

Configure and Deploy Silent Monitoring and Record in CRS

Document ID: 40423

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Cisco Supervisor Desktop Setup

SPAN Setup

- How SPAN Enables Voice Monitoring and Recording
- Setting up SPAN
- Summary of SPAN Limitations and Issues
- SPAN on Catalyst 4000 and 6000 Series Switches
- SPAN on Catalyst 3500 and 2900 Series Switches

When Voice Monitoring and Recording Work

- VoIP Monitor and Phones on the Same Switch
- VoIP Monitor and Phones on a Downstream Switch

When Voice Monitoring and Recording Does Not Work

- VoIP Monitor and Phones in Multiple VLANs
- VoIP Monitor and Voice Ports over a WAN
- Network Interface Card (NIC) Teaming Enabled

Conclusion

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

Voice monitoring and recording are features of the IP Integrated Contact Distribution (ICD) Cisco Supervisor Desktop (CSD) client. These features allow a Supervisor to silently monitor and record an agent phone call. Silent monitoring is a term used synonymously with voice monitoring. It refers to the ability of a Supervisor to monitor agent phone conversations without being heard or without the knowledge of the agent. The recording features allow the Supervisor to record, save, and play back calls from their CSD. The other Supervisor features, barge-in and intercept, do not depend on Switched Port Analyzer (SPAN) and are not discussed in this document.

Voice monitoring and recording functions are available in the Enhanced CSD client. Neither of these features work unless the network is configured to monitor between the Ethernet ports for both of these:

- The Voice-Over IP (VoIP) Monitor server, which accomplishes voice monitoring and recording functions by sniffing voice packets to and from IP phones (destination port).
- All agent IP phones (source ports).

This document addresses some design and configuration issues faced when you set up the port monitoring SPAN feature on a Cisco Catalyst switch. These issues are discussed as related to the integration of silent monitoring and recording in a single-site AVVID Campus network. SPAN does not run automatically on Cisco switches. SPAN must be manually configured on the switch to enable the voice packets going to and from an agent phone to be sent to the VoIP Monitor server destination port.

Note: Voice monitoring and recording are supported only on IPCC Express Enhanced and Premium Edition, not on Standard Edition.

This document only describes the set-up process for voice monitoring and recording with Customer Response Solution (CRS) version 3.0 and IP ICD. This document does not describe the installation procedures for IP-ICD/CRS/CSD, or for Cisco CallManager. For such references, refer to Cisco Customer Response Applications 3.0. For further detailed information on SPAN, refer to Configuring the Catalyst Switched Port Analyzer (SPAN) Feature.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco CallManager Administration
- CRS 3.x
- Basic knowledge of the Catalyst SPAN feature

Components Used

The information in this document is based on these software and hardware versions:

- Cisco CallManager 3.2.x
- CRS 3.x
- Cisco Catalyst SPAN enabled switches
- Supervisor PC to install Cisco Supervisor Desktop

Note: This document assumes the Administrator logins are available for both the Cisco CallManager and CRS Server.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Cisco Supervisor Desktop Setup

On the Supervisor PC, first install the Cisco Supervisor Desktop. The Cisco Supervisor Desktop is not a supported co-resident with the CRS server. Refer to Cisco Customer Response Applications 3.0 for detailed installation information.

Next, set up SPAN. Without SPAN, the Supervisor is unable to hear an agent conversation, and nothing happens when the Supervisor clicks the record button in the CSD.

SPAN Setup

This section describes the prerequisites for a SPAN set-up. These sections describe the scenarios in which SPAN works or does not work. It also includes sample configurations of SPAN on a Catalyst 3524 switch.

How SPAN Enables Voice Monitoring and Recording

This section describes how SPAN is used to monitor voice calls from agent phones, and the mechanics of how the Supervisor monitors the agent phones.

The set-up process for SPAN, in order to enable voice monitoring and recording, is the same as the set-up for a packet sniffer. A packet sniffer is a program that can record all network packets that travel past a given network interface, on a given computer, on a network. Ethernet works when packet information (for example, voice packets from agent phones) is sent to all the hosts on the same circuit. The packet header contains the proper address of the destination machine which accepts the packet. However, the destination SPAN port for VoIP Monitor accepts, or monitors, all packets regardless of what the packet header says, and is said to be in promiscuous mode.

If a Supervisor wants to listen to a specific agent phone conversation, SPAN uses these mechanics:

- Supervisor (CSD) submits a request to the CRS to monitor that agent call.
- VoIP Monitor server sets up a relay agent to the Supervisor PC.
- SPAN presents the voice traffic to the VoIP Monitor server, which filters out packets of interest and forwards them to the Supervisor PC.

Setting up SPAN

For additional information on how to set up SPAN ports for monitoring and recording, refer to the Cisco Desktop Product Suite 4.3 (ICD) Installation Guide. Specifically, *Section 1–11 (Required SPAN Port Configuration)*. This Installation Guide clearly describes the limitations of SPAN. Service Information Cisco Desktop Product Suite 4.3 (ICD) also describes the packet sniffers and network configuration for the CRS agent.

Summary of SPAN Limitations and Issues

As mentioned earlier, there is a requirement for RTP streams to be available at the VoIP Monitor server location in order for it to be able to function correctly. The limitations are that a monitor port cannot be:

- In a Fast EtherChannel or Gigabit EtherChannel port group
- Enabled for port security
- Multi-VLAN port
- Dynamic-access port or a trunk port
- Protected port

These restrictions present the potential for these issues:

- Where the network topology is hierarchical (for example, in the case where an attempt is made to connect switches together), SPAN limitations make it very difficult to monitor an agent phone port on a downstream or remote switch. As mentioned, VoIP Monitor directly monitors agent voice ports, and cannot monitor those ports over trunks between switches. See the VoIP Monitor and Phones on a Downstream Switch section for a workaround in order to monitor ports on downstream switches.
- When a Supervisor resides in a remote branch office, the Supervisor is not able to silently monitor or record local agents in their remote branch. The reason is that voice packets that go to and from an agent source phone ports need to be sent to the VoIP Monitor server destination port over the WAN. The voice packet MAC address changes as the packet moves across a network router (at the edge of a WAN), so the VoIP Monitor can no longer monitor or filter these packets (between the phone and the VoIP Monitor destination port). See the How Span Enables Voice Monitoring and Recording section in order to understand how SPAN works better.

- Another issue to keep in mind when you set up voice monitoring and recording is security. SPAN relies on running in a promiscuous mode and by sniffing all packets on the network. If those packets are encrypted, there is no way for the monitored packets to be decoded and processed by the VoIP Monitor. This is particularly an issue for VPN solutions.

Note: Refer to VoIP Monitor Server 4.2 Best Practices Configuration Guide for more information on SPAN limitations.

SPAN on Catalyst 4000 and 6000 Series Switches

Catalyst 4000 and 6000 Series Switches are able to monitor ports that belong to multiple VLANs. They are also able to monitor agent phones on remote or downstream switches with the help of a feature known as Remote SPAN (RSPAN). However, there is still a requirement for both the VoIP Monitor server port and source port that monitors the agent phones to be a member of the same VLAN. The monitor ports do not necessarily have to connect to the same switch, though this is the simplest configuration.

RSPAN can be used in the same way as a regular SPAN session to monitor voice traffic from a trunk port. The traffic monitored by SPAN, instead of being directly copied to the destination port, is flooded into a special RSPAN VLAN. The destination port for VoIP Monitor can then be located anywhere in this RSPAN VLAN.

Note: RSPAN requires all downstream switches to be either Catalyst 4000 or 6000. For a detailed description of how an RSPAN session works, refer to Configuring the Catalyst Switched Port Analyzer (SPAN) Feature – Remote SPAN and for an RSPAN configuration guide, refer to Configuring RSPAN.

SPAN on Catalyst 3500 and 2900 Series Switches

RSPAN is not available on the Catalyst 3500, 2900, or 3524–PWR switches. This presents some design issues where access switches (to which agent ports are attached) are trunked back to a distribution switch. It is not possible to monitor source voice traffic from these trunks (since RSPAN is not supported). The possible workarounds include these:

- Run a separate cable from the VoIP Monitor to the access switch monitoring the agent phones (there must be no other agent phones on remote switches). An issue here is that the second cable between the two switches provides a second path and spanning tree blocks one of these paths in order to prevent a spanning tree loop. Spanning tree needs to be disabled for voice packets to be successfully forwarded to the VoIP Monitor with this workaround (which makes it an undesirable option).
- A better approach is to configure a second network interface card (NIC) on the VoIP Monitor server, and place that NIC in a dedicated VLAN (Layer 2 configuration only). If you have not already installed Carrier Routing System (CRS), then run the CRS installation file and specify the address of the second NIC in the VoIP Monitor address configuration. If CRS is already installed, you need to install CRS again to specify the second NIC as the VoIP Monitor address (this is configurable during the CRS re-installation). This workaround has been successfully tested, and resolves the spanning tree issues. An explanation and network diagram for this workaround is shown in diagram 2.

Note: With CRS 3.0(2) and later, the customer can install the VoIP Monitor services on a separate box from the CRS server. All of the other required configurations, including the SPAN port, are still necessary. Since there is significant overhead in recording and monitoring many calls, this change allows customers to offload that CPU utilization to another server.

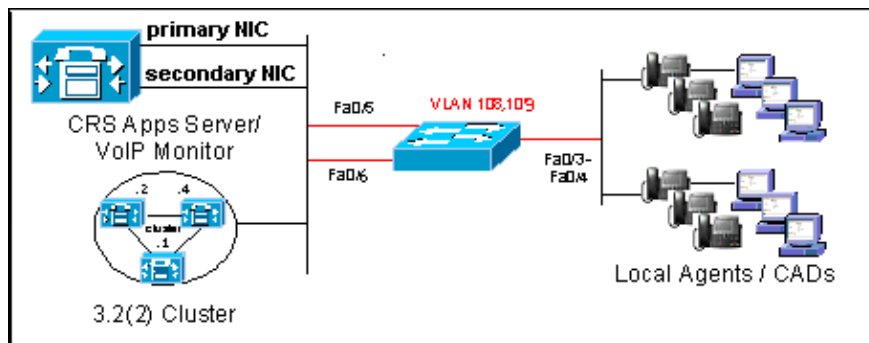
When Voice Monitoring and Recording Work

With respect to how you make SPAN work on the Catalyst 2900XL and 3500XL switches, diagrams 1 and 2 show valid SPAN scenarios in which the VoIP Monitor and voice streams are monitored for silent monitoring and recording.

VoIP Monitor and Phones on the Same Switch

In diagram 1, both the VoIP Monitor and agent phone ports are co-located in the same VLAN on the same switch.

Diagram 1 VoIP Monitor and Voice Ports on Same Switch (works)



This is the port monitor (SPAN) configuration for a Catalyst 3524 switch that is tested in the previous scenario. It is assumed that Ethernet ports for VoIP Monitor and phones reside on the same switch.

```
interface FastEthernet0/5
!--- Destination port to which VoIP Monitor is connected.
duplex full
speed 100
!--- Commands enable monitoring of agent phone source ports.
port monitor FastEthernet0/3
port monitor FastEthernet0/4
port monitor FastEthernet0/6
switchport access vlan 108
!
```

In the configuration example, interface FastEthernet0/5 is the destination port to which the VoIP Monitor server is attached. A destination port (also called a monitor port) is a switch port where SPAN sends voice packets for analysis. Once a port becomes an active destination port; it does not forward any traffic except that required for the SPAN session. On a Catalyst 3524, the active destination port is enabled and permits both incoming (Rx) and outgoing (Tx) traffic. Incoming traffic from the source phone ports is switched in the native VLAN of the destination port, in this case VLAN 108.

Note: The destination port does not participate in spanning tree while the SPAN session is active.

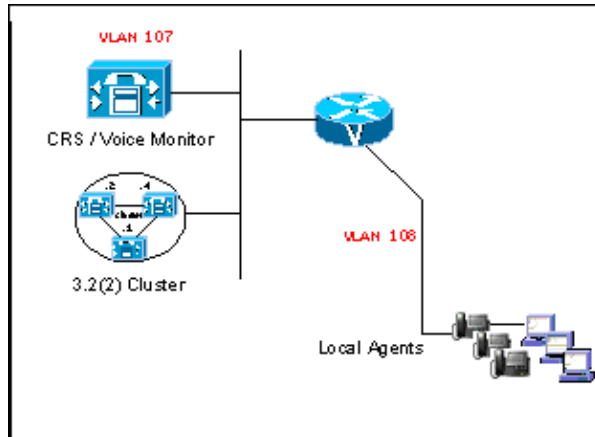
VoIP Monitor and Phones on a Downstream Switch

In diagram 2, the VoIP Monitor has two NICs.

1. The primary NIC uses the IP address accessible to the Cisco Agent Desktop (CAD) clients. It is connected to a distribution switch (for example, Fa0/5) in the VLAN accessible to the CADs or agents (for example, VLAN 108).
2. The secondary NIC uses a different IP address in a dedicated SPAN VLAN. This is connected to the same distribution switch (for example, Fa0/6) in a dedicated SPAN VLAN (for example, VLAN 109).

Agent phone ports are connected to downstream switches, and should be placed in the same VLAN as the VoIP Monitor primary NIC (VLAN 108). All CAD desktops must be able to ping the IP address of the CRS server. There are uplinks from these downstream switches to the distribution switch, where the VoIP Monitor server's two physical cables (from NIC 1 and 2) are connected.

Diagram 2 Voice Ports on Downstream Switch (works)



Refer to Configuring the Catalyst Switched Port Analyzer (SPAN) Feature for more information on SPAN.

This is the port monitor (SPAN) configuration for the Catalyst 3524 (distribution) switch in the previous scenario:

```
interface FastEthernet0/5

!--- Destination port to which VoIP Monitor s primary NIC is connected.

switchport access vlan 108
duplex full
speed 100
!
interface FastEthernet0/6

!--- Destination port to which VoIP Monitor s secondary NIC is connected.

switchport access vlan 109
duplex full
speed 100

!--- Commands enable monitoring of uplink ports from downstream switches.

port monitor FastEthernet0/3
port monitor FastEthernet0/4
!
```

In this scenario, the dedicated SPAN VLAN (109) promiscuously sniffs all voice packets from the monitored uplink ports that travel past FastEthernet0/6, and these packets are then replicated to the VoIP Monitor server.

Note: In both scenarios, if the monitor server has been moved, or new agent IP phones have been added, you

need to manually reconfigure SPAN to reflect these changes. This involves some management overhead to maintain a voice monitoring and recording setup.

Note: Use the Dual NIC cards on the same CRS server and use the second card for voice monitoring. (Co-located Cisco CallManager and CRS/VoIP Monitor Server configurations with dual NIC cards are not supported.)

Make sure that you have an IP address bound to the Monitor NIC before this procedure is attempted to determine the correct ServiceName for your VoIP Monitor NIC on the VoIP Monitor server:

1. From the task bar, choose **Start > Run**.
2. Issue the **regedit32** command.
3. In the **regedit32** window, navigate to this registry key:

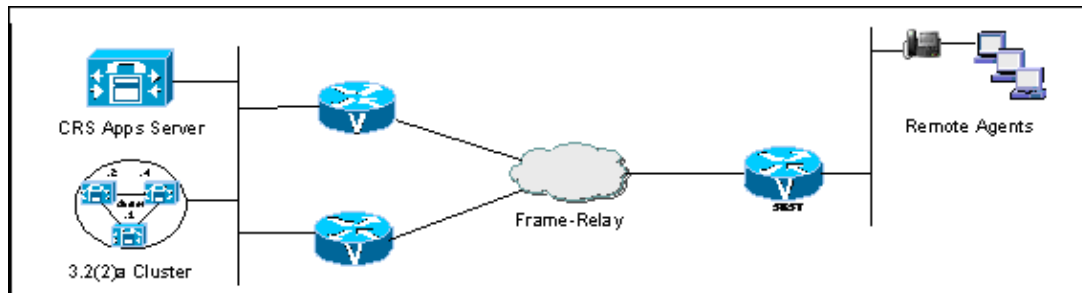
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\  
Interfaces
```

4. Search on the IP address connected to the Monitor NIC, and click **View > Find Key**.
5. The entry key, as shown in step 3, appears. This is the IP address of the Monitor NIC. The name of the folder that contains the match under the Interfaces is the ServiceName for the Monitor NIC.

In this example, the Monitor NIC has an IP address of 10.89.228.116 and the first NIC card has an IP address 10.89.228.115 bound to it. The ServiceName for the NIC is: {81B27D00-C66E-4969-A4CA-A2E89101A90E}.

Note: The examples here are not actual IP Address or MAC Addresses. They are for informational purposes only.

Figure 1: Registry Editor [HKEY_LOCAL_MACHINE on Local Machine]



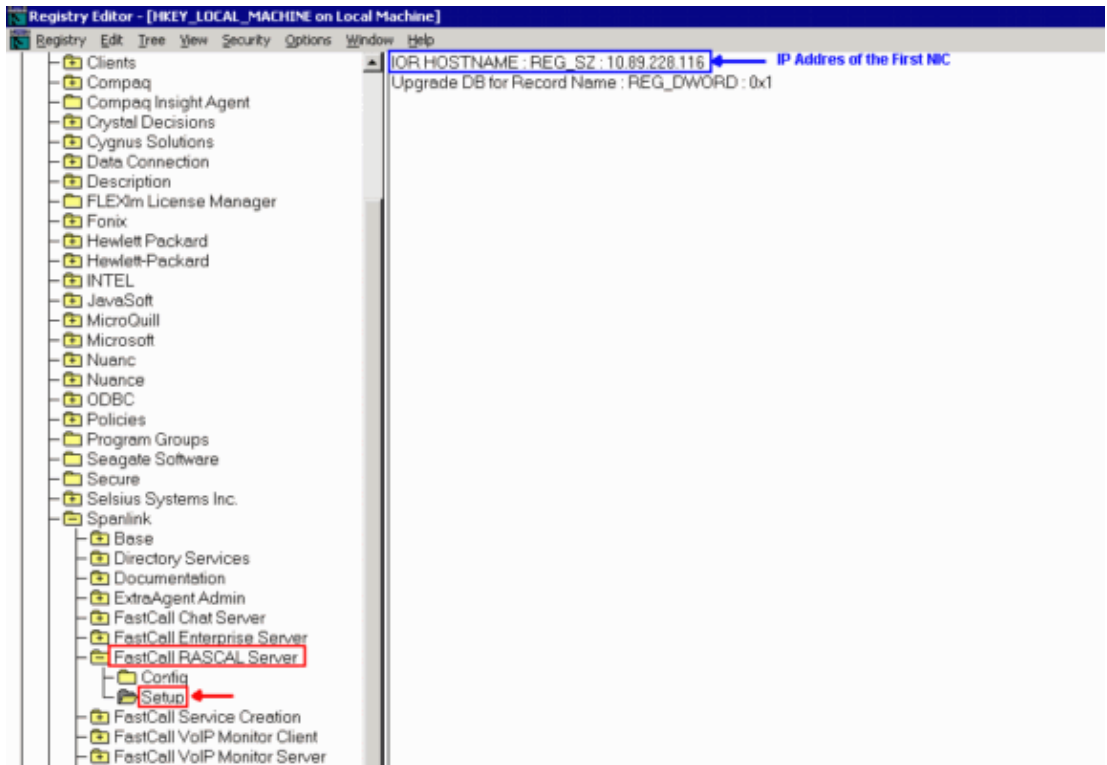
On the VoIP Monitor server, set these registry keys:

- Set this registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\FastCall VoIP Monitor Server/  
Setup/MONITOR_DEVICE
```

to **\Device\Splkpc_ ServiceName**, which is {81B27D00-C66E-4969-A4CA-A2E89101A90E}, as shown by the red arrow in the figure:

Figure 2: Registry Editor – [HKEY_LOCAL_MACHINE on Local Machine]



- Set the registry key:

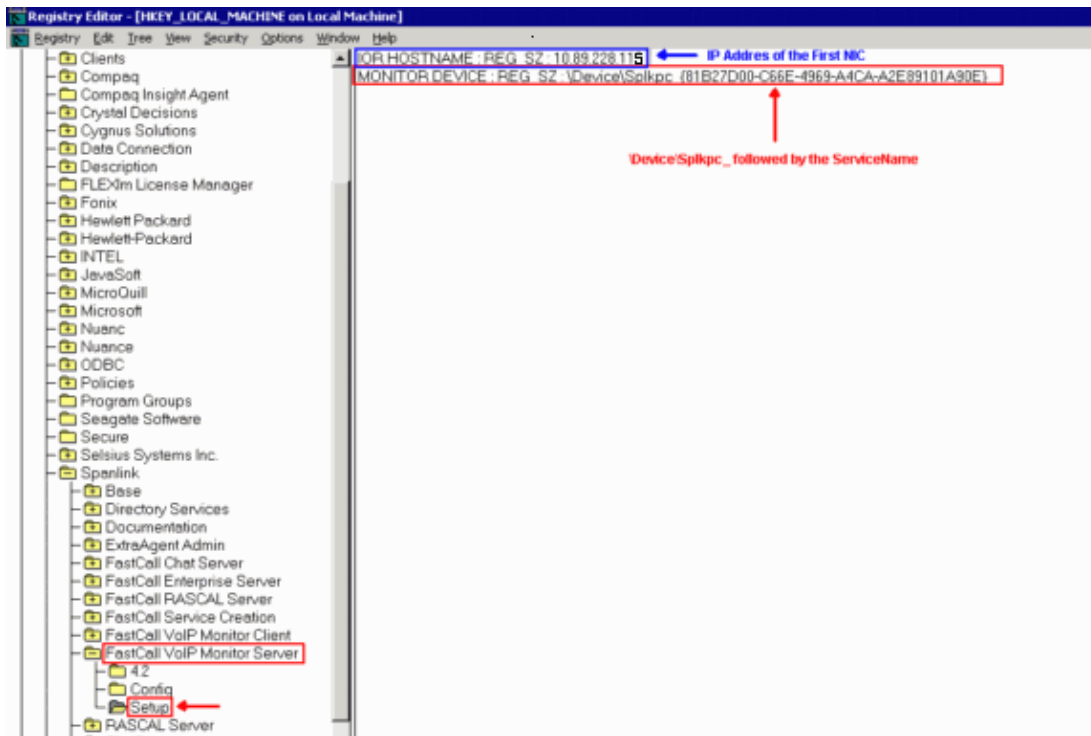
```
HKEY_LOCAL_MACHINE/SOFTWARE/Spanlink/FastCall VoIP Monitor Server/  
Setup/IOR_HOSTNAME
```

to the IP address of the first NIC, indicated by the blue arrow in Figure 2.

When Voice Monitoring and Recording Does Not Work

VoIP Monitor and Phones in Multiple VLANs

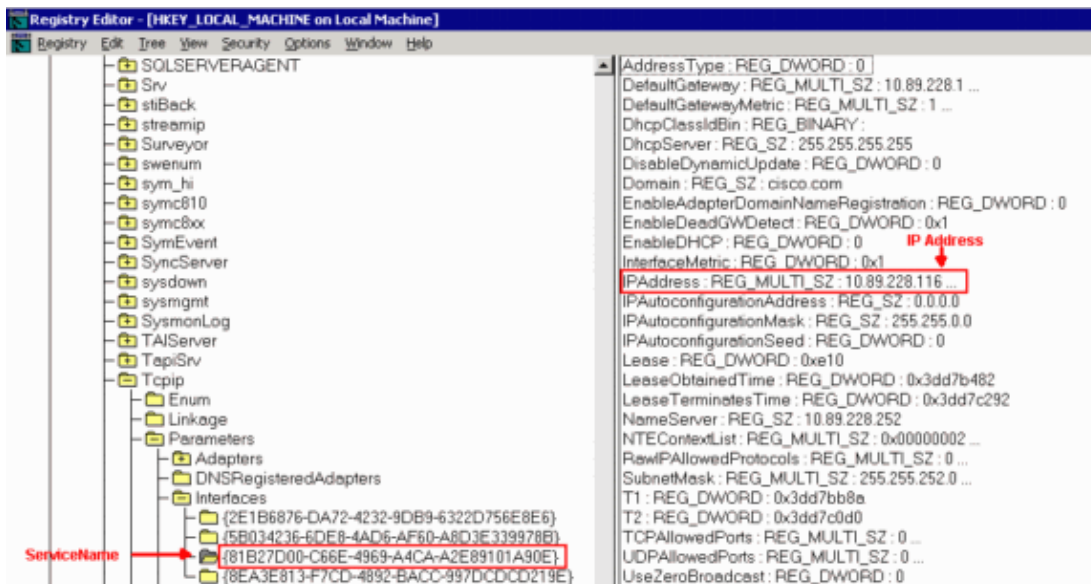
Diagram 3 Voice Monitor and Phones in Multiple VLANs (does not work)



The scenario in diagram 3 involves the use of multiple VLANs. For example, where the VoIP Monitor resides on the same server as the CRS 3.0 server in a server farm, and the agent phones are located in a different subnet with a private address space. This topology does not work because there must not be a router between the IP phone and the port the VoIP Monitor server monitors.

VoIP Monitor and Voice Ports over a WAN

Diagram 4 VoIP Monitor and Voice Ports over a WAN (does not work)



The VoIP Monitor server must be on the same VLAN as the agent IP phones, and requires an available SPAN port. Accordingly, the VoIP Monitor and agent phones cannot be separated by a WAN. Monitoring and recording do not work in the scenario shown in diagram 4.

Network Interface Card (NIC) Teaming Enabled

The Silent Monitor feature on IP Contact Center (IPCC) agents does not work if unsupported Network Interface Card (NIC) teaming is enabled. Refer to Desktop Monitoring Checklist and Troubleshooting Guide for more information on proper NIC configuration.

In order to fix the problem, disable NIC teaming and perform the steps as mentioned in the Desktop Monitoring Checklist section of Desktop Monitoring Checklist and Troubleshooting Guide.

Conclusion

The VoIP silent monitoring server must be on the same VLAN as the agent phones and requires an available SPAN port. See the workarounds described in SPAN on Catalyst 3500 and 2900 Series Switches in order to set up VoIP Monitor and agent phones on remote switches. The VoIP Monitor and agent phones cannot be separated by a WAN. They can be on different Catalyst switches, if the switches support RSPAN. Otherwise, voice monitoring and recording does not work.

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 Voice
Service Providers: Voice over IP
Voice & Video: Voice over IP
Voice & Video: IP Telephony
Voice & Video: IP Phone Services for End Users
Voice & Video: Unified Communications
Voice & Video: IP Phone Services for Developers
Voice & Video: General

Related Information

- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Recommended Reading: Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation – Cisco Systems**

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: May 14, 2007

Document ID: 40423
