



Avaya Solution & Interoperability Test Lab

Configure an Avaya Centralized Messaging Solution with Avaya Communication Manager and Cisco Unified Communications Manager 7.0 – Issue 1.0

Abstract

These Application Notes describe how to configure an Avaya Centralized Messaging Solution consisting of Avaya Communication Manager and Avaya Modular Messaging at one site, and Cisco Unified Communications Manager at another site. The Avaya Modular Messaging system at the first site provided voice messaging services to subscribers at both sites. T1 QSIG was used as the common network protocol for connectivity between Avaya Modular Messaging and Avaya Communication Manager, and between Avaya Communication Manager and Cisco Unified Communications Manager.

1. Introduction

These Application Notes describe how to configure an Avaya Centralized Messaging Solution consisting of Avaya Communication Manager and Avaya Modular Messaging at one site, and Cisco Unified Communications Manager at a second site.

QSIG is a worldwide standard for private networks. In the test configuration shown in **Figure 1**, QSIG allowed users at one site (Site 2) to “cover” to the Avaya Modular Messaging system at another site (Site 1). T1 QSIG trunks were used for communication between Avaya Communication Manager and Avaya Modular Messaging, and between Avaya Communication Manager and Cisco Unified Communications Manager. The original calling party information, called party information, and reason for coverage is provided by Cisco Unified Communications Manager over the signaling D-channel to Avaya Modular Messaging via Avaya Communication Manager, so that the information can be used for proper voice message recording and retrieval.

In the Test Configuration (**Figure 1**), Avaya Communication Manager utilized the TN2464CP DS1 Interface card for T1 QSIG and Cisco Unified Communications Manager utilized the Cisco 2811 Media Gateway Control Protocol (MGCP) Gateway for T1 QSIG. For the sample configuration, Avaya Communication Manager was running on Avaya S8500 Server with Avaya G650 Media Gateway. The information contained in these Application Notes is applicable to other Avaya servers and media gateways. A four digit Uniform Dial Plan (UDP) was used to facilitate dialing between the two sites. Unique extension ranges were associated with Avaya Communication Manager at Site 1(22xx) and Cisco Unified Communications Manager at Site 2 (6xxx).

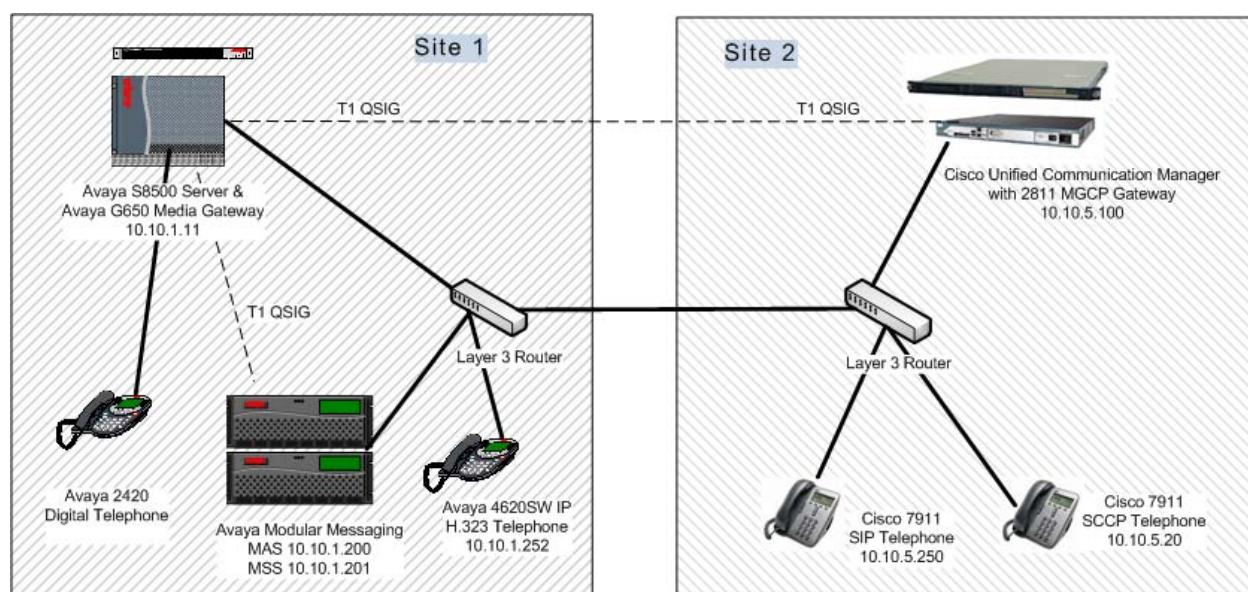


Figure 1: Test Configuration

The detailed administration of Avaya Modular Messaging system with Avaya Communication Manager using T1 QSIG is described in the Configuration Note “CN 88003 Avaya Definity G3, Prologix & S8300/S8500/S8700 T1 QSIG “ referenced in **Section 9**, and will not be repeated here. These Application Notes will focus on the additional configuration needed for Cisco Unified Communications Manager to form a Centralized Messaging Solution with Avaya Communication Manager and Avaya Modular Messaging.

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Server	Avaya Communication Manager 5.1.2 (S8500-015-01.2.416.4)
Avaya G650 Media Gateway <ul style="list-style-type: none"> TN799DP C-LAN Circuit Pack TN2602AP IP Media Processor TN2464CP DS1 Interface TN2214B Digital Line 	HW01 FW026 HW08 FW041 HW02 FW022 Vintage 000003
Avaya 4620SW IP H.323 Telephone	2.8
Avaya 2420 Digital Telephone	NA
Avaya Modular Messaging <ul style="list-style-type: none"> Messaging Storage Server Messaging Application Server 	5.0 (Patch MM500007) 5.0 (Patch MM500007)
Cisco Unified Communications Manager	7.0.2.10000-18
Cisco 2811 MGCP Gateway <ul style="list-style-type: none"> WIC2-1MFT-T1/E1 PVDM (DSP resources) 	IOS 12.4 (31) (C2800NM-SPSERVICESK9-M)
Cisco 7911 SIP Telephone	SIP11.8-4-3S
Cisco 7911 SCCP Telephone	SCCP11.8-4-3S

3. Configure Avaya Communication Manager

This section focuses on configuring the T1 QSIG trunks on Avaya Communication Manager to reach Cisco Unified Communications Manager, and provides a sample routing using Automatic Alternate Routing (AAR). The configuration procedures include the following areas:

- Administer DS1 Circuit Pack
- Administer ISDN Trunk Group
- Administer Signaling Group
- Administer Trunk Group Members
- Administer Route Pattern
- Administer Public Unknown Numbering
- Administer Uniform Dial Plan
- Administer Automatic Alternate Routing (AAR) analysis

3.1. Administer DS1 Circuit Pack

Log into the System Access Terminal (SAT). Administer a DS1 circuit pack to be used to connect to Cisco Unified Communications Manager by issuing the **add ds1 1a06** command. Note that the actual slot number may vary and in this case **1a06** is used as the slot number. Enter the following values for the specified fields and retain the default values for the remaining fields. Submit these changes.

- **Name:** Cisco_GW (A descriptive name)
- **Line Coding:** b8zs
- **Framing Mode:** esf
- **Signaling Mode:** isdn-pri
- **Connect:** pbx
- **Interface:** peer-master
- **Peer Protocol:** Q-SIG

```
add ds1 1a06                                     Page 1 of 2
                                         DS1 CIRCUIT PACK

      Location: 01A06                               Name: Cisco_GW
      Bit Rate: 1.544                             Line Coding: b8zs
Line Compensation: 1                             Framing Mode: esf
      Signaling Mode: isdn-pri
      Connect: pbx                                Interface: peer-master
TN-C7 Long Timers? n                          Peer Protocol: Q-SIG
Interworking Message: PROgress                  Side: a
Interface Companding: mulaw                     CRC? n
      Idle Code: 11111111
```

The setting of the **Interface** parameter must be complementary on both switches. For the sample configuration, Avaya Communication Manager is administered as the *network/master* (**peer-master**), and Cisco Unified Communications Manager is administered as the *user/slave*. Administering the *user/slave* is described in **Section 6.5**.

3.2. Administer ISDN Trunk Group

Administer an ISDN trunk group to interface with Cisco Unified Communications Manager. Use the **add trunk-group n** command, where **n** is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** **isdn**
- **Group Name:** **Cisco-QSIG-Trunk** (A descriptive name)
- **TAC:** **116** (An available trunk access code)
- **Direction:** **two-way**
- **Service Type:** **tie**

```
add trunk-group 60                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 60          Group Type: isdn          CDR Reports: y
  Group Name: Cisco-QSIG-Trunk      COR: 1          TN: 1          TAC: 116
  Direction: two-way      Outgoing Display? n
Dial Access? n          Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie          Auth Code? n          TestCall ITC: rest
                          Far End Test Line No:
TestCall BCC: 4
```

Navigate to **Page 2**. For the **Supplementary Service Protocol** field, enter **b** for QSIG. For the **Format** field, enter **unk-unk**. Retain the default values for the remaining fields.

```
add trunk-group 60                                     Page 2 of 21
Group Type: isdn
TRUNK PARAMETERS
  Codeset to Send Display: 6      Codeset to Send National IEs: 6
  Max Message Size to Send: 260  Charge Advice: none
  Supplementary Service Protocol: b  Digit Handling (in/out): enbloc/enbloc
Trunk Hunt: cyclical
Digital Loss Group: 13
Incoming Calling Number - Delete: Insert:          Format: unk-unk
  Bit Rate: 1200      Synchronization: async      Duplex: full
Disconnect Supervision - In? y  Out? n
Answer Supervision Timeout: 0
Administer Timers? n          CONNECT Reliable When Call Leaves ISDN? n
```

Navigate to **Page 3**. Enable the **Send Name**, **Send Calling Number**, and **Send Connected Number** fields. For the **Format** field, enter **unknown**. Submit these changes.

add trunk-group 60		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Wideband Support? n
	Internal Alert? n	Maintenance Tests? y
	Data Restriction? n	NCA-TSC Trunk Member:
	Send Name: y	Send Calling Number: y
Used for DCS? n	Hop Dgt? n	Send EMU Visitor CPN? n
Suppress # Outpulsing? n	Format: unknown	
Outgoing Channel ID Encoding: preferred	UII IE Treatment: service-provider	
	Replace Restricted Numbers? n	
	Replace Unavailable Numbers? n	
	Send Connected Number: y	
	Hold/Unhold Notifications? y	
	Modify Tandem Calling Number? n	
Send UII IE? y		
Send UCID? n		
Send Codeset 6/7 LAI IE? y	Dsl Echo Cancellation? n	
Apply Local Ringback? n		
Show ANSWERED BY on Display? y		
	Network (Japan) Needs Connect Before Disconnect? n	

3.3. Administer Signaling Group

Administer an ISDN signaling group for the new trunk group to use for signaling. Use the **add signaling-group n** command, where **n** is an available signaling group number. The **Max number of NCA TSC** is set to **10** to ensure the Message Waiting Indicators work correctly at the Cisco Site. For the **Primary D-Channel** field, enter the slot number for the DS1 circuit pack from **Section 3.1** and port **24**. For the **Trunk Group for NCA TSC** and **Trunk Group for Channel Selection** fields, enter the ISDN trunk group number from **Section 3.2**. For the **TSC Supplementary Service Protocol** field, enter **b** for QSIG. Maintain the default values for the remaining fields, and submit these changes.

add signaling-group 60		Page 1 of 1
SIGNALING GROUP		
Group Number: 60		
Associated Signaling? y	Max number of NCA TSC: 10	
Primary D-Channel: 01A0624	Max number of CA TSC: 0	
	Trunk Group for NCA TSC: 60	
Trunk Group for Channel Selection: 60		
TSC Supplementary Service Protocol: b		

3.4. Administer Trunk Group Members

Use the **change trunk-group n** command, where **n** is the trunk group number added in **Section 3.2**. Navigate to **Page 3**. For the **NCA-TSC Trunk Member** field, enter the highest trunk group member number to use for routing of tandem QSIG call independent signaling connections.

```
change trunk-group 60                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                     Measured: none      Wideband Support? n
                                     Internal Alert? n      Maintenance Tests? y
                                     Data Restriction? n      NCA-TSC Trunk Member: 23
                                     Send Name: y            Send Calling Number: y
  Used for DCS? n                                     Hop Dgt? n          Send EMU Visitor CPN? n
  Suppress # Outpulsing? n      Format: unknown
  Outgoing Channel ID Encoding: preferred      UII IE Treatment: service-provider

                                     Replace Restricted Numbers? n
                                     Replace Unavailable Numbers? n
                                     Send Connected Number: y
                                     Hold/Unhold Notifications? y
  Send UII IE? y                                     Modify Tandem Calling Number? n
  Send UCID? n
  Send Codeset 6/7 LAI IE? y                        Dsl Echo Cancellation? n

  Apply Local Ringback? n
  Show ANSWERED BY on Display? y
                                     Network (Japan) Needs Connect Before Disconnect? n
```

Navigate to **Page 5** and **6**. Enter all 23 ports of the DS1 circuit pack into the **Port** fields, and the corresponding **Code** and **Sfx** fields will be populated automatically. Enter the ISDN signaling group number from **Section 3.3** into the **Sig Grp** fields as shown below. Submit these changes.

```
change trunk-group 60                                     Page 5 of 21
TRUNK GROUP
  Administered Members (min/max): 1/23
GROUP MEMBER ASSIGNMENTS      Total Administered Members: 23

  Port      Code Sfx Name      Night      Sig Grp
1: 01A0601  TN2464 C                      60
2: 01A0602  TN2464 C                      60
3: 01A0603  TN2464 C                      60
4: 01A0604  TN2464 C                      60
5: 01A0605  TN2464 C                      60
6: 01A0606  TN2464 C                      60
7: 01A0607  TN2464 C                      60
8: 01A0608  TN2464 C                      60
9: 01A0609  TN2464 C                      60
10: 01A0610 TN2464 C                     60
11: 01A0611 TN2464 C                     60
12: 01A0612 TN2464 C                     60
13: 01A0613 TN2464 C                     60
14: 01A0614 TN2464 C                     60
15: 01A0615 TN2464 C                     60
```

change trunk-group 60 Page 6 of 21

TRUNK GROUP

Administered Members (min/max): 1/23

GROUP MEMBER ASSIGNMENTS

Total Administered Members: 23

	Port	Code	Sfx	Name	Night	Sig	Grp
16:	01A0616	TN2464	C			60	
17:	01A0617	TN2464	C			60	
18:	01A0618	TN2464	C			60	
19:	01A0619	TN2464	C			60	
20:	01A0620	TN2464	C			60	
21:	01A0621	TN2464	C			60	
22:	01A0622	TN2464	C			60	
23:	01A0623	TN2464	C			60	
24:							

3.5. Administer Route Pattern

Create a route pattern for the new ISDN trunk group to use for routing. Use the **change route-pattern n** command, where **n** is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name:** Cisco_MM (A descriptive name)
- **Grp No:** 60 (The trunk group number from Section 3.2)
- **FRL:** 0 (Level that allows access to this trunk, with 0 being least restrictive)
- **TSC:** y
- **CA-TSC Request:** as-needed
- **Numbering Format:** unk-unk

change route-pattern 80 Page 1 of 3

Pattern Number: 80 **Pattern Name: Cisco_MM**

Secure SIP? n

Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/	IXC
No			Mrk	Lmt	List	Del	Digits	QSIG	
							Dgts	Intw	
1:	60	0						n	user
2:								n	user
3:								n	user
4:								n	user
5:								n	user
6:								n	user

	BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR
	0	1	2	M	4	W	Request		Dgts	Format	
									Subaddress		
1:	y	y	y	y	y	n	y	as-needed	rest	unk-unk	none
2:	y	y	y	y	y	n	n		rest		none
3:	y	y	y	y	y	n	n		rest		none
4:	y	y	y	y	y	n	n		rest		none
5:	y	y	y	y	y	n	n		rest		none
6:	y	y	y	y	y	n	n		rest		none

3.6. Administer Public Unknown Numbering

Use the **change public-unknown-numbering 0** command, to define the calling party number to be sent to Cisco Unified Communications Manager. Add an entry for the trunk group defined in **Section 3.2**. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Ext Len:** 4
- **Ext Code:** 22
- **Trk Grp(s):** 60
- **Total CPN Len:** 4

In the example shown below, all calls originating from a 4-digit extension beginning with 22 and routed to trunk group 60 will result in the 4-digit calling number to be sent. Submit these changes.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	22	60		4	Total Administered: 0 Maximum Entries: 9999

3.7. Administer Uniform Dial Plan

This section provides a sample uniform dial plan used for routing calls with dialed digits 6xxx to Cisco Unified Communications Manager. Use the **change uniform-dialplan 0** command, and add an entry to specify use of AAR for routing of digits 6xxx. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Matching Pattern:** The dialed prefix digits to match on, in this case **6**.
- **Len:** 4 (The length of the full dialed number)
- **Del:** 0 (The number of digits to delete)
- **Net:** aar

change uniform-dialplan 0					Page 1 of 2
UNIFORM DIAL PLAN TABLE					
					Percent Full: 0
Matching Pattern	Len	Del	Insert Digits	Net	Conv Num
6	4	0		aar	n
					n
					n
					n

3.8. Administer Automatic Alternate Routing (AAR) Analysis

Use the **change aar analysis 0** command, and add an entry to specify how to route the calls to 6xxx. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** **6** (The dialed prefix digits to match on)
- **Total Min:** **4** (The minimum number of digits)
- **Total Max:** **4** (The maximum number of digits)
- **Route Pattern:** **80** (The route pattern number from **Section 3.5**)
- **Call Type:** **aar**

change aar analysis 0							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all							Percent Full: 1	
Dialed String	Total		Route	Call	Node	ANI		
	Min	Max	Pattern	Type	Num	Reqd		
2	7	7	999	aar		n		
3	7	7	999	aar		n		
4	4	4	1	aar		n		
5	7	7	999	aar		n		
6	4	4	80	aar		n		
7	7	7	999	aar		n		
8	7	7	999	aar		n		
9	7	7	999	aar		n		

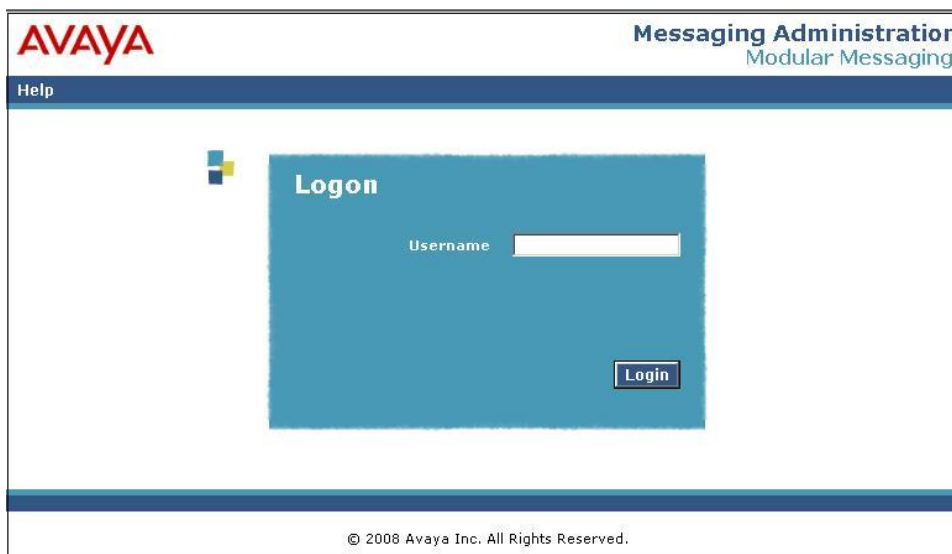
4. Configure Avaya Modular Messaging

This section focuses on configuring the Cisco users as local subscribers on Avaya Modular Messaging. The subscriber management is configured on the Avaya Messaging Storage Server (MSS) component. The configuration procedures include the following areas:

- Launch Messaging Administration
- Administer Subscriber Extension Ranges
- Administer Subscribers

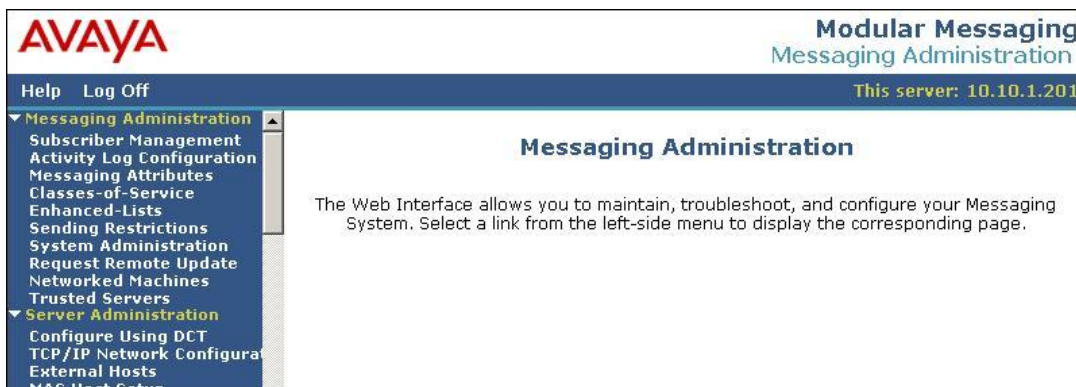
4.1. Launch Messaging Administration

Access the Avaya Messaging Storage Server (MSS) web interface by using the URL “http://ip-address” in an internet browser window, where “ip-address” is the IP address of the Avaya Messaging Storage Server. The **Logon** screen is displayed below. Log in using a valid user name and password. The **Password** field will appear after a value is entered into the **Username** field.



The screenshot shows the Avaya Messaging Administration web interface. At the top left is the AVAYA logo. At the top right, it says "Messaging Administration" and "Modular Messaging". Below the logo is a "Help" link. The main content area features a blue box with the title "Logon". Inside this box, there is a "Username" label followed by a text input field. Below the input field is a "Login" button. At the bottom of the page, there is a copyright notice: "© 2008 Avaya Inc. All Rights Reserved."

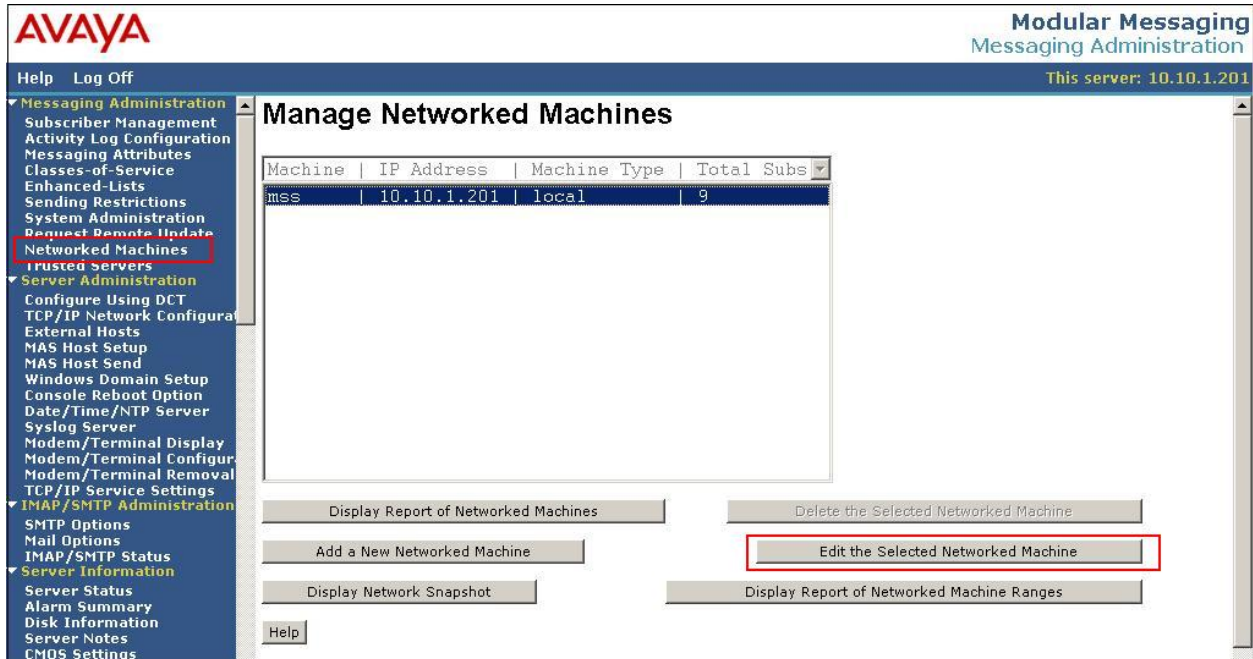
The **Messaging Administration** screen appears, as shown below.



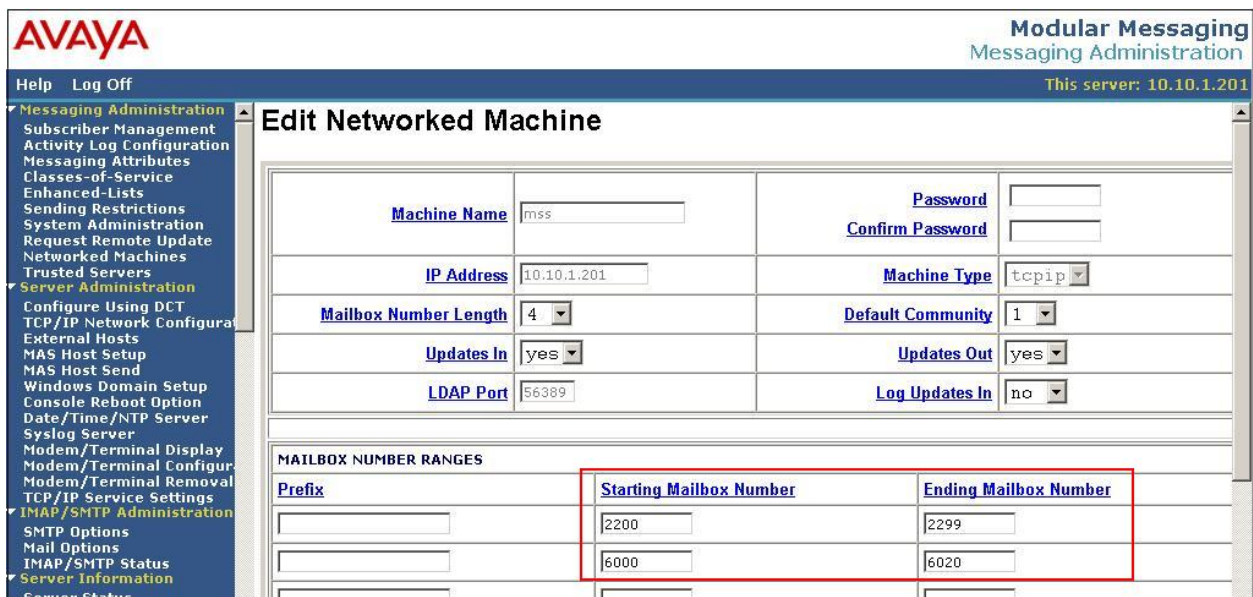
The screenshot shows the main Avaya Messaging Administration web interface. At the top left is the AVAYA logo. At the top right, it says "Modular Messaging" and "Messaging Administration". Below the logo are "Help" and "Log Off" links. A status bar at the top right indicates "This server: 10.10.1.201". On the left side, there is a navigation menu with two main sections: "Messaging Administration" and "Server Administration". The "Messaging Administration" section includes links for Subscriber Management, Activity Log Configuration, Messaging Attributes, Classes-of-Service, Enhanced-Lists, Sending Restrictions, System Administration, Request Remote Update, Networked Machines, and Trusted Servers. The "Server Administration" section includes links for Configure Using DCT, TCP/IP Network Configuration, External Hosts, and MMS Host Setup. The main content area has the title "Messaging Administration" and a paragraph: "The Web Interface allows you to maintain, troubleshoot, and configure your Messaging System. Select a link from the left-side menu to display the corresponding page."

4.2. Administer Subscriber Extension Ranges

Select **Messaging Administration** → **Networked Machines** from the left pane, to display the **Manage Networked Machines** screen. Select the MSS server from the table listing, and click **Edit the Selected Networked Machine** toward the bottom right of the screen.



The **Edit Networked Machine** screen is displayed. Under the **MAILBOX NUMBER RANGES** section, locate an available entry line and enter the desired **Starting Mailbox Number** and **Ending Mailbox Number** to be used for the Cisco subscribers. Scroll down to the bottom of the screen and click **Save** (not shown).



4.3. Administer Subscribers

Select **Messaging Administration** → **Subscriber Management** from the left pane, to display the **Manage Subscribers** screen. For the **Local Subscriber Mailbox Number** field, enter a mailbox number within the range administered in **Section 4.2** to add as a local subscriber, click **Add or Edit**.

The screenshot shows the Avaya Modular Messaging Messaging Administration interface. The left pane is expanded to 'Subscriber Management'. The main area is titled 'Manage Subscribers'. At the top, there is a form for 'Local Subscriber Mailbox Number' with the value '6010' and an 'Add or Edit' button. Below this is a table with columns: Machine Name, Subscriber Licenses Used, Total Subscribers, and Filtered Subscribers. The table has two rows: 'Local Subscribers' (mss, 5 of 10, 9, 9) and 'Remote Subscribers' (internet, 0, 0). Each row has a 'Filter' button and a 'Manage' button. A 'Help' button is at the bottom left.

	Machine Name	Subscriber Licenses Used	Total Subscribers	Filtered Subscribers
Local Subscribers	mss	5 of 10	9	9
Remote Subscribers	internet		0	0

The **Add Local Subscriber** screen is displayed next. Enter the desired string into the **Last Name**, **First Name**, **Password**, **Mailbox Number**, **Numeric Address**, **Email Handle**, **Common Name**, and **ASCII Version of Name** fields. In the interoperability testing, the same telephone extensions for the Cisco subscribers were used for the **Mailbox Number**, **Numeric Address**, and **PBX Extension** fields. Scroll down to the bottom of the screen and click **Save** (not shown). Select **Community ID** and **Class Of Service** created for Avaya Modular Messaging as described in the Configuration Note CN 88003 in **Section 9**. Repeat this section to add all Cisco subscribers.

The screenshot shows the Avaya Modular Messaging Messaging Administration interface. The left pane is expanded to 'Subscriber Management'. The main area is titled 'Add Local Subscriber'. It contains two sections: 'BASIC INFORMATION' and 'SUBSCRIBER DIRECTORY'. The 'BASIC INFORMATION' section has fields for: *Last Name (Cisco), First Name (SCCP), *Password (****), *Mailbox Number (6010), *Numeric Address (6010), PBX Extension (6010), *Class Of Service (3 - Cisco_MM), and *Community ID (1). The 'SUBSCRIBER DIRECTORY' section has fields for: Email Handle (@mss.avayalabs.com), Telephone Number (6010), Common Name (Cisco SCCP), and ASCII Version of Name (Cisco SCCP).

BASIC INFORMATION	
* (Required Fields)	
*Last Name	Cisco
First Name	SCCP
*Password	****
*Mailbox Number	6010
*Numeric Address	6010
PBX Extension	6010
*Class Of Service	3 - Cisco_MM
*Community ID	1

SUBSCRIBER DIRECTORY	
Email Handle	@mss.avayalabs.com
Telephone Number	6010
Common Name	Cisco SCCP
ASCII Version of Name	Cisco SCCP

5. Configure Cisco 2811 MGCP Gateway

The procedures for configuring Cisco 2811 MGCP Gateway include the following areas:

- Log into Gateway
- Administer MGCP Protocol
- Administer T1 Interface Card
- Administer Dial Peers and Voice Ports
- Administer MGCP PRI Backhaul

5.1. Log into Gateway

Access the MGCP Gateway command line interface via a hyper terminal application running on a personal computer. This computer has a serial cable connected to the MGCP Gateway console port. The output from the MGCP Gateway has been trimmed down in the subsequent sections, in order to focus on the key settings for the configuration. Values highlighted in bold italics represent values entered by the system administrator.

Command	Comment
User Access Verification	User Access Verification is displayed.
Password: xxxxx	Enter a valid user password.
2811>	A sample response indicating successful log in. 2811> in this case is the gateway hostname that was previously configured.
2811> enable	Enter the enable command to enable the privileged EXEC mode.
Password: yyyyy	Enter the valid user password for the EXEC mode.
2811#	A sample response indicating successful entry into the EXEC mode.

5.2. Administer MGCP Protocol

Use the command line interface to enable support for the MGCP protocol and support for Cisco Unified Communications Manager.

Command	Comment
2811# <i>configure terminal</i>	Enables the global configuration mode.
2811(config)#	A sample response indicating successful entry into the global configuration mode.
2811(config)# <i>mgcp</i>	Enables the MGCP protocol.
2811(config)# <i>mgcp call-agent callmgr.avayalabs.com service-type mgcp version 0.1</i>	Specifies the Cisco Unified Communications Manager, the gateway control service, and version of service-type. In this case, callmgr.avayalabs.com is the fully qualified domain name for the Cisco Unified Communications Manager. The servicetype is mgcp , and the version for MGCP is 0.1 .
2811(config)# <i>mgcp dtmf-relay voip codec all mode out-of-band</i>	Specifies the codec type and dual tone multifrequency (DTMF) relay services.
2811(config)# <i>ccm-manager mgcp</i>	Enables the MGCP gateway to support Cisco Unified Communications Manager.

5.3. Administer T1 Interface Card

Use the command line interface to administer the T1 controller.

Command	Comment
2811(config)# <i>card type t1 0 0</i>	From the global configuration mode use the card type command to configure the card type of the controller as T1.
2811(config)# <i>controller t1 0/0/0</i>	From the global configuration mode, use the controller command to enter the controller configuration mode. In this case, t1 is used to specify T1. The first 0 implies the module is directly inserted into the 2811 chassis. The second 0 is the physical slot number of the network module card and the third 0 is the port number.
2811(config-controller)# <i>framing esf</i>	Specifies esf as the framing type.
2811(config-controller)# <i>linecode b8zs</i>	Specifies b8zs as the line encoding method.
2811(config-controller)# <i>pri-group timeslots 1-24 service mgcp</i>	Specifies MGCP as the control protocol with 24 ports.
2811(config-controller)# <i>exit</i>	Exits the controller configuration mode.

5.4. Administer Dial Peers and Voice Ports

Use the command line interface to administer dial peers and voice ports for MGCP, beginning in the global configuration mode.

Command	Comment
2811(config)# dial-peer voice 1 pots	From the global configuration mode, use the dial-peer command to enter the dial peer configuration mode, and designate the specified dial peer as a POTS dial peer using VoIP encapsulation.
2811(config-dial-peer)# Service MGCPAPP	Enables MGCP on the dial peer. Note that the command is case-sensitive in some Cisco IOS versions.
2811(config-dial-peer)# port 0/0/0:23	Binds the MGCP application to the specified voice ports. In this case, 0/0/0 represents “0/slot/ port”. The first 0 signifies the card is inserted directly into the rear of the 2811 chassis.
2811(config-dial-peer)# exit	Exits the dial-peer configuration mode.
2811(config)# voice-port 0/0/0:23	From the global configuration mode, use the voice-port command to enter the voice port configuration mode. In this case 0/0/0 represents “0/slot/ port”.
2811(config-voiceport)# no shut	Activates the voice port.
2811(config-voiceport)# exit	Exits the voice port configuration mode.

5.5. Administer MGCP PRI Backhaul

MGCP PRI backhaul is a method for transporting information from the signaling D-channel of the MGCP gateway to Cisco Unified Communications Manager over a TCP connection. Use the command line interface to configure for MGCP PRI backhaul, beginning in the global configuration mode.

Command	Comment
2811(config)# <i>interface serial 0/0/0:23</i>	From the global configuration mode, use the interface serial command to enter the serial interface configuration mode. In this case, 0/0/0:23 represents “0/slot/port:timeslot”.
2811(config-if)# <i>isdn switchtype primary-qsig</i>	Specifies QSIG as the ISDN switch type.
2811(config-if)# <i>isdn bind-L3 ccm-manager</i>	Enables ISDN to backhaul Q.931.
2811(config-if)# <i>exit</i>	Exits the serial interface configuration mode.

6. Configure Cisco Unified Communications Manager

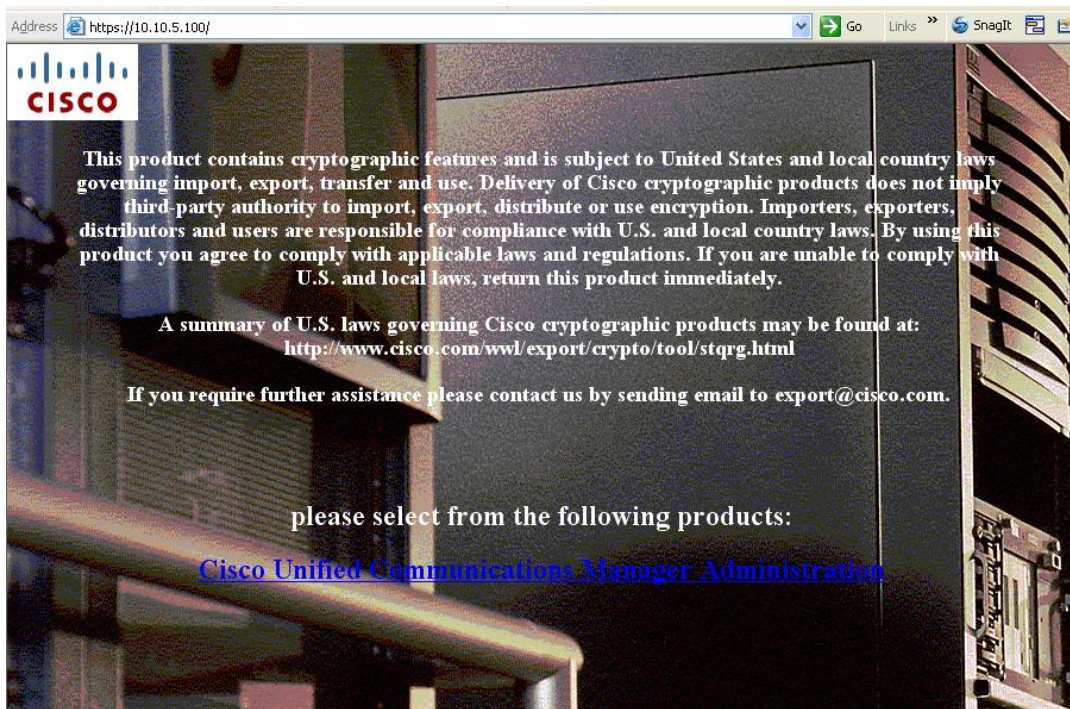
The procedures for configuring Cisco Unified Communications Manager include the following areas:

- Log into Cisco Unified Communications Manager
- Administer Media Resource Group
- Administer Media Resource Group List
- Administer Service Parameters
- Administer MGCP Gateway
- Administer Route Pattern
- Administer Voice Mail Pilot
- Administer Voice Mail Profile
- Administer Phones

6.1. Log into Cisco Unified Communications Manager

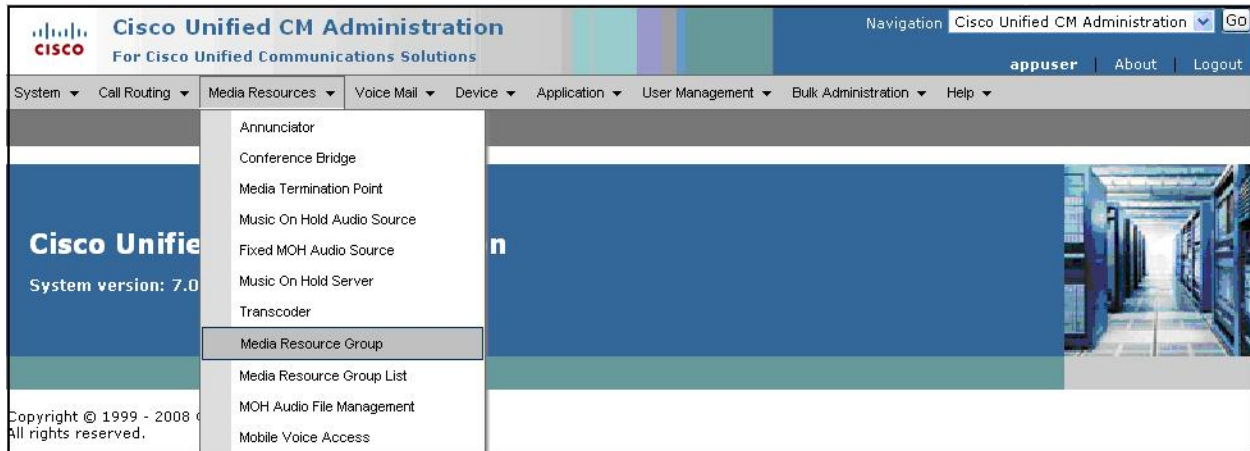
Access the Cisco Unified Communications Manager Administration web interface by using the URL “<http://<ip-address>>” in an Internet browser window, where “<ip-address>” is the IP address of the Cisco Unified Communications Manager. Note that the IP address for the Cisco Unified Communications Manager may vary, and in this case “10.10.5.100” is used. This was configured as part of installation.

Click on **Cisco Unified Communications Manager Administration** at the bottom of the screen, and log in with appropriate credentials.

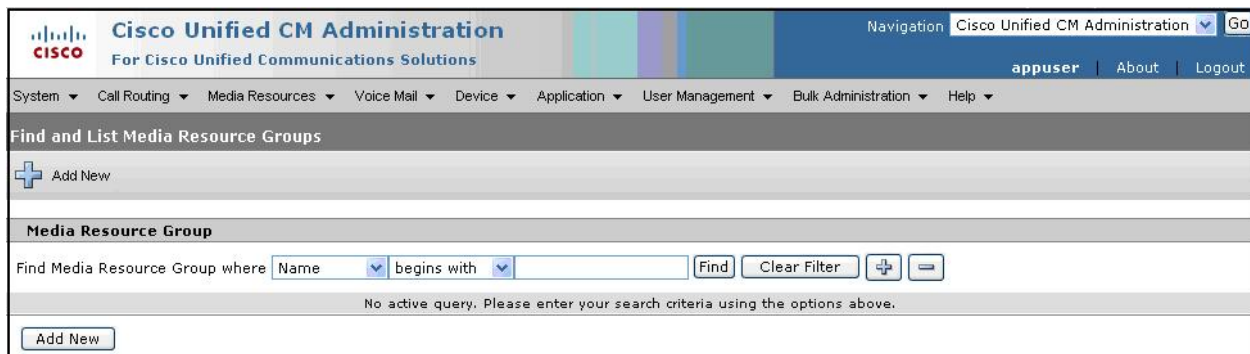


6.2. Administer Media Resource Group

The **Cisco Unified CM Administration** screen is displayed. Select **Media Resources** → **Media Resource Group**, as shown below.



The **Find and List Media Resource Groups** screen is displayed next. Click **Add New** to add a new **Media Resource Group**.



The **Media Resource Group Configuration** screen is displayed. Enter descriptive text into the **Name** and **Description** fields. Select the desired resources from the **Available Media Resources** section, and use the down arrow to move the resources to the **Selected Media Resources** section. For this interoperability testing, all available media resources were selected. Click **Save**.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

appuser About Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Media Resource Group Configuration Related Links: Back To Find/List Go

Save

Media Resource Group Status
Media Resource Group: New

Media Resource Group Information
Name* DublinA
Description All Media

Devices for this Group
Available Media Resources**
Selected Media Resources*
ANN_2
CFB_2
MOH_2
MTP_2

☐ Use Multicast for MOH Audio (If at least one multicast MOH resource is available)

Save

6.3. Administer Media Resource Group List

Scroll to the top of the screen, and select **Media Resources** → **Media Resource Group List**, as shown below.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

appuser About Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Media Resource Group Related Links: Back To Find/List Go

Save Delete

Status
Add successful
Devices associated may impact call pro

Media Resource Group
Media Resource Group: C

Media Resource Group
Name* DublinA
Description All Media

Annunciator
Conference Bridge
Media Termination Point
Music On Hold Audio Source
Fixed MOH Audio Source
Music On Hold Server
Transcoder
Media Resource Group
Media Resource Group List
MOH Audio File Management
Mobile Voice Access

The **Find and List Media Resource Group Lists** screen is displayed next. Click **Add New** to add a new media resource group list.

The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes the Cisco logo, the title 'Cisco Unified CM Administration For Cisco Unified Communications Solutions', and a user profile 'appuser' with links for 'About' and 'Logout'. A secondary navigation bar contains dropdown menus for 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The main content area is titled 'Find and List Media Resource Group Lists'. It features an 'Add New' button with a plus icon. Below this is a search section titled 'Media Resource Group List' with a text input field containing 'begins with', a 'Find' button, a 'Clear Filter' button, and two small icons. A message below the search bar states: 'No active query. Please enter your search criteria using the options above.' At the bottom left of the search section is another 'Add New' button.

The **Media Resource Group List Configuration** screen is displayed. Enter a descriptive text into the **Name** field. Select the media resource group created in **Section 6.2** from the **Available Media Resource Groups** section, and use the down arrow to move to the **Selected Media Resource Groups** section. Click **Save**.

The screenshot displays the 'Media Resource Group List Configuration' screen. At the top right, there is a 'Related Links' section with a 'Back To Find/List' link and a 'Go' button. Below the title bar is a 'Save' button with a floppy disk icon. The configuration is organized into several sections: 'Status' shows 'Status: Ready'; 'Media Resource Group List Status' shows 'Media Resource Group List: New'; 'Media Resource Group List Information' contains a 'Name*' field with the value 'DublinSIL'; and 'Media Resource Groups for this List' contains two list boxes. The 'Available Media Resource Groups' list box is empty, while the 'Selected Media Resource Groups' list box contains 'DublinA'. Between the two list boxes are up and down arrow icons. At the bottom left is a 'Save' button. A legend at the bottom left indicates that '*' indicates a required item.

6.4. Administer Service Parameters

Scroll to the top of the screen, and select **System** → **Service Parameters**, as shown below.

The screenshot shows the Cisco Unified CM Administration web interface. The top navigation bar includes the Cisco logo, the title "Cisco Unified CM Administration", and a "Navigation" dropdown menu. Below this is a secondary navigation bar with tabs for "System", "Call Routing", "Media Resources", "Voice Mail", "Device", "Application", "User Management", "Bulk Administration", and "Help". The "System" tab is selected, and a left-hand navigation menu is open, showing a list of system-related options. "Service Parameters" is highlighted in the menu. The main content area displays the "Service Parameters" configuration page, which includes a "Related Links" section with a "Back To Find/List" button, a "Reset" button, and an "Add New" button. Below these are several input fields for configuration, including "Server", "Service", and "List".

The **Service Parameter Configuration** screen is displayed next. Select the appropriate values in the **Server** and **Service** fields for the network configuration, which were administered as part of installation. The **Service Parameter Configuration** screen is updated with service parameter fields (not shown).

The screenshot shows the "Service Parameter Configuration" screen. It has a title bar "Service Parameter Configuration". Below the title bar is a "Status" section with an information icon and the text "Status: Ready". Below the status section is a "Select Server and Service" section. This section contains two dropdown menus: "Server*" with the value "callMgr (Active)" and "Service*" with the value "Cisco CallManager (Active)". Below the dropdown menus is a note: "All parameters apply only to the current server except parameters that are in the Clusterwide group(s)."

Scroll down to the **Clusterwide Parameters (Feature – Forward)** section. For the **Forward By Reroute Enabled** field, select **True** from the drop-down list to enable the QSIG forward by reroute feature. For the **Include Original Called Info for Q.SIG Call Diversions** field, select **Always** from the drop-down list to enable encoding of the original called party name and number for all QSIG call diversions. Retain the default values for the remaining fields.

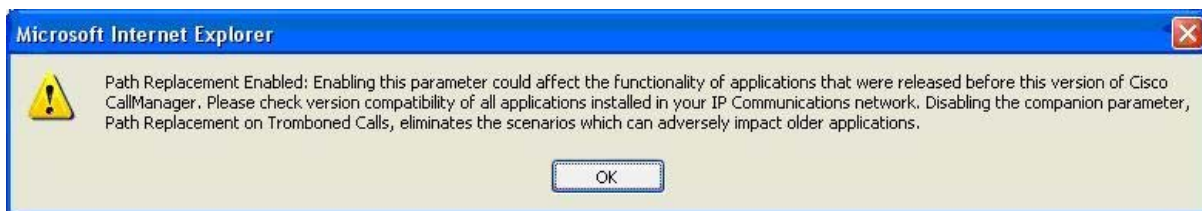
Clusterwide Parameters (Feature - Forward)		
Forward Maximum Hop Count *	12	12
Forward No Answer Timer *	12	12
Max Forward Hops to DN *	12	12
Retain Forward Information *	False	False
Forward By Reroute Enabled *	True	False
Transform Forward by Reroute Destination *	True	True
Always Forward Switch Voice Mail Calls *	True	True
Forward By Reroute T1 Timer *	10	10
Include Original Called Info for Q.SIG Call Diversions *	Always	Only after the first diversion
Set Private Numbering Plan for Call Forward *	False	False
Set Type of Number for Call Forward *	Level1RegionalNumber	Level1RegionalNumber
Max Forward UnRegistered Hops to DN *	0	0
CFA CSS Activation Policy *	With Configured CSS	With Configured CSS
Cause Code When Maximum Forward Hop Count is Triggered *	Normal Unspecified	Normal Unspecified

There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

Scroll down to the **Clusterwide Parameters (Feature – Path Replacement)** section. For the **Path Replacement Enabled** field, select **True** from the drop-down list to enable the QSIG path replacement feature.

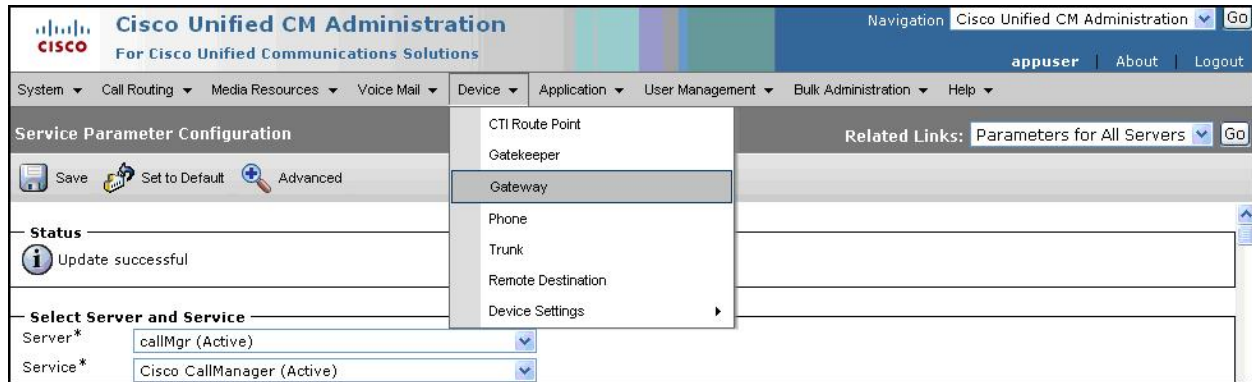
Clusterwide Parameters (Feature - Path Replacement)		
Path Replacement Enabled *	True	False
Path Replacement on Tromboned Calls *	True	True
Start Path Replacement Minimum Delay Time *	0	0
Start Path Replacement Maximum Delay Time *	0	0
Path Replacement T1 Timer *	30	30
Path Replacement T2 Timer *	15	15
Path Replacement PINX ID		
Path Replacement Calling Search Space	< None >	

The message pop up box below is displayed, click **OK** to proceed. Retain the default values for the remaining fields. Scroll down to the bottom of the screen and click **Save** (not shown).

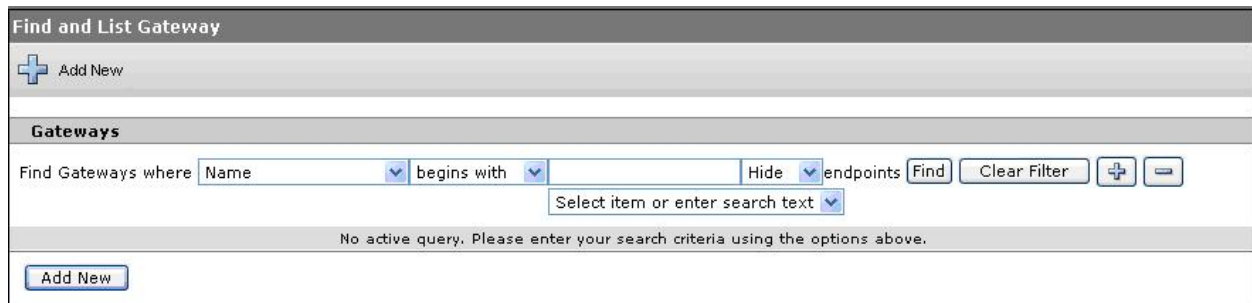


6.5. Administer MGCP Gateway

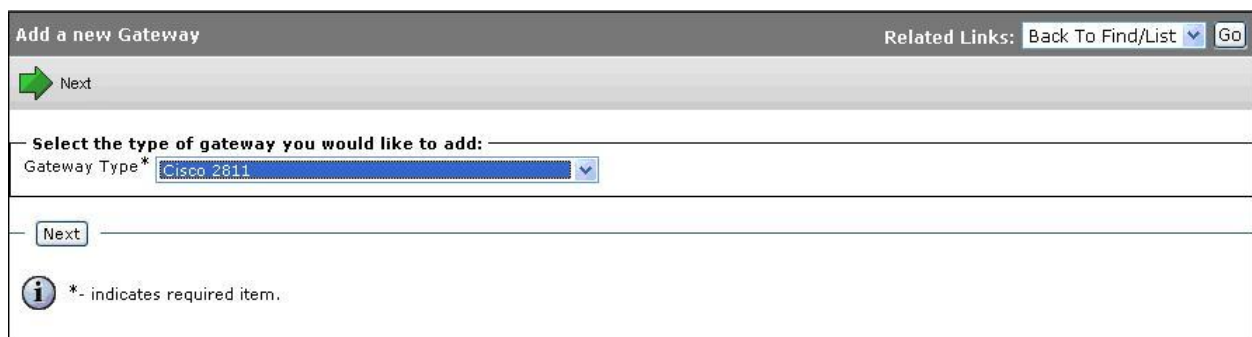
Scroll to the top of the screen, and select **Device** → **Gateway**, as shown below.



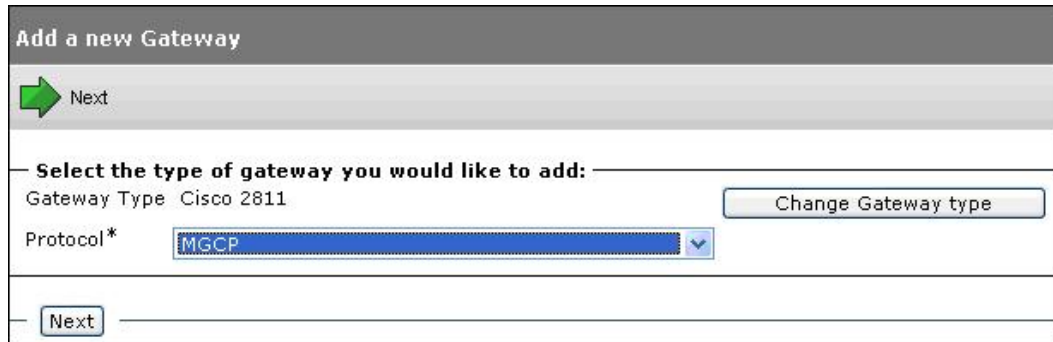
The **Find and List Gateway** screen is displayed. Click **Add New** to add a new gateway.




The **Add a new Gateway** screen is displayed next. Select **Cisco 2811** from the **Gateway Type** drop-down list. Click **Next** to proceed.



On the subsequent screen select **MGCP** from the **Protocol** drop-down list. Click **Next** to proceed.



Add a new Gateway

 Next

Select the type of gateway you would like to add:

Gateway Type Cisco 2811 Change Gateway type

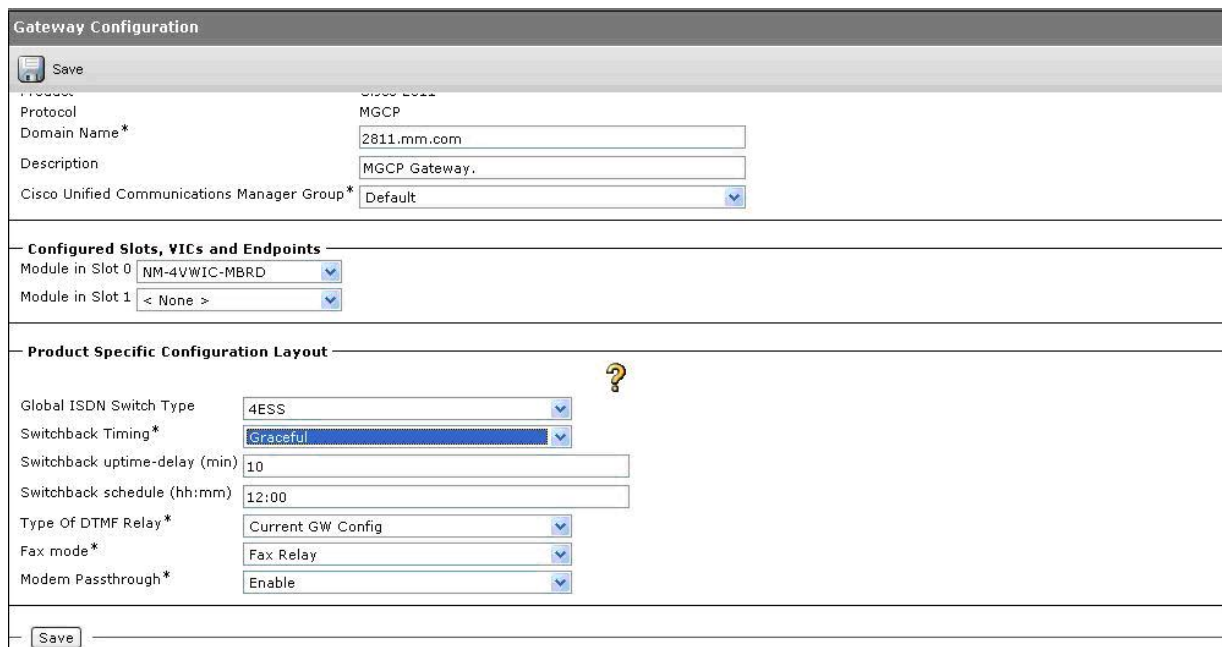
Protocol* MGCP

Next


The **Gateway Configuration** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Domain Name:** **2811.mm.com** (The fully qualified domain name for the gateway)
- **Description:** **MGCP Gateway** (A descriptive text)
- **Cisco Unified Communication Manager Group:** **Default**
- **Module in Slot 0:** **NM-4VWIC-MBRD**

Scroll down to the bottom of the screen and click **Save**.



Gateway Configuration

 Save

Protocol MGCP

Domain Name* 2811.mm.com


Description MGCP Gateway

Cisco Unified Communications Manager Group* Default

Configured Slots, VICs and Endpoints

Module in Slot 0 NM-4VWIC-MBRD

Module in Slot 1 < None >

Product Specific Configuration Layout 

Global ISDN Switch Type 4ESS

Switchback Timing* Graceful

Switchback uptime-delay (min) 10

Switchback schedule (hh:mm) 12:00

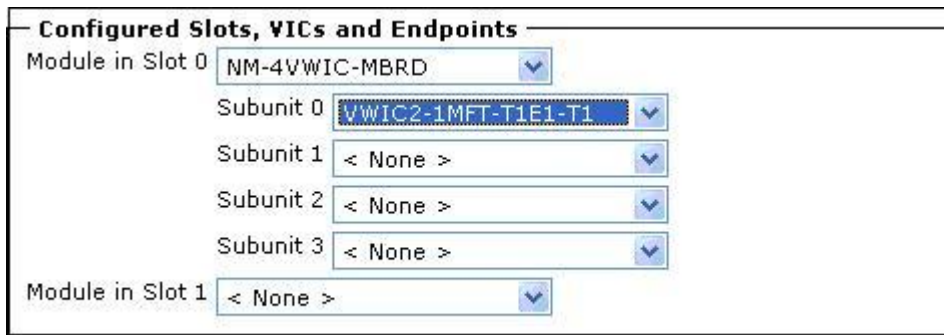
Type Of DTMF Relay* Current GW Config

Fax mode* Fax Relay

Modem Passthrough* Enable

Save

The screen is updated with 4 **Subunit** fields appearing below the **Module in Slot 0** field. For the **Subunit 0** field, select **VWIC2-1MFT-T1E1-T1** from the drop-down list. Scroll down to the bottom of the screen and click **Save** (not shown).



Configured Slots, VICs and Endpoints

Module in Slot 0: NM-4VWIC-MBRD

Subunit 0: VWIC2-1MFT-T1E1-T1

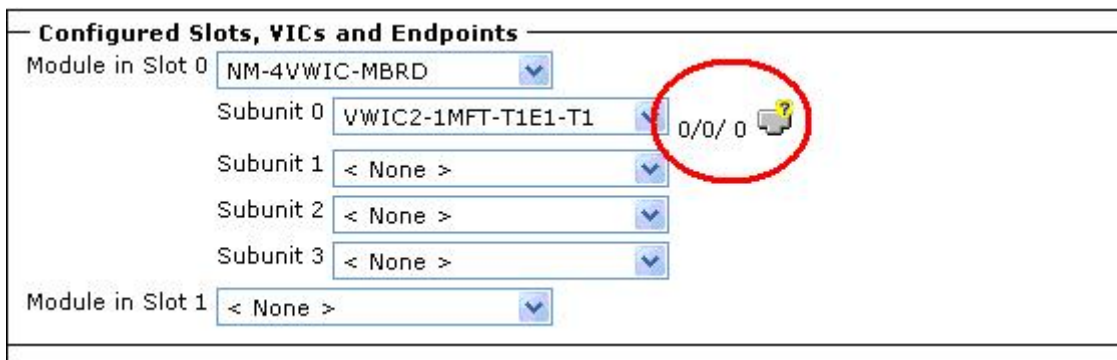
Subunit 1: < None >

Subunit 2: < None >

Subunit 3: < None >

Module in Slot 1: < None >

The screen is updated with icons appearing to the right of the **Subunit 0** field. Click the icon next to the **0/0/0** field.



Configured Slots, VICs and Endpoints

Module in Slot 0: NM-4VWIC-MBRD

Subunit 0: VWIC2-1MFT-T1E1-T1 0/0/0 ?

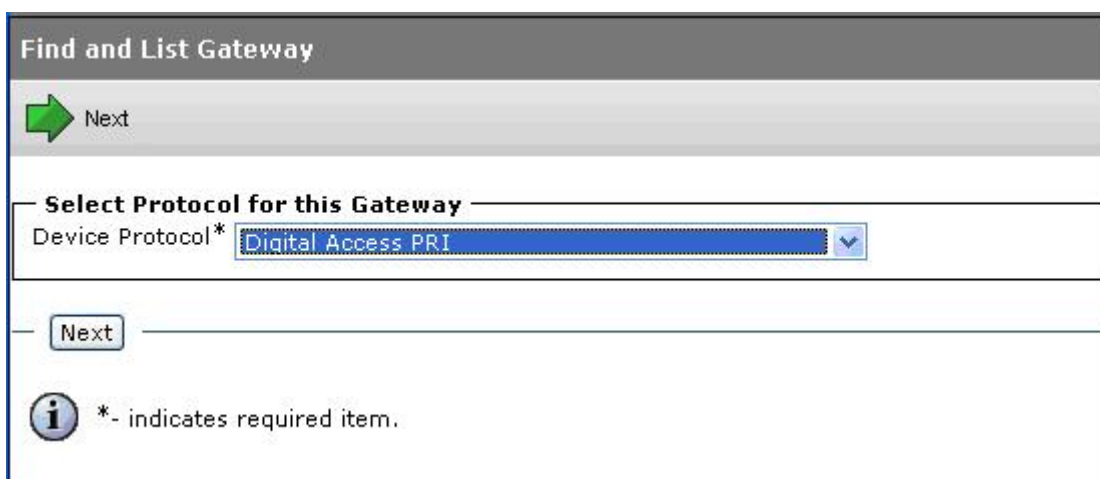
Subunit 1: < None >

Subunit 2: < None >

Subunit 3: < None >

Module in Slot 1: < None >

The **Find and List Gateway** screen is displayed. Select **Digital Access PRI** from the **Device Protocol** drop-down list, and click **Next**.



Find and List Gateway

Next

Select Protocol for this Gateway

Device Protocol*: Digital Access PRI

Next

*- indicates required item.

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

- **Device Pool:** **Default**
- **Call Classification:** **OffNet**
- **NetworkLocale:** **Ireland** (The applicable locale for the network configuration)
- **Media Resource Group List:** **DublinSIL** (The media resource group list from **Section 6.3.**)

Gateway Configuration

Save

Status: Ready

Device Information

Product	Cisco MGCP T1 Port
Gateway	2811.mm.com
Device Protocol	Digital Access PRI
End-Point Name *	S0/SU0/DS1-0@2811.mm.com
Description	S0/SU0/DS1-0@2811.mm.com
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	OffNet
NetworkLocale	Ireland
Packet Capture Mode*	None
Packet Capture Duration	0
Media Resource Group List	DublinSIL
Location*	Hub_None
AAR Group	< None >
Load Information	

☐ Transmit UTF-8 for Calling Party Name

☐ V150 (subset)

Scroll down to the **Interface Information** section. Select **PRI ISO QSIG T1** for the **PRI Protocol Type** field. Ensure **Protocol Side** is set to **User** (User/Slave) to mirror the **Interface** setting of **Peer-Master** (network/master) configured in **Section 3.1**. Select **Top Down** for the **Channel Selection Order** field. Retain the default values for the remaining fields.

Interface Information

PRI Protocol Type*	PRI ISO QSIG T1
Protocol Side*	User
Channel Selection Order*	Top Down
Channel IE Type*	Use Number when 1B
PCM Type*	μ-law
Delay for first restart (1/8 sec ticks)*	32
Delay between restarts (1/8 sec ticks)*	4

☒ Inhibit restarts at PRI initialization

☐ Enable status poll

☐ Unattended Port

☐ Enable G.Clear

Scroll down to the **Call Routing Information – Outbound Calls** section. Select **Allowed** for the **Calling Party Presentation** field and retain the default values for the remaining fields.

Call Routing Information – Outbound Calls	
Calling Party Presentation*	Allowed
Calling Party Selection*	Originator
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Number of digits to strip*	0
Caller ID DN	
SMDI Base Port*	0
Called Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Called Party Transformation CSS	
Calling Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Calling Party Transformation CSS	

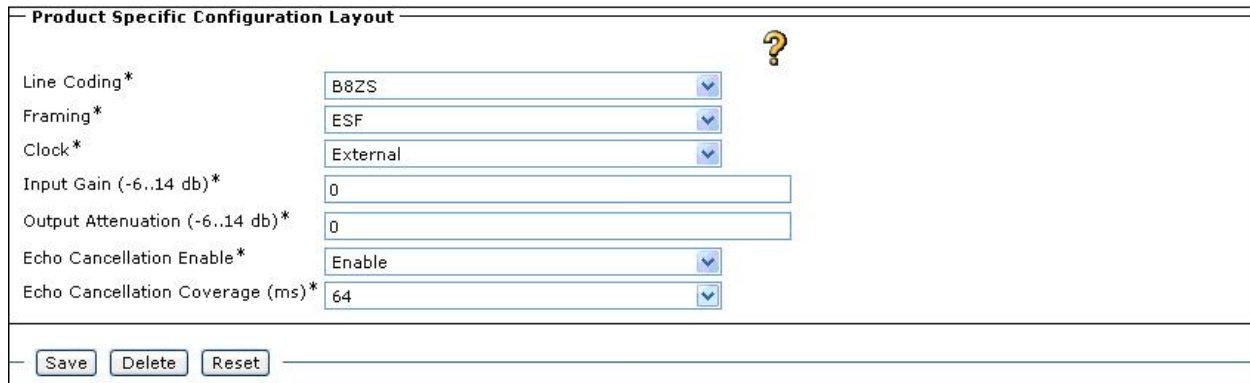
Scroll down to the **PRI Protocol Type Specific Information** section. Select **Allowed** for the **Connected Line ID Presentation (QSIG Inbound Call)** field.

PRI Protocol Type Specific Information	
<input type="checkbox"/> Display IE Delivery	
<input type="checkbox"/> Redirecting Number IE Delivery - Outbound	
<input type="checkbox"/> Redirecting Number IE Delivery - Inbound	
<input checked="" type="checkbox"/> Send Extra Leading Character in Display IE***	
<input type="checkbox"/> Setup non-ISDN Progress Indicator IE Enable****	
<input type="checkbox"/> MCDN Channel Number Extension Bit Set to Zero**	
<input type="checkbox"/> Send Calling Name In Facility IE	
<input type="checkbox"/> Interface Identifier Present**	
Interface Identifier Value**	0
Connected Line ID Presentation (QSIG Inbound Call)*	Allowed

Scroll down to the bottom of the screen. Maintain all default values in the remaining fields, and click **Save**. Click **OK** to the subsequent **Reset Gateway** message pop up box. (Not shown).

Product Specific Configuration Layout	
Line Coding*	B8ZS
Framing*	ESF
Clock*	External
Input Gain (-6..14 db)*	0
Output Attenuation (-6..14 db)*	0
Echo Cancellation Enable*	Enable
Echo Cancellation Coverage (ms)*	64
<input type="button" value="Save"/>	

Next, the screen is updated with additional buttons appearing at the bottom of the screen. Click **Reset**.

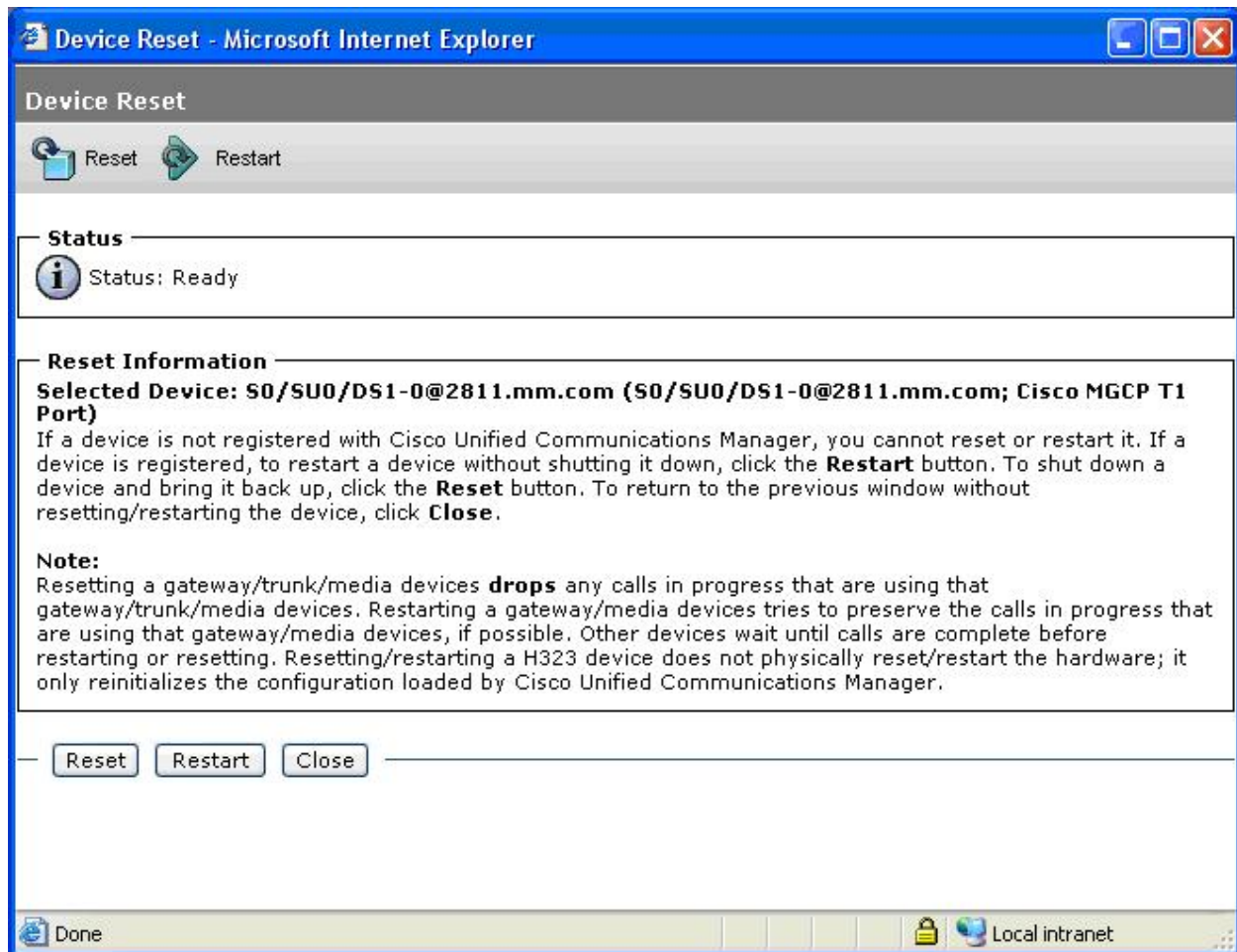


The image shows a web form titled "Product Specific Configuration Layout". It contains several configuration fields with dropdown menus and text inputs. At the bottom, there are three buttons: "Save", "Delete", and "Reset".

Line Coding*	B8ZS
Framing*	ESF
Clock*	External
Input Gain (-6..14 db)*	0
Output Attenuation (-6..14 db)*	0
Echo Cancellation Enable*	Enable
Echo Cancellation Coverage (ms)*	64

Buttons: Save, Delete, Reset

In the **Device Reset** dialog box, click **Reset**, followed by **Close**.



The image shows a "Device Reset" dialog box within a Microsoft Internet Explorer window. The dialog has a title bar "Device Reset - Microsoft Internet Explorer". Inside, there are "Reset" and "Restart" buttons. Below them is a "Status" section showing "Status: Ready". The "Reset Information" section contains text about device registration and a "Note" about call drops. At the bottom, there are "Reset", "Restart", and "Close" buttons.

Device Reset

Reset Restart

Status

Status: Ready

Reset Information

Selected Device: S0/SU0/DS1-0@2811.mm.com (S0/SU0/DS1-0@2811.mm.com; Cisco MGCP T1 Port)

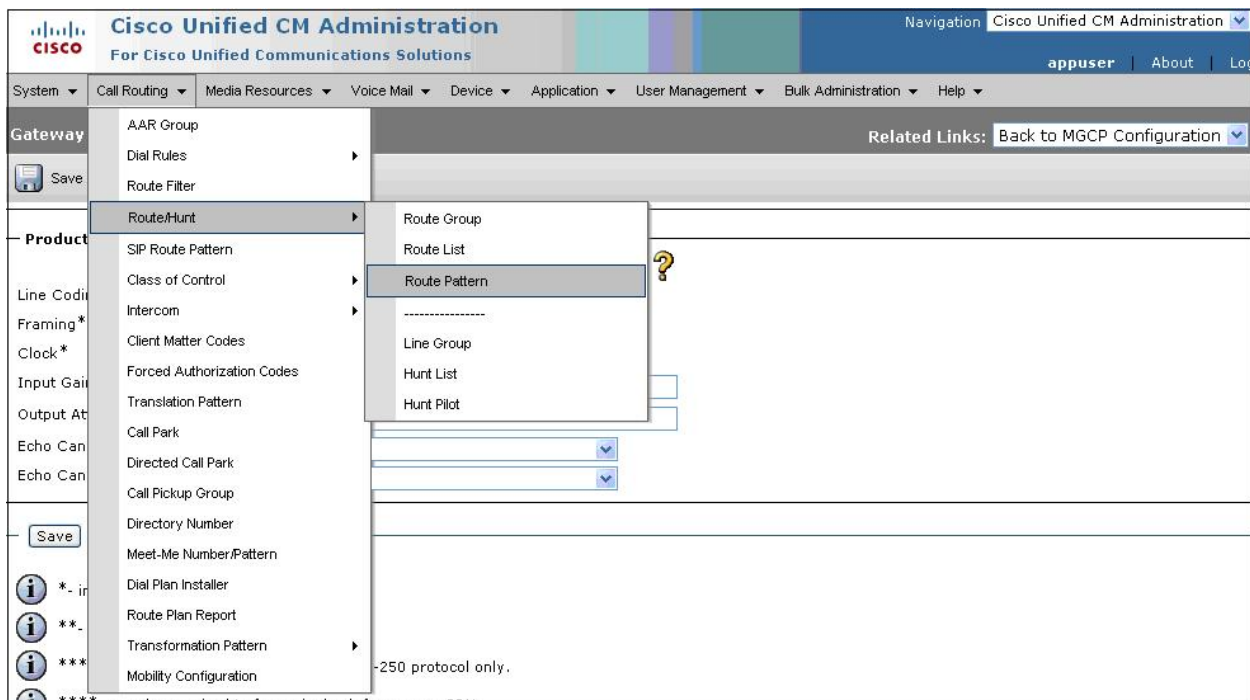
If a device is not registered with Cisco Unified Communications Manager, you cannot reset or restart it. If a device is registered, to restart a device without shutting it down, click the **Restart** button. To shut down a device and bring it back up, click the **Reset** button. To return to the previous window without resetting/restarting the device, click **Close**.

Note:
Resetting a gateway/trunk/media devices **drops** any calls in progress that are using that gateway/trunk/media devices. Restarting a gateway/media devices tries to preserve the calls in progress that are using that gateway/media devices, if possible. Other devices wait until calls are complete before restarting or resetting. Resetting/restarting a H323 device does not physically reset/restart the hardware; it only reinitializes the configuration loaded by Cisco Unified Communications Manager.

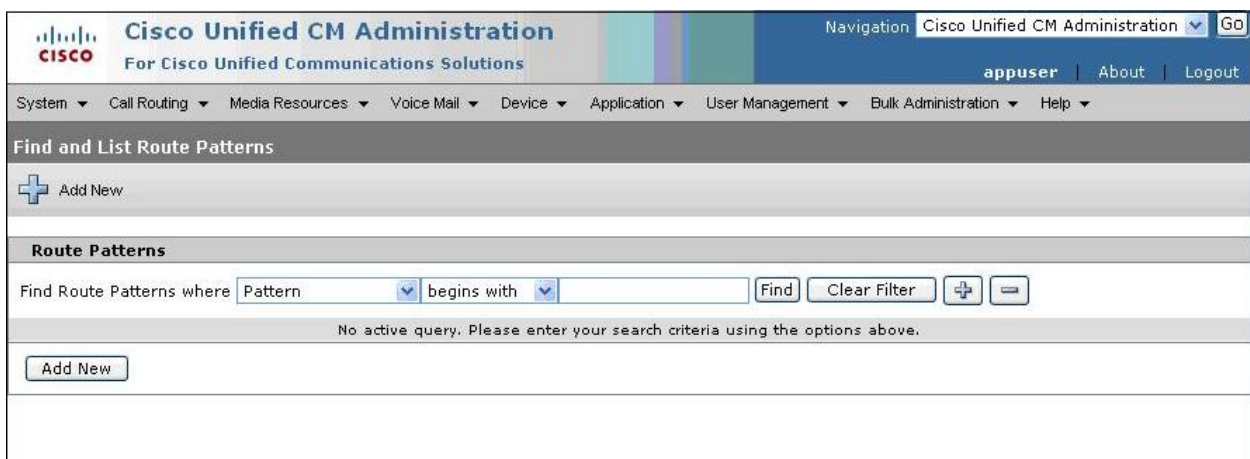
Reset Restart Close

6.6. Administer Route Pattern

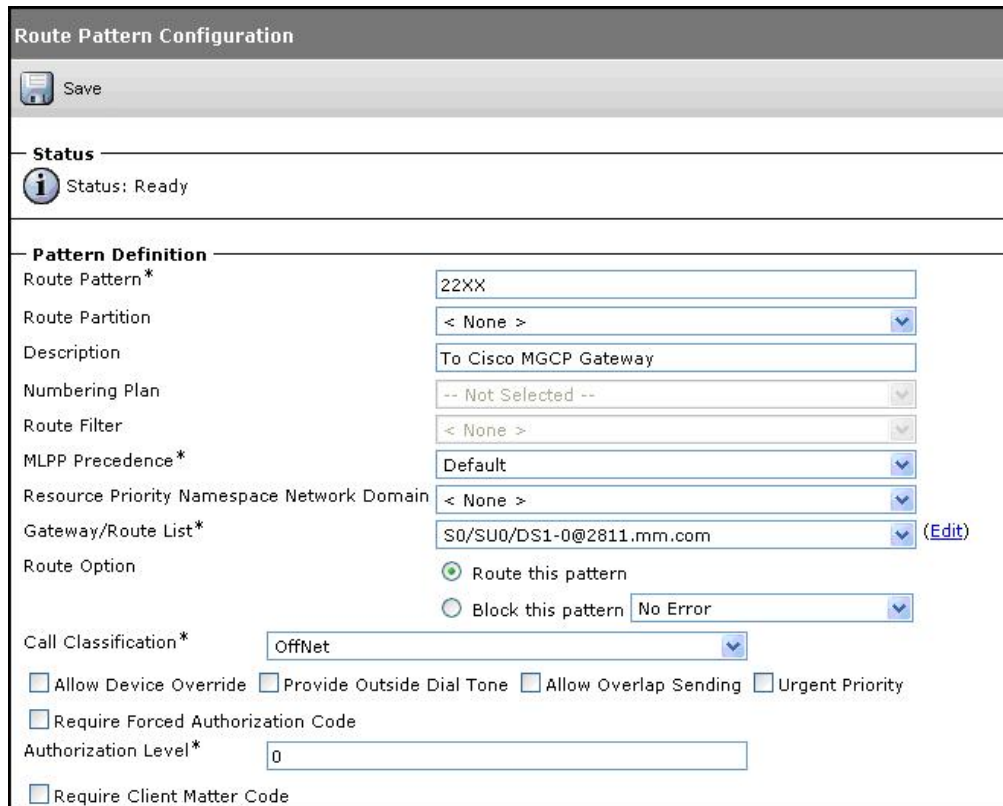
Scroll to the top of the screen, and select **Call Routing → Route/Hunt → Route Pattern**, as shown below.



The **Find and List Route Patterns** screen is displayed. Click **Add New** to add a new route pattern.



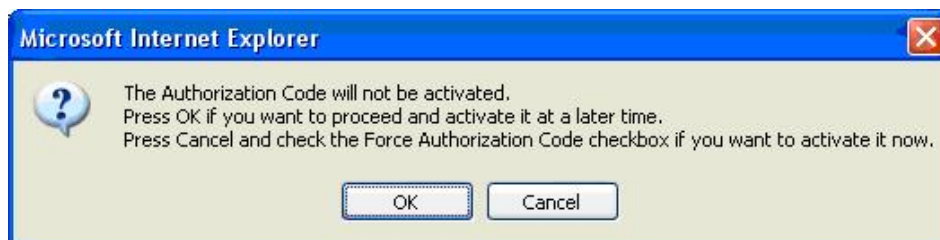
The **Route Pattern Configuration** screen is displayed. Enter a route pattern for the **Route Pattern** field, in this case **22XX** to denote the 4-digit numbering plan for extensions at the Central site. Enter a descriptive text for the **Description** field, and select the MGCP gateway from **Section 6.5** for the **Gateway/Route List** field drop-down list. Uncheck the **Provide Outside Dial Tone** field. Retain the default values in the remaining fields, and scroll down to the bottom of the screen to click **Save** (not shown).





The screenshot shows the 'Route Pattern Configuration' window. At the top is a 'Save' button. Below it is a 'Status' section showing 'Status: Ready'. The main section is 'Pattern Definition' with the following fields:

- Route Pattern*: 22XX
- Route Partition: < None >
- Description: To Cisco MGCP Gateway
- Numbering Plan: -- Not Selected --
- Route Filter: < None >
- MLPP Precedence*: Default
- Resource Priority Namespace Network Domain: < None >
- Gateway/Route List*: S0/SU0/DS1-0@2811.mmm.com (with an 'Edit' link)
- Route Option:
 - ☒ Route this pattern
 - ☐ Block this pattern (with a 'No Error' dropdown)
- Call Classification*: OffNet
- Checkboxes:
 - ☐ Allow Device Override
 - ☐ Provide Outside Dial Tone
 - ☐ Allow Overlap Sending
 - ☐ Urgent Priority
 - ☐ Require Forced Authorization Code
- Authorization Level*: 0
- ☐ Require Client Matter Code

Click **OK** on the two subsequent pop up dialog boxes.

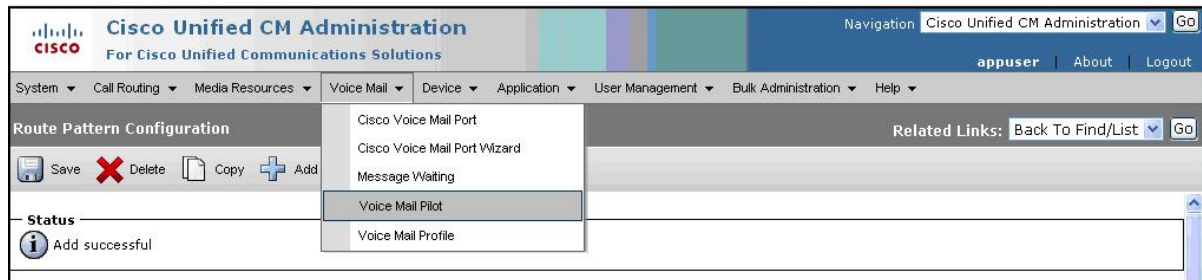


In this test configuration the Mail Pilot number used was 4299. Therefore a second route pattern must be administered for 4299 to allow calls to be sent to the centralized Avaya Modular Messaging system. Repeat the steps described earlier in this section using 4299 as the **Route Pattern** as shown below.

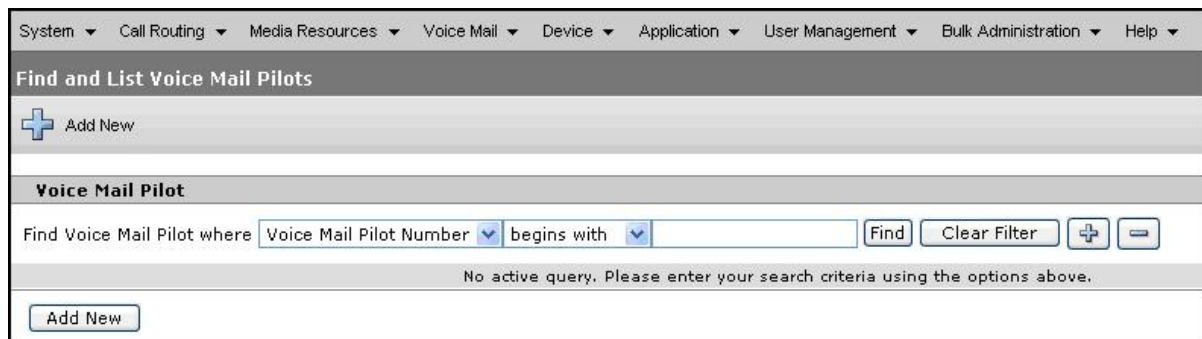
Route Pattern Configuration	
 Save	
Status  Status: Ready	
Pattern Definition	
Route Pattern*	4299
Route Partition	< None >
Description	MM Number
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
Resource Priority Namespace Network Domain	< None >
Gateway/Route List*	S0/SU0/DS1-0@2811.mm.com (Edit)
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error
Call Classification*	OffNet
<input type="checkbox"/> Allow Device Override <input checked="" type="checkbox"/> Provide Outside Dial Tone <input type="checkbox"/> Allow Overlap Sending <input type="checkbox"/> Urgent Priority <input type="checkbox"/> Require Forced Authorization Code	
Authorization Level*	0
<input type="checkbox"/> Require Client Matter Code	

6.7. Administer Voice Mail Pilot

Scroll to the top of the screen, and select **Voice Mail** → **Voice Mail Pilot**, as shown below.



The **Find and List Voice Mail Pilots** screen is displayed. Click **Add New** to add a new voice mail pilot for Avaya Modular Messaging.

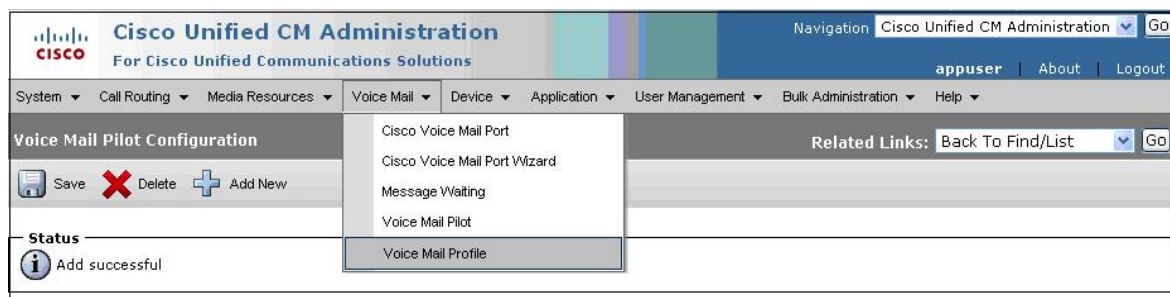


The **Voice Mail Pilot Configuration** screen is displayed next. Enter the Avaya Modular Messaging pilot number into the **Voice Mail Pilot Number** field, in this case **4299**. Enter a descriptive text into the **Description** field, and click **Save**.

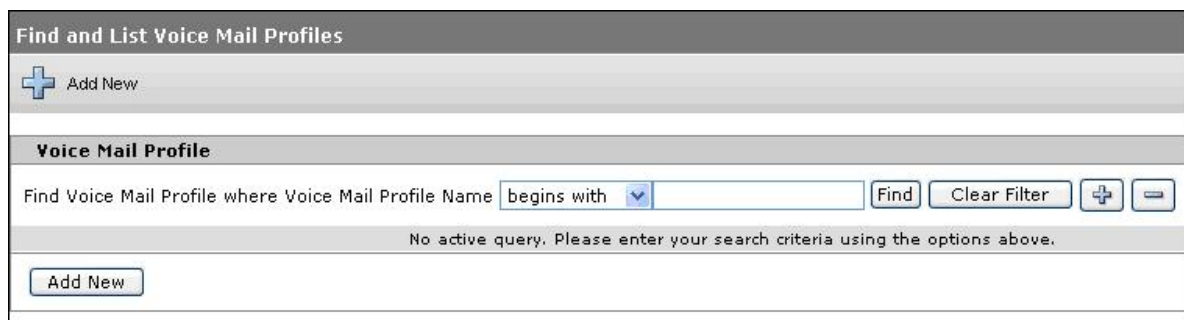
The screenshot shows the 'Voice Mail Pilot Configuration' screen. It has a 'Save' button at the top left. The 'Status' section shows 'Status: Ready'. The 'Voice Mail Pilot Information' section has fields for 'Voice Mail Pilot Number' (4299), 'Calling Search Space' (< None >), and 'Description' (Centralized Messaging with Avaya Modular Messaging). There is a checkbox for 'Make this the default Voice Mail Pilot for the system'. A 'Save' button is at the bottom left.

6.8. Administer Voice Mail Profile

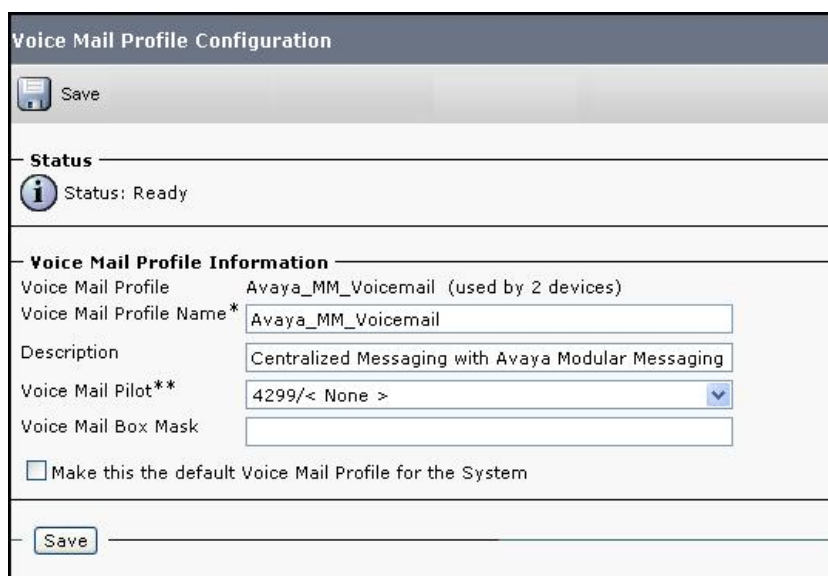
Scroll to the top of the screen, and select **Voice Mail** → **Voice Mail Profile**, as shown below.



The **Find and List Voice Mail Profiles** screen is displayed. Click **Add New** to add a new voice mail profile for Avaya Modular Messaging.

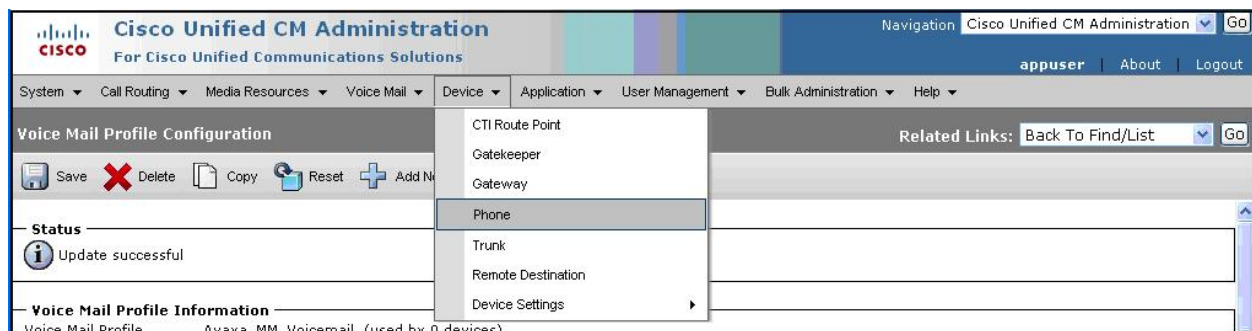


The **Voice Mail Profile Configuration** screen is displayed next. Enter a descriptive name and description into the **Voice Mail Profile Name** and **Description** fields. For the **Voice Mail Pilot** field, select the voice mail pilot number administered in **Section 6.7** from the drop-down list. Click **Save**.

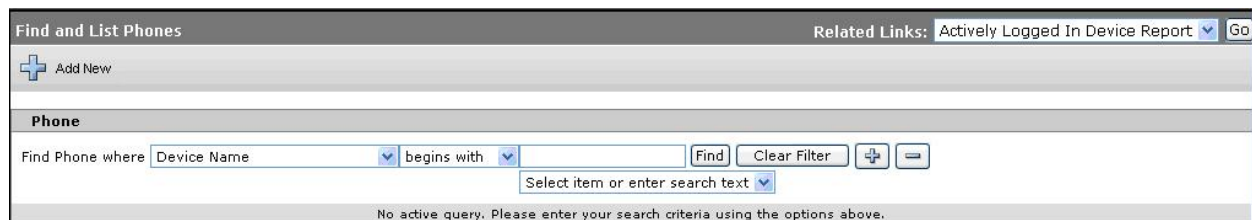


6.9. Administer Phones

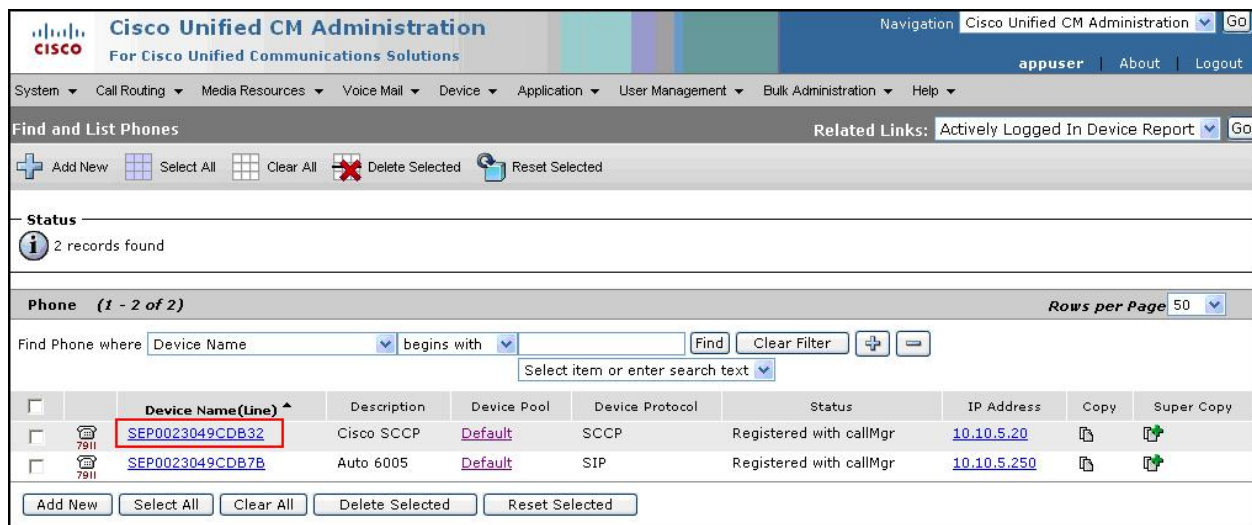
Scroll to the top of the screen, and select **Device** → **Phone**, as shown below.



The **Find and List Phones** screen is displayed. Click **Find**.



The **Find and List Phones** screen is updated with a listing of all existing phones. Click on the **Device Name** field for a phone that will use Avaya Modular Messaging for voice messaging services.



The **Phone Configuration** screen is displayed next. Click the first directory number in the left pane, in this case **Line [1] – 6010 (no partition)**.

Phone Configuration Related Links: [Back To Find/List](#) Go

Save Delete Copy Reset Add New

Status
Status: Ready

Association Information
Modify Button Items

1	7911 Line [1] - 6010 (no partition)
2	None
3	Add a new SD
4	Add a new SD
5	Add a new SD
6	Add a new SD

Phone Type
Product Type: Cisco 7911
Device Protocol: SSCP

Device Information
Registration: Registered with Cisco Unified Communications Manager callMgr
IP Address: 10.10.5.20
MAC Address*: 0023049CDB32
Description: Cisco SSCP
Device Pool*: Default [View Details](#)

The **Directory Number Configuration** screen is displayed. Scroll down to the **Directory Number Settings** section. For the **Voice Mail Profile** field, select the voice mail profile created in **Section 6.8** for Avaya Modular Messaging. Retain the default values in the remaining fields.

Cisco Unified CM Administration Navigation: [Cisco Unified CM Administration](#) Go

appuser | About | Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Directory Number Configuration Related Links: [Configure Device \(SEP0023049CDB32\)](#) Go

Save Delete Reset Add New

Directory Number Settings

Voice Mail Profile: Avaya MM Voicemail (Choose <None> to use system default)

Calling Search Space: <None>

Presence Group*: Standard Presence group

User Hold MOH Audio Source: <None>

Network Hold MOH Audio Source: <None>

Auto Answer*: Auto Answer Off

AAR Settings

	Voice Mail	AAR Destination Mask	AAR Group
AAR	<input type="checkbox"/> or		<None>

☒ Retain this destination in the call forwarding history

Scroll down to the **Call Forward and Call Pickup Settings** section. Check the call forward related parameters as shown below.

Call Forward and Call Pickup Settings		
	Voice Mail	Destination
Calling Search Space Activation Policy		
Forward All	<input type="checkbox"/> or	<input type="text"/>
Secondary Calling Search Space for Forward All		
Forward Busy Internal	<input checked="" type="checkbox"/> or	<input type="text"/>
Forward Busy External	<input checked="" type="checkbox"/> or	<input type="text"/>
Forward No Answer Internal	<input checked="" type="checkbox"/> or	<input type="text"/>
Forward No Answer External	<input checked="" type="checkbox"/> or	<input type="text"/>
Forward No Coverage Internal	<input checked="" type="checkbox"/> or	<input type="text"/>
Forward No Coverage External	<input checked="" type="checkbox"/> or	<input type="text"/>
Forward on CTI Failure	<input checked="" type="checkbox"/> or	<input type="text"/>
Forward Unregistered Internal	<input checked="" type="checkbox"/> or	<input type="text"/>
Forward Unregistered External	<input checked="" type="checkbox"/> or	<input type="text"/>
No Answer Ring Duration (seconds)	<input type="text"/>	
Call Pickup Group	<input type="text" value=" < None >"/>	

Scroll down to the **Forwarded Call Information Display on Device SEP0023049CDB32** section. Check all checkboxes, and click **Save**.

Forwarded Call Information Display on Device SEP0023049CDB32
<input checked="" type="checkbox"/> Caller Name
<input checked="" type="checkbox"/> Caller Number
<input checked="" type="checkbox"/> Redirected Number
<input checked="" type="checkbox"/> Dialed Number

Repeat this section for all directory numbers on the phone and for all phones that will use Avaya Modular Messaging for voice messaging services.

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, Avaya Modular Messaging, Cisco 2811 MGCP Gateway and Cisco Unified Communications Manager.

7.1. Verify Avaya Communication Manager

From the SAT interface, verify the status of the T1 QSIG trunk group by using the **status trunk n** command, where **n** is the trunk group number administered in **Section 3.2**. Verify that all trunks are in the **in-service/idle** state as shown below.

```
status trunk 60

                                TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                                Busy

0060/001 01A0601  in-service/idle    no
0060/002 01A0602  in-service/idle    no
0060/003 01A0603  in-service/idle    no
0060/004 01A0604  in-service/idle    no
0060/005 01A0605  in-service/idle    no
0060/006 01A0606  in-service/idle    no
0060/007 01A0607  in-service/idle    no
0060/008 01A0608  in-service/idle    no
0060/009 01A0609  in-service/idle    no
0060/010 01A0610  in-service/idle    no
0060/011 01A0611  in-service/idle    no
0060/012 01A0612  in-service/idle    no
0060/013 01A0613  in-service/idle    no
0060/014 01A0614  in-service/idle    no
```

Verify the status of the T1 QSIG signaling group by using the **status signaling-group n** command, where **n** is the signaling group number administered in **Section 3.3**. Verify the signaling group is **in-service** as indicated in the **Group State** and **Level 3 State** fields shown below.

```
status signaling-group 60

                                STATUS SIGNALING GROUP

Group ID: 60                      Active NCA-TSC Count: 0
Group Type: isdn-pri              Active CA-TSC Count: 0
Signaling Type: facility associated signaling
Group State: in-service

                                Primary D-Channel

Port: 01A0624                    Level 3 State: in-service
```


7.2. Verify Avaya Modular Messaging

Make a call from an Avaya subscriber to a Cisco subscriber and verify that the call covers to Avaya Modular Messaging upon no answer. Leave a voice message for the Cisco subscriber. From the Cisco subscriber, dial the Avaya Modular Messaging pilot number to retrieve the message. Verify that the Avaya Modular Messaging system identifies the Cisco subscriber as a local subscriber, and that the voice message can be retrieved.

Log in to the Avaya Message Storage Server web interface as described in **Section 4.1**. Select **Logs → Subscriber Activity** from the left pane. Enter the mailbox number of the Cisco subscriber, enter the appropriate date and time for the above activities, and click **Display**. Verify that a listing of the detailed activities is displayed into the bottom portion of the right hand pane. Verify that there is an entry showing the message left by the Avaya subscriber (in this case 2203). Also verify that there is an entry showing the message being retrieved.

The screenshot shows the Avaya Modular Messaging Administration web interface. The left sidebar contains a navigation menu with categories like Help, Log Off, Alarm Summary, Disk Information, Server Notes, CMOS Settings, RAID Status, Rebuild RAID Status, Reboot Interval, Utilities, and Logs. The main content area is titled "Subscriber Activity Log" and includes search filters for Mailbox Number (6006), Start Date (March 26, 2009, 14:00), and End Date (March 26, 2009, 14:07). A "Display" button is present. Below the filters, a table lists activities for Name: SIP, Cisco and Mailbox Number: 6006. The table has columns for Date, Time, Activity, and Description. Red circles highlight specific entries in the table.

Date	Time	Activity	Description
03/26/2009	14:00	received	CA message from 2203 new=1(v=1 f=0 e=0 dsn=0) un=0 o=0 d=0 x=0
03/26/2009	14:01	inbox-stat	id=c2ab0 port=55143 IP=192.168.1.250 new=1(v=1 f=0 e=0 dsn=0) un=0 o=0 d=0 x=0
03/26/2009	14:01	inbox-sel	id=c2ab0 port=55143 IP=192.168.1.250 msgs=1
03/26/2009	14:01	status	changed from new to old for message received 3/26/09 at 14:00
03/26/2009	14:01	status	changed from old to deleted for message received 3/26/09 at 14:00
03/26/2009	14:01	inbox-stat	id=c2ab0 port=55143 IP=192.168.1.250 new=0(v=0 f=0 e=0 dsn=0) un=0 o=0 d=1 x=0
03/26/2009	14:01	status	changed from deleted to removed for message received 3/26/09 at 14:00
03/26/2009	14:01	inbox-dsel	id=c2ab0 port=55143 IP=192.168.1.250 msgs=0

7.3. Verify Cisco 2811 MGCP Gateway and Cisco Unified Communications Manager

From the Cisco 2811 MGCP Gateway command line interface, enter the **show isdn status** command to verify connectivity. Verify that the **Layer 1 Status** is **ACTIVE**, and that the **Layer 2 Status** is **MULTIPLE_FRAME_ESTABLISHED**, as shown below.

```
2811#show isdn status
Global ISDN Switchtype = primary-qsig

%Q.931 is backhauled to CCM MANAGER 0x0003 on DSL 0. Layer 3 output may not apply

ISDN Serial0/0/0:23 interface
    dsl 0, interface ISDN Switchtype = primary-qsig
    **** Slave side configuration ****
    L2 Protocol = Q.921 0x0000 L3 Protocol(s) = CCM MANAGER 0x0003
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask: 0x8000003F
    Number of L2 Discards = 1, L2 Session ID = 63
    Total Allocated ISDN CCBs = 0
```

Enter the **show ccm-manager** command to verify the registration status with Cisco Unified Communications Manager. Verify that the **Status** is **Registered**, and that the **Host** contains the name administered in **Section 5.2**.

```
2811#show ccm-manager
MGCP Domain Name: 2811.mm.com
Priority      Status      Host
=====
Primary      Registered  callmgr.avayalabs.com (10.10.5.100)
First Backup  None
Second Backup None

Current active Call Manager: 10.10.5.100
Backhaul/Redundant link port: 2428
Failover Interval: 30 seconds
Keepalive Interval: 15 seconds
Last keepalive sent: 14:01:36 UTC Mar 26 2009 (elapsed time: 00:00:03)
)
Last MGCP traffic time: 14:01:36 UTC Mar 26 2009 (elapsed time: 00:00:03)
)
Last failover time: None
Last switchback time: None
Switchback mode: Graceful
MGCP Fallback mode: Not Selected
Last MGCP Fallback start time: None
Last MGCP Fallback end time: None
MGCP Download Tones: Disabled
```

7.4. Verification Scenarios

The verification scenarios for the configuration described in these Application Notes included the following:

- The Cisco subscribers were properly recognized by Avaya Modular Messaging upon dialing the Avaya Modular Messaging pilot number, and that the Cisco subscribers can log in without entering the mailbox number.
- The Cisco subscribers were properly identified by Avaya Modular Messaging as the calling party for voice messages left for other subscribers.
- Avaya Modular Messaging turns the message waiting indicator ON and OFF appropriately for voice messages left and retrieved for the Cisco subscribers.
- The Cisco subscribers can activate Call Forwarding and have calls cover immediately to Avaya Modular Messaging. Avaya Modular Messaging appropriately identifies the Cisco subscribers as the called party.
- Avaya Modular Messaging appropriately identifies the original dialed endpoint as the called party for scenarios with Multiple Call Forwarding, where a called party has calls forwarded to another party that covers to Avaya Modular Messaging upon no answer.
- The following Avaya Modular Messaging features work properly with Cisco subscribers:
 - Receptionist
 - Auto Attendant
 - Find Me
 - Call Me
 - Call Sender
 - Transfer

8. Conclusion

As illustrated in these Application Notes, Avaya Communication Manager 5.1.2 can interoperate with Cisco Unified Communications Manager 7.0 and Avaya Modular Messaging 5.0 to form a Centralized Messaging Solution using T1 QSIG.

There are two interoperability issues to note from the testing.

1. For the Multiple Call Forwarding scenario involving an Avaya calling endpoint to a Cisco called endpoint that has calls forwarded to another Avaya endpoint, the unanswered call continues to ring at the forward-to destination (Avaya endpoint) instead of covering to the original called party's voicemail.
2. A Cisco subscriber's Busy greeting will not be heard by callers. For example, a caller will hear the Ring No Answer greeting if the called Cisco subscriber is on the telephone, and the call is answered by Avaya Modular Messaging. This limitation does not apply to Avaya subscribers with configured Busy greetings.

9. Additional References

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

- *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 4, January 2008, available at <http://support.avaya.com>.
- *CN 88003 Avaya Definity G3, Prologix & S8300/S8500/S8700 T1 QSIG*, Version AM, February 2009, available at <http://support.avaya.com>.
- *Modular Messaging for the Avaya Message Store Server (MSS) Configuration Release 5.0 Installation and Upgrade*, February 2009, available at <http://support.avaya.com>.
- *Cisco Unified Communications Manager and Cisco IOS Interoperability Configuration Guide*, available at <http://www.cisco.com>.
- *Cisco 2600 and 3600 Routers MGCP Voice Gateway Interoperability with Cisco Communication Manager*, available at <http://www.cisco.com>.
- *Cisco Unified Communications Manager Administration Guide*, Release 7.0(1), available at <http://www.cisco.com>.
- *Cisco 1-, 2-, and 4-Port T1/E1 HWICs and 8-Port T1/E1 Network Module*, available at <http://www.cisco.com>.

©2009 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 interoplabinotes@list.avaya.com