# Cisco CAD Service Information

CAD 6.5 for Cisco CRS Release 6.0
September 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: 6.5

*Cisco CAD Service Information*

# Contents

# Contents

# Contents

# Contents

# Introduction

# 1

## CAD Documentation

The following documents contain additional information about CAD 6.5:

- *Cisco CAD Installation Guide*
- *Cisco Desktop Administrator User Guide*
- *Cisco Agent Desktop User Guide*
- *Cisco IP Phone Agent User Guide*
- *Cisco Supervisor Desktop User Guide*
- *Cisco CAD Error Code Dictionary*

## CAD 6.5 Applications

CAD 6.5 includes the following applications:

**User Applications**

- Cisco Desktop Administrator (CDA)
- Cisco Agent Desktop (CAD)
- Cisco Supervisor Desktop (CSD)
- Cisco IP Phone Agent (IPPA)

**Services**

- Chat Service
- Directory Services
- Enterprise Service
- IP Phone Agent Service
- LDAP Monitor service
- Licensing & Resource Manager Service
- Recording & Playback Service
- Recording & Statistics Service
- Sync Service
- Voice-Over IP Monitor Service

## Version Information

All CAD applications include version information. This can be obtained by:

- Checking the About dialog box (clicking **Help > About** on desktop application menu bars)
- Right-clicking the application executable and selecting **Properties** from the resulting menu
- Opening *.jar and *.war files with Winzip and locating the Mainifest.mf file, which contains version information

Version information is a series of 4 numbers separated by periods (for example, **6.5.1.15**). From left to right, these represent:

- The major feature version number
- The minor feature version number
- The service level (maintenance) number
- The build number

# Capacity and Performance Guidelines

# 2

## Codecs

The Voice-Over IP Monitor service supports G.711 u-law and a-law and G.729. Conversations using any codec other than G.711 and G.729 will not be available for monitoring. The codec that an IP phone uses is configurable in the Unified CallManager.

## Packet Sniffing and Network Configuration

The monitor service is H.323- and SIP (Standard Interface Protocol)- independent. Both of these protocols use the Real Time Transport Protocol (RTP) to transport voice. The monitor service looks specifically for RTP version 2 packets.

> **NOTE:** The RTP packets must be carried over UDP (User Datagram Protocol), IPv4, and Ethernet II.

As a network switch will not normally deliver packets to Ethernet ports other than the destination (an IP phone, in this case), the switch must be configured to do so. The Ethernet port for the monitor service must be configured to monitor the Ethernet ports for all of the agent IP phones. If the voice packets to and from an agent's IP phone are not sent to the monitor service's port for any reason, that conversation will not be available to the supervisor.

When a request is made to monitor or record an agent, the monitor service looks up the MAC address of the agent's IP phone in the Unified CallManager database. The monitor service then looks for packets to and from this MAC address, and if it is an RTP packet, it is forwarded to Supervisor Desktop (for monitoring) or to the Recording & Playback service (for recording).

It is not enough for the monitor service to monitor a port that all voice traffic goes through, such as the Ethernet port to which a gateway to the PSTN is connected. The monitor service must monitor the Ethernet ports that the IP phones are directly connected to. This is because MAC addresses change as packets pass through OSI Layer 3 devices (e.g. routers).

The monitor service sniffs packets on a single NIC (network interface card), and therefore a single Ethernet port. This port needs to be configured to monitor the Ethernet ports of all agent IP phones. This does not necessarily require that the monitor service and all agent IP phones be connected to the same network switch. That depends on the monitoring capabilities of the network switch.

> **NOTE:** The VoIP Monitor service does not support hubs.

Cisco Catalyst switches use SPAN (switched port analyzer) to monitor ports. Some of the capabilities and restrictions of Catalyst switches are:

### Catalyst 2900XL and 3500XL Switches

- A monitor port cannot be in a Fast EtherChannel or Gigabit EtherChannel port group.
- A monitor port cannot be enabled for port security.

- A monitor port cannot be a multi-VLAN port.
- A monitor 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.
- A monitor port 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

- You can monitor ports belonging to multiple VLANS on these switches.
- The Catalyst 6000 with CatOS 5.3 or higher has a feature called Remote SPAN (RSPAN) which allows you to monitor ports spread over a switched network. With RSPAN on a Catalyst 6000, the monitor service and IP phones can be on separate switches.

For more information on SPAN limitations, see the web document “Configuring the Catalyst Switched Port Analyzer (SPAN) Feature” at:

www.cisco.com/warp/public/473/41.html

# Service Autorecovery

## Fault Tolerance

CAD 6.5 uses the “warm standby” approach to fault tolerance and autorecovery. No manual intervention is required to recover a failed service.

Data and features might be lost at the time of the failure. For instance:

- Active monitoring is stopped. It can be restarted manually after the failover.
- Enterprise data for the call in progress is lost at the time of the failure.

All CAD features are fault-tolerant to a single point of failure with several exceptions. They are:

- Playback. Recordings are tied to a specific service, and thus are not replicated.
- SPAN-based monitoring and recording. Desktop monitoring can be used for CAD agents if fault tolerance is required.

CAD uses LDAP replication to provide fault tolerance for configuration information, such as work flows, agent hot seat settings, and so on. It uses MSDE merge replication to provide fault tolerance for Recording & Statistics service-related data, such as call logs, agent state logs, recording logs, and so on.

A subset of the base services fail over together. These services will either all be active or all be inactive on the same box:

- Chat service
- Enterprise service
- LRM service
- Sync service
- Recording & Statistics service
- IP Phone Agent service

## Agent Desktop and Supervisor Desktop

The service autorecovery feature enables Agent Desktop and Supervisor Desktop to automatically recover their connections to the Cisco Desktop services in the case of a service restart or a network outage.

When Agent Desktop or Supervisor Desktop detects that it is unable to communicate with a service (generally within one minute of the service failure), the application

status bar displays “Partial Service” or “No Service” to indicate some or all of the services have failed.

When Agent Desktop or Supervisor Desktop detects that the service is again available (usually within one minute of service recovery), the status bar displays “In Service” to indicate the services have recovered.

To learn more about what is affected by the service failure, double-click the status message on the status bar. The application displays a popup box that lists the application features and indicates if that feature is available or not due to the service outage.

## IP Phone Agent Service

The IP Phone Agent service pushes an error screen to all the logged in IP phone agents when it detects a failover in Cisco Unified Contact Center Express. During the time it is unable to communicate with Cisco Unified Contact Center Express, any attempt to change agent state or perform other IP Phone Agent functionality returns the service error screen.

If the IP Phone Agent service fails, agents receive no indication of that failure unless they are on the Contact Service Queue (CSQ) Statistics screen. In that case, the agent sees an error message.

Once the IP Phone Agent service is able to reconnect to Cisco Unified Contact Center Express, it pushes either of the following screens to the agent’s phone:

- The Login screen, if the agent in not logged into Cisco Unified Contact Center Express
- The Contact Service Queue (CSQ) Statistics screen, if the agent is still logged into Cisco Unified Contact Center Express

In a redundant system, when the IP Phone Agent service fails the agent must select the other IP Phone Agent service and log in to it manually in order to continue working.

## VoIP Monitor Service

VoIP Monitor service recovery is a special case, since more than one VoIP Monitor service can be installed in a single logical contact center. Supervisor Desktop is notified when one VoIP Monitor service in a multiple VoIP Monitor service configuration goes down. However, agent monitoring is not disabled because it is not possible to tell which agents are monitored by which VoIP Monitor service. The only indication a supervisor receives that a particular agent is assigned to the downed VoIP Monitor service is an error message when attempting to monitor that agent.

**NOTE:** This does not apply to desktops with desktop monitoring enabled.

# Guidelines for Sizing Deployments

Service capacities vary based on the total number of agents in a contact center and whether or not silent monitoring and recording are required.

> NOTE: The following guidelines are based on testing with a combination of real and simulated agents.

## Component Sizing

The Cisco Desktop base services consist of a set of services that run as NT services. The base services include:

- Chat service
- Directory Services
- Enterprise service
- IP Phone Agent service
- LDAP Monitor service
- LRM service
- Recording & Statistics service
- Sync service

There are other services that can be placed on the same or separate computer as the base services. These include:

- Voice-Over IP Monitor service
- Recording & Playback service

A set of the base services plus the additional services is a logical contact center, or LCC.

The maximum number of agents that can be supported by a single LCC is 300 (approximately 4,500 Busy Hour Call Completion [BHCC] with a call volume of 20 calls per agent per hour).

### Recording and Licensing

Recording and playback are licensed features. The number of licenses available is determined by the type of bundle you purchase.

| Bundle Type | Number of Recording and Playback Licenses |
|---|---|
| Standard | 0 |
| Enhanced | 32 |
| Premium | 80 |

A license is used whenever a supervisor or agent triggers the recording function, and is released when the recording is stopped.

A license is also used whenever a supervisor opens the Supervisor Record Viewer, and is released when the Supervisor Record Viewer is closed.

### Voice-Over IP Monitor Service

> **NOTE:** Agent desktops can be monitored at the desktop ("desktop monitoring") as well as by a VoIP Monitor service ("server monitoring"). The following information applies to installations where VoIP Monitor services are used to monitor one or more agents.

The Voice-Over IP (VoIP) Monitor service monitors the RTP streams spanned on the local switch. It uses a SPAN port to sniff each RTP stream that might potentially be monitored by a supervisor. All streams are monitored all the time. The maximum number of simultaneously monitored sessions (the total number of supervisors actively monitoring agents plus the number of concurrent recording sessions) is 40 (80 RTP streams).

The VoIP Monitor service application must be at the same physical location as the agents it monitors. A physical location is defined as a set of interconnected switches with no intervening routers or hubs. Deployments with agents at multiple sites must provision for a VoIP Monitor service application at each site.

The VoIP Monitor service application is certified for both uni-processor and multi-processor machines.

The VoIP Monitor service application is sized based on a combination of active calls and total streams being monitored by the service. For example, if the percentage of time that agents are actually talking is low, more streams may be monitored. If agents are on the phone most of the time, fewer streams may be monitored.

The number of sessions monitored by supervisors is fixed at 40 total simultaneous sessions.

### Desktop Monitoring

Desktop monitoring requires more bandwidth of a CAD instance than does server monitoring (using a VoIP Monitor service). Please refer to the best practices document, *Cisco Agent Desktop Bandwidth Requirements*, for more information.

There is no limit to the number of agents who can use desktop monitoring—all the agents in a LCC may use desktop monitoring.

### Recording & Playback Service

The Recording and Playback Service stores recorded conversations and makes them available to the Supervisor Record Viewer application.

A co-resident Recording & Playback service can support up to 32 simultaneous recordings. A dedicated Recording & Playback service can support up to 80 simultaneous recordings (this option is available in the Premium version only). The capacity of the Recording & Playback service is not dependent on the CODEC used.

**Example**

Assumptions:

- 10-hour working day
- 20 calls per agent per hour (average handle time [AHT] 180 seconds: 120 seconds per call with a 60-second wrapup)
- 8% of calls, or 16 call per agent per day, are recorded
- Service level of 90% of calls answered in 10 seconds
- Agent:supervisor ratio is 10:1

Agent resources are calculated using an Erlang C computation.

Recording resources are calculated using the above assumptions and an Erlang B computation, assuming 0.001 blockage. In the case of recording, there will not be actual blockage, instead, an additional recording resource will be used.

A formula for simultaneous recording resources needed in the busy hour based on percentage of calls monitored can be calculated as follows:

(BHCC = busy hour call completion)

$$\left(\frac{\text{BHCC}}{\text{hour}}\right) \times (\%\ \text{Recorded}) \times \left(\frac{2\ \text{min}}{\text{call}}\right) \times \left(\frac{1\ \text{hour}}{60\ \text{min}}\right) = \text{req sim recording resources}$$

$$\frac{\text{BHCC} \times \% \text{ Recorded}}{30} = \text{required simultaneous recording resources}$$

In a contact center with 1000 calls per hour and an 8% call recording rate, the recording Erlang is:

$$\frac{1000 \times 0.08}{30} = 2.667$$

Using an Erlang B calculator with 0.001 blocking, this contact center requires no more than 10 simultaneous recording resources.

The following table summarizes the number of agents and simultaneous recording resources required for BHCC values from 1,000–4,000 with an 8% call recording rate.

| BHCC | No. Agents | No. Supervisors | Simultaneous Recording Resources Required |
|---|---|---|---|
| 1,000 | 59 | 6 | 10 |
| 2,000 | 112 | 11 | 14 |
| 4,000 | 215 | 22 | 22 |

## Coresidency Options

The base services are coresident on a CRS server.

| No. Agents | Base services plus Recording & Playback service | VoIP Monitor Service |
|---|---|---|
| up to 100 | coresident on CRS server | coresident on CRS server |
| 101–300 | coresident on CRS server | dedicated server |

# Technical Package Information

# 3

## Service Connection Types and Port Numbers

Consult the *Cisco CRS (IP IVR and IPCC Express) Port Utilization Guide* for a complete listing of ports and connection types used in CAD 6.5.

# Registry Entries

## Site Setup

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Site Setup

**Table 1. Site setup registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Site Setup | Install Directory | string | Base install directory for Cisco software |
| | IOR Hostname | string | Hostname or IP address of Cisco services |
| | LDAP Bind DN | string | User ID used to log in to the LDAP service. Default = cn=Cient, ou=People, o=Spanlink Communications. |
| | LDAP Connection Timeout | dword | Maximum time, in seconds, before a connection attempt times out. Default = 15. |
| | LDAP Heartbeat Enabled | dword | Is heartbeat enabled? 1=yes, 0=no. Default = 1. |
| | LDAP Heartbeat Retry Time | dword | Heartbeat time, in milliseconds. Default = 10000. |
| | LDAP Host 1 | string | LDAP service hostname/IP address. There can be multiple LDAP hosts. |
| | LDAP LCC | string | Default logical contact center |
| | LDAP Port 1 | dword | LDAP service port. There can be multiple LDAP ports. Default = 38983. |
| | LDAP Pwd | string | Encrypted user password |
| | LDAP Recovery Retry Time | dword | Recovery retry time, in milliseconds. Default = 3000. |
| | LDAP Request Timeout | dword | Maximum time, in seconds, before an LDAP request times out. Default = 15. |

Table 1. Site setup registry entries — *Continued — Continued*

| Key | Value | Type | Description |
|---|---|---|---|
| | LDAP Root | string | Root of the LDAP data. Default = o=Spanlink Communications. |
| | Serial Number | string | Counter to indicate changes to site setup values. Default = 0. |
| | CALLCENTERLANG | string | Language selected during installation. |
| | INSTALLDIR | string | Parent directory of base install directory for Cisco software. |
| | MONITOR DEVICE | string | Network card on which to sniff packets. |

## Agent Desktop

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Agent\

Table 2. Agent Desktop registry entries

| Key | Value | Type | Description |
|---|---|---|---|
| Config | App Version | string | Used by installation scripts to identify the version of the service software. The service itself does not use this entry |
| | Update Version | string | Future use: tracks any hot fixes installed |
| | Shortcut icon path | string | Location of the start shortcut under StartMenu > Programs |
| | Type | string | Type of telephony switch the system is running under |

Table 2. Agent Desktop registry entries — *Continued*

| Key | Value | Type | Description |
|---|---|---|---|
| Desktop Monitoring | IOR Hostname | string | Host name or IP address of the agent's desktop. Reserved for future use. |
| | Monitor Device | string | NIC adaptor used by the WinPcap software to sniff VoIP traffic for monitoring and recording agent calls. It is set automatically at installation to the first available adaptor found that can be used by the WinPcap driver. |
| | OmniOrbUsePort | unsigned long | Port that the desktop monitor process listens on for CORBA calls from clients. Default = 59002. |
| | VpnUsePort | unsigned long | Port used to communicate with a VPN server located on the same machine as a VoIP Monitor service. If none found, uses the default value defined in fcvmsTypes.h. |

## Enterprise Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Enterprise Server\

**Table 3. Enterprise Service registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Setup | Max Wait Time* | dword | Maximum time, in milliseconds, to wait for enterprise data. Default = 100. |
| | Initial Time* | dword | Number of milliseconds to wait after the first request for enterprise data, if data is not guaranteed. Default = 10. |
| | Increment* | dword | Number of milliseconds to add to the retry time at each interval, if data is not guaranteed. Default = 20. |
| | Retry Sleep Interval* | dword | Number of milliseconds used to calculate the interval for retry attempts, if call is not known to enterprise. The interval is calculated by (retry sleep interval × retry attempt). Default = 150. |

* These registry keys need to be created only if there are timing issues when an agent requests data from the Enterprise service and the Enterprise service does not have the data yet.

## IP Phone Agent Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\IPPA\

**Table 4. IP Phone Agent service registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Config | TOMCAT HOME | string | Location of the Tomcat web server files. Default = C:\Program Files\wfavvid\tomcat_appadmin\ |

## LRM Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\LRM Server\

**Table 5. LRM Service registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Config | App Version | string | Used by installation scripts to identify the version of the service software. The service itself does not use this entry. |
| | Update Version | string | Future use: tracks any hot fixes installed |

## Recording & Playback Client

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Recording & Playback Client\

**Table 6. Recording & Playback Client registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Setup | Jitter Buffer | dword | The amount of voice data to buffer before playing. Default value = 1000 ms. On a typical internal network, this value can be set as low as 50 ms. The default is set higher so that the sound quality is good even on a congested network. |
| | From Client Port | dword | |
| | Port Range End | dword | |
| | Port Range Start | dword | |
| | Sound Buffers | dword | |
| | To Client Port | dword | |
| | VPN Port | dword | |

## Recording & Playback Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Recording & Playback Server\

**Table 7. Recording & Playback Service registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Config | Update Version | string | Future use: tracks any hot fixes installed |
| | Audio Directory | string | |
| | IOR HostName | string | |
| | Maximum Playback | dword | |
| | Maximum Recordings | dword | |
| | OmniOrbUsePort | dword | |

## Recording & Statistics Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\RASCAL Server\

**Table 8. Recording & Statistics service registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Config | DB Script Message | string | Error message used by technical support for troubleshooting. |
| | DB Script Result | string | The Boolean result returned after running the Recording and Statistics service set up script. 1 = Completed successfully. 0 = error. |

## Supervisor Desktop

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Supervisor\

**Table 9. Supervisor Desktop registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Config | App Version | string | Used by installation scripts to identify the version of the service software. The service itself does not use this entry |
| | Update Version | string | Future use: tracks any hot fixes installed |
| | Shortcut Icon Path | string | Location of the start shortcut under StartMenu > Programs |
| | Type | string | Type of telephony switch the system is running under |

## Sync Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Sync Server\

**Table 10. Sync service registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Config | Update Version | string | Future use: tracks any hot fixes installed |

## Voice-Over IP Monitor Client

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\VoIP Monitor Client\

Table 11. Voice-Over IP Monitor Client registry entries

| Key | Value | Type | Description |
|---|---|---|---|
| Config | FROM AGENT PORT | dword | IP port for RTP stream being sent from IP agent. Default value = 59012. Port must be an even number. The next port is reserved for RTCP stream. |
| | JITTER BUFFER | dword | The amount of voice data to buffer before playing. Default value = 400 ms. On a typical internal network this value can be set as low as 50 ms. The default is set higher so the sound quality is good even on a congested network. |
| | SERVER HOST | string | Host name of the VoIP service. |
| | SOUND BUFFERS | dword | Number of sound card buffers. Default = 30; minimum is 3. If the monitor sound quality is choppy, stuttering, or like a motorboat you might be able to make it sound better by adjusting this value higher. Setting the value higher increases the sound lag, and might cause a slight stutter at the beginning of a monitor session. |
| | TO AGENT PORT | dword | IP port for RTP stream being sent to Agent IP Phone. Default value = 59010. The port must be an even number. The next port is reserved for RTCP stream. |

## Voice-Over IP Monitor Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\VoIP Monitor Server\

Table 12. Voice-Over IP Monitor Service registry entries

| Key | Value | Type | Description |
|---|---|---|---|
| Config | App Version | string | Used by installation scripts to identify the version of the service software. The service itself does not use this entry |
| | Update Version | string | Future use: tracks any hot fixes installed |
| | Monitor Device | string | Network card on which to sniff packets |

## Voice-Over IP Monitor Record Client (Optional)

These registry entries should not be needed because the Voice-Over IP Monitor Record API has built-in defaults. They can be used to override the defaults.

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\VoIP Monitor Client

Table 13. Voice-Over IP Monitor Record Client registry entries

| Key | Value | Type | Description |
|---|---|---|---|
| Setup | Recording Jitter Buffer | dword | The number of milliseconds that a packet expires for recording. |
| | Recording Port Range Start | dword | The starting port number for receiving UDP packets for recording. |
| | Recording Port Range End | dword | The end port number for receiving UDP packets for recording. |

# Logs and Debugging

# 4

## Event/Error Logs

Logs are listings of CAD events and errors.

Events may represent the following:

- Actions taken by a Desktop application
- Implications of user-defined configuration settings
- Limitations of the hardware

Error codes are brief descriptions of system events.

Error and event logging is always enabled. The log files are limited to a default of 3 MB. (You may change the limit in the application's configuration file. When a log file reaches that size, it is closed and a new file is started.

The files are numbered, up to the total number of files set in the configuration file (the default number is 2). For example:

- agent0001.log
- agent0002.log

When agent0001.log reaches its size limit, it is closed and agent0002.log is created. When the total number of log files have been created, the first log file is overwritten.

IPPA JSP client log files are numbered, up to the total number of files set in the configuration file. The file without an appended number is the current file, and the file with the highest number is the oldest. For example:

- TIAJ.log
- TIAJ.log.1
- TIAJ.log.2

CAD generates the following error and event logs:

**Table 14. CAD Event/error logs**

| Log Name | Records Events and Errors In: |
|---|---|
| administrator.log | Desktop Administrator–Desktop Configuration module |
| agent.log | Agent Desktop |
| CDBRTool.log | Backup and Restore utility |
| CTI Storage Server.log | Enterprise service |
| db.cra_repl_add.sql.log | Recording & Statistics service |
| db.cra_repl_base.fcrassvr.sql.log | Recording & Statistics service |
| db.cra_utils_base.fcrassvr.sql.log | Recording & Statistics service |
| db.createdbadmin.sql.log | Recording & Statistics service |
| db.instrasdb.fcrassvr.sql.log | Recording & Statistics service |
| db.lockdown.sql.log | Recording & Statistics service |
| db.memcap.sql.log | Recording & Statistics service |
| db.splk_repl_base.sql.log | Recording & Statistics service |
| DirAccessSynSvr.log | Sync service |
| FCCServer.log | Chat service |
| FCRasSvr.log | Recording & Statistics service |
| fcuninstall.log | CAD uninstall process |
| FCVoIPMonSvr.log | Voice-Over IP Monitor service |
| IPCCAdm.log | Desktop Administrator–IPCC Configuration module |
| IPPASvr.log | IP Phone Agent service |
| LDAPMonSvr.log | LDAP Monitor service |
| LRMServer.log | LRM service |
| Personnel.log | Desktop Administrator–Personnel Configuration module |
| PostInstall.log | CAD Configuration Setup |
| RPServer.log | Recording & Playback service |

**Table 14. CAD Event/error logs — *Continued***

| Log Name | Records Events and Errors In: |
|---|---|
| slapd.log | Directory Services service |
| slurpd.log | Directory Services replication service |
| Splkview.log | Desktop Administrator–framework |
| supervisor.log | Supervisor Desktop and Supervisor Record Viewer |
| SWFAdmin.log | Supervisor Workflow Administrator |
| TIAJ.log | IP Phone Agent service JSP client |
| TSSPAdm.log | Desktop Administrator–Enterprise Data Configuration module |
| WorkflowEngine.log | Enterprise service |

# Debugging

## Debugging Logs

CAD can create debugging logs, although by default this capability is disabled. If you want debugging turned on, you must edit the appropriate configuration file.

Debugging information is written to the various debug files, all of which have a ***.dbg** suffix. These files are located in the ...\Cisco\Desktop\log directory.

The debug files are numbered, up to the total number of files set in the configuration file (the default number is 2). For example:

- agent0001.dbg
- agent0002.dbg

When agent0001.dbg reaches its size limit, it is closed and agent0002.dbg is created. When the total number of debug files have been created, the first debug file is overwritten.

***To turn on debugging:***

1. Open the appropriate configuration file.
2. Under the section headed [Debug Log], set the debugging threshold to an appropriate value. For example:

   THRESHOLD=DEBUG
3. Save the configuration file with the new setting.

## Debugging Thresholds

When setting the debugging threshold, keep in mind that the more detail the threshold provides, the slower the performance of your PC and increases the size of the debug file.

> **NOTE:** There is a high probability of server crash if higher levels of debugging are set and left to run for an extended period (for example, TRACE or DUMP for 24 hours).

The available debugging thresholds are:

Table 15. Debugging Thresholds

| Threshold | Records: |
|---|---|
| Debug | • Minor and frequently-occurring normal events. This level is usually sufficient for debugging a problem, and will not affect the computer's performance. |
| Call | • Minor and frequently-occurring normal events<br>• Entering and exiting functions |
| Trace | • Minor and frequently-occurring normal events<br>• Entering and exiting functions<br>• Detail debugging (for instance, loops) |
| Dump | • Minor and frequently-occurring normal events<br>• Entering and exiting functions<br>• Detail debugging (for instance, loops)<br>• Byte dumps |
| Off | Turns off debugging. This is the default setting. |

## Debugging for the IP Phone Agent Client

The Cisco IP Phone Agent Client is a JSP application with its own debug methods. The configuration file that controls debugging does not follow the CAD standard debugging thresholds.

The configuration file is located on the computer where the CAD services are installed, at:

C:\Program Files\wfavvid\tomcat_appadmin\conf\TIAJ.cfg

***To turn on debugging:***

1. Open the TIAJ.cfg file in a text editor.
2. Locate the line:

   log4j.rootLogger=info, R
3. Replace **info** with **debug**.
4. Save the configuration file with the new setting.

## Configuration Files

The following configuration files can be edited to turn on threshold debugging:

**Table 16. CAD configuration files**

| Application/Service | Configuration File |
|---|---|
| Backup and Restore utility | CDBRTool.cfg |
| IP Phone Agent Service | IPPASvr.cfg |
| Chat Service | FCCServer.cfg |
| Cisco Agent Desktop | agent.ini |
| Cisco Desktop Administrator<br>Framework module<br>Enterprise Data Configuration module<br>IPCC Configuration module<br>Personnel Configuration module | admin.ini<br>SplkView.cfg<br>TSSPAdm.cfg<br>IPCCAdm.cfg<br>personnel.cfg |
| Cisco Supervisor Desktop | supervisor.ini |
| Directory Services | slapd.cfg |
| Directory Services Replication | slurpd.cfg |
| Enterprise Service | ssCTIConfig.cfg |
| IP Phone Agent client<br>File is located under C:\Program Files\wfavvid\tomcat_appadmin\conf\ | TIAJ.cfg |
| Cisco Desktop LDAP Monitor service | LDAPMonSvr.cfg |
| LRM Service | LRMServer.cfg |
| Recording & Playback Service | RPServer.cfg |
| Recording & Statistics Service | FCRasSvr.cfg |
| Supervisor Record Viewer | supervisorlogviewer.ini |
| Supervisor Workflow Administrator | SWFAdmin.ini |
| Sync Service | DirAccessSynSvr.cfg |
| VoIP Monitor Service | FCVoIPMonSvr.cfg |

# Troubleshooting

# 5

## Converting Recordings From *.raw to *.wav Format

Recordings made by supervisors are archived as raw voice data packets; they can only be reviewed using the Supervisor Record Viewer. However, if you wish to permanently save selected recordings as .wav files, you can use either of two methods:

- Using the “Play and Save” button in Supervisor Record Viewer and saving the recording to a selected folder
- Using the CRSraw2wav.exe command line utility

See the *Cisco Supervisor Desktop User’s Guide* for information on saving recordings as .wav files through Supervisor Record Viewer.

### Using the CRSraw2wav Utility

This utility is located in the C:\Program Files\Cisco\Desktop\bin folder. It must be run from this location in a command window on the computer that hosts the Recording & Playback service (RPServer.exe).

Each .raw format recording is comprised of 2 files:

- <name>.to.raw, containing data sent to the agent phone
- <name>.from.raw, containing data sent from the agent phone

You need use only one of the file pair when running the utility. The utility finds the other file and combines the two files into one .wav file named <name>.wav.

The naming convention used for <name> is as follows:

<YYYYMMDD>_<HHMMSS>_<counter>_<extension>_<agent ID>

Where

<YYYYMMDD>Date the file was recorded

<HHMMSS>Time the file was recorded

<counter>Counter that is reset every time the agent logs in. It is incremented sequentially starting from 00000 every time a recording of that agent is made during that session.

<extension>The extension of the agent recorded

<agent ID>The ID of the agent recorded

The utility finds the location of the .raw files from the registry. If this information is not in the registry it assumes that the location is C:\Program Files\Cisco\Desktop_Audio. The utility writes the converted .wav files to a folder it creates located at C:\Program Files\Cisco\Desktop_wav.

The utility syntax is:

```
CRSraw2wav.exe <filename>
```

where <filename> is either the <name>.to.raw or <name>.from.raw file.

## Running CRSraw2wav in a Batch File

You can use the CRSraw2wav utility from a batch file that iterates through a wildcard-specified set of source files.

If the utility finds a .wav file with a name identical to one that is about to be created, the conversion is not executed.

> **NOTE:** If the utility is halted prematurely, the .wav file being written at that time may be corrupted.

A batch file is a text file with a *.bat extension. You can put DOS commands into this file and then run the file as if it were an executable.

For example, the following series of DOS commands can be put into a batch file called **convert.bat**:

```
c:\
cd c:\program files\cisco\desktop\bin
for %%c in (..\..\desktop_audio\*.raw) do crsraw2wav
"%%~nc%%~xc"
```

These DOS commands cause all the *.raw files in the C:\Program Files\Cisco\Desktop_audio folder to be converted to *.wav format and placed in the

C:\Program files\Cisco\Desktop_wav folder, leaving the original *.raw files in the Desktop_audio folder.

Additional lines can be added to the batch file to copy the files to another folder or file server.

> **NOTE:** The utility has a feature that prevents it from reconverting files that are already present in the Desktop_wav directory, so the batch file does not have to explicitly check to see if the files have already been converted.

If you want the batch file to run automatically on specific days at a specific time, the Windows “at” command can be used.

For example, if you want convert.bat to run automatically every 13th and 23rd day of the month at 1:46 pm, do the following:

1. Put convert.bat in the C:\Program Files\Cisco\Desktop\bin folder.
2. Open a command window and enter the following DOS command:

```
at 1:46p /every:13,23 cmd /c "c:\program
files\cisco\desktop\bin\convert.bat" ^>
c:\splkconvert.txt
```

# Recovering the Directory Services Database

## Corrupted Directory Services Database

If the Directory Services database becomes corrupted, follow these steps.

***To recover the Directory Services database (Method 1):***

1. On the PC hosting the database, stop the Cisco Desktop LDAP Monitor Service.
2. Open a command window.
3. Change directories to ...Cisco\Desktop\bin (the drive and exact location of this directory depends on where the services were installed).
4. In the ...Cisco\Desktop\bin directory, type the command:

   db_recover -h ../database -v

   and press **Enter**.
5. Type **exit** and press **Enter** to close the DOS window.
6. Restart the Cisco Desktop LDAP Monitor Service.

If this procedure does not work, follow these steps.

***To recover the Directory Services database (Method 2):***

1. On the PC hosting the database, stop the Cisco Desktop LDAP Monitor Service.
2. Open a command window.
3. Change directories to ...Cisco\Desktop\bin (the drive and exact location of this directory depends on where the services were installed).
4. In the ...Cisco\Desktop\bin directory, type the command:

   slapcat -f slapd.conf -l backup.ldif -c

   and press **Enter**.
5. Rename the existing folder ...Cisco\Desktop\database to ...Cisco\Desktop\old_database.
6. Create a new folder called Cisco\Desktop\database.
7. Copy DB_CONFIG and all files with a .dat extension from the **old_database** folder to the **database** folder.
8. In the database folder, create an empty file called **rep.log**.
9. Open a command window.

10. Change directories to ...Cisco\Desktop\bin (the drive and exact location of this directory depends on where the services were installed).
11. In the ...Cisco\Desktop\bin directory, type the command:

    slapadd -f slapd.conf -l backup.ldif -c

    and press **Enter**.
12. Type **exit** and press **Enter** to close the DOS window.
13. Restart the Cisco Desktop LDAP Monitor Service.

## Out of Sync Directory Services Databases

The secondary Directory Services database can become out of sync with the primary Directory Services database. A possible reason for this to occur is that the secondary database was reinstalled.

Follow these steps to sync up the two databases:

1. On the PC hosting the primary database, stop the Cisco Desktop LDAP Monitor service.

   The secondary LDAP can be down at this time.
2. Remove all contents from the files repl.log and repl.log.lock from the ...\Cisco\Desktop\database folder.
3. Delete all files in the ...\Cisco\Desktop\run\logs\replica, ...\Cisco\Desktop\logs\replica, and ...\Cisco\Desktop\logs\ReplLogs folders.
4. Open a command window on the primary database computer.
5. Change folders to ...\Cisco\Desktop\bin (the drive and exact location of this folder depends on where the service was installed).
6. In the ...\Cisco\Desktop\bin folder, type the command:

   slapcat -f slapd.conf -l backup.ldif -c

   and press **Enter**.

   A file called **backup.ldif** is generated.
7. Copy the backup.ldif file to the computer on which the secondary LDAP service is installed, into the ...\Cisco\Desktop\bin folder.
8. On the PC hosting the secondary database, stop the Cisco Desktop LDAP Monitor service if is not already stopped.
9. Remove all contents from the files repl.log and repl.log.lock from the ...\Cisco\Desktop\database folder.
10. Delete all files in the ...\Cisco\Desktop\run\logs\replica, ...\Cisco\Desktop\logs\replica, and ...\Cisco\Desktop\logs\ReplLogs folders.

11. To remove the secondary LDAP database, delete all files except the following files from the ...\Cisco \Desktop\database folder:
    - files with a .dat suffix
    - DB_CONFIG
12. Open a command window on the secondary database computer.
13. Change folders to ...\Cisco\Desktop\bin (the drive and exact location of this folder depends on where the service was installed).
14. In the ...\Cisco\Desktop\bin folder, type the command:

    slapadd -f slapd.conf -l backup.ldif -c

    and press **Enter**.
15. Type **exit** and press **Enter** to close the DOS window.
16. Restart the Cisco Desktop LDAP Monitor service on the secondary computer.
17. Restart the Cisco Desktop LDAP Monitor service on the primary computer.

# Diagnostic Procedures

## Basic Checks

When CAD has problems, check that:

- The computers that host CAD services, Unified Unified CallManager, CRS, and other system components are running.
- The registry is correct (see "Registry Check" on page 43).
- The network is set up correctly (see "Network Check" on page 43).
- The CAD services are running and active (see "Active Service Check" on page 43).
- The CAD Configuration Setup utility has run correctly. See the *CAD Installation Guide* for more information.

## Active Service Check

This applies only to the following services: LRM, Chat, Enterprise, Recording & Statistics, IP Phone Agent, and Sync.

### For Nonredundant Systems

- Check the service's log file for a statement that the service is active.

### For Redundant Systems

- Check the service's log file for a statement that the service is active.
- Only one instance of each service should be active at the same time. The other instance should be in standby mode.

## Registry Check

Using Windows Regedit:

- Verify that HKEY_LOCAL_MACHINE\Software\Spanlink\CAD\Site Setup exists and contains the entries specified in "Site Setup" on page 22.
- Verify that the registry entries used by specific services exist and are valid. See "Registry Entries" on page 22.

## Network Check

- On the CAD services computer, verify that the IP address in the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Site Setup\IOR HOSTNAME is the correct IP address of the public NIC.

- To view information about the NICs on the computer, open a command window and type **ipconfig /all**.
- Verify that the hostname and IP address are as expected.
- Verify that the subnet mask is correct. It is probably **255.255.255.0.**
- If there are multiple NICs enabled, verify that the public NIC comes before the private NIC:
  1. In the Control Panel, double-click **Network and Dial-up Connections**.
  2. From the menu bar, choose **Advanced > Advanced Settings**.
  3. On the Adapters and Bindings tab, verify that the NICs are in the correct order in the **Connections** pane.
- Check the network connectivity by pinging from the CAD services computer to others in the configuration, for example, the Unified CallManager computer. Then reverse it by pinging from the other computers to the CAD services computer. Do this using both hostnames and IP addresses and ensure that the ping results match.
- If hostnames are used, verify that the appropriate DNS, WINS, and hosts files are correct.
- If there is a problem connecting to a particular service, try typing **telnet <IP address/hostname> <port>** in a command window, where <IP address/hostname> is the IP address or host name of the computer where the service is running and <port> is the port used by the service.
- Use a network protocol analyzer like Ethereal (www.ethereal.com) to analyze network communications.

## Memory Check

- Ensure that the amount of memory on the computer is at least the minimum required for CAD and other installed software. If the amount of memory is below the recommended level, it could be the source of the problem.
- Use Microsoft Perfmon (perfmon.exe) to perform most memory checking.
  - Add the following counters for _Total and process of interest:
    - Private Bytes
    - Virtual Bytes
    - Handle Count
    - Thread Count

    If the values for those counters keep growing without leveling or decreasing, it is likely the process has a memory leak.

If the values for those counters for a process are a significant part of the total memory used, it may be of concern. Note that certain processes will normally use more memory than others.

- Try rebooting the computer and see if it fixes the problem. Check how much and how fast processes increase their memory usage.

## CPU Check

- Ensure that the computer's processor is at least the minimum required for CAD and other installed software. If the processor is below the recommended level, it could be the cause of the problem.
- Use Task Manager to sort processes/applications by CPU usage. Check which process seems to be using the CPU most of the time.
- Use Windows Perfmon (perfmon.exe) for additional CPU checking.
  - Add the %Processor Time counter for Processor > _Total and each CPU as well as Process >_Total and process of interest.
  - Check which process seems to be using the CPU most of the time.
  - If the counter values for a process are a significant part of the total CPU use, it may be of concern. Short spikes are acceptable but a significant time with high CPU usage is of concern.
- Try rebooting the computer to see if it fixes the problem.

## Blocked Ports Check

To check whether a port is blocked:

- Using telnet:
  1. Ensure that the service is running and active.
  2. From the command line, type **telnet <hostname/IP address> <port>** and press **Enter**, where <hostname/IP address> is the hostname or IP address of the service computer and <port> is the port the service is listening on.
  3. If it is successful, the command window will clear with cursor at top left corner; you will need to close the window.
  4. If the telnet fails, you will probably see a connection failure.
- Check firewall settings on the client and server computers.
- Check firewall logs.

## CAD Service Problems

**Problem** How can I tell if a CAD service is running?

**Solution** To view the status of all the services in the CAD system, log into Cisco Response Solutions Administration. Select **System** > **Control Center**. Then select the server where the CAD services are located.

CAD services are now visible on the right panel. You can view their running status, and whether they are in an active (M) or standby (S) state.

**Problem** How can I check if the CRS services are running?

**Solution** Log into Cisco Response Solutions Administration. Select **System** > **Control Center**. Then select the server where CRS services are located.

CRS services are now visible on the right panel. You can view their running status, and whether they are in an active (M) or standby (S) state.

**Problem** When the user attempts to start Enterprise Service, the following error displays:

> "Could not start the Cisco Desktop Enterprise Service on *Computer*
>
> Error 2140: An internal Windows error occurred."

**Solution** Look at the Windows event log to see why the Service failed to start.

1. Click **Start > Programs > Administrative Tools > Event Viewer**.
2. On the **Log** menu, click **Application**.
3. Select a message that displays **Enterprise Server** as the source. This should provide more information on the cause of the failure.

**Problem** No screen pops appear when the user makes calls to and from devices.

**Solution** Try the following:

- Check to see if CTI Server is running.
- Check to see if an agent is logged in to the device.
- Check if the device is configured in Unified CallManager.

**Problem** Enterprise data does not pop on the IP Phone Agent's IP phone when the phone rings or when it is answered.

**Solution** Verify that:

- the phone is associated with the **telecaster** user in Unified CallManager.
- the authentication URL set up in Unified CallManager uses an IP address instead of a hostname.
- the agent is logged into the phone.
- if the agent logs into Cisco Agent Desktop using the same phone and user ID, enterprise data does pops correctly.
- the user **telecaster** exists in Unified CallManager and uses the password **telecaster**.
- Log the agent out, unplug the phone, and then plug it back in. This ensures there is a hard reset. This might be necessary if the phone previously pointed to a different Unified CallManager.

**Problem** When trying to view agent state or call logs, no data is presented.

**Solution** The agent may not have received a call, or logged in for that particular day. The agent's or supervisor's PC's clock may not be in the correct time zone.

**NOTE:** All state and call times are based on server time.

**Problem** When monitoring an agent's customer contact, nothing can be heard, and after 15 seconds, an error message is received that no packets are

being received. Attempting to record an agent's customer contact results in an empty recording. The agent's desktop is monitored using desktop monitoring.

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

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

In the Product Specific Configuration section of the Device Configuration screen, 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 screen, 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.

You must also configure the agent phones to use the G.711 or G.729 Codecs. Other Codecs, such as G.722, are not supported for silent monitoring and recording.

---

**Problem** The CPU usage on the VoIP Monitor service PC has gone to 99%, and the PC has locked up.

**Solution** This can happen when you disable the sniffing adapter through the Windows Network and Dialup Connections window while the VoIP Monitor service is running. Re-enabling the sniffer adapter while the VoIP Monitor service is running will not solve the problem. You must

stop the VoIP Monitor service, re-enable the sniffer adapter, and then restart the VoIP Monitor service to restore normal functionality.

**Problem** The message, "At least one or more errors occurred during synchronization" appeared when the administrator performed synchronization in Desktop Administrator.

**Solution** Check the Sync service log file.

- If the logged error points to a problem with the Acmi connection, look for problems with the CTI Server. Also look for similar problems in the Enterprise Server logs.
- If the logged error points to an LDAP error, make sure the LDAP service is running and the LDAP Host 1 registry setting in the following location has the correct value:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Site Setup`

**Problem** Voice traffic generated by Desktop Monitoring, the VoIP Monitor Service, and the Recording Playback Service is not tagged for QoS (quality of service).

**Solution** Winsock QoS is disabled for Windows XP and Server 2000/2003 by default, and must be enabled through the Windows registry.

Follow these steps to enable the QoS Setting for VoIP Services on Windows 2000, Windows XP, or Windows Server 2003:

If you are running Windows 2000:

1. In the Registry Editor, access the key

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpIp\Parameters
2. On the Edit menu, click **Add Value**.
3. In the Value name box, type **DisableUserTOSSetting**.
4. In the Data Type list, click **REG_DWORD**, and then click **OK**.
5. In the Data box, type a value of **0** (zero), and then click **OK**.

If you are running Windows XP or Windows Server 2003:

1. In the Registry Editor, access the key

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\TcpIp\Parameters

2. On the Edit menu, point to **New**, and then click **DWORD Value**.
3. Type **DisableUserTOSSetting** as the entry name, and then press **Enter**.

   When you add this entry, the value is set to 0 (zero). Do not change the value.
4. Quit Registry Editor, and then restart the computer.

---

**Problem** How can I tell if the Tomcat webserver is installed correctly?

**Solution** Perform the following tests:

- Log into Cisco Response Solutions Administration. Select **System** > **Control Center**. Then select the server where CRS services are located. Verify that the CRS Administration is running.
- On the PC where the IP Phone Agent service is installed, check Services in the Control Panel to see if the IP Phone Agent service is running.
- Attempt to display the following page in your web browser without an error: http:*//IP address of the machine where Tomcat is installed*:6293/ipphone/jsp/sciphonexml/IPAgentInitial.jsp

If these tests fail, check the following:

- JRE is installed on your PC.
- The file that maps URLs with JSP pages to the correct java servlets, web.xml, must be in the C:\Program Files\wfavvid\tomcat_appadmin\webapps\ipphone\web-inf directory.
- This entry must be set in the registry: HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\IPPA\Config\TOMCAT HOME = C:\Program Files\wfavvid\tomcat_appadmin\

---

**Problem** slapd.exe is not running even though the Cisco Desktop LDAP Monitor service is running.

**Solution** Do the following:

- Check slapd.conf to ensure it is correct.
- Make sure no other instances of slapd.exe are running.
- Make sure the ...\Cisco\Desktop\database folder contains 7 files with a *.dat extension and DB_CONFIG. If these are missing, copy them from another system or reinstall the CAD services.
- Make sure the ...\Cisco\Desktop\database folder contains log.*, __db.* and 8 files with a *.bdb extension. If not, follow the procedure in "Out of Sync Directory Services Databases" on page 41, copying from the one that works to the one that does not. Otherwise, you will need to reinstall the CAD services.
- Get more information about why slapd.exe cannot start:

1. Stop the Cisco Desktop LDAP Monitor service.
2. Open a DOS command window and navigate to the ...\Cisco\Desktop\bin folder.
3. Enter **slapd.exe -f slapd.conf** and press **Enter**.
4. If it aborts, use the resulting error messages to diagnose the problem.
5. If it runs successfully, type **Ctrl-C** to end it.
6. Check the Cisco Desktop LDAP Monitor service configuration file to make sure it is starting slapd.exe correctly.

**Problem** Clients are unable to connect to the LDAP service.

**Solution** Some solutions:

- The wrong IP addresses are set for LDAP Host 1 and/or LDAP Host 2 in the registry.
- The Cisco Desktop LDAP Monitor service is not running. Start it.
- Check if slapd.exe is running. If it is not running, follow the troubleshooting steps for this problem.
- The LDAP database is corrupted. Follow the steps outlined in "Corrupted Directory Services Database" on page 40.

**Problem** Clients do not find the same information from LDAP after failing over from one LDAP to the other.

**Solution** Some solutions:

- Ensure replication is set up correctly.
- Check that registry entries for LDAP Host 1 and 2 on both CAD services computers are the same and contain the right information.
- Check that slapd.conf on both CAD services computers are correct and reference each other.
- If all else fails, follow the steps outlined in "Out of Sync Directory Services Databases" on page 41.

**Problem** The VoIP Monitor Service fails with the following exception when using server-based monitoring:

FATAL FCVMS112 splk_pcap_open_live() failed. errorBuf = Error opening adapter: Access is denied.

**Conditions**: A second NIC is installed/enabled on the server. CAD Configuration Setup (PostInstall) is run to detect the second NIC and then the VoIP Monitor Service is restarted.

**Solution** The splkpcap driver must be reinitialized. To do this, unload and then reload the driver. Open a command window on the computer where the new NIC was installed and type these commands:

```
net stop spcd
net start spcd
```

Close the command window and start CAD Configuration Setup. In the VoIP Monitor Service window, select the IP address of the new NIC and save the changes.

## Cisco Agent Desktop Problems

**Problem** The CPU usage on the agent's PC has gone to 99%, and the PC has locked up.

**Solution** This can happen when you disable the sniffing adapter through the Windows Network and Dialup Connections window while Agent Desktop is running and is being monitored and/or recorded by the supervisor or recorded by the agent, using Desktop Monitoring. Re-enabling the sniffer adapter while Agent Desktop is running will not solve the problem You must stop Agent Desktop, re-enable the sniffer adapter, and then restart Agent Desktop to restore normal functionality.

**Problem** An agent using Windows XP was able to start CAD, but was not able to enter an active state.

**Solution** Windows XP can be configured so that the Internet Connection Firewall (ICF) is active. ICF acts by keeping track of all traffic to and from the computer; it will only allow information through that has originated from that particular computer. If a message originates from outside the computer, it will be discarded.

To solve this problem, either turn off ICF (requires someone with administrator rights to the computer) or override the defaults to include known "good" connections like the CAD servers.

**Problem** The agent received the error message, "The agent- or workflow-initiated action request failed."

**Solution** This error message is displayed when a request to the CRS engine, for example a call control action or agent state change, is rejected. Try the action again.

**Problem** The agent is unable to log in to Cisco Agent Desktop.

**Symptom.** An agent receives an error message when trying to log in to Cisco Agent Desktop.

**Message.** The error message might be one of the following:

- Failed to login into CTI Manager Server! Please talk to your administrator.
- The ID you entered was not found.
- Unable to log agent in.
- A critical error has been received. Either your phone or the Unified CallManager is offline. If you are not already logged out, you may need to logout and try to log in again.

**Cause.** Depending upon the error message, the cause could be one of the following:

- If the error message involves the CTI Manager Server, the problem might be that the Enable CTI Application Use is not configured for the agent user ID, the Cisco CTIManager service is not running on the Unified CallManager server, or you are using an invalid password.
- If the ID you entered was not found, the ID could be invalid.
- If the agent cannot log in, the agent's phone might not be associated with the RM JTAPI provider in the Unified CallManager.
- If you receive the critical error message, the Unified CallManager server might be offline or the Agent's IP phone has reset.

**Solution** Correct the problem related to the error message:

- If the message relates to the CTI Manager server, make sure that the Cisco CTIManager service is running on the Unified CallManager server.
- If the ID was not found, make sure that you are typing the user ID correctly. User IDs are case sensitive. Verify that you are using the correct Unified CallManager password.
- If the agent's phone is not associated with the RM JTAPI provider in Unified CallManager, go to the User ID field in the Unified CallManager IPCC Express Configuration web page, and associate the agent's phone with the RM JTAPI provider.
- If you receive the critical error message, make sure that the Unified CallManager server is online, and verify that the agent's phone is in service.

- Unified CallManager is up and running, provided the Cisco CRS setup is pointing to a cluster of Unified CallManagers.

**Problem** No data appears in the Enterprise Data fields

**Symptom.** When an agent receives a call, the Enterprise Data pane does not display the expected data.

**Message.** None.

**Cause.** The CRS server is not correctly passing enterprise data from the Enterprise service to Cisco Agent Desktop. This situation can be a result of incorrect step configuration in the script or in the Enterprise Data Configuration section of Cisco Desktop Administrator. This situation can also be a result of an out-of-sync condition between the Enterprise Data subsystem and the Enterprise service.

**Solution** Complete the following steps:

1. Verify the step configuration in the script and in the Enterprise Data Configuration section in Cisco Desktop Administrator.
2. Stop and restart the Enterprise service.
3. If the problem persists, stop and restart the CRS engine.

**Problem** Partial Service or No Service message displays in the Agent Desktop status bar

**Symptom.** The agent sees a message in the Agent Desktop status bar.

**Message.** Partial Service or No Service.

**Cause.** Agent Desktop has detected that it is unable to communicate with a service (generally within three minutes of the service failure), and displays the “Partial Service” or “No Service” message to indicate some or all of the services have failed.

**Solution** Double-click on the message in the status bar to display the Server Status popup window. This window lists Agent Desktop features and indicates which features are affected by the service failure. When CAD detects that the failed service is again available (usually within one minute of the service recovery) the status bar displays “In Service” to indicate that the service has recovered.

**Problem** Agent toggles between Ready and Reserved states

**Symptom.** The agent toggles between the Ready state and the Reserved state.

**Message.** None.

**Cause.** This might happen if a dial plan exists that starts with the same digit that the agent's Cisco Unified Contact Center Express extension starts with. If the total number of digits in the agent's extension in such a situation is less than the total number of digits configured for the dial plan, this symptom might occur.

**Solution** Make sure that the following two things do not happen concurrently:

- An agent's Cisco Unified Contact Center Express extension starts with a digit for which a dial plan exists in Unified CallManager.
- The total number of digits in the agent's Cisco Unified Contact Center Express extension is less than the total number of digits configured for the dial plan.

**Problem** When agents start Agent Desktop, they see the following error: "A licensing error has occurred. Please try again in five minutes. If the problem persists, please see your log file or the System Administrator for details"

**Symptom.** Telnet tests from the agent PC to the LRM service on the CAD server (port 65432) fail. The LRM service is running and agents are able to connect some of the time. Cisco Security Agent (CSA) is installed and running on the CAD server.

CSA log reports the following: "Event: Possible SYN Flood detected. Source addresses include 10.X.X.X. TCP ports, including port 59004, SYN Flood protection has been enabled."

**Cause.** CSA is in SYN Flood detection mode. Agent PCs have the firewall enabled and are blocking packets, and CSA thinks the PC is non-responsive.

**Solution** Short-term solution: Restart CSA on the CAD servers.

Long term solution options include:

- **Option 1**: Leave the systems as is. Risk: SYN Flood detection mode might become enabled, which can prevent agents from logging in. If not discovered immediately, the problem can persist until SYN Florrd turns off by itself (approximately 2 hours).
- **Option 2**: Turn off SYN Flood detection mode. Risk: Leaves the server open to SYN Flood.
- **Option 3**: Turn off Agent PC firewall. Risk: Could leave agent PCs vulnerable to viruses.

Recommendation: Option 2. SYN Flood is generally not effective against modern networks.

**Problem** Every time the agent hangs up the telephone, Agent Desktop disappears.

**Solution** In Normal mode, Agent Desktop automatically minimizes when there are no active calls. Set up this behavior in Desktop Administrator. To prevent the Agent Desktop window from minimizing, click the Preferences button on the toolbar and select Always Open or Always on Top.

**Problem** The administrator has made changes in Desktop Administrator, but they are not showing up in Agent Desktop.

**Solution** Agent Desktop must be restarted in order for the changes to take effect.

**Problem** The agent has changed Agent Desktop's window behavior (from the File menu), but when Agent Desktop is restarted, the setting has not been saved.

**Solution** Changes made to local settings via Agent Desktop are only temporary overrides of the global settings. Permanent changes must be made via Desktop Administrator.

**Problem** Sometimes during a conference call, a conference member shows up as <Unavailable>.

**Solution** <Unavailable> represents a party outside the switch. The switch sends the trunk number of the external party to the desktop, where it has no meaning. Agent Desktop replaces the trunk number with <Unavailable>.

**Problem** The agent sent the supervisor an emergency chat message but the supervisor never received it.

**Solution** Supervisors receive emergency chat messages only if they are monitoring the team to which the agent who sent the message belongs.

**Problem** While running Agent Desktop, the error message, "Macro file failed to open," keeps appearing.

**Solution** Turn off any virus scanning applications on the desktop. Virus scanning applications attempt to intercept calls to open a file to do their own processing first. This might cause the file to be opened in such a way that restricts other applications from opening the file.

**Problem** The agent can't view any skills statistics in Agent Desktop.

**Solution** If an agent is not assigned to a skill group, no skills statistics are available.

**Problem** When the agent starts Agent Desktop, a call appearance is displayed showing that the agent is on a call, even though there is no active call on the agent's phone.

**Solution** On startup, Agent Desktop asks the CTI server for a snapshot of any existing phone calls to display to the user. Occasionally the CTI server returns invalid data. To dismiss the invalid data, click the Drop button on the toolbar. If the call appearance persists, the agent might have to

close Agent Desktop, pick up the phone receiver to get a dial tone, hang up, and then restart Agent Desktop.

**Problem** Sometimes after placing a call on hold, the agent is unable to retrieve the call. Once the call is hung up, the agent state still reflects On Hold. Exiting and restarting Agent Desktop doesn't help.

**Solution** A task in Unified CallManager administration is associating devices with JTAPI users. The peripheral gateway JTAPI user should be associated with agent telephones. The IP IVR JTAPI user should be associated with the CTI ports corresponding to the virtual ports on the IP IVR.

Each of these device categories is distinct. A device cannot belong to more than one category. Failure to assign a device to exactly one category can cause problems.

**Problem** Sometimes while talking on a call, the agent is unable to change the agent state to Not Ready. As a result the agent keeps receiving calls from the ACD, even after closing the application.

**Solution** A task in Unified CallManager administration is associating devices with JTAPI users. The peripheral gateway JTAPI user should be associated with agent telephones. The IP IVR JTAPI user should be associated with the CTI ports corresponding to the virtual ports on the IP IVR.

Each of these device categories is distinct. A device cannot belong to more than one category. Failure to assign a device to exactly one category can cause problems.

**Problem** The agent is using Cisco Desktop Agent with an IP soft phone (for instance, Cisco IP Communicator) on a computer with multiple network adapter cards. When the agent switches from using one NIC to the other to connect to the network, the agent cannot log in. (An example of this situation is running CAD with an IP soft phone on a laptop that can connect to the network using either an Ethernet or wireless connection.)

**Solution** Each NIC has its own MAC address. The Unified CallManager must be able to associate a MAC address with an extension in order for CAD to function correctly. If the Unified CallManager knows about only one of

the multiple NICs, only that one will work. If an agent is going to use a computer with multiple NICs, Unified CallManager must be configured to recognize each NIC's MAC address.

**Problem** The agent is logged out unexpectedly.

**Solution** Possible reasons are:

- Another agent with the same ID or extension has logged in, causing the first agent to be logged out.
- A supervisor has logged the agent out.
- The telephony service has failed.
- The network has failed.

**Problem** The agent can make and receive internal calls but gets errors when trying to make an external call.

**Solution** The dial string properties must be configured properly for outgoing calls. Some switches are set up to automatically dial a 9 to get an outside line, while others require you to dial a 9. The dial string must take into account how the switch is set up.

**Problem** The agent's call control action does not work properly.

**Solution** Try performing the same action manually using the dial pad. Telephone numbers are formatted the same way when used in call control actions as they are when making calls manually. Make sure that the dial string is configured properly for outgoing calls.

**Problem** There are four actions assigned to an event, but only the first two run.

**Solution** When executing a set of actions, execution is halted if any of the actions fail. This is because some actions might depend on previous actions executing correctly. Find out why the third action is failing and correct it.

**Problem** The only phone book appearing on the dial pad dialog box is the recent call list.

**Solution** The administrator disabled the phone books.

**Problem** Global phone books appear but there is no personal phone book.

**Solution** The administrator disabled personal phone books.

**Problem** When editing a phone book, the agent can't add an entry after editing the first name, last name, or notes.

**Solution** The agent must enter a phone number before the Add button is enabled.

**Problem** The agent can edit the personal phone book, but not other phone books.

**Solution** The personal phone book is not shared by other agents. The other phone books are shared, and can be edited only by the administrator.

**Problem** The agent changed the viewing options but pressed cancel. Why weren't the changes to the filters canceled?

**Solution** There is a cancel button for each of the filter dialog boxes. Once a filter has been accepted, it is saved. The cancel button on the options dialog box only cancels changes made to the columns.

**Problem** The keystroke macros do not play back correctly on dropped events.

**Solution** If Agent Desktop is running in normal mode (maximized when a call is received, and minimized when there are no call appearances), keystroke macros might play back to the wrong window. When Agent

Desktop minimizes after a call is dropped, it steals focus from the target keystroke macro window. To fix this, place a [Delay]<*milliseconds* command at the beginning of the keystroke macro. This allows time for Agent Desktop to minimize before playing back the keystroke macro. For example:

[DELAY] 1000
[APPLICATION:NOTEPAD=UNTITLED - NOTEPAD]

**Problem** Macros are not playing back correctly.

**Solution** When playing keystrokes to a window, Agent Desktop must first find the window. When recording the macro, Agent Desktop saves the window's title and class name (an internal Windows variable associated with a window). On playback, Agent Desktop searches in this order:

1. Find a window with the saved title and class name.
2. Find a window with the saved class name.
3. Find a window with the saved title.

If Agent Desktop does not find a window matching one or more of these criteria, it displays an error message.

If there are two windows with the same name and class, Agent Desktop might play back the macro to the incorrect window.

If there are several windows with the same class name, and the title of the target window has changed, Agent Desktop might play back the macro to the incorrect window.

Some compilers/class libraries use the same class name for all windows. If you have developed an in-house application, you might need to change the class name in your application.

**Problem** A keystroke macro will not play back even though the target application is running.

**Solution** Agent Desktop uses the application's class name and title to find the target application. Some applications change title and class name when changing screens. If this happens, Agent Desktop might not be able to locate the target application. Try using just the window title or class name to find the target application.

**Example 1**: Find both the title (NOTEPAD) and class (UNTITLED - NOTEPAD).

[APPLICATION:NOTEPAD=UNTITLED - NOTEPAD]
[SHIFT] D
et cetera.

**Example 2**: Find just the class (NOTEPAD):

[APPLICATION:NOTEPAD=]
[SHIFT] D
et cetera.

**Example 3**: Find just the title (UNTITLED - NOTEPAD):

[APPLICATION:=UNTITLED - NOTEPAD]
[SHIFT] D
et cetera.

---

**Problem** The administrator created a macro and put in some delays. Now the PC appears to lock up while the macro runs.

**Solution** When a macro runs, the operating system takes over the PC and locks out all user input. This is a characteristic of the operating system. Try to minimize the length of time your macro runs.

---

**Problem** A keystroke macro plays the wrong keys to the wrong window.

**Solution** Make sure macro playback starts from the same place every time it runs. Have the macro start from the same starting window with the cursor in the same starting position as when the macro was recorded.

---

**Problem** When a macro is played back, it seems to be missing keystrokes, or the PC locks up.

**Solution** Due to the wide variety of systems and configurations, macro playback speed can vary. To slow down the rate at which a macro plays back keystrokes, add a Delay command. This command tells the macro to wait a certain number of milliseconds before performing the next macro key or command.

For example, if you add **[DELAY] 1000** before a macro action, it delays the next macro key or command by 1 second.

**Problem** After a macro runs, focus remains on the application to which it played. How can the macro be written to make it change focus to Agent Desktop (or some other application)?

**Solution** To change focus to Agent Desktop, edit the macro and insert this line at the end:

[APPLICATION:AGENT_DESKTOP=AGEN T_DESKTOP]

You can also change focus to an application other than Agent Desktop. To determine the line to insert, create a dummy macro and play a few keystrokes to the application. When you finish recording, cut and paste the application's text identifier from the dummy macro to the macro you wish to edit.

**Problem** Sometimes when a macro is running, the PC appears to lock up for short periods of time.

**Solution** A [DELAY] statement in a macro causes the system user-input hook to keep control of the system. The PC runs but rejects all user input until the macro finishes playing. To limit this problem, use the shortest delays possible.

**Problem** The agent pressed Ctrl-Alt-Del while a macro was running, and now the Agent Desktop window is locked up.

**Solution** You cannot click **Start** or press **Ctrl-Break**, **Ctrl-Esc**, or **Ctrl-Alt-Del** when recording a macro. The Windows operating system unhooks the system keyboard hook when Start is pressed.

**Problem** The agent is participating in a blind conference call, but cannot see all parties on the call.

**Solution** In CAD 6.5, a blind conference is defined as adding an alerting party to a conference. All parties on a blind conference call might not show up in either Supervisor Desktop or Agent Desktop. This is a limitation of the Cisco CTI server software.

## Work Flow

**Problem** The administrator made some changes in Work Flow Setup, and then decided to cancel them. However, they were already saved.

**Solution** When a new action is created, any changes are automatically saved before returning to the Select Action dialog box.

**Problem** The administrator cannot get a rule to work based on an internal extension number.

**Solution** When Agent Desktop compares the telephone numbers, if the dial string number format includes a leading x, then the telephone numbers in the list must also include a leading x.

**Problem** An action that launches an external application is not working correctly.

**Solution** Sometimes the operating system can be confused by spaces in directories and file names. If you have an application such as **C:\Program Files\Acme\Search Database.exe /t/x**. you might need to add quotes around the directory and executable. For example, the above would be "**C:\Program Files\Acme\Search Database.exe" /t/x**

**Problem** When Agent Desktop attempts to launch an external application, the following error message appears: "Error Launching Application...The system cannot find the file specified."

**Solution** When creating a launch external application action, you must include the extension of the application you wish to launch. For example, to launch Windows Notepad, **C:\Windows\Notepad.exe** is correct, while **C:\Windows\Notepad** is incorrect.

If the path to the executable or an argument contains spaces, it must be enclosed in quotes, for instance, **"C:\Program Files\MyFile.doc"**.

**Problem** The administrator configured a task button to send an email message, and changed the hint to Send Email (Ctrl + S). The shortcut keys do not work.

**Solution** For any task button, you can only change the hint text. You cannot change the shortcut key.

**Problem** The phone points to a different Unified CallManager, but the user was able to log into Agent Desktop using the phone's extension. When you try to call the extension you get a busy signal.

In Unified CallManager, there is no fixed association between agents and their extensions. An agent can login with any extension that has the "allow watch" setting. If the agent logs into Agent Desktop using an extension on a phone that points to a different Unified CallManager, the agent will get an error message when changing to the Ready state.

**Solution** Log into Agent Desktop using the extension on a phone that points to the correct Unified CallManager.

# Chat Problems

**Problem** Chat and Supervisor Desktop do not work properly on PCs with multiple IP addresses.

**Solution** Chat and Supervisor Desktop are both CORBA servers and CORBA clients. When they start up, the CORBA service arbitrarily picks one on the IP addresses to use when forming its Interoperable Object Reference (IOR). The IOR is what clients (in this case, the client is the Chat Service) use to connect to the service (Chat or Supervisor Desktop). If one of the IP addresses is inaccessible to the Chat service, then it will be unable to send data to Chat or Supervisor Desktop.

You can force Chat and Supervisor Desktop to use a particular IP address by setting the environment variable OMNIORB_USEHOSTNAME to the IP address that you wish to use. The variable must be set before starting Agent Desktop or Supervisor Desktop.

To set the environment variable:

- **WIndows 2000 Professional and Windows XP**: In the Control Panel, double-click System. In the System Properties dialog, select the Advanced tab. Click the Environment Variable button and then Add to add OMNIORB_USERHOSTNAME and the IP address to the System Variable list.

**Problem** After completing a conference call, Chat and Supervisor Desktop show an extra party on the call.

**Solution** Occasionally, each agent receives different data from the CTI server. For example, a customer (555-5555) calls Agent A. The CTI server reports 555-5555 as the calling number to Agent A. Agent A then conferences in Agent B. However, in this case the CTI server reports <Unavailable> as the customer number to Agent B. When the time comes to merge the data from the two agents (Agent A, Agent B, customer number, and <Unavailable>. an extra party is added because the customer number and <Unavailable> cannot be distinguished.

## Cisco Desktop Administrator Problems

**Problem** The following error appeared while attempting to install Desktop Administrator configuration files on a network drive:

"The drive does not support long file names. You must choose a drive that support long file names. See your network administrator for more information."

**Solution** You must enable long file name support on the network drive, or choose another drive that does support them. You can also install the configuration files on the administrator PC. You must enable File Sharing If you install the configuration files on the administrator PC.

**Problem** The administrator cannot create a new work flow group.

**Solution** The work flow group name is already used for another group, and/or the work flow group name is not a valid Windows directory name.

**Problem** The administrator cannot restore a Desktop Administrator backup.

**Solution** The Desktop Administrator config directory is write-protected, and/or Desktop Administrator cannot create the config directory to which to restore the files.

# Enterprise Data Problems

**Problem** Enterprise Data displays data after a call has been dismissed.

**Solution** Enterprise Data displays data from the last call until a new call is received. This allows agents to use the enterprise data for after-call work.

## Enterprise Service Problems

**Problem** When the user attempts to start Enterprise Service, the following error displays:

"Could not start the Cisco Enterprise Service on *Computer.* Error 2140: An internal Windows error occurred."

**Solution** Look at the Windows event log to see why the Service failed to start.

1. Click **Start > Programs > Administrative Tools > Event Viewer**.
2. On the **Log** menu, click **Application**.
3. Select a message that displays **Enterprise Server** as the source. This should provide more information on the cause of the failure.

**Problem** No screen pops appear when the user makes calls to and from devices.

**Solution** Try the following:

- Use Enterprise Administrator to make sure the device is being monitored.
- Check to see if CTI Server is running.
- Check to see if an agent is logged in to the device.
- Check if the device is configured on Cisco Unified Contact Center Express.

**Problem** Nothing happens when the user calls a particular device.

**Solution** Try the following:

- Make sure the device is being monitored.
- Check the event log to see if there are any error messages for the device.

**Problem** Incomplete or no enterprise data is displayed when an agent received a call.

**Solution** Try the following:

- Check if the device is being monitored in the Enterprise service.
- Set the debug level to DEBUG, CALL, TRACE, or DUMP (see "Debugging" on page 34 for more information on setting debug levels). Stop and restart Agent Desktop. Repeat the call scenario, and then check ssctihandler.dbg for warnings about non-monitored devices. Search for “monitoring” in the debug file.

## IPCC License Administration Problems

**Problem** The message, “There are no licenses available. Please contract your Administrator for help,” appeared.

**Solution** All licenses are currently in use. Contact your sales representative to obtain additional licenses.

## Cisco IP Phone Agent Problems

**Problem** Agents do not see the IP Phone Agent service on their IP phones.

**Solution** The following are some reasons for the service to not appear when the Services menu is accessed:

- The IPPA service has not been configured in Unified CallManager.
- The phone is not subscribed to the IPPA service.
- The service URL in Unified CallManager has a hostname and the phone cannot resolve it. Use the IP address instead.
- The phone has not been rebooted after changes were made in Unified CallManager. If a soft reboot does not work, try a hard reboot (unplug the phone's power cord and then plug it back in).

**Problem** Agents see an HTTP error when selecting the IP Phone Agent service on their phone.

**Solution** Some solutions:

- The IP Phone Agent service URL in Unified CallManager has a hostname and the phone cannot resolve it. Use the IP address instead.
- The IP Phone Agent service URL in Unified CallManager has an incorrect hostname, IP address, or port. The port is specified in <Parameter name="port" value="6293"/> under the <!-- Normal HTTP --> section in C:\Program Files\wfavvid\tomcat_appadmin\conf\server.MADM.xml.
- The IP Phone Agent service URL is case sensitive. Enter it exactly as specified in the *Cisco CAD Installation Guide*.
- The Tomcat service is not running on the CAD services computer.
- The IP Phone Agent service is not running on the CAD services computer.
- The agent's phone was not rebooted after changes were made in Unified CallManager. If a soft reboot does not work, try a hard reboot (unplug the power cord and plug it back in).

**Problem** The agent sees an error message that the IP Phone Agent service is not active.

**Solution** Some solutions:

- The system is set up with redundant CAD services and the agent has selected the standby IP Phone Agent service instead of the active service. For redundant CAD services, there should be two IP Phone Agent services set up in Unified CallManager, each pointing to a different IP Phone Agent service, and all IP Phone Agent agent phones must be subscribed to both services.
- On a nonredundant system, if the LRM service is down, then the IP Phone Agent service will become standby. Restart the LRM service.
- Agent Desktop or Supervisor Desktop was installed on the same computer as the CAD services. They clear a registry key (IOR Hostname under Site Setup) required by the IP Phone Agent service. Set the registry to the IP address of the CAD services computer.

**Problem** The agent gets the Force Login screen when trying to log in, but attempting to force the login does not work.

**Solution** The agent is using an agent ID that is already logged in on another extension, or using an extension that is already logged in with a different agent ID. Forced logins work only for the same ID/extension pair. Use a different agent ID or extension, or find the other user and have them log out.

**Problem** The agent does not see the Enterprise Data screen when receiving/answering a call, or receive Contact Service Queue (CSQ) Statistics screen updates.

**Solution** Some solutions:

- The authentication URL in Unified CallManager has a hostname and the phone could not resolve it. Use the IP address instead.
- If the Unified CallManager authentication URL (one with authenticate.asp) is used, make sure that a telecaster user with a password of telecaster exists in Unified CallManager and that the phone is associated with this user.

- The agent's phone was not rebooted after changes were made in Unified CallManager. If a soft reboot does not work, try a hard reboot (unplug the power cord and plug it back in).
- Verify that the agent is logged in to the phone.
- Verify that if the agent logs into CAD using the same phone and user ID, enterprise data does pop correctly.

**Problem** The agent sees nonsense characters in reason codes and/or enterprise data.

**Solution** The reason codes and/or enterprise data configured in Desktop Administrator contain characters not supported by the phone. Examples are multibyte Chinese or Kanji characters. Make sure that no unsupported characters are used when configuring reason codes and/or enterprise data.

**Problem** A supervisor cannot record or monitor an IP Phone Agent agent.

**Solution** The phone is not set up for SPAN port monitoring.

## Recording & Playback Service Problems

**Problem** The Recording & Playback service is not recording the audio file.

**Solution** Check the following:

- Make sure that a SPAN port has been created on the switch for the PC's network port where the VoIP monitor service is connected.
- Make sure that the Recording & Playback service has permission to write to the AudioFiles directory.
- If the audio files are saved on a drive using the FAT32 file system, there is a limitation of 21,844 objects in the folder. If the folder has reached this limit, delete unused audio files, or convert the drive to the NTSF file system.

To check the user of the service, open the Control Panel. Double-click **Administrative Tools** and then **Services**.

Search for the service named Cisco Desktop Recording & Playback Service and click the Startup button. Account should be selected and a domain account given along with the password.

**Problem** After CRS is upgraded or newly installed, recording does not function.

**Solution** The Recording Count parameter in CRS Administration must be changed from 0 a number up to 32 (Enhanced version) or 80 (Premium version).

To change this parameter:

1. In CRS Administration, choose **System > System Parameters** from the toolbar.
2. Scroll down the page to find the **Recording Count** parameter. The value is set at 0 (zero).
3. Change the parameter to either 32 (for CAD Enhanced) or 80 (CAD Premium) and then click **Update**.

## Recording & Statistics Service Problems

**Problem** The Recording & Statistics service is returning an error when retrieving the Global ID or it is returning zero (0).

**Solution** Check the following:

- Verify that the FCRasSvr database has been created in the SQL server. This will require the SQL server tool Enterprise Manager. Or, you can try creating an ODBC connection to the SQL server and try to select FCRasSvr as the database. It will not appear in the list if it does not exist.
- Make sure that the server is connected to the database by checking the log file ...\log\FCRasSvr.log for the error string FCRVS306.

If the database does not exist, run CAD Configuration Setup from Desktop Administrator. Using this tool, create the database. See the *Installation Guide* or the *Cisco Desktop Administrator User's Guide* for information on using CAD Configuration Setup.

**Problem** When trying to view agent state or call logs, no data is presented.

**Solution** The agent might not have received a call, or logged in for that particular day. The agent's or supervisor's PC's clock might not be in the correct time zone.

**NOTE:** All state and call times are based on server time.

**Problem** Data appears to be in incorrect chronological order in Agent Desktop or Supervisor Desktop logs and reports, or in Supervisor Record Viewer. Cisco Unified Contact Center Express is in a redundant configuration, and a failover just occurred.

**Solution** If the system clocks on the redundant Cisco Unified Contact Center Express servers are not synchronized, report and log data will appear to be in the wrong order after a failover from one server to the other. To

correct this situation, use a network time service to automatically synchronize all server system clocks, or manually adjust them so that they are in sync.

# Silent Monitoring/Recording Problems

**Problem** When using desktop monitoring to monitor a remote CAD agent who uses the Cisco VPN Client 4.x to connect to the network, only the agent's side of the conversation is audible. The monitoring supervisor's computer uses the Windows 2000 operating system.

**Solution** When the monitoring supervisor uses a Windows 2000 desktop, and the remote agent uses VPN Client 4.x, only the agent's side of conversations will be heard. This is due to a problem with the VPN Client's virtual VPN adapter driver.

To fix the problem, do one of the following:

- Do not use a VPN connection.
- Do not use the Windows 2000 operating system to monitor remote agents who use VPN Client 4.x.
- Have the remote agent use VPN Client 3.x.
- Monitor the remote agent with server monitoring, not desktop monitoring.

**Problem** The CPU usage on the VoIP Monitor service PC has gone to 99%, and the PC has locked up.

**Solution** This can happen in several scenarios. It may occur when you disable the sniffing adapter through the Windows Network and Dialup Connections window while the VoIP Monitor service is running. Re-enabling the sniffer adapter while the VoIP Monitor service is running will not solve the problem You must stop the VoIP Monitor service, re-enable the sniffer adapter, and then restart the VoIP Monitor service to restore normal functionality.

This may also occur if you install Cisco Security Agent (CSA) and do not reboot the computer when prompted. Manually rebooting the computer will correct the situation.

**Problem** When the supervisor clicks on an agent to start monitoring, Supervisor Desktop displays the speaker icon next to the call but there is no sound.

**Solution** Check these things:

- Move the volume slider all the way to the right.
- Verify that the sound card in the PC is working properly.
- Check to see if another application is using the sound card. Some combinations of operating system, sound card, and drivers do not support multiple users.
- Verify that the agent is on a call, and is talking.

If using SPAN port (server-based) monitoring:

- Verify that the SPAN port on the switch has been configured correctly. If the monitor service has been moved, or new agent IP phones have been added, then you might need to reconfigure the SPAN port.
- Check the Windows application log on the Voice-Over IP Monitor service for errors.

If using desktop (agent-based) monitoring:

- Verify that the PC is connected to the phone in the 10/100 SW port.
- Verify that the agent PC is daisy-chained to the phone, which is connected to the network.
- Verify that the agent's PC is connected to the same IP phone that the agent is logged into.
- Verify that the Unified CallManager has the correct MAC address for this extension.
- Verify that the agent's PC uses a NIC that is fully NDIS-compliant. For a procedure for testing if a NIC is fully NDIS-compliant, see Appendix C of the *Cisco CAD Installation Guide*.
- 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 workaround solution is available from the Intel Technical Support website (Solution ID: CS-005897). Other solutions include:

- Using another type of NIC that is fully NDIS-compliant.

- Monitoring agents via a VoIP Monitor service.

**Problem** The supervisor clicks a recording in Supervisor Record Viewer, but it does not play.

**Solution** Check the following:

- Move the volume slider all the way to the right.
- Verify that the sound card in the PC is working properly.
- Check to see if another application is using the sound card. Some combinations of operating system, sounds card, and drivers do not support multiple users.
- Verify that the SPAN port on the switch has been configured correctly. IF the monitor service has been moved, or new agent IP phones have been added, then you might need to reconfigure the SPAN port.
- Check the Windows application log on the Voice-Over IP Monitor service for errors.

**Problem** When monitoring an agent's customer contact, nothing can be heard, and after 15 seconds, an error message is received that no packets are being received. Attempting to record an agent's customer contact results in an empty recording. The agent's desktop is monitored using desktop monitoring.

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

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

In the Product Specific Configuration section of the Device Configuration screen, 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 screen, 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.

**Problem** The VoIP Monitor Service fails with the following exception when using server-based monitoring:

FATAL FCVMS112 splk_pcap_open_live() failed. errorBuf = Error opening adapter: Access is denied.

**Conditions**: A second NIC is installed/enabled on the server. CAD Configuration Setup (PostInstall) is run to detect the second NIC and then the VoIP Monitor Service is restarted.

**Solution** The splkpcap driver must be reinitialized. To do this, unload and then reload the driver. Open a command window on the computer where the new NIC was installed and type these commands:

```
net stop spcd
net start spcd
```

Close the command window and start CAD Configuration Setup. In the VoIP Monitor Service window, select the IP address of the new NIC and save the changes.

## Cisco Supervisor Desktop Problems

**Problem** Error when trying to select skills in the Team View pane.

**Symptom.** When you try to select skills in the Team View pane in the Cisco Supervisor Desktop, the following message appears:

**Message.** Cisco Agent Desktop must be active before call intervention, call recording, and queue stats are available.

**Cause.** To view skill group statistics, you must log in to a Cisco Agent Desktop as a supervisor.

**Solution** Log in to a Cisco Agent Desktop as a supervisor.

**Problem** Display of agents in Supervisor Desktop.

**Symptom.** The following symptoms related to the display of agents in the Supervisor Desktop can occur:

- Agents disappearing from Supervisor Desktop
- Agent not listed in Supervisor Desktop
- Supervisor Desktop does not display any agent

**Message.** None.

**Cause.** Incorrect configuration or IP connectivity issues between the Agent and the CRS system or the CRS system and the Supervisor.

**Solution** Complete the following steps:

1. Verify that the agent belongs to the team which the Supervisor is monitoring. Refer to the Team configuration in the *Cisco Desktop Administrator User Guide*.
2. Verify that all instances of Cisco Agent Desktop and Cisco Supervisor Desktop have been upgraded to the same version as the CAD services running on the CRS server.
3. Make sure the agent is not closing the Chat window. This is the element of the Agent Desktop software that sends information to the Chat server about the agent's status. The Chat server then relays these messages to the Supervisor for display.

4. Determine whether the Supervisor Desktop or Agent Desktop has multiple NICs.
5. Determine whether any ports in the 59000–59030 range are closed off by a firewall.
6. Go to **Local Area Connection settings > Advanced** tab to determine if the Agent Desktop or Supervisor Desktop running on Windows XP has the Internet Connection Firewall enabled.
7. To test for blocked ports, use telnet from the command line as follows with agent and supervisor logged in:
   - From Chat server to agent: telnet <agent PC IP address> 59020
   - From Chat server to supervisor: telnet <supervisor PC IP address> 59021
   - From agent to Chat server: telnet <CRS server IP address> 59000

If you get a failed to connect error, then you need to determine why the port is blocked.

---

**Problem** Agent moved to Not Ready state for no apparent reason

**Symptom.** In some situations, an agent might be moved to the Not Ready state for no apparent reason.

**Message.** None.

**Cause.** To determine the reason, check the reason code:

- If the reason code is 32763, the agent went Not Ready because of Ring No Answer (RNA). If the agent phone is configured on Unified CallManager with auto-answer enabled, then this is likely a Unified CallManager issue since the call is not answered in time. Please consult Unified CallManager support.
- If the reason code is 32759, the agent went Not Ready because the phone went out of service. Check to make sure the phone is still functional and that you can call the phone directly. If everything seems fine, it is most likely a temporary problem and the phone has since recovered. If the phone is still down, it is most likely a Unified CallManager problem. Please consult Unified CallManager support.

- If the reason code is 32757, the agent went Not Ready because the phone rehomed due to a Unified CallManager failover. As long as the agent is able to go Ready after the failover, this is not an issue.

**Solution** In many cases, an agent going Not Ready is not a serious issue. Simply click the Ready button to move the agent to Ready.

To determine the reason code, do one of the following:

- Open the **Agent State Report**. From Cisco Agent Desktop, click the **Reports** button. Select **Agent IPCC Express State Log**. Look for the entry which says "Not Ready" at the time the agent went to Not Ready state. Check the reason code for this entry.
- Run the Agent State Detail Report, a CRS Historical Report, and look for the "Not Ready" entry of the agent at the time the agent went to Not Ready state. Check the reason code for this entry.

In situations where the agent is unable to go to Ready state because the phone is still down, contact Unified CallManager support.

---

**Problem** Agents who connect to the contact center through a VPN are not displayed in the Supervisor Desktop Team View pane. The agents disappeared from the Team View pane after disconnecting and then reconnecting to the VPN. The status bar displays In Service.

**Solution** If either agents or supervisors use a VPN connection, their desktops must be restarted after disconnecting and then reconnecting to the VPN.

---

**Problem** A supervisor using Windows XP was able to start Supervisor Desktop, but was not able to load a team or display any agent information.

**Solution** Windows XP can be configured so that the Internet Connection Firewall (ICF) is active. ICF acts by keeping track of all traffic to and from the computer; it will only allow information through that has originated from that particular computer. If a message originates from outside the computer, it will be discarded.

To solve this problem, either turn off ICF (requires someone with administrator rights to the computer) or override the defaults to include known "good" connections like the CAD servers.

**Problem** Chat and Supervisor Desktop do not work properly on PCs with multiple IP addresses.

**Solution** Chat and Supervisor Desktop are both CORBA servers and CORBA clients. When they start up, the CORBA service arbitrarily picks one on the IP addresses to use when forming its Interoperable Object Reference (IOR). The IOR is what clients (in this case, the client is the Chat Service) use to connect to the service (Chat or Supervisor Desktop). If one of the IP addresses is inaccessible to the Chat service, then it will be unable to send data to Chat or Supervisor Desktop.

You can force Chat and Supervisor Desktop to use a particular IP address by setting the environment variable OMNIORB_USEHOSTNAME to the IP address that you wish to use. The variable must be set before starting Agent Desktop or Supervisor Desktop.

To set the environment variable:

- **WIndows 2000 Professional and Windows XP**: In the Control Panel, double-click System. In the System Properties dialog, select the Advanced tab. Click the Environment Variable button and then Add to add OMNIORB_USERHOSTNAME and the IP address to the System Variable list.

**Problem** When the supervisor clicks on an agent to start monitoring, Supervisor Desktop displays the speaker icon next to the call but there is no sound.

**Solution** Check these things:

- Move the volume slider all the way to the right.
- Verify that the sound card in the PC is working properly.
- Check to see if another application is using the sound card. Some combinations of operating system, sounds card, and drivers do not support multiple users.
- Verify that the agent is on a call, and is talking.
- Verify that the SPAN port on the switch has been configured correctly. IF the monitor service has been moved, or new agent IP phones have been added, then you might need to reconfigure the SPAN port.
- Check the Windows application log on the Voice-Over IP Monitor service for errors.

**Problem** The supervisor cannot log into the Voice-Over IP Monitor service, and receives the error “Could not access sound card”.

**Solution** The Voice-Over IP Monitor service was unable to find or access the system sound card. Make sure the sound card is working properly:

- Click **Settings > Control Panel > Sounds** and try to play a sound .wav.
- Click **Settings > Control Panel > Multimedia > Audio > Playback > Preferred Device** to make sure the correct device is selected.

**Problem** The sound quality is poor, and sounds choppy like a motorboat.

**Solution** Try this:

- Adjust the Sound Buffers registry entry. Set it higher; and if that doesn’t work set it down to 3 and work your way up.
- Adjust the Jitter Buffer registry entry. It should be at least 400; try setting it higher. If that doesn’t work you might have to use a different sound card.

**Problem** The sound is lagged. There is a noticeable delay between when the agent speaks and when I hear the sound on the PC sound card.

**Solution** A little lag time is normal. Since the voice is being sent in discrete packets across the network, which might have some delay variance. The software buffers up a few seconds before playback. Try adjusting the Jitter Buffer registry entry. You might be able to set it as low as 50 ms, however, if the network gets congested this might cause the monitor to sound choppy.

**Problem** The supervisor doesn’t see any of his teams or other personalized settings in the Supervisor Desktop window.

**Solution** If you add Supervisor Desktop to your Startup menu and your configuration files are on a network, it is possible that your configuration files aren’t loaded before Supervisor Desktop starts

because your PC hasn't had time to map the network drives. As a result, your personalized settings will not show.

Close Supervisor Desktop and start it again, and your personal settings will be loaded. To avoid the problem in the future, remove Supervisor Desktop from the Startup menu, and create a desktop shortcut icon to use to start the program.

**Problem** The supervisor scrolled the Data View (or Message View) pane sideways to view more information, and the toolbar icons disabled.

**Solution** Click anywhere in the Team View pane to enable the toolbar again.

**Problem** The supervisor clicked the Record button to record an agent conversation and nothing happened.

**Solution** There is no visible message displayed if a recording fails. If nothing happens, assume that the request failed. You will know that a recording succeeds if the icon next to the agent's conversation in the Team View pane changes to the recording icon.

**Problem** The supervisor tried to change an agent's state and nothing happened.

**Solution** There is no visible message displayed if an agent state change request fails. If nothing happens, assume that the request failed. You will know that an agent state change succeeds if the icon next to the agent's name in the Team View pane changes to the current agent state icon.

**Problem** Supervisor Desktop is no longer displaying any skills statistics.

**Solution** The supervisor is also an agent logged into the ACD. If the supervisor is inactive (in the Not Ready state) long enough he or she is logged out of the ACD.

The supervisor should log back in to see skills statistics again. A workaround to the logout situation is to create a skill group that has only supervisors in it and that does not receive ACD calls. The

supervisors can then place themselves in the Ready state and remain logged in as long as necessary.

**Problem** The supervisor clicks a recording, but it does not play.

**Solution** Check the following:

- Move the volume slider to maximum volume.
- Verify that the sound card in the PC is working properly.
- Check to see if another application is using the sound card. Some combinations of operating system, sounds card, and drivers do not support multiple users.
- Verify that the SPAN port on the switch has been configured correctly. IF the monitor service has been moved, or new agent IP phones have been added, then you might need to reconfigure the SPAN port.
- Check the Windows application log on the Voice-Over IP Monitor service for errors.

**Problem** After completing a conference call, Chat and Supervisor Desktop show an extra party on the call.

**Solution** Occasionally, each agent receives different data from the CTI server. For example, a customer (555-5555) calls Agent A. The CTI server reports 555-5555 as the calling number to Agent A. Agent A then conferences in Agent B. However, in this case the CTI server reports <Unavailable> as the customer number to Agent B. When the time comes to merge the data from the two agents (Agent A, Agent B, customer number, and <Unavailable>. an extra party is added because the customer number and <Unavailable> cannot be distinguished.

**Problem** If the supervisor's hook state changes during Chat service failure and recovery, the Barge-In and Intercept buttons get out of sync in Supervisor Desktop.

**Solution** Once the supervisor takes another call after the Chat service recovers, the Barge-In and Intercept buttons will display correctly. The problem can also be corrected by restarting Desktop Supervisor.

**Problem** Supervisors are getting randomly logged out of the Chat service.

**Solution** If a supervisor attempts to log into the Chat service with the same ID as another supervisor, the Chat service logs the first supervisor out. To avoid this problem, make sure that each supervisor has a unique ID. The ID is the extension stored in Phonedev.ini (located in the config folder). Phonedev.ini is populated with the extension field from the Login dialog box when Agent Desktop is started.

**Problem** The supervisor starts recording an agent's conversation, but after a short time the recording stops by itself.

**Solution** Check to make sure that no other supervisors are currently viewing the same team of agents. Any supervisor using Supervisor Desktop can see all conversations being recorded, and can stop a recording of an agent conversation even if that supervisor did not initiate the recording.

**Problem** The supervisor is viewing a blind conference call, but cannot see all parties on the call.

**Solution** In CAD, a blind conference is defined as adding an alerting party to a conference. All parties on a blind conference call might not show up in either Supervisor Desktop or Agent Desktop. This is a limitation of the Cisco CTI server software.

## Sync Service Problems

**Problem** How can I tell if the Sync service is running properly?

**Solution** In Desktop Administrator, perform a manual synchronization for a specific logical contact center. Make sure that all agents, supervisors, and teams are correctly listed for that logical contact center.

**Problem** The message, "At least one or more errors occurred during synchronization" appeared when the administrator performed synchronization in Desktop Administrator.

**Solution** Check the Sync service log file.

If the logged error points to IPCC Express database ODBC connection failure, then make sure that:

- the user ID and password in the Sync service configuration file is a valid IPCC Express database user.
- the user account that the Sync service is running has privileges to open a Name Pipe connection/
- the manual connection through the Sync service DSN works.

If the logged error was "...could not prepare SQL statement" then make sure that the IPCC Express peripheral ID key that is under *LCC*\Application Data\Site Setup in LDAP has a value.

If the logged error points to LDAP connection failure, then make sure that the LDAP service is running and that the LDAP_HOSTA registry setting in HKEY_LOCAL_MACHINE\SOFTWARE\
Spanlink\Site Setup has the correct value.

# Using Multiple NICs with the VoIP Monitor Service

A

## 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.

There may be other reasons for using a second NIC dedicated to receiving RTP traffic. The information shown below details the configuration of the second NIC to allow CAD's Silent Monitoring and Recording features to work properly.

Consult the *Cisco Agent Desktop (CAD) and CTI Toolkit Desktop Silent Monitor — Reference Information* for the most recent information on compatible NICs. This document is located at:

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

## Limitations

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

CAD's 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 explicitly specifies what NIC adapter to use for capturing audio packets, but it does not specify which NIC should be used when sending out packets. These outgoing packets would be going to either the Recording & Playback service or a supervisor's desktop that is silently monitoring an agent's call. 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 steams 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 tables so that normal traffic does not go through the sniffing NIC. Contact your network administrators for details.

An alternative solution is to give the sniffing NIC and 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.

In addition to these steps, the NCI that is used by the VoIP Monitor service must not be the first NIC in the network binding order. By default, the first NIC adapter in the binding order will be used by applications to send traffic out to the network. Contact your network administrator for details.

Uninstalling and installing NICs may cause the binding order of the systems network adapters to change. Whenever these kinds of changes are made, the binding order may need to be changed manually.

# Installing a Second NIC on a VoIP Monitor Service Computer

***To install a second NIC on a VoIP monitor service computer:***

1. Shut down the computer.
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. Assign valid IP addresses to the adapters.
5. Determine which of the two adapters will be used for sniffing.
6. Connect the sniffing adapter to the switch SPAN port.
7. Use the route command to customize the local routing table so that normal traffic does not go through the sniffing adapter.
8. Verify that the sniffing adapter is not registered with DNS and WINS by using the following command:

   `ping` *`local_host_name`*

   Where *local_host_name* is the IP address or DNS name of the adapter. This ensures that the local name always resolves to the normal traffic card IP address.

   Verify that the sniffing adapter is not the first adapter in the system's binding order.

## Additional Configuration Steps

The CAD installation process offers the user the option to choose the IP address that the VoIP Monitor service will use for packet sniffing. In a system with multiple NICs, the first adapter found is the default network adapter becomes the sniffing adapter. This may not be the adapter you want to use.

To change the NIC that is used by packet sniffing, use the CAD Configuration Setup utility. See the *CAD Installation Guide* for more information. This utility contains a screen that lists all valid NIC adapters in the system by IP address. Simply select the IP address associated with the NIC configured for packet sniffing and save your changes. This information is used by the VoIP Monitor service the next time the service is started.

To uninstall or reinstall the packet sniffing NIC or install a different packet sniffing NIC, use the CAD Configuration Setup utility as described above. If you do not use the CAD

Configuration Setup utility to point to the correct packet sniffing NIC, the silent monitoring and recording features may not work.

You do not need to perform these additional steps in a single-NIC system after you install CAD. If you uninstall and reinstall the packet sniffing NIC in a single-NIC system or install a different packet sniffing NIC in a single-NIC system, use the CAD Configuration Setup utility as described above. If you do not use the CAD Configuration Setup utility to point to the correct packet sniffing NIC, the silent monitoring and recording features may not work.

# Index

## R



## S



## T



## V



## W