Lucent Technologies
Bell Labs Innovations

Internet Call Center

Version 1

Solution Guide

585-215-090
Comcode 108048398
Issue 1
September 1997

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Your Responsibility for Your System's Security

Toll fraud is the unauthorized use of your telecommunications system by an unauthorized party, for example, persons other than your company's employees, agents, subcontractors, or persons working on your company's behalf. Note that there may be a risk of toll fraud associated with your telecommunications system and, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

You and your system manager are responsible for the security of your system, such as programming and configuring your equipment to prevent unauthorized use. The system manager is also responsible for reading all installation, instruction, and system administration documents provided with this product in order to fully understand the features that can introduce risk of toll fraud and the steps that can be taken to reduce that risk. Lucent Technologies does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunication services or facilities accessed through or connected to it. Lucent Technologies will not be responsible for any charges that result from such unauthorized use.

Lucent Technologies Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical support or assistance, call the Technical Service Center Toll Fraud Intervention Hotline at 1-800-643-2353.

Trademarks

- CentreVu, DEFINITY, AUDIX, and PassageWay are registered trademarks of Lucent Technologies.
- Java, Sun, Solaris, and SPARC are registered trademarks of Sun Microsystems, Inc.
- LynxOS is a registered trademark of Lynx Real-Time Systems, Inc.
- Microsoft, Windows, NT, and NetMeeting are registered trademarks of Microsoft Corp.
- Netscape and Netscape Navigator are registered trademarks of Netscape Communications, Inc.
- pcANYWHERE is a registered trademark of Symantec Corporation.
- Pentium is a registered trademark of Intel Corporation.
- UNIX is a registered trademark licensed exclusively through X/Open Company, Ltd.
- All other product names mentioned herein are the trademarks of their respective owners.

Ordering Information

Call: Lucent Technologies Publications Center
Voice: 1-800-457-1235
International Voice: +1-317-322-6416
Fax: 1-800-457-1764
International Fax: +1-317-322-6699

Write: Lucent Technologies BCS Publications Center
2855 N. Franklin Road
Indianapolis, IN 46219
U.S.A.

Order: Internet Call Center Solution Guide
Document No. 585-215-090
Comcode 108048398
Issue 1, September 1997

For additional documents, refer to the section entitled "Related Documents" in the Preface.

You can be placed on a Standing Order list for this and other documents you may need. Standing Order will enable you to receive updated versions of individual documents or document sets automatically, billed to account information that you provide. For more information on Standing Orders, or to be put on a list to receive future issues of this document, please contact the Lucent Technologies Publications Center.

Lucent Technologies National Customer Care Center

Lucent Technologies provides a telephone number for you to use to report problems or to ask questions about your call center. The support telephone number is 1-800-242-2121.

Document Support Telephone Number

Lucent Technologies provides telephone numbers for you to use to report errors or to ask questions about the information in this document. The support telephone numbers are as follows:
Voice: 1-888-584-6366 and
International Voice: +1-317-322-6848.

European Union Declaration of Conformity

Lucent Technologies Business Communications Systems declares that the equipment specified in this document conforms to the referenced European Union (EU) Directives and Harmonized Standards listed below:

EMC Directive	89/336/EEC
Low Voltage Directive	73/23/EEC

CE

The "CE" mark affixed to the equipment means that it conforms to the above Directives.

Disclaimer

Intellectual property related to this product (including trademarks) and registered to AT&T Corporation has been transferred to Lucent Technologies Incorporated.

Any references within this text to American Telephone and Telegraph Corporation or AT&T should be interpreted as references to Lucent Technologies Incorporated. The exception is cross references to books published prior to December 31, 1996, which retain their original AT&T titles.

Heritage Statement

Lucent Technologies—formed as a result of AT&T's planned restructuring—designs, builds, and delivers a wide range of public and private networks, communication systems and software, consumer and business telephone systems, and microelectronics components. The world-renowned Bell Laboratories is the research and development arm for the company.

Warranty

Lucent Technologies provides a limited warranty on this product. Refer to the "Limited use Software License Agreement" card provided with your package.

Table of Contents

ICC Connectivity Overview

Firewall and Security Guidelines

DEFINITY ECS Within ICC

ITG and *Java* Server Guidelines

PassageWay Telephony Server Guidelines

Call Management System for Internet (ICMS)

ITG and *Java* Server Administration Field Descriptions

P

Preface

Introduction

The *Internet Call Center Solution Guide* (585-215-090) provides an overview of elements of the Internet Call Center (ICC) solution, such as operations and features, prerequisites and the baseline configuration, some troubleshooting items, and a glossary.

The Preface introduces the main elements of the document, including the following:

- Elements of the ICC Solution
- Contents of This Document
- Conventions Used in This Document
- Using This Document
- Related Documents.

Audience

This solution guide is intended for anyone installing, configuring, administering or using the ICC solution, including agents, supervisors, trainers, Webmasters, and system administrators. This document should also be useful to Lucent Technologies personnel in Technical Service Centers (TSC), Sales, the Design Support Center, the International Technical Assistance Center (ITAC), the NetCare Services organization, and the Centers of Excellence. It should also be helpful for Webmasters, data networking security personnel, firewall administrators, and anyone else who might use or support an ICC solution.

This document is intended for anyone who needs to know:

- Overall configuration and connectivity of the ICC solution
- Data connectivity for the ICC solution with the call center's network
- Operational details about the ICC solution
- *DEFINITY*® Enterprise Communications Server (ECS) switch administration and connectivity for the ICC solution
- *CentreVu*® Call Management System (CMS) connectivity, installation, and database items for the ICC solution
- New *CentreVu* CMS and Supervisor reports for the ICC solution
- *PassageWay*® Telephony Server connectivity and administration for the ICC solution
- Recommended Web page design guidelines for the ICC solution
- Firewall and security issues relative to the ICC solution
- Troubleshooting.

Contents of This Document

The *Internet Call Center Solution Guide* is organized into the following chapters:

Chapter 1	About Internet Call Center Introduces and briefly describes the *Internet Call Center solution. Includes descriptions of components, features, requirements, and how it works.*
Chapter 2	How to Process Internet Calls Provides descriptions of agent login and logout, agent / caller interactions on calls, and the "look and feel" of major ICC features.
Chapter 3	ICC Connectivity Overview Specifies the configuration and connectivity of the equipment required to use the *ICC solution*. Explains what pieces are necessary to install, configure, and administer the ICC solution.
Chapter 4	Firewall and Security Guidelines Provides a high-level overview of firewall and security for the ICC solution, including firewall administration.
Chapter 5	DEFINITY ECS Within ICC Describes the *DEFINITY* ECS administration that supports the ICC environment.
Chapter 6	ITG and Java Server Guidelines Covers installation, administration, and support of the Internet Telephony Gateway (ITG) platform and the *Java* server for the ICC solution.

Chapter 7	PassageWay Telephony Server Guidelines Lists ICC-specific items to be added and administered on the *PassageWay* Telephony Server.
Chapter 8	Call Management System for Internet (ICMS) Provides ICC-specific details about connecting *CentreVu* CMS hardware and software, descriptions of new reports on ICC activity, and information on new ICC database items.
Chapter 9	Web Page Guidelines Contains guidelines for creating or modifying Web pages for the ICC.
Chapter 10	Troubleshooting Identifies problems that may occur during installation and operation of the ICC, and suggests diagnostic and corrective actions that can be taken toward their resolution.
Appendix	ITG and Java Server Administration Field Descriptions Contains ITG / ICC configuration files and administration on-line Help for the ITG and *Java* server.
Glossary	Provides a list of terms and definitions that relate to the ICC solution.

Conventions Used in This Document

This document uses the following conventions:

Convention	Description
Initial Capital Letters	Names of windows and keyboard keys. Example: This field is in the Phone Settings window.
`Courier Text`	Text you are asked to enter, URLs, and system commands. Example: Enter `COM1` in the **COM Port** field.
KEY + KEY	Key combinations for which you must press and hold down one key while you press another. Example: **ALT+4**
Italic Text	References to other documents, trademarked names, file names, and for emphasis.
Bold Text	To identify keys and buttons. Example: the **Send Page** button
“ “	Sections and chapters that are referenced. Example: About Internet Call Center for a discussion of features and requirements.
click and double click	Whenever you are asked to click or double click the mouse button, click the left-hand, or primary button, unless the right-hand, or secondary button, is specified.
Terms	For definitions of terms and acronyms used in this guide, please see “Glossary”.

Using This Document

Basic Assumptions

This document includes stand-alone chapters for each major component of the ICC solution. This document only includes specific changes that apply to ICC. Standard installation and administration activities are covered in referenced documents for each component.

About Customer-Provided Equipment

This guide assumes that it is the call center's responsibility to procure, provision and maintain all customer-provided equipment.

About Customer Expertise

This guide assumes that the customer is familiar with basic call center operations and has the technical expertise to implement the changes for ICC described in this document.

Related Documents

Many documents besides the *Internet Call Center Solution Guide* pertain to the ICC solution. The most important documents are listed in this section. Each chapter references those documents related to the features and components discussed in that particular chapter.

- *Internet Telephony Gateway Technical Reference* (555-027-212)
- *BCS Product Security Handbook* (555-025-600)
- *CentreVu™ CMS R3V5 Administration* (585-215-820)
- *CentreVu™ CMS R3V5 Real-Time and Historical Reports* (585-215-821)
- *CentreVu™ CMS R3V5 Custom Reports* (585-215-822)
- *CentreVu™ CMS R3V5 Change Description* (585-215-823)
- *CentreVu™ CMS R3V5 Upgrades and Migration* (585-215-826)
- *CentreVu™ CMS R3V5 Sun SPARCserver Computers Connectivity Diagram* (585-215-828)
- *CentreVu™ Report Designer Version 5 User Guide* (585-215-831)
- *CentreVu™ Supervisor Version 5 User Guide* (585-215-829*)
- *CentreVu™ Supervisor Version 5 Installation and Getting Started* (585-215-830)
- *CentreVu™ Supervisor Version 5 Change Description* (585-215-832)
- *DEFINITY Enterprise Communications Server Release 5 Implementation* (555-230-302)
- *DEFINITY Communications System, Generic 3, Installation, Administration, and Maintenance of CallVisor ASAI over the DEFINITY LAN Gateway* (555-230-223)
- *DEFINITY Communications System Call Vectoring/EAS Guide* (555-230-520)

*This document is also available in the following languages: French (FR), Dutch (NL), Japanese (JA), Portuguese (PTB), German (DE), and COlumbian Spanish (ESC). A two- or three-letter code after the ordering number indicates the language of the document.

- *DEFINITY Communications System Implementation* manual (555-230-655)
- *DEFINITY Communications System Generic 3 Feature Description* manual (555-230-204)
- *DEFINITY Communications System Generic 3 System Description and Specifications* manual (555-230-206)
- *PassageWay Telephony Services Solution, Microsoft* Windows† NT‡ Telephony Services, DEFINITY ECS Network Manager's Guide* (555-201-505)—This document is available on the CD-ROM provided during installation.
- *PassageWay Telephony Services Solution, Microsoft Windows NT Telephony Services, Network Manager's Guide* (555-201-506)—This document is available on the CD-ROM provided during installation.
- *PassageWay Telephony Services Solution, Microsoft Windows NT Telephony Services Installation Guide* (555-201-116)—This document is available on the CD-ROM provided during installation.

*Microsoft is a registered trademark of Microsoft Corp.
†Windows is a registered trademark of Microsoft Corp.
‡NT is a registered trademark of Microsoft Corp.

1

About Internet Call Center

Introduction

The Internet Call Center (ICC) solution provides access, call management, transaction processing, and management information support to integrate World Wide Web (WWW) and call center functionality. The ICC solution accomplishes this by means of a combination of premises-based hardware, software, and NetCare Services for call center sales and service environments.

This chapter introduces the ICC solution, including discussions of major components, features, and system operations in general. Specific topics covered by this chapter include:

- Elements of the ICC Solution
- ICC Features
- How ICC Works
- Caller Requirements
- Product Assistance.

Audience

This chapter is intended for anyone interested in an overview of the ICC solution, features and elements of the solution, and how it is supported before and after the sale.

Elements of the ICC Solution

The ICC solution incorporates and integrates several new and existing platforms. This section presents solution components, a summary of associated requirements, and an overview of how they operate within the ICC solution.

Internet Telephony Gateway (ITG)

The ITG is an industrial grade, *Pentium*[*]-based PC running *LynxOS*[†] (a *UNIX*[‡]-compatible operating system). The ITG is supplied by Lucent Technologies as part of the ICC offer. It contains one or more voice processing boards to convert between packetized Internet voice and circuit-switched voice used by the *DEFINITY*® Enterprise Communications Server (ECS).

The ITG houses the Computer-Telephony Integration (CTI) processes that communicate with the PassageWay Telephony Server. These processes allow the ITG to log agents in and out of *DEFINITY* ECS skills, monitor calls placed into the *DEFINITY* ECS, and place outbound Callback calls.

See the *Internet Telephony Gateway Technical Reference* (555-027-212) for details.

Java[**] Server

The ICC offer requires installation of a separate server supplied by the call center. During ICC installation, Lucent Technologies personnel load the *Java* server software used for ICC, scripts, and certain Web pages onto this server. The requirements for this include:

- A *Pentium*-based PC with at least 32MB of RAM, a CD-ROM drive and an Ethernet network interface card (NIC)

---

*Pentium is a registered trademark of Intel Corporation.
†LynxOS is a registered trademark of Lynx Real-Time Systems, Inc.
‡UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.
**Java is a registered trademark of Sun Microsystems, Inc.

- *Microsoft*[*] *Windows*[†] *NT*[‡] 4.0 Server operating system with Service Pack 1 or greater
- *Microsoft* Internet Information Services (IIS) software.

The *Java* server hosts *Java* applets for the agent and caller, as well as certain Web pages and CGI scripts.

See Chapter 6, "ITG and Java Server Guidelines," and the *Internet Telephony Gateway Technical Reference* (555-027-212) for detailed information.

PassageWay Telephony Server

The ICC offer requires installation of a separate server supplied by the call center to host *PassageWay Telephony Services for Windows NT* (Release 2.22, Version 4.4 or greater) software. Requirements for this server include:

- A *Pentium*-based PC with 32MB of RAM, a CD-ROM drive and two Ethernet NICs, one for local area network (LAN) access and the other to connect to the *DEFINITY* LAN Gateway.
- *Microsoft Windows NT* 4.0 Server operating system with Service Pack 2 or greater.

This server sends and receives information to and from the *DEFINITY* ECS, and provides a Telephony Services Application Programming Interface (TSAPI) to the ITG subnet. This server also provides a standard CTI interface which allows the ITG to monitor and control activities that take place in the *DEFINITY* ECS, acting somewhat like a proxy for all requests to and from the *DEFINITY* ECS. It serves to isolate the *DEFINITY* ECS Adjunct/Switch Applications Interface (ASAI) and provides a standard interface (TSAPI) with which the ITG controls ICC call functions.

See the documentation on the CD-ROM provided with the *PassageWay* Telephony Services software for details.

---

*Microsoft is a registered trademark of Microsoft Corp.
†Windows is a registered trademark of Microsoft Corp.
‡NT is a registered trademark of Microsoft Corp.

DEFINITY ECS

Requirements for *DEFINITY* ECS software include version G3V4 or greater, Expert Agent Selection (EAS), vectoring, ASAI Proprietary Adjunct links, Primary Rate Interface (PRI) hardware and software, and the *DEFINITY* LAN Gateway.

The *DEFINITY* ECS is a digital switch that processes and routes voice communications. It also houses sophisticated Automatic Call Distribution (ACD) software that allows any voice terminal (telephone) on the *DEFINITY* ECS to act as a call center agent terminal. The ICC solution utilizes the *DEFINITY* ECS's advanced ACD features to process and route ICC calls to the appropriate endpoints. The ICC uses the ASAI feature on the *DEFINITY* ECS via a TSAPI to integrate the data networking portions of the ICC solution with the *DEFINITY* ECS CTI. This interface provides capabilities such as call progress monitoring, third party call control, and agent state changes (log in, log out, AUX mode, and so on).

There are ICC installation and administration requirements for the *DEFINITY* ECS. See Chapter 5, "DEFINITY ECS Within ICC," for details.

CentreVu Call Management System (CMS) and Supervisor

ICC requires additional *CentreVu* CMS for Internet (ICMS) software installed on a *CentreVu* CMS R3V5 or greater system (with ai.f or greater load software). *CentreVu* CMS for ICC must be on a Sun *SPARC*[*] server running *Solaris*[†] which is LAN-connected and augmented with a 2GB external disk. *CentreVu* Supervisor, Version 5 (with the bj.02 or greater load), and CMS provide a call center with a series of reports on Internet-initiated call activity.

ICMS collects ICC-specific data such as Web page hits, call requests when there are no ISDN-PRI trunks available, call requests when there are no agents logged in, and voice call requests when there are no resources available to perform the Internet Voice-to-PSTN Voice transcoding.

See Chapter 8, "Call Management System for Internet (ICMS)," for detailed information.

---

*SPARC is a registered trademark of Sun Microsystems, Inc.
†Solaris is a registered trademark of Sun Microsystems, Inc.

Call Center Data Infrastructure

The call center environment has LAN connectivity to agent PCs, to the Web server, between the *PassageWay* Telephony Server, the *Java* server, and the ITG, and between the *DEFINITY* LAN Gateway and the *PassageWay* Telephony Server. The call center also has connectivity to the Internet with access through the firewall (if any) to the ITG, *Java* server, and *CentreVu* CMS.

Firewall/Security

The ICC offer contains strong recommendations about the necessity of protecting organizational data and restricting access via the Internet and telephone lines.

See Chapter 4, “Firewall and Security Guidelines,” for detailed information.

NetCare Services

Because the ICC offer is complex, spans several platforms, and is tightly integrated with individual call center environments, NetCare Services plays a key role in integrating and suporting the ICC solution for each call center. They can be reached at 1-800-4NetCare.

ICC Features

This section lists and describes the significant functional features of the ICC solution.

- ICC agents can answer both Internet-initiated and conventional (audio-only) telephone calls. Regular telephone calls as well as Internet telephony calls are delivered to the agent's voice terminal, so the agent answers all calls using a single headset or handset.
- The ICC solution provides callers with several ways to contact an agent:
  - — Text Chat enables agent and caller to type and send messages to each other's desktops by means of the downloaded Agent and Caller Control Windows.
  - — Internet telephony enables callers to talk with agents via an existing Internet connection using the multimedia capabilities of their computers and only one phone line.
  - — Caller-requested PSTN Callback enables callers whose computers are not equipped for Internet telephony, or who are located behind firewalls, to request that an agent call them on a regular telephone line.
  - — Agent-initiated PSTN Callback is useful if voice quality degrades during a call. In that case, the caller would provide a telephone number and the agent would call the caller back.
- The Web Pop feature provides Web-based information to the caller and agent at the beginning of a call:
  - — The caller may browse the Internet while awaiting connection with an agent. Web Pop returns the browser to an administered Web page when an agent is connected.
  - — The content of the Web page presented to an agent when a call is connected is administrable by the call center. This may include the Web page that the caller called from or information that was entered by the caller prior to the call and / or information extracted from a database based on some caller identification.

- During a call, agent and caller can use their browsers to navigate to other Web pages or sites. The Escorted Browsing feature provides two ways in which the parties can share Web pages with each other.
  - — Either party can use the **Send Page** button to synchronize the other's browser to the Web page they are currently viewing.
  - — Either party can type (or copy and paste) a Uniform Resource Locator (URL) into the Text Chat window and send that message to update both parties' browsers with the contents of that URL. Note that a URL that is normally inaccessible to one party (for example, behind a firewall) remains inaccessible during Escorted Browsing.
- Call centers can collect data on Internet-initiated calls and then view reports to display Internet call statistics via *CentreVu* CMS and Supervisor.
- Both agent and caller have the ability to end a call.
- When a callback is placed to a caller who has a second phone line, the caller may continue to have Escorted Browsing and Text Chat available via the Internet connection and also talk with an agent on the phone.

How ICC Works

In a typical ICC facility, agents log into the call center via a Web page, using a browser on a desktop. A *Java*-based Agent Control Window is launched on the agent's desktop to complete the login process and, later, to provide an interface for Text Chat and Escorted Browsing during calls. After the agent logs in, an association is made by the ITG between the agent's phone, the Web browser, and the Agent Control Window.

A typical call starts with a person surfing the Web who discovers a need to contact the call center and selects a **Call Us** button on a Web page. A Call Us window opens. The caller enters a name and telephone number (and any other information requested), and then selects a type of call to request:

- **Voice and Chat**—an Internet telephony call with Text Chat,
- **Chat Only**—a Text Chat call with no voice, or
- **Call Back Only**—to have an agent call back using a regular telephone line.

The caller then submits the request by means of the **Call Us** button.

NOTE:
The caller's desktop must meet certain requirements in order to place an Internet telephony or Text Chat call successfully; see the "Caller Requirements" section of this chapter.

If the caller requests a call type other than Call Back Only, a Caller Control Window is downloaded to the caller's desktop. The Caller Control Window provides call progress status, enables the Text Chat and Escorted Browsing functions, and allows the caller to end the call.

The ITG launches a call across a PRI facility to the *DEFINITY* ECS, where the call is queued, awaiting an available ICC agent.

When an agent becomes available, the call is delivered to the agent's phone (for example, a *Callmaster*® voice terminal). When the agent answers the phone, the *PassageWay*® Telephony Server sends a "call answered" message to the *Java* server by way of the ITG. The *Java* server delivers a URL to the agent's browser via Web Pop, which displays information related to the call including any information entered by the caller.

After the call is answered, the caller and agent communicate via the Text Chat box in their respective Control Windows and may share Web pages by means of the Escorted Browsing feature. If the call is an Internet telephony call, they may also talk to each other, the agent using a phone and the caller using a headset or microphone and speakers connected to the desktop.

If a callback is requested, a window opens on the agent's desktop displaying the phone number for the callback. The agent has the opportunity to screen this number, then clicks a button to launch a voice call over the PSTN to the caller.

During a session, statistics for ICC calls are collected using *CentreVu* CMS. In addition, page hits on ICC Web pages and other ICC-related statistics are collected on the *CentreVu* CMS server. Statistics are collected whenever HTTP requests are placed to Web server software running on *CentreVu* CMS. Statistics are collected and stored in a database similar to the ones used for traditional telephone calls.

Either party has the capability to end the session.

See Chapter 2, "How to Process Internet Calls," for details on how ICC works from an agent's point of view.

Caller Requirements

The caller's environment should consist of a desktop or workstation with the following:

- *Microsoft Windows* 95 or *Windows NT.* Systems running Mac OS 7.1 or above, *Solaris*, and *Sun*[*] OS currently support Text Chat, Escorted Browsing and PSTN Callback but not Internet telephony.
- A *Java*-enabled Web browser, such as *Microsoft* Internet Explorer 3.x[†] or *Netscape Navigator*[‡] 3.x. Note that 4.x versions of these browsers currently support all features except the **Send Page** button.
- Multimedia components (a sound card, plus a headset or speakers and a microphone) to enable Internet voice.
- A single telephone line for Internet voice, Text Chat, and non-collaborative callback. A second phone line is required to support collaborative PSTN callback.
- Access to the Internet via modem or other network connection. Internet voice sessions require a connection speed of 28.8kbps; Text Chat sessions require 14.4kbps.
- *Microsoft NetMeeting*[**] 2.0 or greater software to provide Internet telephony capability.

---

*Sun is a registered trademark of Sun Microsystems, Inc.
†x = digits or combinations of digits.
‡Netscape Navigator is a trademark assigned to Netscape Communications Corp.
**NetMeeting is a registered trademark of Microsoft Corp.

Agent Environment

The agent's environment consists of the following:

- A desktop on the LAN.
- *Microsoft* Internet Explorer 3.x or *Netscape Navigator* 3.x, with *Java* enabled.

  NOTE:
  The 4.x versions of these browsers currently support all ICC functionality except the **Send Page** button.

- A voice terminal associated with the *DEFINITY* ECS call center.

  NOTE:
  PC speakers and microphones are not required because voice is carried through the telephone.

Product Assistance

Training Considerations

ICC training is provided on site, as part of the ICC installation process, to help agents learn how to operate the software.

ITG administration training is also conducted on site as part of the ICC installation process. The training is intended for those responsible for administration of the ITG server and for trouble resolution.

Training is available from Lucent Technologies for all other aspects of call center operations, in classroom, CD-ROM or video format. The ICC solution is included as part of standard call center training.

Optional Professional Services

Lucent Technologies provides a wide array of Professional Services offerings to assist with the Internet Call Center solution. These offers include:

- Network Integration Services—This offer provides engineering assistance in planning, provisioning, and upgrading an Internet Call Center.
- Call Center Application Integration Services—This offer provides an experienced Lucent Technologies Call Center consultant to evaluate a call center and engineer the optimum configuration for it.
- Call Center Tune-Ups—This service is provided on an as-needed basis or seasonally, to fine-tune a call center's configuration and translations based upon available reports and feedback.
- Firewall Offers—The Lucent Technologies Network Consulting Group can engineer, provision and maintain a new or existing firewall. They also offer testing of an existing infrastructure to ensure security. Equipped to provision and administer the leading enterprise firewall product offerings, the Network Consulting Group can help ensure that a network provides the access its callers require while protecting valuable internal resources.

- Data Networking Equipment and Services—The Lucent Technologies Advanced Data Networking Group can engineer and provision industry-leading solutions from Lucent Technologies, Agile (a Lucent Technologies Company), Bay Networks, Ascend, Paradyne, Hypercom, and other leading edge companies. Solutions are maintained and monitored by Lucent Technologies' NetCare Services, the oldest and largest network management service in the industry. Lucent's data networking solutions provide solid, highly available infrastructures on which to base business applications.

Lucent Technologies has highly trained and experienced resources ready to work for you. If you are interested in the above offers, or to inquire about other services, contact 1-800-4NetCare for details.

Call Center Helpline

1-800-242-2121 is the Helpline number that connects clients with the appropriate service organization for repair or assistance. This number is valid for all Lucent Technologies products.

Customers calling this number are asked to identify the product or offer (such as ICC) involved and to describe the problem. A trouble ticket is generated so the problem can be tracked throughout the services organization.

Helpline services, with the exception of consultative services, are provided to customers whose product is covered by warranty or a valid maintenance contract during the hours specified by the contract. A customer whose product is not covered by warranty or a maintenance contract may still utilize these services for the appropriate time and materials charges.

2

How to Process Internet Calls

Introduction

This chapter details how an Internet Call Center (ICC) agent logs in, handles various types of incoming calls, and logs out. The call-handling information covers Web Pop, Escorted Browsing, and Call Control Windows.

This chapter includes the following:

- Agent Login
- Agent Control Window
- Caller Control Window
- Receiving Calls
- Dropping Internet Calls
- Dropping Callback Calls
- Agent Logout.

Audience

This chapter is intended as an overview for anyone who needs to know how various types of incoming calls are handled by the ICC system and how they appear to the consumer and to the agent.

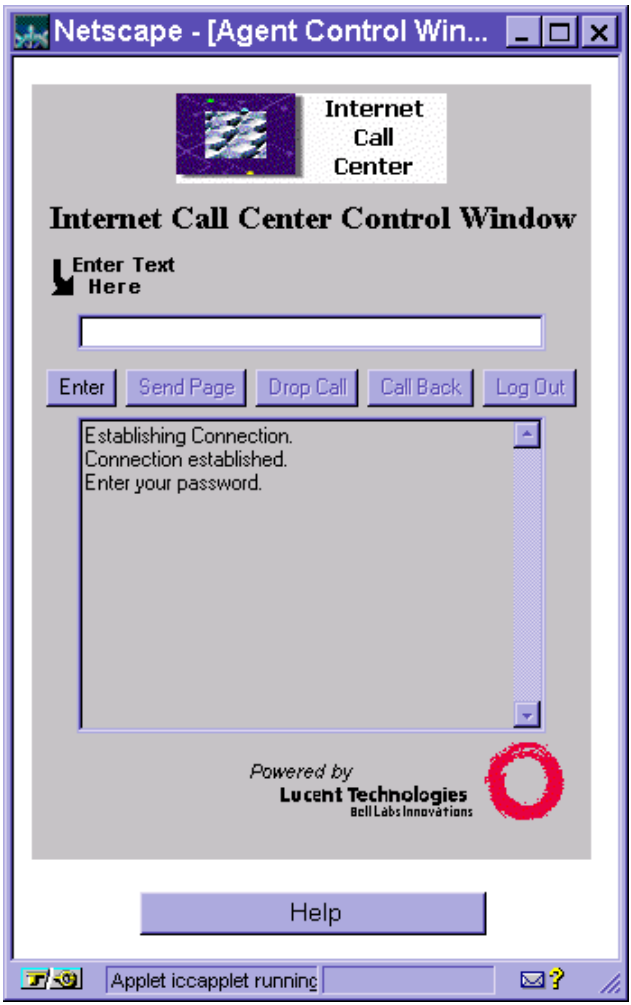
Agent Login

In order to take Internet calls, an agent must first register with the Internet Call Manager (ICM). The following steps describe how an agent logs in.

1. In the location or address field of your Web browser, enter the Uniform Resource Locator (URL) for the Agent Login screen. The Agent Login screen opens. The following is a sample Agent Login screen:

2. Enter your agent ID, extension, your name, and any additional items requested.

A new window, the Agent Control Window, appears as follows:



Notice that most of the control buttons are greyed out. Control buttons become active when a call is connected.

3. Enter your password, if any, into the text entry field labeled **Enter Text Here**, then select either **Enter** on the keyboard or the **Enter** button.

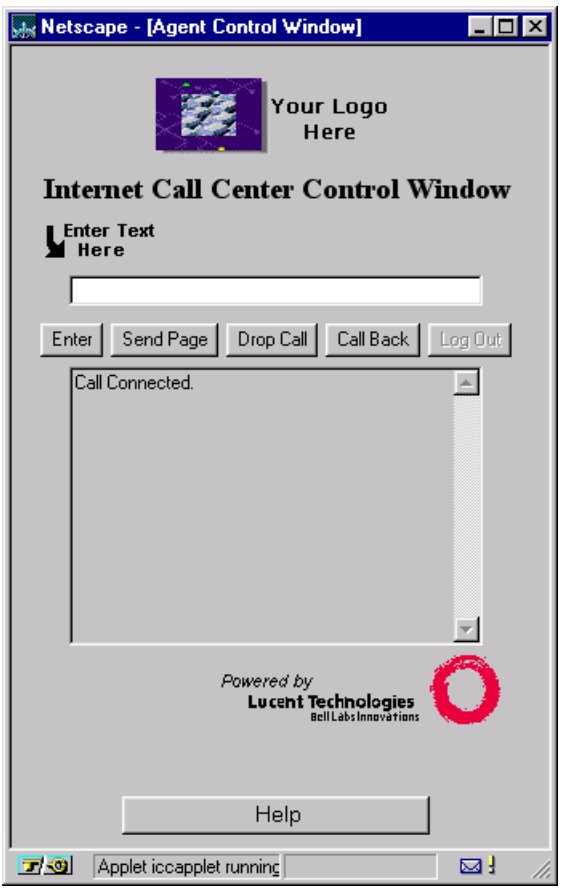
4. If no password is required, select **Enter** on the keyboard.

A series of connection status messages is displayed. If the login process fails, an error message is displayed and you are prompted to try again. If login succeeds, the last status message you see is “Waiting for a call.” The Agent Control Window also indicates that you are in the “Agent Idle” state. At this point, you can either accept calls or log out.

5. When you are ready to take calls, put your voice terminal in Manual-In or Auto-In mode.

Agent Control Window

After an agent is logged in and a call is connected with that agent, the Agent Control Window appears as follows:



The top of the Agent Control Window optionally displays your company's logo and title.

NOTE:
The company logo is definable by each call center. See Chapter 9, "Web Page Guidelines," for information.

The Agent Control Window has a text entry field indicated by an arrow and labeled **Enter Text Here**. Assuming default browser colors, the text entry field is white when it is active, indicating that text can be entered, and appears grey when it is inactive.

Information that can be entered into the text entry field includes: the agent's password (during agent login); text to be sent to the Caller Control Window (for Text Chat); and a URL to display the specified Web page in both the agent and caller's browser windows. The text entry field also supports copy-and-paste entries.

The text entry field is only active when an agent is logging in or on a call. When finished typing in text, either click the **Enter** button with the mouse, or press the **Enter** key on the keyboard. The text is then sent to the *Java* server for processing.

NOTE:
In *Netscape Navigator** in a *Windows*† environment, the text field is limited because that browser does not support either word wrap or a horizontal scroll bar for *Java* applet text boxes. You can use a carriage return whenever the text you are entering nears the right edge of the text display box. At the same time, keep in mind that each Text Chat message has either "Agent:" or "Caller:" inserted at the beginning to identify who sent it.

If an agent or caller receives a Text Chat message that runs beyond the text field on the right, it may seem that they cannot read the text because there is no horizontal scroll bar. However, they can click in the text field and use the arrow keys on the keyboard to access and read the text.

Below the text entry field is a row of buttons. The text of a button label is black when it is enabled and can be selected; otherwise it appears grey.

- The **Enter** button is used to submit information from the text entry field to the *Java* server for processing.
- The **Send Page** button is used for Escorted Browsing. When a Web page of interest is displayed in the agent's Web browser window, pressing this button sends the URL of that Web page to the caller's Web browser, which attempts to load the URL. This button is only enabled when the

*Netscape Navigator is a trademark assigned to Netscape Communications, Inc.
†Windows is a registered trademark of Microsoft Corp.

agent is involved in an active call. Alternatively, URLs can be entered in the text entry field and sent like a message to support Escorted Browsing.

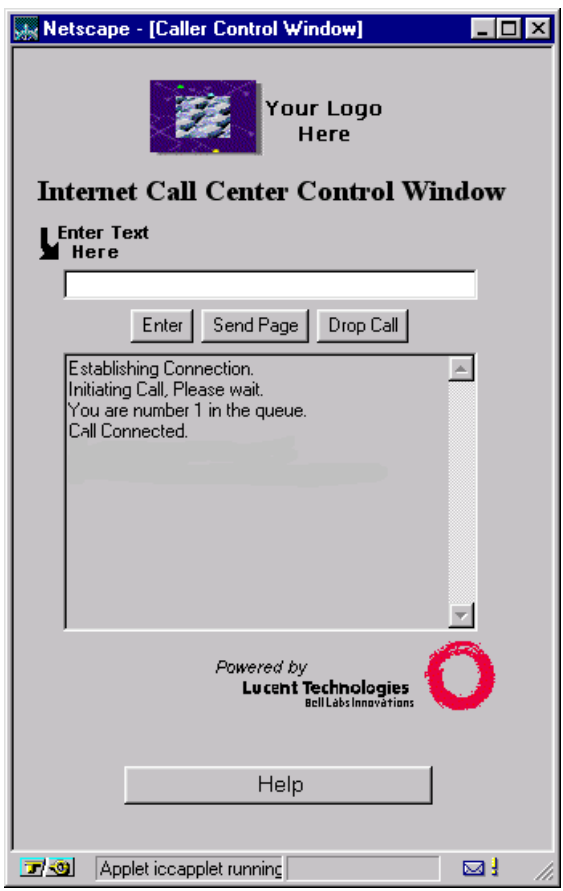
- The **Call Back** button is used to initiate a Public Switched Telephone Network (PSTN) callback to the caller. It is active when the agent is on a call and not already involved in a callback. Use of this button is explained in greater detail later in this chapter.
- The **Log Out** button is enabled (if so administered) to log out an agent from the Automatic Call Distribution (ACD) and disconnect the agent from the *Java* server so that the agent can no longer receive Internet calls. This button is enabled only when an agent is logged in but is not active on a call. (See Chapter 9, "Web Page Guidelines," for information.)

Below the row of buttons is the text display box. This is where text information is displayed, including Text Chat, prompts, status messages, and error messages.

- Below the text display box is the Lucent logo and, at the very bottom, the **Help** button. Press the **Help** button to display help information in a separate browser window.

Caller Control Window

The Caller Control Window resembles the Agent Control Window and enables the caller to view call status, perform Escorted Browsing and Text Chat, and drop calls. The following is a sample Caller Control Window:



The layout of the Caller Control Window is essentially the same as the Agent Control Window, except that it has neither a **Call Back** button nor a **Log Out** button. Caller-initiated callback is requested from the Web "Call Us" page. (See the "Agent Control Window" section for a discussion of the **Enter**, **Send Page** and **Drop Call** buttons and the **Enter Text Here** text field.)

Various status and error messages may appear in the text display box of the Caller Control Window. These include the following:

- "No facilities are currently available" is displayed when there are no Primary Rate Interface (PRI) lines available to complete the call.
- "No agents are currently available" is displayed when no agents are logged in, or no agents are staffed in the proper skills to handle a particular type of incoming call.
- "Internet telephony capacity exceeded" is displayed when the limit of Internet voice calls has been reached.
- "You are number **n** in the queue" is displayed when there are more callers than agents available to handle calls.

  NOTE:
  Number-in-queue information is displayed once and is not updated.

- "Call connected" is displayed when an agent successfully receives the call and communication is established.
- "Callback disabled" is displayed when the callback feature has been disabled via the Web administration page.

  NOTE:
  Callback is only disabled for caller-initiated Callback. Agent-initiated PSTN Callback is always available regardless of the Web administration setting.

See Chapter 6, "ITG and Java Server Guidelines," for information on how to administer the URLs for these messages.

Receiving Calls

There are three types of calls an agent can receive from the ICC:

- Voice and Chat
- Chat-Only
- Request for Callback.

In all cases, when a call comes into the agent, the agent's voice terminal alerts the agent of an incoming call and is active for the call whether or not voice is used (for example, voice is not used during a Chat-Only call).

If the Vector Directory Number (VDN) of Origin Announcement (VOA) feature is used, the agent hears a brief announcement to indicate the type of call that is coming in (for example, "Voice" or "Chat"), depending on how the VDN of Origin announcements are administered in a particular call center. The Agent Control Window displays the "call connected" message and the agent's browser updates with a Web Pop.

Chat-Only Calls

When a caller requests a Chat-only call, the following events occur:

- The Caller Control Window is downloaded to the caller's desktop.
- Call control functions on the Agent Control Window are enabled.
- Agent and caller can communicate via Text Chat by typing text into the text entry field and selecting either the **Enter** key or the **Enter** button.
- Escorted Browsing is supported in one of two ways:
  - — Clicking on the **Send Page** button in the Control Window. (The 4.0 or greater versions of *Microsoft* Internet Explorer and *Netscape Navigator* do not support the **Send Page** button.)
  - — Typing a URL (including the `http://` designation) in the text entry field in the Control Window and then pressing **Enter.**

  Either of these methods results in display of the same Web page to both the agent and the caller.

Voice and Chat Calls

When a caller requests a call that involves both Internet telephony and Text Chat, the following occurs:

- The Caller Control Window is downloaded to the caller's desktop.
- Call control functions on the Agent Control Window are enabled.
- *NetMeeting** is launched on the caller's desktop.

  NOTE:
  To use *Netscape*, configure *NetMeeting* as follows:

  — When the "unknown file type" pop-up window appears, select the **Pick App** button.

  — Under "configure external viewers", enter `rundll32.exe msconf.dll,OpenConfLink`.

  — Select **OK**.

  — *NetMeeting* should launch.

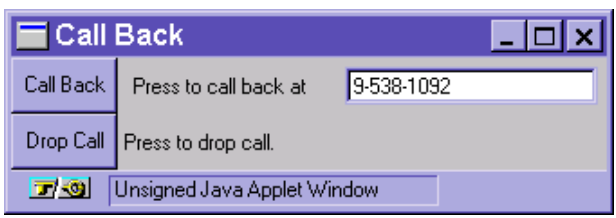
- The call may be queued, with appropriate status message / Web pages being delivered to the caller's desktop.
- The call is delivered to an agent.
- The agent and caller's browsers update to the "call answered" URL.
- The agent communicates with the caller by voice over the Internet via voice terminal. The caller communicates with the agent via microphone and speakers (or headset) via PC.
- The Text Chat and Escorted Browsing features work as described previously.

*NetMeeting is a registered trademark of Microsoft Corp.

Caller-Initiated Callback

A caller can request a callback by an agent. In such a case, the caller wants to receive a call from an agent over the PSTN. Here is how caller-initiated callback works:

- The caller enters a telephone number and requests a callback from the "Call Us" Web page.
- Once the caller has processed a request for callback and is awaiting a response from an agent, the caller sees a Web Pop page with a message, such as "We will be calling you back shortly." If the caller only has a single telephone line, the caller should immediately disconnect from the Internet to make that line available for the callback.
- In the call center, an agent is selected and the callback request is delivered to that agent in the form of a window displaying the requested callback number, as follows:



- The agent has two options:
  - — Proceed with the callback. The agent selects the **Call Back** button to call the number displayed.
  - — Cancel the callback. Selecting the **Drop Call** button results in termination of the call. There is no indication to the caller that the callback is not being processed.
- If the agent proceeds with the callback, the Internet call is put on hold on the agent's voice terminal and an outbound call is placed to the displayed number using a second telephone line.

- The caller receives the PSTN call by telephone, and the caller and agent conduct voice communication.

NOTE:
When a caller requests a callback from the "Call Us" Web page, no Caller Control Window is downloaded to the caller's desktop; therefore, the Text Chat and Escorted Browsing features are not available.

Agent-Initiated Callback

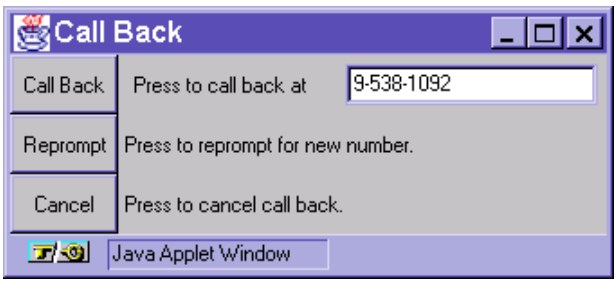
Sometimes Internet telephony voice quality deteriorates during a call, or for some other reason the agent and caller want to talk on a regular telephone line. The caller can request a callback in such instances; however, only the agent can place a callback during a call.

During Voice and Chat calls or Chat-Only calls, the **Call Back** button in the Agent Control Window is enabled. By pressing this button, an agent can request the caller to submit a phone number where the agent can reach the caller via the PSTN. Here's how it works:

- The agent clicks the **Call Back** button in the Agent Control Window.
- The caller is prompted to submit a phone number to the agent via a pop-up window, as follows:

- The caller enters and submits a phone number.

- The agent receives a pop-up window that displays the submitted phone number, as follows:



- The agent has three options:
  - — Proceed with the callback. To proceed with the callback, the agent selects the **Call Back** button.
  - — Request the caller to resubmit a callback number. This request basically begins the agent-initiated callback process again. To ask the caller for another number, the agent selects the **Reprompt** button.
  - — Cancel the callback. Selecting the **Cancel** button results in termination of the call. There is no indication to the caller that the callback is not being processed.

Proceeding with the call results in the following:

- On the agent's voice terminal, the original Internet call line is put on hold and an outbound call to the displayed number is placed on a second line. If the original Internet call was a Voice and Chat call, this means that the Internet voice connection is suspended or put on hold.
- The caller receives the PSTN call, and the caller and agent conduct voice communications.
  - — If the caller has more than one phone line, the caller can maintain an Internet connection and participate in Text Chat and Escorted Browsing with the agent while talking on the telephone.
  - — If the caller has only one telephone line, the caller must disconnect from the Internet to receive the callback, thereby losing the Text Chat and Escorted Browsing features.

Dropping Internet Calls

There are several ways to drop calls for both the agent and the caller. Different methods of dropping a call may impact what part of a call is dropped.

Voice and Chat or Chat-Only Calls

Voice and Chat calls and Text Chat-only calls may be dropped in several ways, as follows:

- Either the agent or the caller can drop the call by clicking the **Drop Call** button on the Control Window. In this case, the entire call is dropped and the agent is returned to the Agent Idle state.
- If either the agent or the caller exits the Web browser during a call, the entire call is dropped.
- The agent can drop the entire call by hanging up the voice terminal or by pressing the **Release** button.
- Although it is not recommended, if either the agent or the caller closes the Control Window during a call, the entire call is dropped.

Dropping Callback Calls

Caller-Initiated Callbacks

During a caller-initiated callback, the caller can drop the entire call by hanging up the telephone. (There is no caller applet and therefore no Text Chat or Escorted Browsing to disable.) Likewise, the agent can drop the entire call by hanging up the voice terminal.

If the agent clicks the **Drop Call** button in the Agent Control Window, the agent is presented with the option to either **Cancel** or **Drop Call**. Selecting **Cancel** results in cancelling the request to drop the call, and the call is unaffected. Selecting **Drop Call** results in the entire call being dropped and the agent's being returned to the Agent Idle state.

If for some reason a caller-initiated callback doesn't go through (such as a busy signal), the agent can press the **Drop Call** button and receive the following options:

- **Cancel**—to cancel the drop request
- **Drop Call—**to drop the entire call and return to the Agent Idle state
- **Drop and Re-Dial**—to drop the entire call and automatically re-dial the number submitted by the caller.

Agent-Initiated Callbacks

During an agent-initiated callback, the following call drop scenarios are handled as indicated:

- If the caller hangs up the phone, only the PSTN portion of the call is dropped. If the original Internet call was a voice call, then Internet voice, Text Chat, and Escorted Browsing are unaffected and thus still available.
- If the caller closes the Caller Control Window or clicks on the **Drop Call** button, the entire call is dropped and the agent is returned to the Agent Idle state.

- If the caller exits the Web browser, the entire call is dropped and the agent is returned to the Agent Idle state.
- If the agent releases the call from the voice terminal, the PSTN portion of the call is dropped (because there are actually two active lines). Internet voice (if applicable), Text Chat, and Escorted Browsing are still available. The agent must again release the call to end the entire call.
- If the agent clicks the **Drop Call** button in the Agent Control Window, the following options are offered:
  - **Cancel**—to cancel the drop request
  - **Drop Call**—to drop the entire call and return to the Agent Idle state
  - **Drop Callback**—to drop only the PSTN portion of the call and resume the Internet voice (if applicable), Text Chat and Escorted Browsing features.
- If for some reason an agent-initiated callback doesn't go through (such as a busy signal), the agent can press the **Drop Call** button and receive the following options:
  - **Cancel**—to cancel the drop request
  - **Drop Call**—to drop the entire call and return to the Agent Idle state
  - **Drop and Re-Dial**—to drop the entire call and automatically re-dial the number submitted by the caller
  - **Drop Callback**—to drop only the PSTN portion of the call and resume using the Internet voice (if applicable), Text Chat and Escorted Browsing features.

Agent Logout

Agents can log out from the voice terminal. This logout procedure is always available and logs the agent out of all Internet Call Center solution equipment. If reason codes are administered and desired, the agent should log out this way.

Using the **Log Out** button (when enabled) from the Agent Control Window is another method for logging out of the Internet Call Center. Enabling / disabling the **Log Out** button is an administrative option on the ITG. See Chapter 6, “ITG and Java Server Guidelines,” for details. If the agent logs out this way, the default reason code is recorded.

In either of these cases, the agent receives a "Connection terminated. Please quit" message on the Agent Control Window. The agent can close the Agent Control Window and / or browser after receiving this message.

NOTE:
Neither closing the Agent Control Window nor closing the browser is recommended as a logout method.

3

ICC Connectivity Overview

Introduction

This chapter provides an overview of how Internet Call Center (ICC) components are positioned into the existing local area network (LAN) and call center environment. It identifies hardware components and network integration considerations for installation and maintenance of ICC components.

This chapter includes the following sections:

- ICC Connectivity
- ICC Components and Connectivity
- Ancillary ICC Components
- Functional Descriptions.

Audience

Installers, system administrators, or any other persons involved in connecting or installing hardware or software for the ICC. This includes Lucent Technologies' Technical Support Organizations.

References

The following documents contain information relevant to the connectivity of the ICC solution:

- *Internet Telephony Gateway Technical Reference* (555-027-212)
- *DEFINITY Communications System Generic 3 System Description and Specifications* manual (555-230-*206)*
- *DEFINITY Communications System Generic 3 Installation, Administration, and Maintenance of CallVisor ASAI over the DEFINITY LAN Gateway* (555-230-223).

ICC Connectivity

Topology Overview

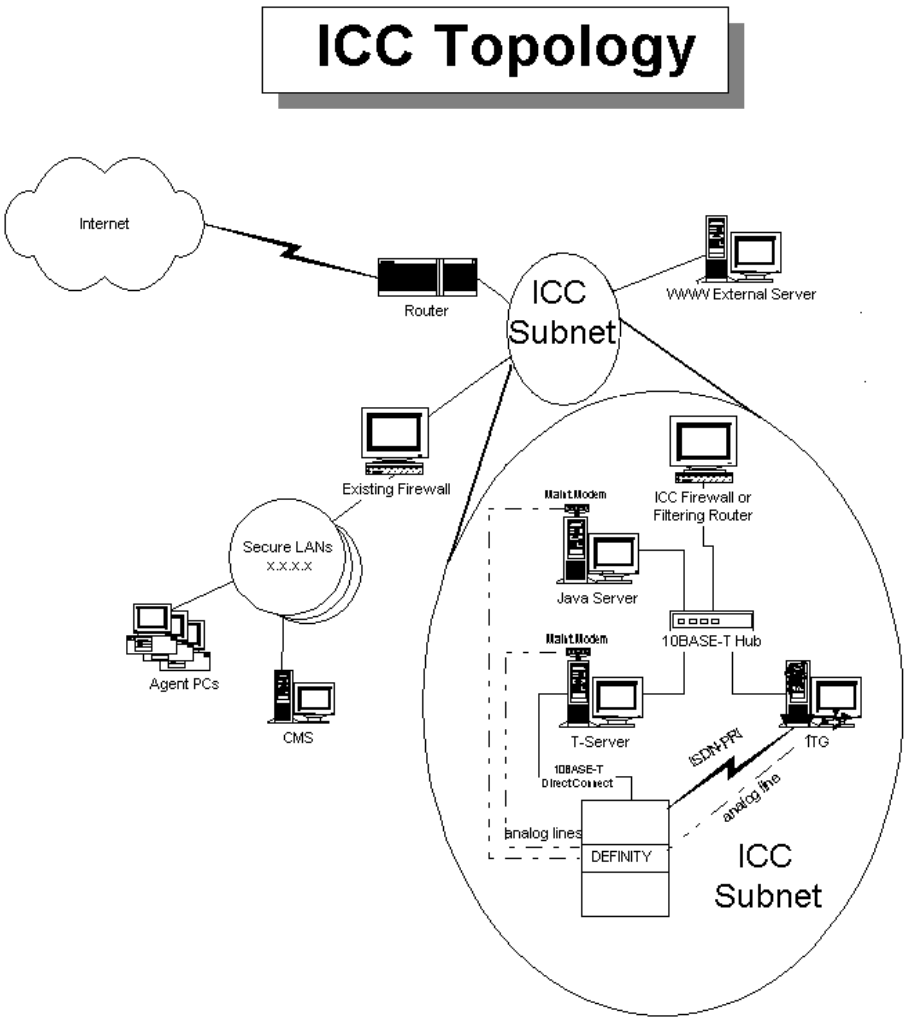
The ICC solution involves several platforms and related offers, including:

- Internet Telephony Gateway (ITG)
- *Java** server
- *DEFINITY*® Enterprise Communications Server (ECS)
- *Passageway*® Telephony Server
- *CentreVu*® Call Management System (CMS)
- *CentreVu* Supervisor
- the call center's local area network (LAN) consisting of intervening switches, routers, and hubs
- the call center's wide area network (WAN) consisting of intervening routers
- the call center's Web server
- the call center's firewall.

All of these components are involved in the ICC solution, and all must be managed correctly for full ICC functionality. Subsequent chapters detail how these components are administered and connected for the ICC solution.

*Java is a registered trademark of Sun Microsystems, Inc.

The figure which follows represents a typical ICC topology. The ICC subnet is not firewalled from the Internet to the same extent that internal, secure LANs are.



Topology Discussion

Components of the ICC solution are best provisioned using the topology just shown. This topology is advantageous in several ways.

The first advantage is that ports and protocols required by ICC can be allowed to connect with the ICC subnet but not with other secure, internal networks.

See Chapter 4, “Firewall and Security Guidelines,” for complete details of the ports and protocols required by ICC.

The second advantage of this topology is that it serves to keep all Internet voice away from internal, secure networks. Internet voice is sent to the ITG on the ICC subnet. The ITG then performs transcoding and passes the voice to the *DEFINITY* ECS over the ISDN-PRI. Voice traffic, although it is highly compressed, never touches internal networks and therefore has no traffic implications.

The third advantage is that even though the ICC components only support ethernet, they are confined to their own segment. This confinement allows call centers to use any LAN type for internal networks. The firewall, or a separate router, can route or bridge between ethernet and whatever LAN type a call center chooses to use.

ICC Components and Connectivity

Each ICC component and its connections are discussed briefly in this section. Please refer to the specific chapter and / or referenced document on any specific component for more detailed preparation, installation, and operation information.

Internet Telephony Gateway

The ITG provides transcoding capabilities that convert Internet telephony audio. The ITG also houses the Computer-Telephony Integration (CTI) processes that communicate with the *Passageway* Telephony Server.

The ITG is connected to the ICC subnet via 10BASE-T or 100BASE-T ethernet. This allows the ITG to communicate with the *Java* server, the *Passageway* Telephony Server, and the caller's PC (for Internet Voice calls).

The ITG is connected to the *DEFINITY* ECS via one or two ISDN-PRI spans (depending on the configuration purchased). This provides "PSTN-like" connectivity to the *DEFINITY* ECS call center.

The ITG also requires a direct-dialed analog line from the *DEFINITY* ECS for the Remote Maintenance Board (RMB). This connection allows the ITG to place alarm calls to the Lucent Technologies Technical Services Organization if maintenance routines detect an alarm, and allows off-site engineers to provision, upgrade, and troubleshoot the ITG. It is recommended that this dial-in port be protected using a Lucent Technologies Remote Port Security Device (RPSD) lock. The RPSD lock provides strong protection against unauthorized access to any dial-up port. Using security algorithms based on the Data Encryption Standard (DES), the RPSD lock helps ensure that this access point is secured while allowing the ITG to "call for help" and providing authorized callers with unhampered access.

See the *Internet Telephony Gateway Technical Reference* (555-027-212) for detailed system information on the ITG.

Java Server

The *Java* server is connected to the ICC subnet via a single 10BASE-T or 100BASE-T ethernet network interface card (NIC). The *Java* server should be equipped with *pcANYWHERE** software and a maintenance modem on an analog line to allow remote administration and diagnostics for this server.

The *Java* server acts as an intermediary in ICC functions by processing data exchanges such as Text Chat between PCs. Agents connect to the *Java* server (via hypertext transfer protocol [HTTP] and transmission control protocol [TCP]) to log in, log out, drop calls, conduct Text Chat sessions, and perform Escorted Browsing.

The *Java* server and ITG communicate (via TCP) to launch ICC calls to the *DEFINITY* ECS, provide status on call progress, launch Callbacks, log agents in and out, and so on. The *Java* server contacts the ITG to perform all CTI-related activities.

See the *Internet Telephony Gateway Technical Reference* (555-027-212) for detailed system information on the *Java* server.

DEFINITY ECS

The *DEFINITY* ECS connects to the ITG via one or two ISDN-PRI connections. These are generally cabled from the *DEFINITY* ECS DS1 card (via a 356A adapter) directly to the ITG using a D8W (8-conductor) cable. If the distance exceeds the supported range, Channel Service Units (CSUs) may be required. See Chapter 5, "DEFINITY ECS Within ICC," for complete details.

The *DEFINITY* ECS connects to the *Passageway* Telephony Server via a *DEFINITY* LAN Gateway card. This card provides a 10BASE-T connection which is either directly cabled to the *Passageway* Telephony Server via an ethernet cross-over cable, or is cabled to a 10BASE-T hub to which the *Passageway* Telephony Server is also connected.

The *DEFINITY* LAN Gateway should ***not*** be connected to the ICC subnet or any other network. The ethernet connection between the *DEFINITY* ECS and the *Passageway* Telephony Server carries the *DEFINITY* ECS Adjunct/Switch Applications Interface (ASAI) message set, which should

*pcANYWHERE is a registered trademark of Symantec Corporation.

remain local to these two devices. The *Passageway* Telephony Server terminates this message set and provides the standard Telephony Services Application Programming Interface (TSAPI) interface to the ICC subnet.

See the *DEFINITY Communications System Generic 3 Installation, Administration, and Maintenance of CallVisor ASAI over the DEFINITY LAN Gateway* (555-230-223) document for complete details.

PassageWay Telephony Server

The *Passageway* Telephony Server has two NICs. The NIC used to connect the *Passageway* Telephony Server to the *DEFINITY* LAN Gateway card must be a 10BASE-T NIC. As just mentioned in the "*DEFINITY* ECS" section, this connection must be isolated to these two servers. The other NIC provides the standard TSAPI to the ICC subnet.

CMS for Internet (ICMS)

CentreVu CMS is software that resides on a *Sun*[*] workstation running the *Solaris*[†] operating system. The CMS workstation is equipped with a LAN NIC to provide LAN-based supervisory terminals and/or connectivity to ICC components for the collection of statistics. The CMS collects call data from the *DEFINITY* ECS and creates management reports.

ICC requires an additional disk that is loaded with special *CentreVu* CMS for Internet (ICMS) software. This software collects ICC data such as Web page hits, call requests when there are no ISDN-PRI trunks available, call requests when there are no agents logged in, and voice call requests when there are no resources available to perform the Internet Voice-to-PSTN Voice transcoding. These statistics would otherwise be unavailable.

*Sun is a registered trademark of Sun Microsystems, Inc.
†Solaris is a registered trademark of Sun Microsystems, Inc.

The minimum version of *CentreVu* CMS supported for ICC is R3V5, running on a *Sun SPARCserver** computer. See *DEFINITY Communications System, Generic 3, Installation, Administration, and Maintenance of CallVisor ASAI over the DEFINITY LAN Gateway* (555-230-223). Also see Chapter 8, "Call Management System for Internet (ICMS)," for administration and configuration information.

*SPARCserver is a registered trademark of Sun Microsystems, Inc.

Ancillary ICC Components

The components discussed below are considered ancillary. They play an important role in providing transport and protection of Internet calls but do not contribute directly to feature functionality of the ICC offer.

LAN

The LAN, composed of hubs, routers, and possibly switches, is used to connect ICC components, including agent PCs. The LAN that agents reside on can be of any type, but ICC components (apart from the CMS) are only supported using an ethernet interface. The LAN ***must*** provide dependable transport between agent PCs, the Internet, the Web server, and ICC components. ICC communications between the agent and the *Java* server use TCP connections that must remain up for the duration of an agent's logged-in time.

Lucent Technologies' Advanced Data Networking specialists or NetCare Services can assist in provisioning and tuning data networks. Contact a Lucent Technologies account team for information and assistance.

WAN

The WAN, composed of routers and possibly switches, is used to connect the Internet to ICC components. It may also be used to connect agents to the *Java* server if the agents are on remote *DEFINITY* ECS expansion port networks (EPNs). The WAN ***must*** provide dependable transport of Internet calls between agent PCs, the Internet, and ICC components.

As for the LAN, ICC communications between the agent and the *Java* server use TCP connections that must remain up for the duration of an agent's logged-in time. In addition, the Internet connection, perhaps once an educational tool or even a luxury, is now a mission-critical business application. Internet callers must be able to reach agents, and agents must be able to pull up Web pages to share with callers. This requires a robust Internet connection that reflects the availability required of a business application.

Lucent Technologies' Advanced Data Networking specialists can assist in provisioning and tuning data networks. Contact your Lucent Technologies account team for information and assistance.

Web Server

A Web server may be on site behind a firewall, in a minimally firewalled subnet, on the Internet and not firewalled, or even across the country, hosted and managed by another organization. A Web server contains the Web pages that make up a call center's Web site. One of these pages may be the login page for agents. This page should not be known outside the organization and may be housed on a separate Web server.

The Web server is the first point of contact for any ICC activity. When agents log in, they generally access the login page from this Web server. When callers place ICC calls, they invariably do so from a page on this Web server. For this reason, the Web server and services surrounding it must be as robust as any of the other ICC components. Just as the LAN and WAN must provide reliable transport, the Web server must provide reliable services.

NOTE:
Web pages should be changed periodically to maintain caller interest.

Firewall

One of the most important components of a call center's Internet connection is the firewall. The firewall protects a call center's internal assets from the general public on the Internet. It also helps to protect against malicious damage to internal networks.

The firewall must also secure ICC components from unauthorized access, and should be administered to deny all ports and protocols not explicitly identified in Chapter 4, "Firewall and Security Guidelines."

ICC components are generally placed on their own subnet (as illustrated in the ICC Topography figure). This placement keeps ICC traffic off the call center's network and allows the firewall to pass the ports necessary for ICC functionality without significantly disrupting existing firewall rules for internal networks. The firewall port to the ICC subnet allows ICC-required

TCP and User Datagram Protocol (UDP) traffic (as detailed in Chapter 4, “Firewall and Security Guidelines”), while firewall ports to the internal, secure LANs drop such traffic.

Lucent Technologies’ Network Consulting Group can provide an enterprise firewall. This group can also test firewalls for security, lock down Intranets, and provide ongoing, periodic security checks. Call (972) 419-3803 or email security@lucentncg.com for details on these and other offers.

Functional Descriptions

This section describes the activities that take place during an ICC session, and in particular how the various components play a role. The numerous operations that are part of these activities but do not affect overall connectivity are not discussed.

Agent Login

An ICC agent accesses the agent login form from a Web server using a browser. The agent populates the form and submits the information to the *Java* server. The *Java* server downloads the Agent Control Window (via HTTP) and when it receives the agent's password, it contacts the ITG with a request to log the agent in. If the request is successful, the agent is logged into the *DEFINITY* ECS, the *DEFINITY* ECS notifies the *PassageWay* Telephony Server, the *PassageWay* Telephony Server notifies the *Java* server, and then the *Java* server updates the agent's Agent Control Window with a message that login was successful. The *Java* server also instructs the Agent Control Window to "pop" the "Agent Idle" Uniform Resource Locator (URL) into the browser on the agent's desktop.

Caller

A caller brings up a Web page through a browser from the Web server that has a **Call Us** button administered. When the caller selects this button, it submits a string of information (administered on the Web page) to the *Java* server. This information is sent directly from the caller's browser, not by way of the Web server. The submitted information identifies the type of call (Voice and Text, Text-Only, or Callback) and what Vector Directory Number (VDN) in the *DEFINITY* ECS the call should be placed to. The *Java* server performs certain checks (such as making sure an ICC agent is logged in) and contacts the ITG to check for available trunks, available resources to handle the call, and so on. After these checks, the *Java* server executes a script that causes the caller's PC to establish a *Microsoft NetMeeting*[*] conference with

*NetMeeting is a registered trademark of Microsoft Corp.

the ITG. The *Java* server also instructs the ITG to place a call to the specified VDN in the *DEFINITY* ECS over the ISDN-PRI and to monitor the progress of that call. When the call is answered in the *DEFINITY* ECS, the *DEFINITY* ECS notifies the *PassageWay* Telephony Server, the *PassageWay* Telephony Server notifies the ITG, and the ITG notifies the *Java* server. The *Java* server updates the Caller Control Window and Agent Control Window on their respective PCs, and "pops" administered pages to their respective browsers. Text Chat and Escorted Browsing occur between the caller's PC and the *Java* server and between the agent's PC and the *Java* server. Voice communications to and from the caller's PC are encoded and decoded by the ITG.

ICC Administration

During ICC administration, the ICC administrator uses a browser to access a Web page on the ITG, then populate or edit various administrable parameters. When these options are saved (via the browser), the ITG updates appropriate ITG and *Java* server files.

4

Firewall and Security Guidelines

Introduction

This chapter provides a high-level overview of firewall and security for the Internet Call Center (ICC) solution. This chapter includes the necessary ports and protocols required for the ICC solution.

Audience

Network administrators, system administrators, or other persons who need to understand how firewalls impact the ICC solution should read this chapter.

Background Information

“Firewall” is a term that represents a network component designed to protect an internal network (an intranet) from unauthorized network requests. For example, most corporate sites on the Internet have a firewall between the Internet and their corporate intranet to protect internal systems and information from malicious or casual access. Many intranets also have firewalls between subnets to protect sensitive information.

Firewall Administration

Firewall administration for an ICC varies from customer to customer. You must understand the ports and protocols that are used by the various ICC components in order to properly configure your own firewall rules.

A firewall **must** be configured with an appropriate length of timeout on Transmission Control Protocol (TCP) connections. Many firewalls have a parameter that sets the maximum amount of time a TCP connection can remain idle before the firewall drops the session. ICC agents who have gone on break or stepped away from their desks can incur significant idle time and may lose their connection to the *Java** server. If the firewall causes the TCP connection between the agent and the *Java* server to be lost, the next call to the agent results in the agent's being placed in Auxiliary (AUX) work mode and the call's being lost.

See Chapter 9, "Web Page Guidelines," for details about the Agent Login Web page.

*Java is a registered trademark of Sun Microsystems, Inc.

ICC-Specific Ports and Protocols

This section provides the ports and protocols used to administer minimum firewall requirements for the ICC solution:

Source	Destination	Protocol	Reason
>1023 Internet	8001 CMS	TCP	Page hit counts in CMS
8001 CMS	>1023 Internet	TCP	Response to Browser from CMS
>1023 Java Server	80 CMS	TCP	ICC Event Data NO Agents, No Trunks, No Voice Channels
80 CMS	>1023 Java Server	TCP	Response to Above
>1023 Agent PC	80 Java Server	TCP (HTTP)	Download of Call Control Window
80 Java Server	>1023 Agent PC	TCP (HTTP)	Download of Call Control Window
>1023 Agent PC	8101 Java Server	TCP	Agent login & Communications
8101 Java Server	>1023 Agent PC	TCP	Response to Above
>1023 Internet	80 Java Server	TCP (HTTP)	Download of Call Control Window
80 Java Server	>1023 Internet	TCP (HTTP)	Download of Call Control Window
>1023 Internet	8102 Java Server	TCP	Caller Interactions
8102 Java Server	>1023 Internet	TCP	Response to Above
>1023 Java	8103 ITG	TCP	CTI Process Communication
8103 ITG	>1023 Java	TCP	CTI Process Communication
>1023 ITG	8104 Java Server	TCP	ICC Administration
8104 Java Server	>1023 ITG	TCP	Response to Above
>1023 ITG	>1023 T-Server	TCP	CTI Communications
>1023 T-Server	>1023 ITG	TCP	CTI Communications
>1023 Internet	>1023 ITG	TCP	NetMeeting Call Setup Control
>1023 ITG	>1023 Internet	TCP	NetMeeting Call Setup Control
>1023 Internet	>60000+ # voice ITG	UDP	G.723.1 Voice
>60000+ # voice ITG	>1023 Internet	UDP	G.723.1 Voice

Data Communications Detail

This section details the communications between ICC components. This information was acquired through packet captures during ICC activity and is targeted at data communications personnel who have an in-depth knowledge of TCP/IP. This is a more detailed reference than the matrix on the previous page and should be helpful when developing firewall rules.

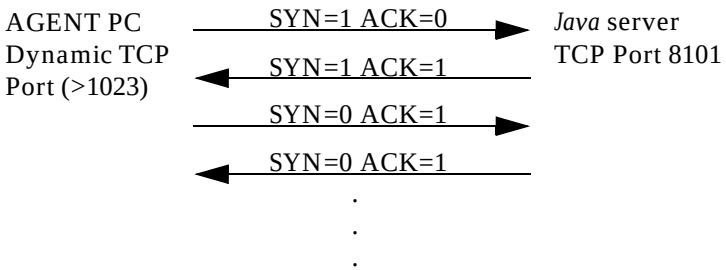
Agent PC to *Java* Server Data Communications

Agent PCs only need to communicate with the *Java* server and whatever Web servers the agent uses in the course of a call (at a minimum, the Web server the agent uses to log in). The agent logs in by accessing a Web page, populating a form with agent ID and phone extension information (and any other information requested), then submitting the form to the ICM process running on the *Java* server (TCP port 80) via Hypertext Transfer Protocol (HTTP). The agent then communicates with the *Java* server using a dynamic TCP port from the agent PC to TCP port 8101 on the *Java* server.

The agent PC conducts all ICC communications with the ICM process on the *Java* server, **not** directly with the caller's PC. As mentioned above, if the firewall or a network error causes the TCP connection between an agent's PC and the ICM process to be lost, then the next call to that agent causes the agent to be placed in Auxiliary (AUX) work mode and the call to be lost.

TCP port 8101 must be blocked from unauthorized sources (for example, the Internet) so that hackers cannot log into the *DEFINITY*® Enterprise Communications Server (ECS). HTTP sessions (TCP port 80) and TCP sessions to port 8101 on the *Java* server must be allowed from agent PCs.

The following diagram illustrates agent PC-to-*Java* server communications. It illustrates all data communications necessary for an agent to log in, conduct Text Chat and Escorted Browsing activities, initiate a callback, and so on. The only other data communication taking place from the agent's PC during an ICC session is Internet browsing.



Caller Communications

When a caller initiates a call to an Internet Call Center, the ICC system downloads a Caller Control Window to the caller's desktop from the *Java* server using World Wide Web HTTP. Once an agent is connected to the caller, both can send and receive Text Chat and Escorted Browsing data using a dynamic TCP port to contact TCP port 8102 on the *Java* server.

The caller is also the source of a request made to *CentreVu*® Call Management System (CMS) that records page hit statistics. Coding on the Web page includes a request for an image (a 1x1 transparent pixel) from the CMS on TCP port 8001 to accompany the caller's request for a connection with an agent. *CentreVu* CMS runs Web page software that listens only on port 8001 and is programmed to provide only this pixel on this port (for security). Any request to port 8001 other than for this image results in an error. The request for the image is recorded as a page hit to increment *CentreVu* CMS data.

Internet voice calls use *Microsoft** *NetMeeting*† on the caller's desktop to set up a conference with the Internet Telephony Gateway (ITG). *NetMeeting* requires dynamic TCP ports for call setup and control, and dynamic User

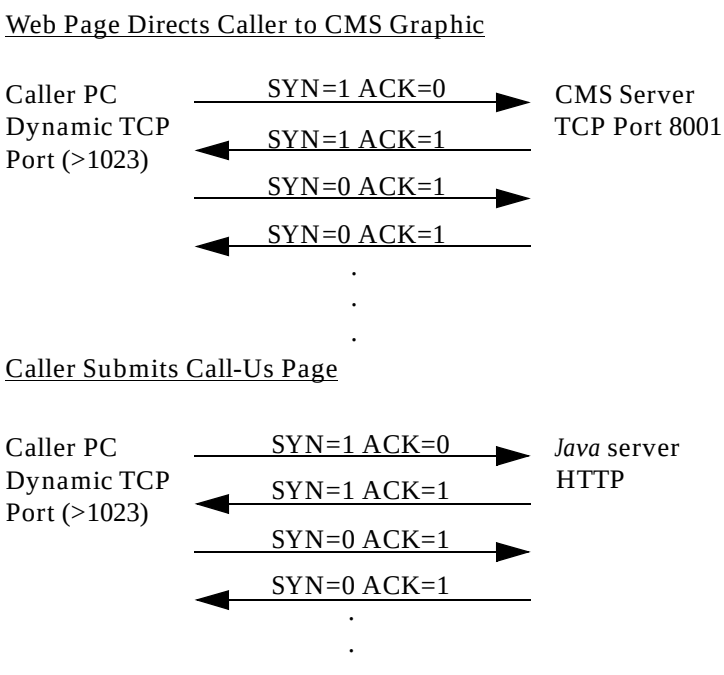
*Microsoft is a registered trademark of Microsoft Corp.
†NetMeeting is a registered trademark of Microsoft Corp.

Datagram Protocol (UDP) ports to carry the voice. The caller must be able to get TCP and UDP traffic to the ITG for Internet voice calls. Internet voice is carried from the ITG starting at UDP port 60000 (administrable) and continuing upward.

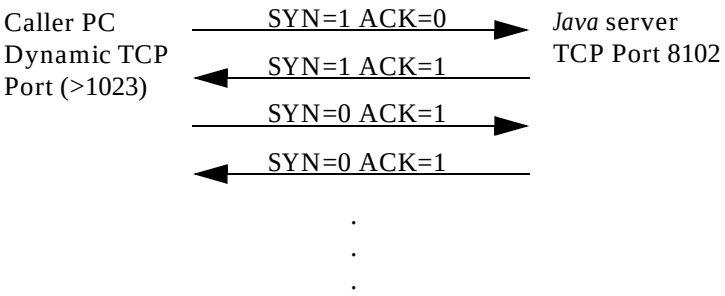
The ITG must be able to respond to the caller's dynamic TCP ports for *NetMeeting* setup and to the caller's dynamic UDP port for voice.

In summary, the firewall must allow Internet sources to reach the *Java* server on TCP port 8102, and the *Java* server must be able to respond to that dynamic (>1023) TCP port. The firewall must allow Internet sources to reach the ITG on dynamic (>1023) TCP ports and on UDP ports 60000 or higher (or whatever is administered in the ITG if the default is not used), and the ITG must be able to respond. Internet sources must be able to access the CMS on port 8001 to get page hit statistics. The CMS must be able to respond to the dynamic TCP port that initiated the request.

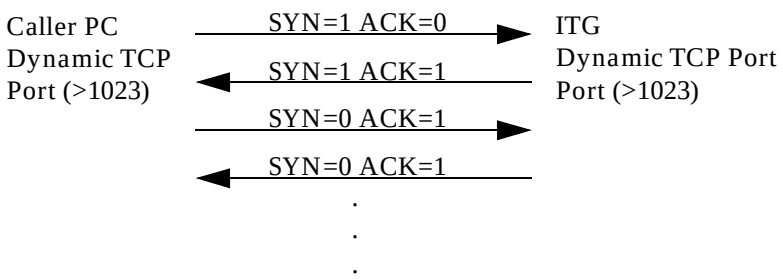
The following illustrates TCP traffic to and from a caller's PC during an ICC call.



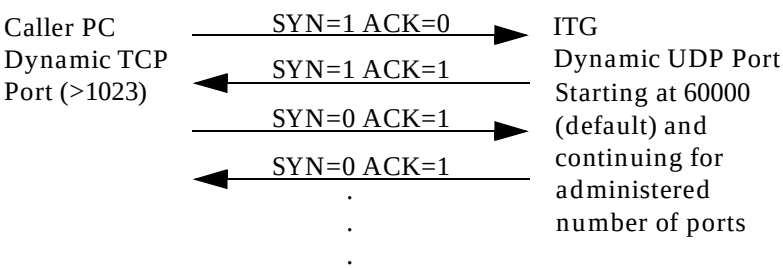
Caller Connects to *Java* Server



NetMeeting Initiation and Call Control of Audio Conference

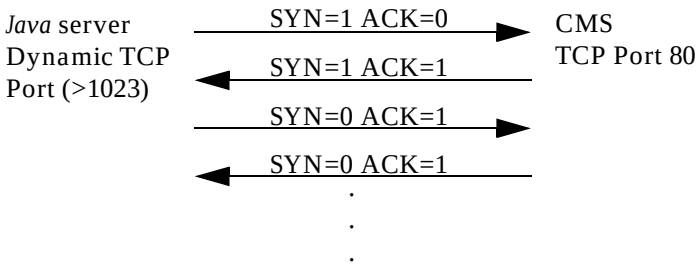


Audio Between Caller's PC and ITG



Server-to-Server Communications

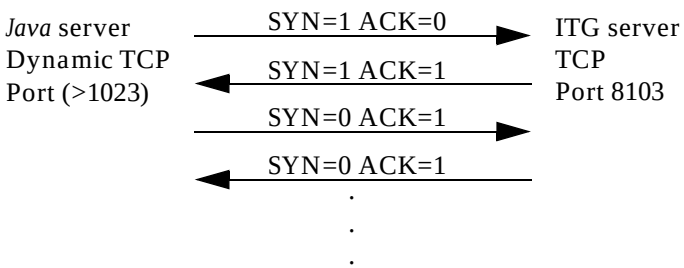
Java Server to CMS



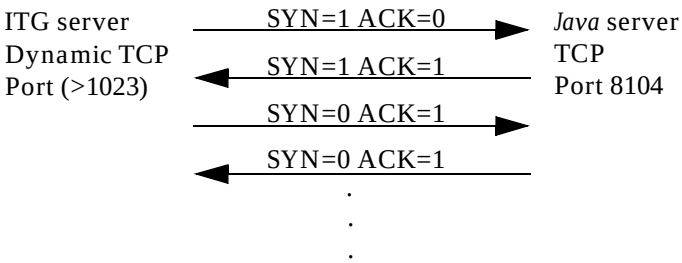
NOTE:
If Agent Web page hits are to be included in Internet CMS reports (along with caller hits), then the agent computer must be able to communicate with port 8001 on the CMS. If the agent and CMS are on opposite sides of a firewall, this port must be opened to allow this functionality. If there is no firewall between the agents and the CMS, then agent page hits are recorded.

The following communications would not normally cross the firewall, but are included for your information.

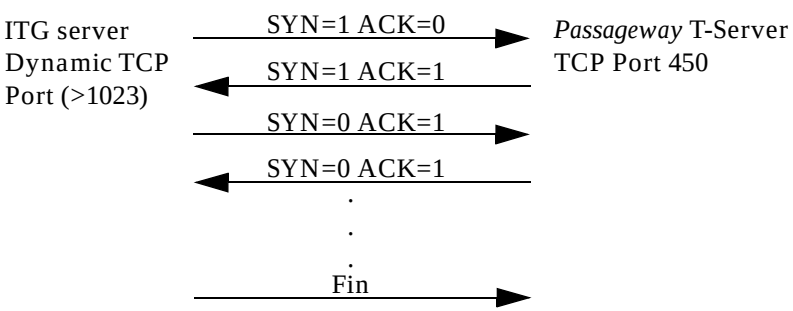
ITG Communications with the *Java* Server
(During Boot / Operation)



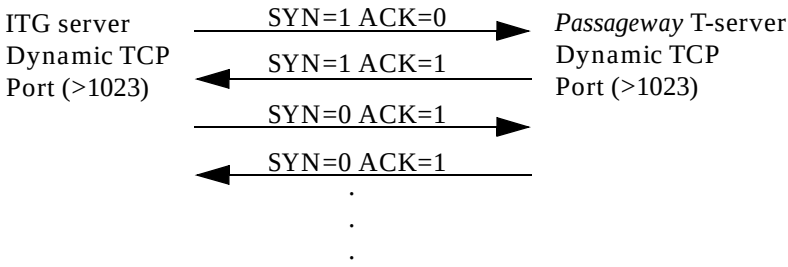
ITG Communications with the *Java* Server
(During Administrative Update)



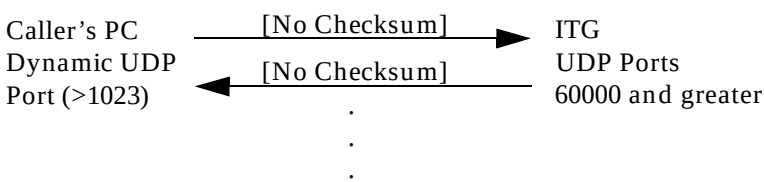
ITG Communications with the *Passageway*® Telephony Server



ITG Communications with the *Passageway* Telephony Server



Audio Between Caller's PC and ITG



Security

The ITG requires a direct-dialed analog line for the Remote Maintenance Board (RMB). This connection allows the ITG to place alarm calls to the Lucent Technologies Technical Services Organization if maintenance routines detect an alarm, and allows remote engineers to provision, upgrade, and troubleshoot the ITG. It is recommended that this dial-in port be protected using a Lucent Technologies Remote Port Security Device (RPSD) lock. The RPSD lock provides strong protection against unauthorized access to any dial-up port. Using security algorithms based on the Data Encryption Standard (DES), the RPSD lock helps ensure that this access point is secured while allowing the ITG to “call for help” and provide authorized callers with hampered access.

The *Java* server and *PassageWay*® Telephony Server require direct-dialed analog lines as well. *pcANYWHERE** software and a modem are used to provide remote maintenance, diagnostics, and support for the *Java* server and the *PassageWay* Telephony Server. This software is very important for the maintenance and support of these servers. It does, however, offer an access point into your server and, possibly, into your network. It is recommended that these dial-in ports also be protected by anRPSD lock.

It is also recommended that the *pcANYWHERE* software be, at a minimum, password protected. Please consult the *pcANYWHERE* documentation for additional security recommendations.

*pcANYWHERE is a registered trademark of Symantec Corporation.

5

DEFINITY ECS Within ICC

Introduction

This chapter covers requirements and changes to the *DEFINITY*® Enterprise Communications Server (ECS) that are specific to the Internet Call Center (ICC) solution. Sections in this chapter are as follows:

- References
- Functional Overview
- Planning
- Installation and Administration.

Audience

This chapter is intended for *DEFINITY* ECS system administrators or persons responsible for translating the *DEFINITY* ECS for ICC functions.

References

The following list represents documents that contain information relevant to the Internet Call Center (ICC) solution:

- *DEFINITY Communications System Call Vectoring/EAS Guide* (555-230-520)
- *DEFINITY Communications System Implementation* manual (555-230-655)
- *DEFINITY Communications System Generic 3 Installation, Administration, and Maintenance of CallVisor ASAI over the DEFINITY LAN Gateway* (555-230-223)
- *DEFINITY Communications System Generic 3 Feature Description* manual (555-230-204)
- *DEFINITY Communications System Generic 3 System Description and Specifications* manual (555-230-*206)*
- *BCS Product Security Handbook* (555-025-600)
- *Internet Telephony Gateway Technical Reference* (555-027-212).

Functional Overview

The *DEFINITY* ECS accepts calls from the Internet Telephony Gateway (ITG) over an ISDN-PRI, performs call routing through vectoring and world class routing, delivers calls to agents, notifies the ITG (through the *PassageWay* Telephony Server) that a call is answered by an agent, and identifies which agent answered the call. ICC functionality uses Automatic Call Distribution (ACD) functionality, it does not replace it.

The *DEFINITY* ECS accepts calls from the ITG over an ISDN-PRI trunk group. The first ISDN-PRI can carry up to 23 simultaneous voice, text, and callback calls (with one channel being used for signalling); the second ISDN-PRI adds 24 channels. The maximum number of simultaneous voice calls is bounded by the ICC package that was purchased—either 20 or 40.

Text Chat and Callback calls are not restricted and are limited only by the number of available ISDN-PRI channels. All calls—whether they are voice and chat, text-only, agent-initiated callback, or caller-initiated callback—use one trunk between the ITG and the *DEFINITY* ECS. Callbacks also require an outgoing trunk from the *DEFINITY* ECS to the PSTN.

The actual functionality of the *DEFINITY* ECS can be described in the context of agent operations during ICC calls. To staff an ICC agent position, an agent uses a browser to access a login Web page and inputs their Expert Agent Selection (EAS) agent ID and the physical extension where they will take calls. The agent submits the completed form to the ITG and *Java** server, which work in conjunction with each other. The ITG / *Java* server sends a login request containing the agent's ID and extension to the *PassageWay* Telephony Server, which uses Adjunct / Switch Applications Interface (ASAI) to log the agent in. This lets the *DEFINITY* ECS know about the agent. Refer to the *DEFINITY Communications System Call Vectoring/EAS Guide* (555-230-520) document for details.

When the ITG / *Java* server receives a call request from the Internet, it launches a call over an available B channel on the ISDN-PRI between the *DEFINITY* ECS and the ITG. This call is sent to the Vector Directory Number (VDN) extension specified on the Web page used by the caller. The *DEFINITY* ECS uses vectoring to process the call and EAS skills to deliver the call to an agent's voice terminal.

---

*Java is a registered trademark of Sun Microsystems, Inc.

Throughout this process the *DEFINITY* ECS is reporting the progress of the call to the *PassageWay* Telephony Server. The ITG / *Java* server notes the extension of the answering agent. When the agent answers the call, the agent's physical extension is sent to the ITG / *Java* server via the *PassageWay* Telephony Server so that the ITG / *Java* server knows which agent to connect to the Caller Control Window and enables Text Chat and Escorted Browsing.

Once a call is connected, if the agent hangs up using the voice terminal, rather than dropping the call through the Agent Control Window, the *DEFINITY* ECS notifies the ITG / *Java* server via the *PassageWay* Telephony Server that the call has been dropped. If the agent drops the call through the Agent Control Window, the ITG / *Java* server notifies the *DEFINITY* ECS via the *PassageWay* Telephony Server that the call has been dropped.

When the agent logs out via the browser, the ITG / *Java* server notifies the *DEFINITY* ECS via the *PassageWay* Telephony Server by issuing a logout request. If the agent logs out via the *DEFINITY* ECS using the voice terminal, the ITG / *Java* server is notified via the *PassageWay* Telephony Server.

Planning

The *DEFINITY* ECS is connected to the *PassageWay* Telephony Server through a LAN Gateway card and a dedicated LAN connection. The *DEFINITY* ECS components must meet the following requirements:

- *DEFINITY* ECS G3V4 or later
- Five contiguous slots available for the LAN Gateway card (These slots cannot be in carrier C of a multi-carrier cabinet, nor in a carrier already containing a LAN Gateway or *DEFINITY AUDIX*® system.)
- ASAI Proprietary Adjunct Links software enabled (to support the *PassageWay* Telephony Server).

An existing LAN Gateway card and / or an existing *PassageWay* Telephony Server may be used. However, discussions regarding security and interoperability of this design must take place prior to implementation. Such designs should be configured and technically assured by a Lucent Technologies account team through normal channels for *PassageWay* Telephony Server support.

The *DEFINITY* ECS and ITG are connected using ISDN-PRI circuits. Requirements for this connection include:

- One ISDN-PRI DS1 circuit pack per ISDN-PRI (TN464 or TN767, depending on system type and configuration).
- One 356A adapter per ISDN-PRI (if the ITG and *DEFINITY* ECS are co-located within direct cabling distance). See the *DEFINITY Communications System Implementation* (555-230-655) document for details. Otherwise, Channel Service Units (CSUs) must be used on both the *DEFINITY* ECS side and the ITG side, along with appropriate cabling for the *DEFINITY* ECS-to-CSU connection and the ITG-to-CSU connection.
- ISDN-PRI must be enabled on the *DEFINITY* ECS.

Installation and Administration

Installation of ICC-related *DEFINITY* ECS hardware and software is included in the ICC offer. Physical installation of hardware is included in the installation charges for individual components. The PBX engineering professional services offer from Lucent Technologies' Multimedia Applications Customer Support (MACS) group (part of the ICC offer) includes designing the appropriate *DEFINITY* ECS translations for connecting the ITG, remotely entering the translations into the switch (with customer permission), and assuring proper operation. This installation does not include any ACD / Call Center translations other than those listed in this section. The MACS works closely with customers to acquire the necessary data and to advise on recommended procedures and translations.

Installation activities for ICC-related *DEFINITY* ECS components are detailed through the associated documents for individual components. The remainder of this section gives an overview of installation activities.

DEFINITY LAN Gateway

DEFINITY LAN Gateway implementation consists of installing the five-slot circuit pack and translating a station of type ADJLK against a port on the card. When translating the ADJLK station in the *DEFINITY* ECS, use the following options:

Event Minimization? `N`

XID? `N`

Fixed TEI? `Y`

TEI: `3`

MIM Support? `N`

CRV Length: `2`

The LAN Gateway is then optioned, separately from the *DEFINITY* ECS, with an IP address, subnet mask, and so on, and cabled to the ethernet LAN.

See the *DEFINITY Communications System Generic 3 Installation, Administration, and Maintenance of CallVisor ASAI over the DEFINITY LAN Gateway* (555-230-223) document for details.

DS1 Circuit Pack

Installing the *DEFINITY* ECS DS1 circuit pack consists of installing the circuit pack and translating it for `esf` framing, `b8zs` zero code suppression, and as signaling type `isdn-pri`. See the *DEFINITY Communications System Implementation* manual (555-230-655) document for details.

If the ITG and *DEFINITY* ECS are within direct cabling distance, connect the 356A adapter to the back of the *DEFINITY* ECS carrier on the amphenol connector corresponding to the slot in which the DS1 circuit pack was installed. Use a shielded or unshielded 8-conductor cable with RJ45 connectors on each end (a D8W cable) to connect port 8 of the 356A adapter with the appropriate port (A or B) on the ITG ISDN-PRI card.

If the *DEFINITY* ECS and ITG are not within direct cabling distance, CSUs need to be used on both the *DEFINITY* ECS and ITG sides, along with appropriate cabling. See the *DEFINITY Communications System Generic 3 System Description and Specifications* (555-230-*206)* and *Internet Telephony Gateway Technical Reference* (555-027-212) documents for details.

ISDN-PRI Trunk Group

The ISDN-PRI trunk group connecting the *DEFINITY* ECS and the ITG is translated as an `isdn-pri` trunk type, with a service type of `tie` and a direction of `incoming`. On page 2 of the trunk group form, the data restriction value should be `Y` so that music is not played across the Internet during an agent-initiated Callback. See the *DEFINITY Communications System Implementation* (555-230-655) document for details.

ISDN-PRI trunk group security ***must*** be addressed. Because the extension number used to launch an ICC call is actually submitted by a browser, there is the risk that a hacker may attempt to submit a false dial string in order to compromise call center security. Therefore, the ISDN-PRI trunks ***must*** be restricted from placing outbound calls. Unless so restricted, the `vdn_ext` parameter submitted by a consumer's browser could be changed to dial a long distance number through the *DEFINITY* ECS. Additionally, to limit other malicious activities, the ISDN-PRI trunks should be restricted from destinations in the *DEFINITY* ECS that are not intended for Internet calls (such as individual agent stations, non-Internet VDNs, and so on).

There are two ways by which an ICC ISDN-PRI trunk group can be secured. The first is within the ITG itself, denying fraudulent calls before they are placed to the *DEFINITY* ECS. The second is within the *DEFINITY* ECS, denying calls to locations other than those specified as valid endpoints. This provides a two-tiered security plan. See Chapter 6, “ITG and Java Server Guidelines,” for details on securing the ITG dial plan.

The *DEFINITY* is secured using Classes of Restriction (CORs) to restrict destinations from the ITG trunk group. The COR for this trunk group specifies, among other things, what calls the trunk group is able to complete. In this way the ISDN-PRI trunk group can be restricted from making any outbound (off the *DEFINITY* ECS) calls and can be restricted to only calling a resource with a COR which is used uniquely for Internet destinations.

As an example, the ISDN-PRI trunk group to the ITG could be assigned a COR of 49, which is outward restricted, and limited to only calling COR 48 (assuming both 48 and 49 are previously unused CORs). COR 48 is then used for any VDN extension expected to receive Internet traffic. If a call comes across the ISDN-PRI trunk group destined for any other extension, that call is denied by the *DEFINITY* ECS (assuming that the destination extension is assigned a COR other than 48). The permissions assigned to this COR (COR 48) should reflect the security the call center would normally assign to VDNs.

Naturally, as Internet calls are "blended" with Public Switched Telephone Network (PSTN) calls, the CORs discussed above may need to be modified to reflect all the requirements of the call center. When establishing CORs, administrators should thoroughly review Class of Restriction instructions and guidelines found in the *DEFINITY Communications System Generic 3 Feature Description* document (555-230-204), the *DEFINITY Communications System Implementation* manual (555-230-655), and the *BCS Product Security Handbook* (555-025-600).

ACD Translations

The MACS group inputs standard *DEFINITY* ECS ACD translations as part of ICC installation. These include:

- Three standard, measured VDNs. See the *DEFINITY Communications System Call Vectoring/EAS Guide* (555-230-520) for a complete description. The first VDN is for Internet Text Chat, the second is for Internet Voice Calls, and the third is for Callback. The MACS obtain necessary extensions from the customer.
- Two standard vectors. The first is for Internet Voice. This vector queues the call to the Internet skill and optionally plays a delay announcement. The second is for Internet Text Chat and Callback requests. This is a single-step vector that contains a queue to the main skill command. Both vectors queue an Internet-initiated call to a customer-assigned skill. The MACS obtain these vector numbers from the customer.

The customer is responsible for translating Internet skills, Expert Agent IDs, and agent telephones. Lucent Technologies personnel can provide this design work, as well as enhanced vector designs, as part of the Call Center Application Integration NetCare Services offer. Call your account executive or 1-800-4NetCare for details.

Some general guidelines to consider when translating skills and agents include the following.

- It is recommended that the same skill be used for all types of Internet-initiated calls (voice, text, and callback). This is because ICC only checks to see whether an agent is logged into the ITG / *Java* server, not which skill they might be in. If an agent with only a Text Chat skill logs into the ICC, voice calls are still passed to the *DEFINITY* ECS.
- The implementation of stroke counts can be used to help track conditions such as bad voice quality, no one on the other end of a call, collaboration did not work, and so on.
- The Multiple Call Handling feature is ***not*** supported by the ICC solution.
- Multi-switch call centers are ***not*** supported in the initial release of the ICC solution. All agents must be on the same *DEFINITY* ECS. Agents on remote Port Networks are supported.

Some general guidelines to consider when translating VDNs and vectors for ICC include the following.

- Do ***not*** use the "wait with music" vector step. It would add unnecessary processor usage to the caller's PC and traffic to the Internet circuit.
- Do ***not*** use the "converse" vector step. It is incompatible with ICC functionality.
- Do ***not*** use digit collection in ICC vectors. There is currently no good way to pass Dual Tone Multi Frequency (DTMF) tones (aka touchtones) across the Internet; therefore, there are no digits to collect.
- VDN of Origin Announcements (VOAs) are strongly recommended. When an agent receives an ICC Text Chat call, there is no audio for that call. With VOA, the agent hears an identifying message (such as "Voice Call" or "Text Chat Call") and knows whether to answer audibly or through Text Chat. Without VOA, the only way the agent has to identify a call type is to note the VDN name on the terminal display. Agents' class of service must be set to receive VOAs.
- It is recommended to use a different vector for Text Chat and Callback calls than for Internet voice calls. The voice call vector can provide in-queue announcements, which are unnecessary for Text Chat and Callback calls. In addition, the initial setup delay for *Microsoft*[*] *NetMeeting*[†], used for Internet voice, requires a unique strategy to be used in the voice call vector; that strategy is not needed for Text Chat or Callback calls. Finally, voice calls can be routed to a voice mail box, whereas Text Chat and Callback calls cannot.

When an Internet voice call is requested, the audio connection is not set up until answer supervision is returned from the *DEFINITY* ECS. As a result, the following may occur:

- There is a lag of approximately five seconds (on a dial-up connection) between the time the agent answers the call and the time when the agent can be heard by the caller.
- If a time-in-queue announcement is used, the caller does not hear the first five seconds of the announcement.

---

*Microsoft is a registered trademark of Microsoft Corp.
†NetMeeting is a registered trademark of Microsoft Corp.

In order to provide the best experience to the caller, write vectors to answer each Internet voice call with an announcement that does not exceed five seconds. (This is a “null” announcement in a way, since it is not heard by anyone.) Such a setup serves to establish an audio connection so that any follow-up announcements should be heard in full and, more importantly, as soon as the agent answers the call, they can begin speaking with the caller.

The vector could look like the following:

1. announcement 2000 (a normal delay announcement that is less than five seconds in length)

   NOTE:
   The announcement in steps 1 and 4 can be the same if it is less than 5 seconds in length.

2. queue to main skill 10 priority m
3. wait time 10 seconds hearing silence
4. announcement 2000
5. goto step 3 if unconditional

Ongoing Operations

Once the *DEFINITY* ECS has been set up for ICC functionality, it requires very little administration. Call capacity may be increased up to system limits at any point by adding an ISDN-PRI and adding VDNs to handle more ICC calls.

ISDN-PRI administration is described in the “Installation” section of this chapter. Additional voice call capacity requires the purchase of additional software and may require additional hardware. Contact your Lucent Technologies account team for configuration assistance.

When translating additional VDNs, be sure to assign them the ICC VDN COR, the same COR as initially established for Internet destinations. Otherwise, the *DEFINITY* ECS will reject call attempts from the ITG to the new extensions. When adding VDNs, also remember to add the new extension numbers to the ITG dial plan. See the *Internet Telephony Gateway Technical Reference* (555-027-212) document for details.

VDNs should be established for each entry point (Web page) the customer wishes to measure. This may be one VDN per Web page, or one VDN for each logical grouping (such as women's slacks, disk drive problems, NYSE inquiries, and so on). Different VDNs can also be used to track call type (such as Text Chat or Internet voice or Callback).

6

ITG and *Java* Server Guidelines

Introduction

This chapter covers the administration and support of the Internet Telephony Gateway (ITG) platform and the *Java** server for the Internet Call Center (ICC) offer.

Audience

This chapter is intended for system administrators, support personnel and anyone who wants an overview of administering and maintaining the ITG and *Java* servers in an ICC environment.

Reference

See the *Internet Telephony Gateway Technical Reference* (555-027-212) for more information about the ITG and *Java* servers.

---

*Java is a registered trademark of Sun Microsystems, Inc.

Background Information

ITG and *Java* Server

The ITG and *Java* server together act as a gateway between the Internet and the call center, by connecting callers on the Internet to agents in the call center and merging the communication and browsing capabilities of the two mediums.

The ITG consists of special software and hardware running under the *LynxOS*[*] (a *UNIX*[†]-compatible operating system) on an industrial-grade *Pentium*[‡] PC. The ITG receives caller requests and launches calls into the call center over an Integrated Services Digital Network-Primary Rate Interface (ISDN-PRI) interface to the *DEFINITY*® Enterprise Communications Server (ECS). It uses special voice processing cards for transcoding voice between the Internet and the call center. The ITG monitors and reports the progress of calls launched into the call center.

The *Java* server is an *NT*[**] 4.0 server with ITG software that interacts with *Java* applets running in caller and agent browser windows. It sends caller-initiated call requests through the ITG and passes call progress information back to the caller. Once an agent is selected in the call center, the *Java* server provides ICC features (Text Chat and Escorted Browsing) during the session. See Chapter 1, "About Internet Call Center," for details.

Refer to the *Internet Telephony Gateway Technical Reference* (555-027-212) for detailed information about configuration and ordering for the ITG and *Java* server.

---

*LynxOS is a registered trademark of Lynx Real-Time Systems, Inc.
†UNIX is a registered trademark licensed exclusively through X/Open Company, Ltd.
‡Pentium is a registered trademark of Intel Corporation.
**NT is a registered trademark of Microsoft Corp.

ITG Capacities

The ITG can be ordered in two configurations:

- 20 voice calls
- 40 voice calls.

NOTE:
With sufficient T1 channels available, up to 47 calls (voice and chat) are available.

Planning Overview for the ITG and *Java* Servers

This section is an overview of the ITG and *Java* server requirements you should consider while planning your Internet Call Center. Other sections of this document, along with the *Internet Telephony Gateway Technical Reference* (555-027-212), provide greater detail on the topics covered here.

Your Lucent Technologies Account Team helps you to design and order the ITG and configure the *Java* server in accordance with your business' unique needs and requirements. This team works closely with the Lucent Technologies MultiMedia Applications Support team who approves all ITG configurations before an order is placed.

Planning an ITG and *Java* Server Configuration

More information about the equipment listed here, as well as the other important components of the Internet Call Center, is available in Chapter 1, "About Internet Call Center." Planning, ordering and implementing these items are part of your activities in preparation for your Internet-enabled Call Center.

- The ITG is a rack-mountable *Pentium* PC equipped with Voice Processor Cards, an ISDN-PRI interface card (supporting one or two T-1 network connections), an Ethernet 10/100 NIC, and for domestic installations, a remote maintenance board (RMB). Environmental requirements and technical specifications are available in the *Internet Telephony Gateway Technical Reference* (555-027-212). You may increase the call-handling

capacity of the ITG (up to system limits) by purchasing the appropriate hardware and software in the aftermarket.

— The location of the ITG server should allow an Ethernet 10BaseT or 100BaseT connection to your TCP/IP LAN. The ITG Server must be able to communicate with the *Java* server and *Passageway*® Telephony Server.

— There must be access to the Internet (probably via your corporate firewall) from the ITG server. Lucent Technologies can help you plan your firewall configuration to maintain your secured corporate network.

— A CD-ROM drive must be accessible to the ITG and *Java* server.

— An analog line is required for the RMB in order for Lucent Technologies to provide remote maintenance support.

— The *DEFINITY* ECS must support ISDN-PRI and have DS-1 card(s) available to connect to the ITG Server.

— The ITG is configured to support ICC Offer-based configurations supporting 20 or 40 Internet voice calls.

- A *Pentium* PC, which you provide, to be used as a *Java* server. This *Java*-enabled PC should be connected to your LAN and able to communicate with the ITG.

  — This PC should be running *Microsoft Windows NT* 4.0 server with Service Pack 2 or greater.

  — This PC should be running *Microsoft* Internet Information Server (IIS) software.

Installing the ITG and *Java* Server

To install the ITG and *Java* server, follow standard installation procedures detailed in the *Internet Telephony Gateway Technical Reference* (555-027-212).

Administering ITG and *Java* Server

The ITG and *Java* server must be administered to customize each call center's configuration. Basic ITG server administration and connectivity to a *DEFINITY* ECS are described in the *Internet Telephony Gateway Technical Reference* (555-027-212).

This section describes the administration specific to the ICC offer. A Web-based interface is provided to assist in making these administrative changes.

NOTE:
The ITG and *Java* server can also be administered by editing configuration files directly and running specific commands on the ITG. However this administration interface is not recommended for local use! It is intended for remote administrative support by Lucent personnel who may not have access to administration Web pages.

The next few sections provide step by step instructions with sample screens and input to help show ITG and *Java* server administration. See the Appendix, "ITG and Java Server Administration Field Descriptions," for a useful description of all the fields to be administered and should be consulted when necessary. In addition, Web-based help is available for each screen and field encountered during administration.

Prerequisites

It is assumed that the following items have been completed or are available for ICC offer administration. Consult the *Internet Telephony Gateway Technical Reference* (555-027-212) for details.

- Both the ITG and *Java* server must be installed, administered, connected and functioning on the LAN.
- The ICM application must be running on the *Java* server.
- A console or terminal connection must be available on the ITG.
- A Web browser must be available for administrative access.
- IP addresses for the ITG, *Java* server and *Passageway* Telephony Server must be known.

Configuring Web Services on the ITG

A hypertext transfer protocol (HTTP) process must be configured on the ITG before Web-based administration can begin. This step should only occur at the initial installation and administration of the ITG and *Java* server. Once that is completed, subsequent administration can be done through a Web interface.

To configure the Web services on the ITG:

1. Log into the ITG over the console or other terminal connection. See the *Internet Telephony Gateway Technical Reference* (555-027-212) for details about logging in.

2. At the system prompt, execute the following command:

   ```
   /www/bin/adminHTTP
   ```

3. This command starts a script, which prompts you to supply information. A sample session is shown below:

   ```
   Apache HTTPd administration

   This product includes software developed by the
   Apache Group for use in the Apache HTTP server
   project(http://www.apache.org/).

   The following tidbits of information are needed to
   properly administer the HyperText Transfer
   Protocol daemon (HTTPd). No changes to
   administration will be made until you have
   confirmed your settings.

   You may break out of this script at any time before
   confirmation to abandon your changes.

   Default values (if any) are in square brackets.
   Administrator e-mail address [] ? root
   MMCX ITG Server Name [] ? mmcs13
   MMCX ITG Server IP Address [000.0.000.000] ?
   135.9.144.106
   Admin Port Number [81]?
   HTTP Proxy On or Off [On] ?
   Proxy Port Number [8000]
   ```

```
Remote Proxying On or Off [Off] ?
Admin Access Restrictions On or Off [Off] ?
Admin Password Protection On or Off [Off] ?
Java Server (ICM) IP Address [000.0.000.000] ?
135.9.134.132
Java Server (ICM) Util Port Number [8104]?
Administrator E-mail Address: root
```

4. Enter responses to the questions, as appropriate. (Refer to the "Appendix" for a description of fields and responses.) Also, many field values are defaulted and the default values are usually acceptable. The fields are described below:

Field	Description
`Administrator e-mail address []?` Example: webmaster@enterprise.com	Internet e-mail address. This prompt requests the e-mail address of a mailbox that is to receive e-mail from callers should they experience trouble using the service. The HyperText Transfer protocol (HTTP) daemon generates error messages for the browser to display when the daemon encounters difficulty. The daemon embeds this e-mail address in these error messages, inviting the caller to send e-mail to this address describing the problem encountered. This field may **not** be empty.
`ITG Server Name []?` Example: itg.enterprise.com	Network name. This prompt requests the network name of the ITG. It must be a network name that the ITG can resolve either via its `/etc/hosts` file or via Dynamic name Services (DNS), if available. This field may **not** be empty.

Field	Description
`ITG Server IP Address []?` Example: 135.88.44.157	IP address (XXX.XXX.XXX.XXX where XXX is a number between 0 and 255). This prompt requests the network address of the ITG. This field may **not** be empty.
`Admin Port Number []?` Example: 81	An integer (port number). This prompt requests the TCP/IP port number on which the ITG accepts HTTP (Web)requests to perform administration of the ITG via a browser. The firewall protecting the ITG from unauthorized access should be administered so that network sites that do not need to administer the ITG cannot connect to this TCP/IP port.
`HTTP Proxy On or Off []?` Example: Off	`On` or `Off`. The Apache HTTP daemon delivered with the ITG/ICC has the capability to provide HTTP proxy services. A site would typically turn on HTTP proxy services if agents have no other access to the Internet and the ITG/ICC has DNS available through the Internet Service Provider (ISP) to which it is attached or the ISP has an HTTP proxy to which the HTTP daemon can forward HTTP requests. Most installations of the ITG/ICC would not turn on HTTP proxy services. The response to this prompt must be either `On` or `Off` (case sensitive).

Field	Description
`Proxy Port Number []?` Example: 8000	An integer (port number). If HTTP proxy administration is turned `on`, the administrator asks for the HTTP proxy port number. This is the port number on which the Apache HTTP daemon listens for the proxied HTTP requests. The firewall protecting the ITG from unauthorized access must be administered so only those network sites that need proxy services, such as the call center's agents, can access the HTTP proxy services port. No others should be permitted to access this port.
`Remote Proxying On or Off []?` Example: Off	`On` or `Off`. The HTTP proxy also has the ability to forward proxied HTTP request that it cannot fulfill to another HTTP proxy. Many ISPs have HTTP proxy services available for their customers. This HTTPd feature allows an ITG/ICC site to use these services, if necessary. The response to this prompt must be either `On` or `Off` (case sensitive).

Field	Description
`Enter its IP address and port (w.x.y.z:p)` Example: 125.9.202.20:8000	A network address and port number. The network address is of the form XXX.XXX.XXX.XXX where XXX is a number between 0 and 255. This is followed by a colon, followed by the port number on which the remote proxy is listening for proxied HTTP requests. If HTTP remote proxying is turned on, the administrator is prompted for the network address and port number of the HTTP proxy to which requests are to be forwarded. The network address above may be a network node name instead of an IP address if that network name is resolvable by the ITG / ICC through use of the `/etc/hosts` file or DNS.
`Admin Access Restrictions On or Off [off]?` Example: Off	`On` or `Off`. The Apache HTTP daemon supplied with the ITG / ICC has the capability to restrict access to the administration Web pages based on the apparent IP address of the originating HTTP request. These access restrictions should be used to augment and enhance the firewall protections of the ITG / ICC, not in place of them. Typically, these restrictions are used to restrict access to specific network addresses or subnets behind the firewall. The response to this prompt must be either `On` or `Off` (case-sensitive).

Field	Description
`Please specify IP addresses for which admin access is to be allowed (comma-list):` Example: 135.9.141,198.2.77.224	Comma-separated list of IP addresses or subnet addresses. If administration access restrictions are turned on, the system prompts for a set of IP address (or network subnets) from which access to the administration Web pages is allowed. If a subnet address is specified, administration access is allowed from all requests originating from that subnet.
`Admin Password Protection On or Off []?` Example: Off	`On` or `Off`. The HTTP daemon has the capability to challenge any request for administration access to the ITG / ICC for a login and password. The administration password is set to the default administration password until it is changed the first time using Web-based administration screens or the `htpasswd` command (found in `/www/bin`). The response to this prompt must be either `On` or `Off` (case-sensitive).
`Java Server (ICM) IP Address?` Example: 135.9.88.44	IP address (either symbolic or XXX.XXX.XXX.XXX where XXX is between 0 and 255). The ITG / ICC must be given some network information about the *Java* server. The following prompts request this information. If a symbolic IP address is used, it must be one that can be resolved by the ITG / ICC through the use of the `/etc/hosts` file or DNS. This value must be specified.

Field	Description
Java Server (ICM)Util Port Number Example: 8104	Integer (port number). The ITG/ICC needs to be told the port number on which the *Java* server is listening for administration requests. Unless otherwise instructed, the default value should be used.

Remember that the default values are acceptable and that any value can be changed later through the Web interface.

5. Once all the fields have been entered, the script presents all the information and asks if the information is correct. If it is not correct, then enter "n" and the script goes through all the prompts again. If it is correct, then enter "y" and the script terminates.

6. To complete the configuration execute the following command on the ITG server:

   ```
   reset level=boot
   ```

   This command displays a "Waiting for reply..." status message that reboots the ITG. Any network connection to the ITG is dropped.

7. Once the ITG has rebooted (this takes several minutes), the HTTP process should be running and ready to serve administration Web pages. This can be verified by entering the following command from the ITG console or a terminal connection:

   ```
   ps ax | grep httpd
   ```

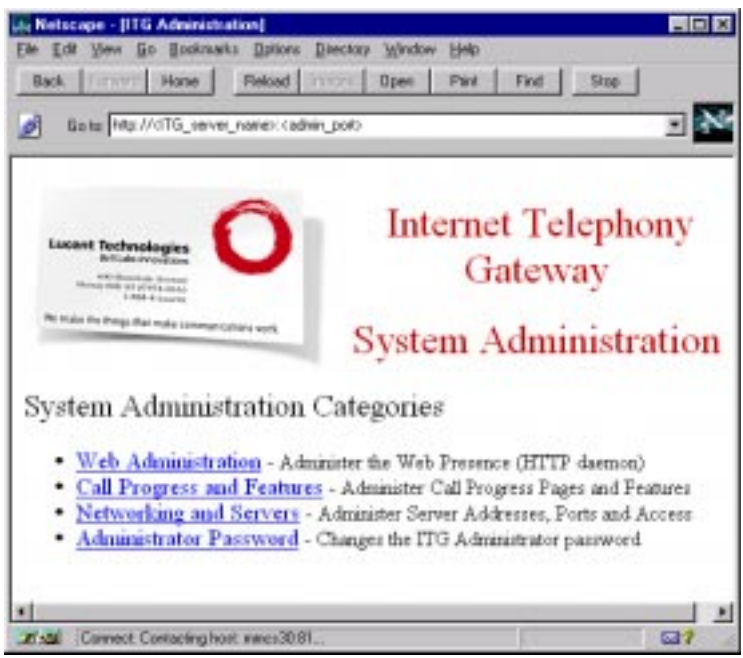
   Several lines should appear, indicating that several instances of the HTTPd process are running. If not, repeat the administration described in this section.

Web Administration of ITG and *Java* Server

To access the main administration page for the ITG and *Java* server, enter the page location in the browser window:

```
http://<ITG_server_name>:<admin_port>
```

Use the ITG server name and the admin port number previously administered (probably the default port number, which is 81). The administration Web page may be protected, requiring a login ID and password. The initial default login ID and password are `sysadm` and `sysadmpw`. The password can be changed through the Web administration interface. The main administration Web page (Internet Telephony Gateway System Administration) appears:



This page shows the available administration categories. Each category links to another page for administration and is described in the following sections. Click on the text link of a category to begin the administration.

Most of the administration Web pages have similar characteristics. The initial page displays the fields and each field has a text link to help

information. The current field values are also displayed, but the values cannot be changed on the initial page. Selecting the **Edit** button moves to a page that allows field value changes.

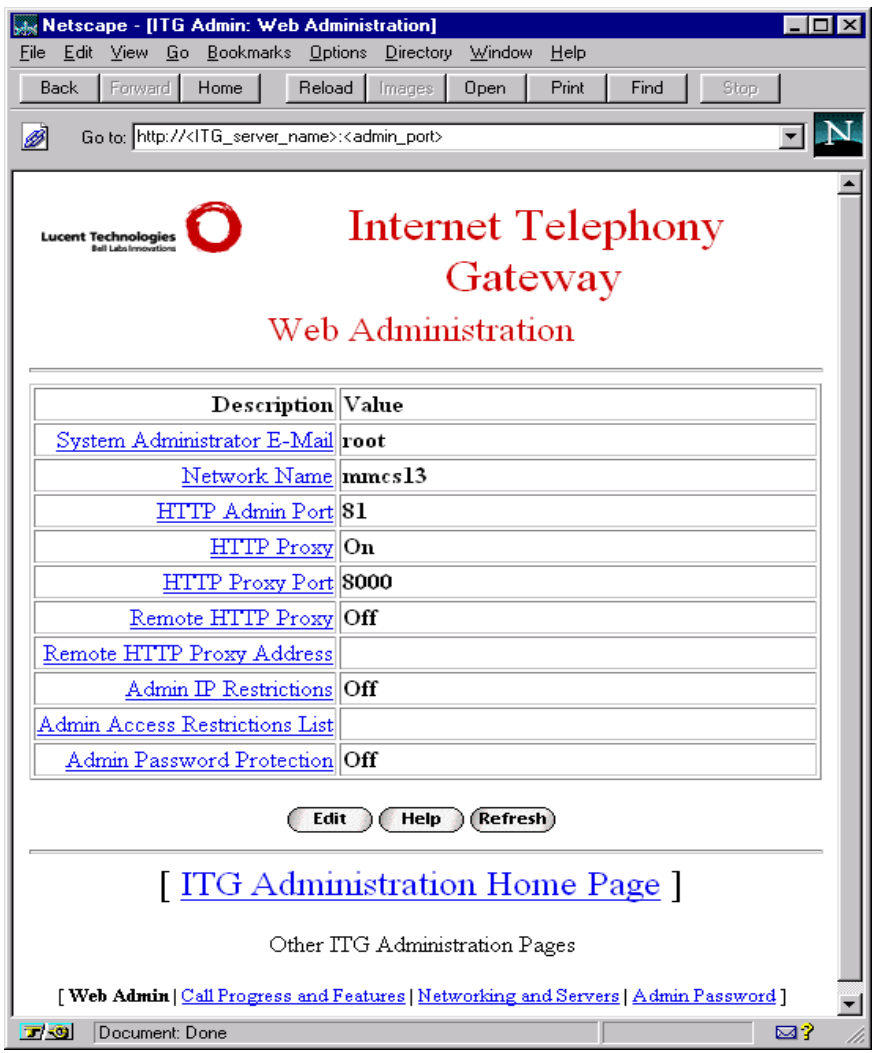
Links to other pages are displayed at the bottom of each page. Following these links to move through administration may be easier than backing out of the current pages each time.

The buttons and their associated actions are as follows:

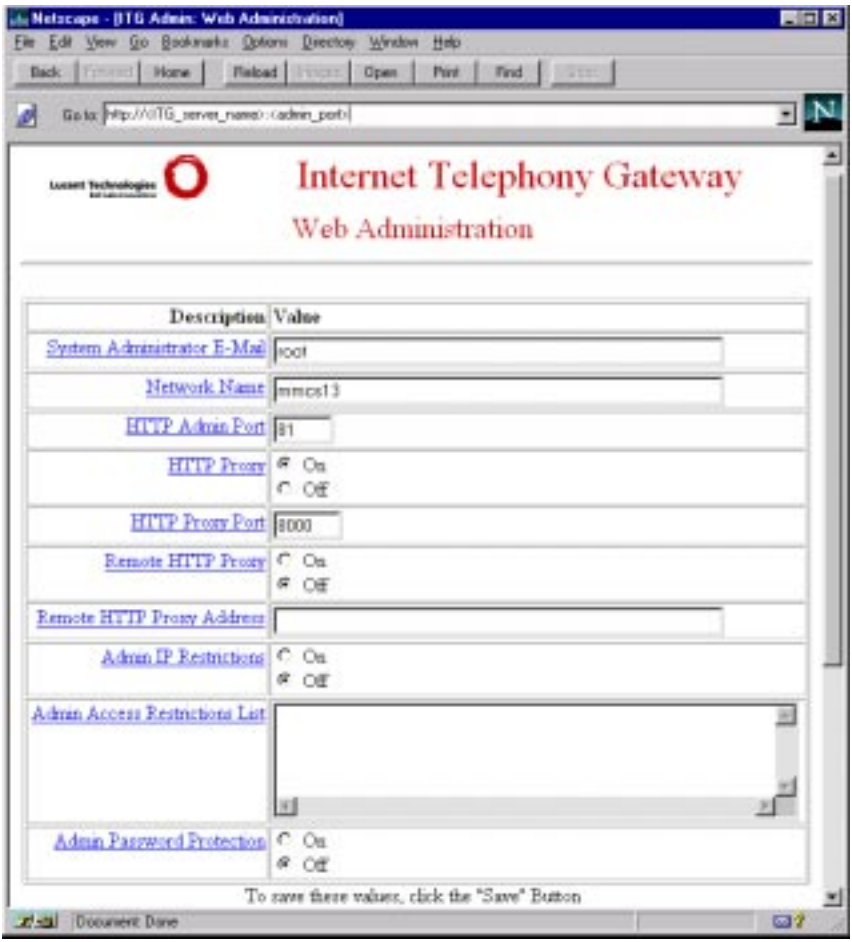
Buttons	Action(s)
	Redisplays the current page with any updated values.
	Links to the Help page associated with this page. All Help selections open a separate browser window so that Help can be viewed simultaneously with the page being administered. Help browser windows can be closed at any time without affecting the administration process.
	Allows field values to be modified on a similar page.
	Returns to the page and displays any updated values.
	Disregards (undoes) any changes that have been made on the form but not yet saved to the system.
	Activates the new administration changes made on this screen. Each specific section identifies the action taken or necessary steps to ensure that the administrative changes are in effect.

Web Administration

The Web Administration page is shown below. It contains the fields and associated values needed for HTTP administration on the ITG (similar to the initial fields administered in the “Configuring for HTTP on the ITG Server” section).



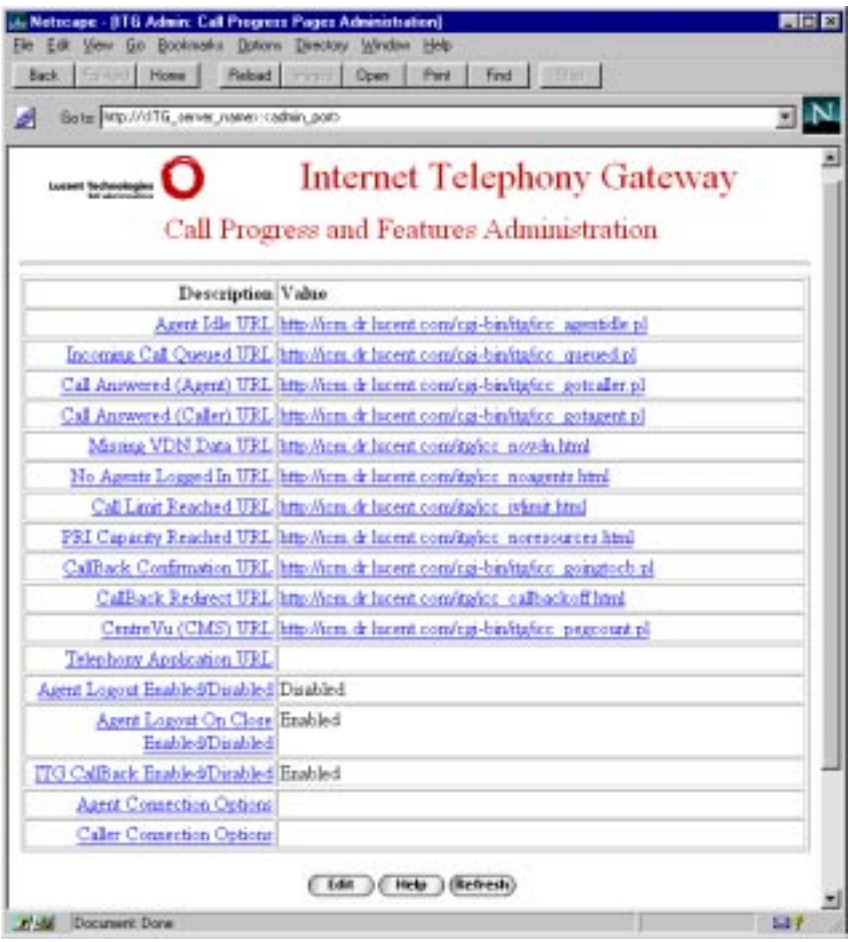
The Edit Web Administration page is shown below. It is similar to the previous page; however, field values are displayed differently and can now be modified.



Choose the Save button at the bottom of this page to store the new values and to restart the Web services (HTTP process) automatically using the new administered values. Changes take effect immediately with no service disruption (with valid entries). Once the Web Administration is complete, choose the next administration page link from the bottom of the page, or return to the main administration page to continue.

Call Progress and Features Administration

The Call Progress and Features Administration Web page is shown below. It allows administration of the URLs associated with call progress or failure events. These are the Web pages or scripts to be used whenever a specific event occurs. Refer to the "Appendix" for associated Help pages, or to Chapter 9, "Web Page Guidelines," for more information. Other call features or agent capabilities are also administered from this page.



In addition to the Help text links, each URL is also presented as a link on this page. This allows the administrator to verify that the URL is correct and

accessible. For example, clicking on the Agent Idle URL should bring up the associated page in a separate browser window. If you click on the URL that represents a CGI script or other non-site HTML page, you may not get a Web page.

The Call Progress and Features Administration editing page as shown below is available through the Edit button. URLs can be modified from this page, but cannot be verified as from the previous page.

Modification of some fields may not be available on this page. Some fields are display-only and cannot be edited through the browser. These fields

require careful administration and may impact the service of a call center significantly when modified. It is recommended that Lucent personnel be consulted to investigate, modify, and explain the impact of these fields.

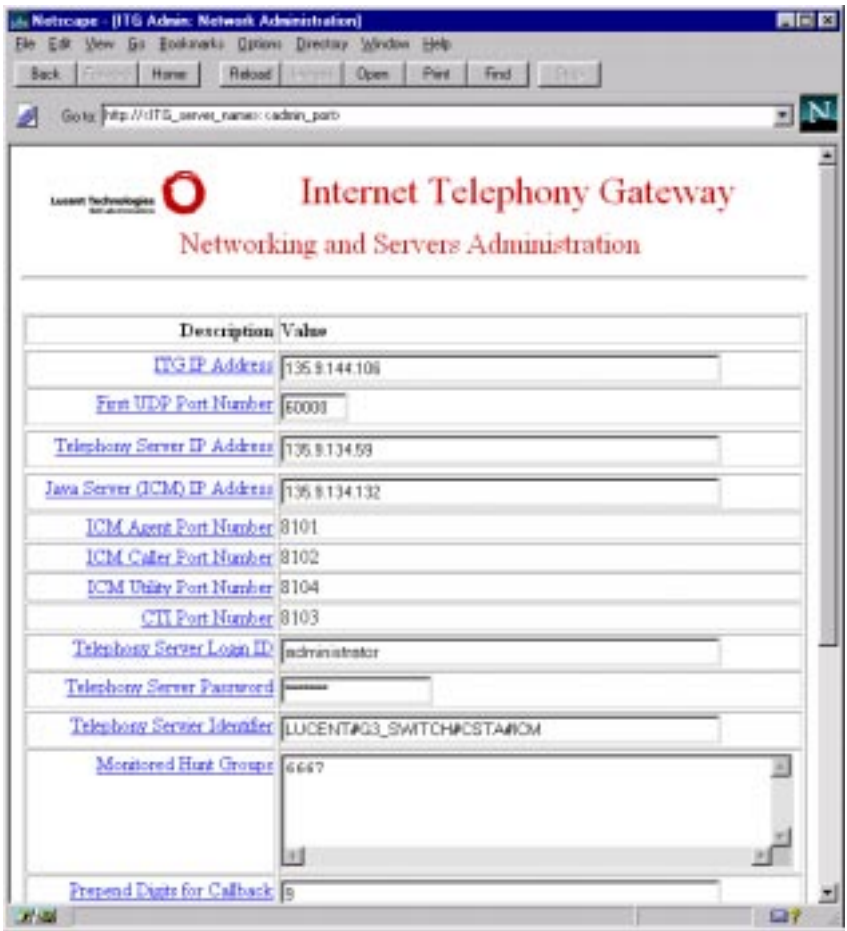
Choose the Save button on this page to store the new values and make them available to the ITG and *Java* server immediately—no reboot or restart is required.

Once Call Progress and Feature Administration is complete, choose the next administration page link from the bottom of the page, or return to the main administration page to continue.

Networking and Servers Administration

The Networking and Servers Administration Web page is shown below. It allows administration of addresses and port numbers or ranges required by the ITG and *Java* server. Specific information needed for accessing and monitoring calls through the *Passageway* Telephony Server is also administered from this page. Refer to the “Appendix” or to the Help page for specific information about a field.

The Networking and Servers Administration editing page as shown below is accessed by means of the Edit button.



Modification of some fields may not be available on this page. Some fields are display-only and cannot be edited. These fields require careful administration and may impact the service of a call center significantly when modified. It is recommended that Lucent personnel be consulted to investigate, modify and explain the impact of these fields.

Choose the Save option on this page to store the new values.

NOTE:
These new values do not take effect until the ITG and *Java* server (or processes) have been restarted!

To restart the ITG, execute the following command on the ITG console or terminal connection:

```
reset level=cold1
```

This command restarts all the affected processes and instructs them to execute with the new values.

To stop the Internet Call Manager application on the *Java* server, close the Internet Call Manager Control Panel window on the server. Then use the startup menu or ICM icon on the desktop to restart the application with the new values.

Once Networking and Servers Administration is complete, choose the next administration page link from the bottom of the page, or return to the main administration page to continue.

Administrator Password Administration

The Administrator Password Administration Web page is shown below. It varies from other Web administration pages because it has only one screen where changes are allowed immediately. This page is for changing the password for the `sysadm` login.

The password must be entered in both fields.

Two buttons are displayed. They have the following actions:

Button	Action
Change Password	Activate the password changes.
Reset	Clear the password fields above.

Once Administrator Password Administration is complete, choose the next administration page link from the bottom of the page, or return to the main administration page to continue.

Changing ITG and *Java* Server Configuration Files

This section describes the steps involved in changing the ITG and *Java* server configuration files.

CAUTION:
This method of modifying ITG and *Java* server configuration files is intended for Lucent personnel. Use the Web-based administration unless you must modify configuration files and / or do not have Web access. Make sure to back up your configuration before changing the ITG and *Java* server configuration files.

Configuration files and commands are identified in this section. Refer to the "Appendix" or to the *Internet Telephony Gateway Technical Reference* (555-027-212) for information about a file or fields within a file. Refer to the *ITG Technical Reference* or on-line ITG manual for details about commands.

The main configuration file for the ITG and *Java* server is the `/mmcs/etc/itg.cfg` file on the ITG (shown in the "Appendix"). It is a flat text file that can be edited using a text editor (for example, vi). Each field has a name / value pair separated by an equal sign (`AgentPort=8101`). A missing value to the right of an equal sign means the field is blank (`AgentPort=`).

To change the configuration, perform the following steps:

1. Edit the `/mmcs/etc/itg.cfg` file. Change the desired field(s) and save the changes to the file.

2. After making changes, certain commands must be executed based on which fields were changed.

   If any fields associated with HTTP were changed, execute the following command on the ITG to restart Web services with the new values:

   ```
   /www/bin/restartHTTP
   ```

   — If the IP address of the *Passageway* Telephony Server was changed, then execute the following command on the ITG:

   ```
   setTSLIBRC <tserver IP address>
   ```

— If any other fields were changed, then execute the following command on the ITG to update the values to the *Java* server:

```
updateICM
```

3. The ITG and Internet Call Manager (ICM) application may need to be restarted if any address or port fields were changed. To restart the ITG, execute the following command on the ITG console or terminal connection:

   ```
   reset level=cold1
   ```

   This command restarts all the affected processes so they begin executing with the new values. To stop the ICM application on the *Java* server, close the Internet Call Manager Control Panel window on the server. Then use the startup menu or ICM icon on the desktop to restart the application with the new values.

See the Appendix, “ITG and Java Server Administration Field Descriptions,” for more information on the configuration files.

General ITG Server Administration

The previous sections cover administering connectivity and capabilities for the ICC offer on the ITG. In addition, some general ITG administration is needed in order for the server to receive and route calls to a *DEFINITY* ECS. The minimum required administration is described here. Refer to the *Internet Telephony Gateway Technical Reference* (555-027-212) for details and descriptions of the commands. See Chapter 5, "*DEFINITY* ECS Within ICC," for details.

The following general administration is required on the ITG:

1. A PRI interface must be added to the ITG. Use the `addpri` command for this. This command has numerous options and must be administered in a manner consistent with the PRI interface on the *DEFINITY* ECS. See Chapter 5, "*DEFINITY* ECS Within ICC," for details. For example, the line coding (zcs or b8zs), framing mode (esf), and interface type (caller or network side of the protocol) must correspond with the administration of the PRI interface of the *DEFINITY* ECS.

   The minimum command to add the PRI on the ITG is:

   ```
   addpri slot=i5 port=1
   ```

   This administers the first port on a PRI card in ISA slot 5 (default location) on the server.

   If a second PRI is to be used (for a 47 channel system) then the following command would activate the second port:

   ```
   addpri slot=i5 port=2
   ```

   The ITG must be restarted (`reset level=cold1` command) each time a PRI is added. The server does not attempt to bring the PRI into service until it has been restarted.

2. A trunk group must be added on the ITG. The `addptg` command identifies the trunk group, associates it with the correct PRI ports, and describes the type of use (voice, data, etc.). The minimum command to add a PRI trunk group is:

   ```
   addptg tg=1 intf=i5:1 aud=100 vid=0 app=0
   ```

This creates trunk group 1, using port 1 of the PRI in ISA slot 5 and indicates that all of the channels are used for voice (only voice should be used for the ICC offer).

3. The trunk group must be identified as having 47 channels in a non-facility associated signal (NFAS) arrangement (47 B channels using the same D channel). Each of the commands described below is presented as adding the administration for the first time.

   a. If this is the first time for adding the administration, use the following command to add both PRI facilities at the same time:

      ```
      addptg tg=1 intf=i5:1,i5:2 nfas=1 aud=100 vid=0
      app=0
      ```

   b. If this is **not** the first time for adding the administration, add a second PRI using the following command with the same parameters:

      ```
      chgptg tg=1 intf=i5:1,i5:2 nfas=1 aud=100 vid=0
      app=0
      ```

   NOTE:
   The change command (`chgptg`) is more relevant during the operation of a call center.

4. A PRI routing plan must be added to the ITG. The `addprp` command identifies a route plan number and associates it with a trunk group. The following command associates the trunk group created above with the routing plan identified as 1:

   ```
   addprp plan=1 tg=1
   ```

5. Once a routing plan and trunk group exist, the dial plan on the ITG must be administered to recognize dial strings and route them to the correct plan and trunk group. The `adddp` command is used to recognize and manipulate dial strings for routing. It can add or delete digits to a dial string to change how the call is handled through other systems. For the ICC offer, the recommended dial plan on the ITG should identify each dial string (VDN) exactly and route it to the *DEFINITY* ECS without any special digit recognition or manipulation.

The following command tells the ITG that a VDN of 5555 should be routed out of the ITG over routing plan 1 (which in the previous example associated with PRI trunk group 1 to the *DEFINITY* ECS):

```
adddp dial=5555 dir=out plan=1
```

Similarly, each command has a corresponding `show` command to display current information or status. For example, use the `showpri` command to verify that the PRI on the ITG is in service and functioning with the PRI on the *DEFINITY* ECS. Use the `showptg` command to display the number of channels in service or currently in use.

Refer to the *Internet Telephony Gateway Technical Reference* (555-027-212) for more information on these other commands.

Supporting the ITG and *Java* Server

Various commands and log files are available for monitoring and maintaining the ITG and *Java* server for the ICC solution. This section describes how to monitor and maintain the servers, references the commands and log files, and shows examples. Refer to the *Internet Telephony Gateway Technical Reference* (555-027-212) for more information.

Because the ITG and *Java* server are separate units, supporting them requires dealing with each separately, as discussed in the following sections.

Prerequisites

Access to the ITG and *Java* server is a prerequisite to supporting them. Multiple access methods are available. These methods are listed below and described when appropriate.

Call center and Lucent support personnel should determine which access methods they use from the following:

1. ITG
   - console connected to the serial port on the CPU card
   - terminal connected over a Local Area Network (LAN)
   - remote connected through the Remote Maintenance Board (RMB).
2. *Java* server
   - console
   - telnet session from the ITG
   - remote connection through *pcANYWHERE*[*].

*pcANYWHERE is a registered trademark of Symantec Corporation.

Supporting the ITG

Log Files on the ITG

The ITG has one main log file where all system processes log information about call progress or system status. The log file name is `logfile0` and it is located in the `/mmcs/log` directory on the ITG. It can grow to 10MB of data, then logging continues into `logfile1`. When `logfile1` reaches its maximum size, `logfile0` is cleared and again used for logging.

The log file is not intended to be readable, easily understood, or for general consumption. It is a software development log that provides cryptic descriptions of what is occurring, and it is useful for software developers to determine the cause of a problem.

Logging levels can be turned up and down for specific processes during operation, which is not recommended, but it may be needed when troubleshooting a problem. For the ICC, the Computer-Telephony Integration (CTI) process may need to have the logging level turned up for troubleshooting.

The following command allows the CTI process to log all of its information:

```
reset level=mask loc=CTI
```

The following command turns the CTI logging level down to its default logging level:

```
reset level=mask loc=CTI
   type=DEBUG_LVL2:DEBUG_LVL3 enable=off
```

Status on the ITG

Numerous commands exist on the ITG for obtaining status information. Some useful commands for an ICC environment are shown below:

- `showalarm`—lists any alarms on the server. This command can also give information about repair actions for the alarm.
- `showdp`—shows the current dial plan administration.
- `showpri`—displays the current PRI interface administration and status.
- `showptg`—displays current PRI trunk group administration, channel status and usage.

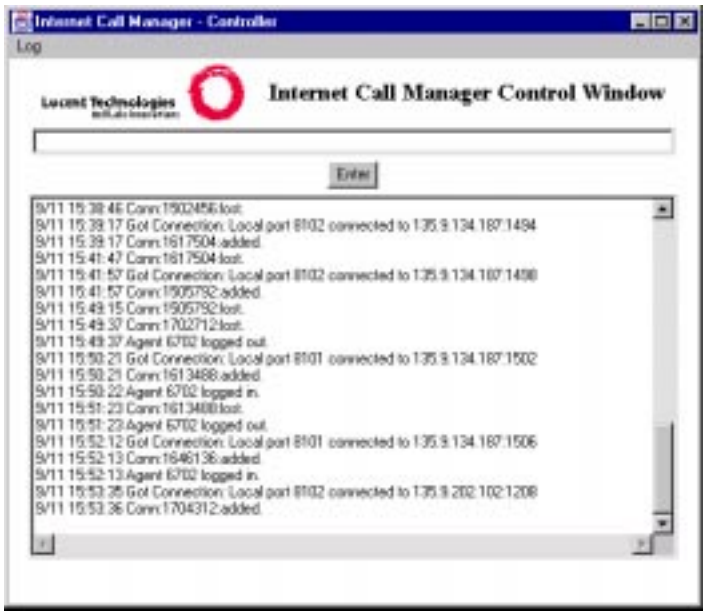
Refer to the *Internet Telephony Gateway Technical Reference* (555-027-212) for detailed information and additional commands.

Supporting the *Java* Server

Access to the *Java* Server

There are several methods to access the *Java* server. The support capabilities differ depending on the access method. The most complete support access is available from the console terminal and keyboard on the *Java* server. This displays the Internet Call Manager Control Window (shown below). This control panel displays the ICM log file, controls the logging level of this file,

and allows an administrator to enter commands to obtain status information.



The next best support access method is a telnet session from the ITG (or any other server with LAN access) into the maintenance and administration ICM Utility Connection port 8104 supported by the ICM application on the *Java* server. In a manner similar to the control panel, the ICM log is actively displayed and commands can be entered.

An example of access to the *Java* server over port 8104 is as follows:

1. On ITG server, enter:

   ```
   telnet <address of Java server> 8104
   id mtce ext none
   ```

2. After no response or a prompt, enter:

   ```
   patchmein
   ```

The ICM log file begins to display as the information is logged. Commands can be entered at any time (see the "Commands" section below). The session can be ended by normal telnet termination (press the tilde "~" followed by a period ".") or by using the `status` command.

The *pcANYWHERE* `package` allows access to the *Java* server, but that access is limited to examining the ICM log file only. The *pcANYWHERE* package is required for full-remote support of the ITG and *Java* server.

Log Files on the *Java* Server

The only ICC-related log file available on the *Java* server is the `icmlog.log` which is maintained in the ITG installation directory (default is `c:\itg`). Once this log file reaches 2MB, it is copied to the `icmlog.bak` file and logging continues in the `icmlog.log` file.

The log file contains all events that occur for agent login, caller access, and agent/caller interactions. The log file also contains the results of any status commands executed.

Information contained in the log file is not intended for general consumption. It is useful for experienced support personnel to obtain status information and call events from the server. Information logging levels can be controlled from the pulldown menu on the Internet Call Manager Control Panel or from a remote command over the telnet (`patchmein`) session from the ITG (see the "Commands" section below). The normal logging level displays errors and connection events as agents, callers, or calls interact with the ICM application. The debugging logging level displays all the events that occur for an agent, caller, or call.

Status on the *Java* Server

Status information available on the *Java* server consists of the current agent, caller, and call connections maintained by the ICM application.

Commands on the *Java* Server

Commands are available on the *Java* server through the Internet Call Manager Control Panel or over a telnet session to the maintenance and administration port of the ICM application. These commands are intended for use by experienced support personnel to help monitor and troubleshoot the ICM application on the *Java* server. These commands are identified in the following table:

Command	Description
`close <connection ID>`	Clears (drops) the identified connection.
`debug <on/off>`	Changes the ICM logging level for more / less detail.
`dumpcalls`	Displays the current calls that are known to the ICM application. Also displays the connection ID of the parties on the call.
`dumpconns`	Displays all the available agents and callers that are known to the ICM application. A connection ID is given for each and may be useful for following all the events for that ID or for subsequent commands.
`id <description> <type> <parameters>`	Identifies the incoming connection over the administration and maintenance port. Use only: `id mtce ext none`.
`patchmein`	Directs ICM log file output to the administration and maintenance port and recognizes commands over this port.
`sendagents <text>`	Broadcasts text to all active agent's control windows.

Command	Description
`sendto cti logout <agent extension> <group extension> <agend id>`	Forces the logout of the indicated agent in the call center through the CTI process on the ITG server. The `<group extension>` is typically "none."

Refer to the *Internet Telephony Gateway Technical Reference* (555-027-212) for information and additional commands.

7

PassageWay Telephony Server Guidelines

Introduction

This chapter includes the following:

- Background Information
- Administering *PassageWay*® Telephony Services Software.

Audience

Installers, system administrators, and anyone involved in connecting, installing, administering, and integrating hardware or software at the system level for the Internet Call Center (ICC) solution.

References

Complete documentation containing information on *PassageWay* Telephony Services software in general, and as it pertains to the ICC solution, is provided to customers in PDF format on the CD-ROM that accompanies the software. The document set includes the following:

- *PassageWay Telephony Services Solution, Microsoft* Windows NT Telephony Services, DEFINITY ECS Network Manager's Guide* (555-201-505)
- *PassageWay Telephony Services Solution, Microsoft Windows NT Telephony Services, Network Manager's Guide* (555-201-506)
- *PassageWay Telephony Services Solution, Microsoft Windows NT Telephony Services Installation Guide* (555-201-116).

Background Information

PassageWay Telephony Services is a software application that runs on a server (a dedicated PC) to track and associate various elements of calls between callers and agents. It also helps other components of the ICC solution administer call elements.

PassageWay Telephony Services has an open architecture, based on the European Computer Manufacturers Association (ECMA) Computer Supported Telephony Application (CSTA) international standard, which allows customers to employ the communications system and Computer-Telephony Integration (CTI) software that best meet their needs. *PassageWay* Telephony Services enhances the functionality of existing communications and computer equipment.

Major components of *PassageWay* Telephony Services include the following:

- The *PassageWay* Telephony Server—The *PassageWay* Telephony Server acts as a conduit between individual client/server applications and the *DEFINITY*® Enterprise Communications Server (ECS). It routes return messages from the *DEFINITY* ECS to the client/server that expects them. It also ensures that agents log in using a valid login ID and password and that they have the required permissions to perform whatever action they are requesting.

*Microsoft is a registered trademark of Microsoft Corp.

- The Security Database (SDB)—This *PassageWay* Telephony Services database stores information about callers and the devices they control. Telephony Services uses this information for validation. Administrators can control caller access to *PassageWay* Telephony Services by placing restrictions on the types of requests callers can make. Telephony Services Release 2.22 uses Btrieve for the Security Database engine (the underlying software that controls data).
- Telephony Services Library (TSLIB)—A set of functions that acts as an interface between client or server applications and the *PassageWay* Telephony Server.

The PBX driver resides on the *PassageWay* Telephony Server. It receives TSAPI messages from the *PassageWay* Telephony Server and routes them to the PBX over CTI links, performing any necessary conversions in the process. It receives messages from the PBX, reformats them, and sends them back to the *PassageWay* Telephony Server. The PBX driver is supplied by a PBX vendor.

Direct connections between other ICC solution components and the *PassageWay* Telephony Server include:

- TCP / IP to hub(s) and the ITG
- TCP / IP to the *DEFINITY* ECS.

Installation and connection of the *PassageWay* Telephony Services application are performed by Lucent Technologies' Professional Services Organization.

There is an optional mechanism by which Bell Laboratories can support the *PassageWay* Telephony Services software remotely (from off site). If a call center wants this type of support, then *pcANYWHERE** remote control client software is loaded and a modem is installed for remote access by the Lucent Technical Service Center (TSC).

---

*pcANYWHERE is a registered trademark of Symantec Corporation.

Administering *PassageWay* Telephony Services Software

When the *PassageWay* Telephony Server is installed, some administration is required to integrate it with the ICC. The following are administered in the Security Database during ICC installation:

- The ICC phone devices and Automatic Call Distribution (ACD) devices (VDNs and lead extensions of the ACD group extensions) are added.
- A device group(s) is added and all phone devices are added to the group.
- The ICC User (TMAN) is added, and the Classes of Service for the ICC device group and the *Windows** User Domain are administered.
- The *DEFINITY* ECS switch setting is administered.
- Alarm parameters are administered.
- Message trace parameters are administered.
- Error log parameters are administered.

The ICC User must also be administered in the *NT*† User Domain Manager.

NOTE: No administration is required specifically for the ICC solution. Refer to the installation documentation on the CD-ROM provided with the software for details.

On-site training is conducted for persons who will maintain the *PassageWay* Telephony Server after installation.

*Windows is a registered trademark of Microsoft Corp.
†NT is a registered trademark of Microsoft Corp.

8

Call Management System for Internet (ICMS)

Introduction

This chapter provides details about the following:

- Connecting ICC-specific *CentreVu*® CMS hardware
- Installing ICC-specific *CentreVu* CMS software
- Using standard reports for ICC call statistics—call centers can use these reports to get regular Internet call statistics (for example, ASA, Hold Time, ACD Time, etc.)
- Using Internet Call Management System (ICMS) and Supervisor reports
- Database items specific to ICC.

Audience

Installers, system administrators, Call Center Supervisors, or anyone else involved in connecting, installing, administering hardware or software, setting up reports, or maintaining database items for the ICC solution. This chapter also describes the *CentreVu* CMS and *CentreVu* Supervisor ICC enhancements.

Background Information

About *CentreVu* CMS and Supervisor

CentreVu CMS is a software product used by customers who have Lucent Technologies telecommunication switches and receive telephone calls that are processed through the Automatic Call Distribution (ACD) feature of the switch. *CentreVu* CMS collects call-traffic data, formats management reports, and provides an administrative interface to the ACD feature in the switch.

CentreVu Supervisor software is a Lucent Technologies *Windows*[*]-based interface to the *CentreVu* CMS. The Supervisor software runs on any *IBM*[†]-compatible PC running a *Microsoft*[‡] *Windows-based* operating system.

See the *CentreVu* Supervisor and *CentreVu* CMS documentation described in the "References" section of this chapter for details.

About *CentreVu* CMS for Internet Software

CentreVu CMS for Internet (ICMS) is a new software package that works in conjunction with the standard *CentreVu* CMS and Supervisor software and provides new features designed specifically for the ICC solution.

The *CentreVu* CMS for Internet software package allows you to do the following:

- Gather Internet call statistics
- Correlate the number of page hits with the calls that are launched from the corresponding Web pages
- Determine staffing needs for the ICC solution
- Determine capacity needs for the ICC solution.

---

*Windows is a registered trademark of Microsoft Corp.
†IBM is a registered trademark of International Business Machines Corporation
‡Microsoft is a registered trademark of Microsoft Corp.

The ICMS package runs on top of the standard CMS package. The ai load of *CentreVu* CMS R3V5 is required to support these new ICC features. Also, if *CentreVu* Supervisor is used, the Version 5 bj load is the minimum required load.

About *CentreVu* CMS and Supervisor Enhancements

CentreVu CMS and Supervisor enhancements and reports provide additional statistics for Web page hits and calls launched from the page. *CentreVu* CMS enhancements for ICC include the following:

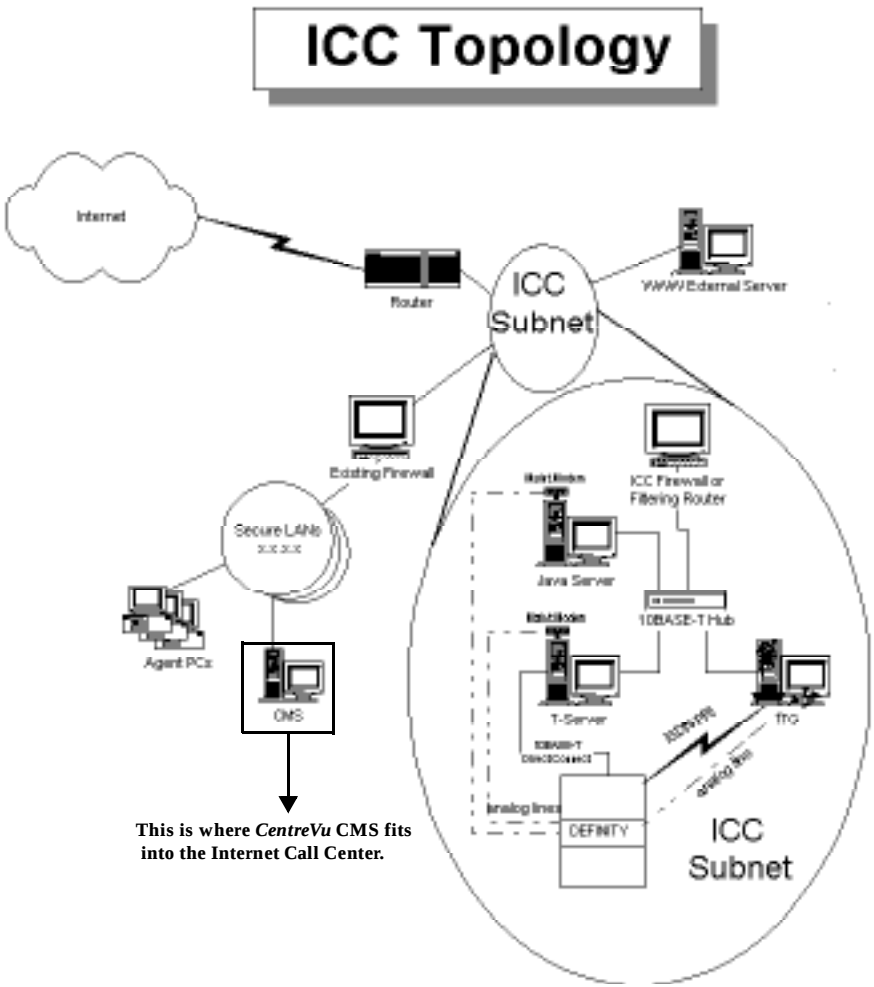
- New ICC data items—CMS collects the Internet calls offered, page hits for ICC-enabled Web pages, and statistics for situations where a call could not be launched to the ACD.
- New ICC reports—New reports for *CentreVu* CMS and Supervisor are provided which relate to the ICC. Access to the new ICC reports uses the same mechanisms that are already in place for *CentreVu* CMS. *CentreVu* Supervisor reports appear as Purchased Reports in the Designer category.
- Standard collection of call-related statistics—Regular call statistics (for example, speed of answer, talk time, etc.) are collected for Internet calls.

NOTE:
BCMS and *BCMSVu*™ are not supported for Internet statistics. However, normal call statistics (for example, speed of answer, talk time, etc.) can still be collected using unmodified versions of *CentreVu* CMS, BCMS, or *BCMSVu*. Only Internet-specific data items require the special *CentreVu* CMS software.

Connecting *CentreVu* CMS Hardware

To use *CentreVu* CMS for Internet software, the *CentreVu* CMS must be on a LAN and have a specific port on the firewall administered to allow collection of page hit information. For information about *CentreVu* CMS and firewalls, see Chapter 4, “Firewall and Security Guidelines,”

The following diagram shows the relationship of *CentreVu* CMS to the Internet Call Center.



Installing the ICMS Hardware

Hardware Prerequisites

An extra 2 GB hard disk must be provisioned with the system to ensure that the customer's *CentreVu* CMS does not run out of disk space due to the ICC.

Installing ICC-Specific Hardware

1. Attach an additional external disk to the SCSI chain by choosing a SCSI ID that is not being used. See chapter 9 of the *CentreVu Call Management System R3V5, Sun SPARCserver Computers, Installation and Maintenance, Volume 2* (585-215-827) document for details.

   a. The disk should be formatted and partitioned as a single partition. (Use the format command and carefully select the appropriate disk so existing disks are not disturbed. Use the **Format** option to reformat the disk, the **Print** option to verify that only one partition exists after formatting, and the **Label** option to write the partition map to disk.)

   b. Mount this partition as `/webcms`. An entry in the `/etc/vfstab` file for the Web CMS partition should look like this:

      ```
      /dev/dsk/c0tXd0s1 /dev/rdsk/c0tXd0s1 /webcms
         ufs 2 yes -
      ```

      The **"X"** should be replaced by the actual SCSI ID selected for the new disk. This is the file system name for this SCSI drive.

Installing the ICMS Software

Software Prerequisites

Support for the ICC is provided as an add-on package to standard *CentreVu* CMS. This ICC add-on package software is delivered on a separate CD-ROM and uses standard `pkgadd/pkgrm` commands.

ICC-required software must be installed for *CentreVu* CMS and Supervisor for the Internet database:

- Release 3 Version 5 (ai EDI load) of *CentreVu* CMS software

  This load is required on the *CentreVu* CMS server if the customer wishes to run or create ICC reports. Although the R3V5 load is required, it can be received as a maintenance patch for the G3V4 switch.

- BJ EDI load of *CentreVu* Supervisor for viewing ICC reports.

Installing ICC-Specific Software

1. Log in to the CMS server as `root`.
2. If not already installed, install the *CentreVu* CMS R3V5 (ai load) and *CentreVu* Supervisor Version 5 (bj load) software. See the *CentreVu* CMS and *CentreVu* Supervisor installation documents for details.
3. You must turn `off` CMS before beginning the ICMS installation. To do this, select option number 3 from the `cmssvc` menu.
4. Insert the CD ROM with the ICMS package into the CD ROM drive. Wait a minute or so for the volume manager to mount it.
5. At the *UNIX** prompt, enter the following command:

   ```
   $ mount
   ```

   The system lists all the mounted drives including `/cdrom`.

---

*UNIX is a registered trademark of X/Open Company, Ltd.

6. Verify that the ICMS package is available on the CD ROM by entering the following command at the *UNIX* prompt:

   ```
   $ ls -F /cdrom/cdrom0/
   ```

   This command displays the presence of an icms directory.

7. Add the software package by entering the following command at the *UNIX* prompt:

   ```
   $ pkgadd -d /cdrom/cdrom0 icms
   ```

   Release numbers and the names of the files in the package displays.

8. If you are using more than one ACD, the system prompts you for information about setting up ACDs.

9. Select option number `3` from the `cmssvc` menu to turn CMS `on` and verify that processes are running.

   The `***CMS is now up***` message displays.

10. Verify that the Web server is running on *CentreVu* CMS by entering the following command at the *UNIX* prompt:

    ```
    $ ps -ef | grep http
    ```

    One or more lines of process information displays for the Web server.

    NOTE:
    If process information does not display, you must reboot your machine and repeat step 10.

11. Verify that you can reach the *CentreVu* CMS machine from the *Java* server. To do this, enter the following URL into a Web browser on the Java server:

    ```
    http://<cmshost>/cgi-bin/uncgi/inc_data?
       vdn=<xxxx>&page_url=<yyyy>&<parameter>=<zzz>
    ```

<cmshost>	The CMS server.
<xxxx>	*<xxxx>* is the VDN you are using.

<*yyyy*>	<*yyyy*> is the URL you are using.
<*parameter*>	The <*parameter*> can be icalls_offered, pri_limit, no_agents, or ivoice_limit.
<*zzz*>	<*zzz*> is the amount you want to increment this parameter.

12. Verify that at least port 8001 is accessible from external sites if the Web page counter is to be used. To do this, enter the following URL into your Web browser from a connection outside of the firewall:

```
http://<cmshost>:8001/cgi-bin/uncgi/pgcnt?
     callUsSrcPage=<pageid>
```

<cmshost>	<*cmshost*> is the CMS server.
<*pageid*>	<*pageid*> is the URL of the page you are using.

Every time you send this URL (or select **Reload**) you get a blank screen. If errors are present, check Chapter 4, “Firewall and Security Guidelines,” for details. The installation is now complete.

13. Eject the CD-ROM using the following command:

```
$ eject -d
```

The installation of the ICMS software is complete.

Internet Call Center Report Summary

New reports that support the ICC are available for *CentreVu* CMS and Supervisor. Details about these reports can be found in the sections that follow. In addition, customers can create their own custom and designer ICC reports.

NOTE:
Real-Time and Historical reports can be created for *CentreVu* CMS, but only Historical or Snapshot reports can be created for *CentreVu* Supervisor. (All Supervisor report descriptions appear in the Historical tabbed folder.)

The following table summarizes the standard ICC reports available for *CentreVu* CMS and *CentreVu* Supervisor.

Report Name	Type[a]	Page Hit Information[b]
CMS Reports		
VDN Call Attempts	Real-Time	No
Web Page Call Attempts	Real-Time	Yes
Call Attempts	Real-Time	Yes
VDN Call Attempts	Historical	No
VDN and URL	Historical	Yes
Page Hits	Historical	Yes
Supervisor Reports		
Graphical Internet VDN Call Attempts (Snapshot)	Snapshot	No
Internet Web Page Call Attempts (Snapshot)	Snapshot	Yes
Internet Call Attempts (Snapshot)	Snapshot	Yes
Graphical Internet VDN Call Attempts	Historical	No

Report Name	Type[a]	Page Hit Information[b]
Internet VDN and URL	Historical	Yes
Internet Page Hits	Historical	Yes
Graphical Internet VDN Calls Summary	Historical	No

a. The “Type” column refers to the type of report: Real-Time, Historical, or Snapshot. (Snapshot reports display a snapshot of the Real-Time data but do not automatically refresh.)
b. The “Page Hit Information” column indicates whether page hit information is displayed in the report. If page hit data is not collected, the content of the reports may be affected.

About ICMS Database Items

The following are new database items for Internet-specific data:

- `icalls_offered`—Refers to the number of Internet Calls that are offered by the ITG. This data item is associated with the VDN and URL sent with the VDN and URL sent with the message.
- `ivoice_limit`—Refers to the number of Internet voice calls that could not be serviced because the administered limit for simultaneous Internet Voice calls was reached. This data item is associated with the VDN and URL sent with the message. Text Chat only and PSTN Callback calls shall not affect this database item.
- `no_agents`—Refers to the number of calls that could not be serviced because there were no agents logged in to handle Internet calls. This database item is associated with the VDN and URL sent with the message.
- `page_hits`—Refers to the number of times ICC enabled pages were accessed.

  Data is collected for this item only if access to the CMS server is allowed through the firewall and proper changes are made to the Web page. See Chapter 4, “Firewall and Security Guidelines,” or Chapter 9, “Web Page Guidelines,” for details.
- `pri_limit`—Refers to the number of calls that could not be serviced because there was insufficient PRI channels available. This data item is associated with the VDN and URL sent with the message.
- `page_url`—Refers to a unique identifier for the ICC enabled Web page (this may be the Web page’s URL).

Internet CMS Reports

This section provides a description of the standard reports to be provided for the ICC on *CentreVu* CMS.

Things to Know About These Reports

For the ICC, a set of standard reports is available to present and correlate data from Internet calls. Custom reports can also be created by the customer.

- An Internet category is available from the Reports menu within the Real-Time and Historical submenus.
- For standard *CentreVu* CMS report information and details about input windows, see the *CentreVu CMS Real-Time and Historical Reports* (585-215-821) document.

CMS Internet Real-Time Reports

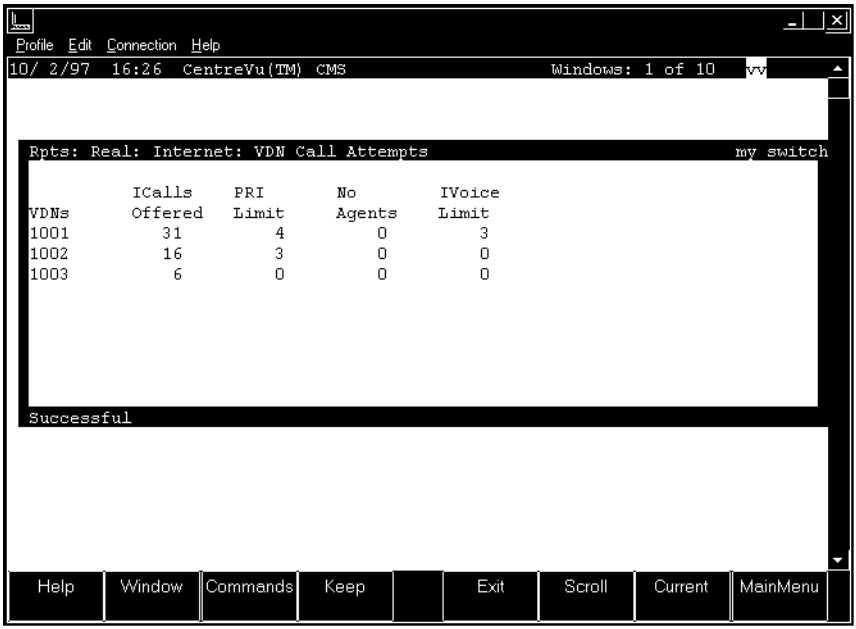
Internet VDN Call Attempts Report

This report provides a real-time summary of calls offered by the ITG for each of the specified Internet VDNs during the current interval. The report includes the number of calls offered by the ITG along with the number of calls that had to be turned away due to PRI limit, No agent, and IVoice limit conditions.

Things to Know About This Report

- Sorts data by VDN extension.
- Uses stored database items in the `r_vdnsum` table.
- Requires Administrators to specify inputs:
  - One or more VDNs
  - Refresh rate.

Report Example



Report Heading	Description	Database Item/ Calculation
VDNs	The number or name of the VDN for which the report shows data (selected in the report input window).	VDN
ICalls Offered	The number of the calls launched for the specified VDN(s) across all pages.	icalls_offered
PRI Limit	The number of calls turned away due to a lack of PRI facilities.	pri_limit

Report Heading	Description	Database Item/ Calculation
No Agents	The number of calls turned away due to a situation where no agents are logged in for ICC calls.	no_agents
IVoice Limit	The number of Internet Telephony calls turned away because the administered maximum was exceeded.	ivoice_limit

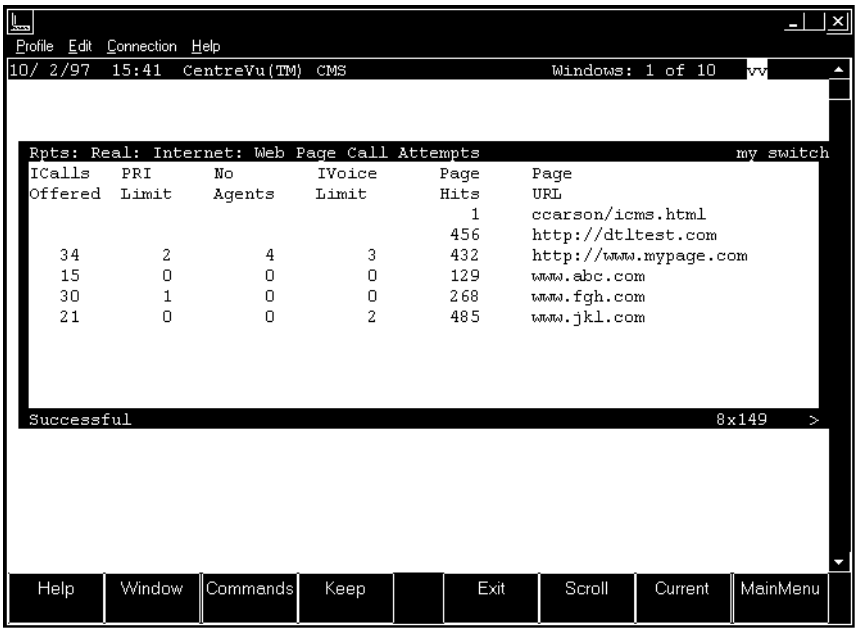
Internet Web Page Call Attempts Report

This report provides real-time Internet call information for all of the ICC enabled Web pages during the current interval. The report includes the number of calls offered by the ITG, the number of page hits, and the number of calls that had to be turned away due to Pri_limit, No agent, and IVoice limit conditions.

Things to Know About This Report

- Sorts data alphabetically by URL.
- Displays data only for URLs which are visited during the interval (in other words, URLs which are not accessed during the interval are not displayed).
- Uses stored database items in the `r_pagesum` table.
- Requires one input field—Refresh rate.
- Displays no data when page hit information is not available (for example, if the firewall prevents external access to CMS).

Report Example



Report Heading	Description	Database Item/ Calculation
ICalls Offered	The number of the calls offered for each URL during the current interval.	icalls_offered
PRI Limit	The number of calls turned away due to a lack of PRI facilities.	pri_limit
No Agents	The number of calls turned away due to a situation where no agents are logged into the ICC.	no_agents

Report Heading	Description	Database Item/ Calculation
IVoice Limit	The number of Internet Telephony calls turned away because the administered maximum was exceeded.	ivoice_limit
Page Hits	The number of page hits counted for the page_url during the current interval.	page_hits
Page URL	A unique identifier for the ICC enabled Web page (may be the Web page's URL)	page_url

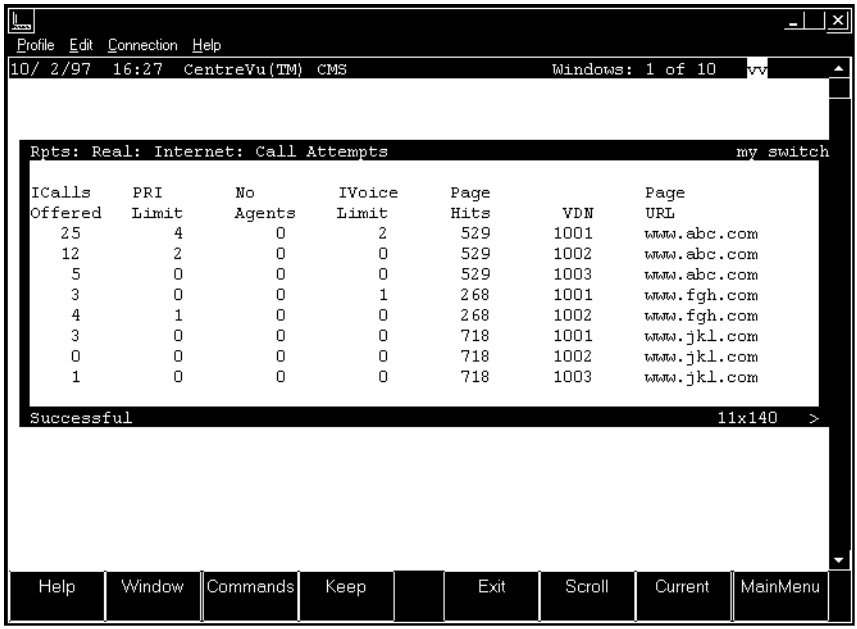
Internet Call Attempts Report

This real-time report provides real-time Internet call information for the specified VDN(s) along with page hit and URL information during the current interval. The report includes the number of calls offered by the ITG along with the number of calls that had to be turned away due to PRI Limit, No agent, and IVoice limit conditions.

Things to Know About This Report

- First sorts data alphabetically by URL, then numerically by VDN.
- Uses stored database items in the `r_pagevdn` table.
- Displays "Page URLs" multiple times with the "Page Hits" data being the same for each entry. This is due to the fact that multiple VDNs can be assigned to the same page.
- Requires inputs:
  - — One or more VDNs
  - — Refresh rate.

Report Example



Report Heading	Description	Database Item/ Calculation
ICalls Offered	The number of the calls offered for the table row's vdn/page_url pair during the current interval.	icalls_offered
PRI Limit	The number of calls turned away due to a lack of PRI facilities during the current interval. This value is tracked based on the table row's vdn/page_url pair.	pri_limit

Report Heading	Description	Database Item/ Calculation
No Agents	The number of calls turned away due to a situation where no agents are logged into the ICC. This value is tracked based on the table row's vdn/page_url pair.	no_agents
IVoice Limit	The number of Internet Telephony calls turned away because the administered maximum was exceeded. This value is tracked based on the table row's vdn/page_url pair.	ivoice_limit
Page Hits	The number of page hits counted for the page_url during the current interval.	page_hits
VDN:	The number or name of the VDN for which the report shows data (selected in the report input window).	VDN
Page URL	A unique identifier for the ICC enabled Web page (may be the Web page's URL)	page_url

CMS Internet Historical Reports

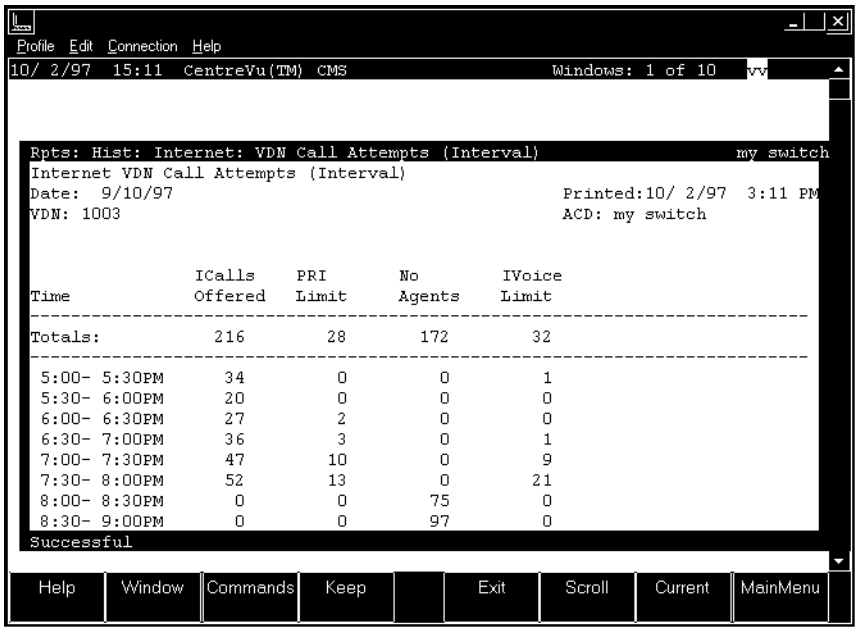
Internet VDN Calls Attempts Report

This historical report displays the sum of the Internet calls offered and PRI_limit, No_agents, and IVoice Limit situations for the specified VDN during each recorded interval.

Things to Know About This Report

- Provides interval, daily, weekly, and monthly report formats.
- Uses stored database items in the `vdnsum` table.
- Requires inputs:
  - A single VDN
  - Time range and date for Interval report
  - Date range for daily, weekly, and monthly reports.

Report Example (Interval)



Report Heading	Description	Database Item/ Calculation
Date: (for Interval)	The date of the report.	ROW_DATE
Printed:	Day and time *CentreVu* CMS printed or displayed the report.	No database item or calculation.
VDN:	The VDN requested from the input window.	vdn
ACD:	The ACD name or number for which the data was collected.	syn(ACD)

Report Heading	Description	Database Item/ Calculation
Time (for Interval reports only)	Intervals which the data applies.	<STARTTIME, STARTTIME + INTRVL>
Date (for Daily, Weekly, and Monthly)	Day, week, or month for which the report was run.	ROW_DATE
ICalls Offered	The sum of the number of the calls offered for the specified VDN.	icalls_offered
PRI Limit	The sum of the number of calls turned away due to a lack of PRI facilities for the specified VDN.	pri_limit
No Agents	The sum of the number of calls turned away due to a situation where no agents are logged in for ICC calls for the specified VDN.	no_agents
IVoice Limit	The number of Internet telephony calls turned away because the administered maximum was exceeded.	ivoice_limit

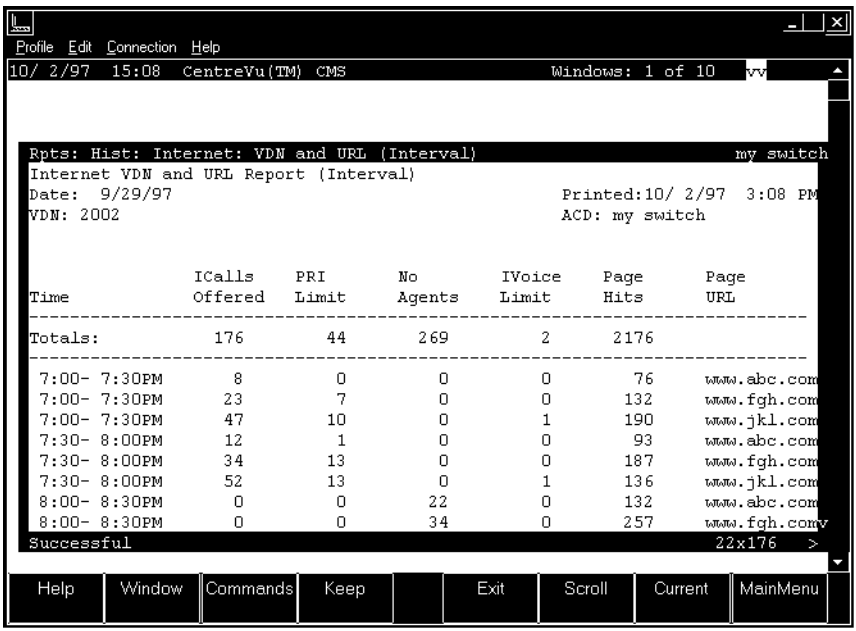
Internet VDN and URL Report

This historical report displays the number of the Internet Calls Offered, PRI Limit, No_agents, and IVoice Limit situations, page hits and page URLs for Web pages associated with the specified VDN during each recorded interval.

Things to Know About This Report

- Provides interval, daily, weekly, and monthly report formats.
- Uses stored database items in the `h_pagevdn` (interval), `d_pagevdn` (daily), `w_pagevdn` (weekly), or `m_pagevdn` (monthly) tables.
- Requires inputs:
  - A single VDN
  - Time range and date for Interval report
  - Date range for daily, weekly, and monthly reports.
- Differs from the Historical Internet VDN Call Attempts report in that it also provides URL information for the associated VDN (multiple URLs may map to the same VDN).
- Determines which pages result in the most calls.

Report Example



Report Heading	Description	Database Item/ Calculation
Printed:	Date and time *CentreVu* CMS printed or displayed the report.	No database item or calculation.
Date: (Interval, Daily, Weekly, and Monthly)	The day for which the report was run.	ROW_DATE
ACD:	Name or number of the ACD for which the report was run.	syn (ACD)
VDN:	The specified VDN.	vdn

Report Heading	Description	Database Item/ Calculation
Time (for interval reports only)	Intervals which the report covers.	<STARTTIME, STARTTIME+ INTRVL>
ICalls Offered	The number of Internet calls offered for the table row's vdn/page_url pair.	icalls_offered
PRI Limit	The number of calls turned away due to a lack of PRI facilities. This value is tracked based on the table row's vdn/page_url pair.	pri_limit
No Agents	The number of calls turned away due to a situation where no agents are logged into the ICC. This value is tracked based on the table row's vdn/page_url pair.	no_agents
IVoice Limit	The number of Internet Telephony calls turned away because the administered maximum was exceeded. This value is tracked based on the table row's vdn/page_url pair.	ivoice_limit
Page Hits	The number of page hits counted for the page_url.	page_hits
Page URL	A unique identifier for the ICC enabled Web page (may be the Web page's URL).	page_url

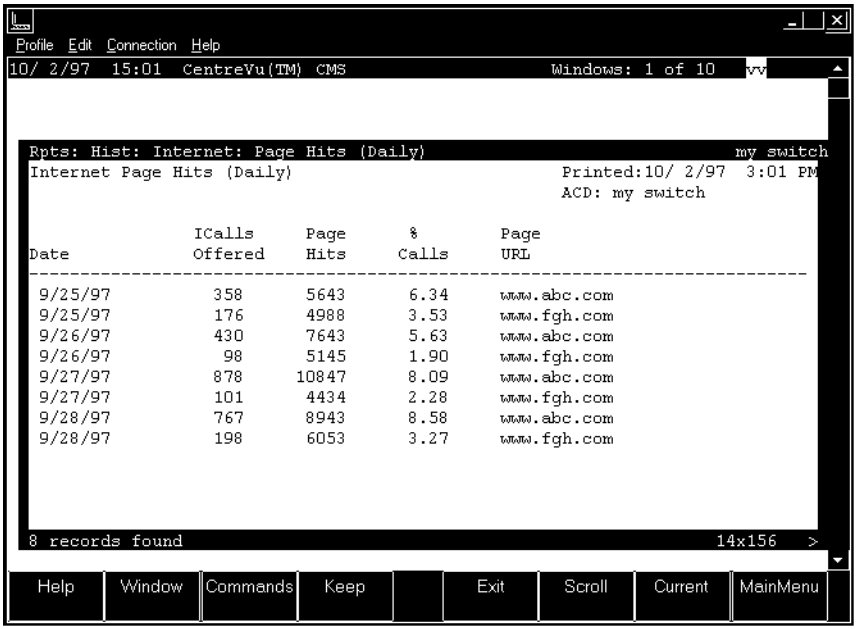
Internet Page Hits Report

This historical report displays the number of page hits for each ICC enabled URL and the number of calls launched from that page.

Things to Know About This Report

- Provides interval, daily, weekly, and monthly report formats.
- Displays the number of ACD calls, the number of page hits, and the ratio of calls to page hits for each ICC-enabled URL. Data for the URL displays only if the page was loaded by a consumer.
- Uses stored database items in the `pagesum`, `h_pagesum` (interval), `d_pagesum` (daily), `w_pagesum` (weekly), or `m_pagesum` (monthly) tables.
- Requires inputs:
  - Time range and date for Interval report
  - Date range for daily, weekly, and monthly reports.
- Displays no data in the event that page hit information is not available (for example, if a firewall prevents external access to CMS).

Report Example



Report Heading	Description	Database Item/ Calculation
Date:	The day for which the report was run.	ROW_DATE
Printed:	The day and time *CentreVu* CMS printed or displayed the report.	No database item or calculation.
ACD:	The ACD that contains the associated VDN in the report.	syn(ACD)

Report Heading	Description	Database Item/ Calculation
Time: (Interval only)	The time the report captured data.	<ROW_TIME, STARTTIME, STARTTIME+ INTRVL>
Date: (Daily, Weekly, Monthly)	The day for the data.	ROWDATE
ICalls Offered	The sum of the number of Internet calls launched for all VDNs associated with the page_url.	icalls_offered
Page Hits	The number of page hits counted for the page_url.	page_hits
% Calls	The ratio of calls offered to page hits.	icalls_offered / page_hits
Page URL	A unique identifier for the ICC enabled Web page (may be the Web page's URL)	page_url

CentreVu Supervisor Internet Reports

Things to Know About These Reports

- *CentreVu* Supervisor does not support Internet real-time reports. However snapshots of information can be displayed. These ICC-specific Supervisor reports are called “Snapshot” reports and can be found in the Designer category of the Historical table folder (for example, Internet Calls Denied Snapshot, Internet Page Hits Snapshot). These reports do not refresh automatically. It is therefore up to the administrator to restart the report manually to get a current snapshot.
- For information on how to use standard *CentreVu* Supervisor report information, and for details about input windows, see the *CentreVu Supervisor User Guide* (585-215-829).
- Three new graphical historical *CentreVu* Supervisor reports are available for ICC:
  - — Graphical Internet VDN Calls Attempts (Snapshot)
  - — Graphical Internet VDN Call Attempts
  - — Graphical Internet VDN Calls Summary.
- *CentreVu* CMS reports are also available in *CentreVu* Supervisor, but with differences. The following table maps the CMS report names to the Supervisor report names.

CMS Report Name	Supervisor Report Name
Real-Time Web Page Call Attempts	Internet Web Page Call Attempts (Snapshot)
Real-Time Call Attempts	Internet Call Attempts (Snapshot)
Historical VDN and URL	Internet VDN and URL
Historical Page Hits	Internet Page Hits

- See the “CentreVu Supervisor Internet Reports” section of this document for details about equivalent *CentreVu* Supervisor reports.
- All Supervisor Internet reports are available from the Designer Category in the Historical tab.
- Only historical or snapshot designer reports can be created using *CentreVu* Supervisor’s Report Designer.

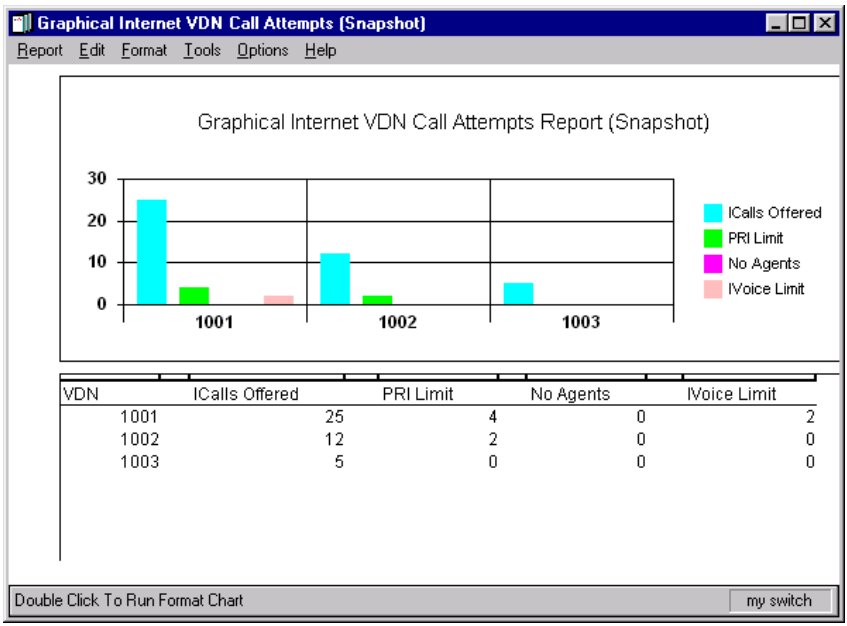
Graphical Internet VDN Call Attempts (Snapshot) Report

This historical report graphically displays data regarding the number of Internet calls-offered and the number of calls that had to be turned away for one or more VDNs during the current interval.

Things to Know About This Report

- Displays a graphical version of the *CentreVu* CMS Real-Time VDN Call Attempts report.
- Displays a snapshot of the data for the current interval and does not automatically refresh.
- Uses stored database items in the `r_vdnsum` table.
- Requires input for one or more VDN.

Report Example



Report Heading	Description	Database Item/ Calculation
VDN	The VDN requested on the input page.	vdn
ICalls Offered	The number of Internet calls offered for the current interval for the specified VDN.	icalls_offered
PRI Limit	The number of calls turned away due to a lack of PRI facilities for the current interval for the specified VDN.	pri_limit

Report Heading	Description	Database Item/ Calculation
No Agents	The number of calls turned away due to a situation where no agents are logged in for ICC calls for the current interval for the specified VDN.	no_agents
IVoice Limit	The number of Internet Telephony calls turned away because the administered maximum was exceeded for the current interval for the specified VDN.	ivoice_limit

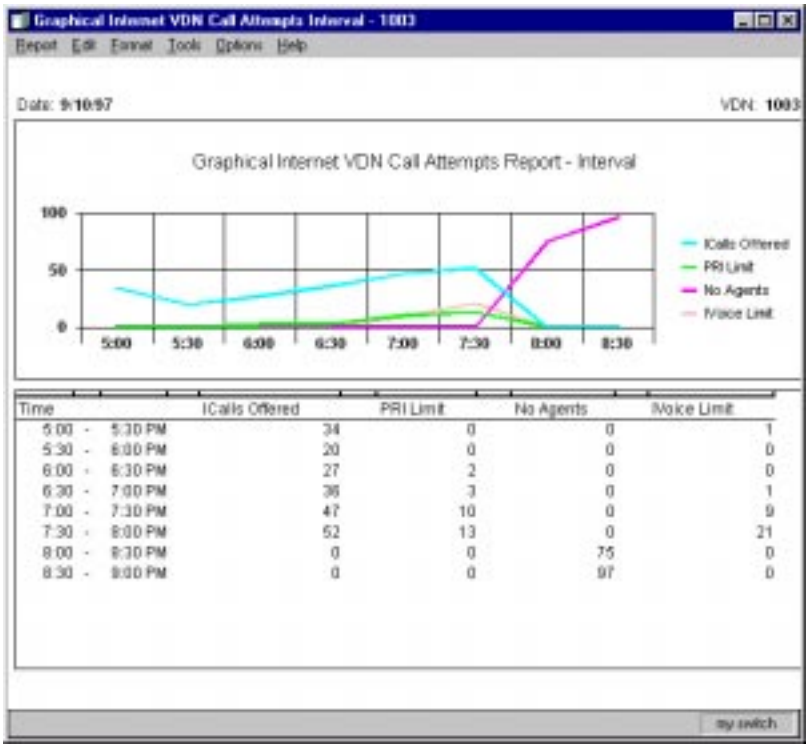
Graphical Internet VDN Call Attempts Report

This historical report graphically displays the number of calls offered by the ITG and the number of calls turned away for a particular VDN over the specified interval.

Things to Know About This Report

- Displays a graphical version of the *CentreVu* CMS VDN Call Attempts report.
- Provides interval or daily report formats.
- Uses stored database items in the `r_vdnsum`, `h_vdnsum` (interval), `d_vdnsum` (daily) tables.
- Displays the number of calls offered by the ITG and the number of calls turned away due to PRI Limit, No Agents, and Ivoice Limit data for the specified VDN.
- Requires inputs:
  - A single VDN
  - Time range and date for Interval report
  - Date range for daily reports.

Report Example



Report Heading	Description	Database Item/ Calculation
Date: (Interval and Daily)	The day for which the report was run.	ROW_DATE
Time: (Interval only)	The time that the report covered.	STARTTIME
VDN:	The VDN requested on the input page.	vdn

Report Heading	Description	Database Item/ Calculation
Time (for Interval reports only)	Intervals which the data applies.	<STARTTIME, STARTTIME + INTRVL>
ICalls Offered	The sum of the number of Internet calls offered for the specified VDN.	icalls_offered
PRI Limit	The number of calls turned away due to a lack of PRI facilities.	pri_limit
No Agents	The number of calls turned away due to a situation where no agents are logged in for ICC calls for the current interval for the specified VDN.	no_agents
IVoice Limit	The sum of Internet Telephony calls turned away because the administered maximum was exceeded.	ivoice_limit

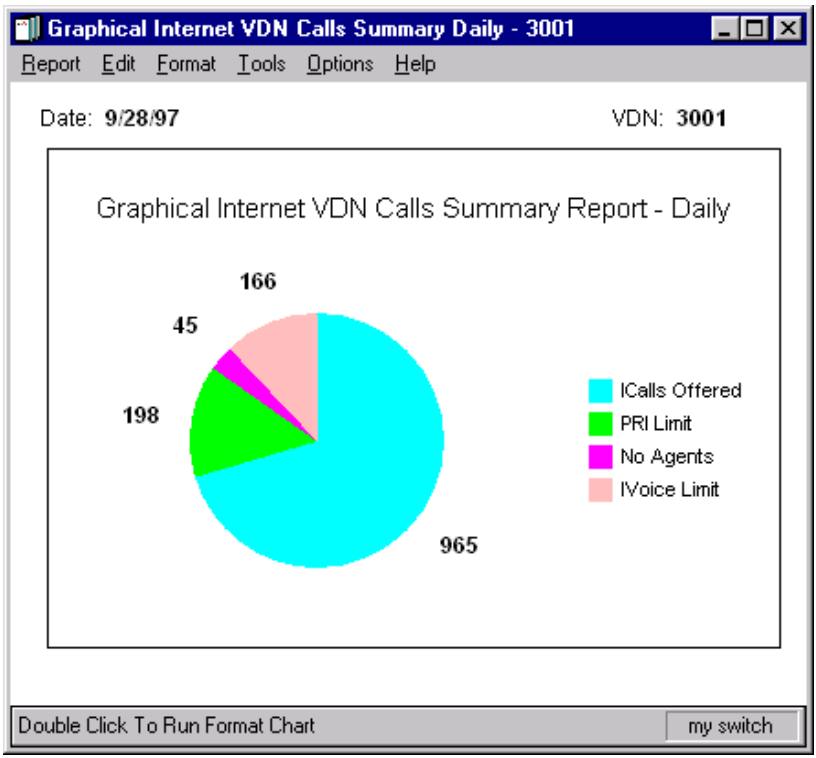
Graphical Internet VDN Calls Summary Report

This historical report shows a graphical summary of the number of Internet calls offered and the number of calls that had to be turned away for a particular VDN during the specified interval. This statistical information for a specified Internet VDN is displayed in a pie chart.

Things to Know About This Report

- Provides interval or daily report formats.
- Requires inputs:
  - A single VDN
  - A single date according to interval and daily data.
- Uses stored database items in the `r_vdnsum`, `h_vdnsum` (interval), `d_vdnsum` (daily) tables.
- Graphs a pie chart of Internet Call statistics for a specified Internet VDN, in particular, the number of calls offered by the ITG, the number of calls turned away due to a lack of PRI facilities, the number of calls turned away due to a no agents staffed situation, and the number of calls turned away due to the Internet Voice limit being reached.
- Displays no chart if no data is found for the specified VDN.

Report Example



Report Heading	Description	Database Item/ Calculation
Date:	The day for which the report was run.	ROW_DATE
VDN:	The VDN requested on the input page.	vdn
ICalls Offered	The number of calls offered by the ITG for the specified VDN.	icalls_offered

Report Heading	Description	Database Item/ Calculation
PRI Limit	The number of calls turned away due to a lack of PRI facilities for the specified VDN.	pri_limit
No Agents	The number of calls turned away due to a situation where no agents are logged in for ICC calls for the specified VDN.	no_agents
IVoice Limit	The number of Internet Telephony calls turned away because the administered maximum was exceeded for the specified VDN.	ivoice_limit

ICMS Database Tables

This section contains the tables and items that support the *CentreVu* CMS enhancements for the ICC.

NOTE:
Database tables and items that are standard to *CentreVu* CMS and *CentreVu* Supervisor are described in the standard *CentreVu* CMS and *CentreVu* Supervisor documentation.

page table

The "page" table stores URL and page hit information. This information, based on data embedded in the ICC-enabled Web pages, is sent to *CentreVu* CMS any time the page is loaded for viewing. The table names are r_page, c_h_page, c_d_page, c_w_page, and c_m_page. These names identify the real-time, interval, daily, weekly, and monthly tables, respectively.

Database Item	Description
page_url	A unique identifier for the ICC-enabled Web page (may be the Web page's URL).
page_hits	The number of page hits counted for the page_url.
row_date	Date on which data was collected.
starttime	The start time for the interval data that was collected (only applies to the r_page and c_h_page tables).

ivdn table

The "ivdn" table stores information associated with a VDN / URL pair such as the number of calls offered by the ITG and the number of calls turned away for various reasons. This information is sent to *CentreVu* CMS by the ITG. The table names shall be r_ivdn, c_h_ivdn, c_d_ivdn, c_w_ivdn, and c_m_ivdn. These names identify the real-time, interval, daily, weekly, and monthly tables, respectively.

Database Item	Description
page_url	A unique identifier for the ICC enabled Web page (may be the Web page's URL).
vdn	A VDN associated with the Web page.
icalls_offered	The number of Internet calls offered by the ITG for the table row's vdn/page_url pair.
pri_limit	The number of calls turned away due to a lack of PRI facilities for the table row's vdn/page_url pair.
no_agents	The number of calls turned away due to a situation where no agents are logged in for ICC calls for the table row's vdn/page_url pair.
ivoice_limit	The number of Internet Telephony calls turned away because the administered maximum was exceeded for the table row's vdn/page_url pair.
acd	The ACD number for which data was collected.
row_date	Date on which data was collected.
starttime	The start time for the interval data that was collected (only applies to the r_ivdn and c_h_ivdn tables).

pagesum view

The "pagesum" view is generated from the data in the page and ivdn tables. This view sums the number of calls for each URL. The names of this view shall be r_pagesum, h_pagesum, d_pagesum, w_pagesum, and m_pagesum. These names identify the real-time, interval, daily, weekly, and monthly tables, respectively.

Database Item	Description
page_url	A unique identifier for the ICC enabled Web page (may be the Web page's URL).
icalls_offered	The number of Internet calls offered by the ITG. This value is summed across all VDNs associated with the page_url.
page_hits	The number of page hits counted for this page_url.
pri_limit	The sum of the number of calls turned away due to a lack of PRI facilities. This value is summed over all VDNs for the specified URL.
no_agents	The sum of the number of calls turned away due to a situation where no agents are logged in for ICC calls. This value is summed over all VDNs for the specified URL.
ivoice_limit	The sum of the number of Internet Telephony calls turned away because the administered maximum was exceeded. This value is summed over all VDNs for the specified URL.
acd	The ACD number for which data was collected.
row_date	Date on which data was collected.
starttime	The start time for which the interval data that was collected (only which applies to the r_pagesum and h_pagesum tables).

vdnsum view

The "vdnsum" view is generated from the data in the page and ivdn tables. This view sums the number of calls that were processed and denied for each VDN. The names of this view shall be r_vdnsum, h_vdnsum, d_vdnsum, w_vdnsum, and m_vdnsum. These names identify the real-time, interval, daily, weekly, and monthly tables, respectively.

Database Item	Description
vdn	A VDN associated with the Web page.
icalls_offered	The number of Internet calls offered by the ITG. This value is summed over all URLs for the specified VDN.
pri_limit	The number of calls turned away due to a lack of PRI facilities. This value is summed over all URLs for the specified VDN.
no_agents	The number of calls turned away due to a situation where no agents are logged in for ICC calls. This value is summed over all URLs for the specified VDN.
ivoice_limit	The number of Internet Telephony calls turned away because the administered maximum was exceeded. This value is summed over all URLs for the specified VDN.
acd	The ACD number for which data was collected.
row_date	Date on which data was collected.
starttime	The start time for which the interval data that was collected (only applies to the r_vdnsum and h_vdnsum tables).

pagevdn view

The "pagevdn" view is generated from the data in the page and ivdn tables. The names for this view shall be r_pagevdn, h_pagevdn, d_pagevdn, w_pagevdn, and m_pagevdn. These names identify the real-time, interval, daily, weekly, and monthly tables, respectively.

Database Item	Description
vdn	A VDN associated with the Web page.
page_url	The ICC enabled Web page's URL identifier.
icalls_offered	The number of calls offered by the ITG for the table row's vdn/page_url pair.
pri_limit	The number of calls turned away due to a lack of PRI facilities for the table row's vdn/page_url pair.
no_agents	The number of calls turned away due to a situation where no agents are logged in for ICC calls for the table row's vdn/page_url pair.
ivoice_limit	The number of Internet Telephony calls turned away because the administered maximum was exceeded for the table row's vdn/page_url pair.
page_hits	The number of page hits counted for the page_url.
acd	The ACD number for which data was collected.
row_date	Date on which data was collected.
starttime	The start time for which interval data that was collected (only applies to the r_pagevdn and h_pagevdn tables).

Cross-Product Information

Page Hit Data

In order to receive page hit information, access from the consumer's browser to the *CentreVu* CMS unit is needed through the call center's firewall. The counter used on the *CentreVu* CMS system is on a well-defined port and requests for other services on this port shall be denied. See Chapter 4, "Firewall and Security Guidelines," or see Chapter 9, "Web Page Guidelines," for more details.

CentreVu CMS and ITG

Internet call data is also sent from the ITG to the *CentreVu* CMS server. HTTP access between these systems through port 80 is required.

CentreVu Supervisor

As noted earlier, Real-Time Internet reports are not supported by Supervisor. Therefore, all that is available are Historical and Snapshot reports. Snapshot reports provide a snapshot of the Real-Time data, but do not automatically refresh. All reports (including Snapshot reports) are found in the Historical tabbed folder.

References

The following documents include additional information about *CentreVu* CMS or Supervisor:

- *CentreVu™ Supervisor Version 5 User Guide* (585-215-829*)
- *CentreVu™ Supervisor Version 5 Installation and Getting Started* (585-215-830)
- *CentreVu™ Report Designer Version 5 User Guide* (585-215-831)
- *CentreVu™ Supervisor Version 5 Change Description* (585-215-832)
- *CentreVu™ CMS R3V5 Administration* (585-215-820)
- *CentreVu™ CMS R3V5 Real-Time and Historical Reports* (585-215-821)
- *CentreVu™ CMS R3V5 Custom Reports* (585-215-822)
- *CentreVu™ CMS R3V5 Change Description* (585-215-823)
- *CentreVu™ CMS R3V5 Upgrades and Migration* (585-215-826)
- *CentreVu™ CMS R3V5 Sun SPARCserver Computers Installation and Maintenance* (585-215-827)
- *CentreVu™ CMS R3V5 Sun SPARCserver Computers Connectivity Diagram* (585-215-828).

*This document is also available in the following languages: French (FR), Dutch (NL), Japanese (JA), Portuguese (PTB), German (DE), and Columbian Spanish (ESC). A two- or three- letter code after the ordering number indicates the language of the document.

9

Web Page Guidelines

Introduction

This chapter contains guidelines for designing, creating, modifying, or enhancing Web pages to work in conjunction with the Internet Call Center (ICC) solution. Sections in this chapter include:

- Agent Login Web Page
- Consumer Web Pages.

For additional examples of Web pages, see the "itg" Web directory on the *Java* server by entering the following URL:

```
http://javaserver/itg/icc_samples.html.
```

Audience

This chapter is intended for supervisors, system administrators, and persons responsible for designing and implementing Web pages for an Internet Call Center. Audiences for this chapter should already be familiar with Hypertext Markup Language (HTML) and want to make their Web pages ICC-enabled. Contact Lucent Technologies' NetCare Services for assistance in developing Web pages. Otherwise, developing a Web site is the responsibility of the call center.

Agent Login Page

An Agent Login Web page must be developed so that agents can log into the ICC. This page may provide the agent with instructions, but more importantly, a form must be constructed to collect agent information and pass it to the CGI script: `agentapplsu.pl`.

The Agent Login Web page must contain the following parameters. These parameters must be passed to the `agentapplsu.pl` script located in the `itg/cgi-bin` directory on the *Java* server.

Input Name	Value	Description
`agentId`	Numeric	Expert Agent Selection (EAS) Login ID for the agent.
`agentExt`	Numeric	Extension of the agent's voice terminal.
`agentName` (optional)	Text	Agent's name.
`browseWinURL` (optional)	URL	This URL is displayed to the agent while the agent applet is downloading. It defaults to `/itg/icc_welcome.html` (if not specified).
`helpURL` (optional)	URL	This URL is displayed when the Help button found on the Agent Control Window is pressed. The default is `/itg/cphelp.html`.

Input Name	Value	Description
showLogout (optional)	yes/no	This parameter controls the visibility of a Logout button on the Agent Control Window. If set to yes, a Logout button is displayed on the agent's applet. If set to no, the Logout button is not visible. **NOTE:** This parameter must be used in conjunction with the Agent Logout Button Administration. If the Agent Logout option is disabled, the button on the Agent Control Window does not work even though it may be visible. The default for the showLogout parameter is no.

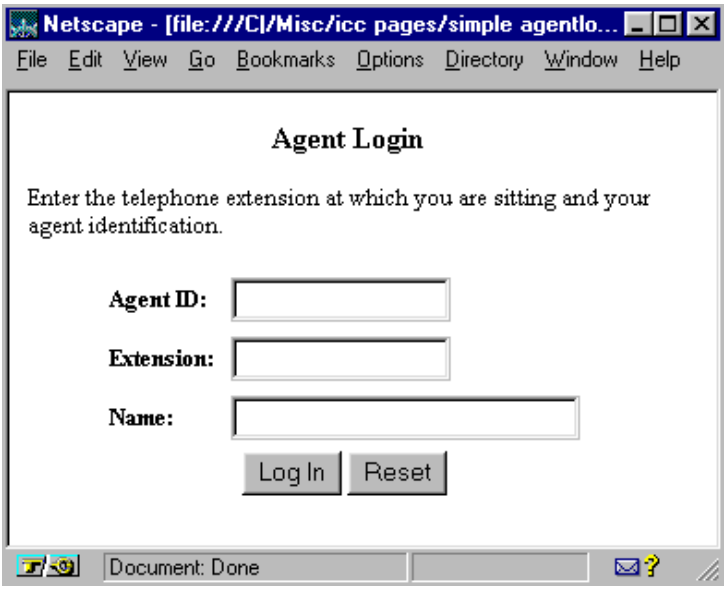
Additional customer-defined parameters can be submitted to the agentapplsu.pl script. These parameters do not affect the login process but are passed to the URL administered for the Agent Idle event.

NOTE:
The Agent Name parameter is optional because it does not affect the login process. However, this parameter is special in that it is also passed to the URL associated with the Caller's Call Answered event message. Using this parameter, a script can display the agent's name to the customer when the call is answered.

The following is an example HTML code used to create an Agent Login Web page:

```
<center>
<h3>Agent Login</h3>
</center>

Enter the telephone extension at which you are
sitting and your agent identification.

<p>
<form action="http://javahost.com/cgi-
bin/itg/agentapplsu.pl" method="post">
<center>
<table>
<tr>

        <th align=left>Agent ID:

        <TD><input type=text name="agentId"
size="15" maxlength="50">
<tr>

        <th align=left>Extension:

        <TD><input type=text name="agentExt"
size="15" maxlength="50">
<tr>

        <th align=left>Name:

        <TD><input type=text name="agentName"
size="25" maxlength="50">
</table>
<input type=hidden name="browseWinURL"
value="/itg/icc_welcome.html">

<input type=hidden name="helpURL"
value="http://javahost.com/itg/cphelp.html">
<input type=hidden name="showLogout" value="yes">
<input type=submit name="Login" value="Log In">
<input type=reset name="Reset" value="Reset">
</center>
```

The following is an example of an Agent Login Web page:



Consumer Web Pages

This section describes the ICC enhancements necessary for a call center's Web pages:

- Enhancements for Access
- Example of Using a Form
- Enhancements to Support *CentreVu* CMS
- Customer-Defined Parameters
- Special Considerations About Frames
- Other ICC Web Pages
- Call Control Window Logo.

Enhancements for Access

Customers can access a call center agent from the Web by requesting a Voice and Chat (Internet telephony), Chat Only (Text Chat), or Call Back Only (customer-initiated callback) session. For example, the call center can provide one or more methods of access on any Web page by referencing the `/cgi-bin/itg/callerapplsu.pl` script found on the *Java* server in the installation.

The following is a list of parameters that must be submitted to the `callerapplsu.pl` script:

Input Name	Value	Description
`vdn_ext`	Numeric	VDN to which the Internet call should be routed. If the `vdn_ext` parameter is not set, the call cannot be processed (the ITG does not know where to launch the call) and the consumer is taken to the “Missing VDN Data” URL that tells the consumer that something is wrong and to try a different method of contacting the call center. This page can be created and administered by the call center. See Chapter 6, “ITG and Java Server Guidelines,” for administration details.
`type` (optional)	Text	Type of call. Valid values include "voice" for Voice and Text Chat calls, "chatter" for Text Chat-only calls, and "callback" for PSTN Callback. If the `type` parameter is not set, the call is processed, but the input defaults to a Text Chat-only call as “chatter.”
`callUsSrcPage` (optional)	Text	The URL of the Web page that originated the call request (used for tracking call statistics). Can also be used for a Web Pop when the call is connected to bring both parties to the originating page. If the `callUsSrcPage` parameter is not set, the call is processed and a message is sent to *CentreVu* CMS to increment the counter for the URL as the default "none.”

Input Name	Value	Description
`browseWinURL` (optional)	Text	As soon as the ITG receives a call request, this URL displays on the consumer's browser while the Caller Control Window downloads and opens. If the `browseWinURL` parameter is not set, the call is processed and the Web page found at `/itg/icc_welcome.html` is the default page displayed to the consumer while the Caller Control Window is downloading.
`cbno` (optional)*	Numeric	This is the number to be dialed when a callback is requested* (only required for the Callback option).
`helpURL` (optional)	Text	This page is displayed when the Help button on the Caller Control Window applet is selected. When the consumer selects the **Help** button on the Caller Control Window, the Web page at `/itg/cphelp.html` is displayed. If the helpURL parameter is not set, the default Web page found at `/itg/cphelp.html` is displayed.
The default uses relative addressing to locate the `cphelp.html` file. This is done because each ICC installation has a different name for the *Java* server. *Netscape Navigator*[a] assumes that addressing is relative to the server that downloaded the applet (the *java*`host.com` machine). However, *Microsoft*[b] Internet Explorer assumes the addressing is relative to the server that downloaded the current Web page. Therefore, it is highly recommended that a full URL path name be provided for this parameter (for example, `http://`…).		

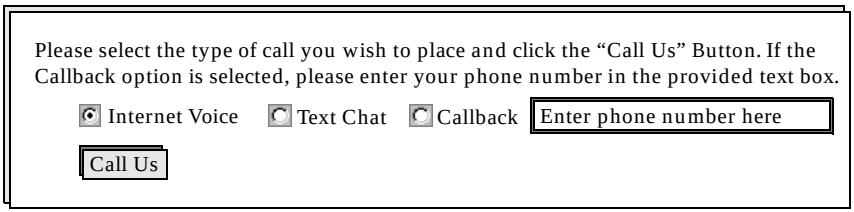
a. Netscape Navigator is a trademark assigned to Netscape Communications, Inc.
b. Microsoft is a registered trademark of Microsoft Corp.

Example of Using a Form

In the following example of HTML code used for creating a “call us” page, `javahost.com` refers to the name or IP address of the *Java* server. Text links, image buttons, image maps, and other methods of creating hypertext links can be used.

```
<FORM NAME=”Form1”
    ACTION=”http://javahost.com/cgi-
bin/icc/callerapplsu.pl”>
Please select the type of call you wish to place
and click the “CallUs” Button.
<P>
<INPUT TYPE-HIDDEN NAME=vdn_ext
VALUE=81234
<INPUTTYPE=HIDDENNAME=callUsSrcPage
VALUE=”http//catalog.com/shirts/thispage.html”
<INPUTTYPE=HIDDENNAME=helpURL
VALUE=”http//javahost.com/icc/cphelp.html”>
<INPUT TYPE=radio NAME=”type”
VALUE=”voice” checked
onclick=”Formt.vdn_ext.value=81234”>

Internet Voice
<INPUT TYPE=radio NAME=”type”
VALUE=”chatter”
onclick=”Formt.vdn_ext.value=81235”>

Text Chat
<INPUT TYPE=radio NAME=”type”
VALUE=”callback”
onclick=”Formt.vdn_ext.value=81236”>

Call back
<INPUT TYPE=text NAME=”cbno”
VALUE=”Enter Phonenumber here”
SIZE=”25”
MAXLENGTH=”50”<I>
<INPUT TYPE=SUBMIT VALUE=”Call Us”>

</FORM>
```

The following is an example of radio buttons on a form:



Enhancements to Support *CentreVu* CMS

If the ICC enhancements have been installed on a call center's *CentreVu* CMS, then Web page hits and call statistics can be correlated and integrated into a single report. This saves the call center from having to retrieve page hit statistics from the Web server and call statistics from the *CentreVu* CMS. In order for *CentreVu* CMS to collect these statistics, the following enhancements must be made to the Web pages. It is assumed that HTTP access to the *CentreVu* CMS server has been provided through the call center's firewall on the well-defined port of 8001. See Chapter 4, "Firewall and Security Guidelines," for details.

Page hit statistics are collected by sending the `callUsSrcPage` parameter to the `pgcnt` CGI script found on the *CentreVu* CMS server. Each ICC-enabled page references this script through the use of the IMG tag. In order for page statistics to be accurate, the value of the `callUsSrcPage` parameter must be the same as the `callUsSrcPage` parameter passed to the `callerapplsu.pl` script. See the "Enhancements for Access" section in this chapter for details.

The following example of HTML shows the code that must be embedded into the Web page.

```
<img src="http://cms-host.com:8001/cgi-bin/
   uncgi/pgcnt?callUsSrcPage="http://catalog.com/
   shirts/thispage.html" WIDTH=1 HEIGHT=1>
```

Although it appears that this places a 1x1 pixel image on the page, the reference is really accessing a script that counts the number of hits to the ICC-enabled Web page.

Customer-Defined Parameters

In addition to the input parameters that the ICC requires, a call center can also define its own parameters that can be passed to the `callerapplsu.pl` script. The ICC forwards them to the URLs administered to be associated with call progress messages and events. For example, a call center may request that the consumer enter a registration or account number into a Web form. If this information is sent to the `callerapplsu.pl` script, it is forwarded to the URLs associated with all of the events triggered by the call (for example, Incoming Call Queued, Call Answered, and so on).

This account number can then be used in a CGI script to perform a database lookup to present a personalized message to the consumer (for example, "Thank you, David, for calling us via the Internet…"), or account information can be accessed and presented in the Agent's Call Answered URL. However, additional CGI programming is required to access a call center's customer database.

NOTE:
The support for customer-defined inputs is available until a call is connected to an agent. After the call is connected, URLs are no longer directed to the browsers by the ICC. However, because the call is connected, the agent should be able to get any further information from the consumer via the communication path (that is, Text Chat, Internet telephony, or Callback).

Special Considerations About Frames

Frames introduce complex interactions to support Escorted Browsing. This involves significant changes to frame-based Web pages.

With Escorted Browsing, the consumer can press the Send Page button on the Caller Control Window, and the agent's browser is updated to display the same URL (and vice versa). This update is accomplished using a technique called URL sharing wherein the URL that is visible in one party's browser toolbar is sent to the other party's browser. The receiving browser then accesses the URL to display the same screen.

The challenge arises when a frame-based Web page is being viewed, because the URL visible in the toolbar is the frame definition file. Although a consumer may surf around within a frame, thereby changing the frame's contents, the URL displayed remains that of the frame definition file. When the **Send Page** button is pressed, the URL that is sent is the one for the frame definition file. As a result, pages are loaded based on the defaults specified in the frame definition file, not based on the current contents of the frames.

The ICC solution to support frames requires some *Java*script to be added to both the frame definition file and the frame content files.

In the frame definition file, add the following script:

```
<script language="Javascript">
   var syncToFrameNo = -1;
   var syncToLoc = location.href;
   </script>
```

This piece of *Java*script defines the scripting variables used by the frame content files. `SyncToFrameNo` is used to store which frame has changed and `syncToLoc` stores the frame content's URL.

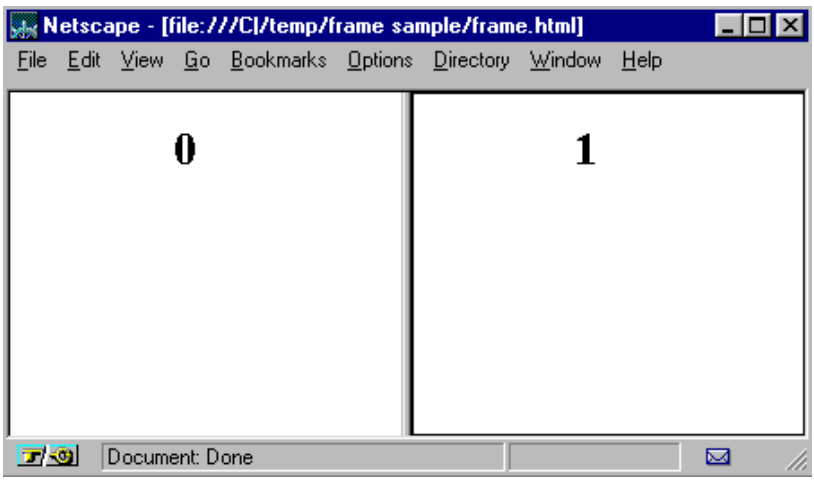
In the frame content files, some *Java*script is used to set these variables. The `syncToLoc` variable is set to the current URL by using the `location.href` environment variable. However, to understand how to set the `syncToFrameNo` variable, some explanation is needed to describe how frames are numbered.

Numbering for a Single Frameset

The following HTML code is an example for a simple two-frame Web page:

```
<FRAMESET COLS="*, *">
<FRAME src="frame0.html">
<FRAME src="frame1.html">
</FRAMESET>
```

The following image is displays:



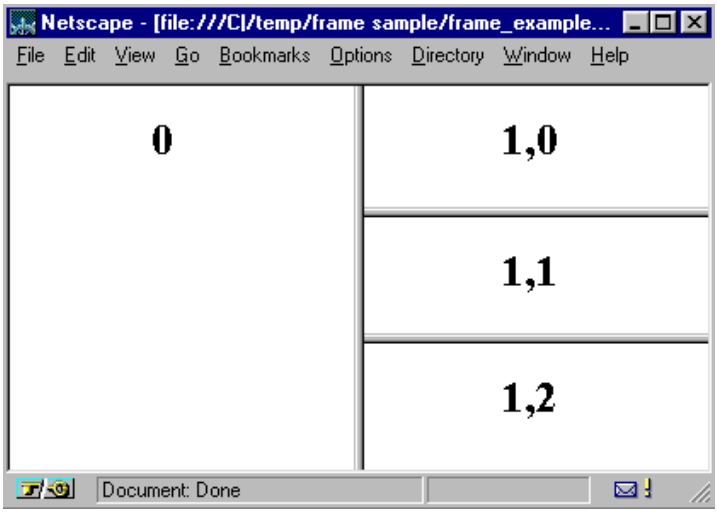
The code uses a single Frameset and the frames are numbered from left to right starting at 0 (zero).

Numbering for Two Framesets

The following HTML code divides one of the frames into three subframes:

```
<FRAMESET COLS="*, *">
<FRAME src="frame0.html">
<FRAMESET ROWS="*,*,*">
<FRAME src="frame10.html">
<FRAME src="frame11.html">
<FRAME src="frame12.html">
</FRAMESET>
</FRAMESET>
```

The following image is displayed:



In this example, two framesets are used.

The frame numbering for the left frame is still 0, but the right half has a numbering scheme that resembles how an array is indexed. The first number indicates the right half of the first frameset and the second number indicates the frame within the frame. For example, the lower right frame in the second frame of the first frameset (1) and the third frame of the second frameset (2). Notice that frame numbering always starts at 0.

Adding *Java*script to Frame Content Files

When the contents of a frame change, *Java*script in the frame content files is needed to update the ITG with the new information.The code to add looks like the following:

```
<script language="Javascript">
parent.syncToLoc=location.href;
parent.syncToFrameNo="1,1";
</script>
```

The `syncToLoc` variable informs the ITG of the new URL to display in the frame designated by the `syncToFrameNo` variable.

NOTE:
The frame number is in quotation marks and has no spaces (for example, "`1,1`"). Also note that the variables are prefixed with the keyword "`parent`."

Other ICC Web Pages

Web pages on CGI scripts can be displayed for various event and error conditions (for example: Incoming Call Queued, Call Answered, Call Limit Reached, etc.). See the Appendix, "ITG and Java Server Administration Field Descriptions," for a complete list of these administrable Web pages. Example pages are available in the itg directory on the *Java* server.

Call Control Window Logo

The logo that appears at the top of the Call Control Window can be changed. Simply create a .gif image no larger than 300x150 pixels, name it `customer.gif` and place it in the `itg\images` directory on the *Java* server.

10

Troubleshooting

Introduction

This chapter provides troubleshooting guidelines for the Internet Call Center (ICC) solution. Information in this chapter represents a compilation of known problems and suggested solutions, based on actual installations.

Audience

This document is intended for installers, administrators, agents, and anyone who uses the ICC solution.

References

- *DEFINITY® Communications System Call Vectoring/EAS Guide* (555-230-520)
- *PassageWay® Telephony Services Solution, Microsoft* Windows† NT‡ Telephony Services Installation Guide* (555-201-116) (provided on the *PassageWay* Telephony Services CD)
- *PassageWay Telephony Services for Microsoft Windows NT Telephony Services DEFINITY Enterprise Communications Server Network Manager's Guide* (555-201-505) (provided on the *PassageWay* Telephony Services CD)
- *Internet Telephony Gateway Technical Reference* (555-027-212).

Background Information

This chapter documents problems that might occur, offers suggestions for isolating and fixing problems, lists reference documents for solution components, and identifies items to check before calling NetCare Services at 1-800-4NetCare.

*Microsoft is a registered trademark of Microsoft Corp.
†Windows is a registered trademark of Microsoft Corp.
‡NT is a registered trademark of Microsoft Corp.

Call Center Trouble Scenarios

The following sections describe typical call center trouble scenarios and list actions to take when troubleshooting them. In general, each action builds on the previous ones.

Administration Web Pages Cannot Be Accessed

Description

An attempt to access the ICC Web-based administration at `http://<ITG_address>:<admin_port>` produces an error or else no Web page appears.

Action

1. Verify that the HTTP process is actually executing on the ITG. Run the command `ps -ax | grep http` from the ITG console or terminal connection. This command displays several lines which indicate that multiple HTTP processes are executing. If there are no processes executing, then execute the commands `/www/bin/adminHTTP` and `/www/bin/startHTTP`, or `reset level=boot`, on the ITG. Refer to Chapter 6, "ITG and *Java* Server Guidelines," for details.

2. Web administration access may be restricted to specific IP addresses. On the ITG, execute the command `/www/bin/adminHTTP`. When asked **"**Please specify IP addresses for which admin access is to be allowed (comma-list),**"** enter the correct address(es) or leave blank.

3. If there is a connectivity problem between the current browser and the ITG, troubleshoot LAN connectivity. Verify that the ITG is accessible on the LAN and from the computer running the browser.

Agent Control Window Fails to Launch Properly

Description

The Agent Control Window fails to download or display properly after the agent fills out the form on the login page and submits it.

Actions

1. Verify that the agent's Web browser is *Java**-enabled:
   - On *Netscape Navigator*† 3.x, from the **Options** menu select the **Network Preferences** item, and then select the **Languages** tab to display its contents. Both the "Enable Java" and "Enable JavaScript" items should be checked.
   - On Internet Explorer 3.x, from the **View** menu select the **Options** item, and then select the **Security** tab. The "Enable Java Programs" and "Run ActiveX Scripts" items should be checked.
2. Check for error messages on the browser window. Also open the *Java* Console window and look for errors:
   - On *Netscape Navigator,* use **Options->Show Java Console**.
   - On Internet Explorer, check the "Enable Java Logging" box on the **View->Options->Advanced** tab. Stop and restart Internet Explorer, then periodically use a text editor (such as Notepad) to examine the `c:\windows\javalog.txt` file.
3. Check to see whether network settings have been changed. The browser may need to be changed to reflect "no proxy" settings for the ICC components on the network.
4. Connect a PC to the same LAN segment as the *Java* server and verify that the agent can log in. If so, then examine the administration of the firewall and other intermediate equipment, using the rules in Chapter 4, "Firewall and Security Guidelines," as a reference.

---

*Java is a registered trademark of Sun Microsystems, Inc.
†Netscape Navigator is a trademark assigned to Netscape Communications Corp.

Agent Cannot Log In

Description

The initial download of the Agent Control Window occurs properly, but the login sequence fails.

Action

1. If no further progress is seen after the “Establishing Connection” message appears in the Agent Control Window, verify that the *Java* server is up and the Internet Call Manager (ICM) application is running.
2. Check that the firewall is administered to allow TCP connections from a dynamic TCP port (>1023) on the agent’s PC to the *Java* server, TCP port 8101. Review Chapter 4,“Firewall and Security Guidelines,” for further details on firewall rules and the port required by ICC components.
3. If Agent Control Window activity stops after the “Logging In, Please Wait” message, perform the following:
   - See whether the specified Agent extension is in use. If so, hang up the phone and enter the password again**.**
   - Verify *DEFINITY* ECS status for station xxxx, using the adjunct link (ADJLK) extension. Check the status of the *DEFINITY* LAN Gateway board. If the status station command reveals that the ADJLK station is “disconnected,” refer to *PassageWay* documentation to troubleshoot the *DEFINITY* ECS-to-*PassageWay* Telephony Server connection.
   - Confirm that the ITG, the *PassageWay* Telephony Server, and the *Java* server are communicating. See the “System Problems” section elsewhere in this chapter.

4. If a “Login failed” message is displayed in the Agent Control Window with one of the following additional messages, perform the indicated action:
   - “Agent_Already_Logged_Into_Switch” means that the specified agent ID or extension has been logged into the *DEFINITY* ECS via a voice terminal rather than through the Web login page. Use the *DEFINITY* ECS `list agent-id` command to discover whether the agent ID or the extension is in use.
   - “Requested_AgentID_Ext_Mismatch” means that the specified agent ID has been logged into the *DEFINITY* ECS at the specified extension rather than through the Web login page. Log off from the voice terminal and log in again through the Web login page.
   - “Agt_Not_Split_Member_Or_Bad_Passwd” means that an incorrect password was entered. (In a non-EAS environment, this can also mean that the agent attempted to log into a split that the agent is not a member of.)
   - “Invalid_Skill/Split” means that an invalid agent ID was entered. The agent ID was either entered incorrectly or the *DEFINITY* ECS administration is incorrect. Be sure that the agent is administered with the ICC skill, then have the agent try to log in manually from a phone. If the login attempt fails, troubleshoot the *DEFINITY* ECS. If the login attempt works, have the agent log out and try to log in again via the browser.
   - “Tsrv_Device_No_Admin” means that the specified extension was entered incorrectly or that it is not administered in the *Passageway* Telephony Server’s Security Database.
5. If a pop-up window appears stating “You are already logged in at Extension xxx. What would you like to do?”, perform the following:
   - The ICM Control Window shows that the specified agent ID is logged in at the indicated extension. Select the **Force Log Out** button on the pop-up window to log the other session out, or select the **Quit** button to abort the login attempt.

- If the **Force Log Out** button is used but the message "Force Out FAILED Agent_Is_Busy**"** is displayed, then a call is in progress at the other agent station. When that call terminates, the agent is logged out.
- If the forced logout does not work, then on a *DEFINITY* ECS console enter `list agent-id xxxx`. If it shows as "unstaffed," then there may be a *Java* server or *Passageway* Telephony Server problem.

6. Check the *PassageWay* Telephony Server hardware to make sure that it is fully in service (not in the login window) and does not have any status windows showing a problem. Make sure the agent's physical phone extension is administered as a device in the *Passageway* Telephony Server's Security Database.

   NOTE:
   Shut down any software packages running on the *PassageWay* Telephony Server (except for *Passageway*). Do not run any other applications on the server until the problem is resolved.

7. Check the status of the *Java* server:
   - Make sure that the ICM application is running by looking in the *Windows NT* Task Bar for ICM.BAT and Internet Control Manager. Check for any status windows showing a problem.
   - Enter the command `dumpconns` in the text entry field. See whether ICM thinks the agent is already logged in, as shown by a line listing the `Agent` with the specified ID.
   - If the agent is shown to be logged in, issue the ICM command `sendto cti logout extension passageway_group agent-id`. (The `passageway_group` is typically "none.") Reissue the `dumpconns` command to verify the agent is logged out, and have the agent try logging in again from the Web page. If the command does not log the agent out, verify the phone extension and group in the *PassageWay* Telephony Server.

Agent Cannot Receive Calls

Description

Once an agent is logged in and the Agent Control Window is open on the desktop, calls should be able to reach the agent. If it becomes apparent that the agent is not receiving calls, follow these steps to identify the problem. Also see the *DEFINITY Communications System Call Vectoring/EAS Guide* (555-230-520) for more detailed *DEFINITY* ECS troubleshooting guidelines.

Action

1. Confirm that the agent is logged into the *DEFINITY* ECS ACD by entering the `list agent_id xxxx` command on a *DEFINITY* ECS console. Also note whether the agent is administered with the Internet skill(s).

2. If the call center has BCMS, enter the command `monitor bcms skill <Internet skill>`. Verify that the agent is staffed, has the correct physical extension, and is in the "Available" state.

3. On the *Java* server, confirm that the ICM lists the agent as logged in by entering the command `dumpconns` in the text entry field. Look for a line listing the agent with the specified ID.

4. Verify that the VDN is processing the call correctly by placing a test call from another phone to an Internet VDN. Check vector steps for the correct call flow.

5. Verify that the trunks between the *DEFINITY* ECS and the ITG are in service. On the ITG console, use the `showptg` and `showpri` commands. On the *DEFINITY* ECS console issue the command `test trunk-group xx long`. Troubleshoot any trunk problems using *DEFINITY* ECS documentation.

6. Verify the caller Web page has the correct URL reference with the correct VDNs and call types. See Chapter 9, "Web Page Guidelines," for details.

7. Place a call from a browser inside the firewall. If the call completes, there may be a firewall issue. See Chapter 4, "Firewall and Security Guidelines," for further information.

Agent Gets Voice Call But No Audio Connection

Description

If an agent is getting calls from the Voice VDN (as indicated by the phone display and / or the VDN of Origin announcement) without any audio connection to the caller, use these suggestions to identify the problem.

Action

1. Check the caller Web page to see that `type=voice` for the radio button used to select a voice call. See Chapter 9, "Web Page Guidelines," for details.
2. Verify that the Telephony Application URL, administered via the ICC administration Web pages, references a script that correctly launches the *NetMeeting* application. The default URL is `http://java_server/itg/cgi-bin/icc_nmit.pl`.
3. Check to see whether the firewall is passing User Datagram Protocol (UDP) packets to the ITG. See Chapter 4, "Firewall and Security Guidelines," for details. If the caller's firewall is not passing UDP packets, the Callback feature may be useful.

Agent Gets a Call But No Web Pop

Description

As part of the process of connecting with an incoming Internet-initiated call, the browser should display a Web Pop (the page the caller initiated the call from, or some other page as defined by the call center). If no Web Pop occurs when a call comes in, use the following steps to identify the problem.

Action

1. Verify that the call was a Web-initiated call (in other words, that it arrived on an Internet VDN).
2. Confirm that the caller page is programmed correctly. See Chapter 9, “Web Page Guidelines,” for details.
3. Confirm that the Call Progress and Features URL administration on the ITG is correct. See Chapter 9, “Web Page Guidelines,” for details.

Escorted Browsing Does Not Work

Description

The caller (or agent) attempts to send a URL using the **Send Page** button on their Control Window but the other party does not receive the page.

Action

1. If the receiver gets a Web page with an error such as “Access Denied,” check to see whether the person has permission to access a particular URL (for example, if it is behind a firewall).
2. Determine which version of the Web browser is being used. The 4.0 and greater versions of *Netscape Navigator* and Internet Explorer have blocked the feature that supports the **Send Page** operation, so that button does not work with a 4.0 or greater version of either browser. However, Escorted Browsing can still be accomplished in a 4.x browser environment by entering the URL to be shared in the Text Chat entry box on the Control Window, by typing or by cutting and pasting, and sending it like a regular text message.

No Calls Arrive at a New VDN

Description

A new VDN is added to the system (for example, for a new call type or to direct calls for a specific product), but no calls arrive at that VDN.

Action

1. Verify via *DEFINITY* ECS administration that the new VDN has been assigned the same Class of Restriction (COR) as other Internet VDNs.
2. Use the `showdp` command on the ITG console to verify that the new VDN has been added to the ITG dial plan. See the *Internet Telephony Gateway Technical Reference* (555-027-212) for details on how to add a VDN to the dial plan.
3. Examine the caller Web page to confirm that the new VDN is specified appropriately as the `vdn_ext`.

Caller Is Unable to Launch *NetMeeting*

Description

A caller must have *NetMeeting* 2.0 to launch an Internet telephony call to an Internet Call Center. The *NetMeeting* application is launched on the caller's machine as a helper application associated with the browser.

If the caller is using Internet Explorer, then the helper application is launched automatically. If the caller is using *Netscape Navigator*, then the caller must identify the helper application to the browser the first time an ICC call is launched.

Action

If the caller is unable to launch *NetMeeting*, try the following.

1. Identify which browser the caller is using.
2. Verify that the caller has installed *NetMeeting* 2.0. It can be downloaded at no charge from `http://www.microsoft.com`.
3. If the caller's browser is *Netscape Navigator*, the caller must identify the helper application to the browser when the "Unknown File Type" dialog box appears:
   - Select the **Pick App** button.
   - Under "Configure External Viewer," enter `rundll32.exe msconf.dll,OpenConfLink`. The entry field is case sensitive, so the entry must be typed exactly as shown.
   - Select **OK**.
4. Verify, via the Web administration Call Progress and Features Administration page at `http://<ITG_address>:<admin_port>`, that the Telephony Application URL correctly points to `http://<java_server_address>/itg/cgi-bin/icc_nmit.pl`. If not, edit file `/mmcs/etc/itg.cfg` on the ITG and set the `TelephonyAppURL` to that URL.

Caller Is Unable to Connect to an Agent

Description

If a caller launches a call but is not connected with an agent (the Caller Control Window is downloaded but stops after the “Establishing Connection” message), this may be due to a firewall issue on the caller side. If the caller is behind a firewall, the firewall may block the messaging needed to establish an Internet call session.

Action

1. Verify that the call center’s firewall is not the problem by placing an Internet call from outside the firewall.
2. If the caller’s firewall is the problem, nothing can be done from within the call center. However, the caller can still request a PSTN Callback. See the “Agent Cannot Receive Calls” section in this chapter for more suggestions.

Status Messages for Callers

Description

Sometimes a caller cannot connect with an agent due to various reasons within the call center. In those cases, the caller sees one of the following status messages:

- "No facilities are currently available." This is displayed when there are no PRI lines available to complete the call.
- "No agents are currently available." This is displayed when no agents are logged in.
- "Internet telephony capacity exceeded." This is displayed when the limit of Internet voice calls has been reached.

Action

Any of these conditions prevents a caller from being connected on the type of call requested. It is advisable to incorporate additional information and options for the caller on the Web page (such as hours of operation, an 800 number, an e-mail address, and so on), and to consider adding extra capacity, more agents and/or longer staffed hours of operation.

Control Window Closes During a Call

Description

In general, if the Caller Control Window closes during a call, the call is dropped. (A PSTN Callback voice call, however, stays up.) This can happen, for instance, if the caller explicitly closes the window or uses the **Back** button on Internet Explorer to back up past the page that launched the call.

If the Agent Control Window closes while the agent is still staffed, the current call, if any, ends and the agent is logged out. The agent needs to log in from the Agent Login Web page again, then put the voice terminal into Manual-In or Auto-In work mode.

There is no way to reconnect or recover the original call.

“Connection Lost” Message Appears on the Agent Control Window

Description

A “Connection Lost” message appears in the Text Chat region of the Agent Control Window. A pop-up window also appears with the message “Your connection has been lost. Would you like to reconnect?” These actions indicate that the TCP connection between the agent’s PC and the *Java* server has been dropped, so the agent has no communication channel to the ICC for browser-based activities.

Action

1. Select the **Yes** button on the pop-up window. If there are no further error messages, there was probably a temporary LAN glitch.
2. Verify that the *Java* server is up and the ICM application is running.
3. Check the firewall administration for a rule that causes TCP connections to time out after a certain interval of inactivity. Consider increasing this timeout parameter.
4. Troubleshoot LAN problems. Inspect all intermediary equipment (hubs, switches, routers) for errors. Check for excessive LAN congestion. To have the LAN inspected by a Lucent Technologies Network Consultant, contract for this work by calling 1-800-4NetCare.

Agent Transfers or Conferences an Internet Voice Call

Description

The agent attempts to transfer or conference an Internet voice call. This can be done the same way as any other call; however, the Agent Control Window is not transferred or conferenced with the audio portion of the call. Therefore, the recipient of the transfer or conference can participate in the conversation but cannot participate in Text Chat or Escorted Browsing activities.

Action

The agent needs to be aware that only the voice portion of a call can be transferred or shared in a conference. This action is not recommended.

Agent Hears an Echo

Description

An agent hears an echo of the agent's own voice when talking with a caller.

Action

1. Determine whether the caller is using an external microphone and speakers. If so, it is likely that the echo is caused by the caller's microphone picking up sound from the speakers. Ask the caller to change the location of the microphone to minimize the echo. For the best sound quality in Internet telephony connections, callers should use a headset.
2. The echo may be coming from the caller's sound card due to a crosstalk problem.

Internet Voice Quality Is Poor

Description

Internet telephony voice quality or audio delay during a call starts out poor or becomes poor during a call.

Action

1. Determine whether the caller's PC is equipped with a half-duplex, rather than full-duplex, sound card. This type of card does not support two-way voice very well
2. Verify that the caller has a *Pentium* PC and at least 16Mb of RAM. CPU- or network-intensive activity can reduce voice quality. Such activities include downloading large files or graphic-rich Web pages, playing music on the PC, or running another application on the PC. Have the caller shut down other applications that may be occupying the CPU.
3. Verify the caller has at least a 28.8kbps connection to the Internet. A low-speed Internet connection, or heavy Internet traffic, or other disruptions from the Internet Service Provider, can cause voice quality to be poor or deteriorate, or produce long audio delays.

The agent may wish to initiate a PSTN callback for better voice quality.

System Problems

ITG Cannot Connect to the *Java* Server

Description

The problem appears when the Internet Call Manager (ICM) process is not running, or the *Java* server is not available on the LAN. This problem is alarmed by the Computer-Telephony Integration (CTI) process in the ITG.

Action

Refer to the repair action for the CTI alarm in the *Internet Telephony Gateway Technical Reference* (555-027-212).

Java Server Cannot Connect to the ITG

Description

If the ICM process on the *Java* server is not able to connect to the ITG, it displays the message "Connection failed, will try again in 10 seconds" in the Agent Control Window. Agents are blocked from logging in or out, and callers are not able to place calls.

This connection may fail due to administration or LAN problems, or because the ITG is not in service. The ICM process periodically attempts to re-establish the connection.

Action

1. If there have been administration changes to the ITG or *Java* server, then first verify that the administration information is correct:
   - Refer to the *Internet Telephony Gateway Technical Reference* (555-027-212) or the Web-based administration on-line Help on the ITG at `http://<itg_address>:<admin_port>` for a description of the administration.
   - Examine the "Networking and Servers" page at `http://<itg_address>:<admin_port>` and verify that all the IP Address fields have valid entries.
   - Once the administration has been checked, verify that the components can communicate across the network. Any firewalls or routers must be administered to allow these components to communicate through the administered port number. Refer to specific router or firewall documentation to verify this functionality.
2. If the connection has been working but has recently gone down, then:
   - Verify that the ITG is in service by entering the `showstatus` command on the console. It should show a system state of `IS`. If the ITG is not in service, then follow standard procedures to bring it into service.
   - Verify that the components can communicate with each other across the network by pinging each component.

ITG Cannot Connect to the *PassageWay* Telephony Server

Description

The CTI process log on the ITG (`/mmcs/debug/cti.log`) displays alarms when it is unable to connect with the *PassageWay* Telephony Server. When this connection is not available, agents are not able to log in or out, and caller requests are not routed to agents.

The CTI process periodically attempts to reconnect with the server.

Action

Refer to the repair action for the CTI alarm in the *Internet Telephony Gateway Technical Reference* (555-027-212).

No CMS Pegs From the Web

Description

Whenever the ICC solution is working but no data is being recorded in CMS regarding Web page hits, use these suggestions to help identify the problem.

Action

1. Access the Web page to verify that it is up and in service. If you cannot access the page, notify the Webmaster.
2. If you can access the Web page, look for a “broken image” icon. If one appears, notify the Webmaster.
3. Test whether the counter script on the CMS server is accessible from the browser from inside the firewall. Enter the URL below into the browser:

   ```
   http://<CMS_address>:8001/cgi-
   bin/uncgi/pgcnt?callUsSrcPage=<pageid>
   ```

   where `<pageid>` is the URL of the Web page that is being counted.
4. Check the HTTP address of the CMS server and the parameters on the Web page to be sure they are correct.
5. Check that the reference to the CMS host uses port 8001. If not, notify the Webmaster.
6. Verify that the firewall allows the CMS TCP port to be passed. Test this by repeating Step 3 from outside the firewall.

No CMS Reports for Call Attempts/Failures

Description

If the ICC solution is working but no data is being recorded in CMS for call attempts when no agents are staffed, voice call attempts when no resources are available, or call attempts when no trunks are available, then use these suggestions to help identify the problem.

Action

1. Verify network connectivity by sending a ping from the *Java* server to CMS. (This test may fail if there is an intervening firewall or filtering router.)
2. Verify that the firewall is administered to allow HTTP requests from the *Java* server to Port 80 on the CMS.
3. Verify, from the Call Progress and Features Web administration page, that the ITG is administered with the correct CMS host name.
4. Verify that the Web pages have the correct page count script. Refer to Chapter 9, “Web Page Guidelines,” for more details.
5. Verify that page hit messages are coming in correctly. See log file `/webcms/db/apache/logs/access_log` on the CMS.

VDN Is Not Pegging Call Data from the *DEFINITY* ECS to CMS

Description

If the ICC solution is working but no call data is being recorded in CMS from the *DEFINITY* ECS, use these suggestions to help identify the problem.

Action

1. Check *DEFINITY* ECS administration to verify that the VDN is measured. The “measured” field on the VDN should be set to “both” or “external.”
2. Verify that CMS is in service.
3. Confirm that the maximum number of VDNs measured on the CMS has not been exceeded.
4. Verify that the X.25 link is up between CMS and the *DEFINITY* ECS.

A

ITG and *Java* Server Administration Field Descriptions

Introduction

This appendix describes Internet Telephony Gateway (ITG) and *Java*[*] server administration fieldpps for the ICC offer.

Audience

This appendix is intended for system administrators, support personnel and anyone who wants an overview of the administration fields.

References

- Chapter 5, “ITG and *Java* Server Guidelines”
- *Internet Telephony Gateway Technical Reference* (555-027-212).

*Java is a registered trademark of Sun Microsystems, Inc.

ITG Configuration File

Shown below is the ITG configuration file (`/mmcs/etc/itg.cfg`) which contains all the administration fields for both the ITG and *Java* server:

```
[HTTP]
SysAdmin=
NetworkName=
HTTP_AdminPort=81
HTTP_Proxy=On
HTTP_ProxyPort=8000
HTTP_RemoteProxy=Off
HTTP_RemoteProxyAddr=
AdminAccessRestrictions=Off
AdminAccessRestrictionsList=
AdminPasswordProtection=Off
LastAdminIP=

[CPP]
AgentIdleURL=
CallAnsweredAgentURL=
CallAnsweredCallerURL=
NoAgentsURL=
PRILimitURL=
MissingDataURL=
CallLimitURL=
CMSPegCountURL=
CallQueuedURL=
CallBackConfirmURL=
TelephonyAppURL=
CallBackRedirectURL=

[JSERVER]
AgentPort=8101
CallerPort=8102
UtilPort=8104
AgentConnectOpts=
CallerConnectOpts=
AgentLogoutOnClose=Enabled
```

```
[NWK]
ServerIP=000.0.000.000
ICMHost=000.0.000.000

[VPH]
;    STARTING_LOCAL_UDP_PORT:
;    Value specifies the local UDP port that will
;    be used to receive incoming voice traffic.
;    These ports will be pre-allocated such that a
;    small range of ports will be used to support
;    all voice traffic (for firewalls, etc.).
;    be reserved.
;
STARTING_LOCAL_UDP_PORT=60000

[ITG]
ITGCALLBACK=Enabled

[cti]
Tserver_LoginID=login
Tserver_Passwd=password
Tserver_ID=LUCENT#G3_SWITCH#CSTA#TSRVICC
HuntGroups=
PrependCallback=
CTIHost=000.0.000.000
PORT=8103
```

This configuration file is laid out in sections. Each section contains related name / value pairs for administration. Section and field names are case sensitive and should not be changed. Fields should not be added, removed, or moved between sections.

Different fields have different formats (text, numbers or keywords). Each field and its format are described in this appendix. Comments exist or can be placed in the file on lines that begin with a semicolon (“;”).

NOTE:
All ICC administration should be performed using Web administration (see the “Administering ITG and Java Server” section in Chapter 5, "ITG and *Java* Server Guidelines"). Lucent Technologies support personnel (who may not have remote Web access to the server) are the only people who should directly edit the ITG configuration file for administrative purposes.

About the ITG Configuration File

Administration field values can be changed by editing the configuration file. A field is considered “blank” if no value is specified. The following example indicates that no system administrator mail address is administered:

```
SysAdmin=
```

To edit the file, either provide a value or replace the current value. The following example shows the field `SysAdmin` with a value of `webmaster@enterprise.com`:

```
SysAdmin=webmaster@enterprise.com
```

Descriptions of each section of the configuration file and its related administration fields are described in the next sections of this Appendix. The field descriptions and examples and are similar to the on-line help that is available from the Web administration pages.

[HTTP] Section

The HTTP section contains fields needed to administer Web services on the ITG.

SysAdmin

This field contains the electronic mail address of the system administrator or some other mailbox that should receive reports of trouble encountered while performing system administration. If the HTTP server encounters an error, it may generate an error message with this e-mail address in it.

Web Name	System Administrator E-Mail
Format	<*login*>@<*domain*> where <*login*> is the mailbox name of the mailbox to receive e-mail and <*domain*> is the domain name where the mailbox can be found.
Example	`webmaster@enterprise.com`
Default	`None`
Notes	This field may be empty.

NetworkName

This field contains the network name or IP address of the ITG as it needs to be known to the HTTP daemon.

Web Name	Network Name
Format	Alphanumeric name of the ITG or IP address.

Examples	`itg`
	`itg.enterprise.com`
	`135.9.224.121`

Default	`None`
Notes	This field may **not** be empty.

HTTP_AdminPort

This field contains the TCP/IP port number on which ITG administration requests are accepted by the ITG.

Web Name	HTTP Admin Port
Format	Numeric
Example	`81`
Default	`81`
Notes	This value may **not** be the value `80`. This field may **not** be empty.

HTTP_Proxy

This field turns proxying capabilities of the HTTP daemon on and off. If the ITG has direct Internet access, proxying allows desktops without Internet access to make HTTP Internet requests through the ITG.

Web Name	HTTP Proxy
Format	Keywords `On` and `Off`
Default	`Off`

HTTP_ProxyPort

This field sets the TCP/IP port number on which the HTTP daemon listens for proxied HTTP requests.

Web Name	HTTP Proxy Port
Format	Numeric
Example	`8000`
Default	`8000`
Notes	This value may **not** be `80` or the HTTP_AdminPort number.

HTTP_RemoteProxy

This field turns remote proxying capabilities of the HTTP daemon on and off. Typically, this is used if the ITG does not have complete Internet access and the Internet Service Provider (ISP) providing the Internet connection gives Internet access through an HTTP proxy.

Web Name	Remote HTTP Proxy
Format	Keywords `On` and `Off`
Default	`Off`

HTTP_RemoteProxyAddr

This field contains the remote HTTP proxy address where the HTTP daemon proxy passes requests that it cannot resolve.

Web Name	Remote HTTP Proxy Address
Format	<*domain*>:<*port*> where <*domain*> is the domain name where the remote HTTP proxy can be found and <*port*> is the TCP/IP port number on which the remote HTTP proxy receives proxy requests.
Example	`proxy.isp.com:8000`
Default	`None`
Notes	This field may **not** be empty if HTTP_Remote Proxy is turned `on`; otherwise, it has no effect.

AdminAccessRestrictions

This field controls the ability to restrict access to ITG administration screens.

Web Name	Admin IP Restrictions
Format	Keywords `On` and `Off`
Default	`Off`

AdminAccessRestrictionsList

This field contains the IP addresses and/or IP address ranges that are allowed access to the ITG administration screens.

Web Name	Admin Access Restrictions List
Format	<*ipaddr*>,<*ipaddr*> where <*ipaddr*> is the address or subnet from which requests for administration pages are to be honored.
Example	`135.9.111.23` allows requests originating from the IP address `135.9.111.23` `135.9.101` allows requests originating from any address in the `135.9.101` subnet
Default	`None`

Notes	Care must be taken when changing this field. Make sure that the IP addresses of the machines that need to perform ITG administration are included in this list. This field can contain multiple entries separated by a comma. This field may **not** be empty if AdminAccessRestrictions is turned `on`; otherwise, it has no effect.

AdminPasswordProtection

This field controls the ability to restrict ITG administration screens to the `sysadm` user-ID. A user is required to enter the correct administrator's user-ID and password before access is allowed.

Web Name	Admin Password Protection
Format	Keywords `On` and `Off`
Default	`Off`

LastAdminIP

This is an internally managed field that contains the last IP address that performed Web administration.

Web Name	Not available through Web administration
Format	IP address
Notes	There is no reason to change this field.

[CPP] Section

The CPP section defines the URLs to be used by the ICC offer for Web page display to agents or callers during call processing.

AgentIdleURL

This field contains the URL of the page to be displayed to an agent who is logged in but not currently active on a call.

Web Name	Agent Idle URL
Format	URL
Example	`http://www.enterprise.com/itg/agentidle.html`
Default	`None`
Notes	This field must be a fully qualified URL. This field may **not** be empty.

CallAnsweredAgentURL

This field contains the URL of the page to be displayed to an agent receiving an incoming Internet call.

Web Name	Call Answered (Agent) URL
Format	URL
Example	`http://www.enterprise.com/itg/agentans.html`
Default	`None`
Notes	This field must be a fully qualified URL. This field may **not** be empty.

CallAnsweredCallerURL

This field contains the URL of the page to be displayed to the caller whose call is received by an agent.

Web Name	Call Answered (Caller) URL
Format	URL
Example	`http://www.enterprise.com/itg/callerans.html`
Default	`None`
Notes	This field must be a fully qualified URL. This field may **not** be empty.

NoAgentsURL

This field contains the URL of the page to be displayed to the caller when there are currently no agents logged in to take an Internet call.

Web Name	No Agents Logged In URL
Format	URL
Example	`http://www.enterprise.com/itg/noagents.html`
Default	`None`
Notes	This field must be a fully qualified URL. This field may **not** be empty.

PRILimitURL

This field contains the URL of the page to be displayed to the caller when their Internet call cannot be placed into the call center due to insufficient PRI resources between the ITG and call center.

Web Name	PRI Limits Reached URL
Format	URL
Example	`http://cms.enterprise.com/prilimit.html`
Default	`None`
Notes	This field must be a fully qualified URL. This field may **not** be empty.

MissingDataURL

This field contains the URL of the page to be displayed to the caller when a call request is submitted but the VDN extension information is missing.

Web Name	Missing VDN Data URL
Format	URL
Example	`http://www.enterprise.com/itg/missingdata.html`
Default	`None`
Notes	This field must be a fully qualified URL. This field may **not** be empty.

CallLimitURL

This field contains the URL of the page to be displayed to the agent when the ITG is currently processing the maximum number of Internet voice calls, as defined by the purchased system limits.

Web Name	Call Limit Reached URL
Format	URL
Example	`http://www.enterprise.com/itg/calllimit.html`
Default	`None`
Notes	This field must be a fully qualified URL. This field may **not** be empty.

CMSPegCountURL

This field contains the URL of the script for reporting peg counts to CMS.

Web Name	*CentreVu*® (CMS) Peg Count URL
Format	URL
Example	`http://www.enterprise.com/cgi-bin/uncgi/inc_data`
Default	`None`
Notes	This field must be a fully qualified URL. If this field is empty, no CMS peg counting is performed.

CallQueuedURL

This field contains the URL of the page to be displayed to a caller when they are placed in queue for the next available agent.

Web Name	Incoming Call Queued URL
Format	URL
Example	`http://www.enterprise.com/itg/callqued.html`
Default	`None`
Notes	This field must be a fully qualified URL. This field may **not** be empty.

CallBackConfirmURL

This field contains the URL of the page to be displayed to the caller to confirm a request for callback.

Web Name	CallBack Redirection URL
Format	URL
Example	`http://www.enterprise.com/itg/callbackoff.html`
Default	`None`
Notes	This field must be a fully qualified URL. This field may **not** be empty.

TelephonyAppURL

This field contains the URL of the script to execute for launching the caller's Internet telephony application.

Web Name	Telephony Application URL
Format	URL
Example	`http://www.enterprise.com/cgi-bin/itg/icc_nmit.pl`
Default	`None`
Notes	**This field is read-only.** Contact a Lucent Technologies support organization to modify this value. This field must be a fully qualified URL. This field may **not** be empty.

CallBackRedirectURL

This field contains the URL of the page to be displayed to the caller when they request a callback but the feature has been turned off.

Web Name	CallBack Redirection URL
Format	URL
Example	`http://www.enterprise.com/itg/callbackoff.html`
Default	`None`
Notes	This field must be a fully qualified URL. This field may **not** be empty.

[JSERVER] Section

The JSERVER section contains fields specific to communications with the *Java* server or features provided by the *Java* server.

AgentPort

This field contains the TCP/IP port number where the ICM application on the *Java* server is listening for connections from the agent.

Web Name	ICM Caller Connection Port Number
Format	Numeric
Example	`8101`
Default	`8101`
Notes	**This field is read-only.** Contact the Lucent Technologies support organization if the configuration requires that another port be used. This field may **not** be empty.

CallerPort

This field contains the TCP/IP port number where the ICM application on the *Java* server is listening for connections from callers.

Web Name	ICM Caller Connection Port Number
Format	Numeric
Example	`8102`
Default	`8102`
Notes	**This field is read-only.** Contact the Lucent Technologies support organization if the configuration requires that another port be used. This field may **not** be empty.

UtilPort

This field contains the TCP/IP port number where the ICM application on the *Java* server is listening for maintenance and administration requests.

Web Name	ICM Utility Connection Port Number
Format	Numeric
Example	`8104`
Default	`8104`
Notes	**This field is read-only.** Contact the Lucent Technologies support organization if the configuration requires that another port be used. This field may **not** be empty.

AgentConnectOpts

This field contains optional timer values used by the Internet Call Manager (ICM) application on the *Java* server to periodically verify agent connections.

Web Name	Agent Connection Options
Format	Three numeric fields (separated by spaces) specifying milliseconds
Example	`10000 5000 30000`
Default	`None`
Notes	**This field is read-only.** Contact the Lucent Technologies support organization to modify this field.

CallerConnectOpts

This field contains optional timer values used by the ICM application on the *Java* server to periodically verify caller connections.

Web Name	Caller Connection Options
Format	Three numeric fields (separated by spaces) specifying milliseconds
Example	`10000 5000 30000`
Default	`None`
Notes	**This field is read-only.** Contact the Lucent Technologies support organization to modify this field.

AgentLogout

This field enables / disables the Logout button on the Agent Control Window.

Web Name	Agent Logout Button Enable / Disabled
Format	Keywords `Enabled` or `Disabled`
Default	`Disabled`

AgentLogoutOnClose

This field enables / disables the automatic agent logout from the call center if the agent connection to the ICM application on the *Java* server is lost or dropped.

Web Name	Agent Logout On Close Enabled / Disabled
Format	Keywords `Enabled` or `Disabled`
Default	`Disabled`

[NWK] Section

The NWK section contains IP address fields for the ITG and *Java* server.

ServerIP

This field contains the IP address of the Internet Telephony Gateway (ITG).

Web Name	ITG IP Address
Format	IP Address
Example	`135.9.101.2`
Default	`None`
Notes	This field may **not** be a network name. This field may **not** be empty.

ICMHost

This field contains the IP address or network name of the *Java* server where the ICM application is executing.

Web Name	Java Server (ICM) IP Address
Format	Alphanumeric Network Name or IP address
Example	`135.9.101.221` `icm.entrprise.com`
Default	`None`
Notes	This field may **not** be empty.

[VPH] Section

The VPH section contains fields needed for Internet voice processing protocols.

STARTING_LOCAL_UDP_PORT

This field contains the starting UDP port number where the ITG is listening for Internet Telephony connections.

Web Name	First UDP Port Number
Format	Numeric
Example	`60000`
Default	`60000`
Notes	This field may **not** be empty.

[ITG] Section

The ITG section contains fields for activating ITG features.

ITGCallBack

This field controls the ability for callers to request an outgoing call from the call center to a specified number.

Web Name	ITG CallBack Enabled / Disabled
Format	Keywords `Enabled` or `Disabled`
Default	`Enabled`

[cti] Section

The cti section contains fields needed by the Computer Telephony Integration (CTI) process on the ITG for communication and interaction with the *PassageWay*® Telephony Server and the *Java* server.

Tserver_LoginID

This field contains a valid *PassageWay* Telephony Server Login-ID to be used by the CTI process on the ITG.

Web Name	Telephony Server Login ID
Format	Alphanumeric
Example	`tsrv`
Default	`None`
Notes	This field may **not** be empty.

Tserver_Passwd

This field contains a valid *PassageWay* Telephony Server password (associated with the login-ID) to be used by the CTI process on the ITG.

Web Name	Telephony Server Password
Format	Alphanumeric (hidden password)
Example	`tsvrpw`
Default	`None`
Notes	This field may **not** be empty.

Tserver_ID

This field contains the link type description and *PassageWay* Telephony Server identification name to be used by the CTI process on the ITG.

Web Name	Telephony Server Identifier
Format	Alphanumeric
Example	LUCENT#G3_SWITCH#CSTA#TSRVICC
Default	`LUCENT#G3_SWITCH#CSTA#TSRVICC`
Notes	This field must match (exactly) an administered Tlink Name on the *PassageWay* Telephony Server. This field may **not** be empty.

HuntGroups

This field identifies the set of hunt groups (or Skill Set extensions in an EAS environment) that the *PassageWay* Telephony Server is requested to monitor.

Web Name	Monitored Hunt Groups
Format	<*huntgrp*>,<*huntgrp*> where <h*untgrp*> is the extension of the hunt group or skill set.
Example	`5014`, `5015`, and `2442`
Default	`None`
Notes	This field can contain multiple entries separated by a comma. This field may **not** be empty.

PrependCallback

This field contains the digit(s) that must be prepended to any requested callback number in order to place an outgoing call from the call center.

Web Name	Prepend Digits for Callback
Format	Dial String
Example	9
Default	None
Notes	An empty field indicates that no digits are to be prepended. The dial string may contain any telephone keypad digit (0-9,*,#).

CTIHost

This field contains the IP address or network name of the *PassageWay* Telephony Server.

Web Name	Telephony Server IP Address
Format	Alphanumeric Network Name or IP Address
Example	tserver.enterprise.com 135.9.101.121
Default	None
Notes	This field may **not** be empty

PORT

This field contains the TCP/IP port number where the CTI process on the ITG is listening for a connection from the *Java* server.

Web Name	CTI Port Number
Format	Numeric
Example	`8103`
Default	`8103`
Notes	**This field is read-only.** Contact the Lucent Technologies support organization if the configuration requires that another port be used. This field may **not** be empty.

Glossary

GL

ACD	Automatic Call Distribution—A switch feature that distributes incoming calls to available agents.
agent	A call center employee who services calls from the call center's customers.
Agent Control Window	The Internet Call Center Control Window downloaded to the agent's browser.
ANI	Automatic Number Identification—A telecommunications industry term referring to knowledge of the calling party's number.
applet	A small application that is downloaded from the Internet and executed in a browser on a desktop.
ASAI	Adjunct/Switch Applications Interface—Lucent's CTI offering/recommendation for interfacing data adjuncts and communications systems. ASAI supports activities such as event notification and call control.
BCMS	Basic Call Management System—A *DEFINITY* ECS feature that provides a variety of measurements that may be used to monitor the ACD.

call center A business that provides service to its customers via agents. Traditionally, requests for service have come through the use of the telephone, but modern technology has broadened that channel to include fax, voice mail, e-mail, and the Internet.

caller A call center's customer; the person requesting contact with an agent.

Caller Control Window The Internet Call Center Control Window downloaded to the caller's browser.

CGI Common Gateway Interface—The programming interface for executing programs on Web (HTTP) servers. CGI defines the structure for passing data from the server to the server's gateway program, which does the processing, and returning the results from the gateway program to the HTTP server back to the requesting client.

CGI script A program that is run on a Web server, triggered by a request from a browser.

CMS *CentreVu*® Call Management System—An application which runs on an adjunct processor to collect, store, and report call statistics from the ACD. CMS enables call centers to monitor and manage their operations by generating reports on the status of agents, splits/skills, trunks, trunk groups, vectors, and VDNs.

codec

COder / DECoder—An electronic circuit that converts audio or video into digital code, and vice versa. An example of a codec is an analog / digital and digital / analog converter. A codec can also be software that converts packets or streams from one protocol to another.

collaborative browsing

A feature of the ICC solution that includes Web Pop and Escorted Browsing.

CSTA

Computer Supported Telephony Application--An international standard interface between a network server and a telephone switch established by the European Computer Manufacturers Association (ECMA).

CSU

Channel Service Unit—A device residing between customer and Central Office equipment that serves to terminate and recondition the digital signal on a circuit. CSU generally refers to equipment terminating a DS1 circuit.

CTI

Computer-Telephony Integration—The integration of services provided by a computer and a telephone (data adjuncts and communication systems).

Designer Reports

CentreVu Supervisor reports that are developed by Lucent associates and generally sold to customers. ICC-specific Supervisor reports are specially tagged to appear and run even if the Report Designer feature is not purchased.

DNIS Dialed Number Identification Service—An ACD capability that enables calls to be routed based on the number dialed by the caller.

DS1 Digital Signal, level 1—A 1.544Mbps digital circuit, generally split into 24 64Kbps channels (aka trunks), with 8Kbps reserved for signaling.

DSP Digital Signal Processor—A high-speed chip (specialized microprocessor) that is customized for specific applications such as voice / video encoding / decoding.

EAS Expert Agent Selection—A *DEFINITY*® ECS feature that provides a group of capabilities, including assigning skills to VDNs and agents. This is a skills-based form of call routing.

ECMA European Computer Manufacturers Association--An organization devoted to international standards for the computer manufacturing industry.

ECS Enterprise Communications Server—A *DEFINITY* switch providing features and capabilities specially designed to enhance call center operations.

EPN Expansion Port Network—A *DEFINITY* ECS cabinet that holds *DEFINITY* ECS circuit packs. This cabinet may be attached to the PPN (Processor Port Network, the cabinet that houses the switch processing element) via fiber or via DS1.

Escorted Browsing

The ability for one party's Internet browser session to cause another's browsing session to display the same information that is currently being viewed (also known as "URL sharing").

ethernet

An industry standard, high-speed data network protocol commonly used in a LAN environment.

firewall

A network node set up as a boundary to prevent traffic on one segment from crossing over to another segment based on a set of administered rules. Firewalls are used to improve network traffic as well as for security purposes. A firewall may be implemented in a router or it may be a device specialized for such purposes.

hacker

A person who tries to gain unauthorized entrance into a corporate network for the purpose of theft, malicious destruction, and/or amusement. A hacker may try to gain access to computer systems by electronic or brute force means.

HTTP

HyperText Transport Protocol—The client/server protocol used to connect to servers on the World Wide Web. Addresses of Web sites begin with an "http://" prefix.

Hunt Group

A group of trunks/agents selected to work together to provide specific routing of special purpose calls.

ICC Internet Call Center—An offer that provides a caller with the ability to communicate with an agent over the Internet. Communications can take place via Text Chat, Internet telephony, PSTN Callback, and / or by collaboratively browsing the Web.

ICMS Call Management System for Internet—The software added to CMS to support the gathering and reporting of ICC-specific statistics.

IIS Internet Information Services—A *Microsoft*[a] software package that runs on a *Microsoft NT*[b] server and allows it to perform Web server functionality, among other services.

Internet telephony The capability to communicate verbally across the Internet. Also known as Voice On the Net (VON) and Voice Over Internet Protocol (VOIP).

IP Internet Protocol—The underlying protocol used to pass data from one Internet host to another.

ISDN Integrated Services Digital Network—International telecommunications standard for transmitting voice, video, and data over a digital communications line.

ISP Internet Service Provider—A business that members subscribe to in order to gain access to the Internet (examples include AT&T WorldNet, America On-Line, NetCom, and Compuserv).

ITG Internet Telephony Gateway—The server providing the connection between the *DEFINITY* ECS and the Internet for the purpose of converting packetized voice to circuit-switched voice and vice versa.

***Java*[c]** A cross-platform programming language developed by Sun Microsystems.

***Java* Server** Platform from which the ICC *Java* applets are served and where the *Java* call control code executes. The *Java* server also proxies data between the Agent and Caller Control Windows.

LAN Local Area Network—A short-range data communication network linking computers and peripherals, such as printers. Ethernet is a common LAN protocol.

MACS Multimedia Applications Customer Support—A group of engineers within Lucent Technologies who perform pre-sale, installation, and post-sale escalated support for the ICC and MMCX (MultiMedia Communications eXchange).

NCG Network Consulting Group—A Professional Services group within Lucent Technologies composed of data engineers who provide data networking consulting services, including firewall provisioning, configuration, and maintenance.

NIC Network Interface Card—A circuit board inserted into a computer to allow communication with other systems on a network or access to a network.

packet-switched network — A network that divides messages into smaller packets, each with its own identifying and routing information. Packets travel to their destinations by a variety of routes. For data transmissions, a packet-switched network does not dedicate a channel for the duration of a call like a circuit-switched network. Instead, it queues packets and sends them on a standby basis as channel capacity becomes available. The Internet is an example of a packet-switched network.

PBX — Private Branch eXchange—A customer premises telephone-switching system that interconnects telephone extensions to each other as well as to the outside telephone network.

ping — Software that tests data connectivity to a remote system.

PRI — Primary Rate Interface—An ISDN standard interface which specifies B and D channels for T1 and E1 trunks.

PSTN — Public Switched Telephone Network—The traditional medium for telephone communications.

RTDBM — Real-Time Database Manager—The real-time data manager for *CentreVu* CMS.

TCP — Transmission Control Protocol—A protocol that enables different computer hardware and operating systems (such as PCs, Apple computers, *UNIX*[d] workstations, and mainframes) to communicate.

Telephony Server — *PassageWay*® Telephony Services server.

TSAPI Telephony Services Application Programming Interface—A telephony programming interface based on the international CSTA standard. TSAPI is designed to interface a PBX with a server to provide interoperability between PCs and telephone equipment.

UDP User Datagram Protocol—A TCP/IP protocol used to transmit data on data networks; commonly used to transmit Internet telephony voice packets.

URL Uniform Resource Locator—Address used to locate information on the World Wide Web.

VDN Vector Directory Number—A switch extension that provides a software link between trunk groups and vectors, enabling incoming ACD calls to be processed by specified vectors.

VOA VDN of Origin Announcement—An identifying message sent by *DEFINITY* ECS to an agent about the source of an incoming call so that the agent knows how to answer the call.

voice terminal Another term for a telephone.

WAN Wide Area Network—A network usually connecting LANs (local area networks).

the Web Shortened term for the World Wide Web, the body of information available on the Internet. Also called WWW.

Web Pop — A feature that automatically displays Web pages to the caller and/or agent based on call events (for example, call queued, call answered, and so on).

work mode — One of several different states an agent can be in while logged into a call center. Work modes include Auto-In, Manual-In, Auxiliary, and After Call Work (ACW).

WWW — World Wide Web—The body of information available on the Internet. Also referred to as "the Web."

a. Microsoft is a registered trademark of Microsoft Corp.
b. NT is a registered trademark of Microsoft Corp.
c. Java is a registered trademark of Sun Microsystems, Inc.
d. UNIX is a registered trademark licensed exclusively through X/Open Company, Ltd.

IN

Index

D

E

F

H

I

J

L

N

P

R

S

T

V

W