# Using Cisco Unified Communications Manager to Configure MGCP Gateway Support

This chapter provides information about using Cisco Unified Communications Manager to configure MGCP Gateway Support on the Cisco VGD 1T3 voice gateway platform. This chapter describes the MGCP Gateway support information and configuration procedures and includes the following:



## Prerequisites for MGCP Gateway Support

Prerequisites for MGCP Gateway Support are defined in the following sections:



### Cisco IOS Voice Gateway

The following prerequisites pertain specifically to the configuration of MGCP Gateway Support on a Cisco IOS voice gateway:

- Cisco IOS Release 12.4(20)YA or a later release.
- Transcoder and MTP services must be configured on the voice gateway. See "Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers" on page 67.
- SCCP must be enabled on the local interface that the voice gateway uses to register with Cisco Unified Communications Manager. See the "Enabling SCCP on the Cisco Unified Communications Manager Interface" section on page 81.


**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

- The **sccp ccm** command must use the keyword **version 6.1.2** or **version 7.0.3**.

## Cisco Unified Communications Manager

The following prequesities pertain specifically to RSVP Agent in a Cisco Unified Communications Manager network:

- Cisco Unified Communications Manager 6.1.2, 7.0.3, or a later release.
- Transcoder and MTP services must be configured in Cisco Unified Communications Manager. See the following chapters in the *Cisco Unified Communications Manager Administration Guide*:
  - "Media Termination Point Configuration"
  - "Transcoder Configuration"

# Restrictions for Configuring MGCP Gateway Support

- Support for adding the Cisco VGD 1T3 as a Cisco Unified Communications Manager controlled MGCP gateway requires Cisco Unified Communications Manager version 6.1(2), 7.0(3), or later.
- Only one Cisco VGD 1T3 gateway is supported per Cisco Unified Communications Manager subscriber node.
- Integrated access is not supported when you control voice traffic using MGCP and Cisco Unified Communications Manager. Integrated access is when the channels on a T1 interface are divided between a group used for voice and another group used for WAN access.
- T1 protocols, such as QSIG T1 FGD, and PRI NFAS, are not supported with MGCP.

**Note** Any configuration update that affects MGCP should be performed during a planned maintenance window while MGCP is disabled; otherwise, updating the configuration could disrupt MGCP functionality. Before making any configuration changes, disable MGCP using the **no mgcp** command. After all configuration changes are completed, use the **mgcp** command to enable MGCP.

# Information About MGCP Gateway Support

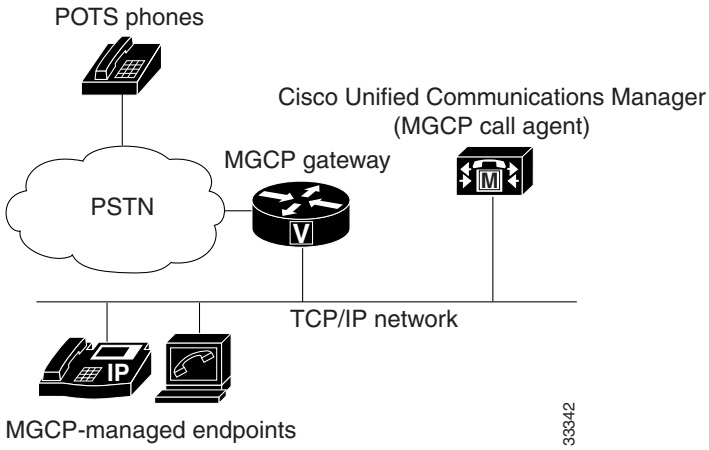
MGCP enables the remote control and management of voice and data communications devices at the edge of multiservice IP packet networks. Because of its centralized architecture, MGCP overcomes the distributed configuration and administration problems inherent in the use of protocols such as H.323. MGCP simplifies the configuration and administration of voice gateways and supports multiple (redundant) call agents, eliminating the potential for a single point of failure in controlling the Cisco IOS gateway in the network.

MGCP can be configured as a master or slave protocol to ensure that the gateway receives and executes the configuration, control, and management commands that are issued by Cisco Unified Communications Manager. The MGCP gateway is under the control of Cisco Unified Communications Manager.

MGCP uses endpoints and connections to construct a call. Endpoints are sources of or destinations for data and can be physical or logical locations identifying a device. The voice ports on the Cisco MGCP gateway are its endpoints. Connections can be point-to-point or multipoint. Cisco Unified Communications Manager acts as the MGCP call agent, managing connections between endpoints and controlling how the Cisco IOS gateway functions.

Figure 1 shows a typical MGCP gateway that is controlled by an MGCP call agent.

***Figure 1 MGCP Gateway Controlled by Cisco Unified Communications Manager***




The MGCP gateway receives most of its required configuration from the call agent. To configure an MGCP gateway, you simply identify the Cisco Unified Communications Manager server associated with the gateway and identify the gateway to the call agent. The MGCP gateway handles the translation between voice signals and the packet network and interacts with the Cisco Unified Communications Manager server. The server performs signal and call processing.

# Configuring MGCP Gateway Support

This section contains the following procedures:

- Configuring MGCP on the Cisco VGD 1T3 Voice Gateway, page 120 (required)
- Verifying MGCP Configuration on the Cisco VGD 1T3 Voice Gateway, page 121 (optional)
- Configuring Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback, page 123 (required)
- Verifying Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback, page 128
- Configuring POTS Dial Peers on MGCP Gateways, page 129 (required)
- Verifying Dial Peer Configuration for MGCP Gateways, page 131 (optional)
- Configuring Single-Point Configuration for MGCP Gateways, page 133 (optional)
- Verifying Single-Point Configuration for MGCP Gateways, page 135 (optional)
- Configuring Multicast Music-on-Hold Support for Cisco Unified Communications Manager, page 136 (optional)
- Verifying Music-on-Hold, page 138 (optional)

- Configuring MGCP PRI Backhaul and T1 CAS Support for Cisco Unified Communications Manager, page 139
- Verifying the MGCP PRI Backhaul Configuration, page 142


# Configuring MGCP on the Cisco VGD 1T3 Voice Gateway

Perform this task to configure MGCP on the Cisco VGD 1T3 voice gateway to support Cisco Unified Communications Manager.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitEthernet** *slot/port*
4. **ip address** *ip-address subnetmask*
5. **no shutdown**
6. **exit**
7. **hostname** *name*
8. **mgcp**
9. **mgcp call-agent** {*ip-address* | *host-name*} [*port*] [**service-type** *type*] [**version** *version-number*]
10. **mgcp dtmf-relay voip codec** {**all** | **low-bit-rate**} **mode** {**cisco** | **nse** | **out-of-band**}
11. **ccm-manager mgcp**
12. **exit**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password when prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface gigabitEthernet** *slot/port*<br><br>**Example:**<br>`Router(config)# interface gigabitEthernet 0/0` | Enters interface configuration mode so that you can configure the gigabitEthernet interface for communicating with Cisco Unified Communications Manager.<br>• *slot* and *port* syntax is platform-dependent; type **?** to determine. |

| | Command | Purpose |
|---|---|---|
| **Step 4** | **ip address** *ip-address subnetmask*<br><br>**Example:**<br>`Router(config-if)# ip address 10.10.2.23 255.255.255.255` | Configures an IP address and subnet mask on the router's Ethernet interface. |
| **Step 5** | **no shutdown**<br><br>**Example:**<br>`Router(config-if)# no shutdown` | Activates the Ethernet port. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | Exits interface mode and enters global configuration mode. |
| **Step 7** | **hostname** *name*<br><br>**Example:**<br>`Router(config)# hostname smith` | Assigns a unique name to a network router which enables Cisco Unified Communications Manager to identify the device.<br>• Default device name is Router. |
| **Step 8** | **mgcp**<br><br>**Example:**<br>`Router(config)# mgcp` | Enables the MGCP protocol. |
| **Step 9** | **mgcp call-agent** {*ip-address* \| *host-name*} [*port*] [**service-type** *type*] [**version** *version-number*]<br><br>**Example:**<br>`Router(config)# mgcp call-agent 10.0.0.21 mgcp 0.1` | Specifies the primary Cisco Unified Communications Manager server's IP address or domain name, and the port gateway service type and version number. |
| **Step 10** | **mgcp dtmf-relay voip codec** {**all** \| **low-bit-rate**} **mode** {**cisco**\| **nse** \| **out-of-band**}<br><br>**Example:**<br>`Router(config)# mgcp dtmf-relay voip codec all mode cisco` | Selects the codec type and the dual tone multifrequency (DTMF) relay services. |
| **Step 11** | **ccm-manager mgcp**<br><br>**Example:**<br>`Router(config)# ccm-manager mgcp` | Enables the MGCP gateway to support Cisco Unified Communications Manager. |
| **Step 12** | **exit**<br><br>**Example:**<br>`Router(config)# exit` | Exits global configuration mode. |

# Verifying MGCP Configuration on the Cisco VGD 1T3 Voice Gateway

The **show** commands described in this section can be used to verify the MGCP configuration.

## SUMMARY STEPS

1. **show running-config**
2. **show interfaces ethernet** [*number*]
3. **show mgcp**

## DETAILED STEPS

### Step 1 show running-config

Use the **show running-config** command to verify that MGCP is enabled on the voice gateway:

```
Router# show running-config
.
.
.
hostname vgd 1t3
!
.
.
.
mgcp
mgcp call-agent 10.0.0.21 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
!
ccm-manager mgcp
!
interface Ethernet0/1
 ip address 10.10.2.23 255.255.255.0
 half-duplex
```

### Step 2 show interfaces gigabitEthernet

Use the **show interfaces gigabitEthernet** command to verify that a Gigabit Ethernet interface is configured to communicate with the Cisco Unified Communications Manager server, for example:

```
Router# show interfaces gigabitEthernet0/0

interface GigabitEthernet0/0
 ip address 10.1.200.68 255.255.0.0
 duplex auto
 speed auto
 negotiation auto
 no keepalive
 no cdp enable
 no mop enabled
!
```

### Step 3 show mgcp

Use the **show mgcp** command to display the MGCP settings on the CiscoVGD 1T3 voice gateway:

```
Router# show mgcp

MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
!MGCP call agent with IP address for Cisco Unified Communications Manager:
MGCP call-agent: 10.0.0.21 2427 Initial protocol service is MGCP, v. 0.1
MGCP block-newcalls DISABLED
MGCP send RSIP for SGCP is DISABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
```

```
!DTMF-relay voip codec parameters:
MGCP dtmf-relay voip codec all mode out-of-band
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough mode: CISCO, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough mode: NSE, codec: g711ulaw
MGCP TSE payload: 0
MGCP Network (IP/AAL2) Continuity Test timer: 200
MGCP 'RTP stream loss' timer: 5
MGCP request timeout 500, MGCP request retries 3
MGCP rtp unreachable timeout 1000
MGCP gateway port: 2427, MGCP maximum waiting delay 3000
MGCP restart delay 0, MGCP vad DISABLED
MGCP simple-sdp DISABLED
MGCP undotted-notation DISABLED
MGCP codec type g711ulaw, MGCP packetization period 20
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lmw 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP IP ToS low delay disabled, MGCP IP ToS high throughput disabled
MGCP IP ToS high reliability disabled, MGCP IP ToS low cost disabled
MGCP IP RTP precedence 5, MGCP signaling precedence: 3
MGCP default package: line-package
MGCP supported packages: gm-package dtmf-package trunk-package line-package
hs-package rtp-package ms-package dt-package sst-packagc-package
MGCP VoAAL2 ignore-lco-codec DISABLED
MGCP T.38 Fax is DISABLED
```

**Note** For a description of the fields displayed in this output, see the individual commands in the *Cisco IOS Voice Command Reference*.

# Configuring Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback

This section describes how to configure Cisco Unified Communications Manager failover capabilities on the MGCP gateway.

## Switchover (Failover)

Cisco IOS gateways can maintain links to up to two backup Cisco Unified Communications Manager servers in addition to a primary Cisco Unified Communications Manager. This redundancy enables a voice gateway to switchover to a backup if the gateway loses communication with the primary. The backup server takes control of the devices that are registered with the primary Cisco Unified Communications Manager. The second backup takes control of the registered devices if both the primary and first backup Cisco Unified Communications Manager fail. The gateway preserves existing connections during a switchover to a backup Cisco Unified Communications Manager.

When the primary Cisco Unified Communications Manager server becomes available again, control reverts to that server. Reverting to the primary server can occur immediately, after a configurable amount of time, or only when all connected sessions are released.

## Switchback

Switchback is the process a voice gateway uses to reestablish communication with the primary Cisco Unified Communications Manager server when the server becomes available again. Switchback can occur immediately, at a specified time after the last active call ends, or after a specified length of time.

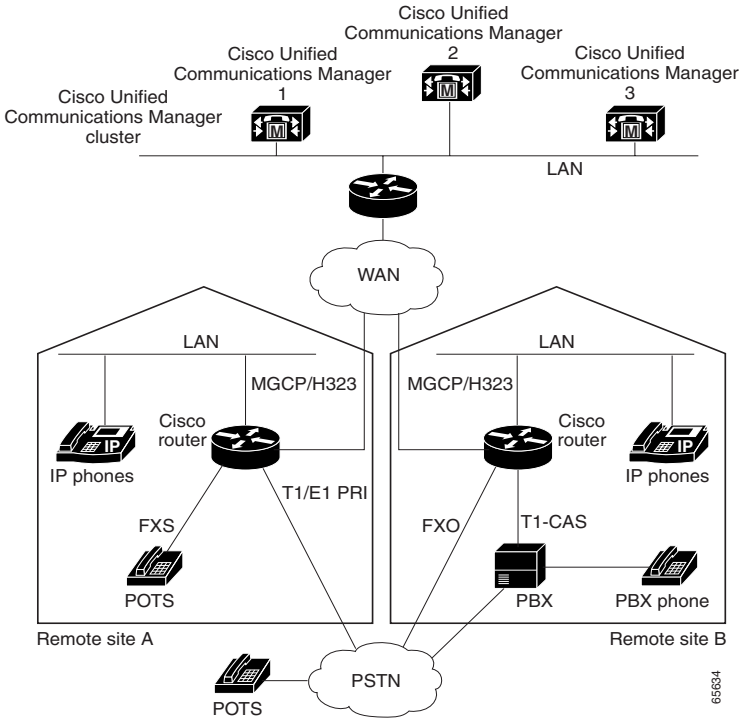
## MGCP Gateway Fallback

The MGCP gateway maintains a remote connection to a centralized Cisco Unified Communications Manager cluster by sending MGCP keepalive messages to the Cisco Unified Communications Manager server at 15-second intervals. If the active Cisco Unified Communications Manager server fails to acknowledge receipt of the keepalive message within 30 seconds, the gateway attempts to switch over to the next available Cisco Unified Communications Manager server.

If none of the Cisco Unified Communications Manager servers respond, the gateway switches into fallback mode and reverts to the default H.323 session application for basic call control. H.323 is a standardized communication protocol that enables dissimilar devices to communicate with each other through use of a common set of codecs, call setup and negotiating procedures, and basic data transport methods. The gateway processes calls on its own using H.323 until one of the Cisco Unified Communications Manager connections is restored.

Figure 2 illustrates a typical VoIP network topology in which MGCP gateway fallback is supported.

***Figure 2 Typical VoIP Network Topology Supporting the MGCP Gateway Fallback Feature***




The MGCP Gateway Fallback feature provides the following functionality:

- MGCP gateway fallback support—All active MGCP analog and T1 CAS calls are maintained during the fallback transition. Callers are unaware of the fallback transition, and the active MGCP calls are cleared only when the communicating callers hang up. Active MGCP PRI backhaul calls are released during fallback.

  Any transient MGCP calls (that is, calls that are not in the connected state) are cleared at the onset of the fallback transition and must be attempted again later.

- Basic connection services in fallback mode—Provides basic connection services for IP telephony traffic that passes through the gateway. When the local MGCP gateway transitions into fallback mode, the default H.323 session application assumes responsibility for handling new calls. Only basic two-party voice calls are supported during the fallback period.

  Except for ISDN T1 PRI calls, all the MGCP calls that are active at the time of fallback are preserved, but transient calls are released. When a user completes (hangs up) an active MGCP call, the MGCP application handles the on-hook event and clears all call resources.

- Rehome support—Provides a rehome function in the gateway fallback mode that detects the restoration of a WAN TCP connection to the primary Cisco Unified Communications Manager server.

  When the fallback mode is in effect, the affected MGCP gateway repeatedly tries to open a TCP connection to a Cisco Unified Communications Manager server in the prioritized list of call agents. This process continues until one of the Cisco Unified Communications Manager servers in the prioritized list responds.

  The TCP open request from the MGCP gateway is honored, and the gateway reverts to MGCP mode. The gateway sends a Restart-in-Progress (RSIP) message to begin registration with the responding Cisco Unified Communications Manager.

  All currently active calls that are initiated and set up during the fallback period are maintained by the default H.323 session application, except ISDN T1 PRI calls. Transient calls are released. After rehome occurs, the new Cisco Unified Communications Manager assumes responsibility for controlling new IP telephony activity.

The following types of interfaces on the gateway are supported:

- FXS analog interfaces—For connecting to the PSTN or analog phones
- FXO analog interfaces—For connecting to the PSTN or PBXs
- T1 CAS digital interfaces—For connecting to the PSTN or PBXs
- T1 PRI digital interfaces—For connecting to PBXs and central offices (COs)

## MGCP Gateway Registration with Cisco Unified Communications Manager

Table 1 describes what can happen when either the gateway loses connection to the primary Cisco Unified Communications Manager or the gateway also loses connection to all backup Cisco Unified Communications Manager servers.

*Table 1 Registration Scenarios*

| Terminology | Connection | Registration |
|---|---|---|
| **Gateway Connection to Primary Cisco Unified Communications Manager** | | |
| Failover (also called switchover) | Gateway loses connection to primary Cisco Unified Communications Manager. | Gateway switches over to a backup. |
| Switchback | Gateway reconnects to primary Cisco Unified Communications Manager. | Gateway switches back to the primary. |
| **Gateway connection to all Cisco Unified Communications Manager Servers** | | |
| Fallback | Gateway loses connection to primary and all backup Cisco Unified Communications Manager servers. | Gateway falls back to H.323 call processing. |
| Rehome | Gateway reconnects to one of the Cisco Unified Communications Manager servers. | Gateway rehomes, resuming MGCP call processing. |

Any calls at the time of reregistration (even those in a transient state such as call setup) remain undisturbed. The newly registered Cisco Unified Communications Manager determines the status of existing calls and maintains or deletes them as appropriate.

## Benefits of Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback

- Eliminates a potential single point of failure in the VoIP network by allowing you to designate up to two backup Cisco Unified Communications Manager servers. Your MGCP voice gateways can continue working if the primary Cisco Unified Communications Manager server fails.
- Ensures greater stability in the voice network by preserving existing connections during a switchover to a backup Cisco Unified Communications Manager server.
- Prevents call-processing interruptions or dropped calls in the event of a Cisco Unified Communications Manager or WAN failure.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ccm-manager redundant-host** {*ip-address* | *DNS-name*} [*ip-address* | *DNS-name*]
4. **ccm-manager switchback** {**graceful** | **immediate** | **schedule-time** *hh*:*mm* | **uptime-delay** *minutes*}
5. **ccm-manager fallback-mgcp**
6. **application**
7. **global**
8. **service** {**alternate** {**default** | *service-name location* } | **default**}
9. **exit**
10. **ccm-manager switchover-to-backup**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password when prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ccm-manager redundant-host** {*ip-address* \| *DNS-name*} [*ip-address* \| *DNS-name*]<br><br>**Example:**<br>`Router(config)# ccm-manager redundant-host 10.0.0.50` | Identifies up to two backup Cisco Unified Communications Manager servers. |
| **Step 4** | **ccm-manager switchback** {**graceful** \| **immediate** \| **schedule-time** *hh*:*mm* \| **uptime-delay** *minutes*}<br><br>**Example:**<br>`Router(config)# ccm-manager switchback immediate` | Configures switchback mode for returning control to the primary Cisco Unified Communications Manager.<br>• Default is **graceful**. |
| **Step 5** | **ccm-manager fallback-mgcp**<br><br>**Example:**<br>`Router(config)# ccm-manager fallback-mgcp` | Enables the MGCP fallback feature. |
| **Step 6** | **application**<br><br>**Example:**<br>`Router(config)# application` | Enters application configuration mode. |
| **Step 7** | **global**<br><br>**Example:**<br>`Router(config-app)# global` | Enters application configuration global mode. |
| **Step 8** | **service** {**alternate** {**default** \| *service-name location* } \| **default**}<br><br>**Example:**<br>`Router(config-app-global)# service alternate default` | Loads and configures a specific, standalone application that takes over if the MGCP application is not available.<br>• If the **alternate** keyword is entered, the *service-name* and *location* arguments identify an alternate service and its location to take over if the MGCP application is not available. The **default** keyword after **alternate** specifies that the default service on the dial peer is used if the MGCP application fails.<br>• The **service default** command specifies a default service to use when no service is configured via the dial-peer. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **exit**<br><br>**Example:**<br>`Router(config-app-global)# exit` | Exits application configuration global mode and returns to privileged EXEC mode. |
| **Step 10** | **ccm-manager switchover-to-backup**<br><br>**Example:**<br>`Router# ccm-manager switchover-to-backup` | Manually redirects the MGCP gateway to the backup Cisco Unified Communications Manager server. The switchover to the backup Cisco Unified Communications Manager server occurs immediately.<br><br>**Note** This command does not switch the gateway to the backup Cisco Unified Communications Manager server if you have set the **ccm-manager switchback** command to **immediate** and the primary Cisco Unified Communications Manager server is still running. |

# Verifying Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback

Use the **show** commands described in this section to verify the Cisco Unified Communications Manager switchover and MGCP gateway fallback configuration.

## SUMMARY STEPS

1. **show running-config**
2. **show ccm-manager**
3. **show ccm-manager fallback-mgcp**

## DETAILED STEPS

### Step 1 show running-config

Use the **show running-config** command to verify configuration of the Cisco Unified Communications Manager failover options, for example:

```
Router# show running-config
...
ccm-manager switchback immediate
ccm-manager fallback-mgcp
ccm-manager redundant-host 10.0.0.50
ccm-manager mgcp
.
.
.
call application alternate DEFAULT
!
```

### Step 2 show ccm-manager

Use the **show ccm-manager** command to verify the Cisco Unified Communications Manager failover options.

The following example shows one Cisco Unified Communications Manager backup server is configured. Switchback mode is set for immediate return to the primary Cisco Unified Communications Manager server as soon as the server is available.

```
Router# show ccm-manager

MGCP Domain Name: router.cisco.com
Total number of host: 2
Priority        Status         Host
================================================
Primary         Registered     10.0.0.201
First backup    Backup polling 10.0.0.50
Second backup   Undefined

Current active Communications Manager: 10.0.0.201
Current backup Communications Manager: 10.0.0.50
Redundant link port:         2428
Failover Interval:           30 seconds
Keepalive Interval:          15 seconds
Last keepalive sent:         00:20:18 (elapsed time: 00:00:06)
Last MGCP traffic time:      00:20:18 (elapsed time: 00:00:06)
Last switchover time:        None
Switchback mode:             Immediate
```

**Step 3** **show ccm-manager fallback-mgcp**

Use the **show ccm-manager fallback-mgcp** command to verify whether MGCP fallback is enabled and whether it is active or not (on or off), for example:

```
Router# show ccm-manager fallback-mgcp

Current active Communications Manager:    10.00.71.29
MGCP Fallback mode:            Enabled/OFF
Last MGCP Fallback start time: 00:00:00
Last MGCP Fallback end time:   00:00:00
```

**Note** For a description of the fields displayed in these output examples, see descriptions of the individual commands in the *Cisco IOS Voice Command Reference*.

# Configuring POTS Dial Peers on MGCP Gateways

Perform this task to enable the POTS dial peers on your MGCP gateway to communicate with Cisco Unified Communications Manager.

When you have finished this procedure, the voice gateway is ready to communicate with Cisco Unified Communications Manager. It periodically sends out messages attempting to establish a connection. When the Cisco Unified Communications Manager configuration is complete, the connection should automatically establish itself. You should not have to make any further changes on the MGCP gateway.

## Restrictions for POTS Dial Peers on MGCP Gateways

- All dial-plan configuration elements are controlled by Cisco Unified Communications Manager and should not be configured on the MGCP gateway for MGCP-managed endpoints (that is, any endpoint with an **application mgcpapp** command in its associated dial peer).

- Do not use the **destination-pattern** or **session target** dial-peer configuration commands or the **connection** voice-port configuration command on the MGCP gateway, unless you are configuring MGCP gateway fallback. To configure MGCP gateway fallback, you must configure the H.323 dial peers with the **destination-pattern** and **session target** dial-peer configuration commands.
- Do not use the **application mgcpapp** command in dial peers that support PRI backhaul or BRI backhaul.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **pots**
4. **service mgcpapp**
5. **direct-inward-dial**
6. **port** *port/slot/DS1 port number***:***group*
7. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password when prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **dial-peer voice** *tag* **pots**<br><br>**Example:**<br>`Router(config)# dial-peer voice 101 pots` | Designates the specified dial peer as a POTS device and enters dial-peer configuration mode. |
| **Step 4** | **service mgcpapp**<br><br>**Example:**<br>`Router(config-dial-peer)# service mgcpapp` | Enables MGCP on the dial peer.<br>**Note** Do not use this command in dial peers that support PRI backhaul or BRI backhaul. |
| **Step 5** | **direct-inward-dial**<br><br>**Example:**<br>`Router(config-dial-peer)# direct-inward-dial` | (Optional) Enables the direct inward dialing (DID) call treatment for an incoming called number.<br>• Required for T1 PRI dial peers. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **port** *port*/*slot*/*DS1 port number*:*group*<br><br>**Example:**<br>`Router(config-dial-peer)# port 1/0/1:23` | Binds the MGCP application to the specified voice port.<br>• The *slot*, *port*, *DS1 port number*, and *group* arguments identify the specific port identification. |
| **Step 7** | **exit**<br><br>**Example:**<br>`Router(config-dial-peer)# exit` | Exits dial-peer configuration mode and returns to global configuration mode. |

# Verifying Dial Peer Configuration for MGCP Gateways

Use the **show** commands described in this section to verify the dial-peer configuration for MGCP gateways.

## SUMMARY STEPS

1. **show running-config**
2. **show dial-peer voice** *tag*

## DETAILED STEPS

**Step 1** **show running-config**

Use the **show running-config** command to verify the dial peer configuration.

The following example shows a configuration on MGCP voice gateways for T1 CAS with e&m-fgb emulation.

```
ccm-manager switchback immediate
ccm-manager fallback-mgcp
ccm-manager mgcp
!
controller T1 1/0:1
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-24 type e&m-fgb
!
voice-port 1/0:1:1
!
dial-peer voice 1 pots
 service mgcpapp
 destination-pattern 91.........
 port 1/0:1:1
```

The following example shows a configuration on MGCP gateways for VoIP calls, when the fallback feature is used.

```
dial-peer voice 555 voip
 application mgcpapp
 destination pattern 555...
 incoming-called-number 444...
 session-target ipv4:172.20.21.8
 codec g711ulaw
```

**Note** When you configure MGCP gateway fallback support, the POTS dial peer must include the **service mgcpapp** command and must specify the voice port. For the default session application to take over during fallback, you must also configure a destination pattern.

**Step 2** **show dial-peer voice**

Use the **show dial-peer voice** command to verify the configuration of the POTS dial peer, for example:

```
Router# show dial-peer voice 1000

VoiceEncapPeer1000
information type = voice,
description = `',
tag = 1000, destination-pattern = `',
answer-address = `', preference=0,
numbering Type = `unknown'
group = 1000, Admin state is up, Operation state is down,
incoming called-number = `', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
huntstop = disabled,
in bound application associated: 'mgcpapp'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
outgoing COR list:minimum requirement
type = pots, prefix = `',
forward-digits default
session-target = `', voice-port = `',
direct-inward-dial = disabled,
digit_strip = enabled,
register E.164 number with GK = TRUE
Connect Time = 0, Charged Units = 0,
Successful Calls=0, Failed Calls=0, Incomplete Calls=0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
```

**Step 3** **show voice port**

Use the **show voice port** command to verify that the voice port is operational. The following is sample output for a T1 PRI backhaul voice port on a Cisco VGD 1T3 voice gateway:

```
Router# show voice port 4/0:1:23

ISDN 4/0:1:23 - 4/0:1:23
 Type of VoicePort is XCC
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
```

```
Echo Cancel Coverage is set to 128 ms
Echo Cancel worst case ERL is set to 6 dB
Playout-delay Mode is set to adaptive
Playout-delay Nominal is set to 60 ms
Playout-delay Maximum is set to 1000 ms
Playout-delay Minimum mode is set to default, value 40 ms
Playout-delay Fax is set to 300 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 15 s
Interdigit Time Out is set to 10 s
Call Disconnect Time Out is set to 60 s
Ringing Time Out is set to 180 s
Wait Release Time Out is set to 30 s
Spe country is not configured
Region Tone is set for US
Continuity Test Tone CO1 is set to 2010
Continuity Test Tone CO2 is set to 1780
Station name None, Station number None
Translation profile (Incoming):
Translation profile (Outgoing):


DS0 channel specific status info:
                                          IN      OUT
PORT            CH  SIG-TYPE    OPER STATUS    STATUS    TIP     RING
=============== == ============ ==== ======    ======    ===     ====
4/0:1:23         01  xcc-voice   up   none      none
4/0:1:23         02  xcc-voice   up   none      none
```

**Note** For a description of the fields displayed in this output, see the information for the individual commands in the *Cisco IOS Voice Command Reference*.

# Configuring Single-Point Configuration for MGCP Gateways

When you configure MGCP gateways to support Cisco Unified Communications Manager, you can use a centralized TFTP boot directory on a host device in your network to automatically download most of the configuration in the XML files. Each MGCP gateway in your VoIP network has an associated gateway-specific configuration that is stored in the centralized TFTP boot directory. A tailored XML file can be created and downloaded from the TFTP server to your designated MGCP gateway. The Cisco Unified Communications Manager server can be configured concurrently as a TFTP server.

When you make changes to the configuration in the database, a message is sent by Cisco Unified Communications Manager to the affected MGCP gateway, instructing the gateway devices to download the new XML configuration file. Each device has an XML parser that interprets the XML file according to its device-specific requirements. Cisco MGCP gateways, for example, translate the content of the XML file into specific Cisco IOS commands for local execution.

When an MGCP gateway is first started up, it is preconfigured with the following information or it obtains the information through Dynamic Host Configuration Protocol (DHCP):

- A unique device identifier, which can be either of the following:
  - Specific device name on the Cisco MGCP gateway
  - MAC address of the device for gateways that are not using Cisco IOS software

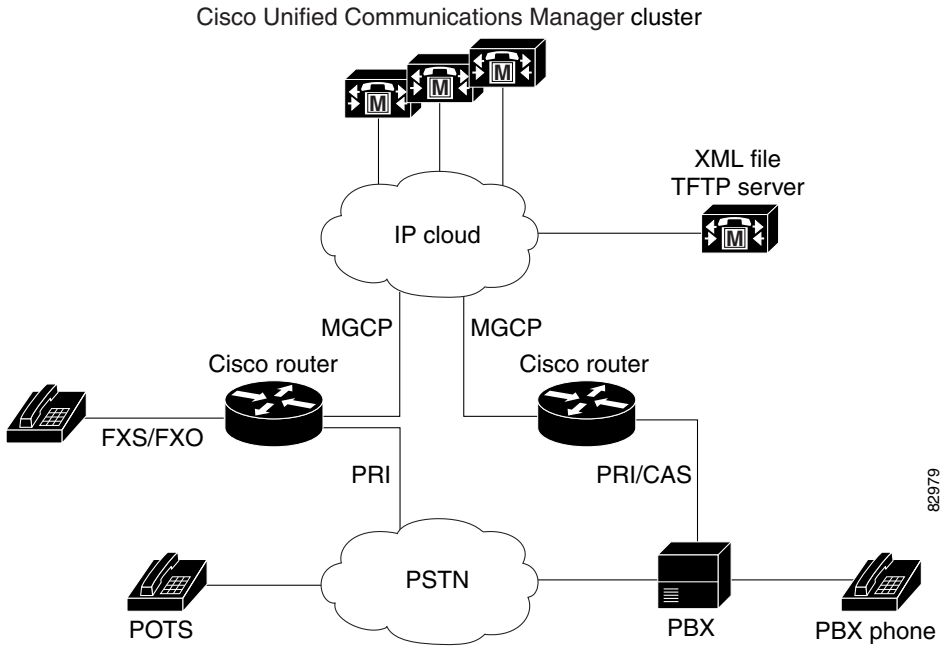
- IP address of the TFTP server in the network and routing information required for access
- Sufficient information for configuration of an IP interface on the device

With this configuration information available at startup, the MGCP gateway downloads the XML file from the TFTP server. The gateway parses the XML file, converts the information to appropriate Cisco IOS configuration commands, and configures itself to run in the VoIP network. Finally, the gateway registers itself with Cisco Unified Communications Manager using an RSIP message. At that point, the MGCP gateway is ready for service in the network.

After a successful configuration download, the MGCP gateway saves the running configuration to nonvolatile random-access memory (NVRAM), which updates the startup configuration. Any manually-added configuration parameters are also saved to NVRAM if they were not previously saved. Manually-added configuration parameters are updates to the configuration that were made using the command-line interface (CLI). Manual configuration updates are separate from the automatic configuration updates made during the configuration download process.

In the event of a configuration failure, the MGCP gateway attempts to restore its current configuration by copying the startup configuration from NVRAM into the running configuration. Because this overwrites the running configuration, any manually added configuration parameters could be lost if they were not saved to NVRAM before running the automatic configuration-download process.

***Figure 3 Single-Point Configuration for Cisco MGCP Gateways***




## Prerequisites for Single-Point Configuration for MGCP Gateways

- MGCP should be configured in your VoIP network through the Cisco Communications Manager web-based graphical user interface (GUI).
- The IP hostname should match the gateway name that is specified in the Cisco Unified Communications Manager configuration.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ccm-manager config server** {*ip-address* | *name*}
4. **ccm-manager config**
5. **exit**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password when prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ccm-manager config server** {*ip-address* \| *name*}<br><br>**Example:**<br>`Router(config)# ccm-manager config server 10.10.1.10` | Specifies the TFTP server by IP address or logical name. |
| **Step 4** | **ccm-manager config**<br><br>**Example:**<br>`Router(config)# ccm-manager config` | Enables the gateway to be configured by a centralized XML file and triggers the gateway to download a new configuration. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router(config)# exit` | Exits global configuration mode. |

# Verifying Single-Point Configuration for MGCP Gateways

Use the **show** commands described in this section to verify the single-point configuration for MGCP gateways.

### SUMMARY STEPS

1. **show running-config**
2. **show ccm-manager config-download**

### DETAILED STEPS

**Step 1** **show running-config**

Use the **show running-config** command to verify the single-point download configuration, for example:

```
Router# show running-config
.
.
.
ccm-manager switchback immediate
ccm-manager fallback-mgcp
ccm-manager redundant-host 10.10.10.1
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.1.10.10
ccm-manager config
!
```

**Step 2** **show ccm-manager config-download**

Use the **show ccm-manager config-download** command to verify the download status. The output indicates that four downloads were successful.

```
Router# show ccm-manager config-download

Configuration Auto-download Information
=======================================
Current version-id: {1645327B-F59A-4417-8E01-7312C61216AE}
Last config-downloaded:00:00:49
Current state: Waiting for commands
Configuration Download statistics:
        Download Attempted             : 4
          Download Successful          : 4
          Download Failed              : 0
        Configuration Attempted        : 1
          Configuration Successful     : 1
          Configuration Failed(Parsing): 0
          Configuration Failed(config) : 0
Last config download command: New Registration
```

**Note** For a description of the fields displayed in this output, see the individual commands in the *Cisco IOS Voice Command Reference*.

# Configuring Multicast Music-on-Hold Support for Cisco Unified Communications Manager

This section describes how to configure your gateway to provide music to customers on hold.

## Prerequisites for Multicast Music-on-Hold (MOH)

The default router in the network for handling multicast traffic must have the following enabled:

- Multicast routing
- A multicast routing protocol, for example Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP)
- An IP routing protocol, for example Routing Information Protocol (RIP) or Open Shortest Path First (OSPF)

- Cisco Unified Communications Manager 3.1 (formerly known as Cisco CallManager 3.1) or higher

## Multicast Music-on-Hold

The Music-on-Hold (MOH) feature enables you to subscribe to a music streaming service when you are using a Cisco IOS MGCP voice gateway. Music streams from an MOH server to the voice interfaces of on-net and off-net callers that have been placed on hold. Cisco Communications Manager supports the capability to place callers on hold with music supplied from a streaming multicast MOH server. This integrated multicast capability is implemented through the H.323 signaling in Cisco Communications Manager.

By means of a preconfigured multicast address on the gateway, the gateway can "listen" for Real-Time Transport Protocol (RTP) packets that are broadcast from a default router in the network and can relay the packets to designated voice interfaces in the network. Whenever a called party places a calling party on hold, Cisco Communications Manager requests the MOH server to stream RTP packets to the "on-hold" interface through the preconfigured multicast address. In this way, RTP packets are relayed to appropriately configured voice interfaces that have been placed on hold. When you configure a multicast address on a gateway, the gateway sends an Internet Gateway Management Protocol (IGMP) "join" message to the default router, indicating to the default router that the gateway is ready to receive RTP multicast packets.

Multiple MOH servers can be present in the same network, but each server must have a different Class D IP address, and the address must be configured in Cisco Communications Manager and the MGCP voice gateways.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ccm-manager music-on-hold**
4. **ccm-manager music-on-hold bind** *interface*
5. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password when prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ccm-manager music-on-hold**<br><br>**Example:**<br>`Router(config)# ccm-manager music-on-hold` | Enables music-on-hold. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ccm-manager music-on-hold bind** *interface*<br><br>**Example:**<br>`Router(config)# ccm-manager music-on-hold bind async` | (Optional) Binds the multicast MOH feature to a designated interface. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router(config)# exit` | Exits global configuration mode. |

# Verifying Music-on-Hold

Use the **show** commands described in this section to verify music-on-hold.

## SUMMARY STEPS

1. **show running-config**
2. **show ccm-manager music-on-hold**

## DETAILED STEPS

**Step 1** **show running-config**

Use the **show running-config** command to verify the MOH configuration, for example:

```
Router# show running-config
.
.
.
ccm-manager redundant-host 10.0.0.21
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.0.0.21
ccm-manager config
!
```

**Step 2** **show ccm-manager music-on-hold**

Use the **show ccm-manager music-on-hold** command to display information about the currently active MOH sessions, for example:

```
Router# show ccm-manager music-on-hold

Multicast       RTP      Packets       Call                Incoming
Address         Port     In/Out        ID       Protocol   Interface

10.10.20.22     16256    3000/3000     1        IGMP       fe0/0
```

**Note** For a description of the fields displayed in this output, see the individual commands in the *Cisco IOS Voice Command Reference*.

# Configuring MGCP PRI Backhaul and T1 CAS Support for Cisco Unified Communications Manager

This section describes the procedures for enabling MGCP PRI backhaul support on the Cisco VGD 1T3 voice gateway.

## Prerequisites

The following prerequisites must be met to configure MGCP PRI backhaul support:

- Cisco IOS Release 12.4(20)YA.
- QSIG signaling is required to support supplementary services over the T1 time-division multiplexing (TDM) trunks that support the PRI backhaul mechanism.

## Restrictions

The following restrictions apply to configuration of MGCP PRI backhaul support:

- Integrated access, in which the channels on a T1 or E1 interface are divided between a group used for voice and another group used for WAN access, is not supported when voice is controlled by Cisco Unified Communications Manager through MGCP.
- T1 and E1 protocols, such as QSIG, E1 R2, T1 FGD, and PRI NFAS, are not supported with MGCP only with H.323.
- E1 CAS is not supported.
- Do not add the **application mgcpapp** command to dial peers that support PRI backhaul.

## Information About MGCP PRI Backhaul and T1 CAS Support

To configure MGCP PRI backhaul, you should understand the following concepts:

- MGCP PRI Backhaul Overview, page 139
- ISDN NSF in Route Patterns, page 140

### MGCP PRI Backhaul Overview

MGCP PRI backhaul is a method for transporting complete IP telephony signaling information from an ISDN PRI interface in an MGCP gateway to Cisco Unified Communications Manager using a highly reliable TCP connection. The gateway uses a single TCP connection to backhaul all ISDN D channels to Cisco Unified Communications Manager. The “SAP/Channel ID” parameter in the header of each message identifies individual D channels. In addition to carrying the backhaul traffic, the TCP keepalive mechanism also determines MGCP voice gateway connectivity to an available call agent.

MGCP PRI backhaul terminates all ISDN PRI Layer 2 (Q.921) signaling functions on the MGCP gateway while, at the same time, packaging all the ISDN PRI Layer 3 (Q.931) signaling information into packets for transmission to Cisco Unified Communications Manager through an IP tunnel over a TCP connection. This ensures the integrity of the Q.931 signaling information that passes through the network for managing IP telephony devices. A rich set of user-side and network-side ISDN PRI calling functions is supported by MGCP PRI backhaul.

The MGCP gateway also establishes a TCP link to the backup (secondary) Cisco Unified Communications Manager server. In the event of a Cisco Unified Communications Manager switchover, the secondary Cisco Unified Communications Manager server performs the MGCP PRI backhaul functions. During the switchover, all active ISDN PRI calls are preserved, and the affected MGCP gateway is registered with the new Cisco Unified Communications Manager server through a Restart-in-Progress (RSIP) message. In this way, continued gateway operation is ensured.

T1 CAS is supported in nonbackhaul fashion. Cisco Unified Communications Manager supports the following CAS signaling types: E&M, wink-start, and E&M delay-dial. E1 CAS is not supported.

## ISDN NSF in Route Patterns

The MGCP Gateway Support for Cisco Unified Communications Manager Network Specific Facilities (NSF) feature supports the use of the ISDN NSF information element in the route pattern. This feature is compatible with Cisco Communications Manager 3.3(2) (formerly known as Cisco CallManager 3.3(2)) and later.

The route pattern design in Cisco Unified Communications Manager enables facilities or services to be invoked on a call-by-call basis. The NSF information element, which is used in ISDN PRI setup messages for outgoing calls, includes the carrier identification code (CIC) and service parameters. The NSF configuration is done in Cisco Unified Communications Manager as part of the route pattern for MGCP-controlled PRI ports. The NSF information element is inserted in the Q.931 stream so that the attached PSTN switch can interpret the information elements and select the service and route the call to a network.

With NSF configured, NSF can be used on a call-by-call basis. Without NSF configuration, you must configure associated gateways as standalone H.323 gateways for which NSF services are configured locally within the router. No configuration is required on the MGCP gateway to use the NSF feature.

Complete the following task to configure MGCP PRI backhaul on the Cisco VGD 1T3 voice gateway.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller t1** *slot/ds3 port:ds1 port*
4. **framing** {**esf** | **sf** | **crc4** | **no crc4** | **mp-crc4**} [**australia**]
5. **linecode** {**ami** | **b8zs**}
6. **isdn switch-type** {**primary-4ess** | **primary-5ess** | **primary-dms100** | **primary-ni** | **primary-net5** | **primary-ntt** | **primary-qsig** | **primary-ts014**}
7. **pri-group timeslots** *timeslot-range* **service mgcp**
8. **exit**
9. **interface serial** *slot/ds3 port*:*ds1 port*:*timeslot*
10. **isdn bind-L3 ccm-manager**
11. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password when prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **controller t1** *slot*/*ds3 port*:*ds1 port*<br><br>**Example:**<br>`Router(config)# controller t1 3/0:23` | Enters controller configuration mode and identifies the location of the T1 controller. |
| **Step 4** | **framing** {**esf** \| **sf** \| **crc4** \| **no-crc4** \| **mp-crc4**} [**australia**]<br><br>**Example:**<br>`Router(config-controller)# framing esf` | Specifies the framing type on a T1 PRI line.<br>• Default is **sf** (super frame) for T1 lines. |
| **Step 5** | **linecode** {**ami** \| **b8zs**}<br><br>**Example:**<br>`Router(config-controller)# linecode b8zs` | Specifies the line encoding method for the link.<br>• Default is **ami** (alternate mark inversion) for T1 lines. |
| **Step 6** | **isdn switch-type** {**primary-4ess** \| **primary-5ess** \| **primary-dms100** \| **primary-ni** \| **primary-net5** \| **primary-ntt** \| **primary-qsig** \| **primary-ts014**}<br><br>**Example:**<br>`Router(config-if)# isdn switch-type primary-5ess` | Specifies the ISDN switch type.<br>**Note** This command can be entered in either global configuration mode or interface configuration mode. |
| **Step 7** | **pri-group timeslots** *timeslot-range* **service mgcp**<br><br>**Example:**<br>`Router(config-controller)# pri-group timeslots 1-24 service mgcp` | Specifies MGCP as the control protocol used for backhaul.<br>**Note** The controller time slots cannot be shared between backhaul and other Layer 3 protocols. |
| **Step 8** | **exit**<br><br>**Example:**<br>`Router(config-dial-peer)# exit` | Exits controller configuration mode and returns to global configuration mode. |
| **Step 9** | **interface serial** *slot*/*ds3 port*:*ds1 port*:*timeslot*<br><br>**Example:**<br>`Router(config)# interface serial 3/0:0` | Enters serial interface configuration mode and identifies the location of the interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **isdn bind-L3 ccm-manager**<br><br>**Example:**<br>`Router(config-if)# isdn bind-L3 ccm-manager` | Enables ISDN to backhaul Q.931. |
| **Step 11** | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |

# Verifying the MGCP PRI Backhaul Configuration

## SUMMARY STEPS

To verify the MGCP PRI backhaul configuration, complete the following steps.

1. **show isdn status**
2. **show ccm-manager**
3. **show ccm-manager backhaul**

## DETAILED STEPS

**Step 1** **show isdn status**

Use the **show isdn status** command to verify connectivity.

In the following sample output, the Layer 2 protocol is Q.921, and the Layer 3 protocol is CCM-MANAGER. This output verifies that the Layer 2 and Layer 3 protocols are configured to backhaul ISDN. If you are connected to a live line, you should see Layer 1 status as active and Layer 2 as MULTIPLE_FRAME_ESTABLISHED.

```
Router# show isdn status

*00:03:34.423 UTC Sat Jan 1 2000
Global ISDN Switchtype = primary-net5
ISDN Serial1:23 interface
!
******* Network side configuration *******
!
 dsl 0, interface ISDN Switchtype = primary-net5
!
**** Master side configuration ****
!
 L2 Protocol = Q.921 L3 Protocol(s) = CCM-MANAGER
 Layer 1 Status:
 ACTIVE
 Layer 2 Status:
 TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
 Layer 3 Status:
 NLCB:callid=0x0, callref=0x0, state=31, ces=0 event=0x0
 NLCB:callid=0x0, callref=0x0, state=0, ces=1 event=0x0
 0 Active Layer 3 Call(s)
 Activated dsl 0 CCBs = 0
 Number of active calls = 0
 Number of available B-channels = 23
```

```
 Total Allocated ISDN CCBs = 0
```

**Step 2** **show ccm-manager**

Use the **show ccm-manager** command to view the registration status with Cisco Unified Communications Manager, for example:

```
Router# show ccm-manager

MGCP Domain Name: AV-2620-4
Priority        Status                      Host
============================================================
Primary         Registered                  10.16.240.124
First Backup    Backup Ready                10.16.240.128
Second Backup   None

Current active Call Manager:    10.16.240.124
Backhaul/Redundant link port:   2428
Failover Interval:              30 seconds
Keepalive Interval:             15 seconds
Last keepalive sent:            00:45:31 (elapsed time: 00:00:04)
Last MGCP traffic time:         00:45:31 (elapsed time: 00:00:04)
Last failover time:             None
Switchback mode:                Graceful
MGCP Fallback mode:             Not Selected
Last MGCP Fallback start time:  00:00:00
Last MGCP Fallback end time:    00:00:00
PRI Backhaul Link info:
  Link Protocol:       TCP
  Remote Port Number:  2428
  Remote IP Address:   10.16.240.124
  Current Link State:  OPEN
  Statistics:
     Packets recvd:    32
     Recv failures:    0
     Packets xmitted:  32
     Xmit failures:    0
  PRI Ports being backhauled:
     Slot 1, port 0

Configuration Auto-Download Information
=======================================
Current version-id: {1645327B-F59A-4417-8E01-7312C61216AE}
Last config-downloaded:00:00:49
Current state: Waiting for commands
Configuration Download statistics:
        Download Attempted             : 6
          Download Successful          : 6
          Download Failed              : 0
        Configuration Attempted        : 1
          Configuration Successful     : 1
          Configuration Failed(Parsing): 0
          Configuration Failed(config) : 0
Last config download command: New Registration
Configuration Error History:
FAX mode: cisco
```

**Step 3** **show ccm-manager backhaul**

Use the **show ccm-manager backhaul** command to verify the PRI backhaul link information, for example:

```
Router# show ccm-manager backhaul
```

```
PRI Backhaul Link info:
 Link Protocol:          TCP
 Remote Port Number:     2428
 Remote IP Address:      10.20.71.38
 Current Link State:     OPEN
 Statistics:
  Packets recvd:         0
  Recv failures:         0
  Packets xmitted:       21
  Xmit failures:         0
PRI Ports being backhauled:
 Slot 1, port 1
```

For a description of the fields displayed in these output examples, see the individual commands in the *Cisco IOS Voice Command Reference*.

# Configuration Examples for MGCP Gateway Support

This section provides the following configuration examples:


- MGCP Gateway with T1 CAS: Example, page 144
- MGCP Gateway with T1 PRI: Example, page 146
- Multicast Music-on-Hold: Example, page 148


**Note** To view relevant configuration examples, go to the Cisco Systems Technologies website at http://cisco.com/en/US/tech/index.html. From the website, choose **Voice > IP Telephony/VoIP**, then click **Technical Documentation > Configuration Examples**.

## MGCP Gateway with T1 CAS: Example

The following example shows MGCP fallback configured on a voice gateway with T1 CAS.

```
Current configuration : 2181 bytes
!
version 12.4
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Test-vgd1t3
!
logging rate-limit console 10 except errors
!
memory-size iomem 25
voice-card 3
!
ip subnet-zero
!
no ip domain-lookup
ip domain-name example.com
!
no ip dhcp-client network-discovery
```

```
frame-relay switching
mgcp
mgcp call-agent 10.0.0.21 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000
mgcp package-capability rtp-package
no mgcp timer receive-rtcp
call rsvp-sync
!
ccm-manager switchback immediate
ccm-manager fallback-mgcp
ccm-manager redundant-host 10.0.0.21
ccm-manager mgcp
!
controller T1 3/0:1
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1 type e&m-fgb
!
controller T1 4/0:1
 framing sf
 linecode ami
!
interface FastEthernet0/0:1:23
 ip address 10.0.0.21 255.255.255.224
 duplex auto
 speed auto
!
interface Serial0/0:1:23
 ip address 10.0.0.21 255.255.255.224
 encapsulation frame-relay
 no keepalive
 frame-relay interface-dlci 300
!
interface Serial1/0:1:23
 no ip address
 shutdown
 clockrate 2000000
!
interface Ethernet2/0:1:23
 ip address 10.0.0.21 255.255.255.224
 half-duplex
!
interface TokenRing2/0
 no ip address
 shutdown
 ring-speed 16
!
ip classless
ip route 10.0.0.21 255.255.255.0 14.0.0.1
ip route 10.0.0.21 255.255.255.0 14.0.0.1
ip route 10.0.0.21 255.255.255.0 14.0.0.1
ip route 10.0.0.21 255.255.255.0 14.0.0.1
ip route 10.0.0.21 255.255.255.255 Ethernet2/0
ip route 10.0.0.21 255.255.255.255 Ethernet2/0
no ip http server
!
snmp-server manager
!
voice-port 1/0:1
!
voice-port 1/0:2
!
voice-port 1/1:1
```

```
!
voice-port 1/1:2
!
voice-port 3/0:1
!
dial-peer cor custom
!
dial-peer voice 44 pots
 application mgcpapp
 destination-pattern 4301
 port 1/1:0
!
dial-peer voice 55 pots
 application mgcpapp
 destination-pattern 4302
 port 1/1:1
!
dial-peer voice 85 voip
 destination-pattern 805....
 session target ipv4:10.0.0.21
 codec g711ulaw
!
dial-peer voice 33 pots
 service mgcpapp
 destination-pattern 807....
 port 3/0:1
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
end
```

**Note** If the **ccm-manager config** command is enabled and you separate the MGCP and H.323 dial peers under different tags, make sure that the MGCP dial peers are configured before the H.323 dial peers.

# MGCP Gateway with T1 PRI: Example

The following example shows MGCP fallback configured on a voice gateway with T1 PRI ports.

```
version 12.4
no parser cache
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname vgd1t3
!
logging rate-limit console 10 except errors
!
voice-card 1
!
ip subnet-zero
!
no ip domain-lookup
!
no ip dhcp-client network-discovery
mgcp
```

```
mgcp call-agent 172.16.240.124 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp modem passthrough voip mode cisco
mgcp package-capability rtp-package
mgcp package-capability sst-package
no mgcp timer receive-rtcp
!
ccm-manager fallback-mgcp
ccm-manager redundant-host CM-B
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server cm-a
ccm-manager config
!
controller T1 1/0:1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 1/0:2
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
interface Serial1/0:23
 no ip address
 no logging event link-status
 isdn switch-type primary-ni
 isdn incoming-voice voice
 isdn T306 30000
 isdn bind-l3 ccm-manager
 no cdp enable
!
voice-port 1/0:23
!
dial-peer voice 9991023 pots
 application mgcpapp
 direct-inward-dial
 port 1/0:23
!
dial-peer voice 9991123 pots
 application mgcpapp
 direct-inward-dial
 port 1/1:23
!
dial-peer voice 1640001 pots
 destination-pattern 16.....
 direct-inward-dial
 port 1/0:23
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

**Note** DID is required for T1 PRI dial peers.

# Multicast Music-on-Hold: Example

The following example shows multicast MOH configured for an MGCP voice gateway:

```
version 12.4
no parser cache
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname voice-3640
!
logging rate-limit console 10 except errors
!
memory-size iomem 10
voice-card 1
!
ip subnet-zero
!
ip domain-name example.com
!
no ip dhcp-client network-discovery
mgcp
mgcp call-agent 10.0.0.21 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000
mgcp modem passthrough voip mode cisco
mgcp package-capability rtp-package
mgcp package-capability sst-package
no mgcp timer receive-rtcp
call rsvp-sync
!
ccm-manager redundant-host 10.0.0.21
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.0.0.21
ccm-manager config
!
controller T1 2/0:1
 framing sf
 linecode ami
 ds0-group 0 timeslots 1 type e&m-fgb
!
controller T1 2/0:2
 framing sf
 linecode ami
!
interface FastEthernet0/0:1
 ip address 10.0.0.21 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 no cdp enable
!
voice-port 1/0:0
!
voice-port 1/0:1
!
voice-port 2/0:0
!
dial-peer cor custom
!
```

```
dial-peer voice 125 pots
 application mgcpapp
 port 1/0:0
!
dial-peer voice 150 pots
 service mgcpapp
 port 2/0:0
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
no scheduler max-task-time
scheduler allocate 4000 4000
!
end
```

# Additional References

- *Configuring Media Gateway Control Protocol and Related Protocols*—Describes MGCP concepts and configuration procedures.
- *Configuring the Cisco IOS MGCP Gateway*—Describes the basics of configuring an MGCP gateway to support Cisco Unified Communications Manager.
- *Cisco Unified Communications Manager Administration Guide*—Describes how to configure and register Cisco VGD 1T3 Voice Gateways on Cisco Unified Communications Manager.
- *How to Configure MGCP with Digital PRI and Cisco Unified Communications Manager*—Describes how to configure MGCP with PRI.
- *MGCP Gateway Fallback Transition to Default H.323 Session Application*—Describes how to enable an MGCP gateway to fallback to an H323 session application when the WAN connection to the primary Cisco Communications Manager server is lost, and no backup Cisco Unified Communications Manager server is available.
- *MGCP with Digital CAS and Cisco Unified Communications Manager Configuration Example*—Describes how to use MGCP between a Cisco IOS gateway and a Cisco Unified Communications Manager Media Convergence Server (MCS).

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.