Cisco CAD Installation Guide

CAD 6.4 for Cisco Unified Contact Center Express Release 5.0
Cisco Unified Communication Manager Express Edition
December 2007

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

Customer Order Number:
Text Part Number: 6.4

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco CAD Installation Guide

Revision History

Revision Date	Description
May 2007	First Customer Ship (FCS) version 6.4(1)
December 2007	FCS version 6.4(2)

Revision History

Contents

Contents

Contents

Introduction

1

Overview

This manual guides you through the process of installing the CAD client applications: Cisco Agent Desktop, Cisco Supervisor Desktop, and Cisco Desktop Administrator.

The CAD services are integrated into the Cisco Unified Contact Center Express (CCX) installation program. See the Cisco Customer Response Solutions Installation Guide for information on installing Cisco Unified CCX.

After you have successfully installed the CAD desktop applications into a properly-configured Cisco Unified CCX environment and licensed the applications, the basic functionality of Cisco Agent Desktop, Cisco Supervisor Desktop, and Cisco Desktop Administrator are ready to use with no further configuration required.Related Documentation

What's New In This Release

CAD 6.4(1) includes the following new features:

- Support for Windows 2003 Server
- Support for Cisco Unified Communications Manager Express (CME)
- Support for wrap-up data
- Support for MSI-based installations, which enable non-administrative users to install CAD desktop applications in a context with elevated privileges

CAD 6.4(2) includes the following new features:

- Support for Microsoft Vista Business and Ultimate Editions
- Standard Bundle no longer includes Cisco Agent Desktop (available now only in the Enhanced and Premium bundles)

- New utility (the NIC Qualification Tool) that tests if a NIC is compatible with CAD desktop monitoring requirements

CAD 6.4 Elements

CAD 6.4 includes the following client applications and services.

Client Applications

Cisco Desktop Administrator

Cisco Desktop Administrator provides centralized administration tools to configure the Cisco desktop applications. It supports multiple administrators, each able to configure the same data (although not all at the same time; only one person can work in one node at any one time to ensure data integrity).

See the *Cisco Desktop Administrator User Guide* for more information.

Cisco Agent Desktop

Cisco Agent Desktop is an application that helps agents manage their customer contacts. It includes enterprise data, call activity information, reports, a chat client for chatting with other agents and supervisors, and an integrated browser window.

The agent must use a hard IP phone or the Cisco IP Communicator soft phone with Cisco Agent Desktop.

Cisco Agent Desktop controls the telephony activities on the agent's CCX phone line. CAD cannot coexist with other applications, such as Cisco Attendant Console and Cisco Unified Personal Communicator, that attempt to share or control the agent's CCX phone line.

See the *Cisco Agent Desktop User Guide* for more information.

Cisco IP Phone Agent

Cisco IP Phone Agent is a service that runs on the agent’s Cisco IP phone. It enables agents to manage their customer contacts without the need of a computer. It includes enterprise data, agent states, reason codes, and skill statistics.

See the *Cisco IP Phone Agent User Guide* for more information.

Cisco Supervisor Desktop

Cisco Supervisor Desktop allows contact center supervisors to manage agent teams in real time. They can observe, coach, and view agent status details, as well as view conference information. Without the caller’s knowledge, supervisors can initiate chat sessions with agents to help them handle calls. They can also silently monitor and record customer calls. Through the Supervisor Record Viewer, supervisors can play back and save recorded agent calls.

See the *Cisco Supervisor Desktop User Guide* for more information.

Services

The following are the individual CAD services that are installed on the Cisco Unified CCX server as part of the Cisco Unified CCX installation.

The group of services referred to as the “CAD Base services”, which are always installed on the Cisco Unified CCX server, include the following:

- Chat service
- Directory Services
- Enterprise service
- IP Phone Agent service
- LDAP Monitor service
- Licensing & Resource Manager service
- Recording & Statistics serve
- Sync service

Chat Service

The Chat service acts as a message broker between the Chat clients and Supervisor Desktop. It is in constant communication with all agent and supervisor desktops.

Agents’ desktops inform the Chat service of all call activity. The service, in turn, sends this information to all appropriate supervisors. It also facilitates the sending of text chat and team performance messages between agents (excluding IP Phone agents) and supervisors.

Directory Services

All other Cisco Desktop services register with Directory Services at startup. Clients use Directory Services to determine how to connect to the other services.

The majority of the agent, supervisor, team, and skill information is kept in Directory Services. Most of this information is imported from Cisco Unified CCX and kept synchronized by the Sync (Synchronization) service.

Enterprise Service

The Enterprise service tracks calls in the system. It is used to attach IVR-collected data to a call in order to make it available at the agent desktop. It also provides real-time call history.

IP Phone Agent Service

The IP Phone Agent (IPPA) service enables IP phone agents to log in and out of Unified CCX, change agent states, and enter reason codes and wrap-up data without having the Agent Desktop software.

This service works in conjunction with the Services feature of Unified CM and supported Cisco IP phones.

LDAP Monitor Service

The LDAP Monitor service starts Directory Services and then monitors it to ensure that it keeps running. It also sets up the configuration for LDAP replication, and resynchronizes LDAP data.

Licensing & Resource Manager Service

The License & Resource Manager (LRM) service distributes licenses to clients and oversees the health of the CAD services. In the event of a service failure, it initiates the failover process.

Recording & Playback Service

The Recording & Playback service extends the capabilities of the VoIP Monitor service by allowing supervisors and agents to record and play back calls.

Recording & Statistics Service

The Recording & Statistics service maintains a 1-day history of agent and team statistics, such as average time an agent is in a particular agent state, last login time, number of calls an agent has received. It maintains a rolling 7-day history of recordings (unless they are saved, in which case they are saved for 30 days).

Sync Service

The Sync service connects to Unified CC Express via ACMI and retrieves agent, supervisor, team, and skill information. It then compares the information with the information in Directory Services and adds, updates, or deletes entries as needed to stay consistent with the Unified CC Express configuration.

Voice-Over IP Monitor Service

The Voice-Over IP (VoIP) Monitor service enables supervisors to silently monitor agents. The service accomplishes this by “sniffing” network traffic for voice packets.

Multiple VoIP Monitor services can be installed in one logical contact center to ensure there is enough capacity to handle the number of agents.

CAD Feature Levels

There are three feature levels of CAD: Standard, Enhanced, and Premium. The following chart outlines the features available at each level. All features not listed here are present in all three levels.

Table 1. CAD Feature Levels

	Standard	**Enhanced**	**Premium**
Cisco Agent Desktop (not available in Standard bundle)			
Task buttons		×	×
Event-triggered work flows		×	×
Enterprise data thresholds		×	×
Integrated browser			×
Reason codes		×	×
Wrap-up data		×	×
Agent-initiated chat		×	×
Automated recording (part of a work flow)		×	×
Cisco IP Phone Agent			
Agent-initiated recording		×	×
Caller data	×	×	×
Reason codes	×	×	×
Contact service queue statistics	×	×	×
Work agent state		×	×
Wrap-up data		×	×
Cisco Supervisor Desktop			
Silent monitoring		×	×
Recording (up to 32 simultaneous recordings/playbacks)		×	×
Team Messages	×	×	×

Table 1. CAD Feature Levels — *Continued*

	Standard	Enhanced	Premium
CSQ statistics	×	×	×
Reports	×	×	×
Cisco Desktop Administrator			
Configure CAD interface		×	×
Configure work flows		×	×
Configure integrated browser			×
Agent work flow HTTP Post/Get Action			×
Wrap-up data		×	×

Localization

In CAD 6.4, the CAD desktop applications are localized in the languages displayed in Table 2.

Table 2. CAD applications and supported languages.

Language	CAD	CSD	IPPA	CDA
Chinese (Simplified)	×	×		
Chinese (Traditional)	×	×		
Danish	×	×	×	
Dutch	×	×	×	
English (US)	×	×	×	×
French	×	×	×	
German	×	×	×	
Italian	×	×	×	
Japanese	×	×	×*	
Korean	×	×		
Portuguese (Brazilian)	×	×	×	
Spanish	×	×	×	
Swedish	×	×	×	

* IP Phone Agent does not support Japanese if it is running on a SIP phone. Reason codes and wrap-up data must be Katakana half-width in Shift-JIS format. Kanji will not display properly.

Before You Install CAD 6.4

2

System Configurations

Supported system configurations are documented in the *Cisco Unified Contact Center Express Solution Reference Network Design (SRND)*, available for download on www.cisco.com.

Citrix and Microsoft Terminal Services Environments

CAD is supported in Citrix and Microsoft Terminal Services environments. See the document, *Integrating CAD Into a Citrix MetaFrame Presentation Server or Microsoft Terminal Services Environment*, included in the CAD documentation on your installation CD.

System Requirements

CAD 6.4 is integrated into the following environment:

	CAD 6.4(1)	CAD 6.4(2)
Unified CCX	5.0(1)	5.0(2)
Unified Communications Manager Express	4.2(1)	4.2(1)

Consult the *Cisco Unified Communications Manager Compatibility Matrix* for the appropriate versions of other Cisco applications required in your contact center environment. The compatibility matrix is located at:

www.cisco.com/en/US/products/sw/voicesw/ps4625/prod_installation_guide09186a00805acf50.html

Operating Environment

CAD 6.4 runs on the following minimum operating systems and hardware.

Table 1. Desktop application minimum operating systems and hardware

Operating System	Hardware
Windows 2000 Professional Service Pack 4	500 MHz processor 128 MB RAM 650 MB free space 100 Mbit NIC supporting Ethernet 2 800 ×600 screen resolution
Windows XP Professional Service Pack 1 and 2	500 MHz processor 128 MB RAM 650 MB free space 100 Mbit NIC supporting Ethernet 2 800 ×600 screen resolution
CAD 6.4(2) Only Windows Vista Business or Ultimate Edition	800 MHz processor 512 MB RAM 650 MB free space 100 Mbit NIC supporting Ethernet 2 800 ×600 screen resolution
Citrix MetaFrame Presentation Server 3.0 and 4.0, full window mode	Refer to Citrix documentation for minimum hardware requirements
Microsoft Terminal Server for Windows 2003	Refer to Microsoft Terminal Server documentation for minimum hardware requirements

Table 2. Server minimum operating systems and hardware

Operating System	Hardware
Windows 2003 Server	2.8 GHz processor 2 GB RAM 1 GB free space 100 Mbit NIC supporting Ethernet 2

Operating Environment Language Requirements

The CAD services must be installed on machines running an English language operating system.

Cisco Agent Desktop and Cisco Supervisor Desktop can be installed on machines running localized operating systems. For a list of supported languages, see "Localization" on page 16.

Cisco Desktop Administrator is always installed on the Unified CCX server, which runs an English language operating system. However, in a non-English language environment, it is necessary to run a second instance of Cisco Desktop Administrator on a machine with a localized operating system so that chat messages, tooltips, enterprise data names, and other communications within the contact center are in the local language.

A site cannot support more than one localized language. All agents and supervisors must use the same language—there cannot be some agents and supervisors using one language and other agents and supervisors using another language.

NAT and VPN Requirements

The use of network address translation (NAT) with firewalls or routers is supported for the CAD client desktops. It is not supported for CAD services servers.

The CAD client desktops must use virtual private network (VPN) software to ensure full bi-directional network connectivity between the contact center servers and the desktop. Failure to use VPN software will result in conectivity issues and a loss in functionality. Also, using a VPN is recommended in order to provide a more secure connection.

It has been verified that Cisco VPN 3000 Concentrator and Cisco VPN Client work properly with CAD client desktops, and are supported for access. VPN solutions from other vendors may work correctly, but since they have not been formally verified, they are not supported. If you want an alternative solution to be verified, please contact your Cisco distributor.

Using NAT With IP Phone Agent

NAT is supported with IP Phone Agent. However, it is required that you use static IP addresses for the IP Phone Agent phones as well as Static NAT. Dynamic NAT and address overloading are not supported.

Recording and monitoring do not work with IP Phone Agent when it is used with NAT.

For more information on NAT, see *How NAT Works* (Cisco document ID 6450), located at:

http://www.cisco.com/warp/public/556/nat-cisco.shtml

Third Party Software Environment

CAD 6.4 requires the following software applications to run successfully:

Table 3. Third party software requirements

Application	Where Installed/Description
Apache Tomcat 5.5	Cisco Unified CCX server Tomcat is a Java-based webserver. If you are installing IP Phone Agent, it is needed to work with the XML pages displayed by IP phones. More information about Tomcat can be found at http://jakarta.apache.org. Tomcat is shipped with CAD 6.3 and is automatically installed.
Microsoft Internet Explorer 6 or 7	Client desktops Internet Explorer is required for the integrated browser portion of Cisco Agent Desktop and Cisco Supervisor Desktop/ The integrated browser makes use of a Windows OS library distributed with the Microsoft IDEs that supports the rendering of HTML.
Java Runtime Environment (JRE) 1.5.0_11	Cisco Unified CCX server JRE is required to run the Java applets and JavaServer pages (JSP) used by Cisco IP Phone Agent. JRE is shipped with CAD 6.3. It is installed automatically with the CAD services.

Monitoring Requirements

All Monitoring

CAD supports the G.711 and G.729 codecs. Silent monitoring and recording will not function correctly if IP phones use any other codec.

Consult the Cisco Unified CM documentation for information on changing a phone device's codec.

Desktop Monitoring

The use of desktop monitoring in your contact center increases bandwidth requirements. Consult the best practices document, *Cisco Agent Desktop Bandwidth Requirements*, for more information.

Required Device Settings for Desktop Monitoring

The following device settings are required for desktop monitoring to function correctly with CAD. The settings are configured with the Cisco Unified CM Administration application.

> NOTE: Not all devices or Unified CM versions use all these settings. Configure those that do appear for your device and Unified CM version.

> NOTE: CAD does not support Secure Realtime Transport Protocol (SRTP) in desktop monitoring.

In the Product Specific Configuration section of the Device Configuration page, configure these settings as follows:

- 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 page, configure this setting as follows:

- 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.

Qualifying NICs for Desktop Monitoring

Desktop monitoring does not function with some NICs. The Intel PRO/100 and PRO/1000 NIC series are unable to detect both voice packets and data packets in a multiple VLAN environment, which prevents desktop monitoring from functioning properly. These NICs do not fully support NDIS Promiscuous Mode settings.

A list of NICs tested with Cisco Agent Desktop is located on the Cisco website at:

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

A workaround solution for the problems with the Intel PRO/100 and PRO/1000 NICs is available from the Intel Technical Support website (Solution ID: CS-005897). Other solutions include:

- Monitoring agents via a VoIP Monitor service
- Using another type of NIC that is fully NDIS-compliant

The workaround described in CS-005897 might not work for some newer Intel PRO/100 and Intel PRO/1000 cards and drivers.

If the workaround does not solve the problem, the VLAN ID of the IP phone to which the agent computer is directly connected must be added to the VLANs tab of the Intel NIC’s Network Connection Properties dialog box.

The IP phone’s VLAN ID can be obtained from the phone’s Network Configuration screen (press **Settings** and then choose **Network Configuration**). See the documentation specific to your version of Cisco Unified Communications Manager and IP phone model for more information.

You can test a NIC to verify that it is suitable for desktop monitoring by following the procedure, “Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring” (Document ID 46301). This document is located on the Cisco website at:

> http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/products_tech_note09186a00801f42f9.shtml

A sample packet capture file used in this procedure is located at:

> http://www.cisco.com/cgi-bin/tablebuild.pl/nic-qual

NIC Qualification Tool for CAD 6.4(2)

A utility called the NIC Qualification Tool (NICQ) is included with CAD 6.4(2) installations of the VoIP Monitor service and Cisco Agent Desktop (on agent PCs).

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

NICQ performs three major tasks:

- Tests the NICs on agent PCs and the server hosting the VoIP Monitor service to verify whether the machine supports FTP packet sniffing used to perform silent monitoring and recording
- Tests agent PCs and the server hosting the VoIP Monitor service as part of troubleshooting to determine why monitoring/recording is not working properly
- Gather information about NICs that are qualified in order to create an accurate list of NICs that will work with CAD

Complete instructions for using NICQ are in the *Cisco CAD Service Information* manual.

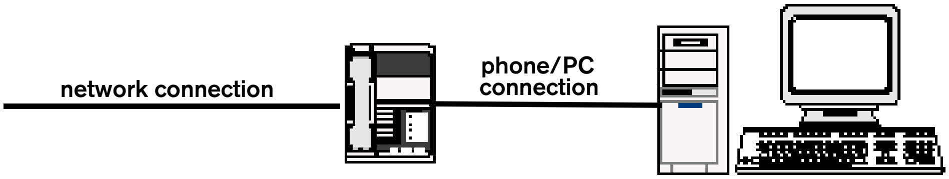
Desktop Monitoring Hardware Setup

For desktop monitoring to function, the phone is connected to the network, and the agent PC is daisy-chained to the phone (see Figure 1).

> NOTE: Desktop monitoring of multiple phones daisy-chained to the agent PC is not supported.

> NOTE: An agent should log into CAD using the extension of the phone daisy-chained to the agent PC for desktop monitoring to function.

Figure 1. Desktop monitoring hardware setup



Server Monitoring

The following device setting is required for server monitoring to function correctly with CAD. The setting is configured with the Cisco Unified Communications Manager Administration application.

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: CAD does not support Secure Realtime Transport Protocol (SRTP) in server monitoring.

Recording Requirements

NOTE: The CAD recording functionality is intended for “on demand” use only, and not for recording all calls in the contact center.

The space requirements for the Recording & Playback service and the Recording & Statistics service depend on the size of the contact center. In general, requirements are as follows:

Agent Data Store Database

The Agent Data Store database (the MSDE database associated with the Recording & Statistics service) requires 1.2 GB to store agent state and call activity records for a 7 days per week/10 hours per day, with calls that last 1 minute each. This assumes that the contact center has the maximum configuration of:

- CAD 6.4(1): 150 agents and 32 simultaneous recordings
- CAD 6.4(2): 300 agents and 64 simultaneous recordings

Recording & Playback Service

The Recording & Playback service requires the following space.

- ~800 kB for each minute of a recorded G.711 voice call
- ~200 kB for each minute of a recorded G.729 voice call
- 2.6 GB to store voice calls assuming that there are 32 supervisors, each supervisor recording 10 G.711 calls per day, each call lasting 5 minutes. This space requirement is divided over all Recording & Playback server, because they balance the recording load.

If the audio files are stored on a partition using the FAT32 file system, a limit of 21,844 objects can be stored. If this recording limit is exceeded, supervisors will be unable to record any more audio files. There is no such limitation on an NTFS file system partition.

Setting Up Agents in Cisco Unified CCX

For CAD 6.4 applications to work properly, your agents must be organized into teams and some must be designated as supervisors. This is accomplished in Cisco Unified CCX. See your Cisco Unified CCX documentation for information on how to do this.

System Capacity

CAD 6.4 supports the system capacities displayed in Table 4.

Table 4. Unified CME system capacity.

Description	6.4(1)	6.4(2)
Maximum number of agents per site	50	50
Maximum number of agents per team	50	50
Maximum number of skills per agent (for real-time reporting)	50	50
Maximum number of CSQs per agent (for real time reporting)	25	25
Maximum number of supervisors per site	10	10
Maximum number of supervisors per team	10	10
Maximum number of simultaneous recordings/playbacks per Recording & Playback service	32	16

Supported IP Phones

For a list of supported IP phones, see the *Cisco Customer Response Solutions (CRS) Software and Hardware Compatibility Guide*. This document is available on the web at

http://www.cisco.com/application/pdf/en/us/guest/products/ps1846/c1683/ccmigration_09186a008086dfe9.pdf

Caveats on Using a Cisco 7920 Wireless Phone

Only SPAN port monitoring can be used with the 7920 wireless IP phone. The port that is to be included in the SPAN is the one to which the access point is wired.

Due to the nature the 7920 phone's mobility, there are certain conditions under which monitoring and/or recording calls may result in gaps in the voice:

- Agent to agent conversations when both agents are using the same wireless access point
- When an agent roams from one monitoring domain to another

The 7920 phone is not supported as a second line appearance for an agent's wired phone.

1.

Installation

3

Important Notice for Standard Bundle Customers

It is important to remember that if you are upgrading from CAD 6.4(1) to CAD 6.4(2), the 6.4(2) Standard bundle does not support Cisco Agent Desktop. It supports IP Phone Agent only. Please contact your Cisco or Cisco partner account team for further details on how to obtain Cisco Agent Desktop.

Overview

In a typical configuration, all CAD services and Cisco Desktop Administrator are installed on the Cisco Unified CCX server before the desktop applications are installed.

> NOTE: After you install the CAD services on the Unified CCX server, do not change the name of that server. If you do change the computer's name, various required databases and licensing will no longer function correctly. To correct this problem, change the server's name back to the original name and functionality will be restored.

This chapter describes the procedure for installing Cisco Supervisor Desktop and Cisco Agent Desktop, and the procedure for installing a second instance of Cisco Desktop Administrator.

Client Installation Failure

If the installation program for any CAD client application will not run, and you receive the error message, "This installation is not fully configured. See product documentation for properly configuring your system", it means that the installation programs are not correctly configured through CAD Configuration Setup. You must reconfigure the client installation programs.

To correct this problem, follow this procedure.

> NOTE: In a redundant configuration, you must complete this procedure on both the primary and secondary CAD Base Services servers.

To reconfigure CAD client installation programs:

1. Run CAD Configuration Setup on the Cisco Unified CCX server (see "CAD Configuration Setup Utility" on page 39 for more information).
2. From the menu, choose File > Reset Client Installs.

   This process reconfigures the client installation programs.
3. When the process is complete, the message, "Client installs reset" is displayed. Click OK to close the message.

   You can now install the client applications.

Installing CAD Desktop Applications

Before you install Cisco Agent Desktop, you need to know:

- The IP address of the Unified CCX server
- The user ID and password to access the Customer Response Solutions Administration web application
- The destination folder on the user's PC in which you will install the application

Installation Procedure

The CAD desktop applications can be installed either of two ways:

- The desktop applications can be "pushed" to the agent desktops using an automated package distribution tool
- The agent can install the application from the Customer Response Solutions Administration web application

The desktop user must have either administrator or elevated privileges to install the CAD desktop applications. This applies to installations pushed to the desktop via an automated package distribution tool or manual installation.

When you install CSD, it automatically installs CAD as well on the desktop. If you already have CAD installed on a desktop and want to install CSD, you must first uninstall the existing instance of CAD.

Installing a CAD Desktop Application

The CRS Administrator download page includes installation files for all CAD desktop applications. The CRS Administrator web page, when accessed using a supervisor username and password, contains only the installation file for CSD. The CRS User web page contains only the installation file for CAD.

If you do not want agents and supervisors to access the CRS Administration web application as administrators, direct them to one of the alternatives given in the following procedure.

To install a CAD desktop application:

1. Open your web browser and access the appropriate Unified CCX application. Use the IP address or hostname of the Cisco Unified CCX server in the URLs listed below.
    - If you are an administrator, complete the following steps.
        a. Access http://<Cisco Unified CCX server>/appadmin.

           The CRS Administration Authentication page appears.

        b. At the prompt, enter your username and password, then click Log On.

The CRS Administration home page appears.

c. From the **Tools** menu, choose **Plug-ins.**

d. On the Plug-ins page, click **Cisco Unified CCX.**

- If you are a supervisor, complete the following steps.

  a. Access http://<Cisco Unified CCX server>/appadmin.

  The CRS Administration Authentication page appears.

  b. At the prompt, enter your Cisco Supervisor Desktop username and password, and then click **Log On.**

  The CRS Supervision home page appears.

  c. From the **Tools** menu, chose **Plug-ins.**

  d. On the Plug-ins page, click **Unified CCX.**

- If you are an agent, complete the following steps.

  a. Access http://<Cisco Unified CCX server>/appuser.

  The CRS User Authentication page appears.

  b. At the prompt, enter your Cisco Agent Desktop username and password, and then click **Log On.**

  The Download page appears.

2. Click the link for the application you want to install.

   The File Download - Security Warning dialog box appears.

3. Click **Run** to run the installation program.

4. You might see a security warning that the publisher could not be verified. Click **Run** to run the installation program.

   You can also save the installation file to your local computer and run it from there.

   The InstallShield Wizard starts. Follow the instructions in the wizard to install the selected application.

Using Automated Package Distribution Tools

CAD's MSI-based desktop application installations can be deployed ("pushed") via automated package distribution tools that make use of the Microsoft Windows Installer service.

Requirements

CAD support for automated package distribution depends on compliance with the requirements listed below.

Execution

Installations must be executed on the target machine. Deployment methods that capture a snapshot of an installation and redistribute that image are not supported.

Per-Machine vs. Per-User Installation

Installations must be deployed on a per-machine basis. Per-user installations are not supported.

It might be necessary to ensure per-machine installation via command line.

Privileges

CAD installations require either administrative or elevated privileges.

By default, Windows Installer installations run in the context of the logged-on user.

If the installation is run in the context of an administrative account, there is no need to enable policies to grant elevated privileges.

If the installation is run in the context of an account with reduced privileges, then it must be deployed with elevated privileges. The target machine must have the Windows policy "Always Install with Elevated Privileges" enabled for both the User Configuration and the Computer Configuration. When this policy is enabled, Windows Installer installations will run in a context with elevated privileges, thus allowing the installation to successfully complete complex tasks that require a privilege level beyond that of the logged-on user.

Automated Package Installation vs. Manual Installation

Automated installations must use the same files and meet the same installation criteria as manually-deployed installations.

CAD MSI packages are located in a specified location (C:\Program Files\wfavvid\tomcat_appadmin\webapps\TUP\CAD) on a successfully-installed production server and are intended for both manual and automated deployment.

Alteration of these files or the use of other MSI files included with the product at other locations is not supported.

Installation criteria such as supported operating systems, product deployment configurations, installation order, and server/client version synchronization must be met. Altering the supplied MSI packages to circumvent the installation criteria is not supported.

Multiple Software Releases

Multiple software releases must not be combined into a single deployment package. Each CAD software release is intended for distribution in its entirety as a distinct deployment. Combining multiple releases (for example, a software package's base release and a subsequent service release) into a single deployment package is not supported.

Reboots

Any reboots associated with CAD installations are required. If the installation’s default reboot behavior is suppressed, the target machine must be rebooted before running the installed applications to ensure expected functionality.

Delaying a reboot is not know to be an issue at this time, as long as a reboot occurs before launching the installed applications. If it is determined in the future that delaying a reboot via command line suppression affects expected behavior, then that delayed reboot will not be supported.

Best Practices

Best practices recommendations are listed below.

Windows Installer Logging

Window Installer logging should be enabled. The installations should be run with the following command line argument:

```
/l*v <logfile path and name>
```

NOTE: The logfile path and name must be a location to which the installation’s user context has permission to write.

This ensures that any loggable issues are captured efficiently.

Deployment

Each installation package should be deployed using its own deployment package. Using separate packages offers faster isolation of potential issues than does a composite deployment package.

Installation and Uninstallation Deployment Packages

The deployment engineer should create and test both an installation and uninstallation deployment package.

This is especially important for service release installations, which must be uninstalled before upgrading the underlying software.

Recommended Deployment Preparation Model

1. Use a lab environment to model the pending deployment.
2. Install the servers to obtain valid client installation packages.
3. Manually deploy client installation packages to ensure that the installs are compatible with your environment. This will isolate product installation vs. automated deployment issues.
4. Create your deployment packages in accordance with the requirements listed in "Requirements" on page 35.
5. Test the deployment packages.
6. At deployment time modify your deployment packages, replacing the client installation packages from the lab environment with valid client installation packages from the production server.

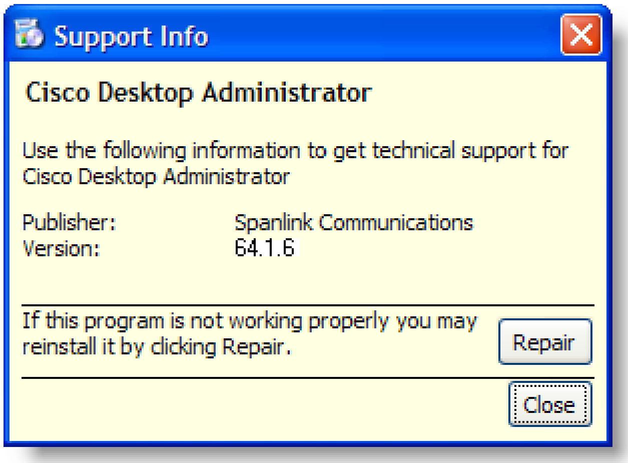
Repairing CAD

If one of the CAD client or server applications is not functioning properly, you can use the Repair function to reinstall it. If you do repair a CAD application, you must also repair any service release that has been installed.

To repair a CAD client or server application:

1. In Windows Control Panel, start the Add or Remove Programs tool.
2. In the list of currently installed programs, locate the CAD application you want to repair.
   - CAD client applications are repaired using the listing for the specific application (for example, “Cisco Desktop Administrator”).
   - CAD server applications are repaired using the listing for Cisco Unified CCX.
3. Click the **Click here for support information** link to display the Support Info dialog box (see Figure 2).

Figure 2. Support Info dialog box.



Cisco Desktop Administrator

Use the following information to get technical support for Cisco Desktop Administrator

Publisher: Spanlink Communications
Version: 6.4.1.6

If this program is not working properly you may reinstall it by clicking Repair.

4. Click **Repair.** The program will be reinstalled.
5. Repeat Steps 2 though 4 on the CAD service release, if one has been installed.

CAD Configuration Setup Utility

You can use the Cisco Agent Desktop Configuration Setup utility to configure the CAD services.

CAD Configuration Setup runs initially as part of the Cisco Unified CCX installation process. After initial installation, you can change your configuration settings by launching it from Desktop Administrator or running PostInstall.exe (located in the ...\Program Files\Cisco\Desktop\bin folder on any CAD computer).

CAD Configuration Setup displays different step windows depending on which host computer it runs on. Table 5 shows which step windows appear when CAD Configuration Setup is run on a specific host computer. Refer to this table to determine where you should run Configuration Setup to change the desired configuration setting.

> NOTE: If you run CAD Configuration Setup on a computer that hosts only Desktop Administrator, and no other CAD application or service, you will receive a message that there is nothing to configure on that computer. Run CAD Configuration Setup on another computer that hosts CAD services or applications.

Table 5. CAD Configuration Setup windows displayed per host computer

Step Name	Base[1]	VoIP	Rec	CAD CSD	CDA
VoIP Network Device Step (page 41)	×	×		×	
Services IP Address Step (page 42)	×	×	×		
Terminal Services Step (page 43)				×	

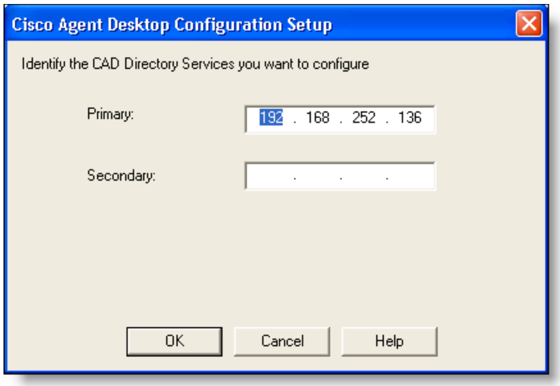
[1] Header key: Base—Base services; VoIP—VoIP Monitor service: Rec—Recording service: CAD CSD—Cisco Agent Desktop, Cisco Supervisor Desktop—CDA: Cisco Desktop Administrator

To modify configuration data:

1. Start CAD Configuration Setup.
   - In Desktop Administrator, select the Call Center 1 node in the left pane and then choose **Setup > Configure Systems** from the menu bar.
   - On another CAD host computer, navigate to the ...\Program Files\Cisco\Desktop\bin folder and double-click **PostInstall.exe.**

Configuration Setup starts and displays the CAD Directory Services dialog box.

Figure 3. Cisco Agent Desktop Directory Services dialog box.



Cisco Agent Desktop Configuration Setup

Identify the CAD Directory Services you want to configure

Primary: 192 . 168 . 252 . 136

Secondary: . . .

2. Ensure that the correct primary (and optional secondary) Directory Services IP addresses are entered, and then click **OK.**

   The Cisco Agent Desktop Configuration Setup utility is displayed, with the CallManager node selected.

   NOTE: You can press F6 to switch between the left and right pane, and the up and down arrows to move up and down the navigation tree in the left pane.

3. Select the step window you want to modify from the left pane, enter the new data in the right pane, and then click **Apply.**

   - You can display the step windows in any order you wish.
   - If you modify something in a step window, you must click **Apply** to save your changes before you move on to another window.

4. When you are done making your changes, choose **File > Exit** from the menu or click **Close.**

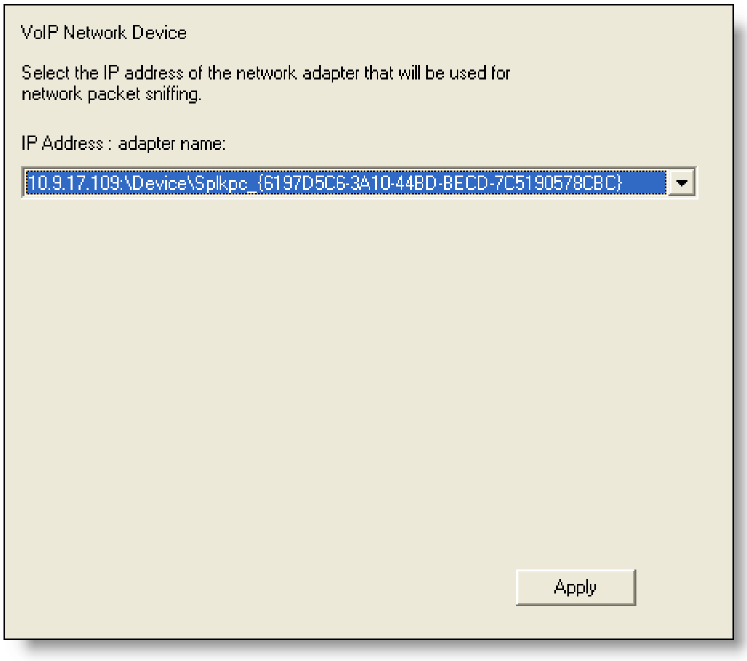
   CAD Configuration Setup closes.

5. Stop and restart the modified service and all desktops for the change to go into effect.

Configuration Setup Step Windows

VoIP Network Device Step

Figure 4. VoIP Network Device step.



VoIP Network Device

Select the IP address of the network adapter that will be used for network packet sniffing.

IP Address : adapter name:

10.9.17.109:\Device\Splkpc_{6197D5C6-3A10-44BD-BECD-7C5190578CBC}

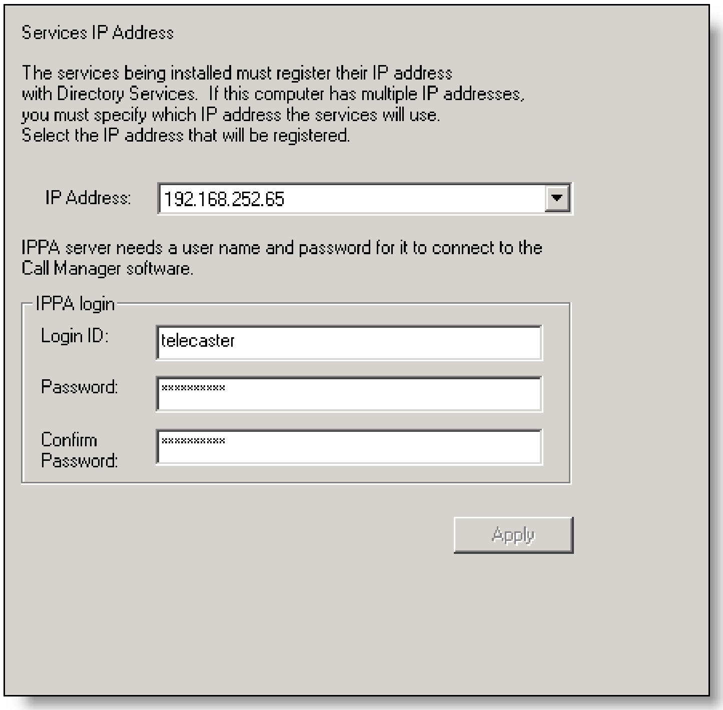
Select the IP address of the network adaptor to which voice packets are sent to be sniffed by the VoIP Monitor service (if this is a server box) or the desktop monitor (if this is a client desktop).

- On a VoIP Monitor Service server, it is the IP address of the NIC that is connected to the port configured for SPAN.
- On a client desktop computer, it is the IP address of the NIC on which the computer is daisy-chained to the phone.

NOTE: If you change these settings after initial setup, you must restart the VoIP Monitor service or the client application (depending on where you run CAD Configuration Setup) to ensure that the change is registered with them properly.

Services IP Address Step

Figure 5. Services IP Address step.



Services IP Address

The services being installed must register their IP address with Directory Services. If this computer has multiple IP addresses, you must specify which IP address the services will use. Select the IP address that will be registered.

IP Address: 192.168.252.65

IPPA server needs a user name and password for it to connect to the Call Manager software.

IPPA login

Login ID: telecaster

Password: **********

Confirm Password: **********

If the computer has more than one IP address, select the IP address of the NIC used to connect to the LAN—it must be accessible by the client desktops.

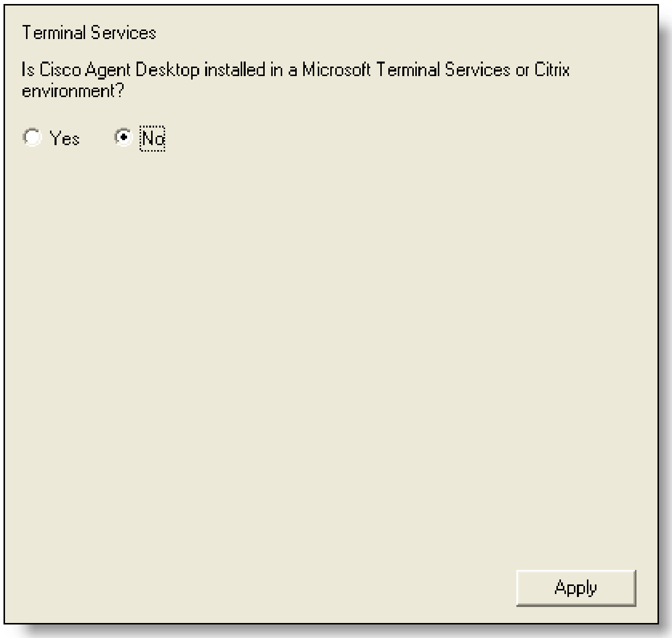
In order to connect to the Unified CM, the IPPA service must have a user ID and password. This user ID and password are also set up in Unified CM (see “Configuring Cisco Unified CM IP Phones to Work With IP Phone Agent” in the Cisco CAD Installation Guide). You can complete these fields before actually setting up the user in Unified CM, but the user ID and password must be identical in both places. If they are changed in this window or in Unified CM, they must be changed in both.

NOTE: If Directory Services is not running when you view this step, the IPPA login information cannot be changed.

NOTE: If you change these settings, you must restart all CAD services to ensure that the change is registered with them properly.

Terminal Services Step

Figure 6. Terminal Services step.



Terminal Services

Is Cisco Agent Desktop installed in a Microsoft Terminal Services or Citrix environment?

○ Yes ● No

If this installation of Cisco Agent Desktop is installed in a Microsoft Terminal Services or Citrix environment, click Yes. If not, click No.

Changing Cisco Unified CCX Cluster IP Addresses

It might become necessary to change the IP address of a server in the Cisco Unified CCX cluster. When this happens, you must update the configuration so that the new IP address is properly registered.

See the *Cisco Customer Response Solutions Administration Guide* for this procedure.

Configuring IP Phones for Use With a Localized IP Phone Agent Service

If a contact center is using a non-English language version of CAD, the IP Phone Agent service will be displayed on the agent's IP phone in that non-English language (see "Localization" on page 16 for a list of supported languages). The phone does not need to be configured for the chosen locale. However, in this situation, the IP phone itself will display in English, the default locale for the phone, while the IP Phone Agent service displays in the non-English language.

For information on configuring the IP phone itself to display in the non-English language, consult the *Cisco Unified Communications Manager Express System Administrator Guide*, available at:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html

After all IP agent phones are added to the Cisco Unified CME, you must perform the following tasks.

1. Telnet to your CME router.
2. Configure the Telephony Services URL.
3. Configure the Telephony Authentication URL.

   All phones now subscribe to the IP Phone Agent Service.

   NOTE: If there are multiple UCCX servers pointing to a single CME router, then only one UCCX server can support IP phone agents. This is due to the limitation of configuring only one telephony-services URL and telephony-Authentication URL on the CME router.

The following sample telnet log illustrates steps 2 and 3 in the procedure above. In this example, the IP address of the UCCX server is 20.1.1.252.

```
Cisco2800#conf t

Cisco2800(config)#telephony-service

Cisco2800(config-telephony)#url services
http://20.1.1.252:6293/ipphone/jsp/sciphonexml/IPAgent
Initial.jsp

Cisco2800(config-telephony)#url authentication
http://20.1.1.252:6293/ipphone/jsp/sciphonexml/IPAgent
Authenticate.jsp

Cisco2800(config-telephony)#no create cnf-file

Cisco2800(config-telephony)#create cnf-file
```

```
Cisco2800(config-telephony)#restart all
Cisco2800(config-telephony)#end
```

Removal

4

Removing CAD 6.4

To remove a CAD application:

1. From the Start menu, click Settings, then Control Panel.
2. Double-click Add/Remove Programs.
3. From the list, select the application you wish to remove and click Add/Remove.

   The application is removed.

Rolling Back Client-Side Service Releases

There are two types of service releases that can be applied to the Cisco Unified CCX server, the service release (SR) and the engineering special (ES), which is an update to an SR. Only one type, the SR, is applied to the CAD clients.

When an ES is applied to the Cisco Unified CCX server, an SR equivalent might or might not be applied to the CAD clients. As a result, the numbering of SRs on the server and on the clients can become out of step with each other.

The following chart illustrates a hypothetical series of SRs and ESs applied to a configuration.

Unified CCX Server	CAD Clients
Main Release	Main Release
SR1	SR1
ES1	SR2
ES2	SR3

If ES2 is removed from the Cisco Unified CCX server, that server reverts to the SR1 release level. (ESs are cumulative, so when ES2 is removed, so is ES1.) However, the CAD clients cannot roll back from SR3 (the equivalent to ES2 on the server) to SR1. Instead, SR3 must be removed from the CAD clients so that they revert to the main release, and then SR1 applied again.

> NOTE: If the client desktop is not rolled back to the server SR level, the user sees an error message that the client and server are running incompatible versions and will not start.

The client-side SR1 can be applied via True Update the next time the client application is started, or installed individually on each client desktop.

To roll back a CAD client-side SR:

1. Roll back the SR on the Cisco Unified CCX server to the desired SR or ES. See your Cisco Unified CCX documentation for this procedure.

   It is recommended that SRs are rolled back on the Cisco Unified CCX server first in order to avoid True Update issues.

2. On the client computers, use the Windows Add or Remove Programs utility in the Control Panel to remove the client-side SR.

The SR is removed and the client applications are rolled back to the main release version. The next time the client application is started, True Update detects that an SR is present on the Cisco Unified CCX server and automatically updates the client application to the current SR.

Appendix A: Voice-Over IP Monitor Service Installation Notes

A

The VoIP Monitor server application is used to enable the silent monitoring and recording features of CAD 6.4. It accomplishes this by monitoring (sniffing) network traffic to and from IP phones.

By default, Ethernet switches do not deliver packets to ports other than the destination port. However, Cisco Catalyst switches have a feature called Switched Port Analyzer (SPAN) which allows copying all traffic from a list of ports or VLANs to another port.

In some cases, a single VoIP Monitor server is not able to handle the traffic in an entire contact center for these reasons:

- The VoIP Monitor server cannot see or identify the voice traffic because of the way the network is configured
- A single VoIP Monitor server cannot keep up with the amount of voice traffic in the contact center

The VoIP Monitor server identifies packets by MAC address. When a request comes in to monitor or record an agent's conversation, it retrieves the MAC address of the agent's IP phone from the Cisco CallManager.

A problem arises if the VoIP Monitor server, using SPAN, is monitoring an Ethernet port that hits a router before it reaches the IP phone. In this case, the VoIP Monitor server will not associate that packet with the IP phone because it sees the router's MAC address, not the IP phone's MAC address. For this reason, the ports that SPAN is configured to monitor must be in the same layer-2 domain (VLAN/subnet) as the IP phones to ensure that the packets it sees contain the IP phone MAC addresses.

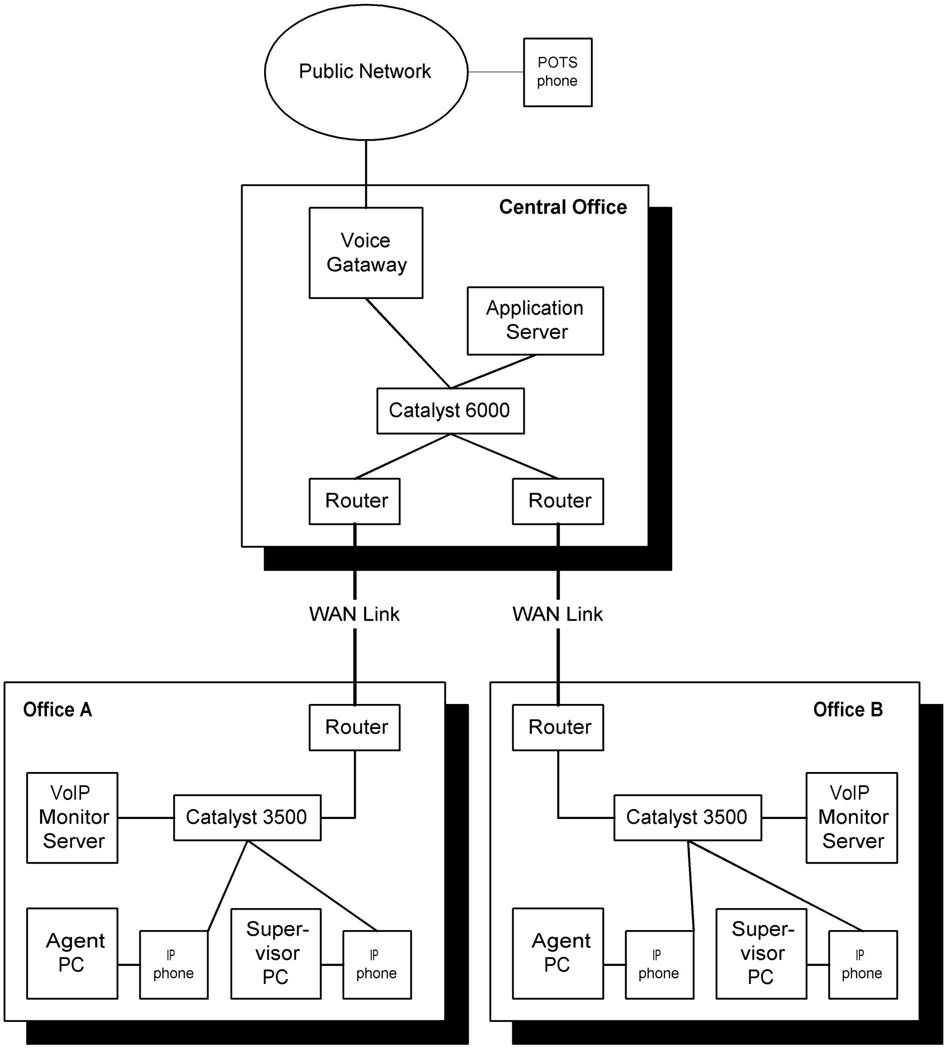
Figure 7 illustrates a situation in which more than one VoIP Monitor server is required. In this figure, a central office connects two agent offices to the voice gateway. The agent offices are separated by a WAN link.

NOTE: If you install additional VoIP Monitor servers, the Recording & Playback service must be restarted in order to recognize the additional VoIP Monitor servers added since its last restart.

A single VoIP Monitor server cannot be placed in the central office because there are routers between the central office and the agent offices. If a VoIP Monitor server were placed in the central office, it would see the MAC addresses of those routers rather than those of the IP phones it is supposed to monitor.

CAD 6.4 enables network architecture to include multiple VoIP Monitor servers in a single logical contact center. When this is done, IP phones are assigned to a specific VoIP Monitor server using Cisco Desktop Administrator.

Figure 7. System architecture that requires more than one VoIP Monitor service.



General Installation Guidelines

When setting up a network and configuring SPAN on a Catalyst switch, follow these guidelines:

- Have separate voice and data VLANs. On many switches, SPAN can be configured to monitor a VLAN. The VoIP Monitor server is only interested in voice traffic, not data, so this feature can be used to minimize the amount of extra traffic that the VoIP Monitor server will bear.
- On Catalyst 2900XL and 3500XL switches, the VoIP Monitor server and the IP phones must be in the same VLAN.
- When monitoring the entire voice VLAN on Catalyst 4000, 6000, and 6500 switches, configure SPAN to monitor only the inbound (rx) or outbound (tx) packets. Monitoring both types of packets (the default setting) can result in duplicate packets being sent to the VoIP Monitor server.

  For example, if a voice VLAN setting is 10, and the VoIP Monitor server Ethernet port is 2/20, then the Catalyst SPAN command is:

  ```
  Cat6000> (enable) set span 10 2/20 rx inpkts enable create
  ```

  (Text you enter is in bold.)

  In this example, rx specifies inbound packets only, and inpkts enable allows the VoIP Monitor server connected to this port to send and receive normal network traffic in addition to the traffic that is sent to it by SPAN. By default, this option is disabled. It must be enabled for the server to function properly.
- Catalyst switches can have varying numbers of simultaneous SPAN ports, depending on the model. For example, a 3500XL can have only one SPAN port, while a 6000 can have two SPAN ports with the inpkts enable option.

Specific Configuration Examples

Single Catalyst 3524XL

In a network configuration where:

- IP phones are on ports FastEthernet0/1 through 0/5
- VoIP Monitor server is on port FastEthernet0/10
- IP phones and VoIP Monitor server are in the same VLAN

Catalyst 3524XL SPAN commands are:

```
Cat3524XL(config)#interface FastEthernet 0/10
Cat3524XL(config-if)#port monitor FastEthernet 0/1
Cat3524XL(config-if)#port monitor FastEthernet 0/2
Cat3524XL(config-if)#port monitor FastEthernet 0/3
Cat3524XL(config-if)#port monitor FastEthernet 0/4
Cat3524XL(config-if)#port monitor FastEthernet 0/5
```

```
Cat3524XL(config-if)#exit
```

Single Catalyst 6000

In a network configuration where:

- IP phones are in VLAN 15
- VoIP Monitor server is on port 2/10

Catalyst 6000 SPAN commands are:

```
Cat6000> (enable) set span 15 2/10 rx inpkts enable create
```

Single Catalyst 6000 and Multiple Catalyst 3524XLs, with Gateway-Only Monitoring and No Agent-to-Agent Monitoring

In this configuration, the supervisors are interested only in calls going through the gateway, so that the network configuration can have a single VoIP Monitor server on the Catalyst 6000. Silent monitoring and recording of agent-to-agent calls is not required.

In this configuration, the:

- Voice gateway is directly connected to the Catalyst 6000
- Catalyst 3524XLs are directly trunked to the Catalyst 6000
- IP phones are in VLAN 15
- VoIP Monitor server is on port 2/10 on the Catalyst 6000

The Catalyst 6000 SPAN commands are:

```
Cat6000> (enable) set span 15 2/10 rx inpkts enable create
```

Single Catalyst 6000 and Multiple Catalyst 3524XLs, with Required Agent-to-Agent Monitoring

In this configuration, the supervisors must be able to monitor both gateway and agent-to-agent calls. Since agent-to-agent calls on a single 3524XL switch would not be visible on the Catalyst 6000, we need to install two VoIP Monitor servers, one for each Catalyst 3524XL.

In this configuration, the:

- Voice gateway is directly connected to the Catalyst 6000
- Catalyst 3524XLs are directly trunked to the Catalyst 6000

For Catalyst 3524XL Number 1:

- IP phones are on ports FastEthernet 0/1 and 0/4

- VoIP Monitor server is on port FastEthernet 0/5
- IP phones and VoIP Monitor server are in the same VLAN

For Catalyst 3524XL Number 2:

- IP phones are on ports FastEthernet 0/3 and 0/4
- VoIP Monitor server is on port FastEthernet 0/6
- IP phones and VoIP Monitor server are in the same VLAN

For Catalyst 3524XL Number 1, the SPAN commands are:

```
Cat3524XL1(config)#interface FastEthernet 0/5
Cat3524XL1(config-if)#port monitor FastEthernet 0/1
Cat3524XL1(config-if)#port monitor FastEthernet 0/4
Cat3524XL1(config-if)#exit
```

For Catalyst 3524XL Number 2, the SPAN commands are:

```
Cat3524XL2(config)#interface FastEthernet 0/6
Cat3524XL2(config-if)#port monitor FastEthernet 0/3
Cat3524XL2(config-if)#port monitor FastEthernet 0/4
Cat3524XL2(config-if)#exit
```

Single Catalyst 6000 and Multiple Catalyst 3524XLs, with Routers Separating the Switches

In this configuration, routers separate the various Catalyst switches. Regardless if it is necessary or not to monitor agent-to-agent calls, at least two VoIP Monitor servers are required, one for each Catalyst 3524XL switch.

Monitoring on the Catalyst 6000 is not possible because there is a router between the Catalyst 6000 and the Catalyst 3524XLs.

In this case, the implementation of the configuration is the same as for the section “Single Catalyst 6000 and Multiple Catalyst 3524XLs, with Required Agent-to-Agent Monitoring” above.

> NOTE: For detailed information on SPAN, see “Configuring the Catalyst Switched Port Analyzer (SPAN) Feature” on the Cisco website in the Tech Notes section (www.cisco.com/warp/public/473/41.html).

Appendix B: Using Multiple NICs with the VoIP Monitor Service

B

Overview

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.

Limitations

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

SplkPCap 3.0, the packet sniffing library, works only with NICs that are bound to TCP/IP. Make sure the sniffing card is bound to TCP/IP.

Issues

The VoIP Monitor service does not specify which NIC should be used when sending out packets. 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 table so that normal traffic does not go through the sniffing NIC. Contact your network administrator for details.

An alternative solution is to give the sniffing NIC an 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.

Installing a Second NIC on a VoIP Monitor Service Computer

This procedure applies only to computers running Windows 2000.

1. Install the second NIC in the computer.
2. Start the computer.
3. Make sure that neither adapter is using dynamic host configuration protocol (DHCP) to get its IP address.
4. Give the adapters valid IP addresses.
5. Determine which of the two adapters is to be used for sniffing.
6. Connect the sniffing adapter with the switch SPAN port.
7. Connect the second adapter with a normal switch port that is not monitored by the 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 PING <local host name> command. This ensures that the local name always resolves to the normal traffic card IP address.

Required Registry Changes

The installation process offers the user the option to choose the IP address that the VoIP Monitor Service will use for normal traffic and the IP address of the network adapter that the server will use for sniffing.

However, the installation is such that the user can only specify the IP address of the sniffing card. The IP address that the VoIP Monitor Service is receiving requests at is, by default, the first one to appear in the system-supplied enumeration.

While this works in a one-NIC scenario, it may be wrong in a two-NIC scenario. If the first IP address that appears in the enumeration is the sniffing card then the same card would be used for both sniffing and other traffic. This is the situation we are trying to avoid by making sure that the correct IP address is written in the CAD service registry settings, as outlined in the procedure below.

Second NIC is Present Before Unified CC Express Installation

1. Enter the sniffing card's IP address when asked for the VoIP Monitor Service during the installation process.
2. After the installation finishes, make sure the following registry key has the normal traffic IP address value:

   HKLM\SOFTWARE\Spanlink\Site Setup\IOR HOSTNAME

Second NIC is Installed After Unified CC Express Installation

1. Navigate to the following registry key:

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\
NetworkCards

2. Find the newly-inserted card entry.
3. Copy the value in ServiceName.
4. Paste this value in the following registry key:

   HKLM\SOFTWARE\Spanlink\VoIP Monitor Server\Config\MONITOR DEVICE
5. Prefix the value with **\Device\Splkpc_**. This string is case sensitive—it must match exactly.
6. Close the Windows registry.

Installing CAD Services

After you install CAD services on a server that has more than one enabled NIC, or if you install a second NIC after the CAD services are installed, run the CAD Configuration Setup utility (see "CAD Configuration Setup Utility" on page 39) and select the appropriate NIC to use from the Services IP Address window.