



Cisco ICM Enterprise Edition Installation Guide

ICM Software Version 6.0(0)

May 2004

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number:

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

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

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

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

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

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

Cisco ICM Enterprise Edition Installation Guide

Copyright © 1996–2004, Cisco Systems, Inc.

All rights reserved.



About This Guide ix

Purpose **ix**

Audience **ix**

Organization **ix**

Conventions **x**

Other Publications **xi**

Obtaining Documentation **xi**

 Cisco.com **xi**

 Ordering Documentation **xii**

Documentation Feedback **xii**

Obtaining Technical Assistance **xiii**

 Cisco TAC Website **xiii**

 Opening a TAC Case **xiii**

 TAC Case Priority Definitions **xiv**

Obtaining Additional Publications and Information **xiv**

CHAPTER 1

Introduction 1-1

Pre-Installation Planning **1-1**

 Windows 2000 Planning and Staging **1-2**

The ICM Components **1-2**

 Duplexed Components **1-3**

 Communication Between Components **1-5**

 Instances, Customers and Components **1-5**

 Customer Types **1-6**

- Before You Install an ICM Component **1-7**
 - SQL Server **1-8**
 - Hardware Requirement Summary **1-8**
 - Logon User Account Names **1-8**
 - Machine Names **1-8**
- Setup Warning Messages **1-10**
- Cisco Security Agent Considerations **1-11**
- The Setup Program **1-12**
 - Post-Installation Setup **1-14**
 - Installing Multiple Components **1-14**
- Installing RMS Update Files **1-14**

CHAPTER 2

Logger Setup 2-1

- Installing the Logger **2-1**
- Creating the Central Database **2-6**

CHAPTER 3

CallRouter Setup 3-1

- Router Properties **3-1**

CHAPTER 4

Admin Workstation Setup 4-1

- Before Installing the Admin Workstation **4-2**
- Admin Workstation Properties **4-3**
- Real-time Distributor Node Properties **4-5**
- Real-time Distributor Properties **4-7**
- Admin Workstation Client Properties **4-8**
- AW Databases **4-10**

CHAPTER 5**Device Configuration 5-1**

- Configuration Changes **5-1**
- CallRouter Device Setup **5-2**
 - Device Management Protocol (DMP) **5-3**
 - NIC Configuration **5-3**
 - MCI NIC **5-3**
 - Sprint NIC **5-4**
 - Stentor NIC **5-5**
 - Nortel NIC **5-5**
 - ICRP NIC **5-6**
 - INCRP NIC **5-7**
 - Concert NIC **5-8**
 - CAIN NIC **5-8**
 - GKTMP NIC **5-9**
 - AT&T NIC **5-10**
 - BT INAP NIC **5-11**
 - Deutsche Telekom NIC **5-12**
 - France Telecom NIC **5-13**
 - CRSP NIC **5-13**
 - CWC NIC **5-14**
 - Energis INAP NIC **5-15**
 - AUCS INAP NIC **5-16**
 - Telfort INAP NIC **5-16**
 - BTV2 INAP NIC **5-17**
 - TIM INAP NIC **5-18**
 - SS7IN NIC **5-19**
 - NTL NIC **5-20**

CHAPTER 6**Peripheral Gateway Setup 6-1**

- Peripheral Gateway Properties **6-2**

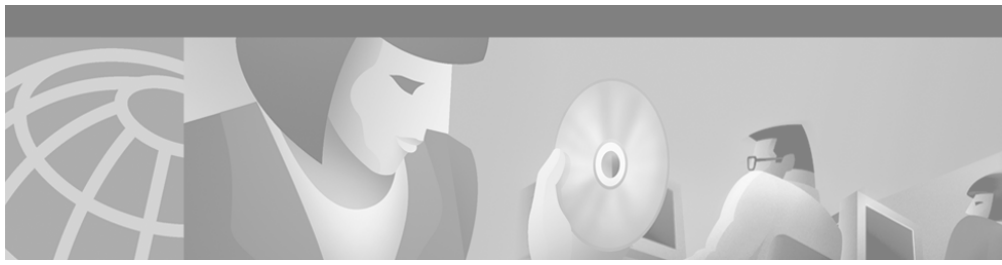
Peripheral Interface Managers	6-7
ACP1000	6-8
Alcatel A4400	6-9
Aspect	6-9
Avaya Definity ECS (AT&T PIM)	6-11
DMS-100	6-13
CallManager/SoftACD	6-15
G2 ACD	6-16
Galaxy	6-17
MD110	6-18
Meridian	6-19
MediaRouting	6-21
NEAX2400	6-23
NonVoiceAgent PG	6-24
Rolm 9005	6-25
Siemens Hicom	6-25
Spectrum	6-26
Symposium	6-26
VRU	6-28
Device Management Protocol Properties	6-28
Application Bridge Server	6-32
Application Bridge Server Properties	6-32
CompuCALL Server Gateway	6-34
CompuCALL Server Gateway Properties	6-34

CHAPTER 7**CTI Server Setup 7-1**

Installing the CTI Server	7-1
CTI Server Component Properties	7-3

CHAPTER 8**After the Installation 8-1**Files and Directories **8-1** The ICM Directory Structure **8-2** Other Admin Workstation Files **8-4** Configuration Registry **8-4** Services **8-5** Cisco Admin Workstation Program Group **8-6**Registering Users **8-7** User Accounts Created by ICM Setup **8-8**Moving Forward **8-15**

INDEX



About This Guide

Purpose

This manual describes how to install the components of the Cisco Intelligent Contact Management software. It includes information about hardware configuration and software setup.

Audience

This document is intended for anyone installing one or more components of the Intelligent Contact Management software.

Organization

The following table describes the information contained in each chapter of this guide

Chapter	Description
Chapter 1, “Introduction”	Includes references to Pre-Installation documentation. Describes how to get started with the ICM Setup program.
Chapter 2, “Logger Setup”	Explains how to install and configure the Logger software.

Chapter	Description
Chapter 3, “CallRouter Setup”	Explains how to install and configure the CallRouter software.
Chapter 4, “Admin Workstation Setup”	Explains how to install and configure the Admin Workstation software.
Chapter 5, “Device Configuration”	Explains how to configure devices for Peripheral Gateways and Network Interface Controllers.
Chapter 6, “Peripheral Gateway Setup”	Explains how to install and configure the Peripheral Gateway software.
Chapter 7, “CTI Server Setup”	Explains how to install and configure the CTI Gateway software.
Chapter 8, “After the Installation”	

Conventions

This manual uses the following conventions:

Format	Example
Boldface type is used for user entries, keys, buttons, and folder and submenu names.	Choose Design > Retrieval Arguments from the InfoMaker menu bar.

Format	Example
<p>Italic type indicates one of the following:</p> <ul style="list-style-type: none"> • A newly introduced term • For emphasis • A generic syntax item that you must replace with a specific value • A title of a publication 	<ul style="list-style-type: none"> • A <i>skill group</i> is a collection of agents who share similar skills. • <i>Do not</i> use the numerical naming convention that is used in the predefined templates (for example, persvc01). • IF (<i>condition, true-value, false-value</i>). • For more information, see the <i>Cisco ICM Enterprise Edition Database Schema Handbook</i>.
<p>An arrow (>) indicates an item from a pull-down menu.</p>	<p>The Save command from the File menu is referenced as File > Save.</p>

Other Publications

For additional information about Cisco Intelligent Contact Management (ICM) software, see the [Cisco web site](#) listing ICM 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:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

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

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- 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:

<http://tools.cisco.com/RPF/register/register.do>

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:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

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:

<http://www.cisco.com/go/marketplace/>

- 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:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *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>
- *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:
<http://www.cisco.com/packet>
- *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:
<http://www.cisco.com/go/iqmagazine>
- *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:
<http://www.cisco.com/en/US/learning/index.html>



Introduction

This manual explains how to install the major components of Intelligent Contact Management (ICM) software. The ICM platform is a contact routing system that runs on several PCs (or *nodes*) which may be distributed across many sites.

This chapter includes the following:

- Before you install. Where to find information relating to ICM pre-installation tasks.
- Information you will need before you install ICM components.
- Information about hardware and third party software requirements for individual ICM components.
- Information about ICM multi-channel options.
- An introduction to the ICM Setup program.

Subsequent chapters explain how to install and configure specific ICM components.

Pre-Installation Planning

The Cisco Intelligent Contact Management (ICM) software is a distributed computer telephony integration (CTI) application that routes toll-free calls, web inquiries, and e-mail across geographically distributed contact centers. A typical ICM system includes a number of computers located at different sites.

Because the ICM works with different types of contact center equipment and sometimes one or more carrier networks, some pre-installation planning is necessary to ensure successful installation of the ICM software.

The pre-installation documentation includes information on topics such as provisioning IXC access, preparing ACDs, and determining the ICM datacom requirements.

For complete details on ICM software pre-installation planning refer to the *Cisco ICM Enterprise Edition Pre-Installation Planning Guide*.

Windows 2000 Planning and Staging

Understanding and planning for a supported Windows 2000 model is a critical task during the planning phase of an ICM software deployment.

During this phase, you must document the specifications of the ICM system and then you must accept them prior to the start of staging a new system. This System Design Specification should include a detailed description and diagrams of the Windows 2000 Model for Active Directory and DNS implementation.

For more information on Window 2000 pre-installation requirements, refer to the *Cisco ICM Enterprise Edition Windows 2000 Planning and Staging Guide*.

The ICM Components

This manual describes how to install the following ICM components:

- **CallRouter.** The component of the Central Controller that makes routing decisions and both gathers and distributes data from remote sites. The Central Controller is the term used when discussing a CallRouter/Logger configuration.
- **Logger.** The component of the Central Controller that controls the central database.
- **Admin Workstation.** The human interface to ICM software. An Admin Workstation can be located at any central or remote site. It allows users to monitor call handling within the system and make changes to configuration data or routing scripts.

- **Peripheral Gateway.** The interface between the ICM platform and third-party hardware in each contact center, such as an ACD. A Peripheral Gateway (PG) is typically located at the contact center.

The ICM CD-ROM contains the software for all of these components. You can install any component from the ICM Setup program.

Duplexed Components

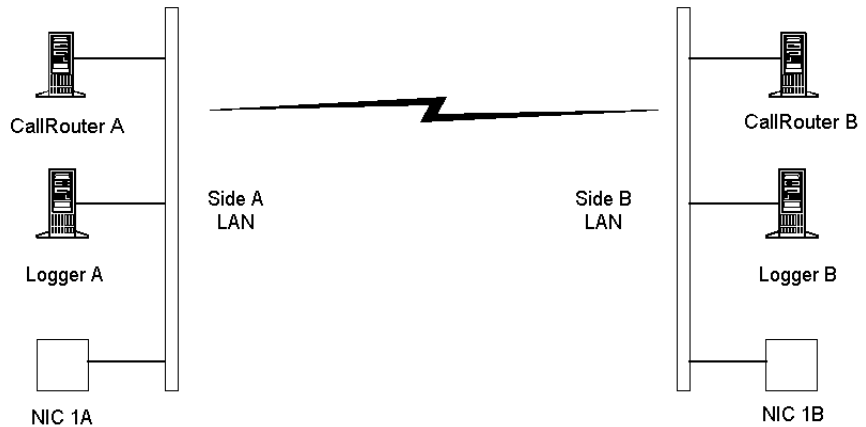
To allow ICM software to continue operating when a single node fails, all major components of the system can be duplicated on separate nodes, or *duplexed*. This allows the system to be fault-tolerant; that is, to continue operating when a component fails.

For example, two computers can run the CallRouter software. If one of those computers fails for any reason, the other computer continues to run and ICM software continues to operate without interruption. The CallRouter and Logger processes are typically duplexed and Peripheral Gateways may be duplexed.

The failure of a single Admin Workstation does not prevent the rest of the ICM from operating. Therefore, Admin Workstations are not duplexed.

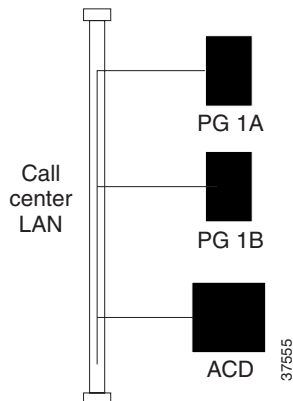
In a fully duplexed configuration, one CallRouter and one Logger compose one *side* of the Central Controller; the other CallRouter and Logger compose the other side. The sides are called Side A and Side B.

Figure 1-1 The Two Sides of the Central Controller



The components of a single side must be located at a single site; that is, the CallRouter and Logger for Side A must be collocated. For maximum fault-tolerance, the Side B components may be at a different site than Side A. If a Peripheral Gateway (PG) is duplexed, both PGs (A and B) are typically located at a single site; usually, the same site that contains the contact center equipment.

Figure 1-2 Duplexed Peripheral Gateways



If a disaster causes the entire site to fail, the contact center equipment itself is unavailable. Therefore, having a duplexed PG at another site would provide little benefit.

For more information about the ICM's fault-tolerant architecture, see the *Cisco ICM Enterprise Edition Administrator Guide*.

Communication Between Components

The ICM platform requires both local and wide area networks for communication among the nodes. Each site requires Ethernet unshielded twisted pair (UTP) for local communications. The ICM uses TCP/IP for communication between sites.

The ICM uses visible networks, which might also be used by other equipment, and private networks that are reserved for its own use.

For information about setting up the networks for the ICM, see the *Cisco ICM Enterprise Software Pre-Installation Planning Guide*.

Instances, Customers and Components

An *instance* is a single logical ICM. An instance typically consists of several software components (CallRouter, Logger, Peripheral Gateways, Admin Workstations)—some of which may be duplexed—typically installed on several different computers. A single computer may run multiple components of a single instance or components of multiple instances.



Note

You can also install multiple instances on a single computer. However, ICM has a limitation of 25 instances per machine.

A *customer* is an organization that uses the ICM to manage its contact center enterprise. Each customer has its own dialed numbers, labels, call types, scripts, and scheduled targets. However, all Peripheral Gateways, peripherals, services, skill groups, etc. are associated with the instance rather than a specific customer. Therefore, customers who share an instance cannot have their own Peripheral Gateways. Such customers, however, can be assigned a network VRU with customer-specific scripts for special call treatment.

Table 1-1 summarizes what data can be associated with a specific customer and what data are shared by an entire instance.

Table 1-1 Customer Data and Instance Data

Customer	Instance
Dialed numbers, labels, call types, scripts, scheduled targets, and network VRU scripts.	NICs and PGs; peripherals, trunk groups, peripheral targets, skill targets; regions; announcements; application gateways



Note

No special security is applied at the customer level. Any Admin Workstation user with access to an instance can choose to view data for any or all customers in that instance. However, you can set up WebView or Quick Edit users who have access to only the data for a specific customer.

Customer Types

You can use the customer concept to support multiple independent organizations with a single ICM instance rather than assigning a separate instance to each organization. However, customers that share an instance have more limited capabilities than a customer using a full instance. Table 1-2 summarizes the abilities of these two customer types.

Table 1-2 Customer Types

Full Instance Customer	Shared Instance Customer
Monitored targets (skill groups, agents, and services) and scheduled targets	Scheduled targets only
Full routing capabilities based on Longest Available Agent, Minimum Expected Delay, etc.	Percent allocation routing and scheduled targets routing only
Dedicated Peripheral Gateways	No dedicated Peripheral Gateways

Table 1-2 Customer Types (continued)

Full Instance Customer	Shared Instance Customer
Admin Workstation, Quick Edit, and/or WebView access	Quick Edit or WebView access only
Full configuration, scripting, and administration capabilities.	Limited script modifications through Advanced Services Terminal.

Note that all configuration and scripting for a shared instance customer must be performed by the service provider that manages the instance. The customer themselves can only perform quick edits within a script.

Before You Install an ICM Component

Before you install ICM software, the computers must have the Microsoft Windows 2000 operating system and, for some components, Microsoft SQL Server database management software installed.

If you are installing WebView, there are third-party components that you must first install on the Admin Workstation machine.

You must also ensure that you have enough disk space available on each computer to install the ICM component or components.

Hardware Compatibility List

Windows 2000 Setup automatically checks your hardware and software and reports any potential conflicts. To ensure a successful installation, however, check to make sure your computer hardware is compatible with Windows 2000 Server before starting Setup.

To do this, check the Cisco ICM Bill of Material (BOM). If your hardware is not listed, Setup might not be successful. This list is found at:

<http://www.cisco.com/univercd/cc/td/doc/product/icm/ccubom/ccubom.pdf>

In addition, check that you have updated drivers for your hardware devices and that you have the latest system BIOS. The device manufacturers can assist you in obtaining these items. Finally, before installing Windows 2000 Server, consider taking a device inventory of the hardware devices in your computer.

SQL Server

The ICM requires Microsoft SQL Server databases on each Logger, Historical Data Server (HDS), and each Real-time Distributor Admin Workstation (SQL Server is not required for Client AWs). SQL 2000 must be installed on each of these computers before you install the ICM software.

**Note**

SQL 7.0 is supported for ICM upgraded installations. Only SQL 2000 is supported for new ICM installation.

Refer to the *Cisco ICM Enterprise Edition Planning and Staging Guide* for more information about installing SQL 2000 software.

Hardware Requirement Summary

For complete ICM hardware requirements, see:

http://www.cisco.com/warp/partner/icsg/service/hw_sw_platform.html

Logon User Account Names

The ICM creates service logon user accounts for Logger and Distributor services. The domain\username of these accounts must not exceed 30 characters. The names are formed as follows:

- Logger service name: <domain>\<instance name><Side><hostname>
- Distributor service name: <domain>\<instance><hostname>

In ICM, the <instance> is limited to 5 characters and the <side> is limited to 1 character. This means that the combine total characters for <domain> + <hostname> must not exceed 24.

Machine Names

Cisco has defined a set of conventions for naming ICM computers. The general syntax is as follows:

CSOSSSCCCM

The terms in this syntax are as follows:

- *SSS* is a unique short code (maximum five letters) that identifies the entire system.
- *CCC* is a two- or three-letter code indicating the component type.
- *M* is a one- or two-character machine identifier (typically, the side and/or a device number).

Cisco Customer Support provides a unique system identifier. [Table 1-3](#) lists the codes and machine identifiers for each component type.

Table 1-3 Component Codes

Component Type	Code	Machine IDs
Admin Workstation	AW	1, 2, 3, . . .
CallRouter	RTR	A or B
CTI Server	CG	1A, 1B, 2A, 2B, 3A, . . .
Logger	LGR	A or B
Network Interface Controller	NIC	1A, 1B, 1C, 1D, . . . ; 2A, 2B, 2C, 2D, . . .
Peripheral Gateway	PG	1A, 1B, 2A, 2B, 3A, . . .

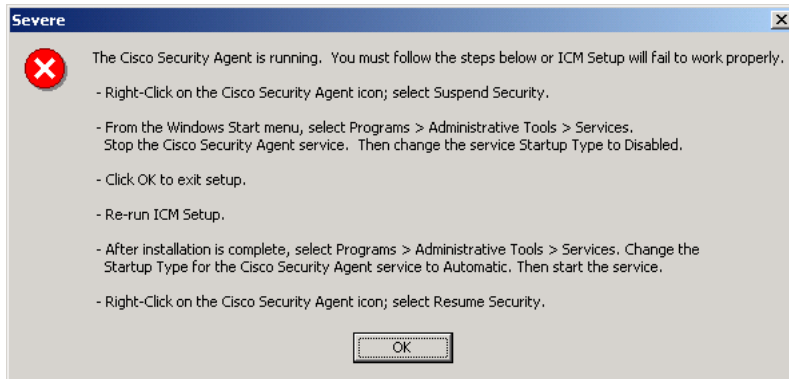
For example, if the system identifier is XYZ, the Logger on the B side is named CSOXYZLGRB.

The letter in the NIC's machine code indicates the relative location of the NIC. The first NIC is named 1A. If its duplexed peer is located at the same site, that NIC is named 1B; if the duplexed peer is located at another site, that NIC is named 1C. If each of two sites contain duplexed NICs, the two at one site are named 1A and 1B and the two at the other site are named 1C and 1D.

Setup Warning Messages

ICM displays a warning message for the following conditions

- **CSA Installed.** This message displays when you have the Cisco Security Agent installed on your system and you are running the Setup program. You must stop this service before you can run Setup.



- **NAM configurations not supported.** ICM 6.0 is for Enterprise configurations only and does not support NAM configurations. If you are attempting to upgrade a NAM system to ICM 6.0, a warning message appears when you attempt to install NAM components.

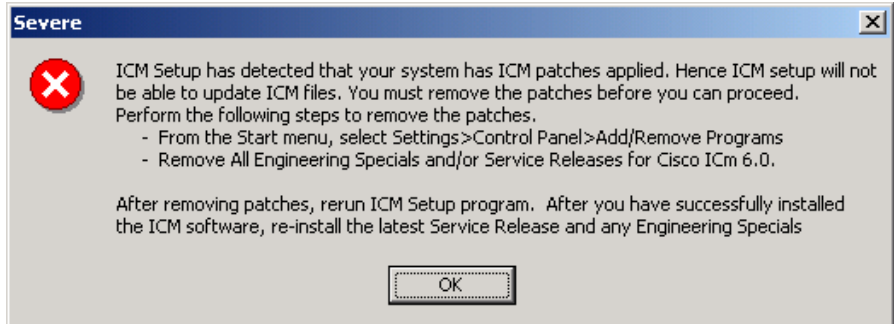


Note

ICM to ICM Gateway is also not support in ICM 6.0



- ICM patches applied. This warning displays when you are installing ICM and have Service Releases and/or Engineering Specials installed on the machine. You must uninstall any Services Releases and Engineering Specials and rerun the Setup program.



Cisco Security Agent Considerations

In addition to stopping the Cisco Security Agent before you install the ICM software, you also need to do the following:

- If you plan to use Cisco Security Agent, Cisco recommends that you always use the default directories when installing ICM software on your server.
- You must disable the Cisco Security Agent service before performing **any** software installation. This includes not only Cisco ICM software, but also third-party software that you intend to use with the ICM software.

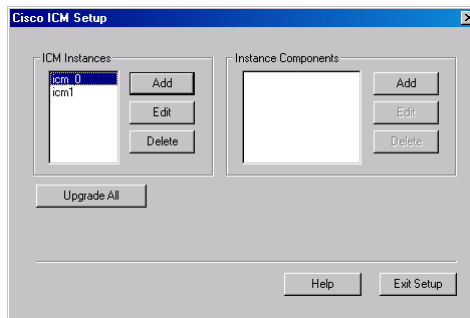
Ensure that the service does not get enabled at any time during the installation or upgrade. Failure to do so may cause problems with the installation or upgrade.

After installing or upgrading the software, you must re-enable the Cisco Security Agent Service. With the service disabled, the Agent no longer provides intrusion detection for the server.

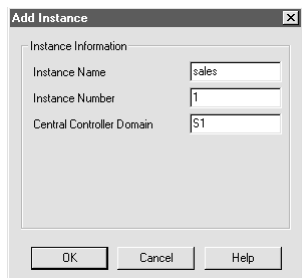
The Setup Program

To add an instance and install ICM components:

- Step 1** Run the Setup program (SETUP.EXE) from the ICM CD-ROM. Setup first creates a few files in your Temp directory (This is the C:\Temp directory. You can also view the ICM setup log file in this directory.) The main Setup screen appears as follows:



- Step 2** To add an instance, click the **Add** button in the ICM Instances section. The Add Instance dialog box appears.



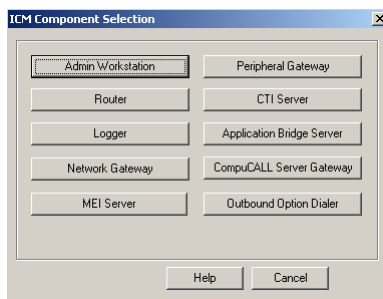
- Step 3** Enter an instance name having a maximum of five characters. Use the instance number generated by the ICM (for standard ICM configurations, the instance number is 0).



Note The mappings of instance names to instance numbers must be the same on every node in the system.

Step 4 Click the **OK** button to add the instance and return to the main Setup window.

Step 5 To install software for an instance from the CD-ROM, choose the instance and then click the **Add** button in the Instance Components section. The Setup program prompts you to choose the component to install.



Step 6 After you choose a component, Setup leads you through a series of screens in which you specify configuration settings.

For information about how to use Setup to configure a specific component, see Chapters 2 through 7.

After you have set the configuration values, Setup copies the files to your local disk and performs some initialization and customization procedures. During this time, Setup indicates its progress.

If Setup detects that less than 5% of the space on a disk is available, the Low indicator turns red. (This indicates low space on one of the drives to which files are being copied: either the drive you chose for the installation or the drive where the Windows OS is installed.) If this happens, you can create space by deleting unnecessary files or moving files to another disk. Setup does not reset the Low indicator or the disk space bar until it has finished copying and configuring the files.

In some cases, Setup cannot copy one or more files because it would have to overwrite a file that is in use. If this happens, Setup installs all the files it can and then prompts you to restart the computer.

Save any work in progress in other programs before choosing to restart the computer. When the computer shuts down, Setup is able to overwrite the files. When the computer restarts, the installation is complete.

- Step 7** If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager.
- Step 8** Click **Finish** to complete the component setup and optionally start the Node Manager. If you choose to start it, the Node Manager automatically starts the other ICM processes for the component you installed. Regardless of your choice, the main Setup screen reappears so that you can install another component.

Post-Installation Setup

A version of the Setup program is installed as part of each ICM component. (On an Admin Workstation, the Cisco Admin Workstation group contains an icon for this program.) This version allows you to change the configuration settings of the software after it is installed. It does not allow you to install new software. To reinstall the software, you must run Setup from the CD-ROM.

Installing Multiple Components

In some cases, you might want to install more than one ICM component on a single computer. For example, you might install the CallRouter and Logger software on a single node. In this case, you must run Setup from the CD-ROM for each component. Similarly, to install a specific component for more than one customer, you must run Setup from the CD-ROM for each instance.

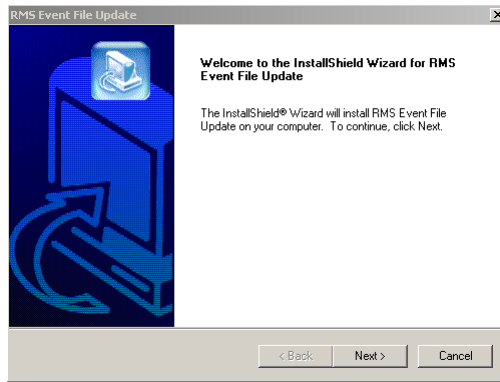
Installing RMS Update Files

The ICM CD contains a separate installer program that allows you to update the RMS files for Listener and Alarm Tracker.

To install the RMS update files:

-
- Step 1** From the ICM CD, open the RMSEventFileUpdate folder.

Step 2 Click on Setup.exe. The RMS Event File Update screen displays.



Step 3 Click Next to install the update. Click Finish when the update is complete



Logger Setup

The Logger is the component of the Central Controller that acts as an intermediary between the CallRouter and the database manager. You can install the Logger software on the same machine as the CallRouter software, or on a separate machine.

For information on installing the CallRouter software, see [Chapter 3, “CallRouter Setup”](#).

Before installing the Logger software, you must have the following installed on the machine:

- Windows 2000 operating system (SP 4)
- SQL Server 2000 (SP 3A)

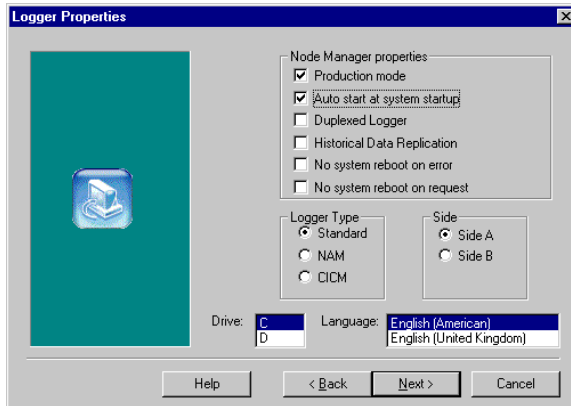
To completely configure the Logger, you must know the private network addresses of the CallRouter machines and, in a duplexed configuration, the other Logger.

To set up a Logger, you must first install the Logger software and then create the Logger's database.

Installing the Logger

To install the Logger software, run SETUP.EXE from the ICM CD-ROM. Add the customer if you have not already done so. Proceed with the Logger installation, as follows:

- Step 1** Click **Add** in the Instance Components section and choose **Logger**. The Logger Properties window appears.



- Step 2** Choose **Production Mode** and **Auto Start at System Startup** unless you are specifically told otherwise by your Cisco Support representative. This ensures that the Logger can restart itself automatically if necessary.

**Note**

You should set the Auto Start feature only after the installation is complete. You may need to reboot the server a number of times during installation, and problems could occur if the node starts before hotfixes and/or databases are applied.

- Step 3** Check the **Duplexed Logger** option if you are configuring redundant Logger machines.
- Step 4** If one or more admin sites will use an Historical Data Server (HDS), check the **Historical Data Replication** option. This enables the Logger to forward historical data to an HDS database at an admin site.
- Step 5** Do not check the **No System Reboot on Error** option if the machine runs only a single Logger component and no other critical applications. This will allow the ICM to reboot the machine when necessary to recover from errors or when the Logger specifically requests a reboot.

If multiple instances of the Logger run on the same physical machine or if other critical processes run on the machine, check this option. If you choose this option, you may need to manually recover from some failures.



Note Do not check the **No System Reboot on Request** option unless specifically told to do so by Customer Support. Checking this option prevents the Logger from rebooting even if it detects a serious system-wide problem.

- Step 6** Choose a Logger type that corresponds to your ICM system. Note that NAM systems are supported with ICM 6.0
- Step 7** If the Logger will be duplexed, specify which side you are installing: Side A or Side B. If the Logger will be simplexed, choose Side A.
- Step 8** Choose the disk on which you want to install the software.



Note Be sure to note the drive you are using for future reference, since this information is required when applying hotfixes.

- Step 9** Choose the language from the drop-down list.
- When you click the **Next** button within the Logger Properties window, the Logger Component Properties window appears.



Note Cisco TAC no longer supports new customers with the Remote Monitor Suite. Cisco no longer documents nor sells TAC monitoring of ICM systems via Remote Monitoring Suite. Refer to your MSA/Master Service Agreement for more information.

- Step 10** To enable the DDSN, in the Customer Support section, check the **Phone Home** option and then click the **Configure** button. The Phone Home Configuration dialog box appears.
- Step 11** Enter the customer and site names in the CSFS Configuration section. In the Contacting Support section, specify how to contact the Listener. Either specify the telephone number for a RAS connection in the Phone Number field or check the **Send Data Over Local Network** option for a direct network connection. Modify the Import Directory value by replacing the string *customer_name* with the actual customer name. Set Import System Name and Import Domain to point to the machine running the Listener. If you have a backup Listener, enter the phone and import information for the backup Listener.

- Step 12** Check the Enable box to enable the ICM Serial Feed facility. This facility allows you to monitor ICM events locally through a serial port.



Note The ICM software cannot be installed on the same machine that is running the Listener software.

- Step 13** Complete the Com Port field with the port on the Logger through which you want to receive events. This port must be after the port used by DTP. By default, DTP uses COM1 and the Serial Feed facility uses COM2. Enter the named pipe through which the Serial Feed facility receives events. This should always be set to CSFSEventFeed. Set the speed at which the listening device can receive events. The default is 9600.

- Step 14** Click the **OK** button to return to the Logger Component Properties window.

- Step 15** Check the **Enabled** box in the CiscoWorks 2000 Support section if you are using the optional CiscoWorks 2000 feed. Enter the name of the CiscoWorks server in the Server name field. Note that the Cisco Discovery Protocol (CDP) is required for Cisco Works 2000. CDP is included on the ICM setup CD and must be installed manually. Note that if CDP is not installed or is disabled, CiscoWorks 2000 will not run.

- Step 16** If you are using the Cisco Outbound Option, check the Enabled box and click Configure. The Outbound Option Configuration window displays.

Enter the host name or IP address of the machine that has the SQL database. Enter the heartbeat for the connection. The default is usually acceptable.



Note Refer to the Cisco *ICM/IP Contact Center Enterprise Edition Outbound Option Setup and Configuration Guide* for more information.

- Step 17** Check the **Enabled** box in the SNMP feed section and click Configure if you are using the optional SNMP event feed. The SNMP Feed Configuration window displays.

For information on the SNMP event feed, see the Cisco *ICM Enterprise Administrator Guide*.

Step 18 The central ICM database resides on the Logger machine. The Purge and Statistics buttons let you modify advanced settings that determine how the Logger manages the database.

To prevent the central ICM database from growing to infinity, the Logger must periodically purge old data from historical tables. By default, the Logger runs a purge every day during which it deletes any historical data that is greater than 100 days old. You can also configure the Logger to run a daily purge adjustment when the database fills to a defined percentage (the default is 80%). The Logger also runs a purge any time the database becomes more than 95% full.

You can change when the purge job executes and how long you want the Logger to retain data for each historical table. To modify these settings, click the **Purge** button. The Purge Configuration dialog box appears.

To change the length of time that the Logger retains data in a table, choose that table and enter a new value for Retention Period. You can also change the schedule for the daily purge job. In addition, specify whether you want a purge to execute automatically when the database reaches the daily and/or automatic purge thresholds. Specify these thresholds as the percentage of the database that becomes full.

Step 19 To execute queries efficiently, the database manager must maintain up-to-date statistics about the data in each table. To keep these statistics current, the Logger executes an Update Statistics procedure daily. To change the schedule for this process, click the **Statistics** button. The Update Statistics dialog box appears. Usually, there is no reason to change the default schedule.

Step 20 Click **Next** in the Logger Component Properties window. The Network Interface Properties window displays.

Specify the private network interfaces for the A and (if applicable) B sides of the CallRouter and Logger. You can use either the host name or the IP address.

Step 21 Click **Next**. The Check Setup Information window appears.

Ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button. When the settings are correct, click the **Next** button to begin copying files.

The copying process may take several minutes to complete. You can continue with other work while Setup operates in the background.

If Setup successfully copies all the files, it displays the final screen.

Step 22 Click **Finish** to exit Setup.

When you have completed the Logger installation, you must use the ICMDBA utility to create the Logger database.

Creating the Central Database

You must create a database for each Logger. To create the database and determine the appropriate size of the database, run the ICM Database Administration (ICMDBA) tool. This tool is installed on each Admin Workstation and on each ICM component that has an installed database.

Refer to the *Cisco ICM Enterprise Edition Administrator Guide* for more information on using the ICMDBA tool.



CallRouter Setup

The CallRouter is the Central Controller component that executes routing scripts and determines the destination for each routed task. The CallRouter also gathers data from the Peripheral Gateways and distributes monitoring data to Admin Workstations.

Before you install the CallRouter software, the Windows Server operating system must be installed on the computer.

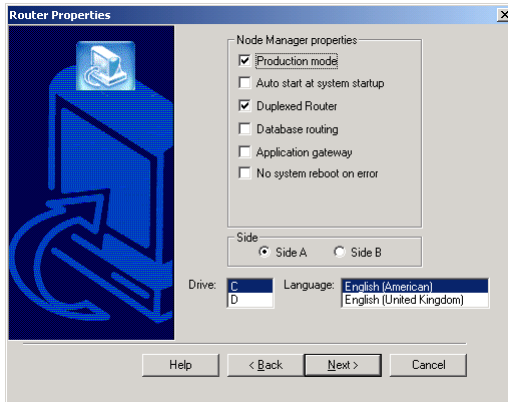
This chapter explains how to install the CallRouter software and perform some basic configuration. For this configuration, you must know the visible and private network addresses of the CallRouter and, for a duplexed configuration, its duplexed peer.

[Chapter 5, “Device Configuration”](#) describes how to configure the devices attached to the CallRouter.

Router Properties

To install the CallRouter software, run SETUP.EXE from the ICM CD-ROM. Add the customer if you have not already done so.

Click **Add** in the Instance Components section and choose **Router**. The Router Properties window appears.



Complete the Router Properties window, as follows:

- Step 1** Choose **Production Mode** and **Auto Start at System Startup** unless you are specifically told otherwise by your Cisco Support representative. This ensures that the CallRouter can restart itself automatically if necessary.



Note

It is recommended that you set the Auto Start feature after installation is complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before hotfixes and/or databases are applied.

- Step 2** Check the **Duplexed Router** option if you are configuring redundant CallRouter machines.
- Step 3** Check the **Database Routing** option if you plan to use the ICM's optional database routing feature to route calls based on data read from an external database. This requires that you purchase the DbLink product. You might use this, for example, to look up the caller's telephone number (calling line ID) in your corporate database.
- Step 4** Check the **Application Gateway** option if you plan to use the ICM's optional custom gateway feature to access an external application from within a routing script. This requires that you purchase the Cisco *Gateway* product.
- Step 5** If the machine runs only a single CallRouter component and no other critical applications, then you should allow the ICM to reboot the machine when necessary to recover from a CallRouter failure. If multiple instances of the

CallRouter run on the same physical machine or if other critical processes run on the machine, check the **No System Reboot on Error** option. If you choose this option, you may need to manually recover from some failures.

Step 6 If the CallRouter will be duplexed, specify which side you are installing: Side A or Side B. If the CallRouter will be simplexed, choose Side A.

Step 7 Choose the local disk on which you want to install the software.

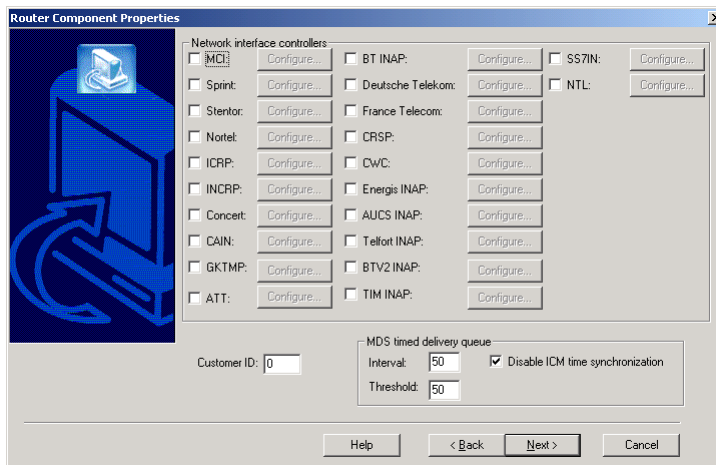


Note

Be sure to note the drive you are using for future reference, since this information is required when applying hotfixes.

Step 8 Choose the language from the drop-down list.

Step 9 Click **Next**. Setup loads any current installation settings and then displays the Router Component Properties window.



Step 10 In the Customer ID field, enter your unique customer identifier. If you do not know your identifier, check with your Support representative.

Step 11 If you are routing calls with an interface to Interexchange carrier (IXC), or you are using the INCRP, ICMP or INAP protocols, you must set up the appropriate Network Interface Controller (NIC) within the CallRouter. However, before you can set up a NIC, you must create the related database records using Configure ICM on an Admin Workstation. If you are performing the initial installation of the ICM, leave the NIC configuration for later.

For information about setting up a NIC, see [Chapter 5, “Device Configuration”](#).

- Step 12** Accept the default values for the timed delivery queue unless told otherwise by your Cisco Support representative.

The **Disable ICM Time Synchronization** box is used to select time synchronization service. The box is checked, by default, since the Windows 2000 operating system uses its own integrated time service. If the machine you are configuring is a domain controller, leave this box unchecked. However, if the machine is a workgroup machine, check this box to enable ICM Time Synchronization. You should note setup will not change current configuration when performing an Upgrade all.

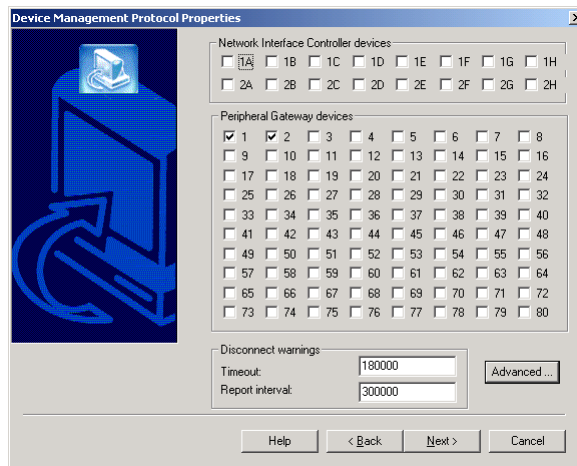
For a domain machine, setup will also show the current status of Windows Time service.



Note

If OS is upgraded from NT4 to Win2k, it maybe necessary to run setup to reconfigure this value.

- Step 13** When you click **Next** in the Router Component Properties window, the Device Management Protocol Properties window displays.



You must enable connections within the CallRouter Device Management Protocol (DMP) for each Peripheral Gateway (PG) and for each AT&T or British Telecom NIC (if any) that communicates with the CallRouter.

For information on the DMP configuration, see [Chapter 5, “Device Configuration”](#).

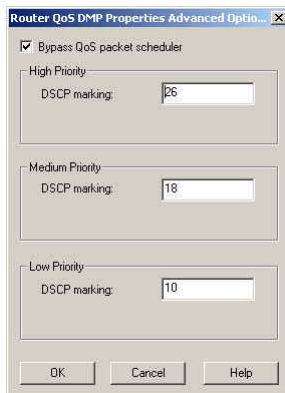
AT&T NICs can be simplexed, duplexed locally, or duplexed remotely. The first physical NIC is always designated A; that is, NIC 1A or NIC 2A. If duplexed NICs are collocated, the second NIC is designated B; that is, NIC 1B or NIC 2B. If duplexed NICs are located at different sites, the second NIC is designated C; that is, NIC 1C or NIC 2C. A BT NIC can have up to eight physical controllers (A through H) associated with a single logical controller.

Up to 80 PGs can be connected to the CallRouter. Each PG has a device number in the range 1 through 80. Check the boxes for the PG devices you use. When you configure a PG, you must reference a PG device number enabled here.


Caution

A duplexed CallRouter must have at least one PG defined. Only the CallRouter side that has active connections to the majority of the PGs routes calls. (This prevents both Side A and Side B from routing calls simultaneously.) If no PGs are defined, neither side is activated. If necessary, create a PG with no associated peripherals to satisfy this requirement.

- Step 14** The Disconnect Warnings settings determine when the CallRouter reports that a device is disconnected. Accept the default values unless told otherwise by your Cisco Support representative.
- Step 15** To configure QoS for the Central Controller selected on the Device Management Properties screen, click the Advanced button. The Router DMP Properties Advanced Options window displays.



Set the DSCP (DiffServ Codepoint) marking for each priority of the ICM traffic going to the PG. The defaults are acceptable if your network is Cisco AVVID (Architecture for Voice, Video and Integrated Data) compliant. Otherwise, you need to consult your network administrator or Cisco representative for the proper values for these fields.

Uncheck the Bypass QoS packet scheduler box if you plan to use the Microsoft Packet Scheduler utility. This changes the appearance of the Router QoS DMP Properties Advanced Options window.

The edit boxes for Medium Priority are grayed out and the Medium Priority always has the same settings as the High Priority. This is because Microsoft Packet Scheduler supports at most two classification levels (except best effort).

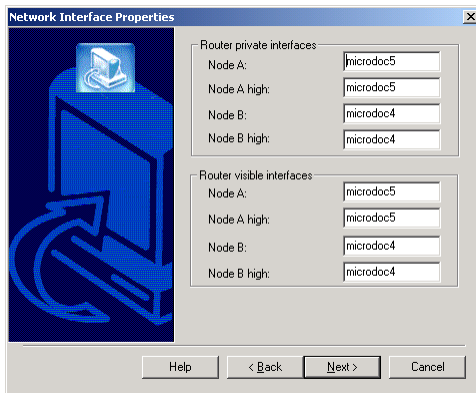
In addition to DSCP marking, the Class-of-Service (802.1p) marking is supported. The default values are set in compliance with Cisco AVVID recommendations. Consult your network administrator or Cisco representative for changes.



Note

Microsoft Packet Scheduler must be installed separately from the ICM setup if you uncheck the Bypass Packet Scheduler box. For more information about ICM QoS, refer to the *Cisco ICM Enterprise Edition Pre-Installation Planning Guide*.

- Step 16** When you click **Next** in the Device Management Protocol window, the Network Interface Properties window appears.



The CallRouter must have two addresses on the private network: one to be used by high priority traffic and another to be used by normal traffic. If the CallRouter is duplexed, each side must have two addresses. Enter the addresses in the appropriate fields of the dialog box. If the CallRouter is simplexed, enter **localhost** in the Node B fields.

- Step 17** Click **Next**. from the Network Interface Properties window, the Check Setup Information window appears:

Ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button. When the settings are correct, click the **Next** button to begin copying files.

The copying process may take several minutes to complete. You can continue with other work while Setup operates in the background.

If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager now. It is not recommended that you start the Node Manager until you have completed the entire ICM installation.

- Step 18** Click **Finish** to exit Setup and optionally start the Node Manager.

If you choose to start it, the Node Manager automatically starts the other ICM processes on the CallRouter.



Admin Workstation Setup

The Admin Workstation software is the human interface to the ICM software. It allows you to monitor activity within your enterprise, modify configuration data and routing scripts, and perform other maintenance and administration tasks.

Cisco recommends that you install the AW software on node separate from other ICM software. The node can be located on any LAN that has WAN access to the Central Controller.

You have two options when installing the Admin Workstation software:

- Client (no Real-time Distributor)
- Real-time Distributor

[Table 4-1](#) summarizes the difference between Real-time Distributor and client-only Admin Workstations.

Table 4-1 Distributor Vs. Client Admin Workstation

	Distributor Admin Workstation	Client Admin Workstation
Types	Standard	Standard
Applications	Full complement, depending on type	Full complement, depending on type
Local Database	Yes	No
Windows Service	Cisco ICM Distributor	N/A

Table 4-1 Distributor Vs. Client Admin Workstation (continued)

	Distributor Admin Workstation	Client Admin Workstation
Background Processes	logger, rtclient, rtdist, updateaw	N/A
Optional Processes	schman, replication	N/A

If you have more than one Admin Workstation on a single LAN, then only one of those machines needs to receive the real-time feed from the Central Controller. That machine acts as the real-time distributor and passes the real-time data to other Admin Workstations at the site. If possible, configure two machines at the site as real-time distributors: one as the primary and the other as the secondary (backup) distributor.

Optionally, you can configure a real-time distributor to also act as a Historical Data Server (HDS). The Logger then forwards historical data to a special database on the distributor. Admin Workstations at the local site can then access historical data from the distributor rather than from the central database.

**Note**

For a Historical Data Server, you must first install the Admin Workstation software without the HDS option enabled. Then create the HDS database and run Setup locally to enable HDS.

Refer to *Cisco ICM Enterprise Edition Administration Guide* for information on setting up the HDS.

Before Installing the Admin Workstation

Before you install the Admin Workstation software, the machine must have the following installed:

- Windows Server operating system (for Real-time Distributor Admin Workstations) or Window Professional operating system (for Client Admin Workstations) or Windows 2000 operating system for either Real-time Distributor or Client Admin workstations.

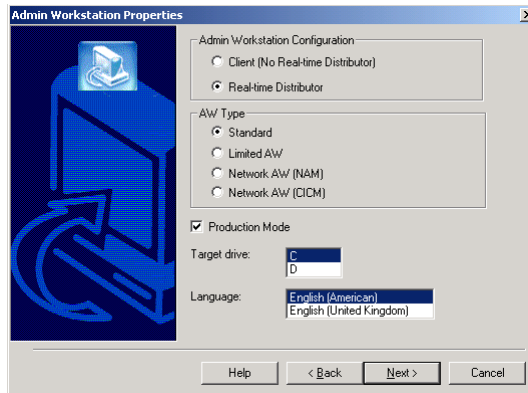
- SQL Server database, SQL 2000 and service packs. Client AWs require ODBC 2.5 or greater with a SQL Server driver.
- If you plan on using InfoMaker for ICM to create report templates, you should install Powersoft's InfoMaker before you install the Admin Workstation. If you install InfoMaker after you install the Admin Workstation, the InfoMaker for ICM will not be available. You will have to install the Admin Workstation again.
- If you are installing WebView, there are third-party components that you must first install on the Admin Workstation machine.

Admin Workstations (AWs) may be part of the Central Controller domain or in another domain. If the AW is in another domain, you must establish a two-way trust relationship between the AW and Central Controller domain.

Admin Workstation Properties

To install the Admin Workstation software, run SETUP.EXE from the ICM CD-ROM. Add the customer if you have not already done so. Proceed with the Admin Workstation installation, as follows:

- Step 1** Click **Add** in the Instance Components section and choose **Admin Workstation**. The Admin Workstation Properties window appears.



Step 2 Choose the type of Admin Workstation configuration:

Client (No Real-time Distributor). This configuration includes standard Admin Workstation applications, such as Script Editor and Configure ICM. It does not include the processes that directly manage a database.

Real-time Distributor. This configuration includes the real-time distributor and real-time client processes, and all processes that directly manage the local database. A single distributor Admin Workstation can run the distributor processes for multiple customers simultaneously. However, it can run client applications (such as Script Editor and Configure ICM) for only one customer at a time. Use AW Select to change the customer.

Step 3 Select the standard type for ICM Enterprise solutions.



Note Network AW's are not supported in ICM 6.0. If you select a Network AW, you will receive a warning message.

Step 4 Always choose **Production Mode** for the Node Manager unless your Cisco Support representative tells you otherwise.

Step 5 Choose the disk on which to install the software.



Note Be sure to note the drive you are using for future reference, since this information is required when applying hotfixes.

Step 6 Choose the language from the drop down list (ICM 6.0 supports seven languages). This determines which on-line help files are installed.

The language you select also determines the date format that is used in reports. The following table describes date formats for each language.

Table 4-2 Report Date Format for Languages

AW Setup Language	WebView UI	Date Format in Reports
English (USA)	English	MM/DD/YYYY
English (UK)	English	DD/MM/YYYY
French	English (with French report descriptions)	DD/MM/YYYY

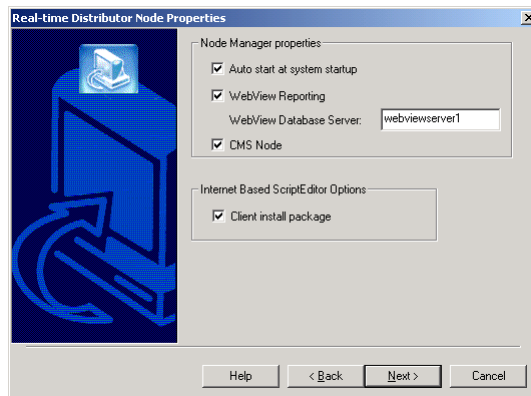
Table 4-2 Report Date Format for Languages

AW Setup Language	WebView UI	Date Format in Reports
German	English	DD/MM/YYYY
Spanish	English	DD/MM/YYYY
Chinese (Simplified)	Chinese	YYYY/MM/DD
Japanese	Japanese	YYYY/MM/DD
Korean	Korean	YYYY/MM/DD

Customers who want to run ICM on Windows 2000 which is **not** localized in one of these languages, but who want to use the DD/MM/YYYY date format, must select UK English, French, German, or Spanish as the AW Setup language.

Real-time Distributor Node Properties

If you chose the **Real-time Distributors** from the Admin Workstation Properties screen and click the **Next** button, the Real-time Distributor Node Properties window appears.



The Real-time Distributor Node runs as an Windows service and manages several ICM processes (including the local Logger process, real-time client, and the real-time distributor). Complete this window, as follows:

-
- Step 1** You can choose to have the Node Manager start automatically each time you start the computer. If you do not choose the **Auto Start** option then you must start the Node Manager manually before you can use the ICM tools.



- Note** In most cases, real-time distributors should use the Auto Start option to ensure they are available when needed. However, it is recommended that you set the Auto Start feature after installation is complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before hotfixes and/or databases are applied.
-

- Step 2** If you are using the optional Cisco *WebView* product and you want this Admin Workstation to act as a Web server, check the **WebView Reporting** option. This allows WebView clients to connect to the Admin Workstation and view real-time and historical data in a Web browser. In the WebView Database Server field, enter the IP address or host name of the machine that contains the WebView database.



- Note** If you changed your Jaguar Sybase EAServer connection password from the default when you installed the EAServer, ICM setup will display the Jaguar Password Needed screen if you select the WebView Reporting option.
-

- Step 3** Check this box to enable the Configuration Management System node. This engine can access the ICM configuration and manages connectivity and resources for applications, such as the Cisco ICM Collaboration Server option and Cisco ICM Email Manager option, that connect to the ICM platform.

- Step 4** Check the Client install package check box if you want to download the Internet based Script Editor software.

For new Script Editor installations, you must access a web page on the ICM distributor to download the software. The Script Editor software is a self-extracting archive that you must download and run. You can do this from either Netscape or Internet Explorer browsers.

You must have write access to the install directory they choose, and to registry branch HKEY_LOCAL_MACHINE.

**Note**

Refer to the *Cisco ICM Enterprise Edition Configuration Guide* for more information on the Internet Based Script Editor option.

Real-time Distributor Properties

The Real-time Distributor Properties screen displays only for Real-time Distributor Admin Workstation installations. This screen appears when you click the **Next** button from the Real-time Distributor Node Properties screen.

Complete this window, as follows:

- Step 1** Enter the site name and indicate whether this the secondary distributor for the site.

**Note**

Cisco recommends, that when naming AW's at the same site, you use the same site name for all Distributor and Client AWs at the site.

- Step 2** In the Database section, select, if your require, the Historical Data Server, Partitioning, and the SQL Server Directory.

**Note**

If you want to configure the AW as a Historical Data Server, do **not** check the Historical Data Server box the first time you run Setup.

Refer to the *Cisco ICM Enterprise Edition Administrator Guide* for more information on configuring the HDS.

Check the **Partitioning** box to install the ICM's optional partitioning software. This allows you to partition data in the ICM database and selectively limit access that groups of users have to specific data.

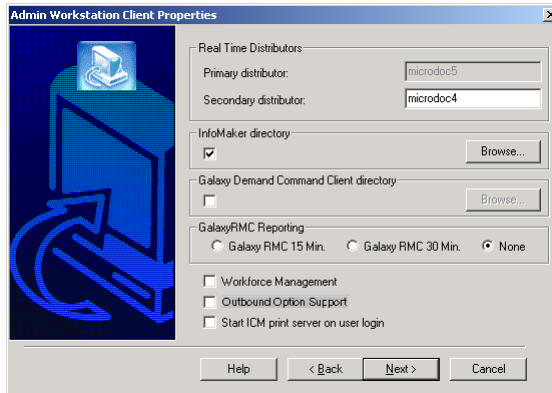
Each Real-time Distributor Admin Workstation must have a Microsoft SQL Server database version SQL 2000 and service packs (this is not a requirement on Client Admin Workstations). Specify the directory that contains the data devices.

Enter information about the Central Controller connection for the distributor. Indicate the side of the Central Controller from which you prefer to receive real-time data. (This is important, for example, if the Admin Workstation is collocated with one side of the Central Controller. You can prevent unnecessary traffic on the wide area network by choosing the local side of the Central Controller as the preferred side.)

Enter the names of the real-time servers (typically, the Call Router machine) for each side and the machine that contains the central SQL Server database (typically the Logger) for each side. Enter the name of the HDS server for historical data.

Admin Workstation Client Properties

The Admin Workstation Client Properties screen appears for both Client and Real-time Distributor Admin Workstation setups.



Complete the window as follows:

- Step 1** Specify whether this Admin Workstation serves as either the primary or secondary real-time distributor for the site.



Note

If you are configuring a HDS, be sure that you indicate it as the primary distributor. Otherwise your WebView reports will go to your logger machine rather than to your HDS machine.

Every Admin site must have at least one—and preferably two—Admin Workstations serve as real-time distributors. At any time, one distributor at each site receives real-time data directly from the Central Controller. Other Admin Workstations receive their real-time data from the distributor.

For a description of the real-time architecture and advice about choosing Admin Workstations to act as distributors, the *Cisco ICM Enterprise Edition Pre-Installation Planning Guide*.



Caution

All Admin Workstations for a site must specify the same two machines as the primary and secondary real-time distributors.

- Step 2** The ICM's InfoMaker for ICM is based on Powersoft's InfoMaker product. This product lets you create your own report templates to add to the standard templates available in Monitor ICM.

If InfoMaker is already installed on the machine, check the box for **InfoMaker Directory** and enter the name of the directory in which it is installed. If InfoMaker is not installed, you cannot use the InfoMaker for ICM.

- Step 3** For systems using Rockwell Galaxy ACDs, the ICM includes an optional Demand Command Client utility. This utility lets you send Demand commands to the ACD from an Admin Workstation. If you want to install this utility, check this box. By default, Setup installs the Demand Command Client in a DCClient directory under the customer subdirectory (for example, \icm\cust1\DCClient). To choose a different directory, click the adjacent **Browse** button.
- Step 4** If you are using Galaxy ACDs, you can optionally load Galaxy Resource Management Center (RMC) data from the ACDs to the local database. Specify the reporting interval used by the ACDs: 15 minutes or 30 minutes.
- Step 5** Check this box to install the ICM's optional Cisco *Schedule Link* product. This allows you to import scheduling information from a third-party workforce management system.
- Step 6** Check this box to enable the Outbound Option configuration tools in the ICM Configuration Manager.
- Step 7** In addition to viewing reports on your screen, the ICM software also lets you schedule specific reports to be printed at certain times of day. For example, you might want to print a daily summary report each night after midnight. In order for these scheduled reports to print, the Print Server process must be running in the background. To ensure that this process is available, check the **Start ICM Print Server on User Login** option.
- Step 8** When you click **Next** from the Admin Workstation Client Properties screen, the Check Setup Information window appears.

Ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button. When the settings are correct, click the **Next** button to begin copying files.

The copying process may take several minutes to complete. You can continue with other work while Setup operates in the background.

If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager now. It is not recommended that you start the Node Manager until you have completed the entire ICM installation.

- Step 9** Click **Finish** to exit Setup and optionally start the Node Manager.

If you choose to start it, the Node Manager automatically starts the other ICM processes on the Admin Workstation: the local logger process, the real-time client, and (if the Admin Workstation is the active distributor) the real-time distributor.

AW Databases

When you install a Distributor Admin Workstation, ICM Setup automatically sizes and creates a local database on the machine. Because this database is constantly overwritten by new data, the database size remains fairly constant. You normally do not need to resize the Distributor AW real-time database. If you do need to resize the Distributor AW database, you can do so using the ICM Database Administration (ICMDBA) tool.

After you install the AW, you must create an HDS database on a real-time Distributor Admin Workstation. The same considerations that affect the size of the central database also affect the size of the HDS database.

For complete instructions on installing the HDS database with ICMDBA, refer to the *Cisco ICM Enterprise Edition Administration Guide*.



Device Configuration

Before you can complete the installation of Network Interface Controllers (NICs) and Peripheral Gateways (PGs), you must create configuration records in the ICM database. To create these configuration records you must have installed a CallRouter, a Logger, and an Admin Workstation.

This chapter explains the following:

- Running the ICM Configuration Manager on an Admin Workstation to create configuration records for NICs and PGs.
- Running the local ICM Setup on the CallRouter machine to activate device assignments.
- Setting up NICs on the CallRouter machine.

[Chapter 6, “Peripheral Gateway Setup”](#) describes how to install and configure Peripheral Gateway software using the configuration records you create in the Configuration Manager.

Configuration Changes

To create the configuration records:

-
- Step 1** Start the ICM AW, Logger and Router services.
 - Step 2** Start the Configuration Manager on the Admin Workstation. To start the Configuration Manager, double-click on its icon within the ICM Admin Workstation program group.

For information about the Configuration Manager, see the *Cisco ICM Enterprise Edition Configuration Guide*.

Step 3 To create the appropriate configuration records for a NIC or a PG, run the NIC Explorer or PG Explorer from the ICM Admin Workstation Group directory. The following records are created with these options:

- Logical_Interface_Controller (one for each NIC or PG)
- Physical_Interface_Controller (one for each PG; one or more for each NIC)
- Peripheral (from 1 to 5 for each PG)
- Routing_Client (one or more for each NIC and for each PG that uses Post-Routing)

Step 4 You can view and edit the individual records through the Configuration Manager. For example, to view a Logical_Interface_Controller record, choose **Logical Interface Controller** from the Requesters menu. The Configuration Manager displays a list of records. To view a specific record, double-click on it, or select it and click the **Update** button.

To complete the installation of NICs and PGs, you need to get a few specific values from the records you create in the Configuration Manager:

- For a NIC, you need the Physical Controller ID from each Physical_Interface_Controller record.
- For a PG, you need the Logical Controller ID from the Logical_Interface_Controller record and the Peripheral ID from each Peripheral record.

CallRouter Device Setup

You must enable DMP assignments within the CallRouter for each PG and for each AT&T NIC and BT NIC (if any). For all other NICs, you must configure the appropriate subcomponents within the CallRouter.

To make these changes, run the local version of ICM Setup that was installed on the CallRouter machine. The executable is SETUP.EXE in the \icm\bin directory.

Device Management Protocol (DMP)

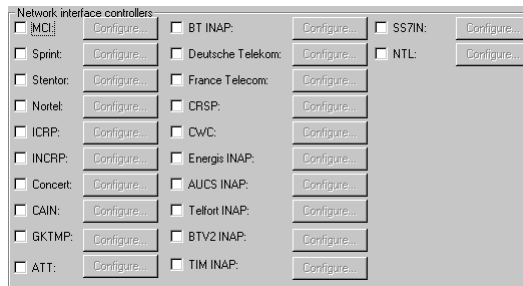
Within the CallRouter configuration, you must enable Device Management Protocol (DMP) connections for each PG and for each AT&T NIC and each BT NIC (if any) in the system.

See [Chapter 3, “CallRouter Setup”](#) for information on the DMP settings.

NIC Configuration

The Network Interface Controller (NIC) runs as subcomponents of the CallRouter (with the exception of the AT&T and BT NICs, which run as a separate components on separate computers). After you have defined the NICs in the Configuration Manager, you must run ICM Setup on the CallRouter to complete the NIC configuration.

In the Router Component Properties dialog box, you can indicate whether you want to enable any or all of the NICs:



The following subsections describe how to set up each of the ICM NICs.

MCI NIC

To configure an MCI NIC, check the **MCI NIC** option in the Router Component Properties window and then click the adjacent **Configure** button. The MCI NIC Properties dialog box appears. You need to enter the Physical Controller ID value from the Configuration Manager.

MCI NIC Properties

Network Interface Controller properties

IP name: 161.44.231.78 Physical controller ID: 0

Handshake timeout: 5000 Consecutive timeout:

Idle timeout: 20000

Use DES encryption for message authentication

Remote data gateway properties

RDG0 description: XRDG1 - Irving, TX	RDG3 description: CARDG2 - Doming
RDG0 A: xxx.40.208.132	RDG3 A: xxx.40.208.147
RDG0 B: xxx.40.208.140	RDG3 B: xxx.40.208.155
RDG1 description: TXRDG2 - Irving, T	RDG4 description: NJRDG1 - West Or
RDG1 A: xxx.40.208.131	RDG4 A: xxx.40.208.172
RDG1 B: xxx.40.208.139	RDG4 B: xxx.40.208.180
RDG2 description: CARDG1 - Doming	RDG5 description: NJRDG2 - West Or
RDG2 A: xxx.40.208.148	RDG5 A: xxx.40.208.171
RDG2 B: xxx.40.208.156	RDG5 B: xxx.40.208.179

OK Cancel Help

Typically, you do not need to change any other values in this dialog box. The first field is initialized to the high priority, private network IP address of the CallRouter machine. The other values are standard defaults for all MCI NICs.

Sprint NIC

To configure a Sprint NIC, check the **Sprint NIC** option in the Router Properties window and then click the adjacent **Configure** button. The Sprint NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

Sprint NIC Properties

Number SCPs: 3

Number links per SCP: 1

Idle timeout: 30000

Physical controller ID: 0

Consecutive timeout limit:

OK Cancel Help

Set the Number SCPs to 4. Typically, you do not need to change any other values in this dialog box. The Number SCPs and Number Links Per SCP are standard for all Sprint NICs. Do not change the Idle Timeout or Transaction Overflow Limit unless told to do so by your Cisco Support representative.

Stentor NIC

To configure a Stentor NIC, check the **Stentor NIC** option in the Router Properties window and then click the adjacent **Configure** button. The Stentor NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

Network Interface Controller properties			ATfG properties			
Physical controller ID:	0		Keepalive timeout:	1		
Consecutive timeout:			Keepalive Retry Limit:	2		
Local IP Address:						
Stentor Advanced Toll-Free Gateways						
Description	IP Address	TCP Port	Username To ATfG	Password To ATfG	Username From ATfG	Password From ATfG
			OK	Cancel	Help	

For the other fields in the top part of the dialog box, the default values are usually appropriate. In the bottom part of the dialog box, fill in the specific information for each network ATfG that communicates with the NIC.

Nortel NIC

To configure a Nortel NIC, check the **Nortel NIC** option in the Router Properties window and then click the adjacent **Configure** button. The Nortel NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

For the other fields in the top part of the dialog box, the default values are usually appropriate. In the bottom part of the dialog box, fill in the specific information for each network SCP that communicates with the NIC.

ICRP NIC



Note

NAM configurations are not supported in ICM release 6.0(0)

To configure an ICRP NIC, check the **ICRP** option in the Router Properties window and then click the adjacent **Configure** button. The ICRP NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

For the other fields in the top part of the dialog box, the default values are usually appropriate. In the Network Applications Manager/Service Control Point section, specify the Side A and Side B addresses for each Network Applications Manager (NAM) that acts as a Service Control Point (SCP) for the ICRP NIC.

INCRP NIC



Note

NAM configurations are not supported in ICM release 6.0(0)

To configure an INCRP NIC, check the **INCRP** option in the Router Properties window and then click the adjacent **Configure** button. The INCRP NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

Enable	Description	Client Id	AppGatewayId	Side A address	Side B address
<input checked="" type="checkbox"/>	First INCRP par	0	0	0.0.0.0	0.0.0.0
<input type="checkbox"/>		0	0	0.0.0.0	0.0.0.0
<input type="checkbox"/>		0	0	0.0.0.0	0.0.0.0
<input type="checkbox"/>		0	0	0.0.0.0	0.0.0.0
<input type="checkbox"/>		0	0	0.0.0.0	0.0.0.0
<input type="checkbox"/>		0	0	0.0.0.0	0.0.0.0
<input type="checkbox"/>		0	0	0.0.0.0	0.0.0.0
<input type="checkbox"/>		0	0	0.0.0.0	0.0.0.0
<input type="checkbox"/>		0	0	0.0.0.0	0.0.0.0
<input type="checkbox"/>		0	0	0.0.0.0	0.0.0.0

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Client ICM to set up each Client ICM that acts as a Service Control Point (SCP) for the INCRP NIC. Check the box to enable the Client ICM. In the Description field, enter a description of the Client ICM. In the Client ID field, enter the name of the Client ICM machine (client ID in this case is the NAM). In the AppGateway ID field, specify the ApplicationGatewayID for the INCRP NIC as configured in the Client ID database. Use the Side A and Side B address fields to enter the high priority visible address of the NAM for the Side A and Side B SCP.

Concert NIC

To configure a Concert NIC, check the **Concert** option in the Router Properties window and then click the adjacent **Configure** button. The Concert NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the Concert Gateway. In the Description field, enter any descriptive text you want for the connection to the Concert Gateway. In the Address field, enter the IP address or hostname for the Concert Gateway. In the Port field, enter the TCP port to use for connection to the Concert Gateway.

CAIN NIC

To configure a CAIN NIC, check the **CAIN** option in the Router Properties window and then click the adjacent **Configure** button. The CAIN NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the CAIN Gateway. In the Description field, enter any descriptive text you want for the connection to the CAIN Gateway. In the Address field, enter the IP address or hostname for the CAIN Gateway. In the Port field, enter the TCP port to use for connection to the CAIN Gateway.

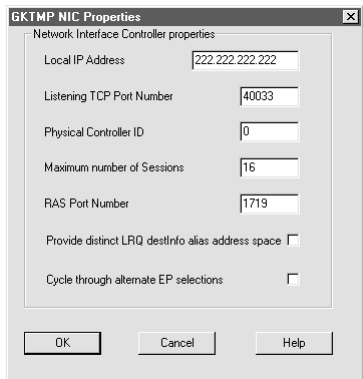
GKTMP NIC



Note

NAM configurations are not supported in ICM release 6.0(0)

To configure a GKTMP NIC, check the **GKTMP** option in the Router Properties window and then click the adjacent **Configure** button. The GKTMP NIC Properties dialog box appears.



Use the Network Interface Controller Properties to apply settings to the NIC device. In the Local IP Address field, enter the IP address or host name for the GKTMP NIC. In the Listening TCP Port Number field, enter the port number that the GKTMP NIC will use to listen for TCP/IP connections. In the Physical controller ID field, enter Integer identifier for the GKTMP NIC from the Physical_Interface_Controller table in the ICM database. In the Maximum Number of Sessions field, enter the number of sessions you want the NIC to support. The GKTMP NIC supports up to a maximum of 64 sessions. In the RAS Port Number field, enter the port number used in the LCF response message for the Registration, Admission and Status protocol address. The default is 1719.

Check the **Provide distinct LRQ destInfo alias address space** box if you want the GKTMP NIC to add a special prefix character to all LRQ destinationInfo aliases before they go to the NAM router.

Check the **Cycle through alternate EP selections** box to enable the GKTMP NIC to cycle alternate EP selections. A maximum of ten endpoint transport addresses will be configurable in the NAM.

AT&T NIC

To configure a AT&T NIC, check the **AT&T** option in the Router Properties window and then click the adjacent **Configure** button. The AT&T NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

AT&T NIC Properties

Network Interface Controller properties

Physical controller ID: Consecutive timeout:

Close timeout: Open timeout:

Gateway Properties

Description	Address	Port	Description	Address	Port
GW0	<input type="text"/>	<input type="text"/>	GW8	<input type="text"/>	<input type="text"/>
GW1	<input type="text"/>	<input type="text"/>	GW9	<input type="text"/>	<input type="text"/>
GW2	<input type="text"/>	<input type="text"/>	GW10	<input type="text"/>	<input type="text"/>
GW3	<input type="text"/>	<input type="text"/>	GW11	<input type="text"/>	<input type="text"/>
GW4	<input type="text"/>	<input type="text"/>	GW12	<input type="text"/>	<input type="text"/>
GW5	<input type="text"/>	<input type="text"/>	GW13	<input type="text"/>	<input type="text"/>
GW6	<input type="text"/>	<input type="text"/>	GW14	<input type="text"/>	<input type="text"/>
GW7	<input type="text"/>	<input type="text"/>	GW15	<input type="text"/>	<input type="text"/>

OK Cancel Help

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the AT&T Gateway. In the Description field, enter any descriptive text you want for the connection to the AT&T Gateway. In the Address field, enter the IP address or hostname for the AT&T Gateway. In the Port field, enter the TCP port to use for connection to the AT&T Gateway.

BT INAP NIC

To configure a BT INAP NIC, check the **BT INAP** option in the Router Properties window and then click the adjacent **Configure** button. The INAP NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

INAP NIC Properties

Network Interface Controller properties

Physical controller ID: Consecutive timeout:

Close timeout: Open timeout: No answer timeout:

Inter-update minimum:

Gateway Properties

Description	Address	Port	Description	Address	Port
GW0	<input type="text"/>	<input type="text"/>	GW8	<input type="text"/>	<input type="text"/>
GW1	<input type="text"/>	<input type="text"/>	GW9	<input type="text"/>	<input type="text"/>
GW2	<input type="text"/>	<input type="text"/>	GW10	<input type="text"/>	<input type="text"/>
GW3	<input type="text"/>	<input type="text"/>	GW11	<input type="text"/>	<input type="text"/>
GW4	<input type="text"/>	<input type="text"/>	GW12	<input type="text"/>	<input type="text"/>
GW5	<input type="text"/>	<input type="text"/>	GW13	<input type="text"/>	<input type="text"/>
GW6	<input type="text"/>	<input type="text"/>	GW14	<input type="text"/>	<input type="text"/>
GW7	<input type="text"/>	<input type="text"/>	GW15	<input type="text"/>	<input type="text"/>

OK Cancel Help

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the BT INAP Gateway. In the Description field, enter any descriptive text you want for the connection to the BT INAP Gateway. In the Address field, enter the IP address or hostname for the BT INAP Gateway. In the Port field, enter the TCP port to use for connection to the BT INAP Gateway.

Deutsche Telekom NIC

To configure a Deutsche Telekom NIC, check the **Deutsche Telekom** option in the Router Properties window and then click the adjacent **Configure** button. The Deutsche Telekom NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

Deutsche Telekom NIC Properties		
Network Interface Controller properties		
Physical Controller ID	[Dropdown]	Maximum Dialog Duration [Text]
Local IP Address	161.44.231.78	
SCP Clients		
Enabled	Description	IP Address
<input type="checkbox"/>	[Text]	[Text]
<input type="checkbox"/>	[Text]	[Text]
<input type="checkbox"/>	[Text]	[Text]
<input type="checkbox"/>	[Text]	[Text]
<input type="checkbox"/>	[Text]	[Text]
<input type="checkbox"/>	[Text]	[Text]
<input type="checkbox"/>	[Text]	[Text]
<input type="checkbox"/>	[Text]	[Text]
<input type="checkbox"/>	[Text]	[Text]
OK Cancel Help		

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the SCP Clients section to enter values for each connection between the NIC and SPC Clients. Check the **Enabled** box to enable the connection. In the Description field, enter any descriptive text you want to use to describe the connection. In the IP Address field, enter the IP address or hostname for the SCP.

France Telecom NIC

To configure a France Telecom NIC, check the **France Telecom** option in the Router Properties window and then click the adjacent **Configure** button. The France Telecom NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

The dialog box is titled "France Telecom NIC Properties" and contains the following fields and sections:

- Physical controller ID:** []
- Consecutive timeout link:** []
- Eicon Port:** []
- Open Dialog timeout:** [6000]
- Routing Server ID:** [CRG1]
- Close Dialog timeout:** [6000]
- Routing Server Local NUA:** [000000000]
- Idle Link timeout:** [15000]

Switched Virtual Circuits:

Enabled	Description	NUA	ID
<input type="checkbox"/>	Primes CVC	[000000000]	[SCP00]
<input type="checkbox"/>	Quatre CVC	[000000000]	[SCP01]
<input type="checkbox"/>	France CVC	[000000000]	[SCP02]
<input type="checkbox"/>	Quatre CVC	[000000000]	[SCP03]
<input type="checkbox"/>	Quatre CVC	[000000000]	[SCP04]
<input type="checkbox"/>	France CVC	[000000000]	[SCP05]
<input type="checkbox"/>	France CVC	[000000000]	[SCP06]
<input type="checkbox"/>	France CVC	[000000000]	[SCP07]
<input type="checkbox"/>	Neuville CVC	[000000000]	[SCP08]
<input type="checkbox"/>	Dwaine CVC	[000000000]	[SCP09]

Buttons: OK, Cancel, Help

For the other fields in the top part of the dialog box, the default values are usually appropriate. In the Switched Virtual Circuits section, fill in the specific information for each network SCP that communicates with the NIC. Check the **Enable** box to enable the SCP. In the Description field, provide a description of the SCP. In the NUA field, enter a 15-digit Network User Address of the SCP. In the ID field enter a 5-character id that the X.25 network uses to identify the SCP in the Open Dialog.

CRSP NIC

To configure a CRSP NIC, check the **CRSP** option in the Router Properties window and then click the adjacent **Configure** button. The CRSP NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

CRISP NIC Properties

Network Interface Controller properties

Physical controller ID: [0] Consecutive timeout: []

Local IP Address: [222.222.222.222] Open Dialog timeout: [6000]

Retrain retry count: []

SCP/VRU Clients

Enabled	Description	IP Address	Client ID
<input type="checkbox"/>	[]	[]	[0]
<input type="checkbox"/>	[]	[]	[0]
<input type="checkbox"/>	[]	[]	[0]
<input type="checkbox"/>	[]	[]	[0]
<input type="checkbox"/>	[]	[]	[0]
<input type="checkbox"/>	[]	[]	[0]
<input type="checkbox"/>	[]	[]	[0]
<input type="checkbox"/>	[]	[]	[0]
<input type="checkbox"/>	[]	[]	[0]
<input type="checkbox"/>	[]	[]	[0]
<input type="checkbox"/>	[]	[]	[0]

OK Cancel Help

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the SCP/VRU Clients section to enter values for the SCP. Check the **Enabled** box to enable the SCP. In the Description field, enter a description of the SCP. In the IP Address field, enter the IP address of the SCP. In the Client ID field, enter the ID of the SCP. If there are multiple SCPs using the same IP address, the Client ID must be unique for each SCP at the address.

CWC NIC

To configure a CWC NIC, check the **CWC** option in the Router Properties window and then click the adjacent **Configure** button. The CWC NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

CWC NIC Properties

Network Interface Controller properties

Physical controller ID: [0] Consecutive timeout: [10]

Close timeout: [30] Open timeout: [10] No answer timeout: [15]

Inter-update minimum: []

Gateway Properties

Description	Address	Port	Description	Address	Port
GW0	[]	[]	GW8	[]	[]
GW1	[]	[]	GW9	[]	[]
GW2	[]	[]	GW10	[]	[]
GW3	[]	[]	GW11	[]	[]
GW4	[]	[]	GW12	[]	[]
GW5	[]	[]	GW13	[]	[]
GW6	[]	[]	GW14	[]	[]
GW7	[]	[]	GW15	[]	[]

OK Cancel Help

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the CWC Gateway. In the Description field, enter any descriptive text you want for the connection to the CWC Gateway. In the Address field, enter the IP address or hostname for the CWC Gateway. In the Port field, enter the TCP port to use for connection to the CWC Gateway.

Energis INAP NIC

To configure a Energis INAP NIC, check the **Energis INAP** option in the Router Properties window and then click the adjacent **Configure** button. The Energis INAP Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

ENERGIS INAP Properties					
Network Interface Controller properties					
Physical controller ID:	<input type="text"/>	Consecutive timeout:	<input type="text" value="10"/>		
Close timeout:	<input type="text" value="30"/>	Open timeout:	<input type="text" value="10"/>	No answer timeout:	<input type="text" value="15"/>
Inter-update minimum:	<input type="text"/>				
Gateway Properties					
Description	Address	Port	Description	Address	Port
GW0	<input type="text"/>	<input type="text"/>	GW8	<input type="text"/>	<input type="text"/>
GW1	<input type="text"/>	<input type="text"/>	GW9	<input type="text"/>	<input type="text"/>
GW2	<input type="text"/>	<input type="text"/>	GW10	<input type="text"/>	<input type="text"/>
GW3	<input type="text"/>	<input type="text"/>	GW11	<input type="text"/>	<input type="text"/>
GW4	<input type="text"/>	<input type="text"/>	GW12	<input type="text"/>	<input type="text"/>
GW5	<input type="text"/>	<input type="text"/>	GW13	<input type="text"/>	<input type="text"/>
GW6	<input type="text"/>	<input type="text"/>	GW14	<input type="text"/>	<input type="text"/>
GW7	<input type="text"/>	<input type="text"/>	GW15	<input type="text"/>	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>					

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the Energis INAP Gateway. In the Description field, enter any descriptive text you want for the connection to the Energis INAP Gateway. In the Address field, enter the IP address or hostname for the Energis INAP Gateway. In the Port field, enter the TCP port to use for connection to the Energis INAP Gateway.

AUCS INAP NIC

To configure a AUCS INAP NIC, check the **AUCS INAP** option in the Router Properties window and then click the adjacent **Configure** button. The Unisource NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

Gateway Properties			Gateway Properties		
Description	Address	Port	Description	Address	Port
GW0			GW8		
GW1			GW9		
GW2			GW10		
GW3			GW11		
GW4			GW12		
GW5			GW13		
GW6			GW14		
GW7			GW15		

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the Unisource INAP Gateway. In the Description field, enter any descriptive text you want for the connection to the Unisource INAP Gateway. In the Address field, enter the IP address or hostname for the Unisource INAP Gateway. In the Port field, enter the TCP port to use for connection to the Unisource INAP Gateway.

Telfort INAP NIC

To configure a Telfort INAP NIC, check the **Telfort INAP** option in the Router Properties window and then click the adjacent **Configure** button. The Telfort NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the Telfort INAP Gateway. In the Description field, enter any descriptive text you want for the connection to the Telfort INAP Gateway. In the Address field, enter the IP address or hostname for the Telfort INAP Gateway. In the Port field, enter the TCP port to use for connection to the Telfort INAP Gateway.

BTV2 INAP NIC

To configure a BTV2 INAP NIC, check the **BTV2 INAP** option in the Router Properties window and then click the adjacent **Configure** button. The BTV2 INAP NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

BTV2INAP NIC Properties

Network Interface Controller properties

Physical controller ID: Consecutive timeout:

Close timeout: Open timeout: No answer timeout:

Inter-update minimum:

Gateway Properties

Description	Address	Port	Description	Address	Port
GW0	<input type="text"/>	<input type="text"/>	GW8	<input type="text"/>	<input type="text"/>
GW1	<input type="text"/>	<input type="text"/>	GW9	<input type="text"/>	<input type="text"/>
GW2	<input type="text"/>	<input type="text"/>	GW10	<input type="text"/>	<input type="text"/>
GW3	<input type="text"/>	<input type="text"/>	GW11	<input type="text"/>	<input type="text"/>
GW4	<input type="text"/>	<input type="text"/>	GW12	<input type="text"/>	<input type="text"/>
GW5	<input type="text"/>	<input type="text"/>	GW13	<input type="text"/>	<input type="text"/>
GW6	<input type="text"/>	<input type="text"/>	GW14	<input type="text"/>	<input type="text"/>
GW7	<input type="text"/>	<input type="text"/>	GW15	<input type="text"/>	<input type="text"/>

OK Cancel Help

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the BTV2 INAP Gateway. In the Description field, enter any descriptive text you want for the connection to the BTV2 INAP Gateway. In the Address field, enter the IP address or hostname for the BTV2 INAP Gateway. In the Port field, enter the TCP port to use for connection to the BTV2 INAP Gateway.

TIM INAP NIC

To configure a TIM INAP NIC, check the **TIM INAP** option in the Router Properties window and then click the adjacent **Configure** button. The TIM INAP NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the TIM INAP Gateway. In the Description field, enter any descriptive text you want for the connection to the TIM INAP Gateway. In the Address field, enter the IP address or hostname for the TIM INAP Gateway. In the Port field, enter the TCP port to use for connection to the TIM INAP Gateway.

SS7IN NIC

To configure a SS7IN NIC, check the **SS7IN** option in the Router Properties window and then click the adjacent **Configure** button. The SS7IN NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

For the other fields in the top part of the dialog box, the default values are usually appropriate. Use the Gateway Properties section to enter values for each connection between the NIC and the SS7IN Gateway. In the Description field, enter any descriptive text you want for the connection to the SS7IN Gateway. In the Address field, enter the IP address or hostname for the SS7IN Gateway. In the Port field, enter the TCP port to use for connection to the SS7IN Gateway.

NTL NIC

To configure a NTL NIC, check the **NTL** option in the Router Properties window and then click the adjacent **Configure** button. The NTL NIC Properties dialog box appears. Enter the Physical Controller ID value from the Configuration Manager.

For the other fields in the dialog box, the default values are usually appropriate.



Peripheral Gateway Setup

A Peripheral Gateway (PG) is the part of the ICM software that communicates directly with the local switch within a call center. Each ACD, VRU, or PBX that receives calls from the ICM software must be associated with a PG. The PG reads information from the switch and transfers it to the Central Controller. The ICM software may also pass information to the switch through the PG. A single PG may serve several switches. For each switch you must configure a Peripheral Interface Manager (PIM) within the PG.

Before you install the PG software, the Windows operating system must be installed on the computer.

To configure a PG, you must know the visible network addresses for the CallRouter machines. If the PG is duplexed, you must know the visible and private network addresses of its duplexed peer.

For each PG, you must have defined a Logical_Interface_Controller record, a Physical_Interface_Controller record, and from one to five Peripheral records. (Configure ICM creates these records automatically if you choose Configure a PG using the PG Explorer.)

For information on using Configure ICM to set up the database records for a PG, see [Chapter 5, “Device Configuration”](#).



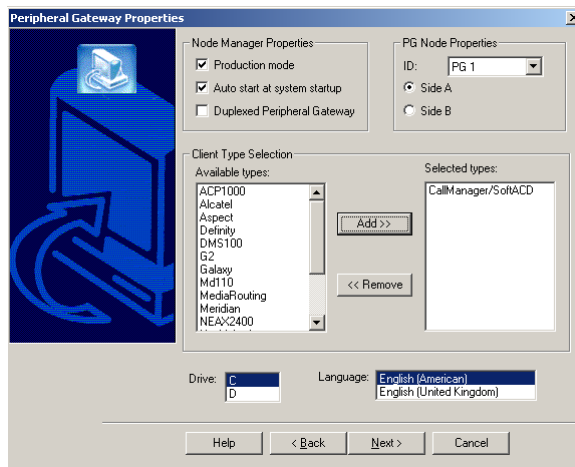
Note

ICM software restricts running more than two PGs of the same instance on a single machine at the same time.

Peripheral Gateway Properties

Run SETUP.EXE from the ICM CD-ROM. Add the customer if you have not already done so. Install a PG, as follows:

- Step 1** Click **Add** in the Customer Components section and choose **Peripheral Gateway** from the ICM Component Selection window. The Peripheral Gateway Properties window appears.



- Step 2** Choose **Production Mode** and **Auto Start at System Startup** unless you are specifically told otherwise by your Cisco Support representative. This ensures that the Peripheral Gateway can restart itself automatically if necessary.

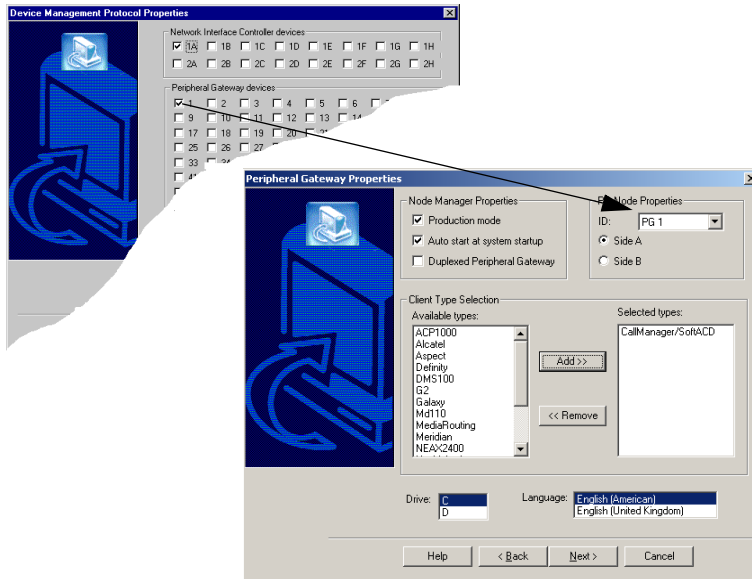


Note

It is recommended that you set the Auto Start feature after installation is complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before hotfixes and/or databases are applied.

- Step 3** Specify whether the PG is part of a duplexed pair.
- Step 4** In the ID field, choose the PG's device identifier as enabled in the CallRouter's DMP configuration dialog box.

Figure 6-1 Peripheral Gateway DMP Configuration

**Note**

Each logical PG must have a unique device assignment at the CallRouter. (If a PG is duplexed, both physical machines use the same device assignment.) To add another logical PG, you must enable another PG device for the CallRouter.

- Step 5** If the PG is duplexed, specify whether you are installing Side A or Side B. If the PG is simplexed, select Side A.
- Step 6** Use Client Type Selection section of the screen to select the type of Peripheral Gateway you want to add. Use the **Add** and **Remove** buttons to select or de-select PG types. You can install one PG type and one VRU PG at the same time.

**Note**

To allow the ICM software to route email if there is no CallManager or ACD PG installed, you need to install and configure both a MediaRouting PG and a NonVoiceAgent PG. CTI Sever must also be configured on both PG machines. The MR PG interface provides routing instructions to the CEM application, while the non-voice Agent PG configuration is used to report agent state and status to the ICM software.

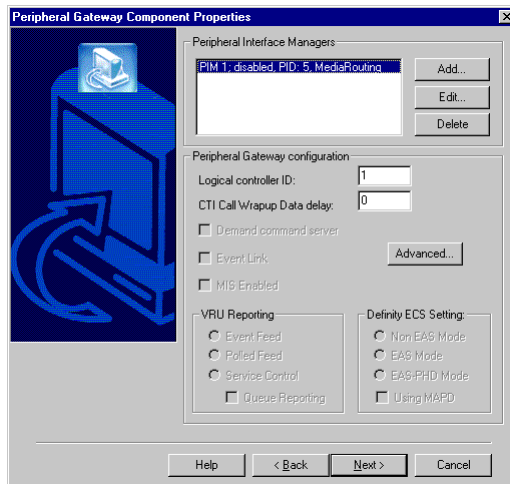
Step 7 Choose the local disk on which you want to install the PG software.



Note Be sure to note the drive you are using for future reference, since this information is required when applying hotfixes.

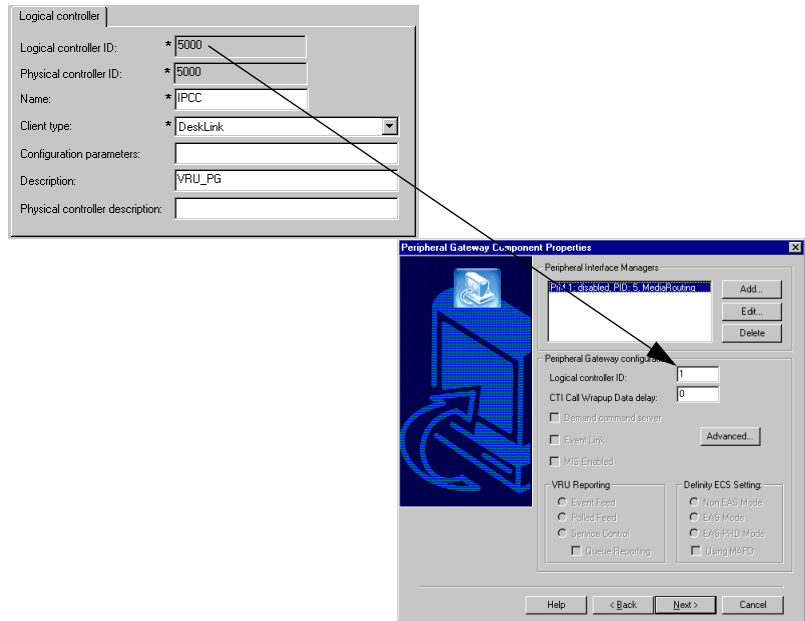
Step 8 Choose the language.

Step 9 Click **Next**. The Peripheral Gateway Component Properties window appears.



Step 10 In the Peripheral Gateway Configuration section of the window, enter the Controller ID from the Logical_Interface_Controller record for the PG. You can view the Logical_Interface_Controller record for the PG using the PG Explorer tool from the Configuration Manager.

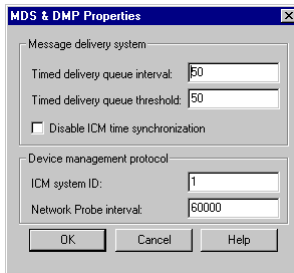
Figure 6-2 Peripheral Gateway Logical Controller ID



- Step 11** The CTI Call Wrapup Data Delay applies only if a CTI application interfaces with the PG. The option specifies the number of seconds the PG waits for the CTI client to send data after the agent finishes call wrap-up. The default is 120 seconds. The PG waits this long for the CTI client to explicitly release the wrap-up data. If the time expires, the PG assumes the wrap-up data are complete.
- Step 12** Each of the remaining options in this window is available only for specific peripheral types:
- The **Demand Command Server** option is enabled only if the PG supports Galaxy ACDs. Check this option if you want to use the ICM's Demand Command Client to send demand commands to the ACD.
 - The **EAS mode** options are available only if the PG supports Avaya Definity ECS ACDs. Check the appropriate option to specify whether the ACD runs in non-EAS mode, normal EAS mode, or EAS with PHD mode. The **Using MAPD** option is for Definity ACDs which use the MAP/D interface.

- The **Event Link** option is available only if the PG supports Aspect CallCenter ACDs. Check this option if you want the PG to communicate with the ACD through the Aspect Event Link.
- The **VRU Reporting** options are available only if the PG supports VRUs. Select the option that you want to use for VRU reporting. The Service Control option will be enabled by default.

Step 13 When you click the **Advanced** button in the Peripheral Gateway Component Properties window, the MDS & DMP Properties dialog box appears.



Do not change the default values for the Timed Delivery Queue unless told to do so by your Cisco Support representative.

The **Disable ICM Time Synchronization** box is used to select time synchronizatoin service. The box is checked, by default, since the Windows 2000 operating system uses its own integrated time service. If the machine you are configuring is a domain machine, leave this box checked. However, if the machine is a workgroup machine, uncheck this box to enable ICM Time Synchronization. You should note setup will not change current configuration when performing an Upgrade all.

For a domain machine, setup will also show the current status of Windows Time service.

For the ICM System ID, enter the number of the PG as specified in the Peripheral Gateway Properties window (for example, enter 3 for PG 3).

The Probe Interval determines how frequently the PG sends test messages to the CallRouter. Do not change this value unless told to do so by your Cisco Support representative.

Step 14 Click OK when you are finished with this window.

Continue to next section of this chapter, which describes the Peripheral Interface Manager (PIM) portion of the PG installation.

Peripheral Interface Managers

A Peripheral Interface Manager (PIM) is that part of the PG software that communicates directly with a peripheral. You must add a PIM for each peripheral associated with the PG. Each PG can have up to 32 associated peripherals (and, hence, up to 32 PIMs). All associated peripherals must be of the same type. The switch type was indicated earlier in the Setup process.

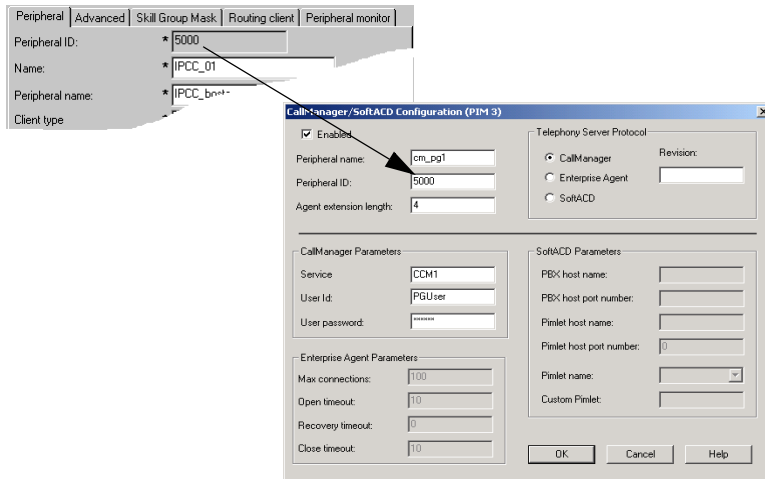
To add a PIM:

-
- Step 1** Click **Add** in the Peripheral Gateway Component Properties window. The standard Add PIM dialog box displays.
- Step 2** Choose the PIM to add from the Available PIMs list. The list contains only PIM numbers that are not already defined for this PG.

When you click the **OK** button, a dialog box appears in which you can enter the properties of the peripheral. The fields in this dialog box are different for each switch type. The specific dialog boxes are described later in this section. Each dialog box contains an Enabled option, a Peripheral name field, and a Peripheral ID field.

- To put the PIM into service, check the **Enabled** option. This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.
- Enter the peripheral name in the Peripheral name field. In most cases, you will want to use the enterprise name from the associated Peripheral record.
- Enter the Peripheral ID from the Peripheral record, as shown in [Figure 6-3](#). You can view the Peripheral ID of the PG using the PG Explorer tool in the Configuration Manager.

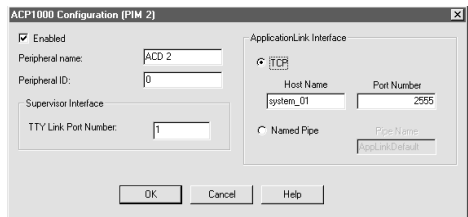
Figure 6-3 Peripheral Interface Manager Peripheral ID



The following subsections describe the dialog boxes for each switch type.

ACP1000

The ACP1000 dialog box appears as follows:



In the Supervisor Interface section, enter the TTY Link Port Number. The ACP1000 PIM uses this link to obtain agent configuration information with the PIM starts up.

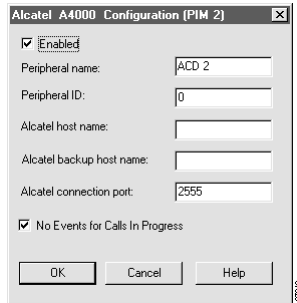
In the ApplicationLink Interface section, select the type of interface you want to establish between the PG and the host server:

- **TCP.** Click this radio button if you want to configure an ethernet connection to the host server. Enter the host name of the server and the TCP port number.

- **Named Pipe.** Click this radio button if you want to configure a named pipe connection to the host server. Enter the pipe name.

Alcatel A4400

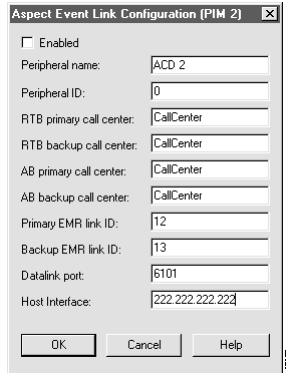
The Alcatel A4400 dialog box appears as follows:



In the Alcatel A4400 host name field, enter the TCP host name of the Alcatel A4400 system. In the Alcatel A4400 connection port field, enter the TCP port number of the Alcatel A4400 system. For Alcatel switch releases 3.0 and greater, you need to check the box labeled **No Events for Calls In Progress**.

Aspect

The dialog you see for Aspect ACDs depends on whether you choose Event Link in the Peripheral Gateway Component Properties window. If you choose Event Link, the following dialog box appears:



Aspect Event Link Configuration (PIM 2)

Enabled

Peripheral name: ACD 2

Peripheral ID: 0

RTB primary call center: CallCenter

RTB backup call center: CallCenter

AB primary call center: CallCenter

AB backup call center: CallCenter

Primary EMR link ID: 12

Backup EMR link ID: 13

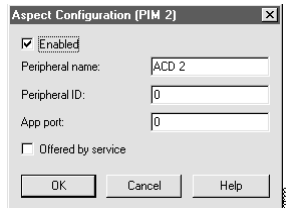
Datalink port: 6101

Host Interface: 222.222.222.222

OK Cancel Help

Specify the primary and backup CallCenter ACDs for the Aspect Real-Time Bridge (RTB), Application Bridge (AB), and Event Monitor Request (EMR) link. Specify the TCP port used for the Event Monitor Request link. Also, if you are using the private PG interface, specify that interface in the Host Interface field. Otherwise the PG uses the public interface by default. The public and private PG interfaces are IP addresses, or names associated with the IP addresses, defined in the HOSTS file.

If you do not choose Event Link, the following dialog box appears:



Aspect Configuration (PIM 2)

Enabled

Peripheral name: ACD 2

Peripheral ID: 0

App port: 0

Offered by service

OK Cancel Help

Do not check the **Offered By Service** option unless your Cisco Support representative tells you otherwise. This option prevents the PIM from gathering statistics about individual ICM routes.

To provide full functionality, the PIM must establish a connection to the Aspect Application Bridge. Enter the port number for this connection (from the Aspect Data Link configuration table) in the App Port field.

Avaya Definity ECS (AT&T PIM)

The dialog you see for the Definity ACD depends on whether or not you select the MAP/D option in the Peripheral Gateway Component Properties window. If you do not select the **MAP/D** option, the Definity ECS Configuration dialog box appears as follows:

Enter the revision number for the Definity ECS ACD.

Fill in the information about the CMS connection in the Call Management System section. The Data Timeout is in milliseconds.

Enter the requested information about the CallVisor setup for both sides of a duplexed PG (or only for Side A if simplex). In the Min ASAI for Failover field, enter the minimum number of Adjunct Switch Application Interface (ASAI) links needed to handle the expected call load. (Each ASAI link can handle up to 8000 busy hour calls.) For each CallVisor host, enter the name, indicate which ASAI links to use and which ASAI links to use for Post-Routing. (Each ASAI link connects to a BRI or Ethernet port on the DEFINITY ECS.)

If you select the **Using MAPD** option on the Peripheral Gateway Component Properties screen, the following screen displays:

Definity ECS PIM Configuration [CVLAN on MAPD] [PIM 2]

Enabled

Peripheral name: Peripheral ID:

Call Management System (CMS) Configuration

CMS Enabled (NOTE: DISABLE if CMS-less)

CMS Hostname: Port number to listen on:

CMS Data Timeout (Typ. 3x Refresh rate) [Millesec]:

Multiple Cisco Reports

Number of Cisco Reports for this PIM: Port number delta (typ: 10):

CVLAN/MAPD Configuration

Host 1: Enabled

Hostname:

ASAI Link # 1 2 3 4 5 6 7 8

Monitor ASAI links:

Post-Route ASAI links:

Heartbeat Maintenance:

Host 2: Enabled (if DUPLEXED)

Hostname:

ASAI Link # 1 2 3 4 5 6 7 8

Monitor ASAI links:

Post-Route ASAI links:

Heartbeat Maintenance:

Minimum number of overall ASAI links before failover:

Default Timed ACW value (Seconds): CMS-less Smart Agent Timer:

OK Cancel Help

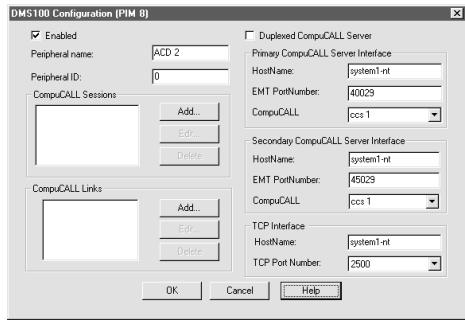
Use the CVLAN/MAPD Configuration fields to describe the Multi-Application Platform in Definity (MAP/D) connections for the PG (and its duplexed pair, if any).

In the Monitor ASAI links field, indicate which ASAI Links in the MAP/D system the PG should use for monitoring calls, stations, etc. In the Post-Route links field, indicate which ASAI Links in the MAP/D system the PG should use for ICM Post-Routingpostroute_def. In the Heartbeat Maintenance field, indicate which ASAI Links in the MAP/D system the ICM will use for heartbeat maintenance.

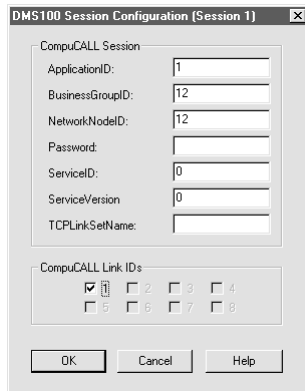
In the Minimum number of overall ASAI links before failover field, indicate the minimum number of ASAI links required for the expected call load. If the PG is duplexed and the number of links available to the PG falls below this value, the ICM attempts to switch over to the other PG. Use the Default Timed ACW value (Seconds) field to indicate the default after-call-work (ACW) value for agents. A zero in the field indicates that the ICM will get this value from the peripheral monitor table. Values entered in this field apply only to monitored agents.

DMS-100

The DMS-100 dialog box appears as follows:



To configure a new CompuCALL session, click the **Add** button to invoke the DMS100 Session Configuration screen. To modify an existing session, select the session and click the **Edit** button to invoke the DMS100 Session Configuration screen. To remove a session, select the session and click the **Delete** button. If adding or editing a session, the CompuCALL dialog box appears:



The ApplicationID is an integer that identifies the ICM as the application that is initiating the logon request.

The BusinessGroupID is an integer that identifies your company. Your Interexchange Carrier defines this ID.

The NetworkNodeID is an integer identifier that specifies the switch that the ICM will use to communicate. This is the switch the host computer connects to via the CompuCALL link. Your Interexchange Carrier defines this ID.

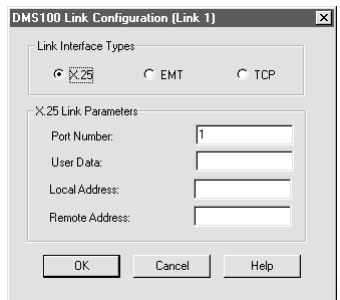
The password corresponds to the BusinessGroupID.

The ServiceID is an integer that identifies the application context to be set for the session (i.e., a service profile containing Application Service Options or subsets, as defined by your Interexchange Carrier).

ServiceVersion is an integer that specifies the application level or the signaling version that the host application is using (i.e., 35 for BCS35).

The CompuCALL Links section lists the CompuCALL links defined on the local computer. The CompuCALL link defines how the ICM PG interacts with the DMS-100.

To configure a new CompuCALL link, click the **Add** button to invoke the DMS100 Link Configuration screen. To modify an existing session, select the session and click the **Edit** button to invoke the DMS100 Link Configuration screen. To remove a link, select the link and click the **Delete** button. When you select add or edit the CompuCALL Link Configuration dialog appears:



The X.25 link option is the only one currently available. The X25 Port is an integer identifier for the X25 card install on the local computer.

X25 User Data is four octets of data (each octet ranging from 0 to 255, expressed in hexadecimal). These data are provided by the Interexchange Carrier as the PROTOCOL subfield.

The X25 Local Address is the X25 address of the local computer. The system administrator provides this value.

X25 Remote refers to the X25 address of the remote switch. The system administrator provides this value.

CallManager/SoftACD

The CallManager/SoftACD Configuration dialog allows you to configure a PG for CallManager or SoftACD applications. The dialog box appears as follows:

To put the PIM into service, check the **Enabled** option. This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.

- Enter the peripheral name in the Peripheral name field. In most cases, you'll want to use the enterprise name from the associated Peripheral record.
- Enter the Peripheral ID from the Peripheral record.
- Enter the number of digits in the agent extension.

In the Telephony Server Protocol section, select the type of application that you want to configure the PG for: IPCC, Enterprise Agent, or SoftACD.

When configuring the PG for IPCC, complete the IPCC parameters section, as follows:

- **Service.** Enter the host name or the IP address of the machine that is running the Cisco CallManager software. If using the host name, the name must be in the hosts file.

- **User ID.** Enter the User ID for the PG. This is the same User ID entered for the PG on the Cisco CallManager Administrator web page when you added the PG as a new user.
- **User Password.** Enter the User Password for the PG. This is the same User Password entered for the PG on the Cisco CallManager Administrator web page.

When configuring the PG for SoftACD, complete the SoftACD parameters section, as follows:

- **PBX host name.** Enter the host name or IP address of the PBX that the pimlet will connect to the PBX.
- **PBX host port number.** Enter the port number on the PBX that the pimlet will use to communicate with the PBX.
- **Pimlet host name.** Enter the host name or IP address of the pimlet machine that the PBX will use.
- **Pimlet host port number.** Enter the port number on the pimlet machine that the PBX will use.
- **Pimlet name.** Select the pimlet from the drop-down list. Select **custom** if you are using a custom pimlet.
- **Custom Pimlet.** If using a custom pimlet, enter the pimlet executable name.

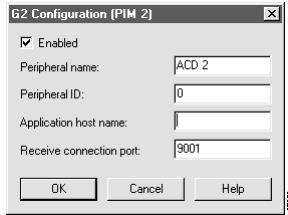
If configuring the PG for Enterprise Agent, complete the Enterprise Agent parameters section, as follows:

- **Max Connections.** Enter the maximum number of agents that can be connected to the peripheral.
- **Open timeout.** Enter the time (in seconds) allowed for the PG to connect to the desktop before session is terminated.
- **Recovery timeout.** Not currently used.
- **Close timeout.** Enter the time (in seconds) allowed for the graceful termination of the session. If the timeout is exceeded the PG closes the session.

Click the **OK** button to save the PIM configuration.

G2 ACD

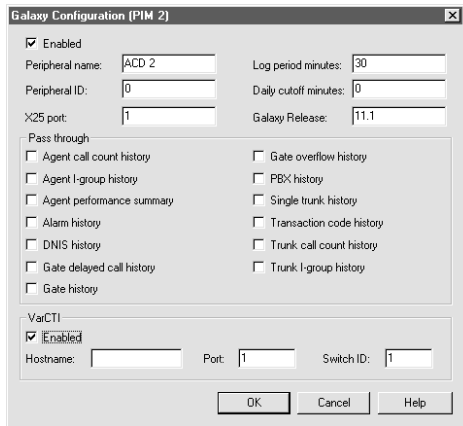
The G2 dialog box appears as follows:



In the Application Host Name field, enter the name of the host computer that passes information to the PIM. In the Receive Connection Port field, enter the PG port number on which the PIM receives the information.

Galaxy

The Galaxy dialog box appears as follows:



Specify the Galaxy ACD X.25 port used for the Foreign Processor Data Link (FPDL). The PIM connects to this port to monitor data from the Galaxy ACD.

The ICM collects information from the Galaxy ACD at the end of each logging period. In the Log Period Minutes field, specify the length of the logging period used by the ACD. In the Daily Cutoff Minutes field, specify how many minutes after midnight the first period of each day begins.

In addition to the normal database tables for peripheral historical and real-time data, the ICM optionally populates additional tables with unprocessed historical data directly from the Galaxy. This allows you, for example, to run legacy reports on Galaxy data. You can choose to populate any or all of these additional tables by checking the appropriate options in the Pass Through section.

The VarCTI facility is an optional feature of the Galaxy ACD that provides host computing services through a VarCTI server. If the PG connects to the VarCTI server for the ACD, check the Enabled box in the VarCTI section. Enter the host name or IP address of the VarCTI server, the port on the server that the PG uses, and the identifier for the ACD recognized by the server.

MD110

The Md110 dialog box appears as follows:

In the Application Link Host field, enter the IP host name or IP address of the machine with the Application Link software. In the Connection Port field, enter the TCP server port used by the Application Link machine. The default is 2555. The Application Link Option field should be set to 1. The CCM ODBC DSN name should be the same name used when configuring the DSN for the Call Center Manager (CCM) connection. The CCM Machine Name should be the name of the machine that holds the CCM database. The CCM User Name is the name of the user that has access to the CCM machine. The CCM Password is the password assigned for the CCM user.

Meridian

The Meridian dialog box appears as follows:

The **Simulator Machine** option is for internal Cisco use only.

In the Interface section, select the interface to be used between the Meridian and the PG. [Table 6-1](#) summarizes the interface options.



Note

The Enhanced CTI interface provides additional detail about call handling (such as transfers and conferencing), but also requires additional configuration. For help in choosing the best interface, consult your Cisco Support Representative.

Table 6-1 Meridian to PG Interfaces

Interface	Description
Enhanced CTI using MEI and Meridian Link or SCCS with MLS	Provides enhanced data for CTI applications in addition to normal Pre-Routing, Post-Routing, and monitoring capabilities.
MEI with Meridian Link or SCCS with MLS for Post-Routing only	Provides normal Pre-Routing, Post-Routing, and monitoring capabilities.
MEI with no Meridian Link or SCCS with MLS	Provides normal Pre-Routing and monitoring capabilities.
High Speed Link	Provides limited capabilities; supported for backwards compatibility only.

If you choose the enhanced CTI interface, you can also choose what information to save in Termination Call Detail rows. Information from the MEI or High Speed Link includes queuing information such as delay times. Information from the Meridian Link or SCCS with MLS contains information set by a CTI client, such as call variables and wrap-up data. (If you choose both, the ICM software writes two Termination Call Detail rows for each call.)

You can specify the type of DNIS matching that the PG applies to the ACD by checking the **Enable Partial DNIS Matching**, **Partial DNIS Matches on Last 4 Digits**, and **Match Any Trunk Group** options.

The PG must connect to either the ACD's High Speed Link (HSL) or to the Meridian Event Interface (MEI) of an associated MAX system. If the HSL interface is used, check the **Use HSL Interface** option. The PG can also connect to an MEI proxy server if there is more than one MEI client.

To support Post-Routing, the PG must connect to the ACD's Meridian Link or SCCS with MLS interface. To enable this feature, check the **Use Meridian Link** option.

If the PG communicates with the PG through the Meridian Event Interface (MEI), fill in the fields in the MEI Configuration section. In the Server Name field, enter the IP name or address of the MAX system that is running the MEI. (If you use a name, that name must be in the PG's host file.) In the Server Port field, enter the port number used when MEI was configured on the MAX. The suggested port number is 44444. Set the Client ID to Cisco_ICM (the default).

If the PG has a connection to the ACD's Meridian Link or SCCS with MLS, fill in the fields in the Meridian Link Configuration section. In the Server Name field, enter the IP name or address of the Meridian Link or SCCS with MLS system. (If you use a name, that name must be in the PG's host file.) In the Server Port field, enter the well-known port used by the Meridian Link or SCCS with MLS (3000, by default). In the Link Host Name field, enter the TCP hostname specified in the Meridian Link's link 1 configuration file. In the Link Machine Name field, enter the Meridian 1 Machine name specified in the Meridian Link's link 0 configuration file. Finally, enter the Meridian 1 customer number for which the PG routes calls.

If the PG communicates with the ACD through the High Speed Link (HSL), fill in the fields in the High Speed Link Configuration section. In the HSL Port field, enter the name of the Meridian HSL port to which the PG connects. To allow the proper initialization of agent state data, set MAX Screen Scrape to 1 and set MAX Port to the name of the Meridian MAX port. Also, enter the MAX supervisor ID and password to be used to retrieve the information.

MediaRouting

The Media Routing Configuration dialog is used to configure the Media Routing interface. This interface allows application software, such as Cisco Email Manager and Cisco Collaboration Server, to access the ICM software task and agent management services for different customer contact mediums, such as email, fax, Web-collaboration, Internet-chats, and voice.



Note

In most cases, the MediaRouting PG tracks and records the state and activity of all voice and non-voice agents. However, you can configure a Non-Voice PG rather than a Media Routing PG to monitor state and activity of agents who are non-voice agents. However, this is optional, and not necessary if you already have a MediaRouting PG configured for Voice agents.

Customer contact applications use the MediaRouting interface to request instructions from the ICM software, when they receive a contact request from a customer using one of the mediums, such as email, fax, Web-collaboration, Internet-chat or voice. When the ICM software receives a new task request from the application, the ICM runs a pre-defined ICM script to determine how to handle the task. As a result of the execution of the ICM script, ICM send an instructions to the application to do one of the following:

- Execute an application script that is stored on the application server, and return the application script execution result to ICM. ICM then tries to find a best available agent that has the matching skill within the enterprise, and assigns this agent to this task.
- Handle the new task with an ICM determined best available agent that has the matching skill within the enterprise.

The MediaRouting Configuration box appears as follows:

To put the PIM into service, check the **Enabled** option. This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.

- Enter the peripheral name in the Peripheral name field. In most cases, you'll want to use the enterprise name from the associated Peripheral record.
- Enter the Peripheral ID from the Peripheral record.
- **Application Hostname (1)**. Enter the host name or the IP address of the application server machine (i.e. Collaboration Server or Email Manager). If using the host name, the name must be in the hosts file.
- **Application Connection Port (1)**. Enter the port number on the application server machine that the PIM will use to communicate with the application.



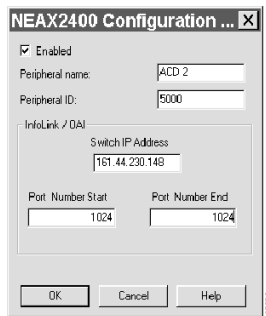
Note

If you are configuring the PIM for the Cisco ICM E-Mail Manager option, use 1600 for the connection port number. For the Cisco ICM Collaboration Server option, use the default of 2000. This also applies for the application connection port (2).

- **Application Hostname (2)**. If two applications will interface with the ICM software, enter the host name or the IP address of the second application server machine (i.e. Collaboration Server or Email Manager). If using the host name, the name must be in the hosts file.
- **Application Connection Port (2)**. Enter the port number on the second application server machine that the PIM will use to communicate with the application.
- **Heartbeat Interval (seconds)**. Specify how often the PG should check its connection to the application server. The default value is usually appropriate.
- **Reconnect Interval (seconds)**. Specify how often the PG should try to re-establish a lost connection to the application server. The default value is usually appropriate.

NEAX2400

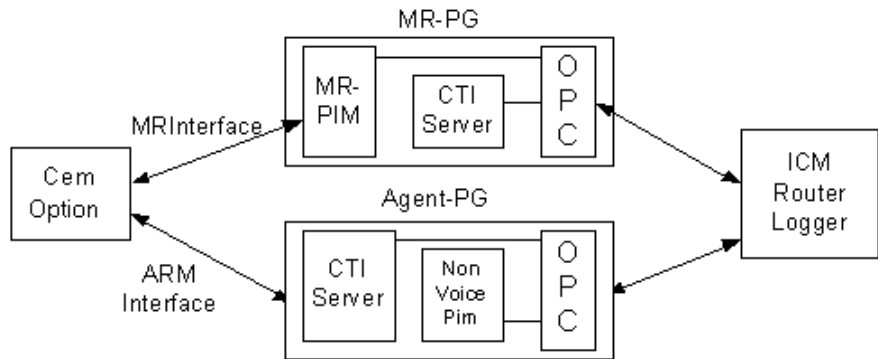
The NEAX2400 dialog box appears as follows:



Configure the IP address of the OAI/Infolink interface of the NEC switch. This can be found by using the AIPT command of the NEC IMXMAT utility. The Port Number Start and Port Number End should be set to the port number of the first port in the 16 port range of ports provided by the NEC switch. This is currently 1024.

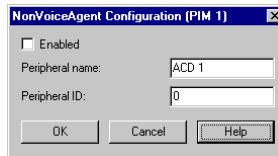
NonVoiceAgent PG

In most cases, the Media Routing PG tracks and records the state and activity of all voice and non-voice agents. However, you can configure a Non-Voice PG rather than a Media Routing PG to monitor state and activity of agents who are non-voice agents. However, this is optional, and not necessary if you already have a Media Routing PG configured for Voice agents.



The MR PG interface provides routing instructions to the CEM application, while the Agent PG configuration is used to report agent state and status to the ICM software.

The NonVoiceAgent Configuration dialog appears as follows:



To put the PIM into service, check the Enabled option. This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.

Enter the peripheral name in the Peripheral name field. In most cases, you'll want to use the enterprise name from the associated Peripheral record.

Enter the Peripheral ID from the Peripheral record. Click the OK button to complete the configuration.

Rolm 9005

The Rolm 9005 dialog box appears as follows:

In the Rolm9005 Revision field, enter the revision number of the ACD.

In the Supervisor Terminal Settings section, enter the login ID and password that the PG should use to connect to the ACD's Supervisor terminal port. Enter the number of the first COM port on the PG through which the PG communicates with the Supervisor terminal interface and the total number of COM ports the PG uses.

In the COM Port Setting section, specify the idle and wait timeout values in milliseconds. Also specify the baud rate and parity for the COM ports.

Siemens Hicom

The Siemens dialog box appears as follows:

In the CallBridge Host Name field, enter the TCP/IP host name for the CallBridge for Workgroups connection on the ACD. In the CallBridge Connection Port, enter the port number for the connection (1040, by default).

Spectrum

The Spectrum dialog box appears as follows:

In the Spectrum Revision field, enter the revision number of the Spectrum ACD. If you use a group number greater than 255, set Two Byte Groups to 1; otherwise, set to 0.

In the Supervisor CRT section, enter the login ID and password that the PG should use to connect to the Spectrum's Supervisor CRT port. Enter the number of the COM port on the PG through which the PG communicates with the Supervisor CRT interface and the baud rate of that port.

In the Transaction Link section, first specify whether to use the X.25 or TCP interface. If you choose X.25, enter the number of the X.25 port on the PG through which the PG communicates with the Spectrum's Transaction Link. If you choose TCP, enter the TCP hostname for the ACD and the port number for the Transaction Link.

Symposium

The Symposium dialog box appears as follows:

Symposium Configuration (PIM 1)

Enabled

Peripheral Name: SCCS Host:

Peripheral ID: Symposium Version: 1.5 3.0

Meridian Link Configuration:

Link Host Name: Server port:

Link Machine: Instance Number:

RTD Link Configuration:

Client Login: Client Password:

HDX Link Configuration:

Client Host Name: Client Instance:

Client Provider:

OK Cancel Help

In the SCCS Host field, enter the IP host name or IP address of the Symposium Call Center Server. If using the IP host name, the name must be in the IP hosts file used by the PG. Use the radio button to set the Symposium version number you are using.

Use the Meridian Link Configuration section to configure the link to the Meridian switch. In the Link Host Name field, enter the TCP hostname specified in the link 1 configuration file on the Meridian Link system. In the Link Machine Name field, enter the Meridian 1 Machine name specified in the link 0 configuration file on the Meridian Link system. The default, Lanlink, is usually appropriate. In the Server port field, enter the well-known port used by the Meridian Link. The default is 3000. In the Instance Number field, enter the instance number on the Meridian 1 for which the PG routes calls. The default is 0.

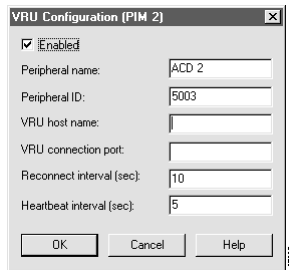
Use the RTD Link Configuration section to configure the Real Time Data link, which is used for agent reporting. In the Client Login field, enter the user name that was assigned for RTD requesters on the SCCS. The default is sysadmin. In the Client Password field, enter the password for the specified user. The default is nortel.

Use the HDX Link Configuration section to configure the Host Data Exchange link, which is used for Symposium call scripting processing. In the Client Host Name field, enter the IP name or IP address for the Symposium PG machine. If using the IP name, the name must be in the IP hosts file used by the PG.

In the Client Provider field, enter the ID by which the HDX server will identify the Symposium PG. The default is 64206. Normally, the default is used. In the Client Instance field, enter the instance string that the Symposium PG sends to the HDX server. The default is Cisco Symposium PIM. Normally, the default is used.

VRU

The VRU dialog box appears as follows:

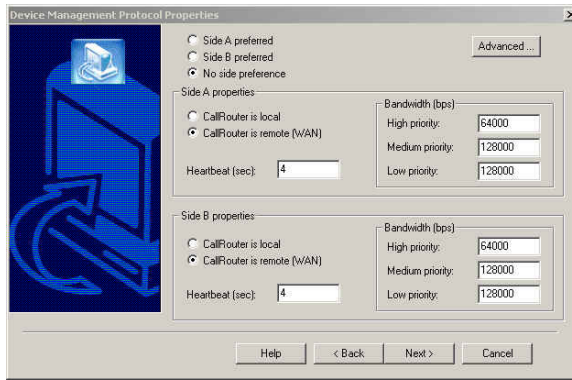


In the VRU Host Name field, enter the name by which the VRU is known to the network. Enter the number of the VRU port that the PG connects to.

In the Reconnect Interval field, specify how often the PG should try to re-establish a lost connection to the VRU. In the Heartbeat Interval field, specify how often the PG should check its connection to the VRU. The defaults for these values are usually appropriate.

Device Management Protocol Properties

When you click **Next** in the Peripheral Gateway Component Configuration window, the Device Management Protocol Properties window appears:

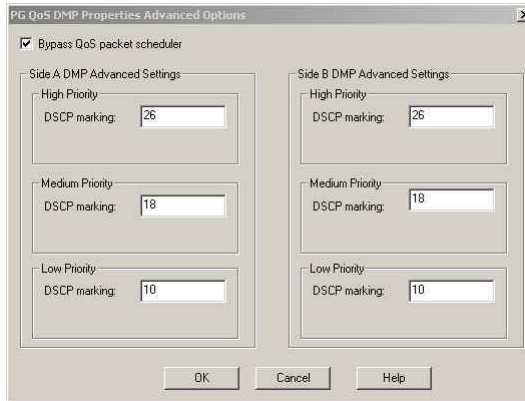


Complete this window, as follows:

-
- Step 1** If you prefer that the PG communicate with one side or the other of the Central Controller (for example, if the PG is collocated with one side), indicate the preferred side. Whether you specify a preferred side or not, if the PG cannot communicate with one side, it will automatically switch to the other.
- Step 2** Indicate whether the PG is local to or remote from each side of the Central Controller. If the PG is remote from either side, specify the maximum amount of bandwidth (in bits per second) the PG can use for communication with the CallRouter. Use this option to prevent the PG from overloading the wide-area network.
- Step 3** If the Call Router is not local, in the Bandwidth fields, input the bandwidth for the WAN link to the Call Router side A and side B. In the case that QoS is not an intended feature, you do not need to worry about how to divide the link bandwidth into each priority. The sum for the three priorities, however, must be the physical bandwidth you actually have, and the input for each priority must be at least 1K (1024) bps.

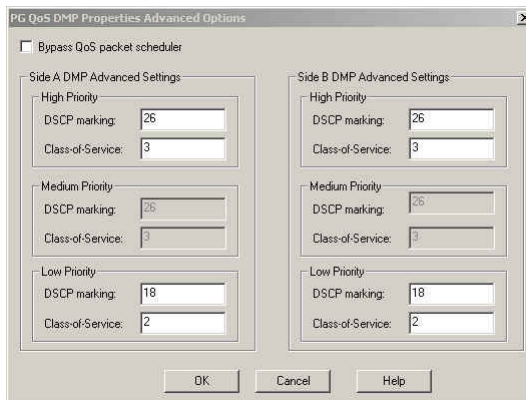
For QoS connections, you need to enter the appropriate bandwidth value for the High, Medium and Low priority individually. Consult with you network administrator or Cisco representative to determine the bandwidth requirements for your network.

To configure the PG QoS settings, click Advanced. The PG QoS DMP Properties Advanced Options window displays.



Set the DSCP (DiffServ Codepoint) marking for each priority of the ICM traffic going to the Call Router. The defaults are acceptable if your network is Cisco AVVID compliant (Architecture for Voice, Video and Integrated Data). Otherwise, you need to consult your network administrator or Cisco representative for the proper values for these fields.

Uncheck the Bypass QoS packet scheduler box if you plan to use the Microsoft Packet Scheduler utility. This changes the appearance of the PG QoS DMP Properties Advanced Options window.



The edit boxes for Medium Priority are grayed out and the Medium Priority always has the same settings as the High Priority. This is because Microsoft Packet Scheduler supports at most two classification levels (except best effort).

In addition to DSCP marking, the Class-of-Service (802.1p) marking is supported. The default values are set in compliance with Cisco AVVID recommendations. Consult your network administrator or Cisco representative for changes.

**Note**

Microsoft Packet Scheduler must be installed separately from the ICM setup if you uncheck the Bypass Packet Scheduler box. For more information about QoS for the ICM software, refer to the *Cisco ICM Enterprise Edition Pre-Installation Planning Guide*.

- Step 4** Click **Next** in the Device Management Protocol Properties window. The Peripheral Gateway Network Configuration window appears.

Field	Value
PG private A:	pg_01
PG private A high:	
PG visible A:	pg_01
PG private B:	pg_02
PG private B high:	
PG visible B:	pg_02
Router visible A:	rtr_01
Router visible A high:	
Router visible B:	rtr_02
Router visible B high:	

Enter the TCP/IP addresses of the PG and, if it is duplexed, its pair. If the PG is simplex, enter **localhost** for the B side addresses. Also enter the visible network addresses for the CallRouter machines.

- Step 5** Click **Next**. The Check Setup Information window appears. Ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button. When the settings are correct, click **Next** to begin copying files.

The copying process may take several minutes to complete. You can continue with other work while Setup operates in the background.

If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager now. It is not recommended that you start the Node Manager until you have completed the entire ICM installation.

Step 6 Click **Finish** to exit Setup and optionally start the Node Manager.

If you choose to start it, the Node Manager automatically starts the other ICM processes on the PG.

After installing the PG software for an Aspect ACD, you might also have to install the Application Bridge Server.

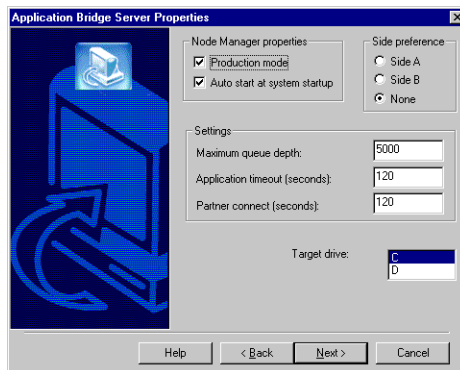
Application Bridge Server

For an Aspect ACD, the ICM Peripheral Gateway connects to the Aspect Application Bridge. If another application also requires a connection to the Application Bridge, then you must install the Application Bridge Server (ABS). Install the ABS after you have installed the PG software.

If the PG is duplexed, the ABS can be either simplexed (run on only one of the PG machines) or duplexed (run on each PG machine). Running ABS duplexed allows applications to continue to receive data if one PG node fails.

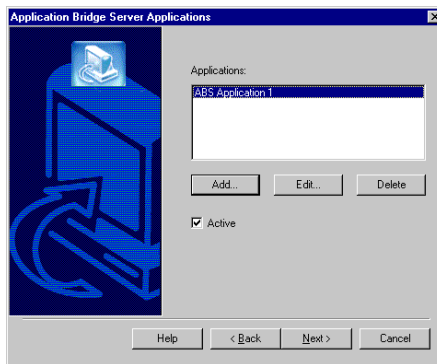
Application Bridge Server Properties

To install the ABS, run SETUP.EXE again from the ICM CD-ROM and choose **Application Bridge Server** as the component to install. The Application Bridge Server Properties screen appears.



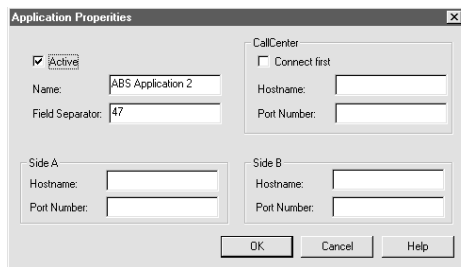
Complete this window, as follows:

- Step 1** In the Node Manager Properties section, choose **Production Mode** and **Auto Start at System Startup** unless you are specifically told otherwise by your Cisco Support representative. If you are installing duplexed ABS and you prefer that one side run rather than the other, specify the preferred side.
- Step 2** In the Settings section, specify the maximum number of unsent messages you want the ABS to queue for each application and the maximum amount of time you want the ABS to wait for an application to accept a connection. If the ABS is duplexed, specify the maximum amount of time you want the ABS to wait for its duplexed peer to establish a connection.
- Step 3** Click **Next**. The Application Bridge Server Applications window appears.



This screen lets you activate, deactivate, add, edit, or remove ABS applications.

- Step 4** When you click the **Add** or **Edit** button in the Application Bridge Server Applications window, the Application Properties dialog box appears.



- Step 5** Enter or modify information about each application. The field separator may be 47 for a slash (/) or 124 for a vertical line (|). Specify whether the ABS should connect to the CallCenter ACD before connecting to the application. Specify the address of the ACD and the port number that connects to the ACD for the application on the PG.
- Step 6** In the Side A section, enter the application's address and the PG port number that connects to it. If the application is duplexed, enter information in the Side B section also.
- Step 7** After you have set up the applications, click the **Next** button in the Application Bridge Server Applications window to copy files and complete the ABS installation.

CompuCALL Server Gateway

For a DMS-100 ACD, the ICM Peripheral Gateway connects to the DMS-100 CompuCALL interface. If another application also requires a connection to the DMS-100, then you must install the CompuCALL Server (CCS) so that the PG and application can share a session on the DMS-100. Install the CCS after you have installed the PG software.

If the PG is duplexed, the CCS can be either simplexed (run on only one of the PG machines) or duplexed (run on each PG machine). Running CCS duplexed allows applications to continue to receive data if one PG node fails.

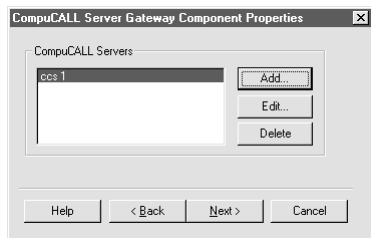
CompuCALL Server Gateway Properties

To install the CCS, run SETUP.EXE again from the ICM CD-ROM and choose **CompuCALL Server Gateway** as the component to install. The CompuCALL Server Gateway Properties screen appears.

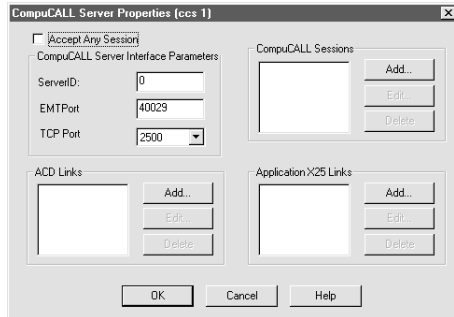


Complete the window, as follows:

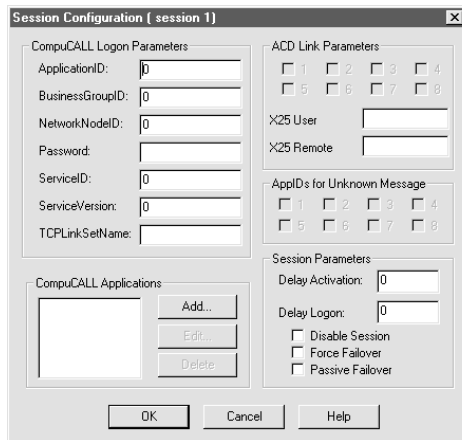
-
- Step 1** In the Node Manager Properties section, choose **Production Mode** and **Auto Start at System Startup** unless you are specifically told otherwise by your Cisco Support representative. If you are installing duplexed CCS, choose duplexed here.
- Step 2** In the CCS node properties section, enter the CCS Gateway ID and the ICM system ID number for the CCS Node. If the CCS is duplexed, and you have a preference that one side runs rather than the other, specify the preferred side.
- Step 3** Click **Next**. The CompuCALL Server Component Properties window appears. The screen allows you to Add, Edit or Delete a CompuCALL Server configuration.



- Step 4** When you click **Add** or **Edit**, the CompuCALL Server Properties dialog displays.



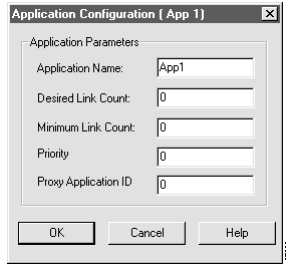
- Step 5** If you want the server to accept any session, check the **Accept Any Session** box. The following sections describe the other options in this window.
- Step 6** In the CompuCALL Server Interface Parameters section, enter the parameters required to configure the connection to the CompuCALL Server. It is not necessary to enter the ServerID. In the EMTPort field, enter the port number that the DMS PIM uses to communicate with the CCS (40429 is default). In the TCP Port field, enter the port number that the third-party application and the DMS PIM will use to communicate with the CCS (2500 is the default).
- Step 7** In the CompuCALL Sessions section, you can Add, Edit or Delete a CompuCALL session. When you click the **Add** or **Edit** button, the following dialog displays.



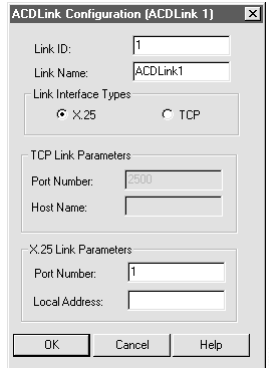
- Step 8** In the CompuCALL Login Properties section, enter the following information:

- The ApplicationID is an integer that identifies the ICM as the application that is initiating the logon request.
- The BusinessGroupID is an integer that identifies your company. Your Interexchange Carrier defines this ID.
- The NetworkNodeID is an integer identifier that specifies the switch that the ICM will use to communicate. This is the switch the host computer connects to via the CompuCALL link. Your Interexchange Carrier defines this ID.
- The password corresponds to the BusinessGroupID.
- The ServiceID is an integer that identifies the application context to be set for the session (i.e., a service profile containing Application Service Options or subsets, as defined by your Interexchange Carrier).
- ServiceVersion is an integer that specifies the application level or the signaling version that the host application is using (i.e., 35 for BCS35).
- The TCPSetLinkName is “TCPLinkSetName” specifies the linkset parameter for TCP connections.

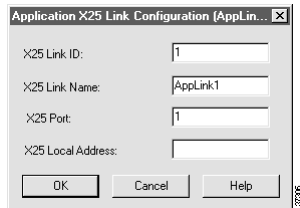
- Step 9** In the ACD Link Parameters section, select links that will be used by the session. Use the link numbers that are assigned with the ACDLink Configuration dialog. Enter the X.25 SVC call parameter configured on the DMS-100 in the X25 User field. Enter the X.25 SVC call parameter destination DTE address configured on the DMS-100 in the X25 Remote field.
- Step 10** In the AppIDs for Unknown Messages section, select the applications that will receive unknown messages. Unknown messages are those that may be introduced in future versions of the CompuCALL interface. The AppID corresponds to the ID listed in the CompuCALL Applications section of this window.
- Step 11** In the Session Parameters section, the Delay Logon and Delay Activation are not used. Select Disable Session if no lower priority applications are allowed to logon, or allowed to remain logged on, unless the highest priority configured application is logged on. Force Failover and Passive Failover are not used.
- Step 12** In the CompuCALL Applications section, you can choose to Add, Edit or Delete an application. When you click on **Add** or **Edit**, the following dialog displays.



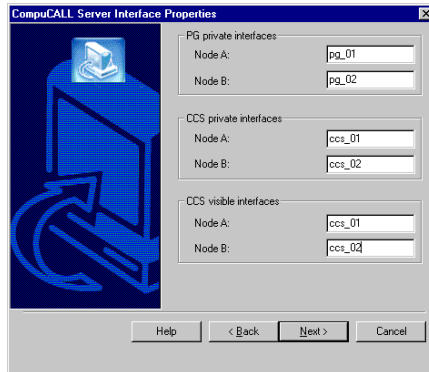
- Step 13** Use the Application Configuration dialog to configure the DMS-100 peripheral interface manager and the third party applications that will run for the session.
- Enter the Application Name. In the Desired Link Count field, enter the desired number of active links, which is the desired number for the active application with the highest priority. If you have a duplexed configuration, in the Minimum Link Count field, enter the minimum number of links allowed before a failover occurs. In the Priority field, assign a priority number for the application (lower number indicates higher priority). In the ProxyApplication ID field, enter the Application ID of the third-party application and the DMS-100 PIM (this is the same as the ServerID in the CompuCALL application logon message).
- Step 14** Click **OK** when you have finished to return to the Session Configuration screen.
- Step 15** When you are finished entering information on the Session Configuration screen, click **OK** to return to the CompuCALL Server Properties dialog.
- Step 16** In the ACD Links section of the CompuCALL Server Properties dialog, you can Add, Edit or Delete an ACD link. When you click the **Add** or **Edit** button, the following dialog displays.



- Step 17** Use the ACDLink Configuration dialog to configure the link between the CCS and the DMS-100 ACD. You can choose either a X.25 link or a TCP link. For either link, enter the port number. For a X.25 link the Local Address is not used. For a TCP link the Host Name is the DMS-100 ACD TCP well-known port number.
- Step 18** In the X25 Application Link section, you can Add, Edit or Delete an X.25 application link. When you click the **Add** or **Edit** button, the following dialog displays.



- Step 19** Use the Application X.25 Link Configuration dialog to configure the link between a third-party application and the CCS.
- Enter Link ID, which corresponds to the labels used in the Application Configuration dialog. In the Name field, enter a name for the link. Enter the X.25 Port number in the X25 Port field and the X.25 DTE address assigned to the link in the Local Address field. Click OK to return to the CompuCALL Server Properties dialog.
- Step 20** When you click the **Next** button from the CompuCALL Server Properties window, the CompuCALL Server Interface Properties window displays.



Use this window to enter the node names for the PG private interface, CCS private interface and the CCS visible interface. If you have a duplexed configuration, enter the names for both Node A and Node B.

- Step 21** Click **Next** to proceed to the Check Interface Setup screen. Review the settings to ensure they are correct. If the settings are not correct, use **Back** to go back and modify the configuration. If the settings are correct, click **Next** to begin copying the files and complete the installation.



CTI Server Setup

The CTI Server is an optional component that allows an external CTI application to communicate with a Peripheral Gateway. The CTI Server is part of the Cisco *Enterprise CTI* product.



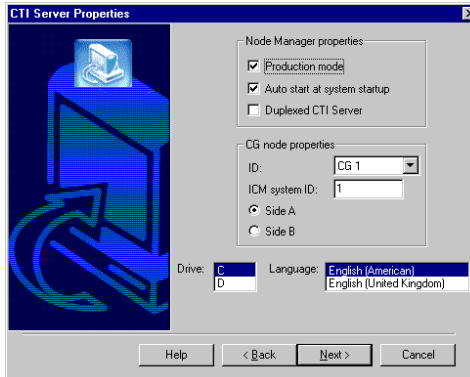
Note

Cisco supports installation of CTI Server on the same machine where the Peripheral Gateway software is installed. Installing CTI Server on a machine separate from the PG may cause network problems including, but not limit to, network disconnects, agents missing calls, and Agents forced into Not_Ready.

Installing the CTI Server

To install the CTI Server software, run SETUP.EXE from the ICM CD-ROM. Add the customer if you have not already done so. Install the CTI Server as follows:

-
- Step 1** Click **Add** in the Customer Components section and choose CTI Server. The CTI Server Properties window appears.



Step 2 Choose **Production Mode** and **Auto Start at System Startup** unless you are specifically told otherwise by your Cisco Support representative. This ensures that the CTI Server can restart itself automatically if necessary.

It is recommended that you set the Auto Start feature after installation is complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before hotfixes and/or databases are applied.

Step 3 Check the **Duplexed CTI Server** option if you are configuring redundant CTI Server machines.

For the CG node properties, the CG node ID must match the PG node ID (i.e CG1 and PG 1).

If the CTI Server will be duplexed, specify which side you are installing: Side A or Side B. If the CTI Server will be simplexed, choose Side A.

Step 4 Choose the local disk on which you want to install the software.

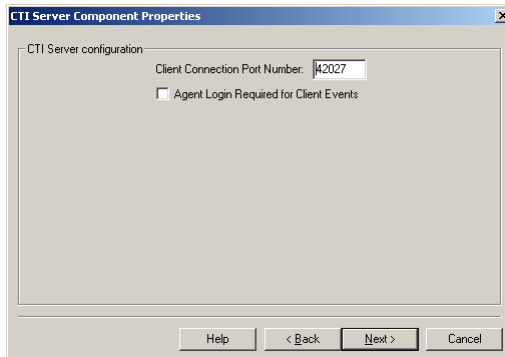


Note Be sure to note the drive you are using for future reference, since this information is required when applying hotfixes.

Step 5 Choose the language.

CTI Server Component Properties

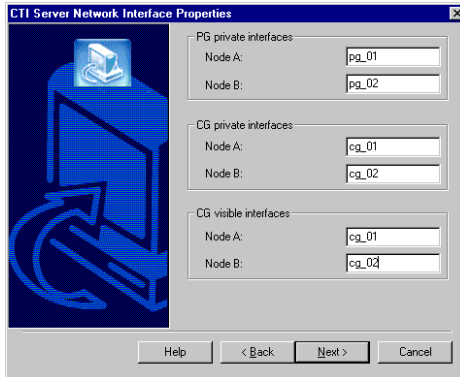
- Step 6** Click **Next**. Setup loads any current installation settings and then displays the CTI Server Component Properties window.



- Step 7** Setup automatically generates a client connection port number. You can use this value or change to a standard port number. Clients use this port number to connect to the CTI Server.

If you have multiple nodes running on a single machine, each must use a different port number.

- Step 8** Optionally, you can require that an agent be logged in to the client before the client receives events from the CTI Server. This prevents clients from accessing data for other agents.
- Step 9** Click **Next**. The CTI Server Network Interface Properties window appears.



- Step 10** Enter the private network addresses for the PG associated with the CTI Server. Enter the private network and visible network addresses of the CTI Server.
- Step 11** Click **Next**. The Check Setup Information window appears.

Ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button. When the settings are correct, click the **Next** button to begin copying files.

The copying process may take several minutes to complete. You can continue with other work while Setup operates in the background.

If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager now.

- Step 12** Click **Finish** to exit Setup and optionally start the Node Manager. It is not recommended that you start the Node Manager until you have completed the entire ICM installation.

If you choose to start it, the Node Manager automatically starts the other ICM processes on the CTI Server.



After the Installation

This chapter describes what you should do after you have completed the ICM software installation. Information is provided on what the ICM Setup program installs, including directories and their contents, Program Manager icons, and Windows services. This chapter covers the following specific tasks:

- Managing the programs in the Cisco Admin Workstation application group.
- Registering new users and assigning user types on the Admin Workstation.
- Enabling and disabling Windows services.
- Viewing the configuration data that is stored in the Windows configuration registry and the AW.INI file.

This chapter also includes information on the domain and local accounts that are created when you install ICM software.

Files and Directories

ICM Setup installs most of the ICM files under a directory named ICM. If you install the Admin Workstation software, ICM Setup also creates or updates several other files.

The ICM Directory Structure

The ICM Setup procedure creates a directory named ICM in the root directory of the drive you choose. The ICM directory contains a subdirectory for the customer you created in Setup.

The customer directory contains a subdirectory for each component you installed. [Table 8-1](#) lists the directory names for each component.

Table 8-1 Component Installation Directories

Component	Directory Name
Application Bridge Server	ABS
Admin Workstation	AW
Blended Agent Dialer	BADialer
CTI Server	CG1A (for CG 1, side A), CG1B (for CG 1, side B), CG2A (for CG 2, side A), etc.
Distributor	DIS
Logger	LA (for side A) or LB (for side B)
Peripheral Gateway	PG1A (for PG 1, side A), PG1B (for PG 1, side B), PG2A (for PG 2, side A), etc.
Router	RA (for side A) or RB (for side B)

For example, if you install the router software for side A, a directory named RA is created in the customer directory under ICM directory.

[Table 8-2](#) describes the contents of each subdirectory under the component directories. Note that not all subdirectories apply to all components.

Table 8-2 Installation Subdirectories

Directory	Components	Contents
ataman	all	Third-party telnet server software. Do not modify these files.
bin	all	ICM executable files. Do not modify these files.
custom	Admin Workstation	Monitoring templates and reports. You can add your own templates and reports.
export	Admin Workstation, Logger, Distributor	Initially empty. Files written to the export directory on the Logger are automatically copied to Customer Support.
filters	Logger	Files that determine which events are automatically reported to Cisco. Do not modify these files.
hist	Peripheral Gateway	Used by the PG as temporary storage for historical data.
install	Admin Workstation, Logger, Distributor	Files that are used by ICM Setup during initial installation or subsequent setup changes.
logfiles	all	Initially empty. ICM processes may write log files to this directory.

When you install the ICM Admin Workstation software, you can optionally choose to install the InfoMaker for ICM. This requires that you have previously installed Powersoft's InfoMaker 8.0. The ICM Setup program upgrades specific files within the directory where InfoMaker is installed (for example, InfoMaker might be installed in C:\Program Files\Powersoft\InfoMaker 8.0). You can use the InfoMaker for ICM to create your own report templates for use in Monitor ICM.

**Note**

If you install InfoMaker after you install the Admin Workstation software, the InfoMaker for ICM is still not available. You must reinstall the Admin Workstation software from the CD to enable the InfoMaker for ICM.

Other Admin Workstation Files

In addition to the files and subdirectories under the ICM directory, the ICM installs a few additional files in the main Windows and System directory (as indicated by the variables %WINDIR% and %SYSDIR%) on each Admin Workstation.

The value of %WINDIR% is the main Windows directory, for example C:\WINNT. The value of %SYSDIR% is the directory that contains Windows system files, for example C:\WINNT\SYSTEM32. Setup may install or upgrade various runtime files in %SYSDIR%.

Configuration Registry

The ICM software stores its environment information in the configuration registry. The configuration registry is a database repository for information about the computer's configuration. You might want to view this information to help diagnose configuration problems. To view the registry, run the Registry Editor (REGEDIT.EXE or REGEDT32.EXE).



Caution

Do not change data directly within the registry. Changes made here can cause unexpected behavior and might be overwritten during a subsequent reboot or setup. Instead, run ICM Setup and make the appropriate changes.

Within the HKEY_LOCAL_MACHINE tree, Cisco information is stored under SOFTWARE\Cisco Systems, Inc.\ICM. Within the ICM subtree is a subtree for the customer you created in Setup. Within the customer subtree is a key with the ICM node names installed for the customer on this machine (for example, AW, LA, PG2B, RB). Under that are keys for specific parts of the ICM system. For example, under RealTimeClient on an Admin Workstation you can find information about the real-time distributors, and the names and logon information for the central and local databases.

The Script Editor and several other ICM tools store information within the HKEY_LOCAL_USER tree. This information is stored in subtrees under SOFTWARE\Cisco Systems, Inc.

Services

As part of the installation process, the ICM installation software automatically sets up two services on the machine:

- **Ataman Telnetd Server.** Third-party software that allows for telnet access to the machine through Internet TCP. For multi-customer and multi-component machines, only one copy of the Telnetd Server is installed.
- **Cisco ICM Node Manager.** Cisco software that manages the other Cisco processes on the machine. Each component for each customer has its own Node Manager.

The Node Manager is installed on every ICM system node. The Telnet Server is installed on Admin Workstations, Distributors, Loggers, and Peripheral Gateways. The installation software allows you to set up the Node Manager to start automatically or manually. To see all the services installed on a machine, run the ICM Service Control tool and choose the **All** checkbox.

You can also view and control services through the Services applet in the Control Panel.

The Node Manager starts either automatically or manually depending on the setting you chose for Auto Start in ICM Setup.

Normally, you need not make any changes to these services. However, if you need to remove the Telnetd Server service from your machine, execute the following command from the ataman directory under ICM root directory:

```
telnetd stop remove
```

To set up the service again, execute the following command from that same directory:

```
telnetd install start
```

To remove the Node Manager service, execute the following from the bin directory under the ICM root directory:

```
rnmn customer component
```

For example to remove the node manager for pg1b for the customer cust1:

```
rnmn cust1 pg1b
```

To set up the Node Manager service again, run the local version of ICM Setup.

Cisco Admin Workstation Program Group

When you install the ICM Admin Workstation software on a computer, the Cisco Admin Workstation program group is created in the Windows Program Manager. This group contains icons for the programs to be run by Admin Workstation users.

To view information about an item in the group, click on the item and choose **Properties** from the Program Manager's File menu. [Table 8-3](#) lists the properties for each item in the Cisco Admin Workstation group.

The ICM Setup program lets you modify the configuration of the Admin Workstation.

Table 8-3 Program Item Descriptions

Program	Command Line	Working Directory
AW Select	awselect.exe	\ICM\bin
Call Tracer	scripted.exe/calltracer	\ICM\bin
Check Routes	rtcheck.exe	\ICM\bin
CMS Control	cmscontrol.exe	\ICM\bin
Configuration Manager	Launcher.exe	\ICM\bin
Glossary	icmgloss.hlp	\ICM\bin
Initialize Local Database	AWInit.exe	\ICM\bin
Lock Admin	lockadmin.exe	\ICM\bin
Router Log Viewer	rtrlog.exe	\ICM\bin
Scheduled Target Manager	schtargetman.exe	\ICM\bin
Schema Help	schema.hlp	\ICM\bin
Script Editor	scripted.exe	\ICM\bin
Service Control	servicecontrol.exe	\ICM\bin
Setup	setup.exe	\ICM\bin

Registering Users

Before someone can use an Admin Workstation, you must register that person as a user within the Windows domain. The ICM supports two types of users:

- **Administrative users** have the ability to add new ICM users. Administrative users are assigned to the SQLAdmin group.
- **Non-administrative users** cannot add new ICM users. Non-administrative users are assigned to the SQL User group. The group name has the form *custSQLUser* where *cust* is the customer name you defined in Setup.

**Note**

Administration and management of ACDs, PBXs, VRUs, and networking hardware and software fall outside the scope of these groups.

Domain administrators are automatically mapped to the sa administrative user. If necessary, you can create other administrative users by running User Manager for Domains and adding users to the SQLAdmin group. User Manager for Domains is a standard part of Windows.

**Note**

A user on a Client Admin Workstation must be a member of either the SQLAdmin group for the domain, or the customer-specific SQLUser group (for example, cus01SQLUser).

To add non-administrative users, run Configure ICM. Choose **Users** from the Security menu. The ICM Users dialog box appears.

This dialog box lists ICM users. To add a new user, click the **Add** button. The Add User dialog box displays.

**Note**

The user group options are available only if you have purchased the optional Cisco *Partition* feature.

Enter the user name, description (usually the full name of the user), and password. Enter the password again in the Confirm Password field to ensure that you type it correctly.

The following options determine the level of access the user has to the system:

- **Able to create other Windows users.** Check this box to allow the user to add other ICM users through Configure ICM. When you choose this option, the Read Only option becomes disabled.
- **Read Only.** Check this box to limit the user to read-only access to the ICM. A read-only user cannot make changes to configuration data or scripts.
- **WebView and Internet Script Editor only.** Check this box to allow the user permission to use only WebView and the Internet Script Editor.

To view information about all registered users, run User Manager for Domains. For specific information about this tool, see your Windows documentation.

User Accounts Created by ICM Setup

When installed, ICM software adds both local and domain user accounts. It also creates global groups and SQL accounts. These groups allow software to manage their roles and rights, a critical element to maintaining the lowest possible security profile. These user accounts are usually created by setup. In some cases they are installed by ICMDBA.

The tables below captures all instances where ICM accounts are created and made members of various user groups. The ICM setup creates both domain and local accounts. For example, the domain account <instance>SQLUser is created as a Global Group and is made a member of <domain>\DbagtWrite and <domain>\LocalSQLUser groups. It is also made a member of LocalSQLUser in both the logger and distributor.

In the tables below, local groups are identified by the system on which they are created as <logger>, <distributor>, or <router>.

Table 8-4 Domain Accounts

Account Name	Type	Member	Member of	Installed by
<instance>SQLUser	Global Group	Added by User List	<domain>\Administrator <domain>\DbagtWrite <logger>\LocalSQLUser <distributor>\LocalSQLUser <distributor>\Power Users <distributor>\Users	Logger Router Distributor

Table 8-4 Domain Accounts

Account Name	Type	Member	Member of	Installed by
<instance>WVScript	Global Group	Added by User List	<distributor>\LocalWVScript	Distributor
NTDomainOperators	Global Group	Added by User List	<domain>\Account Operators	Distributor
SQLAdmin	Global Group	<domain>\jag <distributor>	<domain>\DbagtWrite <logger>\LocalSQLAdmin <distributor>\Users <distributor>\LocalSQLAdmin <router>\DbagtWrite	Logger Router Distributor
SQLAWAdmin	Global Group	<domain>\<instance> <distributor>	<domain>\DbagtWrite <logger>\LocalSQLAdmin <distributor>\LocalSQLAdmin <router>\DbagtWrite	Logger Router Distributor
DbagtWrite	Global Group	<domain>\ <instance> SQLUser <domain> \SQLAdmin <domain> \SQLAWAdmin	None	Router
ICRPerfmon	Global Group	None	<router>\LocalICRPerfmon	Router Distributor
jag<distributor>	Domain User	N/A	<domain>\SQLAdmin <distributor>\Administrators	Distributor
Account Operators	Local Group	<domain> \NTDomainOperators	None	Operating System

■ Registering Users

Table 8-4 Domain Accounts

Account Name	Type	Member	Member of	Installed by
<instance>SQLUser	Global Group	Added by User List	<domain>\Administrator <domain>\DbagtWrite <logger>\LocalSQLUser <distributor>\LocalSQLUser <distributor>\Power Users <distributor>\Users	Logger Router Distributor
<instance> <distributor> This account is used as the service logon account for the ICM Logger service.	Domain User	N/A	<domain>\SQLAWAdmin <distributor>\Administrators	Distributor
<instance><side> <logger> This account is used as the service logon account for the ICM Logger service.	Domain User	N/A	<domain>\SQLAdmin <logger>\Administrators	Logger

The following table describes the Windows 2000 accounts created on the Logger.

Table 8-5 Operating System Accounts created on the Logger

Account Name	Type	Member	Member of	Installed by
LocalSQLAdmin	Local Group	<domain>\SQLAdmin <domain>\SQLAWAdmin	Logger SQL Login	Logger
LocalSQLUser	Local Group	<domain>\<instance>SQLUser	Logger SQL Login	Logger

Table 8-5 *Operating System Accounts created on the Logger*

Account Name	Type	Member	Member of	Installed by
Administrators	Local Group	<domain>\<instance><logger>	None	Logger assigns members to OS account

The following table describes the SQL Server accounts created on the Logger.

Table 8-6 *SQL Server Accounts created on the Logger*

Account Name	Type	Member	Member of	Installed by
<logger>\LocalSQL Admin	SQL Login	None	Sysadmin Server Role	Logger setup
<logger>\LocalSQL User	SQL Login	None	None	Logger setup
GeotelGroup	SQL AW DB Role	Added by User List	None	ICMDBA
GeoTelAdmin	SQL AW DB Role	None	None	ICMDBA
Sysadmin	SQL Server Role	<distributor>\LocalSQLAdmin	None	SQL Server

■ Registering Users

The following table describes Windows 2000 accounts created on the Distributor and Client Admin Workstation.

Table 8-7 *Operating System Accounts created on the Distributor and Admin Workstation*

Account Name	Type	Member	Member of	Installed by
Users	Local Group	<domain>\<instance>SQLUser <domain>\SQLAdmin	None	Distributor assigns members to OS account
Power Users	Local Group	<domain>\<instance>SQLUser	None	Distributor assigns members to OS account
Administrators	Local Group	<domain>\<instance><distribu tor> <domain>\jag<distributor>	None	Distributor assigns members to OS account
LocalSQLAdmin	Local Group	<domain>\SQLAdmin <domain>\SQLAWAdmin	Distributor SQL Login	Distributor
LocalSQLUser	Local Group	<domain>\<instance>SQLUser	Distributor SQL Login	Distributor
LocalWVScript	Local Group	<domain>\<instance>WVScrip t	None	Distributor

The following table describes SQL Server accounts created on the Distributor and Client Admin Workstation.

Table 8-8 *SQL Server Accounts Created by the Distributor and Client Admin Workstation*

Account Name	Type	Member	Member of	Installed by
<distributor> \LocalSQLAdmin	SQL Login	None	Sysadmin Server Role	Distributor

Table 8-8 SQL Server Accounts Created by the Distributor and Client Admin Workstation

Account Name	Type	Member	Member of	Installed by
<distributor>\LocalSQLUser	SQL Login	None	None	Distributor
GeotelGroup	SQLAW DB Role	Added by User List	None	Distributor
GeoTelAdmin	SQLAW DB Role	None	None	Distributor
Sysadmin	SQL Server Role	<distributor>\LocalSQLAdmin	None	SQL Server

The following table provides information about Operating System Assigned Permission Changes for the Distributor and Client Admin Workstation.

Table 8-9 Distributor and Client AW Permission Changes

Account Name	Change
Users	Access to the following registry keys: <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM • HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>

The following table describes operating system accounts created on the router.

Table 8-10 *Operating System Accounts created on the Router*

Account Name	Type	Member	Member of	Installed by
DbagtWrite	Local Group	<domain>\<instance>SQLUser <domain>\SQLAdmin <domain>\SQLAWAdmin	None	Router
LocalICRPerfmon	Local Group	<domain>\ICRPerfmon	None	Router
<instance>DbagtRead	Local Group	None	None	Router

The following table provides information about Operating System Assigned Permission Changes for the router

Table 8-11 *Router Permission Changes*

Account Name	Change
LocalICRPerfmon	Access to the following registry keys: <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM • HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance> • HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services • HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Cisco ICM Router
DbagtWrite	Access to the following NTFS file or directory objects <ul style="list-style-type: none"> • <icm install drive>:\icm\<instance>\ra • <icm install drive>:\icm\<instance>\ra\dbagt.acl
<instance>DbagtRead	Access to the following NTFS file or directory objects <ul style="list-style-type: none"> • <icm install drive>:\icm\<instance>\ra • <icm install drive>:\icm\<instance>\ra\dbagt.acl

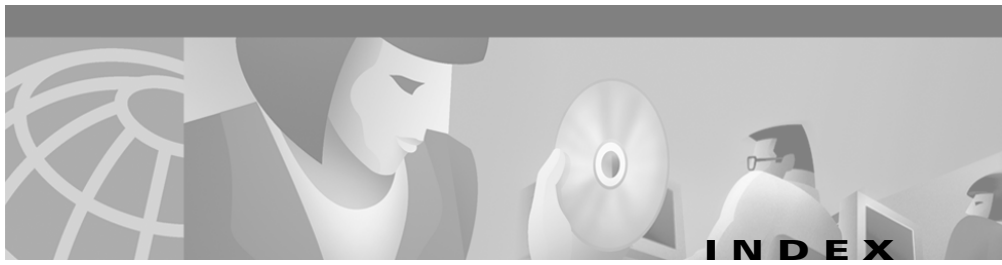
Moving Forward

After installing ICM software, you can move on to the following tasks:

- Setting up your configuration in the ICM database. See the *Cisco ICM Enterprise Edition Configuration Guide*.
- Creating routing scripts to specify how calls are routed. See the *Cisco ICM Enterprise Edition Script Editor Guide*.
- Monitoring call center performance. See the *Cisco ICM Enterprise Edition WebView* product documentation.
- Designing an administration strategy for the ICM. See the *Cisco ICM Enterprise Edition Administrator Guide*.

The CTI OS is an optional component that allows an external CTI application to communicate with a Peripheral Gateway.

You can install the CTI OS on the same machine as the Peripheral Gateway software or on a separate machine.



A

Access levels [8-7](#)

Addresses

 CallRouter [3-7](#)

 Logger [2-5](#)

 Peripheral Gateway [6-31](#)

Adjunct Switch Application Interface [6-11](#)

Admin site

 real-time distributors [4-9](#)

Admin Workstation

 installing [4-1](#)

 real-time distributors [4-9](#)

Application Bridge [6-10](#)

Application Bridge Server [6-32, 6-34](#)

Application Gateway

 custom [3-2](#)

Application Host Name [6-17](#)

Applications

 external [3-2](#)

AppLink [3-2](#)

ASAI links [6-11](#)

Aspect CallCenter [6-9](#)

Aspect PIM [6-9](#)

AT&T G3 [6-11](#)

AT&T NIC [3-5](#)

Ataman directory [8-3](#)

Ataman Telnetd Server [8-5](#)

Auto Start

 CallRouter [3-2](#)

 CTI Gateway [7-2](#)

 Peripheral Gateway [6-2](#)

Avaya Definity ECS (AT&T PIM) [6-11](#)

AW Select [8-6](#)

B

Bin directory [8-3](#)

Bridges

 Application [6-10](#)

BRI ports [6-11](#)

C

CallBridge [6-25](#)

CallCenter ACD [6-9](#)

CallRouter

 failures [3-2](#)

 installing [3-1](#)

 private network addresses [3-7](#)

- with no PGs [3-5](#)
- Call Tracer [8-6](#)
- CallVisor [6-11](#)
- CD-ROM [1-12](#)
- Central Controller [1-3](#)
- Check Routes [8-6](#)
- Client connection port [7-3](#)
- CMS [6-11](#)
- Component selection [1-13](#)
- Configuration registry [8-4](#)
- Configure ICR [8-6](#)
 - adding devices [5-1](#)
 - adding users [8-7](#)
- Configure NIC [5-2](#)
- Configure PG [5-2](#)
- Controller ID
 - Peripheral Gateway [6-4](#)
- Control Panel [8-5](#)
- CTI Call Wrapup Data Delay [6-5](#)
- CTI Gateway
 - client port number [7-3](#)
 - installing [7-1, 8-15](#)
- CTI Gateway Properties [7-1](#)
- Custom directory [8-3](#)
- customer [1-5](#)
- Customer ID [3-3](#)
- Customers
 - names [1-12](#)
 - numbers [1-12](#)

- customer types [1-6](#)
- Custom Screen Builder [4-9, 8-3](#)

D

- Database
 - central [2-6](#)
 - external [3-2](#)
 - on Admin Workstation [4-8](#)
 - requirements [1-8](#)
 - routing [3-2](#)
 - sizing [2-6](#)
- DbLink [3-2](#)
- Demand Command Client [4-9](#)
- Demand Command Server [6-5](#)
- Device Management Protocol [3-4](#)
- Devices
 - configuring [5-1](#)
- Directories [8-1](#)
- Disconnect warnings [3-5](#)
- Disk space [1-13](#)
- DMP [5-3](#)
 - CallRouter configuration [3-4](#)
 - Peripheral Gateway configuration [6-6, 6-28](#)
- DMS-100 ACD PIM [6-13](#)
- DNIS matching
 - for Meridian ACDs [6-20](#)
- Documentation [8-6](#)
- Duplexed

CallRouter [3-2, 3-5](#)
 CTI Gateway [7-2](#)
 Logger [2-2](#)
 Peripheral Gateway [6-2](#)
 Duplexed components [1-3](#)

E

EAS [6-5](#)
 Ethernet [1-5](#)
 Event Link [6-6](#)
 Expert Agent Selection [6-5](#)
 Export directory [8-3](#)

F

Failures
 CallRouter [3-2](#)
 Logger [2-2](#)
 Fault tolerance [1-3](#)
 Files installed [8-1](#)
 Filters directory [8-3](#)
 FPDFL [6-17](#)

G

G2 ACD PIM [6-16](#)
 G3 [6-11](#)
 Galaxy ACD [6-17](#)

Demand Command Client [4-9](#)
 pass-through data [6-18](#)
 RMC reports [4-9](#)
 VarCTI [6-18](#)
 Galaxy PIM [6-17](#)
 Glossary help file [8-6](#)

H

High Speed Link [6-20, 6-21](#)
 Hist directory [8-3](#)
 Historical data
 purging [2-5](#)
 Historical Data Server [2-2](#)
 HKEY_LOCAL_MACHINE [8-4](#)
 HKEY_LOCAL_USER [8-4](#)
 HSL [6-20, 6-21](#)

I

ICR Node Manager [8-5](#)
 ICR Setup [1-12, 1-14, 8-5, 8-6](#)
 Importing schedules [4-10](#)
 InfoMaker [4-9, 8-3](#)
 Install directory [8-3](#)
 instance [1-5](#)

L

Language

- Admin Workstation [4-4](#)
- CallRouter [3-3](#)
- CTI Gateway [7-2](#)
- Peripheral Gateway [6-4](#)

Logfiles directory [8-3](#)

Logger

- failures [2-2](#)
- installing [2-1](#)
- private network addresses [2-5](#)
- reboot [2-2, 2-3](#)

Logical Interface Controller

- Peripheral Gateway [6-4](#)

Low indicator [1-13](#)**M**Manage Configuration Lock [8-6](#)MAX [6-20, 6-21](#)MCI NIC [3-3](#)

MDS

- Peripheral Gateway [6-6](#)

MEI [6-20](#)Meridian ACD [6-19](#)

- Enhanced CTI interface [6-19, 6-20](#)
- High Speed Link [6-20](#)
- Meridian Link [6-20](#)

Post-Routing [6-20](#)Meridian Event Interface [6-20](#)Meridian Link [6-20, 6-21](#)Meridian PIM [6-19](#)Multi-customer systems [1-14](#)Multiple components [1-14](#)**N**

Naming conventions

- directories [8-2](#)
- NICs [1-9](#)
- nodes [1-8](#)

Network Interface Controller

- AT&T [3-5](#)
- France Telecom [5-13](#)
- MCI [3-3, 5-3](#)
- naming [1-9](#)
- Nortel [5-5, 5-6, 5-7](#)
- Sprint [3-3, 5-4](#)
- Stentor [5-5](#)

Network Interface Properties

- CallRouter [3-6](#)

Networks

- private [2-5, 3-7, 6-31](#)
- visible [6-31](#)

NIC [3-3](#)Node Manager [8-5](#)

- Admin Workstation [4-4](#)

- CallRouter [3-2](#)
- CTI Gateway [7-2](#)
- NT service [8-5](#)
- Peripheral Gateway [6-2](#)
 - removing [8-5](#)
 - starting from Setup [1-14, 2-6, 3-7, 4-10, 6-32, 7-4](#)
- Northern Telecom Meridian [6-19](#)
- NT services [8-5](#)

P

- Partitioning [4-8](#)
- Pass-through tables [6-18](#)
- Peripheral Gateway
 - connecting to peripheral [6-7](#)
 - device number [3-5](#)
 - duplexed [1-4](#)
 - installing [6-1](#)
 - private network addresses [6-31](#)
 - required [3-5](#)
 - with Central Controller [6-29](#)
- Peripheral Gateway Configuration [6-4](#)
- Peripheral Gateway Interfaces [6-31](#)
- Peripheral Gateway Properties [6-2](#)
- Peripheral ID
 - Peripheral Gateway [6-7](#)
- Peripheral Interface Manager [6-7](#)
- Peripherals
 - interface manager [6-7](#)
- PG [6-1](#)
- Physical Controller ID
 - MCI NIC [5-3](#)
- PIM [6-7](#)
 - Aspect [6-9](#)
 - DMS-100 ACD [6-13](#)
 - G2 ACD [6-16](#)
 - Galaxy [6-17](#)
 - Meridian [6-19](#)
 - Rolm 9005 [6-25](#)
 - Siemens [6-25](#)
 - Spectrum [6-26](#)
- Polled VRU [6-6](#)
- Print Server [4-10](#)
- Private network
 - CallRouter [3-7](#)
 - Logger [2-5](#)
 - Peripheral Gateway [6-31](#)
- Probe Interval
 - Peripheral Gateway [6-6](#)
- Production Mode
 - Admin Workstation [4-4](#)
 - CallRouter [3-2](#)
 - CTI Gateway [7-2](#)
 - Peripheral Gateway [6-2](#)
- Program group [8-6](#)
- Program items [8-6](#)
- Purging historical data [2-5](#)

R

Real-time distributors [4-9](#)
Reboot [2-2, 2-3, 3-2](#)
Registering users [8-7](#)
Registry Editor [8-4](#)
RegistrySee Configuration registry [8-4](#)
RMC reports [4-9](#)
rmm.bat [8-5](#)
Rockwell Galaxy [6-17](#)
Rockwell Spectrum [6-26](#)
Rolm 9005 ACD [6-25](#)
Rolm 9005 PIM [6-25](#)
Router Log Viewer [8-6](#)
Router Properties [3-1](#)

S

Schedule import [4-10](#)
Schema Help [8-6](#)
Script Editor [8-6](#)
 workspace data [8-4](#)
Security [4-8, 8-7](#)
Service Control [8-6](#)
Services
 NT [8-5](#)
Setup [1-12, 8-5, 8-6](#)
 Admin Workstation [4-3](#)
 CallRouter [3-1](#)

 CTI Gateway [7-1](#)
 errors [1-13](#)
 Logger [2-1](#)
 Peripheral Gateway [6-2](#)
 post-install [1-14](#)
 Router [3-1](#)
Side
 CallRouter [3-3](#)
 CTI Gateway [7-2](#)
 Logger [2-3](#)
 Peripheral Gateway [6-3](#)
Sides [1-3](#)
Siemens Hicom ACD [6-25](#)
Siemens PIM [6-25](#)
Spectrum ACD [6-26](#)
Spectrum PIM [6-26](#)
Sprint NIC [3-3](#)
SQL Server [1-8](#)
 on Admin Workstation [4-8](#)
Supervisor CRT [6-26](#)
Supervisor terminal [6-25](#)
System ID [6-6](#)

T

Target Drive
 CallRouter [3-3](#)
 CTI Gateway [7-2](#)
 Logger [2-3](#)

Target drive

Admin Workstation [4-4](#)

Telnetd Server [8-5](#)

Temp directory [1-12, 1-13](#)

Termination Call Detail

for Meridian ACDs [6-20](#)

Timed Delivery Queue

Peripheral Gateway [6-6](#)

Timed delivery queue

CallRouter [3-4](#)

Tools [8-6](#)

Transaction Link [6-26](#)

U

Users

adding [8-7](#)

administrative [8-7](#)

read-only [8-8](#)

UTP [1-5](#)

V

VarCTI [6-18](#)

VRUs [6-28](#)

polled [6-6](#)

W

Web access [4-6](#)

WebView [1-7, 4-3, 4-6, 4-9](#)

Workforce management [4-10](#)

X

X.25 interface [6-17, 6-26](#)