



Operate

Introduction to Operating the System

To ensure that your network operates efficiently and reliably, your daily operations should consist of system and performance management practices. These practices include scheduled routine maintenance; keeping maintenance records; and maintaining up-to-date upgrade, troubleshooting, and recovery strategies.

You can navigate to any topic on this tab by using the tab navigation pane at the left of the content pane. This navigation pane contains the table of contents (TOC) for the active tab.

Before You Begin

User acceptance testing is completed and any problems that surfaced have been resolved. Users have been trained in using the new system.

Output of This Process

The Operate phase produces data that will inform the Optimize phase.

Major Tasks in This Process

- [Managing Your System](#)
- [Using Network Monitoring Tools](#)
- [Call Load Testing](#)
- [Troubleshooting Daily Operations](#)

Managing Your System

This topic provides a high-level summary of the ongoing tasks required for managing your system and the options for how these tasks can be performed. For detailed maintenance and operation guides for each component in your Cisco Unified Communications system, see the product documentation listed in [Component Resources](#) in the Resource Library.

System Management Tasks

Managing a Cisco Unified Communications system consists of performing the following activities:

- Integrating monitoring and management tools—Select, order, configure, integrate, and test a set of tools for monitoring and managing the Cisco Unified Communications system.
- Monitoring—Set thresholds, monitor events, and generate notifications when service-impacting events occur.
- Ticketing—Generate and track system trouble tickets for each event.
- Diagnosing incidents—Analyze and troubleshoot incidents to determine the cause.
- Resolving incidents—Define and execute an action plan which can include performing break and fix activities, applying software updates and patches, managing hardware replacements, and executing change management processes.
- Managing changes in the network—Define a change management process for performing moves, adds, changes, and disconnects (MACDs) for your Cisco Unified Communications system including network devices, phones/endpoints, software upgrades, voice- mail boxes, dial plan updates, security patches, OS applications, and voice applications.
- Archiving configurations—Back up device configurations daily and restore device configurations when necessary.
- Managing voice as a network service—Track, measure and resolve quality of service (QoS) issues such as jitter, delay, and dropped packets, and monitor service level agreements (SLAs) with service providers.
- Managing security posture—Detect, analyze, and address security events.
- Reporting—Define, develop, and generate performance, availability, event, and inventory reports.

System Management Options

There are two options for managing a Cisco Unified Communications system:

- Do It Yourself—In this model, you are responsible for managing the entire Cisco Unified Communications system. This approach requires developing business processes; integrating, provisioning and maintaining network management tools; and developing data and voice management skills and knowledge. Cisco offers the Cisco Unified Operations Manager tool as a means for monitoring the network; see [Using Network Monitoring Tools](#) for more information.
- Outtasking Hybrid Model—Using the [Cisco Lifecycle Services](#) approach, Cisco and its partners provide a broad portfolio of end-to-end services and support that can help increase your Cisco Unified Communications system's business value and return on investment. This approach includes two services that provide different levels of management:
 - [Cisco Unified Communications Select Operate Service](#) combines Cisco award-winning maintenance support with basic voice applications monitoring and reporting.
 - [Cisco Unified Communications Remote Management Service](#) includes monitoring and reporting plus managing day-to-day system issues such logical moves, adds, changes, and disconnects; resolving incidents; performing configuration backups; and reporting.

For more information about the Cisco Unified Communications Select Operate Service, Cisco Unified Communications Remote Management Service or other Cisco Unified Communications services, see <http://www.cisco.com/go/ipcservices> or contact your Cisco service account manager.

Using Network Monitoring Tools

The Cisco Unified Operations Manager provides a consolidated view of the entire Cisco Unified Communications infrastructure and presents the current operational status of each element in the network. It continuously monitors the current operational status of elements such as Cisco Unified CallManager, Cisco Unified CallManager Express, Cisco Unity, Cisco Unity Express and Cisco Unified Contact Center Enterprise, as well as Cisco gateways, routers, and IP phones. The Cisco Unified Operations Manager also provides diagnostic capabilities for faster trouble isolation and resolution.

On a day-to-day basis, operations personnel and network administrators are likely to use the following network monitoring tools:

- [Cisco Unified Operations Manager Monitoring Dashboards](#) to monitor devices throughout the overall IP telephony network deployment.
- [Cisco Unified Operations Manager Diagnostics](#) to solve IP phone and connectivity problems.

Cisco Unified Operations Manager also offers additional functions for tracking adds, moves, and changes of IP phones, graphing performance data and generating a variety of reports. For complete information on employing the Cisco Unified Operations Manager to monitor your IP telephony network deployment, see the [Cisco Unified Operations Manager documentation](#).

Cisco Unified Operations Manager Monitoring Dashboards

The Cisco Unified Operations Manager provides four dashboard displays:

- [Service Level View](#)
- [Alerts and Events Display](#)
- [Service Quality Alerts Display](#)
- [IP Phone Status](#)

The displays are described in detail in the [User Guide for Cisco Unified Operations Manager](#).

Service Level View

The Service Level View displays a logical topology of your IP telephony implementation. This logical view focuses on call control relationships between devices and shows all Cisco Unified CallManager clusters, Cisco Unified CallManager Express servers, associated gateways, gatekeepers, application servers, and Survivable Remote Site Telephony (SRST) enabled devices, as well as each device's registration status with a Cisco Unified CallManager. The Service Level View provides much of the same network information described in [Network Topology Diagrams](#), without requiring you to create and maintain separate diagrams and spreadsheets of IP addresses.

The Service Level View is designed so that you can set it up and leave it running, providing an ongoing monitoring tool that signals you when something needs attention. When a fault occurs in your network, the Cisco Unified Operations Manager generates one or more events that are rolled up into an alert. If the alert occurs on a particular device, it is shown on the Service Level View for that device. A complete listing of all events and alerts collected by the Cisco Unified Operations Manager is available in the Alerts and Events display.

For more detailed information on the Service Level View, see [Using the Service Level View](#) in the *User Guide for Cisco Unified Operations Manager*.

Alerts and Events Display

The Alerts and Events display provides a consolidated real-time view of the operational status of your IP telephony environment and IP fabric. When a fault occurs in your network, the Cisco Unified Operations Manager generates an event (or events). Events are rolled up into alerts, one alert for each device with a fault. When an alert occurs on an element in your active view (a logical group of devices), it appears on your Alerts and Events display. You can customize your view to include only those device groups that are important to you (for example, devices residing at sites that you are responsible for maintaining).

From the Alerts and Events display you can also:

- Drill down into an alert to see what events caused the alert and add alert annotations for other users to read.
- Drill down into specific events for MIB attribute values.
- Open a Detailed Device View to examine device components and suspend or resume monitoring of them.

For more detailed information on the Alerts and Events display, see [Using the Alerts and Events Display](#) in the *User Guide for Cisco Unified Operations Manager*.

Service Quality Alerts Display

The Service Quality Alerts display provides real-time information about IP phone service quality, such as Mean Opinion Scores (MOSs) associated with poor voice quality between pairs of endpoints (Cisco IP phones, Cisco Unity messaging systems, or voice gateways) involved in a call and other associated details about the voice-quality problem.



Note

The Service Quality Alerts displays alerts that the Cisco Unified Operations Manager generates based on Simple Network Management Protocol (SNMP) traps sent by Cisco Unified Service Monitor. To use the Service Quality Alerts display, you must have a licensed copy of Cisco Unified Service Monitor configured to send traps to Cisco Unified Operations Manager. You must also add Cisco Unified Service Monitor to Cisco Unified Operations Manager. For more information on the Cisco Unified Service Monitor, see the [Cisco Unified Service Monitor documentation](#).

For more detailed information on the Service Quality Alerts display, see [Monitoring Service Quality Alerts](#) in the *User Guide for Cisco Unified Operations Manager*.

IP Phone Status

The IP Phone Status display provides real-time information about the operational status of your IP phones, such as when IP phones in your network that have become disconnected from the switch, are no longer registered to a Cisco CallManager, or have gone into SRST mode.

Phone status testing is protocol-independent and can be performed on phones that operate, for example, under the following protocols:

- MGCP
- SCCP
- SIP

For more detailed information on the IP Phone Status display, see [Using the Phone Activities Display](#) in the *User Guide for Cisco Unified Operations Manager*.

Cisco Unified Operations Manager Diagnostics

The Cisco Unified Operations Manager offers the following diagnostic tests to provide performance and connectivity details about different elements of the Cisco Unified Communications infrastructure:

- [Phone Status Tests](#)
- [Synthetic Tests](#)
- [Node-to-Node Tests](#)

Phone Status Tests

Phone status tests use Cisco IOS IP Service Level Agreement (IP SLA) technology to monitor the status of key phones in the network. You can define tests for selected IP phones that are executed based on a reoccurring testing schedule. These tests send IP SLA-based pings from an IP SLA-capable device (for example, a switch, a router, or a voice router) to the selected IP phones or, optionally, pings from Cisco Unified Operations Manager to the IP phones.

For more detailed information on using phone status tests, see [Using Phone Status Testing](#) in the *User Guide for Cisco Unified Operations Manager*.

Synthetic Tests

Synthetic tests are used to measure the availability of voice applications by simulating end-user activity. Synthetic tests verify whether voice applications can service requests from a user, such as whether phones can register with a Cisco Unified CallManager. Synthetic tests use synthetic phones to measure the availability of voice applications by emulating user actions. For example, a synthetic test places a call between clusters and then checks to see if the call is successful. Synthetic tests are available for the following Cisco Unified Communications elements:

- Cisco Unified CallManager and Cisco Unified CallManager Express
- Cisco TFTP Server
- Cisco Unified Emergency Responder
- Cisco Conference Connection
- Cisco Unity and Cisco Unity Express

For more detailed information on using synthetic tests, see [Using Synthetic Tests](#) in the *User Guide for Cisco Unified Operations Manager*.

Node-to-Node Tests

Node-to-node tests monitor the response time and availability of multiprotocol networks on both an end-to-end and a hop-by-hop basis. After collecting this data you can use the Cisco Unified Operations Manager graphing function to examine changes in network performance metrics. You can select, display, and chart network performance data in real time. These tests also enable you to perform a probable path trace between two endpoints and the report on any outages or problems on intermediate nodes in the path.

For more detailed information on using node-to-node tests, see [Using Node-to-Node Tests](#) in the *User Guide for Cisco Unified Operations Manager*.

Call Load Testing

Call load testing captures the results of busy hour call attempts (BHCA) tests. BHCA tests measure the volume of calls generated and handled, regardless of whether the calls are answered. The BHCA data is used in capacity calculations. Review the [Call Load Testing](#) chapter in the *System Test Architecture Reference Manual for IP Telephony: Cisco Unified Communications Release 5.0(2)* for an overview of the call loads that were tested with these site models:

- Very Large Campus with Clustering over the WAN
- Large SIP Site
- Small Campus SIP Site
- Small Campus H.323 Site
- Cisco Unified CallManager Interoperability Site (NA)

See also [Develop Traffic Engineering Specifications](#) on the Design tab for more information on capacity calculations.

Troubleshooting Daily Operations

This topic describes how to diagnose and resolve system-level problems that occur during daily operations of a Cisco Unified Communications network. It contains the following sections:

- [Common Problems Reported by Users](#)
- [Problems Caused by Password Changes](#)
- [PBX Interoperability Issues with Cisco Unified CallManager](#)
- [Using Call Flows to Resolve Call Processing Problems](#)
- [Failover and Recovery Procedures](#)

Common Problems Reported by Users

This section describes basic approaches to diagnose and resolve common problems reported by end users in an IP telephony environment. Note that this section demonstrates various tools and diagnostic approaches available in the context of specific problems, but does not provide a comprehensive list of all possible problems that may occur. Problems described in this section include:


- [One-Way Audio](#)
- [Call Indication Without a Connection](#)
- [Poor Voice Quality](#)

One-Way Audio

One-way audio and no audio at all (no-way audio) are problems that are fairly common during a new IP telephony network installation. The majority of these problems are caused by misconfigurations. For one-way audio problems, always pay attention the direction in which the one-way audio is occurring. For no audio in either direction, the troubleshooting methodology is the same. You might need to repeat

the procedure for each direction of audio, but more likely you will find the source of the problem when trying to troubleshoot one direction. There are several steps you can take to troubleshoot a one-way/no-way audio problem:

1. [Verify Bidirectional IP Connectivity](#).
2. [Check Cisco IOS Software Gateway Configurations](#).
3. [Check for NAT or Firewall Restrictions](#).

For additional directions on troubleshooting one-way audio problems, refer to the [Troubleshooting One-Way Voice Issues Tech Note](#) .

Verify Bidirectional IP Connectivity

You should verify IP connectivity as the first step in troubleshooting a one-way or no-way audio problem because IP connectivity must be present for voice packets to be exchanged between two devices. A large number of one-way or no-way audio problems are caused by lack of IP connectivity. Check that:

- If the two endpoints involved in the call are on different IP subnets, each endpoint has the correct default gateway and subnet mask settings
- If one of the endpoints is a Unified IP phone, the DHCP scope has an incorrectly configured default gateway parameter.
- If one of the endpoints is a Cisco IOS software gateway, the default route is correct. Also, ping the other endpoint from the gateway. If the ping is successful, you know that you have IP connectivity. If the ping is unsuccessful, perform a **tracert** to determine where the problem lies.



Note

Remember that signaling packet traffic is always between Unified CallManager and the endpoint, whereas the RTP voice packet traffic is directly between the endpoints. So just because the endpoints are registered to Unified CallManager and can set up a call through Unified CallManager does not mean that the endpoints have proper IP connectivity between them.

Another useful tool for troubleshooting such a problem is the help (**i** or **?**) button on Cisco Unified IP phones. Press the help (**i** or **?**) button twice in quick succession during an active call. The display shows you receive and transmit statistics for the call. If you do not see the receive counter (RxCnt) incrementing, the packets are probably not arriving on that IP phone. If you go to the originating IP phone and the transmit count (TxCnt) is incrementing, the packets are probably being lost somewhere in the network. If a ping or traceroute does not provide enough information about where the packets are being lost, you may need to connect a sniffer to the network and perform the following steps:

1. Connect the sniffer to the back of the originating IP phone and make verify that the phone is actually transmitting packets.
2. On the originating phone, verify that the IP address and MAC address information is correct.
3. If the network settings on the originating phone are correct, go to the terminating IP phone to verify that the packets are not arriving.
4. If the voice packets are not arriving at the terminating phone, move the sniffer from network hop to network hop to isolate where the packets are being dropped. A common reason for a problem such as this is a missing or improperly configured IP route.

Check Cisco IOS Software Gateway Configurations

There are various reasons why you might encounter one-way audio on calls to a Cisco IOS software gateway. Most of these problems can be solved using simple configuration commands.

1. Check if IP routing is enabled on the gateway that you are using—You do not need to be running a routing protocol such as RIP, EIGRP, or OSPF, but IP routing must not be disabled. Make sure that the **no ip routing** command is not in your configuration. If it is, be sure to eliminate it by configuring the **ip routing** command. You can also issue the **show ip route** command to see if IP routing is enabled. If IP routing is disabled, there are no routes listed in the output, and the list of routing protocols is not present.
2. Determine if the VoIP subsystem is enabled—The VoIP subsystem in Cisco IOS software uses the IP routing code to aid in encapsulating and transmitting the VoIP packets, so the subsystem must be enabled to transmit and receive VoIP packets. It does not need the IP routing code to perform signaling such as H.323 or MGCP, so the signaling still works with IP routing disabled.
3. Check IP address configurations on gateway interfaces—Another common occurrence of one-way audio appears on Cisco IOS software H.323 voice gateways that have more than one data interface, such as a gateway that has both an Ethernet connection to the LAN and a serial connection to the WAN. When an H.323 gateway is configured in Cisco Unified CallManager Administration, you configure a specific IP address. Cisco Unified CallManager always uses this IP address for all its signaling to the gateway; however, Cisco IOS software voice gateways by default use the IP address of the interface that is closest to the destination. This could be a problem if Unified CallManager is connected via one interface and the device to which the RTP audio stream is destined for is connected to a different interface. To force the voice gateway to always use the same IP address, configure the **h323-gateway voip bind srcaddr ip-address** command on the interface that you are using for signaling on the Cisco IOS software voice gateway. Make sure this is the same IP address configured in Cisco Unified CallManager Administration. Failure to do so could result in one-way audio when the gateway tries to use a different source interface than the one configured in Unified CallManager.
4. Configure voice rtp send-recv on the gateway—Sometimes you have one-way audio problems only when calling specific numbers, such as 411 or 911 in the North American numbering plan (NANP) or after you transfer a call or put it on hold. If you are having these problems when going through a Cisco IOS software voice gateway, be sure that the **voice rtp send-recv** command is configured on the gateway. Numbers such as 411 and 911 sometimes do not send back answer supervision (that is, an ISDN connect message) when the remote end answers. As a result, the Cisco IOS software voice gateway does not cut through audio in both directions to prevent toll fraud. Configuring the **voice rtp send-recv** command forces the voice gateway to cut through audio in both directions immediately.
5. If you are using a Cisco AS5350 or AS5400 as a gateway, configure the **no voice-fastpath enable** command in global configuration mode—When enabled, this command causes the voice gateway to cache the IP address and UDP port number information for the logical channel opened for a specific call and forwards the packets using the cached information. This helps marginally reduce CPU utilization in high-call-volume scenarios. Because of how Cisco Unified CallManager opens and closes logical channels to redirect RTP audio streams, such as in the case of a transfer or music on hold (MOH) server, the Cisco AS5350 and AS5400 cache the IP address information of the old IP address. Therefore, you end up with one-way audio when the call gets redirected to a new IP address because the voice gateway still uses the cached information instead of the newly negotiated information.

Check for NAT or Firewall Restrictions

One common cause of one-way or no-way audio is when Network Address Translation (NAT), Port Address Translation (PAT), or firewalls exist between two endpoints. The SCCP protocol embeds IP addresses in the IP packet's payload to signal which IP address to send RTP packets to. If the device performing NAT or PAT is unaware of this fact, the embedded IP addresses are not translated. Therefore, one-way or no-way audio results.

Firewalls can also be a problem if they are unaware of the voice traffic passing through them. Firewalls often are configured to block all UDP traffic going through them. Because voice traffic is carried over UDP, it might be blocked while the signaling carried over TCP is passed. A sniffer is the best tool for debugging such a scenario. If both devices appear to be transmitting audio but the audio is not reaching the opposite side, take a sniffer trace at each hop along the way until you find the hop where the audio is not passing through. If the firewall is blocking UDP packets, you might need to open a hole in it to allow the voice traffic to pass through.

Problems Occurring After the Call Connects Successfully

The scenarios discussed so far are cases in which you have one-way audio or no-way audio from the beginning of the call or after a hold/transfer. Occasionally, however, you might encounter scenarios in which a call is up and suddenly becomes one-way or audio disappears entirely. Network problems are largely to blame for failures of this sort. Ensure that network connectivity between the two endpoints still exists and that nothing on the network might be causing intermittent network connectivity. An example would be a *flapping* network connection—a network connection that is transitioning between up and down states over and over again—or a routing protocol that cannot converge correctly. Again, a sniffer is the best tool for diagnosing this kind of problem. The best place to start is on the device that originates the RTP stream to ensure that the stream is still being generated when the loss of audio occurs. If you discover that the originating device stops sending packets for no reason, you might be dealing with a software or hardware problem on the originating device.

A common cause of such a failure is a Digital Signal Processor (DSP) crash. If the end device is a Cisco IOS software voice gateway, you see an error displayed on the console that looks similar to the following:

```
%VTSP-3-DSP_TIMEOUT: DSP timeout on event 6: DSP ID=0x2312: DSP error stats
```

This message is also sent to a Syslog server if the Cisco IOS software voice gateway is configured to send Syslog information to a Syslog server. On a Cisco VG200, 2600, or 3600, you can issue the following command to check the status of the DSPs:

```
test dsprm slot #
```

The **show voice dsp** command displays which port and time slot are allocated to each DSP. If the **test dsprm slot #** command detects a DSP that has crashed, you can compare this with the information obtained from a **show call active voice** command (or a **show call history voice** command if the call has been disconnected) to see if the time slot of the failed call is the same as the slot of the DSP that is no longer available. Unfortunately, the only way to recover from this condition is to reload the gateway.

Call Indication Without a Connection



Note

The information in this section will be available in a future release.

Poor Voice Quality

Nearly all voice quality problems can be attributed to some kind of degradation on the IP network that the voice traffic traverses. Network problems that might not be noticeable for normal data traffic are very apparent in a voice conversation because of the need to minimize packet loss and variable delay in an IP telephony network.

A variety of issues can result in poor voice quality:

- [Packet Drops](#)
- [Queuing Problems](#)

In addition to the information in this section, refer to the [Troubleshooting QoS Choppy Voice Issues](#) document on Cisco.com for additional techniques on resolving voice quality issues.

Packet Drops

IP telephony demands that voice packets reach their destination within a predictable amount of time and without being dropped somewhere along the path from the source to the destination. In a properly designed network with appropriate QoS provisioning in place, packet loss should be near zero. All voice codecs can tolerate some degree of packet loss without dramatically affecting voice quality. Upon detecting a missing packet, the codec decoder on the receiving device makes a best guess as to what the waveform during the missing period of time should have been. Most codecs can tolerate up to five percent random packet loss without noticeable voice quality degradation. This assumes that the five percent of packets being lost are not being lost at the same time, but rather are randomly dropped in groups of one or two packets. Losing multiple simultaneous packets, even as a low percentage of total packets, can cause noticeable voice quality problems.



Note

You should design your network for zero packet loss for packets that are tagged as voice packets. A converged voice/data network should be engineered to ensure that only a specific number of calls are allowed over a limited-bandwidth link. You should guarantee the bandwidth for those calls by giving priority treatment to voice traffic over all other traffic. For more information on prioritizing voice over data, refer to the [Voice Quality](#) information available on Cisco.com.

There are various tools that you can use to determine whether you are experiencing packet loss in your network and where in the network the packets are getting dropped. The starting point to look for lost packets is the call statistics screen on Cisco Unified IP Phones.

1. Do one of the following:
 - If you are troubleshooting at the phone experiencing the problem, access these statistics by pressing the help (i or ?) button on the IP phone twice in quick succession during an active call.
 - If you are working with a remote user, open a web browser on your computer and enter the IP address of the user's phone. During an active call, choose the **Streaming Statistics > Stream 1** options from the display.
2. Examine the counters RxDisc and RxLost shown on the IP phone (or Rcvr Lost Packets if you are viewing the statistics remotely using a web browser).
 - RxLost measures the number of packets that were never received because they were dropped in the network somewhere. By detecting a missing RTP sequence number, the IP phone can determine that a packet has been lost.
 - RxDisc corresponds to packets that were received but were discarded because they could not be used at the time they arrived. RxDisc can come from an out-of-order packet or a packet that arrived too late.

3. If either of these two counters increments, you should investigate to learn why packets are being lost or discarded.

Regardless of how low your packet loss is, if it is not zero, you should investigate the root cause because it might be a sign of a bigger problem that will get worse with higher call volume. Also, although small packet loss might not be perceptible in a conversation between two people, it can be detrimental to fax and modem transmissions. The packet loss can be occurring at any layer of the OSI model, so be sure to check for all possibilities for each hop. For example, if there is a Frame Relay connection over a T1 between two sites, you should:

- Make certain that there are no errors at the physical layer on the T1.
- Determine if you are exceeding your committed information rate (CIR) on the Frame Relay connection.
- Verify that you are not dropping the packets at the IP layer because you are exceeding your buffer sizes.
- Check that you have your QoS improperly configured.
- Ensure that your service provider not only guarantees packet delivery but also guarantees a low-jitter link. Some service providers may tell you that they do not provide a CIR but guarantee that they will not drop any packets. In a voice environment, delay is as important as packet loss. Many service providers' switches can buffer a large amount of data, thereby causing a large amount of jitter.

One common cause of drops in an Ethernet environment is a duplex mismatch, when one side of a connection is set to full duplex and the other side is set to half duplex. To determine if this is the case, perform the following steps:

1. Check all the switch ports through which a given call must travel and ensure that there are no alignment or frame check sequence (FCS) errors. Poor cabling or connectors can also contribute to such errors; however, duplex mismatches are a far more common cause of this kind of problem.
2. Examine each link between the two endpoints that are experiencing packet loss and verify that the speed and duplex settings match on either side.

Although duplex mismatches are responsible for a large number of packet loss problems, there are many other opportunities for packet loss in other places in the network as well. When voice traffic must traverse a WAN, there are several places to look. First, check each interface between the two endpoints, and look for packet loss. On all Cisco IOS software platforms, you can find this information using the **show interface** command. If you are seeing dropped packets on any interface, there is a good chance that you are oversubscribing the link. This could also be indicative of some other traffic that you are not expecting on your network. The best solution in this case is to take a sniffer trace to examine which traffic is congesting the link.

Sniffers are invaluable in troubleshooting voice quality problems. With a sniffer, you can examine each packet in an RTP stream to see if packets are really being lost and where in the network they are being lost. To troubleshoot using a sniffer, perform the following steps:

1. Start at the endpoint that is experiencing the poor-quality audio where you suspect packet loss.
2. Take a sniffer trace of a poor-quality call and filter it so that it shows you only packets from the far end to the endpoint that is hearing the problem. The packets should be equally spaced, and the sequence numbers should be consecutive with no gaps.
3. If you are seeing all the packets in the sniffer trace, continue taking traces after each hop until you get a trace where packets are missing.
4. When you have isolated the point in the network where the packet loss is occurring, look for any counters on that device that might indicate where the packets are being lost.

Queuing Problems

Queuing delay can be a significant contributor to variable delay (*jitter*). When you have too much jitter end-to-end, you encounter voice quality problems. A voice sample that is delayed over the size of the receiving device's jitter buffer is no better than a packet that is dropped in the network because the delay still causes a noticeable break in the audio stream. In fact, high jitter is actually worse than a small amount of packet loss because most codecs can compensate for small amounts of packet loss. The only way to compensate for high jitter is to make the jitter buffer larger, but as the jitter buffer gets larger, the voice stream is delayed longer in the jitter buffer. If the jitter buffer gets large enough such that the end-to-end delay is more than 200 ms, the two parties on the conference feel like the conversation is not interactive and start talking over each other.

Remember that every network device between the two endpoints involved in a call (switches, routers, firewalls, and so on) is a potential source of queuing or buffering delays. The ideal way to troubleshoot a problem in which the symptoms point to delayed or jittered packets is to use a sniffer trace at each network hop to see where the delay or jitter is being introduced.

For more information on jitter, refer to the [Understanding Jitter in Packet Voice Networks](#) document on Cisco.com.

Problems Caused by Password Changes

In general, Cisco Systems strongly recommends that you do not change passwords on Cisco devices once they are set during the initial installation (naturally, you should change the passwords from the factory defaults during the installation process but not after the devices are put into operation). In the event that you decide to change passwords, the following sections describe the rules, restrictions and impact of modifying the following passwords:

- [Passwords Used in Cisco Unified CallManager Configuration](#)
- [Passwords in a Cisco Customer Response Solutions Environment](#)

Passwords Used in Cisco Unified CallManager Configuration

The following passwords are used in Cisco Unified CallManager 5.0 configuration:

- [Platform Administrator Password](#)
- [Security Password](#)
- [Cisco Unified CallManager Administration Passwords](#)

Platform Administrator Password



Note

The information in this section will be available in a future release.

Security Password



Note

The information in this section will be available in a future release.

Cisco Unified CallManager Administration Passwords

**Note**

The information in this section will be available in a future release.

Passwords in a Cisco Customer Response Solutions Environment

This section provides information about passwords in the Cisco Customer Response Solutions 4.0(2) configuration:

- **Customer Response Solutions Server Password**—This is the Windows Administrator's password for the server on which Customer Response Solutions is installed. This password is used during the installation (or upgrade) of Customer Response Solutions and should be the same on all Customer Response Solutions servers in the cluster.
- **Customer Response Solutions Account Password Phrase**—When you install or upgrade Customer Response Solutions, you are prompted to enter an Account Password Phrase. Customer Response Solutions uses the string that you enter to create a unique, encrypted password for the Customer Response Solutions Administrator account and for the services running under this account (CCMServices). This password phrase should be the same on all Customer Response Solutions servers in the cluster. To change this password phrase after installation, use the Customer Response Solutions AdminUtility.
- **Cisco Unified CallManager Password**—The Cisco Unified CallManager password is used during the installation (or upgrade) of Customer Response Solutions and for:
 - **JTAPI Provider**—When configuring a JTAPI Provider, you must specify the Cisco MCS that is running Cisco Unified CallManager CTI Manager and provide the Windows Administrator ID and password for the Cisco Unified CallManager server.

**Note**

If the LDAP setting is Microsoft Active Directory instead of DC, you must manually set this password using Active Directory.

- **JTAPI Client**—When configuring a JTAPI Client, you must specify the Cisco MCS that is running Cisco Unified CallManager and provide the Windows Administrator ID and password for the Cisco Unified CallManager server.
- **Cisco Agent Desktop**—When logging into Cisco Agent Desktop, agents use their Cisco Unified CallManager user ID and password.
- **Unified CallManager Security Password**—The Unified CallManager Security Password set for the Unified CallManager services is used by Customer Response Solutions. If you change the Security Password for Unified CallManager services, you must update the password on the Customer Response Solutions servers using the AdminUtility.

**Note**

If the Cisco Desktop VoIP Monitor Server Service or Cisco Desktop Sync Server Service fails to start and you receive error 1069, you must synchronize the passwords on the Cisco Unified CallManagers and the Cisco Customer Response Solutions Server.

- **LDAP Administrator Password**—Cisco Customer Response Solutions typically requires a single LDAP account with administrator privileges. The LDAP Administrator Password is set during Customer Response Solutions installation. You cannot reset it using the LDAP Server information

web page. You can reset it only using the Customer Response Solutions Serviceability Utility. If you change the LDAP password, be sure to update the password in Customer Response Solutions in Cisco Customer Response Solutions LDAP Information.

PBX Interoperability Issues with Cisco Unified CallManager

If calls to destinations outside the IP network are failing, it may be because the calls must be routed through non-Cisco PBX switches that are connected to the PSTN. In order for the Cisco Unified CallManager to properly direct calls out trunks on the PBX, proper interoperability configuration is required. Information on configuring PBXs to interoperate with Cisco devices is available on an [Interoperability Portal](#) website. This site has information on third-party PBX interoperability with the following Cisco Unified Communications products:

- Cisco Unified CallManager
- Cisco Unity
- Cisco Unified Contact Center Enterprise
- Cisco Unified MeetingPlace

The information is provided in a series of application notes. If you cannot find your exact configuration in the list of available application notes, you may be able to use other application notes to meet your needs. Here are some suggestions:

- PBX product families should have similar results. For example:
 - PBXs in the Nortel Meridian 1 family should have similar results. The Nortel Meridian 1 Option 11C will have similar configurations as the Nortel Meridian 1 Option 61C and the Nortel Meridian 1 Option 81C.
 - PBXs in the Avaya Definity G3 family should be similar. The versions VSI, R, CSI, and SI should have similar configurations.
 - PBXs in the Siemens 300 family also should have similar configuration results. This family includes the 330, 340, and 370.
- Gateways configurations should be similar if the gateways are Cisco IOS based and have the same protocol (for example, MGCP, H.323, or SIP). For example, a Cisco 2801 gateway should have similar configurations to the 3845 when used with the Cisco Unified CallManager.

Using Call Flows to Resolve Call Processing Problems

This topic provides information about a typical call flow in an IP telephony environment. [Figure 5-1](#) shows a call flow that illustrates the actions in a typical call between the following devices at two different sites:

- Cisco Unified IP Phone (SCCP)
- Cisco Unified CallManager
- Gatekeeper

Figure 5-1 Call Flow in an IP Telephony Environment

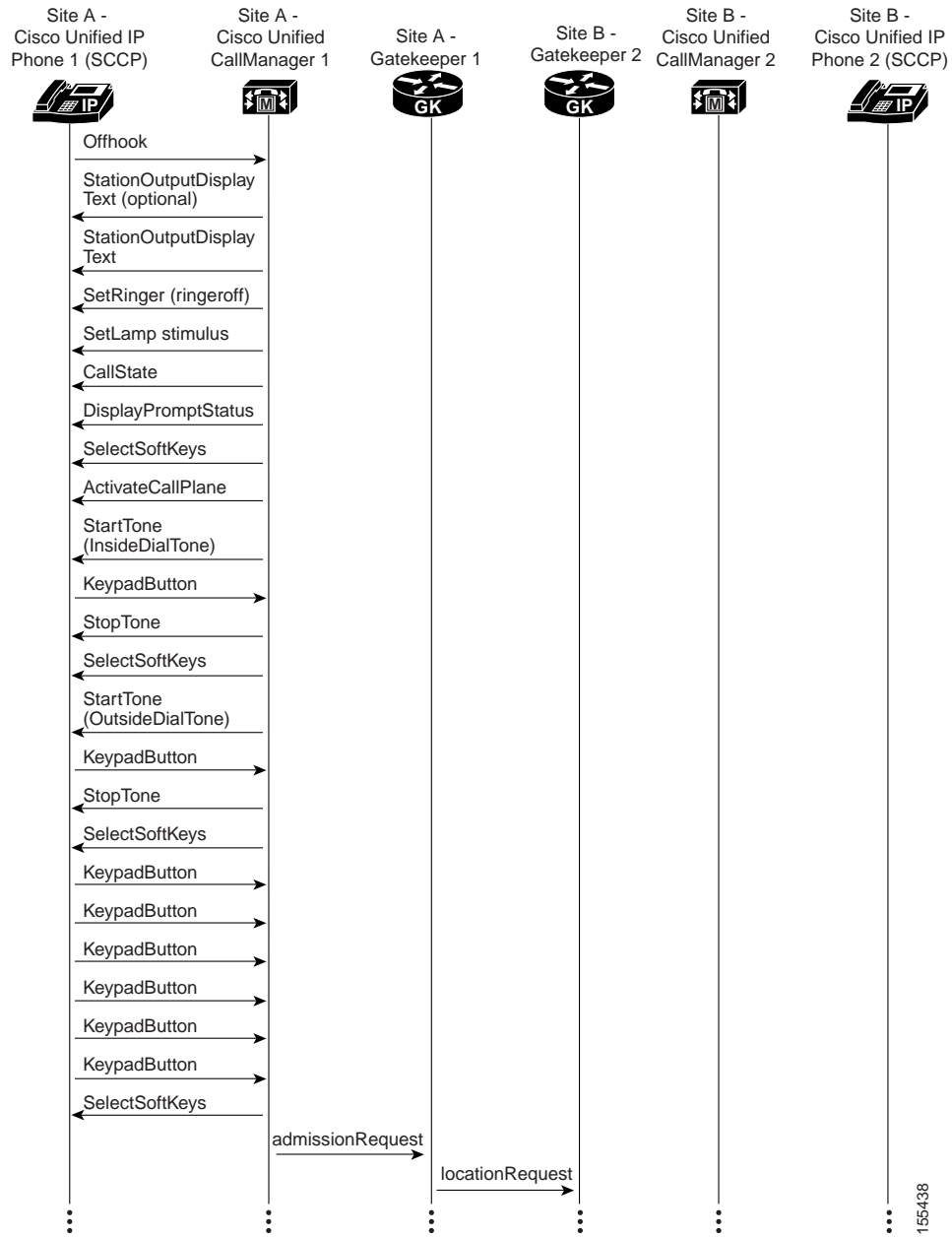
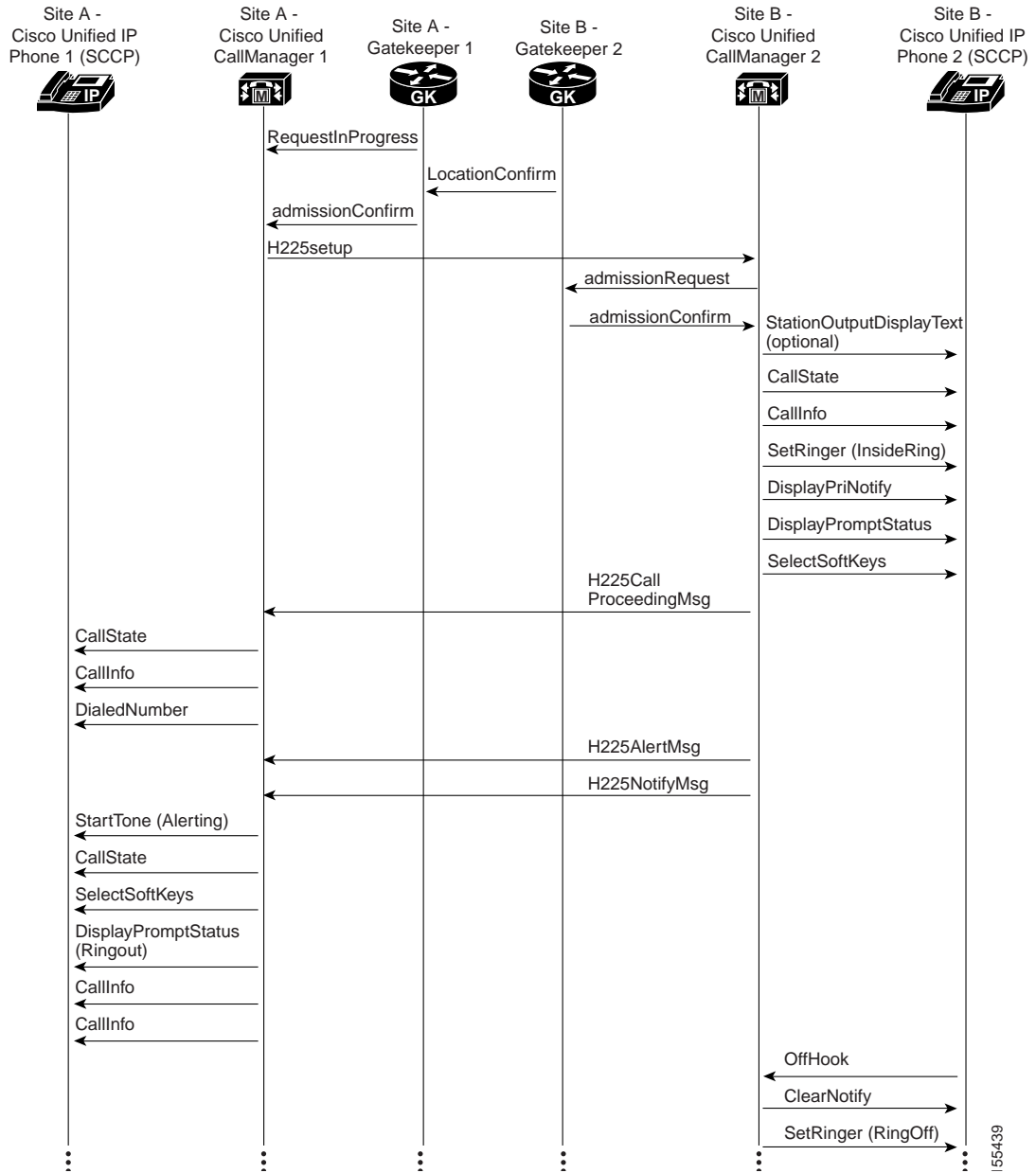
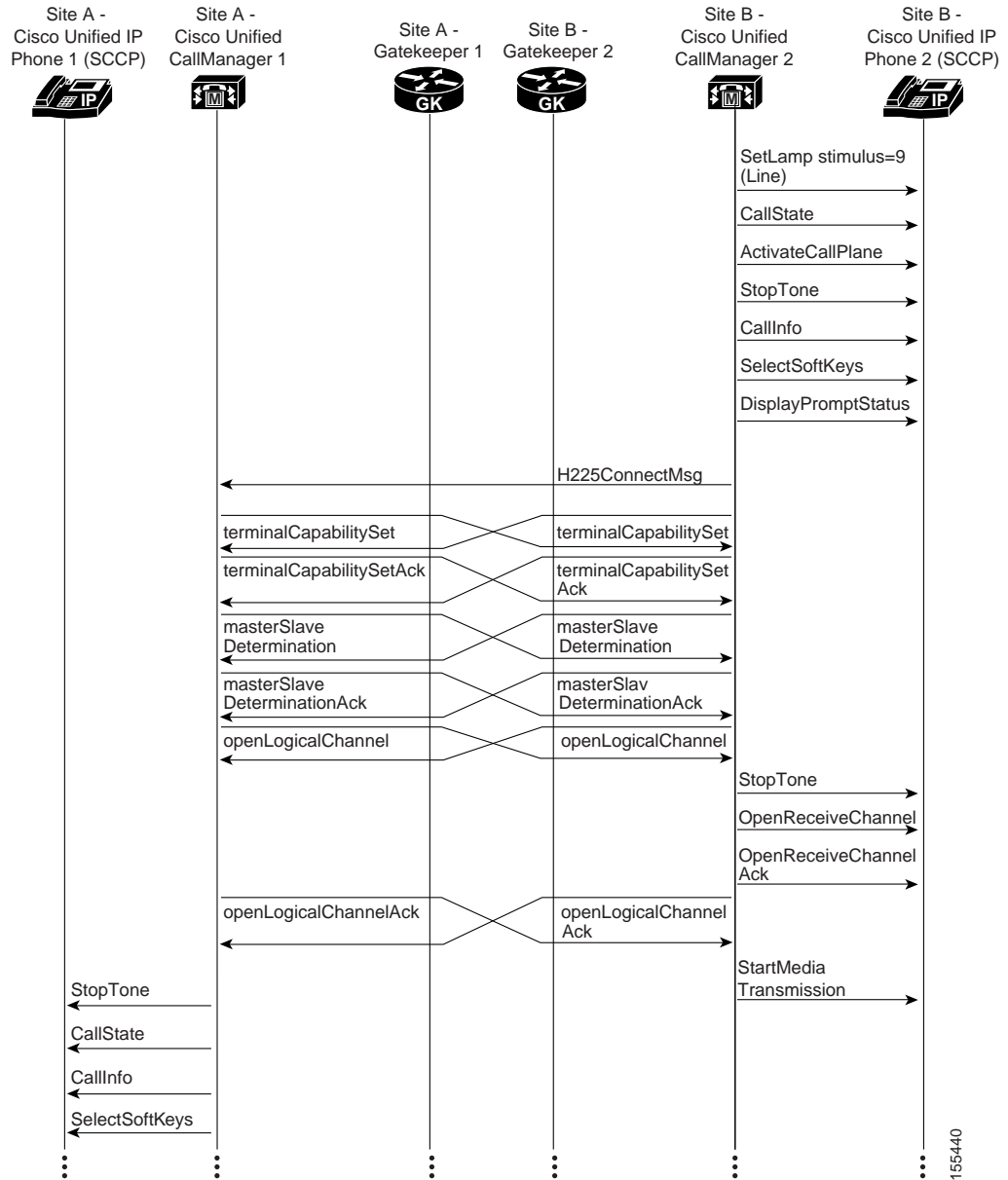


Figure 5-2 Call Flow in an IP Telephony Environment (continued)



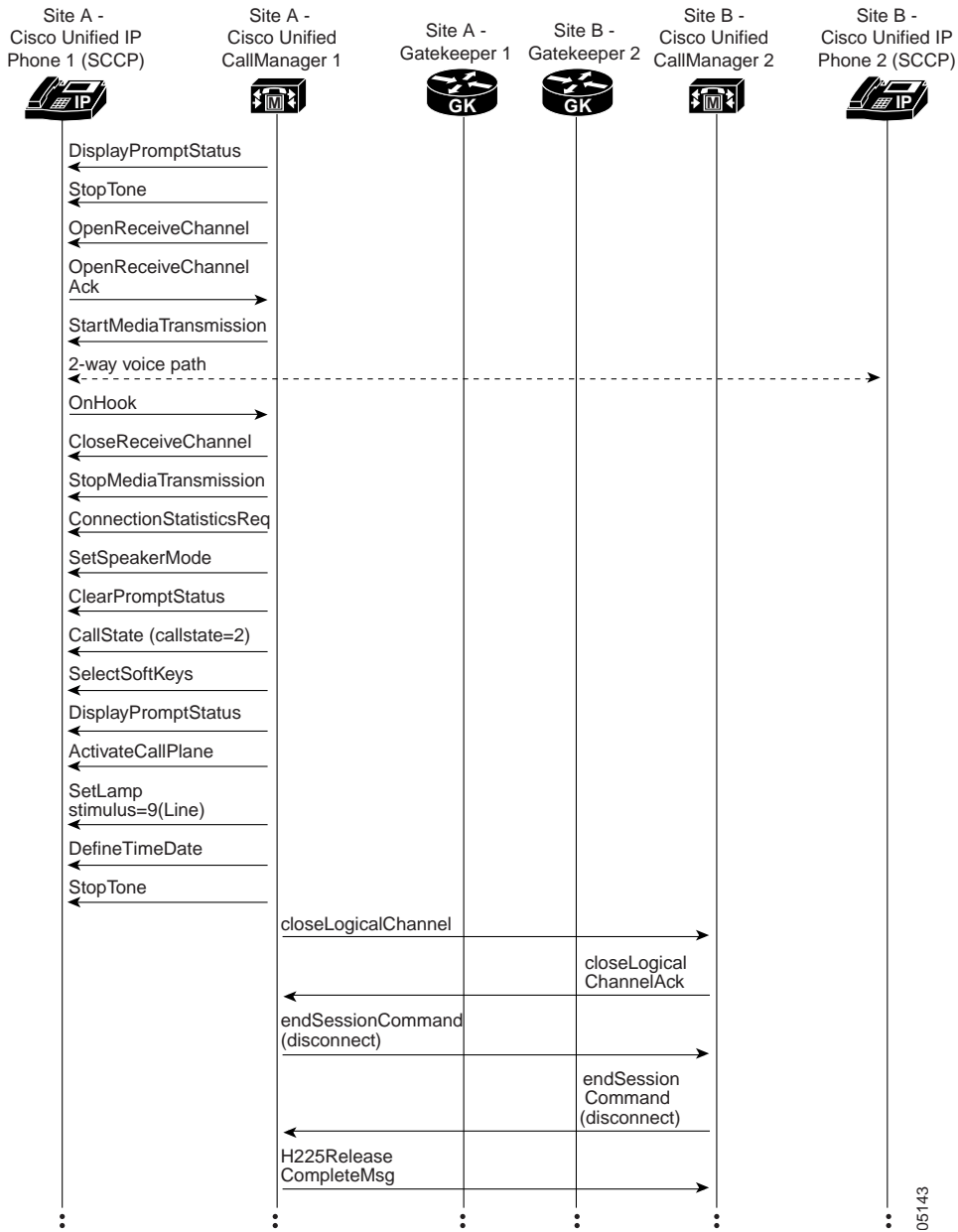
155439

Figure 5-3 Call Flow in an IP Telephony Environment (continued)



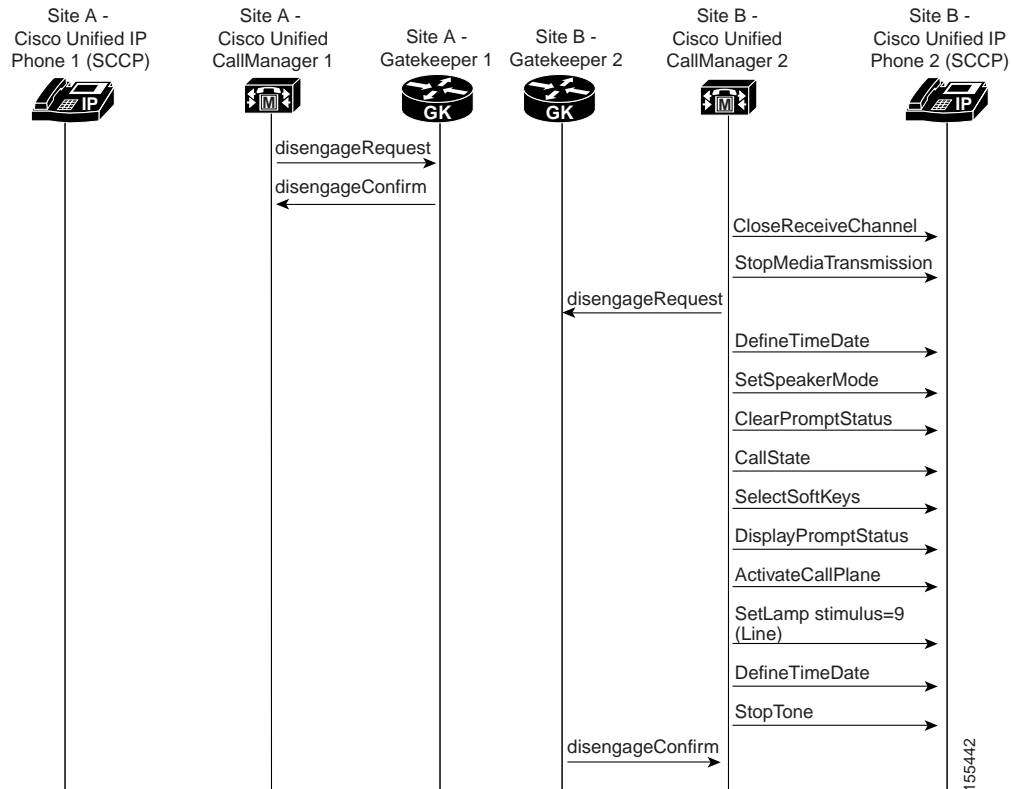
155440

Figure 5-4 Call Flow in an IP Telephony Environment (continued)



05143

Figure 5-5 Call Flow in an IP Telephony Environment (continued)



For both successful and unsuccessful calls, an industry-standard cause code value appears in the disconnect or release signaling messages. The cause code reveals if the call was disconnected normally (typically cause code 16) or abnormally. Table 5-1 lists the standard cause values that may appear in the trace files as part of disconnect processing.

Table 5-1 Disconnect Cause Code Values

Hexadecimal Code with High-Order Bit Set	Hexadecimal Code Without High-Order Bit Set	Decimal Code	Description
0x81	0x01	1	Unallocated (unassigned) number. This cause indicates that the destination requested by the calling user cannot be reached because the number is unassigned. This number is not in the routing table, or it has no path across the ISDN network.
0x82	0x02	2	No route to specified transit network (National use). This number was dialed with a transit network code such as 108880 to go from AT&T and MCI, and there is no route across. The wrong transit network code was dialed.
0x83	0x03	3	No route to the destination. The dialed number is in the routing plan, but there is no physical route to the destination. The most likely cause of this is that the PRI D-channel is down, or the span or WAN is not connected correctly.
0x84	0x04	4	Send special information tone.

Table 5-1 Disconnect Cause Code Values (continued)

Hexadecimal Code with High-Order Bit Set	Hexadecimal Code Without High-Order Bit Set	Decimal Code	Description
0x85	0x05	5	Misdialed trunk prefix (National use).
0x86	0x06	6	Channel unacceptable.
0x87	0x07	7	Call awarded and being delivered in an established channel.
0x88	0x08	8	Preemption.
0x89	0x09	9	Preemption. Circuit reserved for reuse.
0x90	0x10	16	Normal call clearing. This is one of the most common codes and is received for many reasons. It usually occurs because someone hung up the call.
0x91	0x11	17	User busy. The number dialed is busy and cannot receive any more calls.
0x92	0x12	18	No user responding. The number that is being dialed has an active D-channel, but the far end chooses not to answer.
0x93	0x13	19	No answer from the user (user alerted). The number that is being dialed has an active D-channel, but the far end chooses not to answer.
0x94	0x14	20	Subscriber absent.
0x95	0x15	21	Call rejected.
0x96	0x16	22	Number changed. This cause code is generated when a subscriber on the PSTN has changed his or her phone number. Usually this message is accompanied by a progress indicator stating that in-band information is available. The PSTN provides an announcement in-band indicating the new phone number, if available.
0x9A	0x1A	26	Nonselected user clearing.
0x9B	0x1B	27	Destination is out of order. The number dialed is a working number, but the span is not active.
0x9C	0x1C	28	Invalid number format (address incomplete). This can happen when you are calling out using a network type number (enterprise) when you should be calling out Unknown or National.
0x9D	0x1D	29	Facility rejected.
0x9E	0x1E	30	Response to STATUS ENQUIRY.
0x9F	0x1F	31	Normal, unspecified. This is another common code. It happens when the network cannot determine what to do with the call being made.
0xA2	0x22	34	No circuit/channel is available. No B-channels are available to make the selected call.
0xA6	0x26	38	Network is out of order.
0xA7	0x27	39	Permanent frame mode connection is out of service.
0xA8	0x28	40	Permanent frame mode connection is operational.
0xA9	0x29	41	Temporary failure. The call was disconnected due to a network failure. This code appears for some long distance providers if the hunt sequence is incorrect. PRI lines must be set up for a flex hunt sequence (not a float hunt sequence).
0xAA	0x2A	42	Switching equipment congestion.

Table 5-1 Disconnect Cause Code Values (continued)

Hexadecimal Code with High-Order Bit Set	Hexadecimal Code Without High-Order Bit Set	Decimal Code	Description
0xAB	0x2B	43	Access information discarded. Usually reported when the far-end ISDN switch removes some piece of information before tandem-switching a call. For example, some PBXs strip the display IE before sending a call out toward the PSTN and send back a message with this cause code.
0xAC	0x2C	44	Requested circuit/channel is unavailable. This happens when you get in a glare condition: Both sides are selected top-down or bottom-up. Change the Allocation Direction (so that one end is top-down and the other is bottom-up).
0xAE	0x2E	46	Precedence call blocked.
0xAF	0x2F	47	Resource unavailable, unspecified. Whenever you see Cisco Unified CallManager initiate a disconnect with cause code 0xAF, 99% of the time the problem is related to a media setup failure. Check for codec capabilities mismatches, especially your regions configuration.
0xB1	0x31	49	Quality of service unavailable.
0xB2	0x32	50	Requested facility not subscribed. This code typically indicates you are trying to use a service you are not permitted to use. For example, you might be trying to make a voice call on an ISDN circuit provisioned for data only.
0xB5	0x35	53	Outgoing calls barred within Closed User Group (CUG).
0xB7	0x37	55	Incoming calls barred within CUG.
0xB9	0x39	57	Bearer capability not authorized. This code indicates that you are placing a call with a bearer capability you are not allowed to use.
0xBA	0x3A	58	Bearer capability not presently available. This code indicates that you are placing a call with a bearer capability for which the service provider does not currently have capacity to supply.
0xBE	0x3E	62	Inconsistency in designated outgoing access information and subscriber class.
0xBF	0x3F	63	Service or option unavailable, unspecified.
0xC1	0x41	65	Bearer capability not implemented. The cause could be one of the following occurrences: <ul style="list-style-type: none"> You need to change the PCM Type value to the setting appropriate for your country. This is the most common cause, especially in countries where G.711 A-law companding is the standard. If your gateway is configured for μ-law and the service provider or PBX is expecting A-law, you will see calls disconnected with this cause code. The central office (CO) does not understand an information element in the setup message. You are connected to a PBX and you are sending out a network type number when the switch accepts only Unknown or National. You are selecting European PRI and you have the progress indicators turned on when they should be off.
0xC2	0x42	66	Channel type not implemented.
0xC5	0x45	69	Requested facility not implemented.

Table 5-1 Disconnect Cause Code Values (continued)

Hexadecimal Code with High-Order Bit Set	Hexadecimal Code Without High-Order Bit Set	Decimal Code	Description
0xC6	0x46	70	Only restricted digital information bearer capability is available (National use).
0xCF	0x47	79	Service or option not implemented, unspecified.
0xD1	0x51	81	Invalid call reference value. This code indicates that the far-end switch did not recognize the call reference for a message sent by the gateway.
0xD2	0x52	82	Identified channel does not exist. This code indicates a call attempt on a channel that is not configured on the far end. This could happen if you are using a fractional PRI. As of Cisco Unified CallManager Release 3.3, fractional PRIs are no longer supported.
0xD3	0x53	83	A suspended call exists, but this call identity does not.
0xD4	0x54	84	Call identity in use.
0xD5	0x55	85	No call suspended.
0xD6	0x56	86	Call having the requested call identity has been cleared.
0xD7	0x57	87	User is not a member of CUG.
0xD8	0x58	88	Incompatible destination. The cause could be one of the following occurrences: <ul style="list-style-type: none"> • The number being dialed is not capable of the type of call. • You are calling a restricted line in unrestricted mode. • You are calling a POTS phone using unrestricted mode.
0xDA	0x5A	90	Nonexistent CUG.
0xDB	0x5B	91	Invalid transit network selection (National use).
0xDF	0x5F	95	Invalid message, unspecified.
0xE0	0x60	96	Mandatory information element is missing. The far-end switch states that a message was received missing an information element it considers to be mandatory per the Q.931 specification.
0xE1	0x61	97	Message type nonexistent or not implemented.
0xE2	0x62	98	Message is incompatible with the call state, or the message type is nonexistent or not implemented. This code is usually indicative of an ISDN protocol mismatch. Each ISDN protocol variant has a slightly different state machine based on the state machines defined in the Q.931 specification. If the two sides of an ISDN connection are not configured for the same protocol, one side might violate the other's call state machine. If an ISDN message is sent that is not expected in the current call state, this cause is generated.
0xE3	0x63	99	An information element or parameter does not exist or is not implemented.

Table 5-1 Disconnect Cause Code Values (continued)

Hexadecimal Code with High-Order Bit Set	Hexadecimal Code Without High-Order Bit Set	Decimal Code	Description
0xE4	0x64	100	Invalid information element contents. The cause could be one of the following occurrences: <ul style="list-style-type: none"> The call has an information element that is not understood by the switch being called. The E4 is usually followed by the information element that is causing the problem. The most common problem is that you are trying to place a call using a network number when the switch being called accepts only National, International, or Unknown dialing. This code is also generated when you are using Network-Specific Facilities as an element when they are not needed.
0xE5	0x65	101	The message is incompatible with the call state. This code is usually indicative of an ISDN protocol mismatch. Each ISDN protocol variant has a slightly different state machine based on the state machines defined in the Q.931 specification. If the two sides of an ISDN connection are not configured for the same protocol, one side might violate the other's call state machine. If an ISDN message is sent that is not expected in the current call state, this cause is generated.
0xE6	0x66	102	Recovery on timer expiry. This occurs when ISDN messages don't arrive in specified time according to the Q.931 specification. The E6 is sometimes followed by the timer that has expired (for example, 03 01 00—the 310 timer).
0xE7	0x67	103	Parameter nonexistent or not implemented—passed on (National use).
0xEE	0x6E	110	Message with unrecognized parameter discarded.
0xEF	0x6F	111	Protocol error, unspecified.
0xFF	0x7F	127	Interworking, unspecified.

Failover and Recovery Procedures

This section provides an overview of the failover testing that was performed during Cisco Unified Communications Release 5.0(2) testing for IP telephony systems.

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified CallManager 5.0 Administration, provides full data backup and restore capabilities for all servers in a Cisco Unified CallManager cluster. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups. DRS supports only one backup schedule at a time.

The Cisco Disaster Recovery System performs a cluster-level backup, which means that it collects backups for all servers in a Cisco Unified CallManager cluster to a central location and archives the backup data to physical storage device.

When performing a system data restoration, you can choose which nodes in the cluster you want to restore.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.

- A distributed system architecture for performing backup and restore functions.
- A scheduling engine to initiate tasks at user-specified times.
- Archive backups to a physical tape drive or remote sftp server.

The Disaster Recovery System contains two key functions, Master Agent (MA) and Local Agent (LA). The Master Agent coordinates backup and restore activity with all the Local Agents. The system automatically activates both the Master Agent and the Local Agent on all nodes in the cluster. However, you can only access the Master Agent functions on the first node of the cluster.

For more information on the Cisco Unified CallManager Disaster Recovery System, see the [Disaster Recovery System Administration Guide](#).

Additional Sites and Services

Steps to Success is a Cisco methodology that outlines the tasks required to complete a successful customer engagement. Registered users can visit the [Steps for Success](#) resource site for Cisco Unified Communications process flows.

Advanced Services is a Cisco service offering that provides engineering expertise and best practices.

- Registered users can visit the Advanced Services resource site for [Cisco Unified IP telephony](#) lifecycle services.
- Nonregistered users can visit the [Advanced Services](#) external site.