



Installation Guide

Cisco Desktop Product Suite 4.5.5 (ICD)

Corporate 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: 408 526-4100

Customer Order Number:
Text Part Number: OL-4203-02



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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)

Installation Guide: Cisco Desktop Product Suite 4.5.5 (ICD)

Copyright © 2004, Cisco Systems, Inc.

All rights reserved.

Contents

1	Before You Install Cisco Desktop Product Suite	
	■ Overview	1-1
	Product Bundles	1-1
	■ About This Document	1-2
	Intended Audience	1-2
	Conventions	1-2
	■ Elements of the Cisco Desktop Product Suite	1-4
	Desktop Applications	1-4
	Servers	1-5
	■ CRA System Configuration	1-8
	■ System Requirements	1-10
	Computer Hardware and Operating Systems	1-10
	Agent Phones	1-11
	Recording and Statistics Server Hard Disk Space Requirements	1-11
	■ Prerequisites	1-12
	Required SPAN Port Configuration	1-12
	■ Preinstallation Considerations	1-14
	Sharing Configuration Files	1-14
	Share Considerations for an Off-Board Recording and Statistics Server	1-16
	Installing the VoIP Monitor and Recording & Statistics Servers after CRS is Installed	1-17
	Windows NT, Windows 2000, and Windows XP Platforms 1-19	
	Queue Statistics	1-19
	Adding Voice-Over IP Monitor Servers	1-19

2	Installing Desktop Applications	
	■ Overview	2-1
	■ Upgrading from Version 4.3.x	2-2
	■ Installing Agent Desktop	2-3
	Overview	2-3

Contents

Before You Install	2-3
Installation Procedure	2-3
JTAPI on the Agent PC	2-4
■ Installing Supervisor Desktop	2-6
Overview	2-6
Upgrading from Standard to Advanced Supervisor Desktop 2-7	
Before You Install	2-7
Installation Procedure	2-7
■ Installing Desktop Administrator	2-9
Overview	2-9
Before You Install	2-9
Installation Procedure	2-9
■ Configuring Cisco CallManager IP Phones to Work With IP Phone Agent 2-12	
Creating an IP Phone Service	2-12
Assigning the IP Phone Service to IP Agent Phones . . .	2-13
Creating the “telecaster” User	2-14
Changing the Default URL Authentication Parameter . .	2-14
■ Configuring Media Termination Phones	2-16
Cisco IP SoftPhone	2-16
■ Using Multiple NICs with the VoIP Monitor Service 2-17	
Overview	2-17
Limitations	2-17
Issues	2-17
Installing a Second NIC on a VoIP Monitor Service Computer 2-18	
Installing Cisco Desktop	2-18

3 Removing Applications

■ Removing Cisco Desktop Product Suite Applications	3-1
Removing a VoIP Monitor Server from CRS	3-2

Contents

Manually Removing Cisco Desktop Applications 3-2

Contents

Before You Install Cisco Desktop Product Suite

1

Overview

This document tells you how to install Cisco Agent Desktop, Cisco Supervisor Desktop, and Cisco Desktop Administrator in your contact center after the Customer Response (CRA) platform is installed and configured.

Upon successful installation into a properly-configured ICD environment, the basic functionality of Agent Desktop and Supervisor Desktop are ready to use with no further configuration required.

Product Bundles

Cisco Desktop Product Suite 4.5 offers four different bundles:

- Standard Bundle
- Standard Bundle with Media Termination
- Enhanced Bundle
- Enhanced Bundle with Media Termination

Media Termination enables the Agent Desktop soft phone to perform call functions, so that no hard IP phone is needed.

The Enhanced Bundle, with or without Media Termination, offers the full range of functionality described in the section “Elements of the Cisco Desktop Product Suite” on page 1-4.

The Standard Bundle, with or without Media Termination, offers the same basic functionality, with these exceptions:

- Agent Desktop—No task buttons (no work flow automation).
- Supervisor Desktop—No call monitoring, recording, barge-in, or intercept.
- Desktop Administrator—No work flow automation or Agent Desktop interface customization.

About This Document

Intended Audience

This document is written for personnel who install the desktop applications of the Cisco Desktop Product Suite.

Conventions

In this document, terminology and typographic conventions are as follows.

Terminology

- The word *enter* means to press the sequence of keys specified. For example, an instruction to enter the letter “y” is shown as

Enter **y** to continue.

- The word *click* means to use your mouse to execute the action represented by a button. For example, an instruction to click the Next button is shown as

Click **Next**.

- The words *check* and *uncheck* mean to activate or deactivate a check box. For example, an instruction to deactivate the Dial Number as Entered check box is shown as

Uncheck the **Dial Number as Entered** check box.

- The word *choose* means to pick an option from a menu or submenu. For example, an instruction to choose the Desktop option from a series of submenus is shown as

Choose **Start > Programs > Cisco > Desktop**.

- The word *select* means to mark text or other elements to be copied or cut. For example, an instruction to select text is shown as

Select an entry from the list to edit.

- Simultaneous keystrokes (as when you hold down the first key, then press the second and third keys) are represented as a series of bolded key names joined by hyphens. For example, an instruction to press and hold the Alt key while pressing the letter “d” is shown as

Press **Alt-d**

- Function keys are represented by the letter F followed by the function key number. For example, an instruction to press function key 3 is shown as

Press **F3**.

Typography

- Commands and text you type, the names of windows, buttons, menus, and menu options appear in bold type:

From the **Options** menu, choose **Local Admin**.

- Variables you must enter appear in italics:

http://servername/appadmin

- Terms that are being defined appear in italics:

Actions are commands that perform a task.

- Menu paths appear in bold type with menu options separated by right angle brackets:

Choose **Options > Status Bar**.

Elements of the Cisco Desktop Product Suite

The Cisco Desktop Product Suite includes the following elements:

Desktop Applications

Desktop Administrator

Desktop Administrator provides centralized administration tools to configure the Cisco Desktop components. It supports multiple administrators, each able to configure the same data.

Desktop Administrator includes the following components:

Enterprise Configuration. Enterprise Configuration is used to define the fields for displaying the data collected by the CallManager or the ICD and stored on the Enterprise server, and for assigning devices to be monitored by the VoIP Monitor server(s) in your system.

Desktop Configuration. Desktop Configuration defines the look and feel of the agent's desktop and work flows. With it you control the configuration of:

- Dial Strings: format how phone numbers are displayed
- Phone Book: create and administer global phone books
- Reason Codes: create and administer reason codes
- Work Flow Groups: create and administer work flows, customize the Agent Desktop interface, and administer enterprise data

ICD Configuration. ICD Configuration enables you to use the ICD component administrative applications. From this tool you can launch your web browser to access these websites:

- Cisco CallManager Administration
- Cisco Customer Response Application Administration

Personnel Configuration. Personnel Configuration enables you to view and extend the attributes for the contact center's resources beyond their definitions in ICD. You can view the attributes for agents, and create, modify, and delete supervisors and teams.

Agent Desktop

Agent Desktop screen pops caller information to the agent desktop along with the call. It can populate any sort of third-party application based on the calling number, called number, or other telephone identifier.

Agent Desktop includes a soft phone that allows agents to control calls from the PC. The optional Media Termination feature enables Agent Desktop to function as an IP phone, so no actual phone is needed at an agent's workstation. (For Media Termination to function, a sound card in the agent's PC is required.)

Agent Desktop's toolbar automates common telephony functions. The toolbar includes a task bar which can launch applications based on telephony and/or data events.

Supervisor Desktop

Supervisor Desktop allows contact center supervisors to manage agent teams in real time. They can observe, coach, and communicate with agents in writing, 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 agent calls and, if necessary, conference in or take over those calls using the barge-in and intercept features. Through the supervisor log viewer, supervisors can play back, save, and delete recorded agent calls.

Call/Chat

Call/Chat is used in conjunction with Agent Desktop. It enables agents to communicate in writing among themselves or with their supervisors so they can handle calls more efficiently. It also provides a marquee message function that allows supervisors to send important messages to some or all agents on their teams.

Enterprise Data

Enterprise Data is a server-based data management system. Used in conjunction with Agent Desktop, it displays the additional enterprise data associated with a call. Enterprise Data also displays call activity information for the active call.

Servers

Directory Services Server

The Directory Services server is an LDAP server. All other Cisco Desktop servers register with this server at startup. Clients use the Directory Services server to determine how to connect to the other servers.

The majority of the agent, supervisor, team, and skill information is also kept on the Directory Services server. Agent and skill information is imported from ICD and kept synchronized by the Directory Services Sync (Synchronization) server. Supervisor and team information is configured in Desktop Administrator.

The Cisco Desktop Product Suite is capable of working with four different Directory Services servers. They are:

- DC Directory
- Microsoft Active Directory
- Netscape iPlanet
- OpenLDAP

Directory Services Sync Server

The Directory Services Sync server connects to the ICD database via an ODBC connection and retrieves agent information. It then compares the information with the information in the Directory Services server and adds, updates, or deletes LDAP entries as needed to stay consistent with the ICD configuration.

Call/Chat Server

The Call/Chat server is a CORBA server program that acts as a message broker between the Call/Chat clients and Supervisor Desktop. The Call/Chat server is in constant communication with all agent and supervisor desktops.

Agents' desktops inform the Call/Chat server of all call activity. The server, in turn, sends this information to all appropriate supervisors. It also facilitates the sending of text chat and marquee messages between agents (excluding IP Phone agents) and supervisors.

Enterprise Server

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

Voice-Over IP Monitor Server

The Voice-Over IP Monitor server is a CORBA server program that is used to enable supervisors to silently monitor agents. The server accomplishes this by "sniffing" network traffic for voice packets.

Multiple Voice-Over IP Monitor servers can be installed in one logical contact center to ensure there is enough capacity to handle the number of agents in the contact center.

Recording and Statistics Server

The Recording and Statistics server is a CORBA server program that extends the capabilities of the Voice-Over IP Monitor server by allowing supervisors and agents to record calls. Supervisors can play back recorded agent calls through the Supervisor Log Viewer. The Log Viewer also maintains a 7-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, and many more statistics.

IP Phone Agent Server

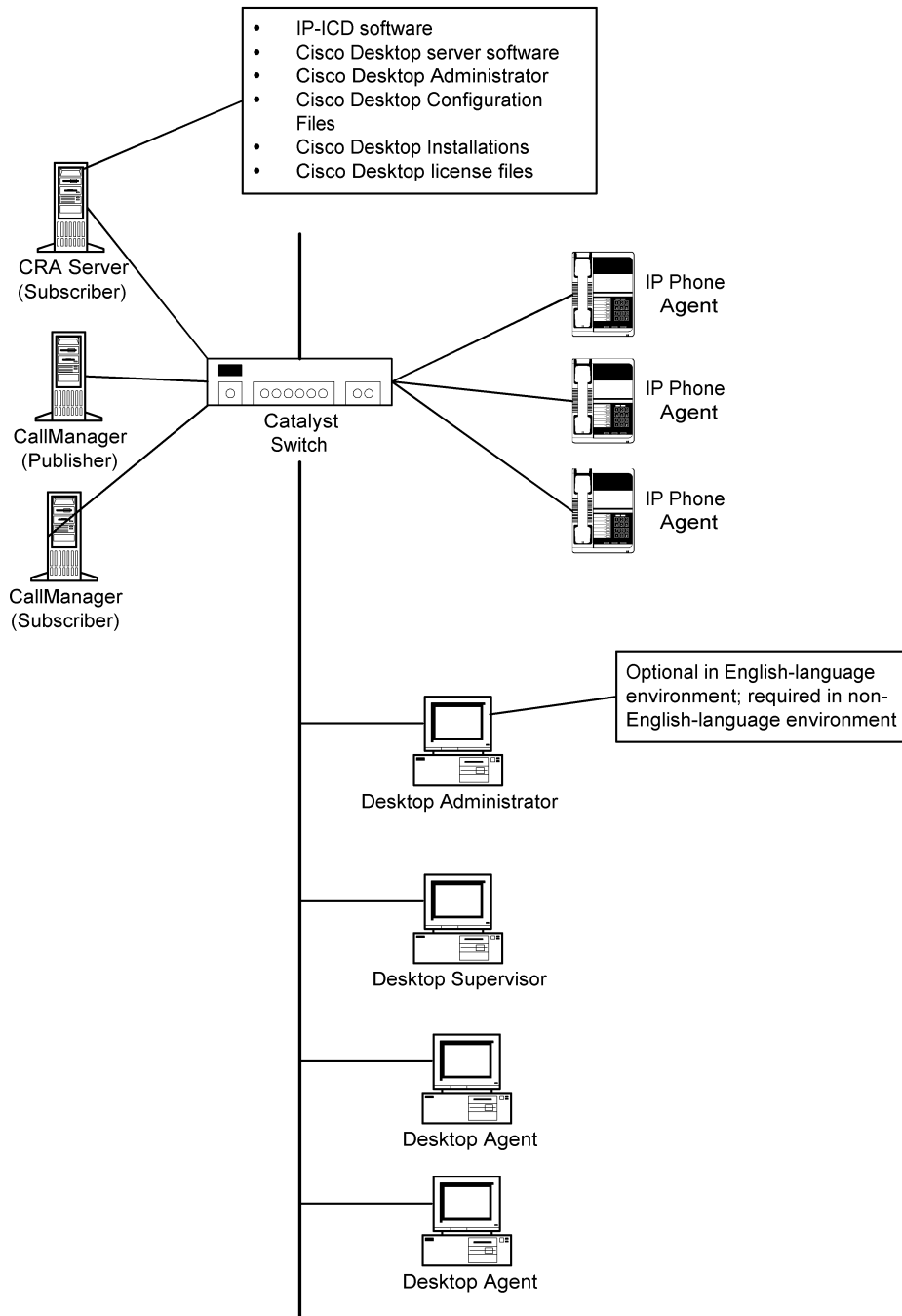
The IP Phone Agent server enables IP phone agents to log in and out of ICD, change agent states, and enter reason codes without having the Agent Desktop software.

This server works with the Services feature of CallManager and model 7940/7960 Cisco IP phones.

CRA System Configuration

Figure 1.1 depicts the standard CRA system configuration for a contact center.

Figure 1-1. Standard ICD configuration.



NOTE: Desktop Administrator is always installed on the CRA server. However, in a non-English-language environment, it is necessary to run a second instance of Desktop Administrator on a machine with a local-language operating system so that chat messages, tooltips, enterprise data names, and other communication within the contact center is in the local language.

NOTE: No other CTI application (such as Cisco Attendant Console) can share the same line as the agent ICD extension.

System Requirements

Computer Hardware and Operating Systems

The following are the minimum system requirements for running Cisco Desktop Product Suite.

NOTE: It is recommended that desktops running Media Termination have more memory and faster processors than the minimums listed below.

Cisco Desktop servers and applications require significant system resources. Running other resource-intensive applications at the same time may adversely affect their performance.

Required Hardware and Operating Systems

Operating System	Desktop Applications	Servers
Windows 98 OSR1, OSR2	<ul style="list-style-type: none"> • 233 MHz Pentium • 32 MB RAM • 16 MB free space • NIC supporting Ethernet 2 	not supported
Windows NT Professional 4.0 Service Pack 6	<ul style="list-style-type: none"> • 233 MHz Pentium • 64 MB RAM • 16 MB free space • NIC supporting Ethernet 2 	not supported
Windows 2000 Professional Service Pack 3	<ul style="list-style-type: none"> • 233 MHz Pentium • 64 MB RAM • 16 MB free space • NIC supporting Ethernet 2 	not supported
Windows XP Professional Edition	<ul style="list-style-type: none"> • 300 MHz Pentium • 128 MB RAM • 16 MB free space • NIC supporting Ethernet 2 	not supported
Windows NT Server 4.0 Service Pack 6	not supported	<ul style="list-style-type: none"> • 1 GHz Pentium • 1 GB RAM • 16 MB free space • NIC supporting Ethernet 2
Windows 2000 Server Service Pack 3	not supported	<ul style="list-style-type: none"> • 1 GHz Pentium • 1 GB RAM • 16 MB free space • NIC supporting Ethernet 2
Windows 2000 Advanced Server	not supported	supported

Agent Phones

Cisco Desktop Product Suite supports the following phones:

- Cisco IP Phones models 7910, 7940, and 7910
- Cisco IP SoftPhone

Unsupported Configurations for Agent Phones

The following configurations are not supported for agent phones:

- Two lines on an agent's phone that have the same extension but exist in different partitions
- An ICD extension assigned to multiple devices (configuring an ICD extension in a device profile is supported)
- Call forwarding on an ICD line
- Call waiting enabled on an ICD line

Recording and Statistics Server Hard Disk Space Requirements

The Recording and Statistics server has the following hard disk space requirements:

Data Stored	Space Required	
	75 agents, 10 supervisors	200 agents, 30 supervisors
Agent states and call activity records (contact center open seven days per week, ten hours per day, each agent handling calls of one minute each)	0.3 GB	0.8 GB
Each minute of recorded call	1.0 MB	1.0 MB
Voice calls (each supervisor recording ten five-minute calls per day)	0.5 GB	1.5 GB

NOTE: 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.

Prerequisites

Required SPAN Port Configuration

The Voice-Over IP (VoIP) Monitor server accomplishes voice monitoring and recording functions by “sniffing” voice packets to and from IP phones.

Because network switches do not normally deliver packets to Ethernet ports other than the destination port (in this case, an IP phone), the switch must be configured to do this. To accomplish this, the Ethernet port for the VoIP Monitor server must be configured to monitor the Ethernet ports for all agent IP phones. If the voice packets going to and from an agent’s IP phone are not sent to the VoIP Monitor server’s port for any reason, that conversation will not be available to the supervisor.

Having the VoIP Monitor server monitor a port that all voice traffic goes through (for instance, the Ethernet port to which a gateway to the PSTN is connected) is not sufficient. It must monitor the Ethernet ports to which the IP phones are directly connected. The reason for this is that the server identifies packets by the IP phone’s MAC (medium access control) address. The packet’s MAC address changes as the packet moves around the network. There must not be a router between the IP phone and the port the server is monitoring.

The server sniffs packets on a single network interface card (NIC) and thus a single Ethernet port. This is the port that must be configured. This does not necessarily require that the server and the IP phones be connected to the same network switch. That depends on the switch’s monitoring capabilities.

The port monitoring feature on Cisco Catalyst switches is called Switched Port Analyzer (SPAN). 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).

Switch Capabilities and Restrictions

The following capabilities and restrictions are from the above-mentioned document. Refer to Cisco documentation for more details.

Catalyst 2900XL and 3500XL Switches

A monitor port:

- Cannot be in a Fast EtherChannel or Gigabit EtherChannel port group
- Cannot be enabled for port security
- Cannot be a multi-VLAN port

- Must be a member of the same VLAN as the port monitored. VLAN membership changes are disallowed on monitor ports and ports being monitored
- Cannot be a dynamic-access port or a trunk port. However, a static-access port can monitor a VLAN on a trunk, a multi-VLAN, or a dynamic-access port. The VLAN monitored is the one associated with the static-access port
- Port monitoring does not work if both the monitor and monitored ports are protected ports

Catalyst 4000, 5000, and 6000 Series Switches

4000, 5000, and 6000 series switches are able to monitor ports belonging to multiple VLANs.

Preinstallation Considerations

Sharing Configuration Files

Configuration and licensing files are installed on the CRA server. They must be read-write accessible to Agent Desktop and Supervisor Desktop users.

NOTE: If installing a second instance of Desktop Administrator, that instance must use the configuration files on the CRA server.

NOTE: Windows 2000 Professional machines have a built-in limitation of ten shared sessions. Take this into consideration if you intend to install the shared configuration files on this type of platform.

There are a number of ways to ensure that the configuration files are accessible to all agents. among these methods are:

- Using a login script to establish the shared configuration location
- Manually mapping the shared configuration location
- Automatically mapping the shared configuration location

Login Script Method

In this method, agents use an agent user account to connect to the CRA server.

1. Set up an agent user account on the CRA server.
 - a. Choose **Start > Control Panel > Performance & Maintenance > Administrative Tools > Computer Management**.
The Computer Management window appears.
 - b. Choose **Action > New User**.
The New User dialog box appears.
 - c. Enter user name **Agent** and password **agent**, uncheck all check boxes, and then check the **Password Never Expires** check box.
 - d. Click **Create**.
The new user "Agent" is created as a member of the Users group, and appears in the navigation pane under the Users folder.
2. Find out the CRA server's NT domain or NT work group.
 - a. Right-click **My Computer**, and then choose **Properties**.
The System Properties dialog box appears.

- b. Select the Network Identification tab.

The CRA server's NT work group or NT domain name is shown on the tab.

- 3. Add the following net use command to the agent PC's login script or autoexec.bat file.

For Windows NT and Windows 2000:

```
net use drive: \\IPaddress\DESKTOP_CFG /USER:workgroup  
or domain\account password
```

where:

<i>drive</i>	Available drive letter on the agent's PC
<i>IPaddress</i>	CRA server's IP address
DESKTOP_CFG	Name of the shared folder
/USER:	Optional net use parameter that allows you to specify which account to use when logging in
<i>workgroup or domain</i>	CRA server's NT work group or NT domain name
<i>account</i>	The user account used when logging in
<i>password</i>	User account's password

Example 1: User account JohnK, with password 12345, maps drive f to the shared folder DESKTOP_CFG on CRA server 192.168.252.46. The user account is in the same domain as the CRA server.

```
net use f: \\192.168.252.46\DESKTOP_CFG /user:  
JohnK 12345
```

Example 2: User account JohnK, with password 12345, maps drive f to the shared folder DESKTOP_CFG on CRA server 192.168.252.46. The CRA server is in the CALLCENTER domain; the user account is in another domain.

```
net use f: \\192.168.252.46\DESKTOP_CFG /user:  
CALLCENTER\JohnK 12345
```

For Windows 98:

```
net use drive: \\IPaddress\DESKTOP_CFG password
```

where:

<i>drive</i>	Available drive letter on the agent's PC
<i>IPaddress</i>	CRA server's IP address
DESKTOP_CFG	Name of the shared folder
<i>password</i>	User account password

Example: User account JohnK, with password 12345, maps drive f to CRA server 192.168.252.46.

```
net use f: \\192.168.252.46\DESKTOP_CFG 12345
```

NOTE: On a Windows 98 platform, the login used by the agent is the same login that is used by net use to gain access to the CRA server. As a result, that login must be created on the CRA server.

Share Considerations for an Off-Board Recording and Statistics Server

Audio files are stored with the Recording and Statistics server. If your system is configured so that this server is off-board (not installed on the same machine as the CRA server), you must ensure that supervisors are mapped to the shared audio files folder on that server so that they are able to listen to the recorded calls. The shared folder is located at:

```
\\IPaddress\AudioFiles
```

where:

<i>IPaddress</i>	Recording and Statistics server's name or IP address
AudioFiles	Name of the shared folder in which recordings are stored

NOTE: If you have converted the partition where the audio files are stored from the FAT32 file system to the NTFS file system, you will need to ensure that supervisors have rights to the shared folder. If they do not have rights to that shared folder, they will be unable to play back or save recordings made after the file system was converted. See "Permissions Requirements" in Chapter 3 of the Service Information manual for more information on permissions

Installing the VoIP Monitor and Recording & Statistics Servers after CRS is Installed

If you need to install the VoIP Monitor server and Recording & Statistics server on the CRS machine after you have already installed the CRA server, you must reinstall the CRA server. If you do not reinstall the CRA server, the Recording and Statistics server assumes that it is being installed on a stand-alone server and will create a separate share drive.

To install correctly, select the following options in the Cisco AVVID Cisco IP Telephony Applications Server QuickBuilder installation window:

- CRA Server
- VoIP Monitor Server
- ICD Record/Statistics Server

If you omit to install the CRA server, you can point the Recording & Statistics server to the correct location for audio files by removing the following registry key on the CRA server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\FastCall RASCAL  
Server\Setup\Audio directory
```

Manual Mapping Method

Follow these steps to manually map the shared drive to the agent's PC:

1. Double-click **Network Neighborhood** on your Windows desktop.
The Network Neighborhood window appears.
2. Double-click the host on which the Cisco Desktop Administrator configuration files are located.
The host's window appears.
Explore it to find the directory in which the configuration files are stored.
3. Select the directory, and then click **File > Map Network Drive....**
The Map Network Drive dialog box appears.
4. Map the drive to a drive letter on your local PC, check the **Reconnect at Logon** check box to ensure you will have access to the mapped drive, and then click **OK**.
The agent PC is now mapped to the network drive.

NOTE: When you map a drive using manual mapping, the user is prompted for his or her password every time the drive is mapped to the PC, once per logon process.

Automatic Mapping Method

If a trust relationship is established between the Cisco and corporate domains, it is possible to create a script that will map the drive when an agent logs into his or her PC.

A sample script is as follows:

```
rem login.bat--simple login script for mapping drives
if exists drive:\nul net use drive: /del
if exists path\*. * net use drive: path
```

where:

<i>drive</i>	Available drive letter
<i>path</i>	Path to the Customer Response Applications (CRA) folder

The first line of the script (after the comment line) unmaps the drive letter you need if the user has manually mapped it. The second line of the script maps the drive if it is available.

Windows NT, Windows 2000, and Windows XP Platforms

When installing a Desktop application on a Windows NT, Windows 2000, or Windows XP platform, the user must have administrator privileges.

Desktop Administrator users must also have Administrator or Power User privileges on these platforms. The reason for this is that the user must have sufficient rights to update registry settings.

Queue Statistics

The number displayed in the statistics field "Waiting" in the Queues statistics windows in Agent Desktop and Supervisor Desktop is dependent on how you configure skill groups and set up queues in Configuration Manager. The following rules apply:

- If calls are queued to a base skill group, there must be no sub skill groups configured.
- If a skill group does have sub skill groups configured, calls cannot be queued to the base skill group.

If calls are queued to the base skill group, all the calls queued to that skill group are reported in the Waiting field.

If sub skill groups are configured, and calls are queued to those sub skill groups, only the calls queued to the primary sub skill group are reported in the Waiting field.

See your Configuration Manager documentation for more information on setting up skill groups and queues.

Adding Voice-Over IP Monitor Servers

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

Cisco Desktop Product Suite 4.5 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.

NOTE: Before installing an additional VoIP Monitor server, you must use the functionality in Desktop Administrator to assign devices to a specific

VoIP Monitor. For details, see Section 2, “VoIP Monitor,” in the *Cisco Desktop Administrator User Guide*.

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

Installing Desktop Applications

2

Overview

In a typical configuration, all server software, global configuration files, and Desktop Administrator are installed on the CRA server prior to the installation of the desktop applications.

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

Upgrading from Version 4.3.x

To upgrade version 4.3.x of Agent Desktop, Supervisor Desktop, and Desktop Administrator, install version 4.5 over the previous version. No special steps are required.

NOTE: Whenever you upgrade Cisco CRA, you must upgrade Agent Desktop and Supervisor Desktop.

Installing Agent Desktop

Overview

You can choose to install either Agent Desktop, or Agent Desktop with Media Termination.

NOTE: It is recommended that you not install Agent Desktop on the CRA server. However, if you do so, ensure that Agent Desktop's LDAP registry information does not point to your production CRA server.

If you install Agent Desktop with Media Termination, the agent can use Agent Desktop's soft IP phone for call control. A hard IP phone is not necessary.

NOTE: If Media Termination is installed, the Media Termination phone must be set up in Cisco CallManager as phone type 30 SP+. The Media Termination phone does not support auto-registration with the CallManager. Therefore, the device DN should be set up in the CallManager using the MAC address of the PC where the Media Termination phone is installed.

Before You Install

Before you install Agent Desktop, you need to know:

- The IP address of the CRA server
- The user ID and password to access the CRA User Options web page (the same user ID and password used to access Cisco Agent Desktop)
- The destination folder on the user's PC in which you will install the application

Installation Procedure

► **To install Agent Desktop, follow these steps:**

1. Open your web browser and access the Cisco CRA User web page at <http://servername/appuser>.

Replace *servername* with the IP address of the Cisco CRA server.

The CRA User Options Authentication window appears.

2. At the prompt, enter your username and password, and then click **Log On**.
The Welcome window appears.
3. Click **ICD Downloads**.

The Download Cisco IP ICD Agent Desktop window appears.

4. Use the Windows Copy function to copy the following command line from the Download Cisco IP ICD Agent Desktop window. (*Servename* is the IP address of your CRA server.)

```
\\Servename\DESKTOP_CFG\desktop\InstallManager
```

5. From the Windows taskbar, choose **Start > Run**.

The Run dialog box appears.

6. In the Open field in the Run dialog box, use the Windows Paste command to paste the command line that you copied in Step 4, and then click **OK**.

The Enter Network Password dialog box appears.

7. Enter your user name and password, and then click **OK**.

The Welcome dialog box appears.

8. Click **Next**.

The Select Options dialog box appears.

9. Check the version of Agent Desktop you wish to install, and then click **Next**.

The Choose Destination Location dialog box appears.

10. Accept the default destination folder, or click **Browse** to navigate to another destination folder, and then click **Next**.

The Start Copying Files dialog box appears.

11. Click **Next** to start the installation.

Installation Manager installs the application you chose.

NOTE: You may need to install Java 2 Runtime Environment if you do not already have this application on your PC, or you have an older version that needs to be updated. InstallManager displays the appropriate screens to do this.

When the installation is complete, the Install Results dialog box appears.

12. Click **Finish** to complete the installation process.

JTAPI on the Agent PC

JTAPI (Java Telephony API) is Sun's telephony programming interface for Java. It provides a set of classes and interfaces that provide access to call control and telephony device control as well as media and administrative services.

When the CAD servers are installed, the latest version of JTAPI is installed on the share. During the installation of Agent Desktop on an agent PC, the installation program copies the jtapi.jar file from the share to the agent PC.

Each time Agent Desktop starts, the jtapi.jar file version on the agent's PC and the version on the share are compared. If they are different, the version on the share is copied down to the agent PC.

NOTE: This jtapi.jar file comparison does not take into account version numbering, that is, the version on the share could be older than the version on the agent PC, and it would still be copied down to the agent PC. All that matters is that the versions are different.

JTAPI on the share can be updated with the JTAPI Update Tool. This tool is accessed on the CRS computer by clicking **Start > Programs > Cisco CRA Administrator > JTAPI Update Tool**.

Installing Supervisor Desktop

Overview

There are five versions of Supervisor Desktop available. They are:

- On-Site Enhanced Supervisor Desktop
This version includes all available functionality.
- On-Site Enhanced Supervisor Desktop with Media Termination
This version includes all available functionality, with the addition of Media Termination. Media Termination enables the supervisor to use Agent Desktop's soft IP phone for call control. A hard IP phone is not necessary.
- On-Site Supervisor Desktop
This version does not include call monitoring, recording, barge-in, or intercept features.
- On-Site Supervisor Desktop with Media Termination
This version does not include call monitoring, recording, barge-in, or intercept features. It includes Media Termination, which enables the agent to use Agent Desktop's soft IP phone for call control. A hard IP phone is not necessary.
- Remote Supervisor Desktop
This version enables a supervisor to monitor agents from outside of the local contact center, but not to intervene (barge-in, intercept, or record conversations, or change agent states) in any way.

When you install any version of Supervisor Desktop, Agent Desktop is automatically installed at the same time.

NOTE: It is recommended that you not install Supervisor Desktop on the CRA server. However, if you do so, ensure that Supervisor Desktop's LDAP registry information does not point to your production CRA server.

NOTE: If Media Termination is installed, the Media Termination phone must be set up in Cisco CallManager as phone type 30 SP+. The Media Termination phone does not support auto-registration with the CallManager. Therefore, the device DN should be set up in the CallManager using the MAC address of the PC where the Media Termination phone is installed.

Upgrading from Standard to Advanced Supervisor Desktop

You must uninstall Standard Supervisor Desktop before you install Advanced Supervisor Desktop. It is not necessary to uninstall Standard Agent Desktop—the Advanced version installs over it.

Before You Install

Before you install Supervisor Desktop, you need to know:

- The IP address of the CRA server
- The user ID and password to access the CRA User Options web page (the same user ID and password used to access Cisco Agent Desktop)
- The destination folder on the user's PC in which you will install the application

Installation Procedure

► **To install Supervisor Desktop, follow these steps:**

1. Open your web browser and access the Cisco CRA User web page at `http://servername/appuser`.

Replace *servername* with the IP address of the Cisco CRA server.

The CRA User Options Authentication window appears.

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

The Welcome window appears.

3. Click **ICD Downloads**.

The Download Cisco IP ICD Agent Desktop window appears.

4. Use the Windows Copy function to copy the following command line from the Download Cisco IP ICD Agent Desktop window. (*Servername* is the IP address of your CRA server.)

```
\\Servername\DESKTOP_CFG\desktop\
```

5. From the Windows taskbar, choose **Start > Run**.

The Run dialog box appears.

6. In the Open field in the Run dialog box, use the Windows Paste command to paste the command line that you copied in Step 4, and then click **OK**.

The Enter Network Password dialog box appears.

7. Enter your user name and password, and then click **OK**.

Your Desktop folder opens.

8. From the Windows task bar, choose **Start > Programs > Command Prompt**.

The DOS command window appears.

9. Enter the following command in the DOS command window:

```
\\servername\DESKTOP_CFG\Desktop\InstallManager.exe -f  
\\servername\DESKTOP_CFG\Desktop\AdvancedManager.cfg
```

HINT: To ensure this command is entered accurately, drag the InstallManager.exe file from the Folder window to the DOS command window, type a space, **-f**, and another space, and then drag the AdvancedManager.cfg file from the Folder window to the DOS command window.

10. In the DOS command window, press **Enter**.

The Install Manager program starts and displays the Welcome window.

11. Click **Next**.

The Select Options dialog box appears.

12. Check the version of Supervisor Desktop you want to install, and then click **Next**.

The Choose Destination Location dialog box appears.

13. Accept the default destination folder, or click **Browse** to navigate to another destination folder, and then click **Next**.

The Start Copying Files dialog box appears.

14. Click **Next** to start the installation.

Installation Manager installs the application you chose.

When the installation is complete, the Install Results dialog box appears.

15. Click **Finish** to complete the installation process.

Installing Desktop Administrator

Overview

Desktop Administrator is installed with the CRA applications on the CRA server. In a non-English environment, a second instance of Desktop Administrator must be run on a machine with a local-language operating system, so that chat messages, tooltips, and other communication within the contact center is in the local language.

NOTE: If Agent Desktop and/or Supervisor Desktop are installed on the same machine as the second instance of Desktop Administrator, they must be installed first. If Desktop Administrator is installed first, Install Manager will not install Java.

PDF versions of the Cisco Desktop Product Suite documentation are installed automatically when you install Desktop Administrator.

Before You Install

Before you install Desktop Administrator, you need to know:

- The URL of the Cisco Customer Response Applications (CRA) User web page on the CRA server
- The user ID and password to access the CRA User Options web page (the same user ID and password used to access Cisco Agent Desktop)
- The destination folder on the administrator's PC in which you will install the application

Installation Procedure

► **To install Desktop Administrator, follow these steps:**

1. Open your web browser and access the Cisco CRA User web page at `http://servername/appuser`.

Replace *servername* with the IP address of the Cisco CRA server.

The CRA User Options Authentication window appears.

2. At the prompt, enter your username and password, and then click **Log On**.
The Welcome window appears.
3. Click **ICD Downloads**.

The Download Cisco IP ICD Agent Desktop window appears.

4. Use the Windows Copy function to copy the following command line from the Download Cisco IP ICD Agent Desktop window. (*Servename* is the IP address of your CRA server.)

```
\\Servename\DESKTOP_CFG\desktop\
```

5. From the Windows taskbar, choose **Start > Run**.

The Run dialog box appears.

6. In the Open field in the Run dialog box, use the Windows Paste command to paste the command line that you copied in Step 4, and then click **OK**.

The Enter Network Password dialog box appears.

7. Enter your user name and password, and then click **OK**.

Your Desktop folder opens.

8. From the Windows task bar, choose **Start > Programs > Command Prompt**.

The DOS command window appears.

9. Enter the following command in the DOS command window:

```
\\servename\DESKTOP_CFG\Desktop\InstallManager.exe -f  
\\servename\DESKTOP_CFG\Desktop\AdvancedManager.cfg
```

HINT: To ensure this command is entered accurately, drag the InstallManager.exe file from the Folder window to the DOS command window, type a space, **-f**, and another space, and then drag the AdvancedManager.cfg file from the Folder window to the DOS command window.

10. In the DOS command window, press **Enter**.

The Install Manager program starts and displays the Welcome window.

11. Click **Next**.

The Select Options dialog box appears.

12. Check the Desktop Administrator check box, and then click **Next**.

The Choose Destination Location dialog box appears.

13. Accept the default destination folder, or click **Browse** to navigate to another destination folder, and then click **Next**.

The Start Copying Files dialog box appears.

14. Click **Next** to start the installation.

The Question dialog box appears, asking if you wish to share the existing configuration with other administrators.

15. Click **Yes**.

Installation Manager installs the application you chose.

When the installation is complete, the Install Results dialog box appears.

16. Click **Finish** to complete the installation process.

Configuring Cisco CallManager IP Phones to Work With IP Phone Agent

After all IP agent phones are added to CallManager, you must perform the following tasks in Cisco CallManager Administration:

1. Create an IP phone service.
2. Assign the IP phone service to each IP agent phone.
3. Create a user named “telecaster” and assign to it all the IP agent phones.
4. Change the default URL Authentication parameter.

NOTE: Agent usernames and passwords in CallManager must be in lowercase. If uppercase is used, agents are not able to log into the ICD server when starting the IP Phone Agent service. The allowable characters are those that appear on the IP phone keypad.

Creating an IP Phone Service

From the Cisco CallManager Administration web-based application, follow these steps to create a new IP phone service.

► **To create a new IP phone service:**

1. From the menu at the top of the page, click **Feature > IP Phone Service**.
2. On the Cisco IP Phone Services Configuration page, enter the following information:

Service Name. Enter the service name that will be shown in the IP phone Services window.

Service Description. Optional. Enter a description of the service.

Service URL. Enter the URL for the service. For example:

`http://192.168.252.44:6293/ipphone/jsp/sciphonexml/IPAgentInitial.jsp`

where:

- 192.168.252.44 is the IP address of the machine where the Agent State service is loaded
- 6293 is the Tomcat webserver port (if 6293 is not the port number, check the port parameter in the file `C:\Program Files\wfavid\Tomcat_appadmin\conf\server.xml` for the correct value.)
- `ipphone/jsp/...` is the path to the jsp page under Tomcat on the machine where the Agent State server is loaded (the CRA server)

NOTE: You will not find a file called IPAgentInitial.jsp at this location; there will be a file called IPAgentInitial.class, which contains the implementation of the .jsp file.

NOTE: The Tomcat webserver is included with the ICD installation.

3. Click **Insert** to create the new IP phone service. The new service is now listed in the shaded box at the left of the page.

Assigning the IP Phone Service to IP Agent Phones

Once the IP phone service is created, each agent's phone must be configured to use it.

From the Cisco CallManager Administration web-based application, follow these steps to configure each IP phone.

► **To assign the IP phone service to IP agent phones:**

1. On the Device menu, choose **Phone**.
The Find and List Phones window appears.
2. Use the search function to find the phone. Search results are listed at the bottom of the page.
3. Locate the phone in the list of results and click the red hyperlink.
The Phone Configuration window appears.
4. Click **Subscribe/Unsubscribe Services** in the upper right corner of the window.
A popup window for subscribing to services for that device appears.
5. From the **Select a Service** drop-down list, choose the new service, and then click **Continue**.
A popup window showing the new service appears.
6. Click **Subscribe**.
The new service is listed in the shaded box at the left of the page.
7. Close the popup window.

Creating the “telecaster” User

The next task to accomplish is to create the “telecaster” user.

From the Cisco CallManager Administration web-based application, follow these steps to set up the new user.

► **To create the “telecaster” user:**

1. From the User menu, choose **Add a New User**.

The User Information window appears.

2. Enter the following information.

Entries are case sensitive. Enter them exactly as shown.

First Name telecaster

Last Name telecaster

UserID telecaster

User Password telecaster

PIN 12345

Confirm PIN 12345

3. Check the **Enable CTI Application Use** check box, and then click **Insert**.

4. Click **Device Association** in the shaded box at the left.

The Find and List Phones window appears.

5. Use the search function to locate all phones that are to be associated with the telecaster user. This should be every IP phone that will be used by an IP phone agent.

6. Select the phone(s) from the search results to associate them with the telecaster user, check the **No Primary Extension** check box, and then click **Update** to complete the association.

On the User Information page, the phones you selected are listed by their MAC addresses under Controlled Devices.

7. Continue until all appropriate IP phones are associated.

Changing the Default URL Authentication Parameter

The default URL Authentication parameter can be bypassed to maximize system performance. This prevents the CallManager from polling all devices in the system to authenticate a specific device every time that device pushes information to the CallManager.

1. From the Service menu, choose **Enterprise Parameters**.

The Enterprise Parameters Configuration window appears.

2. Locate the URL Authentication parameter.

3. Change the default value to the following:

`http://CRS Tomcat webserver IP address:6293/ipphone
/jsp/sciphonexml/IPAgentAuthenticate.jsp`

Note: This URL is case sensitive.

Note: Both CRS and CallManager have a Tomcat webserver. Be sure to use the IP address for the CRS Tomcat webserver.

4. Click **Update**.

5. Reset all IP Phone Agent phones by unplugging their power cords, and then plugging them in again.

Configuring Media Termination Phones

From the Cisco CallManager Administration web-based application, follow these steps to configure a Media Termination phone.

1. On the Device menu, choose **Add a New Device**.

The Add a New Device window appears.

2. In the Device Type field, choose **Phone**, and then click **Next**.

The Add a New Phone window appears.

3. From the Phone Type drop-down list, choose **Cisco 30 SP+**, and then click **Next**.

The Phone Configuration window appears.

4. Complete the fields in the Phone Configuration window, and then click **Insert**.

In the MAC Address field, enter the MAC address of the computer on which the Media Termination phone is installed.

The Media Termination phone is inserted into the CallManager database.

NOTE: A Media Termination phone registers with the CallManager only when Agent Desktop is running on the agent PC.

Cisco IP SoftPhone

If the Cisco IP SoftPhone is used as a media termination device, some special steps must be taken in order for silent monitoring and recording to function correctly.

In the Cisco CallManager Administration web page for the SoftPhone CTI port, configure the CTI port Device Name to be **SEP** followed by the MAC address of the SoftPhone PC. The MAC address must be in capital letters.

Using Multiple NICs with the VoIP Monitor Service

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

SpkPCap 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 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.

Installing Cisco Desktop

If a second NIC card is present before installing Cisco Desktop

If the computer on which you are installing the VoIP Monitor service has two NICs before you install the service, follow these steps:

1. During the VoIP Monitor service installation, enter the normal traffic adapter's IP address when prompted for the machine IP address.
2. Enter the sniffing adapter's IP address when prompted for the VoIP Monitor Service.

If a second NIC card is installed after installing Cisco Desktop

If the computer on which you installed the VoIP Monitor service is upgraded to include a second NIC, follow these steps:

1. Open the registry and access the following key:
HKey Local Machine\Software\Microsoft\WindowsNT\
CurrentVersion\NetworkCards
2. Find the newly-inserted card entry.
3. Copy the value in the ServiceName key.

4. Paste this value to the following key:
HKey Local Machine\Software\Spanlink\FastCall VoIP Monitor
Server\Setup\MonitorDevice
5. Add \Device\Splkpc_ at the beginning of the string you pasted in the key.
Be sure to use the correct case when typing this string—it is case sensitive.

NOTE: An alternative to following this procedure is to use the Sniffing Adapter Update utility (UpdateSnifferNIC.exe) that is included on the CAD installation CD. See “Test Programs” in the *Cisco Desktop Product Suite 4.6.0 Service Information Manual* for more information.

Removing Applications

3

Removing Cisco Desktop Product Suite Applications

It is recommended that you remove Cisco Desktop applications in this order:

1. User applications (for example, Agent Desktop, Supervisor Desktop, and Desktop Administrator)
2. Servers
3. Cisco Base

IMPORTANT: Always remove Base last.

► **To remove a Cisco Desktop application:**

1. From the Windows task bar, choose **Start > Settings > Control Panel**.
The Control Panel appears.
2. Double-click **Add/Remove Programs**.
The Add/Remove Properties dialog box appears.
3. Choose the application you wish to remove, and then click **Add/Remove**.
The removal process begins.
4. Follow the instructions in the dialog boxes to remove the application from your computer.

The application is removed. You may be prompted to reboot your computer. It is recommended that you do this in order to completely remove all Cisco Desktop files.

NOTE: You must reboot your computer before reinstalling any Cisco Desktop applications, or remnants of the previous installation may interfere with the new installation.

Removing a VoIP Monitor Server from CRS

If it becomes necessary to remove a VoIP Monitor server installation from the CRS box (for instance, you wish to install it on its own machine for capacity reasons), you must also remove and reinstall Cisco Desktop Administrator.

When the VoIP Monitor server and Cisco Desktop Administrator are on the same box, VoIP installs information in the system registry that Desktop Administrator references. When the VoIP is removed, the uninstallation process removes that registry information, so Desktop Administrator ceases to function. Removing and reinstalling Desktop Administrator restores functionality.

► To uninstall a VoIP Monitor server from CRS:

1. Using the Add/Remove Programs feature in Control Panel, uninstall both the VoIP Monitor server and Cisco Desktop Administrator.
2. Reinstall CRS from the application CD, choosing the **CRA Server** option.
3. Reinstall the VoIP Monitor server in its new location.

Manually Removing Cisco Desktop Applications

It may become necessary to manually remove Cisco Desktop applications. Some reasons for this are:

- The Windows Add/Remove Programs utility does not completely remove a Cisco Desktop application.
- You are unable to upgrade Cisco Desktop applications due to files and settings created in a previous version.

See “Manually Removing Cisco Desktop Applications” in Chapter 5 of the *Service Information* manual for step-by-step instructions.