

VoIP Monitor Server 4.2 Best Practices Configuration Guide

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[VoIP Monitor Server Overview](#)

[Document Organization](#)

[Best Practice Deployments](#)

[Single Switch Deployment](#)

[Collapsed Core \(Single Logical Call Center\)](#)

[Collapse Core \(Multiple Logical Call Centers\)](#)

[Three Layer Network Configured for Redundancy/Load Balancing](#)

[Deployment Planning](#)

[VoIP Monitor Server Assumptions](#)

[VoIP Traffic Exposure](#)

[Layer 2 Switching Domains](#)

[Single Copy of VoIP Packets](#)

[IP Phone Compatibility](#)

[Voice Encoding Protocols](#)

[Single Processor Servers](#)

[Deployment Strategies](#)

[VLANs](#)

[IP Phone Ports](#)

[Voice Gateway and CallManager Ports](#)

[SPAN Overview](#)

[Switch Capabilities](#)

[SPAN Support](#)

[RSPAN Support](#)

[Network Traffic Restrictions](#)

[Ingress and Egress Monitoring](#)

[VSPAN Support](#)

[Number of SPAN Sessions](#)

[Using Multiple NIC Cards with the VoIP Monitor Server](#)

[Problem](#)

[Solution](#)

[Limitations](#)

[Issues](#)

[Installation of a Second Network Adapter on the VoIP Monitor Server Box](#)

[Cisco Agent Desktop for ICD Installation](#)

[Cisco Agent Desktop for IPCC Installation](#)

[Simple Network Deployment Example](#)

[Collapsed Core Network Deployment Example](#)

[NetPro Discussion Forums - Featured Conversations](#)

[Related Information](#)

Introduction

This document provides enough information about the abilities and requirements of Voice over IP (VoIP) Monitor Server version 4.2 so you can effectively deploy the product. Included is information on how the VoIP Monitor Server monitors (sniffs) the network for VoIP packets, recommended network configurations, and examples using several common network configurations.

Prerequisites

Requirements

Readers of this document should be knowledgeable of these requirements:

- Cisco IP Contact Center (IPCC)
- Computer Telephony Integration (CTI) Agent Desktop
- Cisco Switches and LAN Switching

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco Agent Desktop 4.2 and later

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, refer to [Cisco Technical Tips Conventions](#).

VoIP Monitor Server Overview

The VoIP Monitor Server enables the silent monitoring and recording features in Cisco Agent Desktop. It accomplishes this by sniffing network traffic to and from select IP phones, voice gateways, and/or the Cisco CallManager. If the server finds a packet going to, or coming from, a monitored device, the packet is sent to the receiver. If a supervisor is monitoring a call, the receiver is the supervisor's desktop, where the VoIP Client application decodes the voice stream and sends the output to the supervisor's computer sound card. For recording, the receiver is the Recording and Statistics (RASCAL) server, that decodes the voice stream and saves the output as a .wav file.

The VoIP Monitor Server is able to do this by using the monitoring feature of certain Cisco Catalyst switches. This feature is called the Switched Port Analyzer (SPAN) on most Catalyst switches. Some Catalyst switches have the advanced feature called Remote SPAN (RSPAN). The monitoring feature allows the switch to copy the network traffic from one or more sources and copy it to a destination port. These sources can be ports and/or virtual LANs (VLANs). RSPAN allows the source ports to reside on remote switches. The VoIP Monitor Server connects to the switch through the destination port. This allows the VoIP Monitor Server to see the voice traffic going to and coming from IP phones.

The VoIP Monitor Server is only interested in seeing Real time Transport Protocol (RTP) packets. RTP packets are encapsulated by the User Datagram Protocol (UDP) which is encapsulated by the Ethernet protocol. The VoIP Monitor Server knows the Media Access Control (MAC) address of the IP phone that it is monitoring/recording. It uses these MAC addresses and compares them to the source and destination MAC addresses contained in the UDP packet to determine whether to redirect the RTP packet to the receiver.

Document Organization

This document starts with recommended deployments based on several typical network configurations (from simple to complex). Each deployment explanation includes references to features, issues, and limitations. The sections become increasingly detailed and explain the functionality of the VoIP Monitor Server and the deployment issues that need to be worked through to realize a successful deployment. Finally, the [appendices](#) contain reference information and some example deployments using real switches that can be used to help in the decision making process of how the VoIP Monitor Server(s) is deployed.

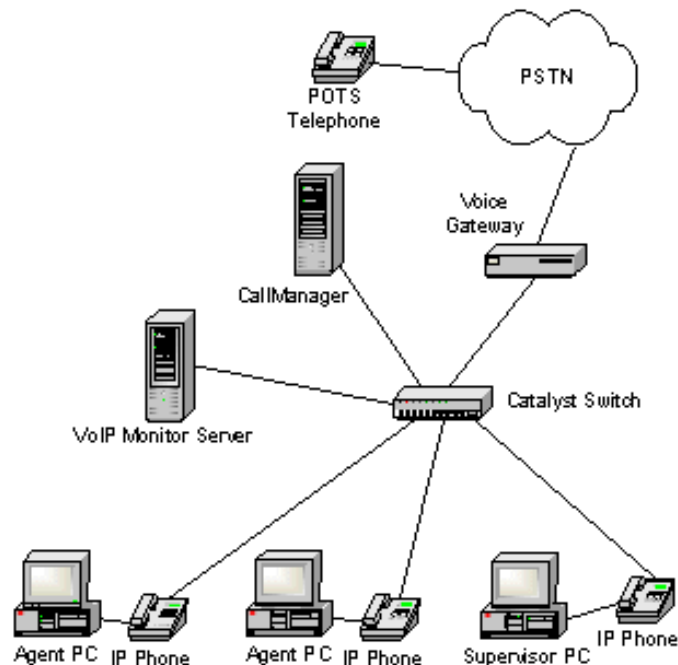
Best Practice Deployments

The following sections show and describe the best practice deployment strategies for the VoIP Monitor Server based upon various common network configurations. Find the network configuration that most closely matches your network and refer to the deployment notes.

Single Switch Deployment

In a single switch deployment, as shown in [Figure 1](#), the network configuration, the CallManager, voice gateway, VoIP Monitor Server, and all IP phones are connected to a single switch. There are a small number of agents. Data and voice are separated by VLANs.

Figure 1: Single Switch Deployment



Agent-to-Agent Monitoring - Option 1

- SPAN is configured on the switch to monitor the Voice VLAN(s). The SPAN is configured to only copy ingress packets.
- If the switch does not support VLAN monitoring ([Table 6](#)), use Option 2.

Agent-to-Agent Monitoring - Option 2

- Set up SPAN to monitor each IP phone's switch port, with SPAN configured to only copy ingress packets.

Caller-to-Agent Monitoring Only - Option 3

- SPAN is configured to monitor the voice gateway and CallManager ports, copying both ingress and egress packets.
- If your switch does not support monitoring ports on other VLANs ([Table 7](#)), then the voice gateway, CallManager, and all IP phones must be on the same VLAN.

Refer to [Simple Network Deployment Example](#) for a configuration example of this network layout using a Catalyst 3524 switch.

Collapsed Core (Single Logical Call Center)

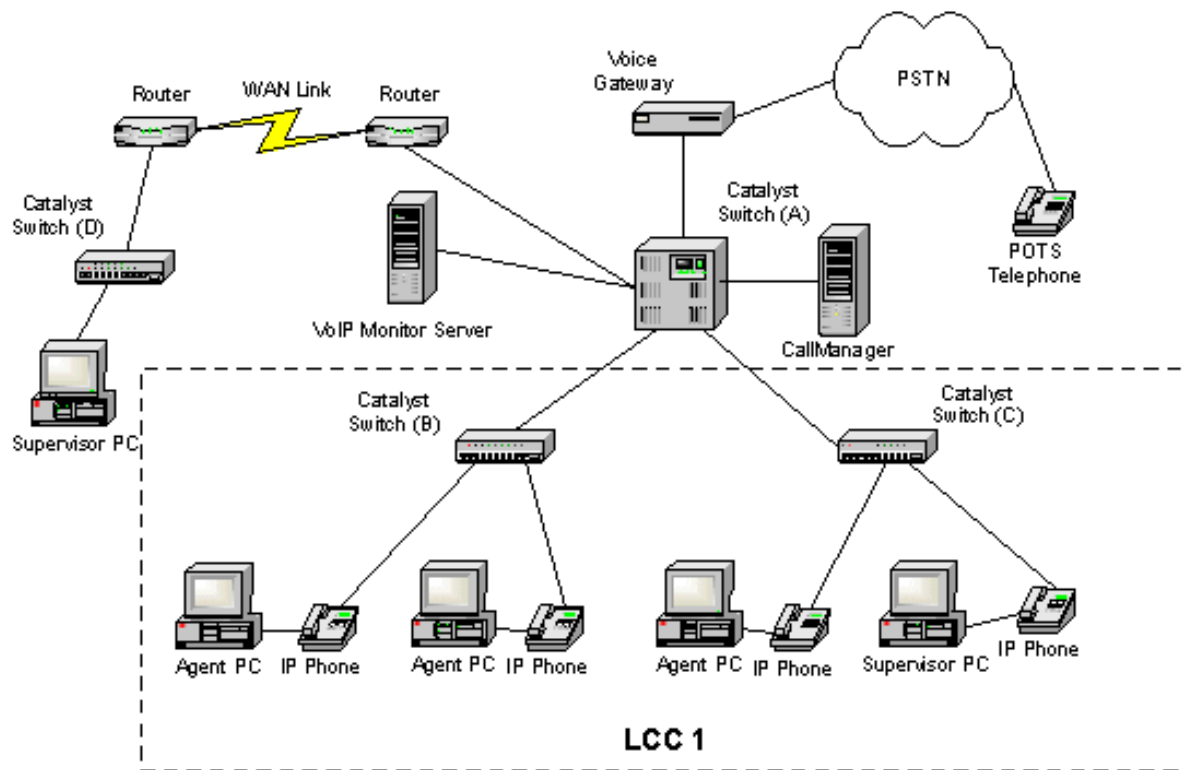
In this configuration, Switch A comprises both the core and distribution layers. Switches B, C, and D are access layer switches. All the agent IP phones are attached to switches B and C. Only a supervisor is attached to switch D. The VoIP Monitor Server is only monitoring IP phones on switches B and C. The routers between switch A and switch D preclude monitoring anything attached to switch D, although the supervisor on switch D could still monitor agents on switches B and C.

There is a single Logical Call Center (LCC), therefore a single installation of the Cisco Agent Desktop servers. Data and voice traffic is separated by data and voice VLANs. All agent IP phones are members of the voice VLAN.

The VoIP Monitor Server could be attached to switch A, B, or C. Where it is placed, and how many servers are used depend on the functionality you need, the number of agents to be monitored, and the features available on the switches. In this case, there are less than 128 agents so you only need a single VoIP Monitor Server to handle the call load.

If there are more than 128 agents, you need to create two or more LCCs, each containing an installation of the Cisco Agent Desktop servers, shown in the following [example](#).

Figure 2: Collapsed Core (Single Logical Call Center)



Agent-to-Agent Monitoring - Option 1

- Set up RSPAN on switch A to monitor each IP phone's IP port on switches B and C, with RSPAN configured to only copy ingress packets.

- If your switch does not support RSPAN monitoring ([Table 3](#)), you cannot use this configuration. You need to create multiple LCCs and use multiple VoIP Monitor Servers. This is described in [Collapsed Core \(Multiple Logical Call Centers\)](#).

Caller-to-Agent Monitoring Only – Option 2

- SPAN is configured on switch A to monitor the voice VLAN, with SPAN configured to copy both ingress and egress packets.
- If agent-to-agent monitoring is attempted with this configuration, the quality of the speech may be very bad due to the problem of duplicate packets. This is described in [Single Copy of VoIP Packets](#).

Caller-to-Agent Monitoring Only – Option 3

- SPAN is configured on the core/distribution switch to monitor the voice gateway and CallManager ports, copying both ingress and egress packets.
- If your switch does not support monitoring ports on other VLANs ([Table 7](#)), then the voice gateway, CallManager, and all IP phones must be on the same VLAN.

Refer to [Collapsed Core Network Deployment Example](#) for a configuration example of this network layout using a Catalyst 6000 switch as the core/distribution switch, and a Catalyst 3524 and Catalyst 4000 switch for the access layer switches.

Collapse Core (Multiple Logical Call Centers)

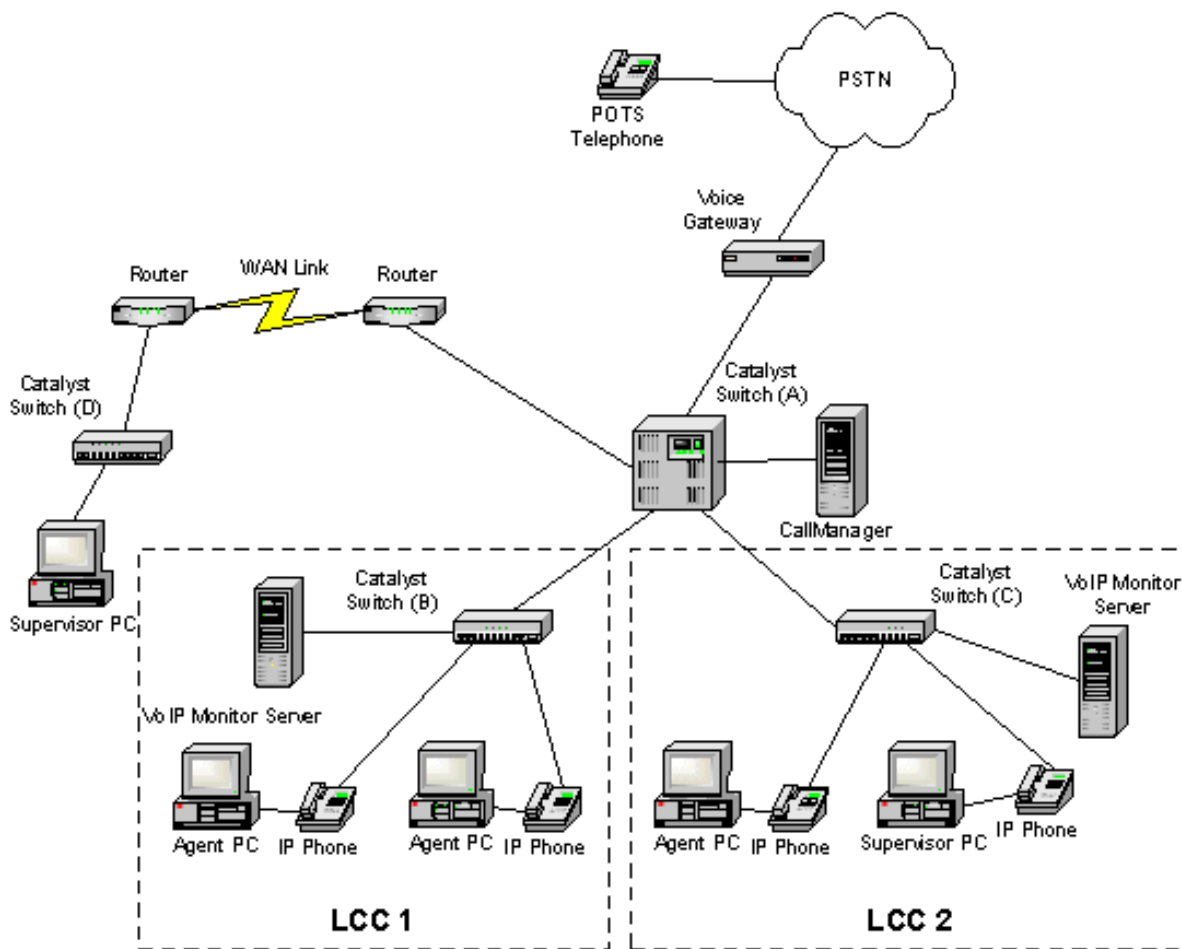
In this configuration, Switch A comprises both the core and distribution layers. Switches B, C, and D are access layer switches. All the agent IP phones are attached to switches B and C. Only a supervisor is attached to switch D. The VoIP Monitor Server is only monitoring IP phones on switches B and C. The routers between switch A and switch D preclude monitoring anything attached to switch D, although the supervisor on switch D could still monitor agents on switches B and C.

Switches B and C each have 100 agents attached to them. Since a single VoIP Monitor Server cannot handle the call traffic of 200 agents (ref), two LCCs are created. Each LCC have an installation of the Cisco Agent Desktop servers therefore, each LCC has its own VoIP Monitor Server.

Note: This is also the configuration to allow agent-to-agent monitoring even if both switches combined have less than 128 agents.

Data and voice traffic is separated by data and voice VLANs on both switch B and C. All agent IP phones are members of the switch voice VLAN.

Figure 3: Collapsed Core (Multiple Logical Call Centers)



Agent-to-Agent Monitoring – Option 1

- SPAN is configured on switch B and C to monitor that switch's voice VLAN. The SPAN copies only ingress packets.
- If the access layer switch does not support VLAN monitoring ([Table 6](#)), use [Option 2](#).

Agent-to-Agent Monitoring – Option 2

- Set up SPAN to monitor each IP phone's IP port on the access layer switch.
- In this configuration, the VoIP Monitor Server is always able to monitor agent-to-agent calls.
- Supervisors are only able to monitor agents within the same LCC.
- A call between an agent in LCC1 and an agent in LCC2 can be monitored by a supervisor of one of those LCCs if they monitor the agent that is in the supervisor's LCC.

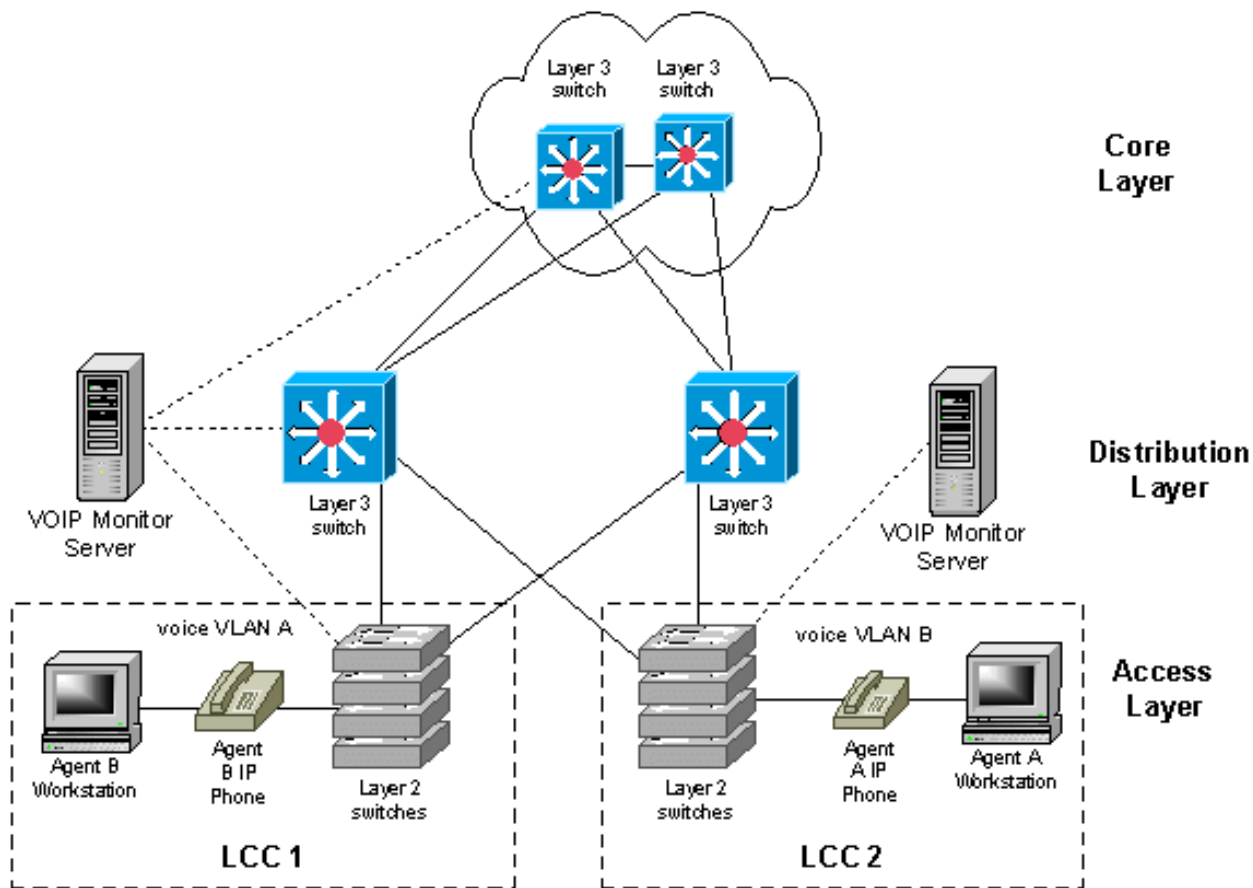
Three Layer Network Configured for Redundancy/Load Balancing

In [Figure 4](#), two redundant core switches are attached to two redundant distribution switches. These switches are, in turn, connected to two stacks of layer 2 switches at the access layer. The switches in the stacks are connected to each other through trunk ports. Stacking makes multiple switches behave as a single switch (from the VoIP Monitor Server point of view). Assume that there are more than 128 agents attached to each stack of access layer switches. For this reason, you have two LCCs, as shown in [Figure 4](#).

This is a common configuration for Cisco networks. It is configured for redundancy, load balancing, or both.

With this configuration, you have several choices on how to deploy the VoIP Monitor Servers, depending on the abilities of the various switches and whether the customer wishes to monitor only caller-to-agent calls or also agent-to-agent calls.

Figure 4: Three Layer Network Configured for Redundancy/Load Balancing



Agent-to-Agent Monitoring – Option 1

- SPAN is configured on switch B and C to monitor that switch's voice VLAN. The SPAN copies only ingress packets.
- If the access layer switch does not support VLAN monitoring ([Table 6](#)), use [Option 2](#).

Agent-to-Agent Monitoring – Option 2

- Set up SPAN to monitor each IP phone's IP port on the access layer switch.

For these installations, the only option for VoIP Monitor Server version 4.2 is to configure each stack of access switches to be an LCC, having all the devices in each LCC part of a voice VLAN, and to have a separate VoIP Monitor Server for each LCC, as shown in [Figure 4](#). On each stack, SPAN is configured to monitor the voice VLAN on that stack.

Deployment Planning

When planning for a deployment of the VoIP Monitor Server, many decisions must be made. These decisions help dictate how many VoIP Monitor Server installations are needed, where they are deployed, and how the switches are going to be configured. [Table 1](#) below shows the major decisions/features that must be taken into account when planning a deployment of the VoIP Monitor Server. The importance, or ramifications to deployment, are summarized. These issues are expanded upon in later sections of this document.

Table 1: Major Decisions/Features

Decision/Feature	Importance

Number of Agents	<p>The VoIP Monitor Server can support the phone traffic of 128 simultaneous calls. Loads greater than this causes performance degradation. As a general equation, you can use $APT * N = X$, where APT = Average Peak Talk time, N = Number of agents, and X must be less than or equal to 128. This, of course, is a simplified formula. Real-world planning is much more complex and employs the use of Erlang tables to calculate the number of VoIP Monitor Server installations needed to support a given Contact Center.</p>
VLANs	<p>Voice and data must be separated by using voice and data VLANs. This improves capacity of the VoIP Monitor Server because it is not sniffing network traffic unrelated to calls. If the switch does not support VSPAN, or is constrained to sniffing only a single VLAN, the placement of the VoIP Monitor Server is limited.</p>
LCCs	<p>A single LCC can contain only one VoIP Monitor Server. Multiple LCCs imply multiple subnets and multiple VLANs, which can affect how the VoIP Monitor Server is deployed.</p>
Router Placement	<p>There can be no routers between the VoIP Monitor Server port and the port(s) being monitored through SPAN. Doing so causes the MAC address of the speech packets to be changed, becoming invisible to the VoIP Monitor Server.</p>
Switch Capabilities	<p>Different catalyst switches have differing capabilities when it comes to SPAN and RSPAN. These capabilities, or lack thereof, dictates where the VoIP Monitor Server can be deployed.</p>

Monitoring Requirements	Caller-to-agent call monitoring is generally less complex than also having agent-to-agent call monitoring capability. The requirements from the customer dictates where the VoIP Monitor Server can be deployed.
Number of Supervisors	The number of simultaneous monitoring/sessions by supervisors must not exceed a ratio of one monitoring session to 10 agent calls. If the ratio needs to be higher, separate LCCs and VoIP Monitor Servers need to be installed to handle the monitoring load.

VoIP Monitor Server Assumptions

VoIP Traffic Exposure

In order for monitoring and recording to function correctly, the VoIP Monitor Server must be exposed to the IP traffic containing the RTP packets to be sniffed. This means the voice traffic must be presented to the network interface of the VoIP Monitor Server service. This is done by setting up SPAN or RSPAN on the switch(es) the agent's phones are connected to. SPAN and RSPAN configurations specify one or more ports or VLANs on a switch as source ports and a single port as a destination port. The destination port is the port used by the machine running the VoIP Monitor Server to connect to the switch. The IP traffic coming over the source ports is copied and sent to the destination port. The VoIP Monitor Server examines each packet to see if it should be copied and sent to a supervisor for monitoring, or the RASCAL server for recording. Ideally, the VoIP Monitor Server only needs to sniff the packets that it is interested in (voice packets). If voice VLANs are not used, or the switch only supports port sniffing ([Table 6](#)), which is sniffing the IP phone port directly, much more extraneous network traffic needs to be processed by the VoIP Monitor Server. This decreases the capacity of the server.

Layer 2 Switching Domains

Because VoIP traffic is sniffed and copied using the designated MAC address of the IP phone, there can be no layer 3 routing performed on the VoIP packets, this changes the MAC address of the Ethernet frames. There can be no routers between the VoIP Monitor Server port and the ports being sniffed (exposed through SPAN and RSPAN).

Single Copy of VoIP Packets

When configuring SPAN and RSPAN on the switch(es), it is important to verify that only a single copy of a VoIP packet is sent to the VoIP Monitor Server. If SPAN is set up to monitor two agent ports, and those agents are on a call with each other, the voice packets exchanged between the two IP phones can be sent to the VoIP Monitor Server twice, once when it leaves agent A's phone, and again when it is received by agent B's phone. For most Catalyst switches, the SPAN can be configured to only copy ingress or egress packets. If agent-to-agent calls are to be monitored, the SPAN/RSPAN must be configured to only copy ingress or egress packets, but not both. For switches that do not support this feature ([Table 5](#)), agent-to-agent call monitoring is not possible.

IP Phone Compatibility

The VoIP Monitor Server works with the Cisco 79xx series phones and the Cisco Agent Desktop soft phone.

Voice Encoding Protocols

The VoIP Monitor Server only supports the voice encoding protocols of G.711 and G.729 (with and without silence suppression). Other encoding schemes are not recognized by the monitoring software.

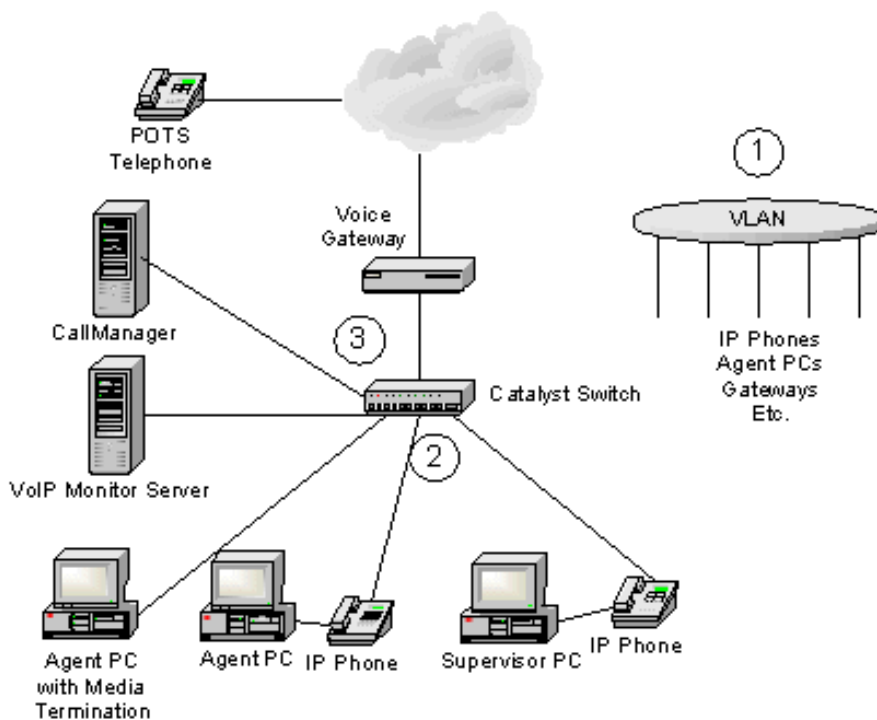
Single Processor Servers

The VoIP Monitor Server must be run on a single-processor machine. The low-level library that is used to sniff the network traffic does not support a symmetric multi-processing environment.

Deployment Strategies

This document provides verified configurations that enable the VoIP Monitor Server to work most efficiently with the least amount of intrusion into other configurations. This section describes, in general terms, the different sniffing configurations that can be used in successful installations. The major goal of these scenarios is to limit the amount of network traffic the VoIP Monitor Server needs to sniff in order to serve your needs. Sniffing excessive network traffic incurs loads on the VoIP Monitor Server machine, the switch(es), and the network. Using the correct sniffing strategies that match your needs allow the system to work most efficiently. Using an invalid sniffing scenario negatively affects the VoIP Monitor Server and the system as well. VoIP sniffing can be done at several locations in the system. In this context, “sniffing” means to set up a SPAN or RSPAN to monitor one or more ports and/or VLANs. The sources used by the SPAN each have issues that affect VoIP monitoring, which you should understand.

Figure 5: Sniffing Locations



As shown in [Figure 5](#), there are three locations that can be sniffed for voice traffic. These sniffing locations include:

1. Voice VLAN
2. IP Phone/Agent Desktop switch ports
3. Voice Gateway and CallManager ports

VLANS

Sniffing voice VLANS is the preferred sniffing method for two primary reasons:

- Separation of voice and data network traffic
- SPAN configuration and maintenance is easier

It is strongly recommended that voice and data network traffic be separated by VLANs, and that the VoIP Monitor Server is only sniffing the voice VLAN. The less network traffic the VoIP Monitor Server needs to process, the more capacity it has.

IP Phone Ports

If VLANs or VSPAN are not supported on the switch, SPAN needs to use individual ports as source ports rather than a VLAN. This is less desirable than VLAN sniffing due to the fact that both voice and data traffic is exposed to the VoIP Monitor Server. This additional traffic reduces capacity of the server.

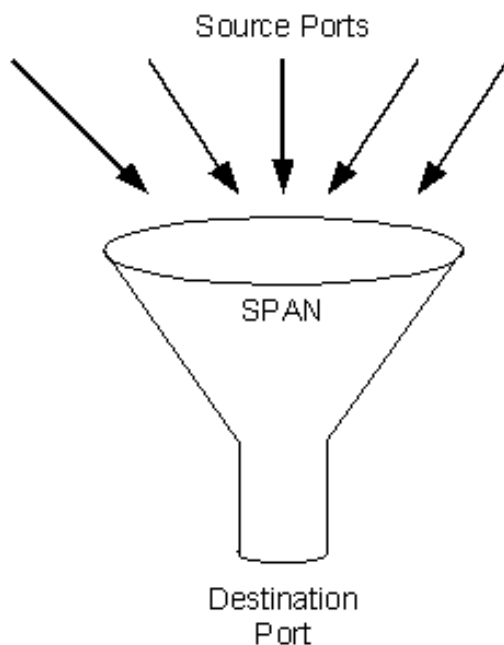
Voice Gateway and CallManager Ports

If agent-to-agent call monitoring/recording is not required, it is possible to set up SPAN to monitor the voice gateway port(s) and the CallManager port. This allows the VoIP Monitor Server to see all the voice packets that are exchanged in a call between an outside caller and the agent. Agent-to-agent calls cannot be monitored as the voice packets do not traverse the voice gateway port. An exception to this is if the agent is speaking to an outside caller and then conferences in another agent. In this case, the merging of the voice streams is handled by CallManager. Because the VoIP Monitor Server is monitoring the CallManager port, this three-way (or more) call can be monitored successfully.

SPAN Overview

The VoIP Monitor Server relies on a SPAN (Switched Port ANalyzer) session configured on the Catalyst switch. A SPAN session on a switch is simply a feature of the Cisco Catalyst switches that allows one or more port's IP traffic to be copied and sent to another single destination port on the switch. The ports that are used for the input to a SPAN are referred to as source ports. The port where all the copied traffic is sent is called the destination port. The SPAN destination port is referred to as the monitor port on some switches. In this document, this port is always referred to as the destination port.

Figure 6: SPAN Concept



Think of SPAN as a funnel that collects network traffic from multiple ports and copies it to a single output port, [Figure 6](#). The destination port of a SPAN is used by the VoIP Monitor Server to sniff for voice traffic to and from agent phones.

The source ports used by SPAN can be, depending on the switch model, ports or VLANs. In addition, only certain types of ports can be used as source ports. Using switch ports as source ports is referred to as PSPAN (Port SPAN). Using VLANs as source ports are referred to as VSPAN (VLAN SPAN). Some switches support only PSPAN. Other switches support both PSPANs and VSPANs. And some switches support the use of both ports and VLANs in a single SPAN configuration.

Local SPANs (LSPANs) are SPANs where all the source ports and the destination port are physically located on the same switch. Remote SPANs (RSPANs) can include source ports that are physically located on another attached switch.

The number of SPANs that can be configured can vary by switch. SPAN configuration and functionality is not the same on all Cisco Catalyst switches. Some switches can have the SPAN destination port configured to only show packets that are incoming to the source port(s) (ingress traffic) or only packets that are outgoing to the source port(s) (egress traffic). The default for many switches is to show both ingress and egress packets hitting the source port(s).

On some Catalyst switches, the destination port of a SPAN does not accept incoming packets. In these cases, the machine running the VoIP Monitor Server must have two NIC cards; one to send and receive normal network traffic, and another to receive voice traffic from the switch.

For more information on SPAN and RSPAN, please refer to your switch documentation.

Switch Capabilities

The VoIP Monitor Server is targeted specifically for the Cisco line of Catalyst switches. It may work with other switches that offer VoIP traffic, but it has not been tested on other switches.

There are differences among the Cisco Catalyst switches that you should be aware of when installing and configuring the VoIP Monitor Server software. The switch issues that are known at this time are shown in the tables below.

SPAN Support

For certain switches, the ability to set up SPAN, or something similar in functionality, does not exist for the switch. In these cases, the VoIP Monitor Server does not work because there is no method for giving the monitor software access to the voice traffic. The following Catalyst switches fall into this category.

Table 2: Catalyst Switches that Do Not Support SPAN

Catalyst Switch
1700
2100
2800
2948G-L3
4840G

RSPAN Support

In some cases, it is desirable to use RSPAN in a VoIP Monitor Server deployment. Not all switches support RSPAN. In some cases, a switch may not support RSPAN, but may be an intermediate switch within an RSPAN configuration. The switches that do not support RSPAN are shown in [Table 3](#).

Table 3: Catalyst Switches That Do Not Support RSPAN

Catalyst Switch
1200
1900
2820
2900

2900XL
2926GS
2926GL
2926T
2926F
2948G
2950
2980G
3000
3100
3200
3500XL
3524-PWR XL
3508GL XL
2550
5000
5002
5500
5505
5509

Network Traffic Restrictions

Some Catalyst switches do not allow the destination port of a SPAN configuration act as a normal network connection. The only traffic that flows through this port is the traffic copied from the SPAN source ports. This means that the computer running the VoIP Monitor Server must have two network connections to function properly. It needs one NIC to receive, monitor, and record requests and to interact with the other components of the Cisco Agent Desktop software, which reside on other machines within the network. The second NIC is dedicated to sniffing VoIP traffic for monitoring and recording. The switches that fall into this category are shown in [Table 4](#).

Table 4: Catalyst Switches That Do Not Support Outgoing Traffic on SPAN Destination Port

Catalyst Switch
2950
3000
3100
3200
3550

The steps required to configure the system so the VoIP Monitor Server works correctly are shown in [Using Multiple NIC Cards with the VoIP Monitor Server](#).

Ingress and Egress Monitoring

In some configurations, the VoIP Monitor Server can receive duplicate voice packets. This issue can potentially happen with many Cisco Catalyst switches. The problem occurs in agent-to-agent calls when SPAN/RSPAN is configured to sniff both ingress and egress packets from both parties on the call. As a voice packet leaves agent A's port, SPAN copies it to the VoIP Monitor Server port. When the voice packet arrives at agent B's port, it is again copied and sent to the VoIP server. The same happens when agent B speaks. All packets are seen twice by the VoIP Monitor Server. This causes very bad speech quality. To avoid this, only ingress packets to a port are sent to the VoIP Monitor Server. This is a setting for SPAN. Some switches do not support this. The switches that do not support ingress-only packet sniffing are shown in [Table 5](#).

Table 5: Catalyst Switches That Do Not Support Ingress/Egress Only Monitoring

Catalyst Switch
1900
2900
2820
2900XL
3000
3100
3200
3500XL

VSPAN Support

In some switches, SPAN cannot use VLANs as sources. In this case, SPAN must designate individual ports to use for monitoring. The switches that do not support VSPAN are shown in [Table 6](#).

Table 6: Catalyst Switches That Do Not Support VSPAN

Catalyst Switch
1200
1900
2820
2900XL
2950
3000
3100
3200
3500XL
3524-PWR XL

Number of SPAN Sessions

There are limits to the number of SPAN/RSPAN sessions that can exist on a switch. These limits are shown in [Table 7](#).

Table 7: SPAN Limits for Catalyst Switches

Switch Model	MAX SPANs Allowed
1200	1

1900	1
2820	1
2900	1
2900XL	1
2926GS	5
2926GL	5
2926T	5
2926F	5
2948G	5
2950	1
2980G	5
3000	1
3100	1
3200	1
3500XL	1
3524-PWR XL	1
3508GL XL	1
3550	2
4003	5
4006	5
4912G	5
5000	5
5002	5
5500	5
5505	5
5509	5
6006	30
6009	30
6506	30
6509	30
6513	30

Using Multiple NIC Cards with the VoIP Monitor Server

Problem

The VoIP Monitor Server sniffs RTP traffic from the network and sends it to the interested registered clients. This requires support from the switch that the server is connected to. Specifically, the VoIP Monitor Server must be connected to the destination port of a configured SPAN/RSPAN. Any traffic that crosses the SPAN/RSPAN source ports is copied also to the destination SPAN/RSPAN port and consequently is seen by the VoIP Monitor Server.

Initially, it was assumed that the VoIP Monitor Server could use the SPAN port to not only receive but also to send out traffic.

However, this is not true with all the switches. There are switches that do not allow outgoing traffic on a SPAN destination port.

Solution

A solution to this problem is to use two network adapters in the machine running the VoIP Monitor Server:

1. One for sniffing the RTP streams; this adapter is connected to the SPAN port.
2. One for sending/receiving normal traffic, such as, requests from the clients, sniffed RTP streams; this adapter is connected to a normal switch port, not monitored by the above mentioned SPAN port.

Limitations

1. Since the Cisco CallManager does not support two network adapters, this solution works only in configurations where CallManager is not co-resident with VoIP Monitor Server.
2. WinPCap 2.2, the sniffing library, works only with network adapters that are bound to TCP/IP. Make sure the sniffing card is bound to TCP/IP.

Issues

- The VoIP Monitor Server does not specify which interface should be used when sending out packets. This is not a problem when using a single network adapter for both sniffing and normal traffic. With two network adapters, we should restrict the normal traffic so that it does not go through the sniffing adapter. Otherwise, the sniffed RTP streams of a currently monitored call may not reach the supervisor because the SPAN destination port does not allow outgoing traffic.

Resolution: Use the **route** command to customize the static routing table so the normal traffic does not go through the sniffing card. Contact your network admin for details.

Alternative: Give the sniffing card an "unusual" IP address, that no other host on the network uses and a subnet mask of "255.255.255.0". Also, leave the default gateway field blank for this card TCP/IP binding.

- When installing, ICD needs to register with Cisco CallManager by passing it an IP address. This IP address is used by the CallManager to callback the ICD. The IP address passed to CallManager is found by resolving the local hostname through a name server (like a DNS server or a WINS server). If the box has two IP addresses which are returned by the server, it is desirable to have the name service not return the sniffing card IP address, as this one cannot be used for outgoing traffic.

Resolution: Use admin commands to unregister sniffing card registration with name services (DNS and WINS). In order for these commands to work the DHCP should be disabled for both network adapters. Check with **ping** <local hostname> to see if the right IP address is returned. Contact your network admin for details.

Installation of a Second Network Adapter on the VoIP Monitor Server Box

(Only Microsoft Windows 2000)

1. Insert the second network adapter into the computer.
2. Boot the computer.
3. Make sure that no adapter is using DHCP to get its IP address.
4. Give the adapters a valid IP address.
5. Decide which of the two adapters is used for sniffing. Connect it with the switch SPAN port.
6. Connect the second adapter with a normal switch port that is NOT monitored by the SPAN port.
7. Use the **route** command to customize the local routing table, so that the normal traffic does not go through the sniffing card. You should talk to the network admin for this information.
8. Make sure the sniffing card is not registered with DNS and WINS. Verify this with the **ping** <local host name> command. This ensures that the local name always resolves to the normal traffic card IP address. Contact to your network admin for

additional information.

Cisco Agent Desktop for ICD Installation

ICD Installation Issue

The Cisco Agent Desktop for IPCC install offers the user the option to choose the IP address that the VoIP Monitor Server uses for normal traffic and the IP address of the network adapter that the server uses for sniffing. However, the ICD install integrates the Cisco Agent Desktop install in such a way that the user can only specify the IP address of the sniffing card. The IP address where the VoIP Monitor Server is receiving requests is, by default, the first one to appear in the system supplied enumeration. While this works in one NIC scenario, it may be wrong in two NIC scenarios. If the first IP address that appears in the enumeration is the sniffing card then the same card is used for both, sniffing and the other traffic. This is exactly what you should try to avoid. Inserting a DDTS for the ICD install may be in order to correct this problem.

Resolution: Make sure the right IP address is written in Cisco Agent Desktop servers registry settings (see below for instructions):

Computer Having the Second Network Adapter before the ICD Setup

1. Insert the sniffing card IP address when asked for “VoIP Monitor Server” during the ICD installation.
2. After install, make sure the following registry keys have the normal traffic IP address value:

```
HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall VoIP MonitorServer\
  Setup\IOR HOSTNAME
HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall RASCAL Server\Setup\IOR HOSTNAME
HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall Chat Server\Setup\IOR HOSTNAME
HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall Enterprise Server\Setup\
  IOR HOSTNAME
```

Note: The above value is displayed over two lines due to space limitations.

Computer Having the Second Network Adapter Installed after the ICD Setup

1. Go in Registry to:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\
  NetworkCards
```

2. Find the newly inserted card entry.
3. Copy the value in “ServiceName”.
4. Paste this value to the HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall VoIP Monitor Server\Setup\MonitorDevice key.
5. Add \Device\Packet_ in front of it.

Cisco Agent Desktop for IPCC Installation

Computer Having the Second Network Adapter Before the ICD Setup

1. Insert the normal traffic card IP address when the “machine IP address” is requested during IPCC installation.
2. Insert the sniffing card IP address when asked for “VoIP Monitor Server” during the IPCC installation.

Computer Having the Second Network Adapter Installed After the ICD Setup

1. Go in Registry to **NetworkCards**.
2. Find the newly inserted card entry.

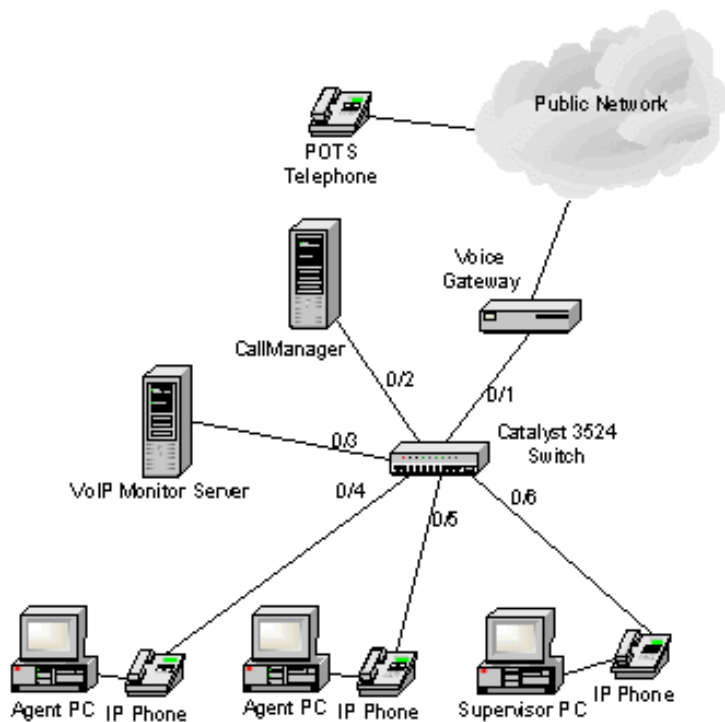
3. Copy the value in “ServiceName”.
4. Paste this value to the HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall VoIP Monitor Server\Setup\MonitorDevice key.
5. Add \Device\Packet_ in front of it.

Simple Network Deployment Example

Assumptions:

- The switch ports are configured as shown in [Figure 7](#).
- The voice VLAN used by the IP Phones is VLAN1.

Figure 7: Simple Network Deployment Example



Create a SPAN Session on the Switch:

Step	Command	Description
1	config t	Enter Configuration mode
2	interface 0/3	Enter configuration mode for Ethernet port 0/3
3	port monitor vlan 1	Set up SPAN to monitor Voice VLAN1

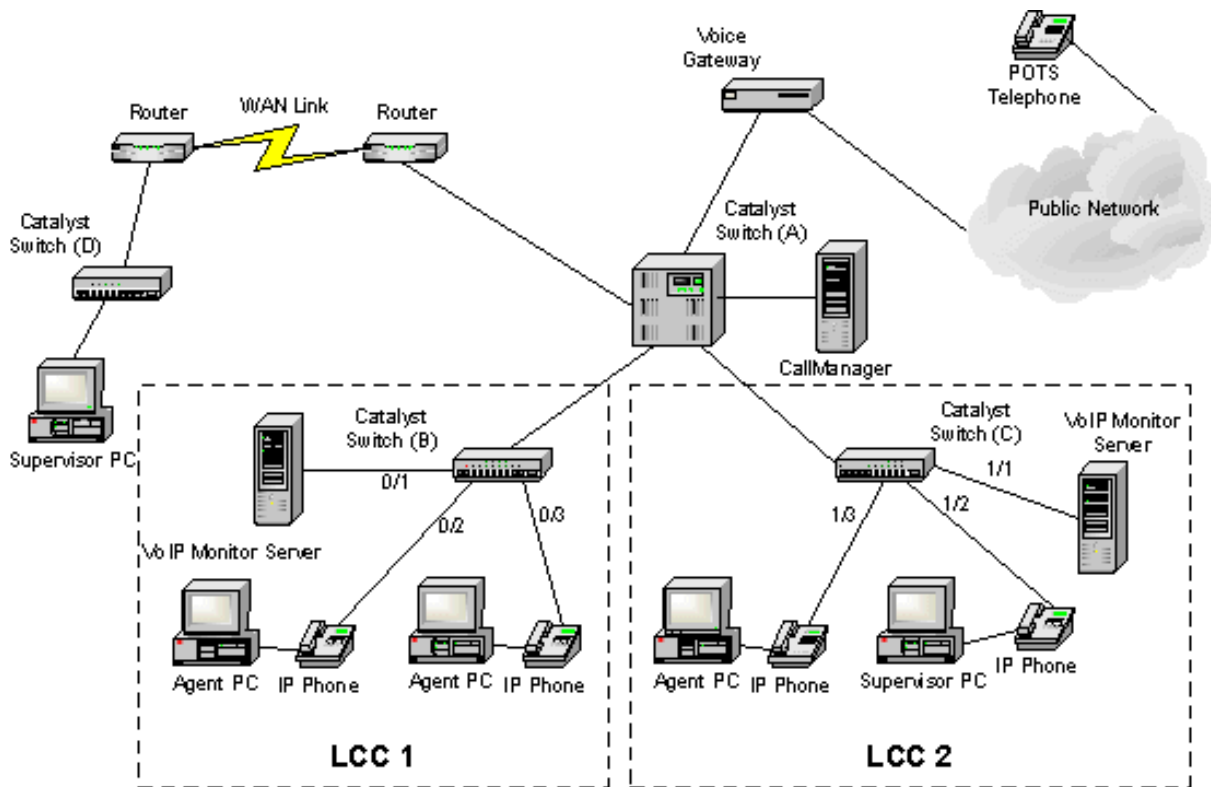
The VoIP Monitor Server can now see all of the voice traffic from the IP phones connected to the switch. Both caller-to-agent and agent-to-agent calls can be monitored/recorded.

Collapsed Core Network Deployment Example

Assumptions:

- The switch ports are configured as shown in [Figure 8](#).
- The voice VLAN used by the IP phones on both switches is VLAN1.

Figure 8: Collapsed Core Network Deployment Example



Create a SPAN Session on Switch B:

Step	Command	Description
1	config t	Enter configuration mode
2	interface 0/1	Enter configuration mode for Ethernet port 0/1
3	port monitor vlan 1	Set up SPAN to monitor Voice VLAN 1

The VoIP Monitor Server can now see all of the voice traffic from the IP phones connected to the switch. Both caller-to-agent and agent-to-agent calls can be monitored/recorded.

Repeat the same steps on switch C.

NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

[NetPro Discussion Forums - Featured Conversations for Customer Contact Software](#)

Related Information

- [Technical Support - Cisco Systems](#)
-

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

All contents are Copyright © 1992-2005 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).