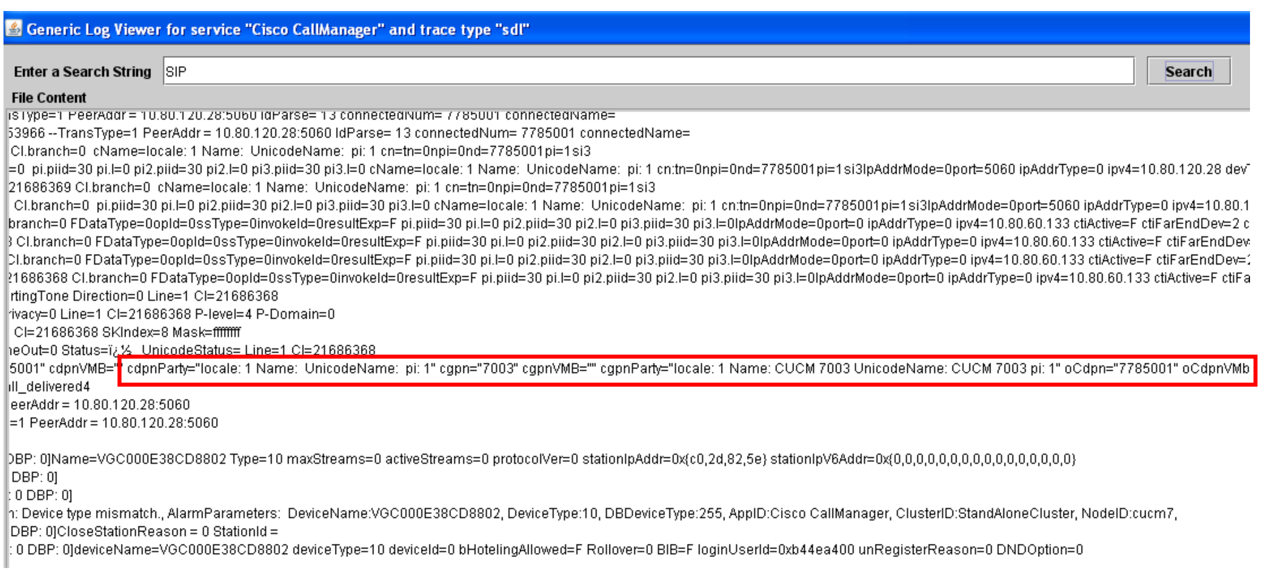
	Service Name	Status	Activation Status	Start Time	Up Time
	Cisco CallManager	Started	Activated	Mon Jan 3 08:40:46 2011	0 days 05:02:47
	Cisco Tftp	Started	Activated	Mon Jan 3 08:40:47 2011	0 days 05:02:46
	Cisco Messaging Interface	Not Running	Activated		
	Cisco Unified Mobile Voice Access Service	Started	Activated	Mon Jan 3 08:41:08 2011	0 days 05:02:25
	Cisco IP Voice Media Streaming App	Started	Activated	Mon Jan 3 08:40:49 2011	0 days 05:02:44
	Cisco CTIManager	Started	Activated	Mon Jan 3 08:40:50 2011	0 days 05:02:43
	Cisco Extension Mobility	Started	Activated	Mon Jan 3 08:40:51 2011	0 days 05:02:42
	Cisco Dialed Number Analyzer	Started	Activated	Mon Jan 3 08:41:05 2011	0 days 05:02:28
	Cisco DHCP Monitor Service	Started	Activated	Mon Jan 3 08:41:06 2011	0 days 05:02:27

Use the Real Time Monitoring Tool (RTMT) to monitor events on Cisco Unified Communications Manager. This tool can be downloaded by expanding **Application → Plugins** from the Cisco Unified CM Administration Web interface. For further information on installing this tool, see **Reference [13**] in **Section 9**.

Expand **Tools** on left panel and select **Trace & Log Central**. Under **Trace and Log Central** section, select **Real Time Trace** to start a real time data capture as shown below.



The following screen illustrates a real time trace of a call from a Cisco IP station with internal Directory Number "**7003**" to station "**778-5001**" on Avaya Communications Server 1000E.



6.4. Call Scenarios Verified

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

Basic Calls:

- Using G.711 audio codec, verify displays and talk path for calls between different types of stations on Avaya Communication Server 1000E and stations on Cisco Unified Communications Manager.
- Using G.729 audio codec, verify displays and talk path for calls between different types of stations on Avaya Communication Server 1000E and stations on Cisco Unified Communications Manager.
- Verify a second call can be made between different types of stations on Avaya Communication Server 1000E and stations on Cisco Unified Communications Manager after the first call is abandoned.

Supplemental Call Features:

- Verify calls from different types of stations on Avaya Communication Server 1000E to a station on Cisco Unified Communications Manager can be placed on hold.
- Verify calls from different types of stations on Avaya Communication Server 1000E to a station on Cisco Unified Communications Manager can be transferred to another station on either the same switch or remote switch.
- Verify calls from different types of stations on Avaya Communication Server 1000E to a station on Cisco Unified Communications Manager can create a conference with another station on either the same switch or remote switch.
- Verify calls from different types of stations on Avaya Communication Server 1000E to a station on Cisco Unified Communications Manager can be forwarded to another station on either the same switch or remote switch.
- Repeat the hold, transfer, conference and forward scenarios with calls originating from a station on Cisco Unified Communications Manager.

Long Duration Calls

- Place a call from different types of stations on Avaya Communication Server 1000E to a station on Cisco Unified Communications Manager. Answer the call, leave the call active for at least 30 minutes, and verify displays and talk path.
- Place a call from different types of stations on Avaya Communication Server 1000E to a station on Cisco Unified Communications Manager. Answer the call, put the call on hold for at least 30 minutes, and verify displays and talk path after returning to the call.
- Repeat the long duration scenarios with calls originating from a station on Cisco Unified Communications Manager.

6.5. Issues Found and Known Limitations

When the SIP trunk between Cisco Unified Communications Manager and Avaya Aura® Session Manager is configured to use a Media Termination Point (MTP) and both telephony systems are configured to use G.711 codecs, all test calls between the two systems were successful.

The following issues were observed during testing:

- Displays on UNIstim and SIP telephones registered to Avaya Communication Server 1000E may not be correctly updated when calls are placed on hold, transferred, or forwarded. **Reference [8]** in **Section 9** indicates Calling Party Name Display (CPND) and Calling Line Identification (CLID) are not updated when SIP telephones receive a REINVITE message which may be causing the display issues observed during testing.
- An MTP was required in order for supplemental calling features such as conferences and transfers to be successful.
- When both Cisco UCM and CS1000E were administered to use the G.729A codec along with "MTP Required" on Cisco UCM two issues were observed:
  - Calls to an 11XX SIP phone failed because the 11XX phone indicated it only supported G.711U.
  - All other calls were actually successful except that they used G.711U-law and bypassed the MTP.

7. Acronyms

CP+PM	Common Processor Pentium Mobile. Hardware platform for Avaya Communication Server 1000E
CUCM	Cisco Unified Call Manager
DTMF	Dual Tone Multi Frequency
GUI	Graphical User Interface
FQDN	Fully Qualified Domain Name (hostname for Domain Naming Resolution)
IP	Internet Protocol
LAN	Local Area Network
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SCCP	Skinny Client Control Protocol. SCCP is session signaling protocol used with Cisco Unified Communications Manager telephony systems.
SIL	Solution Interoperability Lab
SIP	Session Initiation Protocol
SM	Avaya Aura® Session Manager
SMGR	System Manager (used to configure Session Manager)
SNMP	Simple Network Management Protocol
SRE	SIP Routing Element
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
WAN	Wide Area Network

8. Conclusion

These Application Notes describe how to configure a sample network that uses SIP trunks among Avaya Aura® Session Manager Release 6.1, Avaya Communication Server 1000E Release 7.5 and Cisco Unified Communications Manager Release 8.0.

Interoperability testing included making bi-directional calls between several different types of stations on both telephony systems with various features including hold, transfer, conference and forwarding.

9. Additional References

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

Session Manager

1) Avaya Aura® Session Manager Overview, Doc ID 03-603323, available at http://support.avaya.com.
2) Installing and Configuring Avaya Aura® Session Manager, available at http://support.avaya.com.
3) Avaya Aura® Session Manager Case Studies, available at http://support.avaya.com
4) Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, available at http://support.avaya.com.
5) Administering Avaya Aura® Session Manager, Doc ID -3-603324, available at http://support.avaya.com

Avaya Communication Server 1000E

6) IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313, available at http://support.avaya.com
7) Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116, available at http://support.avaya.com
8) SIP Line Fundamentals, Release 7.5, Document Number NN43001-508, Issue 02.03, available at http://support.avaya.com
9) Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509, available at http://support.avaya.com
10) Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, available at http://support.avaya.com

Cisco Unified Communications Manager

11) Cisco Unified Communications Manager Administration Guide, Business Edition, Part Number: OL-15405-01, available at http://www.cisco.com
12) Cisco Unified Communications Manager Features and Services Guide, Business Edition, Part Number: OL-15409-01, available at http://www.cisco.com
13) Cisco Unified Real-Time Monitoring Tool Administration Guide, Part Number: OL-14994-01, available at http://www.cisco.com

Avaya Application Notes

14) Configuring SIP Trunks among Avaya Aura® Session Manager Release 6.0, Avaya Communication Server 1000E Release 7 and Cisco Unified Communications Manager Release 7.1, available at http://www.avaya.com
15) Configuring SIP Trunks among Avaya Aura® Session Manager 6.0, Avaya IP Office 6.0, and Communication Server 1000E, available at http://www.avaya.com
16) Application Notes for Avaya 1100- and 1200-Series IP Deskphones R3.2 with Avaya Aura® Communication Manager R6, Avaya Aura® Session Manager R6, and Avaya Modular Messaging R5.2.
17) Configuring SIP Trunks among Avaya Communication Server 1000E, Avaya Aura® Session Manager 6.0, Avaya Voice Portal 5.0 and Avaya Aura® Communication Manager Evolution Server 6.0, available at http://www.avaya.com

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com