

CSTA Gatekeeper

Installation and Configuration Guide

Order Number: 05-1417-002

Software/Version: CSTA Gatekeeper Version 1.1

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

This guide as well as the software described in it is furnished under license and may only be used or copied in accordance with the terms of the license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without express written consent of Intel Corporation.

Copyright © 2002 Intel Corporation.

Dialogic, DM3, Intel, and IPLink are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Acrobat and Adobe are trademarks of Adobe Systems, Incorporated.

†Other names and brands may be claimed as the property of others.

Publication date: October, 2002

For **Sales Offices** and other contact information, visit our website at <http://www.intel.com>.

Contents

About This Manual	vii
--------------------------------	-----

1 Introduction

1.1	What is the CSTA Gatekeeper?	1-1
1.1.1	CSTA Gatekeeper in an IP Network	1-1
1.2	CSTA Gatekeeper and H.323 Services	1-2
1.3	Using the CSTA Gatekeeper with a CTC Server	1-4
1.3.1	Setting Up a Combined Telephony Network	1-5
1.4	Multiple Gatekeepers	1-6
1.4.1	Remote Gatekeepers	1-6
1.4.2	Alternate Gatekeepers	1-7
1.5	Supported CSTA Services	1-9

2 Installation and Configuration

2.1	Overview	2-1
2.2	H.323 IP Telephony Environment	2-1
2.3	Requirements	2-2
2.4	Pre-Installation Items	2-2
2.4.1	Attaching the Hardware License Key	2-3
2.4.1.1	Types of Hardware Key	2-3
2.4.1.2	Attaching the Hardware Key	2-3
2.5	Installing the CSTA Gatekeeper	2-4
2.6	Reading the Release Notes	2-5
2.7	Reading the Online Documentation	2-5
2.8	Starting the CSTA Gatekeeper	2-6
2.9	Configuring the CSTA Gatekeeper	2-7
2.9.1	Starting the Configuration Program	2-7
2.9.1.1	CSTA Link State	2-8
2.9.1.2	Registered Endpoints	2-8
2.9.2	Getting Started: Setting Up a Basic Configuration	2-9
2.9.3	Displaying Current Settings and Configuring Optional Values	2-13
2.9.3.1	Displaying Current Settings	2-13
2.9.3.2	Configuring Optional Values	2-14
2.9.4	Configuring Alternate and Remote Gatekeepers	2-15
2.9.4.1	Alternate Gatekeepers	2-16

2.9.4.2	Remote Gatekeepers	2-17
2.9.5	Deleting and Resetting Configuration Parameters	2-19
2.10	Removing and Reinstalling the CSTA Gatekeeper	2-19
2.11	Event Logging.	2-20
2.11.1	Starting the Event Logging Application.	2-20
2.11.2	CSTA Gatekeeper Events	2-21

3 Configuring and Registering Endpoints

3.1	Configuring Endpoints	3-1
3.2	Format of Endpoint Aliases	3-1
3.2.1	IP Address	3-1
3.2.2	Domain Name.	3-2
3.2.3	E-mail Address	3-2
3.2.4	Telephone Number.	3-2
3.2.5	URL	3-2
3.2.6	Generic H.323 Identifier (H323Id).	3-3

A Additional Information for CTC Applications

A.1	Monitoring and Controlling URLs and E-mail Addresses	A-1
A.2	Endpoint Registration and Assigning Channels	A-1
A.3	Party Information (ANI, CLID, DNIS)	A-2
A.3.1	Party Information Returned in CSTA Events	A-2
A.3.2	Using CTC Private Data for Party Information	A-3
A.3.2.1	Private Data Fields.	A-4
A.4	Using CTC to Monitor Outbound Calls on a Gateway	A-5
A.5	Using CTC to Monitor Inbound Calls on a Gateway.	A-6

Index

Figures

1-1	A CTC and IP Network	1-2
1-2	A CTC Network.	1-4
1-3	A Combined CTC and IP Telephony Network	1-5
1-4	Multiple Gatekeeper Network	1-8
2-1	NCCS Hardware License Keys	2-3
2-2	Configuration Program Example First Screen	2-7
2-3	Configuration Program Registered Endpoints Screen	2-9

Tables

1-1	Supported CSTA Services	1-10
1-2	Supported CSTA Events	1-11
2-1	Endpoint Configuration Settings	2-11
2-2	Parking Lot and Route Point Configuration Settings	2-12
2-3	Configuration Program Optional Current Settings	2-14
2-4	Alternate Gatekeeper Settings	2-17
2-5	Remote Gatekeeper Settings	2-18
2-6	CSTA Gatekeeper Events	2-21

About This Manual

This manual describes how to install and use the CSTA Gatekeeper. Designed for use with CT Connect, the CSTA Gatekeeper is an H.323 gatekeeper that implements ECMA CSTA (Computer Supported Telecommunications Applications) Phase II and provides the framework for third-party call control in an IP telephony network.

Audience

This manual is for anyone who wants to use CT Connect (CTC) applications in an IP telephony environment. It provides an introduction to the CSTA Gatekeeper and describes how to use the software tools to set up and manage the gatekeeper in conjunction with a CTC server.

This manual assumes that readers have a basic understanding of the concepts of IP telephony and International Telecommunication Union (ITU) Recommendation H.323 and H.450.x. It also assumes that readers are familiar with the CTC software.

The installation and configuration procedures require that users are familiar with installing and configuring network-based products.

Associated Documentation

CSTA Gatekeeper Documentation

In addition to this manual, the CSTA Gatekeeper documentation set includes:

- *CSTA Gatekeeper Management API Guide*—This manual provides detailed descriptions of the procedural routines you can use to create an application that configures and manages the CSTA Gatekeeper. Although a Configuration Program is included with CSTA Gatekeeper software (for details, see Chapter 2), you can use the management API to implement specific features by creating your own application. This manual is provided as a Portable Document File (PDF) only.

- *CSTA Gatekeeper Release Notes*—These online notes provide last-minute information about changes to the CSTA Gatekeeper software and documentation at the time of release. They are installed with the CSTA Gatekeeper software as a “readme.txt” file.

Both online documents are installed at the same time as the CSTA Gatekeeper software. For details, refer to Chapter 2.

CTC Documentation

For more information about CTC, refer to the documentation provided with your CTC software kit. Hard copy CT Connect manuals are provided with the kit and online versions can be installed at the same time as the CTC server software.

ITU Recommendation H.323 and H.450

For details of how to obtain Recommendation H.323 and H.450.x, refer to the ITU web site at <http://www.itu.int>.

CSTA Specification

For the CSTA Phase II specification, refer to standard ECMA-218 on the ECMA web site <http://www.ecma.ch>. ECMA is the international, Europe-based industry association for standardization of Information and Communication Technology (ICT) systems.

Product Web Site

For the latest information about Intel products, visit <http://www.intel.com>.

Terms and Definitions

The following terms are used throughout this manual:

Term	Definition
H.323	The H.323 series of recommendations from the ITU Telecommunication Standardization Sector (ITU-T).
H.450	The H.450.x series of recommendations from the ITU Telecommunication Standardization Sector (ITU-T).
CTC client	A supported system running the CTC API software.
CTC server	A supported system running the CTC server software.
Switch	The telephony switching device. For example, a Private Branch Exchange (PBX), Private Automatic Branch Exchange (PABX) or central office switch.

Conventions

The following conventions are used throughout this manual:

Convention	Meaning
<code>courier</code>	This typeface is used for code examples or interactive examples to indicate system input/output.
<i>drive:</i>	Italic (slanted) typeface indicates variable values, placeholders, and arguments.
<code>C:\></code>	The MS-DOS [†] command prompt. The actual prompt may vary depending on your current drive and default directory.

Introduction

1.1 What is the CSTA Gatekeeper?

The CSTA Gatekeeper is an H.323 gatekeeper that provides CTC applications with the framework for monitoring and making calls across an Internet Protocol (IP) network.

Recommendation H.323 is a standard developed by the Telecommunication Standardization Sector of the ITU describing components and services for real-time multimedia communication over packet-switched networks, such as, IP networks.

An H.323 gatekeeper provides some control in an H.323 network where Quality of Service (QoS) problems can occur. The QoS across IP networks is not guaranteed and typically requires additional management and administration. H.323 gatekeepers perform this additional management (address translation, admissions control, bandwidth and zone management), and other functions such as call-control signaling.

The CSTA Gatekeeper supports both the basic call-control features of H.323 and its supplementary services. CTC applications that support the Computer Supported Telephony Applications (CSTA) protocol can use the CSTA Gatekeeper for third-party call control in an IP network in the same way that they would control calls in a circuit-switched network. For example, an application could seamlessly make a call from either a CSTA-enabled switch or an H.323 component.

1.1.1 CSTA Gatekeeper in an IP Network

Figure 1–1 shows a telephony network that includes the CSTA Gatekeeper, CTC and H.323 components. In this example:

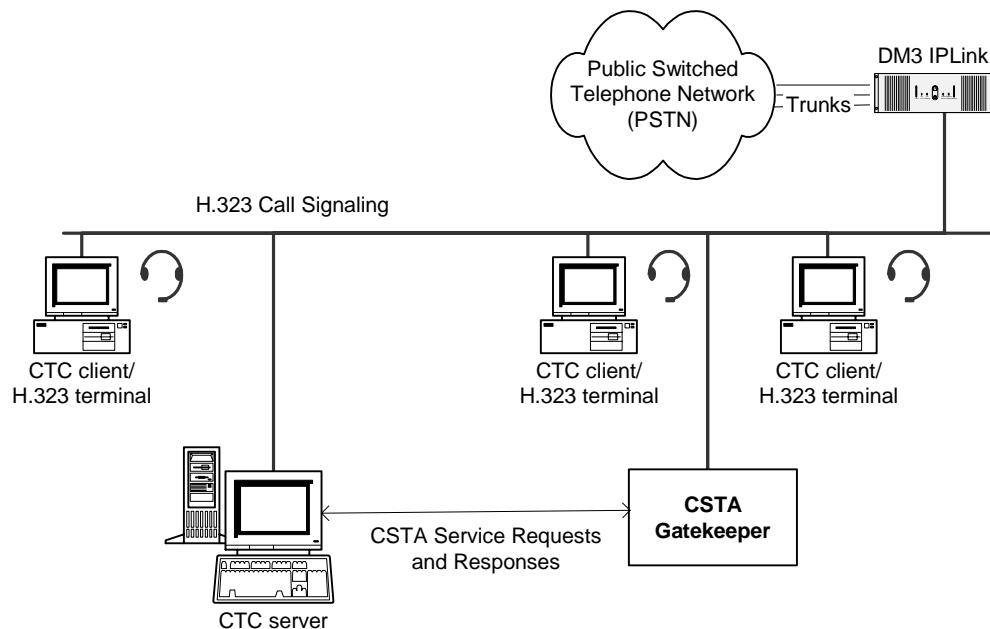
- Each CTC client also acts as an H.323 **terminal**, running H.323 software that provides real-time, two-way communication with other H.323 components. A terminal must support voice communication and can optionally support data and video. Typically, a terminal is an application running on a PC, for example, the Intel Internet Phone or Microsoft[†]

Netmeeting[†].

- An H.323 **gateway** handles the trunks to the Public Switched Telephone Network (PSTN). In Figure 1–1, a DM3™ IPLink™ is the H.323 gateway that provides the interface between the packet-switched network and the circuit-switched network. This enables calls in an IP network to connect to a PSTN.

Collectively, terminals, gateways and other H.323 components are defined as **endpoints** in Recommendation H.323.

Figure 1–1 A CTC and IP Network



1.2 CSTA Gatekeeper and H.323 Services

The CSTA Gatekeeper performs all of the required services defined by H.323 for gatekeepers:

- **Address Translation**

H.323 gatekeepers are required to translate alias addresses to transport addresses. This is particularly important when a PC on the IP network places

a call to a phone on the circuit-switched network. It is also used to identify the gateways in the network.

- **Admissions Control**

If a gatekeeper is present in an H.323 network, all terminals, gateways, and other endpoints must use their services. Endpoints use the Registration/Admission/Status (RAS) protocol to request registration with a gatekeeper. The CSTA Gatekeeper can be configured so that it will accept registration from only certain endpoints within the network.

- **Bandwidth Control**

The CSTA Gatekeeper supports RAS bandwidth messages used to provide bandwidth access or management.

- **Zone Management**

H.323 gatekeepers provide services to endpoints within a specific zone. The zone can be a geographic or logical group of endpoints. The CSTA Gatekeeper can be configured to manage endpoints within a specific domain zone, range of IP addresses, or range of E.164 aliases (telephone numbers).

In addition, the CSTA Gatekeeper performs the following optional services:

- **Call Control Signaling**

The CSTA Gatekeeper processes all call signaling messages between endpoints registered with the gatekeeper. Call signaling messages used in the H.323 environment are defined in ITU-T Recommendation Q.931.

The CSTA Gatekeeper processes and maps H.323 call signaling (Q.931) and H.450 messages to CSTA event messages. When it receives CSTA service request messages it maps them to the H.323 call signaling and H.450 supplementary services messages used to control H.323 endpoints.

- **Call Authorization**

The CSTA Gatekeeper can be configured so that it will authorize or reject calls. For example, if the configured maximum bandwidth has been reached, it can reject the next call requesting additional bandwidth.

- **Bandwidth Management**

The CSTA Gatekeeper can be configured so that no additional bandwidth is available when the total maximum bandwidth has been reached.

All of the management service options available with the CSTA Gatekeeper are set using its Configuration Program (see Chapter 2) or a management

application written using the CSTA Gatekeeper management API (see the *CSTA Gatekeeper Management API Guide*).

1.3 Using the CSTA Gatekeeper with a CTC Server

Figure 1–2 shows a typical CTC network that includes CTC clients, a CTC server, and a CSTA PBX.

Figure 1–2 A CTC Network

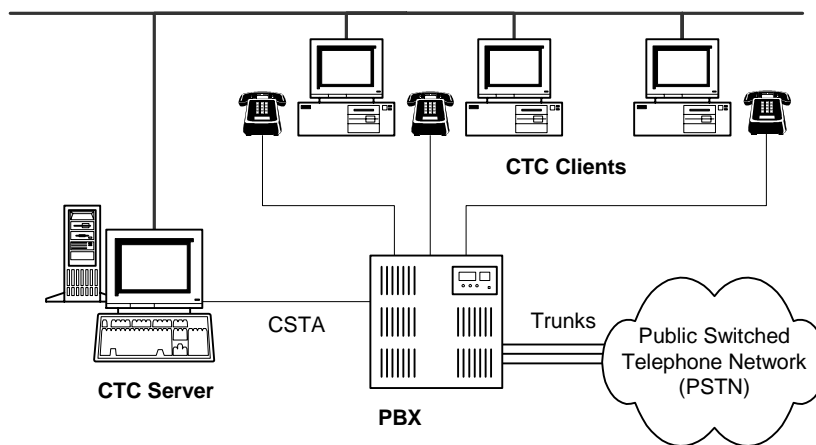


Figure 1–3 shows a similar network with some CTC clients registered as H.323 endpoints. Two CSTA communications links are configured on the CTC server: one to the PBX and another to the CSTA Gatekeeper.

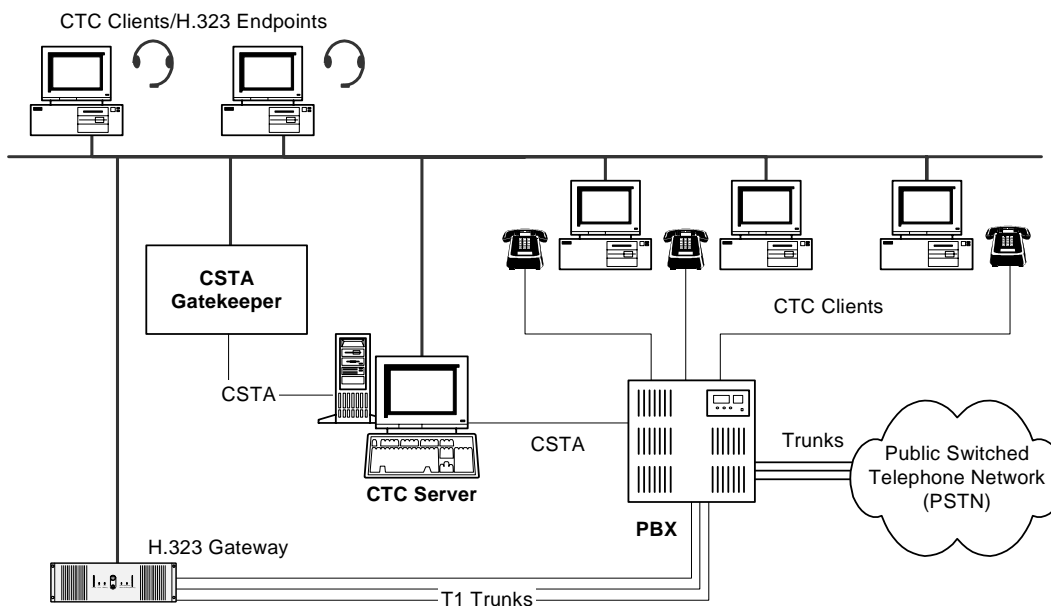
In the network shown in Figure 1–3:

- The same CTC application is running on both sets of clients. However, when an agent uses the application to make a call from the CTC client/H.323 endpoint, the call can be routed through the IP telephony network to the PBX.

The attendants at these clients do not require standard telephones connected to the PBX. With sound cards installed on their PCs, they can use headsets connected to their systems to speak to callers.

- The CTC application can monitor other registered H.323 endpoints within the network. For example, a CSTA Gateway can have multiple E.164 aliases (for example, numbers 2006 to 2010) and an application running on the CTC server could monitor the E.164 aliases.

Figure 1–3 A Combined CTC and IP Telephony Network



1.3.1 Setting Up a Combined Telephony Network

When you set up a combined circuit-switched and IP telephony network with CTC, you must configure the CTC software, CSTA Gatekeeper software and H.323 client software to communicate across the network.

To set up the telephony network shown in Figure 1–3, you must complete the following:

1. Install and start the CTC server, CTC clients, and CSTA Gatekeeper (along with other components of the telephony network, such as the H.323 gateway). The CSTA Gatekeeper software is installed on the CTC server.
2. On the CTC server, use the CTC Configuration Program to configure one link to the CSTA Gatekeeper and another link to the PBX. For details of the Configuration Program, refer to the *CT Connect Installation and Configuration Guide*.
3. Configure the H.323 terminals with E.164 aliases so that they can register with the CSTA Gatekeeper.

Typically, registration takes place automatically when you start the H.323 client software on the terminals. However, you must set up the CSTA Gatekeeper before you start the H.323 client software so that the CSTA Gatekeeper recognizes which registration requests to accept. For more information about starting the H.323 client software, refer to your H.323 client software documentation.

4. Define which H.323 endpoints you want to manage with the CSTA Gatekeeper. You can either use the CSTA Gatekeeper Configuration Program (for details, see Chapter 2) or your own CSTA Gatekeeper management application (for details, see the *CSTA Gatekeeper Management API Guide*).
5. From your CTC application, assign a channel to the E.164 alias at each H.323 terminal/CTC client.

1.4 Multiple Gatekeepers

You may want to use more than one CSTA Gatekeeper in your network to reduce the load on a single gatekeeper or to provide backup should the primary CSTA Gatekeeper become unavailable. The CSTA Gatekeeper software supports up to three CSTA Gatekeepers in the same IP network.

To reduce the load on a single CSTA gatekeeper, you can configure the software to support one or more **remote gatekeepers**. To provide backup, you include one or more **alternate gatekeepers**. These gatekeepers are described in Sections 1.4.1 and 1.4.2 respectively.

1.4.1 Remote Gatekeepers

A remote gatekeeper is a gatekeeper that you include in the same IP network as the CSTA Gatekeeper to share call loading. The CSTA Gatekeeper handles all calls for its own registered endpoints. When it receives a call that it cannot resolve, it polls remote gatekeepers for an alias match in order to distribute the call to its correct destination.

You identify the set of aliases associated with a remote gatekeeper when you configure the CSTA Gatekeeper software. For example, you can specify that a remote gatekeeper receives calls for all E.164 aliases that begin with 72. When the CSTA Gatekeeper receives a call for E.164 alias 7234 and it cannot find a match in its list of registered endpoints, it queries the remote gatekeeper for a match. If the alias 7234 is registered with the remote gatekeeper, the remote gatekeeper provides a positive acknowledgement to the CSTA Gatekeeper and the CSTA Gatekeeper passes on the call.

You can set up a number of remote gatekeepers in this way, each handling calls

with a different prefix. The CSTA Gatekeeper uses the prefix to determine whether a remote gatekeeper has a possible match and does not poll those that could not resolve the call. For example, for a call to 7234, it will not poll a remote gatekeeper with prefix 78.

If you want the CSTA Gatekeeper to poll a remote gatekeeper for all calls that the CSTA Gatekeeper cannot resolve, you specify a blank prefix. Section 2.9.4 provides more information about configuring the CSTA Gatekeeper for remote gatekeeper support.

Remote Gatekeeper Example: Figure 1–4

Figure 1–4 shows a network that includes two CSTA Gatekeepers (A and B).

H.323 endpoints that are configured to register with a specific CSTA Gatekeeper to balance the load. Endpoints with an alias prefix of 71 register with A, endpoints with the alias prefix 72 register with B.

Each CSTA gatekeeper has the other configured as a remote gatekeeper, so that if A receives a call with the prefix 72, it passes the call to B. If B receives a call with the prefix 71, it passes the call to A.

1.4.2 Alternate Gatekeepers

An alternate gatekeeper in the same IP network as the CSTA Gatekeeper provides endpoints with a backup point of registration. If registration with the CSTA Gatekeeper fails, the endpoint can continue to make and receive calls over the IP network by registering with a different gatekeeper.

An endpoint's registration could fail for one of the following reasons:

- The CSTA Gatekeeper becomes unavailable
- The maximum number of registrations configured on the CSTA Gatekeeper has been reached

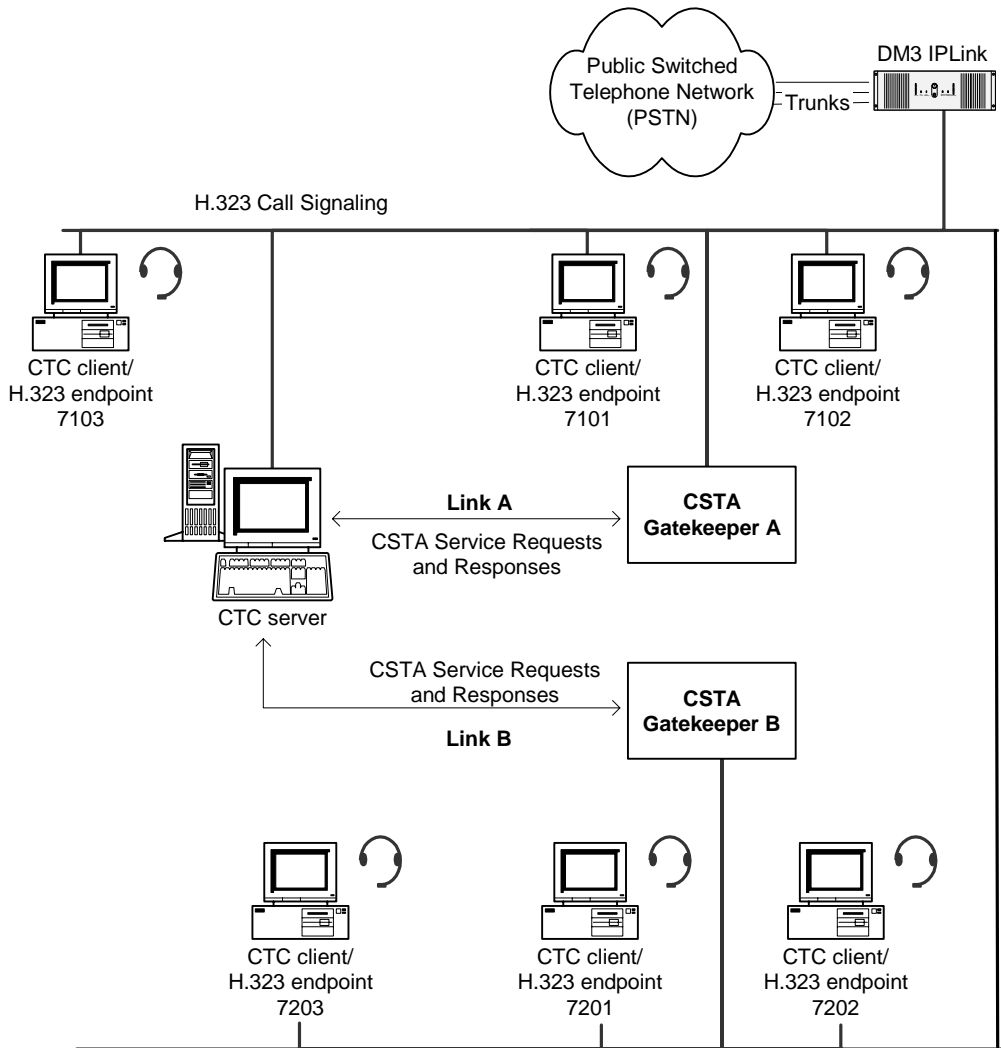
When an endpoint sends a registration request to the CSTA Gatekeeper, the CSTA Gatekeeper automatically sends details of the alternate gatekeepers(s) in its response to the endpoint. The endpoint can then store these details locally (for example, in the Windows registry) and can use the information to locate an alternative gatekeeper if its request is rejected.

To provide an endpoint with details of alternate gatekeepers, the CSTA Gatekeeper must be running when the endpoint sends its initial registration request so that the CSTA Gatekeeper can send a response.

If the CSTA Gatekeeper service is stopped, the CSTA Gatekeeper unregisters all endpoints and the endpoint must use another gatekeeper to continue to make

and receive calls across the IP network.

Figure 1-4 Multiple Gatekeeper Network



Alternate Gatekeeper Example: Figure 1–4

In Figure 1–4, the CSTA Gatekeepers and CTC are configured as follows:

- CSTA Gatekeeper B is set up as an alternate gatekeeper to CSTA Gatekeeper A.
- The CTC server is configured with two links, Link A and Link B.
- All CTC clients in Figure 1–4 have channels assigned to their associated devices over both links. For example, the CTC client/H.323 endpoint at 7101 has a channel assigned to 7101 over Link A and another channel assigned to 7101 over Link B. This ensures that if one link fails, then the CTC client can continue to monitor calls, make and receive calls.
- The CTC client/H.323 endpoint at 7101 registers with CSTA Gatekeeper A.

If CSTA Gatekeeper A is stopped:

1. The CSTA Gatekeeper unregisters all endpoints and CTC sends a `ctcK_OutOfService` event to the CTC application.
2. The endpoints use stored details of alternate gatekeepers to locate an alternative gatekeeper and re-register with CSTA Gatekeeper B.
3. CTC sends a `ctcK_BackInService` event to the CTC application.

1.5 Supported CSTA Services

Table 1–1 shows the set of CSTA services and Table 1–2 shows the set of CSTA events that the CSTA Gatekeeper supports. These services and events provide features you require for monitoring and controlling calls in an H.323 IP telephony environment.

Tables 1–1 and 1–2 also show which features are supported for a telephony device that has a directory number (DN) and which features are supported for a route point. For more information about DNs and route points, refer to your CTC programming documentation.

In Tables 1–1 and 1–2, DN and route points are H.323 endpoints managed by the CSTA Gatekeeper.

Table 1–1 Supported CSTA Services

CSTA Service	DN	Route Point
Associate Data	Supported	Supported
Clear Connection	Supported	Supported
Conference Call ¹	Supported	Not supported
Consultation Call ¹	Supported	Not supported
Deflect Call	Supported	Not supported
Directed Call Pickup ²	Supported	Not supported
Hold Call ¹	Supported	Not supported
Make Call	Supported	Not supported
Make Predictive Call	Supported	Not supported
Monitor Start	Supported	Supported
Monitor Stop	Supported	Supported
Park Call ²	Supported	Not supported
Query Device	Supported for: Call Forward, Device Information, Do-Not-Disturb, Message Waiting	Supported for: Device Information, Route Enable
Retrieve Call ¹	Supported	Not supported
Route Request	Not supported	Supported
Route Select	Not supported	Supported
Set Feature	Supported for: Call Forward Immediate, Do-Not-Disturb, Message Waiting	Supported for: Route Enable
Single Step Conference Call ¹	Supported	Not supported
Single Step Transfer Call ¹	Supported	Not supported
Snapshot Device	Supported	Supported

Table 1–1 Supported CSTA Services (Continued)

CSTA Service	DN	Route Point
System Status	Not applicable	Not applicable
Transfer Call ¹	Supported	Not supported

¹This feature is initiated using either a proprietary mechanism or enhanced functionality at the endpoint. For example, support for two concurrent calls or, for conference features, support for audio-mixing. For more information about support for these features, refer to your H.323 client documentation.

²To support this feature, the endpoint must support the H.450 Park and Pickup supplementary service.

Table 1–2 Supported CSTA Events

CSTA Call Event	DN	Route Point
Conferenced	Supported	Not supported
Connection Cleared	Supported	Supported
Delivered	Supported	Supported
Diverted	Supported	Supported
Established	Supported	Not supported
Failed	Supported	Supported
Network Reached	Not supported	Not supported
Originated	Supported	Not supported
Queued	Supported	Supported
Service Initiated	Supported	Not supported
Transferred	Supported	Not supported

Installation and Configuration

2.1 Overview

The following table provides an overview of the contents of this chapter. To install and configure the CSTA Gatekeeper, refer to Sections 2.3 to 2.9 in turn.

For details of...	See Section...
H.323 IP Telephony Environment	2.2
Requirements	2.3
Pre-Installation Items	2.4
Installing the CSTA Gatekeeper	2.5
Reading the Release Notes	2.6
Reading the Online Documentation	2.7
Starting the CSTA Gatekeeper	2.8
Configuring the CSTA Gatekeeper	2.9
Removing and Reinstalling the CSTA Gatekeeper	2.10
Event Logging	2.11

2.2 H.323 IP Telephony Environment

The CSTA Gatekeeper can be installed in any H.323 IP telephony environment that contains one or more H.323 endpoints.

For an overview of the components in an H.323 network, refer to Chapter 1.

2.3 Requirements

To install and run the CSTA Gatekeeper, you require:

- A PC with a parallel port running one of the following:
 - Windows NT (Windows NT Workstation or Windows NT Server) Version 4.0 (SP6)
 - Windows 2000 (any version)
 - Windows XP (any version)

The parallel port is required so that you can attach the NCCS hardware license key. If the key is not attached, the CSTA Gatekeeper software will install but it will not run. For details, see Section 2.4.1.

- A CTC server running CTC V5.0 or later and in the same network as the CSTA Gatekeeper system. For full details of CTC server requirements, refer to the *CT Connect Installation and Configuration Guide*. Note that you can install the CSTA Gatekeeper on a CTC server that satisfies the CSTA Gatekeeper installation requirements.
- At least 10 Mbytes of free disk space during and after installation.

Depending on the number of applications running on the system you use for the installation, you may also require additional resources such as memory.

- A network adapter card installed on the system. This is required for:
 - A TCP/IP connection used for the CSTA link between the CSTA Gatekeeper and the CTC server. The installation procedure prompts you for details of the TCP/IP port you will use for this connection. If you have more than one network adapter card installed, you must also specify the address of the card during the installation procedure.
 - The TCP/IP connections between the CSTA Gatekeeper and H.323 endpoints. Communication is set up using standard settings for H.323 communication and the installation procedure does not need to prompt you for these.

For details of compatible network adapter cards, refer to the *Hardware Compatibility Guide* for your Windows operating system.

2.4 Pre-Installation Items

Before you start the installation:

- Attach the hardware key to the parallel printer port on your system. For

details of how to do this, see Section 2.4.1.

- Check that you have administrator privileges on the target Windows NT or Windows 2000 system.
- Decide where to install the CSTA Gatekeeper on the target system. The default is: C:\Program Files\Dialogic\CSTA Gatekeeper.

2.4.1 Attaching the Hardware License Key

The CSTA Gatekeeper uses a hardware key to ensure that your system is licensed for running the CSTA Gatekeeper software. A hardware license key is included in the kit along with the CD-ROM and documentation and is labelled *NCCS* which stands for Network Call Control Software.

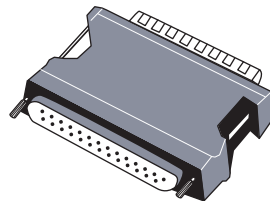
2.4.1.1 Types of Hardware Key

You can order one of the following types of hardware key with the CSTA Gatekeeper software:

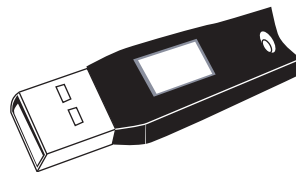
- A hardware key for a parallel printer port
- A hardware key for a USB port

Figure 2–1 shows both types of hardware license key.

Figure 2–1 NCCS Hardware License Keys



Parallel Port license key



USB license key

2.4.1.2 Attaching the Hardware Key

You need to do one of the following, depending on the type of hardware key in your kit:

- For a parallel port license key, attach the key to the parallel printer port. If you already have a hardware license key on the same port (for example, for CT Connect), attach the hardware key to the back of the other key. The key must be present when the software starts, so Intel recommends that you

attach it now, before you install the CSTA Gatekeeper software.

- For a USB license key, attach the key to the USB port. The hardware key must be present before you start the CSTA Gatekeeper software, but Intel recommends that you attach the USB key after installing the CSTA Gatekeeper software. If you attach the USB key before you install the CSTA Gatekeeper software, your system may prompt you for a software driver for the key. If this occurs, cancel the prompt and continue with the CSTA Gatekeeper software installation.

Whether you are using a parallel printer port key or a USB license key, the key should remain attached to the port. If the key is missing, the software will start but it will not run and an event is logged to your system. For details of event logging, see Section 2.11.

2.5 Installing the CSTA Gatekeeper

Complete the following:

1. Start the target system and log in to an account with administrator privileges.
2. Insert the *Network Call Control Software V1.1* CD-ROM into the CD-ROM drive.
3. Select **Run...** from the **Start** menu.
4. Enter *D:\CSTA Gatekeeper\Setup* in the **Open:** text box, where *D* is the CD-ROM drive letter.
5. Click on the **OK** button and follow the on-screen prompts.

The procedure installs the CSTA Gatekeeper software and prompts you for

the following:

Item	Description
Address	The IP address for the network adapter card. Specify an address in this field if there is more than one adapter card installed on the system and you need to identify the card used for the connection to the CSTA Gatekeeper. This field is optional.
Port	The TCP/IP port number that the CSTA Gatekeeper will use to listen for requests from the CTC server. The default offered by the installation procedure is 8888. Make sure that the TCP/IP port number you specify is not used by other application software on your PC. The CTC server must have exclusive access to the port to set up communication with the CSTA Gatekeeper. This field is mandatory.

Paths File

During the CSTA Gatekeeper installation, the file `CTCGK_MGMT.BAT` is copied to your system. This file contains paths for the CSTA Gatekeeper library and definitions files that you can use when you compile and link a management application. For details of `CTCGK_MGMT.BAT`, refer to the *CSTA Gatekeeper Management API Guide*.

2.6 Reading the Release Notes

Intel recommends that you read the release notes now, immediately after installing the software. They may contain important information about how to set up and use the CSTA Gatekeeper.

The release notes are a `readme.txt` file which you can display or print. This file is copied to the drive and directory chosen for the installation. For example:

```
C:\Program Files\Dialogic\CSTA Gatekeeper\readme.txt
```

2.7 Reading the Online Documentation

This guide and the *CSTA Gatekeeper Management API Guide* are copied as PDF files to a `\Docs` folder in the drive and location chosen for the installation. For example:

```
C:\Program Files\Dialogic\CSTA Gatekeeper\Docs\
```

You use Adobe™ Acrobat™ Reader to open the PDF documents. You can install

Acrobat Reader in one of the following ways:

- Download the latest version of Acrobat Reader from the website:
<http://www.adobe.com/>
- Install Acrobat Reader from the *Network Call Control Software V1.1* CD-ROM.

To install from the CD-ROM:

1. Insert the CD-ROM into the CD-ROM drive
2. Open the file:

`D:\Acrobat Reader\ACRD4ENU.EXE`

This starts the installation procedure for Acrobat Reader.

2.8 Starting the CSTA Gatekeeper

When the software is successfully copied to your system, the installation procedure asks if you want to reboot your system now or later. The CSTA Gatekeeper is automatically started when you reboot your system.

Once the CSTA Gatekeeper is running, you can stop and start the software manually using the Services program in Control Panel. For more information about starting and stopping services, refer to the Services program online help.

When the CSTA Gatekeeper starts, it logs a `cgkStarted` event in the Windows event log. For more information about CSTA Gatekeeper event logging, see Section 2.11.

2.9 Configuring the CSTA Gatekeeper

To configure the CSTA Gatekeeper so that it controls and monitors H.323 requests and calls made across the IP telephony network, you run the CSTA Gatekeeper Configuration Program.

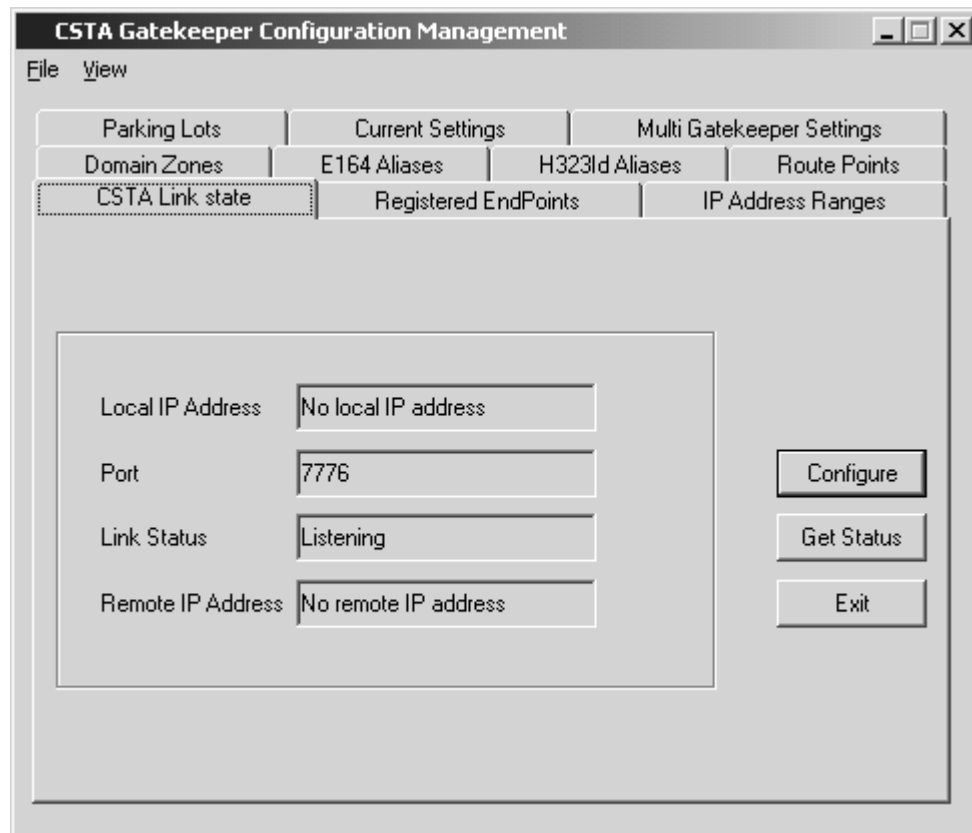
2.9.1 Starting the Configuration Program

From the **Start** menu, select:

Programs → **CSTA Gatekeeper** → **Configuration Program**

Figure 2–2 shows an example of the initial screen displayed.

Figure 2–2 Configuration Program Example First Screen



2.9.1.1 CSTA Link State

The **CSTA Link State** tab shows the port number and any local IP address that you supplied during the installation procedure.

If the displayed settings are correct, follow the procedure in Section 2.9.2 to configure endpoints that communicate with the CSTA Gatekeeper.

If you want to change the **CSTA Link State** settings, click on the **Configure** button.

CAUTION:

If you change the link settings, you must reconfigure the CTC server so that it uses the same port number and local IP address for the link to the CSTA Gatekeeper. If a link is up when you change these settings, it is automatically shut down. For details of how to configure the CTC server, see the *CT Connect Installation and Configuration Guide*.

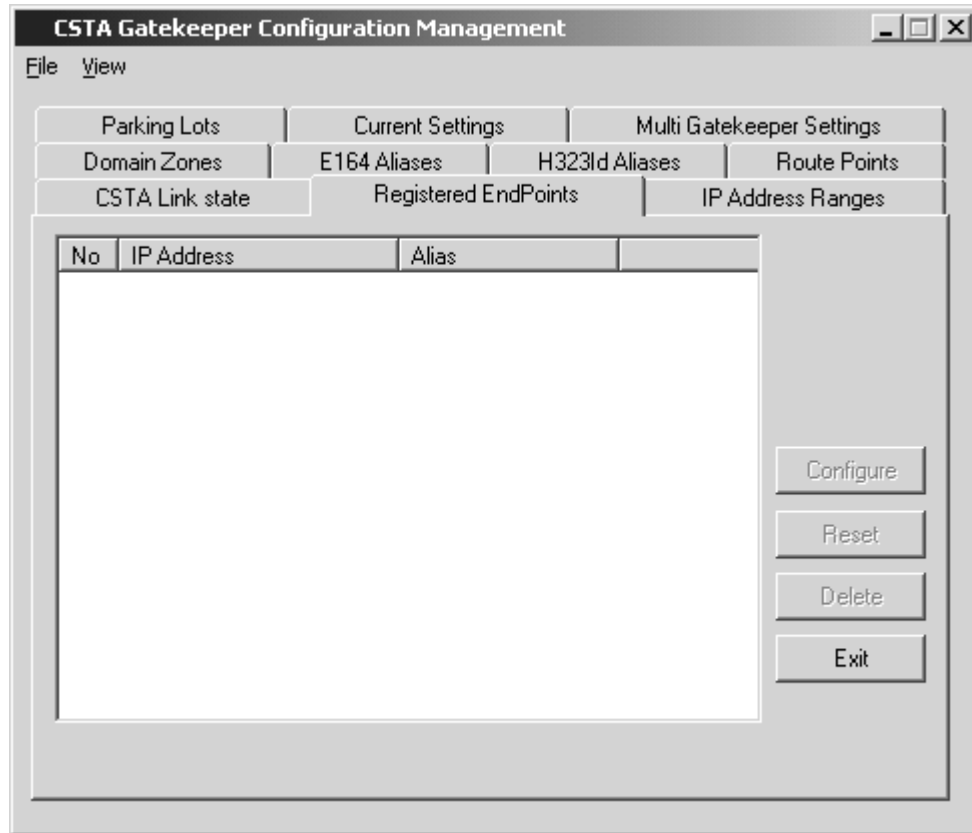
The CSTA Gatekeeper Configuration Program startup screen also shows the status of the link between the CTC server and the CSTA Gatekeeper. To refresh the link status, click on the **Get Status** button.

2.9.1.2 Registered Endpoints

The **Registered Endpoints** tab displays a list of IP addresses and corresponding aliases for endpoints that have been configured and registered with the CSTA Gatekeeper. The list is useful for monitoring how many endpoints are registered with the CSTA Gatekeeper.

When you first start up the Configuration Program, no endpoints are listed. Figure 2–3 shows an example of the **Registered Endpoint** tab.

Figure 2–3 Configuration Program Registered Endpoints Screen



Before an endpoint is listed as a registered endpoint:

1. You must configure the endpoint by providing its details in the Configuration Program. Follow the procedure in Section 2.9.2.
2. The endpoint must register with the CSTA Gatekeeper. Registration usually takes place when the H.323 client software is started at that endpoint.

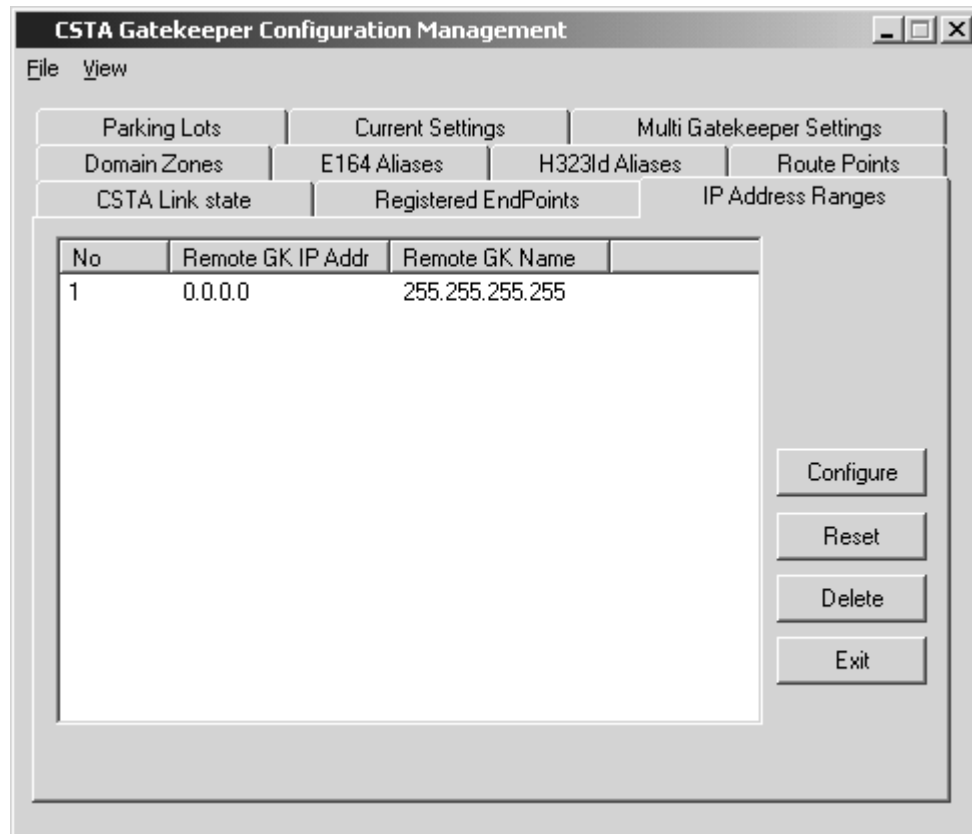
2.9.2 Getting Started: Setting Up a Basic Configuration

A basic configuration requires you to define the area(s) of IP network you want to manage with the CSTA Gatekeeper.

Complete the following:

1. Select the tab for **IP Address Ranges, Domain Zones, E164 Aliases,** or

H323Id Aliases. For example:



2. Click on the **Configure** button, and specify the information shown in Table 2-1.

You can set up a combination of IP address ranges, domain zones, E.164 aliases and H.323 IDs that you want the CSTA Gatekeeper to manage, but you must provide information for at least one range, zone, alias, or H.323 ID.

Table 2–1 Endpoint Configuration Settings

Tab	Description
IP address Ranges	IP address ranges that are managed by the CSTA Gatekeeper. The start address, and all addresses up to, and including, the end address will be managed by the CSTA Gatekeeper. For example: Lower IP Address: 20.234.22.00 Higher IP Address: 20.234.24.00
Domain Zones	Domain zones managed by the CSTA Gatekeeper. The domain zone identifies a group of endpoints by their domain name. For example: com.dialogic.zone1
E164 Aliases	E.164 aliases managed by the CSTA Gatekeeper. The E.164 alias is an alternative address for an endpoint such as a telephone. A typical example is an E.164 quick-dial telephone number. For example: 2253
H323Id Aliases	H.323 ID aliases managed by the CSTA Gatekeeper. An H.323 ID alias is an alternative address for an endpoint that is not defined as another type of alias. For example: agent123

For details of the formats you must use for aliases, refer to Chapter 3.

When you have entered the information, the Configuration Program displays details of your settings, showing the area(s) of IP network you want to manage.

3. You can optionally configure an E.164 alias as a parking lot and/or route point. Refer to Table 2–2 for details.

Table 2–2 Parking Lot and Route Point Configuration Settings

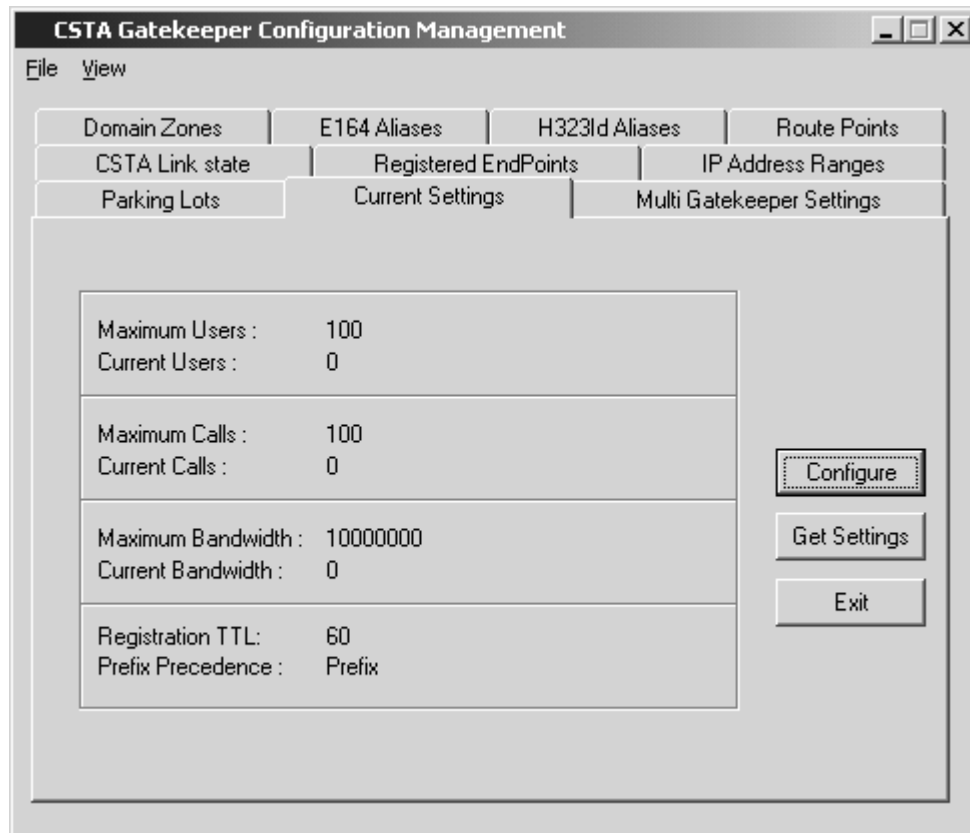
Tab	Description
Parking Lots	<p data-bbox="607 474 1362 558">Lists all endpoints configured as parking lots with the CSTA Gatekeeper. A parking lot is a special class of endpoint used to hold calls for later pickup by another endpoint.</p> <p data-bbox="607 569 1362 653">To configure an endpoint as a parking lot, the endpoint must support parking lot services and register with the CSTA Gatekeeper using an E.164 alias.</p> <p data-bbox="607 663 862 690">To set up a parking lot:</p> <ol data-bbox="607 709 1362 856" style="list-style-type: none"><li data-bbox="607 709 1362 772">1. Configure the endpoint's E.164 alias by selecting the E164 Aliases tab (see step 2 and Table 2–1).<li data-bbox="607 783 1362 810">2. Select the Parking Lots tab and click on the Configure button.<li data-bbox="607 821 1008 856">3. Specify the endpoint's E.164 alias.
Route Points	<p data-bbox="607 873 1362 1020">Displays route points managed by the CSTA Gatekeeper. Route points are virtual endpoints that you set up using the Configuration Program. When a call reaches a configured route point, the CSTA Gatekeeper passes a route request to the CTC server and waits for a response.</p> <p data-bbox="607 1031 862 1058">To set up a route point:</p> <ol data-bbox="607 1077 1362 1245" style="list-style-type: none"><li data-bbox="607 1077 1362 1140">1. Configure the endpoint's E.164 alias by selecting the E164 Aliases tab (see step 2 and Table 2–1).<li data-bbox="607 1150 1362 1178">2. Select the Route Points tab and click on the Configure button.<li data-bbox="607 1188 1362 1245">3. Specify the endpoint's E.164 alias (for example, its phone number). <p data-bbox="607 1262 1362 1318">If you want the CSTA Gatekeeper to manage route points monitored by the CTC server, you must set up each of them in this way.</p>

4. The basic configuration is now complete. You can either exit the Configuration Program or configure the CSTA Gatekeeper further by setting:
 - Additional optional values, such as, the maximum number of clients that can register with the CSTA Gatekeeper. You set these by selecting the Current Settings tab. For details, see Section 2.9.3.
 - Advanced values for networks that include more than one CSTA Gatekeeper. By selecting the Multi Gatekeeper Settings tab, you can set values that enable you to set up alternate gatekeepers and remote gatekeepers. For details, see Section 2.9.4.

To exit the Configuration Program, select **Exit** from the **File** menu.

2.9.3 Displaying Current Settings and Configuring Optional Values

The **Current Settings** tab contains optional values you can set for the CSTA Gatekeeper, along with details of current use:



For example, you can specify the maximum number of client systems that can register with the CSTA Gatekeeper. The Current Settings tab displays both the maximum you have set and the number of client systems currently registered.

2.9.3.1 Displaying Current Settings

Select the **Current Settings** tab. This displays optional values you can configure, plus details of:

- **Current Users**—The number of endpoints currently registered with the CSTA Gatekeeper.

- **Current Calls**—The number of calls currently handled by the CSTA Gatekeeper. These include connected calls, calls waiting to be established and calls in the process of disconnection.
- **Current Bandwidth**—The total data rate for all calls currently handled by the CSTA Gatekeeper.

To get the latest settings and values, do one of the following:

- Click on the **Get Settings** button.
- Select **Refresh** from the **View** menu.

2.9.3.2 Configuring Optional Values

To set the Maximum Users, Maximum Calls, Maximum Bandwidth, Registration Time to Live (TTL) or Prefix Precedence:

1. Select the **Current Settings** tab.
2. Click on the **Configure** button and specify the information shown in Table 2–3.

Table 2–3 Configuration Program Optional Current Settings

Setting	Description
Maximum Users	<p>The maximum number of endpoints that can register with the CSTA Gatekeeper.</p> <p>When the maximum is reached, the CSTA Gatekeeper rejects registration requests and users at the unregistered endpoints are not able to receive or make calls using the CSTA Gatekeeper.</p> <p>You can set up one or more alternate gatekeeper to receive calls when the maximum has been reached on the CSTA Gatekeeper. For more information, see Section 2.9.4.</p>
Maximum Calls	<p>The maximum number of calls that the CSTA Gatekeeper can handle.</p> <p>When the maximum is reached, new call requests are rejected by the CSTA Gatekeeper.</p>
Maximum Bandwidth	<p>The maximum bandwidth handled by the CSTA Gatekeeper.</p> <p>When the maximum is reached, calls are rejected by the CSTA Gatekeeper.</p>

Table 2–3 Configuration Program Optional Current Settings (Continued)

Setting	Description
Registration TTL	The Registration Time to Live displays the interval (in seconds) in which each endpoint must re-register with the CSTA Gatekeeper. Using this setting, you can control how often the CSTA Gatekeeper monitors whether an endpoint is still available.
Prefix Precedence	<p>Enable this setting and, when the CSTA Gatekeeper receives a call, it searches for a prefix match in preference to a full alias match as a destination for the call.</p> <p>For example, if a gateway registers with prefix 9, the CSTA Gatekeeper routes any calls to aliases that begin with 9 to the gateway. So, if the CSTA Gatekeeper receives a call to 9123, it routes the call to the gateway and not to the terminal registered as 9123.</p> <p>In the same example, if the CSTA Gatekeeper receives a call to 7123, 7 is not a registered prefix so the CSTA Gatekeeper routes the call to the terminal registered as 7123.</p> <p>Prefixes are set up on gateways to enable them to access appropriate telephony networks. For example, the prefix 9 could be set up on an H.323 gateway so that it can be used for calls made through a Public Switched Telephone Network (PSTN). When an H.323 gateway registers with the CSTA Gatekeeper, it must specify both its alias and any prefixes as part of the registration process.</p>

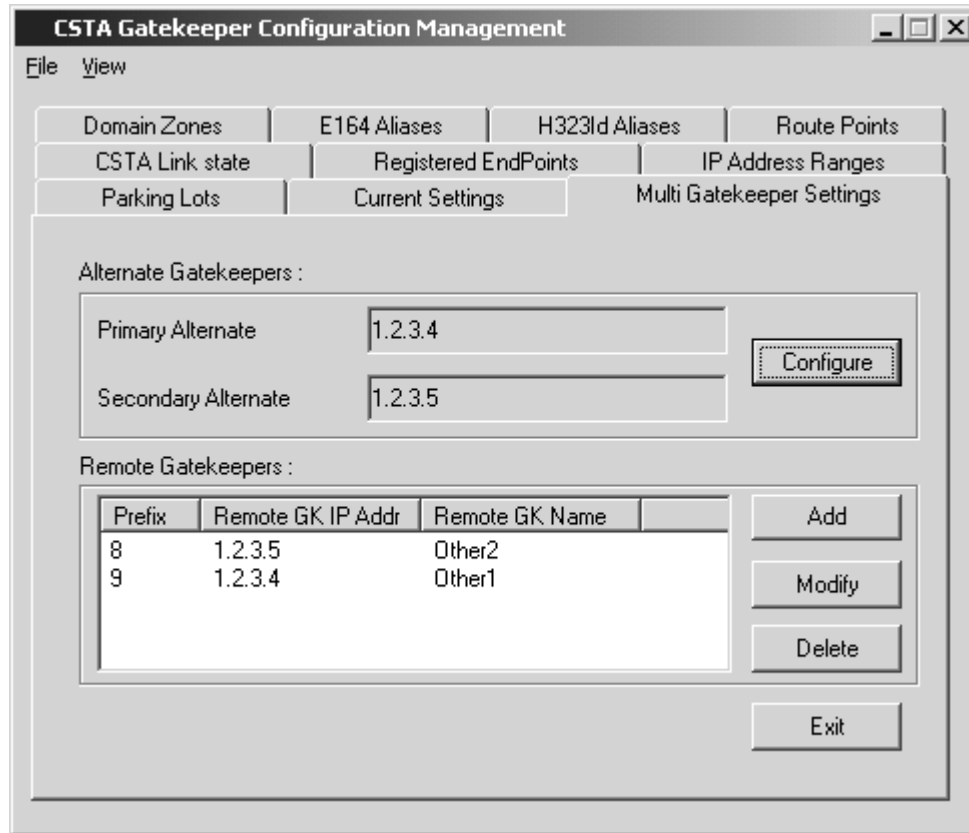
2.9.4 Configuring Alternate and Remote Gatekeepers

If you are using the CSTA Gatekeeper with other gatekeepers in the same IP network, you can optionally set up:

- **Alternate Gatekeepers**—You can specify up to two alternate gatekeepers that an endpoint can use if it fails to register with the CSTA Gatekeeper.
- **Remote Gatekeepers**—You can set up a list of remote gatekeepers that the CSTA Gatekeeper queries when it cannot find a match for a destination alias or prefix in its own list of registered endpoints.

You configure both alternate gatekeepers and remote gatekeepers by selecting

the **Multi Gatekeeper Settings** tab:



Sections 2.9.4.1 and 2.9.4.2 describe these configuration settings in more detail.

2.9.4.1 Alternate Gatekeepers

An alternate gatekeeper is a gatekeeper that endpoints can use if the CSTA Gatekeeper becomes unavailable or if the CSTA Gatekeeper rejects registration requests because the **Maximum Users** setting has been reached (for details of this setting, see Table 2-1).

How do Endpoints Receive Details of Alternate Gatekeepers?

When an endpoint sends a registration request to the CSTA Gatekeeper, the CSTA Gatekeeper includes a list of alternate gatekeepers in its response to the endpoint.

The list of up to two alternate gatekeepers is taken from the Alternate

Gatekeeper settings you enter in the Configuration Program.

The CSTA Gatekeeper sends the list of alternate gatekeepers to the endpoint when it receives the endpoint's registration request, even if the request is rejected. To do this, the CSTA Gatekeeper must be running and able to communicate with an endpoint so that it can send the list as part of its response.

When an endpoint has this information, it can store it (for example, in its Windows registry) so that it knows which alternative gatekeeper(s) to use when it cannot communicate with the CSTA Gatekeeper. For more information, and to find out whether an endpoint supports storing this data, check the software and/or documentation for the endpoint.

Using the Configuration Program, you can specify both a primary and secondary alternate gatekeeper so that an endpoint can attempt to register with both when it cannot register with the CSTA Gatekeeper. The endpoint will attempt to re-register with the primary gatekeeper first, and, if that is unavailable, it will try to register with the secondary gatekeeper.

Setting Up an Alternate Gatekeeper

To set up one or more alternate gatekeepers:

1. Select the **Multi Gatekeeper Settings** tab.
2. Click on the **Configure** button and specify the information in Table 2–4.

Table 2–4 Alternate Gatekeeper Settings

Setting	Description
Primary Alternate	The first alternate gatekeeper that endpoints can use for re-registration. Enter an IP address or domain name.
Secondary Alternate	The secondary alternate gatekeeper that endpoints can use if registration with the primary alternate gatekeeper is not successful. Enter an IP address or domain name.

Section 1.4.2 provides an example of an IP network that includes alternate gatekeepers.

2.9.4.2 Remote Gatekeepers

A remote gatekeeper is a gatekeeper that is in the same IP network as the CSTA Gatekeeper and that may share call loading with the CSTA Gatekeeper. For more information, see Section 1.4.1.

You use the Configuration Program to set up a list of remote gatekeepers that

the CSTA Gatekeeper queries when it cannot find a match for a destination alias in its own list of registered endpoints. Using the list of remote gatekeepers, the CSTA Gatekeeper sends a request to each gatekeeper in turn that could possibly find a match for the alias.

For example, if the CSTA Gatekeeper receives a call for alias 7123 and 7123 is not registered with the CSTA Gatekeeper, the CSTA Gatekeeper:

1. Sends a request to the first remote gatekeeper listed in the Configuration Program that satisfies the requirements for receiving the call. For example, if the remote gatekeeper manages endpoints with the prefix 7. The request prompts the remote gatekeeper to check its list of registered endpoints for 7123.
2. If the remote gatekeeper does not have an endpoint registered as 7123, the CSTA Gatekeeper sends a request to the next remote gatekeeper listed that satisfies the criteria for receiving the call. For example, a remote gatekeeper that has no prefix restriction. Remote gatekeepers that do not satisfy the criteria (for example, a gatekeeper that accepts calls with the prefix 9) are ignored.
3. If the second gatekeeper cannot match the alias, the CSTA Gatekeeper continues to poll valid gatekeepers. If a match is not found, the CSTA Gatekeeper rejects the call.

Setting Up a Remote Gatekeeper

To set up a remote gatekeeper:

1. Select the **Multi Gatekeeper Settings** tab.
2. Click on the Remote Gatekeepers **Add** button and specify the information in Table 2–5.

Table 2–5 Remote Gatekeeper Settings

Setting	Description
Prefix	<p>The prefix identifies the set of E.164 aliases managed by the remote gatekeeper. For example, the prefix 7 indicates that the remote gatekeeper manages aliases that begin with 7 and the CSTA Gatekeeper will send requests to the remote gatekeeper only for these aliases.</p> <p>The default setting for Prefix is blank. This means that the CSTA Gatekeeper sends requests to the remote gatekeeper to check for any aliases that the CSTA Gatekeeper has not been able to match.</p>

Table 2–5 Remote Gatekeeper Settings (Continued)

Setting	Description
Remote Gatekeeper IP/Domain	The IP address or domain name for the remote gatekeeper. You must specify a value in this field. For example: 146.152.189.5 or GK1.intel.com
Remote Gatekeeper Name	An optional name for the remote gatekeeper that you can use to reference it. Specify any name of up to 64 characters.

2.9.5 Deleting and Resetting Configuration Parameters

The settings you specify using the Configuration Program are stored in the registry on your Windows NT, Windows 2000 or Windows XP system.

Using the **Delete** button on the **IP Address Ranges, Domain Zones, E.164 Aliases, H.323Id Aliases** and **Multi Gatekeeper Settings** windows, you can remove a selected entry. The corresponding setting is removed from the registry.

Using the **Reset** button, you can remove all of the configured **IP Address Ranges, Domain Zones, E.164 Aliases** or **H.323Id Aliases** settings from the registry and start a new list of configured endpoints. The **Reset** button resets only those settings displayed in the current window.

2.10 Removing and Reinstalling the CSTA Gatekeeper

To remove the CSTA Gatekeeper, complete the following:

1. Open the Add/Remove Programs dialog box from Control Panel.
2. Select the **Install/Uninstall** tab.
3. Select **CSTA Gatekeeper** from the displayed list of software.
4. Click on the **Add/Remove** button.

If, after removing the software, you want to reinstall:

1. Reboot the CSTA Gatekeeper system
2. Follow the procedures in Section 2.5 to install the software

2.11 Event Logging

Event logging is a feature which keeps a record of all system events for diagnostic purposes. The CSTA Gatekeeper provides events that enable you to monitor use of the CSTA Gatekeeper software and its communication with the CTC server.

Events inform you of what is happening on the CSTA Gatekeeper. For example, the CSTA Gatekeeper logs an event to indicate when the software is started or when the connection to the CTC server has been shut down. Events can also indicate when there may be problems. For example, the CSTA Gatekeeper logs an event if there is no hardware license key attached.

Section 2.11.1 shows how to start event logging. Section 2.11.2 shows the events logged by the CSTA Gatekeeper. If an event is logged, it will be listed as either an information, warning or error event.

2.11.1 Starting the Event Logging Application

To display CSTA Gatekeeper events, follow the procedure for your CSTA Gatekeeper system, as listed below. Look for messages with **CSTA Gatekeeper** as the source.

Windows NT

1. From the **Start** menu select:
Programs → Administrative Tools → Event Viewer
2. To display application events, select **Application** from the **Log** menu.

Windows 2000

1. In the Control Panel, select Administrative Tools
2. Select Event Viewer
3. To display application events, select **Application Log** from the menu on the left.

2.11.2 CSTA Gatekeeper Events

Table 2–6 shows the events logged by the CSTA Gatekeeper.

Table 2–6 CSTA Gatekeeper Events

Event	Description
cgkConnClosed	The connection between the CSTA Gatekeeper and CTC server has been shut down. Typically, shutdown is initiated by the CTC server.
cgkConnRejected	The CSTA Gatekeeper supports one connection to a CTC server and a second connection was requested. The CSTA Gatekeeper rejected the request.
cgkConnUp	The connection between the CSTA Gatekeeper and CTC server is up and running.
cgkIntLockErr	An internal software error occurred. Report the problem to Intel.
cgkInvalidDeviceID	The CSTA Gatekeeper cannot identify the specified alias because it does not recognize its format. For details of alias formats, see Section 3.2.
cgkNoLicenseKey	The NCCS hardware license key is not attached to the parallel port on the CSTA Gatekeeper system. For more information, see Section 2.4.1.
cgkReinsertKey	The NCCS hardware license key has been removed. Please re-insert the key. For more information about the hardware license key, see Section 2.4.1.
cgkServiceError	The CSTA Gatekeeper service could not be started. Check the CSTA Gatekeeper software installation and, if necessary, reinstall the software.
cgkShutdown	The CSTA Gatekeeper service has been shut down.
cgkStarted	The CSTA Gatekeeper service has been successfully started.
cgkWrongLicenseKey	The wrong hardware license key has been detected on the parallel port. Attach the NCCS license key. For more information, see Section 2.4.1.

Configuring and Registering Endpoints

3.1 Configuring Endpoints

When you configure your H.323 client software for use with the CSTA Gatekeeper, make sure that:

- 'Fast Connect' and 'Tunneling' options are disabled.
- The software is configured to use a gatekeeper and that you specify the IP address for the CSTA Gatekeeper as necessary.
- Alias names follow the conventions described in Section 3.2.

3.2 Format of Endpoint Aliases

All endpoint aliases must have a specific format so that the CSTA Gatekeeper can identify them.

The CTC server and CSTA Phase II do not support values that could identify an alias as an IP address, domain name, E-mail address, telephone number, URL or any other type of alias, so the CSTA Gatekeeper must determine the alias type from its format.

The CSTA Gatekeeper compares the alias format against the definitions in Sections 3.2.1 to 3.2.6. For example, if you configure an endpoint with the alias "www.alias.name", the CSTA Gatekeeper can identify it as a URL. However, if you configure an endpoint with an H.323 identifier of 789, the CSTA Gatekeeper would incorrectly determine the alias to be a telephone number.

Refer to Sections 3.2.1 to 3.2.6 for details of each alias you may want to use with the CSTA Gatekeeper.

3.2.1 IP Address

An IP address must contain at least one digit between 0 and 9 and at least one point. For example: 12.23.34.45. It must not contain any other characters. If the format of the alias does not match an IP address, the CSTA Gatekeeper checks to see if it is a domain name.

3.2.2 Domain Name

A domain name must contain at least one point and can contain:

- Lowercase/uppercase alphabetic characters (a to z, A to Z)
- Digits between 0 and 9
- Dashes (-)

For example: diallogic.com

A domain name cannot contain underscores, @, *, # or any other characters except for those listed. The first and last characters must not be dashes, and the name must not start with the letters 'www'. The maximum length for domain names is 26 characters.

If the format of the alias does not match a domain name, the CSTA Gatekeeper checks to see if it is an E-mail address.

3.2.3 E-mail Address

An E-mail address must contain the @ character and can contain:

- Lowercase/uppercase alphabetic characters (a to z, A to Z)
- Digits between 0 and 9
- Dashes (-)
- Points (.)
- Underscores (_)

For example: user@intel.com

An E-mail address cannot contain any other characters such as * or #.

If the format of the alias does not match an E-mail address, the CSTA Gatekeeper checks to see if it is a telephone number.

3.2.4 Telephone Number

A telephone number must contain at least one digit between 0 and 9 and can contain the characters * and #. For example: 7890. It cannot contain any other characters. If the format of the alias does not match a telephone number, the CSTA Gatekeeper checks to see if it is a URL.

3.2.5 URL

A URL must start with the characters 'www' and must contain at least one

point. It can also contain:

- Lowercase/uppercase alphabetic characters (a to z, A to Z)
- Digits between 0 and 9
- Dashes (-)

For example: www.intel.com

A URL cannot contain any other characters and the last character cannot be a dash (-).

If the format of the alias does not match a URL, the CSTA Gatekeeper determines that it is a generic H.323 identifier.

3.2.6 Generic H.323 Identifier (H323Id)

If the CSTA Gatekeeper cannot match the alias to other criteria, the CSTA Gatekeeper determines that the alias is an H.323 identifier.

For example: 7acb98.

3-4 Configuring and Registering Endpoints

A

Additional Information for CTC Applications

This appendix contains additional information you may require when you use the CSTA Gatekeeper with a CTC application. For more information about the CTC functions described in this appendix, refer to the *CT Connect C Programming Guide* or the *CT Connect for the Java™ Platform Programming Reference*.

A.1 Monitoring and Controlling URLs and E-mail Addresses

CTC applications can monitor and control endpoints registered with:

- E.164 aliases
- Domain zones
- IP addresses
- URLs
- E-mail addresses
- H.323 ID aliases

For URLs and E-mail addresses, the following restrictions apply:

- You cannot use the CSTA Gatekeeper Configuration Program to configure URLs or E-mail addresses. However, if the H.323 endpoint registers using a URL or E-mail address from within a configured IP address range, the CSTA Gatekeeper accepts the registration request when the H.323 client software is started.
- A CTC application cannot assign a channel to an unregistered URL or E-mail address. If an application attempts to do so, CTC returns a `ctcObjectNotKnown` error. The URL or E-mail address must be registered with the CSTA Gatekeeper before you can assign a channel to it.

A.2 Endpoint Registration and Assigning Channels

Generally, an endpoint must register with the CSTA Gatekeeper before a CTC application assigns a channel to that endpoint. If your CTC application returns a

ctcObjectNotKnown condition value on assigning a channel, it indicates that the endpoint has not registered with the CSTA Gatekeeper for the first time.

E.164 aliases and H.323 ID aliases are exceptions. When you have configured an E.164 or H.323 ID alias using the CSTA Gatekeeper Configuration Program, your CTC application can assign a channel before the alias registers with the CSTA Gatekeeper for the first time. On registration, the CSTA Gatekeeper generates a CSTA Back in Service event. In CTC, this maps to a ctcK_BackInService event.

Once an endpoint has registered for the first time with the CSTA Gatekeeper, your CTC application can continue to monitor it even if it unregisters and re-registers with the CSTA Gatekeeper a number of times. Your CTC application does not need to deassign and assign a channel to the endpoint each time. This applies to all supported types of endpoint.

The CSTA Gatekeeper generates CSTA events in the following ways:

- On starting up the H.323 client software, the endpoint requests registration with the CSTA Gatekeeper. When the CSTA Gatekeeper accepts the registration request, it generates the CSTA Back in Service event for the endpoint.
- When the H.323 client software is stopped, the endpoint is unregistered and the CSTA Gatekeeper generates the CSTA Out of Service event.

A.3 Party Information (ANI, CLID, DNIS)

If available, the CSTA Gatekeeper provides Dialed Number Identification Service (DNIS) digits, Calling Line Identification (CLID) or Automatic Number Identification (ANI), to CTC when it receives a call from a gateway.

A.3.1 Party Information Returned in CSTA Events

The CSTA Gatekeeper returns the DNIS, CLID or ANI information to CTC in CSTA call and route request events:

- In CSTA call events, ANI or CLID is returned in the calling device field and DNIS in the called device field.
- In CSTA route request events, ANI or CLID is returned in the calling device field and DNIS in the current route field.

This information is returned in CTC call events and route events as party information. For details of these events, refer to the *CT Connect C Programming Guide* or the *CT Connect for the Java™ Platform Programming Reference*.

If available, the CSTA Gatekeeper returns ANI, CLID or DNIS information for the following events:

- Originated
- Delivered
- Established
- Queued
- Route Request

DNIS can also be returned for the Failed Event.

However, the CSTA Gatekeeper cannot provide DNIS, CLID or ANI when:

- The CSTA Gatekeeper receives a call from a gateway and your CTC application redirects the call to another device using the Deflect Call, Consultation Call, Route Select, Single Step Conference, or Single Step Transfer services.

Even if the CSTA Gatekeeper provides DNIS, CLID or ANI to your CTC application when it receives the call, it cannot provide this information when your application sends the call to the new destination.

- Your CTC application initiates a call (using the Make Call service) and the CSTA Gatekeeper routes the call through a CSTA gateway.

To work around this, you can use CTC to handle the party information as private data. Section A.3.2 describes how to do this.

A.3.2 Using CTC Private Data for Party Information

Using CTC private data, you can specify party information for a call before you actually make the call or redirect the call.

C Applications

For a CTC application written in C, use the `ctcCstaSetPrivateData` routine to set `ctcPrivateDataType` to `ctcK_PrivRawByManufacturer`, and set the `ctcPrivateDataRaw` data fields to the values shown in Section A.3.2.1. For more information about the `ctcCstaSetPrivateData` routine, refer to the *CT Connect C Programming Guide*.

Java Applications

For a CTC application written in the Java programming language, use the `setPrivateData` method for the CSTA device channel object to pass a `CtcCstaPrivRawByManufacturer` object. Set the fields for the `CtcCstaPrivRawByManufacturer` constructor to the values shown in Section A.3.2.1. For more information about the `CtcCstaPrivRawByManufacturer` object,

refer to the *CT Connect for the Java™ Platform Programming Reference*.

A.3.2.1 Private Data Fields

Set the private data fields to these values:

Manufacturer String:

1.1.1.1.2

Data length:

Specify the length of data you want to pass. If your CTC application is written in the Java programming language, you do not need to pass this value.

Data:

Specify the data in the following format, omitting the square brackets:

$$30[xx][yy][NumberType][NumberingPlan][Number\dots]$$

where:

- *xx* is the length of the remaining data (from *yy* to the end of *Number\dots*). The maximum length you can specify is 64 bytes.
- *yy* is a Q.931 value that identifies whether the party information is associated with the calling party or the called party. Specify 00 for a calling party or 01 for a called party.

Q.931 messages are used for H.323 call signaling.

- *NumberType* is one of the following (shown in hexadecimal):

0x00	Unknown
0x01	International number
0x02	National number
0x03	Network specific number
0x04	Subscriber number
0x05	Abbreviated number

For more information about these values, refer to the *ITU-T Recommendation Q.931* specification.

- *NumberingPlan* is one of the following (shown in hexadecimal):

0x00	Unknown
0x01	ISDN/telephony numbering plan (Recommendation E.164)
0x03	Data numbering plan (Recommendation X.121)
0x04	Telex numbering plan (Recommendation F.69)
0x08	National standard numbering plan
0x09	Private numbering plan

For more information about these values, refer to the *ITU-T Recommendation Q.931* specification.

- *Number* is the remaining characters containing the DNIS, CLID or ANI.

For example:

300D00020130383030313233343536

where:

- 0D is the length of the data.
- 00 indicates that the data is a CLID
- 02 indicates that the number type is a national number
- 01 indicates that the numbering plan is ISDN/telephony
- 30383030313233343536 is the ASN1 encoding for number 0800 123456

A.4 Using CTC to Monitor Outbound Calls on a Gateway

To monitor outbound calls made through a gateway, a CTC application can assign a channel to:

- The gateway's E.164 alias. By assigning to the gateway's alias, the CTC application will receive events for all outbound IP calls made through the gateway.

Before you assign the channel from the CTC application, you must configure the E.164 alias (see Table 2-1, page 2-11) and the gateway must use the alias to register with the CSTA Gatekeeper.

- The gateway's prefix. Typically, a prefix (for example, 9) on a gateway provides access to a PSTN from the IP telephony network. By assigning to the gateway's prefix, your CTC application can monitor outbound calls made using that prefix.

Before you assign the channel from the CTC application, you must configure the prefix as an E.164 alias (see Table 2–1, page 2-11) and the gateway must supply the prefix when it registers with the CSTA Gatekeeper.

Note that the CTC application can only monitor outbound calls at the gateway; it cannot call CTC functions to control calls (for example, `ctcHangupCall`).

A.5 Using CTC to Monitor Inbound Calls on a Gateway

To monitor inbound calls received by a gateway from a PSTN, a CTC application can assign a channel to:

- The gateway's E.164 alias. By assigning to the gateway's alias, the CTC application will receive events for all inbound IP calls made through the gateway.

Before you assign the channel from the CTC application, you must configure the E.164 alias (see Table 2–1, page 2-11) and the gateway must use the alias to register with the CSTA Gatekeeper.

- A gateway's source alias. Source aliases are configured on the gateway to identify the source of the call within the IP network. They do not necessarily identify the calling party, only an entry point to the IP network. The gateway allocates the alias before it distributes the call to a destination within the IP network.

A CTC application can monitor calls that the gateway distributes from that alias by assigning a channel to a source alias. Complete the following:

1. Configure the E.164 alias (see Table 2–1, page 2-11) for the source.
2. Configure the alias as a route point (see Table 2–2, page 2-12) to identify it as a virtual endpoint.
3. Use your CTC application to assign a channel and monitor the alias. Although you configure the alias as a route point in the CSTA Gatekeeper Configuration Program, your CTC application must assign to the alias as a DN.

Note that the CTC application can only monitor inbound calls at the gateway; it cannot call CTC functions to control calls (for example, `ctcHangupCall`).

Index

C

- Configuration Program
 - delete button, 2-19
 - Domain Zones, 2-9
 - E.164 Aliases, 2-9
 - IP Address Ranges, 2-9
 - reset button, 2-19
 - starting, 2-7
- CSTA events
 - supported, 1-11
- CSTA Gatekeeper and CTC, 1-4
 - definition, 1-1
 - installing, 2-4
 - removing software, 2-19
 - services, 1-2
- CSTA Link State, 2-11, 2-12, 2-14, 2-17, 2-18
- CSTA services
 - supported, 1-9
- CTC server
 - configuring, 2-8
- CTCGK_MGMT.BAT, 2-5

D

- Deleting
 - configuration parameters, 2-19

- Domain Zones, 2-11, 2-12, 2-14, 2-17, 2-18

E

- E.164 Aliases, 2-11, 2-12, 2-14, 2-17, 2-18

I

- Installation
 - privileges, 2-2, 2-4
 - reinstalling, 2-19
 - requirements, 2-2
- IP Address Ranges, 2-11, 2-12, 2-14, 2-17, 2-18

L

- Link to CTC server
 - shut down, 2-8
- Local address, 2-4
- Local IP address, 2-8

P

- Paths file, 2-5
- Port number, 2-4, 2-8
 - changing, 2-8

R

- Registered Endpoints, 2-11, 2-12, 2-14, 2-17, 2-18
- Registry
 - resetting and deleting values, 2-19
- Release notes
 - location of README.TXT, 2-5
- Resetting
 - configuration parameters, 2-19

Route Points, 2-11, 2-12, 2-14, 2-17, 2-18

W

Windows 2000
server, 2-2

Windows NT
server, 2-2
Windows NT Server, 2-2
Windows NT Workstation, 2-2
Windows XP
server, 2-2