Configuring and Troubleshooting VoIP Monitoring

revised November 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Configuring and Troubleshooting VoIP Monitoring

Contents

1 VoIP Monitoring Concepts 7

- Introduction 7
  - Definitions 8
- Capturing an IP Phone Call 11
- Accessing Audio Streams 13
  - Identifying Audio Streams 15
  - Packet Capture Methods 16
    - Desktop Capture Method 17
    - Server Capture Method 18
    - Unified CM Capture Method 19

2 Deployment Issues 23

- Introduction 23
  - Remote Agents 23
  - Mobile Agents 25
  - Packet Capture Methods Used in Cisco Monitoring and Recording Software 26
    - Cisco Agent Desktop 26
    - Quality Monitoring 27
  - NDIS-Compliant NICs 29
  - Agent Phones 29
    - Desktop Capture Method 29
    - Server Capture Method 30
    - Unified CM Capture Method 30
  - SPAN 30
  - RSPAN 32
  - VLANs 34
  - Port Traffic Direction 36
  - Media Mixing 40
  - Gateway SPAN Sniffing 42
  - Trunk Port Monitoring 43
  - MAC Address Changes Due to Layer 2 Routing Devices 43

Contents

Server Capacity 46
Number of SPAN Sessions 46
Network Traffic Restrictions on Destination Ports 47
Switch Operating System Version 47
- Examples of Deployment Planning 48
  - Example 1: ABC Company Deployment 49
  - Example 2: International Sprockets Deployment 51
  - Example 3: Redundant Systems Inc. Deployment 53

3 The NIC Qualification Utility 59

- Overview 59
- Assumptions 61
- Utility Syntax 62
  - Running the NICQ Utility 62
  - Output From the NIC Qualification Tool 63
- NICQ Tests 65
  - Test 1—Check Driver Status 65
  - Test 2—Retrieve List of Valid Network Adapters 65
  - Test 3—Capture Packets 65
  - Test 4—Detect Attached IP Phones 66
  - Test 5—Detect Promiscuous Traffic 68
  - Successful Test Report Example 68
- Using Multiple NICs with the VoIP Monitor Service 71
- Limitations 72
- Issues 73
- Installing a Second NIC in a VoIP Monitor Service Server 74
  - Additional Configuration Steps 74

4 Troubleshooting VoIP Monitoring and Recording 77

- Introduction 77

Contents

- Troubleshooting 78
  - Identifying the Problem's Location 78
  - Common CAD Issues 82
  - Common Recording Solution Live Monitoring and Recording Issues 82
    - Agent not on the Live Monitoring agent list 84
    - Error trying to live monitor an agent 84
    - Agent calls not recorded 85
    - Audio recordings contain no speech 85
    - Recordings for SPAN-configured agents are on the agent desktop 86
    - Call recordings contain pops and clicks 86
    - Call recordings are poor quality 87
    - Portions of an audio call are missing 88
- Troubleshooting Procedures 89
  - Verifying Sound Card Functionality 89
  - Verifying Registry Settings 90
  - Verifying that the Correct NIC Is Being Used 90
  - Testing the Sniffing Adapter 90
  - Testing the Desktop Monitor Library 91
  - Verifying that Required Applications are Running 91
  - Opening a TAC Case 92

A Cisco Catalyst Switch Capabilities 93
- SPAN-Related Feature Descriptions 95

B Supported IP Phones 97
- Desktop Capture Method 97
- Server Capture Method 97
- Unified CM Capture Method 98

Contents

C **Configuring Unified CM for VoIP Monitoring** 99

Configuring Unified CM for Desktop Monitoring 99

Configuring Unified CM for Server Monitoring 100

Configuring Unified CM for Unified CM-based Monitoring (Unified CCE Only) 100

Requirements for Mobile Agent Monitoring and Recording (Unified CCE Only) 100

VoIP Monitoring Concepts

1

Introduction

Cisco software products for IP contact centers have the ability to live-monitor and record calls between contact center agents and customers. These products are:

- Cisco Agent Desktop for Unified Contact Center Enterprise
- Cisco Agent Desktop for Unified Contact Center Express
- Cisco Recording Solution (formerly known as Cisco Quality Management)

To implement these live monitoring and recording features, knowledge of computer networks, the protocols that carry data over a network, and the hardware components that make up the network is required.

The configuration of various network components can be complex. Misconfiguration will lead to the feature failing to work properly. This white paper is intended to take the mystery out of capturing IP phone calls using Cisco software. It will explain the methodology used to capture voice streams, limitations of the technology, and challenges to deploying and maintaining systems supporting this feature.

The information contained in this white paper does not require any specific networking knowledge or software development expertise. The reader should be somewhat familiar with computers, applications/programs, and networks.

Definitions

Table 1 is a list of terms used throughout this white paper and their meanings. It is a good idea to become familiar with these terms in order to best understand this information in this paper.

Table 1. Terms and definitions

Term	Definition
Built-in bridge	A hardware component in many Cisco IP phones that allows audio streams to be merged and forked to support Unified CM Recording and Monitoring.
CAD	Cisco Agent Desktop is a suite of applications used by contact centers to handle incoming and outgoing calls.
Call recording	Application feature found in CAD and Recording Solution that allows calls between an agent and another party to be captured and stored as files on disk. These files can be reviewed at a later time.
Cisco Recording Solution	A suite of applications used by contact centers to record business calls and use those calls to evaluate agents and processes.
Desktop capture	A packet capturing configuration (also known as endpoint capture) in which packet capturing software runs on a user's PC. The user has either a soft phone on the PC or a hard IP phone directly connected to the PC between the PC and the network switch.
Endpoint device	A device, such as a PC or IP phone, with a NIC and IP address that can send or receive network packets.
Hard IP phone	A physical IP phone that is plugged into the network.
IP (network) switch	A hardware device that offers high-speed connections and traffic routing from various network devices such as IP phones, PCs, routers, gateways, and other switches. Port monitoring or SPAN configurations are set up on the switch when server monitoring is used.

Table 1. Terms and definitions (cont'd)

Term	Definition
Live monitoring	A feature in CAD (also known as "silent monitoring") that allows a CAD supervisor to listen in on a phone conversation between a CAD agent and another party. The CAD agent might or might not be notified that the call is being monitored, depending on how CAD is configured. The two audio streams that make up the call are captured and sent to the supervisor's desktop to be played back using the desktop's sound card. A feature of Recording Solution that allows a supervisor to listen to an agent's call by using the Unified CM Recording and Monitoring feature to have the built-in bridge on the agent's phone merge the audio streams and send them to the supervisor's phone as another phone call.
Network recording	A method of call recording used in Recording Solution that uses the Unified CM Recording and Monitoring feature to have the built-in bridge on the agent's phone duplicate the audio streams and send them to a Recording Solution Network Recording server to be stored in files.
Packet capture	The process of capturing network traffic from the network fabric for processing. In most cases, the traffic is captured in promiscuous mode.
Promiscuous mode	A mode of operation for a network interface card (NIC) and its driver. Promiscuous mode allows packets not addressed to the device with the NIC to be captured and processed at the application level.
RSPAN	Remote SPAN allows ports from connected switches to be included as sources for the SPAN session that copies data and sends it to the destination port.
RTP	Real Time Transport Protocol. A network packet format that is used to carry audio data that makes up a phone call between an agent and another party.
Server monitoring	A packet capturing configuration in which the packet capturing software runs on a server that is directly connected to a network switch and to a switch port that has been configured to receive network traffic copied from other ports on the switch.

Table 1. Terms and definitions (cont'd)

Term	Definition
Session initiation protocol (SIP)	A protocol used to set up and manage IP phone calls. This protocol is used when the Unified CM Recording and Monitoring feature is used.
Soft IP phone	A soft IP phone is a computer application that emulates a hard IP phone and runs on an agent's PC.
SPAN	Switched Port Analyzer. A feature, also known as port monitoring, of some switches that allow all the network traffic entering or leaving a switch port to be copied and sent to a destination port. When server monitoring is used, the destination port on the switch is the connection point for the server that is running the packet capturing software.
Unified CM recording and monitoring	A feature of the Cisco Unified Communications Manager (Unified CM) software and supported IP phones that allows a command to be sent to the IP phone, causing the audio streams to be duplicated and sent out from the phone to two destination ports for recording. It also includes the ability to have the agent's phone merge the audio streams of a live call and send them to another phone as a new call so a supervisor can listen to the call. This feature also supports recording and monitoring tones that alert the agent or caller that they are being recorded or monitored.
VLAN	Virtual Local Area Network. A group of related network devices that share some characteristics. These devices do not need to be physically connected to the same switch.

Capturing an IP Phone Call

In order to capture an IP phone call, we need access to the data travelling over the network and the format of the data. We will discuss the access issue later. In this section, we discuss the format of the audio portion of the phone call.

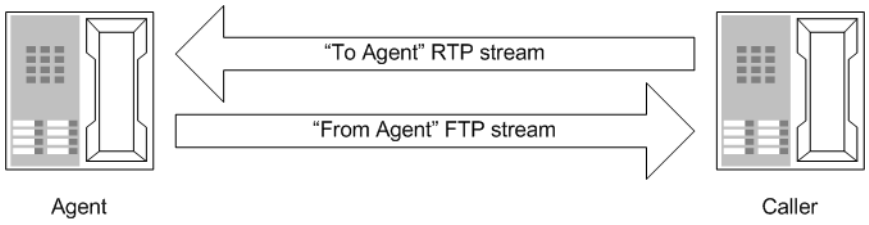
Cisco Unified Communications Manager (Unified CM) and Unified Contact Center (Unified CC) software, in concert with Cisco switches, gateways, and routers, package audio phone calls as streams.

There are two streams of audio data for each call. To help distinguish the two streams of audio data, the end points are referred to here as follows:

- Agent phone. The agent is the person in the contact center whose phone is an IP end point on the contact center's network.
- Caller phone. The caller refers to another person on the call (using an IP phone or appropriate device).

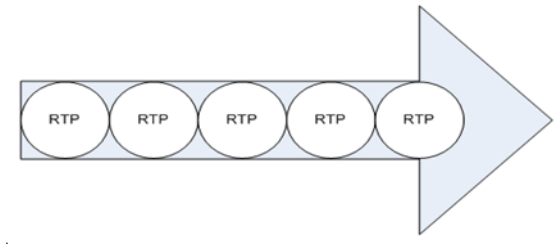
Figure 1 shows one stream of audio being sent from the agent phone to the caller phone and the other stream being sent from the caller phone to the agent phone. If software can capture these two streams of packets from the network, the data can be processed and stored in a format that can be listened to at a later time.

Figure 1. IP phone call audio streams



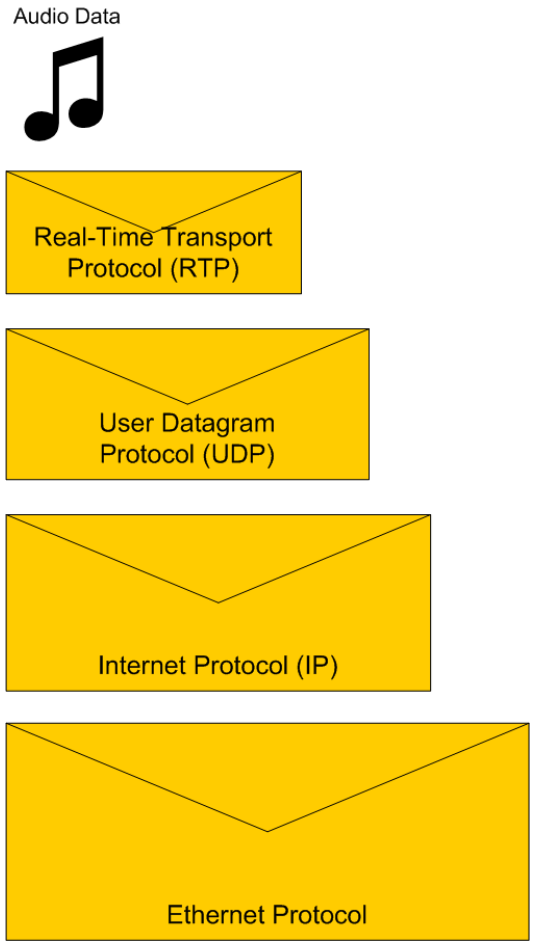
The protocol used to encapsulate the audio data is known as the Real-Time Transport Protocol (RTP). As shown in Figure 2, an audio stream is made up of many individual data packets sent over the network.

Figure 2. RTP audio stream



The RTP packets are encapsulated in UDP, IP, and Ethernet envelopes as shown in Figure 3.

Figure 3. Audio data encapsulation



Audio data is also encoded using different formatting protocols. The audio format used has nothing to do with transport over a network, so it is not shown as an encapsulation in Figure 2.

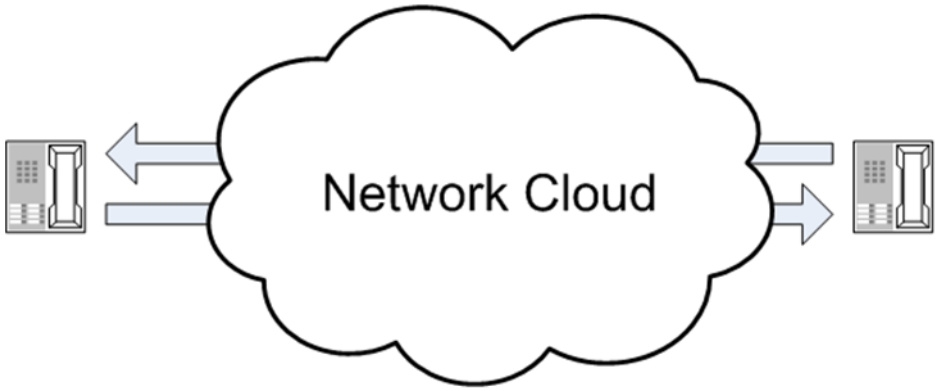
Cisco monitoring and recording software and hardware supports several audio data formats, including G.711 (mulaw and alaw), G.729, and G.722. These formatting protocols are used to encode the audio data for transport over the network. Some formats, like G.729, greatly compress the data so it can be transported over a network faster.

Accessing Audio Streams

Accessing the streams of audio data is where things start to get complex. This is because network hardware and software and IP protocols themselves are created with an eye toward security. When packets of data are to be sent from endpoint A to endpoint B, we don't want other endpoints to see that data because it is considered private. We can't just plug a computer into a network and tell it we want to see all the data being sent to and received from another computer.

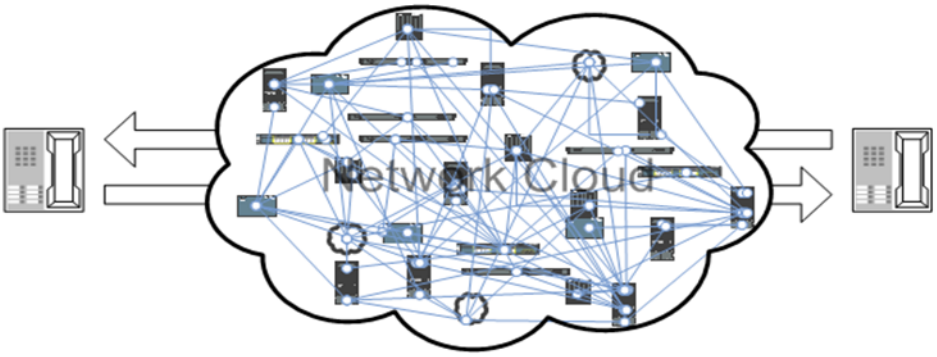
In the case of IP phone calls, all we know is that there are two endpoints (in this case, IP phones) that are exchanging packets containing audio data (Figure 4).

Figure 4. An IP call traversing the network



The phones are sending packets into and receiving packets from the network cloud. This cloud hides a lot of complexity (Figure 5). In a packet-switched network, packets can be routed almost anywhere. They will not always follow the same path through the network cloud. There can be delays or outages that require resending or rerouting data.

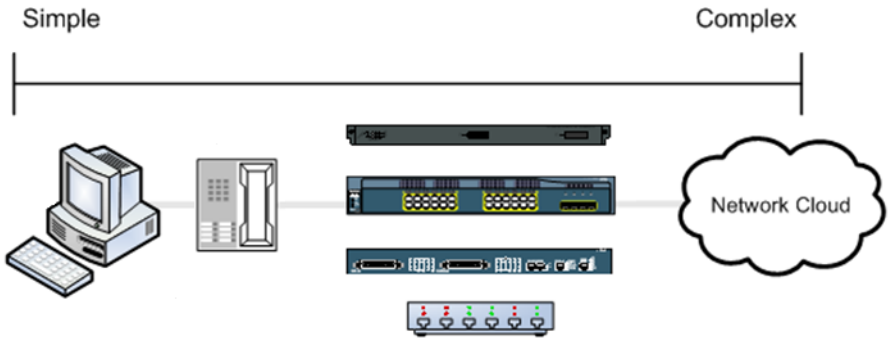
Figure 5. The network cloud revealed



The challenge then is to determine the best location to tap into this network to see the audio packets. The most reliable method is to have the phone itself send the audio streams to your software. This is possible with the Unified CM Recording and Monitoring feature. This feature, which is available on Unified CM 6.0 and later, allows the Unified CM to send a command to the built-in bridge (BIB) on the agent's phone to have it duplicate the two audio streams and send them over the network to another location. For recording, the two streams are sent to two ports on a recording server. For live monitoring, the two streams are merged into one and sent as a new call to a supervisor's phone, thus allowing the supervisor to listen to the call. The mechanics of this feature are shown below.

The next most reliable location to tap into the network is at the IP phone itself. It is at this point that we know the data will be flowing to or from the phone over a single cable. The further away from the IP phone (toward the network cloud) we go, the more complex is the solution to accessing the audio streams.

Figure 6. Audio stream access points and solution complexity



Most Cisco IP phones contain another network connection point where a computer can be daisy-chained. This allows software running on the attached PC to see the audio traffic. This method is referred to as “desktop monitoring” and is discussed in more detail below.

If the IP phone does not support daisy-chaining, or if policy dictates that this configuration is not supported, the next access point away from the phone is the switch to which the phone is connected.

> **NOTE:** The phone must be directly connected to the switch. It cannot be connected to a hub, router, or gateway.

The Cisco Catalyst line of switches supports a feature called Switched Port Analyzer (SPAN), or port monitoring, that allows network traffic flowing through a particular switch port or group of ports to be copied and sent to a destination port. Software listening on this destination port can then get access to packets containing audio data representing a phone call. This method of packet capture is known as server monitoring.

If server monitoring on the switch is not supported due to hardware restrictions, policy, or the network design itself, another option for gaining access to the audio streams is the Unified CM monitoring feature found in Unified CM version 6.0(1) and later. This feature allows software to send a command to the agent IP phone, instructing it to send copies of the audio streams to two ports of a network endpoint. This endpoint must have software running and listening on these ports so it can capture the audio packets and process them.

These are the three packet capture methods (desktop monitoring, server monitoring, and Unified CM monitoring) that are currently employed to capture IP phone call audio traffic by Cisco monitoring and recording software. Before describing the details of each of these methods of monitoring, we need to discuss how Cisco monitoring and recording software identifies audio streams for particular agent devices.

Identifying Audio Streams

The software that is capturing audio packets must be able to tell which audio packets belong to the call for the agent who is being monitored or recorded. If Unified CM recording is being used, we already know the ports that will be used for accepting audio packets from the phone. For endpoint or server monitoring, we need to know something unique about each device or call that can be found in the various network protocol headers. There are two methods that are used for filtering audio packets:

- MAC address filtering
- IP/port filtering

An agent and the phone the agent uses for a call are associated, either statically or dynamically, at runtime. The MAC address or IP/port used by the agent's device allows the correct audio stream to be identified and processed.

The Ethernet header contains the MAC addresses of the network device sending the packet and the intended receiving device, which might be the IP phone or another network component like a router or gateway. The IP header contains the IP address of the sender and intended destination device.

The method that is used to identify the audio packets can depend on the configuration of the agent software or the packet capture method. This information is summarized in Table 2.

Table 2. Audio stream identification methods

Application	Feature	Deployment	Identification Method*	
			Desktop Capture	Server Capture
CAD	Monitoring	Local†	MAC	MAC
		VPN	MAC	—
		Thin client	—	MAC
		Mobile agent	—	IP/Port
		IPPA	—	MAC
	Recording	Local	MAC	MAC
		VPN	MAC	—
		Thin client	—	MAC
		Mobile agent	—	IP/Port
		IPPA	—	MAC
Recording Solution	Recording	Local	MAC	IP/Port
		Thin client	—	IP/Port
		VPN	MAC	—
		Mobile agent	—	IP/Port

* The Unified CM capture method is not listed in this table, because it is a feature of Unified CM. Audio streams are captured within Unified CM and not from CAD.

† "Local" means that the agent is within the contact center's LAN/WAN, which also includes the Unified CM and other system components.

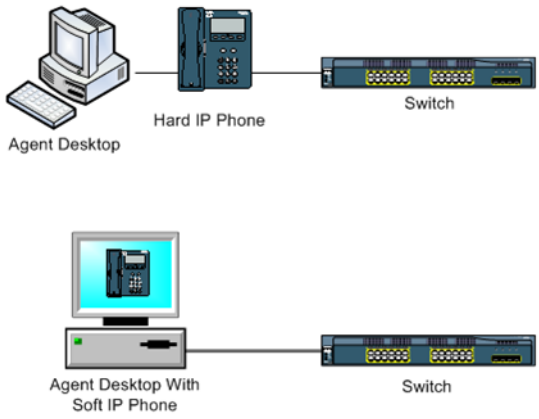
Packet Capture Methods

In this section, each packet capture method will be explained in detail. By understanding the capture methods, it will be easier to understand the various limitations and supported configurations of the Cisco monitoring and recording software.

Desktop Capture Method

The desktop capture method relies upon the fact that many Cisco IP phones contain a small internal switch and a second network port on the back of the phone to which a computer can be daisy-chained.Figure 7 shows that this capture method can work with either a hard or soft IP phone.

Figure 7. Desktop capture hardware configurations



In this configuration, the IP phone and the computer are sharing a single network cable for their network configuration. When a hard phone is used, the phone and the computer are separate network endpoints with their own unique IP and MAC addresses. When a soft IP phone is used, the computer and the phone are a single network endpoint that share a MAC and IP address.

When a hard phone is used, the phone must be configured to send its network traffic down the line to the desktop in order for the NIC on the computer to see the traffic meant for the phone. This is a setting that is accessed through the Unified CM administration application. This allows the audio data for phone calls (as well as other traffic sent to/from the phone) to hit the computer's NIC. But, by definition, the computer's NIC will not pass this data up to an application on the computer because it is not addressed for the computer's NIC. It is addressed to the IP phone. In order to see this traffic, the NIC needs to use promiscuous mode.

NICs that support the Network Driver Interface Specification (NDIS), which includes almost all NICs for PCs, will also support a packet capture feature called *promiscuous mode*. In this mode, the NIC passes packets up to the software on the machine even if they are not addressed to the machine’s NIC. Cisco monitoring and recording software uses a packet sniffing driver that opens a NIC adapter and puts it into promiscuous mode so it can see the daisy-chained IP phone’s audio traffic when the agent is on a call. With this configuration, the software is able to capture both of the agent's phone call audio streams and process them for live monitoring or recording.

Cisco monitoring and recording software also supports the use of approved software-based IP phones. Soft IP phones are applications that run on the agent's PC.

The desktop software treats this soft IP phone as if it is a hard IP phone daisy-chained to the PC. The only difference is that the NIC does not need to be put into promiscuous mode for a soft IP phone, because the soft IP phone and the PC have the same IP address. As a result, the sniffing software automatically has access to all the audio packets when the agent is on a call.

This capture mode is supported by CAD and Recording Solution software.

Requirements

Using the desktop capture method requires the following:

- A PC that can run the Cisco monitoring and recording software and driver
- A NIC that supports promiscuous mode packet capturing (hard IP phone only)
- Either of the following types of supported Cisco IP phones:
  - A hard IP phone with a second network port
  - A soft IP phone
- Proper configuration of the IP phone to send the IP phone's network traffic to the connected PC (hard IP phone only)
- A direct connection between the agent's PC and hard IP phone, and a direct connection between IP phone and the switch with no other devices (for example, other hard IP phones, routers, gateways, or hubs)

Server Capture Method

There will be cases where the desktop capture method cannot be used, for example, when the contact center agent does not have a PC, but just an IP phone. In these cases, the server capture method is an option for monitoring or recording agent calls.

The server capture method assumes that a SPAN or port monitoring session is configured on the switch, in order to copy network traffic from one or more ports to a destination port used by a server machine that is running packet capturing software.

Because we are moving the capture point further away from the IP phone toward the network cloud, configuration becomes more complex. This complexity is the primary cause of support calls concerning the monitoring and recording features not working as expected. The Requirements section below discusses the factors that affect this method of capturing packets.

Requirements

Using the server capture method requires the following:

- A supported hard or soft IP phone connected to a switch
- No Layer 2 routing devices between the IP phone and the switch when the phone's MAC address is used to identify audio packets. See "Layer 2 Routing Device Restriction" on page 19 for more information.

- A SPAN or port monitoring session configured that uses the IP phone's port as one of the session's source ports
- A VoIP monitoring/recording service connected to the SPAN session's destination port
- Proper configuration of the Cisco and Cisco software that associates the agent's IP phone device with a VoIP monitoring/recording service

Layer 2 Routing Device Restriction

A Layer 2 routing device is any piece of networking hardware that causes the MAC address used in a packet to change. This includes almost all network devices except for repeaters.

This is a problem because the monitoring software has an association with the MAC address of the actual phone device being used by the agent. This is the MAC address that is looked for in the audio packets that traverse the switch to which the monitoring server is connected. An audio packet that must traverse a Layer 2 routing device before reaching the phone will have the Layer 2 device's MAC address in the packet rather than the phone's MAC address. As a result, the monitoring software will never see packets with the phone's MAC address, and any monitoring and recording will result in silence.

This restriction affects the server-based capture method in CAD (non-mobile agents only). This restriction does not apply to Recording Solution. Recording Solution does not use MAC addresses for server-based captures; rather, it uses the IP address and port. See "MAC Address Changes Due to Layer 2 Routing Devices" on page 43 for more information.

Unified CM Capture Method

Unified CM Recording and Monitoring is a feature that allows call recording and live monitoring using the built-in bridge of an IP phone to duplicate and send audio streams. APIs exposed by Cisco allow third-party vendors to access this functionality. The two main modes of this feature are Unified CM recording and live monitoring.

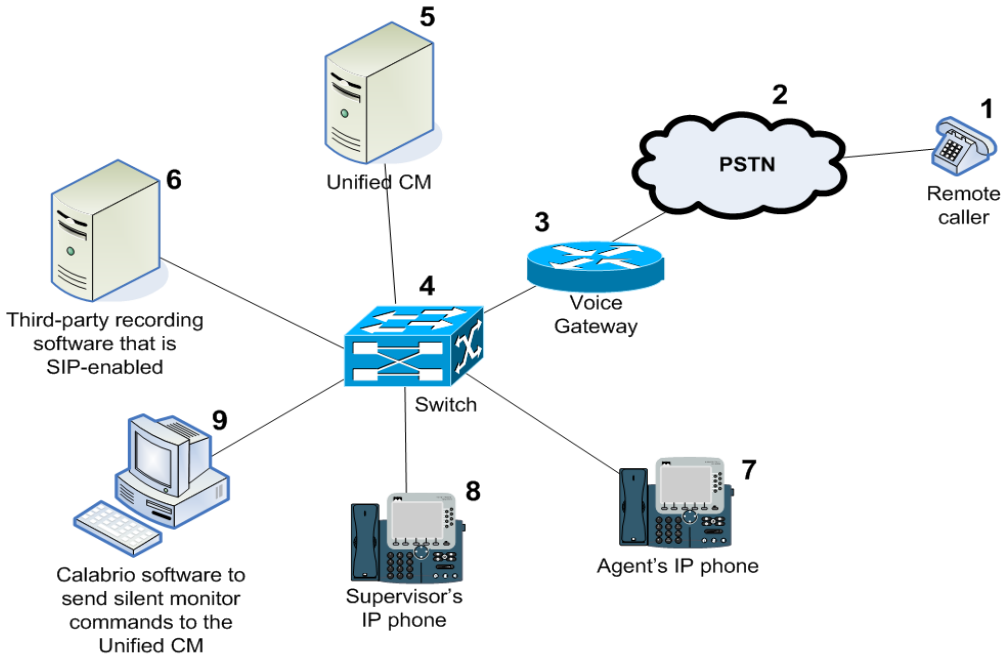
Unified CM Recording

In this mode, an agent's device is configured in Unified CM to be automatically recorded whenever a call is active on the phone. When the agent makes or answers a call, it causes the Unified CM to send a SIP INVITE message to a specific IP address on a recording server.

The recording server accepts the call and responds with an IP address and two ports. The ports are where the phone should send the two audio streams. The Unified CM tells the phone where to send the audio streams. The built-in bridge on the agent's phone copies the two audio streams and sends them to the destination ports. The

recording server reads the audio streams and writes the data to disk so the call can be listened to at a later time.

Figure 8. Unified CM recording



Referring to the numbered devices in Figure 8, the sequence is as follows:

1. The agent receives a call from a remote caller (1 > 2 > 3 > 4 > 7).
2. The Unified CM sends a SIP message to a recording server inviting it to accept copies of the audio streams for the agent's call (5 > 4> 6).
3. The recording server sends a message back, accepting the call and giving its IP address and two ports that will be used to accept the two audio streams (6 > 4 > 5).
4. The Unified CM tells the phone to copy its audio streams and send them to the IP address and ports the recording server responded with (5 > 4 > 7).
5. The IP phone's built-in bridge copies the audio streams and sends them to the two ports on the recording server. The server reads the audio data as it arrives and writes it to disk (7 > 4> 6).

Live Monitoring

In this mode, a supervisor wants to listen in on an agent's call. The supervisor's phone is used to listen to the agent's call. The Unified CM's JTAPI API allows an application to issue the request to live monitor a call. An application is required to issue this command on behalf of the supervisor. The supervisor uses this application to select the agent device that is on a call and issue the command. The command includes the supervisor's extension where the live monitoring call will be sent. The Unified CM tells

the built-in bridge on the agent's phone to duplicate and merge the two audio streams, make a call to the supervisor's phone, and start sending the audio stream. The live monitoring session ends when the original call ends, the supervisor hangs up, or the supervisor transfers the call to another party.

Referring to the numbered devices in Figure 8 on page 20, the sequence is as follows:

1. The agent accepts a call from a remote caller (1 > 2 > 3 > 4 > 7).
2. Software that is monitoring the agent's device via the CTI interface with the Unified CM is informed about the call (5 > 4 > 9).
3. When a supervisor wants to live monitor the agent's call, the supervisor uses Recording Solution to send a command to the Unified CM through the CTI interface to set up a live monitoring session (9 > 4 > 5).
4. The Unified CM receives the command, which includes the supervisor's phone number, and tells the agent's phone to use its built-in bridge to copy and merge the two audio streams into a single audio stream (5 > 4 > 7).
5. A new call is set up between the agent's and supervisor's phones (7 > 4 > 8). The agent's phone answers automatically and the supervisor's phone rings. When the supervisor answer the call, he or she can hear the agent and caller speaking. Neither the agent nor the caller can hear anything the supervisor says.

Starting with Recording Solution 8.0(1), Cisco Unified Contact Center Express installations are supported for both Unified CM live monitoring and call recording.

CAD supports this method for live monitoring only when the following conditions are met:

- The agent uses Cisco Agent Desktop, Cisco Agent Desktop—Browser Edition, or Cisco IP Phone Agent, versions 7.2 for Unified CCE or newer
- The agent is local or remote (over a VPN connection)
- The agent uses a hard or soft IP phone

NOTE: CAD for Unified CCX does not support Unified CM live monitoring. However, starting with CAD 8.5 for both Unified CCX and Unified CCE, a feature was introduced that enables Unified CCX/CCE to use a third party application that does built-in bridge/Unified CM live monitoring and recording, while still supporting desktop-based or SPAN-based monitoring and recording with CAD.

If this method is configured in CAD for live monitoring, the desktop capture and server capture methods are turned off. The result is that agents can be live-monitored, but not recorded. The reason for this is that this method causes additional audio streams to emanate from the phone. If the other methods were used to capture the audio

data, they would capture these extra streams, resulting in duplicate audio packets and poor audio quality.

Note that Recording Solution is still able to record using the server-based capture method even if the Unified CM method is used because it looks at the IP addresses and ports of the two streams. The additional audio stream will be ignored. The Recording Solution desktop capture method, like in CAD, results in duplicate packets and poor quality because the MAC address is used to filter packets and the extra stream of copied audio data cannot be filtered out.

Requirements

Using the Unified CM capture method for CAD live monitoring, Recording Solution live monitoring, or Recording Solution network recording requires the following:

- The correct version of Cisco Unified CM and its related components
- The correct version of CAD or Recording Solution
- Supported IP phones that can respond correctly to the call control commands

Deployment Issues

2

Introduction

Deploying Cisco monitoring and recording software and properly configuring the software and network components can become quite complex. The method of audio capture that is used for the agents is only one aspect of a deployment, but whatever is decided can affect the amount of time and money required for a successful deployment.

In the previous sections, the basics of audio packet transmission and capture were discussed in order to better understand the environment the software runs in and the different options that are available for supporting the live monitoring and recording features. In this section, we are going to look at the issues that are faced when planning a Cisco software deployment and how it relates to the live monitoring and recording features.

These are not all technical issues. Integrating Cisco software into a customer's network can be challenging at times. The customer might want certain features, but be unwilling or unable to make changes to the networking infrastructure to accommodate them. In these cases, the software offers the different methods of capturing audio data to support its features.

Each subsection below details an issue related to deploying Cisco monitoring and recording software to support live monitoring and recording, tells why it is important, which capture method it affects, and why. Understanding each of these issues will enable the best choices to be made for a deployment.

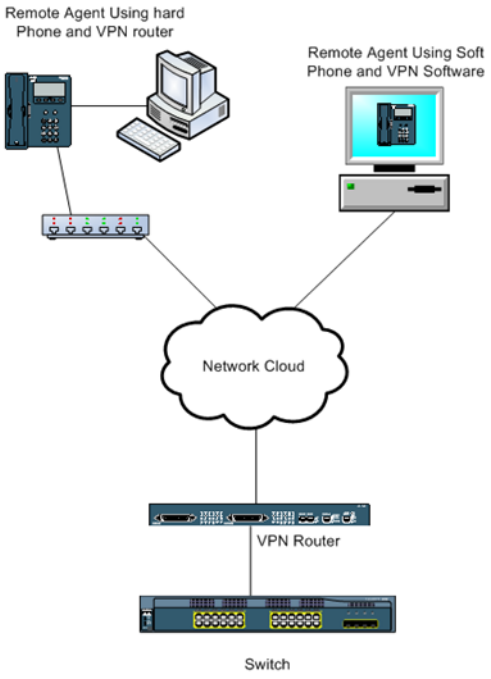
Remote Agents

Issue: The desktop capture method must be used for remote CAD agents.

Cisco monitoring and recording software supports agents that connect to the contact center's network using Virtual Private Network (VPN) software or hardware. This allows a remote desktop to create a secure network connection through the network cloud

that allows the user to access network resources as if they were connected directly to the contact center's network.

Figure 9. Remote agent configuration



Two types of remote VPN agents are supported by the Cisco software:

- If the remote agent has a hard IP phone, the agent must use a supported VPN router (for example, the Cisco 831 or 871 home office routers). If the remote agent is to be monitored or recorded, the agent's PC must be daisy-chained to the IP phone.
- If the remote agent has a soft IP phone installed on the desktop, the agent can use the VPN router or a supported VPN client software package (such as the Cisco VPN client).

In either case, the server capture method is unsupported for these agents in CAD. (Recording Solution supports either desktop or server capture methods over a VPN connection.) This is because of the presence of the VPN router between the remote IP phone and the monitor service, which causes the audio packets' MAC address coming from the agent's phone to be changed as they traverse the network. To understand why, refer to "MAC Address Changes Due to Layer 2 Routing Devices" on page 43.

The VPN router also acts as a network gateway between the network cloud and the internal network. Normally, the IP addresses used are set by Network Address Translation (NAT), which changes the IP address of the audio packets. This leaves the packet capturing software unable to identify the audio packets for a particular agent's phone.

The Unified CM capture method (for monitoring only, not recording) is supported for CAD live monitoring, Recording Solution network recording, and Recording Solution live monitoring. If Cisco IP Communicator is used, it must support the Unified CM feature (version 7.0(1) or later).

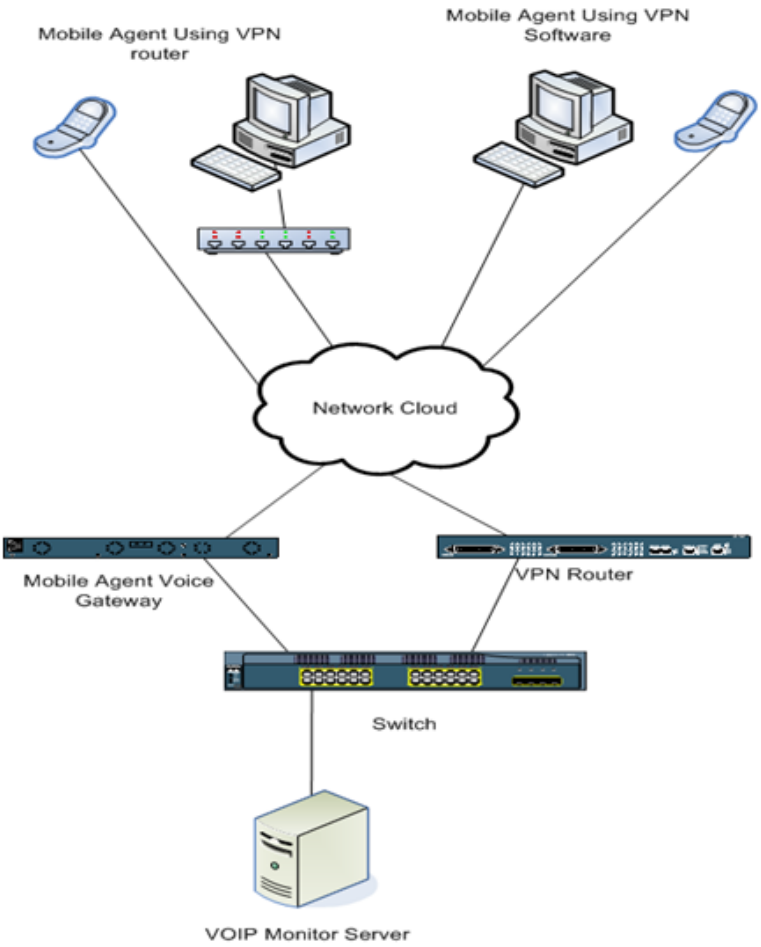
Mobile Agents

Issue: The server capture method must be used for mobile agents

This deployment model applies to Unified Contact Center Enterprise systems only.

Mobile agents, like remote agents, are not located at the contact center. Unlike remote agents, they use a phone that is not controlled by the contact center's Unified CM system. The phone could be an IP phone, an analog phone, or a cell phone. The desktop application still needs to be connected to the contact center's network, either directly or via a VPN connection.

Figure 10. Mobile agent configuration



When a call is to be delivered to the mobile agent, the system uses the assigned CTI port to make a call to the agent's configured phone. The call is then connected to the caller. The audio data for this call flows through the mobile agent voice gateway. A VoIP Monitor service can capture packets from the voice gateway port and use the call's IP address and port information to forward the audio to a supervisor for monitoring, or to a recording service to be stored on disk.

Because the phone is not connected to the mobile agent's desktop, and the phone is not controlled by the contact center's Unified CM, audio streams can not be captured at the agent's desktop. Because the phone is not controlled by the Unified CM, the Unified CM method cannot be used to monitor or record the call. Only the server capture method is supported for mobile agents.

Packet Capture Methods Used in Cisco Monitoring and Recording Software

Issue: The type of agent application used can dictate which capture method must be used.

Cisco monitoring and recording software can be configured to support different methods of capturing packets to support monitoring and recording. In some cases, the configuration or client software will dictate the type of packet capturing that must be used. This section summarizes the packet capture methods that can be used with the various Cisco products. This information is based on the latest versions of each product.

Cisco Agent Desktop

CAD comes in two versions: CAD for Unified Contact Center Enterprise (Unified CCE) and CAD for Unified Contact Center Express (Unified CCX). The Unified CCX version is targeted at small contact centers with fewer than 300 agents. The Unified CCE version is targeted at large contact centers with more than 300 agents. The two versions are virtually identical as far as their feature sets are concerned.

CAD supports live monitoring and on-demand call recording of agents. There are three CAD agent applications that can be deployed.

- **Cisco Agent Desktop**. Agent Desktop is a Windows-based application. It offers the most features of all the agent applications. Agent Desktop supports on-site agents, remote agents (using VPN), and mobile agents. It can also be run in a thin-client (Citrix or Microsoft Terminal Services) environment. Agent Desktop supports the live monitoring feature using the desktop capture, server capture, or Unified CM capture methods. It supports on-demand recording using the desktop capture or server capture methods.
- **Cisco Agent Desktop—Browser Edition (CAD-BE)**. CAD-BE is a Java-based version of Agent Desktop that runs in a web browser. It supports on-site agents, remote agents (using VPN), and mobile agents. CAD-BE supports live monitoring using the server capture and Unified CM capture methods, and

supports on-demand recording using the server capture method. Although the software runs on a PC, the Java code runs in a browser and does not have access to the system resources needed to support the desktop capture method.

- Cisco IP Phone Agent (IPPA). IPPA is a service application that runs on the IP phone itself to enable contact center agents who do not have PCs to function as CAD agents. It allows agents to take calls and set their agent state, but does not support many of the more advanced features found in the other agent applications. IPPA supports on-site agents and remote agents (using a hardware VPN). It supports live monitoring using the server capture and Unified CM capture methods, and supports on-demand recording using the server capture method.

Quality Monitoring

Quality Monitoring is a high-capacity call recording and agent evaluation tool. There is a single agent client application, Recording Solution Desktop Recording service, that runs on the agent's PC. Based on configured criteria, agent calls are recorded on the desktop or on a server and stored for later retrieval and review. Recording Solution can be run in a thin-client (Citrix or Microsoft Terminal Services) environment. Agent call recording is supported using the desktop capture, server capture, and network recording methods. For live monitoring, only the Unified CM method is supported.

This information is summarized in Table 3.

Table 3. Packet capture methods supported, by application

Product*	Client App	Agent Type	Feature	Capture Method		
				Desktop	Server	Unified CM
CAD	Agent Desktop	On-site	Monitoring	y	y	y†
			Recording	y	y	n
		Remote	Monitoring	y	y	y†
			Recording	y	y	n
		Mobile	Monitoring	n	y	n
			Recording	n	y	n
		Thin client	Monitoring	n	y	y†
			Recording	n	y	n
	CAD-BE	On-site	Monitoring	n	y	y†
			Recording	n	y	n
		Remote	Monitoring	n	y	y†
			Recording	n	y	n
		Mobile	Monitoring	n	y	n
			Recording	n	y	n
	IPPA	On-site	Monitoring	n	y	y†
			Recording	n	y	n
		Remote	Monitoring	n	y	y†
			Recording	n	y	n
Recording Solution	C1	On-site	Monitoring	n	n	y
			Recording	y	y	y
		Remote	Monitoring	n	n	y
			Recording	y	y	y
		Mobile	Monitoring	n	n	n
			Recording	n	y	n
		Thin client	Monitoring	n	n	y
			Recording	n	y	y

* Only supported application configurations are shown.

† With a supported hard IP phone and VPN hardware or supported version of Cisco IP Communicator soft phone.

NDIS-Compliant NICs

Issue: NICs that do not support promiscuous mode packet capturing will prevent monitoring and recording from working.

> **NOTE:** The Unified CM capture method of monitoring and recording does not depend on promiscuous mode to work. The information in this section pertains only to the desktop- and server-based capture methods.

In order for the packet capturing software to see the audio packets sent over the network by the phones, the NIC used by the software must support promiscuous mode packet capturing. If this mode is not supported, the phone's audio packets will not be seen by the software. This results in no sound when monitoring or empty files when recording a call and possible error messages that monitoring or recording has failed.

The only exception to this is if the desktop capture method is used and the agent has a soft phone. This is because the soft phone and the agent's PC share the same IP address, so an application running on the PC will be able to see the audio streams.

For the desktop capture method, the NIC is on the agent's PC. For the server capture method, the NIC is on the VoIP server and the one connected to the SPAN session destination port on the network switch.

In practice, the vast majority of available NICs support promiscuous mode packet capturing. In those that do not, there might be a workaround available from the manufacturer that will allow it to support this mode. If there is no workaround, the only other option is to purchase a NIC that supports this mode.

Agent Phones

Issue: Particular phone models might be required to support a selected capture method.

Depending on the capture method, there might be requirements for the model of Cisco IP phone that is used. These requirements are in addition to any set by the software concerning features other than monitoring and recording.

Desktop Capture Method

The hard IP phone used by the agent must be able to be daisy-chained to the agent's PC and be configured to send its audio streams to the PC so the packet capture software can capture and process the data. At a minimum, the phone must contain a second network connection that can be used to connect to the agent's PC. However, not all phones with this second connection can be configured to send its network traffic down to the PC.

The following phone settings must be enabled in Unified CM for desktop packet capture to work:

- PC Port. If this is not enabled, the second network port on the back of the phone will simply not work as a network connection for the user's PC.
- PC Voice VLAN Access. Voice and data traffic can be segregated into separate VLANs in order to best use the networking resources. If the user's PC and phone are daisy-chained, and the voice and data are separated into different VLANS, the cOomputer will be a device in the data VLAN and the phone will be a device in the voice VLAN. If this option is not enabled, no voice traffic will be sent out the second network port to the daisy-chained PC.
- Span to PC Port. If this is not enabled, the phone will not forward any network traffic to the daisy-chained PC.

NOTE: Not all versions of Unified CM have all three options. Enable those that do appear on the phone device configuration.

Server Capture Method

There are fewer restrictions regarding which IP phones can be used with this method. The main restriction is that it cannot be a wireless phone. In fact, if the agent is a mobile agent, there are no restrictions at all, since the software is sniffing a voice gateway port and using the IP address and port rather than a MAC address to identify audio streams.

Unified CM Capture Method

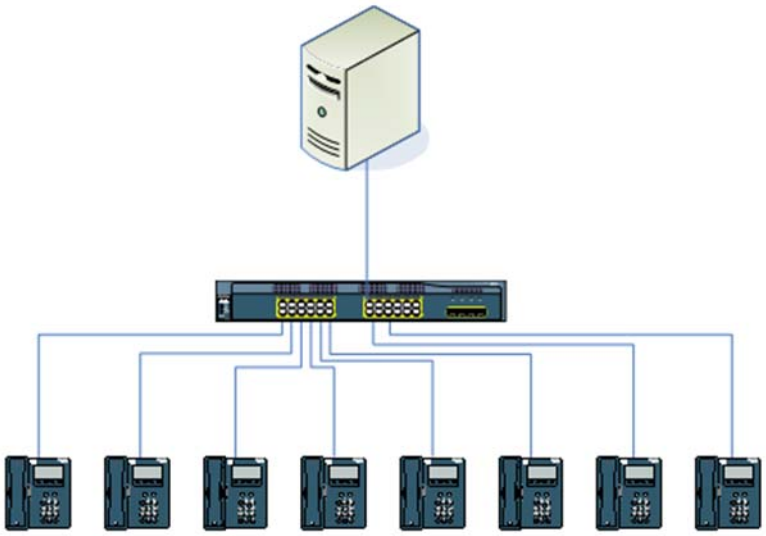
To support this feature in CAD and Recording Solution software, a supported IP phone must be used and configured correctly. The list of supported Cisco IP phones that can be used for each capture method are listed in Appendix B.

SPAN

Issue: The SPAN configuration is complex and must be done correctly for the server capture method to work properly.

The Cisco Catalyst line of IP network switches allows Switched Port Analyzer (SPAN) or port monitoring sessions to be configured. These sessions include a list of one or more switch ports or VLANs as the port monitor source and a single destination port. The switch copies all the packets traversing the source ports and sends them to the destination port. A server running packet capturing software is then connected to the switch using the destination port of the SPAN configuration (Figure 11).

Figure 11. Example of a port monitor configuration



In Figure 11, the eight IP phones are plugged into ports 1–8 on the switch. The server is plugged into port 9 and is running the packet capture software. SPAN is configured on the switch to use ports 1—8 as the source ports and port 9 as the SPAN destination port. When an agent uses one of these phones to take a call, both the incoming and outgoing audio streams for that call are copied and sent to port 9 where they can be retrieved and processed by the server software.

There are several issues with SPAN configurations that are purely logistical. In general, network technicians are very busy and it can be difficult to find one to configure the SPAN sessions. SPAN configuration is not a common activity, so it might not be done correctly the first time. When phones are moved or added to the switch, the SPAN configuration might need to change to include new or different ports. If this is not done in a timely manner, the customer will have monitoring and recording issues with those agent devices. Usually, those who administer the Cisco software and those who configure the network are in different departments, so communication about configuration activities between these two areas is important.

Most technical issues can be dealt with during deployment planning. Because switches only have a fixed set of ports that phones can connect to, other configuration options must be used to increase the number of phones assigned to a single VoIP server. It is also common to have the agent phones for a contact center spread among multiple switches, and even at multiple sites. Since it is expensive to have a VoIP server per switch, deployment planning must be done to properly use all the capacity of each VoIP server. Some of these options include RSPAN, VLANs, and Capture Location, which are discussed below.

For a list of Cisco switches that support SPAN or port monitoring, refer to Appendix A

RSPAN

Issue: The RSPAN feature is not supported on all switch models.

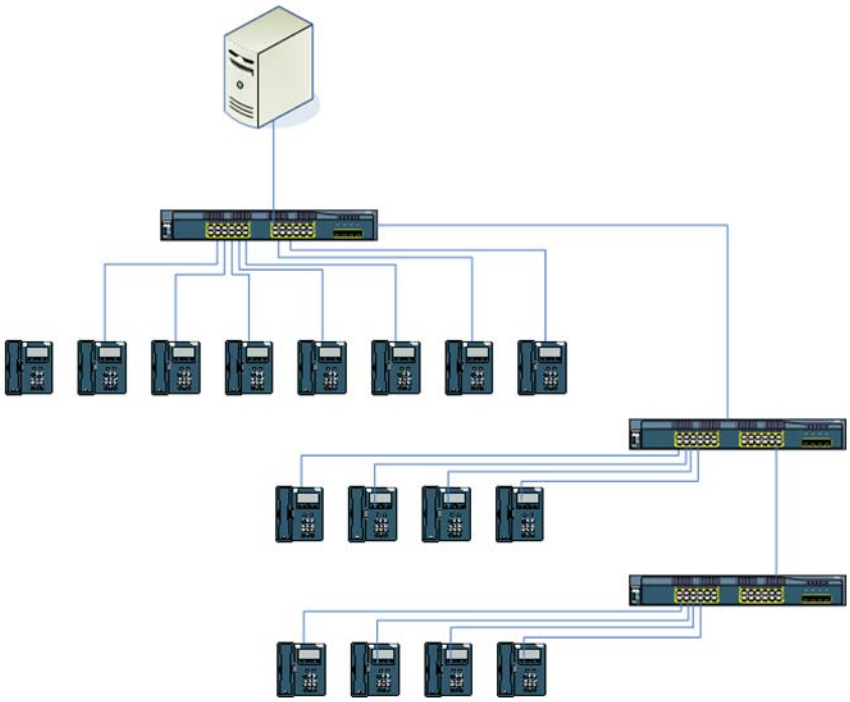
Because switches have a limited number of physical ports to which IP phones and computers can attach, most networks contain multiple switches. These switches are interconnected, either directly or through routers and gateways, to create the network. The Cisco monitoring and recording software that runs on the server can only capture from a single NIC adapter, so if more IP phones are desired as network sources than there are ports on the switch, you can either add another monitoring server attached to another switch where the phones are connected, or you can use the Remote Switched Port Analyzer (RSPAN) feature found on some Cisco Catalyst switches.

This is a quite common scenario in real-world Cisco software deployments. Customers do not like to change their network infrastructure to satisfy software applications. The software must be able to handle the network configuration.

An RSPAN configuration allows ports on different switches to be configured as source ports and delivered to a single destination port. The switches are connected to each other and network traffic from all the ports is sent to the switch with the destination port.

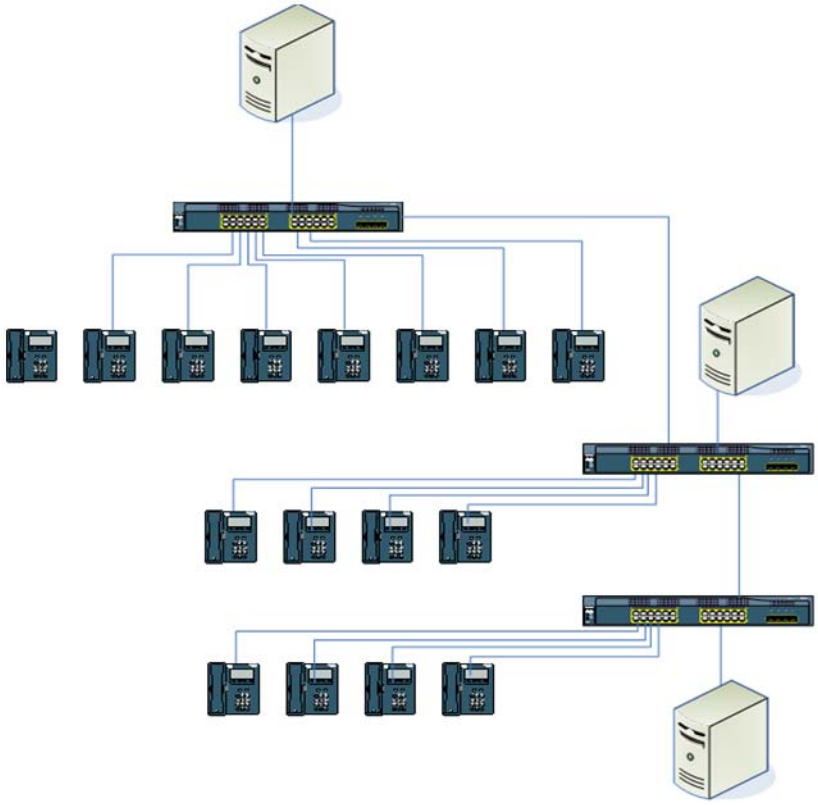
In Figure 12, we have a customer who has three network switches that are connected to each other. Agent phones are connected to all three switches and we want to be able to record their calls. If we assume that all the switches support RSPAN, we can configure an RSPAN VLAN and assign the ports on all the switches that have agent phones attached to this VLAN. On the switch with the Cisco monitoring server attached, we create a SPAN session that uses the RSPAN VLAN as the source and use the Cisco monitoring server port as the destination port. All voice traffic from the phones on all the switches is sent to the destination port where the audio streams can be separated, processed, and saved or forwarded to another PC for reviewing.

Figure 12. Using RSPAN to capture traffic from IP phones on multiple switches



If one or more of the switches in the network do not support RSPAN but have agent phones connected, the only other option is to add another VoIP Monitor server to the installation and connect it to the switch, configuring another SPAN session on that switch as shown in Figure 13.

Figure 13. Multiple switch configuration when RSPAN is not supported



SPAN and RSPAN can both be used in an installation and might be required due to switch models or RSPAN support.

For a list of Cisco switches that support RSPAN, refer to Appendix A.

VLANs

Issue: VLANs can be used to overcome network complexity if configured correctly.

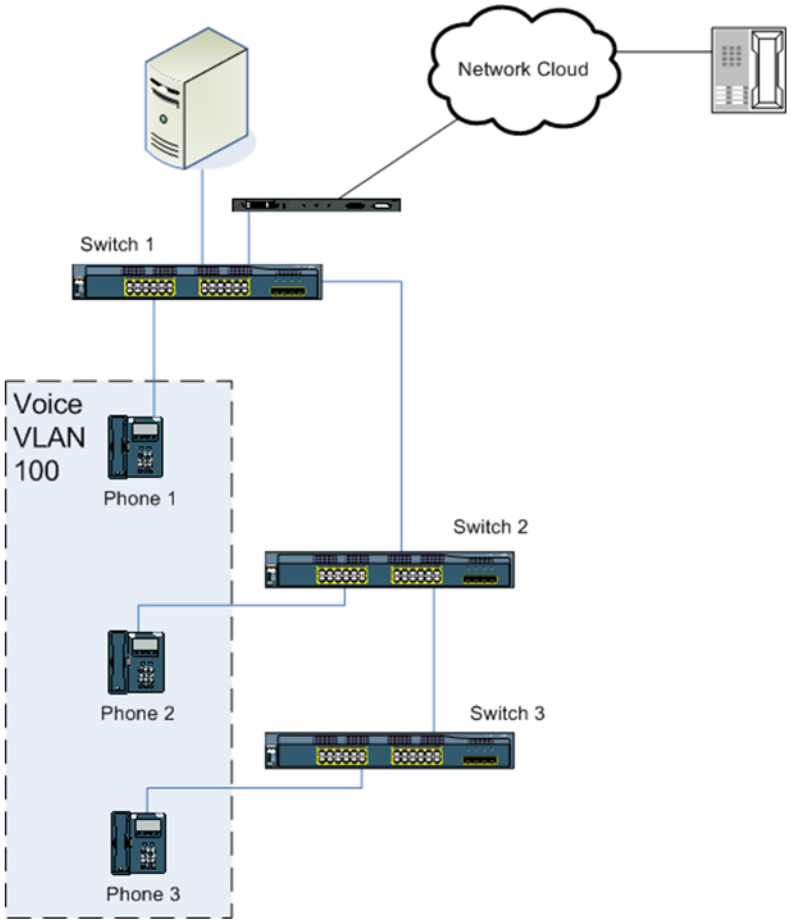
Virtual LANs, or VLANs, are an option for the source of a SPAN session. VLANs are groups of network devices (switch ports) that do not need to physically exist on the same switch. In the real world, it is common for the data traffic to be separated from the voice traffic of IP phone devices. These are usually referred to as *voice VLANs* and *data VLANs*. By doing this, you can reduce the amount of network traffic and also fine-tune Quality of Service (QoS) for audio traffic so your phone calls sound good.

A particular port can be part of more than one VLAN. This is necessary in a network where data and voice are separated by VLANs and an agent has a PC with a soft IP phone installed. In this case, the PC needs access to both normal network data and

audio streams when the agent is on a call. When SPAN is configured and uses a VLAN as a source, the voice VLAN is the one that is selected so only voice traffic is sent to the VoIP server for processing. There are other reasons for using voice VLANs in SPAN configurations as discussed in the section, "Server Capacity" on page 46.

In Figure 13, all the IP phones connected to the three switches shown could be grouped into a VLAN that only carries voice traffic. We could call this Voice VLAN 10. If SPAN is configured on the top switch to use VLAN 10 as the source of network traffic, any voice traffic sent or received by a port that is part of VLAN 10 *that traverses the top switch* will be copied and sent to the SPAN destination port. The emphasis in the previous sentence is very important. Just because we include a port on the bottom switch as part of VLAN 10 does not mean that the top switch will automatically see all its traffic like an RSPAN configuration. It is captured only if the phone is sending packets that hit the top switch. This is also the case if the phone on the bottom switch was on a call with an IP phone connected to the top switch. It also works if the phone on the bottom switch is sending packets through the top switch to a connected gateway, router, and so on. This is illustrated in Figure 14.

Figure 14. Limitations of spanning VLANs



Assume that the three IP phones, each connect to a port on a different switch and are all part of voice VLAN 100. The VoIP Monitor server is connected to switch 1. SPAN is configured on switch 1 to copy all the network traffic for the devices in VLAN 100 to the port connecting the VoIP Monitor server.

If phone 3 calls phone 2, the voice traffic flows between the devices and switch 2 and switch 3. Since this traffic does not go through switch 1, the VoIP monitor server does not see that audio traffic.

If phone 3 calls phone 1, the VoIP Monitor server sees the audio traffic for phone 3 because the traffic flows through switch 1 to get to phone 1.

Similarly, if phone 3 receives a call from an external phone as shown in Figure 14, the traffic flows:

1. from the remote phone through the network cloud to a voice gateway
2. through switches 1, 2, and 3, and finally
3. to phone 3.

Audio packets leaving phone 3 take the reverse route. Since the audio packets traverse switch 1, the VoIP Monitor server sees the audio packets for phone 3.

For some switches, there is a requirement that the SPAN destination port be a member of the same VLAN as the source ports of the SPAN configuration. These switches are shown in Appendix A.

Port Traffic Direction

Issue: Some SPAN configurations lead to duplicate streams and bad audio quality.

There is a subtle issue that is exposed in the example above when phone 3 and phone 1 are on a call with each other. Since both phones are part of the same VLAN, and that VLAN is a source for the SPAN session, the VoIP Monitor server receives duplicate audio packets, which results in very poor audio quality.

By default, when a switch port is configured as a SPAN source port, the SPAN session copies all the packets going to and coming from that port to the SPAN destination port. This is not always the desired behavior. When you have two agent devices that are part of the same SPAN configuration on a call with each other, and their call is recorded or monitored, the resulting audio quality is very bad. The agent voices sound slow and slurred. This is because the VoIP Monitor service is seeing each audio packet twice.

Figure 15. Capturing ingress and egress traffic for two devices in the same SPAN configuration

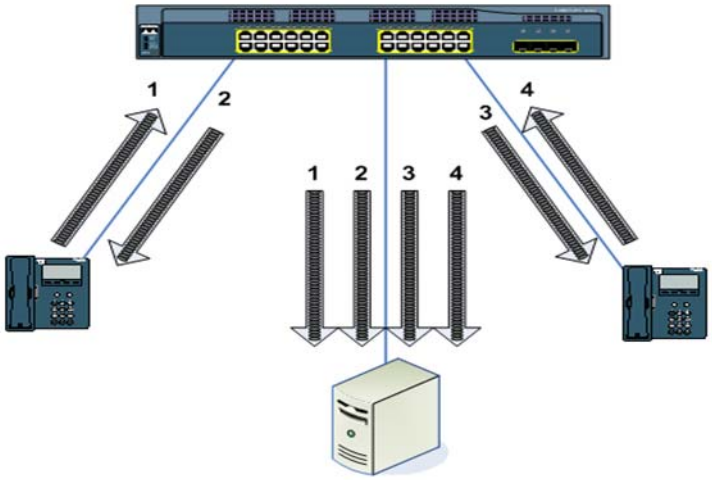
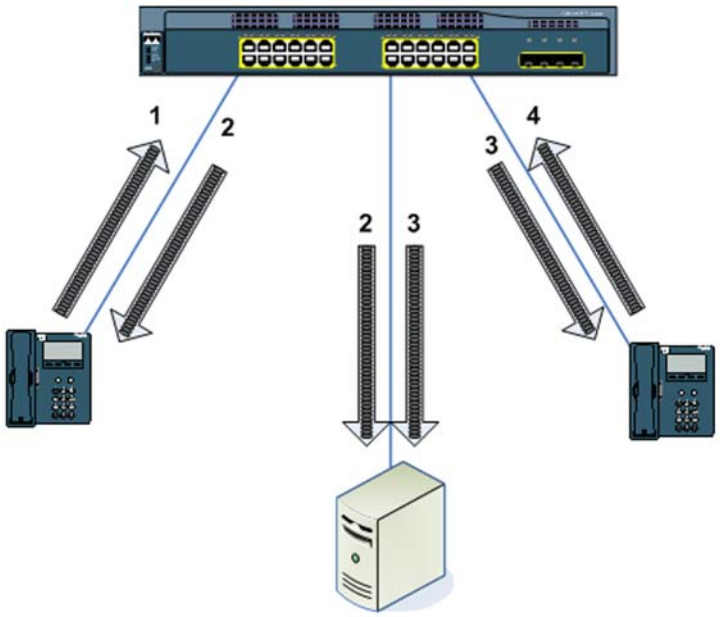


Figure 15 shows the To-Agent and From-Agent audio streams for two IP phones connected to the same switch, where both phone ports are source ports for a SPAN configuration. During a call between these two devices, the packet streams entering and exiting a SPANned port are copied to the SPAN destination port. We see that streams 1 through 4 are copied and sent to the VoIP Monitor server. The problem is that the audio data in stream 1 is identical to the audio data in stream 3. Stream 4 contains the same audio data as stream 2. In this case, each audio packet is seen twice by the software on the VoIP Monitor server.

Network traffic arriving at a switch port is called ingress traffic, and packets leaving a port are called egress traffic. When SPAN is configured on a switch, the session can be set up to capture both ingress and egress traffic, egress-only traffic, or ingress-only traffic. (Some switches do not support ingress-only or egress-only options. See Appendix A for details).

If the SPAN session shown above is reconfigured to capture only egress traffic, the VoIP Monitor software then only sees each stream once as it exits the SPAN source port, as shown in Figure 16.

Figure 16. Capturing egress-only traffic for two devices in the same SPAN configuration



As can be see in Figure 16, only the audio streams exiting the IP phone's switch port are copied to the SPAN destination port. Alternately, the SPAN can be configured to capture only ingress traffic. In that case, streams 1 and 4 are copied to the VoIP Monitor server.

This situation can occur for SPAN configurations using VLANs for sources and for RSPAN configurations. Any time that two or more phone devices (including soft IP phones) are part of the same SPAN configuration delivering audio data to a single VoIP Monitor service, it will see duplicate audio packets and result in poor audio quality for recording or monitoring.

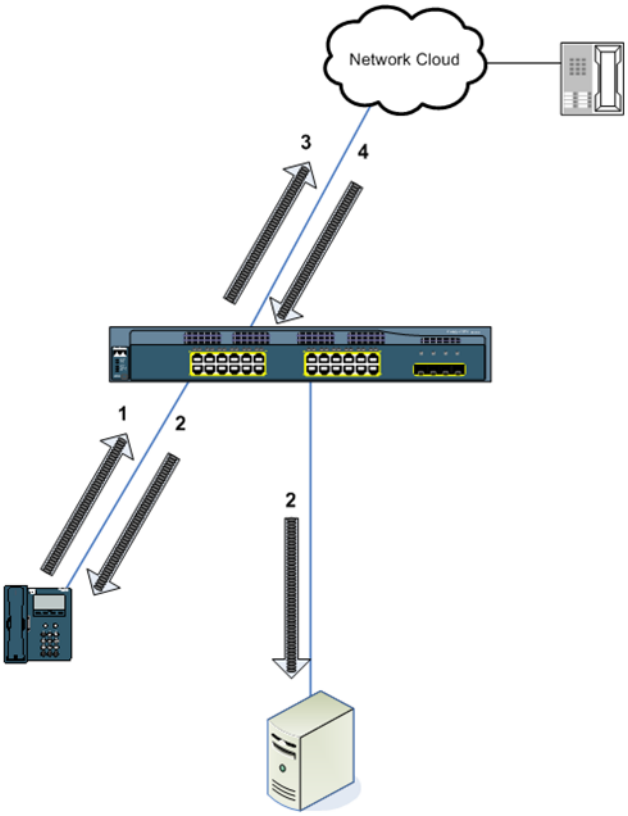
This is an important aspect to understand because it has ramifications for switch configuration and the number of VoIP Monitor servers required for a Cisco software installation.

SPAN configurations are something that are set up once and not changed very often. If we take the network layout shown in Figure 14, with SPAN configured to use VLAN 100 for the source ports, and capturing both ingress and egress packets, calls between phone 1 and phone 2, or phone 1 and phone 3 will sound bad due to duplicate packets, but calls between any of the phones and external callers will sound good.

If we change the SPAN configuration to capture only egress packets, calls between the phones will sound good, but calls between a phone and an external caller will only contain a single audio stream (the To-Agent stream). This is because only the audio

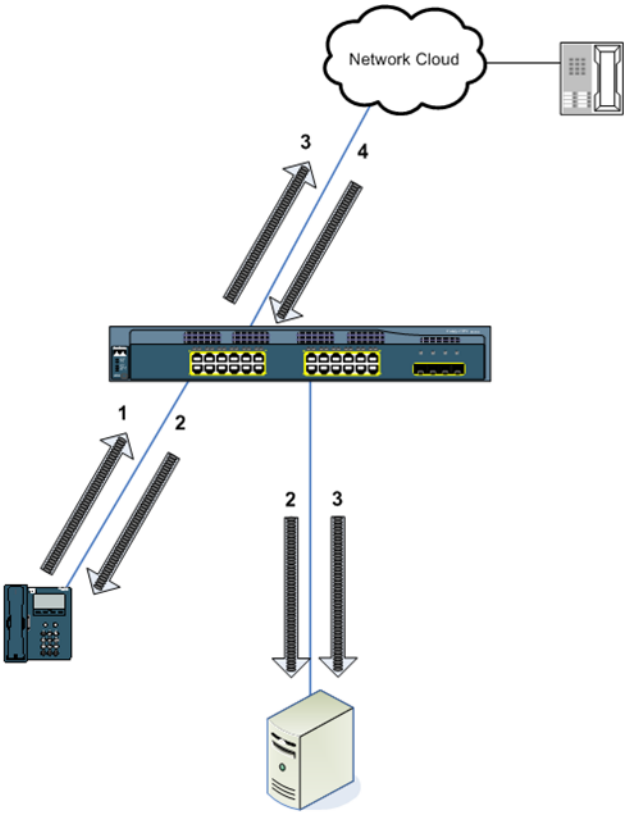
stream with the external caller's voice is exiting the phone's switch port. The agent's voice stream is coming into the phone's port and is ignored due to the egress-only SPAN setting. This is shown in Figure 17.

Figure 17. Egress-only SPAN issue for non-monitored port



In Figure 17, audio stream 2 is the only stream of packets that is going out of the phone's port that is part of the SPAN configuration, so it is the only stream that is sent to the VoIP Monitor server. The way to fix this issue is to add the switch port that connects the external phones to the SPAN configuration (Figure 18). This port is usually connected to a voice gateway device that is used to convert analog phone calls to IP-based phone calls.

Figure 18. Ingress-only SPAN issue resolution



In Figure 18, the SPAN configuration (using egress-only) was changed to include the port used to connect phones from the network cloud. Now we are able to see both audio streams that make up the call between the internal agent and external caller. Stream 3 is the agent's voice that exits the switch port connected to the external network. Stream 2 is the caller's voice that exits the switch port connected to the agent's phone.

In summary, any time two device ports are part of the same SPAN configuration, calls between these two devices will result in packet duplication and bad audio quality unless the SPAN is set to use ingress-only or egress-only packets.

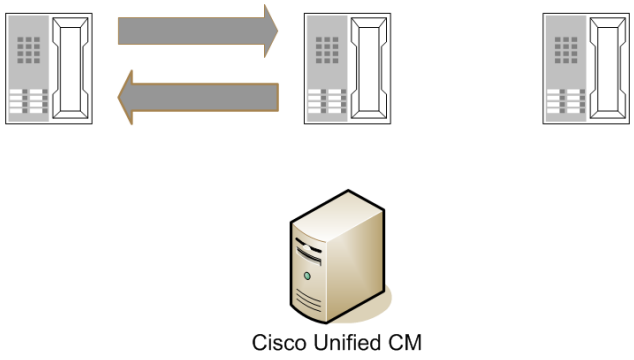
Media Mixing

Issue: Failure to capture the Unified CM port can lead to loss of audio for conference calls.

IP phone calls always consist of two audio streams, as shown in Figure 19, but calls might contain more than two parties. When calls are conference calls, several

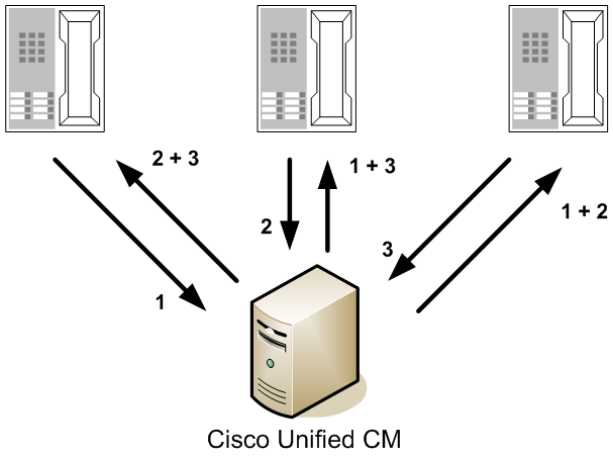
different parties can be on the same call. How does this look to the packet capturing software?

Figure 19. Audio streams for a two-party call



In a normal two-party call, the phones send their stream directly to the other device over the network. Whenever a call is made into a conference call by adding parties, Cisco Unified CM software is responsible for merging the audio data from multiple parties so the phones that are part of the conference call still only see two streams. This is done through a media mixer or media blender software component (Figure 20).

Figure 20. Blended audio streams on a conference call



When a conference call is created, the Unified CM tells each phone that is on the call to send its outgoing audio stream to the media blender component (usually running on the Unified CM server). In Figure 20, the media blender receives three streams (1, 2, and 3), one from each of the phones. It blends the necessary audio streams into a single stream and sends it out to the phone on the call. Stream 2 and 3 are merged and sent to the first phone. Streams 1 and 3 are merged and sent to the second phone. Finally, streams 1 and 2 are merged and sent to the third phone.

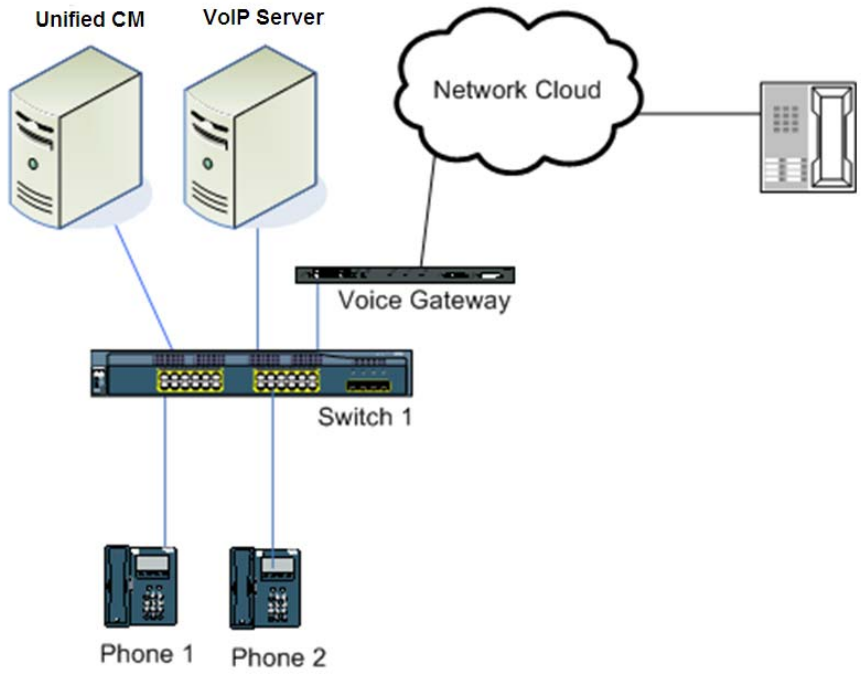
The important point here is that the audio streams sent out by all the phones on the conference call are directed to the Unified CM server port rather than directly to the other phone. The streams that arrive at the IP phones now come from the Unified CM port rather than from another phone directly. This is important if gateway SPAN sniffing is being used.

Gateway SPAN Sniffing

Issue: Agent-to-agent calls are not captured.

If agent-to-agent calls will not be monitored or recorded, gateway SPAN sniffing can be used.

Figure 21. Gateway SPAN sniffing



SPAN can be configured to include only the port used by the voice gateway and the Unified CM (getting both ingress and egress packets). All calls between agents and external callers will traverse the voice gateway port and can be captured by the VoIP Monitor server.

Agent-to-agent calls are not captured unless an agent is on a call with an external caller and the agent conferences another agent into the call. When this occurs, the Unified CM mixes the audio streams, and the streams are captured by the VoIP server. The Unified CM port must be part of the SPAN source ports or the agent streams are lost when the call is conferenced.

In the configuration shown in Figure 21, the same SPAN configuration would work for 1, 4, or 48 phones connected to the switch.

When you look at this example, you might note that, by capturing both ingress and egress packets on both the voice gateway and the Unified CM port, duplicate streams will be captured. The monitoring software, however, is only looking for packets whose MAC address (for CAD) or IP address and port (for Recording Solution) are shown as the source or destination of the packet. If the Unified CM is mixing the streams and sending them out, the source MAC/IP/port does not match the agent's device, so they are ignored by the software. The result is that we process the streams between the agent phone and the Unified CM during the conference.

Trunk Port Monitoring

Issue: Using VLAN filters for SPAN source ports that are trunk ports can reduce traffic to the VoIP server.

In some installations, it might be necessary to include a trunk port as a source port for a SPAN configuration. A trunk port is a port configured to connect two switch devices directly. Trunk ports are different from normal device ports in that they carry all VLANs. A trunk port cannot be a member of a VLAN, which is a method of restricting network traffic on a port. Because of this, if a SPAN configuration includes a trunk port as one of the source ports, all traffic from all VLANs that traverse the port are copied to the SPAN destination port. This might not be desired if that traffic includes non-audio traffic that is of no interest to the VoIP service. It might also reduce the capacity of the VoIP service due to the amount of unnecessary traffic being processed by the service.

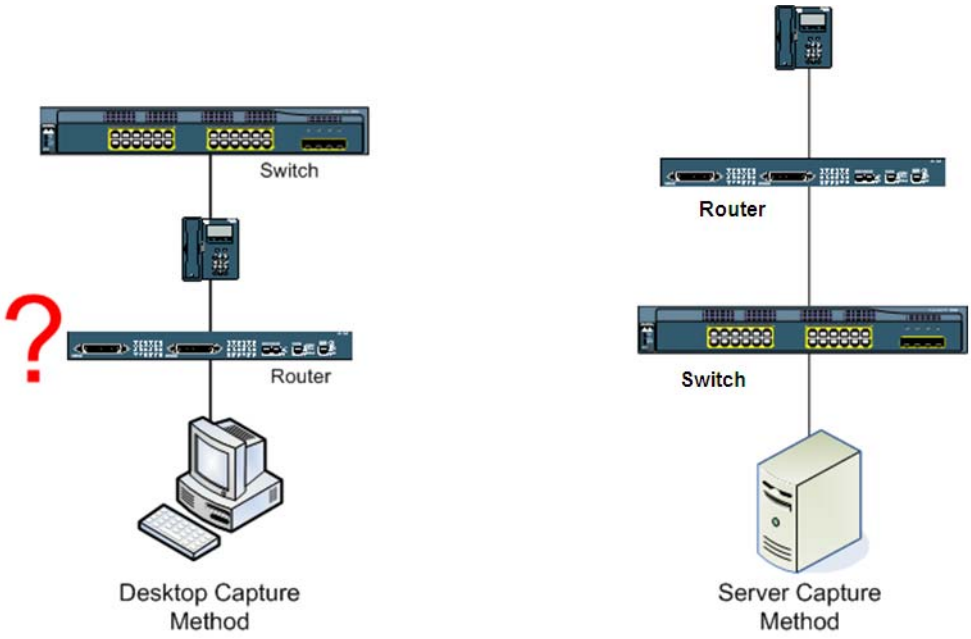
When a trunk port is used as a SPAN configuration source port, some switches allow VLAN filtering on the port. This means that the trunk port is indicated as a SPAN source and only network traffic over the VLAN IDs indicated in the filter are copied and sent to the SPAN configuration destination port. The restriction to this is that you must use ports for SPAN sources when a VLAN filter is used. You cannot use any VLAN IDs as sources of the SPAN. Conversely, if you use a VLAN to indicate the source of a SPAN configuration, you cannot use VLAN filtering. The switches that support VLAN filtering are shown in Appendix A.

MAC Address Changes Due to Layer 2 Routing Devices

Issue: Monitoring and recording do not work when Layer 2 routing devices are between the packet capture software and the IP phone.

This issue affects audio capture methods where MAC address filtering is used (CAD only) and there exists a Layer 2 routing device between the IP phone and the software that is capturing audio packets

Figure 22. Invalid hardware configuration

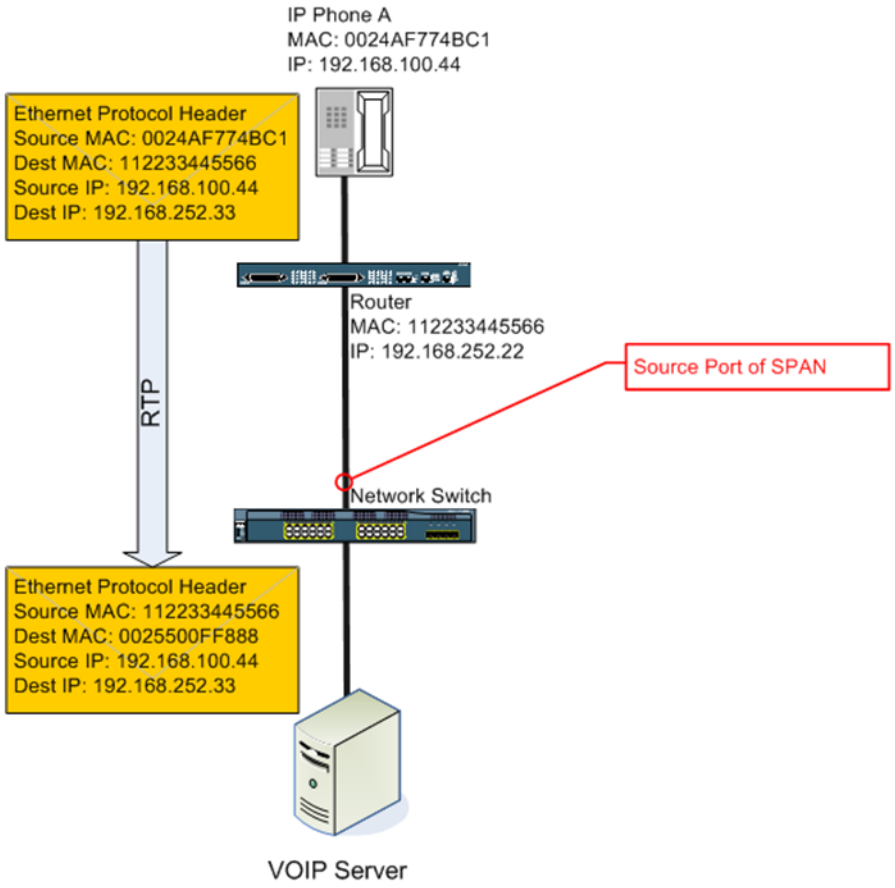


A Layer 2 routing device is any networking hardware that changes the MAC address of a packet as it traverses the network. Routers, gateways, bridges, and hubs are all examples of Layer 2 routing devices. Just about anything other than a network repeater will cause the MAC address of packets flowing through it to change.

It is unusual to see a hardware configuration where a router is found inline between the agent desktop and the agent's phone as shown on the left in Figure 22. It is more likely to be seen when the packet capture software is running on the VoIP Monitor server. Some networks are very complex and it might not be easy to tell if an IP phone is connected directly to the switch or not.

If this configuration is used, MAC address filtering will fail, resulting in no audio for monitored or recorded calls. The reason is that packets being sent over a network will always use the source MAC address of the network device sending the packet and the destination MAC of the next network device along the way toward the packet's destination. The source and destination IP address and port will not change, though, unless it hits a device using NAT or PAT (Figure 23).

Figure 23. MAC address alteration by network routing



To illustrate this, Figure 23 shows an IP phone connected to a router, then connected to a switch. A VoIP server is connected to the same switch and SPAN is configured to capture traffic on the port to which the router is connected. When on a call with another phone, the phone sends out a packet of audio data addressed to the other IP phone at 192.168.252.33.

The VoIP server knows that the MAC address of the agent phone is 0024AF774BC1, so it sets its packet filter to grab only those audio packets where the source or destination MAC address in the Ethernet header match 0024AF774BC1. The RTP packet sent from the phone has the correct source MAC address, but the destination MAC is not that of the other phone—it is the router's MAC address, which is the next hop of the packet to be routed to the other IP phone. When the router routes the packet, it is now the sender of the packet and the source MAC address is set to that of the router. Routers are layer-2 devices, so they will change MAC addresses, but not IP addresses, which are layer-3 entities.

When the SPAN session copies the packet that hits the port it is monitoring and sends it to the VoIP server port, the packet capturing software looks at the packet's source and destination MAC address. Since the source MAC was changed to 112233445566, the software discards the packet. This continues and the packet capturing software never sees an audio packet that contains the MAC address it is looking for.

> **NOTE:** Using IP addresses and ports for packet filtering will work normally under these configurations.

Server Capacity

Issue: Large numbers of agents require multiple VoIP servers.

VoIP server software has limits to the amount of network traffic it can analyze before it starts to lag. This is a CPU resource issue, so using faster CPUs or multiple CPUs in the server will modify this. Published capacity numbers include the hardware specifications of the machine that the software was tested on.

There can also be limitations on the number of simultaneous calls that can be processed by a single VoIP server. These limitations are software-based in that the software has a limit that it will enforce by not accepting more work than it is configured to do.

These two limitations are a major factor when planning large deployments because it dictates to some extent the server count, the capture methods used, and the locations of the VoIP servers.

Because capacity numbers for Cisco software can change with new software releases, this document contains no official capacity numbers. Capacity numbers for illustrative purposes only are used in the deployment examples (see "Examples of Deployment Planning" on page 48).

> **NOTE:** CAD has software-enforced capacity limitations. Recording Solution does not have these limitations.

Number of SPAN Sessions

Issue: Limits on the number of SPAN sessions can affect VoIP server placement and count.

Cisco switches cannot support an unlimited number of active SPAN configurations. Some switches can support only a single SPAN session. In this case, it is not an option to connect more than one VoIP server to a single switch. Appendix A lists the number of SPAN sessions supported by various models of Cisco switches.

Network Traffic Restrictions on Destination Ports

Issue: Some switches do not support normal network traffic on SPAN destination ports.

Normally, a computer or phone connects to a switch port and that port is used to send and receive data from the network. On some switches, a port used as a destination of a SPAN configuration cannot be used to send or receive network traffic (other than the traffic sent to the port by the SPAN configuration). When this is the case, the VoIP server must use two NICs; one for normal network traffic, and a second for receiving copied packets from the SPAN configuration. Each NIC is connected to a different port on the switch. The VoIP software is told which NIC to use for capturing audio packets from the SPAN configuration.

If there is a reason why the VoIP server cannot contain more than one NIC, then the VoIP server cannot be connected to this switch in order to support monitoring or recording. It will need to be connected to a switch that does support both SPAN and normal network traffic on the SPAN destination port, or another capture method such as desktop capture must be used.

The switches that do not support normal network traffic on SPAN destination ports are shown inAppendix A.

Switch Operating System Version

Issue: Some SPAN-related abilities depend on the IOS version.

We have shown many switch capabilities related to SPAN configurations, and these are largely dependant upon the switch model, but switches are computing devices and run operating systems that change and increase in functionality over time. Certain features, such as SPAN, were not available on some switches at one point in time. As their operating system software was improved, this feature was added. The information shown in Appendix A related to switch capabilities is accurate for the latest OS versions available for those switch models. If a customer has a switch with an older operating system, a particular feature related to SPAN might not exist even though it is shown as being available in Appendix A.

For definitive information on switch capabilities, refer to the switch documentation or online documentation on the Cisco web site (www.cisco.com).

Examples of Deployment Planning

This section brings the information previously discussed together and applies it to the task of planning a deployment of Cisco software that includes VoIP capturing software to support monitoring and/or recording.

The first thing to do is gather information about the customer's contact center and the desired functionality of the Cisco software. The answers received from the customer on the questions listed below will help guide the deployment. These questions are used to assess the number of VoIP servers required based on server and software capacity. They will also lead to decisions on the proper capture method(s) used and required SPAN configurations.

Table 4. Contact center questionnaire

Question	Answer
How many agents do you have?	
How many agents will be monitored?	
How many agents will be recorded?	
How many non-agents will be recorded?	
What is the maximum number of agents that might be logged in simultaneously?	
How many agents are local to the contact center site?	
How many remote agents do you have?	
How many mobile agents do you have?	
How many agents have a desktop PC that will run the Cisco monitoring and recording software?	
How many agents have only an IP phone?	
How many contact center sites are there?	
Is agent-to-agent recording or monitoring required?	
Do agents with desktops share a network connection with their IP phone?	
How many agents use soft IP phones on their desktop?	

The next step is to get some information about the customer's network infrastructure that will host the Cisco software. If you can, get a network diagram that shows the network switches (and their model numbers), the current or proposed servers running the Cisco Unified Contact Center software, the voice gateways, routers, and IP phones, the task of planning will be much easier.

In the examples below, several fictional customer deployments will be examined as a Cisco software deployment is planned.

Example 1: ABC Company Deployment

Scenario: Small, simple deployment

ABC Company is a small company that has a contact center with 10 agents. These agents are all on-site, have PCs at their workstations, and use Cisco IP phones. They are currently deploying the Cisco Unified Contact Center Express software to help manage their agents and handle call queuing.

The customer is purchasing CAD and Recording Solution. CAD will be used to manage the agents and automate common tasks. They will use the CAD live monitoring feature, but not the on-demand recording feature. Recording Solution is being used to record calls to evaluate and train the agents.

We interview the customer to get information on how they will be using the software for monitoring and recording and get the following answers.

Table 5. ABC Company questionnaire

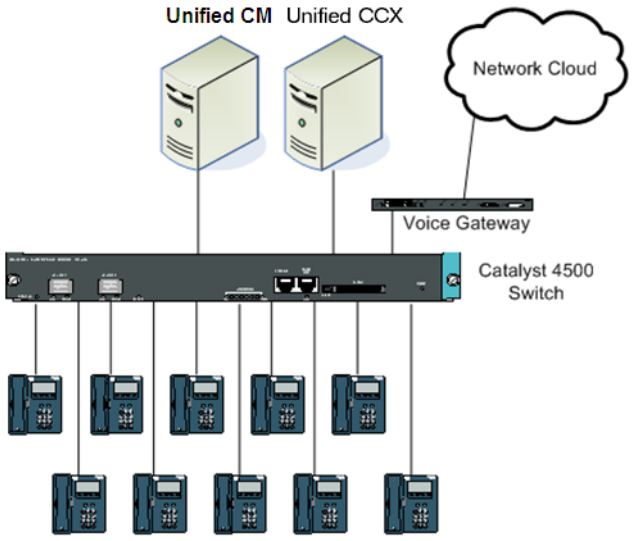
Question	Answer
How many agents do you have?	10
How many agents will be monitored?	10
How many agents will be recorded?	10
How many non-agents will be recorded?	0
What is the maximum number of agents that might be logged in simultaneously?	10
How many agents are local to the contact center site?	10
How many remote agents do you have?	0
How many mobile agents do you have?	0
How many agents have a desktop PC that will run the Cisco monitoring and recording software?	10
How many agents have only an IP phone?	0
How many contact center sites are there?	1
Is agent-to-agent recording or monitoring required?	Yes
Do agents with desktops share a network connection with their IP phone?	Yes
How many agents use soft IP phones on their desktop?	0

The preferred capture method is desktop capture because it is the easiest to configure and deploy. Since they don't have any mobile agents and their agents have PCs daisy-chained with their IP phones, we should be able to use desktop monitoring for all the agents.

An alternate approach is to use Recording Solution network recording (if ABC Company purchases Recording Solution as well as CAD). Configuration is more complex on the Unified CM, but it works well, and is a better choice if there are any issues with NICs on agent desktops not working correctly in promiscuous mode.

ABC Company's network diagram is shown in Figure 24.

Figure 24. ABC Company network diagram



In order to support the desktop capture method, we need to verify that the hardware supports the method.

Since the IP phones and PCs are already daisy-chained, we know that the IP phones have a second network port and can be configured in the Unified CM to send their voice traffic down to the agent's PC for capture.

The only other requirement we need to check is whether the NICs on the agents' PCs support promiscuous mode packet capturing. If the NIC is a known supported card then we are finished. If the NIC is unknown to support promiscuous mode, we can run tools to verify whether the NIC can capture in promiscuous mode. Assuming we find that the NICs do support promiscuous mode packet capturing, we can deploy the software using the desktop capture method for all agents.

If we find that the agent phones do not support Unified CM monitoring and recording, and the NICs do not support promiscuous mode packet capture, we have two choices:

we can buy and install supported NICs in all the agent machines, or we can choose to use the server capture method instead. To do this, we can set up a single SPAN configuration on their Catalyst 4500 switch to use all the IP phone ports as source ports and the port used by the VoIP server as the destination port.

Example 2: International Sprockets Deployment

Scenario: Multi-site contact center with remote agents

International Sprockets is a company that consists of a main office with hundreds of small shops scattered across the country. Each shop is able to take calls related to sprocket orders and answer questions about their inventory. Because of this, each branch is treated as an agent. The headquarters contains a contact center with 20 agents on site. When a caller calls in, the call is routed to the branch office nearest to the caller's location. If that branch's agent cannot handle the call, it is transferred to the main contact center. Each branch has a PC that will run Recording Solution and have a hard IP phone. The branches are connected to the main office using Cisco 831 VPN routers.

Due to regulations, all agent calls need to be recorded and stored. The customer has chosen Recording Solution to record all its agent calls. We'll start with the interview and get a network diagram from the customer.

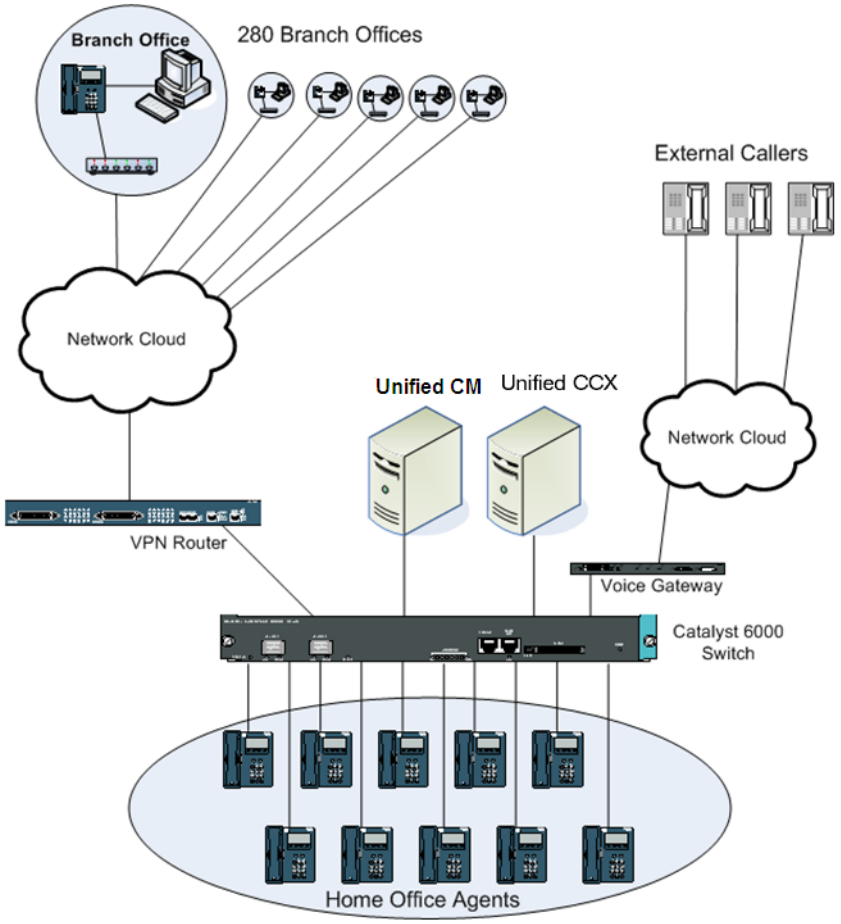
Table 6. International Sprockets questionnaire

Question	Answer
How many agents do you have?	300
How many agents will be monitored?	0
How many agents will be recorded?	300
How many non-agents will be recorded?	0
What is the maximum number of agents that might be logged in simultaneously?	300
How many agents are local to the contact center site?	20
How many remote agents do you have?	280
How many mobile agents do you have?	0
How many agents have a desktop PC that will run the Cisco software?	300
How many agents have only an IP phone?	0
How many contact center sites are there?	280
Is agent-to-agent recording or monitoring required?	Yes
Do agents with desktops share a network connection with their IP phone?	Yes

Table 6. International Sprockets questionnaire (cont'd)

Question	Answer
How many agents use soft IP phones on their desktop?	0

Figure 25. International Sprockets network diagram



Although the agents in the branch offices are widely scattered geographically, the network is still fairly simple. Recording Solution supports both desktop and server capture methods for remote agents using VPN connectivity. Since desktop packet capturing is easier to configure, it is chosen for this deployment.

After verifying that the agents' PCs have NICs that can use promiscuous mode, we can move ahead with the deployment.

Although network recording is supported for Recording Solution in this case, it is not the preferred implementation due to the geographical distance between the agents'

phones and the Recording Solution network recording server and concern over the WAN bandwidth between the phones and server. If necessary, due to incompatible NICs at the branch offices, a small number of agents could be configured to use network recording.

Example 3: Redundant Systems Inc. Deployment

Scenario: Complex network and Citrix environment with mobile agents in a Unified Contact Center Enterprise system

Redundant Systems has its offices in a multi-floor building in Los Angeles. The agents for their contact center are scattered among four floors. Most of these agents have PCs and are using soft IP phones. The software these agents run is via a Citrix server. Eight of the agents have only IP phones and no PCs. There are three agents who are always traveling and use their cell phones and laptop computers to contact the office. Three hours each day, these mobile agents are required to be available for taking calls to answer questions about the company's products.

The customer is very sensitive to network outages, so has installed a complex network system built for redundancy and fail-over. This network complexity can lead to complexities in the Cisco monitoring and recording software deployment if the server capture method needs to be used.

The customer already has Cisco Unified Contact Center Express installed. This includes CAD. Currently, only the IPPA agents are configured for monitoring and recording using the server capture method. The customer wants to add Recording Solution for all agent recordings, both for archiving and for agent evaluations. The information we have for the deployment is shown below.

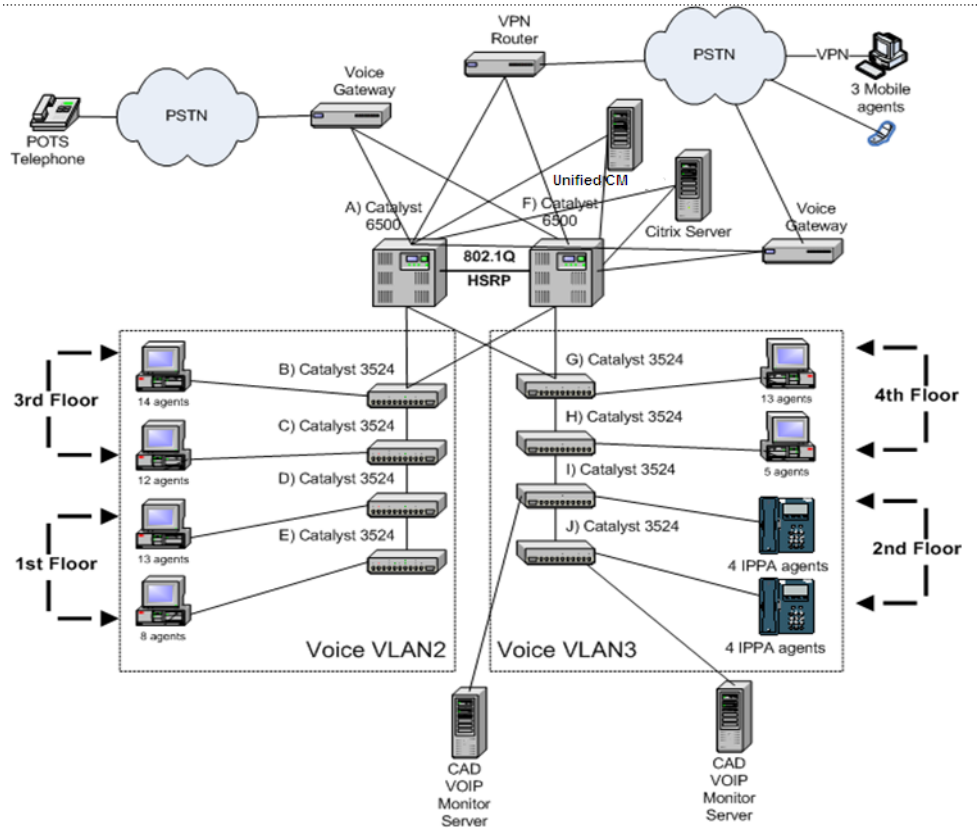
Table 7. Redundant Systems questionnaire

Question	Answer
How many agents do you have?	75
How many agents will be monitored?	26
How many agents will be recorded?	75
How many non-agents will be recorded?	0
What is the maximum number of agents that might be logged in simultaneously?	75
How many agents are local to the contact center site?	72
How many remote agents do you have?	0
How many mobile agents do you have?	3
How many agents have a desktop PC that will run the Cisco software?	67
How many agents have only an IP phone?	8

Table 7. Redundant Systems questionnaire (cont'd)

Question	Answer
How many contact center sites are there?	1
Is agent-to-agent recording or monitoring required?	Rec: Yes Mon: No
Do agents with desktops share a network connection with their IP phone?	Yes
How many agents use soft IP phones on their desktop?	64

Figure 26. Redundant Systems network diagram



We also find out that

- Only the agents on the third floor will be monitored.

- The Catalyst 6500 switches are redundantly connected. Only one is active at any one time. If one switch goes down, the other switch becomes active immediately. Any VoIP servers used for recording calls will also need to be redundant.
- The agents with PCs have NICs that are NDIS compliant and support promiscuous mode packet capturing.
- The current installation includes two CAD VoIP Monitor servers as shown in Figure 26. These will be removed and replaced with Recording Solution VoIP servers for any server-based captures used for recording calls.

Based on the information we have, we can plan for the following:

- Desktop capture cannot be used for the agents for the following reasons:
  - The 64 agents with PCs and soft IP phones will be running CAD and Recording Solution from the Citrix server. Since the applications are not running on agent PCs, we cannot use the desktop capture method for them.
  - The eight IPPA agents have no PCs, so we can not use the desktop capture method for them.
  - The three mobile agents are using cell phones that are not connected to their laptops, so we can not use the desktop capture method for them.
- One or more CAD VoIP servers will be required to monitor the agents on the third floor (since desktop capture cannot be used for these agents).
- The number of agents and possible simultaneous recordings does not exceed the capacity of a single VoIP server.
- A second Recording Solution VoIP server will be required to satisfy the customer's recording redundancy concern.

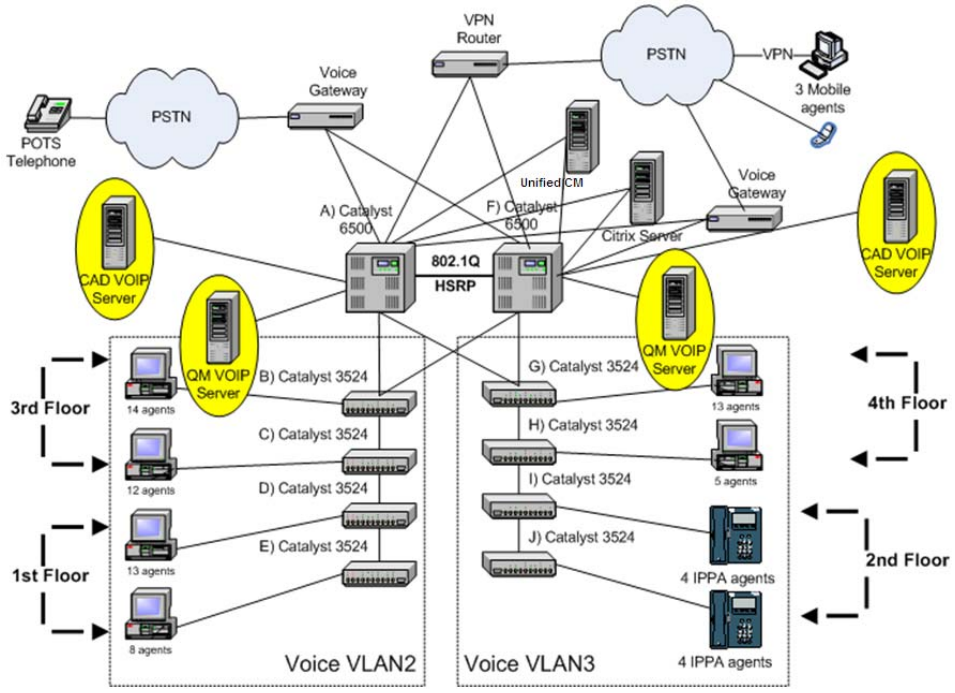
Because of the complexities of the network, the preferred solution is to use Recording Solution and Unified CM recording and monitoring. If the agent phones support this feature, this option is ultimately easier to configure and would only require a single Recording Solution network recording server to support all the agents.

The second possible solution is to use server recording and connect a Recording Solution VoIP server to each of the core 6500 switches and configure SPAN on those switches. But this does not allow the recording of agent-to-agent calls, which is required.

Our next option is to try to use RSPAN across all the Catalyst 3524 switches to copy the traffic up to the core switches. Checking our documentation, we see that the Catalyst 3524 switch will support RSPAN, ingress- or egress-only captures, and can use VLANs for SPAN sources. This will allow us to add our Recording Solution VoIP

servers to the core switches as shown in Figure 27.

Figure 27. VoIP server deployment at Redundant Systems



An RSPAN VLAN is created that includes all the ports that are also in voice VLAN 2 and 3. We will use this RSPAN VLAN in the SPAN sessions we will create.

The mobile agents will be configured as specified for each Cisco product. The required configuration has the mobile agent calls coming through one or more voice gateways that are separate from the gateways used for incoming customer calls. A VoIP server is associated with one or more gateways used by the mobile agents, and is able to extract the mobile agent calls flowing through the voice gateway.

On the two Catalyst 6500 core switches, a SPAN session is configured that uses the RSPAN VLAN and the mobile agent voice gateway as the source, and the port used to connect the Recording Solution VoIP server to that switch as the destination. Only the Recording Solution VoIP server that is attached to the active Catalyst 6500 switch will be used for recording agent calls.

Now we need to plan VoIP servers for CAD monitoring of the agents on the third floor. We have a few options for server placement. Since agent-to-agent calls are not required for monitoring (only calls between agents and external callers), we could connect a CAD VoIP server to each of the Catalyst 3524 switches used for the third floor. Each agent device connected to one of those switches is then configured to use the attached VoIP server for monitoring.

We could also connect two CAD VoIP servers to the core 6500 switches. Since the Catalyst 6500 switch can support 30 SPAN sessions, we can easily add another one that is used only by the CAD VoIP servers. This would require two CAD VoIP servers to be redundant.

In this example, the second option of connecting the CAD VoIP servers to the core 6500 switches is selected. The reason for this choice is that if the customer ever decides to monitor agents from other floors, we will not need to add more VoIP servers for each of the 3524 switches. The two connected to the core switches will handle the calls for the other agents as well.

The NIC Qualification Utility

3

Overview

The Network Interface Card Qualification (NICQ) utility is included with CAD, starting with the following versions:

- CAD 6.6(1) for Unified CCX 7.0(1)
- CAD 7.5(1) for Unified CCE 7.5(1)

This utility is not a general NIC-qualifying tool. It is intended to be used exclusively with CAD installations.

The NIC Qualification (NICQ) utility performs these major functions:

- Tests NICs on agent PCs and the servers that host the VoIP Monitor services to verify that their NICs support RTP packet sniffing
- Validates NICs for compatibility with CAD
- Tests agent PCs and the servers that host the VoIP Monitor services as part of troubleshooting to determine why monitoring or recording is not working properly
- Gathers information about qualified NICs in order to create an accurate list of NICs that will work with CAD

The default location of the NICQ utility (NICQ.exe) on servers hosting the VoIP Monitor service and all CAD client desktops is the following folder:

```
C:\Program Files\Cisco\Desktop\bin
```

The NICQ utility runs a series of tests on all available NICs on a computer and reports the results to the screen and to an output file. In order for all tests to run successfully, the system must be configured to expose the NIC to RTP traffic.

In order to validate whether a NIC will work properly with CAD, the NIC must be capable of capturing network traffic that is not directed to its IP address and make it available to an application. This is called “promiscuous mode”.

The service's NIC card should allow Promiscuous Mode packet capturing. This is true for most NIC cards, but there are some cards that will not allow network traffic sent to the IP phone to be seen by the packet sniffing software.

You can validate the NIC without using the NIC Qualification (NICQ) utility. For a procedure for testing NICs for compatibility, see Technote 46301, *Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring*, available at:

http://www.cisco.com/en/US/partner/products/sw/custcosw/ps427/prod_tech_notes_list.html

Assumptions

It is assumed that the computer being tested is configured correctly, using either desktop monitoring or server monitoring.

- In desktop monitoring, an agent's desktop is daisy-chained to the IP phone, then connected to the switch. RTP packets are captured by the packet-sniffing driver located on the desktop.
- In server monitoring, the VoIP Monitor service receives RTP traffic sent to its switch port by using the switch's Switched Port Analyzer (SPAN) configuration.

Utility Syntax

The syntax for the NICQ utility is:

```
NICQ.exe [-?] [-o outfile] [-t seconds] [-p ipaddr] [-s]
```

Table 8 defines the available parameters.

Table 8. NICQ.exe parameters

Parameter	Description
-?	Causes the usage screen to be displayed.
-o	Defines the name of the file that will receive the results of the tests. By default, the file is named NICQ_Output.txt and is placed in the current folder.
-t	Indicates how long the utility will listen on each NIC for network traffic. The default is 20 seconds.
-p	Allows the IP address (in #.#.#.# format) of the daisy-chained IP phone to be passed to the utility. You can use this if you know the IP address and don't want to take the time to detect it during test runs.
-s	Minimizes the additional system information that is collected and written to the output file. The collection step adds significant time to the length of the tests.

Running the NICQ Utility

Before running the NICQ utility, generate RTP traffic to the desktop or server whose NIC is being tested. This is generally done by placing a phone call to the agent phone or simulating RTP traffic.

To run the NICQ utility:

1. On the computer whose NIC is being tested, open a command window.
2. Navigate to the folder where NICQ.exe is located (by default, C:\Program Files\Cisco\Desktop\bin).
3. In the command window, type the following command. For information about parameters, see Table 8.

   ```
   NICQ.exe
   ```

4. When prompted, type **1** or **2** to select the type of system being tested:
   - Type 1 if your configuration has a daisy-chained IP phone and desktop monitoring.

- Type 2 if your configuration uses SPAN (server monitoring) to send RTP traffic to the NIC.

5. The NICQ utility performs its testing. As it runs, it displays progress messages on the screen and writes detailed information to the output file.
6. After the utility stops, view the output file for detailed test results.

Output From the NIC Qualification Tool

By default, all test results and system information are written to a file named NICQ_Output.txt. This file can be quite large (500 KB or more) on some systems. The majority of this information is system information.

The output file contains the following data and sections:

- Date and time the test was run
- System name
- The results of the following tests for each NIC adapter on the system
  - Check driver status
  - Get the list of valid network adapters
  - Attempt to sniff packets on all valid network adapters
  - Analyze packet capture results
- Information retrieved from phone, including the following:
  - IP address, host name, phone DN, version, model number
  - IP addresses of TFTP server and Cisco Unified Communications Manager
  - Settings for DHCP, PC port, SW port, voice VLAN, SPAN to PC port
- Registry dump from HKEY_LOCAL_SYSTEM\SYSTEM\CurrentControlSet:
  - All keys under . .\Services whose name starts with the “{“character
- Registry dump from HKEY_LOCAL_SYSTEM\SOFTWARE\Spanlink
- Registry dump from HKEY_LOCAL_SYSTEM\SYSTEM\CurrentControlSet:
  - ...\Services\SPCD
  - ...\Services\Tcpip
  - ...\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318} (information on network adapters)
  - ...\Control\Network
- Complete system information (msinfo32), including the following:
  - Hardware Resources
  - Components

- Software Environment
- Internet Settings
- Office 2003 Applications

NICQ Tests

This section describes the functional areas that are tested and the specific tests that are run. The tests are executed in the order shown.

Test 1—Check Driver Status

Test	Corrective Action if Test Fails
Look for installed SPCD driver files	• Reinstall the driver files or Cisco Agent Desktop application
Load the driver	• Verify that the user account being used has administrator privileges • Verify that the files have been installed correctly, and reinstall if necessary

Test 2—Retrieve List of Valid Network Adapters

Test	Corrective Action if Test Fails
Retrieve list of valid adapters from registry	• Verify that the OS is supported by the SPCD driver • Verify that the SPCD DLLs are in the system PATH • Verify that the user account can access the system registry • Check the network configuration on the machine and verify that at least one NIC adapter is defined for the TCP/IP subsystem

Test 3—Capture Packets

This test is run against every adapter found in Test 2. In this test, network traffic is captured and grouped according to the type of packet and identifies the sender and receiver. Only Ethernet traffic is captured. By default, the test is run for 20 seconds against each NIC; you can choose a different duration using the -t parameter when executing the utility.

If a call or simulated RTP stream is not active and the NIC being tested is not exposed to this traffic, no RTP packets will be seen.

These packet-sniffing tests are meant to verify that the NIC can be put into promiscuous mode in order to sniff network traffic not destined for the NIC card being tested. This is a basic requirement of the sniffing design used by CAD.

Test	Corrective Action if Test Fails
Open the adapter	• Verify that system/kernel memory is not below 5 Mb • Verify that the driver is loaded
Capture network traffic	• Verify that the NIC is active • Verify that the NIC is connected to the network and that the cable is good • Verify that network traffic is hitting the NIC. Another network monitoring tool like Wireshark or a Microsoft utility can be used to determine this. Running a browser and accessing non-cached pages from a web server will also determine this.

Test 4—Detect Attached IP Phones

This test detects IP phones connected inline with the NIC/PC. It uses the data captured in Test 3. It looks for specific packets.

- If the IP phone uses SCCP (Skinny Client Control Protocol), the test looks for SCCP KeepAlive messages being sent from the IP phones to the Cisco Unified Communications Manager (Unified CM). These packets have a destination port of 2000 (default). If the port has been changed in the Unified CM, this test might fail.
- If the IP phone uses SIP (Session Initiation Protocol), the test looks for SIP REGISTER messages. These are similar to the KeepAlive messages in SCCP.

If you have more than one IP phone connected inline with the NIC, only one of them is reported, not both.

Test	Corrective Action if Test Fails
Check for SCCP KeepAlive messages	• Verify that the IP phone is connected inline with the NIC being tested • Ensure that the phone uses SCCP • Ensure that the IP phone is configured correctly in Unified CM to pass the traffic out its second network port • Ensure that the SCCP port is 2000 in Unified CM • Ensure that the capture time is long enough to capture the required number (3) of KeepAlive packets. Use the -t parameter to allow more time to capture packets. This might also be the case if the default SCCP KeepAlive refresh rate is changed from its default value of 30 seconds and the capture time is not at least 3 times this value.
Check for SIP REGISTER messages	• Verify that the IP phone is connected inline with the NIC being tested • Ensure that the phone uses SIP • Ensure that the IP phone is configured correctly in Unified CM to pass the traffic out its second network port • Ensure that the capture time is long enough to capture the required number (3) of REGISTER packets. Use the -t parameter to allow more time to capture packets. This might also be the case if the SIP KeepAlive refresh rate is changed from its default value of 18 seconds and the capture time is not at least 3 times this value.

Test 5—Detect Promiscuous Traffic

This test uses the data captured in Test 3. It verifies if the NIC supports promiscuous mode captures, and if valid RTP packets can be captured.

Test	Corrective Action if Test Fails
Check for promiscuous traffic	• Verify that a daisy-chained phone is configured to send voice traffic out its second network port • Ensure that the capture time is long enough. Use the -t parameter to increase the time, if necessary. • Ensure that there is promiscuous traffic available for the NIC to capture. Some reasons for no traffic are: the phone is not daisy-chained and there is no active call, or if using SPAN and there is no call on any of the SPAN source ports. • Look for documented workarounds for this NIC to get it to work correctly in promiscuous mode • Update driver to the latest version and retest
Check for RTP traffic	• Ensure that there is a phone call or simulated RTP traffic exposed to the NIC being tested. Make a call to the IP phone. • Ensure that the phone uses the correct codec (G.711, G.722, or G.729). Change the configuration in Unified CM so that a supported codec is used.

Successful Test Report Example

The following is an example of a successfully-run test. The system information is omitted. The test results state whether the tests are passed and if the NICs will support the packet sniffing solution used by CAD. If one or more tests fail, it might indicate that a particular NIC is not supported. However, it might also indicate that the configuration used in the test is not correct.

```
---------------------------
Test 1: Check Driver Status
---------------------------
Driver is properly installed.
SPCD Driver service is running.
Test 1: SUCCESS

-------------------------------------------
Test 2: Get the List of Valid Network Adapters
-------------------------------------------
Found 2 valid network interfaces:
  Adapter 1:
    Name: \Device\Splkpc_{1AF9AAEF-7AD0-4795-98EB-11AA0C59A106}
    IP: 10.10.49.117
  Adapter 2:
    Name: \Device\Splkpc_{06FF0278-AA0F-44C0-933F-220AD13FDDC2}
```

```
    IP: 10.0.9.162
Test 2: SUCCESS

------------------------------------------------------------
Test 3: Attempt to sniff packets on all valid network adapters
------------------------------------------------------------
Device: \Device\Splkpc_{1AF9AAEF-7AD0-4795-98EB-11AA0C59A106} (10.10.49.117)
  Packet capture completed successfully
------------------------------------------------------------
Sender         Receiver          Count    Packet Type
------------------------------------------------------------
10.10.50.104   10.10.18.142      89       UDP/RTP: (0) PCMU (uLaw G.711 Audio)
10.10.18.142   10.10.50.104      89       UDP/RTP: (0) PCMU (uLaw G.711 Audio)
10.10.50.1     255.255.255.255   1        UDP (17)
10.10.50.1     255.255.255.255   2        ARP
10.10.50.104   172.17.12.20      1        TCP (6)
10.10.50.104   10.10.18.142      884      UDP/RTP: (0) PCMU (uLaw G.711 Audio)
10.10.18.142   10.10.50.104      884      UDP/RTP: (0) PCMU (uLaw G.711 Audio)
172.17.12.20   10.10.50.104      1        TCP (6)
10.10.50.1     255.255.255.255   12       UDP (17)
10.10.18.142   10.10.50.104      4        ARP
10.10.50.1     224.0.0.10        4        unknown (88)
10.10.49.108   10.10.49.255      1        UDP (17)
10.10.50.1     255.255.255.255   18       ARP
10.10.49.1     224.0.0.10        4        unknown (88)
10.10.50.104   10.10.18.142      2        ARP
10.10.49.117   172.17.10.18      46       TCP (6)
172.17.10.18   10.10.49.117      28       TCP (6)

Device: \Device\Splkpc_{06FF0278-AA0F-44C0-933F-220AD13FDDC2} (10.0.9.162)
  Packet capture completed successfully
------------------------------------------------------------
Sender            Receiver          Count      Packet Type
------------------------------------------------------------

Test 3: SUCCESS - One or more devices were able to capture packets

------------------------------------------
Attempting to autodetect the attached phone
------------------------------------------
Searching for phone on device: 10.10.49.117
  Detected phone with IP: 10.10.50.104

------------------------------------------------
Test 4 Attempt 1: Analyze Packet Capture Results
------------------------------------------------
Analyzing results for device: (10.10.49.117)
  Able to put adapter into promiscuous mode
  Able to detect RTP Audio packets
  Able to detect RTP Audio packets from phone (10.10.50.104)
Test 4 Attempt 1: SUCCESS

-------------------------------
Information Retrieved from Phone
-------------------------------
IP Address:            10.10.50.104
MAC Address:           00062895B091
Host Name:             SEP00062895B091
Phone DN:              7639712175
App Load ID:           P00308000400
```

```
Boot Load ID:          PC03A300
Version:               8.0(4.0)
Model Number:          CP-7940

TFTP Server:           172.17.12.20
Operational VLAN ID:   110
CallManager 1:         SPLKCCMS  Active
CallManager 2:         SPLKCCMP  Standby
CallManager 3:
CallManager 4:
CallManager 5:
DHCP Enabled:          Yes
PC Port Disabled:      No
SW Port Configuration: AUTO
PC Port Configuration: AUTO
Voice VLAN Enabled:    Yes
Security Mode:         Non Secure

** Network Port Details **
Neighbor Device ID:    Switch10_4.spanlink.com
Neighbor IP Address:   10.10.49.1
Neighbor Port:         FastEthernet0/3
Port Information:      Full, 100

** Access Port Details **
Neighbor Device ID:
Neighbor IP Address:
Neighbor Port:
Port Information:      Full, 100
```

Using Multiple NICs with the VoIP Monitor Service

The VoIP Monitor service sniffs RTP traffic from the network and sends it to registered clients. This requires support from the switch to which the service is connected.

The VoIP Monitor service must be connected to the destination port of a configured SPAN/RSPAN. Any traffic that crosses the SPAN/RSPAN source ports is copied to the SPAN/RSPAN destination port and consequently is seen by the VoIP Monitor service.

Not all Catalyst switches allow the VoIP Monitor service to use the SPAN port for both receiving and sending traffic. There are switches that do not allow normal network traffic on a SPAN destination port. A solution to this problem is to use two NICs in the machine running the VoIP Monitor service:

- One NIC for sniffing the RTP streams, connected to the SPAN port
- One NIC for sending/receiving normal traffic, such as requests from clients and sniffed RTP streams, connected to a normal switch port not monitored by the above-mentioned SPAN port.

There can be other reasons for using a second NIC dedicated to receiving RTP traffic. The information shown below details the configuration of the second NIC to allow CAD's live monitoring and recording features to work properly.

Consult the *Cisco Agent Desktop (CAD) and CTI Toolkit Desktop Silent Monitor — Reference Information* for the most recent information on compatible NICs. This document is located at:

http://www.cisco.com/en/US/partner/products/sw/custcosw/ps14/prod_installation_guides_list.html

Limitations

CAD's packet sniffing library works only with NICs that are bound to TCP/IP. Make sure the sniffing card is bound to TCP/IP.

In a Unified CCX environment, VoIP Monitor Service is only supported on the CCX unit.

Issues

The VoIP Monitor service explicitly specifies what NIC adapter to use for capturing audio packets, but it does not specify which NIC should be used when sending out packets. These outgoing packets would be going to either the Cisco Recording & Playback Service or a supervisor's desktop that is live-monitoring an agent's call. This is not a problem when using a single NIC for both sniffing and normal traffic. With two NICs, however, normal traffic should be restricted so that it does not go through the NIC used for sniffing. Otherwise, the sniffed RTP steams of a currently-monitored call might not reach the supervisor because the SPAN destination port does not allow outgoing traffic.

To resolve this, use the route command to customize the static routing tables so that normal traffic does not go through the sniffing NIC. Contact your network administrators for details.

An alternative solution is to give the sniffing NIC and IP address that no other host on the network uses, and a subnet mask of 255.255.255.0. Leave the default gateway field blank for this NIC's TCP/IP binding.

In addition to these steps, the NIC that is used by the VoIP Monitor service must not be the first NIC in the network binding order. By default, the first NIC adapter in the binding order will be used by applications to send traffic out to the network. Contact your network administrator for details.

Uninstalling and installing NICs can cause the binding order of the systems network adapters to change. Whenever these kinds of changes are made, the binding order might need to be changed manually.

Installing a Second NIC in a VoIP Monitor Service Server

To install a second NIC on a VoIP Monitor service computer:

1. Shut down the computer.
2. Install the second NIC in the computer.
3. Start the computer.
4. Make sure that neither adapter is using dynamic host configuration protocol (DHCP) to get its IP address.
5. Assign valid IP addresses to the adapters.
6. Determine which of the two adapters will be used for sniffing.
7. Connect the sniffing adapter to the switch SPAN port.
8. Use the route command to customize the local routing table so that normal traffic does not go through the sniffing adapter.
9. Verify that the sniffing adapter is not registered with DNS and WINS by using the following command:

   `ping local_host_name`

   Where *local_host_name* is the IP address or DNS name of the adapter. This ensures that the local name always resolves to the normal traffic card IP address.

   Verify that the sniffing adapter is not the first adapter in the system's binding order.

Additional Configuration Steps

The CAD installation process offers the user the option to choose the IP address that the VoIP Monitor service will use for packet sniffing. In a system with multiple NICs, the first adapter found is the default network adapter becomes the sniffing adapter. This might not be the adapter you want to use.

To change the NIC that is used by packet sniffing, use the CAD Configuration Setup utility. See the *CAD Installation Guide* for more information. This utility contains a screen that lists all valid NIC adapters in the system by IP address. Simply select the IP address associated with the NIC configured for packet sniffing and save your changes. This information is used by the VoIP Monitor service the next time the service is started.

To uninstall or reinstall the packet sniffing NIC or install a different packet sniffing NIC, use the CAD Configuration Setup utility as described above. If you do not use the CAD

Configuration Setup utility to point to the correct packet sniffing NIC, the live monitoring and recording features might not work.

You do not need to perform these additional steps in a single-NIC system after you install CAD. If you uninstall and reinstall the packet sniffing NIC in a single-NIC system or install a different packet sniffing NIC in a single-NIC system, use the CAD Configuration Setup utility as described above. If you do not use the CAD Configuration Setup utility to point to the correct packet sniffing NIC, the live monitoring and recording features might not work.

Troubleshooting VoIP Monitoring and Recording

4

Introduction

The steps required to configure VoIP monitoring and recording can be complex. This chapter describes some of the issues that can occur and methods for resolving them in the CAD and Recording Solution products.

Incomplete or incorrect software and hardware configuration is the cause of 90% of all monitoring and recording problems. If the software has been installed correctly, monitoring and recording problems are rare.

Before applying the troubleshooting methods described below, verify that the appropriate software is installed and that the software is configured correctly. For information about configuration, see the instructions for installing the software.

> **NOTE:** Problems are more likely with server monitoring than with desktop monitoring, due to the complexity of configuring the SPAN feature.

Troubleshooting

This section helps you troubleshoot problems with VoIP monitoring and recording that occur in CAD and Recording Solution.

Identifying the Problem's Location

Figure 28 displays the major components involved when the live monitoring or recording features are used in CAD and Recording Solution. Components for all types of monitoring and recording are shown. The numbered starbursts indicate where a failure of a component or a configuration error can cause live monitoring or recording to malfunction or fail.

Refer to Table 9 for possible causes of malfunction or failure at the corresponding numbered component.

Figure 28. Major components involved with live monitoring and recording

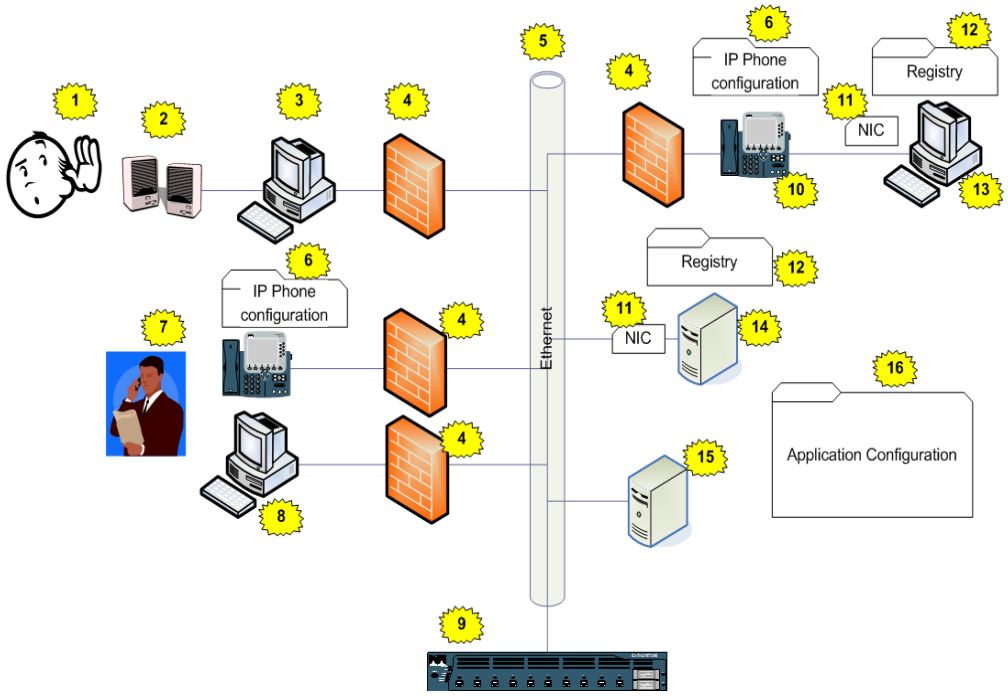


Table 9. Possible causes of failure in monitoring/recording[1]

No.	Component	Issue
1	CAD supervisor	• Listening to the speakers of the correct computer?

Table 9. Possible causes of failure in monitoring/recording[1] (cont'd)

No.	Component	Issue
2	Speakers or headphones	• Are they broken? • Do they have power? • Are they plugged into the computer correctly? • Are they turned on? • Is the volume turned up?
3	CAD supervisor workstation	• Is Cisco Supervisor Desktop running correctly? • Any errors reported? • Is the call still active? • Are the callers speaking? • Is live monitoring or recording shown as "in service"? • Is the PC hung? • Is the network cable plugged in? • Is the network cable good? • Is there network connectivity? • Is there available bandwidth on the network connection? • Is the CPU usage too high due to excessive debugging or another application?
4	Firewalls	• Are the correct ports in the firewall open? • Is VPN connectivity being used with an unsupported application? • Can other PCs ping the supervisor's IP address?
5	LAN	• Does the LAN lack bandwidth? • Is other traffic moving smoothly over the network?
6	IP phone configuration	• Is the phone configured correctly in Unified CM? • Is it set to send voice packets out of the second network port? • Is it using a codec other than G.711, G.729, or G.722? • Is the phone registered and active? CAD Only: • Is extension mobility configured, and is the agent logged into the extension mobility service? • Is extension mobility configured correctly?

Table 9. Possible causes of failure in monitoring/recording[1] (cont'd)

No.	Component	Issue
7	Recording Solution supervisor	• Is the correct phone extension entered for live monitoring? • Is the supervisor's phone able to be called normally by the agent's phone? • Is the agent's call already being live monitored by another supervisor?
8	Recording Solution Desktop	• Is the application running properly? • Is the correct agent selected for live monitoring? • Is the agent on a call? • Did the supervisor click the correct Live Monitoring button?
9	IP switch	• Are switch ports configured correctly? • Is SPAN/RSPAN/port monitoring set up correctly? • Is the switch running smoothly?
10	IP phone	• Is the phone model supported for the type of monitoring being done? • Are the cables plugged in correctly? • Is the phone powered up? • Is the phone daisy-chained to the agent's PC for desktop capture? • Is there more than one IP phone daisy-chained to the agent's PC? • Is there a router between the phone and the PC? • Is the phone muted? • Does the handset work? • Can the other party on the call be heard on this phone? • Is the correct agent device being monitored? • Is there an active call? • Is the phone plugged into a switch port that is part of the SPAN/RSPAN/port monitor (for server capture)?

Table 9. Possible causes of failure in monitoring/recording[1] (cont'd)

No.	Component	Issue
11	NIC	• Is the NIC installed properly? • Are the NIC drivers installed and running? • Are the drivers up to date? • Is this NIC known to be supported or not supported? • Are there additional configuration steps required to make this NIC work properly? • Is the phone properly connected to this NIC? • Is there more than one NIC on the PC?
12	Registry entries	• Is the Cisco software installed correctly? • Is the monitor device name in the registry correct for the NIC that is connected to the phone?
13	CAD Agent Desktop	• Is CAD installed correctly? • Is an unsupported soft phone being used? • Is unsupported VPN software being used? • Is the software reporting any errors? • Is the desktop monitoring subsystem active and functioning? • Are there available CPU resources? • Are the monitoring and recording features shown as "in service" (CAD only)? • Does the agent have an active call? • Is the SPCD/QMPD driver loaded and running? • Are packets being captured from the NIC?
14	Recording service	• Is the service installed correctly? • Is the service active? • Is the disk full? • Do the recording files exist? • Is the server behind a firewall or router?

Table 9. Possible causes of failure in monitoring/recording[1] (cont'd)

No.	Component	Issue
15	Monitor service	• Is the service3 installed correctly? • Is the service active? • Does the service have connectivity with other components and the required database? • Are there available CPU resources? • Are any errors being reported in the log files? • Is the SPCD/QMPD driver loaded and running? • Are packets being captured from the NIC? • Is the server behind a firewall or router?
16	Software configuration	• Is the agent configured correctly? • Are the agent and device configured for the correct method of packet capture? • Are all the associations between agent, device, monitor service, and recording service correct?

1 If a product is not specified, the component applies to both CAD and Recording Solution.

Common CAD Issues

If you are experiencing an issue that is related to VoIP monitoring and recording, refer to *Cisco CAD Troubleshooting Guide*.

Common Recording Solution Live Monitoring and Recording Issues

Table 10 lists some of the issues that might be encountered with VoIP monitoring and recording in Cisco Recording Solution. The issues are listed in order of their frequency (identified in the third column).

The first column briefly describes the issue and identifies the page on which the issue and possible solutions are described in detail. The second column provides a lengthier description of the issue.

> **NOTE:** These are possible issues with features related to the Recording Solution Live Monitoring and Call Recording features that deal with packet capture or stream redirection. Issues related to other features, such as file uploads and scoring calls are not addressed here.

If you are experiencing an issue that is related to live monitoring and recording, choose the issue listed in the table that is most similar to your issue, then refer to the instructions on the corresponding page.

Table 10. Live monitoring and recording issues and their frequency

Issue	Description	Frequency
Agent not on the Live Monitoring agent list (page 84)	The supervisor wants to live monitor a specific agent, but cannot find that agent on the list of agents available for live monitoring.	Common
Error trying to live monitor an agent (page 84)	The supervisor selects an agent in the Live Monitor agent list and clicks the Live Monitor button, but no call is received by the supervisor, and an error is posted.	Common
Agent calls not recorded (page 85)	Calls for a Recording Solution agent or knowledge worker are not being recorded as expected	Common
Audio recordings contain no speech (page 85)	Audio recordings contain no speech. The RAW file size is 1 Kb.	Common
Recordings for SPAN-configured agents are on the agent desktop (page 86)	A Recording Solution agent is configured to use server-based (SPAN) recording, but the files are being created and saved on the agent's desktop.	Rare
Call recordings contain pops and clicks (page 86)	When reviewing an audio call recording, pops and/or clicks are heard at various places in the recording. Speech quality is good otherwise.	Common
Call recordings are poor quality (page 87)	While listening to an audio call recording, the speech is slow. This might occur only for one party on the call, or both parties.	Rare
Portions of an audio call are missing (page 88)	Large sections of a call's audio is missing. Usually, the missing section is at the very beginning or at the end of the call. In some cases, it sounds like the call recording stopped somewhere in the middle of the call and never resumed.	Rare

Agent not on the Live Monitoring agent list

Problem. The supervisor wants to live monitor a specific agent, but cannot find that agent on the list of agents available to live monitor.

Cause. The most common cause for this is that the agent is not configured for network recording. Live monitoring is available only when the Unified CM monitoring and recording feature is used and properly configured for the agent's device. In addition, even if no calls are to be recorded for this agent, the agent still needs to be configured for network recording in Recording Solution Administrator, and either an archive or quality work flow must be associated with the agent via the team the agent is assigned to, even if it is a workflow that specifies that no actual recordings be made for this agent's device.

Configuring the Recording Solution agent to be network recorded allows the agent to be seen on the list of agents who can be live monitored. Associating a workflow with the agent allows Recording Solution to get CTI events for the device associated with the agent. Without the CTI events, the current state of the phone (idle, active, on hold) cannot be displayed, which would not allow the agent to be selected in the list. Only active calls can be selected.

To troubleshoot this problem, complete the following steps:

1. In Recording Solution Administrator, verify that the agent is associated with a device.
2. Verify that the agent/device is configured for network recording.
3. Verify that the agent is part of a team and that the team is associated with a workflow.

Error trying to live monitor an agent

Problem. The supervisor selects an agent in the Live Monitoring agent list and clicks the Live Monitor button, but no call is received by the supervisor and an error is posted.

Cause. The most common cause for this error is that the agent device is already being live monitored by another supervisor. The Unified CM monitoring and recording feature allows at most one live monitoring session and supervisor per call. Additional attempts to live monitor the agent will fail.

To troubleshoot this problem, complete the following steps:

1. Ask other supervisors if they are currently live monitoring the agent.
2. Retry live monitoring that agent later in the call or on another call.

Agent calls not recorded

Problem. Calls for a Recording Solution agent or knowledge worker are not being recorded as expected. Recordings are blank.

Cause. The most common cause for this is Recording Solution workflow configuration. The workflows assigned to an agent contain conditions that indicate which calls to record and keep. Generally, all calls are recorded, and the logic for deciding whether to keep to recorded call or not takes place at the end of the day. An exception to this is if the workflow contains logic that states any of the following:

- Only inbound calls are recorded
- Only outbound calls are recorded
- Listed extensions are included for recording
- Listed extensions are excluded from recording

Because we know at the time of the call whether it is inbound or outbound, and what the calling and called extensions are, we can decide at the time of the call whether or not to record the call. If we know the call will never be uploaded, we will not record the call and evaluate it at the end of the day.

To troubleshoot this problem, complete the following steps:

1. Review the archive and quality workflows assigned to the agent.
2. Verify what calls will and will not be recorded based on the inbound/outbound settings and the inclusion/exclusion list of extensions.

Audio recordings contain no speech

Problem. A Recording Solution agent is configured to use server-based (SPAN) recording, but the files are being created and saved on the agent desktop. The raw file size is 1Kb.

Cause. There are several common causes for this issue. The basic problem is that the software is attempting to record the call, but it is receiving no valid RTP packets, so no packets are written to the RAW files. To fix this issue, the cause of this lack of RTP packets needs to be fixed.

To troubleshoot this problem, complete the following steps.

For desktop capture

1. Verify that the NIC supports promiscuous mode packet capturing.
2. Verify that the agent device is daisy-chained to the Recording Solution agent's desktop.
3. Verify that the agent device is properly configured in Unified CM to send packets out its second network port.

For server capture

1. Verify that the NIC supports promiscuous mode packet capturing.
2. Verify that SPAN is configured correctly on the switch to get audio traffic from the agent's phone.

For network capture

1. Verify the SIP trunk configuration on the Unified CM to make sure that the agent device is properly associated with the correct SIP trunk and that the SIP trunk is sending SIP messages to the correct Recording Solution Recording service.
2. Verify that the agent and device are configured properly in Recording Solution Administrator for network recording and are associated with the correct Recording Solution Recording service that is receiving SIP messages for the agent's device.

Recordings for SPAN-configured agents are on the agent desktop

Problem. A Recording Solution agent is configured to use SPAN (server-based) recording, and the files are created and saved on the agent's desktop, not in the expected location on the recording server.

Cause. This issue occurs if an agent is configured for server recording, and the agent's IP phone is daisy-chained to the agent's desktop. The daisy-chained phone is found and endpoint recording is used instead of server recording. As a result, the RAW or SPEEX files are not found on the recording server; instead they are on the agent desktop. Uploading and other functionality works correctly.

To correct this issue, connect the IP phone directly to the network and do not daisy-chain it to the agent's desktop.

Call recordings contain pops and clicks

Problem. When reviewing an audio call recording, pops and/or clicks are heard at various places in the recording. Speech quality is good otherwise.

Cause. The most common cause of pops and clicks is that the Unified CM is configured to use silence suppression for IP phone calls. In this case, when the audio sound level goes low enough (for example, when a call participant is not speaking or making some sort of noise, such as typing) RTP packets are not sent. This is meant to save bandwidth. The result is that the recording will contain absolute silence during this time. When a call participant begins speaking or making noise again, packets are sent again. If this happens frequently enough, the resulting audio will seem to contain pops and clicks as it goes from a normal sound level to absolute silence, then back up when the call participant makes a noise again. These sound anomalies are normal and Recording Solution does not do any audio data processing to prevent them.

Other causes of this issue include drops in audio during call control events. When a call is put on hold, transferred, or conferenced, a series of CTI events are sent to interested parties to process. Recording Solution sees these CTI events, and in response to them, RTP streams are stopped, started, and recreated. This forces Recording Solution to use different filters for capturing the correct audio traffic. It is at these transitions, when the audio filters are being changed, that a small number of audio packets might be missed and not written to the output files. When the raw audio files are converted to a format that can be listened to, the missing packets are replaced with absolute silence, resulting in the pop or click heard by the listener.

In general, these pops and clicks are so short that they do not affect the resulting audio to the extent that words cannot be heard or understood by a person listening to the recording.

Call recordings are poor quality

Problem. While listening to an audio call recording, the speech is slow. This might occur only for one party on the call, or both parties.

Cause. Poor quality audio, where the speakers seem to be speaking slowly and there seems to be a lot of interference in the audio signal, is most often caused by duplicate FTP streams being captured and written to the raw audio files.

A phone call consists of two RTP audio streams. Recording Solution saves each audio stream to a raw file. There are cases where the same audio stream is captured twice, and duplicate RTP packets are written to the same file. This can happen for server recording if SPAN is not configured properly and we are seeing the RTP stream once as it leaves one port and again as it enters another port that is part of the SPAN configuration.

For end point capture, duplicate streams are possible in these scenarios:

- Both Recording Solution and CAD are on the agent's desktop, the agent is using a soft IP phone, CAD is configured to use desktop monitoring and recording, and CAD is actually monitoring or recording at the same time as Recording Solution is recording a call, and Recording Solution has not been configured with an RTP filter (in Recording Solution Administrator on the Site Configuration > RTP Filters page) to prevent the problem.
- Both Recording Solution and CAD are on the agent's desktop, the agent is using a hard or soft IP phone, CAD is configured to use Unified CM-based monitoring, and the agent is being live-monitored by a CAD supervisor while Recording Solution is recording the call. There is no way to prevent duplicate streams from being recorded in this scenario. Options are to configure the Recording Solution agent for network capture and use the Recording Solution Live Monitoring feature to monitor the agent, or configure CAD to use desktop or server capture for its method of live monitoring.

- Built-in-Bridge (BiB) or Dual Media Streaming (DMS) is enabled on the agent's phone. BiB and DMS are not supported in CAD before version 8.5(1). These features should be disabled in Unified CM.

Portions of an audio call are missing

Problem. Large sections of a call's audio are missing. Usually the missing section is at the beginning of the call or at the end of the call. In some cases, it sounds like the call recording stops somewhere in the middle of the call and never resumes.

Cause. For gaps at the beginning of calls, the problem is commonly due to slow reception of call control events. Anything that causes a delay in Recording Solution receiving CTI events will cause delays in when the audio packets start getting captured and written to the raw files. Network congestion, or high CPU usage on the Recording Solution CTI service or Recording service, or on the Unified CM CTI Manager server might cause this issue. To fix the issue, the server/switch experiencing these lack-of-resource problems must be found and the issue fixed there.

Another reason for gaps or missing audio at the end of the call is due to failover processing. The Unified CM and Recording Solution are able to deal with servers and processes that fail. Usually a failure in one component will cause a backup service to take over those duties and attempt to recreate the call states prior to the failure. This process does take some time. In many cases, this will only cause a short period where audio is not heard during that part of the call when the service failed. In other cases, the call recording is stopped at the point of failure and the remainder of the call is not captured. Usually, the next call will be recorded normally after the backup service has come up.

In the case where the remainder of the call is lost after a failure, this is due to the CTI signaling required for Recording Solution to work properly. Fundamentally, if Recording Solution loses CTI connectivity, it can no longer be sure that it will receive a CTI message when the call ends. If the call ends while the failover to the backup service is occurring, Recording Solution will never get an end call event and continues to write data to the raw file until stopped or the system is shut down. Rather than do this, the call recording is stopped if the CTI connection goes down.

In these cases, the number of affected calls is small. Once the failover occurs, all subsequent calls are recorded normally. Also, the incidence of CTI server failures are very rare, so this issue is not very common.

Troubleshooting Procedures

This section describes the following procedures.

- Verifying Sound Card Functionality on page 89
- Verifying Registry Settings on page 90
- Verifying Registry Settings on page 90
- Testing the Sniffing Adapter on page 90
- Verifying that the Correct NIC Is Being Used on page 90
- Testing the Desktop Monitor Library on page 91
- Verifying that Required Applications are Running on page 91
- Opening a TAC Case on page 92

Verifying Sound Card Functionality

A simple way to verify that your sound card is working is to play a sound file. Complete the following procedure to test your sound card. If you cannot hear anything, complete the subsequent procedure to view your sound card properties.

> **NOTE:** This procedure applies only to CAD live monitoring when Unified CM monitoring is being used.

To test your sound card:

1. Launch an application, such as Windows Media Player, that can play sound files.
2. Open a sound file.

   > **NOTE:** In Microsoft Windows, most sound files are in the folder C:\WINDOWS\Media.

3. Use your speakers or headphones to verify that you can hear the output from the sound card.
4. If you cannot hear anything, complete the following procedure to troubleshoot your sound card.

To view the properties of your sound card:

1. Choose Start > Settings > Control Panel > Sounds and Audio Devices.
2. Select the Hardware tab.
3. Select your sound card from the Devices list.

4. Click Properties to view your sound card's properties.
5. Click Troubleshooting and follow the instructions given in the Troubleshooter.

Verifying Registry Settings

For monitoring to work correctly in CAD and Recording Solution, there are a few settings in the Windows registry that are required. The most important entry to look at is the Monitor Device entry. This is the network adapter that is used to sniff voice packets from the network.

To verify the monitoring adapter in the Windows registry:

1. The Monitor Device entry is found under the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Calabrio\<product name>\Site Setup.

   NOTE: The registry entry is case-sensitive. An incorrect entry will cause VoIP monitoring to fail.

2. If the entry exists and its value appears to be valid, complete the next procedure, "Testing the Sniffing Adapter".

Verifying that the Correct NIC Is Being Used

If the Monitor Device entry in the registry is incorrect, the your product's Configuration Setup utility can be used to change it to the correct entry.

To view and modify the NIC IP address being used for sniffing:

1. In your product's bin folder, run Postinstall.exe.
2. Navigate to the window on which the NIC IP address is entered. Consult the *Installation Guide* for your product for exact information on where the IP address must be entered.

Testing the Sniffing Adapter

If you suspect that the Monitor Device entry in the registry is incorrect, test the entry using the SplkDump or QMDump tool.

To test the sniffing adapter:

1. Open a command window and navigate to the product's bin folder.
2. Run the appropriate file for your product:
   - For CAD: SplkDump.exe

- For Recording Solution: QMDump.exe

You will be presented with a list of adapters that can be used for sniffing voice traffic.

3. If you see the adapter that matches the Monitor Device entry in the Registry, select it and press Enter.
4. Let the program run for a short while and note whether any network traffic is captured.

Testing the Desktop Monitor Library

The VoIP Monitor Test Tool is a testing application that exercises the API of the VoIP Monitor service by acting as an agent or supervisor.

NOTE: This tool is available only for CAD.

You can run this tool on the machine running the VoIP Monitor service or the agent or supervisor's desktop. This will remove some of the variables introduced by using the full CAD package to monitor and record agent calls.

To test the Desktop Monitor library:

1. It is recommended that you attempt to monitor first with the test tool.
2. If you are able to monitor, but not record, this is an important piece of information for TAC personnel to use when troubleshooting problems. For information on using the VoIP Monitor Test Tool, refer to the *Cisco CAD Troubleshooting Guide*.

Verifying that Required Applications are Running

Recording and monitoring operations require several applications to be running. If errors occur during recording or monitoring, verify that the required applications are running. In some cases, stopping and restarting the applications might resolve the problem.

CAD supports autorecovery. The services and clients speak to each other. The client applications (Agent Desktop and Supervisor Desktop) know when a service goes down. During the time that a service is down and attempting to come back up, certain features, like monitoring and recording, will fail. Once the service comes back up, the features become available again.

Opening a TAC Case

If you are unable to discover why you cannot successfully monitor or record agent calls after looking at the debug files, you can open a TAC case. When doing this, provide the following information:

- Product version you are using
- Problem description
- Exact steps you took when you experienced the problem
- Exact text of any error messages you saw
- Debug files from the time you saw the error with the debug level set to maximum
- Configuration information for your system (How many VoIP Monitor services, desktop or service monitoring attempted, IP addresses of VoIP Monitor services, agent extensions you attempted to monitor/record, etc.)

Cisco Catalyst Switch Capabilities

A

The VoIP Monitor service is targeted specifically at the Cisco line of Catalyst switches. It might work with other switches that offer VoIP traffic, but it has not been tested on switches other than the Catalyst switch.

It is important to be aware of the differences among the Catalyst switches when using the server capture method and configuring SPAN. In addition, the version of operating system software running on the switch can affect the features related to SPAN.

Table 11 lists Cisco Catalyst switch models and SPAN-related features. Support for the feature or the functionality of that feature is indicated with a Y (yes) or N (no). This information has been gathered from switch documentation available on Cisco's website. Because switch hardware and software are continuously added and upgraded, the information in Table 11 is not guaranteed to be completely accurate. It is provided here to help in planning deployments and evaluating options for deploying VoIP servers for Cisco software. It is recommended that you consult the documentation for a customer's switches and IOS versions to ascertain the exact SPAN-related feature support for a potential installation.

The features listed in Table 11 are more fully described in the section, "SPAN-Related Feature Descriptions" on page 95.

Table 11. SPAN-related feature support for Cisco Catalyst switches

Model	Supported SPAN-Related Features[1]							
	Max SPAN Sessions	SPAN	RSPAN	VSPAN	Ingress-only/ Egress-only	VLAN Filtering on Trunk Ports	Normal Network Traffic on Destination Ports	Destination and Source Ports Must be in Same VLAN
500 Express	port count[2]	Y	N	N	N	N	Y	N
1200	1	Y	N	N	Y	N	N	N
1900	1	Y	N	N	N	N	N	N
2820	1	Y	N	N	N	N	N	N
2900XL	port count*	Y	N	Y	N	Y	Y	Y
2940	1	Y	N	N	Y	N	N	N
2948G	5	Y	Y	Y	Y	Y	Y	N
2950	1	Y	Y	N	Y	N	N	N
2955	1	Y	Y	N	Y	N	N	N
2960	2	Y	Y	Y	Y	Y	N	N
2980G	5	Y	Y	Y	Y	Y	Y	N
3550	2	Y	Y	Y	Y	N	N	N
3560	2	Y	Y	Y	Y	Y	N	N
3560-E	2	Y	Y	Y	Y	Y	N	N
3750	2	Y	Y	Y	Y	Y	N	N
3750-E	2	Y	Y	Y	Y	Y	N	N
4003	5	Y	Y	Y	Y	Y	Y	N
4006	5	Y	Y	Y	Y	Y	Y	N
4500	6	Y	Y	Y	Y	N	N	N
4912G	5	Y	Y	Y	Y	Y	Y	N
5000	5	Y	N	Y	Y	Y	Y	N
5002	5	Y	N	Y	Y	Y	Y	N
5500	5	Y	N	Y	Y	Y	Y	N

Table 11. SPAN-related feature support for Cisco Catalyst switches (cont'd)

Model	Supported SPAN-Related Features[1]							
	Max SPAN Sessions	SPAN	RSPAN	VSPAN	Ingress-only/ Egress-only	VLAN Filtering on Trunk Ports	Normal Network Traffic on Destination Ports	Destination and Source Ports Must be in Same VLAN
5505	5	Y	N	Y	Y	Y	Y	N
5509	5	Y	N	Y	Y	Y	Y	N
6000	30	Y	Y	Y	Y	Y	Y	N
6006	30	Y	Y	Y	Y	Y	Y	N
6009	30	Y	Y	Y	Y	Y	Y	N
6500	30	Y	Y	Y	Y	Y	Y	N
6509	30	Y	Y	Y	Y	Y	Y	N
6513	30	Y	Y	Y	Y	Y	Y	N

1 ERSPAN might work, but it has not been tested and therefore is not supported.

2 There is no hard limit for the number of port monitoring sessions that can be created. It is limited by the number of ports on the switch.

SPAN-Related Feature Descriptions

The column headers in Table 11 are SPAN-related features or restrictions that can affect the deployment of Cisco VoIP services. Each feature was discussed in earlier sections of this document. The sections below provide summaries so that the table's contents are clear.

Max SPAN Sessions

This column shows the maximum number of simultaneous SPAN sessions, port monitor configurations, or snooping sessions that are supported on the switch. Many of the switches have limitations on the number of sessions based on the type of traffic being captured from the source ports (for example, ingress-only) or whether VLANs are used as sources. Refer to the switch's documentation for details on these limitations.

SPAN

This column shows whether the switch supports some type of facility that allows network traffic from one or more ports to be copied to a destination port. This can be via SPAN, port monitoring, or snooping. Notice that all of the switches in Table 11 support some sort of SPAN functionality. Some very small switches or highly specialized switches do not offer this functionality, but they are not likely to be major components in a contact center network, so they are not shown.

RSPAN

This column shows whether the switch allows a SPAN destination port on one switch to get traffic from a port on another switch.

VSPAN

This column shows whether the switch supports SPAN configurations where VLANs are used to indicate the source traffic rather than having to specify individual ports.

Ingress-only/Egress-only

This column shows whether a SPAN configuration can specify the traffic direction that is to be captured:

- Only traffic entering the port (ingress-only)
- Only traffic exiting the port (egress-only)
- Both directions (ingress and egress)

Note that on some switches a SPAN configuration might only allow traffic in one direction to be copied. Refer to the switch documentation for more detail.

VLAN Filtering on Trunk Ports

This column shows whether SPAN can use a trunk port as a source port, and whether the SPAN configuration can set a filter of one or more VLAN IDs to control the traffic that is copied to the destination port.

Supported IP Phones

B

This appendix contains a list of the Cisco IP phones that are required in order to support a specific packet capture method used by Cisco software.

Desktop Capture Method

- Cisco IP Communicator Soft Phone v1.3(3) or higher
- 7911G
- 7912G-A
- 7940
- 7941G
- 7941G-GE
- 7942
- 7945
- 7960
- 7961G
- 7961G-GE
- 7962
- 7965
- 7970
- 7971G

Server Capture Method

Any Cisco IP phone that is connected via a cable to a switch that can be used for phone calls in the IP network can be used for this method of packet capture.

NOTE: This does not include wireless phones.

Unified CM Capture Method

CAD and Recording Solution support any IP phone that Unified CM supports for the Unified CM Recording and Monitoring feature. This includes the following phone models:

- 7906
- 7911
- 7921
- 7925
- 7941
- 7942
- 7945
- 7961
- 7962
- 7965
- 7970
- 7971
- 7975
- Cisco IP Communicator v7.0.2.0

Configuring Unified CM for VoIP Monitoring

C

The following settings are required to use VoIP monitoring for CAD and Recording Solution. The settings are configured in the Unified CM Administration web application.

Configuring Unified CM for Desktop Monitoring

The following settings are required for desktop monitoring.

> **NOTE:** Not all devices or versions of Unified CM use all of the settings described below. Configure the settings that appear for your device and version of Unified CM.

> **NOTE:** Secure Real-Time Transport Protocol (SRTP) is not supported with desktop monitoring in CAD.

In the Product Specific Configuration section of the Device Configuration screen, configure the following settings as described below.

- PC Port—Enabled. If the PC Port is not enabled, the agent PC that is connected to the port will not have network access. No voice streams will be seen by the desktop monitor module.
- PC Voice VLAN Access—Enabled. If the PC Voice VLAN Access is not enabled, no voice streams will be seen by the desktop if the desktop is not a member of the same VLAN as the phone.
- Span to PC Port—Enabled. If the Span to PC Port is not enabled, the voice streams seen by the phone will not be seen by the desktop monitor module.

In the Device Information section of the Device Configuration screen, configure the following setting as described below.

- Device Security Mode—Non-Secure or Authenticated. If the Device Security Mode is set to Encrypted, the voice streams can be seen but will not be converted correctly, causing the speech to be garbled.

Configuring Unified CM for Server Monitoring

The following device setting is required for server monitoring to function correctly.

In the Device Information section of the Device Configuration screen, set the Device Security Mode to Non-Secure or Authenticated. If it is set to Encrypted, the voice streams can be seen but will not be converted correctly, causing the speech to be garbled.

> **NOTE:** Secure Real-time Transport Protocol (SRTP) is not supported with server monitoring in CAD.

Configuring Unified CM for Unified CM-based Monitoring (Unified CCE Only)

The following settings are required to use Unified CM-based monitoring:

- On the Application User Configuration window, add PG user to the user group Standard CTI Allow Call Monitor. This window is available through the User Management menu.
- On the Phone Configuration (device) window of the agent who will be monitored, enable the option Build-in-bridge. The monitored agent's device must be one of the IP phone models listed above. This window is available through the Device menu.
- On the Directory Number Configuration (line appearance) window of the supervisor who will be monitoring the agent, add the DN partition of the monitored agent to the Monitoring Call Search Space. This window is available through the Device menu.

Requirements for Mobile Agent Monitoring and Recording (Unified CCE Only)

To monitor and record mobile agent phone calls, the following requirements must be satisfied.

- The caller and agent voice gateways must be separate. The VoIP Monitor service must be located in the network where it can see the traffic flowing between agents and customers. If the customer and agent are speaking to each other over the same voice gateway, their voice streams remain local to the gateway and are not exposed to the VoIP Monitor service. SPAN does not

send those packets to the VoIP Monitor service, and the conversation cannot be heard. For this reason, monitoring and recording calls from one mobile agent to another mobile agent is not supported.

- Mappings between the agent voice gateways and VoIP Monitor services must be configured using Cisco Desktop Administrator. For instructions, see the section about mobile agent monitoring in the *Cisco Desktop Administrator User Guide*.
- Cisco Catalyst switches use SPAN (Switched Port ANalyzer) to monitor ports, which is required for mobile agent monitoring. For this reason, VoIP Monitor services must be connected to Cisco Catalyst switches that can sniff the agent voice gateways.
- The VoIP Monitor service identifies voice packets using the IP address of the agent voice gateways. The layer-2 MAC address rewrite issues associated with server monitoring/recording of non-mobile agents does not apply.
- Mobile Agent Monitoring is part of a VoIP Monitor service method. Configuration is also required on the switch in this case. A SPAN session is required for each Agent Voice Gateway that the Monitor Server will be monitoring.