



Operate

- [Introduction to Operating the System, page 1](#)
- [Managing Your System, page 2](#)
- [Backing Up and Restoring Components, page 3](#)
- [Using Network Monitoring Tools, page 4](#)
- [Using Managed Services Documents, page 5](#)
- [Troubleshooting Daily Operations, page 5](#)
- [Additional Sites and Services, page 15](#)

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. This practices include scheduled routine maintenance; keeping maintenance records; and maintaining up-to-date upgrade, troubleshooting, and recovery strategies.

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, on page 2](#)
- [Backing Up and Restoring Components, on page 3](#)
- [Using Network Monitoring Tools, on page 4](#)
- [Using Managed Services Documents, on page 5](#)
- [Troubleshooting Daily Operations, on page 5](#)

Managing Your System

This topic provides a high-level summary of the ongoing tasks that are 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 Collaboration system, see the product documentation listed in the Resource Library.

System Management Tasks

Managing a Cisco Collaboration 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 Collaboration 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 Collaboration system including network devices, phones/clients, software upgrades, voicemail 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.
- Backing up and restoring system components—Define backup methodologies and schedules, define a verification process for backups, secure storage of backups, and document backup processes.

System Management Options

There are two options for managing a Cisco Collaboration System:

- Do It Yourself—In this model, you are responsible for managing the entire Cisco Collaboration 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 tools as a means for monitoring your network; see [Using Network Monitoring Tools](#) for more information.
- Out tasking Hybrid Model—Using the [Services Portfolio](#) approach, Cisco and its partners provide a broad portfolio of end-to-end services and support that can help increase your Cisco Collaboration

system's business value and return on investment. This approach includes two services that provide different levels of management:

- [Cisco Unified Communications Essential Operate Service](#) —Cisco Essential Operate Services, part of Product Support in the Cisco Services Lifecycle framework, is available for Unified Communications software, collaboration software, and network management software. It provides the support you need to help reduce downtime, improve performance, and lead to higher productivity.
- [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 Essential Operate Service, Cisco Unified Communications Remote Management Service or other Cisco Unified Communications services, see <http://www.cisco.com/en/US/products/sw/voicesw/services.html> or contact your Cisco service account manager.

Backing Up and Restoring Components

This topic provides details on backup and restore for Cisco Collaboration components. First and foremost, the backup of Cisco Collaboration components needs to be incorporated into your corporate-wide backup operations. It is an important aspect of disaster recovery and is also essential before doing component upgrades. If you do not have a process in place, you must develop and document a backup and recovery management process. Some items to consider for this process are the following:

- Provide proper storage of operating system and Cisco Collaboration application CDs.
- Define incremental and full backup methodologies and schedules, assign an owner for each Collaboration component and database server.
- Define a verification process for backups:
 - Monitor backup logs on a daily basis for errors.
 - Periodically restore backup images to ensure validity.
- Secure onsite and offsite storage of backups.
- Develop well documented processes for system and configuration restoration.
- Ideally, provide central location(s) (for example, SFTP servers) for backup of data from all the Cisco Collaboration components.

The following topics provide backup and restore details on a component basis along with links to the appropriate component documentation:

- [Cisco Unified Communications Manager](#)
- [Cisco Unified Communications Manager Express](#)
- [Cisco Unified Contact Center Express](#)
- [Cisco Unified Communication Manager IM and Presence Service](#)

For additional information on backing up and restoring Unified Communications system components, as well as other system operations topics, see the documentation wiki (DocWiki) at http://docwiki.cisco.com/wiki/Unified_Communications_System_Operations.

Cisco Unified Communications Manager

Cisco Unified Communications Manager provides the Disaster Recovery System (DRS) for full backup and restore for all servers in a Unified Communications Manager cluster. The DRS performs a cluster-level backup, which means that it collects backups for all servers in a Unified Communications Manager cluster to a central location and archives the backup data to a physical storage device (tape or SFTP). For customers with multiple clusters, DRS must be configured per cluster.

DRS is invoked via the Unified Communications Manager Platform Administration. It allows you to perform scheduled (daily, weekly, monthly) automatic or user-invoked backups. DRS only supports a single backup schedule at a time. It provides a history (last 20 operations) of backup and restore operations.

**Note**

DRS does not support hostname or IP address change during restore. For more information about the Disaster Recovery System, see the [Disaster Recovery System Administration Guide for Unified Communications Manager](#).

Cisco Unified Communications Manager Express

Cisco Unified Communications Manager Express is an application that runs on Cisco IOS. Therefore, for backup and restore, the IOS facility for backup and restoring configuration data would be used. For more information, see specific documents in [Cisco Unified Communications Manager Express Documentation](#).

Cisco Unified Contact Center Express

For Unified CCX Release 10.6(1), the Backup and Restore application is described in Cisco Unified Contact Center Express Disaster Recovery System Administration Guide. For more information, refer [Cisco Unified Contact Center Express Configuration Guides](#).

Cisco Unified Communication Manager IM and Presence Service

Cisco Unified Communication Manager IM and Presence Service uses the Disaster Recovery System (DRS) for full data backup and restore capabilities of all Unified Presence Administration functions. For more information, see the IM and Presence Disaster Recovery System chapter in [Disaster Recovery System Administration Guide for Unified Communications Manager](#).

Using Network Monitoring Tools

Cisco Prime Collaboration allows businesses to actively monitor their Cisco Unified Communications solution to discover potential problems, maintain quality and user satisfaction, and help minimize service downtime. The following network monitoring tool is primarily used:

- Cisco Prime Collaboration

For more information about network monitoring, as well as other system operations topics, see the Cisco Unified Communications category on the documentation wiki (DocWiki) at http://docwiki.cisco.com/wiki/Cisco_Unified_Communications.

Cisco Prime Collaboration

Cisco Prime Collaboration removes management complexity and provides automated, accelerated provisioning, real-time monitoring, proactive troubleshooting, and long-term trending and analytics in one integrated product. The solution delivers a premier operations experience through an intuitive user interface and optimized operator methodology, including automated workflows that ease implementation and ongoing administration.

Provisioning features include automated processes for Cisco Collaboration Systems and Cisco TelePresence®. An intuitive user interface provides a single view of a subscriber and the subscriber's services, as well as a consolidated view of subscribers across the enterprise. With these capabilities, Cisco Prime Collaboration significantly accelerates site rollouts and dramatically reduces the time required for ongoing changes. In addition, by simplifying moves, adds, and changes, the solution facilitates delegation of these tasks, allowing organizations to optimize IT resources and further reduce total cost of ownership.

Cisco Prime Collaboration provides efficient, integrated service assurance management through a single, consolidated view of the Cisco voice and video collaboration environment. This includes continuous, real-time monitoring and advanced troubleshooting tools for Cisco Collaboration Systems and Cisco TelePresence systems including the underlying transport infrastructures.

For details, go to [Cisco Prime Collaboration](#).

Using Managed Services Documents

Managed Services documents provide essential information to ensure the continuous operation of a Cisco Collaboration System by monitoring faults, configuration, performance, and security. These documents define a component's Management Information Base (MIB) structure and also explain the syslogs, alerts, and alarms elements that service providers can incorporate in their managed services. They also describe the component's system architecture while outlining basic concepts such as Simple Network Management Protocol (SNMP) and presenting the capabilities of the management tools available for that component.

Refer to the individual product pages for more information on the managed services.

Troubleshooting Daily Operations

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

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

For an expanded list of general problem areas, as well as other system troubleshooting topics, see the documentation wiki (DocWiki) at http://docwiki.cisco.com/wiki/Unified_Communications_System_Troubleshooting.

Common Problems Reported by Users

This section describes basic approaches to diagnose and resolve common problems reported by end users. 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](#)
- [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 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 terminating devices involved in the call are on different IP subnets, each device has the correct default gateway and subnet mask settings.
- If one of the devices is a Unified IP phone, the DHCP scope has an incorrectly configured default gateway parameter.
- If one of the devices is a Cisco IOS software gateway, the default route is correct. Also, ping the other end from the gateway. If the ping is successful, you know that you have IP connectivity. If the ping is unsuccessful, perform a `traceroute` to determine where the problem lies.

**Note**

Remember that signaling packet traffic is always between Unified Communications Manager and the terminating device, whereas the RTP voice packet traffic is directly between the devices. So just because the devices are registered to Unified Communications Manager and can set up a call through Unified Communications Manager does not mean that the devices 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 Communications Manager Administration, you configure a specific IP address. Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager.

- 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 Communications Manager 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 terminating devices. 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 terminating devices 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 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.

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 terminating devices 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 terminating devices, 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 device 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 device 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 terminating devices 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.

PBX Interoperability Issues with Cisco Unified Communications Manager

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 Communications Manager 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](#)

site. This site has information on third-party PBX interoperability with the following Cisco Collaboration products:

- Cisco Unified Communications Manager
- 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 Communications Manager.

Using Call Flows to Resolve Call Processing Problems

This topic provides information about a typical call flow in an IP telephony environment. The figure 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 Communications Manager

- Gatekeeper

Figure 1: Call Flow in an IP Telephony Environment

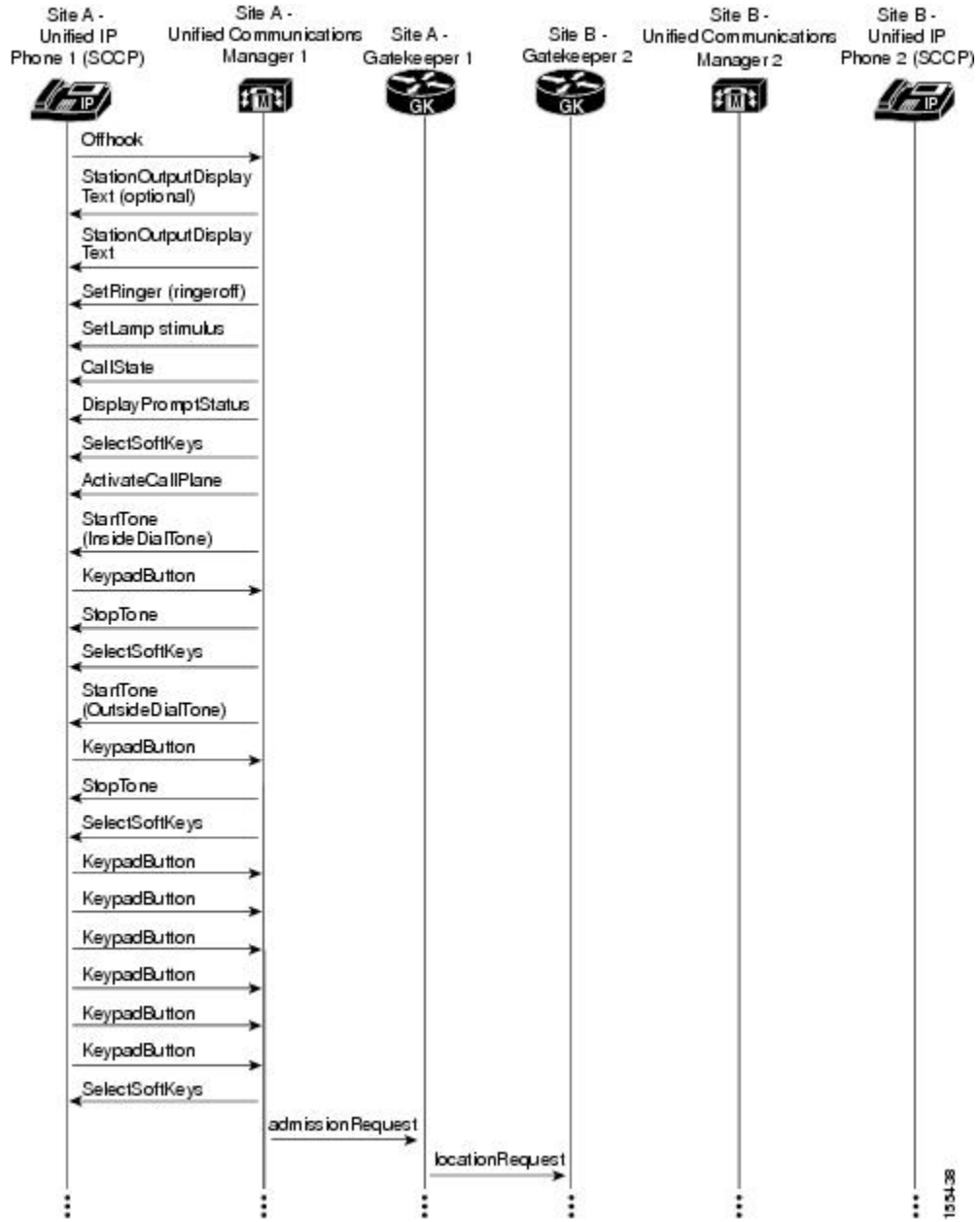
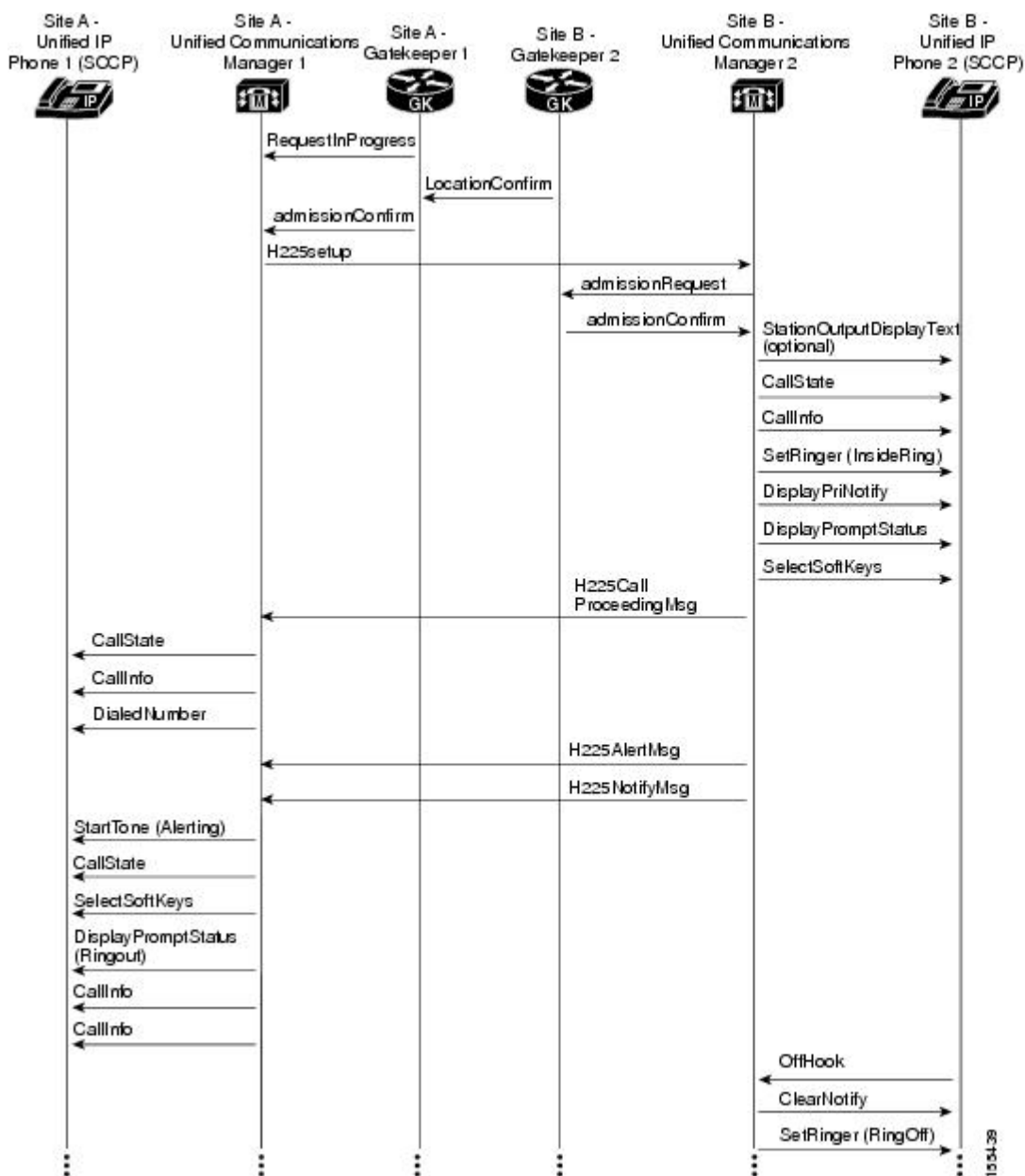


Figure 2: Call Flow in an IP Telephony Environment (continued)



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 6-1 lists the standard cause values that may appear in the trace files as part of disconnect processing.

Failover and Recovery Procedures

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified Communications Manager Administration, provides full data backup and restore capabilities for all servers in a Cisco Unified

Communications Manager 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 Communications Manager 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 Communications Manager Disaster Recovery System, see the [Disaster Recovery System Administration Guide for Unified Communications Manager](#).

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 to Success](#) resource site for Cisco Collaboration process flows.

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

- Registered users can visit the [Sell and Market Services](#) partner site.
- Non-registered users can visit the [Services for Unified Communications](#) site.

