Device Issues

This section addresses common problems that you may experience with Cisco Unified IP Phones, gateways, and related devices.

Voice Quality

You may experience voice-quality issues including lost or distorted audio signal during phone calls. This section covers some common voice-quality problems.

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.

- Gateways
- Phones
- Networks

Related Topics

Lost or Distorted Audio, on page 2
Correcting Audio Problems From the Cisco Unified IP Phone, on page 3
Echo, on page 4
One-Way Audio or No Audio, on page 5

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 time that it takes for a packet to get from point A to point B but is simply the variation in packet arrival times.

Possible 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 reaches its destination and is ready to be put into a conventional audio stream.

The Cisco Unified IP Phone model 7960 can buffer as much as 1 second of voice samples. Because the jitter buffer is adaptive, if a burst of packets is received, the Cisco Unified IP Phone model 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).

Some video endpoints may not support G.728, and using G.728 may result in noise. Use another codec, such as G.729.

Recommended Action

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.
2. Next, disable silence suppression (also known as Voice Activation Detection or VAD). This mechanism does save bandwidth by not transmitting any audio when silence occurs, but may cause noticeable or unacceptable clipping at the beginning of words.

   Disable the service in Unified Communications Manager Administration and choose **System** > **Service Parameters**. From there, choose the server and the Cisco CallManager service.
3. Set SilenceSuppression to **False to disable for all devices in a Cisco Communications Manager cluster**; alternatively, you can set SilenceSuppressionForGateways to **False**. When in doubt, turn both off by choosing the value **False** for each.
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 following table, 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 (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. 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 Call Reporting and Billing Administration Guide for Cisco Unified Communications Manager for more information about CDRs.

Correcting Audio Problems From the Cisco Unified IP Phone

Symptom

Audio problems occur while a call is in progress.

Possible 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 that is connected to the LAN and a slow frame-relay interface that is 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 was not 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 faulty cables, interfaces, or by incorrectly configured devices (such as a port speed or duplex mismatch) cause. Make sure that the traffic is not crossing any shared-media device, such as a hub.

Recommended Action

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

- On an active call, you can press the ***i*** or***?*** button twice rapidly and the phone will display an information screen that contains packet that receive and transmit statistics, as well as average and maximum jitter counters.

Note On this window, jitter represents the average of the last five packets that arrived; the maximum jitter designates the maximum for the average jitter.

- Situations could also occur where the traffic is taking a slower path through the network than expected. If QoS is configured correctly, the possibility exists that no call admission control exists. Depending on your topology, you can accomplish this through the use of **Locations** in Cisco Unified Communications Manager Administration configuration or by using a Cisco IOS router as a gatekeeper. In any case, you should always know the maximum calls that are supported across your WAN.
- Crackling represents another poor-quality symptom, which a defective power supply or some kind of strong electrical interference close to the phone sometimes causes. Try swapping the power supply and moving the phone.
- Verify gateway and phone loads. at `www.cisco.com` for the latest software loads, new patches, or release notes that relate to the problem.

After you apply the appropriate fix, verify the sound quality by performing the following procedure:

1. Test by disabling silence suppression; 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.
2. With the maximum number of calls across the WAN, the calls should all have acceptable quality.
3. Test to make sure that a fast busy is returned when you try to make one more call.

Related Topics

Lost or Distorted Audio, on page 2

Echo

Symptom

Echo occurs when the speech energy that is being generated and transmitted down the primary signal path gets coupled into the receive path from the far end. The speaker then receives 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 occurs so lowly. 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.

Possible Cause

Remember that the cause of the echo always lies 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.

Recommended Action

1. Make sure that the problem phones do not use 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

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 gets 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.

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

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 canceller cannot work properly. This issue should not exist for local calls, and long-distance calls should have external echo cancellers built in to the network at the Central Office. This fact provides one reason why you should note the external phone number of a call that experiences echo.

   Checking Your Loads

5. Verify your gateway and phone loads. Check `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 a phone call is established from an IP station through a Cisco IOS voice gateway/router, only one of the parties receives audio (one-way communication).

When a toll-bypass call is established between two Cisco gateways, only one of the parties receives audio (one-way communication).

Possible Cause

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

Recommended Action

Make Sure IP Routing is Enabled on Cisco IOS Gateway/Routers

Some Cisco IOS gateways, such as the VG200, have IP routing disabled by default. This will lead to one-way voice problems.

Note Before going any further, make sure that your router has IP routing enabled (that is, does not have the global configuration command **no ip routing**).

To enable IP routing, enter the following global configuration command in your Cisco IOS gateway:

voice-ios-gwy(config)#ip routing

Check Basic IP Routing

Ensure that basic IP access should always gets checked first. Because RTP streams have no connections (transported over UDP), traffic may travel successfully in one direction but get lost in the opposite direction.

Check the following conditions:

- Default gateways configured at the end stations
- IP routes on the default gateways, mentioned above, leading to the destination networks

Note The following list explains how to verify the default router/gateway configuration on various Cisco Unified IP Phones:

- Cisco Unified IP Phone model 7960/40—Press Settings button, select option 3, scroll down until the Default Router field shows up.

Note For Cisco DT24+ Gateways, check the DHCP Scope and make sure that a Default Gateway (003 router) option exists in the scope. The 003 router parameter populates the Default Gateway field in the devices and PCs. Scope option 3 should have the IP address of the router interface that will be doing routing for the gateway.

Bind the H.323 Signaling to a Specific IP Address on Cisco IOS Gateway/Routers

When the Cisco IOS gateway has multiple active IP interfaces, some of the H.323 signaling may use one IP address for course, and other parts of it may reference a different source addresses. This can generate various kinds of problems, including being one-way audio.

To avoid the problem, the H.323 signaling can be bound to a specific source address, which can belong to a physical or virtual interface (loopback). The command syntax to use under the interface configuration mode follows:

h323-gateway voip bind srcaddr<ip address>. Configure this command under the interface with the IP address to which the Unified Communications Manager points.

Configuring H.323 Support for Virtual Interfaces documents this command, which was introduced in Cisco IOS Release 12.1.2T.

Note A bug exists in version 12.2(6) where this solution can actually cause a one-way audio problem. For more information, refer to bug ID CSCdw69681 (registered customers only) in Cisco Software Bug Toolkit (registered customers only).

Check that Answer Supervision Is Being Sent and Received Correctly from the Telco or Switch

In an implementation that has a Cisco IOS gateway connected to a Telco or switch, verify that answer supervision gets sent correctly when the called device behind the telco or switch answers the call. Failure to receive the answer supervision will cause the Cisco IOS gateway not to cut through (open) the audio path in a forward direction which causes one-way voice. A workaround involves the need to configure **voice rtp send-recv on**.

Cut-through Two-Way Audio Early Using voice rtp send-recv on Cisco IOS Gateway/Routers

The voice path gets established in the backward direction as soon as the RTP stream is started. The forward audio path will not be cut through until the Cisco IOS gateway receives a Connect message from the remote end.

In some cases you need to establish a two-way audio path as soon as the RTP channel is opened—before the connect message is received. To achieve this, use the **voice rtp send-recv** global configuration command.

Check cRTP Settings on a Link-by-Link Basis on Cisco IOS Gateway/Routers

This issue applies to scenarios, such as toll-bypass, where more than one Cisco IOS router/gateway is involved in the voice path and Compressed RTP (cRTP) is used. cRTP, or RTP Header Compression, designates a method for making the VoIP packet headers smaller to regain bandwidth. cRTP takes the 40-byte IP/UDP/RTP header on a VoIP packet and compresses it to 2-4 bytes per packet, yielding approximately 12Kb of bandwidth for a G.729 encoded call with cRTP.

cRTP occurs on a hop-by-hop basis with decompression and recompression on every hop. Because each packet header needs to be examined for routing, enable cRTP on both sides of an IP link.

Also verify that cRTP is working as expected on both ends of the link. Cisco IOS levels vary in terms of switching paths and concurrent cRTP support.

In summary, the history follows:

- Until Cisco IOS Software Release 12.0.5T, cRTP gets process-switched.
- Cisco IOS Software Release 12.0.7T, fast- and Cisco express forwarding (CEF)-switching support for cRTP, which introduced and continue in 12.1.1T.
- In Cisco IOS Software Release 12.1.2T, introduced algorithmic performance improvements.

If you are running cRTP on Cisco IOS platforms (IOS Release 12.1), verify that bug CSCds08210 (registered customers only) (VoIP and FAX not working with RTP header compression ON) does not affect your IOS version.

Verify Minimum Software Level for NAT on Cisco IOS Gateway/Routers

If you are using Network Address Translation (NAT), you must meet the minimum software level requirements. Earlier versions of NAT do not support skinny protocol translation and will lead to one-way voice issues.

The minimum software levels that are required for using NAT and skinny simultaneously specify Cisco IOS® Software 12.1(5)T for IOS gateways to support skinny and H.323v2 with NAT.

Note If your Unified Communications Manager is using a TCP port for skinny signaling that differs from the default 2000, you need to adjust the NAT router with the **ip nat service skinny tcp port<number>** global configuration command.

The minimum software level that is required for using NAT and skinny simultaneously on a PIX firewall specifies 6.0.

Note These levels of software do not necessarily support all the RAS messages necessary for full gatekeeper support. Gatekeeper support occurs outside the scope of this document.

Disable voice-fastpath on AS5350 and AS5400

The Cisco IOS command **voice-fastpath enable** gets a hidden global configuration command for the AS5350 and AS5400, which is enabled by default. To disable it, use the **no voice-fastpath enable** global configuration command.

When enabled, this command caches the IP address and UDP port number information for the logical channel that is opened for a specific call and prevents the RTP stream from getting to the application layer, but rather forwards the packets at a lower layer. This helps marginally reduce CPU utilization in high-call-volume scenarios.

When supplementary services, such as hold or transfer are used, the voice-fastpath command causes the router to stream the audio to the cached IP address and UDP port, disregarding the new logical channel information that was generated after a call on hold was resumed or a transfer was completed. To avoid this problem, traffic should go to the application layer constantly, so redefinition of the logical channel gets taken into account, and audio gets streamed to the new IP address/UDP port pair. That explains why you should disable voice-fastpath to support supplementary services.

Configure the VPN IP Address with SoftPhone

Cisco IP SoftPhone offers the ability to make a PC work like a Cisco Unified IP Phone model 7900 Series phone. Remote users who connect back to their company network through VPN need to configure some additional settings to avoid a one-way voice problem.

The solution requires you to configure the VPN IP address, instead of the IP address of the network adapter under the Network Audio Settings.

Verification

A useful command to verify packet flow specifies **debug cch323 rtp**. This command displays packets that the router transmits (X) and receives (R). An uppercase character indicates successful transmission/reception whereas a lowercase character indicates a dropped packet. See the following example:

```
voice-ios-gwy#debug cch323 rtp
RTP packet tracing is enabled
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#
```

```
!--- This is an unanswered outgoing call.
!--- Notice that voice path only cuts through in forward
!--- direction and that packets are dropped. Indeed,
!--- received packets are traffic from the IP phone to the PSTN
!--- phone. These will be dropped until the call is answered.

Mar 3 23:46:23.690: ****** cut through in FORWARD direction *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXXrrrrrrrrrrrrrrrr
voice-ios-gwy#
voice-ios-gwy#

!--- This is an example of an answered call:

voice-ios-gwy#
voice-ios-gwy#
*Mar 3 23:53:26.570: ****** cut through in FORWARD direction *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XXrrrrrXrXrXrXrXrXrXrXrXrXrXrXrrXXrrXrXrXrXrXrXXXXXXXXXXXXXXXXXrXXXXXXXXrXrXrXXrrXr
XrXrXrXrXrXrXrXrXXrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr

!-- At this point the remote end picks up the phone.

*Mar 3 23:53:30.378: ****** cut through in BOTH direction *****
XRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXR
XXRRXRXRXXRRXRXRXRXRXXRXRXRXRXRXRRXRXXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XXRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXXRRRXR

!-- End of conversation.
```

Codec and Region Mismatches

If a user gets a reorder tone (busy signal) when going off hook, it could occur as 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 The system does not support codec negotiation with a Cisco IOS router.

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 Unified IP Phone model 7960—G.711A-law/mu-law, G.729, G729A, G.729Annex-B
- Cisco Access Gateway DE30 and DT-24+—G.711a-law/mu-law, G.723.1

Location and Bandwidth

If a user receives a reorder tone after dialing a number, this indicates that the cause may be that the Unified Communications Manager bandwidth allocation for the location of one of the call end devices was exceeded. Unified Communications Manager checks for the available bandwidth for each device before making a call. If no bandwidth is available, Unified Communications Managerwill not set up the call, and the user receives a reorder tone.

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

After the call is established, the Unified Communications Manager will subtract bandwidth from the locations, depending on the codec that is used in that call.

- If the call is using G.711, Unified Communications Manager subtracts 80k.
- If the call is using G.723, Unified Communications Manager subtracts 24k.
- If the call is using G.729, Unified Communications Manager subtracts 24k.

Phone Issues

This section addresses phone issues.

Related Topics

Phone Resets, on page 10
Dropped Calls, on page 11
Phones Not Registering, on page 12

Phone Resets

Symptom

Phone resets.

Possible Cause

Phones will power cycle or reset for two reasons:

- TCP failure while connecting to the Unified Communications Manager
- Failure to receive an acknowledgment to the phone KeepAlive messages.

Recommended Action

1. Check the phones and gateways to ensure that you are using the latest software loads.
2. Check `www.cisco.com` for the latest software loads, new patches, or release notes that may relate to the problem.
3. Check the Syslog Viewer in the Cisco Unified Real-Time Monitoring Tool for instances of phone(s) resetting. Phone resets represent Information events.
4. Look for any errors that may have occurred around the time that the phone(s) reset.
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

   Whether the resets occur during a call or happen intermittently

   Whether any similarities of phone model exist
6. Start a Sniffer trace on a phone that frequently resets. After the phone has reset, look at the trace to determine whether any TCP retries are 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 that DHCP lease expiration occurs every seven days (this value is user-configurable; for example, it could be every 2 minutes).

Dropped Calls

Symptom

Premature termination of dropped calls.

Possible Cause

Premature termination of dropped calls can result from a phone or gateway resetting or a circuit problem, such as incorrect PRI configuration.

Recommended Action

1. Determine whether this problem is isolated to one phone or to a group of phones. Perhaps you will find that the affected phones all exist on a particular subnet or location.
2. Check the Syslog Viewer in the *Cisco Unified Real-Time Monitoring Tool* (RTMT) 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 Unified Communications Manager alive, so the Unified

Communications Manager 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 Performance Monitoring in RTMT.

3. If the problem seems to be occurring only through a certain gateway, 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 *CDR Analysis and Reporting Administration Guide* for detailed information on CDRs.
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/en/US/tech/tk801/tk379/technologies_tech_note09186a008012e95f.shtml
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 Unified Communications Manager. Because the trace tool can affect Unified Communications Manager performance, you will want to use this option only as a last resort or if your network is not yet in production.

Related Topics

Phone Resets, on page 10

Phones Not Registering

Symptom

Cannot register more than 5000 phones.

Possible Cause

The Maximum Number of Registered Devices service parameter specifies the default value.

Recommended Action

Change the value of the Maximum Number of Registered Devices service parameter on each node to the appropriate value.

Gateway Issues

This section addresses gateway issues.

Related Topics

Gateway Reorder Tone, on page 12
Gateway Registration Failure, on page 13

Gateway Reorder Tone

Symptom

Reorder tone occurs.

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

Recommended Action

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

1. Check the gateways to ensure that you are using the latest software loads.
2. Check `www.cisco.com` for the latest software loads, new patches, or release notes relating to the problem.
3. Start an SDI trace and re-create the problem. Reorder tones result from a configuration issue with location-based admission control or gatekeeper-based admission control where the Unified Communications Manager might limit the number of allowable calls. In the SDI trace, locate the call to determine whether it was blocked intentionally by a route pattern or the calling search space or by any other configuration setting.
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 standalone units that do not directly connect to a Network Management Processor (NMP). The second category includes the Analog Access WS-X6624 and Digital Access WS-X6608. These gateways, as blades that are 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 is encountered with gateways on a Unified Communications Manager.

Possible Cause

Registration can fail for a variety of reasons.

Recommended Action

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, this indicates that the gateway software is not running. Normally, this results in an automatic reset of the gateway. Also, consider it as 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 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 displays 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 eight 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.

2. Check that the gateway received its IP address. A standalone gateway must receive its IP address using DHCP or BOOTP. A Catalyst gateway may receive its IP address by DHCP, BOOTP or by manual configuration through the NMP.

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 a definitive indication. Delete the lease at the DHCP server.

4. Reset the gateway.

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?).

6. If performing these checks does not yield the answer, use a sniffer trace to determine the specific problem.

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
```

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.

9. If the gateway is failing to obtain valid DHCP information, use the tracy utility (supplied by Cisco TAC) to determine the problem.

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. Issue the command **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.

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.

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.

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*

14. If you are still seeing the **`DHCPState = INIT`** messages, check whether the DHCP server is functioning correctly.

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.

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.

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 using 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.

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: 0Cmd:    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, bold lines of text make it easier for you to see the messages that are 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: 6Cmd:     show dhcp
```

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

20. After 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 Unified Communications Manager:

```
00:09:05.620 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP
Server00:09:18.620 (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 Unified Communications Manager.

21. If the card is not getting its TFTP information correctly, check the TFTP service on the Unified Communications Managerand make sure it is running.

22. Check the TFTP trace on the Unified Communications Manager.

Another common problem occurs if the gateway is not configured correctly on the Unified Communications Manager. 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
asynchronously2000 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 CiscoCM1
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 CM 10.123.9.2
00:00:05.610 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupUnified CM
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 CM 10.123.9.2
00:00:20.600 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
```

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 =
SentRegister00:00:08.010 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 display.

```
ELVIS>> 00:00:00.020 (XA) MAC Addr : 00-10-7B-00-13-DE00:00:00.050 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 CM 10.123.9.2
00:00:05.730 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
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 = BadUnified CM
00:01:36.300 GMSG: GWEvent = DISCONNECT --> GWState = Rollover
00:01:46.870 GMSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPSocket
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 CM 10.123.9.2
00:01:51.300 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
00:01:51.300 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:01:51.300 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:01:51.890 GMSG: Unified CM#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 Unified Communications Manager Administration.

Gatekeeper Issues

Before starting any gatekeeper troubleshooting, verify that IP connectivity exists within the network. Assuming that IP connectivity exists, proceed to troubleshoot your gatekeeper calls.

Related Topics

Admission Rejects, on page 18
Registration Rejects, on page 19

Admission Rejects

Symptom

The system issues Admission Rejects (ARJ) when Unified Communications Manager has registered with the gatekeeper but cannot send a phone call.

Possible Cause

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

Recommended Action

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

5. Verify the bandwidth configuration.

Registration Rejects

Symptom

The system issues Registration Rejects (RRJ) when Unified Communications Manager cannot register with the gatekeeper.

Possible Cause

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

Recommended Action

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

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

Symptom

When the Unified Communications Manager 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.

Possible 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 Unified Communications Manager server, the Unified Communications Manager 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 MGCP backhaul on the 2600/3600) is used.

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

You see this happening frequently 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.

Recommended Action

Reset the E1 port.

Verification

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

Incorrect Device Registration Status Displays

Symptom

Incorrect device registration status displays in the device windows in Unified Communications Manager Administration.

Possible Cause

Cisco RIS Data Collector service provides the current device registration status to Unified Communications Manager Administration windows. If the status does not display, one of the following causes may exist:

The Cisco RIS Data Collector service is not running or not responding.

Network connectivity issues or DNS name resolution issues exist, so Unified Communications Manager Administration cannot establish communication with the Cisco RIS Data Collector service.

Recommended Action

1. Using Cisco Unified Serviceability, make sure that the Cisco RIS Data Collector service is running. If the service is running, restart the service. For information on checking service status and restarting services, refer to the *Cisco Unified Serviceability Administration Guide*.
2. Ensure that:
   - The DNS server is properly configured and available
   - The hosts file has proper mapping for Unified Communications Manager servers
   - No DNS resolution issues exist for Unified Communications Manager servers in the cluster
   - You add local server name to the hosts file and perform ipconfig /flushdns, ipconfig /registerdns, iisrest.

Note To verify DNS resolution, make sure that the nslookup tool can resolve the hostnames of servers in the cluster.