Pre-installation Planning Guide for Cisco Unified Intelligent Contact Management, Release 12.5(1)

First Published: 2020-02-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

PREFACE

Preface ix

- Change History ix
- About This Guide ix
- Audience ix
- Related Documents x
- Communications, Services, and Additional Information x
- Field Notice x
- Documentation Feedback xi
- Conventions xi

CHAPTER 1

Pre-installation Planning Overview 1

- Pre-requisites to Install Unified ICM 1
- Planning Process 2
  - Coordinating and Scheduling Tasks 2
  - Preinstallation Information Road Map 2
  - NIC and ACD Supplements 4

CHAPTER 2

Cisco Unified ICM Overview 5

- How Unified ICME Software Works 5
  - Unified ICM Call Routing 5
    - Pre-routing 6
    - The IXC Network 6
    - Route Requests 6
    - Route Responses 7
    - ACDs 7
    - Peripheral Gateway 7

Post-routing 7
CTI Server 7
Monitoring and Reporting 7
Administration & Data Server 7
Unified ICM System Software Components 8
CallRouter 8
Logger 8
Network Interface Controller (NIC) 8
Peripheral Gateways 8
Administration and Data Server Control Console 9
Historical Data Server and Detail Data Server 9
ICM Reporting 10
Cisco Unified Intelligence Center 10
ICM Options and Related Products 10
Pre-routing 10
Post-routing 11
Pre- and Post-routing Systems 11
Computer Telephony Integration (CTI) 11
CTI Server 12
Cisco CTI Object Server (CTIOS) 12
VRU Interface 13
ICM Application Gateway 13
ICM Gateway SQL 14
Internet Script Editor 15
Cisco Unified Contact Center 15

CHAPTER 3 IXC Overview 17
ICM Software and IXC Interaction 17
Toll-Free Caller 18
LEC-to-IXC 18
Network Query 19
ICM NIC 19
Unified ICM CallRouter Process 19
Best Destination Address Returned 19

IXC Network 19
Connecting Call 19
Supported Carrier Connections 19
Fault Tolerance to NICs 19
Goal of NIC Fault Tolerance 20
Link Redundancy 20
Route Diversity 21

CHAPTER 4 Switch Overview 23
PG-to-Peripheral Connections 23
Supported ACD Switches 24

CHAPTER 5 Peripheral Gateway Configurations 25
Peripheral Gateway Fault Tolerance 26
PG Platform Options 28
Considerations for PGs and PIMs 29
Standard PG Configuration 29
Remote ACD and VRU Connection to PGs 30
Multiple PGs Connecting to Single ACD 31

CHAPTER 6 CTI Planning 33
CTI Server 33
CTI Server Communications 34
CTI Server Platform Options 34
CTI Server Fault Tolerance 35
Cisco CTI Object Server (CTI OS) 36
CTI Server Client Application Models 37
Agent Workstation Application 37
CTI Bridge Application 37
CTI Server Network and Database Planning 38
Network Topology 38
Network Security 38
Software Distribution Strategy 39
Well-Known Port for CTI Server 39

Fail-over Strategy for CTI Clients 39

Database Strategy 39

CTI Server Messages 39

Typical Call Scenario 40

Message Load and Bandwidth 40

CTI Server Platform 40

Third-Party Call Control 41

ACD Support for Client and Third-Party Call Control 42

CHAPTER 7 Interactive Voice Response (VRU) Systems 43

VRU Configuration Options 43

Configuration with ACD PG Only 45

Configuration with IVR and ACD PGs 46

Network-Side VRU with VRU and ACD PGs 46

In-Network VRU with ACD PG Only 47

In-Network VRU with VRU and ACD PGs 48

VRU Transfer Routing Using Third-Party Call Control 49

VRU Programming and Application Development 50

VRU Peripheral Gateway 50

CHAPTER 8 ICM Application Gateway and ICM Gateway SQL planning 53

ICM Application Gateway planning 53

Host System Preparation 53

Fault Tolerance 54

ICM Gateway SQL Planning 54

Database Server Platform 54

Data Transfer 55

Database Configuration Overview 56

CHAPTER 9 ICM Platform Planning 57

Number of Servers Required 57

ICM Platform Considerations 58

Processor Utilization 58

Paging Requirements 59

Logger Expansion 59
Administration and Data Server Planning 59
Administrator Sites 60
Administration Client Requirements 61
Historical Data Servers 61
HDS Features 62

CHAPTER 10 Site Preparation 63
Site Preparation 63

CHAPTER 11 Datacom Requirements 65
ICM Sites 66
ICM Networks 66
Private and Visible WAN Links 67
Signaling Access Networking 68
Network Topology 69
Network Bandwidth Requirements 69
Network Latency Requirements 70
Heartbeat and Keepalive Detection 71
Synchronization 72
State Transfer 73
Diverse Facilities 74
Cisco ICM Quality Of Service (QoS) 74
Active Directory Services 74
Configure TCP/IP 74
Central Sites 75
Central Site Visible Network 76
Visible IP Router Configuration 77
Central Site Private Network 77
Signaling Access Network 78
CallRouter Node 79
Disabling Windows Server 2012 Networking 81
Logger Node 82
Optional Database Server Platform 84

Administration and Data Servers at Central Site 85
Peripheral Gateways at Central Site 86
Contact Center Sites 88
Simplexed PG Site 88
Duplexed PG Site 89
Duplexed PG Site with Separate IVR LAN 91
PG Network Configuration 91
Contact Center IP Routers 92
Admin Sites 93

CHAPTER 12 **IP Address Worksheets** 95
Visible Network IP Address Requirements 95
Private Network IP Address Requirements 97
Signaling Access Network IP requirements 100
Static Route Requirements 100

Preface

- Change History, on page ix
- About This Guide, on page ix
- Audience, on page ix
- Related Documents, on page x
- Communications, Services, and Additional Information, on page x
- Field Notice, on page x
- Documentation Feedback, on page xi
- Conventions, on page xi

Change History

This table lists and links to changes made to this guide and gives the dates those changes were made. Earliest changes appear in the bottom rows.

Change	Date
Created 12.6(1)	April 2021

About This Guide

Audience

This guide is intended for contact center managers and system support personnel who are planning and preparing contact center sites for a Unified ICM system installation. Readers should be familiar with contact center site planning and preparation issues. They should also have a basic understanding of the Unified ICM system and the components that are installed as part of the system.

Related Documents

Document or resource	Link
	http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-documentation-roadmaps-list.html
Cisco.com site for Cisco Unified Contact Center Enterprise documentation	http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html
	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices

- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.

Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the .
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

CHAPTER 1

Pre-installation Planning Overview

Note This manual deals with Unified ICM. For information on Unified CCE, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

The Unified ICM software is a distributed application that routes telephone calls, web inquiries, and e-mail across geographically distributed contact centers. A typical Unified ICM system includes servers located at several sites, with the number of servers depending on factors such as call volume requirements.

Because the Unified ICM software works with different types of contact center equipment and sometimes one or more carrier networks, some pre-installation planning is necessary to ensure that the Unified ICM installation process proceeds smoothly and on schedule.

This chapter provides an overview of the Unified ICM pre-installation planning process. It also contains a pre-installation planning document roadmap, which provides an order in which you can start the tasks.

- Pre-requisites to Install Unified ICM, on page 1
- Planning Process, on page 2

Pre-requisites to Install Unified ICM

To install and run Unified ICM 12.5(1), you need the following specifications:

- Windows Server - For more information, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
- SQL Server - For more information, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
- For information on all supported configurations and versions for Unified ICM in the Unified CCE solution, see the latest Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.
- For information on supported OVA templates, see the Virtualization Wiki at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

Planning Process

The Unified ICM pre-installation planning process involves coordinating and scheduling several tasks so you can complete them before the Unified ICM server platforms arrive. You typically prepare each site that is to contain Unified ICM components. Some pre-installation tasks take longer than others. Therefore, start the time-consuming tasks early and continue working in parallel on the other pre-installation tasks.

Coordinating and Scheduling Tasks

Designate one person in your organization to have overall responsibility for coordinating and scheduling the pre-installation planning tasks. This person can also delegate responsibility and assign tasks to people with the applicable expertise. For example, your MIS expert can begin working with Cisco to order the server platforms and at the same time, your data communications expert can start provisioning network facilities at each contact center site.

Preinstallation Information Road Map

This document provides guidance on topics such as provisioning IXC access, preparing ACDs, and determining the Unified ICM datacom requirements. In each case, one or more preinstallation tasks are covered. For most tasks, you can find additional information in other Cisco documents listed in the task outline.

It takes several weeks to provision IXC access so plan accordingly. After you compete the preinstallation tasks, make sure your contact center equipment (ACDs, PBXs, VRUs) have the necessary software releases and options. While those tasks are in progress, you can select Unified ICM product options and component platforms and begin preparing the installation sites.

The preinstallation tasks, activities associated with each task, and references to additional information for performing these tasks are as follows:

1. **Getting Started**

   - Understand the Unified ICM software.
   - Review the Unified ICM product options.
   - Determine the Unified ICM configuration.
   - Provide configuration data for contact center sites.
   - Document the current contact handling procedures.

   See the Unified CCE overview section of this guide and the .

2. **IXC Access**

   - Review ICM/IXC interaction.
   - Review IXC access specifics.
   - Determine a fault tolerance strategy for your network links.

   See IXC Overview, on page 17 and the relevant Cisco NIC Supplement document.

3. **Switch Preparation**

- Determine ACD requirements.
- Determine CTI and MIS link requirements.
- Order required upgrades and enhancements.

See the switch overview, site preparation, and peripheral gateway configuration sections of this guide and the relevant Cisco ACD Supplement documents.

4. **Product Options and System Integration**

    - Determine product option requirements.
    - Order any required upgrades or enhancements.

    See the CTI planning, site preparation, and ICM application gateway sections of this guide.

5. **Estimating System Size**

    - Enter data using the Unified ICM database sizing tool.
    - Note the specifications provided by the tool.
    - Determine the number of servers required.

    See the ICM platform planning section of this guide and the discussion of the ICM Database Administration tool (ICMDBA) in the.

6. **Network and Site Requirements**

    - Determine requirements for Unified ICM networking.
    - Order any additional network hardware.
    - Allocate IP addresses.
    - Meet basic site requirements.
    - Order any extra cabling or other required equipment.

    See the datacom requirements, site preparation, and IP address worksheet sections of this guide.

7. Preinstallation End-of Life (EOL) Component Check

    The ICM Installer checks for installed EOL components before upgrading the server. The installer prompts you for confirmation to remove them.

    See the for a list of EOL components for each release.

Related Topics

Cisco Unified ICM Overview, on page 5
CTI Planning, on page 33
Datacom Requirements, on page 65
ICM Application Gateway and ICM Gateway SQL planning, on page 53
ICM Platform Planning, on page 57
IP Address Worksheets, on page 95
IXC Overview, on page 17

Peripheral Gateway Configurations, on page 25
Site Preparation, on page 63
Switch Overview, on page 23

NIC and ACD Supplements

The NIC Supplements are reference documents that contain specific information on how the Unified ICM Network Interface Controller (NIC) interfaces with the supported IXC carrier networks. The NIC is the software process that allows the Unified ICM system to communicate with the carrier's intelligent switching network. For detailed technical information, refer to the NIC supplements when you are planning for IXC access.

The ACD Supplements are reference documents that contain the specific information you need to maintain Unified ICM Peripheral Gateways (PGs) in an Unified ICM environment. The PG is the Unified ICM component that provides an interface to proprietary ACD systems.

CHAPTER 2

Cisco Unified ICM Overview

In the initial phase of pre-installation planning, you need to become familiar with the Unified ICM system and understand how it fits into your overall enterprise contact center. You can then determine which products and components you want to deploy in an Unified ICM virtual contact center.

In this chapter, complete the following pre-installation tasks:

- Determine the role of the Unified ICM software in your enterprise. Understand how the Unified ICM software fits into the enterprise contact center and carrier networks.
- Choose Unified ICM products. Will your system be a complete pre-routing and post-routing system? Will you have other options such as Unified ICM Gateway SQL, Cisco CTI, or Unified IP IVR?

- How Unified ICME Software Works, on page 5
- Unified ICM System Software Components, on page 8
- ICM Options and Related Products, on page 10

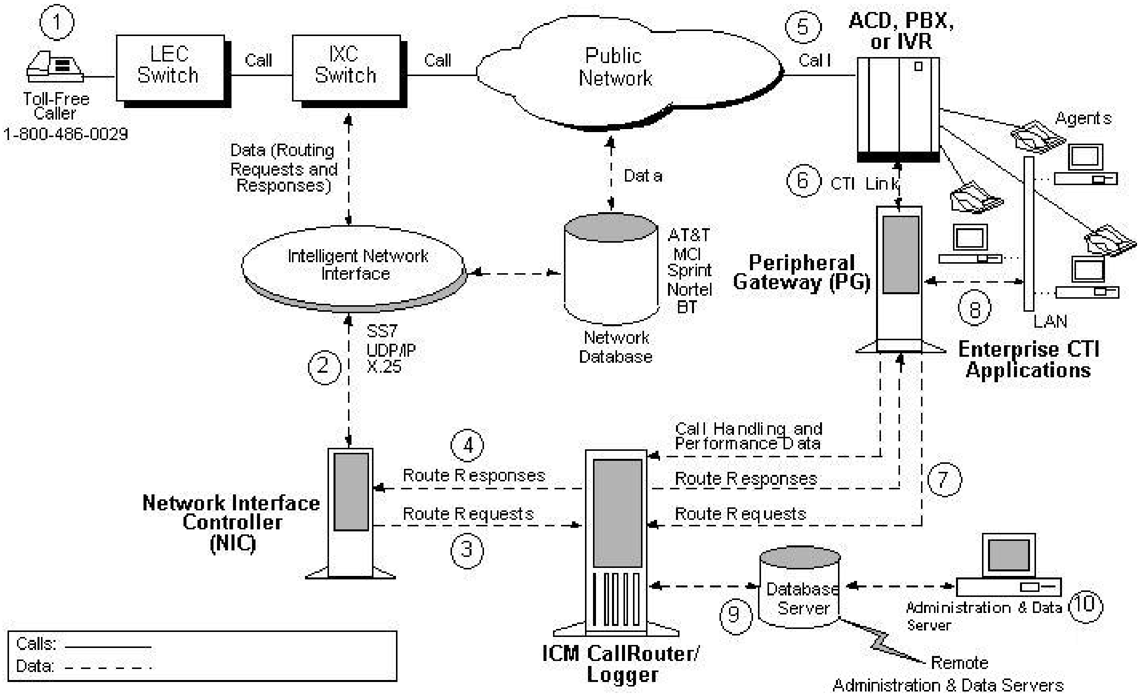
How Unified ICME Software Works

The Unified ICME Edition works with your contact center equipment and the IXC carrier network to create a virtual contact center. In the virtual contact center model, multiple distributed contact centers link to form one Unified CCE. The agents within the Unified CCE become members of a single team that is capable of servicing customer contacts throughout the enterprise.

Unified ICM Call Routing

The Unified ICM software makes the best use of your contact handling resources while ensuring that each customer is directed to the most appropriate resource available. To get an idea of how the Unified ICM software fits into the contact center and carrier environments, refer the following sections. These sections examine how the Unified ICM software routes telephone calls.

Figure 1: Intelligent Contact Routing (Telephone Calls)



Pre-routing

The Unified ICM software executes call routing decisions before a call terminates at a contact center. This concept is called pre-routing. As shown in the preceding figure, calls to be routed usually originate in the public telephone network as calls to a toll-free number (1).

The IXC Network

The Unified ICM software is configured in the intelligent network of the IntereXchange Carrier (IXC) to receive a route request for each designated incoming call (2). A subsystem of the Unified ICM software, called the Network Interface Controller (NIC), communicates with the carrier's network through an intelligent network interface.

Route Requests

The NIC translates the network's description of the call, including point of origin, number dialed, and any customer entered digits, into the language of the Unified ICM software. The NIC passes this call information to the CallRouter in the form of a route request (3).

Note Figures usually show the NIC as a separate computer. Actually, NICs are implemented as software on the Unified ICM software platform (usually on the CallRouter or CallRouter/Logger [Rogger] machines).

Route Responses

At this point, the Unified ICM software may query an ANI or customer profile database before returning a route response to the NIC (4). The NIC passes a destination for the call back to the IXC network. The IXC connects the call and maintains the voice path.

ACDs

Each contact center has one or more Automatic Call Distributor (ACD) systems that direct incoming calls to the telephone sets of individual agents (5). The Unified ICM software maintains real-time communications with the ACDs in each contact center by using a Peripheral Gateway (PG).

Peripheral Gateway

The PG communicates with the ACD over the switch vendor Computer Telephony Integration (CTI) link (6). To make optimal decisions, the Unified ICM software must know the latest status for every call, agent, and agent group in its network. One purpose of the PG is to extract this status information from the ACD and forward it to the CallRouter in-memory database. You can also use the PG as a CTI Server and as a communications interface between the Unified ICM and Voice Response Unit (VRU) systems located at contact center sites or in the network.

Post-routing

In private network configurations, ACDs can also originate call routing requests. This is called post-routing. Post-routing provides the same intelligence used in pre-Routing, but applies it to calls originating from a private network of ACD, PBX, and VRU systems. The PG assists in post-routing by forwarding routing requests to the Unified ICM software and returning the target destinations to the ACD (7).

CTI Server

External server or workstation applications can subscribe with a PG that acts as a CTI Server (8). The CTI Server provides call and agent event data that can be used in screen-pops and other CTI applications. At the desktop level, the Unified ICM CTI desktop provides an environment for integrating soft-phone, screen-pop, and data entry at the agent's workstation.

Monitoring and Reporting

All event data that the PG and router gathers is forwarded to the Unified ICM software and stored in an industry-standard relational database (9). This data is used in real-time monitoring and historical reporting. You can modify the standard Unified ICM monitoring screens and reports with Unified ICM-provided database access tools. Optionally, you can access the data directly with SQL or Open Database Connectivity (ODBC) tools.

Administration & Data Server

An Administration & Data Server (10) monitors and controls the overall operation of the Unified ICM software. The Unified ICM software can support multiple Administration & Data Servers located throughout the contact center network.

Unified ICM System Software Components

Pre-installation planning involves many different Unified ICM system software components. You may want to familiarize yourself with the role of the components in the Unified ICM system.

Note Not every component is used in every Unified ICM system.

CallRouter

The CallRouter is the part of the Unified ICM system that contains the call routing logic. The Unified ICM software receives call routing requests and determines the best destination for each call. It also collects information about the entire system. The Unified ICM software serves as a real-time server by forwarding performance and monitoring information to Administration & Data servers.

Logger

The Logger is the interface between the Unified ICM software and the database manager (Microsoft SQL Server). The Unified ICM software collects performance and monitoring information about the system and passes the information to the Logger for short-term storage in a central relational database. The Logger forwards historical information to the Historical Data Server (HDS). The HDS on the Logger maintains statistics and data for monitoring and reporting.

Network Interface Controller (NIC)

The NIC connects the Unified ICM software to the IXC signaling network. The NIC receives a route request from the signaling network for each incoming call and passes the request to the Unified ICM software. The Unified ICM software responds with routing information (a routing label), which the NIC passes back to the IXC signaling network.

Note Figures usually show the NIC as a separate computer. Actually, NICs are implemented as software on the Unified ICM software platform (usually on the CallRouter or CallRouter/Logger [Rogger] machines).

Peripheral Gateways

Each contact center device (ACD, PBX, or VRU) communicates with a Peripheral Gateway (PG). The PG reads status information from the device and passes it back to the Unified ICM software. The PG runs one or more Peripheral Interface Manager (PIM) processes, which are the software components that communicate with proprietary ACD systems. A single PIM is required for each peripheral to which the PG will interface. Therefore, a single PG (and its associated PIMs) can serve multiple peripherals of the same kind. For example, one PG with four Aspect ACD PIMs can serve four Aspect ACDs in the contact center.

Note A single PG can support both ACD PIMs and VRU PIMs; however, the ACD PIMs and the VRU PIMs must all be the same type of PIM (ACD PIMs must be the same type; VRU PIMs must be the same type).

A single server can support up to two PGs. For details, refer to the .

Administration and Data Server Control Console

The Administration & Data Server is the human interface to the Unified ICM software. It serves as a control console from which you can monitor agent and contact center activity and change how the Unified ICM software routes calls. For example, you can use the Administration & Data Server to configure the Unified ICM contact center data, create call routing scripts, and monitor and report on the Unified ICM system or some part of the system. Administration & Data Servers can be located anywhere, as long as they have LAN or WAN connections to the Unified ICM software.

Administration & Data Servers have several roles: Administration, Real-time data server, Historical Data Server, and Detail Data Server. A Unified ICM deployment must have Administration & Data Servers to fill these roles. The servers can be deployed in the following combinations to achieve the needed scalability with the minimum number of servers:

- Administration Server and Real-time Data Server (AW)
- Configuration only Administration Server
- Administration Server, Real-time and Historical Data Server and Detail Data Server (AW-HDS-DDS)
- Administration Server and Real-time and Historical Data Server (AW-HDS)
- Historical Data Server and Detail Data Server (HDS-DDS)

An Administration Client (formerly known as a “client AW”) serves the administration role, but is deployed as a client to an Administration Server for scalability. The Administration Client can view and modify the configuration, and receive real-time reporting data from the Administration & Data Server, but does not store the data itself, and does not have a database. You must install each Administration & Data Server on a separate server for production systems to ensure no interruptions to the real-time call processing of the Call Router and Logger processes. For lab or prototype systems, you can install the Administration & Data Server on the same server as the Call Router and Logger.

Historical Data Server and Detail Data Server

Administration & Data Servers need to access historical data (half hour data, call detail, and so on) for historical reporting in the Script Editor or in third-party tools. You must install at least one real-time Administration & Data Server in a system with a Historical Data Server (HDS) to support reporting and long-term historical data storage. The HDS IP address requirements are identical to those of a standard Administration & Data Server.

The Historical Data Server (HDS) and Detail Data Server (DDS) are used for longer-term historical data storage. The HDS stores historical data summarized in 15 or 30 minute intervals and is used for reporting.

DDS stores detailed information about each call or call segment and is used for call tracing. Data may be extracted from either of these sources for warehousing and custom reporting.

Typically these Data Servers are deployed with a primary AW as a single server serving all three roles (AW-HDS-DDS).

ICM Reporting

The Unified ICM Reporting solution provides a Unified Intelligence Center interface to access data describing the historical and real-time states of the system.

Reporting concepts and data descriptions are described in ; this description is independent of the reporting user interface being used.

Cisco Unified Intelligence Center

Cisco Unified Intelligence Center (Unified Intelligence Center) is an advanced reporting product used for Unified CCE and other products. This platform is a web-based application offering many Web 2.0 features, high scalability, performance, and advanced features such as the ability to integrate data from other Cisco Unified Communications products or third-party data sources. Unified Intelligence Center incorporates a security model which defines different access and capabilities for specific users. Unified Intelligence Center Standard is included with Unified ICM. Unified Intelligence Center Premium is an optional product with additional features. You must install Unified Intelligence Center on a separate server; it cannot be co-resident with other Unified ICM components.

For a complete description of both Unified Intelligence Center products see .

ICM Options and Related Products

You can set up the Unified ICM software with various options. You can add software to perform database lookups or perform secondary call routing after a call terminates at an ACD. In some cases, the Unified ICM software is part of other Cisco contact center products. Review the Unified ICM software options and related products to learn about the different ways to deploy the Unified ICM software in a Unified CCE.

Pre-routing

The Unified ICM software uses pre-routing to execute routing decisions before a call terminates at a contact center. With pre-routing, the Network Interface Controller (NIC) receives the route request from the IXC and passes the call information to the Unified ICM software. The Unified ICM software processes the route request through a call routing script, which defines how the call should be routed. The Unified ICM software returns a route response to the NIC, which in turn forwards it to the IXC. The route response contains the call's final destination.

In pre-routing, the Peripheral Gateway's role is to keep the Unified ICM software informed of the real-time status of switches, calls, and agents in the Unified CCE. The Unified ICM software uses this real-time data to make an informed call routing decision.

Pre-Routing systems require the following components:

- Network Interface Controller (NIC)
- CallRouter
- Logger

- Administration & Data Server
- Peripheral Gateway (PG)

The pre-routing capabilities are enabled through the Network Interface Controller (NIC) and the CallRouter processes. NICs are implemented as software on the Unified ICM software platform (for example, on the CallRouter or Logger machines).

The Unified ICM routes calls within the public network based on several dynamic variables. You can use any combination of the following variables to route calls:

Agent availability	Day of week
Agent skills	Number dialed
Caller-entered digits	Origin of call
Cost of the call	Cost of the transaction
Customer database lookup	Scheduled agents
Customer-defined business rules	Time of day

Calls are routed in the most efficient manner possible given the current contact center load conditions.

Post-routing

In a traditional time-division multiplexing (TDM) environment, post-routing systems have software that allows the CallRouter to make secondary routing decisions after a call is received at a contact center. In post-routing, the ACD or VRU submits a route request to the Unified ICM software. The Unified ICM software executes scripts to process the routing request and return a destination address to the ACD. The Unified ICM software then directs the ACD to transfer the call to an agent, skill group, or service, either in the same contact center or at a different contact center. In making a post-routing decision, the Unified ICM software can use the same information and script it uses in pre-routing. In other words, the same call routing intelligence that is used in the pre-routing of calls is applied to calls that are interflowed between contact center sites, transferred between agents, or transferred into or out of VRU's.

Pre- and Post-routing Systems

A pre- and post-routing Unified ICM system is a complete intelligent call routing, monitoring, and reporting system. The Unified ICM software can execute routing decisions before a call terminates at a contact center. It can also make secondary routing decisions after a call is received at a contact center. You can expand a Pre- and post-routing system with optional features such as Unified ICM Application Gateway, Unified ICM Gateway SQL, Unified ICM IVR interface, and CTI Server to create an intelligent call routing and management solution in which all the elements of the Unified CCE play a role in intelligent routing.

Computer Telephony Integration (CTI)

Cisco CTI software provides an interface between the Unified ICM software and agent desktop and server applications. The CTI software works with a PG's ACD and IVR interface software and all associated ACDs to track events and transactions and forward call- and transaction-related data to an agent's desktop computer.

The CTI software has full third-party call control features that allow agents and integrated desktop applications to perform tasks such as transferring calls, conferencing calls, and setting call data all within an enterprise framework. An agent at the desktop can transfer voice and data in the form of a screen-pop among agents and across different ACD platforms. This allows customer and transaction data to accompany a call from an IVR or web server to the agent and from site-to-site as required. The Unified ICM system can also use CTI data to determine call destinations based on factors such as customer value, business objectives, market penetration, and personalized service.

CTI Server

CTI Server, the basic server component of Cisco CTI, enables the Unified ICM software to deliver agent, call, and customer data in real-time to a server and/ or workstation application as events occur throughout the life of a call. The CTI Server is a software process that runs on a Peripheral Gateway (PG).

It is a gateway into the Unified ICM software data and services.

- Pre-route indications identify a caller and provide associated attributes to applications while the call is still in the public or private network and before the caller is connected to an agent, web server or VRU.
- Call events are provided throughout all stages of the call flow, from the moment a call arrives at an answering location (ACD, PBX, VRU, web server) until the caller hangs up.
- Agent work state changes are reported as they occur.

Cisco CTI Object Server (CTIOS)

CTI Object Server (CTIOS) is a high-performance, scalable, fault-tolerant server-based solution for deploying CTI applications. It serves as a single point of integration for third-party applications, including Customer Relationship Management (CRM) systems, data mining, and workflow solutions.

CTIOS is a client of CTI Server and has a single all-events connection to Cisco CTI Server. In turn, CTIOS accepts client connections using session, agent, and call interfaces. These interfaces are implemented in .NET, COM, Java, and C++, allowing for a wide range of application development uses. The interfaces are used for call control, to access data values, and to receive event notifications.

CTIOS configuration and behavior information is managed at the CTIOS server, simplifying customization, updates, and maintenance. You can access and manage the servers remotely. Thin-client and browser-based applications that do not require Cisco software on the desktop can be developed and deployed with CTIOS.

CTIOS incorporates the following major components:

- CTIOS Toolkit
- Client Interface Library
- CTIOS Combo Desktop for Agents and Supervisors

Note Refer to the Cisco CTIOS Software documentation for more information.

VRU Interface

The Voice Response (VRU) interface software runs on a PG platform. It allows the Cisco Unified ICM software to route calls to targets on VRU's and collect data from VRU's for use in call routing, real-time monitoring, and historical reporting.

The VRU interface can also provide queuing at a network-based or premises-based VRU. With this feature, calls can be directed to an VRU queue when no other appropriate answering resource is available. The VRU interface is not specific to a particular VRU system or manufacturer. It is based on an open VRU model. Many VRU systems support Cisco's Open VRU Interface Specification, including Unified CVP.

The Cisco Customer Voice Portal integrates with both traditional time-division multiplexing (TDM) and IP-based contact centers to provide a call-management and call-treatment solution with a self-service VRU option that can use information available to customers on the corporate Web server. With support for automated speech recognition (ASR) and text-to-speech (TTS) capabilities, callers can obtain personalized information and can conduct business without interacting with a live agent.

For a list of VRU's that support this interface, contact your Cisco representative.

Note You can integrate VRU systems into the Cisco Unified ICM software in several ways. Interactive Voice Response (VRU) Systems, on page 43 provides more information on VRU integration as well as examples of how you can integrate VRU's with the Cisco Unified ICM system.

ICM Application Gateway

The Cisco Unified ICM Application Gateway option allows the Cisco Unified ICM software to interact with a host system that is running another contact center application. Within the Cisco Unified ICM software, the Gateway feature is implemented as an Application Gateway node in a call routing script. You add an Application Gateway node to a script to instruct the system to execute an external application. This allows the script to evaluate responses from the external application and base subsequent routing decisions on the results produced by the application.

The Gateway option allows the Cisco Unified ICM system to interface with any external application, not just database applications.

You can use the Gateway option within the Cisco Unified ICM system to:

- Allow other applications to select a call's destination.
- Control or trigger external applications through Cisco Unified ICM call routing scripts.
- Pass data to and collect data from other contact center applications.

For example, a simple Gateway application might return a variable to the CallRouter that identifies the caller as having a premium account. The routing script can use this information to control where and how the call is routed. Optionally, the Cisco Unified ICM can pass the retrieved information to the site that is receiving the call. Data such as account numbers, dates, billing phone numbers, and addresses can be passed along with the call to an answering resource.

Note ICM Application Gateway and ICM Gateway SQL planning, on page 53 provides more information on planning for the Gateway feature.

ICM Gateway SQL

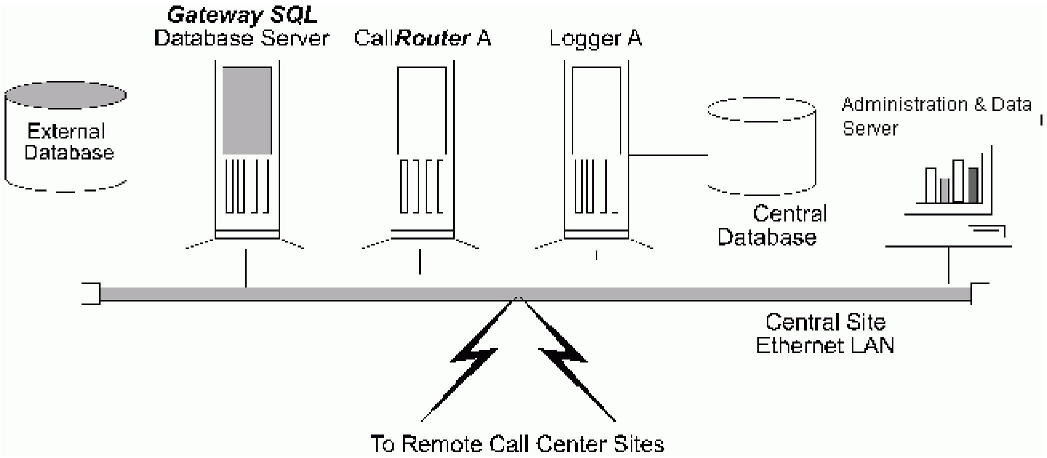
Cisco Unified ICM Gateway SQL allows the Cisco Unified ICM software to query an external Microsoft SQL Server database and use the data in call routing. If you have databases that contain customer account or profile information, you can perform database lookups to assist in call routing. You can base the database lookups on Calling Line ID (CLID), Dialed Number (DN), or Caller Entered Digits (CED) such as account or social security numbers.

A typical Gateway SQL application can prioritize callers. For example, a call routing script can use the caller's CLID to access a database and retrieve data about the caller such as the caller's average monthly bill. Based on this information, the routing script routes the caller to the most appropriate answering resource.

Note Before implementing the Gateway SQL and DB Lookup functionality, consider a Unified CVP VXML Application for database lookup instead. The DB Lookup node will interrupt routing while doing it's queries. The Unified CVP VXML Application will scale well.

The following figure shows a basic Gateway SQL configuration. Note that this configuration requires an additional database server on which you can load the external Microsoft SQL Server database and data.

Figure 2: Gateway SQL Configuration



Note You must perform some pre-installation planning if you are going to use the Cisco Unified ICM Gateway SQL option. ICM Application Gateway and ICM Gateway SQL planning, on page 53 provides more information on planning for the Cisco Unified ICM Gateway SQL feature.

Internet Script Editor

Internet Script Editor is an application that works with routing and administration scripts. It provides the same functionality as the Cisco Unified ICM Script Editor software, without the need for an Administration & Data Server.

Internet Script Editor works through the IIS Web server on Cisco Unified ICM software, using HTTP to communicate with the Cisco Unified ICM software.

The Internet Script Editor and the Cisco Unified ICM Script Editor GUIs are essentially the same. The menus, toolbars, palette, and work space are utilized in the same manner in both applications. The differences between the two occur primarily in the method by which each application communicates with the Cisco Unified ICM software.

Cisco Unified Contact Center

Cisco Unified Contact Center combines Cisco IP telephony products and Cisco Unified ICM software to create an IP-based contact management solution. Cisco Unified Contact Center provides a migration path to an IP-based contact center by supporting integration with legacy call center platforms and networks. With Cisco Unified Contact Center, agents can use Cisco IP phones to receive both time-TDM and VoIP phone calls. Capabilities of the Cisco Unified Contact Center include intelligent call routing, ACD functionality, network-to-desktop CTI, Unified IP IVR integration, call queuing, and consolidated reporting.

Cisco Unified Contact Center is based mainly on two Cisco products: Unified CM and ICM software. Unified CM provides traditional PBX telephony features in an IP telephony environment. Unified ICM software provides enterprise-wide management and distribution of voice and data from ACDs, Unified IP IVR systems, small office/home office (SOHO) agents, and desktop applications. Cisco Unified IP phones and Unified IP IVRs (as well as traditional TDM IVRs) are also part of the Cisco Unified Contact Center.

Note For information on Unified CCE, see the at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.htmland the .

CHAPTER 3

IXC Overview

The Unified ICM Enterprise Edition software requires access to the IntereXchange Carrier intelligent call routing network to perform pre-routing. Each interexchange carrier offers intelligent network services that allow customer-premises equipment to participate in network-level call routing. The Unified ICM software uses a Cisco Network Interface Controller (NIC) to connect to one or more networks.

Specifically, this chapter helps you to complete the following tasks:

- Choose one or more carriers. Cisco supports network interfaces with several carriers. You can use one or more carriers with the Unified ICM software.
- Choose the types of network link fault tolerance to apply. Apply fault tolerance in the network interface and the links to the carrier intelligent network.
- Order intelligent network service. After you review the requirements for your specific Cisco NIC, order intelligent network service and work with the carrier and Cisco to bring the service on line.

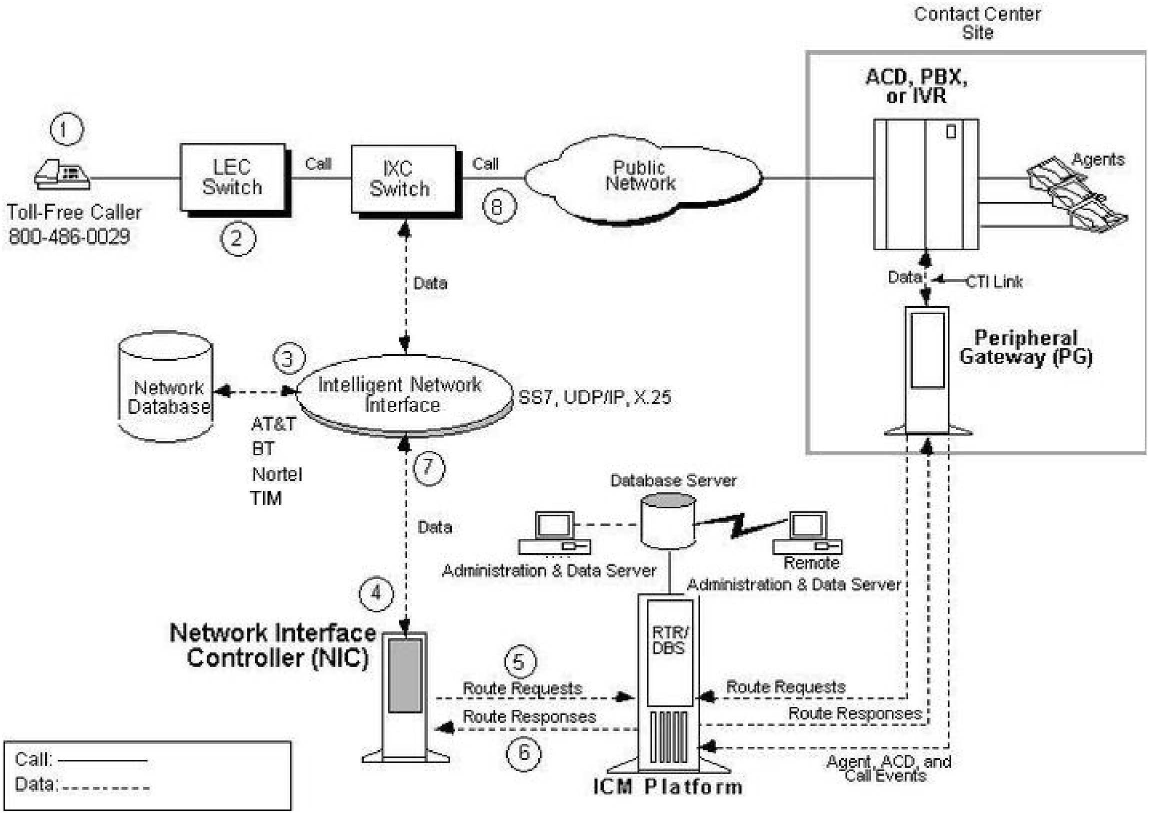
- ICM Software and IXC Interaction, on page 17
- Fault Tolerance to NICs, on page 19

ICM Software and IXC Interaction

The Network Interface Controller (NIC) is the interface between the Unified ICM software and the IXC intelligent network. The NIC uses network control links to communicate with the IXC network. These links are typically offered as part of the carrier intelligent network service.

Cisco provides a NIC to interface with the specific carrier network. For example, if you have TIM service, your Unified ICM system is equipped with a Cisco-supplied TIM NIC. If you use both AT&T and TIM as carriers, your Unified ICM system is equipped with AT&T and TIM NICs. The following figure shows the interaction between the IXC network and the Unified ICM NIC.

Figure 3: Network Interface Controller



You can implement a Unified ICM Network Gateway for Sigtran networks. The Unified ICM Network Gateway is implemented as a separate node on the Unified ICM signaling access network. When this node is implemented, you can install the NIC software on the CallRouter server. For Sigtran networks, you can deploy a Sigtran Gateway on either the CallRouter server or a separate machine; the NIC software is installed on the CallRouter server. However, the INAP Sigtran gateway must be installed on a separate server.

The circled numbers in the preceding diagram show the specific flow of messages to and from the NIC within the Unified ICM software and the IXC network. The following sections explain the message flow.

Toll-Free Caller

As shown in the preceding figure, the flow of messages between the network and the Unified ICM begins when a caller dials a toll-free number (1).

LEC-to-IXC

The Local Exchange Carrier (LEC) determines which interexchange carrier (IXC) is providing transport for that particular number and forwards the call to the IXC switch (2).

Network Query

The IXC switch holds the call momentarily while it queries a network database to determine where to route the call (3).

ICM NIC

The network database forwards the query to the NIC and requests an intelligent routing decision (4).

Unified ICM CallRouter Process

The NIC software process receives the request, translates it into a standard format, and forwards it to the Unified ICM CallRouter process (5)

Best Destination Address Returned

The Unified ICM software selects the appropriate call routing script, assesses the skills and current real-time status of agents throughout the contact center network, and returns the best destination address back to the NIC (6).

IXC Network

The NIC sends the destination address to the IXC network (7).

Connecting Call

The network instructs the originating IXC switch to connect the call to the destination specified by the Unified ICM software (8). The total time the carrier takes to connect the call varies. However, the additional time the Unified ICM software adds to process the route request is typically less than half a second.

Supported Carrier Connections

The basic supported carrier connections and their corresponding Unified ICM software routing client (NIC) and network transport protocol information is provided in the Virtualization for Unified CCE - Additional Information page available at this URL: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/ucce_virt_xtras.html#Virtualization_Support_for_ICM_Network_Interface_Controllers_

Fault Tolerance to NICs

You may already have a strategy for fault tolerance for some parts of the Unified ICM system. For example, you may have decided to use a duplexed, distributed Unified ICM central controller and duplexed PGs at each call center. It is just as important to apply fault tolerance to the NICs and intelligent network access links. Without a connection to the carrier's intelligent network, the Unified ICM system cannot perform pre-routing. If these links are lost, calls are typically routed according to the default routing plans set up in the carrier network.

Note For more information on Unified ICM system fault tolerance, see the for more information.

Goal of NIC Fault Tolerance

The goal in applying NIC fault tolerance is to add levels of protection that successively eliminate single points of failure.

Cisco requires an order of importance to follow when choosing the types of fault tolerance to apply in the carrier network-to-ICM system connection:

- First, use **redundant links** from the Cisco NIC to the carrier's intelligent network.
- Next, if you have redundant links, provision those links on **diverse facilities**. This adds another level of fault tolerance to your network connection.
- For NICs that run on the Unified ICM CallRouter platform, the NIC processes are duplexed when the CallRouter is duplexed.

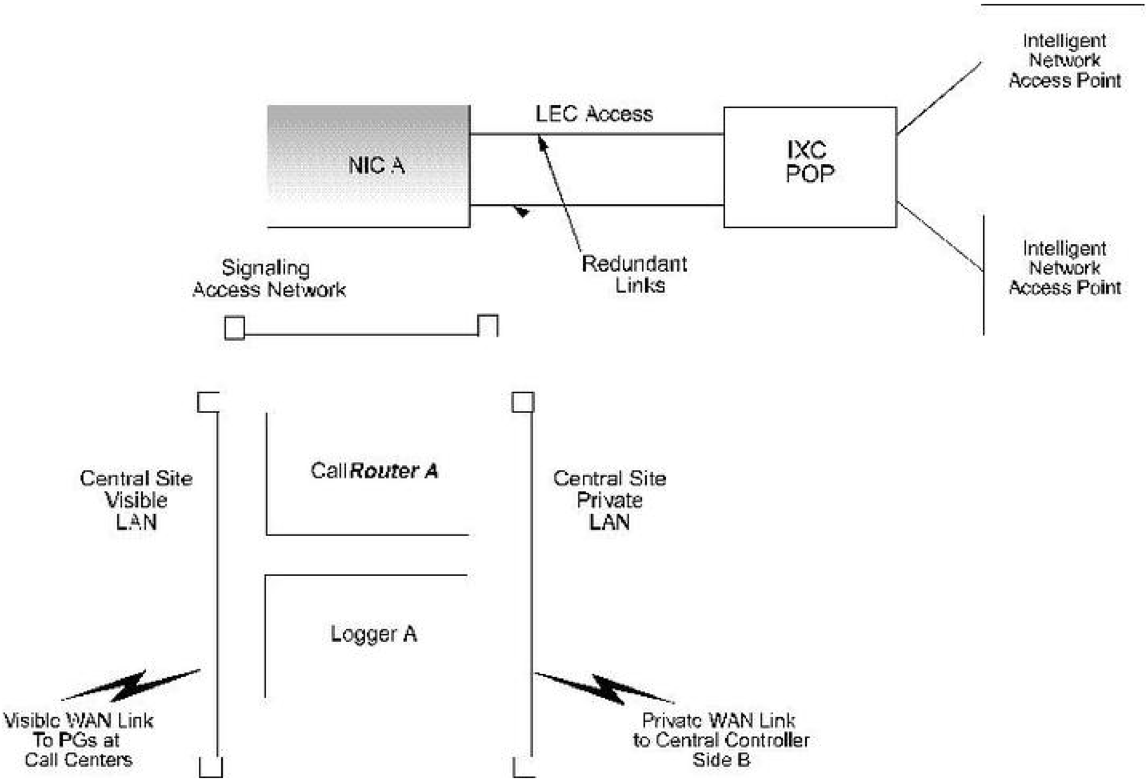
  The types of NIC fault tolerance you apply have a bearing on the number of links you need to provision for IXC intelligent network access.

Link Redundancy

Cisco requires that you configure redundant links to the IXC network. In other words, rather than having a single link from the NIC to the IXC intelligent network, provision two links. Having just one link to the IXC network represents a single point of failure (that is, an area or node in the system that, should it fail, can cause the system to stop routing calls).

By using redundant links, you increase the reliability of the IXC network connection and add an important level of fault tolerance to the system. The following figure shows a simplexed Unified ICM central controller and NIC with redundant links to the IXC network.

Figure 4: Redundant Links


Intelligent Network Access Point
LEC Access
NIC A
IXC POP
Redundant Links
Signaling Access Network
Intelligent Network Access Point
CallRouter A
Central Site Visible LAN
Central Site Private LAN
Logger A
Visible WAN Link To PGs at Call Centers
Private WAN Link to Central Controller Side B

In the preceding figure, single points of failure still exist because the NIC, CallRouter, and Logger are simplexed. The simplexed central controller and NIC configuration are shown here only as an example. This type of simplexed configuration is used only for non-critical systems that can tolerate potentially long interruptions in service (for example, in lab or demo systems).

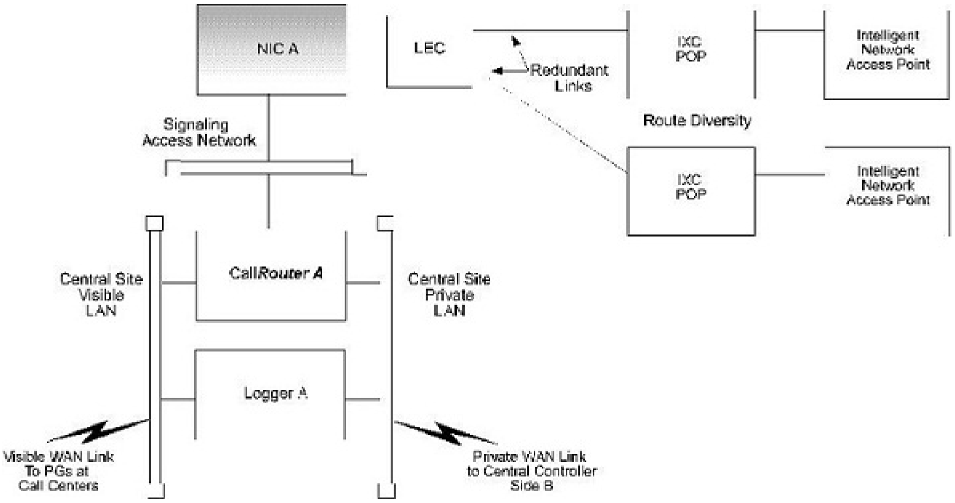
The major IXCs support redundant links to their intelligent networks. Contact your carrier for more information on access link options.

Route Diversity

For even more protection against network outages, Cisco requires that the network links are provisioned on diverse network facilities. By having diverse links, you further reduce the risk that another single point of failure (in this case, the failure of a circuit) could cause you to lose the connection to the IXC network. For example, you might provision one access link on one T1 circuit and provision the other access link on a different T1 circuit. By having diverse links, you protect against network failures in which an entire circuit is lost.

The following figure shows a simplexed Unified ICM system with redundant links and route diversity:

Figure 5: Redundant Links and Route Diversity


NIC A
LEC
Redundant Links
IXC POP
Intelligent Network Access Point
Route Diversity
IXC POP
Intelligent Network Access Point
Signaling Access Network
Central Site Visible LAN
CallRouter A
Central Site Private LAN
Logger A
Visible WAN Link To PGs at Call Centers
Private WAN Link to Central Controller Side B

This example provides more fault tolerance by protecting against circuit failure or the loss of an IXC Point Of Presence (POP). Although the NIC is at one location, the redundant links connect to two different POPs. If one IXC POP is taken out of service (for example, in the event of a natural disaster), one link can still access the IXC network through the other POP.

The major carriers provide options for route diversity. Check with your carrier to discuss having the links handled by different POPs. You need to make sure that both the IXC and the Local Exchange Carrier (LEC) are using diverse circuits. Your LEC may impose some limitations on link diversity from the NIC to the IXC POP (that is, over the “last mile”). These limitations often depend on whether the call center is located in a metropolitan or rural area.

CHAPTER 4

Switch Overview

Each contact center device (ACD, PBX, or VRU) communicates with an Unified ICM Peripheral Gateway (PG). The PG reads status information from the device and passes it back to the Unified ICM software. The PG runs one or more Peripheral Interface Manager (PIM) processes, which are the software components that communicate with proprietary ACD systems. One PIM is required for each peripheral to which the PG will interface, so if you have two identical ACDs, your PG requires two PIMs.

A single PG can serve multiple peripherals of the same kind. For example, one computer with an Aspect PG and several Aspect PIMs can serve several Aspect ACDs in the contact center. Another PG and PIM on the same computer can serve an VRU.

Note A single PG can support both ACD PIMs and VRU PIMs, though the ACD PIMs must all be of the same kind.

This chapter provides an overview of how the PG interfaces with ACDs in a contact center environment.

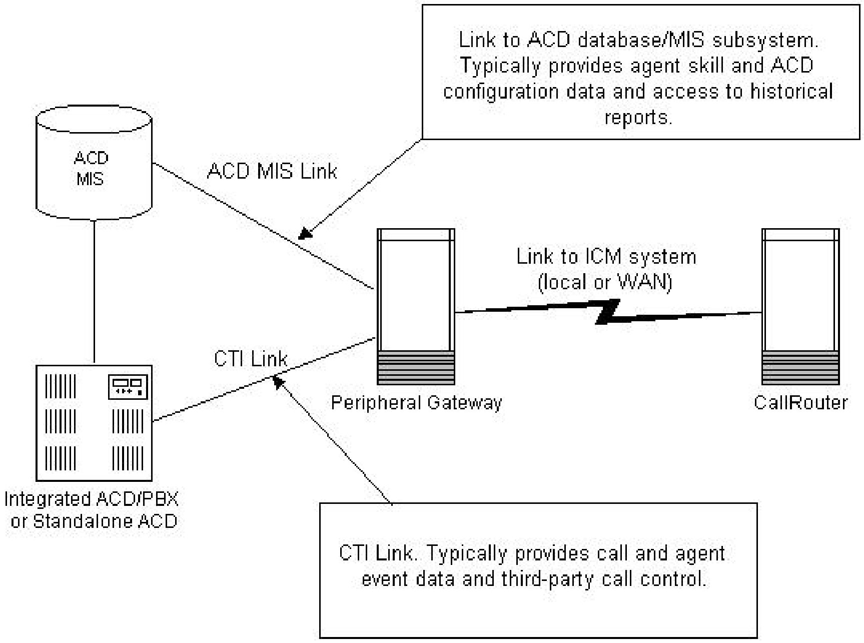
- PG-to-Peripheral Connections, on page 23
- Supported ACD Switches, on page 24

PG-to-Peripheral Connections

Each contact center peripheral (ACD, PBX, or VRU) requires a connection to a Cisco Peripheral Gateway (PG). The Peripheral Gateway provides a software interface between ACD, PBX, and VRU systems and the Unified ICM routing software.

The PG connects to a peripheral via the peripheral's computer telephony integration (CTI) link. In some cases, the PG also connects to the peripheral's MIS subsystem. The MIS subsystem can be on a separate hardware platform or it can be integrated with the ACD, PBX, or VRU. The relationship of the Peripheral Gateway to an ACD system is shown in the following figure.

Figure 6: Peripheral Gateway ACD/PBX Interface


Link to ACD database/MIS subsystem. Typically provides agent skill and ACD configuration data and access to historical reports.
ACD MIS
ACD MIS Link
Link to ICM system (local or WAN)
CTI Link
Peripheral Gateway
CallRouter
Integrated ACD/PBX or Standalone ACD
CTI Link. Typically provides call and agent event data and third-party call control.

Through the CTI link, the PG monitors changes in agent status, calculates call handling performance statistics, and forwards events to the CallRouter. The MIS connection provides additional information such as the mapping of individual agents to skill types and the current status of agents (either by themselves or relative to a given agent group or skill group). Typical agent states include Logged In, Ready, Talking In, Talking Out, and Work Not Ready. The MIS link also provides the Unified ICM system with ACD configuration data and historical reports.

Each PG has one or more connections to the peripheral. The type of connection used depends on the type of peripheral. For example, some ACDs use a TCP/IP Ethernet connection, while others require X.25 links. Refer to the Cisco Unified ICM Software Supported Switches (ACDs) documentation for more information.

Supported ACD Switches

To ensure that your ACD software version is compatible with Unified ICM software, refer to the Unified CCE compatibility information at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html . This document contains the latest information on Unified ICM switch support.

Note For more details on how ACDs interface with the Unified ICM software, see the appropriate Cisco Unified ICM software ACD Supplement. The ACD Supplements provide more technical details on the ICM-to-ACD interface than is provided in this document.

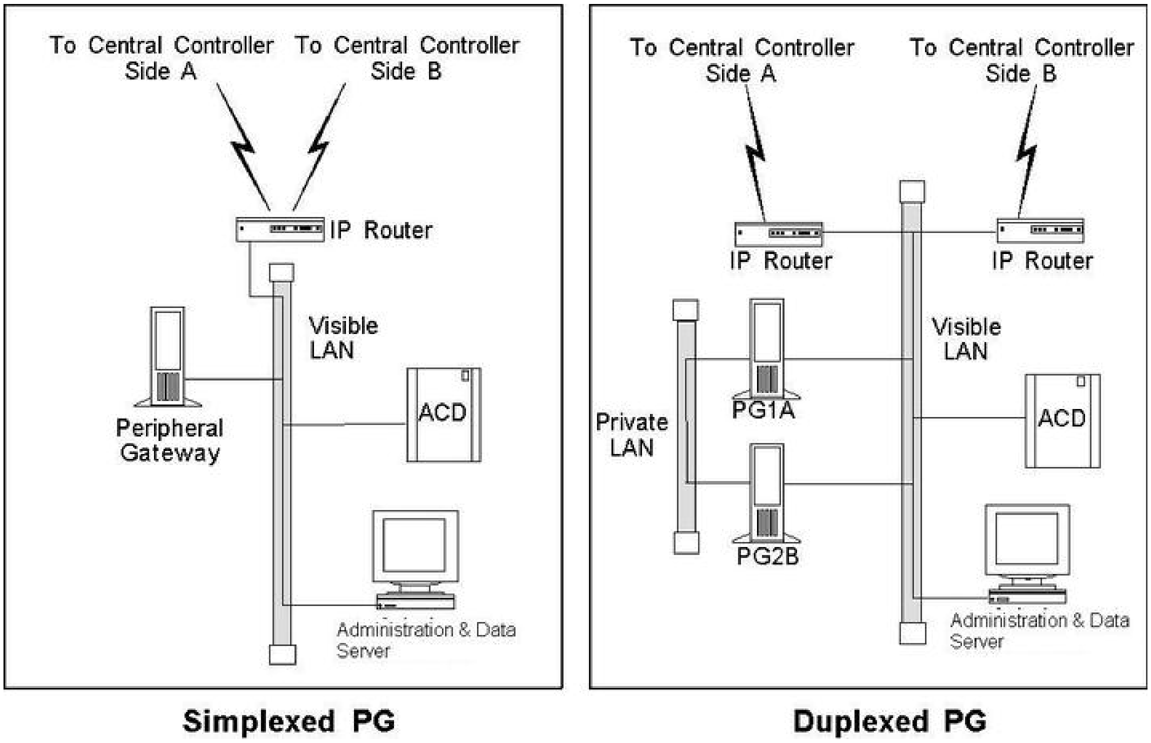
CHAPTER 5

Peripheral Gateway Configurations

As part of planning for ACDs and PGs, you need to decide whether your Peripheral Gateways will be simplexed or duplexed. Simplexed means that one PG is used. Duplexed means that two identical PGs are used, one as a backup system. (Both PGs run simultaneously, with some processes active on both PGs. See the discussion in Peripheral Gateway Fault Tolerance, on page 26.)

The following figure shows examples of simplexed and duplexed contact center configurations. Typically, duplexed PGs are installed for fault tolerance.

Figure 7: PG Contact Center Configurations


To Central Controller Side A
To Central Controller Side B
IP Router
Visible LAN
Peripheral Gateway
ACD
Administration & Data Server
Simplexed PG
To Central Controller Side A
To Central Controller Side B
IP Router
IP Router
Visible LAN
Private LAN
PG1A
PG2B
ACD
Administration & Data Server
Duplexed PG

Note Some ACDs can connect directly to the Unified ICM visible LAN. Others connect to the PG via serial or other types of communication links.

The Peripheral Gateway reads information from one or more peripherals at a contact center and sends status information back to the Unified ICM CallRouter. A peripheral can be an ACD, VRU, PBX, or other device that distributes calls within the contact center. If the Unified ICM system is performing post-routing, the PG also sends route requests to the CallRouter and receives routing instructions in response.

- Peripheral Gateway Fault Tolerance, on page 26
- PG Platform Options, on page 28
- Standard PG Configuration, on page 29
- Remote ACD and VRU Connection to PGs, on page 30
- Multiple PGs Connecting to Single ACD, on page 31

Peripheral Gateway Fault Tolerance

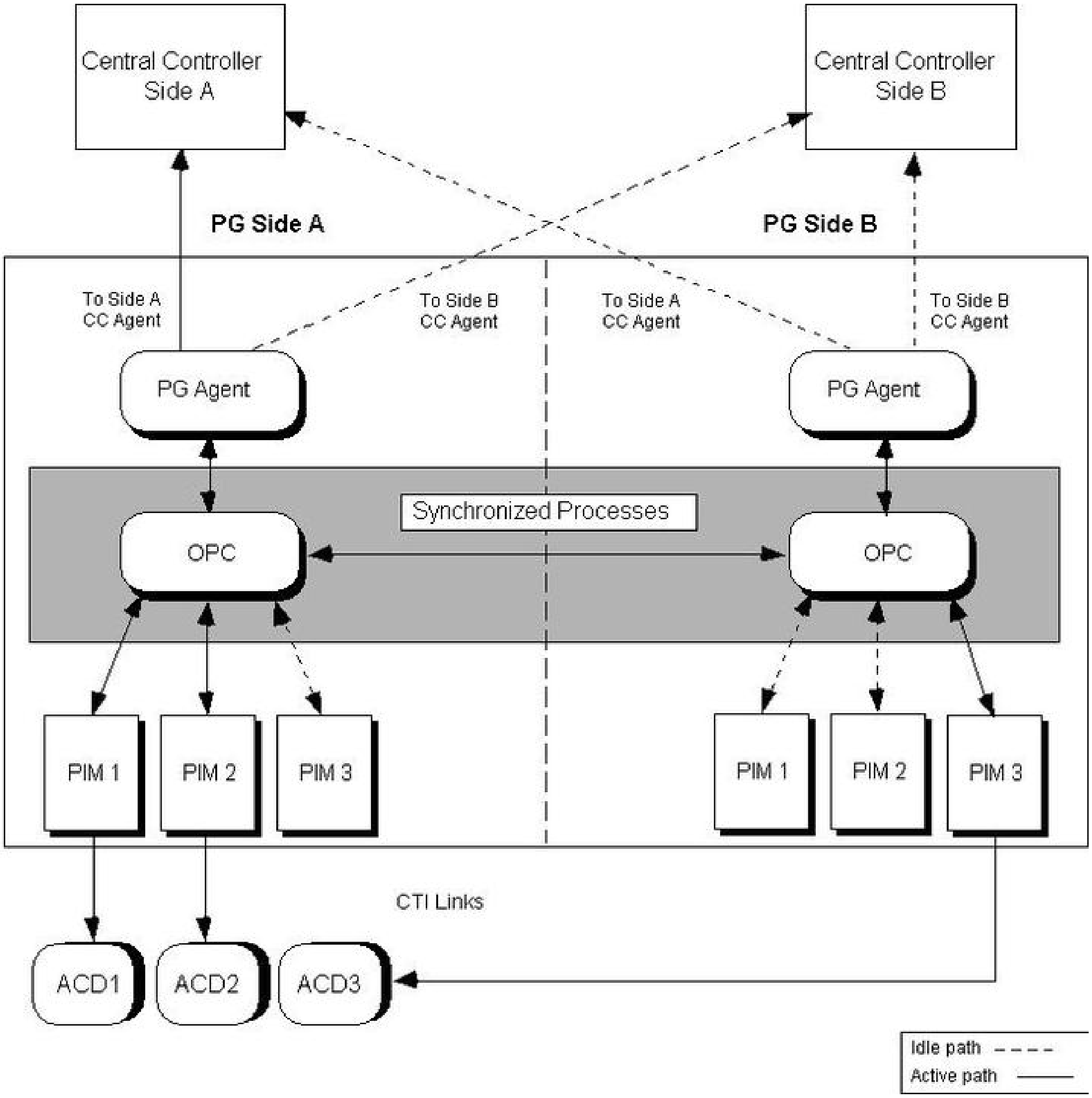
Duplexed PGs are implemented to provide fault tolerance in Unified ICM software communication with peripherals. The duplexed PGs use a private network. The PG private network synchronizes certain processes within a duplexed PG pair. It also conducts “heartbeat detection”, a process by which each PG sends a heartbeat packet every 100ms to keep track of the “health” of the other PG.

PGs use a combination of the hot standby and synchronization approaches to fault tolerance. In the hot standby approach, one set of processes is called the primary, and the other is called the backup. In this model, the primary process performs the work at hand while the backup process is idle. In the event of a primary process failure, the backup process is activated and takes over. In a duplexed PG system, the Peripheral Interface Manager (PIM) processes use the hot standby approach to fault tolerance.

In the synchronization approach, the critical process is duplicated on separate computers. There is no primary and backup. Both process sets run in a synchronized fashion, processing duplicate input and producing duplicate output. Each synchronized process is an equal peer. Cisco refers to these equal peers as a synchronized process pair. In a duplexed PG system, the Open Peripheral Controller (OPC) process operates as a synchronized process pair.

The following figure shows how to use hot standby and synchronization in a duplexed Peripheral Gateway.

Figure 8: PG Fault Tolerance ACD2PG



The OPC processes communicate with each other through a private network connection and the Cisco Message Delivery Service (MDS). The MDS provides a synchronizer service which combines the input streams from the PIMs and PG Agents on both sides of the PG to ensure that both OPC processes see exactly the same input.

The OPC process activates PIMs and PG Agents on each side of the duplexed PG. The OPC process also supplies uniform message sets from various PG types to the Unified ICM central controller.

The PIMs manage the interface between different types of ACDs and the OPC. PIMs are duplicated on each side of the system and operate in hot standby mode. A PIM can be active on either side of the duplexed PG, but not on both sides at the same time. For example, in the preceding figure PIMs 1 and 2 are active on Side A; PIM 3 is active on Side B. The duplexed OPCs communicate with each other through the MDS to ensure that a PIM is active only on one side at a time.

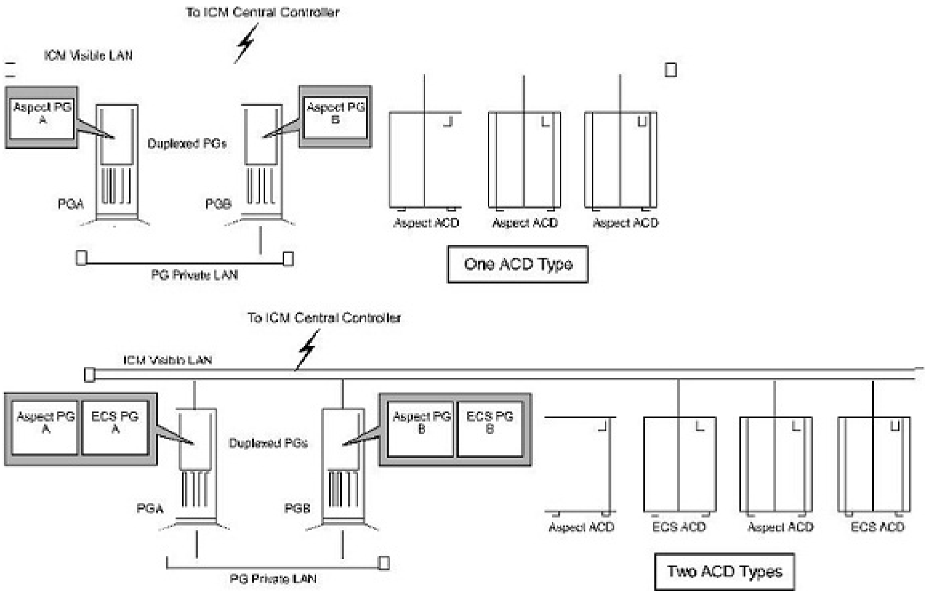
The duplexed PG architecture protects against a failure on one side of the PG. For example, if an adapter card controlling access to an ACD fails, a hot standby PIM can use the alternate PIM activation path. As shown in the preceding figure, PIM3 was activated from Side B of the PG. This might be in response to an adapter failure between the Side A PIM3 and ACD3. In this type of failure scenario, the PG can maintain communication with the attached ACD.

Only one PG Agent actively communicates with a side of the central controller. When messages arrive at the central controller, they are delivered to both sides by the central controller Synchronizer process. The PG maintains idle communication paths to both sides of the central controller in case a switch-over to the other side of the central controller or PG is necessary.

PG Platform Options

A maximum of two PGs can run on a single hardware platform. A single PG can serve only one type of ACD, but can also contain one or more VRU PIMs and/or Media Routing PIMs provided that the server hardware has the capacity to support the aggregate processing load. For a single hardware platform to serve two different types of ACDs, you need two PGs—one for each peripheral type. The following figure shows some possible PG options.

Figure 9: PG Platform Examples



As shown in the preceding figure, you can have an Aspect PG on PGA and an Aspect PG on PGB. This duplexed PG pair can serve multiple Aspect ACDs. One Aspect Peripheral Interface Manager (PIM) is added through Peripheral Gateway Setup to connect each Aspect ACD to this PG. In this example, three Aspect PIMs are installed on each PG. The PIM is the Unified ICM software interface between the PG and different types of contact center peripherals. One PIM is required for each peripheral connected to a PG.

In a mixed contact center environment, you may want to run two different types of PGs on a single hardware platform. For example, you may want to put an Aspect PG and a DEFINITY ECS PG on the same computer. In this way, one hardware platform can serve two types of ACDs provided that the hardware platform has the necessary memory and CPU capacity to support the aggregate processing load.

Considerations for PGs and PIMs

Consider the following points when you plan for PGs and PIMs:

- Maximum PGs on a platform. A maximum of two PGs can run on a single server platform. These PGs can be the same or different types. For example, on a single machine you can have an Aspect PG and an Avaya PG, or you can have two Avaya PGs.
- PIMs and peripherals. You need one PIM for each peripheral connected to the PG. The PIMs are installed with the PG software using the Peripheral Gateway Setup tool.
- A single PG serves peripherals of the same type. A single PG (and its associated PIMs) can serve only ACDs of the same type. For example, an Aspect PG with four PIMs can serve only four Aspect ACDs. It cannot serve three Aspect ACDs and an Avaya DEFINITY ACD. You can put VRU and Media Routing PIMs on the same PG as an ACD, but all VRU PIMs must service VRUs of the same type.
- Using two PGs on a platform. Before you commit to installing two PGs on a single VM, consider the expected call load for the ACDs connected to the PGs.

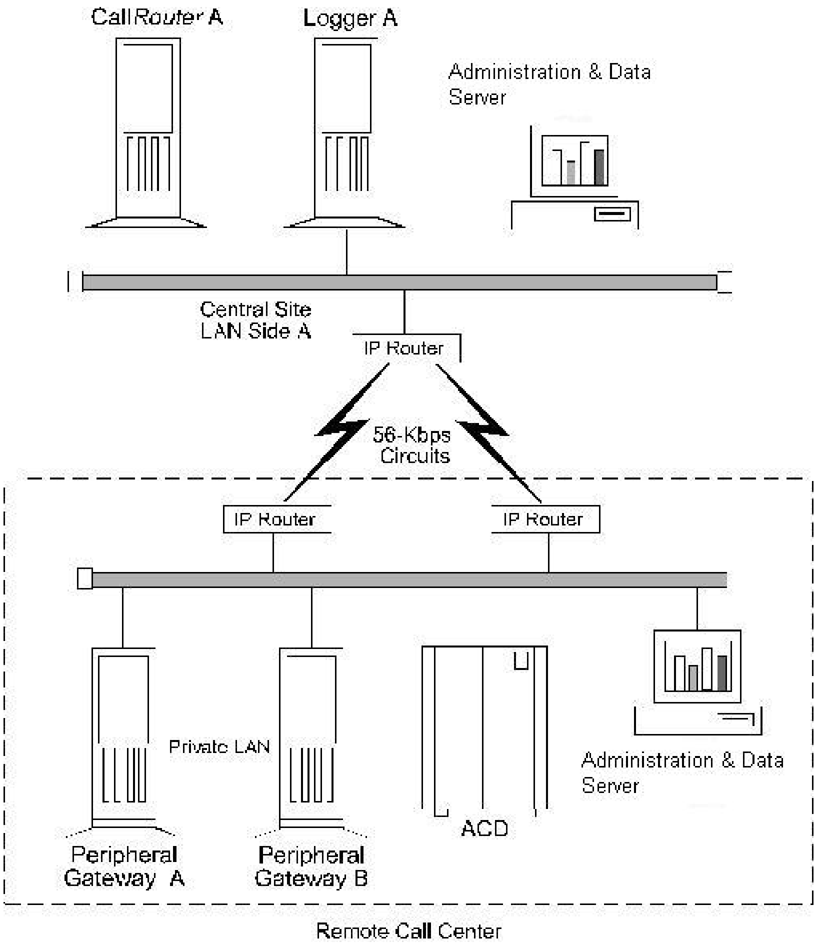
  Note Also consider the number of CTIOS agents and number of VRU ports as factors in determining server capacity.

  Be sure that the VM has enough memory and processing power to handle the expected call load. In addition, ensure that the bandwidth in the network between the PG and the Unified ICM central controller can handle the route request and event traffic generated by the PGs. (These same considerations apply when using multiple PIMs on a PG, but to a lesser extent.)
- **Properly sizing the PG server platform.** See the Design Guide to properly size the PG server platform and to determine which PG configuration is appropriate for your application.
- **CTI Server and an ACD PG on the same platform.** Install CTI Server and an IVR or ACD PG on the same server platform. The PG can run multiple PIMs. (The same considerations described earlier in “Using two PGs on a platform,” also apply to the CTI Server-PG configuration.)
- **UCCE Gateway.** In Unified ICM Enterprise, the UCCE Gateway PG allows the Unified ICM to pre-route calls to Unified CCE call centers and can also post-route Unified CCE calls. The UCCE Gateway feature allows Unified CCE or Unified CCX to act as enhanced ACDs connected to the Unified ICM. Refer to the for more information.

Standard PG Configuration

In most PG configurations, the PG is located with the ACD at a contact center site. The PG communicates with the central controller via the Unified ICM visible network WAN links. These WAN links can be a dedicated circuit, or—if Quality of Service (QoS) is implemented—the corporate WAN. When Administration & Data Servers are located with PGs and ACDs at the contact center site, both PGs and Administration & Data Servers can share the WAN links to the central controller. If the PG is collocated with the Unified ICM central controller, the PGs connect directly to the Unified ICM visible LAN. The following figure shows an example of a standard PG configuration.

Figure 10: Standard PG Configuration (Duplexed PGs)



Remote ACD and VRU Connection to PGs

Some ACDs allow a remote connection to the Unified ICM Peripheral Gateway. In a remote ACD configuration, the PGs are located at the central site along with the CallRouter, Logger, and NIC. The ACD is located at a remote contact center site.

For information on remote PG support, see the ACD Supplement for the particular ACD. Usually Alcatel, Aspect, Avaya, Avaya ACC ACDs are supported over the WAN. However, in all cases, you must check with the ACD manufacturer for any WAN limitations.

The VRU PG can communicate remotely with VRU's via a TCP/IP network. However, you must ensure that the network link between the PG and VRU system provides enough bandwidth to support the call load for the VRU.

Multiple PGs Connecting to Single ACD

Connecting multiple PGs to the same ACD is required when multiple Unified ICM customers need to share the same service bureau ACD. For this configuration to be possible, the ACD must allow multiple CTI applications to share its CTI link(s). Support for multiple PG connections varies depending on the ACD platform. See the appropriate Cisco Unified ICM software ACD Supplement and contact your ACD vendor to determine the availability of this functionality.

CHAPTER 6

CTI Planning

Cisco CTI software provides an interface between the Unified ICM software and agent desktop and server applications. The CTI software works with a Peripheral Gateway's ACD and VRU interface software and associated ACDs to track call events and transactions and forward call- and transaction-related data to an agent's desktop computer.

Pre-installation planning for CTI involves several tasks:

- Review CTI Server communications and platform options.
- Become familiar with the desktop options available with CTI Server.
- Estimate CTI message traffic.
- Plan fault tolerance for the CTI Server.
- Review ACD support for client control and third-party call control.

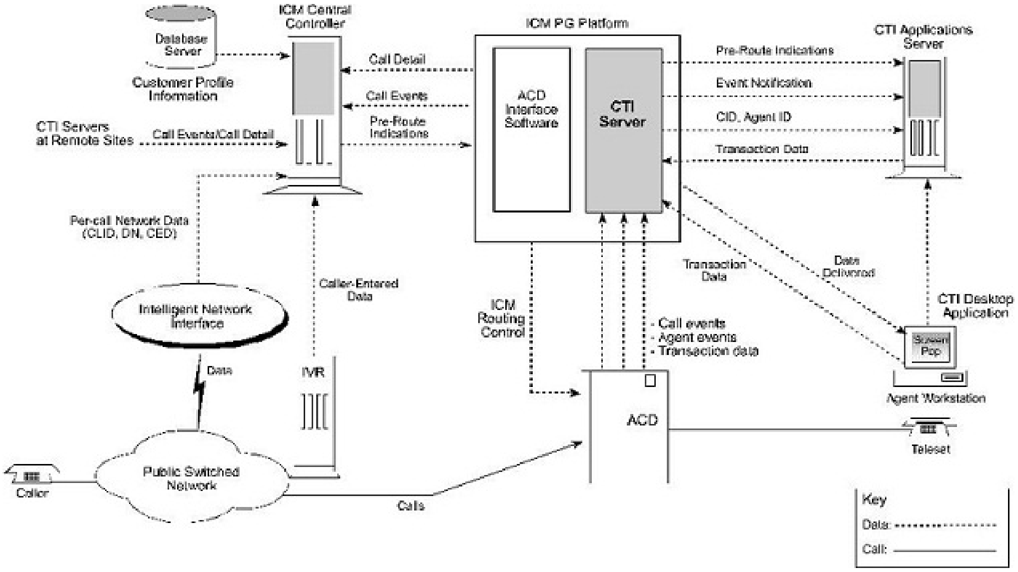
- CTI Server, on page 33
- CTI Server Client Application Models, on page 37
- CTI Server Network and Database Planning, on page 38
- CTI Server Messages, on page 39
- Third-Party Call Control, on page 41
- ACD Support for Client and Third-Party Call Control, on page 42

CTI Server

CTI Server, the basic server component of Cisco CTI, enables the Unified ICM software to deliver agent, call, and customer data in real-time to a server and/or workstation application as events occur throughout the life of a call. The CTI Server is a software process that runs on a Peripheral Gateway (PG). It is the CTI gateway into the Unified ICM software's data and services.

The following figure shows a sample CTI Server system. CTI Servers may be running at one or several call centers in the enterprise.

Figure 11: CTI Server Overview



One function of the CTI Server is to forward pre-route indications to CTI application servers. Pre-route indications identify the caller and provide CTI applications with other call attributes while the call is still in the public or private network (that is, before the call is connected to an agent or IVR resource).

CTI Server also reports call events and agent work state changes as they occur through each stage of the call flow—from the moment a call arrives at an answering resource (ACD, PBX, IVR), until the caller hangs up. In a desktop application environment, call event information is delivered to the targeted agent desktop at the same time the call is delivered.

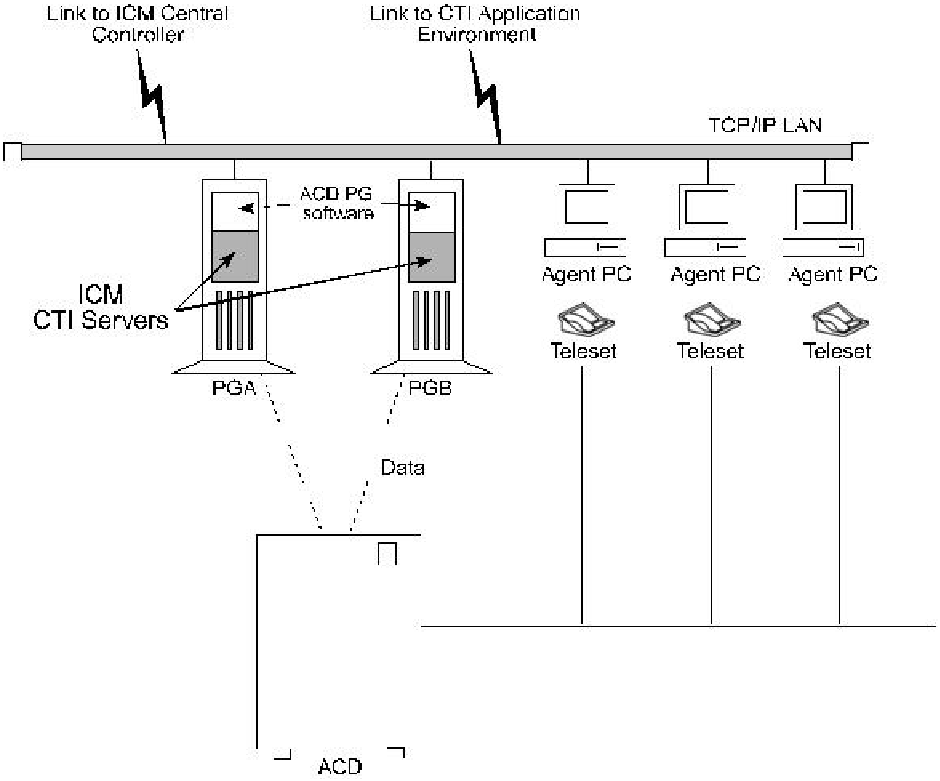
CTI Server Communications

The CTI Server uses TCP/IP Ethernet for communication with clients. You can use multi-protocol IP routers to provide connectivity to clients on other types of LANs. You can use the same LAN for the Peripheral Gateway's visible network interface and for CTI client-to-server communications.

CTI Server Platform Options

The CTI Server runs on a machine that is also running a Cisco ACD (or VRU) PG process. The shared platform option is shown in the following figure.

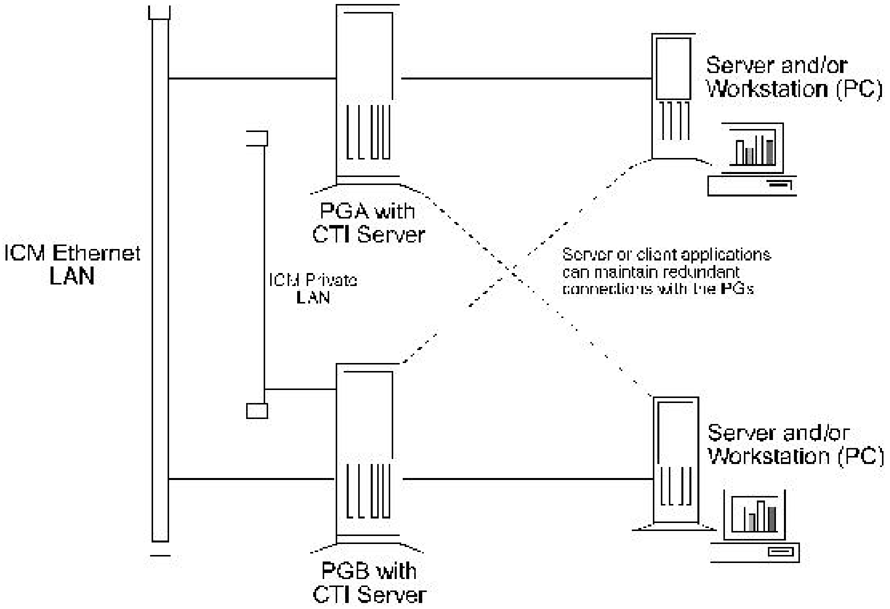
Figure 12: Shared CTI Server Platform



CTI Server Fault Tolerance

You can implement the CTI Server in a duplexed, fully fault-tolerant configuration. In a duplexed configuration, the CTI Server is installed on a pair of server platforms. In the event of a failed CTI client connection, the client process can automatically reestablish a connection to either side of the duplexed CTI Servers. The call's CTI client history list and any updates to call variables remain in effect when the connection is reestablished. The following figure shows a duplexed CTI Server configuration.

Figure 13: Duplexed CTI Server


Server and/or Workstation (PC)
PGA with CTI Server
ICM Ethernet LAN
ICM Private LAN
Server or client applications can maintain redundant connections with the PGs
Server and/or Workstation (PC)
PGB with CTI Server

Cisco CTI Object Server (CTI OS)

CTI Object Server (CTI OS) is a high-performance, scalable, fault-tolerant server-based solution for deploying CTI applications. CTI OS serves as a single point of integration for third-party applications, including Customer Relationship Management (CRM) systems, data mining, and workflow solutions.

Configuration data is managed at the server, which helps simplify customization, updates, and maintenance of CTI applications. You can access and manage servers remotely. Thin-client and browser-based applications that do not require Cisco software on the desktop can be developed and deployed with CTI OS.

CTI OS incorporates the following major components:

- CTI OS Toolkit
- Client Interface Library
- CTI OS Combo Desktop for Agents and Supervisors

CTI OS is a client of CTI Server. It has a single all-events connection to Cisco CTI Server. In turn, CTI OS accepts client connections using session, agent, and call interfaces. These interfaces are implemented in .NET, COM, Java, C++, and C, allowing for a wide range of application development uses. The interfaces are used for call control, to access data values, and to receive event notifications.

For complete and current information about the number of agents supported for CTI OS and other configurations, see the at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html. See at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html for hardware requirements for Unified CCE virtualized systems.

For all installations, the CTI OS Server must be co-resident with the PG.

For more information on CTI OS, refer to the CTI OS document set.

CTI Server Client Application Models

You can use either of two client models to integrate call center applications with the Unified ICM: agent workstation and CTI Bridge.

Agent Workstation Application

In the agent workstation model, the client is an application running on a personal computer on an agent's desktop. This client is interested in the call data and call events related to a single agent teleset. The agent workstation application can also be interested in agent state changes.

Typically, when the agent workstation application is informed of an incoming call, it uses the call data collected by the Unified ICM system to retrieve caller-specific data from a database. This data is presented on the agent workstation screen at approximately the same time that the incoming call is connected to the agent.

While handling the call, the agent can update some of the call data. For example, an agent who is processing an insurance claim can make some adjustments to the call data; an update ensures that the changes are not lost before the call is transferred to a second agent.

Upon completion of the call, the agent can use the client to add call-specific, wrap-up information to the Termination_Call_Detail record logged in the Unified ICM central database. This wrap-up data is a key value that can help locate more detailed transaction information in some other database. If the agent conferences with or transfers the call to another agent on the same ACD with a CTI client workstation, then that agent's CTI client also receives the incoming call data, including any updates made by the first agent. If the transfer or conference involves an agent on another ACD, the call data is provided to the remote CTI client if a translation route is used.

CTI Bridge Application

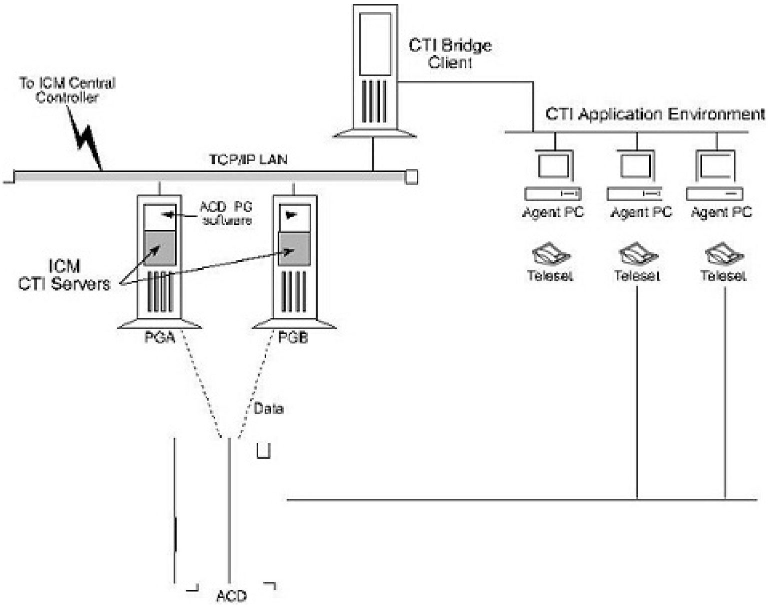
CTI Bridge applications are interested in all call and agent state events that occur on the ACD, unlike agent workstation applications that are interested only in the events associated with a particular teleset. The CTI Bridge application is a user-written program that converts or adapts some or all of the CTI Server messages into another format; a single CTI Bridge application provides such services for multiple agent desktops. You can design the CTI Bridge application to interface with CTI Servers or similar applications on systems that are already in use in the call center.

Some examples of CTI Bridge applications include:

- Message converter applications. For example, an application can convert the CTI Server message set to the message set of a foreign telephony server.
- Server-to-server communication applications. For example, an application can enable the CTI Server to speak directly to a help desk application's middle tier server.

  In a CTI Bridge configuration, a CTI Bridge application provides the connection between an existing desktop CTI application and the Unified ICM.

Figure 14: CTI Bridge Model



Note All of the functionality found in the agent workstation (desktop) model is also available in the CTI Bridge application model. However, you must write the CTI Bridge application to support this functionality.

CTI Server Network and Database Planning

Some pre-installation planning is necessary to prepare your CTI desktop and network environment for the introduction of a CTI Server.

Network Topology

The machine running CTI Server connects to the CTI desktop environment via an Ethernet LAN. Therefore, the CTI desktop environment must reside on an Ethernet LAN. Other networks, such as Token-Ring, can require additional network hardware if you are connecting them to a CTI Server.

Network Security

Be sure that the CTI desktop environment IP routing scheme is compatible with the Unified ICM system and CTI Server. For example, if you have a firewall set up on the CTI environment LAN, you may need to change your system access setup or network configuration.

Software Distribution Strategy

If you are installing the CTIOS or CTI Desktop software components on multiple desktops, you must create a distribution strategy. For example, if you place the software on a centralized server and allow certain desktops within the enterprise to download the software, you must ensure that all sites have access to the centralized server.

Well-Known Port for CTI Server

A well-known port number identifies CTI Server as an application running in your intranet. All CTI clients, as well as the system administrator, must know this well-known port number. If you do not want to use CTI Server's default port numbering scheme, you can choose a well-known port number that fits into your overall network environment. You can use the Peripheral Gateway Setup to override the default port settings used to install the CTI Server PGs.

Fail-over Strategy for CTI Clients

Cisco CTI includes automatic fail-over and recovery mechanisms. Ensure that each CTI client has a clear and established network path to a CTI Server in case of a fail-over. For example, you may plan for each CTI client to have access to local and remote CTI Servers.

Database Strategy

You may have CTI applications that perform database queries to retrieve customer information for use in call processing. Some CTI applications acquire database records “pre-call” (that is, before the call arrives at an agent's desktop). Other applications query a database immediately after the call arrives at the agent's deskset. Plan a strategy for executing database queries in the most efficient and timely manner possible.

CTI Server Messages

The CTI Server makes traffic call data available to applications in real time. To accomplish this task, the CTI Server responds to requests from clients and originates unsolicited messages. All messages share a common message header and use the same set of data types.

The table titled **CTI Server Message Categories** groups the messages into broad categories based on the nature of the message data.

Table 1: CTI Server Message Categories

Category	Description
Session Management	Messages related to the establishment and maintenance of a client connection to the CTI Server. These messages typically happen at client startup, shutdown, and during auto-recovery.
Miscellaneous	Messages related to system-level events on the PG (for example, peripheral offline, loss of PG-to-central controller communications).

Category	Description
Call Events	Messages related to call state changes.
Agent Events	Messages related to agent state changes.
Call Data Update	Messages related to CTI client modification of call data.
Client Control	Messages related to the direct control of agent state (for example, sign-in, sign-out) as well as control of inbound and outbound calls.

CTI Server imposes varying degrees of message traffic against the PG based on the specific call center and CTI application environment in which it is deployed. Document a typical call scenario in your CTI application environment, prepare for adequate bandwidth, and order the proper server platform.

Note For a description of the session management messages, see the latest version of the for more information..

Typical Call Scenario

To estimate CTI Server message traffic, document a typical call scenario in your CTI application environment. The goal of this exercise is to account for all types of potential message traffic in the link between the CTI Server and the CTI application environment.

For example, you can handle a typical call as follows:

- The call is pre-routed.
- The call receives a call treatment such as a request to set call data.
- A simple call release, hold, transfer, or post-route request takes place.
- During this time an agent state may change (for example, from ready to work ready).

Message Load and Bandwidth

Ensure that you have enough bandwidth in the datacom connection to handle the message traffic between the CTI Server and the CTI application environment. For example, are you sure that a 56-Kbps connection is adequate for your environment?

The call scenario process helps you to estimate the message load and calculate how much bandwidth is required in the link between the CTI Server and the CTI application environment (for example, 56K, 256K, or more).

CTI Server Platform

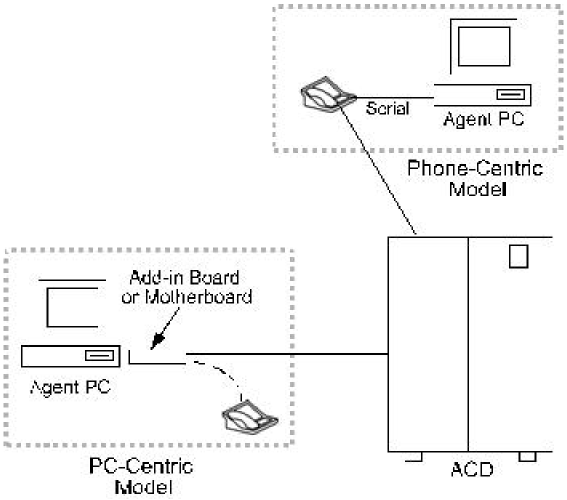
Ensure that the CTI Server platform has adequate CPU processing speed and RAM to handle the message activity. You may require a high-end Cisco CTI Server/PG platform for the CTI Server.

Third-Party Call Control

Call control is the ability of an application that is external to the ACD to programmatically control a telephone call. For example, a CTI application can put a call on hold, transfer the call, or hang up the call.

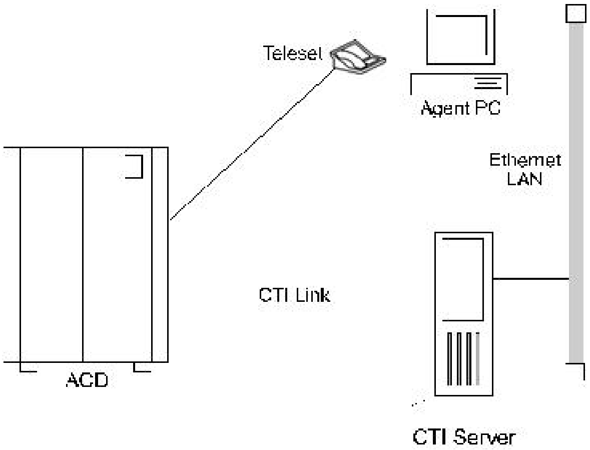
With first-party call control, the CTI application can control only the teleset that is physically connected to the computer running the CTI application. First-party call control requires a physical connection between the computer and the telephone and other add-on hardware (see the following figure).

Figure 15: Desktop First-Party Call Control



CTI Server products support third-party call control. Any call control initiated outside the ACD/teleset domain is referred to as third-party. With third-party call control, there is no physical connection between the computer and the teleset (see the following figure).

Figure 16: Desktop Third-Party Call Control



The desktop CTI application communicates with the Cisco CTI Server over a LAN. The CTI Server in turn communicates with the ACD to send call control requests. In this model, the CTI application is not bound to any particular teleset. The CTI application can control any teleset connected to the ACD and CTI Server.

Note Most, but not all, ACDs support third-party call control.

Depending on the specific ACD, the client application can perform all or most of the following telephony functions:

- Answer/Hang up
- Agent Login and Wrap-up data
- Consultative/Blind Conference
- Consultative/Blind Transfer
- Generate DTMF tones
- Get/Set Agent states
- Get/Set ICM call data (ANI, DNIS, CED, UUI, call vars)
- Hold/Unhold/Swap Hold
- Make a call
- Redirect

ACD Support for Client and Third-Party Call Control

Different peripheral types implement and support varying levels of CTI functionality. For example, a different set of client control requests and call event types are available depending on the peripheral type. In addition, there can be other CTI-related restrictions and implementation differences based on the type of peripheral. Consider these differences when you write a CTI client application that interfaces with third-party switches and devices.

As part of CTI pre-installation planning, review ACD support for client control and third-party call control.

CHAPTER 7

Interactive Voice Response (VRU) Systems

Cisco provides an option for running an interface to Interactive Voice Response (VRU) systems. The VRU interface software allows VRU's to take advantage of Unified ICM call routing features. For example, an VRU can use post-routing capabilities to select targets for calls it needs to transfer. The VRU interface software runs on a standard PG hardware platform. It allows the Unified ICM to route calls to targets on an VRU and collect data from an VRU for use in call routing, real-time monitoring, and historical reporting. The VRU interface is not specific to a particular VRU system or manufacturer. It is based on an open VRU model. Many VRU systems support Cisco's Open VRU Interface Specification, including Unified CVP. For a list of VRU's that support this interface, contact your Cisco representative.

To plan for this VRU option:

- Review the options for integrating VRU's into the Unified ICM system.
- Determine if any VRU programming or application development is necessary.
- Review the Peripheral Gateway platform requirements.

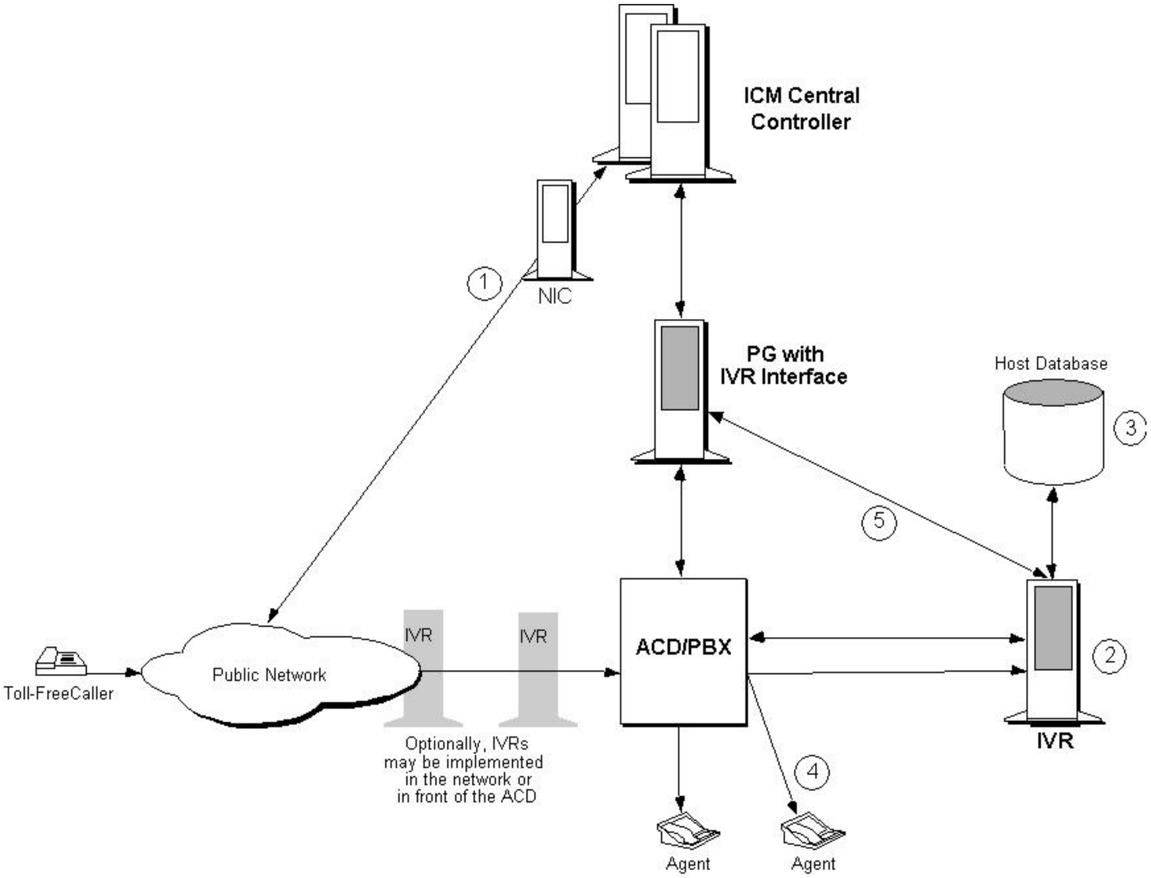
- VRU Configuration Options, on page 43

VRU Configuration Options

VRU's can be located at the customer's call center site or in the IXC network. At the call center, you can connect the VRU on the network side of the ACD or “behind” the ACD. In the IXC network, the network provider can offer the VRU as a service.

In an Unified ICM configuration that includes an VRU, you configure the ACD so that it can transfer calls to the VRU. The following figure shows some of the capabilities of the VRU in an Unified ICM system.

Figure 17: VRU/ICM Integration Overview



Capabilities of VRU:

1. In most Unified ICM /VRU configurations, calls continue to be Pre-Routed by the Unified ICM system.
2. When a call is routed to an VRU, the VRU answers the call and interacts with the caller.
3. The VRU can access a host system (for example, a customer profile database) to retrieve more information to help process the call.
4. Often, the caller can get all the information he or she needs through simple interaction with the VRU. In some cases, however, the VRU needs to transfer the caller to an agent or another call resource.
5. In some configurations, the VRU can invoke post-routing to select an agent from anywhere in the call center enterprise. To do this, the VRU sends a route request to the PG. The PG forwards the request to the Unified ICM system, which responds with a new destination for the call. The PG returns the new destination to the VRU. The VRU then signals the ACD or network to transfer the call to the specified destination.

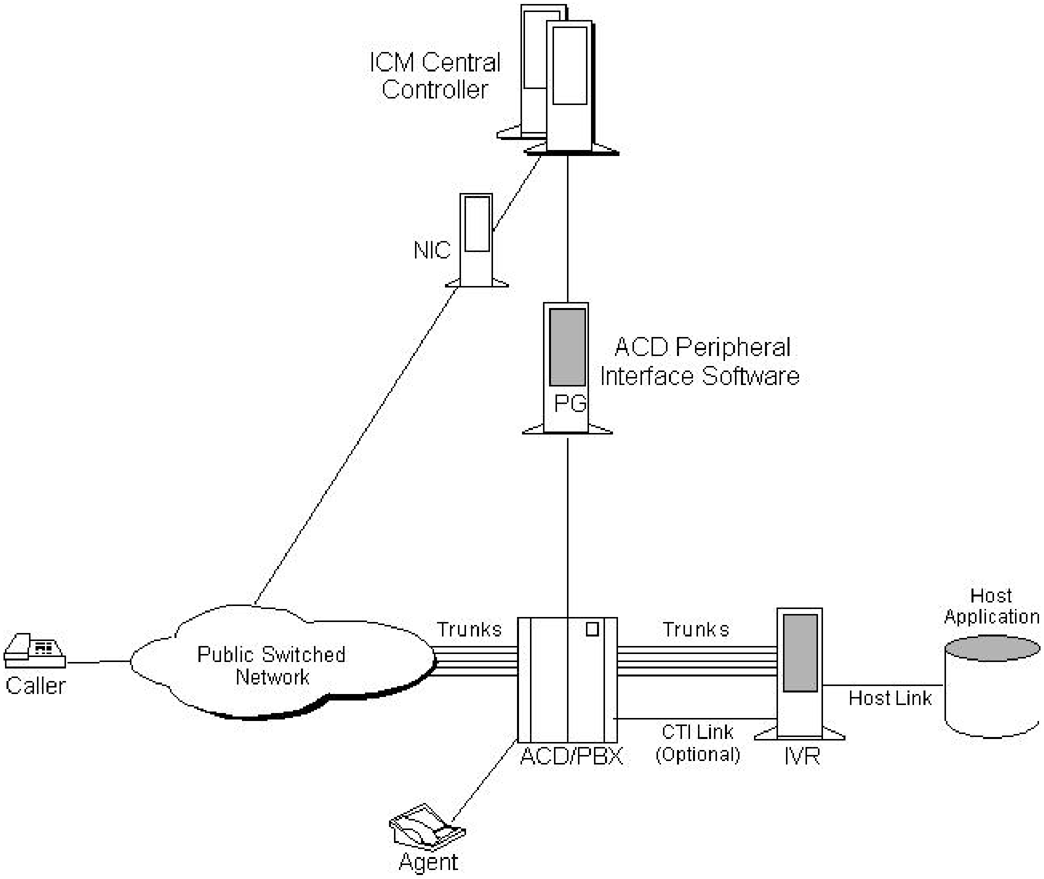
The way in which an VRU is integrated into the Unified ICM system affects the flow of call processing and determines the types of data the Unified ICM can collect from the VRU. For example, an VRU that has a direct interface to an VRU PG provides the Unified ICM system with data that is used in call routing, monitoring, and reporting. A configuration in which the VRU has an interface only to the ACD has more limited capabilities.

You can integrate VRU's into the Unified ICM system in several different ways. Each integration option provides a different set of Unified ICM functionality.

Configuration with ACD PG Only

In this option, the IVR is attached only to the ACD. The ACD, in turn, is attached to a PG. The PG is running the Cisco peripheral interface software (PG software process) required to communicate with the specific type of ACD. There is no direct interface between the IVR and the Unified ICM system (in other words, an IVR process is not implemented).

Figure 18: Configuration with an ACD PG Only



In this configuration, you must connect the IVR to an ACD that supports post-routing. The IVR and ACD cooperate so that calls are transferred from the IVR to the ACD, and then post-routed by the ACD via the PG. The PG in this configuration has only the ACD peripheral interface software. It does not have the IVR interface software; therefore, it does not provide the IVR with full access to post-routing.

In the preceding figure, the IVR can handle a call in two different ways:

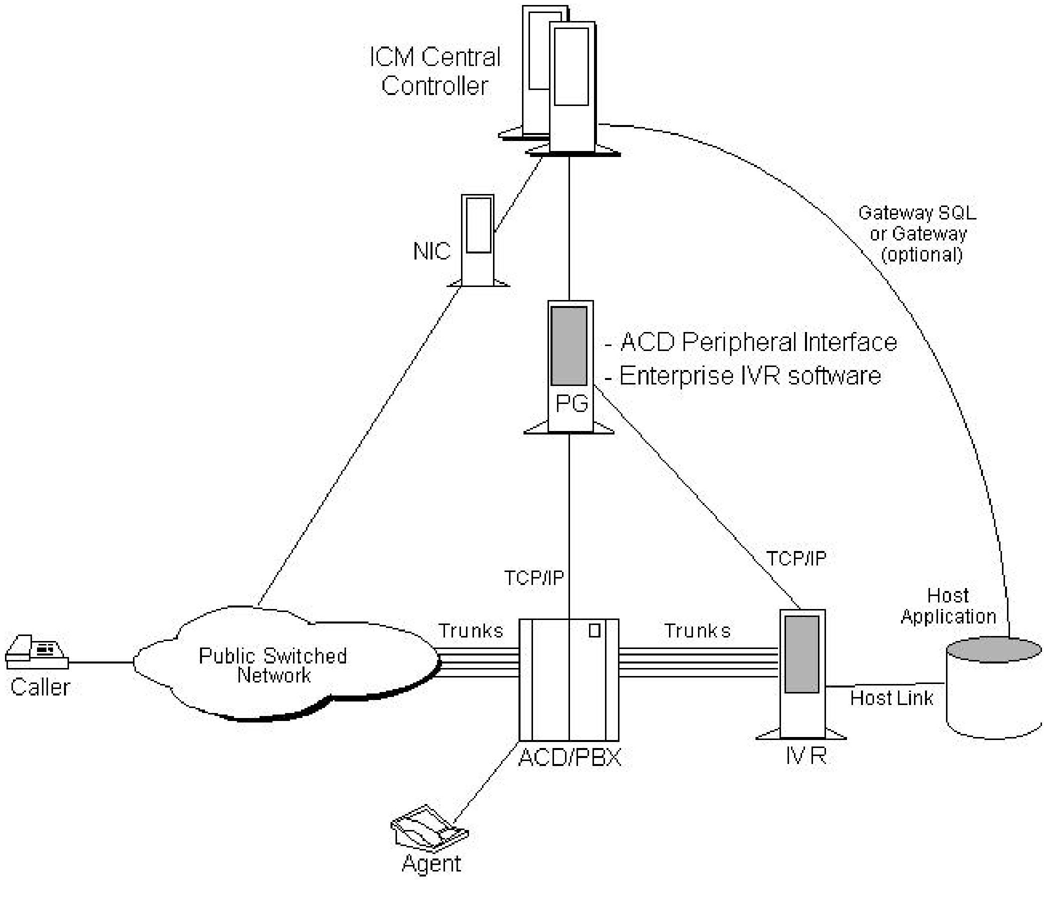
- The IVR can handle the call to completion (for example, if the caller wanted current billing information and needed no further assistance, the IVR can complete the call.)
- The IVR can transfer the call to the ACD. The ACD can then use the PG to post-route the call.

Configuration with IVR and ACD PGs

This configuration option is similar to the previous option except that an IVR process and host link to the IVR are implemented. In addition to monitoring the ACD for real-time agent and call event data, the PG can monitor the IVR for call and application data and control the movement of calls into and out of the IVR. The IVR data is also forwarded to the CallRouter for call routing and reporting.

As shown in the following figure, you can install the IVR and ACD interface software on the same PG hardware platform.

Figure 19: Configuration with IVR and ACD PGs

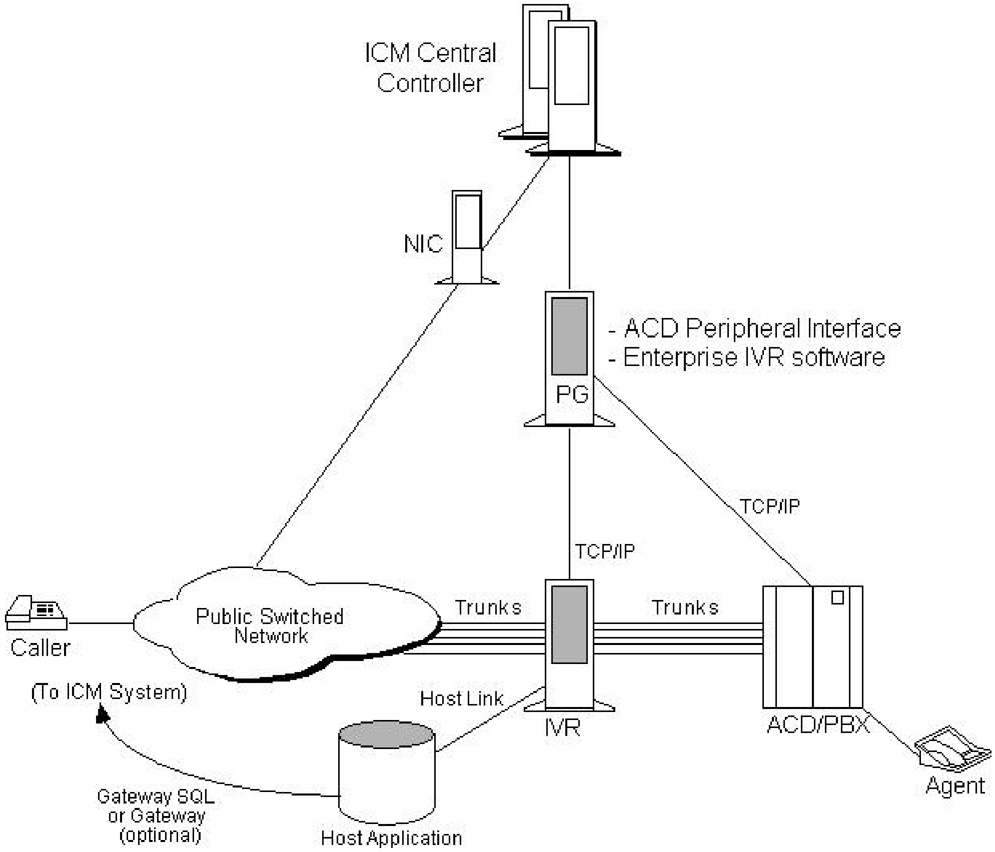


Network-Side VRU with VRU and ACD PGs

The next configuration option places the VRU on the network side of the ACD. In this configuration, the VRU is connected to the network and potentially to the ACD. The VRU can receive calls directly from the network without ACD involvement. The Unified ICM can pre-route these calls, but it is not a requirement.

The VRU can also receive calls from the ACD (for example, when an agent transfers a call to the VRU). Again, the Unified ICM may or may not have routed these calls. The following figure shows an example.

Figure 20: Network-Side VRU with VRU and ACD PGs



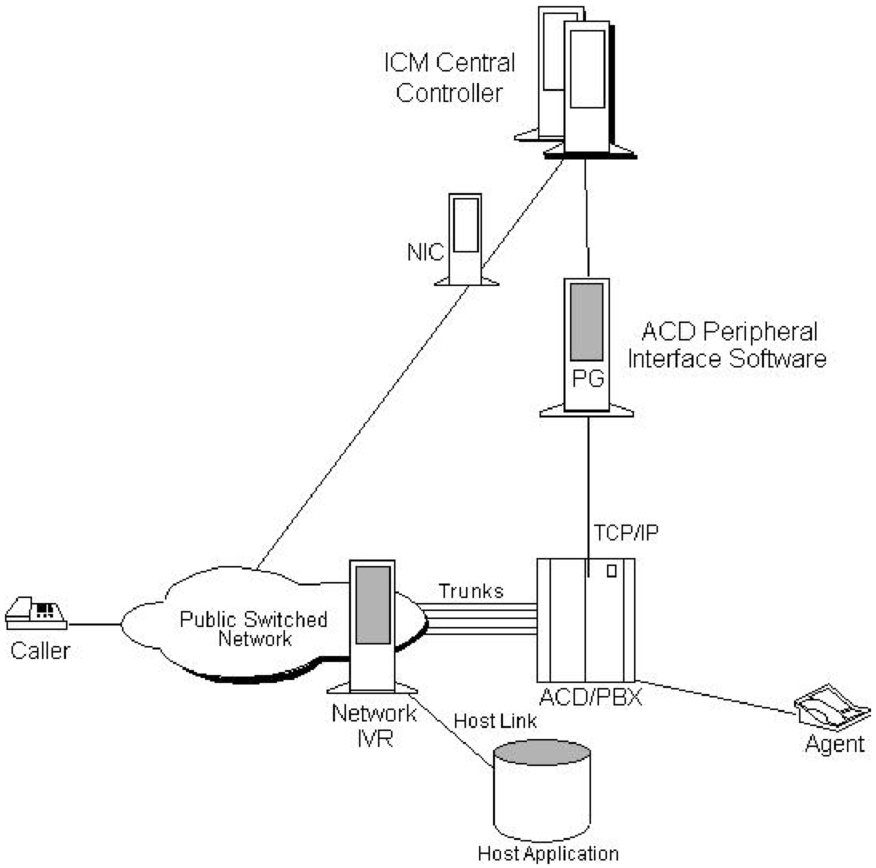
After the VRU receives a call, it handles the call to completion or transfers the call off-VRU for subsequent handling. The VRU can also use post-routing to select a target for the transfer. If the VRU transfers the call to an ACD, the VRU may or may not request routing instructions from the Unified ICM.

This configuration is different from the earlier options in several ways:

- The VRU is connected to both the network and the ACD.
- You can transfer a call that originated in the network to the local ACD by tandem connecting a second trunk with the original trunk. You can transfer a network call to a remote ACD either by connecting a second trunk in tandem with the original trunk, or by invoking a “call take-back” feature in the network.
- You can use post-routing to transfer a call that originated at the local ACD to any target.

In-Network VRU with ACD PG Only

In this configuration, the VRU is provided as a service by the network service provider. The PG monitors the ACD and forwards data to the Unified ICM system for call routing and reporting.

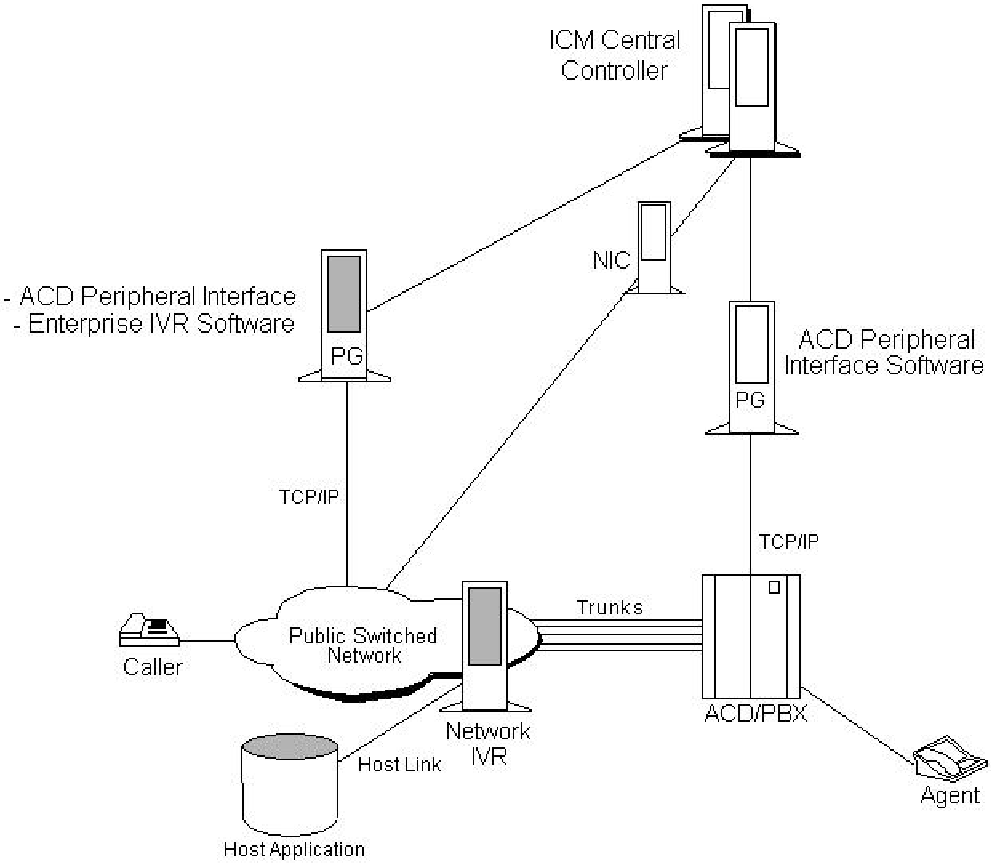


When the caller dials the toll-free number, the Unified ICM instructs the network to transfer the call to the network-based VRU. The network VRU then prompts the caller for input. If the caller requires additional information (such as speaking to an agent), the VRU dials a "hidden" toll-free number. The network then queries the Unified ICM system for a routing destination. The Unified ICM system returns a routing label and the network transfers the call to the specified ACD and DNIS. An agent at the ACD can handle the call to completion or transfer the call for subsequent handling.

In-Network VRU with VRU and ACD PGs

In this configuration, the VRU is provided as a service by the network provider. The network transfers all calls to a destination VRU. The VRU either handles a call to completion or transfers the call to another resource (for example, an agent at an ACD).

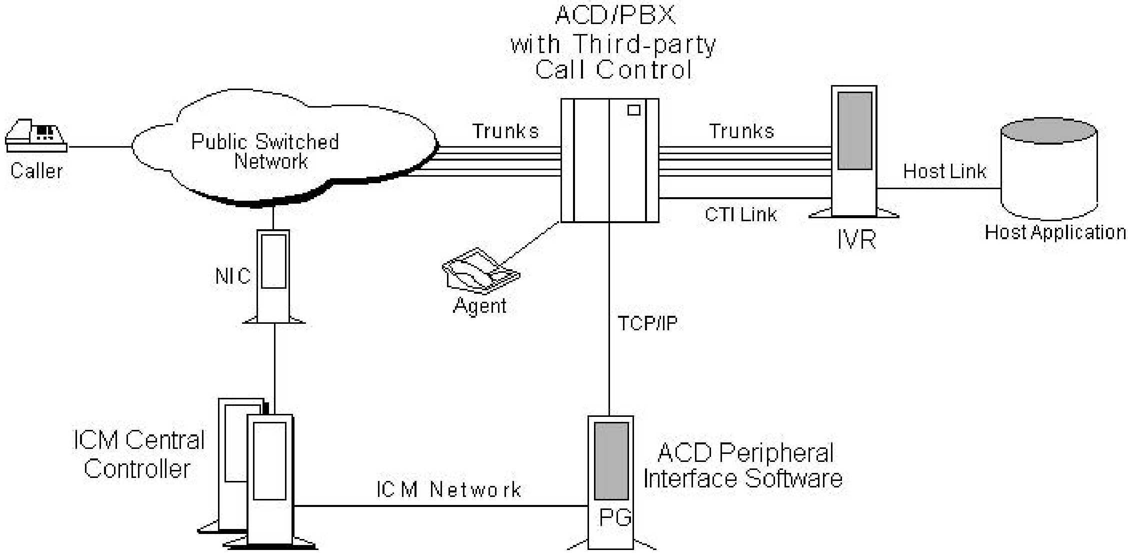
Figure 21: In-Network VRU with VRU and ACD PGs



VRU Transfer Routing Using Third-Party Call Control

In this configuration, the VRU invokes a transfer request to transfer a call to the ACD. The VRU uses a CTI link to the ACD which sets variables in the transfer request (for example, CED, DNIS, CLID, Social Security number, or account number). This configuration is viable only if the VRU is attached to an ACD that supports post-routing. The following figure provides an example of this configuration.

Figure 22: VRU Transfer Routing with Third-Party Call Control



When the ACD receives the transfer from the VRU, it makes a route request to the PG to conduct an enterprise-wide agent selection. The PG routing client sends a route request to the CallRouter. The CallRouter passes a response to the PG and on to the ACD. The ACD then transfers the call to the specified destination.

VRU Programming and Application Development

The Open VRU Interface allows the Unified ICM to see some level of VRU application-specific data (for example, menu selections). An VRU application developer can use the Open VRU Interface to implement call routing (routing client) and monitoring capabilities.

The VRU routing client allows the VRU to send route requests to the Unified ICM via the PG. These requests can include data variables such as Customer ID and Menu Selections. The Unified ICM system uses this data to instruct the VRU where to transfer the call. The application developer uses the VRU monitoring interface to send VRU port and application activity data to the Unified ICM system for call routing and reporting.

VRU Peripheral Gateway

The Cisco VRU interface software runs as a logical PG on a standard Peripheral Gateway hardware platform. A single PG hardware platform can support a maximum of two logical PGs. A single PG platform may run one or two VRU PGs or an VRU PG and an ACD PG. For example, you can have a PG hardware platform that runs an Aspect CallCenter PG and an VRU PG. A logical PG can have PIMs for one type of ACD, plus an VRU PIM. The hardware platform must have sufficient capacity to handle the aggregate load from all attached peripherals.

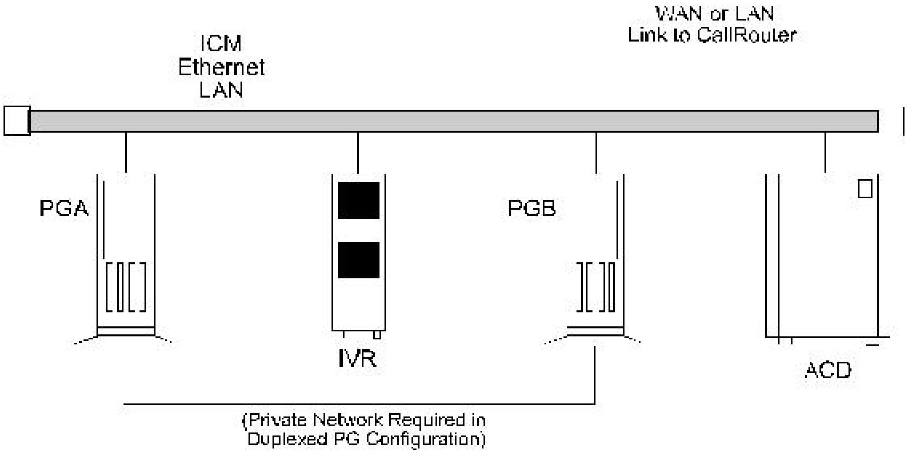
In the following figure, a duplexed set of PGs serve both an VRU system and an ACD system. These PGs are equipped with both ACD and VRU interface software.

Note The VRU can also be on a System UCCE PG or a UCCE Generic PG.

The VRU Peripheral Gateway can run in simplexed or duplexed configurations. In a duplexed configuration, only one side of the PG has an active connection to the VRU at a time.

Note When multiple VRUs are connected to a PG, VRUs that use poll-based monitoring cannot be mixed with VRUs using any other kind of monitoring.

Figure 23: VRU-to-PG Interface



For information on how VRU systems fit into the Unified ICM data communications networks, see Datacom Requirements, on page 65.

CHAPTER 8

ICM Application Gateway and ICM Gateway SQL planning

The Unified ICM Application Gateway and Unified ICM Gateway SQL options allow Unified ICM to integrate external contact center applications into the Unified CCE. Each of these options involves some pre-installation planning. For example, you may need to prepare host systems and databases; review fault tolerance issues; and, in the case of Unified ICM Gateway SQL, plan for data transfer.

- ICM Application Gateway planning, on page 53
- ICM Gateway SQL Planning, on page 54

ICM Application Gateway planning

The Unified ICM Application Gateway option allows the Unified ICM system to interface with any external call center application. Within the Unified ICM software, the Unified ICM Application Gateway feature is implemented as a node in a call routing script. You add a Gateway node to a script to instruct the Unified ICM to execute an external application. This allows the script to evaluate responses from an external application. The Unified ICM can then base subsequent routing decisions on the results produced by the application.

A typical Unified ICM Application Gateway application can return a variable to the CallRouter that identifies the caller as having a certain type of account. The script can then use this information to control where and how the call is routed. Optionally, the Unified ICM software can pass the retrieved information to the site that is receiving the call. In this case, certain data such as account numbers, dates, billing phone numbers, and addresses are passed along with the call to an answering resource.

Host System Preparation

To prepare for the Unified ICM Application Gateway option, you must set up the host system to communicate with the Unified ICM system. This involves configuring the host application to listen to a socket on the target Unified ICM machine. You also need to configure a name and port number to connect the host system to the Unified ICM central database. These steps are performed at system installation; however, you can begin preparing the host applications ahead of time.

During system installation, when connectivity between the Unified ICM system and host system is established, you must identify the host system to be queried by entering data in the Application_Gateway table.

Fault Tolerance

You can configure access to a single host application or duplicate host applications. In a single host configuration, configure the same host for both CallRouters (Side A and Side B). The single host method provides no protection against host failures; however, it does protect against connection failures.

In order to achieve a higher level of fault tolerance in an Unified ICM Application Gateway application, you can connect duplicate host applications to the CallRouter. For example, the Side A and Side B CallRouters can each manage a connection to one of the duplicated host applications. Each time a script initiates a request, both CallRouters query their corresponding host. The CallRouters use the response from the host that responds first. This method is highly reliable. Even if a host or a connection fails, all query requests are satisfied.

ICM Gateway SQL Planning

The Unified ICM Gateway SQL option allows the CallRouter to query an external Microsoft SQL Server database and use the data in call routing.

Note Before implementing the Gateway SQL and DB Lookup functionality, consider a Unified CVP VXML Application for database lookup instead. The DB Lookup node will interrupt routing while doing it's queries. The Unified CVP VXML Application will scale well.

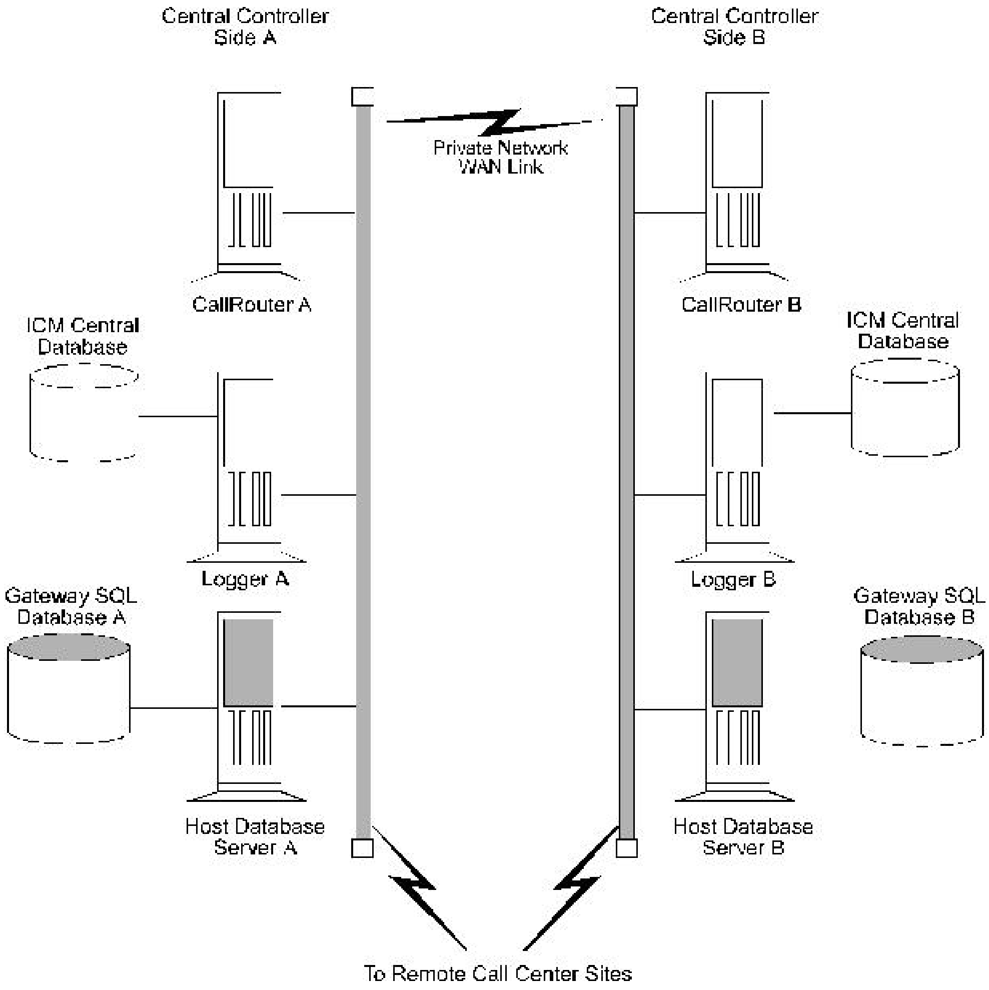
If you are going to use the Gateway SQL option, you need to review several pre-installation planning issues:

- Unified ICM Gateway SQL requires an additional Database Server hardware platform.
- Know the tasks involved in setting up the external host database and populating it with the data you want to use in call routing.

Database Server Platform

The Unified ICM Gateway SQL option requires a host database server. Duplex the host database server to maintain Unified ICM fault tolerance. A duplexed Unified ICM Gateway SQL system requires two identical host database server platforms. Each host database server resides on the same LAN segment as its corresponding Unified ICM CallRouter. The following figure shows a duplexed Unified ICM system that has a duplexed Unified ICM Gateway SQL host database server.

Figure 24: ICM Gateway SQL Duplexed Configuration



Data Transfer

To prepare an Unified ICM system for Unified ICM Gateway SQL, you need to make several decisions:

Decide which data you want to use in the external database. For example, will you be using:

- Customer records?
- Account information?
- Other types of data?

Decide where the data is coming from:

- Another database?
- A flat file?
- Other sources?

Make a plan to transfer the data to the external database:

- What type of media will you use to transfer the data (tape, disk, network)?
- Will the transferred data be in a certain format (comma-separated values, text file, Microsoft SQL Server syntax)?

Database Configuration Overview

For Unified ICM Gateway SQL, you must set up and configure one or more host databases to function with the Unified ICM system.

Configuration considerations include:

- Choosing a host database server platform. The host database server must have adequate processing power and disk space. Cisco can provide you with specifications for basic and high-end host database server platforms.
- Setting up the host database. This includes:

  Installing a Microsoft SQL Server

  - Creating a database on the host database server platform
  - Defining fields and indexes
  - Setting up permissions and replication

- Transferring data from a data source. Transfer data to populate the database with the data to be used in call routing (for example, you might want to transfer customer records to the database).
- Configuring the Unified ICM system to access the host database. Set up user names and passwords that the Unified ICM system can use to access the data in the host database.
- Writing test scripts to test the Unified ICM Gateway SQL option. Monitor test scripts that use the Script Editor DB Lookup node. The monitoring results are captured and stored in the Route_Call_Detail table to validate that the Unified ICM Gateway SQL feature is functioning.

CHAPTER 9

ICM Platform Planning

After you have the system sizing considerations, you can begin to order the appropriate server configuration. First, however, determine how many Unified ICM nodes you need.

The number of servers required in a Unified ICM system depends on the configuration of the central controller, PGs, NICs, and other nodes. For example, a duplexed central controller configuration requires more servers because the CallRouter and Logger are duplicated.

Note All contact center enterprise solutions must now run on virtual machines, they are no longer supported on bare hardware. For hardware requirements for Unified CCE virtualized systems, see the at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html and at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

- Number of Servers Required, on page 57
- ICM Platform Considerations, on page 58
- Historical Data Servers, on page 61

Number of Servers Required

The following table shows how to determine the number of servers required in your system.

The counts of servers in this example are based on an Unified ICM configuration that has the following characteristics:

- The Unified ICM system has a duplexed, geographically distributed central controller (in other words, each central site has a CallRouter and a Logger).
- One side of the central controller (Central Site 1) is located at a call center and consequently has a PG to serve one or more ACDs. The PG is duplexed (two servers) for fault tolerance.
- This Unified ICM installation has three remote call center sites and two Admin sites.

Table 2: Sample Server Requirements

Sites	**Node Types**					
	CallRtr	Lgr	Call/Lgr	DB Server	PG	Administration & Data Server with HDS
Central Site 1	1	1	-	-	2	1
Central Site 2	1	1	-	-	-	1
Remote Call Center 1	-----	-----	-----	-----	2	-
Remote Call Center 2	-----	-----	-----	-----	2	-
Remote Call Center 3	-----	-----	-----	-----	2	-
Admin Site 1	-----	-----	-----	-----	-----	1
Admin Site 2	-----	-----	-----	-----	-----	1
Total Nodes:	2	2			8	4
Key:		--------- These servers are not installed at this type of site. – Not selected as an option in this particular configuration.				

ICM Platform Considerations

For information on server configurations and examples of supported server platforms, see at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Processor Utilization

Note Required only in ICM Gateway SQL configurations.

As a general rule for all Unified ICM nodes, keep processor utilization below 60 percent of the maximum expected call load on the system. This is needed to smooth out call request "spikes" as well as to allow enough reserve capacity to perform activities such as re-synchronization and background cleanup. Non-ICM software can make up a part of the 60 percent maximum load. The processor utilization figure (60 percent) covers all software running on the platform.

In addition to the utilization requirement, no software on the system can run at a priority equal to or higher than the Unified ICM software for more than 100 milliseconds in uninterrupted bursts. In other words, the Unified ICM software needs to run on the system at least as frequently as once every 100 milliseconds. This is usually not a problem unless device drivers or other kernel-level software is installed, or process/thread priorities have changed incorrectly.

Paging Requirements

The most time-critical component of the Unified ICM system, the CallRouter node, must not be delayed due to disk I/O (that is, paging). The only disk I/O that should be occurring on Unified ICM machines is for log file writes and database I/O. The database I/Os occur on Logger and Administration & Data Server machines. The simple rule is to provide enough main memory so that the entire working sets of critical processes remain in memory.

For complete and current information about RAM and other platform requirements, see the Virtualization information https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html .

Make sure the database platforms (Loggers, Administration & Data Servers, and Unified ICM Gateway SQL machines) have enough main memory so that all first level index pages are kept in main memory cache.

Logger Expansion

The Logger platform you order can include a combination of internal and external SCSI hard drives. As your call center enterprise grows, your database requirements typically grow as well. You may have more services, skill groups, and routes in your configuration, and you may route more calls each day. This database growth means more historical data stored in the central database.

When your database requirements change, contact your Unified ICM software support provider to have the storage capacity of the central database increased.

Note For information about data storage in virtualized deployments, see at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

You can allocate more database space after you install your system by:

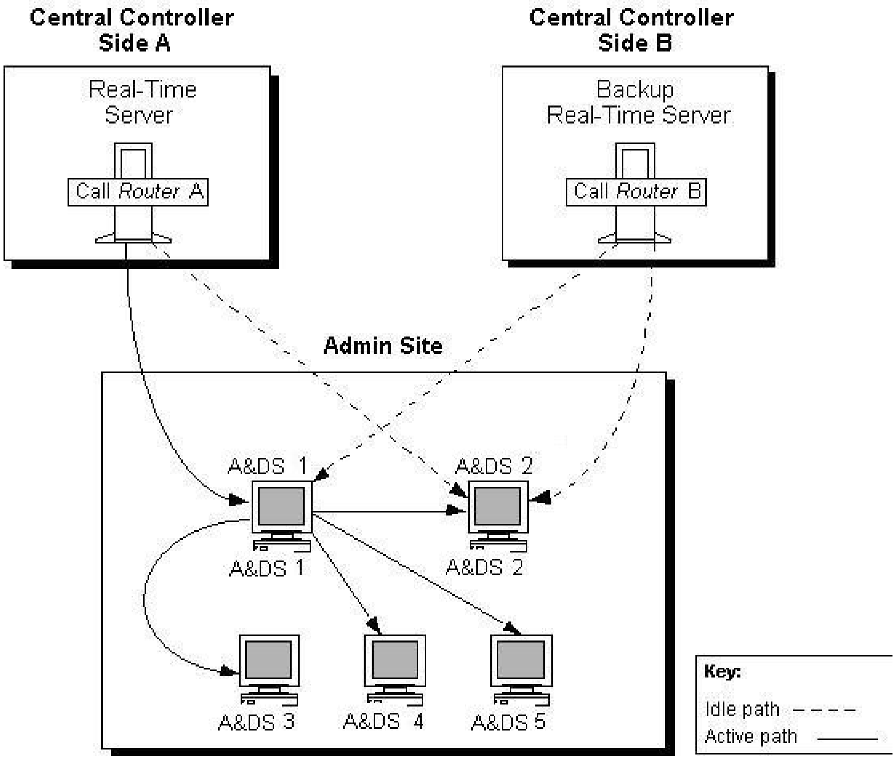
- Remotely adding database space (if current disk space allows).
- Installing “hot-plugable” disk drives and configuring the disks while the system is running.

Note After you install the Unified ICM system, see *Administration Guide for Cisco Unified ICM Enterprise* for information on how to manage database space.

Administration and Data Server Planning

To allow users to monitor current call center activity, the Unified ICM system forwards real-time data to Administration & Data Servers at selected sites throughout the call center enterprise. The following figure illustrates the real-time architecture of the Unified ICM system.

Figure 25: Real-Time Architecture of the Unified ICM System



Real-time call and agent group status data arrives at the central controller from the Peripheral Gateways, which are constantly monitoring activity at each call center. The CallRouter acts as the real-time server. The CallRouter for the other side of the central controller acts as a back-up real-time server.

The CallRouter is responsible for providing real-time data to one or more Administration & Data Servers at each administrator site. Administration Clients at the site receive their real-time data through a connection to a Administration & Data Server. Administration Clients do not have the local database and Administration & Data Server processes are required to receive real-time data directly from the CallRouter.

Administrator Sites

Administration & Data Servers can be located with one or both sides of the central controller, at a call center, or at another site. An administrator site is any site that contains Administration & Data Servers. Each administrator site requires at least one Administration & Data Server. You should use two Administration & Data Servers (as shown in Administration and Data Server Planning, on page 59) to provide fault tolerance in the real-time data distribution architecture.

The primary Administration & Data Server maintains an active connection to the real-time server through which it receives real-time data. The secondary Administration & Data Server also maintains connections to the real-time server; however, these connections remain idle until needed (for example, in cases where the primary Administration & Data Server is unavailable for some reason). In sites that have two Administration & Data Servers, the Administration Clients are configured to automatically switch to a secondary Administration & Data Server if the first distributor becomes non-functional for any reason.

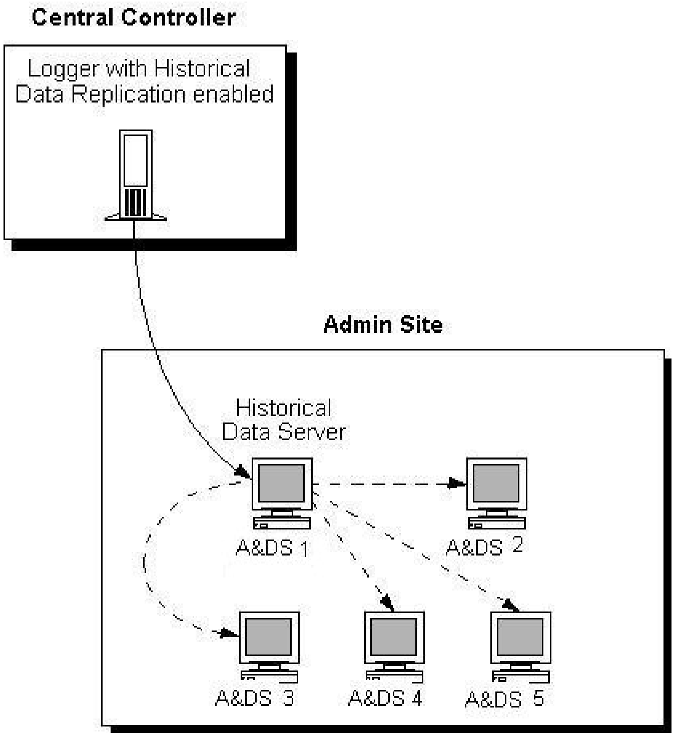
Administration Client Requirements

An Administration & Data Server can serve many Administration Clients. See the at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for information about requirements.

Historical Data Servers

Historical data is stored both as individual call detail records and also rolled up and stored as interval records. An Administration & Data Server with a Historical Data Server (HDS) stores historical data that supports reporting queries. Administration & Data Servers at the site query historical data from the HDS rather than directly from the Logger.

Figure 26: Historical Data Server Architecture



To set up a Historical Data Server, you must configure the Logger to perform historical data replication. You must also configure the real-time Administration & Data Server as an HDS. You can then create an HDS database on the real-time distributor.

Information in the real-time feed tells each Administration Client where to obtain historical data. If the real-time distributor is a Historical Data Server, then it instructs its clients to get historical data from it. Otherwise, it instructs its clients to get historical data from the Logger.

Each Logger can support up to two HDSs. The Administration Server, Real-time and Historical Data Server, and Detail Data Server (AW-HDS-DDS) can be enabled only on the primary distributor. The AW-HDS-DDS server role is disabled on the secondary real-time Administration & Data Server.

HDS Features

The HDS eliminates the performance impact on the central database from multiple Administration & Data Servers accessing the central database to generate reports. In systems that have multiple remote Administration & Data Servers, the HDS brings Unified ICM historical reporting data closer to the user. Each HDS provides a set of database tables. You can set specific times for retaining data in these tables. These capabilities give you flexibility in setting up reporting capabilities on a site-by-site basis.

The Historical Data Server also provides:

- Greater flexibility in leveraging Internet applications.
- An open interface for data mining and data warehousing applications.
- Host for other database tables and have them work with the HDS.
- Improved security and data access capabilities.

  See the at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for information on HDS requirements.

CHAPTER 10

Site Preparation

- Site Preparation, on page 63

Site Preparation

You can begin preparing for the arrival of the Unified ICM equipment, once you do the following:

- Provision IXC access
- Order the required ACD/PBX options
- Order the server platform
- Determine your data communications requirements

Prepare each site that is to contain Unified ICM equipment. The sites must have adequate power facilities, security, and space for equipment layout.

Be sure to consider the following site preparation tasks:

Procedure

	Command or Action	Purpose
Step 1	Meet basic site requirements. Prepare for the arrival of equipment; provide a secure staging area; ensure that sites are ready for occupancy; order and assemble equipment racks.	
Step 2	Design a floor plan for each site. Consider operator workspace, cabling distribution, and maintenance access to Unified ICM nodes.	
Step 3	Meet the power and environmental requirements at each site. Review the server hardware documentation for specifics on power and environmental requirements.	
Step 4	Provide adequate security for the Unified ICM system. Allow only authorized access to the Unified ICM system and any backed-up data.	

	Command or Action	Purpose
Step 5	Determine if you require extra cabling or other equipment. You may need equipment such as rack-mounting hardware or an uninterruptible power supply (UPS).	
Step 6	Order any extra cabling or equipment. Order any additional equipment in time for the arrival of the Unified ICM system components.	

CHAPTER 11

Datacom Requirements

The Unified ICM system needs highly reliable networks to ensure sufficient real-time responsiveness and fault tolerance. Because the Unified ICM system is a mission-critical, fault-tolerant system, it must respond quickly when a node goes offline for any reason. Depending on the situation, the Unified ICM system may need to switch communication paths or activate other nodes to keep the system running without interruption.

In addition to responding to node failures, the Unified ICM system performs diagnostics on failed nodes so they can return to service as soon as possible. Often, the Unified ICM diagnostic procedures take place over a Wide Area Network (WAN).

The Unified ICM system must also respond to route requests from the Interexchange Carriers (IXCs) within a certain minimum time-out period. For example, the AT&T intelligent call processing network requires a response from the Unified ICM system within 200 milliseconds of receiving a route request. In a geographically distributed Unified ICM configuration, this means that the Unified ICM system must perform communications between the NICs and CallRouters on both sides of the central controller and return a route response all within the 200 millisecond time-out period.

This chapter helps you to prepare network facilities for an Unified ICM system installation. In this chapter, complete the following tasks:

- **Determine requirements for visible and private networking.**The Unified ICM networks must meet certain minimum bandwidth and latency requirements.
- **Allocate IP addresses.** Assess the IP address requirements for Unified ICM nodes at each site in the system.
- **Fill out IP address worksheets.** Use the worksheets in IP Address Worksheets, on page 95 to assign IP addresses.
- **Order any additional network hardware.** To prepare the network facilities, you may need to order routers, bridges, or cabling.

This chapter also covers some of the options for configuring the Unified ICM networks and integrating them with your existing networks.

- ICM Sites, on page 66
- ICM Networks, on page 66
- Cisco ICM Quality Of Service (QoS), on page 74
- Active Directory Services, on page 74
- Configure TCP/IP, on page 74
- Central Sites, on page 75

- Contact Center Sites, on page 88

ICM Sites

The Unified ICM system consists of a number of computers, or nodes, which are typically located at more than one site. You can distribute an Unified ICM system among three to fifty sites or more. Each site can contain one or more nodes. The Unified ICM system requires several networks to interconnect nodes within and among the sites.

There are three basic types of Unified ICM sites:

- **Central sites.** Contain one or both sides of the central controller (that is, the CallRouter and Logger) and possibly a Network Gateway . Central sites can also contain Administration & Data Servers and Peripheral Gateways.
- **Contact center sites.** Contain one or more Peripheral Gateways (PGs) and possibly Administration & Data Servers. Sites also support Agents, phone applications and CTI applications.
- **Admin sites.** Contain one or more Administration & Data Servers.

An Unified ICM site can be a combination of any two or more of these. For example, a single location can be both a central site and a contact center site.

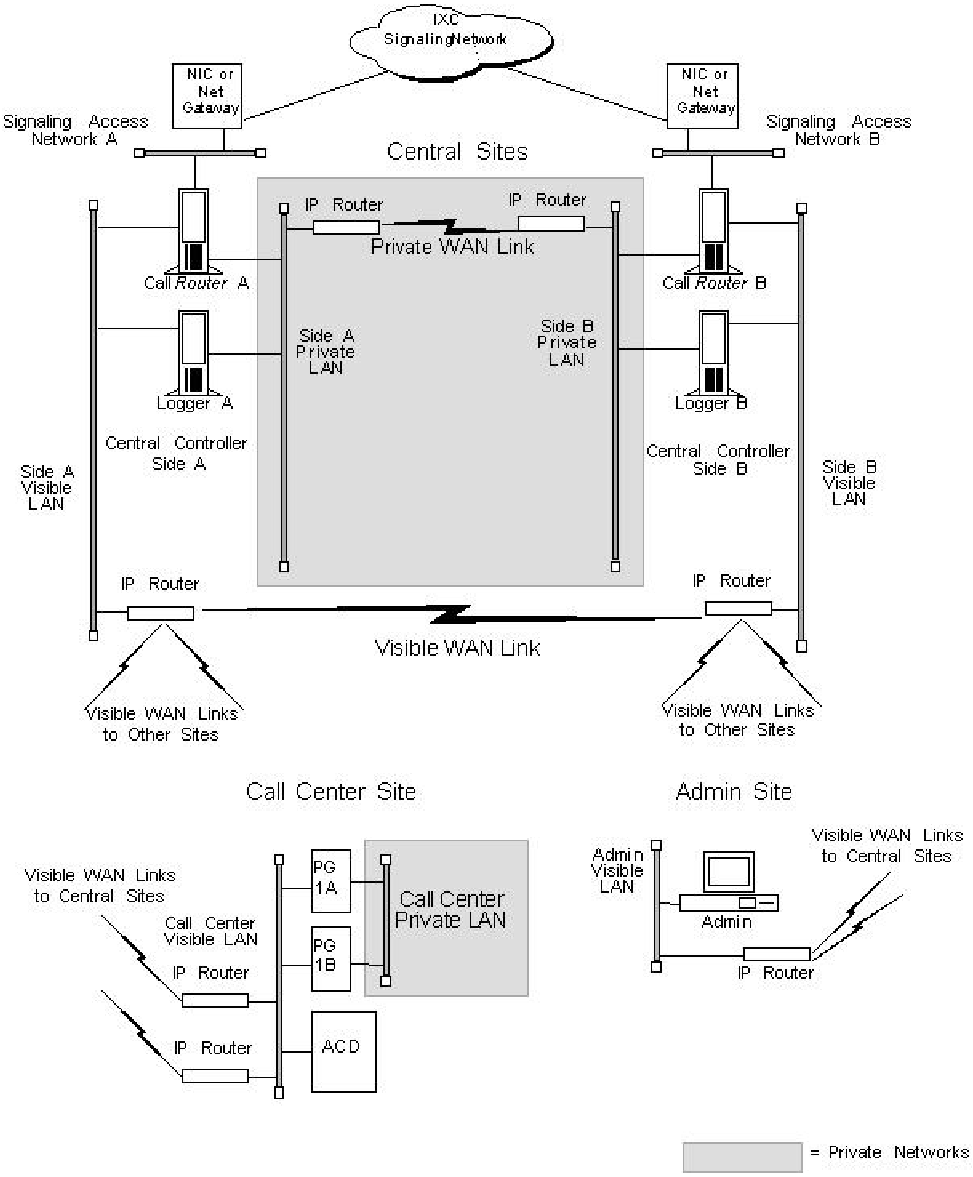
ICM Networks

Following are the three Unified ICM independent communications networks:

- **Private network.** This is a dedicated network that allows specific nodes to communicate with each other without outside interference. This network carries the data that is necessary to maintain and restore synchronization between the systems. The private network is not used for any other purpose.
- **Visible network.** This is a shared network that allows the central controller to communicate with local and remote nodes. It carries traffic between each side of the synchronized system and foreign systems. The fault tolerance software can use the visible network as an alternate network to distinguish between node failures and network failures.
- **Signaling Access Network.** This network connects the Unified ICM system to a carrier network or client network. When a SAN is implemented, the Unified ICM system uses the SAN (not the private network) to communicate with the carrier network.

The following figure shows the two sides of the central controller, a contact center site, and an administrator site. A private WAN links both sides of the duplexed central controller. A visible WAN links the contact center and administrator sites to each side of the central controller. Nodes within each site are linked by a local area network (LAN).

Figure 27: ICM System Network Overview



In the preceding figure, the two sides of the central controller are geographically separated. The wide area network connections in both the private and visible networks are referred to as WAN links. WAN links in the Unified ICM system are typically high-availability provisioned circuits. These links must possess extremely low and extremely predictable latency characteristics. Therefore, you cannot use some types of WAN service for WAN links within the Unified ICM system (for example, packet routing).

Private and Visible WAN Links

The two sides of the duplexed Unified ICM central controller share a single private network and are linked via a private WAN link. They also share a visible network which connects the two sides via a visible WAN link. To ensure a high level of fault tolerance, the private WAN link and visible WAN links must be independent (that is, they must use different trunks and possibly even different service providers).

When the two sides of the central controller are co-located, you do not need the visible WAN link between the sites. The standard visible WAN links to remote contact center sites provide adequate connectivity between the two sides. In a co-located central controller configuration, you use Ethernet switches to implement the private network locally.

Remote contact centers connect to each side of the central controller via the visible network. Each visible WAN link to a contact center must have adequate bandwidth to support PGs and Administration & Data Servers at the contact center (the bandwidth requirement varies greatly as the configuration changes, that is, the call load, the number of agents, and so on).

When a contact center is co-located with a side of the central controller, the PGs and Administration & Data Servers connect to the visible LAN on that side. The PGs and Administration & Data Servers connect to the other side of the central controller via a visible WAN link. In such a configuration, you need a direct visible WAN link between the sides of the central controller to ensure adequate connectivity between the two sides. You may optionally deploy LAN bridges to isolate PGs from the Administration & Data Server LAN segment and to enhance protection against LAN outages.

Note See the section titled Central Site Visible Network, on page 76, for some examples of co-located central controller configurations.

Signaling Access Networking

The CallRouter machine connects to the IXC signaling network via the Signaling Access Network (SAN). A separate LAN interface card in the CallRouter is dedicated for use just by the SAN. The SAN connects the NICs on each side of the duplexed system to the IXC signaling network. In most cases, the NIC software runs on the CallRouter computer. For clarity, in ICM Networks, on page 66, the NIC is shown as a separate computer installed on the SAN.

You can install a node called the Unified ICM Network Gateway on the SAN to interface to some Sigtran-based networks. The Unified ICM Network Gateway is a dedicated machine that provides Sigtran protocol handling services.

In Sigtran networks, you can co-locate Sigtran Gateways on the CallRouter machine or on a separate machine. However, the INAP Sigtran gateway must be installed on a seperate machine. Sigtran Gateways connect to the Sigtran network using the SCCP User Adaptation layer (SUA) with Stream Control Transmission Protocol (SCTP) as the network transport. Sigtran Gateways can serve the following functions, depending on customer requirements:

- Communicate with the Service Switching Point (SSP)
- Communicate with the Media Gateway Controller
- Communicate directly to a Signaling Gateway. In this deployment Sigtran connections are established using a Client / Server message exchange, in which the Sigtran Client requests connections with the Sigtran Server. The Signaling Gateway (such as Cisco's Internet Transfer Point) is a server in this model and accepts incoming connection requests. The Sigtran Gateways act as the Client when connected to a Signaling Gateway.

Network Topology

The Unified ICM system uses Ethernet for local area network connectivity. The particular Ethernet topology used is immaterial from an architectural standpoint. However, the topology used may be relevant from a network or systems management perspective. Typically, UTP is used in the private, visible, and signaling access LANs.

The three networks (visible, private, and signaling) should be on separate LAN segments. This requires the use of three Ethernet cards in the CallRouter machine.

Network Bandwidth Requirements

The visible network bandwidth requirements for a typical Unified ICM system are about 1,000 bytes of data per call over the networks that carry call data. For example, if a remote PG is managing 15 calls per second at a contact center site, it needs to transfer 15,000 bytes of data over the visible WAN to the central site every second (a total of 120,000 bits per second, ignoring packet overhead).

The bandwidth for the private WAN between the two sides of a duplexed central controller must support the total sustained call load for all ACD sites. In addition, bandwidth on this private WAN must provide some degree of burst resilience and enough reserve capacity to perform fault tolerant messaging and synchronization. The following table summarizes the network circuit requirements for visible and private networks within the Unified ICM system.

Table 3: Network circuit requirements

Network	Purpose	Facilities	Min. Bandwidth
Private WAN	Dedicated path that connects both sides of a duplexed, distributed ICM central controller.	Ethernet Unshielded Twisted Pair (UTP)	128-Kbps dedicated.
Visible WAN	Circuits that connect PGs and Administration & Data Servers at remote sites to each side of the ICM central controller.	Ethernet Unshielded Twisted Pair (UTP)	128-Kbps dedicated. **Note** Variable, depending on load. See the section Calculating QoS Bandwidth Requirements, page 11-11, for a means of calculating the minimum required bandwidth for a Quality of Service (QoS) compliant network.

Network	Purpose	Facilities	Min. Bandwidth
Signaling Access Network	Local area network that connects the NIC to the IXC carrier network or client network.	Ethernet Unshielded Twisted Pair (UTP)	100 Mbps
Visible and private LANs	Local area networks that connect ICM nodes at a central site and PGs and Administration & Data Servers at remote contact center sites.	Ethernet Unshielded Twisted Pair (UTP). Cisco requires using manageable hubs.	1000 Mbps **Note** Variable, depending on load. See the section Calculating QoS Bandwidth Requirements, page 11-11, for a means of calculating the minimum required bandwidth for a Quality of Service (QoS) compliant network.

You may require additional bandwidth on the visible WAN. The actual requirement depends on a number of factors, including call load, the number of ACDs, the number of agents, and the number of Admin sites.

Note If your network is utilizing the Cisco Unified ICM Quality of Service (QoS) feature, see Cisco ICM Quality Of Service (QoS), on page 74, for additional latency considerations.

Network Latency Requirements

The Unified ICM system is a real-time, fault-tolerant distributed system.

To guarantee the real-time nature of the system and to support the methods used in fault tolerance, the WAN links in the Unified ICM system must have low and predictable message latency characteristics, especially in these critical areas:

- Route requests and route responses between the CallRouter/NIC and IXC. This communication must meet the strict message latency requirements of the carrier networks.
- Communications involving post-routing requests from PGs and route responses from the CallRouter. This communication must also be fast because callers are online and expect an appropriate agent to answer the call.

- Communications from the PGs to the CallRouter concerning the real-time status of the contact center. The CallRouter needs this information to base its routing decisions on the latest data available from the contact center.

Three fault tolerance mechanisms of the Unified ICM system require reliable, low latency communications. These mechanisms are heartbeat detection, synchronization, and state transfer.

Note If your network uses the Cisco Unified ICM Quality of Service (QoS) feature, see Cisco ICM Quality Of Service (QoS), on page 74, for additional latency considerations.

Heartbeat and Keepalive Detection

As part of its fault-tolerant design, the Unified ICM system must quickly respond when a component goes offline for any reason (typically, because of a failure in the node or in a network link).

Unified ICM uses the Message Delivery Subsystem (MDS) to send synchronization messages. The private network uses TCP keepalive messages that are generated at 100-ms intervals. If no TCP keepalive messages arrive for 500 ms, the system decides that either a network or component failure occurred.

The public network uses the UDP heartbeat mechanism between PGs and the Central Controller. Redundant components generate UDP heartbeats at 100-ms intervals. Routers and PGs generate UDP heartbeats at 400-ms intervals. In both cases, the system decides a failure occurred after missing five UDP heartbeats.

Table 4: Heartbeat Configuration

Node	Medium	Interval
AT&T NIC (or Network Gateway) to CallRouter	Signaling Access Network	200 milliseconds
CallRouter to CallRouter	Private network	100 milliseconds
PG to CallRouter	Visible network	400 milliseconds
PG to PG (if duplexed)	PG to PG (if duplexed) Private network	100 milliseconds

The two sides of a duplexed Unified ICM central controller periodically test each other to see if the other side is operating correctly. As shown in the above table, network latency from CallRouter-to-CallRouter over the private network must support round trip messaging of 100 milliseconds. If the bandwidth of the private network is not adequate, IP routers may need to fragment packets to prevent long messages (greater than 1,500 bytes). Such long messages can delay transmission of User Datagram Protocol (UDP) packets, which indicate that the other side of the central controller is still operating.

Note A consistent heartbeat or keep-alive mechanism is enforced for both the public and private network interface. When QoS is enabled on the network interface, a TCP keep-alive message is sent; otherwise UDP heartbeats are retained.

Another requirement of fault tolerance is that messages cannot be released back to a NIC or PG until the other side of the central controller has acknowledged receipt of a copy of the message. Therefore, in order to meet the 200 millisecond response times established by the carrier networks, and to leave some margin for queuing, a 100 millisecond round trip requirement is established.

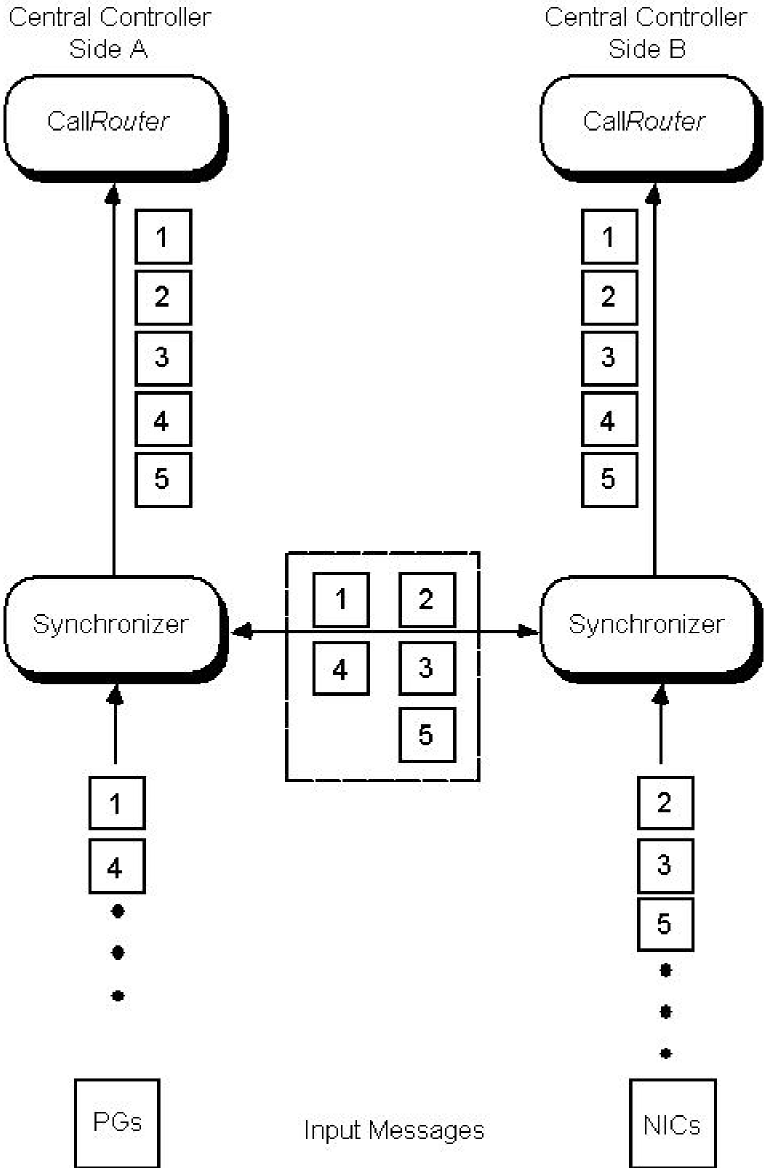
Heartbeats from a remote PG to the CallRouter must compete with other network traffic on the visible WAN.

Synchronization

In a duplexed central controller configuration, the private network allows the CallRouters and Loggers on each side to run in a synchronized fashion. This means that the CallRouter and Logger processes on each side of the system receive the same input and generate the same output.

To ensure synchronization, each message intended for the CallRouter or Logger is received by a Synchronizer process that runs on the CallRouter node. The Synchronizer forwards the message across the private network to the Synchronizer on the other side. The Synchronizers then remove any duplicates before passing the messages on to the CallRouter processes. If a message is intended for the Logger, the CallRouter passes it along.

Figure 28: Role of Synchronizers



The preceding figure shows how the Synchronizers combine input messages and send the messages in the same order to each side of the central controller. Both CallRouters receive the same input and generate the same output. The Synchronizers ensure that both sides of the central controller return identical destinations for the same call and write identical data to the databases.

State Transfer

The fault tolerance of the Unified ICM system enables nodes to restart after a failure. However, when a failed node restarts, the values of variables in its memory are out-of-date. Before returning the node to service, the Unified ICM system must copy the values from its peer on the other side to the recovering node. That is, it must transfer the state of the running machine to the recovering machine. This transfer takes place over the private network.

Note that such state transfers occur after the failure and restart of any synchronized MDS client: PG, Logger, CallRouter, and so on.

Diverse Facilities

The private WAN between central controllers (when the central controllers are geographically separated) and the visible WAN must be on separate facilities. They must use different circuits and different IP routers. As added protection, you may also want to use diverse routes or even different service providers for the private and visible WAN links. Otherwise, you run the risk of having a single network failure disable both the Unified ICM private and visible WANs.

For example, if the private WAN fails, or a visible WAN link to one side of the central controller fails, the Unified ICM system continues to route calls and function normally. However, if the private WAN and the visible WAN are on the same facilities and fail simultaneously, the fault tolerance of the system is compromised. In such a scenario, the failure of any single node on either side of the central controller interrupts system processing. By provisioning the private WAN and visible WAN on separate facilities, you eliminate this potential point of failure.

Cisco ICM Quality Of Service (QoS)

For information on QoS, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html

Active Directory Services

Microsoft Windows Active Directory provides a central repository for managing network resources. Unified ICM software uses Active Directory services to control users' access rights to perform setup, configuration, and reporting tasks. Active Directory services also grant permissions for different components of Unified ICM software to interact; for example, it grants permissions for a Distributor to read the Logger database.

Unified ICME supports the Windows Active Directory domain. Native mode is required. Unified ICM user configuration data is stored in Active Directory Organizational Units (OU).

For more information, see the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Configure TCP/IP

To set up IP addresses for Windows Server 2012 nodes, use the TCP/IP Properties dialog box.

Procedure

- To display this dialog box, go to the Windows Server Start menu:
  a) Choose **Control Panel** > **Network and Internet**.
  b) Click **Network and Sharing Center**.
  c) Click **Change Adapter Settings**.

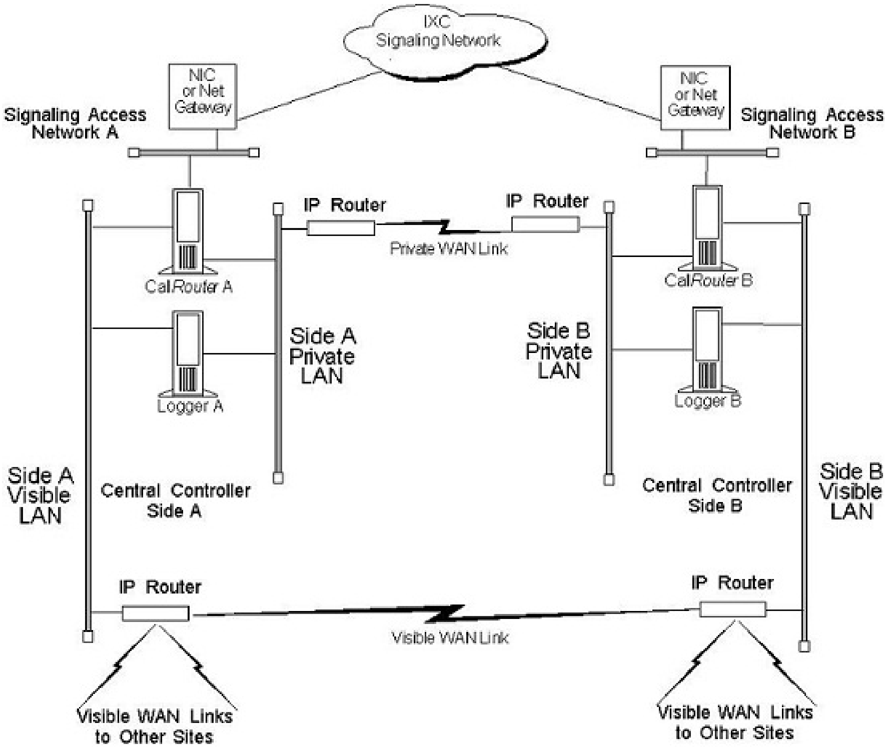
d) Right-click the **Local Adapter**.
e) Click **Properties**.
f) Select Internet Protocol (TCP/IP) and click on **Properties.**

- Select “Use the following IP address”. Enter the IP address and click **OK**. To enter additional IP addresses, open the TCP/IP Properties window again and click **Advanced**. Enter additional IP addresses in the Advanced TCP/IP Settings window.

Central Sites

Each side of the central controller includes the CallRouter, Logger, and Network Interface Controller (NIC). These can be on three separate nodes, two nodes, or a single node. Although the NICs are indicated as separate nodes for clarity, a NIC is implemented as a process within the CallRouter node. The two sides of the central controller can be at two different central sites as shown in the following figure.

Figure 29: Geographically Distributed Central Controller

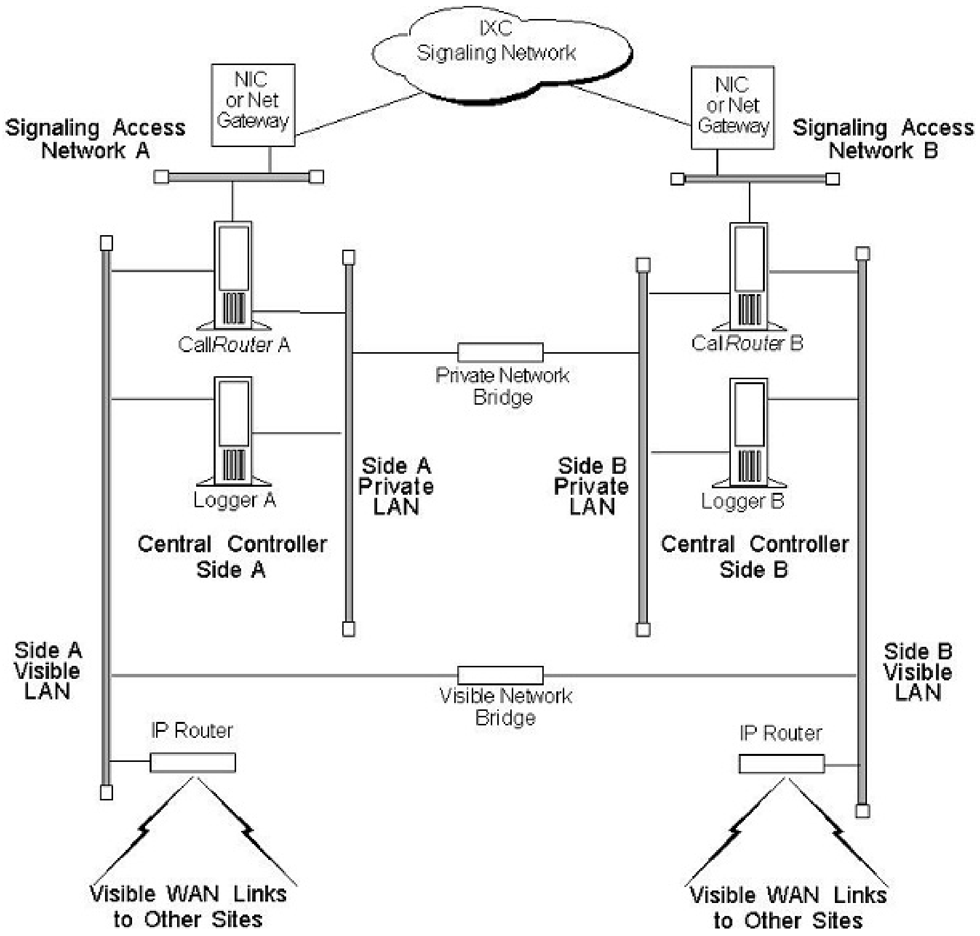


The private network carries Unified ICM system traffic between the nodes on one side of the central controller and between the nodes on both sides of the system. The traffic between the two sides of the central controller consists of synchronization and state transfer messaging between the CallRouters and Loggers. Most communications between the CallRouter and Logger on one side take place over the private network.

The private WAN link (see the preceding figure) is critical to the overall responsiveness of the Unified ICM system. First, it must provide sufficient bandwidth to handle simultaneous synchronizer and state transfer traffic. It must also have enough bandwidth left over to transfer more data as part of a recovery operation. The private WAN link is the only link that carries central controller synchronization and state transfer traffic, so you may want to provision backup service as a contingency for network outages.

The IP routers in the private network always use traffic prioritization. The IP routers in the private network frequently use IP fragmentation, to ensure that high priority Unified ICM system traffic does not experience excessive queuing delay. Alternately, you can co-locate both sides of the central controller at a single site as shown in the following figure.

Figure 30: Co-located Central Controller



In a co-located central controller configuration, Ethernet switches separate Side A, and Side B private Ethernet LANs for fault tolerance. This private network bridge replaces the private WAN link. A visible network bridge also connects the Side A, and Side B visible networks.

Central Site Visible Network

Each central site has a visible network that connects nodes within that site. To allow communication between sites, each side of the central controller must have one IP router on its visible LAN.

Note When a Peripheral Gateway is co-located with one side of a duplexed, geographically distributed central controller, you must have a direct connection between the visible WAN IP routers at the two central sites. This ensures that there is adequate visible network connectivity between the sides of the central controller.

The IP router requires a single address on the LAN. It also requires that you define a static route on the IP router for each contact center's visible LAN and for each administrator site's visible LAN.

Visible IP Router Configuration

To allow optimal tuning of the network, Cisco requires that you use IP routers to prioritize packets based on a range of source or destination port numbers. Typically, you need to set up the IP router to give higher priority to certain outgoing network packets. Also, depending on the bandwidth available on the visible WAN, you may need to set up IP fragmentation. The table titled **Central Site Visible IP Router Configuration** summarizes the configuration for the visible network IP router.

Table 5: Central Site Visible IP Router Configuration

Attribute	Requirements
IP Addresses	One address required.
Default Gateway	The network bridge (or the IP router used as bridge), if any. Otherwise, the IP router does not have a default gateway.
Static Routes	Define one static route for the visible LAN at each remote contact center site and each administrator site. If the central sites are geographically separated, add a static route for the other central site.
Other	Turn off any preset routing protocols. Give higher priority to specific network packets. Use fragmentation if necessary to limit the queuing delay.

You may need to prioritize packets as described in the table titled **Visible Network Packet Priorities from Central Site**.

Table 6: Visible Network Packet Priorities from Central Site

Packet Type	High Priority	Low Priority
TCP	If received from the CallRouter’s high priority address (as derived from the packet’s source address).	If received from any other address.
UDP	If source or destination port number is in the range 39000–39999	All other UDP packets.

The maximum queuing delay is 50 milliseconds to contact center sites that use post-routing or translation routes and 200 milliseconds to other contact center sites. You may have to implement fragmentation to meet these limits.

Central Site Private Network

Each central site must also have its own private LAN. If the sides of the central controller are geographically separated, each private LAN has one IP router to communicate with the private WAN that connects the two sides.

If the two sides of the central controller are co-located, you do not need an IP router on the private LAN. If two central sites are geographically separated, each side requires an IP router on the private network.

The following table summarizes the configuration for the private network IP router.

Table 7: Central Site Private IP Router Configuration

Setting	Requirements
IP Addresses	None.
Default Gateway	Define one static route for the private LAN at the other central site.
Static Routes	Define one static route for the private LAN at the other central site.
Other	Turn off any preset routing protocols. Give higher priority to specific network packets.

The following table describes how you must prioritize private network packets.

Table 8: Private Network Packet Priorities from Central Site

Packet Type	High Priority	Low Priority
TCP	If the source address is the local CallRouter's high priority address or the destination address is the other CallRouter's high priority address.	All other TCP packets.
UDP	If source or destination port number is in the range 39000–39999.	All other UDP packets.

Signaling Access Network

Each central site must have its own Signaling Access Network (SAN). The Unified ICM system uses the Signaling Access Network to communicate with the IXC signaling network.

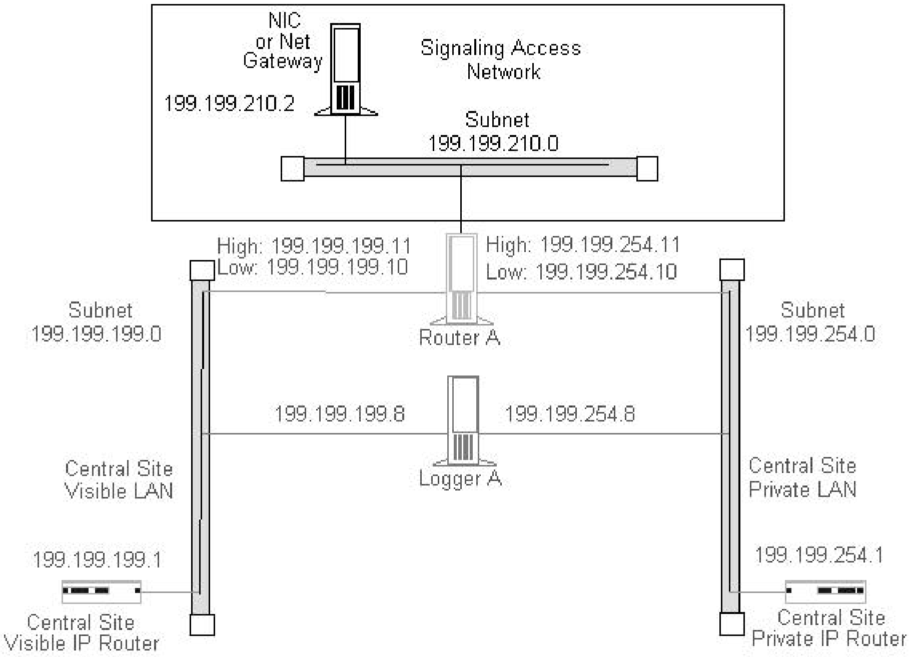
The Signaling Access Network for the following NICs is implemented as an Ethernet LAN. This LAN is separate from the Unified ICM private LAN.

- CRSP
- GKTMP
- ICRP
- Nortel
- NTL
- MCI

The following figure shows a typical Signaling Access Network for a single central site. It assumes that the two sides are geographically separated.

Note The IP addresses shown in this and subsequent figures are examples only. Use addresses specific to your networks.

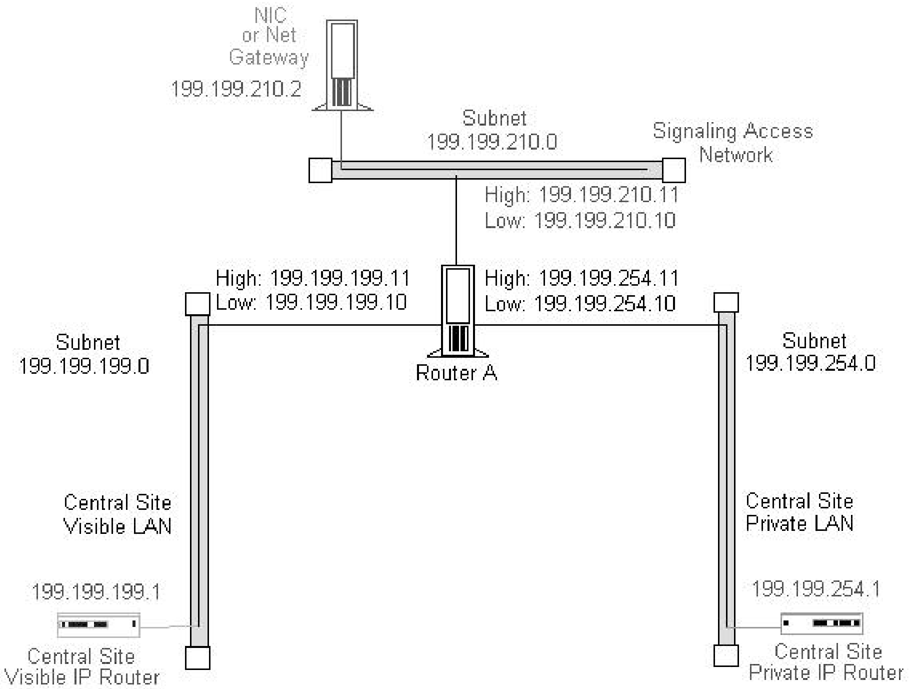
Figure 31: Central Site Signaling Access Network



CallRouter Node

The CallRouter connects to the visible network through the visible LAN; and to the private network through the private LAN. The CallRouter also has a connection to the Signaling Access Network.

Figure 32: CallRouter Network Connections



As shown in the preceding figure, the CallRouter requires two addresses on the visible LAN, two addresses on the private LAN, and two addresses on the signaling access LAN. This allows the Unified ICM system to separate high-priority network traffic from low-priority traffic.

The following table summarizes the visible network configuration for the CallRouter.

Table 9: CallRouter Visible Network Configuration

Setting	Requirements
IP Addresses	Two required: one for high priority data, one for low (normal) priority data. Note that only one address is required if you are using QoS.
Default Gateway	Visible network IP router.
Static Routes	None.
Other	Preferred and alternate DNS server. See Active Directory Model, page 11-21.

The following table summarizes the private network configuration for the CallRouter.

Table 10: CallRouter Private Network Configuration

Setting	Requirements
IP Addresses	Two required: one for high priority data, one for low (normal) priority data.

Setting	Requirements
Default Gateway	None. (The default gateway is on the visible LAN.)
Static Routes	If the sides of the central controller are geographically separated, define one static route for the subnet address of the private LAN on the other side of the central controller.
Other	Disable Windows Server 2003 or 2008 R2 networking on the private LAN.

Note Instructions on disabling Windows Server networking on the private LAN appear later in this section.

The following table summarizes the Signaling Access Network configuration for the CallRouter.

Table 11: CallRouter Signaling Access LAN Configuration

Setting	Requirements
IP Addresses	Two may be required, the second functioning as a serviceability interface for your Unified ICM service provider.
Default Gateway	None.
Static Routes	None.
Other	Disable Windows Server 2003 or 2008 R2 networking on the private LAN.

Disabling Windows Server 2012 Networking

You must disable network bindings for the private LAN adaptor on machines that connect to the Unified ICM private network.

You can disable Windows Server 2012 networking on the private LAN interface through the Network and Dial-up Connections window. Right click on the **My Network Places** icon on the Windows Server 2012 desktop. The Network and Dial-up Connections window appears. (Optionally, you can right-click on the **My Computer** icon, select **Explore**, then right click on **My Network Places** and select **Properties**.) Choose **Advanced** > **Advanced Settings** to display the Advanced Settings window.

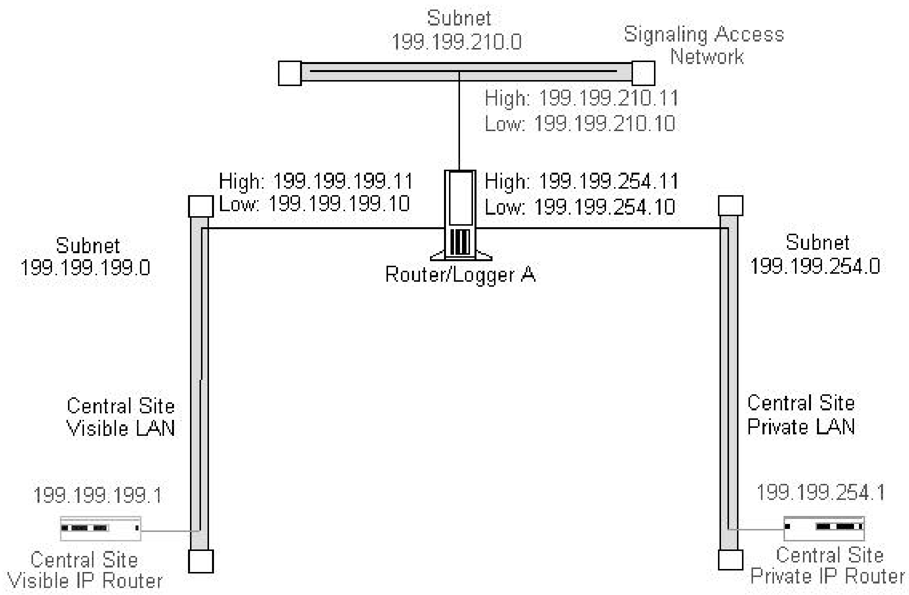
On Windows Server 2014 select **Start** > **Control Panel** > **Network and Internet** > **View network status and tasks** > **Change adapter Settings**. Press the ALT key to make the menu bar appear. Choose **Advanced** > **Advanced Settings** to display the Advanced Settings window.

Make sure that the visible network connection appears first in the list, followed by the private network connection. You can change the order in which the network connections appear by using the arrows on the right side of the window. Select the private network connection and disable both “File and Printer Sharing for Microsoft Networks” and “Client for Microsoft Networks.”

Logger Node

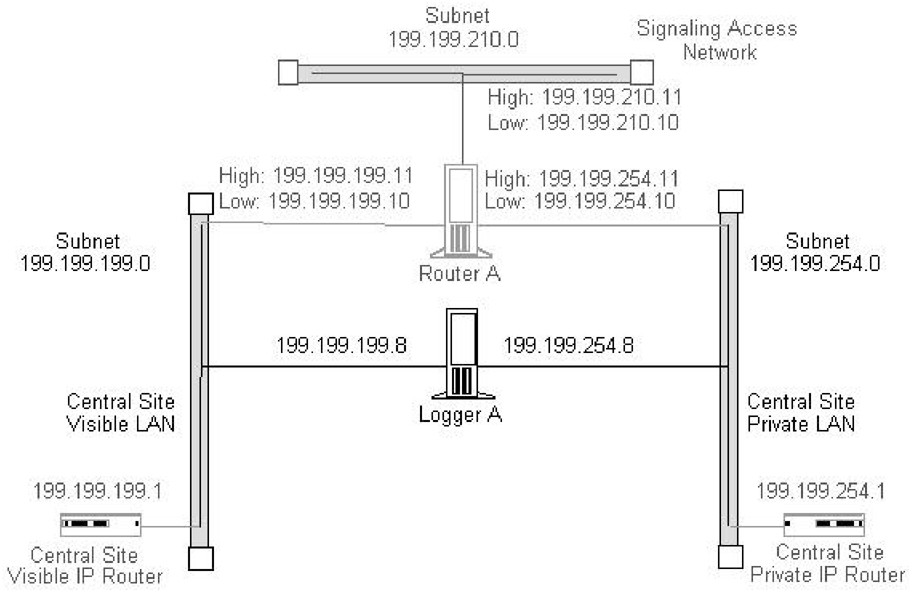
The Logger can be on the same node as the CallRouter, or it can be a separate node.

Figure 33: CallRouter and Logger Combination



If the CallRouter and Logger are on the same node, then the Logger has no specific requirements; it uses low priority addresses defined for the node on the visible and private networks. If the two are on separate nodes, then the Logger requires its own connections to both the visible and private LANs.

Figure 34: Logger as a Separate Node



In addition to the IP addresses shown, the Logger node may require two additional addresses on the visible network. These addresses allow for dial-in connections by your Unified ICM support provider's Distributed

Diagnostic and Service Network (DDSN). The following table summarizes the visible network connections for the Logger.

Table 12: Logger Visible Network Configuration

Setting	Requirements
IP Addresses	Three addresses may be required: one for normal data, two more for DDSN dial-up connections.
Default Gateway	Visible network IP router.
Static Routes	None.
Other	Preferred and alternate DNS server. See Active Directory Services, on page 74.

The following table summarizes the private network configuration for the Logger.

Table 13: Logger Private Network Configuration

Setting	Requirements
IP Addresses	One address required.
Default Gateway	None. (The default gateway is on the visible LAN.)
Static Routes	If the two sides of the central controller are geographically separated, define one static route for the subnet address of the private LAN for the other side of the central controller.
Other	Disable Windows Server 2012 networking on the private LAN interface. (See Disabling Windows Server 2012 Networking, on page 81 for more information.) Disable Windows Server 2014 networking on the private LAN interface. (See Disabling Windows Server 2012 Networking, on page 81 for more information.)

If the Logger is on the same computer as the CallRouter, then the visible and private network IP configuration for the CallRouter is all that is required.

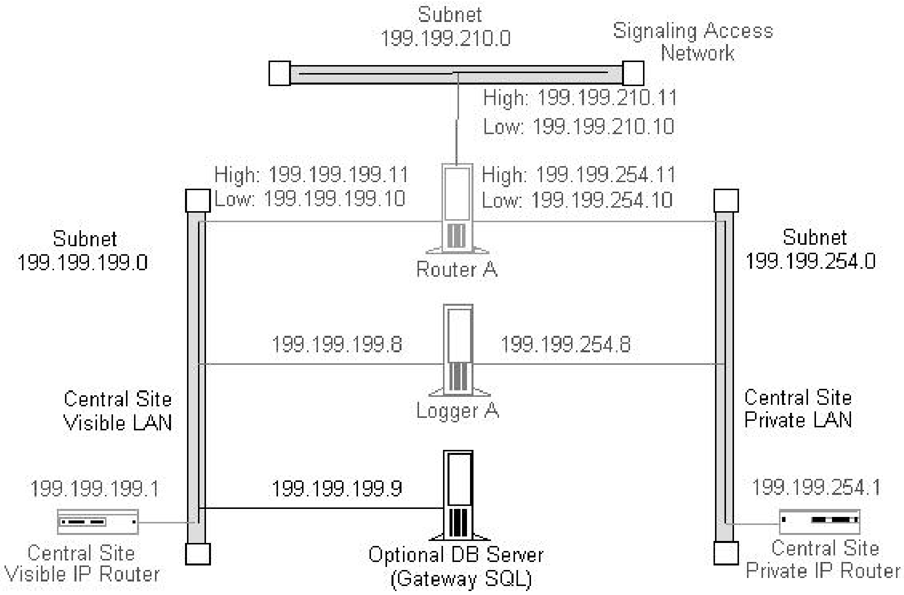
If the Logger is a separate node, you must disable networking on the private LAN interface (as was required for the CallRouter).

Define a static route in ICMEXEC.BAT, as for the CallRouter.

Optional Database Server Platform

If you deploy the Cisco Unified ICM Gateway SQL option, you must set up an additional Microsoft SQL Server database platform. The database server requires one IP address and one connection to the Unified ICM visible network.

Figure 35: Optional Database Server



You can deploy an Unified ICM Network Gateway on the Signaling Access Network in Sigtran network environments. The Unified ICM Network Gateway is a dedicated Windows Server machine that provides Sigtran protocol handling. When you use an Unified ICM Network Gateway, you install the NIC software on the CallRouter machine and use a separate Gateway machine as the interface between the CallRouter and the carrier's Sigtran signaling network.

You install the Network Gateway on a dedicated machine. It connects to both the Signaling Access Network (SAN) and to the Unified ICM visible network. You use the visible network connection strictly for management and maintenance. The Unified ICM Network Gateway does not connect to other nodes at the central site or to nodes at other sites. For example, it does not communicate over the private network with a network gateway on the other side of the system.

The Unified ICM Network Gateway can support up to sixteen signaling links to the IXC signaling network.

In Sigtran networks you can deploy a Sigtran Gateway on either the CallRouter machine or on a separate machine. This Sigtran Gateway can communicate with either a Service Switching Point or a Media Gateway Controller, or it can communicate directly with a Signaling Gateway. In this deployment, a Client / Server message exchange establishes Sigtran connections, in which the Sigtran Client requests connections with the Sigtran Server. The Signaling Gateway (such as Cisco's Internet Transfer Point) is a server in this model and accepts incoming connection requests. The Sigtran Gateways act as the Client when connected to a Signaling Gateway.

The following table summarizes the Signaling Access Network requirements for an Unified ICM Network Gateway.

Table 14: ICM Network Gateway Signaling Access Network configuration

Setting	Requirements
IP Addresses	One address required.
Default Gateway	None.
Static Routes	None.
Other	A HOSTS file is set up and changes are made to the CONFIG.SYS and AUTOEXEC.BAT files. Consult with your ICM support provider before changing these settings.

The following table summarizes the visible network requirements for an Unified ICM Network Gateway.

Table 15: ICM Network Gateway Visible Network configuration

Setting	Requirements
IP Addresses	One address required.
Default Gateway	Visible network IP router.
Static Routes	None.
Other	A HOSTS file is set up and changes are made to the CONFIG.SYS and AUTOEXEC.BAT files. Consult with your Unified ICM support provider before changing these settings.

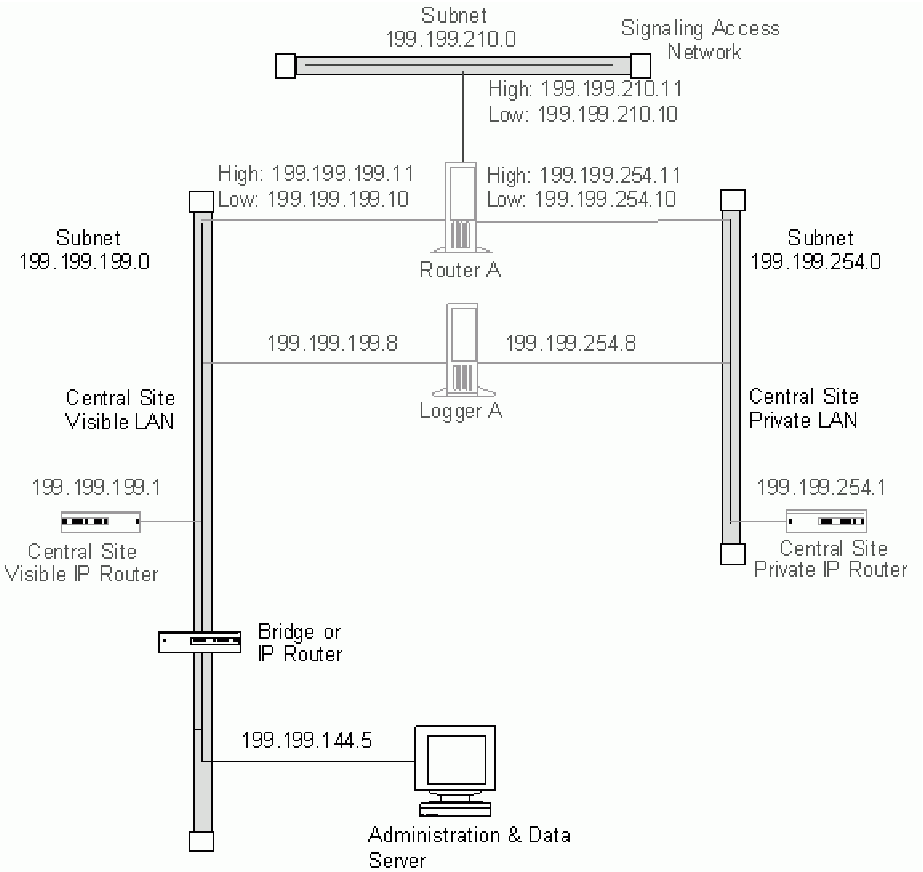
Administration and Data Servers at Central Site

Cisco requires that you use Ethernet switches to isolate the CallRouter, Logger, and PGs from the Administration & Data Server LAN segment. This requirement limits the impact of one network's problems on another. Isolate the central controller and PGs from the Administration & Data Server LAN segment, to protect critical components from network hardware and software failures. For example, you can protect components from failures such as an open Ethernet tap or a network error burst.

For further protection against LAN outages, use an IP router instead of a bridge. You can then place the Administration & Data Server on a separate LAN with other contact center computers and applications. The IP router is a preferable option in this situation. LAN bridges tend to forward network error bursts from one side of a LAN to the other. IP routers provide an enhanced firewall because they do not forward network errors to other LANs.

The Administration & Data Server must reside on a network visible to the Unified ICM software. The following figure shows how you can use a LAN bridge or an IP router to isolate PGs and the central controller from the Administration & Data Server LAN segment.

Figure 36: Administration & Data Server at a Central Site

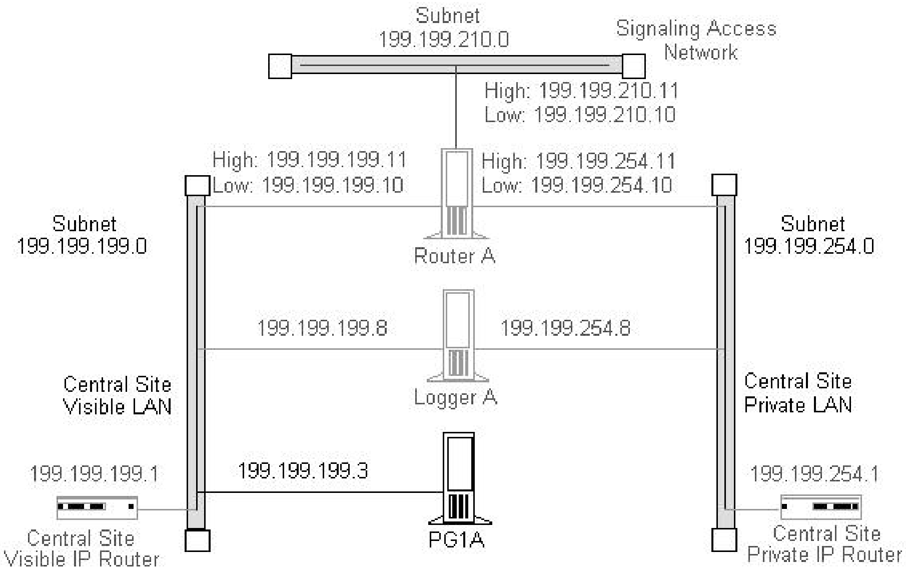


Peripheral Gateways at Central Site

A Peripheral Gateway (PG) that is co-located with one or both sides of the central controller can share the same visible LAN segment as the CallRouter and Logger nodes. The PG can communicate with the local CallRouter through the visible LAN. If the sides of the central controller are geographically separated, the PG communicates with the other side through the visible IP router and a WAN link. (If both sides of the central controller are co-located with the PG, then the PG communicates with both sides through the visible LAN.)

The following figure shows the network connection for a PG at a central site.

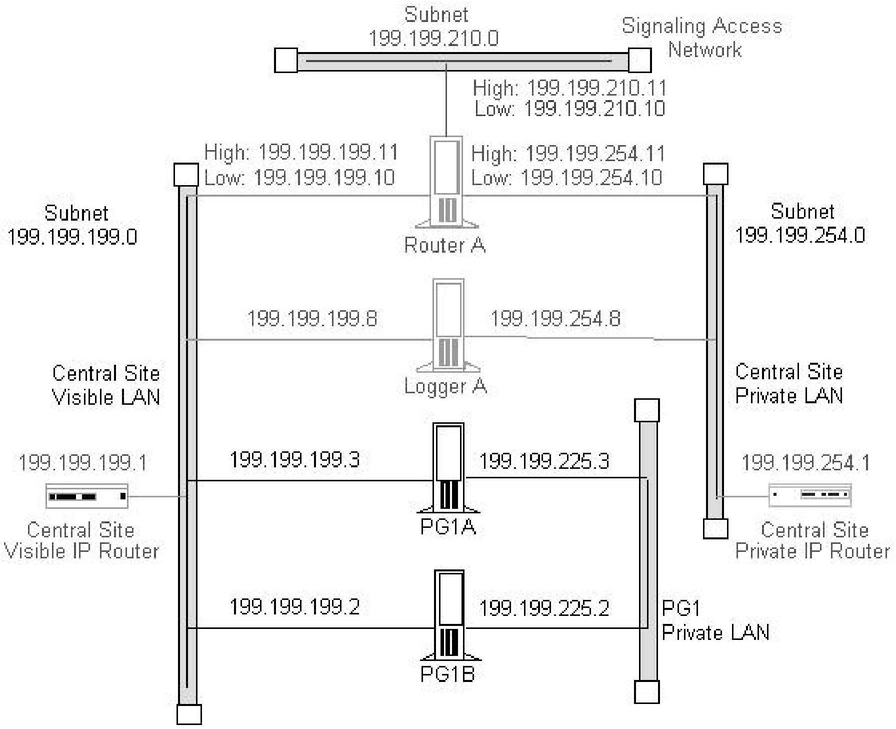
Figure 37: Peripheral Gateway at a Central Site



The ACD itself can also be on the visible LAN.

If the PG is duplexed, then you must connect the two duplexed PGs through a separate private network. (They cannot use the same private network as the CallRouter and Logger.) See the following figure.

Figure 38: Duplexed Peripheral Gateways at a Central Site



If you have more than one pair of duplexed PGs at a site, each pair requires its own private LAN. The private LAN for the PGs allows for synchronization and state transfer between the PGs. It is not used for any other purpose.

Note When a Peripheral Gateway is located with one side of a geographically distributed central controller, you must have a WAN link directly connecting the visible WAN IP routers at the two central sites. This ensures that there is adequate visible network connectivity between the sides of the central controller. For more information on PG networking requirements, see the next section, "Contact Center Sites".

Contact Center Sites

Each contact center site includes at least one ACD, at least one Peripheral Gateway (PG), and optionally, one or more Administration & Data Servers. Contact centers can also have an Interactive Voice Response (IVR) unit. For fault-tolerance, the contact center site must include a duplexed pair of PGs.

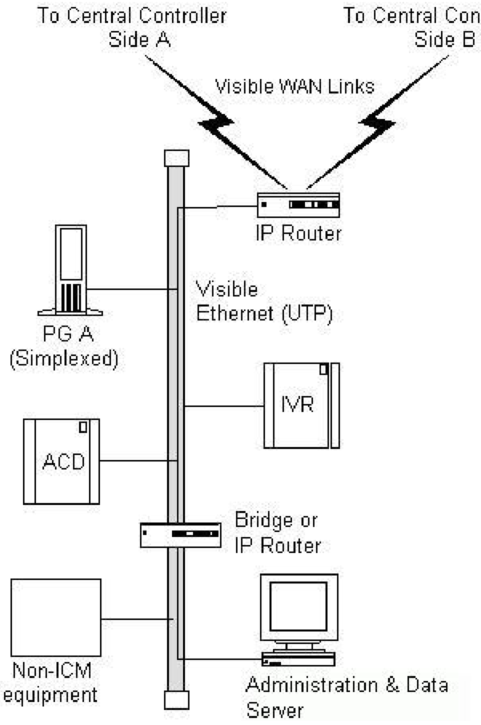
A remote contact center complex is reached via the visible network, often with multiple access paths and through multiple IP routers. The contact center site must have at least one IP router on the visible network to communicate with the central controller. For maximum fault-tolerance, the site should have two IP routers, each connecting to one side of the central controller.

Note For information on installing and configuring the Unified ICM Peripheral Gateway software, see the at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Simplexed PG Site

The following figure shows one option for a contact center configuration with a simplexed PG and an Administration & Data Server. This site contains an ACD and an VRU system. You can install the VRU PG software and the ACD PG software on the same server hardware platform.

Figure 39: Contact Center with Simplexed PG



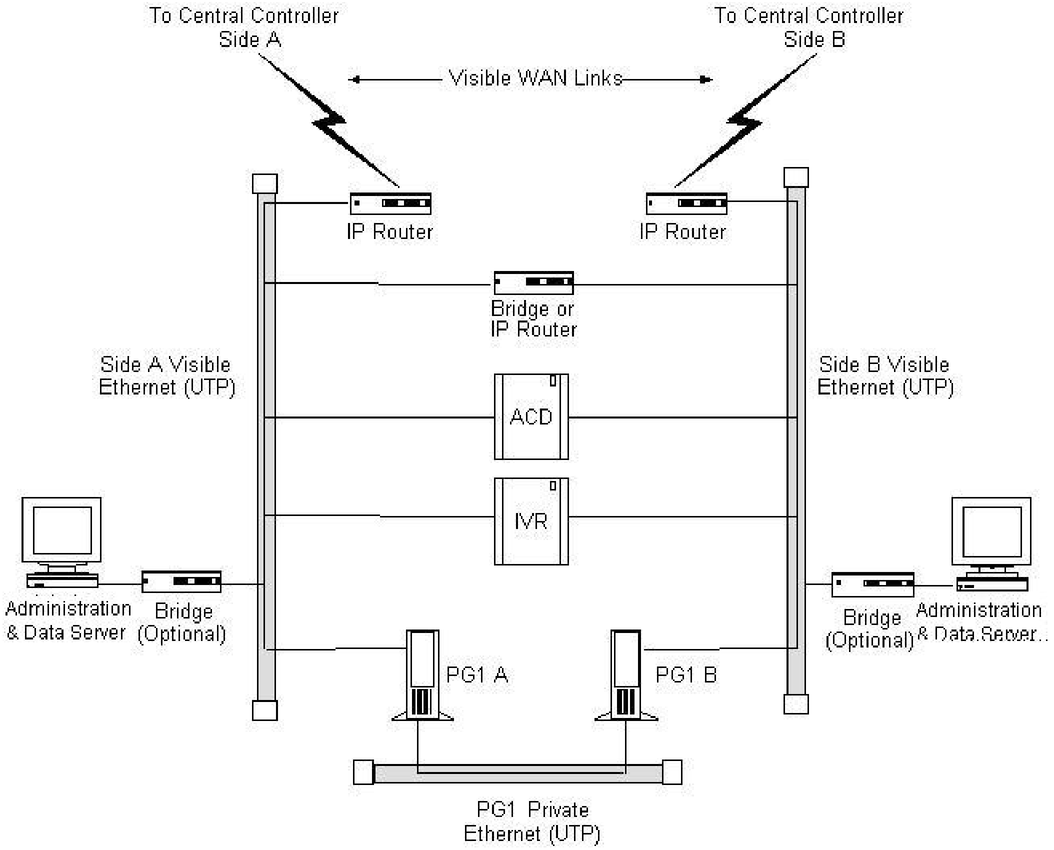
As shown in the preceding figure, the PG and Administration & Data Server share a single Ethernet LAN and an IP router. The IP router uses prioritization and IP fragmentation to minimize queuing delays for high-priority Unified ICM system traffic. Cisco requires that you separate the PG, ACD, VRU, and IP router from other devices by a bridge or IP router. This isolates the critical Unified ICM components from outages that other equipment and networks can cause.

The contact center example shown in the preceding figure is a low fault tolerance configuration. It is only for non-fault tolerant sites (for example, for contact center sites with one PG or administrator sites with Administration & Data Servers only). A simplexed PG configuration can represent a single point of failure. Loss of the only PG stops the flow of real-time data from the contact center to the CallRouter and prevents the use of post-routing and translation routes. You can protect against possible failures by using duplexed PGs.

Duplexed PG Site

A duplexed PG configuration provides enhanced fault-tolerance.

Figure 40: Fault Tolerant Contact Center


To Central Controller Side A
To Central Controller Side B
Visible WAN Links
IP Router
IP Router
Bridge or IP Router
Side A Visible Ethernet (UTP)
Side B Visible Ethernet (UTP)
ACD
IVR
Administration & Data Server
Bridge (Optional)
Bridge (Optional)
Administration & Data Server..
PG1 A
PG1 B
PG1 Private Ethernet (UTP)

Note A PG private LAN is added to allow direct communication between the two PGs. If you have more than one duplexed pair of PGs at a site, each PG pair requires its own private LAN. However, this requirement is slightly relaxed for Unified CCE in a Clustering over the Wan deployment model. For details, see the .

To further enhance the fault-tolerance of the contact center, you can configure each PG with its own visible LAN and IP router. This eliminates the LAN as a single point of failure. Each PG communicates with one side of the central controller using its own LAN and IP router.

If you used a single IP router instead of two, you introduce a potential single point of failure to the contact center site. Loss of the one IP router stops the flow of real-time data from the contact center to the CallRouter and stops the flow of monitoring data from the central controller to the Administration & Data Server. It also prevents the use of post-routing and translation routes for this contact center.

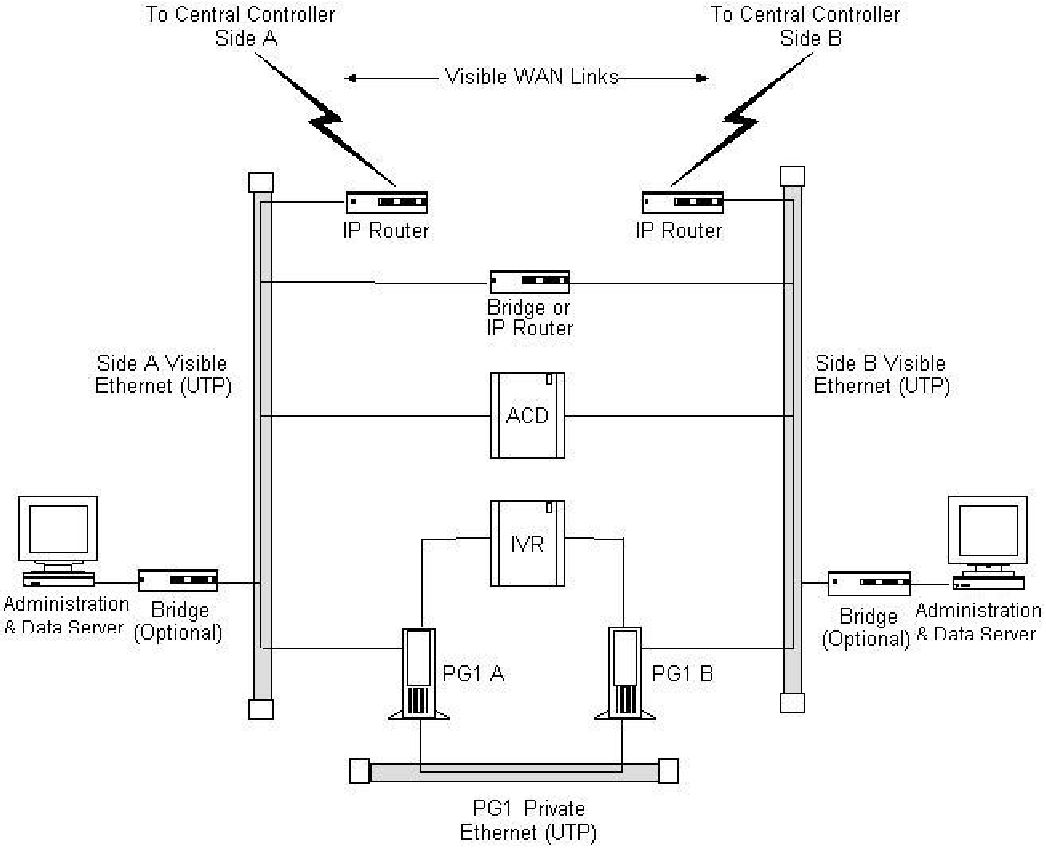
One of the two IP routers shown in the preceding figure serves as the default gateway for the PG. By default, the PG communicates with that side of the central controller. The PG must have a static route defined to the other side of the central controller through the other IP router.

Each PG can contain a modem to allow dial-in access through your Unified ICM support provider's Distributed Diagnostic and Service Network (DDSN). In addition to its normal address on the visible network, the PG then requires two additional visible LAN addresses for this dial-in access.

Duplexed PG Site with Separate IVR LAN

You can use another contact center configuration in cases where you need to separate IVR systems due to security concerns or when you must protect the management of the IVRs. The following figure shows an example of such a fault tolerant contact center site.

Figure 41: Fault Tolerant Contact Center—IVR on Separate LAN


To Central Controller Side A
To Central Controller Side B
Visible WAN Links
IP Router
IP Router
Bridge or IP Router
Side A Visible Ethernet (UTP)
Side B Visible Ethernet (UTP)
ACD
IVR
Administration & Data Server
Bridge (Optional)
Bridge (Optional)
Administration & Data Server
PG1 A
PG1 B
PG1 Private Ethernet (UTP)

With this option, the ACD is on the visible LAN under the assumption that another CTI application needs to interface to the ACD. An alternative is to have the ACD on the same LAN as the IVR system.

PG Network Configuration

The following table summarizes the network configuration for a simplexed PG.

Table 16: Simplexed PG Network Configuration

Setting	Requirements
IP Addresses	Three addresses may be required on the visible LAN: one for normal data and two for use by the DDSN.
Default Gateway	Define one of the visible network IP routers as the default gateway for the PG.

Setting	Requirements
Static Routes	Define one static route to the visible LAN at the central site that is not targeted by the default gateway IP router.
Other	Preferred and alternate DNS server. See Active Directory Services, on page 74.

The following table summarizes the network configuration for a duplexed PG.

Table 17: Duplexed PG Network Configuration

Setting	Requirements
IP Addresses	Each PG may require three addresses on the visible LAN (one for normal traffic plus two addresses for DDSN dial-up connections) and two addresses on the private LAN (one for high priority and one for low priority data). **Note** For Enterprise versions, configure only one IP address on the PG-visible NIC. IP addresses for DDSN dial-up connections are for Hosted versions only.
Default Gateway	Define one of the visible network IP routers as the default gateway for each PG. Do not use the same IP router as the default gateway for both PGs.
Static Routes	Each PG requires a static route to the side of the central controller that is not targeted by its default gateway IP router.
Other	Preferred and alternate DNS server. See Active Directory Services, on page 74.

Note For more information on how Peripheral Gateways connect to ACDs, see Peripheral Gateway Configurations, on page 25.

Contact Center IP Routers

The IP router requires a single address on the LAN. It also requires that you define a static route on the IP router to the side of the central controller (central site visible LAN) that is not targeted by the PG default gateway IP router.

To allow optimal tuning of the network, Cisco requires that you use IP routers to prioritize packets based on a range of source or destination port numbers. Typically, you need to set up the IP router to give higher priority to certain outgoing network packets. Also, depending on the bandwidth available on the visible WAN, you may need to set up IP fragmentation.

The following table summarizes the configuration for the IP routers.

Table 18: Contact center IP Router Configuration

Setting	Requirements
IP Addresses	Each IP router requires one address on the visible LAN.
Default Gateway	Network bridge or IP router used as bridge, if any. Otherwise, the IP router does not have a default gateway.
Static Routes	Each IP router must have a static route to reach one central site visible LAN.
Other	Turn off any preset routing protocols. Give higher priority to specific network packets. Use fragmentation if necessary to limit the queuing delay.

Note The following table summarizes information about packet priorities.

Table 19: Contact Center Packet Priorities

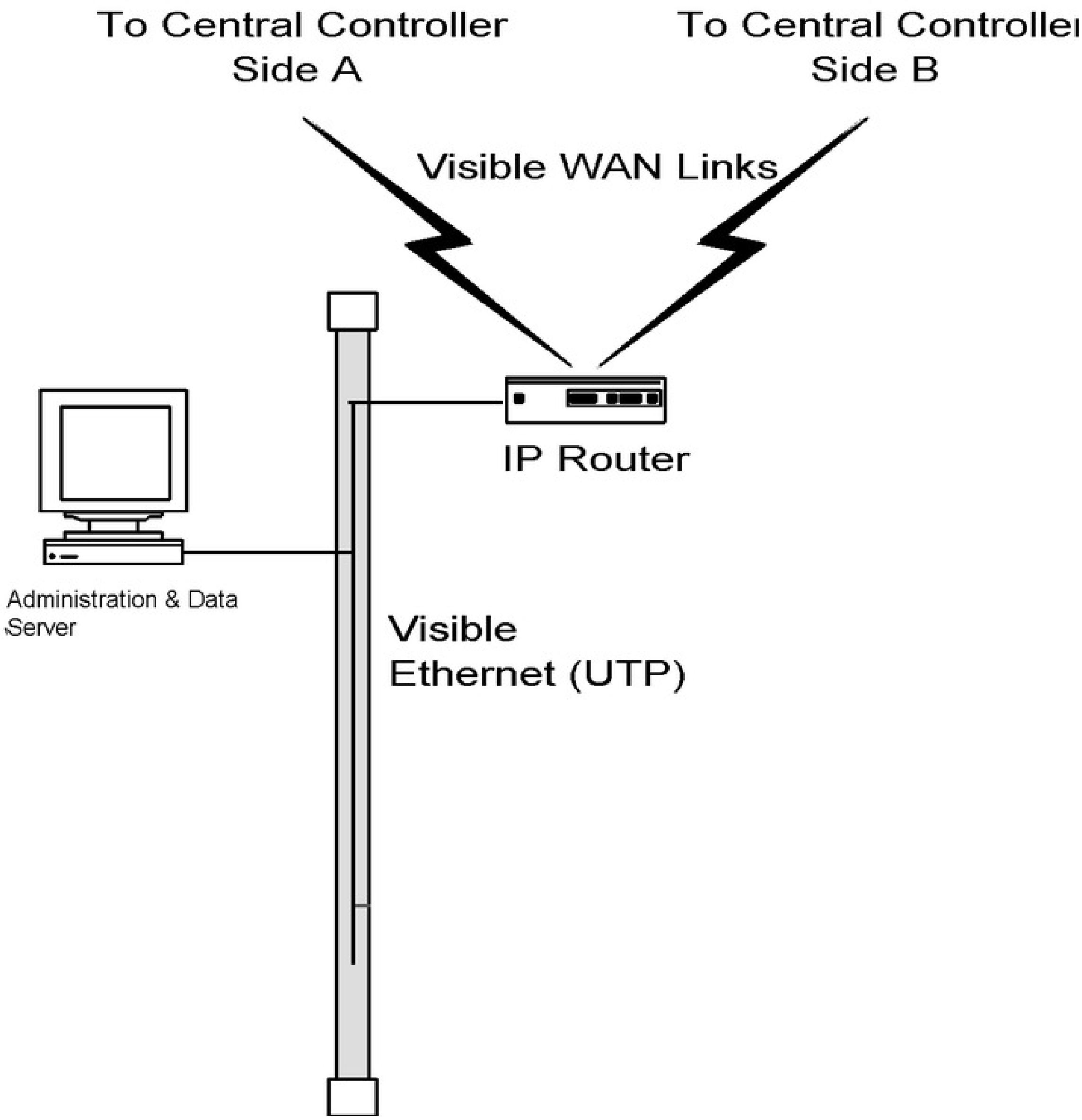
Packet Type	High Priority	Low Priority
TCP	If sending to the CallRouter's high priority address (as derived from the packet's destination address).	If sending to any other address.
UDP	If source or destination port number is in the range 39000–39999.	All other UDP packets.

The maximum queuing delay is 50 milliseconds if the site uses post-routing or translation routes; 200 milliseconds otherwise. You may have to set up fragmentation to meet these limits.

Admin Sites

An administrator site contains one or more Administration & Data Servers. Each administrator site must have a visible LAN and an IP router to communicate with the central sites. An administrator site does not require a private LAN.

Figure 42: Admin Site Configuration



You can have multiple Administration & Data Servers on a single LAN.

CHAPTER 12

IP Address Worksheets

This chapter provides worksheets you can use to record IP addresses for the visible and private networks. You also need to define static routes for some of the nodes in the Unified ICM system.

- Visible Network IP Address Requirements, on page 95
- Private Network IP Address Requirements, on page 97
- Signaling Access Network IP requirements, on page 100
- Static Route Requirements, on page 100

Visible Network IP Address Requirements

The table titled **Visible Network IP Address Requirements** lists the IP address requirements for Unified ICM node connections to the visible network. The Unified ICM nodes are listed as duplexed pairs (for example, CallRouter A and CallRouter B). You may or may not have duplexed nodes in your configuration. Supply IP addresses only for the nodes you have in your configuration.

Table 20: Visible Network IP Address Requirements

Node	Location	Address Type	IP Address
CallRouter A		High Priority	
		Low Priority	
		Default IP Gateway	
		Netmask	
CallRouter B		High Priority	
		Low Priority	
		Default IP Gateway	
		Netmask	
Logger A		Normal Data	
		RAS 1	

Node	Location	Address Type	IP Address
		RAS 2	
		Default IP Gateway1	
		Netmask	
Logger B		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
Central Site IP Router		Normal data	
Remote Contact Center Site IP Route		Normal data	
PG1A		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
PG1B		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
PG2A		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
PG2B		Normal Data	
		RAS 1	

Node	Location	Address Type	IP Address
		RAS 2	
		Default IP Gateway1	
		Netmask	
PG3A		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
PG3B		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
AW1		Normal Data	
		Default IP Gateway1	
		Netmask	
AW2		Normal Data	
		Default IP Gateway1	
		Netmask	

Private Network IP Address Requirements

The table titled **Private Network IP Address Requirements** lists the IP address requirements for Unified ICM node connections to the private network. The Unified ICM nodes are listed as duplexed pairs (for example, CallRouter A and CallRouter B). You may or may not have duplexed nodes in your configuration. You need to supply IP addresses only for the nodes you have in your configuration.

Table 21: Private Network IP Address Requirements

Node	Location	Address Type	IP Address
CallRouter A		High Priority	
		Low Priority	

Node	Location	Address Type	IP Address
		Default IP Gateway	
		Netmask	
CallRouter B		High Priority	
		Low Priority	
		Default IP Gateway	
		Netmask	
Logger A		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
		Modem Tel. Number	
Logger B		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
		Modem Tel. Number	
Central Site IP Router		Normal Data	
Remote Contact Center Site IP Router		Normal Data	
PG1A		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
		Modem Tel. Number	
PG1B		Normal Data	

Node	Location	Address Type	IP Address
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
		Modem Tel. Number	
PG2A		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
		Modem Tel. Number	
PG2B		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
		Modem Tel. Number	
PG3A		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	
		Modem Tel. Number	
PG3B		Normal Data	
		RAS 1	
		RAS 2	
		Default IP Gateway1	
		Netmask	

Node	Location	Address Type	IP Address
		Modem Tel. Number	
AW 1		Normal Data	
		Default IP Gateway1	
		Netmask	
AW 2		Modem Tel. Number	
		Normal Data	
		Default IP Gateway1	
		Netmask	

Signaling Access Network IP requirements

The table titled **Signaling Access Network IP Requirements** lists the IP address requirements for Unified ICM node connections to the Signaling Access Network. The Unified ICM nodes are listed as duplexed pairs (for example, CallRouter A and CallRouter B). You may or may not have duplexed nodes in your configuration. You need to supply IP addresses only for the nodes you have in your configuration

Table 22: Signaling Access Network IP Requirements

Node	Location	Address Type	IP Address
CallRouter A		Normal data	
CallRouter B		Normal data	
Network Gateway 1A		Normal data	
Network Gateway 1B		Normal data	

Static Route Requirements

The IP routers used in the Unified ICM networks must have static routes defined in order to provide the necessary connectivity between the visible LAN at the central site and the visible LANs at remote contact center sites. The static route ensures that the IP router can forward traffic from the central site to the remote site. In addition, CallRouters and Loggers must have a static route defined for the remote private LAN. This static route ensures that private network traffic is segregated from visible network traffic.

You must define all the static routes required in your configuration. However, you cannot define these static routes until you have assigned all Unified ICM nodes IP addresses.

Table 23: Static Route Requirements

Node	Network	Static Route
Central Site Visible Network IP Router—Side A and Side B	Visible	Define one static route for the visible LAN at each remote contact center site and each administrator site. If the central sites are geographically separated, add another static route for the other central site.
Central Site Private Network IP Router—Side A and Side B	Private	Define one static route for the private LAN at the other central site.
CallRouter—Side A and Side B	Private	If the sides of the central controller are geographically separated, define one static route for the subnet address of the private LAN on the other side of the central controller.
Logger—Side A and Side B	Private	If the sides of the central controller are geographically separated, define one static route for the subnet address of the private LAN on the other side of the central controller.
PG (all PGs)	Visible	One of the two IP routers at a contact center is targeted as the default gateway for the PG. However, the PG needs IP connectivity to both sides of the central controller. Therefore, for each PG you must define a static route to the other IP router (that is, to the IP router that is not targeted as the PG's default gateway IP router).
Remote Contact Center IP Routers	Visible	For each IP router, define a static route to one side of the central controller (to the central site visible network IP router).
Admin Site IP Routers	Visible	For each Admin Site IP router, define a static route to one side of the central controller (to the central site visible network IP router).

INDEX

A

Addresses 66, 68, 76–77, 79, 82, 86
- CallRouter 66, 68
- CallRouter, 79
- IP router 76–77
- Logger 82, 86
- Peripheral Gateway 86

Admin site 57
- networking 57

Admin Workstation 59
agent workstation application 37

C

CallRouter 82
configurations 78

I

IP router 85
- IP router 85

P

Peripheral Gateway 76
processor 58

S

Signaling network 78
Sites 30, 86
- central 30

T

TCP packets 77

U

UDP 77
UDP packets 77
Unshielded Twisted Pair 69

V

Visible network 71, 75
- central sites 75

W

WAN 65–66
- admin site 66
- visible 66