About This Guide ix
  Purpose ix
  Audience ix
  Conventions ix
  Organization xi
  Other Publications xi
  Obtaining Documentation xii
    Cisco.com xii
    Ordering Documentation xii
  Documentation Feedback xiii
  Obtaining Technical Assistance xiii
    Cisco TAC Website xiii
    Opening a TAC Case xiv
    TAC Case Priority Definitions xiv
  Obtaining Additional Publications and Information xv

CHAPTER 1
Introduction 1-1
  Overview of CTI OS 1-1
    Advantages of CTI OS as Interface to ICM 1-2
    Key Benefits of CTI OS for CTI Application Developers 1-3
  System Manager Responsibilities 1-4
  System Requirements 1-5
    Desktop User Accounts 1-5
    Network Topology for Silent Monitor 1-6
Calculating Additional Needed Bandwidth 1-8
IPCC Media Termination 1-9
Hardware Requirements 1-9
Software Requirements 1-9

CHAPTER 2
CTI OS Server Installation 2-1
CTI OS Server Installation Guidelines 2-1
Upgrading from a Previous Version 2-2
ODBC File Data Source Name Creation 2-2
SQL User Login Configuration 2-8
Installing CTI OS Server 2-8
Uninstalling CTI OS Server 2-15
Determining Version Number of Installed Files 2-15

CHAPTER 3
CTI OS Client Installation 3-1
Upgrading from a Previous Version 3-1
CTI OS Client Component Installation 3-2
Uninstalling CTI OS Client 3-9
Determining Version Number of Installed Files 3-9
Configuring Supervisory Assistance Features 3-11
IPCC Media Termination 3-15
Configuring the Media Termination Device 3-16
Verifying Auto-Registration 3-16
Associating the New Device with the IPCC PG User 3-17
Add a New Agent 3-17
Adding Media Termination Device Target and Label 3-18
Setting Full Control Permissions to the Registry 3-19
Using Media Termination when using VPN 3-20
CHAPTER 5

Startup, Shutdown, and Failover 5-1

ICM Service Control 5-1

CTI OS Failover 5-3

Setting the /LOAD Configuration Parameter 5-3

Failover of CTI OS Related Components 5-4

IP Phones 5-4

Switches 5-4

Peripheral Gateway 5-5

CTI Server 5-5

CtiServerDriver 5-5

CTI OS Server 5-5

CHAPTER 6

Peripheral-Specific Support 6-1

General ICM Software Support 6-2

Peripheral-Specific Terminology 6-2

ICM Feature Limitations 6-4

CTI OS Support 6-5

Call Events 6-5

Client Control Requests 6-7

Peripheral-Specific Limitations and Differences 6-8

Alcatel 6-8

Aspect Contact Server 6-9

Avaya DEFINITY ECS 6-10

IPCC 6-17

Nortel Meridian 6-19

Nortel Symposium 6-25

Rockwell Spectrum 6-26

Siemens Hicom (North American Version) 6-27

Agent States 6-28
APPENDIX A  Testing an Ethernet Card for Silent Monitor  A-1
    Test Procedure  A-2
    Preparing Test Target  A-3
    Preparing Packet Generator Host  A-5
    Executing Test  A-5
About This Guide

Purpose

This manual provides instructions for installing, configuring, and running the Cisco CTI Object Server (CTI OS) product.

Audience

This manual is for system administrators and other personnel who are responsible for installing and maintaining CTI OS and its associated components. You must have administrator privileges to perform the procedures discussed in this manual.

Conventions

This manual uses the following conventions.
### Conventions

<table>
<thead>
<tr>
<th><strong>Format</strong></th>
<th><strong>Example</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Boldface type is used for user entries, keys, buttons, and folder and submenu names.</td>
<td>Choose <strong>Edit &gt; Find</strong> from the ICM Configure menu bar.</td>
</tr>
<tr>
<td>Italic type indicates one of the following:</td>
<td>• A <strong>skill group</strong> is a collection of agents who share similar skills.</td>
</tr>
<tr>
<td>• A newly introduced term</td>
<td>• <em>Do not</em> use the numerical naming convention that is used in the predefined templates (for example, <strong>persvc01</strong>).</td>
</tr>
<tr>
<td>• For emphasis</td>
<td>• IF (<em>condition</em>, <em>true-value</em>, <em>false-value</em>)</td>
</tr>
<tr>
<td>• A generic syntax item that you must replace with a specific value</td>
<td>• For more information, see the <em>Cisco ICM Software Database Schema Handbook</em>.</td>
</tr>
<tr>
<td>• A title of a publication</td>
<td></td>
</tr>
<tr>
<td>An arrow ( &gt; ) indicates an item from a pull-down menu.</td>
<td>The Save command from the File menu is referenced as <strong>File &gt; Save</strong>.</td>
</tr>
</tbody>
</table>
Organization

The manual is divided into the following chapters.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Introduction”</td>
<td>Provides an overview of Cisco CTI Object Server (CTI OS) and lists the tasks that a CTI OS system manager must perform.</td>
</tr>
<tr>
<td>Chapter 3, “CTI OS Client Installation”</td>
<td>Provides procedures for installing CTI OS Client components.</td>
</tr>
<tr>
<td>Chapter 4, “CTI OS Configuration”</td>
<td>Discusses how to use the Windows Registry Editor to configure CTI OS.</td>
</tr>
<tr>
<td>Chapter 5, “Startup, Shutdown, and Failover”</td>
<td>Explains how to start and stop CTI OS and its associated processes and describes how CTI OS handles failover scenarios.</td>
</tr>
<tr>
<td>Chapter 6, “Peripheral-Specific Support”</td>
<td>Discusses levels of CTI OS support for switch-specific features.</td>
</tr>
<tr>
<td>Appendix A, “Testing an Ethernet Card for Silent Monitor”</td>
<td>Provides a procedure to determine if a particular Ethernet NIC card driver will work with CTI OS Silent Monitor.</td>
</tr>
</tbody>
</table>

Other Publications

For additional information about Cisco Intelligent Contact Management (ICM) software and Cisco Computer Telephony Integration (CTI) products, see the Cisco web site listing ICM and CTI documentation.
Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:
http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:
http://www.cisco.com

International Cisco websites can be accessed from this URL:

Ordering Documentation

You can find instructions for ordering documentation at this URL:

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).
Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

http://www.cisco.com/tac/caseopen

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:


TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.
Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:
  

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
  

- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
  
  [http://www.ciscopress.com](http://www.ciscopress.com)

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
  

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
  
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
  
  http://www.cisco.com/ipj

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
  
Introduction

This chapter provides an overview of Cisco CTI Object Server (CTI OS) and lists the tasks that a CTI OS system manager must perform.

Overview of CTI OS

The Computer Telephony Integration Object Server (CTI OS) is Cisco’s next generation customer contact integration platform. CTI OS combines a powerful, feature-rich server and an object-oriented software development toolkit to enable rapid development and deployment of complex CTI applications. Together with the Cisco CTI Server Interface, CTI OS Server and CTI OS Client Interface Library (CIL) create a high performance, scalable, fault-tolerant three-tiered CTI architecture, as illustrated in Figure 1-1.
Figure 1-1  CTI OS Three-Tiered Architecture Topology

The CTI OS application architecture employs three tiers:

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

**Advantages of CTI OS as Interface to ICM**

CTI OS brings several major advances to developing custom CTI integration solutions. The CIL provides an object-oriented and event driven application programming interface (API), while the CTI OS server does all the ‘heavy-lifting’ of the CTI integration: updating call context information, determining which buttons to enable on softphones, providing easy access to supervisor features, and automatically recovering from failover scenarios.
Rapid integration. Developing CTI applications with CTI OS is significantly easier and faster than any previously available Cisco CTI integration platform. The same object oriented interface is used across programming languages, enabling rapid integrations in C++, Visual Basic, Java, or any Microsoft COM compliant container environment. CTI OS enables developers to create a screen pop application in as little as five minutes. The only custom-development effort required is within the homegrown application to which CTI is being added.

Complex solutions made simple. CTI OS enables complex server-to-server integrations and multiple agent monitoring-type applications. The CIL provides a single object-oriented interface that can be used in two modes: agent mode and monitor mode. See the Cisco ICM Software CTI OS Developer's Guide for an explanation of these two modes.

Fault tolerant. CTI OS is built upon the ICM NodeManager fault-tolerance platform, which automatically detects process failure and restarts the process, enabling work to continue. Upon recovery from a failure, CTI OS initiates a complete, system-wide snapshot of all agents, calls, and supervisors and propagates updates to all client-side objects.

Key Benefits of CTI OS for CTI Application Developers

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

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

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

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

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

## System Manager Responsibilities

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

- Creating and configuring an ODBC file Data Source Name on the CTI OS server machine (see Chapter 2, “CTI OS Server Installation”).
- Installing CTI OS Server (see Chapter 2, “CTI OS Server Installation”).
- Installing CTI OS Client components: CTI OS Agent Desktop, CTI OS Supervisor Desktop for IPCC Enterprise, CTI OS Developer’s Toolkit, IPCC Media Termination. and Silent Monitor. (see Chapter 3, “CTI OS Client Installation”).
- Use the Windows Registry Editor (regedit.exe) to configure the required CTI OS registry keys (see Chapter 4, “CTI OS Configuration”).
- Start CTI OS and its associated processes from ICM Service Control (see Chapter 5, “Startup, Shutdown, and Failover”).
You must have administrator privileges to perform the procedures discussed in this manual.

System Requirements

See the Release Notes for Cisco CTI OS Software Release 6.0 for a list of hardware and software requirements and for information on compatibility and interoperability with related Cisco and third party hardware and software.

Desktop User Accounts

On a Windows 2000 system, a user must be defined as a Power User to have user privileges comparable to the default user privileges of an NT user. Windows 2000 users must either be members of the Power User group or have their user privileges modified to enable them to run legacy applications and have read/write access to the Cisco registry keys that the desktop applications use. To set user privileges to enable users to run CTI OS Agent Desktop and CTI OS Supervisor Desktop for IPCC Enterprise, an administrator must perform the following steps.

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

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

**Step 3** Go to the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\CTI Desktop\Ctios
```

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

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

- **Click Add**. A Select Users dialog box appears.
- Select the user to be added from the list in the top half of the Select Users dialog box.
- **Click Add**, then click **OK**. You return to the Permissions dialog box; the user you just added is now in the list.
Step 6  Click on the user whose privileges you want to set.

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

Step 8  Click Apply.

Step 9  Click OK.

Step 10  Exit Registry Editor.

Network Topology for Silent Monitor

Silent Monitor provides a supervisor with a means to listen in on agent calls in IPCC call centers that use CTI OS. Supervisors can send Silent Monitor requests to agent desktops without the agent being aware of any monitoring activity. Voice packets sent to and received by the monitored agent’s IP hard phone or media termination device are captured from the network and sent to the supervisor desktop. At the supervisor desktop, these voice packets are decoded and played on the supervisor’s system sound card.

Note  Silent Monitor does not capture and translate DTMF digits that are pressed on either the CTI OS Agent Desktop or on an agent's hard phone.

The necessary network topology is shown in Figure 1-2.
Agents in this topology may have either an IP hard phone or IPCC Media Termination. (The supervisor in this topology must have an IP hardphone.) If the agent has an IP hard phone, it must have an agent desktop PC connected to the second IP port. If the agent has IPCC Media Termination, it must be installed on the same machine as the agent desktop.

A CTI OS based desktop application that implements the CTI OS Silent Monitor feature must be installed on the agent desktop and supervisor desktop PCs. In addition, CTI OS Silent Monitor software must be installed on the agent desktop PC and supervisor desktop PC (see Chapter 3, “CTI OS Client Installation”).
Calculating Additional Needed Bandwidth

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

For example, assume the following:

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

You should plan for network capacity for 100 + (20% of 100) concurrent calls, or 120 concurrent calls.

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

For example, the table on the Cisco Voice Over IP – Per Call Bandwidth Consumption website (http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.html#topic1) lists the per-call bandwidth on the G.711 codec (for a call with the default voice payload size) over Ethernet as 87.2 Kbps. You would multiply this 87.2 Kbps by 120 calls to obtain the total required network bandwidth.

For more information on per-call bandwidths for various codecs and network protocols, see the Cisco Voice Over IP - Per Call Bandwidth Consumption website at http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.html.

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

The following are the hardware and software requirements for IPCC Media Termination (see Chapter 3, “CTI OS Client Installation”).

Hardware Requirements

IPCC Media Termination requires the following hardware.

- An ethernet card
- A Full-duplex sound card. Full-duplex sound cards can capture audio and play audio at the same time, thus allowing a conversation. The sound cards on most computers are full-duplex; however in rare instances you may find a computer with a half-duplex card. If you observe one-way traffic only, you may have a half-duplex sound card installed in your computer.
- A two-plug headset (one plug for the microphone, one for speaker out).

Once you have installed the cards, plug the headset into your sound card. Run Microsoft’s Sound Recorder application and verify that you have microphone and voice. To run Sound Recorder, select **Start > Programs > Accessories > Entertainment > Sound Recorder**.

**Note** IPCC Media Termination is not supported on networks that are configured to use a VLAN for voice traffic.

Software Requirements

IPCC Media Termination requires the following software.

- Your call manager must be configured to accept auto-registering devices. To configure your call manager from CCMAdmin, select **System > Cisco Call Manager**. From the left, select the call manager configuration. Verify that Auto Registration is enabled.
If you have upgraded your system from Windows NT to Windows 2000, you must replace your Windows NT sound card drivers with Windows 2000 sound card drivers.

- Name or IP Address
- Port Number
- Audio Stream Port

Ensure that the **Enable Logging** box is checked.
CTI OS Server Installation

This chapter lists some guidelines to consider when you install CTI OS Server and provides procedures for the following tasks.

- Creating and configuring an ODBC file Data Source Name on the CTI OS server machine (optional).
- Installing CTI OS Server.

CTI OS Server Installation Guidelines

Following are some guidelines to consider when you install CTI OS Server.

- CTI OS is typically installed in a duplex configuration. Two CTI OS servers installed on separate systems work in parallel to provide redundancy. Installing only one CTI OS server would prevent failover recovery by client systems. See Chapter 5, “Startup, Shutdown, and Failover” for more information on CTI OS failover.
- CTI OS should be installed on the same subnet on which the PGs are installed.
- Ensure that your CTI OS system meets the minimum hardware and software requirements, as listed in the Release Notes for Cisco CTI OS Software Release 6.0.
Upgrading from a Previous Version

If you are upgrading from a previous release of CTI OS Server, you do not need to uninstall CTI OS Server before you install CTI OS Server Release 6.0.

ODBC File Data Source Name Creation

Agent name resolution is an optional feature used by the Agent and Supervisor Softphones. It maps an agent’s ID to the agent’s name.

If you wish to enable the CTI OS agent lookup feature, you must perform the following tasks before you install CTI OS Server:

- Create an ODBC file Data Source Name (DSN) on the CTI OS server machine.
- Configure it to access the ICM database or any relational DB whose schema for the agent table is the same as the ICM database.
- Adding and configuring the SQL User Login on the Loggers associated with the ODBC connection.

A file DSN stores information about a database connection in a file. The file has the extension .dsn and by default is stored in the $\text{Program Files}\backslash\text{Common Files}\backslash\text{ODBC}\backslash\text{Data Sources}$ directory.

The CTI OS Server install process prompts for the file DSN and creates the appropriate registry keys.

Note

If you are installing more than one CTI OS server, you must create and configure an ODBC DSN entry on each system.

To create a new file DSN, perform the following steps:

**Step 1**
From the Windows 2000 system menu, select Programs > Administrative Tools > Data Sources (ODBC).

**Step 2**
Select the File DSN tab.
Step 3 Specify the directory where you want the DSN file to be stored. On Windows 2000 systems, click the Set Directory button.

Step 4 Click the Add button. The Create New Data Source dialog box appears.

Step 5 Select SQL Server driver from the driver list.
Step 6  Click the Next button. The following dialog box appears, on which you enter the name for the File DSN you are creating.

![Create New Data Source](image1.jpg)

Step 7  Enter a name for your file. This process affixes a default extension of .dsn to the file name that you specify.

Step 8  Click the Next button. The following dialog box appears.

![Create New Data Source](image2.jpg)

Verify that the information in this dialog box is correct.
Step 9  Click the Finish button. The following dialog box appears.

Enter the name or IP Address of your SQL Server. (This should be the machine on which the ICM Logger is running.)

Step 10  Click the Next button. The following dialog box appears.

Step 11  Pick the SQL Server Authentication option. Enter the Login ID and password for the user that you choose to access the database. The user that you select must meet the following criteria.
The user that you choose to access the database must be defined within SQL as a valid user. If you need to create an SQL definition for this user, refer to your SQL Enterprise Manager documentation for instructions.

The user must have at least read access to the data.

You must also manually add the defined password for this user to the File DSN. The password definition line in the File DSN must be in the format

```
PWD=XXXXX
```

where XXXXX is the password in plain text.

**Step 12** Click the Next button. The following dialog box appears.

Click the Change the Default Database To box; select the ICM database from the drop down list. Accept the defaults for all other items.

**Step 13** Click the Next button. The following dialog box appears.
Accept all default settings in this dialog box.

**Step 14**  Click the Finish button. A dialog box similar to the following appears.

![Create a New Data Source to SQL Server dialog box](image)

**Step 15**  Double check this dialog box to ensure that the settings are correct. You can optionally test the data source.

**Step 16**  Click the OK button to end the process.
SQL User Login Configuration

On the machine on which the ICM Logger is running, you need to add and configure the SQL User Login that the ODBC connection will use to authenticate and poll the agent table to populate down to the CTI OS Supervisor Desktop for IPCC Enterprise.

Perform the following steps on the ICM Logger machine:

Step 1 Open Microsoft SQL Server Enterprise Manager. The main Enterprise Manager screen appears.
Step 2 On the left side of this screen, expand Microsoft SQL Servers.
Step 3 Expand SQL Server Group.
Step 4 Expand the server to which you want to add a SQL Server login account.
Step 5 Expand Security.
Step 6 Right-click Logins and click New Login. The SQL Server Login Properties - New Login dialog box appears.
Step 7 On the General tab, specify the default database for this login.
Step 8 On the Server Roles tab, select System Administrators.
Step 9 On the Database Access tab, select the database(s) that can be accessed by this login (i.e., the database(s) containing the agent table).
Step 10 Click OK.

For additional information on these procedures, see your SQL Server documentation.

Installing CTI OS Server

Perform the following steps to install the CTI OS Server.

Step 1 From the Server directory on the CD, run Setup.exe.
Step 2 Click Yes on the Software License Agreement screen.
Chapter 2  CTI OS Server Installation

Installing CTI OS Server

Step 3  A CTI OS Customer Information screen appears if your system does not have an ICM Peripheral Gateway (PG) defined.

Enter an ICM Customer Instance name and click Next. (Setup requires an instance name in order to start the Node server.)

Step 4  If you are installing CTI OS Server for the first time, an Enter Desktop Drive screen appears. Accept the default installation drive or select another drive from the pulldown list.

Step 5  Click the OK button. The CTI Server Information screen appears.
Enter the Name or IP Address and the Port Number for your CTI systems.

**Step 6**  Click the Next button. The Peripheral Identifier screen appears.

Specify the following information.
- A Logical Name for your peripheral. This can be any valid logical name that uniquely identifies your peripheral.
• The Peripheral ID associated with the switch your telephone is connected to
• The Peripheral Type of the switch your telephone is connected to

Note
You can specify information for only one peripheral during CTI OS Server setup. To configure additional peripherals, follow the procedure in the section “Automatic Agent Statistics Grid Configuration” in Chapter 4, “CTI OS Configuration.”

Step 7
Click the Next button. The Connection Information screen appears.

Enter the port number and heartbeat information for your CTI OS server instance.

Step 8
Click the Next button. The Statistics Information screen appears.
Enter the default polling interval for Skillgroup statistics (in seconds).

**Step 9**  
Click the Next button. The ODBC Connection screen appears.

Enter the names of the primary (Side A) and secondary (Side B) ODBC file DSN that you defined earlier in this chapter.

**Step 10**  
Click the Next button. The Peer CTI OS Server screen appears.
Installing CTI OS Server

**Step 11** If you are using more than one CTI OS Server, click the Duplex CTI OS Install box. Enter the following information:

- The server name or IP address of your other CTI OS server
- The port number on which your other CTI OS server receives client connections

**Step 12** Click the Finish button to begin installation. When installation is done, a Setup Complete screen appears.
Installing CTI OS Server

Step 13  Select Yes or No to specify whether or not you want to restart your computer following installation.

Step 14  Click Finish.

Note  In CTI OS Releases 6.0 and later, updates to Cisco CTI OS software (Engineering Specials, Service Releases and Maintenance Releases) are installed with Patch Manager. Once installation completes you cannot move any CTI OS files from the directories in which they are installed, or Patch Manager will be unable to perform CTI OS software updates correctly.
Uninstalling CTI OS Server

To uninstall CTI OS Server, rerun the Setup program for ICM Release 6.0 and delete the ICM Customer Instance that you specified during CTI OS Server Setup.

**Note**
If Release 6.0 software patches for any CTI OS components are installed on your machine, you must uninstall these patches before you uninstall the base Release 6.0 CTI OS Server software.

Determining Version Number of Installed Files

If CTI OS Server is currently running, the title bars of both the Ctidriver and Ctios Server process windows display the CTI OS version number and the build number.

If CTI OS Server is not running, you can determine the version number of an installed CTI OS Server file by performing the following steps.

**Step 1**
Open a window for the ICM\CTIOS_bin subdirectory.
Step 2  Highlight the file ctiosservernode.exe.

Step 3  Right click on the highlighted file.

Step 4  Select **Properties** from the dropdown menu. A properties dialog box appears.

Step 5  Select the Version tab. This tab contains version information (release number and build number) for the file.
Chapter 2  CTI OS Server Installation

Determining Version Number of Installed Files
CTI OS Client Installation

This chapter provides procedures for installing the following CTI OS Client Components:

- CTI OS Agent Desktop
- CTI OS Supervisor Desktop for IPCC Enterprise
- CTI OS Developer’s Toolkit and its associated Client Interface Libraries (C++, COM, Visual Basic, and Java)
- IPCC Media Termination
- Silent Monitor

It also provides procedures for enabling the Emergency Call and Supervisory Call buttons, which enable an agent to make a call to a supervisor, and for configuring IPCC Media Termination.

**Note**

Before you begin installation, verify that your system meets the hardware and software requirements for the components you plan to install, as listed in the Release Notes for Cisco CTI OS Software Release 6.0.

Upgrading from a Previous Version

If you are upgrading from a previous CTI OS release, you do not need to uninstall the CTI OS Client software before you install CTI OS Client Release 6.0.
CTI OS Client Component Installation

To install the CTI OS Client components, perform the following steps.

**Step 1**
From the Installs\CTIOSClient directory on the CD, run Setup.exe.

**Step 2**
Click the Next button on the Welcome screen. The Software License Agreement screen appears.

**Step 3**
Click the Yes button. The Choose Destination Location screen appears.
Chapter 3  CTI OS Client Installation

CTI OS Client Component Installation

Step 4   Accept the default destination directory or click the Browse button and specify another directory.

Step 5   Click the Next button. The Select Components screen appears.

Select the CTI OS Client components that you want to install.
Note

In order to install Media Termination or Silent Monitor, you must also select CTI OS Agent Desktop or CTI OS Supervisor Desktop for IPCC Enterprise.

Step 6
Click the Next button. If you selected CTI OS Agent Desktop or CTI OS Supervisor Desktop for IPCC Enterprise, the CTIOS Server Information screen appears.

Note
If you select Silent Monitor, an additional screen appears first. Please read this screen carefully; it contains important information about using Silent Monitor in a VLAN network.

Enter the Name or IP Address and the Port Number for your CTI OS systems.

Step 7
Click the Next button. If you selected the IPCC Media Termination component, the Media Termination Config screen appears.
Specify the following information:

- The name or IP address of your Cisco CallManager
- The port number of your Cisco CallManager
- The port for your remote IP phone (audio stream port)
- Whether you want to enable logging to a media client trace file for debugging purposes. The default and recommended setting is to enable logging.

**Step 8** Click the Next button. The Start Copying Files screen appears.

**Step 9** Click the Next button to begin installation.

**Step 10** When installation completes, the Setup Complete screen appears.
Step 11  Click the Finish button to exit Setup.

Note  In CTI OS Releases 6.0 and later, updates to Cisco CTI OS software (Engineering Specials, Service Releases and Maintenance Releases) are installed with Patch Manager. Once installation completes you cannot move any CTI OS files from the directories in which they are installed, or Patch Manager will be unable to perform CTI OS software updates correctly.

Installed Files

When you install CTI OS Agent Desktop or CTI OS Supervisor Desktop for IPCC Enterprise, the CTI OS Client installation process installs a number of dynamic link libraries (DLLs). The installation process registers many of these DLLs automatically, but some of these DLLs must be registered manually in order to work correctly.

Table 3-1 lists the Windows DLLs that are installed with CTI OS Agent Desktop or CTI OS Supervisor Desktop for IPCC Enterprise, along with the command line entry for manually registering the DLL (if needed).
### Table 3-1  Windows DLLs

<table>
<thead>
<tr>
<th>DLL</th>
<th>Command Line Entry For Manually Registering</th>
</tr>
</thead>
<tbody>
<tr>
<td>msvcrt.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>msvcrtd.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>msvcp60.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>msvcp60d.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>mfc42.dll</td>
<td>regsvr32 mfc42.dll</td>
</tr>
<tr>
<td>mfc42d.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>atl.dll</td>
<td>regsvr32 atl.dll</td>
</tr>
<tr>
<td>msvbvm60.dll</td>
<td>regsvr32 msvbvm60.dll</td>
</tr>
<tr>
<td>msvbvm60d.dll</td>
<td>regsvr32 msvbvm60d.dll</td>
</tr>
</tbody>
</table>

The following Softphone Controls DLLs are installed with CTI OS Agent Desktop or CTI OS Supervisor Desktop for IPCC Enterprise.

- CtiosStatusbar.dll
- EmergencyAssistCtl.dll
- AgentSelectCtl.dll
- GridControl.dll
- AgentStateCtl.dll
- HoldCtl.dll
- AlternateCtl.dll
- IntlResourceLoader.dll
- AnswerCtl.dll
- Arguments.dll
- BadLineCtl.dll
- ButtonControl.dll
- ChatCtl.dll
- ConferenceCtl.dll
- CtiCommonDlgs.dll
• MakeCallCtl.dll
• ReconnectCtl.dll
• CTIOSAgentStatistics.dll
• RecordCtl.dll
• CTIOSCallAppearance.dll
• SubclassForm.dll
• CTIOSClient.dll
• SupervisorOnlyCtl.dll
• CTIOSSessionResolver.dll
• TransferCtl.dll
• CTIOSSkillGroupStatistics.dll

If the CTI OS Agent Desktop or CTI OS Supervisor Desktop for IPCC Enterprise indicate that a given DLL is not registered, the DLL can be registered manually by the following command.

```
regsvr32 <DLL filename>
```

For example, CtiosStatusbar.dll would be registered by the following command.

```
regsvr32 CtiosStatusbar.dll
```

If you install IPCC Media Termination, the CTI OS Client installation process installs additional DLLs. Table 3-2 lists these DLLs and the command line entry for registering the DLL manually (if needed).

<table>
<thead>
<tr>
<th>DLL</th>
<th>Command Line Entry For Registering Manually</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ccnsmt.dll</td>
<td>regsvr32 ccnsmt.dll</td>
</tr>
<tr>
<td>TraceServer.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>Libg723.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>Kill.exe</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>MediaTerminationProcMonitor.exe</td>
<td>MediaTerminationProcMonitor.exe /regserver</td>
</tr>
<tr>
<td>MediaClient.exe</td>
<td>MediaClient.exe /regserver</td>
</tr>
</tbody>
</table>
Uninstalling CTI OS Client

To uninstall CTI OS Client, run Add/Remove programs from the Windows Control Panel and select Cisco CTI OS Client Uninstall.

Note

If Release 6.0 software patches for any CTI OS components are installed on your machine, you must uninstall these patches before you uninstall the base Release 6.0 CTI OS Client software.

Determining Version Number of Installed Files

If CTI OS Agent Desktop or CTI OS Supervisor Desktop for IPCC Enterprise are currently running, the title bars of the desktop windows display the CTI OS Client version number.

If these desktops are not currently running, you can determine the version number of an installed CTI OS Client file by performing the following steps.

Step 1  Go to the directory

Program Files\Cisco Systems\CTIOS Client\CTIOS Shared\COM

Step 2  Highlight and right click on the file ctiosclient.dll.

<table>
<thead>
<tr>
<th>DLL</th>
<th>Command Line Entry For Registering Manually</th>
</tr>
</thead>
<tbody>
<tr>
<td>DialTone.wav</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>MT_busy.wav</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>MT_fastbusy.wav</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>MT_ringing.wav</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>MT_ringback.wav</td>
<td>Registration not needed.</td>
</tr>
</tbody>
</table>

Table 3-2  IPCC Media Termination DLLs (continued)
Chapter 3      CTI OS Client Installation

Determining Version Number of Installed Files

Step 3  Select Properties from the dropdown menu. A properties dialog box appears.

Step 4  Select the Version tab. This tab contains version information (release number and build number) for the file.
Configuring Supervisory Assistance Features

The CTI OS Agent Desktop includes buttons that enable an agent to make an emergency call to a supervisor or to place a call to request assistance from a supervisor. To enable the functionality for these buttons, an ICM system administrator must perform the following steps.

**Step 1** On the ICM Configuration Manager Dialed Number List screen, create a Dialed Number for the supervisor, as shown in the following screens.
Step 2  On the ICM Configuration Manager Agent Team List screen, enter the Dialed Number in the Supervisor script dialed number field, as shown.
Step 3  On the Script Editor Call Type Manager screen, associate the Dialed Number with your script, as shown.
IPCC Media Termination

The IPCC Media Termination component is a soft alternative to the IP hard phone. IPCC Media Termination resides on the desktop. When used in conjunction with a softphone, IPCC Media Termination transmits and receives audio over an IP connection.

**Note**

IPCC Media Termination is not supported on networks that are configured to use a VLAN for voice traffic.

This section describes how to configure the IPCC Media Termination.
Configuring the Media Termination Device

Note You must complete CTI OS Client component installation before you perform the procedures in this section.

Note The procedures in this section should be performed by the ICM system administrator.

The media termination component (mediaclient.exe) runs as a service on the agent desktop. When it starts, it automatically registers itself with the call manager.

Each media endpoint is uniquely identified by a MAC address read off the Ethernet card encountered. The ipconfig –all command shows the mac address (aka physical Address) read off the Ethernet card. For example:

```
ipconfig -all
Physical Address. . . . . : 00-10-5A-5E-36-FC
```

In this example, the MAC address is registered with your Cisco CallManager as 30 SP+ phone device SEP00105A5E36FC.

Media Termination Device configuration includes the following steps.

Verifying Auto-Registration

Step 1 From the Cisco CallManager Main Menu (CCMAdmin), select Device > Phone.

Step 2 Search by Directory Number to find all phones.

You should see a new entry for your MAC address and the auto-registered number assigned to that address. You need not do anything additional to complete the auto registering step, just verify that it worked and note the dialed number assigned to that device.
### Associating the New Device with the IPCC PG User

**Step 1** From the Cisco CallManager Main Menu (CCMAdmin), select User > Global Directory.

**Step 2** Select the user that represents the IPCC PG (for example, PG User).

**Step 3** Scroll to the bottom of the dialog and press the Associate Devices button.

**Step 4** Click on the Select Devices button, then click OK.

**Step 5** Check the box next to the device name (for example, mac address SEP00105A5E36FC) and extension that matches the Agent’s PC.

**Step 6** Click Update to complete the process.

### Add a New Agent

From the ICM Configuration Manager, perform the following steps to add a new agent.

**Step 1** Navigate to the Peripherals > Agent > Agent Explorer dialog box.

**Step 2** Select the desired peripheral from the pulldown list.

**Step 3** On top left of screen, click Retrieve.

**Step 4** On bottom left of screen, click Add Agent.

**Step 5** On top right of screen, click on the Agent Tab.

**Step 6** Click the Select Person button to pull information out from the Person List for the new agent.

**Step 7** Choose appropriate desk settings for the agent.

**Step 8** Click OK.

**Step 9** Click on the Skill Group Membership Tab.

**Step 10** Click Add.

**Step 11** Choose appropriate skill group(s) for the agent.
Step 12  Click OK.

If you are adding a Supervisor agent, perform the following additional steps.

Step 1  Click on the Supervisor tab.
Step 2  Check the Supervisor Agent box to identify this agent as a supervisor.
Step 3  Enter the supervisor’s Login and Password.
Step 4  Click the Save button.

Adding Media Termination Device Target and Label

Using the ICM Configuration Manager, perform the following steps to add a new device target and label for the IPCC Media Termination device.

Step 1  Bring up the Targets > Device Targets > Device Target Explorer dialog box.
Step 2  On top left of screen, click on Retrieve
Step 3  On bottom left of screen, select Add Device Target.
Step 4  Enter the following Device Target information:
   - Name (for example, 4088535110)
   - Global Address (not the IP address, must be a unique value; for example, MT5110)
   - Config Para (for example, /devtype Cisco Phone /dn 5110)
   - Description (for example, Media Termination ext. 5110)
Step 5  On bottom left of screen, click on the Add Label button.
Step 6  Enter the following label information:
   - Routing Client (for example, CCM_PG_1)
   - Label (for example, 5110)
   - Label type (for example, Normal)
   - Description (for example, Media Termination label 5110)
Step 7  
Click the Save button to complete the process.

Note that device targets are dynamically associated with agent id’s during the agent login process. This means that once you have configured the device target, just login with a peripheral number (agentID) from the agent table.

You can verify that the PIM sees the new device by running the following commands.

```
procmon mt pgla pim1  (substitute your site specific arguments)
>>>mhelp (to see cmds)
>>>leadt (for list EA device targets)
```

You should not have to reboot to see a new device.

You should now be able to successfully login agent on the media termination device.

**Setting Full Control Permissions to the Registry**

To ensure good voice quality, you *must* give the Media Termination user Full Control permissions to the Registry. To do this, perform the following steps:

---

**Step 1**  
Run regedt32.exe (not regedit.exe).

**Step 2**  
Go to the HKEY_CURRENT_USER\Software\Cisco Systems key and select it.

**Step 3**  
From the menu select **Security > Permissions**. A dialog box appears.

**Step 4**  
Select the user who will be running the softphone using Media Termination. For **Type of Access** for this user, select Full Control. If there is a checkbox indicating that subkeys should also have the same permission, make sure this box is also checked.

---

This will enable a Media Termination application user who does not have administrative privileges to write to the registry, ensuring good voice quality.
Using Media Termination when using VPN

When an agent uses a Media Termination softphone across a VPN connection, the agent receives no audio on the call even though the other party can hear him/her. This is due to a confusion of IP addresses that causes the audio to be sent to the wrong IP address.

CTI OS addresses this behavior as follows:

- A special web page (filename “vpn_ip.jsp”) is included on the Install CD for the CTI OS Client components. This web page will return the correct IP Address when requested by the MediaClient if it resides on a web server within the corporate network. To install this web page, copy the file “vpn_ip.jsp” from the install CD to the public directory (or to a subdirectory of the public directory) of a web server that can handle jsp (Java Server Pages).

  You must configure MediaClient to point to this web page. To do this, add a string value under the Registry key HKEY_CURRENT_USER/Software/Cisco Systems/IPMedia on the Media Termination machine. This value should have the name “URL” and the value of “<IPAddressofWebServer>/<your directory name>/vpn_ip.jsp” without “http://” where < IPAddressofWebServer > is in the form xxx.xxx.xxx.xxx, or machine name as shown in the following examples;

  - 120.22.130.67/VPN/vpn_ip.jsp
  - mymachine/VPN/vpn_ip.jsp

- When starting up, be sure to connect to VPN successfully before starting the softphone. Upon softphone startup, MediaClient will read this key and make an http request to determine the correct IP address.

This workaround may not work if Network Address Translation (NAT) is disabled.

Troubleshooting

The media termination component (mediaclient.exe) generates log files that are placed in the IPmedia directory under the install directory you specified during CTI OS Client component setup. Search for files named TraceFile*. 
You can stop the media termination device by stopping the Cisco Media Termination Service.

Login attempt fails due to INVALID_LOGON_DEVICE_SPECIFIED: The request specified an invalid logon device. Ask your ICM administrator to verify that the device target’s global address for this media termination device is a unique string. It must not be an IP address.

**Uninstalling Media Termination**

To uninstall IPCC Media Termination, run Add/Remove programs from the Windows Control Panel.
Chapter 3  CTI OS Client Installation

IPCC Media Termination
CTI OS Configuration

The CTI OS Server install process initializes a configuration that is stored in the Windows System Registry database. This configuration is accessible and editable through the Windows Registry Editor (regedit.exe). Figure 4-1 shows the Registry Editor main window.

Figure 4-1  Windows Registry Editor Main Window
To add a key or registry value under an existing key, perform the following steps:

**Step 1** Highlight the existing key in the lefthand panel.

**Step 2** Position the cursor in the righthand panel.

**Step 3** Click the right mouse button. A popup menu appears.

**Step 4** From the popup menu, select Key, String Value, Binary Value, or DWORD value. If you select Key, a placeholder for the key you want to add appears highlighted in the lefthand panel. For other items, a placeholder for the item you want to add appears highlighted in the righthand panel.

**Step 5** Right click on the highlighted item. A popup menu appears.

- To name the item, select Rename from the popup menu then type the new name for the item.
- To set the value data for String, Binary, and DWORD values, select Modify. A dialog box appears. Enter the value data following the Value Data prompt.

To edit an existing key or registry value, highlight the key or value and right click on it. Select Modify, Delete, or Rename from the popup menu and proceed.

This chapter discusses the required values for the following CTI OS registry keys:

- CTI Driver
- EMS Tracing
- Server
- Mainscreen
- Connection Profiles
- Call Appearance
- ECC Variables
- Peripherals

**Note** Except where otherwise indicated, the CTI OS Registry keys discussed in this chapter are local and start at the [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS<InstanceName>\CTIOS<ServerName>] path.
Note About Registry Directories in Previous CTI OS Releases

In CTI OS Releases prior to 6.0, the [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.] directory was named [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems]. If you upgrade from a previous release of CTI OS Software to Release 6.0, the installation procedure automatically copies the contents of the old Cisco Systems directory to the new Cisco Systems Inc. directory and deletes the old directory.

CTI Driver

The CTI Driver key includes registry settings required for CTI Server connection. The CTI Driver key contains one key, the Config key. Table 4-1 describes the CtiDriver/Config key registry values.

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientID</td>
<td>String Value</td>
<td>The identifier of the CTI Client. This will be displayed in the CTI Server log file to help identify which session the CTI OS Server is connected on.</td>
<td>CTIOSServer</td>
</tr>
<tr>
<td>ClientPassword</td>
<td>String Value</td>
<td>The password of the CTI Client. This will be displayed in the CTI Server log file to help identify which session the CTI OS Server is connected on.</td>
<td>CTIOSServer</td>
</tr>
<tr>
<td>ClientSignature</td>
<td>String Value</td>
<td>The signature of the CTI Client. This will be displayed in the CTI Server log file to help identify which session the CTI OS Server is connected on.</td>
<td>CTIOSServer</td>
</tr>
<tr>
<td>SideAHost</td>
<td>String Value</td>
<td>The CTI Server (sideA) IP address or hostname to which the CtiDriver should connect.</td>
<td>Host specified during CTI Server installation.</td>
</tr>
<tr>
<td>SideAPort</td>
<td>DWORD Value</td>
<td>The CTI Server (sideA) IP port to which the CtiDriver should connect.</td>
<td>Port specified during CTI Server installation.</td>
</tr>
</tbody>
</table>
### EMS Tracing Values

The registry keys located at [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<customer_instance_name>\CTIOSComponent Name\EMS\CurrentVersion\Library\Processes\ctios] and

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>SideBHost</td>
<td>String Value</td>
<td>The CTI Server (sideB) IP address or hostname to which the CtiDriver should connect.</td>
<td>Host specified during CTI Server installation.</td>
</tr>
<tr>
<td>SideBPort</td>
<td>DWORD Value</td>
<td>The CTI Server (sideB) IP port to which the CtiDriver should connect.</td>
<td>Port specified during CTI Server installation.</td>
</tr>
<tr>
<td>Heartbeat Interval</td>
<td>DWORD Value</td>
<td>The interval (in seconds) at which HEARTBEAT_REQ messages should be sent to the CTI Server.</td>
<td>5</td>
</tr>
<tr>
<td>ServicesMask</td>
<td>DWORD Value</td>
<td>The services requested from the CTI Server.</td>
<td>0x00000296 (52)</td>
</tr>
<tr>
<td>CallMsgMask</td>
<td>DWORD Value</td>
<td>The unsolicited call events requested from the CTI Server.</td>
<td>0x00ffffff (16777215)</td>
</tr>
<tr>
<td>AgentStateMask</td>
<td>DWORD Value</td>
<td>The agent states requested from the CTI Server.</td>
<td>0x000003ff (1023)</td>
</tr>
<tr>
<td>ProtocolVersion</td>
<td>DWORD Value</td>
<td>The highest protocol version to use when connecting to the CTI Server. The highest common denominator will be used when establishing the CTI Session.</td>
<td>9</td>
</tr>
<tr>
<td>IdleTimeout</td>
<td>DWORD Value</td>
<td>The session inactivity timeout (in seconds). The CTI Server will disconnect clients after this time threshold has elapsed without other socket messages.</td>
<td>0x7fffffff (2147483647)</td>
</tr>
<tr>
<td>MemoryPoolSize</td>
<td>DWORD Value</td>
<td>Size of the memory pool, in bytes.</td>
<td>0x00000064 (100)</td>
</tr>
</tbody>
</table>
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\ICM\<customer_instance_name>\<CTIOSComponentName>\EMS\CurrentVersion\Library\Processes\ctidriver] define the settings for Event Management System (EMS) tracing. Table 4-2 lists the registry values for these keys.

Table 4-2 Registry values for EMS Tracing

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMSDisplayToScreen</td>
<td>DWORD Value</td>
<td>If set to 1, EMS routines will attempt to write formatted messages to standard output.</td>
<td>0</td>
</tr>
<tr>
<td>EMSAllLogFilesMax</td>
<td>DWORD Value</td>
<td>The maximum total number of bytes that the EMS library will write to all local log files.</td>
<td>5000000</td>
</tr>
<tr>
<td>EMSBreakOnExit</td>
<td>DWORD Value</td>
<td>If set to 1, EMS exit routines will invoke the Debugger.</td>
<td>0</td>
</tr>
<tr>
<td>EMSBreakOnInit</td>
<td>DWORD Value</td>
<td>If set to 1, EMS initialization routines will invoke the Debugger.</td>
<td>0</td>
</tr>
<tr>
<td>EMSDebugBreak</td>
<td>DWORD Value</td>
<td>If set to 1, EMS failure routines invoke the Debugger before exiting the process.</td>
<td>1</td>
</tr>
<tr>
<td>EMSLogFileCountMax</td>
<td>DWORD Value</td>
<td>The maximum number of log files that the EMS library will write.</td>
<td>10</td>
</tr>
<tr>
<td>EMSLogFileLocation</td>
<td>String Value</td>
<td>The directory where the EMS library will create local log files.</td>
<td>Default directory specified at installation.</td>
</tr>
<tr>
<td>EMSLogFileMax</td>
<td>DWORD Value</td>
<td>The maximum number of bytes that the EMS library will write to a single local log file.</td>
<td>500000</td>
</tr>
<tr>
<td>EMSNTEventLogLevel</td>
<td>DWORD Value</td>
<td>The minimum severity event that EMS will log in the Application Event Log.</td>
<td>0xFFFFFFFF</td>
</tr>
<tr>
<td>EMSTraceMask</td>
<td>DWORD Value</td>
<td>A bitmask that specifies the levels of EMS tracing that are enabled.</td>
<td>7</td>
</tr>
</tbody>
</table>
The Server registry key contains CTI OS Server related configuration information. It contains the following subkeys:

- Agent
- AgentInfoLookup
- CallObject
- Connections
- Device
- Peers
- Peripherals
- SkillGroup
- Supervisor
- TimerService

### Agent

The Agent key contains agent related configuration information. Table 4-3 lists the registry values for the Agent key.

<table>
<thead>
<tr>
<th>EMSUserData</th>
<th>DWORD Value</th>
<th>Placeholder for arbitrary binary user data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMSForwardLevel</td>
<td>DWORD Value</td>
<td>The minimum severity event that EMS will forward to the ICM central controller.</td>
</tr>
</tbody>
</table>

0
### Table 4-3 Registry values for [Server\Agent]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentChatLevel</td>
<td>string</td>
<td>Defines the call center personnel with whom an agent is permitted to chat. This must be set to one of the values listed in Table 4-4.</td>
<td>TeamSupervisors</td>
</tr>
<tr>
<td>EnableWrapupDialog</td>
<td>DWORD Value</td>
<td>When enabled (1), a Wrapup dialog box pops up at the end of the call. A value of 0 disables this feature.</td>
<td>1</td>
</tr>
<tr>
<td>LogoutReasonRequired</td>
<td>DWORD Value</td>
<td>On all switches except IPCC, when enabled (1) a Logout Reason Code dialog box pops up when changing state to Logout. On all switches, a value of 0 disables this feature.</td>
<td>1 for Spectrum, 0 for all other switches</td>
</tr>
<tr>
<td>NotReadyReasonRequired</td>
<td>DWORD Value</td>
<td>On all switches except IPCC, when enabled (1) a Not Ready Reason Code dialog box pops up when changing state to NotReady. On all switches, a value of 0 disables this feature.</td>
<td>0</td>
</tr>
<tr>
<td>PollForAgentStatsAtEndCall</td>
<td>DWORD Value</td>
<td>Controls when agent statistics are sent from CTI OS Server to CTI OS clients. A value of 0 means that agent statistics are sent at a regular interval (specified in PollingIntervalSec). A value of 1 means that agent statistics are sent only when a call ends.</td>
<td>1</td>
</tr>
<tr>
<td>PollingIntervalSec</td>
<td>DWORD Value</td>
<td>The agent statistics polling interval, in seconds.</td>
<td>15</td>
</tr>
<tr>
<td>WrapupDataRequired</td>
<td>DWORD Value</td>
<td>When enabled (1), wrapup data is mandatory. When disabled (0), wrapup data is not required. Not applicable to IPCC agents.</td>
<td>0</td>
</tr>
</tbody>
</table>
Note

Changing the value of PollForAgentStatsAtEndCall may degrade performance and is not recommended.

The Agent key also contains the following subkeys:

- ReasonCodes
- WrapupStrings

**ReasonCodes**

The ReasonCodes key is a site-specific key that defines the reason codes the CTI OS Agent Desktop uses. For each reason code, a string is mapped to an unsigned short value. The CTI OS Agent Desktop displays the string and sends the appropriate value to the CTI Server, which in turn passes the value along to the ACD.

The ReasonCodes key contains two subkeys:

- **Logout**. This key defines the reason codes that appear on the Select Reason: Logout screen when an agent logs out. Immediately following CTI OS Server installation, the Logout registry key contains four values that serve as placeholders for Logout reason codes (see Table 4-5).

---

**Table 4-4  AgentChatLevel Values**

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>All agent chat disabled.</td>
</tr>
<tr>
<td>PrimarySupervisor</td>
<td>Agents can chat only with primary supervisor of their team.</td>
</tr>
<tr>
<td>TeamSupervisors</td>
<td>Agents can chat with the primary or secondary supervisor of their team.</td>
</tr>
<tr>
<td>Team</td>
<td>Agents can chat with anyone in team.</td>
</tr>
<tr>
<td>Unrestricted</td>
<td>Agents can chat with anyone on the same peripheral.</td>
</tr>
</tbody>
</table>

---
Table 4-5  Initial Contents of [Server\Agent\ReasonCodes\Logout]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert logout reason code 1 here</td>
<td>DWORD Value</td>
<td>Placeholder for first Logout reason code.</td>
</tr>
<tr>
<td>Insert logout reason code 2 here</td>
<td>DWORD Value</td>
<td>Placeholder for second Logout reason code.</td>
</tr>
<tr>
<td>Insert logout reason code 3 here</td>
<td>DWORD Value</td>
<td>Placeholder for third Logout reason code.</td>
</tr>
<tr>
<td>Insert logout reason code 4 here</td>
<td>DWORD Value</td>
<td>Placeholder for fourth Logout reason code.</td>
</tr>
</tbody>
</table>

To define the text that appears for each Logout reason code in the Select Reason dialog box, set the value data associated with the reason code to the text you want to appear for that reason code. You may also add additional reason code entries as needed.

- **NotReady.** This key defines the reason codes that appear in the Select Reason: NotReady dialog box when an agent goes to NotReady state. As with the Logout key, the NotReady key initially contains four placeholder DWORD values that you can edit to define the reason codes in the Select Reason: NotReady dialog box.

**WrapupStrings**

The WrapupStrings key defines the predefined wrapup text strings that appear in the softphone Wrapup dialog box. The WrapupStrings key contains a subkey, Incoming, that defines the wrapup text for incoming calls. Immediately following CTI OS Server installation, the Incoming key contains the registry values listed in Table 4-6.
To define the text that appears for each wrapup text string in the WrapUp dialog box, set the value data associated with the reason code to the text you want to appear for that wrapup string. You may also add additional wrapup string entries as desired.

**Note**
There are no CTI OS registry keys for defining text for outgoing wrapup strings. The ICM does not save any wrapup data for outgoing calls, therefore you do not need to define outgoing wrapup strings.

---

### Table 4-6 Initial Contents of `[Server\Agent\WrapupStrings\Incoming]`

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String0</td>
<td>String Value</td>
<td>Placeholder for first wrapup text string.</td>
</tr>
<tr>
<td>String1</td>
<td>String Value</td>
<td>Placeholder for second wrapup text string.</td>
</tr>
<tr>
<td>String2</td>
<td>String Value</td>
<td>Placeholder for third wrapup text string.</td>
</tr>
<tr>
<td>String3</td>
<td>String Value</td>
<td>Placeholder for fourth wrapup text string.</td>
</tr>
</tbody>
</table>

---
AgentInfoLookup

The AgentInfoLookup key defines the pathnames associated with the primary and secondary ODBC data source files, which CTI OS uses to look up agent names. The AgentInfoLookup key contains the registry values shown in Table 4-7.

Table 4-7 Registry values for [Server\AgentInfoLookup]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBpathA</td>
<td>String Value</td>
<td>The complete pathname of the primary ODBC source file.</td>
<td>Pathname specified during CTI OS Server setup.</td>
</tr>
</tbody>
</table>

CallObject

The CallObject key defines the values pertaining to call objects. Table 4-8 defines the CallObject key registry values.

Table 4-8 Registry values for [Server\CallObject]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentPreCallEvent Timeout</td>
<td>DWORD Value</td>
<td>Length of time, in seconds, within which an AGENT_PRE_CALL_EVENT must be followed by a BEGIN_CALL_EVENT or the call object will be deleted.</td>
<td>30</td>
</tr>
</tbody>
</table>
Table 4-8  Registry values for [Server\CallObject] (continued)

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPCCConference_</td>
<td>DWORD Value</td>
<td>When set to 1, allows all parties of a Conference to add new parties to the conference as supported by CallManager Version 4.0. If running against an earlier version of CallManager, this should be set to 0. If this is not set to 0 when running against an earlier version of Call Manager, and a non-controller Conference party tries to make a Consult Call for a Conference, the party will receive a Control Failure.</td>
<td>1</td>
</tr>
<tr>
<td>SupportsMultipleControllers</td>
<td>DWORD Value</td>
<td>Controls how often (in seconds) the trash collector activates and removes any stale objects from memory. A value of 0 disables the trash collector.</td>
<td>7200</td>
</tr>
</tbody>
</table>

Connections

The Connections key defines the values for client connections to the CTI OS Server. Table 4-9 defines the Connections key registry values.

Table 4-9  Registry values for [Server\Connections]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>HeartbeatIntervalMs</td>
<td>DWORD Value</td>
<td>The number of milliseconds between heartbeats from the server to its clients.</td>
<td>60000</td>
</tr>
<tr>
<td>HeartbeatRetrys</td>
<td>DWORD Value</td>
<td>The number of missed heartbeats before a connection is closed for unresponsiveness.</td>
<td>5</td>
</tr>
<tr>
<td>ListenPort</td>
<td>DWORD Value</td>
<td>The TCP/IP port on which the CTI OS Server listens for incoming client connections.</td>
<td>Port specified during CTI OS Server setup.</td>
</tr>
</tbody>
</table>
The heartbeating mechanism uses the HeartbeatIntervalMs and HeartbeatRetrys values together to determine when a connection is stale and should be closed. The interval serves as a timeout and the retries is the number of attempts that have timed out before closing the socket.

Example with an interval of 5000ms and 3 retries:

- After 5000ms (5sec Total time), if the server has not heard from the client it sends a heartbeat request and increments the retry count to 1.
- After 5000ms (10sec Total time), if the server has not heard from the client it sends a heartbeat request and increments the retry count to 2.
- After 5000ms (15sec Total time), if the server has not heard from the client it sends a heartbeat request and increments the retry count to 3.
- After 5000ms (20sec Total time), if the server still has not heard from the client, the connection is reported failed and the socket is closed.

To disable heartbeating, set the HeartbeatIntervalMs value to 0.

A Retry value of 0 will cause the connection to timeout after the interval without sending any heartbeat.

Device

The Device registry key contains one value, SnapshotDelaySec. This is a reserved value that should not be changed.

Peers

The Peers registry key informs a CTI OS Server about other CTI OS servers. This allows CTI OS servers to make direct connections with one another for the purposes of routing internal messages. On startup, CTIOSServerNode reads this key and opens client connections to all peer servers.

The Peers key contains the values listed in Table 4-10.
In addition, there must be a subkey for each peer server to which the current server will connect. The key name is the hostname or IP address of the peer server; for example, "HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOSInstanceName>\<CTIOServerName>\Server\Peers\DallasCTIOS". Each such subkey must contain the registry value listed in Table 4-11.

**Table 4-11  Registry values for [Server\Peers] Subkeys**

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>DWORD Value</td>
<td>The number of the TCP/IP port that the peer server is listening for client connection on.</td>
<td></td>
</tr>
</tbody>
</table>

**Peripherals**

The Peripherals key stores the maps of valid PeripheralID and Peripheral Types. On CTI OS System startup, these mappings are read into a map which creates the appropriate peripheral-type objects on the server.

This information must correspond to the ICM database Peripheral table Peripheral.PeripheralID and Peripheral.ClientType. While the values in ClientType are not equal to the PeripheralTypes, there is a one-to-one relationship between ClientTypes and PeripheralTypes.

The symbol PERIPHERAL_LOGICAL_NAME can be any logical name that uniquely identifies a Peripheral, such as “Phoenix ACD 1.” This is equivalent to the Peripheral.EnterpriseName logical name in the ICM database. There should be one entry for each valid Peripheral at this site.
Table 4-12 lists the Peripherals key registry values.

Table 4-12  Registry values for [Server\Peripherals\PERIPHERAL_LOGICAL_NAME]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PeripheralID</td>
<td>DWORD</td>
<td>The PeripheralID configured in the ICM database for this Peripheral.</td>
</tr>
<tr>
<td>PeripheralType</td>
<td>DWORD</td>
<td>The PeripheralType corresponding to this PeripheralID.</td>
</tr>
</tbody>
</table>

Examples:

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\<CTIOS InstanceName>\<CTIOSServerName>\Server\Peripherals\G3 ACD]
"PeripheralID"=dword:00001388
"PeripheralType"=dword:00000005

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\<CTIOS InstanceName>\<CTIOSServerName>\Server\Peripherals\Aspect ACD]
"PeripheralID"=dword:00001390
"PeripheralType"=dword:00000001

SkillGroup

The SkillGroup key defines skill group configuration values. Table 4-13 lists the SkillGroup key registry values.

Table 4-13  Registry values for [Server\SkillGroup]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>PollingInterval Sec</td>
<td>DWORD</td>
<td>The SkillGroup statistics polling interval, in seconds.</td>
<td>15</td>
</tr>
</tbody>
</table>

Supervisor

The Supervisor key contains supervisor related configuration information. Table 4-14 lists the registry values for the Supervisor key.
TimerService

The TimerService key specifies configuration parameters for the CTI OS Server’s internal TimerService. Table 4-16 lists the registry values for the TimerService key.

Table 4-16  Registry values for [Server\TimerService]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResolutionSec</td>
<td>DWORD Value</td>
<td>The interval at which the TimerService services queued requests, expressed in seconds.</td>
<td>1</td>
</tr>
</tbody>
</table>

MainScreen

The MainScreen key, located at [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\ScreenPreferences\
Configuring IPCC Silent Monitor

The IPCCSilentMonitor key contains silent monitor configuration information. The IPCCSilentMonitor key contains one subkey, named Settings.

The IPCCSilentMonitor configuration settings are declared in the registry of each server on the following location.

\[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems Inc.\ CTIOS\<CTIOS InstanceName>\<CTIOS ServerName>\EnterpriseDesktopSettings\All Desktops\IPCCSilentMonitor\Name\Settings\]

The Settings subkey contains the parameters used by the silent monitor subsystem to establish a monitoring session between a supervisor and a monitored agent. The values are listed in Table 4-18.

### Table 4-17 MainScreen Registry Key Values

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>BringToFrontOnCall</td>
<td>DWORD Value</td>
<td>When enabled (1), the softphone window is raised above all other windows when a BeginCallEvent occurs.</td>
<td>1</td>
</tr>
<tr>
<td>FlashOnCall</td>
<td>DWORD Value</td>
<td>When enabled (1), the softphone icon on the taskbar flashes when a BeginCallEvent occurs.</td>
<td>0</td>
</tr>
<tr>
<td>RecordingEnabled</td>
<td>DWORD Value</td>
<td>Controls whether the Record button is enabled on the Agent and Supervisor Softphones (0 = disabled, 1 = enabled).</td>
<td>0</td>
</tr>
<tr>
<td>AgentStatistics IntervalSec</td>
<td>DWORD Value</td>
<td>Controls how often (in seconds) the Agent and Supervisor Softphones update time-in-state agent statistics.</td>
<td>0xF</td>
</tr>
</tbody>
</table>
Defining Connection Profiles

The ConnectionProfiles key contains an organized list of the connection information of all configured CTI OS servers present in the corporate network that can be accessed by a client application. The connection profiles are defined in the registry of each server at the following location:

```
HKLM\SOFTWARE\Cisco Systems Inc.\CtiOs\<CTIOS InstanceName>\<CTIOWServerName>\ EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name
```

To create a profile for a given server, you must define a subkey under ConnectionProfiles\Name with the following format:

```
"PeripheralID"=dword:5000
"Heartbeat"=dword:00000000
"MaxHeartbeats"=dword:00000005
"CtiOsA"="HostName_A"
"CtiOsB"="HostName_B"
"PortA"=dword:0000a42c
"PortB"=dword:0000a42c
"AutoLogin"=dword:00000001
"ShowFieldBitMask"=dword:00000003
"WarnIfAlreadyLoggedIn"=dword:00000001
```

### Table 4-18 Settings Registry Subkey Values

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>HeartbeatInterval</td>
<td>DWORD value</td>
<td>The time in seconds between consecutive heartbeats.</td>
<td>5</td>
</tr>
<tr>
<td>HeartbeatTimeout</td>
<td>DWORD value</td>
<td>The amount of time in seconds that must elapse without receiving data before a disconnect is signaled</td>
<td>15</td>
</tr>
<tr>
<td>MediaTerminationPort</td>
<td>DWORD value</td>
<td>Reserved. This is the TCP/IP port that the silent monitor subsystem uses to render monitored audio.</td>
<td>4000</td>
</tr>
<tr>
<td>MonitoringIPPort</td>
<td>DWORD value</td>
<td>This is the TCP/IP port on the monitoring application to which the monitored application sends monitored audio.</td>
<td>39200</td>
</tr>
</tbody>
</table>
Table 4-19 describes the required ConnectionProfiles key registry values.

<table>
<thead>
<tr>
<th>SubKey/Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CtiOsServerName</td>
<td>The name given to the profile. This string is displayed on the Login Dialog when a user is about to login using the CTI OS Agent State Control.</td>
</tr>
<tr>
<td>PeripheralID</td>
<td>The numeric value of the peripheral the CTI OS Server will be connecting to.</td>
</tr>
<tr>
<td>Heartbeat</td>
<td>Time interval between heartbeat messages between the client and CTI OS Server.</td>
</tr>
<tr>
<td>MaxHeartbeats</td>
<td>Maximum number of heartbeats that can be missed by the CTI OS Client Session before failover occurs.</td>
</tr>
<tr>
<td>CtiOsA</td>
<td>DNS name of IP Address of the primary CTI OS Server a client application can connect to.</td>
</tr>
<tr>
<td>CtiOsB</td>
<td>DNS name of IP Address of the secondary CTI OS Server a client application can connect to.</td>
</tr>
<tr>
<td>PortA</td>
<td>TCP/IP port number assigned to the primary server.</td>
</tr>
<tr>
<td>PortB</td>
<td>TCP/IP port number assigned to the secondary server.</td>
</tr>
<tr>
<td>AutoLogin</td>
<td>Indicates if the client must automatically login an agent or supervisor after it has recovered from a system failure. For all peripherals other than IPCC this field must be set to 0x00000000. For IPCC, set this field to 0x00000001.</td>
</tr>
<tr>
<td>ShowFieldBitMask</td>
<td>Indicates what fields will be displayed in the CTI OS Login dialog box. Fields are displayed on the dialog box only if their corresponding bit in the mask is on. The possible fields and their corresponding masks are shown in Table 4-20. The default value at setup for ShowFieldBit Mask is 0x00000003 (Instrument and Password displayed).</td>
</tr>
</tbody>
</table>
Table 4-19 *ConnectionProfiles Key Registry Values (continued)*

<table>
<thead>
<tr>
<th>SubKey/Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WarnIfAlreadyLoggedIn</td>
<td>Indicates whether to display a warning but still permit login if an agent who is already logged in attempts to log in again. A value of 1 (default) enables the warning; a value of 0 disables the warning. This value is relevant only if RejectIfAlreadyLoggedIn is 0.</td>
</tr>
<tr>
<td>RejectIfAlreadyLoggedIn</td>
<td>Indicates whether to not permit an agent who is already logged in to log in again. A value of 0 (default) permits an agent to log in again. A value of 1 prohibits an agent from logging in again.</td>
</tr>
<tr>
<td>DisableSkillGroupStatistics</td>
<td>Indicates whether skill group statistics are enabled for the agent using this connection profile. A value of 1 disables statistics. If this value is 0 (default) or not present, skill group statistics are enabled for this agent.</td>
</tr>
<tr>
<td>DisableAgentStatistics</td>
<td>Indicates whether agent statistics are enabled for the agent using this connection profile. A value of 1 disables statistics. If this value is 0 (default) or not present, statistics are enabled for this agent.</td>
</tr>
<tr>
<td>IPCCSilentMonitorEnabled</td>
<td>Indicates whether silent monitor is enabled for the clients using this connection profile. A value of 0x00000001 (default) enables silent monitor. If this value is 0x00000000 or not present, silent monitor is disabled for this client. For all peripherals other than IPCC, this field must be set to 0x00000000.</td>
</tr>
<tr>
<td>WarnIfSilentMonitored</td>
<td>Indicates whether to display an indicator on the agent desktop when the agent is silent monitored by the team supervisor. A value of 0x00000001 causes a message to be displayed on the agent desktop when the supervisor is silent monitoring this agent. If this value is 0x00000000 (default) or not present, no message is displayed on the agent desktop when the supervisor is silent monitoring this agent.</td>
</tr>
</tbody>
</table>
Declaring ECC Variables

The ECC key contains a list of the expanded call context variables that are used on a client applications with calls. The variables declared on this key must exist in the ICM database.

The ECC variables are declared in the registry of each server on the following location.

\[
\begin{align*}
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CtiOs\<CTIOS InstanceName>\<CTIOServerName>\ EnterpriseDesktopSettings\ All Desktops\ECC\Name\VariableName]
\end{align*}
\]

To declare a given ECC variable either named array or scalar, you must define a subkey under \ECC\Name\ without the prefix user. However, when creating ECC variables using the ICM Expanded Call Variable List tool, the ECC name must start with the prefix "user.". The subkey name is case sensitive.

For example, to declare the scalar variables user.CustomerID and user.CustomerType in CTI OS you must enter

\[
\begin{align*}
[HKEY_LOCAL_MACHINE\SOFTWARE\...\ECC\Name\CustomerID]  
"Data"="ECC"  
(Note: enter this line without the quotes)  

[HKEY_LOCAL_MACHINE\SOFTWARE\...\ECC\Name\CustomerType]  
"Data"="ECC"  
(Note: enter this line without the quotes)
\end{align*}
\]

To declare a named array user.CustomerAccount with 27 elements, you must enter

\[
\begin{align*}
[HKEY_LOCAL_MACHINE\SOFTWARE\...\ECC\Name\CustomerAccount]  
"Data"="ECCARRAY[27]"  
(Note: enter this line without the quotes)
\end{align*}
\]

<table>
<thead>
<tr>
<th>Field</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instrument</td>
<td>0x00000001</td>
</tr>
<tr>
<td>Password</td>
<td>0x00000002</td>
</tr>
<tr>
<td>Work Mode</td>
<td>0x00000004</td>
</tr>
<tr>
<td>Position ID</td>
<td>0x00000008</td>
</tr>
</tbody>
</table>

*Table 4-20 ShowBitFieldMask Fields*
Configuring the Call Appearance Grid

The CallAppearance key contains a list of all the columns that will be displayed on the softphone Call Appearance grid.

The columns are declared in the registry of each server on the following location.

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CtiOs\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\Position]

Position represents the actual location in the grid where the column will appear. For example for the first column Position will be “1” and for the fifth column it will be “5”.

Table 4-21 lists the attributes that a column declaration can contain.

Table 4-21 Column Declaration Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>String Value</td>
<td>Assigns a column to display the Call information identified by the value of this attribute. Table 4-22 lists the possible values.</td>
</tr>
<tr>
<td>Header</td>
<td>String Value</td>
<td>Contains the text string to be displayed on the header of the column. If not specified, the Type is displayed instead.</td>
</tr>
<tr>
<td>Width</td>
<td>DWORD value</td>
<td>Column width expressed in pixels. If the Auto Resize Columns property is set on the Call Appearance Grid, this attribute has no effect. The column is automatically sized to match the column header or column cell content, whichever is longer. If the Auto Resize Columns property is not set, one of the following will occur:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If Width is specified, the column will size to match it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If Width is not specified, the column will size to a default length.</td>
</tr>
</tbody>
</table>
### Configuring the Call Appearance Grid

#### Table 4-21 Column Declaration Attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxChars</td>
<td>String Value</td>
<td>Maximum of characters that can appear in the column.</td>
</tr>
<tr>
<td>Name</td>
<td>String Value</td>
<td>Used only when the Type is ECC; contains the name of a given ECC variable. The name in this attribute must be entered without the prefix “user.” For the standard Outbound Option ECC variables, use the prefix BA without any dots following it; e.g., BAResponse</td>
</tr>
<tr>
<td>Alignment</td>
<td>String Value</td>
<td>Defines the alignment of the information on the columns. Possible values are “left”, “right” or “centered.”</td>
</tr>
<tr>
<td>NumericOnly</td>
<td>String Value</td>
<td>If “true” the column accepts only numeric values for display. If “false” alphanumeric values may be displayed.</td>
</tr>
<tr>
<td>ReadOnly</td>
<td>String Value</td>
<td>Indicates if the user can modify the cells on the column at runtime.</td>
</tr>
</tbody>
</table>

#### Table 4-22 Type Values

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallID</td>
<td>Associates the column with the unique call ID.</td>
</tr>
<tr>
<td>CallStatus or Status</td>
<td>Associates the column with Call Status.</td>
</tr>
<tr>
<td>DNIS</td>
<td>Associates the column with DNIS.</td>
</tr>
<tr>
<td>ANI</td>
<td>Associates the column with ANI.</td>
</tr>
<tr>
<td>CED</td>
<td>Associates the column with the caller entered digits.</td>
</tr>
<tr>
<td>DialedNumber or DN</td>
<td>Associates the column with the dialed number.</td>
</tr>
<tr>
<td>UserToUser *Info or UserToUser</td>
<td>Associates the column with user to user information.</td>
</tr>
</tbody>
</table>
Configuring the Call Appearance Grid

Table 4-22 Type Values (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WrapUp</td>
<td>Associates the column with the call wrap up data.</td>
</tr>
<tr>
<td>Var1, Var2, ..., Var10</td>
<td>Associates the column with a call variable.</td>
</tr>
<tr>
<td>NAMEDVARIABLE, ECCVariable, ECCVar, ECC, or ECCNAME</td>
<td>Associates the column with an scalar ECC Variable.</td>
</tr>
<tr>
<td>NAMEDARRAY or ECCARRAY</td>
<td>Associates the column with a Named Array ECC variable.</td>
</tr>
<tr>
<td>CampaignID</td>
<td>Campaign ID for value appears in the Agent Real Time table. Set to zero if not used. Applicable to Outbound Option systems only.</td>
</tr>
<tr>
<td>QueryRuleID</td>
<td>Query rule ID for value appears in the Agent Real Time table. Set to zero if not used. Applicable to Outbound Option systems only.</td>
</tr>
</tbody>
</table>

The following are examples of column declarations:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CtiOs\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\1]
"Type"="CallID"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CtiOs\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\10]
"Type"="Var2"
"ReadOnly"="false"
```

The following is an example of associating a column with an ECC variable:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CtiOs\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\19]
"Type"="ECC"
"Name"="bobc"
"Header"="ECC Bobc"
"Maxchars"="8"
"ReadOnly"="false"
```
If you wish to declare a column for an ECC variable you must first declare the ECC variable itself in the registry, as explained in the previous section, “Declaring ECC Variables”. You must also first define columns 1-18, as discussed in the next section.

**Automatic Call Appearance Grid Configuration**

The CTIOSServer directory contains a file, callappearance.default.reg.txt, that provides the following default definition for Call Appearance grid columns 1-18.

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\1]
  "Type"="CallID"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\10]
  "Type"="Var2"
  "maxchars"="39"
  "editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\11]
```
Configuring the Call Appearance Grid

```
"Type"="Var3"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\12]
"Type"="Var4"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\13]
"Type"="Var5"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\14]
"Type"="Var6"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\15]
"Type"="Var7"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\16]
"Type"="Var8"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\17]
```
"Type"="Var9"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\18] "Type"="Var10"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\2] "Type"="CallStatus"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\3] "Type"="DNIS"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\4] "Type"="ANI"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\5] "Type"="CED"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\6] "Type"="DialedNumber"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\7] "Type"="UserToUserInfo"
"maxchars"="129"
Automatic Agent Statistics Grid Configuration

To import this default definition into your registry, perform the following steps:

**Step 1** Bring up the Windows **Start > Run** dialog box.

**Step 2** Rename the callappearance.default.reg.txt file to callappearance.default.reg.

**Step 3** Enter

```
regedit filename
```

where **filename** is the **full pathname** of the callappearance.default.reg file.

**Step 4** Cycle your CTI OS Server process (see the section entitled “ICM Service Control” in Chapter 5, “Startup, Shutdown, and Failover” for instructions).

---

Automatic Agent Statistics Grid Configuration

The CTIOSServer directory contains a file, agentstatistics.default.reg.txt, that contains the default definition for the Agent Statistics grid. The following is an example agentstatistics.default.reg.txt file that defines Agent Statistic grid columns 1 and 2.

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\8]
"Type"="WrapUp"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\9]
"Type"="Var1"
"maxchars"="39"
"editable"="true"
```
Automatic Agent Statistics Grid Configuration

The DisableStatsMinimization registry value controls the quantity of agent statistics that are sent from the CTI OS Server to CTI OS clients. Possible values are 0 (only those agent statistics that are configured to be displayed on the agent statistics grid are sent to the client) and 1 (all agent statistics are sent to the client); default is 0.

To customize the Agent Statistics grid, perform the following steps.

**Step 1** Make a copy of the agentstatistics.default.reg.txt file.

**Step 2** Rename the copied agentstatistics.default.reg.txt file to agentstatistics.default.reg.

**Step 3** Add, remove, and renumber column definitions in the copied file as desired.

**Step 4** Bring up the Windows Start > Run dialog box.
Automatic Skill Group Statistics Grid Configuration

Step 5  Enter

regedit filename

where filename is the full pathname of the edited copy of the
agentstatistics.default.reg file.

Step 6  Cycle your CTI OS Server process (see the section entitled “ICM Service
Control” in Chapter 5, “Startup, Shutdown, and Failover” for instructions).

Automatic Skill Group Statistics Grid Configuration

The CTIOSServer directory contains a file, skillgroupstatistics.default.reg.txt,
that contains the default definition for the Skill Group Statistics grid. The
following is an example skillgroupstatistics.default.reg.txt file that defines
columns 1 through 4.

REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\Columns]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\Columns\Number]
"DisableStatsMinimization"=dword:00000000
"DisableMonitorModeStatsMinimization"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\Columns\Number\1]
Chapter 4  CTI OS Configuration

Automatic Skill Group Statistics Grid Configuration

"Type"="SkillGroupNumber"
"header"="SkillGroupNumber"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\Columns\Number\2]
"Type"="AgentsAvail"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\ Columns\Number\3]
"Type"="AgentsNotReady"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\ Columns\Number\4]
"Type"="AgentsReady"

The DisableStatsMinimization registry value controls the quantity of skill group statistics that are sent from the CTI OS server to CTI OS agent mode clients. Possible values are 0 (only those skill group statistics that are configured to be displayed on the skill group statistics grid are sent to the client) and 1 (all skill group statistics are sent to the client); default is 0.

The DisableMonitorModeStatsMinimization registry value controls the quantity of skill group statistics that are sent from the CTI OS server to CTI OS monitor mode clients. Possible values are 0 (only those skill group statistics that are configured to be displayed on the skill group statistics grid are sent to the client) and 1 (all skill group statistics are sent to the client); default is 0.

To customize the Skill Group Statistics grid, perform the following steps.

---

Step 1  Make a copy of the skillgroupstatistics.default.reg.txt file.

Step 2  Rename the copied skillgroupstatistics.default.reg.txt file to skillgroupstatistics.default.reg.

Step 3  Add, remove, and renumber column definitions in the copied file as desired.

Step 4  Bring up the Windows Start > Run dialog box.

Step 5  Enter

        regedit filename
where filename is the full pathname of the edited copy of the skillgroupstatistics.default.reg file.

**Step 6** Cycle your CTI OS Server process (see the section entitled “ICM Service Control” in Chapter 5, “Startup, Shutdown, and Failover” for instructions).

---

### Configuring Additional Peripherals

The Peripheral Identifier screen in CTI OS Server setup lets you supply peripheral information for a single peripheral only. To configure additional peripherals, perform the following steps.

**Step 1** Define a registry key for the peripheral in [Server\Peripherals\PERIPHERAL_LOGICAL_NAME]. See the section entitled “Peripherals” for instructions.

**Step 2** Create a connection profile for the peripheral, following the directions in the section entitled “Defining Connection Profiles”.

**Note** The value that you specify for Peripheral ID in the Peripherals registry key definition must match the value that you specify for Peripheral ID in the connection profile definition.
Startup, Shutdown, and Failover

This section explains how to start and stop the CTI OS System, and how CTI OS handles failover scenarios.

ICM Service Control

The CTI OS Server runs as a Windows 2000 service on the host computer. The ICM Service Control application is an interface into the Windows platform’s service control manager, which start and stops services.
To start, stop, or cycle the processes in the CTI OS Server, use the appropriate tabs from the ICM Service Control window. To set CTI OS to start automatically on Windows startup (the recommended method), select the service name and click the Automatic button.

When the CTI OS service starts, it launches processes listed in Table 5-1. Some of these processes open and run in console windows. These windows can be minimized, but cannot be closed. Closing the console window in which a process is running forces a restart of that process.

**Table 5-1  CTI OS System Processes**

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Process Description</th>
<th>Runs In Console Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>CtiosServerNode</td>
<td>The main CTI OS Server process. This process manages all CTI OS objects and listens for and manages client connections.</td>
<td>Yes</td>
</tr>
<tr>
<td>CtiServerDriver</td>
<td>The CTI Server Driver process. This process creates and manages the connection to the Cisco ICM CTI Server. It remains idle until it is signaled by the CTI OS Server to open a connection. Once a connection has been opened, it will automatically reconnect to the alternate CTI server in the event of a failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>CTIOSTrace</td>
<td>The CTI OS tracing utility. This process uses the ICM Event Management System (EMS) to trace server messages to local log files in EMS format.</td>
<td>No</td>
</tr>
</tbody>
</table>
CTI OS Failover

The CTI OS Server is a fault-tolerant server. The server processes are managed by a fault tolerance/recovery platform called NodeManager. NodeManager creates and monitors each process running as part of the CTI OS service, and automatically restarts abnormally terminated processes.

Setting the /LOAD Configuration Parameter

In order for CTI OS failover to work correctly, the settings for the peripheral in the PG Explorer need to be configured correctly. Perform the following steps to verify that the parameters are correct:

1. Run the PG explorer.
2. Click on the "+" to open the branch for the correct PG.
3. Select the peripheral.
4. Select the PERIPHERAL tab on the right.

Table 5-1  CTI OS System Processes (continued)

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Process Description</th>
<th>Runs In Console Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>NM</td>
<td>The ICM NodeManager (fault tolerance manager). Each ICM service is started by NodeManager, and NodeManager restarts any abnormally terminated processes.</td>
<td>No</td>
</tr>
<tr>
<td>NMM</td>
<td>The ICM NodeManager (system fault tolerance). Each ICM Node (e.g. CTI OS) starts up a NMM process to handle system-level faults. In the event of a unrecoverable system fault, NMM will restart the host computer.</td>
<td>No</td>
</tr>
</tbody>
</table>
CTI OS Failover

Step 5  In the edit field for the Configuration Parameters, enter "/LOAD 0" (without the quotes).

Step 6  Cycle the PG.

This setting causes agents to be set to NotReady during a failover. The default behavior if no parameters are set is "/LOAD 1". This causes agents to be logged out when they are disconnected during a failure. A forced logout can cause some race conditions and prolong the reconnect process for agents. By setting the agents to NotReady, calls will not be routed to them and the failover will be quicker and cleaner.

Note  The default for ICM versions 4.6.1.x and earlier was "/LOAD 0". It was changed in Versions 4.6.2 and later to "/LOAD 1". If you upgraded from 4.6.1.x to 4.6.2 or later, you must go into the PG explorer and manually set the parameter to "/LOAD 0" if you are using CTI OS.

Failover of CTI OS Related Components

CTI OS handles failover of related components as described in the following sections.

IP Phones

If an IP phone goes out of service, CTI OS sends an event to all softphones associated with the IP phone that their IP phone is out of service. In addition, the affected softphones display the message “Offline.” When the IP phone is back in service, agents will need to log in again manually.

Switches

If a switch goes out of service, CTI OS sends an event to all softphones associated with the switch that the switch is offline. In addition, the affected softphones display the message “Offline.” When the switch is back in service, agents will need to log in again manually.
Peripheral Gateway

As the Peripheral Gateway (PG) is a fault-tolerant process pair, CTI OS is not affected if the PG merely switches active sides. If the PG goes offline, CTI OS sends an “Offline” message to each softphone client.

CTI Server

On a CTI Server failure, the CtiServerDriver process usually reconnects almost immediately to the redundant CTI Server. If reconnection to the redundant CTI Server is not possible, the CtiServerDriver process sends a failure response to any requests made to the CTI Server.

In addition, CTI OS sends an event message to all softphone clients. On receipt of this message, the softphone clients display an “Offline” message.

When the CTI Server comes back online, CTI OS performs a snapshot of all agents, devices, and calls to reestablish state information.

CtiServerDriver

On a CtiServerDriver process failure, the CTI OS Server process sends a failure response to any requests made to the CTI Server except for snapshot requests. Snapshot requests are queued and serviced as soon as the CtiServerDriver process recovers from the failure.

In addition, CTI OS sends an event message to all softphone clients. On receipt of this message, the softphone clients display an “Offline” message.

NodeManager restarts the failed CtiServerDriver. When the CtiServerDriver process comes back online, CTI OS performs a snapshot of all agents, devices, and calls to reestablish state information.

CTI OS Server

On a CTI OS Server failure, CTI OS disconnects all softphones from the failed CTI OS Server. These softphones attempt to reconnect automatically to another CTI OS Server; if reconnection is not possible, CTI OS sends an event message to all softphone clients. On receipt of this message, the softphone clients display an “Offline” message.
NodeManager restarts the CTI OS Server. When the CTI OS Server process comes back online, CTI OS performs a snapshot of all agents, devices, and calls to reestablish state information.
Peripheral-Specific Support

This chapter is intended to provide information on the Time Division Multiplexing (TDM) peripherals supported by CTI OS. Different peripheral manufacturers provide varying levels of support for CTI specific features. These differences need to be taken into account when writing a CTI OS client application. As far as possible, the CTI OS Server and Agent Desktop simulate the hard phone behavior of the peripheral in question. The CTI OS Supervisor Desktop for IPCC Enterprise is specific to IPCC Enterprise and is currently not supported on the TDM switches since they do not, in general, provide the Supervisory features that IPCC provides.

The peripherals mentioned in this chapter are the ones that CTI OS supports. For a complete list of all peripherals supported by the Cisco CTI Server please see the Cisco ICM Software CTI Programmer’s Guide. Please contact Cisco CTI Product Management if you are interested in CTI OS support for a peripheral not mentioned here.

This chapter details some of these considerations. It provides the following information:

- Peripheral-specific equivalents for some common ICM terms
- A list of ICM features that some peripherals do not support
- A table of CTI call event types that are unavailable for different peripheral types
- A table of CTI OS client control requests that are unsupported by different peripheral types
• Differences and limitations in the level of CTI support provided by various peripherals—including a list of CTI Server agent states and the corresponding terminology/functionality associated with the various peripherals

General ICM Software Support

This section describes differences in how various peripherals implement ICM software functionality.

Peripheral-Specific Terminology

Different peripheral manufacturers use different terminology for ICM software terms such as agents, skill groups, and services. For example, other manufacturers might call a service an application, a split, or a gate. Table 6-1 lists several ICM software terms and provides peripheral-specific equivalents.

<table>
<thead>
<tr>
<th>ICM Term</th>
<th>Peripheral-Specific Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Agent</td>
</tr>
<tr>
<td>Peripheral target</td>
<td><strong>Alcatel 400</strong>: DNIS</td>
</tr>
<tr>
<td></td>
<td><strong>IPCC</strong>: Device Target</td>
</tr>
<tr>
<td></td>
<td><strong>Siemens Hicom</strong>: Destination ACD(^1)</td>
</tr>
<tr>
<td></td>
<td><strong>Others</strong>: Trunk group and DNIS(^2)</td>
</tr>
</tbody>
</table>

\(^1\) ACD: Automatic Call Distribution

\(^2\) DNIS: Dialed Number Identification System
### Table 6-1 ICM and Peripheral-Specific Terminology (continued)

<table>
<thead>
<tr>
<th>ICM Term</th>
<th>Peripheral-Specific Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service</strong></td>
<td><strong>Alcatel 400</strong>: Pilot</td>
</tr>
<tr>
<td></td>
<td><strong>Aspect Contact Server</strong>: Application</td>
</tr>
<tr>
<td></td>
<td><strong>Avaya DEFINITY ECS</strong>: Vector Directory Number (VDN)</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Meridian</strong>: ACD Directory Number (ACD DN) or ACD Controlled Directory Number (ACD CDN)³</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Symposium</strong>: Application</td>
</tr>
<tr>
<td></td>
<td><strong>Rockwell Spectrum</strong>: Application</td>
</tr>
<tr>
<td></td>
<td><strong>Siemens Hicom</strong>: ACD Routing Table (ART)</td>
</tr>
<tr>
<td><strong>Skill group</strong></td>
<td><strong>Alcatel 400</strong>: Agent PG</td>
</tr>
<tr>
<td></td>
<td><strong>Aspect Contact Server</strong>: Agent group</td>
</tr>
<tr>
<td></td>
<td><strong>Avaya DEFINITY ECS</strong>: Skill group or hunt group⁴</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Meridian</strong>: ACD DN</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Symposium</strong>: Skill Set</td>
</tr>
<tr>
<td></td>
<td><strong>Others</strong>: Skill group</td>
</tr>
<tr>
<td><strong>Trunk</strong></td>
<td><strong>Alcatel 400</strong>: None</td>
</tr>
<tr>
<td></td>
<td><strong>Aspect Contact Server</strong>: Instrument⁵</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Meridian</strong>: Member of route</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Symposium</strong>: None</td>
</tr>
<tr>
<td></td>
<td><strong>Others</strong>: Trunk</td>
</tr>
<tr>
<td><strong>Trunk group</strong></td>
<td><strong>Alcatel 400</strong>: None</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel DMS-100, DMS-500, SL-100</strong>: None</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Meridian</strong>: Route</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Symposium</strong>: Route</td>
</tr>
<tr>
<td></td>
<td><strong>Others</strong>: Trunk group</td>
</tr>
</tbody>
</table>

1. CTI OS currently supports only the North American version of the Siemens Hicom switch. The European version (Siemens Hicom 300 E) is not supported.
In some cases, the ICM concept is very close to the corresponding ACD feature. For example, the ICM concept of a service is very similar to the Aspect concept of an application. In other cases, the ACD does not have a feature that maps exactly to the ICM feature. In these cases, you might choose a different mapping than shown in Table 6-1. For example, although it might make sense to associate each VDN on a DEFINITY ECS with an ICM service, you could also map each hunt group to a service.

On an Avaya DEFINITY ECS running in EAS mode, each skill group may have multiple subgroups depending on the switch configuration. ICM software emulates this by automatically creating additional skill groups for these peripheral types.

### ICM Feature Limitations

Some ACDs have limitations that prevent them from making full use of specific features of ICM software. Table 6-2 summarizes these limitations for those ACDs.

<table>
<thead>
<tr>
<th>Peripheral Type</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alcatel 4400</td>
<td>No trunk group monitoring</td>
</tr>
<tr>
<td>Aspect Contact Server</td>
<td>Only one skill group assignment per agent</td>
</tr>
<tr>
<td>Avaya DEFINITY ECS</td>
<td>none</td>
</tr>
<tr>
<td>IPCC</td>
<td>Does not support Trunks or Trunk Groups</td>
</tr>
<tr>
<td>Nortel Meridian</td>
<td>Limited trunk group monitoring</td>
</tr>
<tr>
<td></td>
<td>Ring time for a call is included in either queue time or delay time</td>
</tr>
</tbody>
</table>
Chapter 6      Peripheral-Specific Support

CTI OS Support

This section describes how different peripheral types implement and support CTI OS functionality. It includes the following information:

- A table of call event types that are unavailable for different peripheral types
- A table of client control requests that are unsupported by different peripheral types
- A list of other peripheral-specific differences and limitations
- A table of agent states

Call Events

Table 6-3 lists the call events that are not available from different peripheral types.

- The entry “none” indicates that the event is available from all supported peripherals.
- A single asterisk (*) indicates that the event is available from the starred peripheral, subject to the restrictions/limitations listed in the “Peripheral-Specific Limitations and Differences” section on page 6-8.
- A double asterisk (**) indicates that the event is available from Aspect when the PG is configured to use the Aspect Event Link.
### Table 6-3 Call Events NOT Available to Specific Peripherals

<table>
<thead>
<tr>
<th>Unavailable Event</th>
<th>Peripherals</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGENT_PRE_CALL</td>
<td>Alcatel, Aspect, DEFINITY, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>AGENT_PRE_CALL_ABORT</td>
<td>Alcatel, Aspect, DEFINITY, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>AGENT_STATE</td>
<td>none</td>
</tr>
<tr>
<td>BEGIN_CALL</td>
<td>none</td>
</tr>
<tr>
<td>CALL_CLEARED</td>
<td>Aspect*</td>
</tr>
<tr>
<td>CALL_CONFERENCED</td>
<td>Aspect**, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>CALL_CONNECTION_CLEARED</td>
<td>none</td>
</tr>
<tr>
<td>CALL_DATA_UPDATE</td>
<td>none</td>
</tr>
<tr>
<td>CALL_DELIVERED</td>
<td>Aspect*, Rockwell Spectrum*</td>
</tr>
<tr>
<td>CALL_DEQUEUED</td>
<td>Alcatel, DEFINITY, Nortel Meridian, Nortel Symposium, Siemens Hicom</td>
</tr>
<tr>
<td>CALL_DIVERTED</td>
<td>Aspect, IPCC, Nortel Meridian, Nortel Symposium</td>
</tr>
<tr>
<td>CALL_ESTABLISHED</td>
<td>IVR</td>
</tr>
<tr>
<td>CALL_FAILED</td>
<td>Aspect, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>CALL_HELD</td>
<td>Aspect**, IVR, Rockwell Spectrum*</td>
</tr>
<tr>
<td>CALL_ORIGINATED</td>
<td>Aspect, DEFINITY*, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, Siemens Hicom</td>
</tr>
<tr>
<td>CALL_QUEUE</td>
<td>IPCC, IVR</td>
</tr>
<tr>
<td>CALL_REACHED_NETWORK</td>
<td>Aspect, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, Siemens Hicom</td>
</tr>
<tr>
<td>CALL_RETRIEVED</td>
<td>Aspect**, IVR, Rockwell Spectrum*</td>
</tr>
</tbody>
</table>
Table 6-3  Call Events NOT Available to Specific Peripherals (continued)

<table>
<thead>
<tr>
<th>Unavailable Event</th>
<th>Peripherals</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALL_SERVICE_INITIATED</td>
<td>Aspect**, DEFINITY*, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>CALL_TRANSFERRED</td>
<td>IVR</td>
</tr>
<tr>
<td>CALL_TRANSLATION_ROUTE</td>
<td>IPCC</td>
</tr>
<tr>
<td>END_CALL</td>
<td>none</td>
</tr>
<tr>
<td>RTP_STARTED_EVENT</td>
<td>Alcatel, Aspect, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>RTP_STOPPED_EVENT</td>
<td>Alcatel, Aspect, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>none</td>
</tr>
</tbody>
</table>

Client Control Requests

Table 6-4 lists the client control requests that are not supported by the different peripheral types. The entry “none” indicates that the request is available for all supported peripherals.

- A single asterisk (*) indicates that the event is available from the starred peripheral, subject to the restrictions/limitations listed in the “Peripheral-Specific Limitations and Differences” section on page 6-8.

Table 6-4  Client Control Requests NOT Available to Specific Peripherals

<table>
<thead>
<tr>
<th>Unavailable Request</th>
<th>Peripherals</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALTERNATE_CALL</td>
<td>Meridian, Nortel Symposium</td>
</tr>
<tr>
<td>ANSWER_CALL</td>
<td>IVR</td>
</tr>
<tr>
<td>CLEAR_CALL</td>
<td>Alcatel, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>CLEAR_CONNECTION</td>
<td>IVR</td>
</tr>
<tr>
<td>CONFERENCE_CALL</td>
<td>IVR</td>
</tr>
</tbody>
</table>
Peripheral-Specific Limitations and Differences

This section lists CTI OS-related restrictions and implementation differences for various peripherals.

Alcatel

- Conference calls can have a maximum of three parties.
- Single-step/blind transfer or conference is not supported. Transfer and conference calls must be consultative.
When an agent (say 3550) logs into a phone/device (say 3300), the device becomes the agent. So to reach the said agent, one would dial 3550.

Alcatel requires a position ID as part of the Login information. Position ID is the same as instrument (an indication of the physical device).

When an agent logs in, a skill group has to be specified. Failure to specify a skillgroup, or specifying an incorrect skill group, results in a login failure.

An inside call cannot be put on Hold.

Alcatel does not support a second line. When a call is active, the Inside and Outside controls should be unavailable. A second call can only be made as a Consult call in the context of an existing call (via Transfer or Conference).

**Aspect Contact Server**

- AgentExtension and AgentInstrument are defined as the port number that the teleset is connected to.
- Events marked by an asterisk (*) are available when the PG is configured to use the Aspect EventLink.
- Call Alerting (Call Delivered, LocalConnectionState = LCS_ALERTING) is available when the EventLink is used.
- Outbound calls on some trunk types do not always provide Call Cleared events. Interflow calls that are accepted, but handled by the originating site, also sometimes do not provide Call Cleared events.
- Outbound calls require that the CallPlacementType be specified in an outbound request.
- Conference calls can have a maximum of three parties.
- In a single-step/blind transfer of a call, the initial call must come in over a trunk (be a CCT call) and the dialed number must go to a CCT.
- In a regular call transfer, the consult call can be either a CCT call or an agent_inside call.
- Alternate call operations require that the initial call be a CCT call. The second call (consult call) can be either a CCT call or an agent_inside call.
In the MAKE_Predictive_CALL_REQ message, the AnswerDetectControl1 field should contain the binary value of the Application Bridge AD_PARAM setting, and the AnswerDetectControl2 field should contain the binary value of the Application Bridge ANS_MAP setting.

Transfer and Conference behavior is modeled after hard phone behavior. To initiate a Transfer or a Conference, you must first use the MakeCall control (Transfer Init and Conference Init buttons are unavailable at this point) to make a second (consult) call. Once you make this call, the Transfer Complete and Conference Complete buttons become available to complete the desired action.

**Avaya Definity ECS**

- AgentExtension and AgentInstrument are defined as the station extension.
- Definity ECS events are the same with or without EAS (Expert Agent Selection).
- Both EAS and non-EAS versions maintain a list of preconfigured agent groups. When you log in with EAS, the agent is automatically logged into all preconfigured Agent groups. When you log in without EAS, the agent is logged into only those groups that you specify in the login request.
- The Cisco Peripheral Interface Module (PIM)—the Cisco proprietary interface between a peripheral and the Peripheral Gateway (PG)—does support call events on inside calls only when the agent’s station is monitored by ICM software (that is, appears in the ICM Peripheral Monitor Table), when the call goes through a monitored VDN, or when the call is originated by a CTI MakeCallReq. Inside calls are calls originated by an agent on the switch; this includes consult calls prior to a transfer or conference. Once the transfer or conference is completed, you can see call events for the merged ACD call.
- Auto Answer agents must have the phone off the hook or you will be unable to log into the agent. Manual Answer agents should leave the phone on the hook.
- Applications should wait a time interval of three times the refresh rate (defined in the Avaya Call Management System) between login or logout attempts. Failure to do so may cause the PIM to miss the login event and result in a failed call request.
CTI OS clients that access a DEFINITY ECS switch are returned an ASAI cause value if a third-party action fails. If you have a copy of the DEFINITY Technical Reference Manual, you can determine the actual cause of the failure by performing the following steps:

- Refer to Table 6-5 to obtain the DEFINITY ECS value that corresponds to the returned ASAI cause value:

### Table 6-5  DEFINITY Cause Values

<table>
<thead>
<tr>
<th>ASAI Value</th>
<th>DEFINITY ECS Value</th>
<th>Cause Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-MAX_LONG</td>
<td>none</td>
<td>*C_NUSE_LONG</td>
<td>No value was returned by the ECS.</td>
</tr>
<tr>
<td>0</td>
<td>CS0/28</td>
<td>*C_INVLDNUM</td>
<td>Invalid origination or destination address.</td>
</tr>
<tr>
<td>1</td>
<td>CS0/111</td>
<td>*C_PROTERR</td>
<td>Capability sequence has been violated or underlying protocol error has been detected; an unrecognized value was returned by the ECS.</td>
</tr>
<tr>
<td>2</td>
<td>CS3/40</td>
<td>*C_RESUNAVL</td>
<td>Resources to fulfill service are not available.</td>
</tr>
<tr>
<td>3</td>
<td>CS0/50</td>
<td>*C_FACUNSUB</td>
<td>Capability is implemented but not subscribed to by requester.</td>
</tr>
<tr>
<td>4</td>
<td>CS3/79</td>
<td>*C_SER_UNIMP</td>
<td>Incompatible options selected.</td>
</tr>
<tr>
<td>5</td>
<td>CS0/96</td>
<td>*C_MAND_INFO</td>
<td>One of the required parameters is missing.</td>
</tr>
<tr>
<td>6</td>
<td>CS0/100</td>
<td>*C_INVLDIE</td>
<td>Value specified in parameter is not allowed or defined.</td>
</tr>
</tbody>
</table>
### Table 6-5  DEFINITY Cause Values (continued)

<table>
<thead>
<tr>
<th>ASAI Value</th>
<th>DEFINITY ECS Value</th>
<th>Cause Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>CS3/63</td>
<td>*C_SERV_UNAVIL</td>
<td>Domain or call is being monitored by another adjunct.</td>
</tr>
<tr>
<td>8</td>
<td>CS3/86</td>
<td>*C_CALLID_TERM</td>
<td>Call is no longer in active state.</td>
</tr>
<tr>
<td>9</td>
<td>CS0/98</td>
<td>*C_INCOM_ST</td>
<td>Message not compatible with call state.</td>
</tr>
<tr>
<td>10</td>
<td>CS0/81</td>
<td>*C_INVALID_CRV</td>
<td>Invalid call identifier (sao_id also known as cluster_id) used or call does not exist.</td>
</tr>
<tr>
<td>11</td>
<td>CS3/80</td>
<td>*C_INCOM_OPT</td>
<td>Incompatible options used to establish the call.</td>
</tr>
<tr>
<td>12</td>
<td>CS0/102</td>
<td>*C_REC_TIMER</td>
<td>Timer expired.</td>
</tr>
<tr>
<td>13</td>
<td>CS3/15</td>
<td>*C_NOLOGIN</td>
<td>Agent not logged into split.</td>
</tr>
<tr>
<td>14</td>
<td>CS3/11</td>
<td>*C_NOSPLIT_MEM</td>
<td>Agent not member of specified split or split number specified incorrectly.</td>
</tr>
<tr>
<td>15</td>
<td>CS0/17</td>
<td>*C_USER_BUSY</td>
<td>Domain or call is being monitored by another adjunct.</td>
</tr>
<tr>
<td>16</td>
<td>CS0/18</td>
<td>*C_NOUSE_RESP</td>
<td>Originating address does not respond to service.</td>
</tr>
<tr>
<td>17</td>
<td>CS3/43</td>
<td>*C_PERM_DENIED</td>
<td>Permission checks for service have failed.</td>
</tr>
<tr>
<td>18</td>
<td>CS3/87</td>
<td>*C_CLUST_TERM</td>
<td>Association terminated because service is not active.</td>
</tr>
</tbody>
</table>
### Table 6-5  DEFINITY Cause Values (continued)

<table>
<thead>
<tr>
<th>ASAI Value</th>
<th>DEFINITY ECS Value</th>
<th>Cause Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>CS3/27</td>
<td>*C_OUT_OF_SERV</td>
<td>Domain has been removed by administration.</td>
</tr>
<tr>
<td>20</td>
<td>CS3/12</td>
<td>*C_INCS_AGST_ST</td>
<td>Agent not in compatible state.</td>
</tr>
<tr>
<td>21</td>
<td>CS3/13</td>
<td>*C_MAXLOGIN</td>
<td>Agent logged into maximum number of splits.</td>
</tr>
<tr>
<td>22</td>
<td>CS3/14</td>
<td>*C_INC_PASWD</td>
<td>Invalid login password.</td>
</tr>
<tr>
<td>23</td>
<td>CS3/16</td>
<td>*C_AGST_STATE</td>
<td>Request to put agent in same state he/she is already in.</td>
</tr>
<tr>
<td>24</td>
<td>CS3/41</td>
<td>*C_BAD_ADMIN</td>
<td>ACD not provisioned or optioned.</td>
</tr>
<tr>
<td>25</td>
<td>CS0/16</td>
<td>*C_NORMAL</td>
<td>Normal termination; call routed successfully.</td>
</tr>
<tr>
<td>26</td>
<td>CS0/42</td>
<td>*C_NETCONJ</td>
<td>Association terminated because of network congestion.</td>
</tr>
<tr>
<td>27</td>
<td>CS0/99</td>
<td>*C_BAD_IE</td>
<td>Unknown information element detected.</td>
</tr>
<tr>
<td>28</td>
<td>CS3/22</td>
<td>*C_QUEFULL</td>
<td>Queue is full.</td>
</tr>
<tr>
<td>30</td>
<td>CS3/46</td>
<td>C_ADMIN_PROGRESS</td>
<td>Administration is in progress; request cannot be serviced.</td>
</tr>
<tr>
<td>31</td>
<td>CS3/53</td>
<td>C_FEATURE_REJECTED</td>
<td>The ECS has rejected a request from the adjunct.</td>
</tr>
</tbody>
</table>
### Table 6-5  DEFINITY Cause Values (continued)

<table>
<thead>
<tr>
<th>ASAI Value</th>
<th>DEFINITY ECS Value</th>
<th>Cause Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>CS0/1</td>
<td>C_UNASSIGNED_NUM</td>
<td>Unassigned number.</td>
</tr>
<tr>
<td>33</td>
<td>CS0/21</td>
<td>C_CALL_REJECTED</td>
<td>Call rejected.</td>
</tr>
<tr>
<td>34</td>
<td>CS0/22</td>
<td>C_NUM_CHANGED</td>
<td>Number changed.</td>
</tr>
<tr>
<td>35</td>
<td>CS0/31</td>
<td>C_NORMAL_UNSPECIF</td>
<td>Normal, unspecified.</td>
</tr>
<tr>
<td>36</td>
<td>CS0/34</td>
<td>C_NO_CIRCUIT</td>
<td>No circuit or channel available.</td>
</tr>
<tr>
<td>37</td>
<td>CS0/41</td>
<td>C_TEMP_FAILURE</td>
<td>Temporary Failure.</td>
</tr>
<tr>
<td>38</td>
<td>CS0/58</td>
<td>C_BEARER_CAP_UNAVAIL</td>
<td>Bearer capability not presently available.</td>
</tr>
<tr>
<td>39</td>
<td>CS0/88</td>
<td>C_INCOMPAT_DESTINATION</td>
<td>Incompatible destination.</td>
</tr>
<tr>
<td>40</td>
<td>CS0/95</td>
<td>C_INVALID_MESSAGE</td>
<td>Invalid message, unspecified (backward compatibility).</td>
</tr>
<tr>
<td>41</td>
<td>CS0/97</td>
<td>C_NON_EXIST_MESSAGE</td>
<td>Message nonexistent/not implemented.</td>
</tr>
<tr>
<td>42</td>
<td>CS0/127</td>
<td>C_UNSPECIFIED</td>
<td>Unspecified.</td>
</tr>
<tr>
<td>43</td>
<td>CS3/19</td>
<td>C_NO_ANSWER</td>
<td>No answer.</td>
</tr>
<tr>
<td>44</td>
<td>CS3/20</td>
<td>C_NO_TRUNKS</td>
<td>Trunks not available.</td>
</tr>
<tr>
<td>45</td>
<td>CS3/21</td>
<td>C_NO_CLASSIFIERS</td>
<td>Classifiers not available.</td>
</tr>
<tr>
<td>46</td>
<td>CS3/30</td>
<td>C_REDIRECT</td>
<td>Redirected.</td>
</tr>
<tr>
<td>47</td>
<td>CS3/38</td>
<td>C_NETWORK_OUT_OF_ORDER</td>
<td>Network out of order.</td>
</tr>
<tr>
<td>48</td>
<td>Undefined</td>
<td>C_CAUSE_UNKNOWN</td>
<td>Undefined value returned from the ECS.</td>
</tr>
</tbody>
</table>
For example, an ASAI value of 15 corresponds to the DEFINITY ECS value of CSO/17 (C_USER_BUSY).

### Table 6-5  DEFINITY Cause Values (continued)

<table>
<thead>
<tr>
<th>ASAI Value</th>
<th>DEFINITY ECS Value</th>
<th>Cause Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>49</td>
<td>CS0/52</td>
<td>*C_OUT_CALL-_BARRLED</td>
<td>Outgoing call has been barred.</td>
</tr>
<tr>
<td>50</td>
<td>CS3/23</td>
<td>C_REMAINS_IN_Q</td>
<td>Call remains in queue.</td>
</tr>
<tr>
<td>51</td>
<td>CS0/65</td>
<td>C_BEARER_SVC_NOT_IMPL</td>
<td>Bearer service not implemented.</td>
</tr>
<tr>
<td>52</td>
<td>CS3/17</td>
<td>C_TIMED_ ANSWER</td>
<td>Assumed answer based on internal timer.</td>
</tr>
<tr>
<td>53</td>
<td>CS3/18</td>
<td>C_VOICE_ENERGY_ANSWER</td>
<td>Voice energy detected by the ECS.</td>
</tr>
<tr>
<td>54</td>
<td>CS0/82</td>
<td>C_NO_TONE_CHANNEL</td>
<td>Channel and/or tone does not exist (no tone connected to the specified call).</td>
</tr>
<tr>
<td>55</td>
<td>CS3/24</td>
<td>C_ANSWERING_MACHINE</td>
<td>Answering machine detected.</td>
</tr>
<tr>
<td>56</td>
<td>CS0/29</td>
<td>C_FACILITY_REJECTED</td>
<td>Facility rejected.</td>
</tr>
<tr>
<td>57</td>
<td>CS3/25</td>
<td>C_FORWARD_BUSY</td>
<td>Redirection cause.</td>
</tr>
<tr>
<td>58</td>
<td>CS3/26</td>
<td>C_COVER_BUSY</td>
<td>Redirection cause.</td>
</tr>
<tr>
<td>59</td>
<td>CS3/28</td>
<td>C_COV_DONT_ANS</td>
<td>Redirection cause.</td>
</tr>
<tr>
<td>60</td>
<td>CS3/31</td>
<td>C_FORWARD_ALL</td>
<td>Redirection cause.</td>
</tr>
<tr>
<td>61</td>
<td>CS3/8</td>
<td>C_LISTEN_ONLY</td>
<td>Single-Step Conference listen only.</td>
</tr>
</tbody>
</table>
Refer to Table 6-6 to find the chapter of the *DEFINITY Technical Reference Manual* that discusses the third-party action that you attempted:

<table>
<thead>
<tr>
<th>Third-party Action or Request</th>
<th>Chapter in Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party actions via Call Control: Auto Dial (3PAD), Clear (3PCC), Deflect (Redirect) (3PREDIR), Drop (Selective Drop) (3PSD), Listen-Disconnect, Listen-Reconnect, Selective Hold (3PSH), Make Call (3PMC) (or Predictive Call), Relinquish Control (3PRC), Reconnect (Retrieve) (3PR), Send DTMF (3PSDS), Take Control (3PTC)</td>
<td>Chapter 4: ASAI and Call Control</td>
</tr>
<tr>
<td>Third-Party actions via Domain Control: Auto Dial (3PAD), Domain Control (3PDC), Answer (3PANS), Merge (Transfer/Conference) (3PM)</td>
<td>Chapter 5: ASAI and Domain Control</td>
</tr>
<tr>
<td>Call Routing (RT_REQ, RT_SEL, RT_END)</td>
<td>Chapter 7: ASAI and Call Routing</td>
</tr>
<tr>
<td>Agent State change: Login, Logout, Change Workmode: NotReady (AUX), Ready (AVAIL), WorkReady (ACW), etc. Activating/Canceling Call Forwarding Activating/Canceling Send All Calls</td>
<td>Chapter 8: ASAI and Request Feature Capabilities</td>
</tr>
<tr>
<td>Value Queries</td>
<td>Chapter 9: ASAI and Value Query Capabilities</td>
</tr>
<tr>
<td>Set Value: Message Waiting Indicator (MWI) Set Billing Type</td>
<td>Chapter 10: ASAI and Set Value Capabilities</td>
</tr>
</tbody>
</table>

For example, third-party login requests are discussed in Chapter 8, “ASAI and Request Feature Capabilities.”
 Refer to the chapter specified in Table 6-6 for an explanation of the DEFINITY ECS cause value.

IPCC

- **MAKE_CALL** is only supported when the agent is in the *NotReady* state.
- Consult and blind transfers are supported. However, placing a call on hold, making a new call and then completing the transfer is not supported.
- The consult call has to be in the *Talking* state before the Transfer/Conference can be completed. Therefore, if an Alternate is done in the middle of a Transfer/Conference, the operation can only be completed after a second Alternate is done to restore status quo.
- Completing a conference or a transfer to a consulted agent on hold is not supported.
- Transferring conferences to an unobserved party is not supported.
- Overlapping transfer and conference consult operations on the same parties are not supported. For example, Agent A calls Agent B. During the conversation, Agent A needs to conference consult Agent C. Agent B feels that Agent D has more information, so Agent B then transfer consults to Agent D. To end the call, Agent A completes the conference and Agent B completes the transfer. This would fail.
- Only the conference initiator can add parties to the conference.
- Calls do not get queued at the Cisco CallManager but instead at some queue point. Because of this, skill group queue statistics are not available via the QUERY_SKILL_GROUP_STATISTICS_REQ. Service controlled IVRs can be monitored via CTI to get queued and dequeued events, as well as established events.
- RTP_STARTED_EVENT and RTP_STOPPED_EVENT are particular to IPCC to support recording vendors.
- AGENT_PRECALL_EVENT and AGENT_PRECALL_ABORT_EVENT are particular to IPCC. They provide call context data before the routed call arrives.
- A CALL_CONNECTION_CLEARED_EVENT may be received with a cause of CEC_REDIRECTED for the following cases:
  - Agent calls a CTI Route Point and call is directed to another resource
Agent calls an IVR and the IVR redirects the call
Agent calls a number with a forwarding option turned on

- Only devices that have agents logged in can be monitored via CTI OS. The ICM Peripheral Monitor Table is not supported for the IPCC PG.
- For updated information on the Cisco CallManager Multi-line feature, refer to the Cisco CallManager System Guide.
- The Cisco CallManager Shared line feature (agents share the same extension) is not supported.
- Agent Desk Settings will control some agent behaviors. These are configured in ICM and downloaded by the Agent Desktop upon startup. WrapupInMode is the wrapup mode variable for incoming calls and WrapupOutMode is the wrapup mode variable for outgoing calls. The valid values for these parameters are:
  - **REQUIRED**
    For either incoming or outgoing calls, the agent has no option but to go to the Wrapup state when a call ends. While on the call, all agent state buttons are disabled. While in the wrapup state, the Ready and NotReady buttons should be enabled.
    Clicking either the Ready or NotReady buttons should dismiss the Wrapup dialog box and put the agent in the state which was clicked.
    However, if the wrapup timer has been enabled in the PG configuration and timeout occurs before an agent state is chosen, the agent state automatically changes as follows:
    - If the timeout occurred at the end of an incoming call, the agent state changes to Ready.
    - If the timeout occurred at the end of an outgoing call, the agent state changes to NotReady.
  - **REQUIRED_WITH_DATA**
    The same as REQUIRED, but the agent must input some data into the Wrapup dialog box before exiting the dialog box and going to a Ready or NotReady state. This applies only to WrapupInMode.
  - **OPTIONAL**
For either incoming or outgoing calls, the agent is able to enter any after call state—Wrapup, Ready or NotReady—by clicking the appropriate button.

- NOT_ALLOWED

For either incoming or outgoing calls, the agent is only able to enter the Ready or NotReady states. The wrapup button is disabled.

Points of note for API users:

- If the wrapup mode is REQUIRED_WITH_DATA, SetAgentState for returning to ready or not ready will fail with an error code of CF_WRAPUP_DATA_REQUIRED (280) if there is no wrap up data entered into a call.

- If Logout Reason or NotReady Reasons are required, an error of CF_REASON_CODE_REQUIRED (281) will be received if the reasons are not assigned in set agent state request. One must also create Logout Reason and NotReady Reason dialog boxes in the Reason Code if these properties are required.

For more information regarding reason code and wrapup modes, see the Cisco ICM Software IPCC Administrator Guide.

- The PG also uses the Supervisor Interface periodically to interrogate the switch in order to examine agent configuration change. The period interval is controlled by the Windows Registry entry “MonitorGroupTimerQuery”. It is estimated that, at a baud rate of 9600, the PG takes 23 seconds to interrogate a switch with 63 agents configured. If there is an agent skill group assignment change, the PG will know about it only when it next interrogates the switch.

**Nortel Meridian**

- AgentExtension and AgentInstrument are defined as the PositionID.

Meridian can operate in either of two basic modes:

- Agent ID Mode
- Position ID Mode
In Agent ID mode, the agent must enter an Agent ID to login. These Agent IDs are not actually configured anywhere (and they have no associated passwords). The administrator simply defines the minimum and maximum allowable ID values (for example, 1001-9999). As long as an agent specifies an ID that is not already in use by another agent, the login will be allowed.

In Position ID mode, there is no Agent ID. An agent simply presses the InCalls key and is immediately logged in. For the purposes of CTI OS, use the Position ID for the Agent ID.

The AgentPassword can be set to anything. The switch does not have the concept of an agent password.

The AgentSkillGroup is ignored by the switch on login. Meridian Link does not allow an agent to specify a queue at login. The agent is logged in to whatever queue (skill group) the physical telephone is configured to be a member of.

- Table 6-3 and Table 6-4 show the capabilities in the “Enhanced CTI” mode (described in the PIM setup for Meridian) of PG operation.
- Alternate call operations are not supported.
- NotReady is not supported; use WorkReady instead.
- On a consultation call request for Meridian, the request must specify the type of consultation, that is, whether it is conference or transfer.
- The Meridian Multiple Queue Assignment (MQA) feature enables a Meridian agent to log into multiple ACD DN(s) (skill groups) by explicitly keying in the DN numbers on the physical teleset. However, the Meridian Link protocol provided by Nortel does not currently allow you to specify, via CTI OS, the ACD DN(s) into which you are logging when you send a login message. The Meridian Link protocol only allows an agent to log into the default ACD DN for which the teleset is configured.

If an agent must log into multiple ACD DN(s), or a single ACD DN that is different from the default ACD DN for the teleset, then the workaround is to have the agent log in at the physical teleset—and specify the ACD DN(s) through the teleset. After login, you can still receive calls for all of the groups and receive CTI OS notifications for the calls that will include the relevant skill group (ACD DN) information.

- Third-party call control and agent control requests issued through the CTI Server interface sometimes return a Peripheral error code in the failure indication message if the request fails. For the Nortel Meridian, this...
Peripheral error code is either a Status value or a Cause value. Generally, Status values are returned for call requests such as MakeCall and Cause values are returned for agent control requests such as SetAgentState.

The following tables summarize the Status and Cause values.

### Table 6-7  Meridian Status Values

<table>
<thead>
<tr>
<th>Status Value (hex/dec)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Parameters</td>
<td></td>
</tr>
<tr>
<td>0A00 / 2560</td>
<td>Invalid calling TN</td>
</tr>
<tr>
<td>0A01 / 2561</td>
<td>Invalid calling DN; wrong DN specified</td>
</tr>
<tr>
<td>0A02 / 2562</td>
<td>Incomplete calling DN</td>
</tr>
<tr>
<td>0A03 / 2563</td>
<td>Invalid called DN</td>
</tr>
<tr>
<td>0A04 / 2564</td>
<td>Incomplete called DN</td>
</tr>
<tr>
<td>0A05 / 2565</td>
<td>Invalid called TN</td>
</tr>
<tr>
<td>0A06 / 2566</td>
<td>Invalid origination manner</td>
</tr>
<tr>
<td>0A07 / 2567</td>
<td>Invalid destination manner</td>
</tr>
<tr>
<td>0A08 / 2568</td>
<td>Invalid origination user type</td>
</tr>
<tr>
<td>0A09 / 2569</td>
<td>Invalid customer number</td>
</tr>
<tr>
<td>0A0A / 2570</td>
<td>System or data base error</td>
</tr>
<tr>
<td>Unsuccessful Call Origination</td>
<td></td>
</tr>
<tr>
<td>0B00 / 2816</td>
<td>Origination party busy</td>
</tr>
<tr>
<td>0B01 / 2817</td>
<td>Origination resource blocking</td>
</tr>
<tr>
<td>0B02 / 2818</td>
<td>Origination set is maintenance busy</td>
</tr>
<tr>
<td>0B03 / 2819</td>
<td>500/2500 set is onhook</td>
</tr>
<tr>
<td>0B04 / 2820</td>
<td>Origination DN busy</td>
</tr>
<tr>
<td>0B05 / 2821</td>
<td>Origination is ringing</td>
</tr>
<tr>
<td>0B06 / 2822</td>
<td>Unable to disconnect origination (that is, already disconnected)</td>
</tr>
<tr>
<td>0B07 / 2823</td>
<td>Origination access restriction blocking</td>
</tr>
<tr>
<td>0B08 / 2824</td>
<td>Origination call on permanent hold</td>
</tr>
</tbody>
</table>
### Table 6-7  Meridian Status Values (continued)

<table>
<thead>
<tr>
<th>Status Value (hex/dec)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0B0A / 2826</td>
<td>System or database error</td>
</tr>
<tr>
<td>0B0B / 2827</td>
<td>Origination receiving end to end signaling</td>
</tr>
<tr>
<td>0B0C / 2828</td>
<td>The call is currently in an ACD queue</td>
</tr>
<tr>
<td>0B0E / 2830</td>
<td>Origination set invoked hold</td>
</tr>
<tr>
<td>0B14 / 2836</td>
<td>Transfer key not configured</td>
</tr>
<tr>
<td>0B15 / 2837</td>
<td>Transfer key not idle</td>
</tr>
<tr>
<td>0B16 / 2838</td>
<td>Set active in conference call</td>
</tr>
<tr>
<td>0B17 / 2839</td>
<td>Transfer or MPO/TSA class of service not configured</td>
</tr>
<tr>
<td>0B18 / 2840</td>
<td>Cannot put call on hold</td>
</tr>
<tr>
<td>0B1D / 2845</td>
<td>No active call exists on set</td>
</tr>
<tr>
<td>0B1E / 2846</td>
<td>No held call exists on set</td>
</tr>
<tr>
<td><strong>Unsuccessful Call Termination</strong></td>
<td></td>
</tr>
<tr>
<td>0C00 / 3072</td>
<td>Terminating party is busy</td>
</tr>
<tr>
<td>0C01 / 3073</td>
<td>Destination resource blocking</td>
</tr>
<tr>
<td>0C02 / 3074</td>
<td>Destination in invalid state</td>
</tr>
<tr>
<td>0C07 / 3079</td>
<td>Destination access restriction blocking</td>
</tr>
<tr>
<td>0D0A / 3338</td>
<td>System or database error</td>
</tr>
<tr>
<td><strong>Network Interceptions</strong></td>
<td></td>
</tr>
<tr>
<td>0C08 / 3080</td>
<td>Unassigned number</td>
</tr>
<tr>
<td>0C09 / 3081</td>
<td>No route to destination</td>
</tr>
<tr>
<td>0C0A / 3082</td>
<td>No user responding</td>
</tr>
<tr>
<td>0C0B / 3083</td>
<td>Number changed</td>
</tr>
<tr>
<td>0C0C / 3084</td>
<td>Destination out of service</td>
</tr>
<tr>
<td>0C0D / 3085</td>
<td>Invalid number format</td>
</tr>
<tr>
<td>0C0E / 3086</td>
<td>No circuit available</td>
</tr>
<tr>
<td>0C0F / 3087</td>
<td>Network out of order</td>
</tr>
</tbody>
</table>
Table 6-7  Meridian Status Values (continued)

<table>
<thead>
<tr>
<th>Status Value (hex/dec)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0C10 / 3088</td>
<td>Temporary failure</td>
</tr>
<tr>
<td>0C11 / 3089</td>
<td>Equipment congestion</td>
</tr>
<tr>
<td><strong>Network Interceptions with In-Band Information</strong></td>
<td></td>
</tr>
<tr>
<td>0C19 / 3097</td>
<td>Terminating party is busy</td>
</tr>
<tr>
<td>0C1A / 3098</td>
<td>Unassigned number</td>
</tr>
<tr>
<td>0C1B / 3099</td>
<td>No route to destination</td>
</tr>
<tr>
<td>0C1C / 3100</td>
<td>No user responding</td>
</tr>
<tr>
<td>0C1D / 3101</td>
<td>Number changed</td>
</tr>
<tr>
<td>0C1E / 3102</td>
<td>Destination out of service</td>
</tr>
<tr>
<td>0C1F / 3103</td>
<td>Invalid number format</td>
</tr>
<tr>
<td>0C20 / 3104</td>
<td>No circuit available</td>
</tr>
<tr>
<td>0C21 / 3105</td>
<td>Network out of order</td>
</tr>
<tr>
<td>0C22 / 3106</td>
<td>Temporary failure</td>
</tr>
<tr>
<td>0C23 / 3107</td>
<td>Equipment congestion</td>
</tr>
<tr>
<td>0C24 / 3108</td>
<td>Interworking, unspecified</td>
</tr>
<tr>
<td>0CFE / 3326</td>
<td>Other cause</td>
</tr>
<tr>
<td><strong>Unsuccessful Conference or Transfer Operation</strong></td>
<td></td>
</tr>
<tr>
<td>0D00 / 3328</td>
<td>Cannot complete conference</td>
</tr>
<tr>
<td>0D01 / 3329</td>
<td>Cannot initiate transfer</td>
</tr>
<tr>
<td>0D02 / 3330</td>
<td>Cannot complete transfer</td>
</tr>
<tr>
<td>0D03 / 3331</td>
<td>Cannot retrieve original call</td>
</tr>
<tr>
<td>0D04 / 3332</td>
<td>Fast Transfer initiation failed</td>
</tr>
<tr>
<td>0D05 / 3333</td>
<td>Fast Transfer completion failed</td>
</tr>
<tr>
<td>0D0B / 3339</td>
<td>Hold Request failed</td>
</tr>
</tbody>
</table>
### Table 6-8  Meridian Cause Values

<table>
<thead>
<tr>
<th>Cause Value (hex/dec)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1002 / 4098</td>
<td>Access restricted</td>
</tr>
<tr>
<td>1003 / 4099</td>
<td>Resource unavailable</td>
</tr>
<tr>
<td>1004 / 4100</td>
<td>Invalid customer number</td>
</tr>
<tr>
<td>1005 / 4101</td>
<td>Invalid origination address</td>
</tr>
<tr>
<td>1006 / 4102</td>
<td>Invalid destination address</td>
</tr>
<tr>
<td>1007 / 4103</td>
<td>Invalid manner</td>
</tr>
<tr>
<td>1008 / 4104</td>
<td>Unsuccessful retrieve original</td>
</tr>
<tr>
<td>1009 / 4105</td>
<td>Unsuccessful transfer</td>
</tr>
<tr>
<td>100A / 4106</td>
<td>Unsuccessful conference</td>
</tr>
<tr>
<td>100B / 4107</td>
<td>Unsuccessful answer request</td>
</tr>
<tr>
<td>100C / 4108</td>
<td>Unsuccessful release request</td>
</tr>
<tr>
<td>1070 / 4208</td>
<td>Refer to Connection Status IE</td>
</tr>
<tr>
<td>2004 / 8196</td>
<td>The target DN is invalid</td>
</tr>
<tr>
<td>2005 / 8197</td>
<td>The target DN is not AST</td>
</tr>
<tr>
<td>2006 / 8198</td>
<td>The Customer Number is invalid</td>
</tr>
<tr>
<td>2007 / 8199</td>
<td>The feature could not be invoked</td>
</tr>
<tr>
<td>2008 / 8200</td>
<td>The feature is not configured on the set</td>
</tr>
<tr>
<td>2009 / 8201</td>
<td>The requested feature is out of valid range</td>
</tr>
<tr>
<td>200A / 8202</td>
<td>The target set is not ACD agent</td>
</tr>
<tr>
<td>200B / 8203</td>
<td>The target set is a Virtual Agent</td>
</tr>
<tr>
<td>200C / 8204</td>
<td>The set is maintenance busy</td>
</tr>
<tr>
<td>200D / 8205</td>
<td>Set is in wrong state for invocation</td>
</tr>
<tr>
<td>200E / 8206</td>
<td>Set is in target state</td>
</tr>
<tr>
<td>200F / 8207</td>
<td>No NRDY/RDY while ACD set is logged out</td>
</tr>
<tr>
<td>2010 / 8208</td>
<td>Package C customer cannot use NRDY with IDN call</td>
</tr>
<tr>
<td>2011 / 8209</td>
<td>Feature IE is missing or invalid</td>
</tr>
</tbody>
</table>
Table 6-8  Meridian Cause Values (continued)

<table>
<thead>
<tr>
<th>Cause Value (hex/dec)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012 / 8210</td>
<td>DN IE is missing or invalid</td>
</tr>
<tr>
<td>2013 / 8211</td>
<td>Agent ID IE is missing or invalid</td>
</tr>
<tr>
<td>2014 / 8212</td>
<td>Agent ID is invalid</td>
</tr>
<tr>
<td>2015 / 8213</td>
<td>CFW DN IE is invalid</td>
</tr>
<tr>
<td>2016 / 8214</td>
<td>The Call Forward DN is too long</td>
</tr>
<tr>
<td>2017 / 8215</td>
<td>The Call Forward DN is invalid</td>
</tr>
<tr>
<td>2018 / 8216</td>
<td>User is invoking Call Forward</td>
</tr>
<tr>
<td>2019 / 8217</td>
<td>MSB/MSI not supported for 500/2500 sets</td>
</tr>
<tr>
<td>201A / 8218</td>
<td>500/2500 ACD agent already changed status</td>
</tr>
<tr>
<td>201B / 8219</td>
<td>500/2500 ACD agent set is being rung</td>
</tr>
<tr>
<td>201C / 8220</td>
<td>User is manually logging in 500/2500 ACD set</td>
</tr>
<tr>
<td>201D / 8221</td>
<td>Meridian Link Server Option 209 is not equipped</td>
</tr>
</tbody>
</table>

Nortel Symposium

- The Peripheral Gateway (and thus CTI OS clients) will not receive a CallEstablished Event for an off-switch call. As a result of this limitation, some features—such as blind conference or transfer operation off-switch—are not supported. The soft phone has no way to know that the call has been connected off-switch, and thus the application requires manual intervention from the agent (who will either hear a dial-tone, a ring, or an answer, etc.) before completing the conference or transfer operation.
- The Transfer button is not enabled after an off-switch consult.
- Single-step/blind transfer or conference is not supported. Transfer and conference calls must be consultative.
- Consultative Transfer to a Supervisor is not supported.
- One is unable to transfer to an AgentID.
- One is unable to put a conference or consultative call on hold, therefore the button is disabled.
- There is a delay in switching from the NotReady state to the Ready state.
There is no equivalent to the Symposium state WalkAway. The ACD gives a NOT_READY state to ICM software, but the switch will reject a request to set WalkAway to Not_Ready.

Third-party call control and agent control requests issued through the CTI Server interface sometimes return a Peripheral error code in the failure indication message if the request fails. For the Nortel Symposium, this Peripheral error code is either a Status value or a Cause value. Generally, Status values are returned for call requests such as MakeCall and Cause values are returned for agent control requests such as SetAgentState. The Nortel Symposium Status and Cause values are the same as the Nortel Meridian Status and Cause values (See Table 6-7 and Table 6-8).

Rockwell Spectrum

- The dialed number is used for AgentID, AgentExtension, and AgentInstrument, except during agent login.
- In order to perform an agent login, the SET_AGENT_STATE_REQ message must contain the actual agent ID value in the AgentID field instead of the dialed number, and the logical workstation number must be provided in the PositionID field.
- For the Login request, the user is required to enter the AgentID, AgentInstrument and the PositionID. PositionId in this case is an indication of the physical device (phone). Due to the peculiarity of the communication between the switch and the PIM, the Agent Softphone freezes if an INVALID AgentInstrument is provided with a VALID AgentID and VALID PositionID. To fix this issue, a Spectrum specific registry key has been added that provides a time out interval for the Login request. This is set to 60 seconds by default. If your particular configuration calls for a different value (network response time needs to be taken into account), change the following registry key to the appropriate value:
  
  \HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\AllDesktops\Login\ConnectionProfiles\Name\Spectrum\LoginTimeout

- Call Alerting (CallDelivered, LocalConnectionState = LCS_ALERTING) is not available.
When a call is Conferenced, both the original call and the consult call continue to exist as independent calls. Therefore, both calls appear on the Controller's Call Appearance grid. The Controller can individually control each call. If the Controller wants to drop out of the Conference, he must perform a Transfer between the other two parties so they can continue talking.

Held and Retrieved events are only reported on client controlled calls unless you are using Spectrum Release 7.1a or greater.

The AgentInstrument field in the ANSWER_CALL_REQ message is required.

The logical workstation number of the agent answering a call, if known, is placed in the LastRedirectDeviceID field in the CALL_ESTABLISHED_EVENT.

Blind Conference is not supported.

There is no CTI support for answering a specific call. An agent can be made to go Available when a call is alerting so it can be auto-answered.

Spectrum requires the AgentID field to contain the AgentInstrument (aka AgentExtension) for all agent control requests except for the Login. For the Login request, it requires the actual AgentID (assuming that AgentID is distinct from AgentInstrument and AgentExtension).

Agent is required to be in the NotReady state to either make a call or to Logout.

A logout request needs a Reason code.

Transfer and Conference behavior is modeled after hard phone behavior. To initiate a Transfer or a Conference, you must first use the MakeCall control (Transfer Init and Conference Init buttons are unavailable at this point) to make a second (consult) call. Once you make this call, the Transfer Complete and Conference Complete buttons become available to complete the desired action.

### Siemens Hicom (North American Version)

**Note**

CTI OS currently supports only the North American version of the Siemens Hicom switch. The European version (Siemens Hicom 300 E) is not supported.
The Release, Hold and Retrieve buttons are enabled when there is only one call on the device. The Release button is enabled when that call’s state is Initiating, Talking, Failed, or OnHold. The Hold button is enabled when that call’s state is Talking, and the Retrieve button is enabled when the call’s state is OnHold.

When there are two calls at the device, one of which is a consult call, either call may only be hung up via the Reconnect button. Holding and retrieving the calls is accomplished via the Alternate button. To hang up the held call, it is necessary to Alternate first before Reconnecting.

If there are two calls at the device, and the other party on the Talking call hangs up, the Held call may only be retrieved via the Reconnect button.

Neither Single Step Transfer nor Single Step Conference are supported. However, Blind Transfer (completing the transfer before the consulted agent answers) is supported.

SendDTMFSignal Request is valid only for trunk calls; it will fail if called via an inside call.

If an agent has put another agent on hold, the second agent may not initiate a transfer or a conference until the first agent retrieves the call. For example:

- Agent1 is talking to Agent2 and Agent1 clicks Hold
- Agent2’s Transfer_Init and Conference_Init buttons are disabled until Agent1 clicks Retrieve. (Agent1 will also see the same disablement because these actions are not allowed for a held call.) When Agent1 clicks Retrieve, the Transfer_Init and Conference_Init buttons will reenable on both agent’s softphones

Agent States

This section presents the agent-state terminology and functionality used by CTI OS Server and how it corresponds to the terminology and functionality of various call center peripherals.
### Table 6-9  Agent State Functionality and Call Center Terminology

<table>
<thead>
<tr>
<th>State</th>
<th>Peripheral-Specific Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available</strong></td>
<td></td>
</tr>
</tbody>
</table>
| The agent is ready to accept a call. | **Alcatel:** *Idle*
|                               | **Aspect Contact Server:** *Avail*
|                               | **Avaya DEFINITY ECS:** *AVAIL*
|                               | **Nortel Meridian:** *WAIT, DNIHOLD<ACD Ready>, DNOHOLD<ACD Ready>* (these last two states occur only if ACAA is set for the ACD DN in LD 23)
|                               | **Nortel Symposium:** *Idle*
|                               | **Siemens Hicom:** *Available*
| **BusyOther**   |                               |
| The agent is busy performing a task associated with another active Skill Group. | **Alcatel:** *no equivalent* (only one Skill Group)
|                               | **Aspect Contact Server:** *MSG* (if Aspect Event Link is not being used)
|                               | **Avaya DEFINITY ECS:** *OTHER*
|                               | **Nortel Meridian:** *NOT AVAIL*
|                               | **Nortel Symposium:** *no equivalent*
|                               | **Rockwell Spectrum:** *Busy* (on either an internal call or a call for an agent group other than the agent’s primary group)
|                               | **Siemens Hicom:** *no equivalent* (login to multiple Skill Groups not allowed)
| **Hold**        |                               |
| The agent currently has all calls on hold. | **Alcatel:** *Busy*
|                               | **Aspect Contact Server:** *HOLD*
|                               | **Avaya DEFINITY ECS:** *no equivalent*
|                               | **Nortel Meridian:** *no equivalent*
|                               | **Nortel Symposium:** *On Hold, On Hold Walkaway*
|                               | **Rockwell Spectrum:** *no equivalent*
|                               | **Siemens Hicom:** *no equivalent*
### Table 6-9  Agent State Functionality and Call Center Terminology (continued)

<table>
<thead>
<tr>
<th>State</th>
<th>Peripheral-Specific Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login</strong></td>
<td>Although viewed as a state by CTI Server, this is really more an event than a state, and is not treated as a state by the switches.</td>
</tr>
</tbody>
</table>
| **Logout** | Alcatel: *Null/logged off*  
Aspect Contact Server: *Signed Off*  
Avaya DEFINITY ECS: *no equivalent*  
Nortel Meridian: *SPARE*  
Nortel Symposium: *Logout*  
Rockwell Spectrum: *Signed Off*  
Siemens Hicom: *Logged Off* |
| **NotReady** | Alcatel: *Pause/Withdrawn/No agent group after login* (pre-assigned state)  
Aspect Contact Server: *Idle*  
Avaya DEFINITY ECS: *AUX*  
Nortel Meridian: *WALKAWAY* (however, this requires the agent to click Hold and physically unplug the headset – since a physical act is involved, a software request to set the agent state to NotReady will fail)  
Nortel Symposium: *Not Ready Walkaway* (however, this requires the agent to click Hold and physically unplug the headset – since a physical act is involved, a software request to set the agent state to NotReady will fail), *Emergency*  
Rockwell Spectrum: any state in which the Available console lamp is not lit  
Siemens Hicom: *Unavailable* |
<table>
<thead>
<tr>
<th>State</th>
<th>Peripheral-Specific Equivalent</th>
</tr>
</thead>
</table>
| Reserved | Alcatel: no equivalent  
Aspect Contact Server: RSVD  
Avaya DEFINITY ECS: no equivalent  
Nortel Meridian: RESERVED (for network ACD calls)  
Nortel Symposium: Call Presented  
Rockwell Spectrum: no equivalent  
Siemens Hicom: Reserved |
| Talking  | Alcatel: Busy  
Aspect Contact Server: Talking ACD1, Talking ACD2, Talking ACT1, Talking ACT2, Talking Out1, Talking Out2, Talking Inside, Supervisor Line, MSG, HELP (MSG and HELP correspond to Talking only if Aspect Event Link is being used)  
Avaya DEFINITY ECS: AUX-IN, AUX-OUT, ACD-IN, ACD-OUT, ACW-IN, ACW-OUT, DACD  
Nortel Meridian: ACD, ACDH, ACDHOLD, DNIN, DNOUT, DNIHOLD, DNIOUT, NRDY  
Nortel Symposium: Active, Consultation  
Rockwell Spectrum: Busy (other than cases listed under BusyOther)  
Siemens Hicom: Ready |
| Unknown  | Alcatel: no equivalent  
Aspect Contact Server: no equivalent  
Avaya DEFINITY ECS: UNKNOWN  
Nortel Meridian: no equivalent  
Nortel Symposium: no equivalent  
Rockwell Spectrum: no equivalent  
Siemens Hicom: no equivalent |
### Table 6-9  Agent State Functionality and Call Center Terminology (continued)

<table>
<thead>
<tr>
<th>State</th>
<th>Peripheral-Specific Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WorkNotReady</strong></td>
<td></td>
</tr>
<tr>
<td>WorkNotReady</td>
<td>The agent is performing after call work, and is presumed will not be ready to receive a call when completed.</td>
</tr>
<tr>
<td>Alcatel</td>
<td><strong>no equivalent</strong></td>
</tr>
<tr>
<td>Aspect Contact Server</td>
<td><strong>no equivalent</strong></td>
</tr>
<tr>
<td>Avaya DEFINITY ECS</td>
<td><strong>no equivalent</strong></td>
</tr>
<tr>
<td>Nortel Meridian</td>
<td><strong>no equivalent</strong></td>
</tr>
<tr>
<td>Nortel Symposium</td>
<td><strong>no equivalent</strong></td>
</tr>
<tr>
<td>Rockwell Spectrum</td>
<td><strong>Call work</strong> (with Available console lamp not lit)</td>
</tr>
<tr>
<td>Siemens Hicom</td>
<td><strong>no equivalent</strong></td>
</tr>
<tr>
<td><strong>WorkReady</strong></td>
<td></td>
</tr>
<tr>
<td>WorkReady</td>
<td>The agent is performing after call work, and is presumed will be ready to receive a call when completed.</td>
</tr>
<tr>
<td>Alcatel</td>
<td><strong>Working After Call/Wrapup</strong> (may be manually invoked)</td>
</tr>
<tr>
<td>Aspect Contact Server</td>
<td><strong>Wrap-up</strong></td>
</tr>
<tr>
<td>Avaya DEFINITY ECS</td>
<td><strong>ACW, DACW</strong></td>
</tr>
<tr>
<td>Nortel Meridian</td>
<td><strong>NOT READY</strong></td>
</tr>
<tr>
<td>Nortel Symposium</td>
<td><strong>Not Ready, Break, Busy</strong></td>
</tr>
<tr>
<td>Rockwell Spectrum</td>
<td><strong>Call work</strong> (with Available console lamp lit)</td>
</tr>
<tr>
<td>Siemens Hicom</td>
<td><strong>Work Not Ready</strong></td>
</tr>
</tbody>
</table>
Testing an Ethernet Card for Silent Monitor

On a site where IP telephony is or will be deployed, the Cisco Call Manager and the IP Phones are normally configured to use a Virtual Local Area Network (VLAN) such that voice is logically separated from data. Although both traffic types are carried on the same physical channel they are transmitted on different VLAN, one for voice and other for data. This configuration allows voice to be transmitted with higher priority than data.

In a call center that will use silent monitor it is required that the agent desktop system be connected to the PC port on the back of the IP phone, such that, voice packets reaching the phone can be collected by the silent monitor subsystem to then forward to the supervisor workstation. Considering all the facts stated thus far, the agent desktop system will then be using one single physical channel to interact with two different VLANs.

The agent desktop system accesses the physical channel via an Ethernet Network Interface Controller (NIC). The NIC watches the channel and collects Ethernet frames addressed to the agent’s computer. The NIC then runs a pre-processing step to extract IP packets from the Ethernet frames and deliver them to the TCP/IP stack on the operating system.

During internal testing Cisco identified that some Ethernet NIC card drivers available in the market are not capable of pre-processing Ethernet frames that have an IP packet encapsulated in a VLAN frame, i.e. The NIC card driver will discard the Ethernet frame altogether if the IP packet is encapsulated in an 802.1Q frame. Some vendors can provide a configuration setting that allows their NIC card driver to forward VLAN traffic to the TCP/IP stack.

If an agent desktop’s NIC card driver discards VLAN traffic, then the silent monitor subsystem on that desktop will not be able to collect and forward voice packets to the supervisor workstation and silent monitor will not function properly. Cisco has developed a procedure to determine if a particular Ethernet NIC card driver will work with CTI OS Silent Monitor. The procedure is described in the following sections.

**Test Procedure**

The test involves sending sample VLAN packets to a *Test Target NIC* card and verifying that the packets are not discarded by the pre-processing step but are passed onto the TCP/IP stack on the operating system at the computer hosting the NIC card.

The test requires a configuration as shown in the following diagram.

The *Test Target NIC* is connected to one port of a simple Hub. The Hub is connected to the network backbone or subnet. You also need a *Packet Generator Host* capable of generating Ethernet traffic. The *Packet Generator Host* will be connected to another port on the Hub.
The Packet Generator Host equipment can be either a dedicated packet analyzer or a computer with a software based packet analyzer with capabilities to generate Ethernet traffic.

There are a good number of software packet analyzers available that can be used for this purpose. For a comprehensive list of reliable analyzers visit the Cooperative Association for Internet Data Analysis website at [http://www.caida.org/tools/taxonomy/workload.xml](http://www.caida.org/tools/taxonomy/workload.xml). The following sections demonstrate the use of Sniffer Pro.

Once the environment is setup as described above you will have to load the software tools on the Test Target and Packet Generator Host as follows:

## Preparing Test Target

Perform the following steps to prepare the test target.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Install the WinPcap utility. The WinPcap installation program is located at the root directory on the Cisco Computer Telephony Integration CTI Object Server CD.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Create a directory on the Test Target computer named “VLANTest”.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>From the Cisco Computer Telephony Integration CTI Object Server CD, copy WinDump.exe and place it in the directory you created in Step 2. (<em>WinDump is located on the CD under CtiOS\Tools\VLANTest\WinDump</em>).</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Open a console window. Go to the directory where you copied WinDump.exe.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Determine the MAC address of the Test Target NIC by executing <code>ipconfig /all</code> at the command prompt. Write down the number that appears for the Physical Address. For example, consider the “Intel Pro/100” NIC card whose MAC address is <code>00D059d8f7d9</code>.</td>
</tr>
</tbody>
</table>
Appendix A  Testing an Ethernet Card for Silent Monitor

Test Procedure

Step 6  Determine the device interface number of the Test Target NIC. Execute `windump -D` and write down the number of the NIC you want to test. In our example we are interested on the interface number 1 that corresponds to the “Intel Pro/100” NIC card.

Note  If you are not sure which number to pick, repeat the test for each card until the test succeeds for one (sufficient to pass) or this fails for all cards.

Step 7  Start WinDump to monitor the Test Target NIC for incoming VLAN packets. To do this execute `windump -i <device_number> vlan`. In the following example the `device_number` is 1.
Appendix A  Testing an Ethernet Card for Silent Monitor

Test Procedure

Preparing Packet Generator Host

Perform the following steps to prepare the packet generator host.

**Step 1** Load the packet analyzer software onto your *Packet Generator Host*.

**Step 2** Load the sample capture file provided in the Cisco Computer Telephony Integration CTI Object Server CD (Ctios\Tools\VLANTest\VLANCapture\VLANSamplePackets.cap). The capture file was generated in a format that is used by most dedicated and software packet analyzers.

**Step 3** Select the DECODE view from the tab at the bottom of the screen.

Executing Test

The test involves sending sample VLAN packets to a *Test Target NIC* card and verifying that the packet is not discarded by the pre-processing step but is passed onto the TCP/IP stack on the computer hosting the NIC card.
The test case to determine whether or not the Test Target NIC is qualified to work with CTI OS Silent monitor is as follows. (In the test case nomenclature, PA stands for Packet Analyzer and WD stands for WinDump.)

**SMNIC-1 Send Sample VLAN Packets to Test Target NIC Card**

<table>
<thead>
<tr>
<th>Objective</th>
<th>Verify that the Test Target NIC is able to pre-process VLAN packets and able to forward them to the TCP/IP stack on the Test Target Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steps</td>
<td>Party</td>
</tr>
<tr>
<td>1</td>
<td>PA</td>
</tr>
<tr>
<td>2</td>
<td>PA</td>
</tr>
<tr>
<td>3</td>
<td>PA</td>
</tr>
<tr>
<td>4</td>
<td>PA</td>
</tr>
<tr>
<td>5</td>
<td>WD</td>
</tr>
<tr>
<td>Expected Result</td>
<td>At the Test Target computer windump will display five packets for VLAN ID = 85 as shown on Figure A-2. If the test failed, no packets will be displayed at all</td>
</tr>
</tbody>
</table>
Appendix A  Testing an Ethernet Card for Silent Monitor

Test Procedure

Figure A-1  Modifying the Destination MAC address

Figure A-2  Sample Output Showing Successful Packet Capture
If the outcome of this test is successful then your Test Target NIC will work with CTI OS Silent Monitor. Otherwise please contact your NIC card provider and ask what settings are necessary to allow your NIC card driver to forward all packets including VLAN packets to the TCP/IP stack on the computer such that your packet analyzer tool can capture and display them. Then apply the appropriate adjustments and re-run this test procedure.
# Index

## A

- ACD CDN 6-3
- ACD DN 6-3
- ACP1000 6-2, 6-3, 6-4, 6-5, 6-29
- Agent Desktop installation 3-1
- Agent group (Aspect CallCenter) 6-3
- AgentInfoLookup registry key 4-11
- Agent registry key 4-6
- Agents, peripheral terminology 6-2
- Agent states 6-28
- Agent Statistics grid 4-28
- Alcatel 6-2, 6-3, 6-4, 6-5, 6-8, 6-29
- Application, Rockwell Spectrum 6-3
- Aspect 6-2, 6-3, 6-4, 6-5, 6-9, 6-29
- Available state 6-29
- Avaya 6-2, 6-3, 6-4, 6-5, 6-10, 6-29

## B

- BusyOther state 6-29

## C

- CallAppearance registry key 4-22
- CallCenter 6-2, 6-3, 6-4, 6-5, 6-9, 6-29
- Call events 6-5
- Call Object registry key 4-11
- ConnectionProfiles registry key 4-18
- Connections registry key 4-12
- CTI Driver registry key 4-3
- CTI OS
  - advantages 1-2
  - application architecture 1-2
  - benefits 1-3
  - CTI OS Server installation 2-8
  - CTI OS system processes 5-2
  - CTI support by peripherals 6-5

## D

- DEFINITY 6-2, 6-3, 6-4, 6-5, 6-10, 6-29
- DMS-100 6-2, 6-3, 6-4, 6-5, 6-29

## E

- ECC registry key 4-21
- EMS registry key 4-4
- Enterprise Agent 6-17
- Ericsson 6-2, 6-3, 6-4, 6-5, 6-29
Index

Events
  call 6-5

F
  failover 5-3

G
  Galaxy 6-2, 6-3, 6-4, 6-5

H
  Hicom 6-2, 6-3, 6-4, 6-5, 6-29
  Hold state 6-29
  Hunt group (Avaya DEFINITY) 6-3

I
  ICM Service Control 5-1
  installation
    CTI Client component 3-1
    CTI OS Server 2-8
  Instrument (Aspect CallCenter) 6-3
  IPCC 6-17
  IPCC Media Termination 3-15

L
  Limitations of peripherals
    CTI 6-8
    ICM 6-4
  Login state 6-30
  Logout registry key 4-8
  Logout state 6-30

M
  Meridian 6-2, 6-3, 6-4, 6-5, 6-19, 6-29

N
  NEC NEAX 6-2, 6-3, 6-4, 6-5, 6-29
  Nortel 6-2, 6-3, 6-4, 6-5, 6-19, 6-29
  Nortel Symposion 6-25
  NotReady registry key 4-9
  NotReady state 6-30

O
  ODBC File DSN 2-2

P
  Peers registry key 4-13
  Peripherals

Cisco ICM Software CTI OS System Manager’s Guide Release 6.0(0)
### Index

- **CTI support** 6-5  
- **limitations** 6-4  
- **Peripheral-specific limitations, CTI** 6-8  
- **support** 6-1  
- **terminology** 6-2  
- **Peripherals registry key** 4-14  
- **Peripheral targets, peripheral terminology** 6-2

---

**R**

- **ReasonCodes registry key** 4-8  
- **registry keys**  
  - **Agent** 4-6  
  - **AgentInfoLookup** 4-11  
  - **CallAppearance** 4-22  
  - **Call Object** 4-11  
  - **ConnectionProfiles** 4-18  
  - **Connections** 4-12  
  - **CTI Driver** 4-3  
  - **ECC** 4-21  
  - **EMS** 4-4  
  - **Logout** 4-8  
  - **NotReady** 4-9  
  - **Peers** 4-13  
  - **Peripherals** 4-14  
  - **ReasonCodes** 4-8  
  - **Server** 4-6  
  - **SkillGroup** 4-15

---

**S**

- **Server registry key** 4-6  
- **Services, peripheral terminology** 6-3  
- **Siemens** 6-2, 6-3, 6-4, 6-5, 6-26, 6-29  
- **SkillGroup registry key** 4-15  
- **Skill groups**  
  - **base** 6-4  
  - **DEFINITY ECS** 6-3  
  - **primary** 6-4  
  - **secondary** 6-4  
- **Skill Group Statistics grid** 4-30  
- **Spectrum** 6-2, 6-3, 6-4, 6-5, 6-26, 6-29  
- **starting CTI OS** 5-2  
- **States, agent** 6-28  
- **stopping CTI OS** 5-2  
- **Supervisor registry key** 4-15  
- **Support, peripheral-specific** 6-1
Index

**T**

Talking state 6-31
Terminology, peripheral-specific 6-2
TimerService registry key 4-16
Trunk groups, peripheral terminology 6-3
Trunks, peripheral terminology 6-3

**U**

Unknown state 6-31

**V**

VDN 6-3
Vector Directory Number (VDN) 6-3

**W**

Windows Registry Editor 4-1
WorkNotReady state 6-32
WorkReady state 6-32
WrapupStrings registry key 4-9