Configuring and Troubleshooting VoIP Monitoring

March 2009

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
## Contents

### 1 VoIP Monitoring Concepts  7
- Introduction  7
  - Definitions  8
- Networks  10
- Packet Data  13
- Capturing an IP Phone Call  14
- Accessing Audio Streams  17
  - Identifying Audio Streams  19
  - Packet Capture Methods  20
    - Desktop Capture Method  21
    - Server Capture Method  22
    - Unified CM Capture Method  23

### 2 Deployment Issues  27
- Introduction  27
  - Remote Agents  27
  - Mobile Agents  29
- Packet Capture Methods Used in Cisco Monitoring and Recording Software  30
  - Cisco Agent Desktop  30
  - Quality Monitoring  31
- NDIS-Compliant NICs  33
- Agent Phones  33
  - Desktop Capture Method  33
  - Server Capture Method  34
  - Unified CM Capture Method  34
- SPAN  34
- RSPAN  36
- VLANs  38
- Port Traffic Direction  40
- Media Mixing  44
- Gateway SPAN Sniffing  46
3 The NIC Qualification Utility 63

- Overview 63
- Assumptions 65
- Utility Syntax 66
  - Running the NICQ Utility 66
  - Output From the NIC Qualification Tool 67
- NICQ Tests 69
  - Test 1—Check Driver Status 69
  - Test 2—Retrieve List of Valid Network Adapters 69
  - Test 3—Capture Packets 69
  - Test 4—Detect Attached IP Phones 70
  - Test 5—Detect Promiscuous Traffic 72
  - Successful Test Report Example 72
- Using Multiple NICs with the VoIP Monitor Service 75
- Limitations 76
- Issues 77
- Installing a Second NIC in a VoIP Monitor Service Server 78
  - Additional Configuration Steps 78
4 Troubleshooting VoIP Monitoring and Recording  81
  ■ Introduction  81
  ■ Troubleshooting CAD  82
    Identifying the Problem’s Location  82
    Common Issues  85
    Monitored Call is Inaudible  87
    Monitor Button is Disabled  90
    Record Button is Disabled  90
    Recording File is Empty  91
    Speech is Garbled  91
      Audio Stops and Starts Rapidly and Repeatedly  92
      Audio is Slowed Down  93
      Only One Party on the Call is Audible  93
      Audio is Hard to Hear  93
      Audio Has Gaps  94
      Extraneous Noise in Audio  95
    Operation Fails Without An Error  95
    Operation Ends Prematurely  96
    Audio is Distorted  96
    New NIC Breaks Feature  97
    Calls Between Mobile Agents are Inaudible  97
    IP Address of Agent's Voice Gateway Changes  98
    Some Mobile Agents Cannot Be Monitored  98
    Monitoring Will Not Start  98
  ■ Troubleshooting Procedures  99
    Verifying Sound Card Functionality  99
    Verifying Desktop Administrator Settings  100
    Verifying Registry Settings  100
    Testing the Sniffing Adapter  101
    Testing the Desktop Monitor Library  101
    Using Debugging Files  101
    Opening a TAC Case  102
    Verifying that NICs Can Be Sniffed  102
Contents

Verifying that the Correct NIC Is Being Used 103
Verifying that Required Applications are Running 103

A Cisco Catalyst Switch Capabilities 105
   SPAN-Related Feature Descriptions 107

B Supported IP Phones 109
   Desktop Capture Method 109
   Server Capture Method 109
   Unified CM Capture Method 110

C Configuring Unified CM for VoIP Monitoring 111
   Configuring Unified CM for Desktop Monitoring 111
   Configuring Unified CM for Server Monitoring 112
   Configuring Unified CM for Unified CM-based Monitoring (Unified CCE Only) 112
   Requirements for Mobile Agent Monitoring and Recording (Unified CCE Only) 112
VoIP Monitoring Concepts

Introduction

Cisco software products for IP contact centers have the ability to silently 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 Quality Management for Unified Contact Center Express

To implement these silent 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAD</td>
<td>Cisco Agent Desktop is a suite of applications used by contact centers to handle incoming and outgoing calls.</td>
</tr>
<tr>
<td>Call recording</td>
<td>Application feature found in CAD and QM 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.</td>
</tr>
<tr>
<td>Desktop monitoring</td>
<td>A packet capturing configuration 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.</td>
</tr>
<tr>
<td>Endpoint device</td>
<td>A device, such as a PC or IP phone, with a NIC and IP address that can send or receive network packets.</td>
</tr>
<tr>
<td>Hard IP phone</td>
<td>A physical IP phone that is plugged into the network.</td>
</tr>
<tr>
<td>IP (network) switch</td>
<td>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.</td>
</tr>
<tr>
<td>Packet capture</td>
<td>The process of capturing network traffic from the network fabric for processing. In most cases, the traffic is captured in promiscuous mode.</td>
</tr>
<tr>
<td>Promiscuous mode</td>
<td>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.</td>
</tr>
<tr>
<td>QM</td>
<td>Quality Management, a suite of applications used by contact centers to record business calls and use those calls to evaluate agents and processes.</td>
</tr>
<tr>
<td>RSPAN</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 1. Terms and definitions (cont’d)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP</td>
<td>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.</td>
</tr>
<tr>
<td>Server monitoring</td>
<td>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.</td>
</tr>
<tr>
<td>Silent monitoring</td>
<td>An application feature in CAD 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.</td>
</tr>
<tr>
<td>Soft IP phone</td>
<td>A soft IP phone is a computer application that emulates a hard IP phone and runs on an agent's PC.</td>
</tr>
<tr>
<td>SPAN</td>
<td>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.</td>
</tr>
<tr>
<td>Unified CM monitoring</td>
<td>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 further processing.</td>
</tr>
<tr>
<td>VLAN</td>
<td>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.</td>
</tr>
</tbody>
</table>
Networks

Mike wants to connect his two computers together so he can share data between them. To do this he must create a computer network. The simplest network is two computers directly connected to each other with a cable (Figure 1).

Figure 1. A simple network

As long as the two computers speak the same language, they can exchange data with each other.

Problems arise as Mike adds more computers. Now he need a separate cable for every computer he wants to exchange data with (Figure 2). This quickly becomes unmanageable.

Figure 2. An unmanageable network

To alleviate this maze of cables, hardware devices were created that can connect multiple computing devices together (Figure 3). These hardware devices are called
switches, hubs, routers, or gateways, depending on the connectivity features they offer.

**Figure 3.** A packet-switched network

The switch shown in Figure 3 connects all 11 computers together so they can communicate and exchange data. In order for this to work, though, each computer in this network must have a unique name or address so only those chunks of data meant for it are sent to it. Also, all the computers in the network must use the same language and data format or they won't be able to understand the messages.

The language, or protocol, that all the computers (and the switch) speak is called the Internet Protocol (IP). The IP is a specification for encoding data that is sent over a network. IP can contain data of many different types. There are many other protocols that define this data and that can be carried over an IP network. This is called encapsulation, and will be discussed later.

Each computer in Figure 3 has at least one network interface card (NIC). The NIC is a hardware card that plugs into the computer and has a socket for attaching a network cable. The cable connects the computer's NIC to the switch. Software on the computer that understands IP is able to send data out through the NIC to another machine on the network, or receive incoming data to be used by applications running on the computer. Each NIC has a unique number associated with it called a media access control (MAC) address. The MAC address uniquely defines an endpoint on a network. An example of a MAC address is 0122FCE89C12.

In order to allow easier identification of computers on a network and to allow for more flexible routing and network design, IP addresses, in addition to MAC addresses, are usually used to identify particular network end points. An IP address (for example,
192.168.10.1) is assigned to each end point on the network, either directly on the computer or via an address-assigning service like Dynamic Host Configuration Protocol (DHCP). The end result is that each end point on the network has a unique address that can be used to send data to.

IP addresses are used not only to identify specific end points, but also the network itself and any sub-networks. For example, all the end points whose IP address starts with 192.168.20 are parts of the 192.168.20 subnet. A subnet can also be called a local area network (LAN). There are many ways to group end points and there are many names used to describe them. Some of these end point grouping names include:

- WAN (wide area network)
- VLAN (virtual local area network)
- WLAN (wireless local area network)
- MAN (metropolitan area network)
- PAN (personal area network)
- GAN (global area network)

The network shown in Figure 3 is a simple packet-switched network than can exist in Mike’s basement, but is not usually found in the real world. Real-world networks can be quite complex, containing thousands of end points, routers, switches, gateways, and hubs. The World Wide Web/Internet is probably the best-known (and most complex) network that spans the entire globe.

---

1. DHCP is a protocol used by networked devices to obtain the parameters necessary for operation in an IP network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configuration.
Packet Data

The pieces of data sent over an IP network are called packets. A packet of data is a discrete chunk of data formatted per the protocol definition of the container. The container can be thought of as an envelope, and the letter in the envelope is the data that is being sent. Different layers of software take the data and encase it in a protocol envelope before passing it to the next layer. When the packet of data arrives at the end point, layers of software unwrap the message and pass it to the next layer, eventually delivering the data to the application.

As mentioned previously, IP supports many different protocols used for describing data sent over the network. Some of these protocols can carry other sub-protocols as well. When data is sent over the network, each protocol layer is like a smaller envelope stuffed into a larger envelope. The largest envelope is that which contains the proper IP addressing and format to be sent over the network. This is shown conceptually in Figure 4.

Figure 4. Data packaging
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 recording and monitoring software is written to work with specific switches and other network hardware. At this time, it supports particular Cisco Systems hardware and software used in IP contact center installations. The information below refers to specific Cisco hardware and software that Cisco software works with.

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 5 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 5. 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 6, an audio stream is made up of many individual data packets sent over the network.

**Figure 6. RTP audio stream**

The RTP packets are encapsulated in UDP, IP, and Ethernet envelopes as shown in Figure 7.

**Figure 7. 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 6.

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. Cisco monitoring and recording software is able to read the encoded audio data and convert it to a format like Windows Media Audio (WMA) or WAV format to be stored or played back on a PC.
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 8).

Figure 8. 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 9). 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 9. 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 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 10. 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. For this, it needs 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.
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.

<table>
<thead>
<tr>
<th>Application</th>
<th>Feature</th>
<th>Deployment</th>
<th>Identification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Desktop Capture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local†</td>
<td>MAC</td>
</tr>
<tr>
<td>CAD</td>
<td>Monitoring</td>
<td>VPN</td>
<td>MAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Thin client</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile agent</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPPA</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Recording</td>
<td>Local</td>
<td>MAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VPN</td>
<td>MAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Thin client</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile agent</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPPA</td>
<td>—</td>
</tr>
<tr>
<td>QM</td>
<td>Recording</td>
<td>Local</td>
<td>MAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Thin client</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VPN</td>
<td>MAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile agent</td>
<td>—</td>
</tr>
</tbody>
</table>

* 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 11 shows that this capture method can work with either a hard or soft IP phone.

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 silent 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 QM 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 23 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 QM. QM 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 47 for more information.

**Unified CM Capture Method**

This method of capturing audio packets is a recently-added feature to the Unified CM software and used only in a Unified Contact Center Enterprise environment. It is meant to provide a well-documented method for third-party software to have access to agent call audio streams.
This feature enables an application to send a command through an interface library to the IP phone. This command causes the phone to duplicate the two audio streams and send them to a particular IP address and port for further processing.

**Figure 12. Unified CM capture method**

In **Figure 12**, two IP phones are on a call with each other exchanging streams 1 and 2. The phones are sending their audio streams directly to each other. If a supervisor wants to monitor the call, software sends a command to one of the phones on the call to tell it to mix the two streams and send this mixed stream directly to the supervisor's IP phone. This is shown as stream 3 in **Figure 12**. When the monitoring function starts, the supervisor's phone calls the agent device, which answers and allows the supervisor to hear the mixed conversation.

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

- The agent uses Cisco Agent Desktop
- The agent is local or remote (over a VPN connection)
- The agent uses a hard IP phone

At this time, no Cisco monitoring and recording products support the Unified CM method for call recording. In addition, if this method is configured in CAD for silent monitoring, the desktop capture and server capture methods are turned off. The result is that agents can be silently 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 QM 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 QM 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.

Because of the limited support for the Unified CM method of capturing packets, this document concentrates on the other two packet capture methods to support Cisco product features.

Requirements
Using the Unified CM capture method for CAD silent monitoring requires the following:

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

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 silent 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 silent 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 silent 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 13. 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. (QM 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 47.

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 remote agents who use a hard IP phone and a VPN router. The soft IP phone does not support Unified CM monitoring.

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 14. 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 cannot 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 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 silent 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 silent 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 silent 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 silent 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, QM 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. QM can be run in a thin-client (Citrix or Microsoft Terminal Services) environment. Agent call recording is supported using the desktop capture and server capture methods.
This information is summarized in Table 3.

### Table 3. Packet capture methods supported, by application

<table>
<thead>
<tr>
<th>Product</th>
<th>Client App</th>
<th>Agent Type</th>
<th>Feature</th>
<th>Capture Method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Desktop</td>
</tr>
<tr>
<td>CAD</td>
<td>Agent Desktop</td>
<td>On-site</td>
<td>Monitoring</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Recording</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote</td>
<td>Monitoring</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Recording</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile</td>
<td>Monitoring</td>
<td>n</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Recording</td>
<td>n</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Thin client</td>
<td>Monitoring</td>
<td>n</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Recording</td>
<td>n</td>
</tr>
<tr>
<td>CAD-BE</td>
<td>On-site</td>
<td>Monitoring</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recording</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Remote</td>
<td>Monitoring</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recording</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Mobile</td>
<td>Monitoring</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recording</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>IPPA</td>
<td>On-site</td>
<td>Monitoring</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recording</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Remote</td>
<td>Monitoring</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recording</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>QM</td>
<td>Recording</td>
<td>On-site</td>
<td>Recording</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote</td>
<td>Recording</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile</td>
<td>Recording</td>
<td>n</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Thin client</td>
<td>Recording</td>
<td>n</td>
</tr>
</tbody>
</table>

* Only supported application configurations are shown.
† With a supported hard IP phone. If remote, a hardware VPN solution must be employed.
NDIS-Compliant NICs

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

**NOTE:** Where supported, the Unified CM capture method of monitoring 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 computer 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**

This capture method is used only in a Unified Contact Center Enterprise environment, and only specific Cisco IP phones support it. The phone's software needs to be able to support the commands sent to it from the Unified CM.

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 15).
In Figure 15, 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 16, 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.
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 17.
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 50.

In Figure 17, 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 18.
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 18, 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 19 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 20.
As can be see in Figure 20, 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 18, 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 21.

**Figure 21.** Egress-only SPAN issue for non-monitored port

In Figure 21, 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 22). This port is usually connected to a voice gateway device that is used to convert analog phone calls to IP-based phone calls.
In Figure 22, 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 23, but calls might contain more than two parties. When calls are conference calls, several...
March 2009 45

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

Figure 23. 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 24).

Figure 24. 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 24, 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 25. 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 25, 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 QM) 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.
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 26. 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 27).
To illustrate this, Figure 27 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 52).

**NOTE:** CAD has software-enforced capacity limitations. QM 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 in Appendix 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>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many agents do you have?</td>
<td></td>
</tr>
<tr>
<td>How many agents will be monitored?</td>
<td></td>
</tr>
<tr>
<td>How many agents will be recorded?</td>
<td></td>
</tr>
<tr>
<td>How many non-agents will be recorded?</td>
<td></td>
</tr>
<tr>
<td>What is the maximum number of agents that might be logged in simultaneously?</td>
<td></td>
</tr>
<tr>
<td>How many agents are local to the contact center site?</td>
<td></td>
</tr>
<tr>
<td>How many remote agents do you have?</td>
<td></td>
</tr>
<tr>
<td>How many mobile agents do you have?</td>
<td></td>
</tr>
<tr>
<td>How many agents have a desktop PC that will run the Cisco monitoring and recording software?</td>
<td></td>
</tr>
<tr>
<td>How many agents have only an IP phone?</td>
<td></td>
</tr>
<tr>
<td>How many contact center sites are there?</td>
<td></td>
</tr>
<tr>
<td>Is agent-to-agent recording or monitoring required?</td>
<td></td>
</tr>
<tr>
<td>Do agents with desktops share a network connection with their IP phone?</td>
<td></td>
</tr>
<tr>
<td>How many agents use soft IP phones on their desktop?</td>
<td></td>
</tr>
</tbody>
</table>

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 QM. CAD will be used to manage the agents and automate common tasks. They will use the CAD silent monitoring feature, but not the on-demand recording feature. QM 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

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many agents do you have?</td>
<td>10</td>
</tr>
<tr>
<td>How many agents will be monitored?</td>
<td>10</td>
</tr>
<tr>
<td>How many agents will be recorded?</td>
<td>10</td>
</tr>
<tr>
<td>How many non-agents will be recorded?</td>
<td>0</td>
</tr>
<tr>
<td>What is the maximum number of agents that might be logged in simultaneously?</td>
<td>10</td>
</tr>
<tr>
<td>How many agents are local to the contact center site?</td>
<td>10</td>
</tr>
<tr>
<td>How many remote agents do you have?</td>
<td>0</td>
</tr>
<tr>
<td>How many mobile agents do you have?</td>
<td>0</td>
</tr>
<tr>
<td>How many agents have a desktop PC that will run the Cisco monitoring and recording software?</td>
<td>10</td>
</tr>
<tr>
<td>How many agents have only an IP phone?</td>
<td>0</td>
</tr>
<tr>
<td>How many contact center sites are there?</td>
<td>1</td>
</tr>
</tbody>
</table>
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.

ABC Company’s network diagram is shown in Figure 28.

Figure 28. 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

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is agent-to-agent recording or monitoring required?</td>
<td>Yes</td>
</tr>
<tr>
<td>Do agents with desktops share a network connection with their IP phone?</td>
<td>Yes</td>
</tr>
<tr>
<td>How many agents use soft IP phones on their desktop?</td>
<td>0</td>
</tr>
</tbody>
</table>
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 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 QM 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 QM 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**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many agents do you have?</td>
<td>300</td>
</tr>
<tr>
<td>How many agents will be monitored?</td>
<td>0</td>
</tr>
<tr>
<td>How many agents will be recorded?</td>
<td>300</td>
</tr>
<tr>
<td>How many non-agents will be recorded?</td>
<td>0</td>
</tr>
<tr>
<td>What is the maximum number of agents that might be logged in simultaneously?</td>
<td>300</td>
</tr>
<tr>
<td>How many agents are local to the contact center site?</td>
<td>20</td>
</tr>
<tr>
<td>How many remote agents do you have?</td>
<td>280</td>
</tr>
<tr>
<td>How many mobile agents do you have?</td>
<td>0</td>
</tr>
<tr>
<td>How many agents have a desktop PC that will run the Cisco software?</td>
<td>300</td>
</tr>
<tr>
<td>How many agents have only an IP phone?</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 6. International Sprockets questionnaire (cont'd)

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many contact center sites are there?</td>
<td>280</td>
</tr>
<tr>
<td>Is agent-to-agent recording or monitoring required?</td>
<td>Yes</td>
</tr>
<tr>
<td>Do agents with desktops share a network connection with their IP phone?</td>
<td>Yes</td>
</tr>
<tr>
<td>How many agents use soft IP phones on their desktop?</td>
<td>0</td>
</tr>
</tbody>
</table>

Although the agents in the branch offices are widely scattered geographically, the network is still fairly simple. QM supports both desktop and server capture methods.
Examples of Deployment Planning

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.

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 QM 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

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many agents do you have?</td>
<td>75</td>
</tr>
<tr>
<td>How many agents will be monitored?</td>
<td>26</td>
</tr>
<tr>
<td>How many agents will be recorded?</td>
<td>75</td>
</tr>
<tr>
<td>How many non-agents will be recorded?</td>
<td>0</td>
</tr>
<tr>
<td>What is the maximum number of agents that might be logged in simultaneously?</td>
<td>75</td>
</tr>
<tr>
<td>How many agents are local to the contact center site?</td>
<td>72</td>
</tr>
<tr>
<td>How many remote agents do you have?</td>
<td>0</td>
</tr>
<tr>
<td>How many mobile agents do you have?</td>
<td>3</td>
</tr>
</tbody>
</table>
Table 7. Redundant Systems questionnaire (cont’d)

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many agents have a desktop PC that will run the Cisco software?</td>
<td>67</td>
</tr>
<tr>
<td>How many agents have only an IP phone?</td>
<td>8</td>
</tr>
<tr>
<td>How many contact center sites are there?</td>
<td>1</td>
</tr>
<tr>
<td>Is agent-to-agent recording or monitoring required?</td>
<td>Rec: Yes</td>
</tr>
<tr>
<td></td>
<td>Mon: No</td>
</tr>
<tr>
<td>Do agents with desktops share a network connection with their IP phone?</td>
<td>Yes</td>
</tr>
<tr>
<td>How many agents use soft IP phones on their desktop?</td>
<td>64</td>
</tr>
</tbody>
</table>

Figure 30. 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 30. These will be removed and replaced with QM VoIP servers for any server-based captures used for recording calls.

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

- We must use the server capture method for all agents for the following reasons:
  - The 64 agents with PCs and soft IP phones will be running CAD and QM 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 cannot use the desktop capture method for them.
  - The three mobile agents are using cell phones that are not connected to their laptops, so we cannot 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 QM VoIP server will be required to satisfy the customer’s recording redundancy concern.

The easiest solution is to connect a QM 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 QM VoIP servers to the core switches as shown in Figure 31.

Figure 31. 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 QM VoIP server to that switch as the destination. Only the QM 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

Overview

The Network Interface Card Qualification (NICQ) utility is available in the following versions of CAD:

- CAD 6.4(2) for Unified CCX 5.0(2)
- 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.

For a list of tested NICs, see *NICs tested with Cisco CTI Toolkit Desktop Silent Monitor - Reference Information [Cisco Agent Desktop]*, available at:


For a procedure for testing NICs for compatibility, see Technote 46301, *Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring*, available at:

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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-?</td>
<td>Causes the usage screen to be displayed.</td>
</tr>
<tr>
<td>-o</td>
<td>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.</td>
</tr>
<tr>
<td>-t</td>
<td>Indicates how long the utility will listen on each NIC for network traffic. The default is 20 seconds.</td>
</tr>
<tr>
<td>-p</td>
<td>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.</td>
</tr>
<tr>
<td>-s</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

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

Test 2—Retrieve List of Valid Network Adapters

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

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.

<table>
<thead>
<tr>
<th>Test</th>
<th>Corrective Action if Test Fails</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open the adapter</td>
<td>• Verify that system/kernel memory is not below 5 Mb</td>
</tr>
<tr>
<td></td>
<td>• Verify that the driver is loaded</td>
</tr>
<tr>
<td>Capture network traffic</td>
<td>• Verify that the NIC is active</td>
</tr>
<tr>
<td></td>
<td>• Verify that the NIC is connected to the network and that the cable is good</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Test</th>
<th>Corrective Action if Test Fails</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check for SCCP KeepAlive messages</td>
<td>• Verify that the IP phone is connected inline with the NIC being tested</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the phone uses SCCP</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the IP phone is configured correctly in Unified CM to pass the traffic out its second network port</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the SCCP port is 2000 in Unified CM</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Check for SIP REGISTER messages</td>
<td>• Verify that the IP phone is connected inline with the NIC being tested</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the phone uses SIP</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the IP phone is configured correctly in Unified CM to pass the traffic out its second network port</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Test</th>
<th>Corrective Action if Test Fails</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check for promiscuous traffic</td>
<td>• Verify that a daisy-chained phone is configured to send voice traffic out its second network port</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the capture time is long enough. Use the -t parameter to increase the time, if necessary.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Look for documented workarounds for this NIC to get it to work correctly in promiscuous mode</td>
</tr>
<tr>
<td></td>
<td>• Update driver to the latest version and retest</td>
</tr>
<tr>
<td>Check for RTP traffic</td>
<td>• Ensure that there is a phone call or simulated RTP traffic exposed to the NIC being tested. Make a call to the IP phone.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

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}
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

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Count</th>
<th>Packet Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.50.104</td>
<td>10.10.10.124</td>
<td>89</td>
<td>UDP/RTP: (0) PCMU (uLaw G.711 Audio)</td>
</tr>
<tr>
<td>10.10.10.124</td>
<td>10.10.50.104</td>
<td>89</td>
<td>UDP/RTP: (0) PCMU (uLaw G.711 Audio)</td>
</tr>
<tr>
<td>10.10.50.1</td>
<td>255.255.255.255</td>
<td>1</td>
<td>UDP (17)</td>
</tr>
<tr>
<td>10.10.50.1</td>
<td>255.255.255.255</td>
<td>2</td>
<td>ARP</td>
</tr>
<tr>
<td>10.10.50.104</td>
<td>172.17.12.20</td>
<td>1</td>
<td>TCP (6)</td>
</tr>
<tr>
<td>10.10.50.104</td>
<td>10.10.10.124</td>
<td>884</td>
<td>UDP/RTP: (0) PCMU (uLaw G.711 Audio)</td>
</tr>
<tr>
<td>10.10.10.124</td>
<td>10.10.50.104</td>
<td>884</td>
<td>UDP/RTP: (0) PCMU (uLaw G.711 Audio)</td>
</tr>
<tr>
<td>172.17.12.20</td>
<td>10.10.50.104</td>
<td>1</td>
<td>TCP (6)</td>
</tr>
<tr>
<td>10.10.50.1</td>
<td>255.255.255.255</td>
<td>12</td>
<td>UDP (17)</td>
</tr>
<tr>
<td>10.10.10.124</td>
<td>10.10.50.104</td>
<td>4</td>
<td>ARP</td>
</tr>
<tr>
<td>10.10.50.1</td>
<td>224.0.0.10</td>
<td>4</td>
<td>unknown (88)</td>
</tr>
<tr>
<td>10.10.49.108</td>
<td>10.10.49.255</td>
<td>1</td>
<td>UDP (17)</td>
</tr>
<tr>
<td>10.10.50.1</td>
<td>255.255.255.255</td>
<td>18</td>
<td>ARP</td>
</tr>
<tr>
<td>10.10.49.1</td>
<td>224.0.0.10</td>
<td>4</td>
<td>unknown (88)</td>
</tr>
<tr>
<td>10.10.50.104</td>
<td>10.10.10.124</td>
<td>2</td>
<td>ARP</td>
</tr>
<tr>
<td>10.10.49.117</td>
<td>172.17.10.18</td>
<td>46</td>
<td>TCP (6)</td>
</tr>
<tr>
<td>172.17.10.18</td>
<td>10.10.49.117</td>
<td>28</td>
<td>TCP (6)</td>
</tr>
</tbody>
</table>

Device: \Device\Splkpc_{06FF0278-AA0F-44C0-933F-220AD13FDCC2} (10.0.9.162)
Packet capture completed successfully

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Count</th>
<th>Packet Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.50.104</td>
<td>10.10.10.142</td>
<td>89</td>
<td>UDP/RTP: (0) PCMU (uLaw G.711 Audio)</td>
</tr>
<tr>
<td>10.10.10.142</td>
<td>10.10.50.104</td>
<td>89</td>
<td>UDP/RTP: (0) PCMU (uLaw G.711 Audio)</td>
</tr>
<tr>
<td>10.10.50.1</td>
<td>255.255.255.255</td>
<td>1</td>
<td>UDP (17)</td>
</tr>
<tr>
<td>10.10.50.1</td>
<td>255.255.255.255</td>
<td>2</td>
<td>ARP</td>
</tr>
<tr>
<td>10.10.50.104</td>
<td>172.17.12.20</td>
<td>1</td>
<td>TCP (6)</td>
</tr>
<tr>
<td>10.10.50.104</td>
<td>10.10.10.142</td>
<td>884</td>
<td>UDP/RTP: (0) PCMU (uLaw G.711 Audio)</td>
</tr>
<tr>
<td>10.10.10.142</td>
<td>10.10.50.104</td>
<td>884</td>
<td>UDP/RTP: (0) PCMU (uLaw G.711 Audio)</td>
</tr>
<tr>
<td>172.17.12.20</td>
<td>10.10.50.104</td>
<td>1</td>
<td>TCP (6)</td>
</tr>
<tr>
<td>10.10.50.1</td>
<td>255.255.255.255</td>
<td>12</td>
<td>UDP (17)</td>
</tr>
<tr>
<td>10.10.10.142</td>
<td>10.10.50.104</td>
<td>4</td>
<td>ARP</td>
</tr>
<tr>
<td>10.10.50.1</td>
<td>224.0.0.10</td>
<td>4</td>
<td>unknown (88)</td>
</tr>
<tr>
<td>10.10.49.108</td>
<td>10.10.49.255</td>
<td>1</td>
<td>UDP (17)</td>
</tr>
<tr>
<td>10.10.50.1</td>
<td>255.255.255.255</td>
<td>18</td>
<td>ARP</td>
</tr>
<tr>
<td>10.10.49.1</td>
<td>224.0.0.10</td>
<td>4</td>
<td>unknown (88)</td>
</tr>
<tr>
<td>10.10.50.104</td>
<td>10.10.10.142</td>
<td>2</td>
<td>ARP</td>
</tr>
<tr>
<td>10.10.49.117</td>
<td>172.17.10.18</td>
<td>46</td>
<td>TCP (6)</td>
</tr>
<tr>
<td>172.17.10.18</td>
<td>10.10.49.117</td>
<td>28</td>
<td>TCP (6)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>IP Address:</th>
<th>10.10.50.104</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address:</td>
<td>00062895B091</td>
</tr>
<tr>
<td>Host Name:</td>
<td>SEP00062895B091</td>
</tr>
<tr>
<td>Phone DN:</td>
<td>7639712175</td>
</tr>
<tr>
<td>App Load ID:</td>
<td>P003080000400</td>
</tr>
<tr>
<td>Configuration Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Boot Load ID</td>
<td>PC03A300</td>
</tr>
<tr>
<td>Version</td>
<td>8.0(4.0)</td>
</tr>
<tr>
<td>Model Number</td>
<td>CP-7940</td>
</tr>
<tr>
<td>TFTP Server</td>
<td>172.17.12.20</td>
</tr>
<tr>
<td>Operational VLAN ID</td>
<td>110</td>
</tr>
<tr>
<td>CallManager 1</td>
<td>SPLKCCMS Active</td>
</tr>
<tr>
<td>CallManager 2</td>
<td>SPLKCCMP Standby</td>
</tr>
<tr>
<td>CallManager 3</td>
<td></td>
</tr>
<tr>
<td>CallManager 4</td>
<td></td>
</tr>
<tr>
<td>CallManager 5</td>
<td></td>
</tr>
<tr>
<td>DHCP Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>PC Port Disabled</td>
<td>No</td>
</tr>
<tr>
<td>SW Port Configuration</td>
<td>AUTO</td>
</tr>
<tr>
<td>PC Port Configuration</td>
<td>AUTO</td>
</tr>
<tr>
<td>Voice VLAN Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Mode</td>
<td>Non Secure</td>
</tr>
<tr>
<td>** Network Port Details **</td>
<td></td>
</tr>
<tr>
<td>Neighbor Device ID</td>
<td>Switch10.4.spanlink.com</td>
</tr>
<tr>
<td>Neighbor IP Address</td>
<td>10.10.49.1</td>
</tr>
<tr>
<td>Neighbor Port</td>
<td>FastEthernet0/3</td>
</tr>
<tr>
<td>Port Information</td>
<td>Full, 100</td>
</tr>
<tr>
<td>** Access Port Details **</td>
<td></td>
</tr>
<tr>
<td>Neighbor Device ID</td>
<td></td>
</tr>
<tr>
<td>Neighbor IP Address</td>
<td></td>
</tr>
<tr>
<td>Neighbor Port</td>
<td></td>
</tr>
<tr>
<td>Port Information</td>
<td>Full, 100</td>
</tr>
</tbody>
</table>
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 Silent 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:

Limitations

Since Cisco Unified Communications Manager does not support two NICs, using multiple NICs works only in configurations where Cisco Unified Communications Manager is not co-resident with the VoIP Monitor service.

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.
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 silently 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 streams 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 silent 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 silent monitoring and recording features might not work.
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 QM 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 CAD

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

Identifying the Problem’s Location

Figure 32 displays the major components involved when the silent monitoring or recording features are used in CAD. Components for both desktop and server monitoring are shown. The numbered starbursts indicate where a failure of a component or a configuration error can cause silent monitoring or recording to malfunction or fail.

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

Table 9. Possible causes of failure in monitoring/recording

<table>
<thead>
<tr>
<th>No.</th>
<th>Component</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Supervisor</td>
<td>• Listening to the speakers of the correct computer?</td>
</tr>
</tbody>
</table>
Table 9. Possible causes of failure in monitoring/recording (cont’d)

<table>
<thead>
<tr>
<th>No.</th>
<th>Component</th>
<th>Issue</th>
</tr>
</thead>
</table>
| 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   | Supervisor workstation | • Is Cisco Supervisor Desktop running correctly?  
• Any errors reported?  
• Is the call still active?  
• Are the callers speaking?  
• Is silent 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 switch            | • Are switch ports configured correctly?  
• Is SPAN set up correctly?  
• Is the switch running smoothly? |
### Table 9. Possible causes of failure in monitoring/recording (cont’d)

<table>
<thead>
<tr>
<th>No.</th>
<th>Component</th>
<th>Issue</th>
</tr>
</thead>
</table>
| 7   | 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 it daisy-chained to the agent’s PC?  
• Is the cable good?  
• Is it connected to the correct NIC on the agent’s PC?  
• Is there more than one IP phone daisy-chained?  
• 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 it plugged into a switch port that is part of the SPAN? |
| 8   | IP phone configuration | • Is the phone configured correctly in Unified CM?  
• Is it set to send voice packets out the second network port?  
• Is it using a codec other than G.711 or G.729?  
• Is the phone shown as being registered and active?  
• Is extension mobility configured, and is the agent logged into the extension mobility service?  
• Is extension mobility configured correctly? |
| 9   | 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? |
| 10  | Registry entries        | • Is Cisco Agent Desktop installed correctly?  
• Is the Monitor Device entry in the registry correct for the NIC that is connected to the phone? |
Table 9. Possible causes of failure in monitoring/recording (cont’d)

<table>
<thead>
<tr>
<th>No.</th>
<th>Component</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Agent desktop</td>
<td>• Is Cisco Agent Desktop installed correctly?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is an unsupported soft phone being used?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is unsupported VPN software being used?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is the software reporting any errors?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is the desktop monitor subsystem active and functioning?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Are there available CPU resources?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Are the monitoring and recording features shown as “in service”?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Does the agent have an active call?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is the SPCD driver running and loaded?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Are packets being captured from the NIC?</td>
</tr>
<tr>
<td>12</td>
<td>VoIP Monitor service</td>
<td>• Is the service installed correctly?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is the service active?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Does the service have connectivity with other components and the required database?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Are there available CPU resources?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Are any errors being reported in the log files?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is the SPCD driver running and loaded?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Are packets being captured from the NIC?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is the server behind a firewall or router?</td>
</tr>
<tr>
<td>13</td>
<td>Recording &amp; Playback service</td>
<td>• Is the service installed correctly?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is the service active?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is the disk full?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Does the recording file exist?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is the server behind a firewall or router?</td>
</tr>
<tr>
<td>14</td>
<td>CAD configuration</td>
<td>• Is the agent configured correctly?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Is the agent and his/her device configured for the correct method of packet sniffing?</td>
</tr>
</tbody>
</table>

**Common Issues**

Table 10 lists some of the issues that might be encountered with VoIP monitoring and recording. 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.

If you are experiencing an issue that is related to VoIP 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>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitored Call is Inaudible (page 87)</td>
<td>Supervisor selects an agent to monitor and clicks Monitor. Supervisor Desktop displays the speaker icon next to the call, but supervisor cannot hear anyone speaking.</td>
<td>Common</td>
</tr>
<tr>
<td>Monitor Button is Disabled (page 90)</td>
<td>Supervisor selects an agent to monitor. Monitor button is disabled in Supervisor Desktop.</td>
<td>Common</td>
</tr>
<tr>
<td>Record Button is Disabled (page 90)</td>
<td>Supervisor selects an agent to record. Record button is disabled in Supervisor Desktop.</td>
<td>Common</td>
</tr>
<tr>
<td>Recording File is Empty (page 91)</td>
<td>Recording file is only 1 KB long and does not contain any audio.</td>
<td>Common</td>
</tr>
<tr>
<td>Calls Between Mobile Agents are Inaudible (page 97)</td>
<td>Can't hear mobile agent-to-mobile agent calls.</td>
<td>Common</td>
</tr>
<tr>
<td>Speech is Garbled (page 91)</td>
<td>Supervisor hears garbled speech when monitoring or recording an agent.</td>
<td>Occasional</td>
</tr>
<tr>
<td>Operation Fails Without An Error (page 95)</td>
<td>Supervisor selects an agent to monitor (record) and clicks Monitor (or Record). The Monitor (or Record) button returns to the unclicked state, but no error is displayed.</td>
<td>Occasional</td>
</tr>
<tr>
<td>Operation Ends Prematurely (page 96)</td>
<td>The monitored call or recording file ends unexpectedly.</td>
<td>Occasional</td>
</tr>
<tr>
<td>Some Mobile Agents Cannot Be Monitored (page 98)</td>
<td>Not all mobile agents can be monitored.</td>
<td>Occasional</td>
</tr>
</tbody>
</table>
Monitored Call is Inaudible

**Problem.** Supervisor selects an agent to monitor and clicks Monitor. The speaker icon is displayed next to the call, but the supervisor cannot hear anything.

**Cause.** This issue occurs when all the required connectivity and configuration seems correct to the software, but the monitoring service is not seeing voice packets on its network connection. The monitoring service refers to either the VoIP Monitor service running on the server or the desktop monitor running on the agent's desktop.

To troubleshoot this problem, follow the steps in the flowchart shown in Figure 33 and Figure 34.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Will Not Start (page 98)</td>
<td>the supervisor selects and agent to monitor, but receives an error message that the sound card might not be working properly.</td>
<td>Occasional</td>
</tr>
<tr>
<td>Audio is Distorted (page 96)</td>
<td>Beeping sound (no speech) or very distorted speech/noise when monitoring or recording.</td>
<td>Very rare</td>
</tr>
<tr>
<td>New NIC Breaks Feature (page 97)</td>
<td>Monitoring and/or recording stop working after installing a new NIC.</td>
<td>Very rare</td>
</tr>
<tr>
<td>IP Address of Agent's Voice Gateway Changes (page 98)</td>
<td>The IP Address of the agent's Voice Gateway changes.</td>
<td>Very rare</td>
</tr>
</tbody>
</table>
Figure 33. Troubleshooting for inaudible monitored call

**Problem:** Supervisor selects agent and clicks on Monitor. Speaker icon appears next to call, but supervisor cannot hear anything.

**Volume:** May be too low. Move volume slider all the way to the right.

**Verify PC sound card:** Works.

**Verify no other application:** Using the sound card's resources.

**Verify that agent:** Is on a call, and is talking.

**Is supervisor monitoring a Media Terminated agent using a soft phone?**

**Yes**

**Verify phone:** Is configured correctly in Unified CM:
- Phone Type is "Cisco 30 SP+"
- MAC address is for agent's PC
- Phone description is "SEP" followed by MAC address of agent's PC

In Unified CM Administration, under System/Enterprise Parameters, in Security Parameters, verify that Device Security Mode is not set to "Encrypted".

**Is VoIP Monitor Service being used to monitor agent?**

**No**

Go to "Desktop Monitoring: No Speech" on Page 2.

**Yes**

**Verify device:** Is configured correctly in Desktop Administrator:
- Desktop Monitor check box is clear.
- If using multiple VoIP Monitor Services, either the device is assigned a VoIP Monitor Service or there is a default service.

**Verify SPAN port:** Is configured correctly. If monitor server has moved or there are new agent IP phones, you may need to reconfigure SPAN port.

**Verify registry entries:** For VoIP Monitor Service.

**Attempt to monitor:** Same agent with VoIP Monitor Server Test Tool.

**Check VoIP Monitor Service log files:** For errors.

Open a TAC case.
Figure 34. Troubleshooting for inaudible monitored call (cont'd)

**Problem:** (continued)
Desktop Monitoring: No Speech

Verify that the device is configured correctly in the Cisco Desktop Administrator application: the Desktop Monitor box is checked.

Is the agent being monitored a Media Terminated agent using a soft phone?

Yes

Verify that the phone extension used by the agent to log on to CAD is the same extension as the configured soft phone.

No

Verify that the PC is connected to the phone in the 10/100 SW port.

Verify that the phone extension used by the agent to log on to CAD is the same extension of the attached IP phone.

On the Phone Configuration page for the phone(s) you are attempting to monitor, verify the following settings:
- PC Port is set to "Enabled"
- PC Voice VLAN Access is set to "Enabled"

Verify that the NIC card in the agent's PC supports Desktop Monitoring.

Verify the CAD Desktop's registry settings.

Attempt to monitor the same agent using the Desktop Monitor and VoIP Monitor Server Test Tools.

Check the CAD application logs for errors.

Open a TAC case.

End
Monitor Button is Disabled

Problem. In Supervisor Desktop, the supervisor selects an agent to monitor, but the Monitor button is disabled.

Cause. This problem occurs if the selected agent is not eligible to be monitored or if no monitor services are available for monitoring.

To troubleshoot this problem, complete the following steps:
1. Verify that the supervisor selected an agent, not a call.
2. Verify that the supervisor is not already participating in a call as an agent.
3. Verify that the supervisor did not select his or her own agent to monitor.
4. Verify that at least one VoIP Monitor service is running.
5. Open a TAC case. For more information, see "Opening a TAC Case" on page 102.

Record Button is Disabled

Problem. In Supervisor Desktop, the supervisor selects a call to record, but the Record button is disabled.

Cause. This problem occurs if one of the following conditions occur:
- The selected agent is not eligible to be recorded
- None of the monitor services are running
- The Recording and Statistics service is stopped

To troubleshoot this problem, complete the following steps:
1. Verify that the supervisor is not already participating in a call as an agent.
2. Verify that the supervisor selected a call, not an agent.
3. Verify that the supervisor did not select his or her own agent to monitor.
4. Verify that at least one VoIP Monitor service is running.
5. Open a TAC case. For more information, see "Opening a TAC Case" on page 102.
Recording File is Empty

**Problem.** The recording file is only 1 KB long and does not contain any audio.

**Cause.** This problem occurs when all the required connectivity and configuration seems correct to the software, but the monitoring service is not seeing voice packets on its network connection. Hence, no speech packets are being sent to the Recording and Statistics service. The result is the appearance of a successful call recording, but the recording file is only 1 KB long (contains the WAV file header but no data).

To troubleshoot this problem, complete the following steps:

1. Verify that monitoring is working by completing the troubleshooting steps in the problem "Monitored Call is Inaudible" on page 87.
2. Open a TAC case. For more information, see "Opening a TAC Case" on page 102.

Speech is Garbled

**Problem.** While monitoring or recording an agent, the supervisor hears garbled audio. Garbled audio is recognizable as speech or music, but is corrupted in one of the following ways.

- Motor-boating: The audio rapidly stops and starts repeatedly.
- Slowed audio: The person or music appears to be speaking very slowly.
- One-sided conversation: Only one side of the call is audible.
- Low volume: The volume is very low.
- Gaps in the audio: Words or music are truncated.
- Extraneous noise: Pops, clicks, and other sounds that are not coming from the phone conversation itself are audible.

If the audio is so garbled that it is not recognizable as speech or music, or if the audio consists entirely of noises, such as beeping, see "Audio is Distorted" on page 96.

**Cause.** Garbled audio generally occurs for one of the following reasons.

- SPAN is not configured correctly
- The network is congested
- The CPUs are overburdened
- The sound card and/or speakers have hardware problems
Determine which of the following categories the problem belongs to, then refer to the corresponding section for troubleshooting information.

- Motor-boating: see "Audio Stops and Starts Rapidly and Repeatedly" on page 92
- Slowed audio: see "Audio is Slowed Down" on page 93
- One-sided conversation: see "Only One Party on the Call is Audible" on page 93
- Low volume: see "Audio is Hard to Hear" on page 93
- Gaps in the audio: see "Audio Has Gaps" on page 94
- Extraneous noise: see "Extraneous Noise in Audio" on page 95

Audio Stops and Starts Rapidly and Repeatedly

The motor-boating effect occurs if the jitter buffer is too small or the number of sound buffers is too low.

Jitter Buffers

Jitter buffers are used to buffer packets in a pool that is read by the monitoring and/or recording application. Although the packets coming from the network might arrive in bursts, pooling the packets smooths out the bursts for the monitor application. If the jitter buffer is too small, the monitor application empties the buffer more quickly than the buffer is filled. The monitor application must then wait for the buffer to be partially refilled before the monitor application can start reading packets again. The stops and starts cause the motor-boating effect.

The default value for the recording jitter buffer is 100 (packets). If you increase this value, increment in steps of 100 packets. The default value for the monitoring jitter buffer is 400 (packets). If you increase this value, increment in steps of 100 packets.

The applications that receive voice packets from the packet sniffing driver have jitter buffer settings. These applications include Supervisor Desktop for monitoring and the Recording and Statistics service for recording. Depending on the version of CAD you are using, these values are stored in one of three places: LDAP, the Windows registry of the machine on which Supervisor Desktop is running, or the Windows registry of the server on which the Recording and Statistics service is running.

Sound Buffers

The number of sound buffers indicates the amount of sound card buffer resources that are being used. If recordings sound normal, but the motor-boating effect occurs during monitoring, increase the number of sound buffers. To configure the number of sound buffers, you must edit the registry on the supervisor's PC.
**Audio is Slowed Down**

The slow speech effect is due to duplicate voice packets being sent to the monitoring supervisor or the Recording and Statistics Service. This effect can only occur if the extension being monitored or recorded is using a VoIP Monitor service to capture the packets. You will not see this if using Desktop Monitor.

The root cause is that SPAN is not configured correctly on the switch that the agent phones are connected to. If SPAN is configured to monitor phone ports or a VLAN containing agent phones, and it is configured to copy both incoming and outgoing packets, you will see duplicate packets when you monitor a call between two agents on the same switch. You will see packet A as it leaves Agent-1's phone, and the same voice packet as it arrives at Agent-2's phone. To fix this issue, you need to reconfigure SPAN on the switch.

**Only One Party on the Call is Audible**

If you are only hearing one side of a conversation, first check the following:

- Two or more parties are actually on an active call
- All parties are actually speaking through the phone to each other
- The party that you cannot hear via monitoring/recording can be heard by the other parties on the call

If the party that you are able to monitor/record cannot hear the other party, the voice packets won't be seen by the monitor service either. Here are some common reasons that party A would not hear another party B:

- B is whispering.
- B is using a speaker phone and not speaking loudly enough to be heard or is too far from the phone for the speech to be picked up by the phone's microphone.
- B is using a headset or microphone and the microphone is turned off or is broken.

If you can eliminate these as causes, then the cause of this effect is due to a faulty configuration of SPAN on the switch. Since this is dealing with SPAN configuration, this will not apply if using Desktop Monitor for monitoring or recording.

Basically, the SPAN is configured in such a way that it is not capturing the voice packets from one of the parties on the call. To fix this issue, you need to reconfigure SPAN on the switch.

**Audio is Hard to Hear**

If only one of the parties being monitored or recorded has a lower volume, you can check these reasons (where Agent B is the agent that has a lower volume):

- B is whispering.
B is using a speaker phone and not speaking loudly enough to be heard or is too far from the phone for the speech to be picked up by the phone's microphone.

B is using a headset or microphone and the microphone is turned off or is broken.

If all parties are equally soft, then complete the following checks:

- If listening to a recording through Supervisor Desktop, make sure the volume slider is all the way to the right.
- If using headphones, check the volume setting for the headphones.
- If using speakers, check the volume setting for the speakers.
- Try both headphones and speakers to see if there is any difference.
- Try to monitor from another supervisor's desktop, using their speakers/headphones.
- Manually open a WAV file that is not a recording made from CAD and listen to it through the speakers or headphones.

There is nothing in the CAD software that alters volume of monitored or recorded calls except for the volume slider in the Supervisor Desktop application that allows the supervisor to listen to recorded calls. The advice is to make sure your sound hardware is working correctly on the machine being used by the supervisor.

### Audio Has Gaps

Gaps in speech, no speech, or speech that is excessively delayed (when monitoring), can be caused either by network congestion or by inadequate CPU time allocated to the application that is involved in monitoring/recording.

If the network is very congested, the packets will not arrive at the packet sniffing driver fast enough to produce good quality results. Also, packets being sent over the network from the VoIP Monitor service to Supervisor Desktop and the Recording and Statistics service will be delayed, affecting speech quality. Evaluate the load on your network and fix this problem to improve the monitoring quality.

If the network is not congested, gaps in audio can be caused by an overburdened CPU on one or more of the machines running the monitoring/recording software.

<table>
<thead>
<tr>
<th>How agent is monitored/recorded</th>
<th>Computers to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring with VoIP Monitor service</td>
<td>• VoIP Monitor service host</td>
</tr>
<tr>
<td></td>
<td>• Supervisor’s desktop</td>
</tr>
</tbody>
</table>
If you find one of these machines where its CPU usage is very high (over 75%), you will need to reduce the CPU usage on that machine to improve the quality of monitoring and recording.

The first thing to check is the debugging level for the Cisco applications. If these debugging levels are set very high, the software spends most of its time writing out to the debug file. This will, in some cases, drastically increase the CPU time for the application and, in turn, the computer itself. Turn off all the debugging for the service or application that you suspect, then try to monitor or record to see if that fixes the problem.

The next thing to do is to find out what other applications are running on the box in question, determine which application(s) and using the most CPU time, and shutting down or removing these applications from the box to improve performance.

For information on setting debugging levels for CAD applications, refer to the Cisco CAD Troubleshooting Guide.

**Extraneous Noise in Audio**

Pops, clicks, and other extraneous noises are most likely due to the parties on the call being in noisy environments. If the parties on the call are not hearing these noises, but the noises are heard by the monitoring supervisor or can be heard in the recorded WAV file, it might indicate a problem with the software.

**Operation Fails Without An Error**

**Problem.** The Monitor or Record button in Supervisor Desktop returns to the unclicked stated after clicking it.

**Cause.** The most common reason for this failure is that the VoIP Monitor service or the Recording and Statistics Service is down.
Operation Ends Prematurely

**Problem.** Recorded file incomplete or monitored speech stops.

**Cause.** This occurs when the recording or monitoring process is stopped prematurely by some system or application crashing.

1. Verify that the Recording and Statistics Service is configured with an appropriate percentage of disk space. When the Recording and Statistics Service is installed, it creates a directory for storing recording files.
2. Verify that the drive has space available for recording files. For instructions, see XREF.
3. Verify that all of the required applications are running. For instructions, see "Verifying that Required Applications are Running" on page 103.
4. Open a TAC case. For instructions, see "Opening a TAC Case" on page 102.

The Recording and Statistics Service is configured to use a percentage of the available disk space and will stop accepting recording requests if it uses all of the disk space it is configured to use. To fix this problem, you must either tell the Recording and Statistics Service that it can use more of the disk to store recordings, or remove some of the recordings to make room for new recording files.

If the physical drive is out of space, the Recording and Statistics Service cannot write any recordings. If this is the case, you will see many other applications complaining of this as well. You will need to make space on the drive to continue working.

Audio is Distorted

**Problem.** Unexpected noise instead of voice heard with monitoring or recording. Beeping sound (no speech) or very distorted speech/noise when monitoring or recording.

If the call is using the G.711 protocol, you will either hear silence or an irregular beeping sound. There can be other types of effects that we not encountered yet. If the call is using the G.729 protocol, the speech sounds very strange indeed. It has been described as someone speaking in a foreign tongue while under water. (You can use your imagination on this one).

**Cause.** This problem occurs when voice encryption is configured on the CallManager (version 4.0).

1. Verify that Unified CM is not configured to send voice streams as encrypted data.

Unified CM versions 4.0 and later support voice stream encryption. The encrypted packets cannot be unencrypted by the monitor service software. The software processes the encrypted voice stream and outputs what it
thinks is speech. In reality, the result is either a periodic beeping (for G.711) or distorted speech that sounds like someone whispering in a foreign language under water (for G.729). You might get other types of results, but the fix is to turn off encryption on the CallManager. Refer to the appropriate CallManager documentation for instructions on how to do this.

2. Open a TAC case. For instructions, see "Opening a TAC Case" on page 102.

New NIC Breaks Feature

Problem. Monitoring and Recording stop working after installing a new NIC.

Cause. This problem occurs because the network adapter used by the VoIP Monitoring software for sniffing is invalid or becomes invalid.

The voice sniffing software running on the VoIP Monitor service box and the agent desktop (if desktop monitoring is being used) uses a specific network adapter (set at installation) to capture voice packets from the network. After installing a new or another NIC, this adapter might become invalid. There are also cases where the incorrect network adapter is chosen during the installation of the software. In either of these cases, monitoring and recording will not work correctly. You will need to run the Post Install utility to update the sniffing adapter name stored in the registry to fix the problem.

1. Run the UpdateSnifferNic utility.
2. Open a TAC case. For instructions, see "Opening a TAC Case" on page 102.

Calls Between Mobile Agents are Inaudible

Problem. When a supervisor monitors a call between two mobile agents, nothing is heard.

Cause. Monitoring calls between mobile agents is not supported when the agents are connected to the same voice gateway.

Solution. ?
IP Address of Agent's Voice Gateway Changes

Problem.

Cause.

Solution. Complete the following steps to update the Agent Gateway IP address.
1. Launch Cisco Desktop Administrator.
2. Choose Enterprise Configuration > VoIP Monitor.
3. Select the Mobile Agent Monitor tab.
4. Double-click the Agent Gateway IP address that you want to modify.
5. Enter the new IP address.

Some Mobile Agents Cannot Be Monitored

Problem. Some mobile agents cannot be monitored.

Cause.

Solution. Complete the following steps to verify that all mobile agent gateways are configured with a VoIP Monitor service.
1. Launch Cisco Desktop Administrator.
2. Choose Enterprise Configuration > VoIP Monitor.
3. Select the Mobile Agent Monitor tab.
4. For each Agent Gateway IP address field that is blank, update the field with the appropriate IP address.

Monitoring Will Not Start

Problem. In Supervisor Desktop, the supervisor selects an agent to monitor, but receives the error message, “Supervisor has failed to start voice monitor on the device: <device number>. Verify that the sound card in the PC is working properly.”

Cause. This problem occurs if the operating system is Vista and the speakers are not plugged in. Vista checks if the speakers are plugged in, and returns an error if they are not.

To troubleshoot this problem, complete the following steps:
- Verify that the PC speakers are correctly plugged in and that the connection is secure.
Troubleshooting Procedures

This section describes the following procedures.

- Verifying Sound Card Functionality on page 99
- Verifying Desktop Administrator Settings on page 100
- Verifying Registry Settings on page 100
- Testing the Sniffing Adapter on page 101
- Testing the Desktop Monitor Library on page 101
- Using Debugging Files on page 101
- Opening a TAC Case on page 102
- Verifying that NICs Can Be Sniffed on page 102
- Verifying that the Correct NIC Is Being Used on page 103
- Verifying that Required Applications are Running on page 103

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.

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:

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 Desktop Administrator Settings
An agent's device can be monitored by a VoIP Monitor service or by the Desktop Monitor software running on the agent's desktop. The specific application that is used is configured in Cisco Desktop Administrator.

To verify monitoring settings in Cisco Desktop Administrator:
1. Launch Cisco Desktop Administrator.
2. Navigate to the following node:
   - For Unified CCE, choose Enterprise Configuration > VoIP Monitor.
   - For Unified CCX, choose Silent Monitoring & Recording > VoIP Monitoring Device.
3. Find the agent's phone by extension and/or MAC address.
   - If the Enable Desktop Monitoring check box is selected, then the agent’s calls will be monitored using Desktop Monitor.
   - If the Enable Desktop Monitoring check box is not selected, and your LCC has more than one VoIP Monitor service, you must complete one of the following actions:
     - Assign a specific VoIP Monitor service to the agent’s phone.
     - Select a default VoIP Monitor service.

Verifying Registry Settings
For monitoring to work correctly, there are a few settings in the Windows registry that are required. If the VoIP Monitor service is otherwise running normally, 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 HKEY_LOCAL_MACHINE registry key: \SOFTWARE\Spanlink\CAD\VoIP Monitor Client\config, in the format /Device/Splkpc_{<GID>}. <GID> is a Windows global ID that represents the network adapter that is being used to sniff traffic.

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".

Testing the Sniffing Adapter

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

To test the sniffing adapter:

1. Open a command window and navigate to the folder C:\Program Files\Cisco\Desktop\bin.
2. Run SplkDump.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. 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.

Using Debugging Files

If the debugging level for the VoIP Monitor service is set to a value from 1–4, a debug file will be created by the VoIP Monitor service. Debug level 1 provides general debugging information. Level 4 provides a large amount of debugging information.

To look for errors in the VoIP Monitor service logs:

1. Follow the instructions in the Cisco CAD Troubleshooting Guide for setting the debug level for the VoIP Monitor service and attempt to monitor an agent.
2. After the test, you can view the FCVoIPMonSvr.dbg file and look for errors. Start by searching for the words “Fatal” and “Major”. These indicate serious errors that prevent the VoIP Monitor service from running correctly. These errors have an error code with the prefix FCVMS followed by a three-digit number. These error codes are defined in the Cisco CAD Error Code Dictionary. The definitions explain the error, causes of the error, and possibly instructions on how to fix the error or work around it. By following these instructions, you might fix the problem that is preventing monitoring and recording.

3. If you think you have fixed all the problems you can by looking up the serious errors in the Cisco CAD Error Code Dictionary, you can search for the word “error” and see if the debug message indicates what the problem is. Experienced administrators will be able to at least find out what the issue is and use this to report a case to TAC.

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:

- CAD 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.)

Verifying that NICs Can Be Sniffed

There are known issues with some NICs that do not fully support promiscuous mode, the mode that is needed to capture voice traffic from the network. This issue becomes apparent when you are using desktop monitoring and the attached IP phone and the agent’s desktop are in different VLANs (the phone is in the voice VLAN and the desktop is in the data VLAN) on the switch to which they are both attached. In this case, the NIC will not send the voice data to the agent’s PC, thus preventing the monitoring and recording of any call that the agent is on.

If you are able to successfully monitor an agent using a VoIP Monitor service but not by using desktop monitoring, this points to the NIC as being the issue. If this is the case, you can either always use a VoIP Monitor service to monitor agents with this...
NIC, put all IP phones and PCs on the same VLAN, or get a different NIC that supports promiscuous mode.

Verifying that the Correct NIC Is Being Used

On both the VoIP Monitor service server and the agent desktop there is an entry in the registry that identifies the IP address of the NIC that is used to capture voice data from the network. If this entry is incorrect, voice monitoring and recording will not work. In fact, the VoIP Monitor service and desktop monitoring might fail to properly initialize.

To verify that the correct NIC is being used for sniffing:

- Use the CAD Configuration Setup utility to modify/view the current setting. This applies to the VoIP Monitor service and Desktop Monitor.
  
  C:\Program Files\Cisco\Desktop\bin\PostInstall.exe

  The IP address is configured on the VoIP Monitor Service step window.

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.

Table 12 lists the CAD applications that are required depending on the type of operation, the person performing the operation, and the service that is supporting the operation. Your version of CAD might not include all of the software listed. To determine whether your version contains the applications listed, see the appropriate documentation.

The table does not include other hardware and software with which CAD applications interact, such as switches, Cisco Unified Communications Manager (Unified CM), and Cisco Unified Intelligent Contact Management (Unified ICM). If you believe that
another application might be causing a problem, see the documentation for that software for troubleshooting information.

Table 12. Required applications for monitoring and recording

<table>
<thead>
<tr>
<th>Role</th>
<th>Operation</th>
<th>Service/application used</th>
<th>Required applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor</td>
<td>Monitoring</td>
<td>Cisco VoIP Monitor service</td>
<td>Cisco Supervisor Desktop</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco VoIP Monitor service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco LDAP Monitor Service</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Monitoring</td>
<td>Desktop Monitor</td>
<td>Cisco Supervisor Desktop</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Agent Desktop (monitored agent)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco VoIP Monitor service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco LDAP Monitor Service</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Recording</td>
<td>Cisco VoIP Monitor service or Desktop Monitor</td>
<td>Cisco Supervisor Desktop</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Agent Desktop (monitored agent)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco VoIP Monitor service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco LDAP Monitor Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Chat Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Recording and Statistics Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Recording &amp; Playback Service</td>
</tr>
<tr>
<td>Agent</td>
<td>Recording</td>
<td>Cisco VoIP Monitor service</td>
<td>Cisco Agent Desktop (agent)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco VoIP Monitor service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco LDAP Monitor Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Chat Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Recording and Statistics Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Recording &amp; Playback Service</td>
</tr>
<tr>
<td>Agent</td>
<td>Recording</td>
<td>Desktop Monitor</td>
<td>Cisco Agent Desktop (agent)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco VoIP Monitor service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco LDAP Monitor Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Chat Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Recording and Statistics Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cisco Recording &amp; Playback Service</td>
</tr>
</tbody>
</table>

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.
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 13* 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 13* 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 13* are more fully described in the section, "SPAN-Related Feature Descriptions" on page 107.
### Table 13. SPAN-related feature support for Cisco Catalyst switches

<table>
<thead>
<tr>
<th>Model</th>
<th>Max SPAN Sessions</th>
<th>SPAN</th>
<th>RSPAN</th>
<th>VSPAN</th>
<th>Ingress-only/Egress-only</th>
<th>VLAN Filtering on Trunk Ports</th>
<th>Normal Network Traffic on Destination Ports</th>
<th>Destination and Source Ports Must be in Same VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 Express</td>
<td></td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>500 Express</td>
<td>port count 1</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>1200</td>
<td>1</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>1900</td>
<td>1</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>2820</td>
<td>1</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>2900XL</td>
<td>port count *</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>2940</td>
<td>1</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>2948G</td>
<td>5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>2950</td>
<td>1</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>2955</td>
<td>1</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>2960</td>
<td>2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>2980G</td>
<td>5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>3550</td>
<td>2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>3560</td>
<td>2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>3560-E</td>
<td>2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>3750</td>
<td>2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>3750-E</td>
<td>2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>4003</td>
<td>5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>4006</td>
<td>5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>4500</td>
<td>6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>4912G</td>
<td>5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>5000</td>
<td>5</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>5002</td>
<td>5</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>5500</td>
<td>5</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>
The column headers in Table 13 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 13 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.

Table 13. SPAN-related feature support for Cisco Catalyst switches (cont’d)

<table>
<thead>
<tr>
<th>Model</th>
<th>Max SPAN Sessions</th>
<th>SPAN</th>
<th>RSPAN</th>
<th>VSPAN</th>
<th>Ingress-only/Egress-only</th>
<th>VLAN Filtering on Trunk Ports</th>
<th>Destination Ports</th>
<th>Normal Network Traffic on Destination Ports</th>
<th>Source Ports Must \ be in Same VLAN</th>
<th>Destination and Source Ports Must be in Same VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>5505</td>
<td>5</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>5509</td>
<td>5</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>6000</td>
<td>30</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>6006</td>
<td>30</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>6009</td>
<td>30</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>6500</td>
<td>30</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>6509</td>
<td>30</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>6513</td>
<td>30</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

1 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.
**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

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

- 7906G
- 7911G
- 7931G
- 7941G
- 7941G-GE
- 7961G
- 7961G-GE
- 7970G
- 7971G-GE
The following settings are required to use VoIP monitoring for CAD and QM. 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.