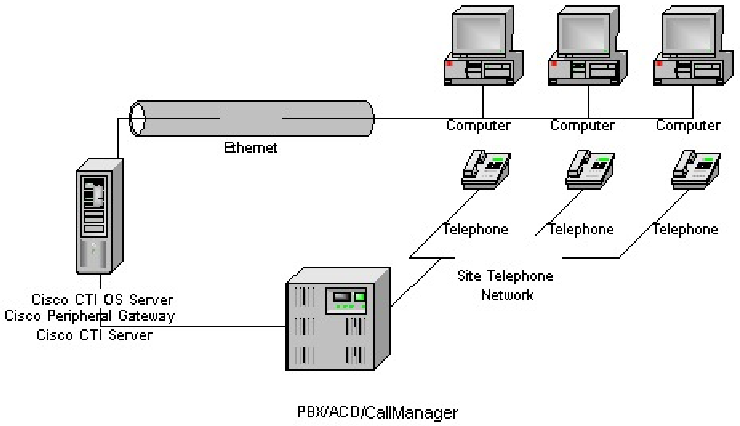
CTI OS Silent Monitor Installation and Configuration

Overview of CTI OS

CTI OS combines a powerful, feature-rich server and an object-oriented software development toolkit to enable rapid development and deployment of complex CTI applications. Together, the Cisco CTI Server Interface, CTI OS Server, and CTI OS Client Interface Library (CIL) create a high performance, scalable, fault-tolerant three-tiered CTI architecture, as illustrated in following figure.

Figure 1: CTI OS Three-Tiered Architecture Topology



The CTI OS application architecture employs three tiers:

- The CIL is the first tier, providing an application-level interface to developers.
- The CTI OS Server is the second tier, providing the bulk of the event and request processing and enabling the object services of the CTI OS system.
- The Cisco CTI Server is the third tier, providing the event source and the back-end handling of telephony requests.

Advantages of CTI OS as Interface to Unified ICM Enterprise

CTI OS brings several major advances to developing custom CTI integration solutions. The CIL provides an object-oriented and event-driven Application Programming Interface (API), while the CTI OS Server does the *heavy-lifting* of the CTI integration: updating call context information, determining which buttons to enable on softphones, providing easy access to supervisor features, and automatically recovering from failover scenarios.

The key advantages of CTI OS include:

- **Rapid integration**. Developing CTI applications with CTI OS is easier and faster than any previously available Cisco CTI integration platform. The same object-oriented interface is used across programming languages, enabling rapid integrations in C++, Visual Basic, .NET, Java, or any Microsoft COM-compliant container environment.

  Note The inclusion of the .NET toolkit allows for custom applications written in C#, VB.NET, or any other CLR-compliant language. By starting with the code for the .NET sample, the CTI Toolkit Combo Desktop developers can quickly customize the code without having to start from scratch.

  CTI OS enables developers to create a screen-pop application in as little as five minutes. The only custom-development effort required is within the homegrown application to which you add CTI.

- **Complex solutions made simple**. CTI OS enables complex server-to-server integrations and multiple agent monitoring-type applications. The CIL provides a single object-oriented interface that you can use in two modes: agent mode and monitor mode. For more information about these two modes, see CTI OS Developer Guide for Cisco Unified ICM/Contact Center Enterprise & HostedCTI OS Developer Guide for Cisco Unified ICM/Contact Center Enterprise at: http://www.cisco.com/en/US/products/sw/custcosw/ps14/products_programming_reference_guides_list.html.
- **Fault tolerant**. CTI OS is built upon the Unified ICM Node Manager fault-tolerance platform, which automatically detects process failure and restarts the process, enabling work to continue. Upon recovery from a failure, CTI OS initiates a complete, system-wide snapshot of all agents, calls, and supervisors and propagates updates to all client-side objects.

Key Benefits of CTI OS for CTI Application Developers

The CTI OS CIL provides programmers with the tools required to rapidly develop high-quality CTI-enabled applications, taking advantage of the rich features of the CTI OS Server. Every feature of CTI OS was designed with ease of integration in mind, to remove the traditional barriers to entry for CTI integrations:

- **Object-oriented interactions**. CTI OS provides an object-oriented CTI interface by defining objects for all call center interactions. Programmers interact directly with Session, Agent, SkillGroup, and Call objects to perform all functions. CIL objects are thin proxies for the server-side objects, where all the 'heavy-lifting' is done. The Session object manages all objects within the CIL. A UniqueObjectID identifies each object. Programmers can access an object by its UniqueObjectID or by iterating through the object collections.

- **Connection and session management**. The CTI OS CIL provides out-of-the-box connection and session management with the CTI OS Server, hiding all of the details of the TCP/IP sockets connection. The CIL also provides out-of-the-box failover recovery. Upon recovery from a failure, the CIL automatically reconnects to another CTI OS Server (or reconnects to the same CTI OS Server after restart), reestablishes the session, and recovers all objects for that session.

- **All parameters are key-value pairs**. The CTI OS CIL provides helper classes to treat all event and request parameters as simply a set of key-value pairs. All properties on the CTI OS objects are accessible by name via a simple Value = GetValue("key") mechanism. Client programmers can add values of any type to the CTI OS Arguments structure using the enumerated CTI OS keywords or their own string keywords (for example, AddItem["DialedNumber", "1234"]). This provides for future enhancement of the interface without requiring any changes to the method signatures.

- **Simple event subscription model**. The CTI OS CIL implements a publisher-subscriber design pattern to enable easy subscription to event interfaces. Programmers can subscribe to the event interface that suits their needs, or use the AllInOne interface to subscribe to all events. Subclassable event adapter classes enable programmers to subscribe to event interfaces and only add minimal custom code for the events they use, and no code at all for events they do not use.

System Manager Responsibilities

The remainder of this document provides step-by-step procedures for the tasks a system manager must perform to set up and configure CTI OS. These tasks include:

- Installing CTI OS Server.

- InstallingCTI Toolkit Agent Desktop, Supervisor Desktop, Tools, Documentation, Win32 SDK, Java SDK, and .NET SDK.

Note You can skip the procedures discussed in Chapters 2 and 3 if you already have CTI OS Release 8.5(3) or the later Service Releases (SRs) installed on your system.

- Enabling CTI OS security.

- Using the Windows Registry Editor (regedit.exe) to configure the required CTI OS registry keys.

- Starting CTI OS and its associated processes from Unified CCE Service Control.

Note You *must* have administrator privileges to perform the procedures discussed in this manual.

System Requirements

See the Unified CCE Solution Reference Network Design (SRND)Solution Design Guide for Cisco Unified Contact Center Enterprise at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html for a quick reference on configuration limits and scalability constraints. For more information on system requirements, see the *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html and the Compatibility Matrix for Unified CCEUnified CCE Solution Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Set User Privileges

On supported Windows client machines, users must have privileges that enables them to run legacy applications and have read/write access to the Cisco registry keys that the desktop applications use. To set user privileges to enable users to run CTI OS Agent Desktop and CTI OS Supervisor Desktop, an administrator must perform the following steps.

Procedure

Step 1 On the Microsoft Windows Start Menu, select **Start** > **Run**.

Step 2 Type in **regedt32** and click **OK**.
The Microsoft Windows Registry Editor window appears.

Step 3 Go to the following registry location:
`HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTI Desktop\Ctios`

Step 4 Select **Security** > **Permissions**.
A Permissions dialog box appears.

Step 5 If you are adding a new user, perform the following steps.

a) Click **Add**.
A Select Users dialog box appears.

b) Select the user to be added from the list in the top half of the Select Users dialog box.

c) Click **Add**, then click **OK**.
You return to the Permissions dialog box; the user you just added is now on the list.

Step 6 Click the user whose privileges you want to set.

Step 7 Set the Full Control permissions for this user to **Allow**.

Step 8 Click **Apply**.

Step 9 Click **OK**.

Step 10 Exit Registry Editor.

Silent monitoring

Silent monitoring is a feature that allows a supervisor to eavesdrop on a conversation between an agent and a customer without allowing the agent to detect the monitoring session. Silent monitoring functionality can be provided by Cisco Unified Communications Manager (Unified CM) or CTI OS.

You can configure each CTI OS Server for either Unified CM-based or CTI OS-based silent monitoring.

Silent Monitor Differences Between Unified CM and CTI OS

Besides the differences in implementation, CTI OS and Unified CM also differ in when they can be invoked and when they end.

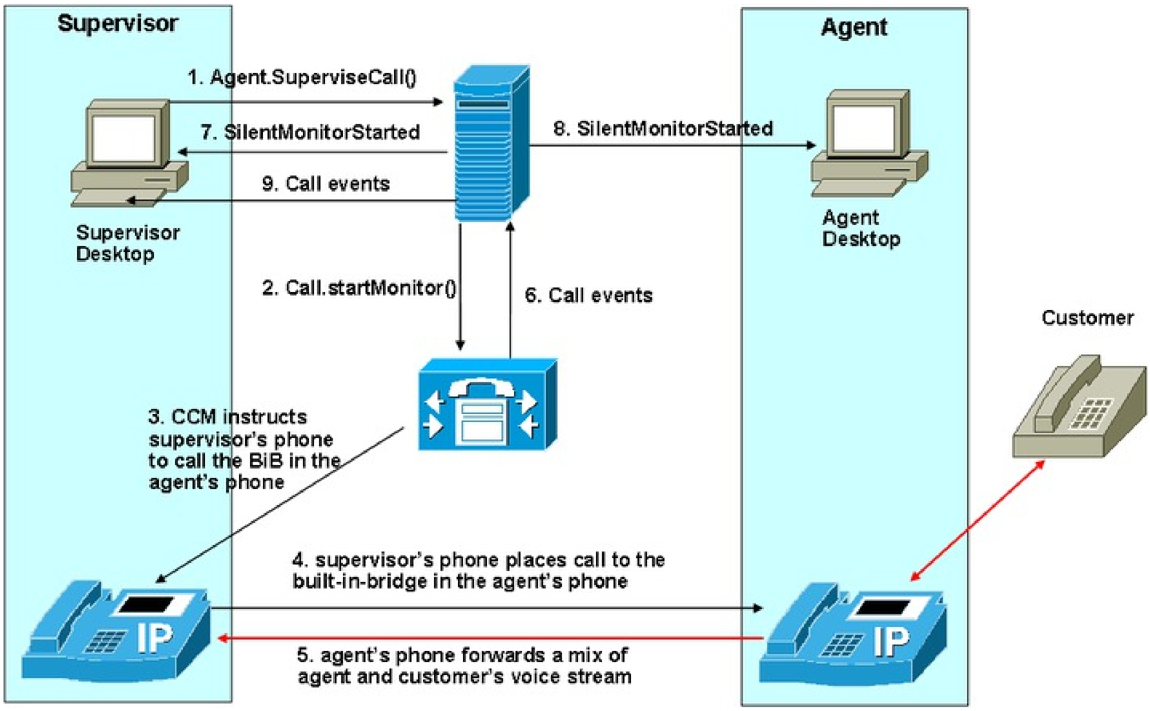
Table 1: Unified CM-Based and CTI OS-Based Silent Monitor Differences

Unified CM-Based silent monitor	CTI OS-Based silent monitor
The supervisor can only silent monitor an agent who is actively talking in a call.	The supervisor can silent monitor an agent in any state as long as the agent is logged in.
Supervisor cannot silent monitor an agent on hold.	Supervisor can silent monitor an agent on hold.
When agent consults, supervisor must stop silent monitoring held call and start silent monitoring conference.	When agent consults, supervisor automatically hears consult call.
Supervisor can only silent monitor in Not Ready state.	Supervisor can silent monitor in any state.
Supervisor must stop silent monitoring before barging in.	Supervisor can barge in while silent monitoring.
When the call that is being silent monitored ends, the silent monitor call ends. The supervisor must restart silent monitor after the agent answers another call.	When call ends, supervisor automatically silently monitors the next call as long as the supervisor has not stopped silent monitoring.

Unified CM-Based Silent Monitoring

Unified CM-based silent monitor allows a supervisor to listen in on agent calls in UCCE call centers. Supervisors can send silent monitor requests to monitor agents without the agent being aware of any monitoring activity. When the Unified CM-based approach is adopted for silent monitoring, the agent phone is used to mix the media streams of the agent call. The mix is then sent to the supervisor phone.

Figure 2: Unified CM-Based Silent Monitor


Supervisor
1. Agent.SuperviseCall()
7. SilentMonitorStarted
9. Call events
Supervisor Desktop
8. SilentMonitorStarted
Agent
Agent Desktop
2. Call.startMonitor()
6. Call events
Customer
3. CCM instructs supervisor's phone to call the BiB in the agent's phone
4. supervisor's phone places call to the built-in-bridge in the agent's phone
5. agent's phone forwards a mix of agent and customer's voice stream
IP
IP

Unified CM Silent Monitor Advantages

Unified CM-based silent monitor provides the following advantages:

- No NIC card restrictions.
- Any 7.x or later version of any desktop (C++, Java, .Net) can be silent monitored provided the agent is not a mobile agent.
- Silent monitor is implemented via a call, therefore, the silent monitor call is carried on the voice LAN. With CTI OS silent monitor, the silent monitor stream is carried on the data LAN.
- Silent monitor calls are reported as agent-to-agent calls for supervisors. With CTI OS silent monitor, the time the supervisor spends silent monitoring is not tracked.

Unified Communications Manager Silent Monitor Limitations and Restrictions

The following items prevent the use of Unified Communications Manager-based silent monitor:

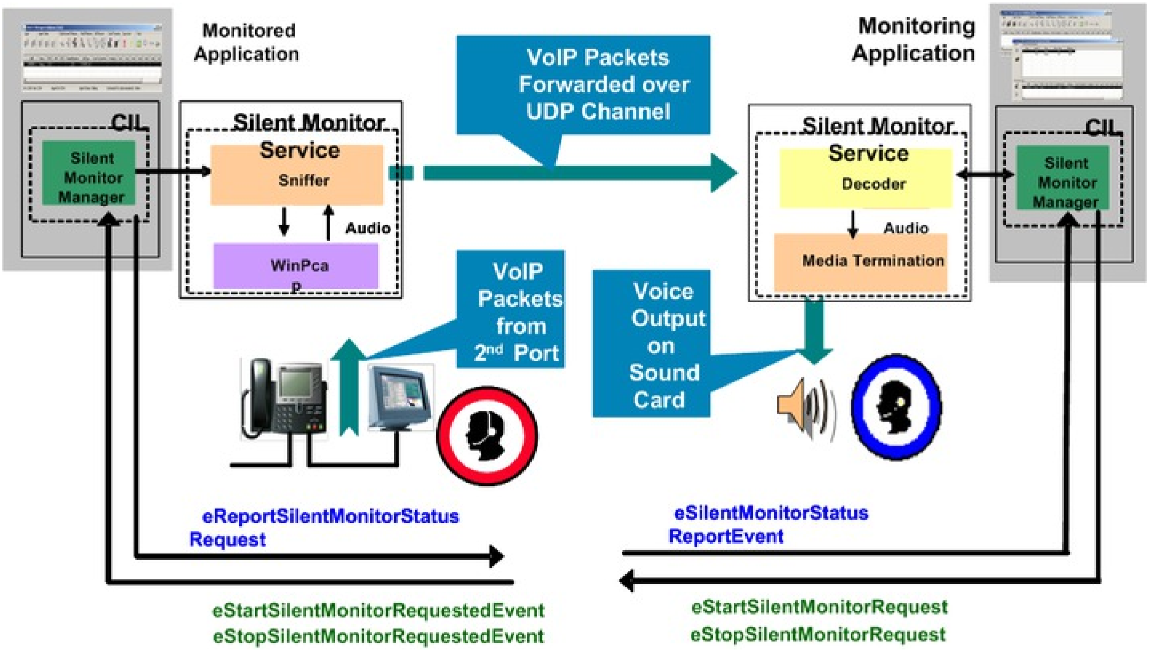
- Agents using phones without a Built-In Bridge (BIB). See the Compatibility Matrix for Unified CCEUnified CCE Solution Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for a list of supported phones.

- Silent monitoring SRTP streams is not supported
- Mobile agents cannot use this method of silent monitoring

CTI OS-Based Silent Monitoring

CTI OS-based silent monitor allows a supervisor to listen in on agent calls in UCCE call centers that use CTI OS. Supervisors can send silent monitor requests to agent desktops without the agent being aware of any monitoring activity. Voice packets sent to and received by the monitored agent's IP desk phone are captured from the network and sent to the supervisor silent monitor service connected to the supervisor desktop. At the supervisor silent monitor service, these voice packets are decoded and played on the supervisor system sound card.

Figure 3: CTI OS-Based Silent Monitor


Monitored Application
CIL
Silent Monitor Manager
Silent Monitor Service
Sniffer
Audio
WinPcap
VoIP Packets Forwarded over UDP Channel
Monitoring Application
Silent Monitor Service
Decoder
Audio
Media Termination
CIL
Silent Monitor Manager
VoIP Packets from 2nd Port
Voice Output on Sound Card
eReportSilentMonitorStatus Request
eSilentMonitorStatus ReportEvent
eStartSilentMonitorRequestedEvent
eStopSilentMonitorRequestedEvent
eStartSilentMonitorRequest
eStopSilentMonitorRequest

Note Silent monitor does not capture and translate DTMF digits that are selected on the CTI OS Agent Desktop or on agent desk phones.

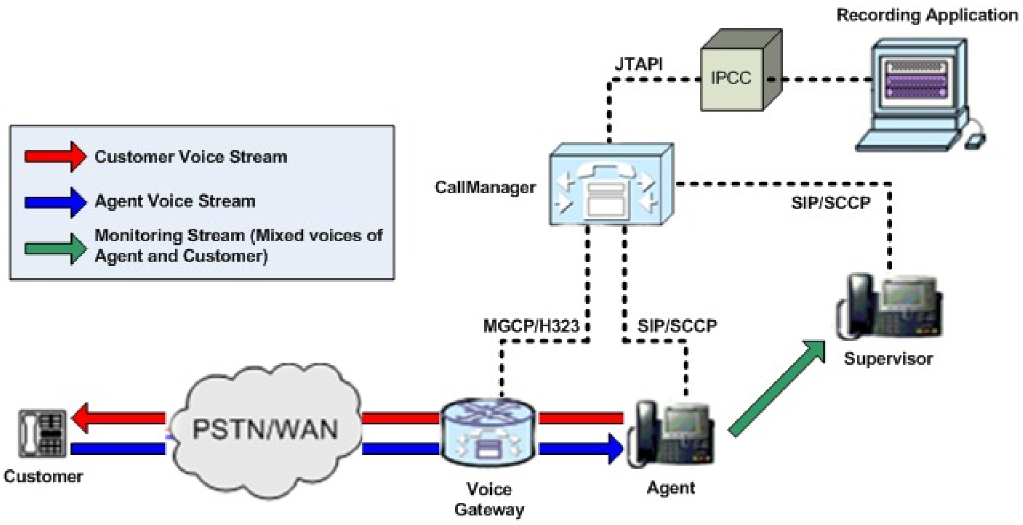
Note For the agent using the 7941, 7961, 7970, and 7971 phones, you must configure these devices on the Unified CM Administration web page with the “Span to PC Port”, “PC Voice VLAN Access” and the “PC Port” enabled. By default, the “Span to PC Port” is disabled and the “PC Voice VLAN Access” and the “PC Port” are enabled.

Network Topology for Silent Monitoring

Unified CM-Based Silent Monitoring

The following figure shows the network components and protocols involved in a Unified CM-based call monitoring session.

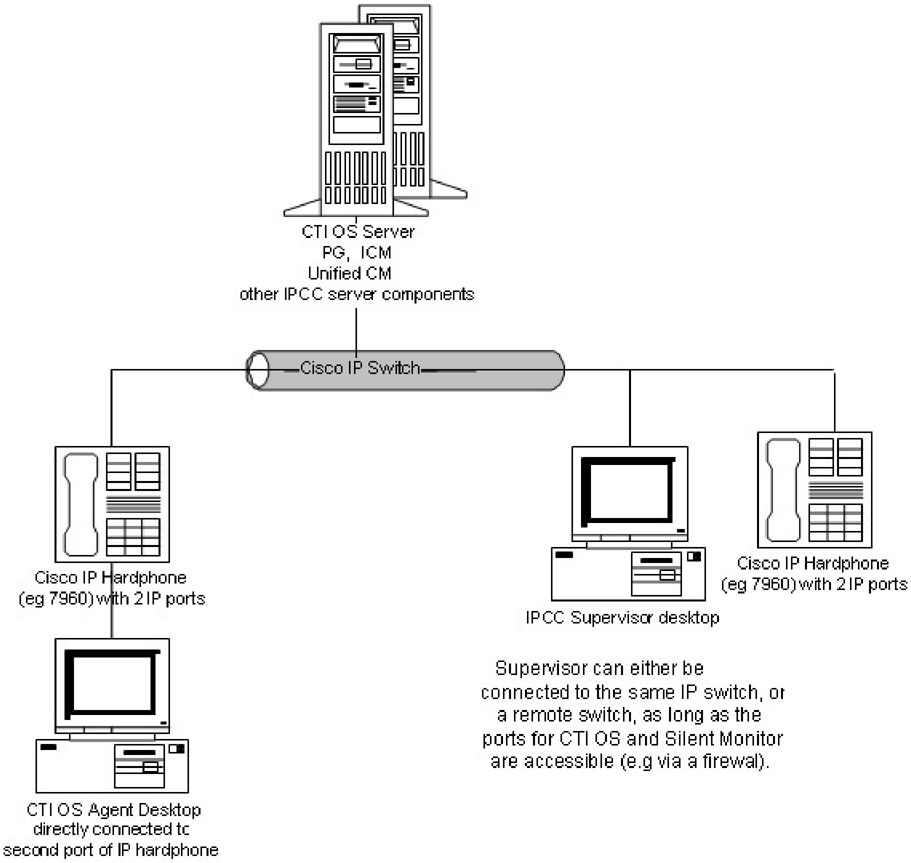
Figure 4: Unified CM-Based Silent Monitoring Network Topology



CTI OS-Based Silent Monitoring

The necessary network topology for non-mobile UCCE agents is shown in the following figure:

Figure 5: CTI OS-Based Silent Monitor Network Topology


CTI OS Server
PG, ICM
Unified CM
other IPCC server components
Cisco IP Switch
Cisco IP Hardphone (eg 7960) with 2 IP ports
CTI OS Agent Desktop directly connected tc second port of IP hardphone
IPCC Supervisor desktop
Cisco IP Hardphone (eg 7960) with 2 IP ports
Supervisor can either be connected to the same IP switch, or a remote switch, as long as the ports for CTI OS and Silent Monitor are accessible (e.g via a firewal).

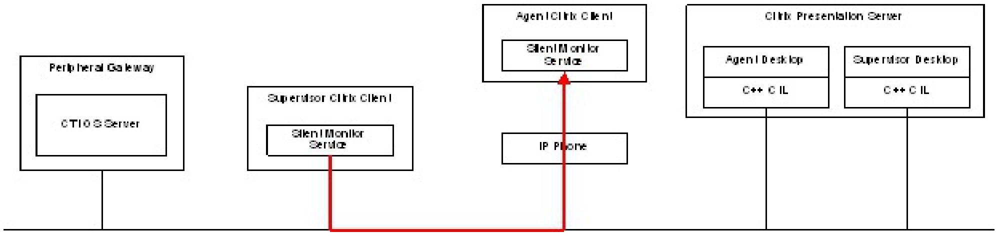
Agents in this topology may have either an IP hardphone or IP Communicator. (The supervisor in this topology must have an IP hardphone. IP Communicator is not an option.) If the agent has an IP desk phone, it must have an agent desktop PC connected to the second IP port. If the agent has IP Communicator, you must install it on the same machine as the agent desktop.

You must install a CTI OS-based desktop application that implements the CTI OS silent monitor feature on the agent desktop and supervisor desktop PCs. In addition, the components needed for an agent to be silently monitored are now automatically installed when the agent desktop is installed and those needed for a supervisor to do the silent monitoring are automatically installed when the UCCE Supervisor Desktop is installed.

Silent Monitoring and Citrix Topology

You can monitor UCCE agents using Citrix clients by installing silent monitor services on the computers running the agent and supervisor Citrix clients. You must deploy the agent Citrix client behind the agent IP phone. The supervisor Citrix client must have a sound card. The necessary network topology is as follows.

Figure 6: Silent Monitoring and Citrix Topology



Related Topics

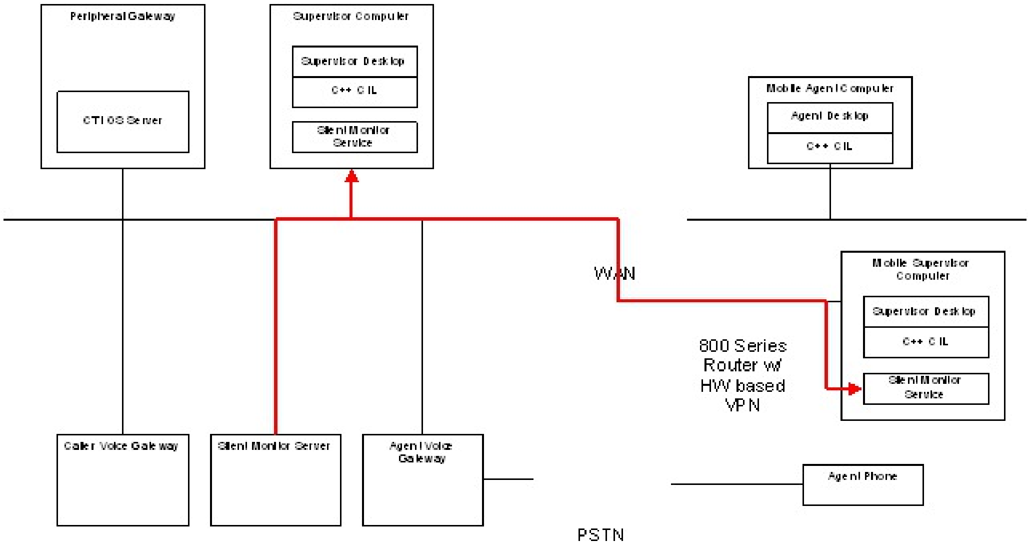
Silent monitor service deployments

Silent Monitoring and Mobile Agent Topology

You can also silently monitor mobile agents. To do this, you must manually deploy a standalone silent monitor server. This silent monitor server gains access to mobile agent voice traffic through a SPAN port that you configure to send all traffic to and from the agent gateway to the silent monitor server. The silent monitor server then filters and forwards voice traffic for the selected agent to the supervisor silent monitor server.

The necessary network topology is as follows.

Figure 7: Silent Monitoring and Mobile Agent Topology



Related Topics

Silent monitor service deployments

Calculation of Additional Needed Bandwidth

Silent monitoring of an agent consumes almost the same network bandwidth as an additional voice call. If a single agent requires bandwidth for one voice call, then the same agent being silent monitored requires bandwidth for two concurrent voice calls.

For example, assume the following:

- You have 100 concurrent agents on your network.
- Up to 20% of the agents are monitored at any given time.

In this case, plan for network capacity for 100 + (20% of 100) concurrent calls, or 120 concurrent calls.

To calculate the total network bandwidth required for your call load, you would then multiply this number of calls by the per-call bandwidth figure for your particular codec and network protocol.

For example, the table on the Cisco Voice Over IP-Per Call Bandwidth Consumption website lists the per-call bandwidth on the G.711 codec (for a call with the default voice payload size) over Ethernet as 87.2 Kbps. You multiply this 87.2 Kbps by 120 calls to obtain the total required network bandwidth.

For more information about per-call bandwidths for various codecs and network protocols, see the Cisco Voice Over IP-Per Call Bandwidth Consumption website at

http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html.

For more information about calculating bandwidth, see the Cisco Voice Codec Bandwidth Calculator at http://tools.cisco.com/Support/VBC/jsp/Codec_Calc1.jsp.