



Avaya Solution & Interoperability Test Lab

Sample Configuration for SIP Trunking between Avaya IP Office R7.0 and Cisco Unified Communications Manager 8.6.2 – Issue 1.0

Abstract

These Application Notes describe the steps for configuring a SIP trunk between Avaya IP Office R7.0 and Cisco Unified Communications Manager (CUCM) Release 8.6.2.

(This page left blank intentionally)

1. Introduction

Session Initiation Protocol (SIP) is a standards-based communication protocol capable of supporting voice, video, instant messaging and other multi-media communication. These Application Notes will outline a solution for using SIP as a trunking protocol between Avaya IP Office and Cisco Unified Communications Manager.

2. Overview

The sample network shown in **Figure 1** consists of two IP PBX systems each belonging to a different domain with its own dialing plan. The Avaya IP PBX system consists of Avaya IP Office system capable of supporting a variety of Avaya 1100 Series SIP Telephones, Avaya 1600 Series IP Telephones along with digital and analog phone/fax stations. The Cisco IP PBX system consists of Cisco Unified Communications Manager (CUCM) supporting Cisco SIP and SCCP stations along with analog fax station through the use of an optional Cisco VG248 gateway (not shown). A SIP trunk is configured between Avaya IP Office and CUCM to support calling between the Avaya and Cisco IP PBX systems. With the use of the SIP trunk trans-coding, media and protocol conversion, calls between any 2 telephones are supported in this sample network regardless of whether they are between SIP, H.323, digital, SCCP or analog stations.

3. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All IP telephones in the 192.45.2.0/24 IP network are registered with Avaya IP Office and use extension 2xx. All IP telephones in the 10.80.60.0/24 IP network are registered with CUCM and use extension 720-567-8xxx. A single SIP trunk was configured and connected between Avaya IP Office and CUCM. All inter-system calls are carried over this SIP trunk.

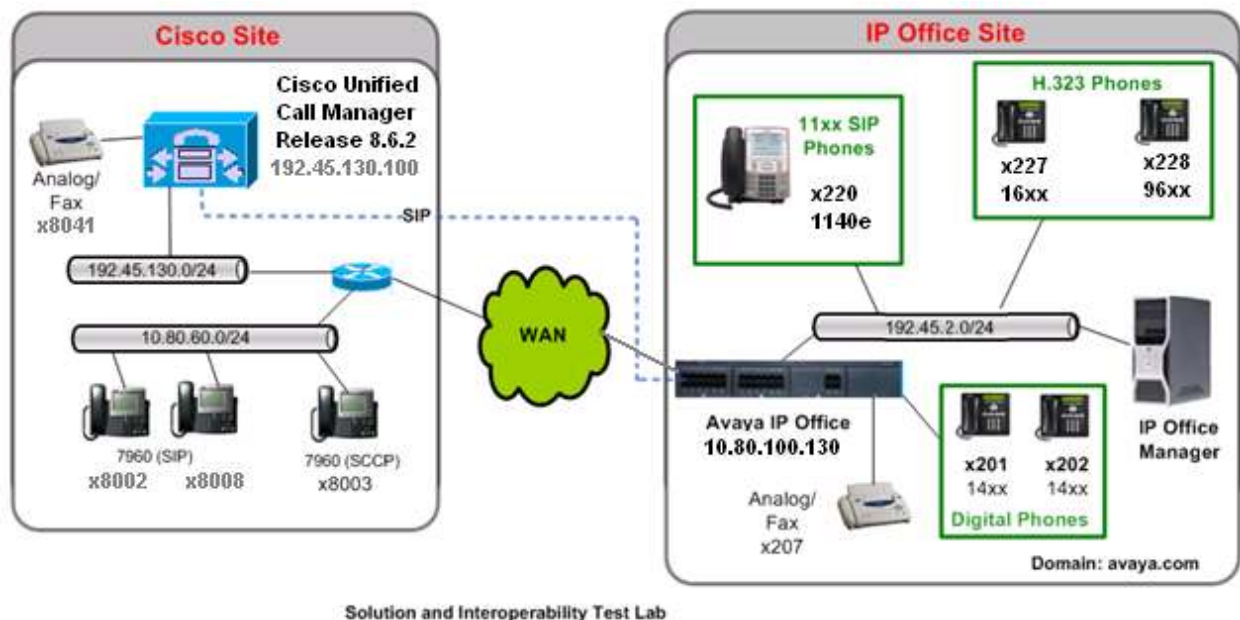


Figure 1: Sample Network Configuration

4. Equipment and Software Validated

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

DEVICE DESCRIPTION	VERSION TESTED
Avaya IP Office 500v2	7.0(232702)
Avaya IP Office Manager	9.0(5)
Avaya 1618 IP Telephone (H323)	1.30
Avaya 9630G IP Telephone (H323)	3.186a
Avaya 1408 Digital Telephone	n/a
Avaya 1140eSIP	04.01.13.00
Cisco Unified Communications Manager	8.6.2.20000-2
Cisco 7975 Unified IP Phone (SIP)	75.9-2-1S
Cisco 7965 Unified IP Phone (SCCP)	45.9-2-1S

5. Configure Cisco Unified CM

This section describes the SIP Trunk configuration for CUCM as shown in **Figure 1**. Fields left using default values are not highlighted. It is assumed that the basic configuration needed to support the VG248 gateway (needed for analog phone and fax support) and support for Cisco IP telephones has been completed. For further information on CUCM, please consult **Section 10**, References [3]-[7].

5.1. Login to Cisco Unified CM Administration

Open Cisco Unified CM Administration by entering the IP address of the CUCM into the Web Browser address field, and log in using an appropriate Username and Password.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

Cisco Unified CM Administration

Username:

Password:

Login Reset

Copyright © 1999 - 2011 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.


5.2. Add a SIP Trunk Security Profile

Select **System** → **Security Profile** → **SIP Trunk Security Profile** from the top menu then click **Add New** to add a new SIP Trunk Security Profile.

The screenshot shows the Cisco Unified CM Administration web interface. The top navigation bar includes the Cisco logo, the title 'Cisco Unified CM Administration For Cisco Unified Communications Solutions', and a user login 'ccmadministrator'. Below the navigation bar is a menu with options: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled 'Find and List SIP Trunk Security Profiles'. It features a search bar with a dropdown menu for 'Name' and a 'Find' button. Below the search bar, there is a message: 'No active query. Please enter your search criteria using the options above.' At the bottom of the page, the 'Add New' button is highlighted with a red rectangular box.

The following is a screen capture of the SIP Trunk Security Profile used in the sample network. The following values were used in the sample configuration:

- Name A descriptive name for the profile
 - Device Security Mode “**Non Secure**” indicates unencrypted SIP signaling
 - Incoming Transport Type “**TCP+UDP**” indicates CUCM will listen for both protocols
 - Outgoing Transport Type “**TCP**” indicates CUCM will only use TCP to initiate SIP signaling
 - Incoming Port “**5060**”. Typical value for UDP and TCP SIP Signaling
-
- Accept Presence Subscription Enable
 - Accept Out-of-Dialog REFER ** Enable
 - Accept Unsolicited Notification Enable
 - Accept Replaces Header Enable


**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Admini

ccmadministrator | Search Documentation | Ab

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Admin

SIP Trunk Security Profile Configuration Related Links: Back To Find/List ▾

 Save

SIP Trunk Security Profile Information

Name* SIP Trunk to IPO 7.0

Description

Device Security Mode Non Secure ▾

Incoming Transport Type* TCP+UDP ▾

Outgoing Transport Type TCP ▾

☐ Enable Digest Authentication

Nonce Validity Time (mins)* 600

X.509 Subject Name

Incoming Port* 5060

☐ Enable Application level authorization

☒ Accept presence subscription

☒ Accept out-of-dialog refer**


☒ Accept unsolicited notification

☒ Accept replaces header

☐ Transmit security status

☐ Allow charging header

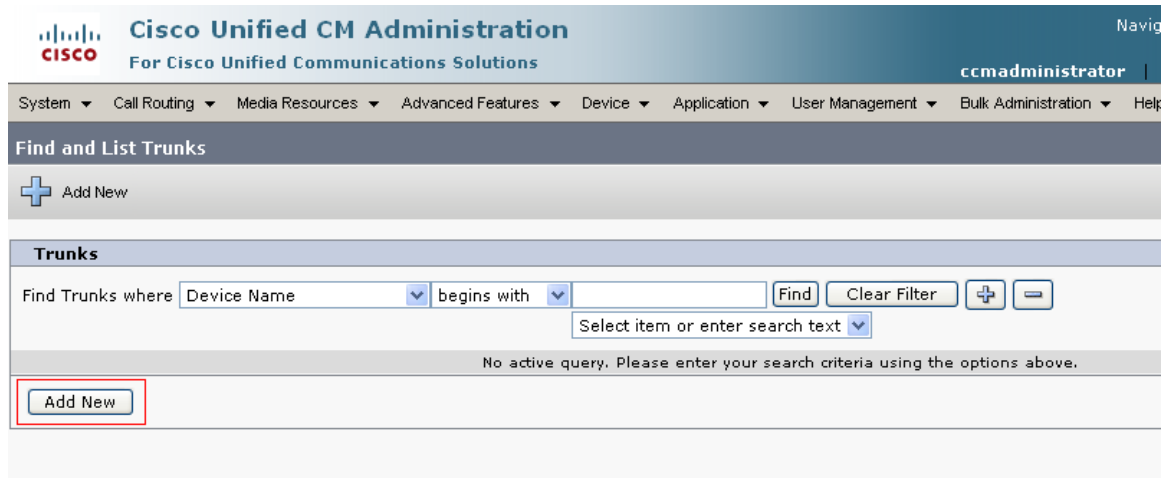
SIP V.150 Outbound SDP Offer Filtering* Use Default Filter ▾

 Save

Click **Save** to commit the configuration.

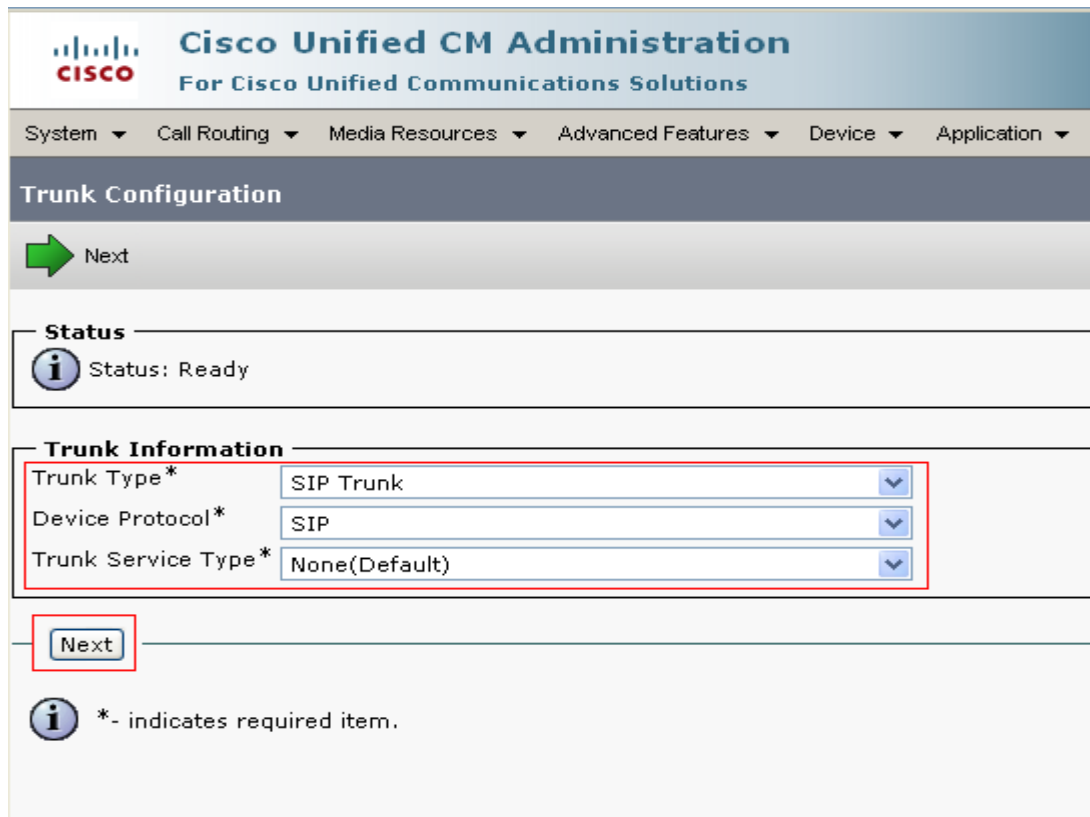
5.3. Create a SIP Trunk

Select **Device** → **Trunk** from the top menu then click **Add New** to begin adding a new SIP trunk.



The screenshot shows the 'Find and List Trunks' page in the Cisco Unified CM Administration interface. The top navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'Device' menu is expanded, showing 'Trunk'. The 'Add New' button is highlighted with a red box. Below the 'Add New' button, there is a search section with a dropdown menu for 'Device Name' and a 'Find' button. A message at the bottom states: 'No active query. Please enter your search criteria using the options above.'

Select **SIP Trunk** as the **Trunk Type** and the **Device Protocol** field will automatically change to **SIP**. Click **Next** to continue.



The screenshot shows the 'Trunk Configuration' page in the Cisco Unified CM Administration interface. The top navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', and 'Application'. The 'Device' menu is expanded, showing 'Trunk'. The 'Next' button is highlighted with a green arrow. Below the 'Next' button, there is a 'Status' section showing 'Status: Ready'. The 'Trunk Information' section contains three dropdown menus: 'Trunk Type*' (SIP Trunk), 'Device Protocol*' (SIP), and 'Trunk Service Type*' (None(Default)). The 'Next' button is highlighted with a red box. A message at the bottom states: '*- indicates required item.'

Enter the following information for the SIP Trunk.

- **Device Name** A descriptive name/identifier for the SIP Trunk.
(Make sure there are no spaces in the device name).
- **Description** Additional descriptive information about the SIP Trunk
- **Device Pool** Select **Default**
- **Media Termination Point Required** This will cause CUCM to include SDP information in its initial SIP Invite message.

The screenshot displays the Cisco Unified CM Administration web interface. The top navigation bar includes the Cisco logo, the title 'Cisco Unified CM Administration', and the subtitle 'For Cisco Unified Communications Solutions'. The user is logged in as 'ccmadministrator'. The main menu shows various configuration categories like System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The 'Trunk Configuration' section is active, showing a list of actions: Save, Delete, Reset, and Add New. The 'Device Information' section is expanded, showing the following configuration details:

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	SIP_to_IPO_7.0
Description	Direct SIP Trunk to IPO 7.0
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	MRGL_1
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	None
Packet Capture Duration	0
<input checked="" type="checkbox"/> Media Termination Point Required	
<input checked="" type="checkbox"/> Retry Video Call as Audio	
<input type="checkbox"/> Path Replacement Support	
<input type="checkbox"/> Transmit UTF-8 for Calling Party Name	
<input type="checkbox"/> Transmit UTF-8 Names in QSIG APDU	
<input type="checkbox"/> Unattended Port	
<input type="checkbox"/> SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so information.	
Consider Traffic on This Trunk Secure*	When using both sRTP and TLS
Route Class Signaling Enabled*	Default
Use Trusted Relay Point*	Default
<input checked="" type="checkbox"/> PSTN Access	
<input type="checkbox"/> Run On All Active Unified CM Nodes	

Scroll down to the section titled **SIP Information** and fill in the fields as indicated below.

- **Destination Address** IP Address of IP Office
- **Destination Port** Port 5060 is typically used for TCP and UDP SIP signaling
- **SIP Trunk Security Profile** Use the Security Profile defined in **Section 5.2**
- **DTMF Signaling Method** Select **RFC2833**.

SIP Information

Destination

☐ Destination Address is an SRV

Destination Address: 1 * 10.80.100.130

Destination Address IPv6:

Destination Port: 5060

MTP Preferred Originating Codec*: 711ulaw

Presence Group*: Standard Presence group

SIP Trunk Security Profile*: SIP Trunk to IPO 7.0

Rerouting Calling Search Space: < None >

Out-Of-Dialog Refer Calling Search Space: < None >

SUBSCRIBE Calling Search Space: < None >

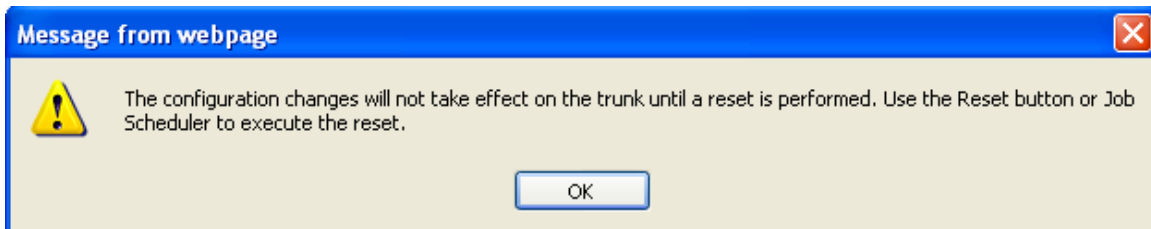
SIP Profile*: Standard SIP Profile

DTMF Signaling Method*: RFC 2833

Save

Click **Save** to complete.

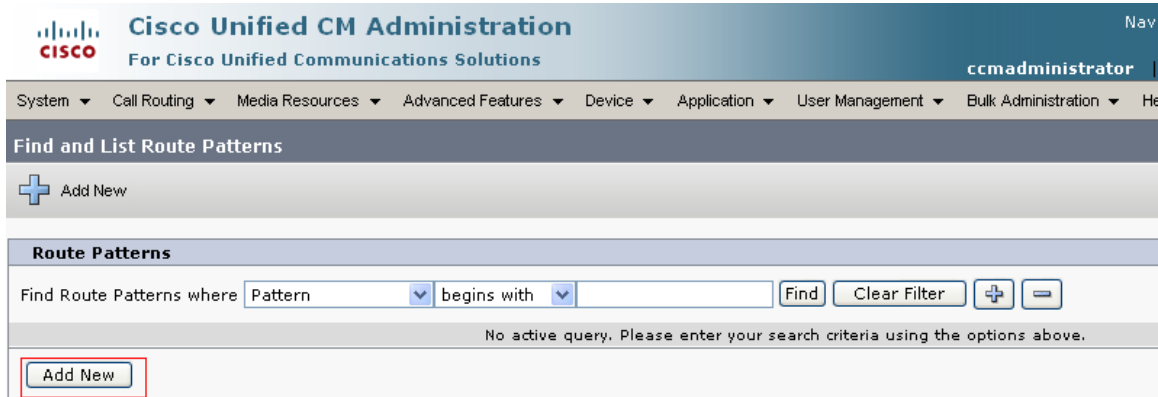
Following screen will appear and click **OK**.



Follow the instructions from **Section 10**, Reference 5 and perform a reset for the Cisco Call Manager.

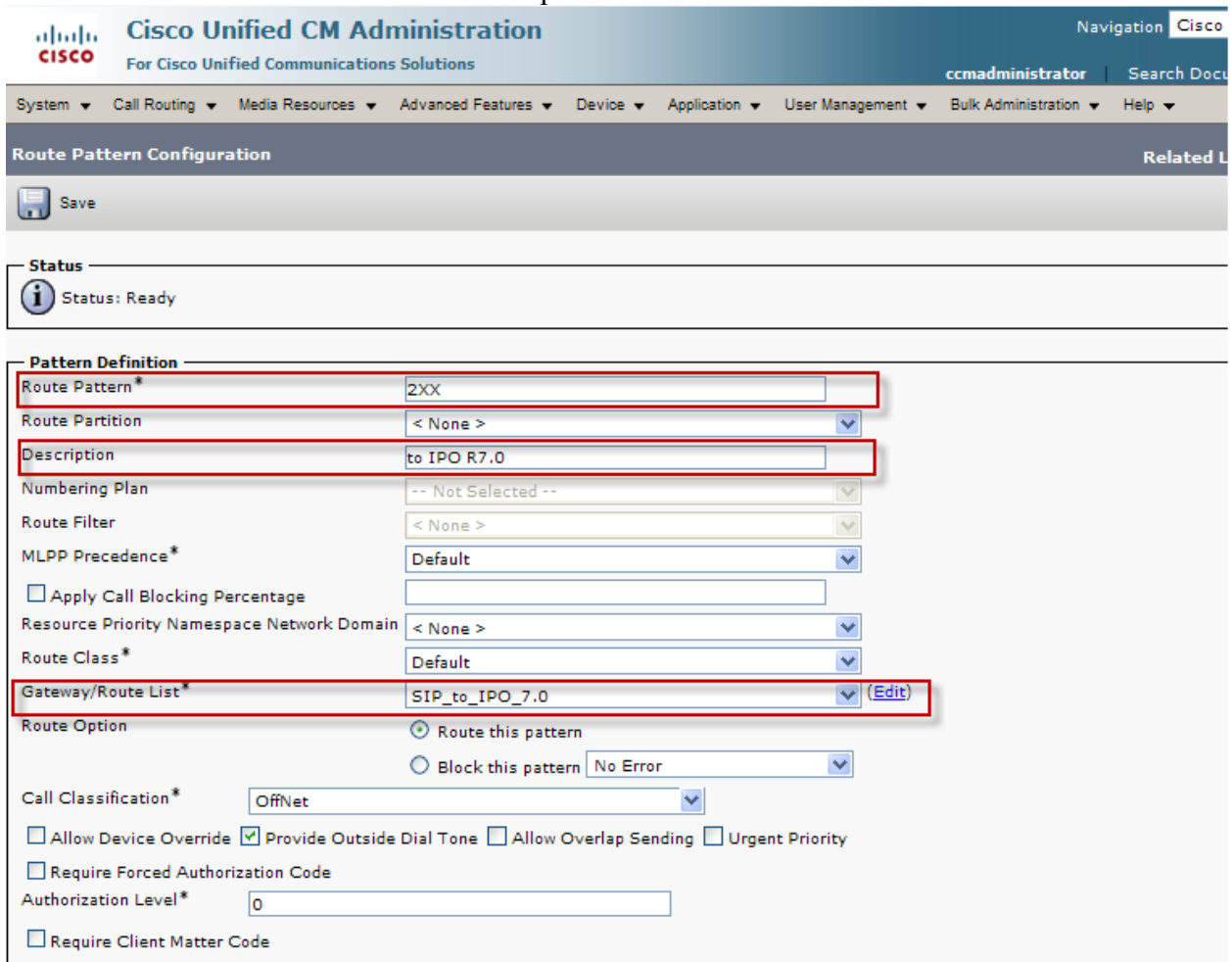
Create a Route Pattern

Select **Call Routing** → **Route/Hunt** → **Route Pattern** then click **Add New** to add a new route pattern for extension **2xx** which are for telephones registered with Avaya IP Office.



The screenshot shows the 'Find and List Route Patterns' page in the Cisco Unified CM Administration interface. The page has a header with the Cisco logo and 'Cisco Unified CM Administration' title. Below the header is a navigation bar with tabs: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The 'Call Routing' tab is selected. The main content area has a 'Find and List Route Patterns' section with a search bar and an 'Add New' button. The search bar contains the text 'Find Route Patterns where Pattern begins with' and a 'Find' button. Below the search bar is a message: 'No active query. Please enter your search criteria using the options above.' The 'Add New' button is highlighted with a red box.

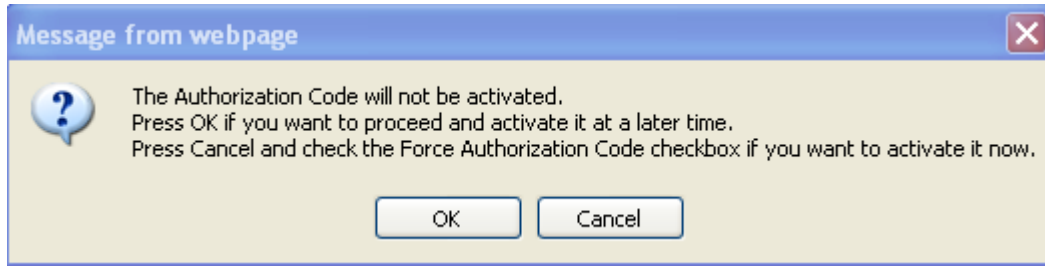
The following screen shows the route pattern used in the sample network. The route pattern **2xx** will cause all 3-digit calls beginning with “2” to be routed to the SIP Trunk defined in **Section 5.3**. Click **Save** to complete.



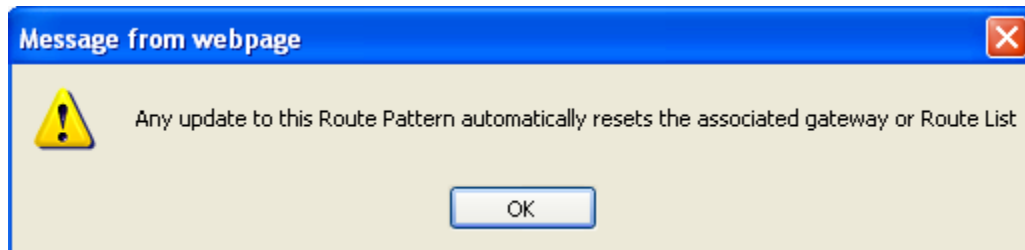
The screenshot shows the 'Route Pattern Configuration' page in the Cisco Unified CM Administration interface. The page has a header with the Cisco logo and 'Cisco Unified CM Administration' title. Below the header is a navigation bar with tabs: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The 'Call Routing' tab is selected. The main content area has a 'Route Pattern Configuration' section with a 'Save' button. Below the 'Save' button is a 'Status' section showing 'Status: Ready'. The 'Pattern Definition' section contains the following fields:

- Route Pattern*: 2XX
- Route Partition: < None >
- Description: to IPO R7.0
- Numbering Plan: -- Not Selected --
- Route Filter: < None >
- MLPP Precedence*: Default
- ☐ Apply Call Blocking Percentage
- Resource Priority Namespace Network Domain: < None >
- Route Class*: Default
- Gateway/Route List*: SIP_to_IPO_7.0 (Edit)
- Route Option: ☒ Route this pattern, ☐ Block this pattern No Error
- Call Classification*: OffNet
- ☐ Allow Device Override, ☒ Provide Outside Dial Tone, ☐ Allow Overlap Sending, ☐ Urgent Priority
- ☐ Require Forced Authorization Code
- Authorization Level*: 0
- ☐ Require Client Matter Code

Following screen will appear and click **OK**.



Following screen will appear and click **OK**.

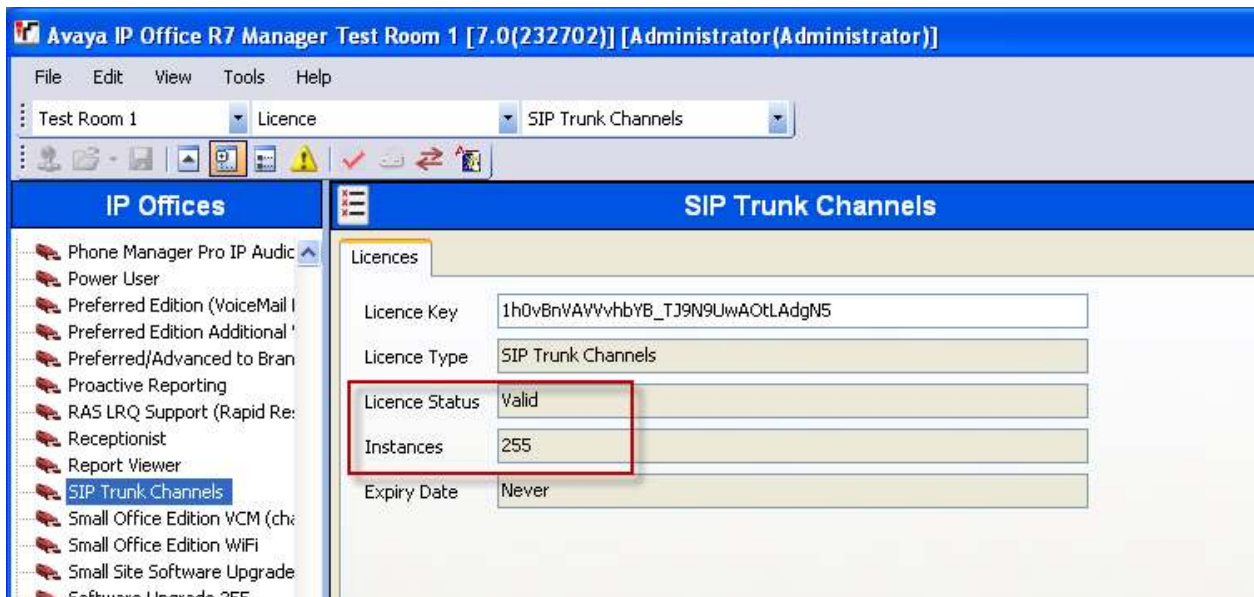


6. Configure Avaya IP Office

This section describes the SIP Trunk configuration for Avaya IP Office as shown in **Figure 1**. It is assumed that the basic configuration has been completed and Avaya IP Office is accessible from the network. Begin by connecting to the Avaya IP Office using the Avaya IP Office Manager and log in using an appropriate User name and Password. Fields that need to be configured are highlighted, all other fields are left with their default value. For further information on Avaya IP Office, please consult **Section 10: Reference [1]**.

6.1. Verify SIP License

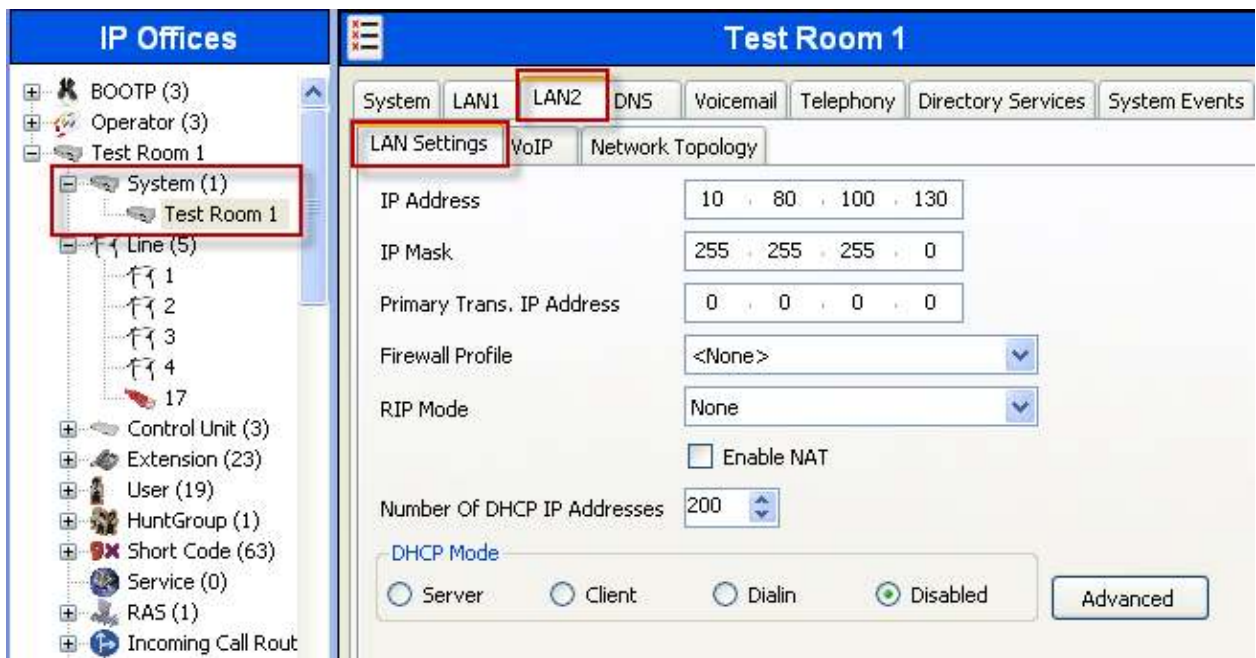
Select **License → SIP Trunk Channels** from the left panel menu and verify that there is a valid **SIP Trunk Channel** license and the quantity. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.



6.2. Obtain LAN2 IP Address

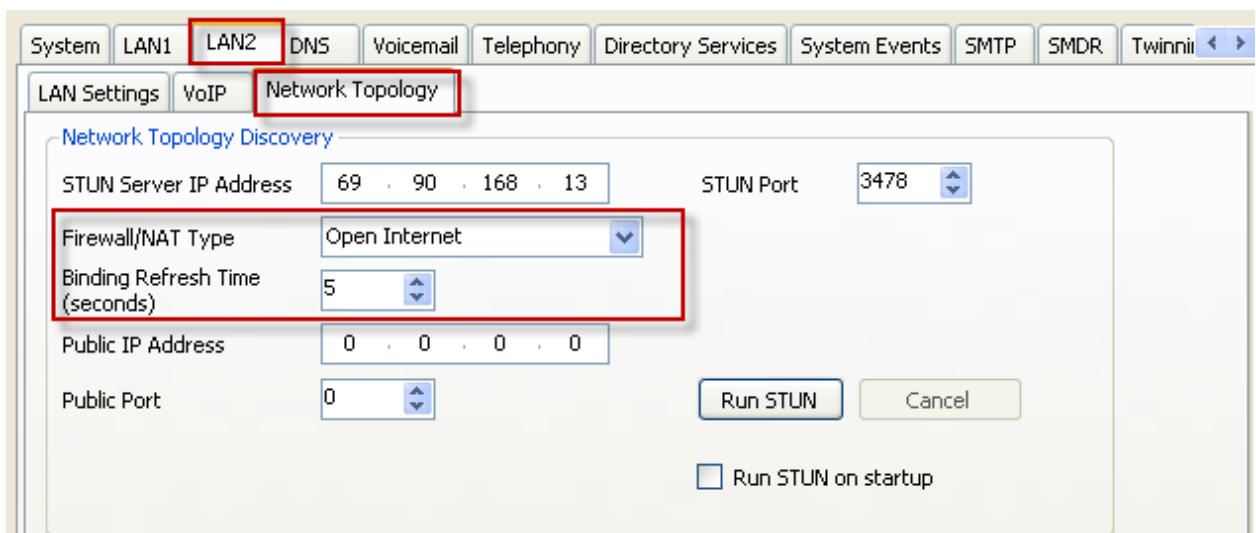
From the configuration tree in the left pane, select **System** to display the **IPO500V2** screen in the right pane. Select the **LAN2** tab, followed by the **LAN Settings** sub-tab in the right pane. This **IP Address** is used in **Section 5.3** to configure SIP Trunks.

Note: The **LAN1** IP Address is used for the LAN port of the IP Office control unit. The **LAN1** interface was used to connect the Avaya IP Office to the enterprise site IP network. The LAN1 interface configuration is not directly relevant to the interface with the Cisco Call Manager, and therefore it is not described in these Application Notes.



6.3. Configure Network Topology

From the configuration tree in the left pane, select **System** to display the **IPO500V2** screen in the right pane. Select the **LAN2** tab, followed by the **Network Topology** sub-tab in the right pane. Configure **Firewall/NAT Type** to “Open Internet”. Configure **Binding Refresh Time** to “5”. Click **OK**.



6.4. Create a SIP Line

Select **Line** from the left panel menu and then right-click and select **New → SIP Line** to create an SIP line to CUCM.

In the **SIP Line** tab, enter the following

- ITSP Domain Name:** Enter the domain name. “avaya.com” was used in the sample configuration.
- Call Routing Method:** Select “To Header” from drop down menu

The screenshot shows the configuration page for a SIP Line. The left sidebar contains a tree view with categories like BOOTP, Operator, Test Room, System, Line, Control Unit, Extension, User, HuntGroup, Short Code, Service, RAS, Incoming Call Route, WanPort, Directory, and Time Profile. The 'Line' category is expanded, showing lines 1 through 17. The main configuration area has several tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax, and SIP Credentials. The 'SIP Line' tab is selected. It contains various input fields and checkboxes. A red box highlights the 'Line Number' (17) and 'ITSP Domain Name' (avaya.com) fields. Another red box highlights the 'Call Routing Method' dropdown menu, which is set to 'To Header'. Other fields include Prefix, National Prefix (0), Country Code, International Prefix (00), Send Caller ID (None), Association Method (By Source IP address), In Service (checked), Use Tel URI (unchecked), Check OOS (checked), and Originator number for forwarded and twinning calls. There is also a section for REFER Support with Incoming and Outgoing protocols set to Auto.

In the **Transport** tab, enter the following

- ITSP Proxy Address:** Enter the IP address of CUCM. “192.45.130.100” was used in the sample configuration. (Administrative screens is not shown)
- Layer 4 Protocol:** Select “TCP” from drop down menu
- Send Port:** Select “5060” from drop down menu
- Use Network Topology Info:** Select the LAN port from **Section 6.2**

SIP Line **Transport** SIP URI VoIP T38 Fax SIP Credentials

ITSP Proxy Address 192.45.130.100

Network Configuration

Layer 4 Protocol TCP Send Port 5060

Use Network Topology Info LAN 2 Listen Port 5060

Explicit DNS Server(s) 205 . 171 . 3 . 65 205 . 171 . 2 . 65

Calls Route via Registrar ☒

Separate Registrar

In the **SIP URI** tab, select **Add** button and enter the following:

- **Local URI:** Select "Use Internal Data" from drop down menu
- **Contact:** Select "Use Internal Data" from drop down menu
- **Display Name:** Select "Use Internal Data" from drop down menu
- **Incoming Group:** Enter the line number created above
- **Outgoing Group:** Enter the line number created above

Select the **OK** button when done.

SIP Line Transport **SIP URI** VoIP T38 Fax SIP Credentials

Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	17 17	1...	*	*	*	*	0: <Non...	10
2	17 17	1...				N...	0: <Non...	10

Add... Remove Edit...

New Channel

Via 10.80.100.130

Local URI Use Internal Data

Contact Use Internal Data

Display Name Use Internal Data

PAI None

Registration 0: <None>

Incoming Group 17

Outgoing Group 17

Max Calls per Channel 10

OK Cancel

In the **VoIP** tab:

- Select **Automatic Select** for **Compression Mode**.
- **DTMF Support** should be set for **RFC2833**.
- Select the **OK** button (not shown) at the bottom of the screen once all changes have been made.

SIP Line Transport SIP URI **VoIP** T38 Fax SIP Credentials

Compression Mode **Advanced** Automatic Select

Fax Transport Support None

Call Initiation Timeout (s) 4

DTMF Support RFC2833

☐ VoIP Silence Suppression
☒ Re-invite Supported
☐ Use Offerer's Preferred Codec
☐ Codec Lockdown

6.5. Create Outgoing Routing Entry for Calls to Cisco UCM

In the left pane, under **9NShort Codes**, by default there should be a short code for **9N** that routes calls to a default ARS group called **Main**. These Application Notes will use ARS to route call to CUCM. The screen capture below shows the default **9N** Short Code.

IP Offices

- *92N;
- *97
- *98
- *99*N#
- *DSSN
- *SDN
- *SKN
- 1303XXXXXX
- 303XXXXXX
- 6N;
- 9N;**
- Service (0)

9N;; Dial*

Short Code

Code 9N;

Feature Dial

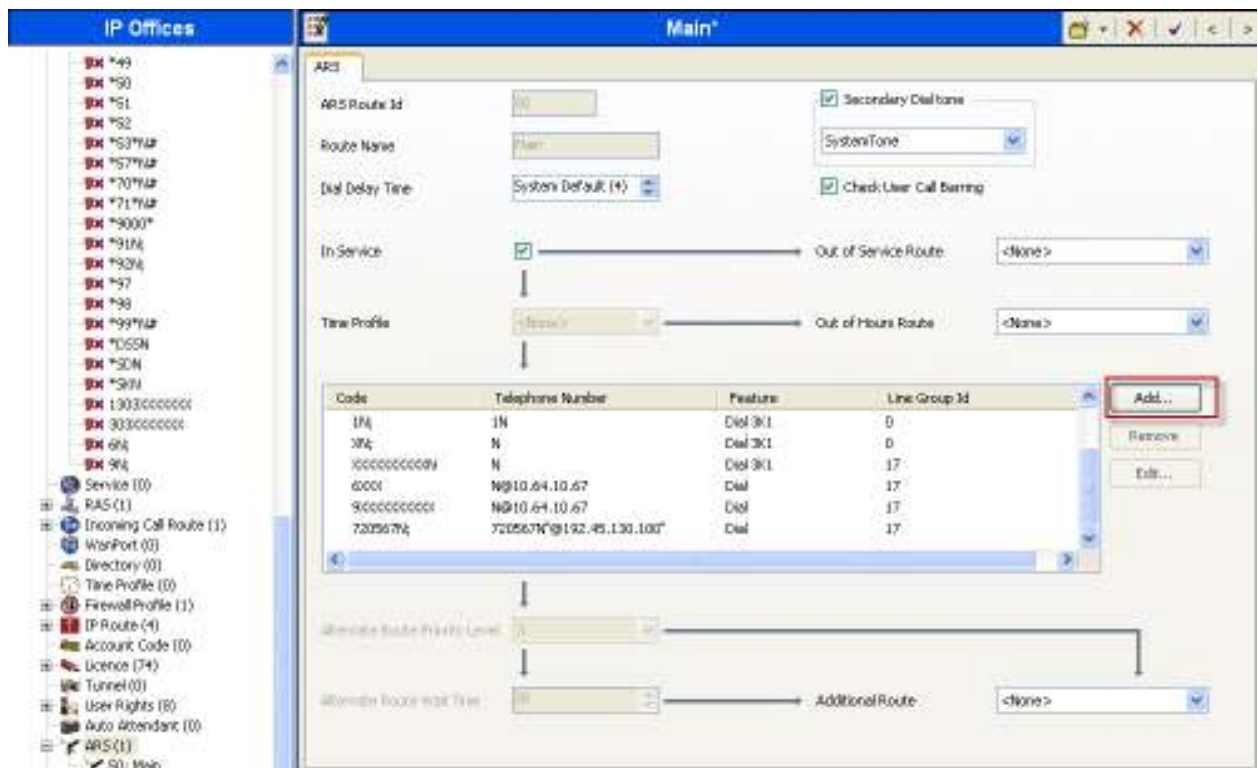
Telephone Number N

Line Group Id 50: Main

Locale

Force Account Code ☐

1. Select **ARS** → **Main** from the left panel menu, and then click on **Add** to create a new Code entry to route calls to CUCM. Note: 50:Main is the default Line Group Id for ARS.



2. Enter the appropriate information for the Code entry. The following screen capture shows a portion of the Cisco dialing plan “720567” is being used as part of the Code. The Telephone Number is composed of the called phone number appended with “@” and the CUCM IP Address. **Line Group ID** created in **Section 6.4** will be used to send out the call.

New Short Code

Code

720567N;

OK

Feature

Dial

Cancel

Telephone Number

720567N"@192.45.130.100"

Line Group Id

17

Locale

Force Account Code

☐

6.6. Create Incoming Routing Entry for Calls From Cisco UCM

1. Select **Incoming Call Route** from the left panel menu and then right-click it and select **New** (not shown) to create a new Incoming Call Route. Under the **Standard** tab, select the Line Group number created in **Section 6.4** in the **Line Group Id** field. The following screen shows the setting used in the sample network.

The screenshot displays the Cisco UCM configuration interface. On the left, the 'IP Offices' tree shows a hierarchy including BOOTP (3), Operator (3), Test Room 1, System (1), Test Room 1, Line (5), Control Unit (3), Extension (23), User (19), HuntGroup (1), Short Code (63), Service (0), RAS (1), and Incoming Call Route (1). The 'Incoming Call Route (1)' entry is selected and highlighted with a red box. On the right, the configuration details for 'Incoming Call Route 17' are shown. The 'Standard' tab is active, and the 'Line Group Id' field is set to '17', which is also highlighted with a red box. Other fields include Bearer Capability (Any Voice), Incoming Number, Incoming Sub Address, Incoming CLI, Locale, Priority (1 - Low), Tag, and Hold Music Source (System Source).

2. Under the **Destination** tab, enter “.” as the **Default Value**. The “.” indicates the incoming call can be routed to the extension specified by the caller. The following screen shows the setting used. Select the **OK** button when complete.

The screenshot shows the 'Destination' tab of the configuration interface. It features a table with columns for TimeProfile, Destination, and Fallback Extension. The 'Default Value' row is highlighted with a red box, showing a period (.) in the Destination field. The Fallback Extension field is also visible.

7. Verification

The following steps may be used to verify the configuration:

1. Call and trunk status (among other things) can be monitored using **IP Office System Status**. From IP Office Manager select the **File** menu → **Advanced** → **System Status**. Log in with appropriate credentials.

IP Office R7 System Status

AVAYA IP Office System Status

Help Exit About

Online Offline

Logon

Control Unit IP Address: 192.168.2.50

Services Base TCP Port: 50804

Local IP Address: Automatic

User Name: Administrator

Password:

☐ Auto reconnect

Logon

Once logged in, in the left-pane expand **Trunks** and select the appropriate SIP Trunk. In the sample configuration this is **Line 17**. The screen below shows 1 active call and several idle channels on Line 17.

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System
Alarms (6)
Configuration (6)
Service (6)
Trunks (9)
Line (9)
Call Quality of Service
Extensions (25)
Trunks (3)
Line: 1 - 4
Line: 17
Active Calls
Resources
Voicemail
IP Networking

SIP Trunk Summary

Peer Domain Name: avaya.com
Resolved Address: 192.45.130.100
Line Number: 17
Number of Administered Channels: 30
Number of Channels in Use: 1
Administered Compression: Auto
Silence Suppression: Off
SIP Trunk Channel Licenses: Unlimited
SIP Trunk Channel Licenses in Use: 1
SIP Device Features: REFER (incoming and outgoing), UPDATE (incoming and outgoing)

Channel Number	LRG	Call Ref	Current State	Time In State	Associate RT Address	Code	Connect Type	Call ID	Other Party	Direction of Call	Round Trip Delay	Receive Loss Prob	Receive Jitter	Transmit Loss Prob	Transmit Jitter
1	0	1	10	Connect	00:00:27	192.45...	67...	RTPR...	Edm 220, Norta	Outgoing					
2			Idle	17:25:49											
3			Idle	17:25:49											
4			Idle	17:25:49											

Trace Output - All Channels:

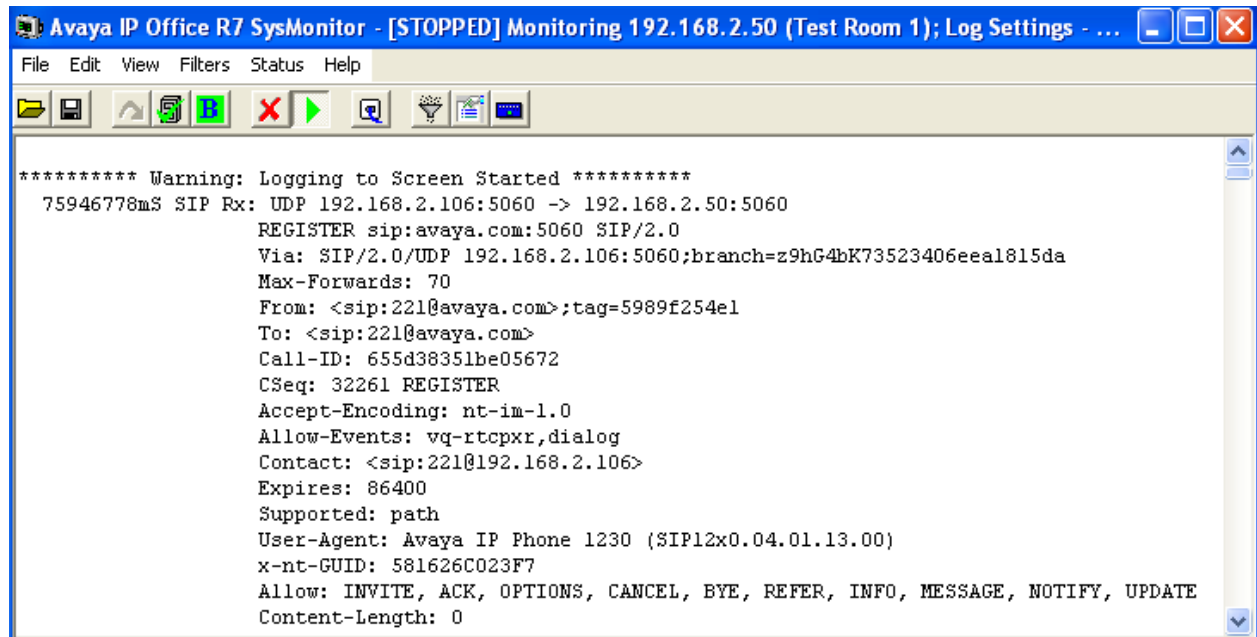
```

12/1/11 4:05:15 AM-029ns: Call Ref = 10, Short Code Matched = System, SR
12/1/11 4:05:15 AM-033ns: Call Ref = 10, Originator State = Dialing, Type = User, Destination State = Seized, Type = Target List
12/1/11 4:05:15 AM-039ns: Line = 17, Channel = 1, SIP Message = Invite, Call Ref = 10, Direction = From Switch, From = 220@avaya.com, To = 7205678002
12/1/11 4:05:15 AM-047ns: Line = 17, Channel = 1, SIP Message = Response, Call Ref = 10, Direction = To Switch, From = 220@avaya.com, To = 720567800
12/1/11 4:05:15 AM-050ns: Call Ref = 10, Originator State = Dialing, Type = User, Destination State = Dialing, Type = Trunk
12/1/11 4:05:15 AM-122ns: Line = 17, Channel = 1, SIP Message = Response, Call Ref = 10, Direction = To Switch, From = 220@avaya.com, To = 720567800
12/1/11 4:05:15 AM-124ns: Call Ref = 10, Alerting, Line = 17, Channel = 1
12/1/11 4:05:15 AM-124ns: Call Ref = 10, Originator State = Ringback, Type = User, Destination State = Outgoing Alerting, Type = Trunk
12/1/11 4:05:18 AM-073ns: Line = 17, Channel = 1, SIP Message = Response, Call Ref = 10, Direction = To Switch, From = 220@avaya.com, To = 720567800
12/1/11 4:05:18 AM-075ns: Line = 17, Channel = 1, SIP Message = Ack, Call Ref = 10, Direction = From Switch, From = 220@avaya.com, To = 7205678002
12/1/11 4:05:18 AM-069ns: Call Ref = 10, Originator State = Connected, Type = User, Destination State = Connected, Type = Trunk
12/1/11 4:05:18 AM-069ns: Call Ref = 10, Answered, Line = 17, Channel = 1

```

Trace Clear Pause Ping Call Data Print... Save As...

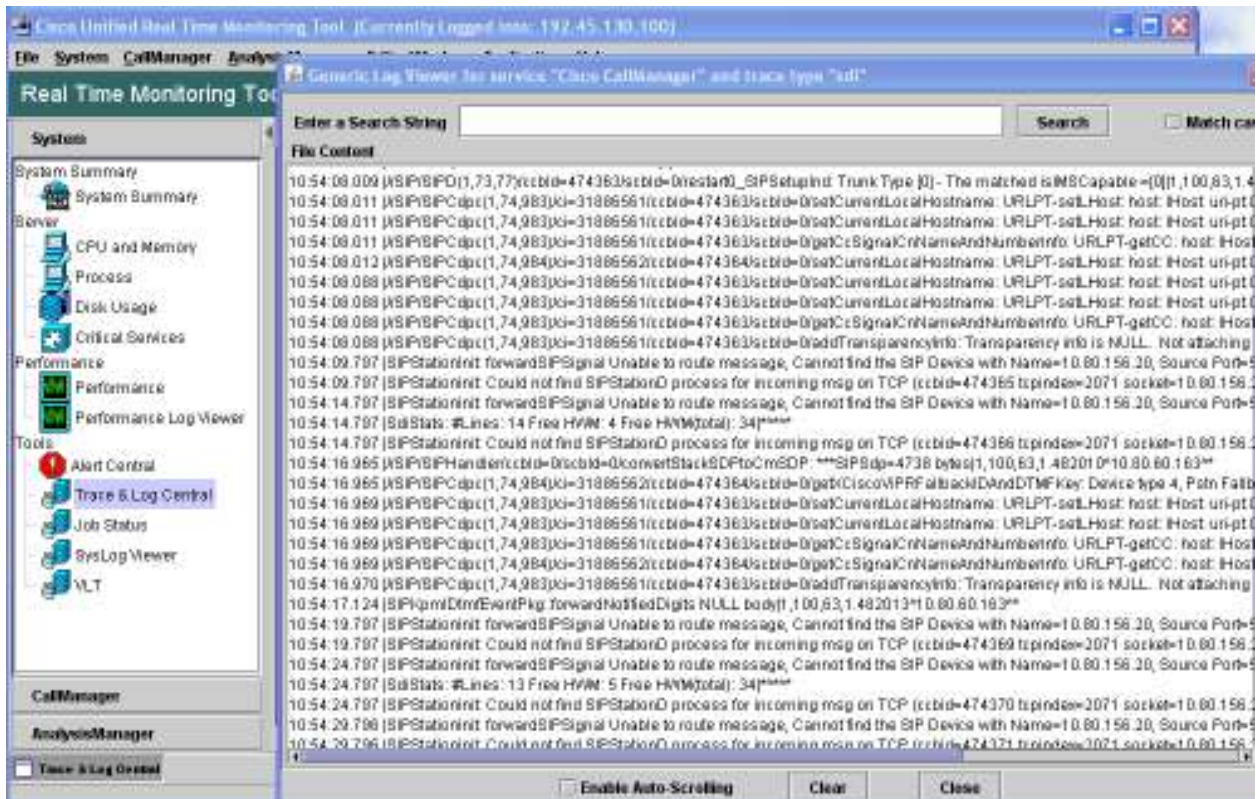
2. From the computer where IP Office Manager is installed, select **Start → Programs → IP Office → Monitor** to view Avaya IP Office debugging information. The following is a screen capture of the sysMonitor window.



The screenshot shows the Avaya IP Office R7 SysMonitor application window. The title bar reads "Avaya IP Office R7 SysMonitor - [STOPPED] Monitoring 192.168.2.50 (Test Room 1); Log Settings - ...". The menu bar includes File, Edit, View, Filters, Status, and Help. The toolbar contains icons for file operations and network monitoring. The main text area displays a log entry for a SIP REGISTER message received at 75946778ms. The message details include the source IP (192.168.2.106), destination IP (192.168.2.50), SIP version (2.0), branch ID, max forwards (70), from and to addresses (sip:221@avaya.com), call ID, CSeq (32261), supported path, user agent (Avaya IP Phone 1230), and allowed methods (INVITE, ACK, OPTIONS, CANCEL, BYE, REFER, INFO, MESSAGE, NOTIFY, UPDATE).

```
***** Warning: Logging to Screen Started *****
75946778ms SIP Rx: UDP 192.168.2.106:5060 -> 192.168.2.50:5060
REGISTER sip:avaya.com:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.106:5060;branch=z9hG4bK73523406eeal815da
Max-Forwards: 70
From: <sip:221@avaya.com>;tag=5989f254e1
To: <sip:221@avaya.com>
Call-ID: 655d38351be05672
CSeq: 32261 REGISTER
Accept-Encoding: nt-im-1.0
Allow-Events: wq-rtcpxr,dialog
Contact: <sip:221@192.168.2.106>
Expires: 86400
Supported: path
User-Agent: Avaya IP Phone 1230 (SIP12x0.04.01.13.00)
x-nt-GUID: 581626C023F7
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, REFER, INFO, MESSAGE, NOTIFY, UPDATE
Content-Length: 0
```


3. The Cisco **Real Time Monitoring Tool (RTMT)** can be used to monitor events on CUCM. This tool can be downloaded by selecting **Application → Plugins** from the top menu of the Cisco Unified CM Administration Web interface. The following is a screen capture of the Cisco Unified Communications Manager Real Time Monitoring Tool showing a call being traced in real time. For further information on this tool, please consult with reference **Section 10**: reference [7].



8. Features Tested

Basic calling features are supported including Hold, Transfer, Conference and Fax Pass-through. Supplemental features such as Call Forward All, Call Park/Unpark are also supported by this configuration.

8.1. Known Limitations

During interoperability testing, several functional limitations were observed:

1. G.729 Codec is not supported with this solution.
2. The version of IP Office shown in these Application Notes only supports an initial SIP Invite message that contains SDP information, which is not the default configuration for CUCM. One way to configure CUCM to include SDP with its initial SIP Invite message is to enable the **Media Terminal Point Required** option as shown in **Section 5.3**.
3. A number of telephone display anomalies were observed while testing call-transfer and call-forwarding scenarios. In several test scenarios it was observed

- that phones on both CUCM and IP Office would not update their display with the 'connected to' name and/or number.
4. IP Office SIP phone displays "transfer failed" when attempt to transfer a call to CUCM using attended call transfer. However, call was successfully transferred.

9. Conclusion

These Application Notes described the administrative steps required to configure a SIP trunk to support calls between Avaya IP Office and a Cisco Unified Communications Manager system.

10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>

- [1] *Avaya IP Office Release 7.0 Manager 9.0, Document Number 156010011*
- [2]
- [3] *Avaya IP Office 7.0: IP Office Installation, Document Number 156010042*

Product documentation for Cisco Systems products may be found at <http://www.cisco.com>

- [4] Cisco Unified Communications Manager Documentation Guide for Release 8.6(2)
- [5] Cisco Unified IP Phone *Administration* Guide for Cisco Unified Communications Manager 8.0 (SCCP and SIP), Part Number: OL-21035-01
- [6] *Cisco Unified Communications Manager Features and Services Guide*, Release 8.0(2), Part Number: OL-21855-01
- [7] *Cisco Unified Real-Time Monitoring Tool Administration Guide*, Release 8.0(2), Part Number: OL-21722-01

©2012 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