



Device Issues

This chapter addresses the following common problems that you may experience with Cisco IP Phones, gateways, and related devices.

- [Voice Quality](#)
- [Codec and Region Mismatches](#)
- [Location and Bandwidth](#)
- [Phone Resets](#)
- [Dropped Calls](#)
- [Gateway Reorder Tone](#)
- [Gateway Registration Failure](#)
- [Gatekeeper Issues](#)
- [B-Channel Remains Locked When Restart_Ack Does Not Contain Channel IE](#)

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, and watery or robotic voice quality. One-way audio, that is, a conversation between two people where only one person can hear anything, does not actually represent a voice quality issue, but this section covers this issue.

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

- Gateways
- Phones
- Networks

This section covers the following common voice quality problems:

- [Lost or Distorted Audio](#)
- [Correcting Audio Problems from the Cisco IP Phone](#)
- [Echo](#)
- [One-Way Audio or No Audio](#)

Lost or Distorted Audio

Symptom

One of the most common problems that you may encounter involves broken audio signal (often described as garbled speech or lost syllables within a word or sentence). Two common causes for this exist: 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 describes 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 it takes for a packet to get from point A to point B but is simply the variation in packet arrival times.

Probable Cause

Many sources of variable delay exist in a network. You can control some of these but not others. You cannot entirely eliminate variable delay in a packetized voice network. Digital Signal Processors (DSP) on phones and other voice-capable devices by design buffer some of the audio in anticipation of variable delay. This dejittering occurs 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 1 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 WAN).

Corrective Action

Procedure

- Step 1** When you are faced with a lost or distorted audio problem, first try to isolate the path of the audio. Try to identify each network device (switches and routers) in the path of the call 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 whether the problem occurs only between two sites, only through a certain gateway, on a certain subnet, and so on. This will help narrow the number of devices that you need to look at more carefully.
- Step 2** Next, disable silence suppression (also known as Voice Activation Detection or VAD). 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.
- Disable the service in Cisco CallManager Administration, choose **Service > Service Parameters**. From there, choose the server and the Cisco CallManager service.
- Step 3** Set SilenceSuppression to **False** to disable for all devices in a Cisco CallManager cluster; alternatively, you can set SilenceSuppressionForGateways to **False**. When in doubt, turn both off by choosing the value **False** for each.

- Step 4** Using a network analyzer, if a network analyzer is available, check whether a monitored call between two phones has 50 packets per second (or 1 packet every 20 ms) when silence suppression is disabled. With proper filtering, you can identify whether an excessive number of packets are lost or delayed.

Remember that delay by itself will not cause clipping, only variable delay. Notice in the table below, which represents a perfect trace, the arrival times between the audio packets (which will have an RTP header) that 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 (sec)	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 the number of places from which the delay is coming from. If no analyzer is available, you will need to use other methods. Examine interface statistics of each device in the path of the audio.

Diagnostic Call Detail Records (CDR) specifies another tool for tracking calls with poor voice quality. Refer to the *Cisco CallManager Serviceability Administration Guide* for more information about CDRs.

Correcting Audio Problems from the Cisco IP Phone

Symptom

Audio problems occurs while a call is in progress.

Probable Cause

Devices, where a higher speed interface feeds into a lower speed interface, provide the most common sources for delay and packet loss. 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, the most likely causes of the problem include

- The router has not been properly configured to give voice traffic priority over data traffic.
- Too many active calls exist for the WAN to support (that is, no call admission control restricts the number of calls that can be placed).
- Physical port errors occur.
- Congestion in the WAN itself occurs.

On the LAN, the most common problems represent physical-level errors (such as CRC errors) that are 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.

Corrective Action

The Cisco IP Phone 7960 provides another tool for diagnosing possible audio problems.

Procedure

-
- Step 1** 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 represents the average of the last five packets that arrived; the maximum jitter designates the maximum for the average jitter.

- Step 2** Situations could also occur where the traffic is taking a slower path through the network than expected. If QoS has been configured correctly, the possibility exists that there is no call admission control. Depending on your topology, you can accomplish this 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 the maximum calls supported across your WAN.

Diagnosing Crackling Sounds

- Step 3** Crackling is another poor quality symptom, 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

- Step 4** Verify gateway and phone loads. Check Cisco Connection Online (CCO) at www.cisco.com for the latest software loads, new patches, or release notes relating to the problem.
-

Verification

Procedure

- Step 1** Test by disabling silence suppression as described in [Lost or Distorted Audio](#); 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.
- Step 2** With the maximum number of calls across the WAN, the calls should all have acceptable quality.
- Step 3** Test to make sure that a fast busy is returned when you try to make one more call.
-

Echo

Symptom

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 goes 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 because packetization and compression contribute to the delay.

Probable Cause

Remember 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. The only exception may occur if one party is using a speakerphone that has the volume set too high or other situations where an audio loop is created.

Corrective Action

Procedure

- Step 1** 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 percent of the maximum audio level). Most of the time, the problems occur when you attach to the PSTN by way of a digital or analog gateway.

Testing the Gateway

- Step 2** Determine which gateway is being used. If a digital gateway is in use, you may be able to add additional padding in the transmit direction (towards the PSTN). Because lower signal strength will yield less reflected energy, this should clear the problem.

Additionally, you can adjust the receive level, so any reflected audio is reduced even further. Remember to make small adjustments at a time. Too much attenuation of the signal will make the audio impossible to hear on both sides.

- Step 3** 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), echo likely will result.

Keeping an Echo Log

- Step 4** 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 cannot 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 fact provides one of the reasons why it is important to note the external phone number of a call that experiences echo.

Checking Your Loads

- Step 5** 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.
-

One-Way Audio or No Audio

Symptom

When one person cannot hear another person during a call, one-way audio exists.

Probable Cause

An improperly configured Cisco IOS Gateway, a firewall, or a routing or default gateway problem, among other things can cause this problem.

Corrective Action

Procedure

- Step 1** You may find that diagnostic Call Detail Records (CDR) are useful for determining whether a call is experiencing one-way audio because they log transmitted and received packets (see [Lost or Distorted Audio](#) and refer to the *Cisco CallManager Serviceability Administration Guide* for more details.).
- 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 the MTP

- Step 2** 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 whether the allocated MTP 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 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, you may experience one-way audio or audio loss. Shut down MTP to find out whether MTP is causing the problem.

Testing Cisco CallManager Configuration

- Step 3** Many causes exist for one-way audio or loss of audio during a call. An improperly configured device provides the most common cause. 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). The Cisco CallManager can 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 happens 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.

- Step 4** 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.
- Step 5** 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, check the configuration carefully.
- Ensure that IP routing is 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

- Step 6** Make sure that if you are using RTP header compression to save bandwidth across the WAN, that it is enabled on each router that is carrying voice traffic that attaches to the WAN circuit. A situation should not occur where the RTP header is compressed on one end but cannot be decompressed on the other side of the WAN. 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 get transmitted from the phone that has pressed the **Mute** button. The **Hold** button stops the audio stream, so no packets get 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.

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 list gives codecs that 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/mu-law, G.723.1

Cisco Access Gateway DE30 and DT-24+—G.711a-law/mu-law, G.723.1

Location and Bandwidth

If a user gets a reorder tone after dialing a number, this could happen because the Cisco CallManager bandwidth allocation for the location of one of the call end devices has been exceeded. Cisco CallManager checks for 24k 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 receives 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.

Phone Resets

Symptom

Phone resets.

Probable Cause

Phones will power cycle or reset for two reasons:

- TCP failure connecting to Cisco CallManager
- Failure to receive an acknowledgement to the phone KeepAlive messages.

Corrective Action

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 represent considered Information events.
- Step 4** Look for 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).
-

Dropped Calls

Symptom

Premature termination of dropped calls.

Probable Cause

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

Corrective Action

Procedure

- Step 1** Determine whether this problem is isolated to one phone or to a group of phones. Perhaps you will find that the affected phones are all on a particular subnet or location.

- Step 2** 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 occur because a phone was turned off or a problem may exist in the network. If this is an intermittent problem, you may find it useful to use Microsoft Performance to record phone registrations.
- Step 3** If the problem seems to be occurring only through a certain gateway, such as a Cisco Access DT-24+, 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. Refer to the *Cisco CallManager Serviceability Administration Guide* for detailed information on CDRs.
- Step 4** Find the disconnect cause values (origCause_value and destCause_value—depending on which side hung up the call), that map to Q.931 disconnect cause codes (in decimal) at the following location:
- <http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/dbook/disdn.htm>.
- Step 5** If the call is going out of a gateway to the PSTN, you can use the CDR to determine which side is hanging up the call. Obtain much of the same information 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.
-

Gateway Reorder Tone

Symptom

Reorder tone occurs.

Probable Cause

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 that the device giving the reorder tone has registered. Also, check your dial plan configuration to ensure that the call can be successfully routed.

Corrective Action

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 re-create 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 occurs 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 that the other party caused the disconnect, and you cannot correct for that.
-

Gateway Registration Failure

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 identify 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, as blades installed in a Catalyst 6000 chassis, provide direct connectivity to the NMP for control and statusing.

Symptom

A registration problem represents one of the most common issues that are encountered with gateways on a Cisco CallManager.

Probable Cause

Registration can fail for a variety of reasons.

Corrective Action

Procedure

Step 1 First, check that the gateway is up and running. All 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, the gateway software is not running. Normally, this results 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, the gateway has suffered a serious failure.

On the Cisco Access Analog gateways, find the green heartbeat LED on the far right of the front panel. On the Cisco Access Digital gateways, find the red LED on the far left on the top edge of the card. On the Cisco Analog Access WS-X6624, a green LED appears 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, a separate heartbeat LED exists for each of the 8 spans on the blade. Eight red LEDs appear across the card (not visible from the front panel) about two thirds of the way towards the back.

- Step 2** Check that the gateway 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.
- Step 3** If you have access to the DHCP server, the best way to check a standalone gateway is to verify that the device has an outstanding lease on an IP address. If the gateway shows up on your server, this provides a good indication but is not definitive. Delete the lease at the DHCP server.
- Step 4** Reset the gateway.
- Step 5** If the gateway reappears on the server with a lease within a couple of minutes, everything works fine in this area. If not, 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?).
- Step 6** If performing these checks does not yield the answer, use a sniffer trace to determine the specific problem.
- Step 7** For a Catalyst 6000 gateway, you should check to make sure that 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 uses this format:

```
127.1.module.port
```

For example, for port 1 on module 7, you would enter

```
Console (enable) ping 127.1.7.1
127.1.7.1 is alive
```

- Step 8** If pinging works, the **show port** command shows the IP address information. Make sure that the IP address information and the TFTP IP address is correct as well.

- Step 9** If the gateway is failing to obtain valid DHCP information, use the tracy utility (supplied by Cisco TAC) to determine the problem.
- Step 10** After obtaining this utility from TAC, issue the following command from the Cat6000 Command Line Interface (CLI):

```
tracy_start mod port
```

In this example, the WS-X6624 represents module 7, and it has only a single 860 processor, so it is port 1. The command to issue is **tracy_start 7 1**.

The following output actually comes from the 860-console port on the gateway board itself; however, the output of the tracy command represents nothing more than a remote copy of the 860-console port.

```

      |
      |
    | |
    | |
  | | | |
  | | | | | : : |
C i s c o   S y s t e m s
CAT6K Analog Gateway (ELVIS)
APP Version : A0020300, DSP Version : A0030300, Built Jun  1 2000
16:33:01

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
00:00:02.870 (CFG) Starting DHCP
00:00:02.870 (CFG) Booting DHCP for dynamic configuration.
00:00:06.570 (CFG) DHCP Request or Discovery Sent, DHCPState =
INIT_REBOOT
00:00:06.570 (CFG) DHCP Server Response Processed, DHCPState =
INIT_REBOOT
00:00:06.780 (CFG) IP Configuration Change!  Restarting now...
00:00:10.480 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT
00:00:14:480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
00:00:22:480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
00:00:38:480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT

```

If this timeout message continues to scroll by, a problem exists with contacting the DHCP server.

- Step 11** First, check that the Catalyst 6000 gateway port is in the correct VLAN. You will find this information in the information that you retrieved by using the **show port** command.
- Step 12** If the DHCP server is not on the same VLAN as the Catalyst 6000 gateway, then make sure that the appropriate IP helper addresses have been configured to forward the DHCP requests to the DHCP server. The gateway can get stuck in the INIT state after a VLAN number change until the gateway resets.
- Step 13** When in the INIT state, try resetting the gateway. Every time that the 860 gets reset, your tracy session will be lost, so you must close your existing session and reestablish a new one by issuing the following commands:

```
tracy_close mod port
```

```
tracy_start mod port
```

- Step 14** If you are still seeing the `DHCPState = INIT` messages, check whether the DHCP server is functioning correctly.
- Step 15** 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 allows the use of the tracy debugging utility. This utility includes a built in feature of the NMP command set for the Catalyst gateways and is available as a helper application that runs on Windows 98/NT/2000 for the standalone gateways.

- Step 16** To use the helper application tracy utility, 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 that you specify.
- Step 17** Verify that the TFTP server IP address was correctly provided to the gateway. DHCP normally provides DHCP in 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. The NMP could configure a Catalyst gateway could be configured by the NMP to disable DHCP, and the NMP operator must then manually enter all configuration parameters 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 that the DHCP server or NMP tells it for the TFTP server address, even if the NMP has DHCP disabled.

- Step 18** 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 tl
```

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

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

- Step 19** The TFTP server IP address then appears. If it is not correct, verify that your DHCP options and other information that it provides are correct.
- Step 20** Once the TFTP address is correct, ensure that the gateway is getting its configuration file from the TFTP server. If you see the following information 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 attempts to connect to the same IP address as the TFTP server if it does not get a configuration file. This works fine unless you are in a clustered environment in which the gateway needs to receive its list of redundant Cisco CallManagers.

- Step 21** If the card is not getting its TFTP information correctly, check the TFTP service on the Cisco CallManager and make sure it is running.
- Step 22** Check the TFTP trace on the Cisco CallManager.

Another common problem occurs if the gateway is not configured correctly on the Cisco CallManager. A typical error involves 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 2 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
```

The following example shows 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 shows that the TFTP server reported that 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, the gateway requests 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 MSG: GWEvent = DISCONNECT --> GWState = Rollover
00:01:46.870 MSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPsocket
00:01:51.300 MSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:01:51.300 MSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket
00:01:51.300 MSG: Attempting TCP socket with CCM 10.123.9.2
00:01:51.300 MSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
00:01:51.300 MSG: 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. You can resolve this problem by correcting the load file name in the Device Defaults area of Cisco CallManager Administration.

Gatekeeper Issues

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

- [Intercluster Trunks or H.225 Trunks](#)
- [Admission Rejects](#)
- [Registration Rejects](#)

Intercluster Trunks or H.225 Trunks

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_3/index.htm

Admission Rejects

Symptom

The system issues Admission Rejects (ARJ) when Cisco CallManager has registered with the Gatekeeper but cannot send a phone call.

Probable Cause

Configuration issues on the gatekeeper should be the primary focus when the gatekeeper issues an ARJ.

Corrective Action

Procedure

- Step 1 Verify IP connectivity from the Cisco CallManager to the gatekeeper.
 - Step 2 Show gatekeeper status and verify that the gatekeeper state is up.
 - Step 3 Is there a zone subnet defined on the gatekeeper? If so, verify that the subnet of the Cisco CallManager is in the allowed subnets.
 - Step 4 Verify that the technology prefix matches between the Cisco CallManager and the gatekeeper configuration.
-

Registration Rejects

Symptom

The system issues Registration Rejects (RRJ) when Cisco CallManager cannot register with the gatekeeper.

Probable Cause

Configuration issues on the gatekeeper should be the primary focus when the gatekeeper is issuing a RRJ.

Corrective Action

Procedure

- Step 1 Verify IP connectivity from the Cisco CallManager to the gatekeeper.
 - Step 2 Show gatekeeper status and verify that 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.
-

Cisco CallManager Locks the B-Channel and Sends Restart

Symptom

Cisco CallManager locks the B-channel and sends a restart on that channel for no apparent reason. For related information, see [B-Channel Remains Locked When Restart_Ack Does Not Contain Channel IE](#).

Outbound calls cause DSPs to lockup.



Note

Release 3.1(2c) Engineer Special 21 resolves this problem.

Probable Cause

Your ISDN channel selection order causes a glare condition. This may occur when a high volume of calls occurs.

Also, B-channel selection for outgoing calls is exclusive (the Cisco CallManager does not accept other B-channels). If a channel is not available, the PABX or CO sends Release Complete.

Corrective Action

Procedure

- Step 1** From Cisco CallManager Administration, choose **Device > Gateway**.
The Find and List Gateways window appears.
- Step 2** Enter search criteria to locate a specific gateway.
- Step 3** Click **Find**.
A list of discovered devices displays.
- Step 4** Click the *device name* of the gateway that you want to update.
The Gateway Configuration window appears.
- Step 5** To access gateway ports, click the icon of the gateway port or the MGCP endpoint link on the left side of the configuration window for the chosen gateway.
- Step 6** Check the **Inhibit Restarts at PRI initialization** check box.
- Step 7** Click **Update**.
- Step 8** Reset the gateway to apply the changes.
- Step 9** Restart the Cisco CallManager server.



Note You must restart the Cisco CallManager server to clear the restart problem after checking the **Inhibit Restarts at PRI Initialization** check box.

For detailed information on E1/T1 PRI configuration settings, refer to the *Cisco CallManager Administration Guide*.

B-Channel Remains Locked When Restart_Ack Does Not Contain Channel IE

Symptom

This issue relates to the previous issue: [Cisco CallManager Locks the B-Channel and Sends Restart](#).

When the Cisco CallManager system receives a Release Complete with cause ie=channel not available, the system sends out a Restart to bring this channel back to the idle state.

Probable Cause

In the Restart, you specify with the Channel IE which channel(s) must be restarted. If the network responds with Restart_Ack without the Channel IE, the system keeps this channel in a locked state. While on network side, this same channel goes back to idle state.

Now you end up with the network requesting this channel for inbound calls.

Because the channel is locked on the Cisco CallManager server, the Cisco CallManager releases any call requests for this channel.

This behavior occurs on numerous sites in the UK and when the gateway is an E1 blade (most likely the same happens when using MGCP backhaul on the 2600/3600).

A glare condition provides the likely reason for the Release Complete.

You see this frequent happening on sites where a high call volume occurs.

If the B-channel selection on the network is top-down or bottom up, all inbound calls will fail until a B-channel in the higher/lower range is freed (if an active call gets cleared).

When B-channel selection is round-robin over a certain time, you will end up with an E1 blade with all locked B-channels.

Corrective Action

Reset the E1 port.

Verification

The B-channel(s) return to the idle state.