



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[®] 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.....	3
2. EQUIPMENT AND SOFTWARE VALIDATED.....	5
3. CONFIGURE AVAYA COMMUNICATION SERVER 1000E.....	6
3.1. CONFIRM NODE AND IP ADDRESSES.....	8
3.2. CONFIRM VIRTUAL D-CHANNEL, ROUTES AND TRUNKS.....	9
3.2.1. <i>Confirm Virtual D-Channel Configuration</i>	9
3.2.2. <i>Confirm Routes and Trunks Configuration</i>	9
3.3. CONFIGURE SIP TRUNK TO AVAYA AURA® SESSION MANAGER	11
3.4. CONFIGURE ROUTE LIST INDEX AND DISTANT STEERING CODE.....	15
3.5. SAVE CONFIGURATION.....	19
4. CONFIGURE AVAYA AURA® SESSION MANAGER	20
4.1. DEFINE SIP DOMAINS	21
4.2. DEFINE LOCATIONS	21
4.3. CONFIGURE ADAPTATION MODULES	23
4.3.1. <i>Create an Adaptation Module for Cisco UCM</i>	23
4.3.2. <i>Create an Adaptation for Communication Server 1000E</i>	24
4.4. DEFINE SIP ENTITIES	25
4.5. DEFINE ENTITY LINKS.....	27
4.6. DEFINE ROUTING POLICY	28
4.7. DEFINE DIAL PATTERN	30
5. CONFIGURE CISCO UNIFIED COMMUNICATIONS MANAGER.....	32
5.1. CONFIGURE AUDIO CODEC	33
5.2. CONFIGURE MEDIA RESOURCES	33
5.2.1. <i>Configure Media Termination Point</i>	33
5.2.2. <i>Add Media Resource Group</i>	34
5.2.3. <i>Add Media Resource Group List</i>	35
5.3. CONFIGURE DEFAULT DEVICE POOL	36
5.4. DEFINE SIP TRUNK SECURITY PROFILE	37
5.5. DEFINE SIP PROFILE.....	38
5.6. DEFINE SIP TRUNK TO AVAYA AURA® SESSION MANAGER	39
5.7. DEFINE ROUTING PATTERN.....	42
6. VERIFICATION STEPS	43
6.1. VERIFY AVAYA COMMUNICATION SERVER 1000E OPERATIONAL STATUS	43
6.2. VERIFY AVAYA AURA® SESSION MANAGER OPERATIONAL STATUS	45
6.2.1. <i>Verify Avaya Aura® Session Manager is Operational</i>	45
6.2.2. <i>Verify SIP Entity Link Status</i>	46
6.3. VERIFY CISCO UNIFIED COMMUNICATIONS MANAGER OPERATIONAL STATUS	47
6.4. CALL SCENARIOS VERIFIED.....	49
6.5. ISSUES FOUND AND KNOWN LIMITATIONS.....	50
7. ACRONYMS.....	51
8. CONCLUSION	52
9. ADDITIONAL REFERENCES	52

1. Introduction

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).

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**.

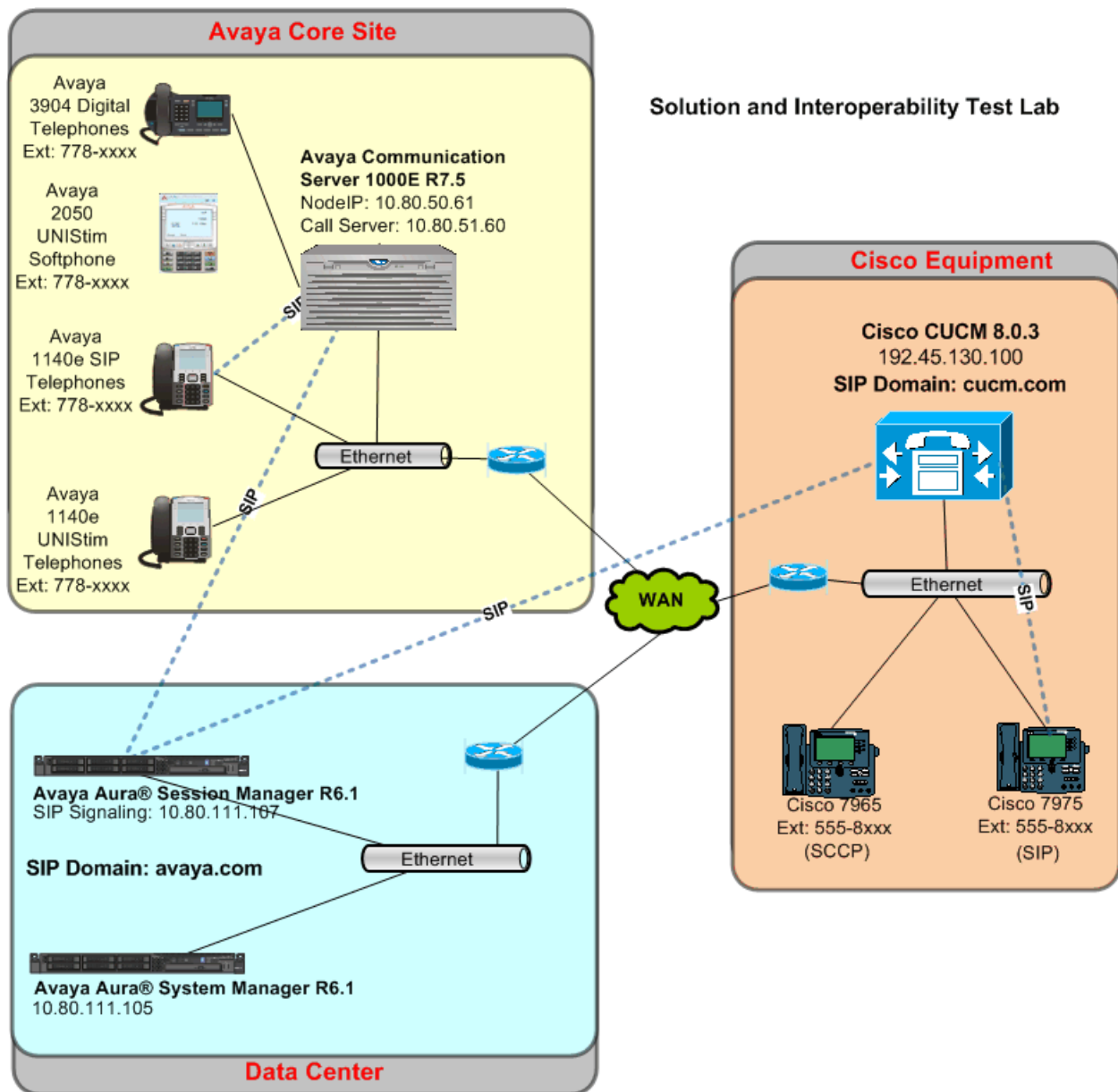


Figure 1 – Sample Configuration

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 (UNISim)	4.0.4.1
Avaya	1 – Avaya 1140E IP Telephone (UNISim)	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.



Users

- Administrators**
Manage Administrative Users
- Groups & Roles**
Manage groups, roles and assign roles to users
- Subscribers**
Manage users and shared resources associated with CS1000, including LDAP/file import and export
- Synchronize and Import**
Synchronize users with the enterprise directory, import users from file
- UCM Roles**
Manage UCM Roles, assign roles to users
- User Management**
Manage users, shared user resources and provision users

Elements

- Application Management**
Manage applications and application certificates
- Communication Manager**
Manage Communication Manager objects
- Conferencing**
Conferencing
- Inventory**
Manage, discover, and navigate to elements, update element software
- Messaging**
Manage Messaging System objects
- Presence**
Presence
- Routing**
Network Routing Policy
- SIP AS 8.1**
SIP AS 8.1
- Session Manager**
Session Manager Element Manager

Services

- Backup and Restore**
Backup and restore System Manager database
- Configurations**
Manage system wide configurations
- Events**
Manage alarms, view and harvest logs
- Licenses**
View and configure licenses
- Replication**
Track data replication nodes, repair replication nodes
- Scheduler**
Schedule, track, cancel, update and delete jobs
- Security**
Manage Security Certificates
- Templates**
Manage Templates for Communication Manager and Messaging System objects
- UCM Services**
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

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.



Host Name: 10.80.111.105 Software Version: 02.20_SMGR-SNAPSHOT(3925) User Name admin

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

	Element Name	Element Type	Release	Address	Description
1	smgr61-smgr.avaya.com (primary)	Base OS	7.5	10.80.111.105	Base OS element.
2	EM on cs1000r75	CS1000	7.5	10.80.51.60	New element.
3	cs1000r75.avaya.com (member)	Linux Base	7.5	10.80.50.60	Base OS element.
4	10.80.51.62	Media Gateway Controller	7.5	10.80.51.62	New element.

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 screenshot shows the CS1000 Element Manager interface. On the left is a navigation tree with 'Nodes: Servers, Media Cards' highlighted. The main area is titled 'IP Telephony Nodes' and shows a table of nodes. The node with ID '1006' is selected and highlighted with a red box. Below the table, there are checkboxes for 'Nodes', 'Component servers and cards', and 'IPv6 address'.

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
1006	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.80.50.61		Synchronized

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.

The screenshot shows the 'Node Details' page for Node ID 1006. The page is titled 'Node Details (ID: 1006 - SIP Line, LTPS, Gateway (SIPGw))'. It contains several fields for configuration, with 'Call server IP address' and 'TLAN IPv4' highlighted with red boxes. Below the fields is a table of 'Associated Signaling Servers & Cards'.

Node ID: 1006 * (0-9999)

Call server IP address: 10.80.51.60 *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)
Gateway IP address: 10.80.51.1 *
Subnet mask: 255.255.255.0 *

Telephony LAN (TLAN)
Node IPv4 address: 10.80.50.61 *
Subnet mask: 255.255.255.0 *
Node IPv6 address:

* Required Value.

Save Cancel

Associated Signaling Servers & Cards

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
cs1000r75	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	10.80.51.60	10.80.50.60	Leader

Show: ☐ IPv6 address

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

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.

The screenshot displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like UCM Network Services, System, Customers, and Routes and Trunks. The 'D-Channels' option under 'Routes and Trunks' is highlighted with a red box. The main content area is titled 'D-Channels' and includes a 'Maintenance' section with links to various diagnostic tools. Below this is a 'Configuration' section with a form to 'Choose a D-Channel Number' (set to 0) and 'type' (set to DCH), with a 'to Add' button. At the bottom, a table lists the configured D-channels:

Channel	Type	Card Type	Description	Action
Channel: 15	DCH	DCIP	VTRKNode1006	Edit

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.

Managing: **10.80.51.60** Username: admin
Routes and Trunks » Routes and Trunks

Routes and Trunks

- Customer: 0	Total routes: 2	Total trunks: 32	Add route	
- Route: 15	Type: TIE	Description: NODE2006SIP	Edit	Add trunk
+ Trunk: 1 - 16	Total trunks: 16			
+ Route: 16	Type: TIE	Description: SIPLINE	Edit	Add trunk

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.

Customer 0, Route 15 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE):	<input type="text" value="RDB"/>
Customer number (CUST):	<input type="text" value="00"/>
Route number (ROUT):	<input type="text" value="15"/>
Designator field for trunk (DES):	<input type="text" value="NODE2006SIP"/>
Trunk type (TKTP):	<input type="text" value="TIE"/>
Incoming and outgoing trunk (ICOG):	<input type="text" value="Incoming and Outgoing (IAO)"/>
Access code for the trunk route (ACOD):	<input type="text" value="1015"/>
Trunk type M911P (M911P):	<input type="checkbox"/>
The route is for a virtual trunk route (VTRK):	<input checked="" type="checkbox"/>
- Zone for codec selection and bandwidth management (ZONE):	<input type="text" value="00003"/> (0 - 8000)
- Node ID of signaling server of this route (NODE):	<input type="text" value="1006"/> (0 - 9999)
- Protocol ID for the route (PCID):	<input type="text" value="SIP (SIP)"/>
- Print correlation ID in CDR for the route (CRID):	<input type="checkbox"/>
Integrated services digital network option (ISDN):	<input checked="" type="checkbox"/>
- Mode of operation (MODE):	<input type="text" value="Route uses ISDN Signaling Link (ISLD)"/>
- D channel number (DCH):	<input type="text" value="15"/> (0 - 254)
- Interface type for route (IFC):	<input type="text" value="Meridian M1 (SL1)"/>
- Private network identifier (PNI):	<input type="text" value="00000"/> (0 - 32700)
- Network calling name allowed (NCNA):	<input checked="" type="checkbox"/>
- Network call redirection (NCRD):	<input checked="" type="checkbox"/>

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.

CS1000 Element Manager

Managing: 10.80.51.60 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1006 - SIP Line, LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.0 * Subnet mask: 255.255.255.0 *
Node IPv6 address:

IP Telephony Node Properties

- [Voice Gateway \(VGW\) and Codecs](#)
- [Quality of Service \(QoS\)](#)
- [LAN](#)
- [SNTP](#)
- [Numbering Zones](#)
- [MCDN Alternative Routing Treatment \(MALT\) Causes](#)

Applications (click to edit configuration)

- [SIP Line](#)
- **[Terminal Proxy Server \(TPS\)](#)**
- [Gateway \(SIPGw\)](#)
- [Personal Directories \(PD\)](#)
- [Presence Publisher](#)
- [IP Media Services](#)

* Required Value.

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.

Managing: 10.80.51.60 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1006 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw) *
SIP domain name: avaya.com *
Local SIP port: 5060 * (1 - 65535)
Gateway endpoint name: node1006 *
Gateway password: *
Application node ID: 1006 * (0-9999)
Enable failsafe NRS: ☐

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)
Information will be captured for the IP addresses listed below.
Monitor IP:
Monitor addresses:

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.

Managing: 10.80.51.60 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1006 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

transport protocol: TCP

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 10.80.111.107
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☐ Support registration
☐ Primary CDS proxy

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.

CS1000 Element Manager

Managing: 10.80.51.60 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1006 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Subscriber (NN):	0	<CCC><Area Code><NN>
National (NN):	0	<CCC><NN>
International:	0	<International number>

SIP URI Map:

Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text" value="udp"/>
Subscriber: <input type="text"/>	CDP: <input type="text" value="cdp.udp"/>
Special number: <input type="text" value="PublicSpecial"/>	Special number: <input type="text" value="PrivateSpecial"/>
Unknown: <input type="text" value="PublicUnknown"/>	Vacant number: <input type="text" value="PrivateUnknown"/>
	Unknown: <input type="text" value="UnknownUnknown"/>

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.

CS1000 Element Manager

Managing: 10.80.51.60 Username: admin
System » IP Network » IP Telephony Nodes » Node Saved

Node Saved

Node ID: 1006 has been saved on the call server.

The new configuration must also be transferred to associated servers and media cards.

You will be given an option to select individual servers, or transfer to all.

You may initiate a transfer manually at a later time.

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

CS1000 Element Manager

Managing: 10.80.51.60 Username: admin

System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1006>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

<input type="button" value="Start Sync"/>	<input type="button" value="Cancel"/>	<input type="button" value="Restart Applications"/>	Print Refresh	
<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1000r75	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

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

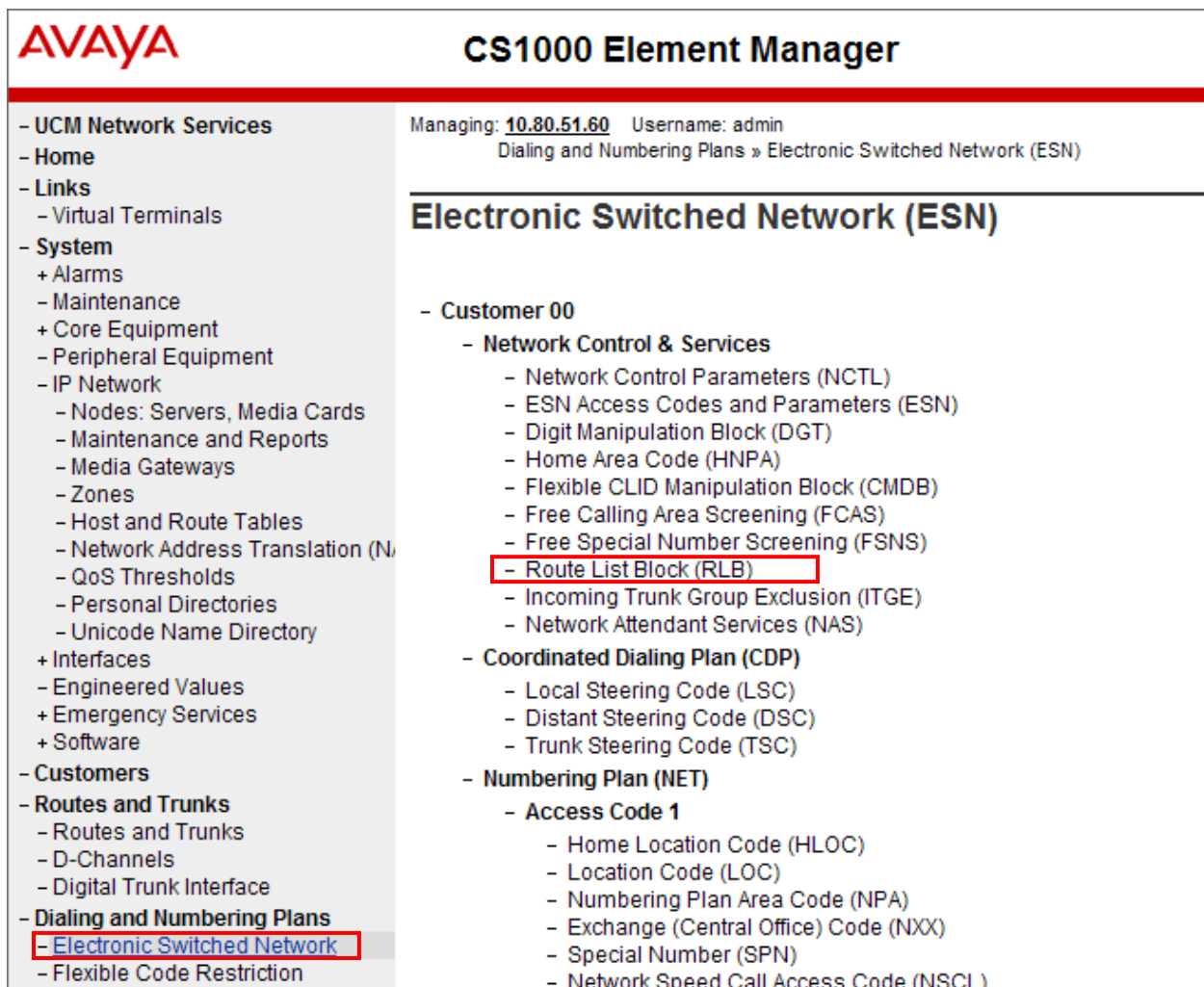
This section provides the configuration of the routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server and Session Manager.

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 screenshot displays the Avaya CS1000 Element Manager web interface. The top header shows the Avaya logo and the title "CS1000 Element Manager". Below the header, the management IP is "10.80.51.60" and the username is "admin". The breadcrumb trail indicates the current location: "Dialing and Numbering Plans » Electronic Switched Network (ESN)".

The left-hand navigation pane lists various system components. Under "Dialing and Numbering Plans", the "Electronic Switched Network" option is highlighted with a red box.

The main content area is titled "Electronic Switched Network (ESN)". It shows a hierarchical tree structure for "Customer 00". Under "Network Control & Services", the "Route List Block (RLB)" option is highlighted with a red box. Other options in this section include Network Control Parameters (NCTL), ESN Access Codes and Parameters (ESN), Digit Manipulation Block (DGT), Home Area Code (HNPA), Flexible CLID Manipulation Block (CMDB), Free Calling Area Screening (FCAS), Free Special Number Screening (FSNS), Incoming Trunk Group Exclusion (ITGE), and Network Attendant Services (NAS).

Other sections visible in the tree include "Coordinated Dialing Plan (CDP)" with Local Steering Code (LSC), Distant Steering Code (DSC), and Trunk Steering Code (TSC); and "Numbering Plan (NET)" with "Access Code 1" containing Home Location Code (HLOC), Location Code (LOC), Numbering Plan Area Code (NPA), Exchange (Central Office) Code (NXX), Special Number (SPN), and Network Speed Call Access Code (NSCL).

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.

Managing: [10.80.51.60](#) Username: admin
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) » Customer 00

Route List Blocks

Please enter a route list index (0 - 1999)

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.

Managing: [10.80.51.60](#) Username: admin
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) » Customer 00 » Network Control & Services » [Route List Blocks](#)

Route List Block

General Properties

Number of Alternate Routing Attempts: (1 - 10)
Initial Set: (0 - 64)
Set Minimum Facility Restriction Level:
Overlap Length: (0 - 24)
Extended Local Calls: ☐
Route List Index:
Entry Number for the Route List: (0 - 63)

Indexes

Time of Day Schedule:
Facility Restriction Level: (0 - 7)
Digit Manipulation Index:
ISL D-Channel Down Digit Manipulation Index: (0 - 1999)
Free Calling Area Screening Index:
Free Special Number Screening Index:
Business Network Extension Route: ☐
Incoming CLID Table: (0 - 200)

Options

Local Termination entry: ☐
Route Number:
Skip Conventional Signaling: ☐
Display Originator's Information: ☐
Use Tone Detector: ☐
Conversion to LDN: ☐

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.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation menu with the following items: UCM Network Services, Home, Links (Virtual Terminals), System (Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Interfaces, Engineered Values, Emergency Services, Software), Customers, Routes and Trunks (Routes and Trunks, D-Channels, Digital Trunk Interface), **Dialing and Numbering Plans** (Electronic Switched Network, Flexible Code Restriction, Incoming Digit Translation), and Phones (Templates). The 'Electronic Switched Network' item is highlighted with a red box. The main content area is titled 'Electronic Switched Network (ESN)' and shows a tree structure: Customer 00 > Network Control & Services (Network Control Parameters (NCTL), ESN Access Codes and Parameters (ESN), Digit Manipulation Block (DGT), Home Area Code (HNPA), Flexible CLID Manipulation Block (CMDDB), Free Calling Area Screening (FCAS), Free Special Number Screening (FSNS), Route List Block (RLB), Incoming Trunk Group Exclusion (ITGE), Network Attendant Services (NAS)), **Coordinated Dialing Plan (CDP)** (Local Steering Code (LSC), **Distant Steering Code (DSC)**, Trunk Steering Code (TSC)), and + Numbering Plan (NET). The 'Distant Steering Code (DSC)' item is highlighted with a red box.

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.

CS1000 Element Manager

Managing: **10.80.51.60** Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 »

Distant Steering Code List

▼

Please enter a distant steering code

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**.

Managing: **10.80.51.60** Username: admin
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) » Customer 00 » Coordinated Dialing Plan (CDP) » [Distant Steering Code](#)

Distant Steering Code

Distant Steering Code:	<input type="text" value="555"/>
Flexible Length number of digits:	<input type="text" value="7"/> (0 - 10)
Display:	<input type="text" value="Local Steering Code (LSC)"/>
Remote Radio Paging Access:	<input type="checkbox"/>
Route List to be accessed for trunk steering code:	<input type="text" value="1"/>
Collect Call Blocking:	<input type="checkbox"/>
Maximum 7 digit NPA code allowed:	<input type="text"/>
Maximum 7 digit NXX code allowed:	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Refresh"/>	

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.

The screenshot shows the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like UCM Network Services, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. Under the 'Tools' category, 'Backup and Restore' is expanded, and 'Call Server' is highlighted with a red box. The main content area is titled 'Call Server Backup'. It shows the current user as 'admin' managing IP '10.80.51.60'. Below this, there's a breadcrumb trail: 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. The main action section has a dropdown menu set to 'Backup' and two buttons: 'Submit' (highlighted with a red box) and 'Cancel'.

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.

```
Backing up reten.bkp to "var/opt/nortel/cs/fs/cf2/backup/single"
Database backup Complete!
TEMU207
Backup process to local Removable Media Device ended successfully.
```

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 as 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.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 15, 2010 10:44 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Domains

Domain Management

1 Item Refresh Filter: Enable

Name	Type	Default	Notes
* avaya.com	SIP	<input type="checkbox"/>	

* Input Required

Commit Cancel

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 screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar has a menu with 'Locations' highlighted. The main content area is titled 'Home / Elements / Routing / Locations- Location Details'. It contains a 'Location Details' section with a 'Name' field set to 'Location 1: Subnet 10.80.50' and a 'Notes' field. Below this is the 'Overall Managed Bandwidth' section with 'Managed Bandwidth Units' set to 'Kbit/sec' and 'Total Bandwidth' set to 0. The 'Per-Call Bandwidth Parameters' section has 'Default Audio Bandwidth' set to 80 Kbit/sec. The 'Location Pattern' section shows a table with one item: 'IP Address Pattern' with a value of '* 10.80.50.*' and a 'Notes' column.

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

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar has a menu with 'Locations' highlighted. The main content area is titled 'Home / Elements / Routing / Locations- Location Details'. It contains a 'Location Details' section with a 'Name' field set to 'Subnet_192.145.130.x' and a 'Notes' field set to 'Cisco stuff'. Below this is the 'Overall Managed Bandwidth' section with 'Managed Bandwidth Units' set to 'Kbit/sec' and 'Total Bandwidth' set to 0. The 'Per-Call Bandwidth Parameters' section has 'Default Audio Bandwidth' set to 80 Kbit/sec. The 'Location Pattern' section shows a table with one item: 'IP Address Pattern' with a value of '* 192.45.130.*' and a 'Notes' column.

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.

The screenshot displays the 'Adaptation Details' configuration page in the Cisco Unified Communications Manager Administration interface. The left-hand navigation menu shows 'Routing' expanded, with 'Adaptations' selected and highlighted by a red rectangle. The main content area is titled 'Adaptation Details' and includes a 'Help ?' link and 'Commit' and 'Cancel' buttons. The 'General' section is highlighted with a red box and contains the following fields:

- * Adaptation name:** CUCM8
- Module name:** CiscoAdapter (selected from a dropdown menu)
- Module parameter:** iosrcd=avaya.com odstd=192.45.130.100
- Egress URI Parameters:** (empty field)
- Notes:** (empty text area)

Below the 'General' section, there is a section titled 'Digit Conversion for Incoming Calls to SM' with 'Add' and 'Remove' buttons.

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.

The screenshot displays the Avaya Session Manager configuration interface. On the left, a navigation menu shows 'Routing' expanded, with 'Adaptations' highlighted. The main panel is titled 'Home /Elements / Routing / Adaptations- Adaptation Details'. It contains two sections: 'General' and 'Digit Conversion for Incoming Calls to SM'. In the 'General' section, the 'Adaptation name' is 'CS1000', 'Module name' is 'CS1000Adapter', and 'Module parameter' is 'fromto=true'. In the 'Digit Conversion for Incoming Calls to SM' section, the 'Add' button is highlighted. Below it, a table lists two items. The second item, with 'Matching Pattern' '555', is highlighted with a red box.

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 333	* 7	* 7	cdp.udp	* 0		both	
<input type="checkbox"/>	* 555	* 7	* 7	cdp.udp	* 0		both	

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 screenshot displays the 'SIP Entity Details' configuration page. The left navigation pane shows 'Routing' expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'Commit' button. The 'General' section contains the following fields:

- Name:** CS1000 Rel7.5
- FQDN or IP Address:** 10.80.50.61
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** CS1000
- Location:** Location 1: Subnet 10.80.50
- Time Zone:** America/Denver

Below the 'General' section, there is an 'Override Port & Transport with DNS SRV' checkbox (unchecked) and a 'SIP Timer B/F (in seconds):' field set to 4. The 'Credential name:' field is empty. The 'Call Detail Recording:' dropdown is set to 'egress'. The 'SIP Link Monitoring' section at the bottom shows the 'SIP Link Monitoring:' dropdown set to 'Use Session Manager Configuration'.

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

Routing

- Domains
- Locations
- Adaptations
- SIP Entities**
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

Home /Elements / Routing / SIP Entities- SIP Entity Details

SIP Entity Details Commit

General

* Name: CUCM8

* FQDN or IP Address: 192.45.130.100

Type: SIP Trunk

Notes: Cisco Unified Call Mgr 8.0

Adaptation: CUCM8

Location: Subnet_192.145.130.x

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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.

Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Entity Links- Entity Links

Entity Links

Commit Cancel Help ?

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CS1K Rel7-5	* ASM1	TCP	* 5060	* CS1000 Rel7.5	* 5060	<input checked="" type="checkbox"/>	

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

- Routing
- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

Home / Elements / Routing / Entity Links - Entity Links
Routing x Home

Entity Links

[Help ?](#)
Commit
Cancel

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Not
* ASM1_CUCM8_506	* ASM1	TCP	* 5060	* CUCM8	* 5060	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

Home / Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details Commit Cancel [Help ?](#)

General

* Name: CSRel7.5

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1000 Rel7.5	10.80.50.61	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

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

Routing Policy Details Commit Cancel

General

* Name: to_CUCM8

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CUCM8	192.45.130.100	SIP Trunk	Cisco Unified Call Mgr 8.0

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

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 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.

Home / Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

Help ?

Commit Cancel

General

* Pattern: 778

* Min: 7

* Max: 7

Emergency Call: ☐

SIP Domain: -ALL-

Notes: to CS1000 R7.5

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	CSRel7.5	0	<input type="checkbox"/>	CS1000 Rel7.5	

Select : All, None

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

Home /Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

CommitCancelHelp ?

General

* Pattern: 5558

* Min: 7

* Max: 7

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

AddRemove

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name <small>1 ▲</small>	Originating Location Notes	Routing Policy Name	Rank <small>2 ▲</small>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to_CUCM8	0	<input type="checkbox"/>	CUCM8	

Select : All, None

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:

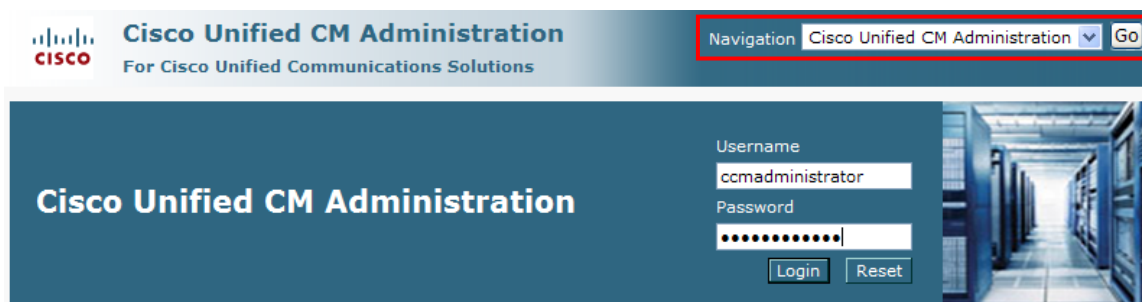
- Verify Audio Codec Configuration
- Configure Media Resources
- Configure Default Device Pool
- Configure SIP Trunk Security Profile
- Define Avaya SIP Profile
- Define SIP Trunk
- Define Routing Pattern

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.

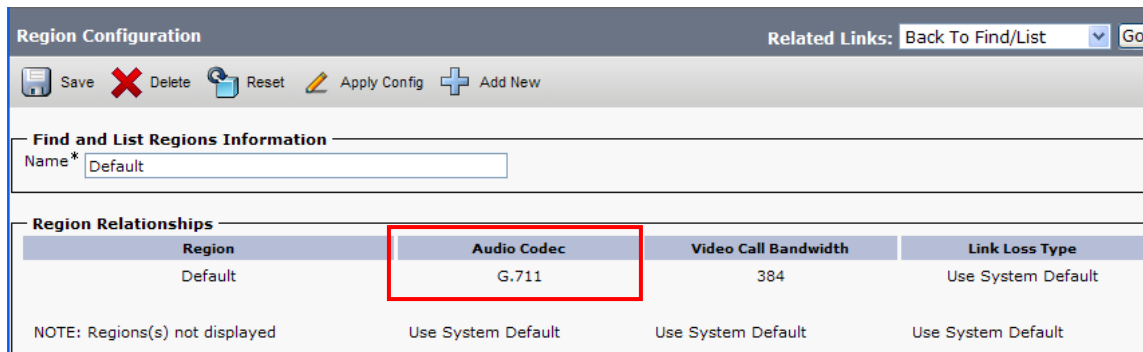
Select the “**Cisco Unified CM Administration**” application from the **Navigation** drop-down menu. Click **Go** and login with the appropriate credentials as shown below.



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.



The screenshot shows the 'Region Configuration' page. At the top, there are tabs for 'Find and List Regions Information' and 'Region Relationships'. The 'Find and List Regions Information' tab is active, showing a search bar with 'Default' entered. Below this, the 'Region Relationships' tab is active, displaying a table with columns: Region, Audio Codec, Video Call Bandwidth, and Link Loss Type. The 'Audio Codec' column for the 'Default' region is highlighted with a red box and contains the value 'G.711'. Below the table, a note states: 'NOTE: Region(s) not displayed'.

Region	Audio Codec	Video Call Bandwidth	Link Loss Type
Default	G.711	384	Use System Default

NOTE: Region(s) not displayed Use System Default Use System Default Use System Default

5.2. Configure Media Resources

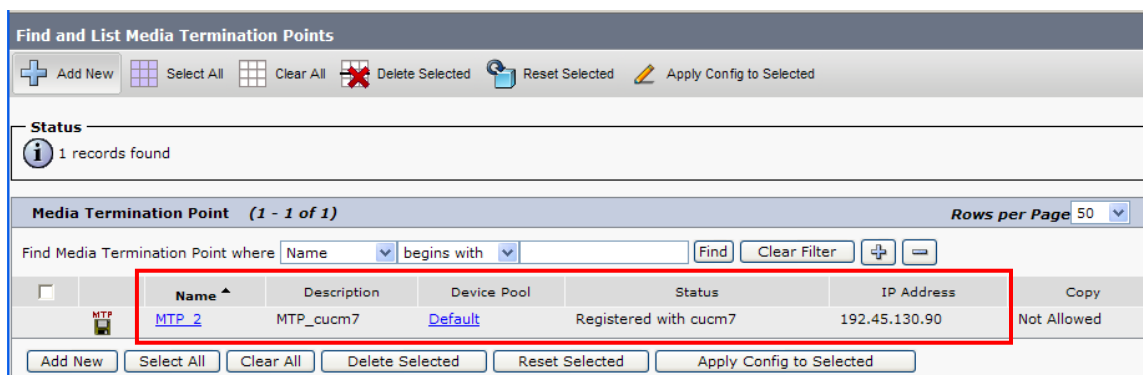
5.2.1. Configure Media Termination Point

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.



The screenshot shows the 'Find and List Media Termination Points' page. At the top, there are tabs for 'Find and List Media Termination Points' and 'Media Termination Point'. The 'Find and List Media Termination Points' tab is active, showing a search bar with 'Name' selected and 'begins with' entered. Below this, the 'Media Termination Point' tab is active, displaying a table with columns: Name, Description, Device Pool, Status, IP Address, and Copy. The 'Name' column for the 'MTP_2' media termination point is highlighted with a red box and contains the value 'MTP_2'. Below the table, a note states: 'NOTE: Media Termination Point(s) not displayed'.

Name	Description	Device Pool	Status	IP Address	Copy
MTP_2	MTP_cucm7	Default	Registered with cucm7	192.45.130.90	Not Allowed

NOTE: Media Termination Point(s) not displayed


5.2.2. Add Media Resource Group

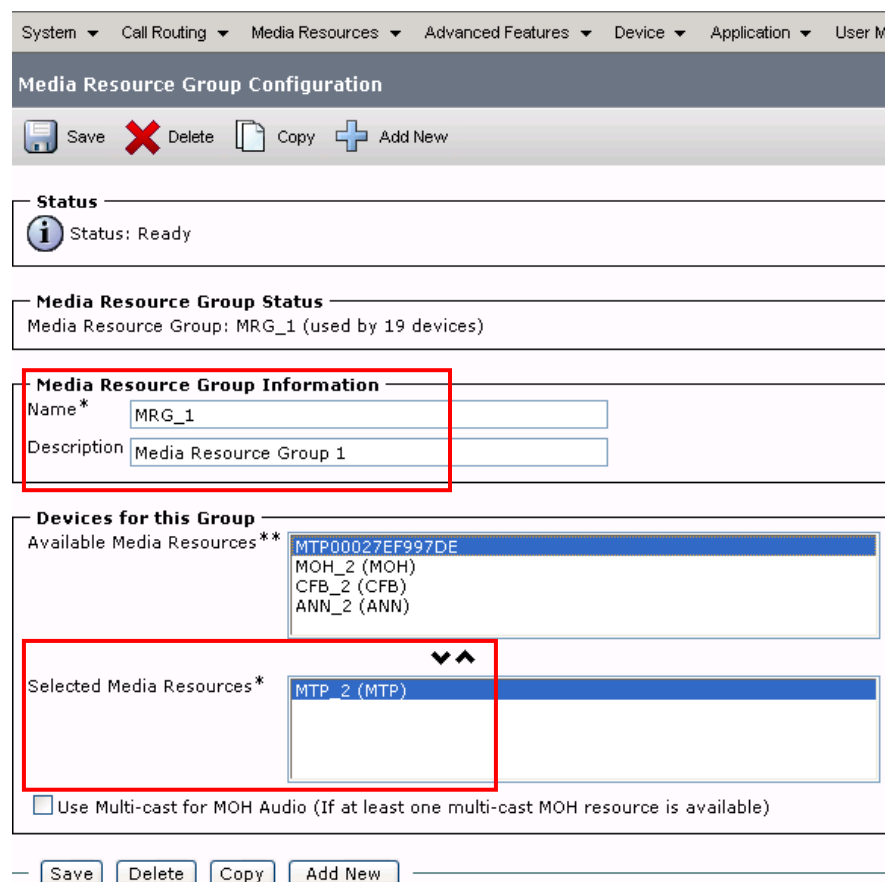
A Media Resource Group is used to group different types of media resources such as annunciators, media termination points, and conference bridges into a single group.

Expand **Media Resources** and select **Media Resource Group**. Click  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  to save new group definition. The screen below shows the Media Resource Group defined for the sample configuration.



System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User M

Media Resource Group Configuration

 Save  Delete  Copy  Add New

Status
 Status: Ready

Media Resource Group Status
Media Resource Group: MRG_1 (used by 19 devices)

Media Resource Group Information

Name*

Description

Devices for this Group





Available Media Resources**

MTP00027EF997DE
MOH_2 (MOH)
CFB_2 (CFB)
ANN_2 (ANN)

Selected Media Resources*

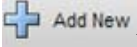
MTP_2 (MTP)

☐ Use Multi-cast for MOH Audio (If at least one multi-cast MOH resource is available)

 Save  Delete  Copy  Add New


5.2.3. Add Media Resource Group List

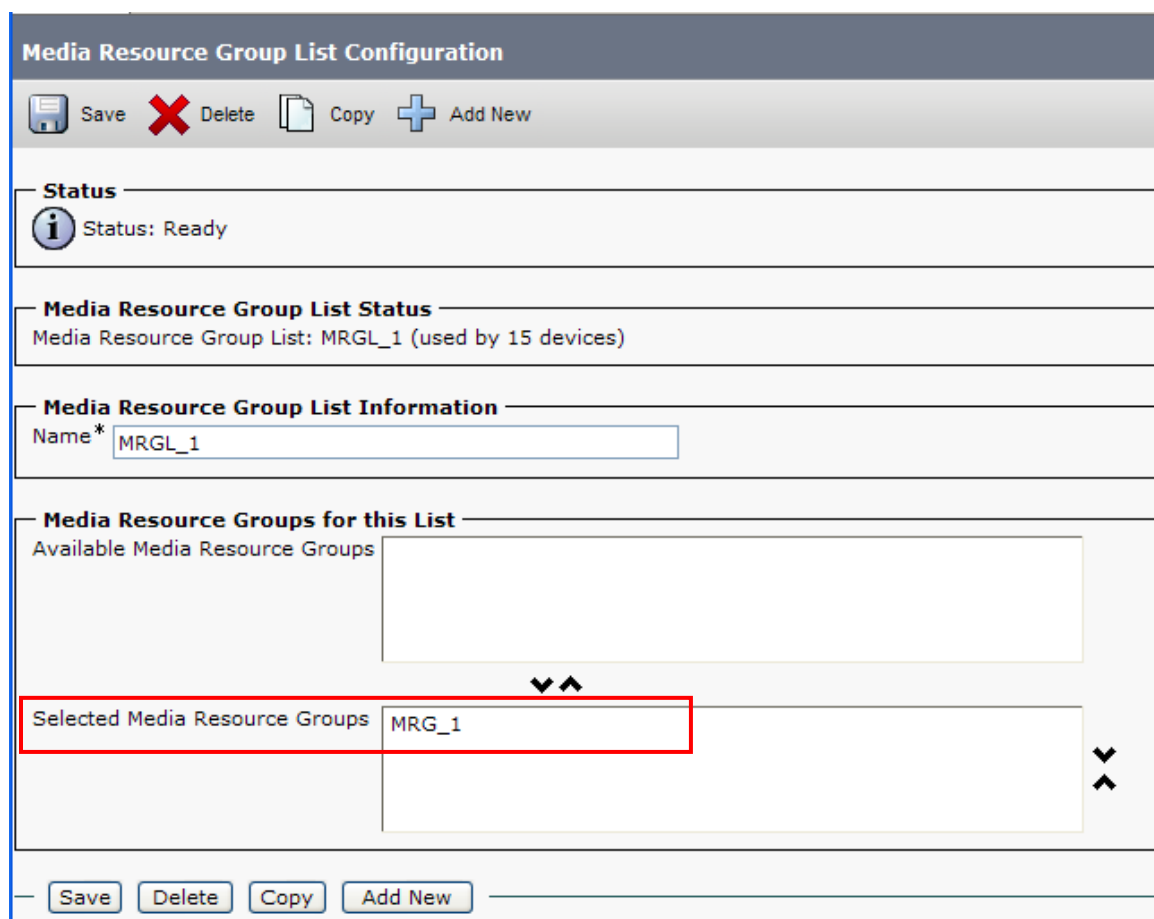
A Media Resource Group List is used to group different types of media resources such as annunciators, media termination points, etc into a single group.

Expand **Media Resources** and select **Media Resource Group List**. Click  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  to save new list. The screen below shows the Media Resource Group List defined for the sample configuration.



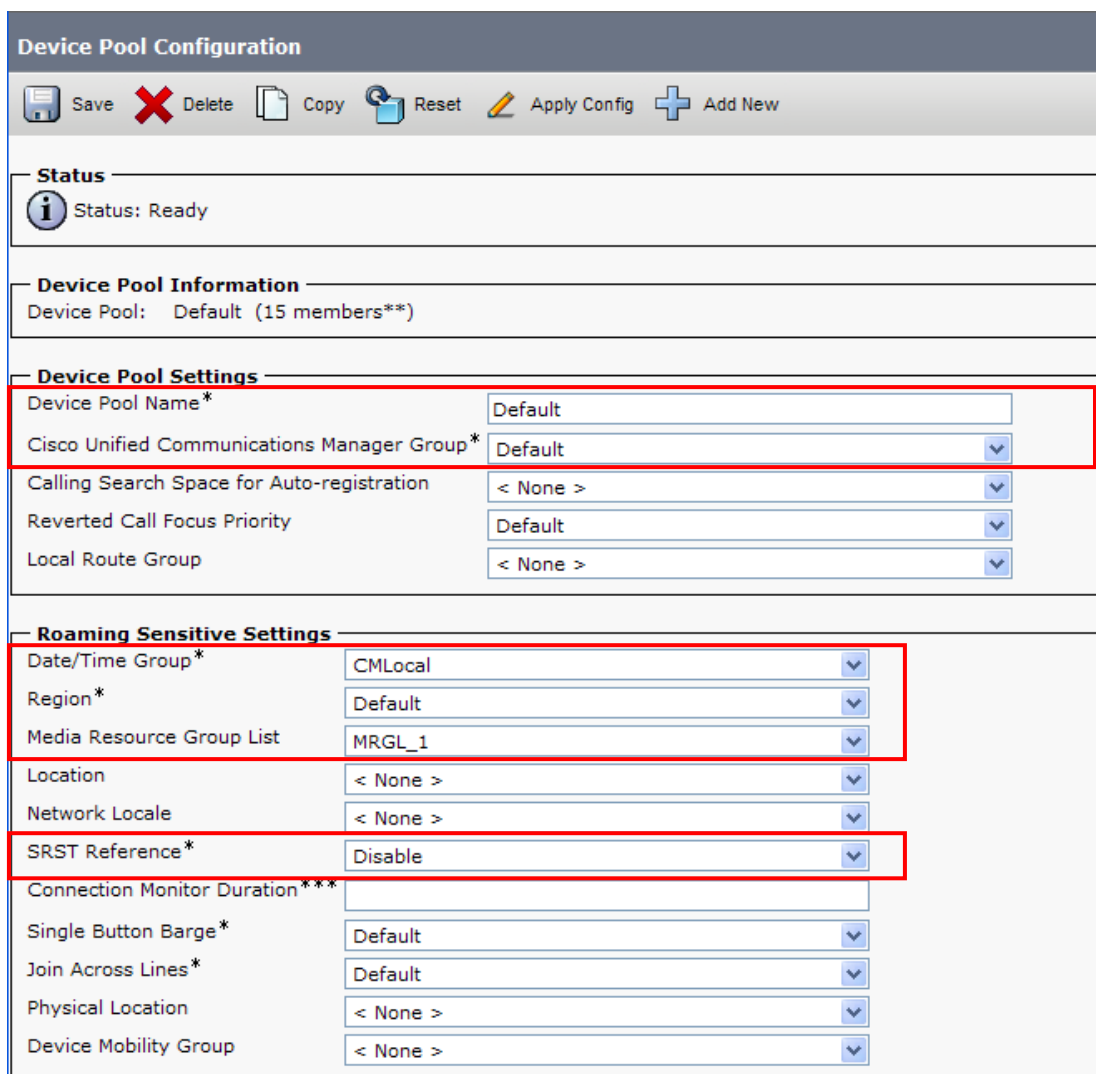
The screenshot displays the 'Media Resource Group List Configuration' interface. At the top, there is a header bar with the title and a toolbar containing 'Save', 'Delete', 'Copy', and 'Add New' buttons. Below the header, the 'Status' section shows 'Status: Ready'. The 'Media Resource Group List Status' section indicates 'Media Resource Group List: MRGL_1 (used by 15 devices)'. The 'Media Resource Group List Information' section has a 'Name*' field with 'MRGL_1' entered. The 'Media Resource Groups for this List' section is divided into two panes: 'Available Media Resource Groups' (empty) and 'Selected Media Resource Groups' (containing 'MRG_1'). A red rectangle highlights the 'Selected Media Resource Groups' pane. Arrows between the panes allow for moving items. At the bottom, there is another toolbar with 'Save', 'Delete', 'Copy', and 'Add New' buttons.

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.






The screenshot displays the 'Device Pool Configuration' interface. At the top, there is a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. Below the toolbar, the 'Status' section shows 'Status: Ready'. The 'Device Pool Information' section indicates 'Device Pool: Default (15 members**)'. The 'Device Pool Settings' section is highlighted with a red box and contains the following fields: 'Device Pool Name*' (Default), 'Cisco Unified Communications Manager Group*' (Default), 'Calling Search Space for Auto-registration' (< None >), 'Reverted Call Focus Priority' (Default), and 'Local Route Group' (< None >). The 'Roaming Sensitive Settings' section is also highlighted with a red box and contains: 'Date/Time Group*' (CMLocal), 'Region*' (Default), 'Media Resource Group List' (MRGL_1), 'Location' (< None >), 'Network Locale' (< None >), 'SRST Reference*' (Disable), 'Connection Monitor Duration***' (empty), 'Single Button Barge*' (Default), 'Join Across Lines*' (Default), 'Physical Location' (< None >), and 'Device Mobility Group' (< None >).

Device Pool Configuration	
Status Status: Ready	
Device Pool Information Device Pool: Default (15 members**)	
Device Pool Settings	
Device Pool Name*	Default
Cisco Unified Communications Manager Group*	Default
Calling Search Space for Auto-registration	< None >
Reverted Call Focus Priority	Default
Local Route Group	< None >
Roaming Sensitive Settings	
Date/Time Group*	CMLocal
Region*	Default
Media Resource Group List	MRGL_1
Location	< None >
Network Locale	< None >
SRST Reference*	Disable
Connection Monitor Duration***	
Single Button Barge*	Default
Join Across Lines*	Default
Physical Location	< None >
Device Mobility Group	< None >

5.4. Define SIP Trunk Security Profile







Expand **System** → **Security Profile** and select **SIP Trunk Security Profile**. Click  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 . The screen below shows SIP Trunk Security Profile for the sample configuration

SIP Trunk Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

Status
 Status: Ready

SIP Trunk Security Profile Information

Name*	Avaya SIP Trunk
Description	Avaya SIP Trunk Security Profile
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP

☐ Enable Digest Authentication

Nonce Validity Time (mins)*

X.509 Subject Name

Incoming Port*

☐ Enable Application Level Authorization

☐ Accept Presence Subscription

☒ Accept Out-of-Dialog REFER

☒ Accept Unsolicited Notification


☒ Accept Replaces Header

☐ Transmit Security Status

5.5. Define SIP Profile

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

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

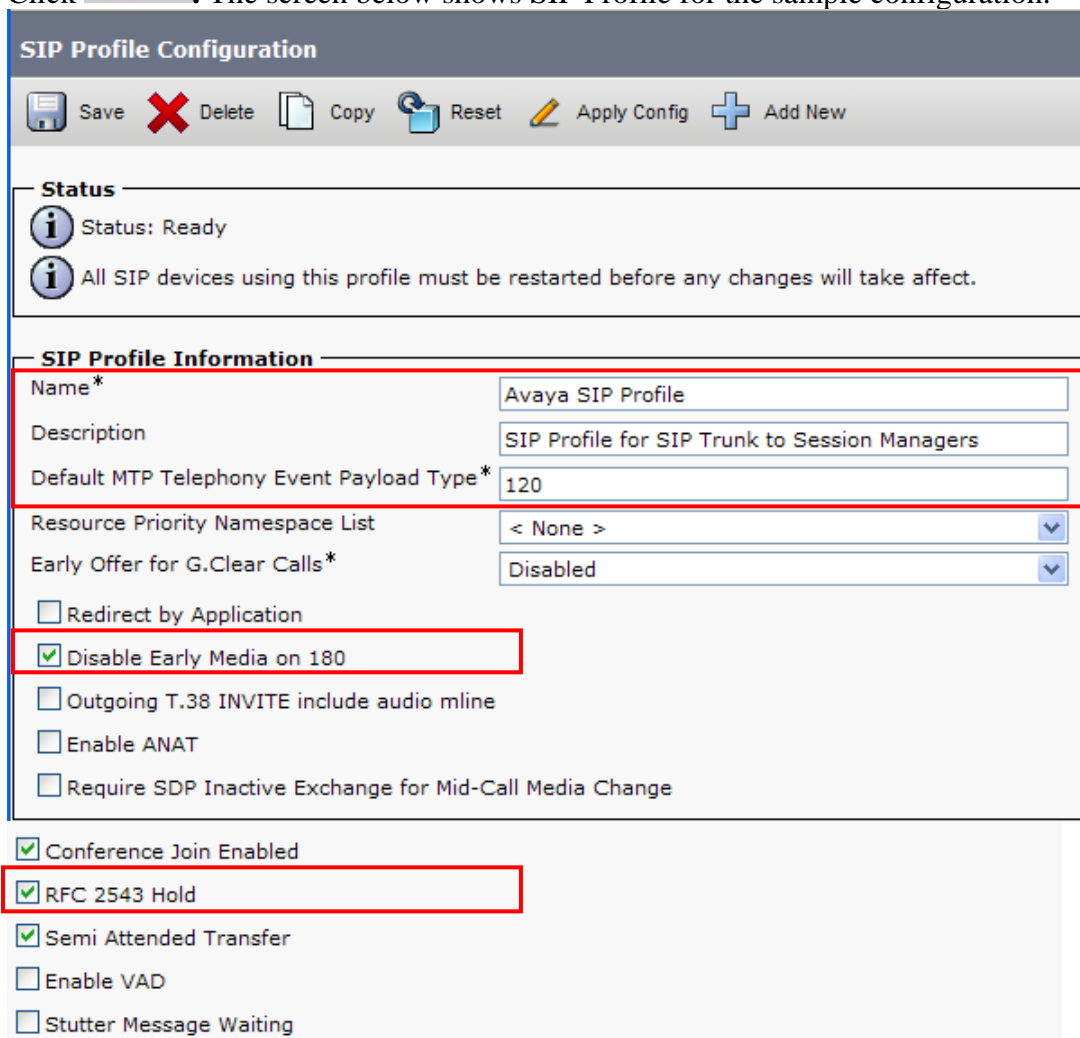
- **Name** Enter name
- **Description** Enter a brief description
- **Default MTP Telephony Event Payload Type** Enter “120”
- **Disable Early Media on 180** Enter 

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 . The screen below shows SIP Profile for the sample configuration.

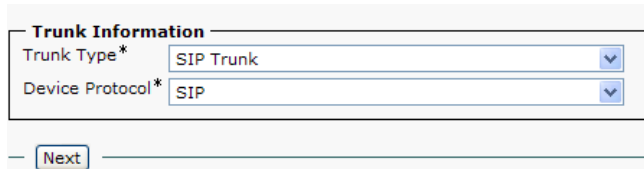


5.6. Define SIP Trunk to Avaya Aura® Session Manager

Expand **Device** select **Trunk**. Click  to define a SIP Trunk to Session Manager.


Under **Trunk Information** section, enter the following values as shown below and click **Next**.

- **Trunk Type** Select “**SIP Trunk**”
- **Device Protocol** Select “**SIP**”



The screenshot shows a web form titled "Trunk Information". It contains two dropdown menus: "Trunk Type*" with "SIP Trunk" selected, and "Device Protocol*" with "SIP" selected. Below the form is a "Next" button.

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.

SIP Information

Destination Address	10.80.111.107
Destination Address IPv6	
<input type="checkbox"/> Destination Address is an SRV	
Destination Port*	5060
MTP Preferred Originating Codec*	711ulaw
Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Avaya SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Avaya SIP Profile
DTMF Signaling Method*	RFC 2833


Geolocation Configuration



Geolocation	< None >
Geolocation Filter	< None >
<input type="checkbox"/> Send Geolocation Information	


Save Delete Reset Add New

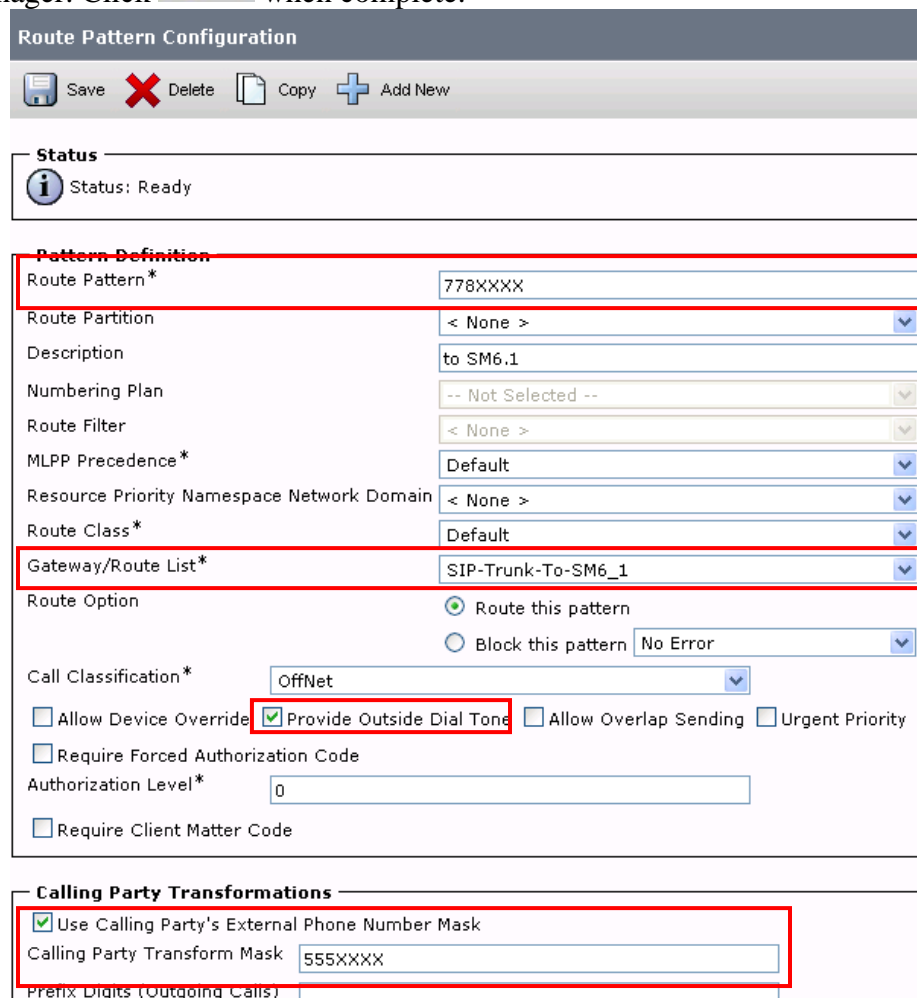
5.7. Define Routing Pattern

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

Click  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  when complete.



The screenshot displays the 'Route Pattern Configuration' window. At the top, there is a toolbar with 'Save', 'Delete', 'Copy', and 'Add New' buttons. Below this is a 'Status' section showing 'Status: Ready'. The main configuration area is titled 'Pattern Definition' and contains several fields: 'Route Pattern*' (778XXXX), 'Route Partition' (< None >), 'Description' (to SM6.1), 'Numbering Plan' (-- Not Selected --), 'Route Filter' (< None >), 'MLPP Precedence*' (Default), 'Resource Priority Namespace Network Domain' (< None >), 'Route Class*' (Default), 'Gateway/Route List*' (SIP-Trunk-To-SM6_1), 'Route Option' (Route this pattern), 'Call Classification*' (OffNet), 'Allow Device Override' (unchecked), 'Provide Outside Dial Tone' (checked), 'Allow Overlap Sending' (unchecked), 'Urgent Priority' (unchecked), 'Require Forced Authorization Code' (unchecked), 'Authorization Level*' (0), and 'Require Client Matter Code' (unchecked). Below the 'Pattern Definition' section is the 'Calling Party Transformations' section, which includes 'Use Calling Party's External Phone Number Mask' (checked) and 'Calling Party Transform Mask' (555XXXX). The 'Prefix Digits (Outgoing Calls)' field is empty.

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.

Managing: 192.168.50.71 Username: admin
System » Maintenance

Maintenance

☒ Select by Overlay ☐ Select by Functionality

<Select by Overlay>

- LD 30 - Network and Signaling
- LD 32 - Network and Peripheral Equipment
- LD 34 - Tone and Digit Switch
- LD 36 - Trunk
- LD 37 - Input/Output
- LD 38 - Conference Circuit
- LD 39 - Intergroup Switch and System Clock
- LD 45 - Background Signaling and Switching
- LD 46 - Multifrequency Sender
- LD 48 - Link
- LD 54 - Multifrequency Signaling
- LD 60 - Digital Trunk Interface and Primary Rate Interface
- LD 75 - Digital Trunk
- LD 80 - Call Trace
- LD 96 - D-Channel**
- LD 117 - Ethernet and Alarm Management
- LD 135 - Core Common Equipment
- LD 137 - Core Input/Output
- LD 143 - Centralized Software Upgrade

<Select Group>

- D-Channel Diagnostics**
- MSDL Diagnostics
- TMDI Diagnostics

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**”

D-Channel Diagnostics

Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH)		Submit
Disable Automatic Recovery (DIS AUTO)	<input type="checkbox"/> ALL	Submit
Enable Automatic Recovery (ENL AUTO)	<input type="checkbox"/> FDL	Submit
Test Interrupt Generation (TEST 100)		Submit
Establish D-Channel (EST DCH)		Submit

DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_RECV	PDCH	BDCH
015	VTRKNode71	OPER	EST ACTV	AUTO		

STAT DCH 015

Command executed successfully.

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**”.

Diagnostic Commands	Command Parameters	Action
TRAC - List Route, type and status of trunks for a Customer	(cust# acod#)	<input type="checkbox"/> DEV <input type="button" value="Submit"/>
TRAD - Trace DTI/DLI calls on a channel of a loop	(loop# ch#)	<input type="button" value="Submit"/>
TRAT - Trace calls for an attendant of a customer	(cust# atnd#)	<input type="checkbox"/> DEV <input type="button" value="Submit"/>
TRIP - Trace Calls for IP Phone	10.80.50.35 (IP Address)	<input type="button" value="Submit"/>

TRIP - Trace Calls for IP Phone 10.80.50.35

VTN 044 0 00 09

KEY 0 SCR MARP ACTIVE VTN 044 0 00 09

ORIG VTN 044 0 00 09 KEY 0 SCR MARP CUST 0 DN 7785014 TYPE 1140

SIGNALLING ENCRYPTION: INSEC

MEDIA ENDPOINT IP: 10.80.50.35 PORT: 5200

TERM VTN 096 0 00 15 VTRK IPTI RMBR 15 16 OUTGOING VOIP GW CALL

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.

```
FAR-END SIP SIGNALLING IP: 192.45.130.100

FAR-END MEDIA ENDPOINT IP: 192.45.130.100 PORT: 27598

FAR-END VendorID: AVAYA-SM-6.1.0.0.610023

MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 5558006
MAIN PM ESID
TALKSLOT ORIG 4 TERM 9 JUNCTOR ORIGO TERMO
```

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** 
- **Service State** 

[Home](#) / [Elements](#) / [Session Manager](#) / [Dashboard- Dashboard](#)

[Help ?](#)

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State ▾

Shutdown System ▾

As of 2:38 PM

2 Items | Refresh | Show ALL ▾ Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
<input type="checkbox"/>	ASM1	Core	1/0/15	✓	Up	Accept New Service	1/7	0	0	6.1.0.0.610023

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.


Reset

Synchronize

Update Installed Certificates

Connection Status

2 Items | Refresh | Show ALL ▾ Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)
	Show	ASM1	SM	Up	12	10.80.111.107/24	---	10.80.111.1	Disabled	7/7

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

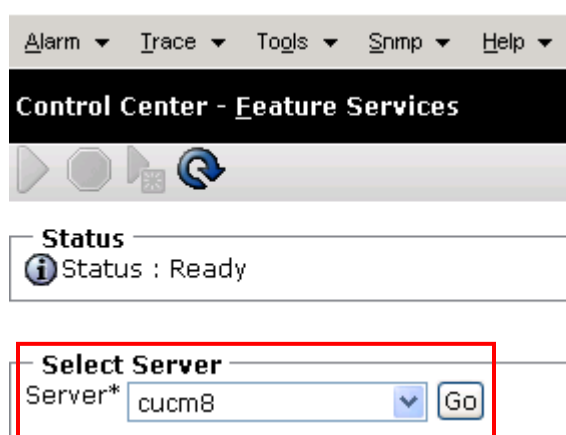
6.3. Verify Cisco Unified Communications Manager Operational Status

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.



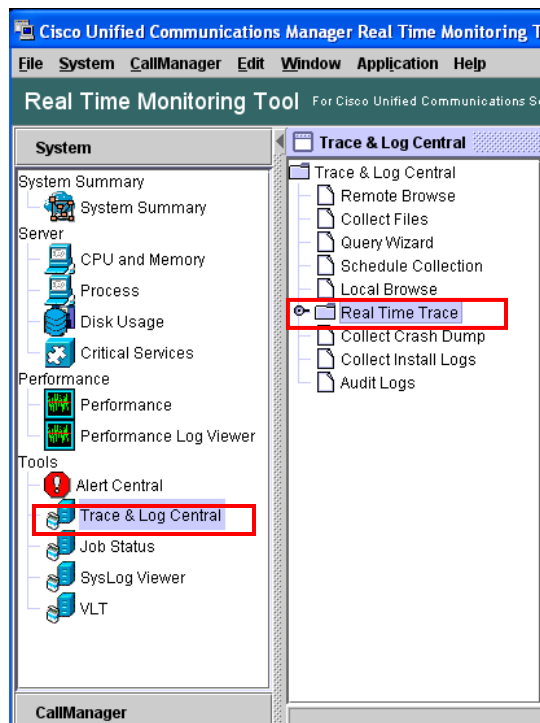
Under **CM Services** section, verify the status of the **Cisco CallManager** and **Cisco IP Voice Media Streaming** services as shown below. Verify the following fields:

- **Status** Verify status is “**Started**”
- **Activation Status** Verify status is “**Activated**”

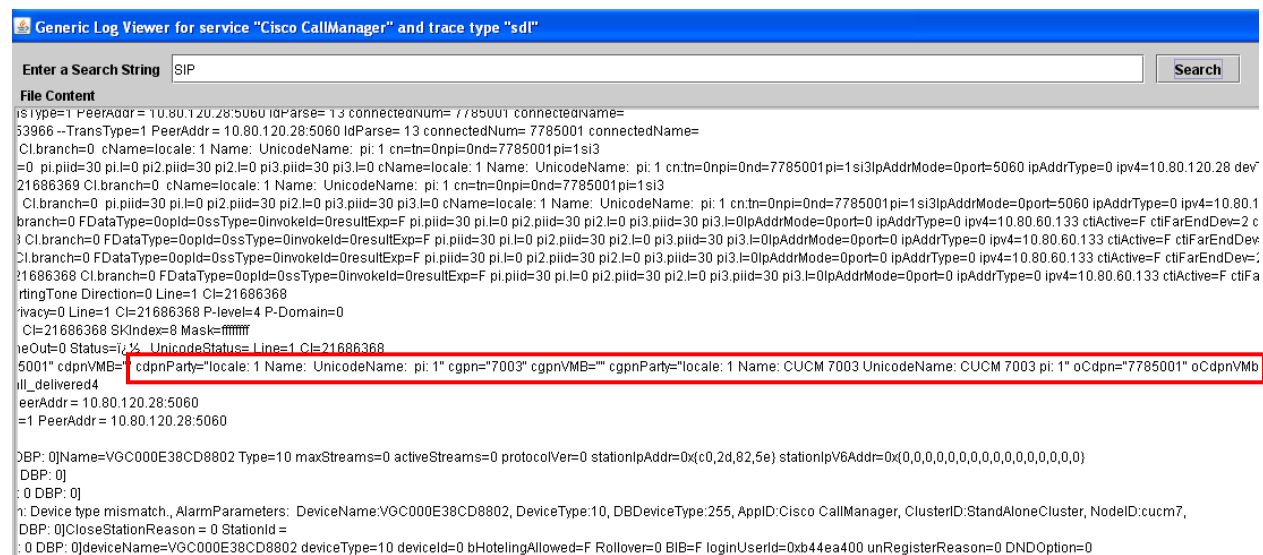
CM Services					
	Service Name	Status	Activation Status	Start Time	Up Time
<input checked="" type="radio"/>	Cisco CallManager	Started	Activated	Mon Jan 3 08:40:46 2011	0 days 05:02:47
<input checked="" type="radio"/>	Cisco Tftp	Started	Activated	Mon Jan 3 08:40:47 2011	0 days 05:02:46
<input checked="" type="radio"/>	Cisco Messaging Interface	Not Running	Activated		
<input checked="" type="radio"/>	Cisco Unified Mobile Voice Access Service	Started	Activated	Mon Jan 3 08:41:08 2011	0 days 05:02:25
<input checked="" type="radio"/>	Cisco IP Voice Media Streaming App	Started	Activated	Mon Jan 3 08:40:49 2011	0 days 05:02:44
<input checked="" type="radio"/>	Cisco CTIManager	Started	Activated	Mon Jan 3 08:40:50 2011	0 days 05:02:43
<input checked="" type="radio"/>	Cisco Extension Mobility	Started	Activated	Mon Jan 3 08:40:51 2011	0 days 05:02:42
<input checked="" type="radio"/>	Cisco Dialed Number Analyzer	Started	Activated	Mon Jan 3 08:41:05 2011	0 days 05:02:28
<input checked="" type="radio"/>	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>

©2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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