



Diagnosing Cisco CallManager Problems

This chapter addresses some common problems that you may experience with Cisco CallManager and related devices. Each problem category provides suggestions for the troubleshooting tools you should use to help isolate the problem. This chapter provides general categories of potential problems and suggestions about how to troubleshoot those problems. It does not provide an exhaustive list of problems and resolutions.

If you encounter a problem that cannot be resolved using the tools and utilities described in this document, consult your Cisco Technical Assistance Center (TAC) for assistance. Be sure to have available the Cisco CallManager Administration Details, plus any diagnostic information (for example, traces) you have gathered before calling the TAC.

This chapter contains the following topics:

- [Voice Quality, page 3-2](#)
- [Diagnosing Phone Resets, page 3-9](#)
- [Diagnosing Dropped Calls, page 3-10](#)
- [Diagnosing Cisco CallManager Feature Issues, page 3-11](#)
- [Diagnosing Slow Server Response, page 3-23](#)
- [Determining Gateway Reorder Tone Problems, page 3-23](#)
- [Diagnosing Gateway Registration Problems, page 3-24](#)
- [Diagnosing Gatekeeper Problems, page 3-31](#)

Voice Quality

You may experience voice quality issues including lost or distorted audio signal during phone calls. Common problems include audio breaks (like broken words), or the presence of odd noises and audio distortion, such as echo, watery or robotic voice quality. One-way audio, that is, a conversation between two people where only one person can hear anything, is not actually a voice quality issue, but will be discussed later in this section.

You may experience audio problems with one or more of the following:

- Gateways
- Phones
- Networks

Diagnosing Lost or Distorted Audio Problems

One of the most common problems you may encounter is broken audio signal (often described as garbled speech, or lost syllables within a word or sentence). There are two common causes for this: packet loss and/or jitter. Packet loss means that audio packets do not arrive at their destination because they were dropped or arrived too late to be useful. Jitter is the variation in the arrival times of packets. In the ideal situation, all Voice over IP (VoIP) packets would arrive exactly at a rate of 1 every 20 microseconds (ms). Notice that this is not the length of time it takes for a packet to get from point A to point B, but is simply the variation in packet arrival times.

There are many sources of variable delay in a network. Some of these cannot be controlled, and some can. Variable delay cannot be eliminated entirely in a packetized voice network. Digital Signal Processors (DSP) on phones and other voice-capable devices are designed to buffer some of the audio, in anticipation of variable delay. This dejittering is done only when the audio packet has reached its destination and is now ready to be put into a conventional audio stream.

The Cisco IP Phone 7960 can buffer as much as one second of voice samples. The jitter buffer is adaptive, meaning if a burst of packets is received, the Cisco IP Phone 7960 can play them out in an attempt to control the jitter. The network administrator needs to minimize the variation between packet arrival times by applying Quality-of-Service (QoS) and other measures in advance (especially if calls cross a wide-area network).

When faced with a lost or distorted audio problem, the first thing to do is to try to isolate the path of the audio. Try to identify each network device (switches and routers) in the path of the call's audio stream. Keep in mind that the audio may be between two phones, or between a phone and a gateway, or it could have multiple legs (from a phone to a transcoding device and from there to another phone). Try to identify if the problem occurs only between two sites, only through a certain gateway, on a certain subnet, and so on. This will help narrow down which devices you need to look at more carefully.

Next, it is often best to disable silence suppression (also known as Voice Activation Detection or VAD) if this has not been done already. This mechanism does save bandwidth by not transmitting any audio when there is silence, but may cause noticeable or unacceptable clipping at the beginning of words.

You can disable this in Cisco CallManager Administration, under **Service > Service Parameters**. From there, select the server and the Cisco CallManager service. Then set `SilenceSuppressionSystemWide` to F (alternatively you can set `SilenceSuppressionWithGateways` to F, but this does not apply to H.323 gateways or MGCP gateways). When in doubt, turn both off by selecting the Value F for each.

Using a network analyzer, if a network analyzer is available, then a monitored call between two phones should have 50 packets per second (or 1 packet every 20 ms) when silence suppression is disabled. With proper filtering, it should be possible to identify if packets are being lost or delayed excessively.

Remember that delay by itself will not cause clipping, only variable delay will. Notice in the table below, which represents a perfect trace, the arrival times between the audio packets (which will have an RTP header), will be 20 ms. In a poor quality call (such as a call with a lot of jitter), the arrival times would vary greatly.

The following table illustrates a perfect trace.

Packet Number	Time - absolute (ms)	Time - delta (ms)
1	0	
2	0.02	20
3	0.04	20
4	0.06	20
5	0.08	20

Placing the packet analyzer into various points in the network will help narrow down where the delay is coming from. If no analyzer is available, other methods will be required. It is important to examine interface statistics of each device in the path of the audio. Another tool for tracking calls with poor voice quality is the Diagnostic Call Detail Records (CDR). See [Appendix D, “Call Detail and Call Management Records”](#) for more information about CDRs.

Diagnosing Audio Problems from the Cisco IP Phone

The Cisco IP Phone 7960 provides another tool for diagnosing possible audio problems. On an active call, you can press the “i” button twice rapidly and the phone will display an information screen that contains packet receive and transmit statistics, as well as average and maximum jitter counters.



Note

On this screen, jitter is the average of the last 5 packets that arrived; the maximum jitter is the high-water mark for the average jitter.

The most common sources for delay and packet loss are devices where a higher speed interface feeds into a lower speed interface. For example, a router may have a 100 Megabyte (MB) fast Ethernet interface connected to the LAN and a slow frame-relay interface, connected to the WAN. If the poor audio quality occurs only when communicating to the remote site, then the most likely causes of the problem include:

- The router has not been properly configured to give voice traffic priority over data traffic
- There are too many active calls for the WAN to support (that is, there is no call admission control to restrict the number of calls that can be placed)
- There are physical port errors
- There is congestion in the WAN itself

On the LAN, the most common problems are physical-level errors (such as CRC errors) caused by faulty cables, interfaces, or by incorrectly configured devices (such as a port speed or duplex mismatch). Make sure that the traffic is not crossing any shared-media device, such as a hub.

There could also be situations where the traffic is taking a slower path through the network than expected. If QoS has been configured correctly, then the possibility exists that there is no call admission control. Depending on your topology, this can be accomplished through the use of Locations in Cisco CallManager Administration configuration, or by using a Cisco IOS router as a gatekeeper. In any case, you should always know how many calls could be supported across your WAN.

If possible, test this by disabling silence suppression as described in the preceding sections, then place calls between the two sites. Do not place the calls on hold or on mute, because this will stop packets from being transmitted. With the maximum number of calls across the WAN, the calls should all have acceptable quality. Test to make sure that a fast busy is returned when trying to make one more call.

Diagnosing Crackling Sounds

Another poor quality symptom may be a crackling, which is sometimes caused by a defective power supply or some kind of strong electrical interference close to the phone. Try swapping the power supply and moving the phone.

Checking Your Loads

Gateway and phone loads should be verified. Check Cisco Connection Online (CCO) at www.cisco.com for the latest software loads, new patches, or release notes relating to the problem.

Echo

Echo occurs when the speech energy being generated and transmitted down the primary signal path is coupled into the receive path from the far end. The speaker then hears his or her own voice, delayed by the total echo path delay time.

Voice can reflect back. This can happen but go unnoticed in a traditional voice network because the delay is so low. To the user, it sounds more like a side-tone than an echo. In a VoIP network, it will always be noticeable, since packetization and compression contributes to the delay.

The important thing to remember is that the cause of the echo is always with analog components and wiring. For instance, IP packets cannot simply turn around and go back to the source at a lower audio level or on digital T1/E1 circuits. So, on a call from one Cisco IP Phone to another, there should never be any problem. The only exception may be if one party is using a speakerphone that has the volume set too high or some other situation where an audio loop is created.

Testing Speakerphone and Volume Levels

Make sure that the problem phones are not using the speakerphone, and that they have the headset volume set to reasonable levels (start with 50% of the maximum audio level). Most of the time, the problems will occur when attaching to the PSTN by way of a digital or analog gateway.

Testing the Gateway

Determine which gateway is being used. If a digital gateway is in use, then it may be possible to add additional padding in the transmit direction (towards the PSTN). Since lower signal strength will yield less reflected energy, this should clear up the problem.

Additionally, you can adjust the receive level so that any reflected audio is reduced even further. It is very important to remember to make small adjustments at a time. Too much attenuation of the signal will make the audio impossible to hear on both sides. Alternatively, you can contact the carrier and request to have the lines checked. On a typical T1/PRI circuit in North America, the input signal should be -15 dB. If the signal level is much higher (-5 dB, for example), then echo will be the likely result.

Keeping an Echo Log

You should keep a log of all calls that experience echo. Record the time of the problem, the source phone number, and the number called. Gateways have a fixed time of 16 ms of echo cancellation. If the delay in the reflected audio is longer than this, the echo cancellor will be unable to work properly. This should not be an issue for local calls, and long distance calls should have external echo cancellers built into the network at the Central Office. This is one of the reasons why it is important to note the external phone number of a call that experiences echo.

Checking Your Loads

Verify your gateway and phone loads. Check Cisco Connection Online at www.cisco.com for the latest software loads, new patches, or release notes that may relate to the problem.

Diagnosing One-Way Audio or No Audio

When one person cannot hear another person during a call, there is one-way audio. This can be caused by an improperly configured Cisco IOS Gateway, a firewall, or a routing or default gateway problem, among other things.

Diagnostic Call Detail Records (CDR) are useful for determining if a call is experiencing one-way audio because they log transmitted and received packets (see [Diagnosing Lost or Distorted Audio Problems, page 3-2](#)). You can also press the *i* button twice quickly on a Cisco IP Phone 7960 during an active call to view details about transmitted and received packets.

Checking MTP

If you are using Media Termination Point (MTP) in a call (to support supplementary services such as hold and transfer with H.323 devices that do not support H.323 version 2), check to see if the MTP allocated is working correctly. Cisco IOS routers support H.323 version 2 beginning in Cisco IOS releases 11.3(9)NA and 12.0(3)T. Starting with Cisco IOS release 12.0(7)T, the optional H.323 Open/Close LogicalChannel is supported, so that software-based MTP is no longer required for supplementary services.

You can use the MTP device, as well as Conference Bridge and Transcoder features to bridge two or more audio streams. If the MTP, Conference Bridge, or Transcoder is not working properly, one-way audio or audio loss might be experienced. Shut down MTP to find out if MTP is causing the problem.

Testing Cisco CallManager Configuration

There are a number of causes for one-way audio or loss of audio during a call. The most common cause is an improperly configured device. For instance, Cisco CallManager handles the call setup for a Cisco IP Phone. The actual audio stream occurs between the two Cisco IP Phones (or between the Cisco IP Phone

and a gateway). It is entirely possible that the Cisco CallManager is able to signal to a destination phone (making it ring) when the phone originating the call does not have an IP route to the destination phone. A common cause for this is when the default gateway in the phone is improperly configured either manually or on the DHCP server.

If a call consistently has one-way audio, use a PC that is configured on the same subnet as the phone and has the same default gateway and try to ping the destination Cisco IP Phone. Then using a PC that is configured on the same subnet as the destination phone (with the same default gateway as the destination phone) ping the source phone. Both of those tests should work. Other things that can affect the audio traffic include a firewall or a packet filter (such as access lists on a router) that may be blocking the audio in one or both directions. If the one-way audio occurs only through a voice-enabled Cisco IOS Gateway, then check the configuration carefully. IP routing must be enabled (look at the configuration to make sure that no ip routing is not found near the beginning of the configuration).

Checking RTP Header Compression

Make sure that if you are using RTP header compression to save bandwidth across the WAN, that it is enabled on each router carrying voice traffic that attaches to the WAN circuit. There should not be a situation where the RTP header is compressed on one end but cannot be decompressed on the other side of the WAN. A Sniffer is a very useful tool when troubleshooting one-way audio problems, because you can verify whether the phone or gateway is actually sending or receiving packets.



Note

When a call is muted, no packets will be transmitted from the phone that has pressed the mute button. The Hold button stops the audio stream, so no packets are sent in either direction. When the Hold button is released, all the packet counters are reset. Remember that Silence Suppression must be disabled on both devices for the TX and RX counters to stay equal. Disabling Silence Suppression system-wide will not affect Cisco IOS Gateways.

Diagnosing Phone Resets

Phones will power cycle or reset for two reasons: 1) TCP failure connecting to Cisco CallManager, or 2) failure to receive an acknowledgement to the phone's KeepAlive messages.

The following procedure shows the steps for troubleshooting phone resets.

Procedure

- Step 1** Check the phones and gateways to ensure that you are using the latest software loads.
 - Step 2** Check Cisco Connection Online at www.cisco.com for the latest software loads, new patches, or release notes that may relate to the problem.
 - Step 3** Check the Event Viewer for instances of phone(s) resetting. Phone resets are considered Information events.
 - Step 4** Look for these and any errors that may have occurred around the time that the phone(s) reset.
 - Step 5** Start an SDI trace and try to isolate the problem by identifying any common characteristics in the phones that are resetting. For example, check whether they are all located on the same subnet, same VLAN, and so on. Look at the trace and determine:
 - If the resets occur during a call or happen intermittently
 - If there any similarities of phone model (such as Cisco IP Phone 7960 or Cisco IP Phone 30VIP)
 - Step 6** Start a Sniffer trace on a phone that frequently resets. After it has reset, look at the trace to determine if there are any TCP retries occurring. If so, this indicates a network problem. The trace may show some consistencies in the resets, such as the phone resetting every seven days. This might indicate DHCP lease expiration every seven days (this value is user-configurable; for example, it could be every two minutes).
-

Diagnosing Dropped Calls

Premature termination of dropped calls can be the result of a phone or gateway resetting (see [Diagnosing Phone Resets, page 3-9](#)) or a circuit problem, such as incorrect PRI configuration.

The first step is to determine whether this problem is isolated to one phone or to a group of phones. Perhaps the affected phones are all on a particular subnet or location. The next step is to check the Event Viewer for phone or gateway resets.

You will see one Warning and one Error message for each phone that resets. This indicates that the phone cannot keep its TCP connection to the Cisco CallManager alive, so the Cisco CallManager resets the connection. This may be because a phone was turned off or there may be a problem in the network. If this is an intermittent problem, it may be useful to use Microsoft Performance to record phone registrations.

If the problem seems to be occurring only through a certain gateway, such as a Cisco Access DT-24+, then the best course of action is to enable tracing and/or view the Call Detail Records (CDR). The CDR files will give a Cause Of Termination (CoT) that may help determine the cause of the problem. See [Appendix D, “Call Detail and Call Management Records”](#) for more information about CDRs.

The disconnect cause values (origCause_value and destCause_value— depending on which side hung up the call), map to Q.931 disconnect cause codes (in decimal) and can be found at the following location:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/dbook/disdn.htm>.

If the call is going out of a gateway to the PSTN, then the CDR can be used to determine which side is hanging up the call. Much of the same information can be obtained by enabling tracing on the Cisco CallManager. Because the trace tool can affect Cisco CallManager performance, you will want to use this option only as a last resort or if your network is not yet in production.

Diagnosing Cisco CallManager Feature Issues

Problems may occur with features that are used in conjunction with Cisco CallManager, such as Conference Bridge or Media Termination Point. Some feature problems can be caused by configuration errors or lack of server resources.

Diagnosing Codec and Region Mismatches

If a user gets a reorder tone (busy signal) when going off-hook, it could be the result of codec disagreement between regions. Verify that both call ends support at least one common codec (for example, G.711). If they do not, you will need to use transcoders.

A region specifies the range of supported codecs that can be used with each of the other regions. Every device belongs to a region.



Note

Codec negotiation with a Cisco IOS router is not supported.

For example, Region1<->Region2 = G.711, means that a call between a device in Region1 and a device in Region2 can use G.711 or any other supported codec that requires the same or less bandwidth as G.711 (any supported codecs within G.711, G.729, G.723, and so on).



Note

The following codecs are supported for each device:
Cisco IP Phone 7960—G.711A-law/ μ -law, G.729AnnexB
Cisco IP Phone SP12 series and VIP 30—G.711A-law/ μ -law, G.723.1
Cisco Access Gateway DE30 and DT-24+—G.711A-law/ μ -law, G.723.1

Diagnosing Location and Bandwidth Problems

If a user gets a reorder tone after dialing a number, it could be because the Cisco CallManager bandwidth allocation for the location of one of the call end devices has been exceeded. Cisco CallManager checks for 24 kilobit available

bandwidth for each device before making a call. If less than 24k bandwidth is available, Cisco CallManager will not set up the call and the user will hear a reorder tone.

```
12:42:09.017 Cisco CallManager|Locations:Orig=1 BW=12Dest=0 BW=-1(-1
implies infinite bw available)
12:42:09.017 Cisco CallManager|StationD - stationOutputCallState
tcpHandle=0x4f1ad98
12:42:09.017 Cisco CallManager|StationD - stationOutputCallInfo
CallingPartyName=, CallingParty=5003, CalledPartyName=,
CalledParty=5005, tcpHandle=0x4f1ad98
12:42:09.017 Cisco CallManager|StationD - stationOutputStartTone:
37=ReorderTone tcpHandle=0x4f1ad98
```

Once the call is established, the Cisco CallManager will subtract bandwidth from the locations depending on the codec used in that call. If the call is using G.711, Cisco CallManager will subtract 80k; if the call is using G.723, Cisco CallManager will subtract 24k; if the call is using G.729, Cisco CallManager will subtract 24k.

Diagnosing Conference Bridge Problems

Use the following information to troubleshoot a No Conference Bridge available error message. This could indicate either a software or a hardware problem.

First, check to see if you have any available software or hardware Conference Bridge resources registered with Cisco CallManager. Use either Microsoft Performance or the Admin Serviceability Tool to check the number of Unicast AvailableConferences.



Note

Cisco CallManager Release 3.1 uses different names for counters and objects. Refer to the *Cisco CallManager Serviceability Administration Guide* for more information.

The Cisco IP Voice Media Streaming application performs the conference bridge function. One software installation of Cisco IP Voice Media Streaming will support 16 Unicast Available Conferences (3 people/conference), as shown in the following trace.

**Note**

The number of supported devices may vary with different Cisco CallManager releases. Refer to the release 3.1 documentation at the following location: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_1/index.htm

```
10:59:29.951 Cisco CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB_kirribilli - Registered
- ConfBridges= 16, Streams= 48, tcpHandle=4f12738
10:59:29.951 Cisco CallManager|UnicastBridgeManager -
UnicastBridgeRegistrationReq - Device Registration Complete for Name=
Xoð ô%ð - DeviceType= 50, ResourcesAvailable= 16, deviceTblIndex= 0
```

One E1 port (WS-X6608-E1 card contains 8x E1 ports) provides five Unicast Available Conferences (max conference size = 6), as shown in the following trace.

```
11:14:05.390 Cisco CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB00107B000FB0 - Registered
- ConfBridges= 5, Streams= 16, tcpHandle=4f19d64
11:14:05.480 Cisco CallManager|UnicastBridgeManager -
UnicastBridgeRegistrationReq - Device Registration Complete for Name=
Xoð ô%ð - DeviceType= 51, ResourcesAvailable= 5, deviceTblIndex= 0
```

The following hardware trace on the Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Module, indicates that the E1 port 4/1 in the card has registered as a Conference Bridge with Cisco CallManager.

```
greece-sup (enable) sh port 4/1
Port Name Status Vlan Duplex Speed Type
-----
4/1 enabled 1 full -Conf Bridge

Port DHCP MAC-Address IP-Address Subnet-Mask
-----
4/1 disable 00-10-7b-00-0f-b0 10.200.72.31 255.255.255.0

Port Call-Manager(s) DHCP-Server TFTP-Server Gateway
-----
4/1 10.200.72.25 - 10.200.72.25 -

Port DNS-Server(s) Domain
-----
4/1 - 0.0.0.0

Port CallManagerState DSP-Type
```

```

-----
4/1      registered      C549

Port  NoiseRegen NonLinearProcessing
-----
4/1  disabled    disabled

```

Second, check the maximum number of users configured in your Ad Hoc or Meet-Me conference to determine if the problem occurred because this number was exceeded.

Transcoding Problems

If you have installed a hardware transcoder in the Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Module, and it does not work as expected (you cannot make calls between two users with no common codec), check to see if you have any available Transcoder resources registered with Cisco CallManager (must be hardware). Use Microsoft Performance or the Admin Serviceability Tool to check the number of MediaTermPointsAvailable available.



Note

Cisco CallManager Release 3.1 uses different names for counters and objects. Refer to the *Cisco CallManager Serviceability Administration Guide* for more information.

One E1 port (WS-X6608-E1 card contains 8x E1 ports) provides Transcoder/MTP resources for 16 calls, as shown in the following trace.



Note

The number of supported devices may vary with different Cisco CallManager releases. Refer to the release 3.1 documentation at the following location: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_1/index.htm

```

11:51:09.939 Cisco CallManager|MediaTerminationPointControl -
Capabilities Received - Device= MTP00107B000FB1 - Registered -
Supports 16 calls

```

The following hardware trace on the Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Module, indicates that the E1 port 4/2 in the card has registered as an MTP/transcoder with Cisco CallManager.

```

greece-sup (enable) sh port 4/2
Port Name Status Vlan Duplex Speed Type
-----
4/2 enabled 1 full - MTP

Port DHCP MAC-Address IP-Address Subnet-Mask
-----
4/2 disable 00-10-7b-00-0f-b1 10.200.72.32 255.255.255.0

Port Call-Manager(s) DHCP-Server TFTP-Server Gateway
-----
4/2 10.200.72.25 - 10.200.72.25 -

Port DNS-Server(s) Domain
-----
4/2 - 0.0.0.0

Port CallManagerState DSP-Type
-----
4/2 registered C549

Port NoiseRegen NonLinearProcessing
-----
4/2 disabled disabled

```

**Note**

The same E1 port cannot be configured for both Conference Bridge and Transcoder/MTP

To make a call between two devices using a low bit rate code (such as G.729 and G.723) that do not support the same codec, a transcoder resource is required.

Assume Cisco CallManager has been configured such that the codec between Region1 and Region2 is G.729. The following scenarios are possible:

- If caller on Phone A initiates a call, Cisco CallManager realizes it is a Cisco IP Phone 7960, which supports G.729. After the digits have been collected, the Cisco CallManager determines that the call is destined for User D who is in Region2. Since the destination device also supports G.729, the call is set up and the audio flows directly between Phone A and Phone D.
- If a caller on Phone B, who has a Cisco IP Phone 12SP+, were to initiate a call to Phone D, then this time the Cisco CallManager would realize that the originating phone only supports G.723 or G.711. Cisco CallManager would need to allocate a transcoding resource so that audio would flow as G.711

between Phone B and the transcoder, but as G.729 between the transcoder and Phone D. If no transcoder were available, Phone D's phone would ring, but as soon as the call was answered, the call would disconnect.

- If a user on Phone B were to call Phone F, which is a Cisco IP Phone 12SP+, the two phones would actually use G.723, even though G.729 is configured as the codec to use between the regions. G.723 is used because both endpoints support it and it uses less bandwidth than G.729.
- If a Cisco uOne voice mail system is added (which only supports G.711) or a Cisco IOS router configured for G.711 to Region1, then a transcoding device must be used if calling from Region2. If none is available, then the call will fail.

MTP Resource Problems

An MTP resource problem could be the source of the transcoding problem if a call is established, but supplementary services are not available on an H.323 device that does not support H323v2. First, determine whether you have any available software or hardware MTP resources registered with Cisco CallManager. Use Microsoft Performance or the Admin Serviceability Tool to check the number of MediaTermPointsAvailable.



Note

Cisco CallManager Release 3.1 uses different names for counters and objects. Refer to the *Cisco CallManager Serviceability Administration Guide* for more information.

Using MTP to support supplementary services with H.323 devices that do not support H.323v2 allows one MTP software application to support 24 calls as shown in the following trace.



Note

The number of supported devices may vary with different Cisco CallManager releases. Refer to the release 3.1 documentation at the following location: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_1/index.htm

```
10:12:19.161 Cisco CallManager|MediaTerminationPointControl -
Capabilities Received - Device= MTP_kirribilli. - Registered -
Supports 24 calls
```

One E1 port (WS-X6608-E1 card contains 8x E1 ports) provides MTP resources for 16 calls, as shown in the following trace.

```
11:51:09.939 Cisco CallManager|MediaTerminationPointControl -
Capabilities Received - Device= MTP00107B000FB1 - Registered -
Supports 16 calls
```

The following hardware trace from the Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Module, indicates that the E1 port 4/2 in the card has registered as an MTP/transcoder with Cisco CallManager.

```
greece-sup (enable) sh port 4/2
Port Name Status Vlan Duplex Speed Type
-----
4/2 enabled 1 full - MTP

Port DHCP MAC-Address IP-Address Subnet-Mask
-----
4/2 disable 00-10-7b-00-0f-b1 10.200.72.32 255.255.255.0

Port Call-Manager(s) DHCP-Server TFTP-Server Gateway
-----
4/2 10.200.72.25 - 10.200.72.25 -

Port DNS-Server(s) Domain
-----
4/2 - 0.0.0.0

Port CallManagerState DSP-Type
-----
4/2 registered C549

Port NoiseRegen NonLinearProcessing
-----
4/2 disabled disabled
```

Second, in the Gateway Configuration screen of Cisco CallManager Administration, check to see if the Media Termination Point Required box is checked.

Third, verify that Cisco CallManager has allocated the required number of MTP devices.

From the SDI file:

```

15:22:23.848 Cisco CallManager|MediaManager(40) started
15:22:23.848 Cisco CallManager|MediaManager - wait_AuConnectRequest
15:22:23.848 Cisco CallManager|MediaManager - wait_AuConnectRequest -
Transcoder Enabled
15:22:23.848 Cisco CallManager|MediaManager - wait_AuConnectRequest -
party1(16777357), party2(16777358), proxies=1, connections=2, current
proxies=0
15:22:23.848 Cisco CallManager|MediaManager - wait_AuConnectRequest -
proxy connections
15:22:23.848 Cisco CallManager|MediaManager - wait_AuConnectRequest -
allocating MTP(ci=16777359)
15:22:23.848 Cisco CallManager|MediaManager -
wait_AllocateMtpResourceRes
15:22:23.848 Cisco CallManager|MediaManager -
wait_AllocateMtpResourceRes - start 2 connections
15:22:23.848 Cisco CallManager|MediaManager -
wait_AllocateMtpResourceRes - creating connection between
party1(16777357) and party2(16777359)
15:22:23.848 Cisco CallManager|MediaManager -
wait_AllocateMtpResourceRes - creating connection between
party1(16777358) and party2(16777359)
15:22:23.848 Cisco CallManager|MediaCoordinator -
wait_MediaCoordinatorAddResource - CI=16777359 count=1
15:22:23.848 Cisco CallManager|MediaCoordinator -
wait_MediaCoordinatorAddResource - CI=16777359 count=2

```

Diagnosing Dial Plan Problems

A Dial Plan is a list of numbers and groups of numbers that tells the Cisco CallManager what devices (such as phones and gateways) to send calls to when a certain string of digits is collected. It is analogous to a static routing table in a router. Please be certain your dial plan concepts, basic call routing, and planning have been carefully considered and properly configured before trying to troubleshoot a potential dial plan issue. Very often, the problem lies with planning and configuration. Refer to the route plan configuration chapters in the *Cisco CallManager Administration Guide* for more information.

Use the following tips to help troubleshoot dial plans problems:

- Identify the Directory Number (DN) that is originating the call.
- Identify the Calling Search Space for this DN.

- If applicable, identify which device the Calling Search Space is associated with this DN. Make sure that you identify the correct device; because multiple line appearances are supported, it is possible to have the same DN on multiple devices. Note the device's Calling Search Space. If this is a Cisco IP Phone originating the call, remember that a particular line (DN) and the device that line is associated with have Calling Search Spaces. They will be combined when making a call. For example, if line instance 1000 has a Calling Search Space of AccessLevelX and the Cisco IP Phone that has extension 1000 configured on it has AccessLevelY as its Calling Search Space, then when making a call from that line appearance, Cisco CallManager will search through partitions contained in Calling Search Space AccessLevelX and AccessLevelY.
- Identify which Partitions are associated with the Calling Search Space(s).
- Identify which Partition of the device to which the call should (or should not) go.
- Identify which number is being dialed. Note that if and when the user is getting a secondary dial tone. Also note what they hear after all the digits have been entered (re-order, fast-busy). Does the user get the progress tones before expecting to hear anything? Make sure callers wait at least 10 seconds after typing the last digit because they may have to wait for the inter-digit timer to expire.
- Generate a Route Plan Report in Cisco CallManager Administration, and use it to examine all the route patterns for the partitions that are in the Calling Search Space for the problem call.
- If necessary, add or modify the Route Patterns or Route Filters.
- If you can find the Route Pattern to which the call is being sent, note the Route List or Gateway to which the pattern points.
- If it is a Route List, check which Route Groups are part of the list and which Gateway(s) is part of the Route Groups.
- Verify that the applicable devices are registered with Cisco CallManager.
- If there is no access to Cisco CallManager, use the show tech command to capture and verify this information.
- Pay attention to the @ sign. This is a macro that can expand to include many different things. It is often used in combination with filtering options.

- If a device is not part of a partition, it is said to be part of the Null or default partition. Every user should be able to call that device. The Null partition is always searched last.
- If you dial an outside number that is matching a 9.@ pattern and it takes 10 seconds before the call goes through, check the filtering options. By default, with a 9.@ pattern, when dialing a 7-digit number, the Cisco IP Phone will wait 10 seconds before placing the call. You need to apply a Route Filter to the pattern that says LOCAL-AREA-CODE DOES-NOT- EXIST and END-OF-DIALING DOES-NOT-EXIST.

Diagnosing Partition Problems

Route partitions inherit the error handling capabilities for the Cisco CallManager software. That is, a console and SDI file trace are provided for logging information and error messages. These messages will be part of the digit analysis component of the traces. It is vital that you know how the Partitions and Calling Search Spaces are configured and what devices are in each partition and its associated calling search space to determine the source of the problem. Refer to the route plan chapters in the *Cisco CallManager Administration Guide* and the *Cisco CallManager System Guide* for more information.

The following trace is an example of a number dialed that is in the device's Calling Search Space. For more detailed explanations about SDI traces, review the case studies in this document.

```
08:38:54.968 Cisco CallManager|StationInit - InboundStim -
OffHookMessageID tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputDisplayText
tcpHandle=0x6b88028, Display= 5000
08:38:54.968 Cisco CallManager|StationD - stationOutputSetLamp stim:
9=Line instance=1 lampMode=LampOn tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputCallState
tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD -
stationOutputDisplayPromptStatus tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD -
stationOutputActivateCallPlane tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="")
```

In the Digit Analysis component of the previous trace, the pss (Partition Search Space, also known as Calling Search Space) is listed for the device placing the call.

In the following trace, RTP_NC_Hardwood;RTP_NC_Woodland;Local_RTP are the partitions this device is allowed to call.

```
08:38:54.968 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:54.968 Cisco CallManager|StationD - stationOutputStartTone:
33=InsideDialTone tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 5 tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationD - stationOutputStopTone
tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5")
08:38:55.671 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:56.015 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 0 tcpHandle=0x6b88028
08:38:56.015 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="50")
08:38:56.015 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:56.187 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 0 tcpHandle=0x6b88028
08:38:56.187 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="500")
08:38:56.187 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:56.515 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 3 tcpHandle=0x6b88028
08:38:56.515 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5003")
08:38:56.515 Cisco CallManager|Digit analysis: analysis results
08:38:56.515 Cisco CallManager||PretransformCallingPartyNumber=5000
```

The key thing to note is that PotentialMatchesExist is the result of Digit Analysis of the numbers that were dialed until the exact match is found and the call is routed accordingly.

The following trace describes what happens when the Cisco CallManager is attempting to dial the directory number 1001 and it is not in the Calling Search Space for that device. Again, the key thing to note is the digit analysis routine had

potential matches until only the first digit was dialed. The route pattern associated with the digit 1 is in a partition that is not in the device's calling search space, RTP_NC_Hardwood;RTP_NC_Woodland;Local_RTP. Therefore, the phone received a reorder tone (busy signal).

```
08:38:58.734 Cisco CallManager|StationInit - InboundStim -
OffHookMessageID tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputDisplayText
tcpHandle=0x6b88028, Display= 5000
08:38:58.734 Cisco CallManager|StationD - stationOutputSetLamp stim:
9=Line instance=1 lampMode=LampOn tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputCallState
tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD -
stationOutputDisplayPromptStatus tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD -
stationOutputActivateCallPlane tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="")
08:38:58.734 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:58.734 Cisco CallManager|StationD - stationOutputStartTone:
33=InsideDialTone tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 1 tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationD - stationOutputStopTone
tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="1")
08:38:59.703 Cisco CallManager|Digit analysis:
potentialMatches=NoPotentialMatchesExist
08:38:59.703 Cisco CallManager|StationD - stationOutputStartTone:
37=ReorderTone tcpHandle=0x6b88028
```

Route partitions work by associating a partition name with every directory number in the system. The directory number can be called only if the calling device contains the partition within a list of partitions to which it is permitted to place calls—its partition search space. This provides for extremely powerful control over routing.

When a call is being placed, Digit Analysis attempts to resolve the dialed address only in those partitions that the partition search space specifies. Each partition name comprises a discrete subset of the global dial-able address space. From each

listed partition, Digit Analysis retrieves the pattern that best matches the sequence of dialed digits. Then, from among the matching patterns, Digit Analysis chooses the best match. If two patterns equally match the sequence of dialed digits, Digit Analysis breaks the tie by selecting the pattern associated with the partition listed first in the partition search space.

Diagnosing Security Problems

Using partitions and calling search spaces, in addition to more common filtering based on sections of the @ macro (which stands for the North American Numbering Plan) in a route pattern, you can configure Cisco CallManager to create a secure dialing plan for users. Partitions and Calling Search Spaces are an integral part of security and are especially useful for multi-tenant environments and for creating an individual user level. Filtering, a subset of the Calling Search Space/Partition concept, can add additional granularity to the security plan.

This is an extension to the [Diagnosing Dial Plan Problems, page 3-18](#). Be advised, usually the last thing you want to do when trying to fix a filtering problem is to run an SDI trace. There is simply not enough information and the potential for causing more harm is too great.

Run a show tech command on Cisco CallManager to diagnose Slow Server Response.

Diagnosing Slow Server Response

Slow response from the server could result if the duplex of the switch does not match the duplex port setting on the Cisco CallManager server. For optimal performance set both switch and server to 100/Full. We do not recommend using the Auto setting on either the switch or the server. You must restart the Cisco CallManager server for this change to take effect.

Determining Gateway Reorder Tone Problems

Users placing a call through the gateway might get a reorder tone if they are attempting to make a restricted call or to call a number that has been blocked. A reorder tone may occur if the dialed number is out of service or if the PSTN has

an equipment or service problem. Check to be sure the device giving the reorder tone has registered. Also, check your dial plan configuration to ensure that the call can be successfully routed.

The following procedure shows the steps for troubleshooting reorder tones through gateways.

Procedure

- Step 1** Check the gateways to ensure that you are using the latest software loads.
 - Step 2** Check Cisco Connection Online at www.cisco.com for the latest software loads, new patches, or release notes relating to the problem.
 - Step 3** Start an SDI trace and recreate the problem. Reorder tones could be the result of a configuration issue with location-based admission control or gatekeeper-based admission control where the Cisco CallManager might limit the number of allowable calls. In the SDI trace, locate the call to determine if it was blocked intentionally by a route pattern or the calling search space, or by any other configuration setting.
 - Step 4** Reorder tones can also occur when calling through the PSTN. Check the SDI trace for Q.931 messages, in particular, for disconnect messages. If a Q.931 disconnect message is present, it means the other party caused the disconnect and you cannot correct for that.
-

Diagnosing Gateway Registration Problems

One of the most common issues encountered with gateways on a Cisco CallManager is a registration problem. Registration can fail for a variety of reasons.

This section describes two similar but different categories of gateways. The Cisco Access AS-X, AT-X and Cisco Access DT-24+ and DE-30+ belong to one category. These gateways are stand-alone units that are not directly connected to a Network Management Processor (NMP). The second category includes the

Analog Access WS-X6624 and Digital Access WS-X6608. These gateways are blades installed in a Catalyst 6000 chassis with direct connectivity to the NMP for control and statusing.

First, check that the gateway is up and running. All of the gateways have a heartbeat LED that blinks 1-second-on, 1-second-off when the gateway software is running normally. If this LED is not blinking at all, or blinking very rapidly, then the gateway software is not running. Normally this will result in an automatic reset of the gateway. Also, it is normal for the gateway to reset itself if it cannot complete the registration process after about 2 to 3 minutes. So you may happen to look at the heartbeat LED while the device is resetting, but if the normal blinking pattern does not appear in 10 to 15 seconds, then the gateway has suffered a serious failure. On the Cisco Access Analog gateways, the green heartbeat LED is on the far right of the front panel. On the Cisco Access Digital gateways, it is the far left red LED on the top edge of the card. On the Cisco Analog Access WS-X6624, it is a green LED inside the blade (not visible from the front panel) on the far right card edge near the front. Finally, on the Digital Access WS-X6608 there is a separate heartbeat LED for each of the 8 spans on the blade. There are 8 red LEDs across the card (not visible from the front panel) about two thirds of the way towards the back.

The second thing to check is that the gateway has received its IP address. A standalone gateway must receive its IP address via DHCP or BOOTP. A Catalyst gateway may receive its IP address by DHCP, BOOTP, or by manual configuration through the NMP. If you have access to the DHCP server, the best way to check a stand-alone gateway is to verify that the device has an outstanding lease on an IP address. If the gateway shows up on your server, this is a good indication, but not definitive. Delete the lease at the DHCP server, and then reset the gateway. If the gateway reappears on the server with a lease within a couple of minutes, then everything is working fine in this area. If not, then either the gateway cannot contact the DHCP server (Is a router improperly configured and not forwarding DHCP broadcasts? Is the server running?), or cannot get a positive response (Is the IP address pool depleted?). If checking these suggestions does not yield the answer, use a sniffer trace to determine the specific problem.

For a Catalyst 6000 gateway, you should check to make sure the NMP can communicate with the gateway. You can check this by trying to ping its internal IP address from the NMP. The IP address is in the format:

```
127.1.module.port
```

In our example, we would enter:

```
Console (enable) ping 127.1.7.1
```


If this timeout message continues to scroll by, then there is a problem contacting the DHCP server. First thing to check is that the Catalyst 6000 gateway port is in the correct VLAN.

You will find this information in the information you retrieved using the **sh port** command. If the DHCP server is not on the same VLAN as the Catalyst 6000 gateway, then make sure the appropriate IP helper addresses have been configured to forward the DHCP requests to the DHCP server. It is possible for the gateway to get stuck in the INIT state after a VLAN number change until the gateway resets. When in this state, it would not hurt to try resetting the gateway. Every time the 860 gets reset, your tracy session will be lost, so you must close your existing session and re-establish a new one by issuing the following commands:

```
tracy_close mod port
```

```
tracy_start mod port
```

If all this checks out and you are still seeing the DHCPState = INIT messages, you should check to see if the DHCP server is functioning correctly. If so, start a sniffer trace to see whether the requests are being sent and the server is responding.

Once DHCP is working correctly, the gateway will have an IP address that will allow the use of the tracy debugging utility. This utility is a built-in feature of the NMP command set for the Catalyst gateways, and available as a helper application that runs on Windows 98/NT/2000 for the stand-alone gateways. To use the helper application tracy utility, you need to connect to the gateway by using the IP address to which it is assigned. This tracy application works on all the gateways, provides a separate trace window for each gateway (up to eight may be traced at once), and allows traces to be logged directly to a file you specify.

The next step is to verify that the TFTP server IP address was correctly provided to the gateway. This is normally provided by DHCP in either Option 66 (by name or IP address), Option 150 (IP address only), or *si_addr* (IP address only). If your server has multiple Options configured, *si_addr* will take precedence over Option 150, which will take precedence over Option 66. If Option 66 provides the DNS_NAME of the TFTP server, then the DNS server(s) IP address(es) must have been specified by DHCP, and the name entered in Option 66 must resolve to the correct TFTP server IP address. A Catalyst gateway could be configured by the NMP to disable DHCP, and the NMP operator must then enter all configuration parameters by hand at the console, including the TFTP server address.

Additionally, the gateways will always attempt to resolve the name CiscoCM1 via DNS. If successful, the CiscoCM1 IP address will take precedence over anything the DHCP server or NMP tells it for the TFTP server address, even if the NMP has DHCP disabled.

You can check the current TFTP server IP address in a gateway by using the tracy utility. Enter the following command to get the configuration task number:

```
TaskID: 0
Cmd:    show t1
```

Look for a line with config or CFG and use the corresponding number as the taskID for the next line. For example, for the Cisco Access Digital gateway. In the examples that follow, we have bolded lines of text to make it easier for you to see the messages being explained. In the actual display output, text is not bolded. The examples are from an WS-X6624 model, the command to dump the DHCP information is:

```
TaskID: 6
Cmd:    show dhcp
```

The TFTP server IP address is then clearly shown. If it is not correct, verify that your DHCP options and other information it provides are correct.

Once the TFTP address is correct, the next step would be to ensure that the gateway is getting its configuration file from the TFTP server. If you see the following in the tracy output, your TFTP service may not be working correctly or the gateway might not be configured on the Cisco CallManager:

```
00:09:05.620 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP
Server
00:09:18.620 (CFG) TFTP Error: Timeout Awaiting Server Response for
.cnf File!
```

The gateway will attempt to connect to the same IP address as the TFTP server if it does not get a configuration file. This is fine unless you are in a clustered environment in which the gateway needs to receive its list of redundant Cisco CallManagers. If the card is not getting its TFTP information correctly, check the TFTP service on the Cisco CallManager and make sure it is running. Also, check the TFTP trace on the Cisco CallManager.

Another common problem is that the gateway is not configured correctly on the Cisco CallManager. A typical error is entering an incorrect MAC address for the gateway. If this is the case, for a Catalyst 6000 gateway, you will probably get the following messages on the NMP console every two minutes:

```

2000 Apr 14 19:24:08 %SYS-4-MODHPRESET:Host process (860) 7/1 got
reset asynchronously
2000 Apr 14 19:26:05 %SYS-4-MODHPRESET:Host process (860) 7/1 got
reset asynchronously
2000 Apr 14 19:28:02 %SYS-4-MODHPRESET:Host process (860) 7/1 got
reset asynchronously

```

This is what the Tracy output would look like if the gateway is not in the Cisco CallManager database:

```

00:00:01.670 (CFG) Booting DHCP for dynamic configuration.
00:00:05.370 (CFG) DHCP Request or Discovery Sent, DHCPState =
INIT_REBOOT
00:00:05.370 (CFG) DHCP Server Response Processed, DHCPState = BOUND
00:00:05.370 (CFG) Requesting DNS Resolution of CiscoCMI
00:00:05.370 (CFG) DNS Error on Resolving TFTP Server Name.
00:00:05.370 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2
00:00:05.370 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP
Server
00:00:05.370 (CFG) TFTP Error: .cnf File Not Found!
00:00:05.370 (CFG) Requesting SAADefault.cnf File From TFTP Server
00:00:05.380 (CFG) .cnf File Received and Parsed Successfully.
00:00:05.380 (CFG) Updating Configuration ROM...
00:00:05.610 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.610 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket
00:00:05.610 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:00:05.610 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
00:00:05.610 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:00:05.610 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState =
SentRegister
00:00:05.680 GMSG: CCM#0 CPEvent = CLOSED --> CPState = NotCPSocket
00:00:05.680 GMSG: GWEvent = DISCONNECT --> GWState = Rollover
00:00:20.600 GMSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:00:20.600 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket
00:00:20.600 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:00:20.600 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM

```

Another possible registration problem could be that the load information is incorrect or the load file is corrupt. The problem could also occur if the TFTP server is not working. In this case, Tracy clearly shows that the TFTP server reported the file is not found:

```

00:00:07.390 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState =
SentRegister
00:00:08.010 GMSG: TFTP Request for application load A0021300
00:00:08.010 GMSG: CCM#0 CPEvent = LOADID --> CPState = AppLoadRequest

```

```
00:00:08.010 GMSG: ***TFTP Error: File Not Found***
00:00:08.010 GMSG: CCM#0 CPEvent = LOAD_UPDATE --> CPState =
LoadResponse
```

In this case, you can see that the gateway is requesting application load A0021300, although the correct load name would be A0020300. For a Catalyst 6000 gateway, the same problem can occur when a new application load needs to get its corresponding DSP load as well. If the new DSP load is not found, a similar message will appear.

```
ELVIS>> 00:00:00.020 (XA) MAC Addr : 00-10-7B-00-13-DE
00:00:00.050 NMPTask:got message from XA Task
00:00:00.050 (NMP) Open TCP Connection ip:7f010101
00:00:00.050 NMPTask:Send Module Slot Info
00:00:00.060 NMPTask:get DIAGCMD
00:00:00.160 (DSP) Test Begin -> Mask<0x00FFFFFF>
00:00:01.260 (DSP) Test Complete -> Results<0x00FFFFFF/0x00FFFFFF>
00:00:01.260 NMPTask:get VLANCONFIG
00:00:02.030 (CFG) Starting DHCP
00:00:02.030 (CFG) Booting DHCP for dynamic configuration.
00:00:05.730 (CFG) DHCP Request or Discovery Sent, DHCPState =
INIT_REBOOT
00:00:05.730 (CFG) DHCP Server Response Processed, DHCPState = BOUND
00:00:05.730 (CFG) Requesting DNS Resolution of CiscoCM1
00:00:05.730 (CFG) DNS Error on Resolving TFTP Server Name.
00:00:05.730 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2
00:00:05.730 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP
Server
00:00:05.730 (CFG) .cnf File Received and Parsed Successfully.
00:00:05.730 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.730 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket
00:00:05.730 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:00:05.730 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
00:00:05.730 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:00:05.730 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState =
SentRegister
00:00:06.320 GMSG: CCM#0 CPEvent = LOADID --> CPState = LoadResponse
00:01:36.300 GMSG: CCM#0 CPEvent = TIMEOUT --> CPState = BadCCM
00:01:36.300 GMSG: GWEvent = DISCONNECT --> GWState = Rollover
00:01:46.870 GMSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPsSocket
00:01:51.300 GMSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:01:51.300 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket
00:01:51.300 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:01:51.300 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
00:01:51.300 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
```

```
00:01:51.300 MSG: CCM#0 CPEvent = REGISTER_REQ --> CPState =  
SentRegister  
00:01:51.890 MSG: CCM#0 CPEvent = LOADID --> CPState = LoadResponse
```

The difference here is that the gateway gets stuck in the LoadResponse stage and eventually times out. This problem can be resolved by correcting the load file name in the Device Defaults area of Cisco CallManager Administration.

Diagnosing Gatekeeper Problems

Before starting any gateway-to-gatekeeper troubleshooting, verify that there is IP connectivity within the network. Assuming that there is IP connectivity, use the information in this section to troubleshoot your gateway.

Inter-Cluster Trunks or H.225 Gateway

Refer to the *Cisco CallManager Administration Guide* and *Cisco CallManager System Guide* at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_1/index.htm

Admission Rejects

Admission Rejects (ARJ) are issued when Cisco CallManager has registered with the Gatekeeper but cannot send a phone call. Configuration issues on the gatekeeper should be the primary focus when the gatekeeper is issuing an ARJ. The following procedure is a general guideline for troubleshooting.

Procedure

-
- Step 1 Verify IP connectivity from the gateway to the gatekeeper.
 - Step 2 Show gatekeeper status—verify the gatekeeper state is up.
 - Step 3 Is there a zone subnet defined on the gatekeeper? If so, verify that the subnet of the gateway is in the allowed subnets.
-

Registration Rejects

Registration Rejects (RRJ) are issued when Cisco CallManager cannot register with the Gatekeeper. Configuration issues on the gatekeeper should be the primary focus when the gatekeeper is issuing a RRJ.

The following procedure is a general guideline for troubleshooting.

Procedure

- Step 1** Verify IP connectivity from the gateway to the gatekeeper.
 - Step 2** Show gatekeeper status—verify the gatekeeper state is up.
 - Step 3** Is there a zone subnet defined on the gatekeeper? If so, verify that the subnet of the gateway is in the allowed subnets.
-